

제53회 2020 온라인 춘계학술발표대회 논문집

일 자 2020년 5월 29일(금) ~ 30일(토)

주 최  사단법인 한국정보처리학회
KIPS Korea Information Processing Society

협 찬  아이티센 ITcen  삼성SDS  Comtec Systems Co., Ltd.  Metanet DT
메타넷대우정보

 울포랜드  kpc 한국생산성본부
KOREA PRODUCTIVITY CENTER  KCC정보통신 (무순)

학술대회 홈페이지

www.manuscriptlink.com/society/kips/conference/2020spring



당신이 오늘 만날 수 있는 혁신

Innovation & Reality

4차산업 플랫폼
비즈니스 전문그룹

cen 아이티센그룹
ITCENGROU

cen 아이티센 KOSDAQ

cen 소프트센 KOSDAQ

cen 굿 KOSDAQ

cen 센 KOSDAQ

cen 시큐센 KOSDAQ

omtec (주) 콤텍시스템 KOSPI

omtec (주) 콤텍정보통신 비상장

GOLD 한국금거래소 비상장



글로벌 통합 4PL 물류 서비스의 새로운 기준

Cello 물류서비스는 글로벌 물류 네트워크 및 최첨단 IT 시스템을 기반으로 해상/항공/육상 운송, 창고 관리 및 통관 처리 등의 물류실행 서비스뿐 아니라 고객사 물류혁신 컨설팅을 포함하는 종합 물류 서비스를 제공합니다. 글로벌 물류 전문성을 보유한 전문 컨설턴트와 최신 IT 인프라를 활용하여 귀사의 물류 운영 성과를 극대화 하세요.



지금 바로 Cello에 대해 더 자세히 알아보세요



www.samsungsds.com
www.cellologistics.com
Cello@Samsung.com

SAMSUNG SDS
Realize your vision

성공하는 기업의 디지털 혁신 메타넷이 함께 만듭니다

컨설팅으로 변화를 디지털로 혁신을 테크놀로지로
미래를 앞당기고 오퍼레이션으로 운영의 효율을 높입니다.

디지털 비즈니스 플랫폼, 메타넷

Consulting | Digital | Technology | Operations



메타넷글로벌 • 메타넷티플랫폼 • 메타넷애자일 • 메타넷핀테크 • 메타넷알피에이 • 메타넷엠플랫폼
메타넷대우정보 • 유티모스트INS • 넥스젠NCG • 엔코아 • IGM세계경영연구원 • 빌포스트 • RDMK • 코마스

“공간정보로 연결하고,
공유하고, 볼 수 있는 세상”

올포랜드가
함께 만들어 가겠습니다.



사업분야



GIS솔루션

map prime CLOUD · OCEAN · 2D/3D GIS



SI

국토/해양 정보화, 환경·교통 서비스 등



DB

국토/해양 GIS, 정밀도로지도, 드론촬영 등

<http://www.all4land.com>

서울시 금천구 가산디지털1로 145 에이스하이엔드타워 3차 1401호

T. 02-855-5724 F. 02-857-5746



실무에서 빛나는 나의 가치 한국생산성본부가 만들어 드립니다.

IT자격, 그래픽자격, 경영자격, CAD, 국제자격 등
연간 60만 명 이상이 실무중심형 KPC자격과 함께 합니다.

2020년 KPC자격 정기시험 일정

자격명	분류	등급	1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월
정보기술자격(ITQ)	국가공인	A,B,C	11	8, 23	14	11	9, 24	13	11	8, 23	12	10	14, 29	12
GTQ(그래픽기술자격)		1, 2, 3	18	22	28	25	23	27	25	22	26	24	28	26
ERP회계정보관리사		1, 2	18		28	25	23		25		26		28	
ERP인사정보관리사		1, 2	18		28	25	23		25		26		28	
ERP생산정보관리사		1, 2	18		28	25	23		25		26		28	
ERP물류정보관리사		1, 2	18		28	25	23		25		26		28	
SMAT(서비스경영자격)		1, 2, 3		8		11	24	13		8		10	29	12
IEQ지도사(인터넷윤리자격)		1, 2, 3					23			22			28	
ICDL(국제컴퓨터활용)	국제자격	모듈	18	22	28	25	23	27	25	22	26	24	28	26
GTQi(그래픽기술자격 일러스트)	민간자격	1, 2, 3		22		25		27		22		24		26
GTQid(그래픽기술자격 인디자인)		1, 2, 3	18				23				26		28	
SW코딩자격(SWC)		1, 2, 3	18	22	28	25	23	27	25	22	26	24	28	26
CAD실무능력평가		1, 2	11	8, 22	14	25	9, 23, 24	13	11, 25	8, 22	12	10	14	12, 26

※GTQ3급(민간자격), IEQ관리사1, 2급(민간자격) / 수시시험은 사전 협의 / SW코딩 1급 일정은 홈페이지에서 확인

목 차


▶ : 학부생 논문

컴퓨터시스템 및 이론

- 001 자바 기반의 스프링 Web MVC와 WebFlux 성능 분석 KIPS_C2020A0050
..... 정명교*, 서태원(고려대학교) • 2
- 002 스마트 더스트 환경을 위한 위치 기반 데이터 축소 시스템 설계 KIPS_C2020A0056
..... 박준수*, 박기현(계명대학교) • 5
- 003 스마트 컨트랙트를 활용한 공유숙박 서비스 KIPS_C2020A0091
..... ▶ 유지성*, 김제인, 서승현(한양대학교) • 9
- 004 적응적 상관도를 이용한 주성분 분석에 관한 연구 KIPS_C2020A0168
..... 고명숙*(부천대학교) • 13

병렬 및 분산컴퓨팅




- 005 다기관 임상연구를 위한 의료 데이터 셋 관리 시스템 KIPS_C2020A0069
..... 이충섭*, 김승진, 김지언, 노시형(원광대학교), 김태훈, 윤권하, 정창원(원광대학교, 원광대학교병원) • 16
- 006 KVM 가상머신에서 도커를 사용하는 시스템의 호스트 메모리 부하에 따른 task 처리 성능 분석
KIPS_C2020A0077
..... 장용현*, 이재학, 유현창(고려대학교) • 20
- 007 Docker Swarm에서 컨테이너간의 메모리 자원에 대한 성능 간섭 측정 KIPS_C2020A0078
..... 정진원*, 이재학, 유현창(고려대학교) • 24
-  008 응용 프로그램 특성 분석 기반 스케줄링 최적화 기법의 확장성 연구 KIPS_C2020A0133
..... 최지은*, 박근철, 노승우, 박찬 열(한국과학기술정보연구원) • 28
- 009 실시간 데이터 분석을 위한 컨테이너 기반 가상화 성능에 관한 연구 KIPS_C2020A0144
..... ▶ 최보아*, 한재덕, 오다솜, 박현국, 김현아(대구가톨릭대학교),
..... 서민관(티쓰리큐㈜), 이종혁(대구가톨릭대학교) • 32

010	모바일 결제 및 정보제공 플랫폼을 활용한 결식아동 급식지원 사업 개선 제안 KIPS_C2020A0019	▶ 전현지*(삼육보건대) • 37
011	사용자의 활동성을 장려하는 AR 콘텐츠 게임 KIPS_C2020A0037	▶ 김다은*, 배민주, 유채현, 이유진, 박수이, 강승석(서울여자대학교) • 41
012	MWSN에서 채널 및 타임 슬롯 공동 스케줄링 데이터 집계를 위한 제안 계획 : 알고리즘 설계 KIPS_C2020A0039	Vi Van Vo*(성균관대학교), 김문성(서울신학대학교), 추현승(성균관대학교) • 44
013	추가적인 백업 가상 네트워크 기능 배치 없이 서비스 체인의 생존성을 보장하는 상호보완적 백업 시스템 KIPS_C2020A0047	이도경, 장영훈*, 샤이드무함마드라자(성균관대학교), 김문성(서울신학대학교), 추현승(성균관대학교) • 47
	014 블루투스 비콘을 사용한 고객 관리와 결제 플랫폼 서비스 KIPS_C2020A0049	고혁준*(고려대학교), 한성수(강원대학교), 전유부(순천대학교), 정창성(고려대학교) • 49
015	만물 접속 네트워크의 소셜 그룹 관리를 이용한 블록체인 프로토콜 운영 방안 KIPS_C2020A0053	김수연*(계명대학교), 강현국(고려대학교) • 52
016	5G 네트워크에서 기계학습 기반 트래픽 예측을 통한 네트워크 슬라이싱 자원 예약 기법 KIPS_C2020A0063	이필원, 이아름*, 박수용, 신용태(숭실대학교) • 56
017	Apache Kudu와 Impala를 활용한 Lambda Architecture 설계 KIPS_C2020A0065	황윤영*, 이필원, 신용태(숭실대학교) • 60
018	대용량 스토리지 기반의 데이터 전송 노드 클러스터 설계 및 구축 KIPS_C2020A0082	홍원택*, 안도식, 이재국(한국과학기술정보연구원) • 63
	019 비콘과 홍채인식 기반의 의료진 신분확인 시스템 제안 KIPS_C2020A0087	▶ 임세진*, 권혁동, 서화정(한성대학교) • 66
020	무선 센서 네트워크에서 장애 검출을 위한 결합 주성분분석과 적응형 임계값 KIPS_C2020A0119	Thien-Binh Dang, Vi Van Vo*, Duc-Tai Le(성균관대학교), Moonseong Kim(서울신학대학교), Hyunseung Choo(성균관대학교) • 69
021	클라우드 환경에서 오토 스케일링이 가능한 센서 데이터 수집 시스템 설계 KIPS_C2020A0135	박수용*, 최수민, 신용태(숭실대학교) • 72
023	노인 일자리 플랫폼 개발에 관한 연구 KIPS_C2020A0158	▶ 김상오*, 공인복, 이혜임, 서정연, 한보현(상명대학교) • 77
024	도시 도로 환경에서의 적용 가능한 동적 군집주행에 관한 연구 KIPS_C2020A0170	최수민*, 박수용, 신용태(숭실대학교) • 80

사물인터넷

- 025 얼굴인식을 이용한 드론의 위치제어 구현 KIPS_C2020A0017
..... 권기환*, 짜오 차오란, 권지승, 김수연(부경대학교) • 84
- 026 차량 인포테인먼트 장치 통합관리 모듈 설계 및 개발 KIPS_C2020A0026
..... ▶ 이채현, 오현경, 박소연, 김성우*, 정중화, 고석주, 김재수(경북대학교), 김지인(주엠펜이오토크) • 87
- 027 VR 콘텐츠를 응용한 로잉머신 시스템의 설계 및 구현 KIPS_C2020A0032
..... ▶ 반현진, 윤다영, 김재립, 백세연, 이나영*, 장영현, 김정민(배화여자대학교) • 91
- 028 스마트홈 환경에서 AR기술을 활용한 슬립테크 제어 방법 KIPS_C2020A0041
..... ▶ 차성민*, 배수민, 박현주, 이재동(단국대학교) • 95
- 029 규칙엔진 기반 인터랙티브 디지털 사이니지 서비스 시스템 설계 및 구현 KIPS_C2020A0075
..... 신은규*, 정선태, 이주호(숭실대학교) • 99
- 031 환경 모니터링을 위한 EDA 기반 데이터 분석 KIPS_C2020A0137
..... 강윤희*(백석대학교), 조재혁(숭실대학교) • 107
- 032 자율주행차 서비스를 위한 차량 엣지 컴퓨팅 모델 연구 KIPS_C2020A0186
..... 윤주상*(동의대학교) • 109
- 033 LoRa 네트워크를 활용한 주차정보 서비스 시스템 설계 KIPS_C2020A0187
..... ▶ 김유찬*, 문남미(호서대학교) • 111

정보보호


- 034 적외선통신 암호화 연구 KIPS_C2020A0003
..... 김민철*, 서태원(고려대학교) • 116
- 035 원자력시설 핵심디지털자산에 대한 코드 난독화 적용에 관한 연구 KIPS_C2020A0009
..... 김상우, 김시원*, 변예은, 권국희(한국원자력통제기술원) • 120
-  036 코드기반암호를 활용한 IoT 환경 보안 프로토콜 설계 KIPS_C2020A0012
..... 장경배*, 심민주, 서화정(한성대학교) • 123
- 037 공동 현관 비밀번호 유출 방지를 통한 블록체인 기반의 안전한 배송 시스템 KIPS_C2020A0014
..... 김현지*, 권용빈, 최승주, 서화정(*한성대학교) • 127
- 038 가상화폐기반 P2P 전기자동차 전력거래 시스템 KIPS_C2020A0015
..... ▶ 한예지*, 신수정(전북대학교) • 131
- 039 오픈소스 보안 취약점 및 패치 현황 실시간 알림 시스템 KIPS_C2020A0016
..... ▶ 최지은*(덕성여자대학교), 구예림(경기대학교), 전선진(숭실대학교), 박우인(수원대학교), 이병희(네이버) • 135
- 040 개인정보보호를 위한 영상 암호화 아키텍처 연구 KIPS_C2020A0020
..... 김정석*(서울시립대학교, 에스케이텔레콤), 이재호(서울시립대학교) • 138

041	실시간 모니터링을 이용한 캐시 부채널 공격 탐지 프레임워크 KIPS_C2020A0023	▶ 임미옥*, 김수진, 신영주(광운대학교) • 142
042	블록체인을 활용한 공공기관 정보시스템에서의 개인 정보 유출 방지 시스템 제안 KIPS_C2020A0025	최승주*, 박재훈, 서화정(한성대학교) • 146
043	단일 부채널 전력 파형을 사용한 마이크로컨트롤러 상에서 소프트웨어 표절 탐지 KIPS_C2020A0028	김현준*, 장경배, 김경호, 서화정(한성대학교) • 150
044	정규표현식을 이용한 시스템 로그 분석 KIPS_C2020A0030	김홍경*, 이경현(부경대학교) • 154
045	사이버 전투 피해평가를 위한 긴급 CAS 임무 자산 스코어링 연구 KIPS_C2020A0038	김재근*, 김성중, 김국진, 이동환, 신동일, 신동규(세종대학교) • 157
046	8-bit AVR 프로세서 상의 Revised CHAM 어셈블리 최적 구현 KIPS_C2020A0042	권혁동*, 김현지, 박재훈, 심민주, 서화정(한성대학교) • 161
047	코사인 유사도 측정을 통한 행위 기반 인증 연구 KIPS_C2020A0044	▶ 김선웅*(인천대학교) • 165
048	독립된 데이터셋을 활용한 효율적인 딥러닝 기반 비프로파일링 부채널 분석 방안 KIPS_C2020A0045	▶ 김주환*, 문혜원, 김연재, 박아인, 한동국(국민대학교) • 169
049	IoT 환경에서 물리적 복제 방지 기술 기반 인증 프로토콜 취약점 분석 및 개선방안 제안 KIPS_C2020A0046	최재현*, 정익래(고려대학교), 변진욱(평택대학교) • 173
050	네트워크 패킷 레벨에서 알려진 실행 파일 식별 및 차단 연구 KIPS_C2020A0052	조용수*, 이희조(고려대학교) • 177
051	지터에 내성을 갖는 딥러닝 기반 부채널 분석 방안 KIPS_C2020A0059	▶ 김주환*, 김수진, 우지은, 박소연, 한동국(국민대학교) • 180
052	실시간 동영상에서의 인물 선별 송출 시스템 KIPS_C2020A0062	▶ 우채윤*, 박나형, 백지윤, 정유진, 김명주(서울여자대학교) • 184
053	원자력시설의 무선통신 사이버보안을 위한 접근통제 방안 연구 KIPS_C2020A0064	김상우*(한국원자력통제기술원) • 188
054	대학생들을 위한 블록체인 기반의 신뢰성 있는 중고 책 거래 플랫폼 구현 KIPS_C2020A0066	▶ 김윤채, 이지혜*, 조윤재, 김명주(서울여자대학교) • 191
 055	FSR Array 마우스 패드를 이용한 사용자 인증 시스템 KIPS_C2020A0085	▶ 권승호*, 김태연, 서승현(한양대학교) • 195
 056	시큐어 C 코딩 학습용 모바일 앱 개발 KIPS_C2020A0089	▶ 박지희*, 우지민, 조민지, 김명주(서울여자대학교) • 199
057	SDN 환경에서 DDoS 공격에 대한 방어 기법 KIPS_C2020A0090	지승훈*(한국방송통신대학교), 박지수(전주대학교), 손진곤*(한국방송통신대학교) • 203

058	개인정보 문서 노출과 가명정보 조합을 통한 개인정보 관련 피해 위험성 연구 KIPS_C2020A0093	▶ 김민주*(서울여자대학교), 김영은, 이준민, 이창현, 하정희(한국정보기술연구원), 정재완(광운대학교), 강대명, 김영철, 허원석(한국정보기술연구원) • 207
059	블록체인을 통한 키오스크 스마트 체크인 방식 제안 KIPS_C2020A0097	▶ 심민주*, 최승주, 서화정(한성대학교) • 211
060	블록체인 분산신원증명에 기반한 공적마스크 중복구매 확인 시스템에 대한 연구 KIPS_C2020A0101	노시완*, 장설아, 이경현(부경대학교) • 214
061	블록체인 기반의 디지털 신원증명 동향 KIPS_C2020A0104	▶ 이정현*, 서화정(한성대학교) • 218
062	로컬 특징 기반 글로벌 이미지를 사용한 CNN 기반의 악성코드 분류 방법 KIPS_C2020A0106	장세준*, 성연식(동국대학교) • 222
063	IoT 센서를 이용한 블록체인 기반 식품 공급망 개발 KIPS_C2020A0107	▶ 심재익*, 김왕록, 전미현, 오동의, 정병규, 신상욱(*부경대학교) • 224
064	Merging Collaborative Learning and Blockchain: Privacy in Context KIPS_C2020A0108	Sandi Rahmadika*, Kyung-Hyune Rhee(Pukyong National University) • 228
065	Empowering Blockchain For Secure Data Storing in Industrial IoT KIPS_C2020A0109	Muhammad Firdaus*, Kyung-Hyune Rhee(Pukyong National University) • 231
066	해킹메일 대응을 위한 기술 표준 분석 KIPS_C2020A0116	변예은*(한국원자력통제기술원) • 235
067	클라우드 하이퍼바이저 구조의 취약점 개선을 위한 고찰 KIPS_C2020A0125	김태우*, 석상기, 박종혁(서울과학기술대학교) • 238
068	확장성이 고려된 Bitcoin-NG 프로토콜 고찰 및 연구 KIPS_C2020A0128	▶ 김수현, 차정훈*, 박종혁(서울과학기술대학교) • 242
069	컨소시엄 블록체인을 이용한 내부자 이상행위 탐지의 관한 연구 KIPS_C2020A0142	▶ 최용철*, 이덕규(서원대학교) • 246
070	이종 장치간 전송 파일의 추적 정보 연구 KIPS_C2020A0145	▶ 조을한*(기전대학교), 김지선, 조태남(우석대학교) • 250
071	GRU를 활용한 악성코드 탐지의 관한 연구 KIPS_C2020A0150	▶ 류경근*, 최용철, 이덕규(서원대학교) • 254
072	사이버위협 동향 분석을 통한 내부망 대응 방안 KIPS_C2020A0152	변예은*(한국원자력통제기술원) • 258
 073	ARM TrustZone 기반 신뢰실행환경의 취약점과 방어기법에 대한 연구 KIPS_C2020A0157	유준승*, 서지원, 방인영, 백윤홍(서울대학교) • 260
074	클라우드 컴퓨팅 환경에서의 동형암호기술 적용에 대한 연구 KIPS_C2020A0160	장지원*, 남기빈, 조명현, 백윤홍(서울대학교) • 264
075	부분적 동형암호 HW 가속기 설계에 관한 연구 KIPS_C2020A0161	남기빈*, 장지원, 조명현, 방인영, 백윤홍(서울대학교) • 268

076	최근 퍼징 기법들과 발전에 관한 연구 KIPS_C2020A0162	전소희*, 이영한, 김현준, 백윤홍(서울대학교) • 272
077	Multi-Variant Execution Environment 연구동향 KIPS_C2020A0163	조명현*, 장지원, 남기빈, 황동일, 백윤홍(서울대학교) • 275
078	스마트 컨트랙트를 사용한 IoT 서비스 접근제어 설계 KIPS_C2020A0164	김미선*, 서재현(국립목포대학교) • 279
079	보안 하드웨어 모니터링 기법에 관한 연구 KIPS_C2020A0166	김현준*, 조명현, 장지원, 오현영, 백윤홍(서울대학교) • 283
080	Open IDS 및 CVE 기반의 OpenIOC가 결합된 CTI 프레임워크 설계 KIPS_C2020A0174	윤경찬*, 유지훈, 신동일, 신동규(세종대학교) • 286
081	Binary lifting을 이용한 안드로이드 라이브러리 취약점 분석 KIPS_C2020A0177	이성원*, 윤종희(영남대학교) • 290
082	원전 다양성보호계통 사이버보안 테스트베드 설계 KIPS_C2020A0179	정성민*(한국원자력연구원) • 292

ICT융합

083	빅데이터를 통한 약 성분명 처방 활용을 위한 시스템 KIPS_C2020A0018	▶ 김한예슬*, 김소연, 문유진(한국외국어대학교) • 296
084	독거노인 이중케어 시스템 개발 연구 KIPS_C2020A0029	▶ 임유빈*, 추은정, 한지민(성공회대학교) • 299
	085 원자력시설 사이버사건 대응훈련 정책 개선을 위한 규제방안 연구 KIPS_C2020A0031	류진호*, 김상우(한국원자력통제기술원) • 302
086	리멤버 어플리케이션에 기반한 배송관리 시스템에 관한 연구 KIPS_C2020A0068	정기혁*(고려대학교), 한울(상명대학교) • 306
087	실버 모빌리언, 노년층의 디지털 소외 해결을 위한 앱 KIPS_C2020A0071	▶ 서진아, 오송희, 오수현, 이영현*, 차승민, 호준원, 김명주(서울여자대학교) • 310
088	실시간 모니터링 및 생체정보 수집 가능한 환자 케어시스템 구현 KIPS_C2020A0072	▶ 김세정*, 윤서빈, 변정훈, 오예은, 유종현, 전홍영, 정길환, 김규겸(원광대학교) • 314
089	증강현실 기반 전자회로 교육 시스템 개발 KIPS_C2020A0096	오도봉*, 심승환(코아원), 최한고(금오공과대학교) • 318
090	딥러닝 기반 이미지 인식 기술을 활용한 동전 자동분류 스마트 저금통 KIPS_C2020A0105	유연승*, 장영진, 심현정, 이슬비, 김정길(남서울대학교) • 320
091	조건부 랜덤 포레스트 기반의 설명 가능한 일사량 예측 KIPS_C2020A0110	문지훈*, 황인준(고려대학교) • 323
092	클라우드 기반의 실험실정보관리시스템 구축 및 SaaS 제공 방안에 관한 연구 KIPS_C2020A0134	임복출*(주식회사 위컴즈), 류기상(주식회사 호원소프트) • 327



- 093 이어핀 삽입 자동화 시스템을 위한 템플릿 매칭 기반 홀 판별 방법 KIPS_C2020A0141
..... 백중환*, 이재열, 정명수, 장민우, 신동호, 서갑호, 홍성호(한국로봇융합연구원) • 330
- 094 코로나 바이러스 확진자 데이터 기반 시뮬레이션 모델 학습 방법 제안 KIPS_C2020A0143
..... 장미*, 이복주(한국기술교육대학교), 강봉구(한국생산기술연구원), 서경민(한국기술교육대학교) • 334
- 095 GPS-Spoofing을 이용한 Anti-Drone KIPS_C2020A0149
..... ▶ 권준우*, 오형석, 서승현(한양대학교) • 338
- 096 Unity 엔진을 이용한 Aveva Marine 뷰어 구현 KIPS_C2020A0173
..... 장원찬*, 양재균(울산대학교), 김삼성, 김병석(에이스이엔) • 342
- 097 스마트 기기를 활용한 노령인구의 헬스케어 플랫폼 개발 KIPS_C2020A0175
..... ▶ 한보현*, 공인복, 김다원, 이혜민, 정유담, 김상오(성명대학교) • 345
- 098 디자인 씽킹 메카니즘과 소프트웨어공학 접목에 관한 연구 KIPS_C2020A0183
..... 서채연*, 김장환, 박보경, 장우성, 손현승, 김영철(홍익대학교) • 349
- 099 독특한 한경이: 학내 챗봇 서비스 설계 및 개발 KIPS_C2020A0185
..... ▶ 박소희, 김미희*(한경대학교) • 352

소프트웨어공학

- 100 언어 학습 음원 분석 방법 및 언어 학습 음원을 재생하는 전자 디바이스 연구 KIPS_C2020A0008
..... ▶ 송규빈(강남대학교), 오정현*, 황채원(기톨릭대학교), 유동완(성공회대학교) • 355
- 101 블록체인을 기반으로 한 새로운 기부시스템 연구 KIPS_C2020A0010
..... ▶ 강건욱*, 유혜진(경북대학교) • 358
- 102 자동화된 트위터 데이터 수집 시스템 설계 및 구현 : 환경 데이터를 중심으로 KIPS_C2020A0011
..... ▶ 김도형*, 구자환, 김웅모(성균관대학교) • 361
- 103 의료영상 기반 간 질환 정량분석 통합소프트웨어 개발과 간 질환 환자 데이터 임상 적용
KIPS_C2020A0084
..... 김지언*, 김승진, 노시형, 이충섭, 김태훈, 정창원(원광대학교) • 365
- 104 DEVS 기반 OHT 시뮬레이션 시스템 설계 KIPS_C2020A0098
..... 이복주*(한국기술교육대학교), 강봉구(한국생산기술연구원), 권용환(주휴민텍),
..... 최영규(한국기술교육대학교), 한경아, 서경민(한국기술교육대학교) • 368
- 105 Inception v3를 이용한 화장품 추천 시스템 KIPS_C2020A0120
..... 장영훈*, 사이드 무하마드 라자(성균관대학교), 김문성(서울신대학교), 추현승(성균관대학교) • 372
- 106 전력 소모 최소화를 통한 성능 개선의 코드 가시화 방법 KIPS_C2020A0180
..... 안현식*, 박보경, 김영철(홍익대학교) • 375

데이터공학



- 107 여행 수요 파악 및 항공 노선 전략 연구 : 웹 크롤링 기반 분석 기법 KIPS_C2020A0004
..... 조창현*, 유현창(고려대학교) • 378
- 108 시차를 고려한 시계열 클러스터링 방법에 관한 연구 KIPS_C2020A0005
..... 정재용*, 이주홍(인하대학교), 송재원(주밸류파인더스) • 382
- 109 빅데이터 분석과 머신러닝을 활용한 특정 정치인의 견해와 평판에 대한 프로파일링 기술
KIPS_C2020A0061
..... ▶ 김민희*, 강재은, 최주영, 황채연, 김명주(서울여자대학교) • 385
- 110 신뢰성있는 온라인 고객 리뷰 텍스트 마이닝 기반 식당 개별 음식 아이тем 평가
KIPS_C2020A0073
..... 무자밀 후세인 사이드*, 정선태(숭실대학교) • 389
- 111 옷 추천 시스템 데이터 셋 구축을 위한 텍스트 데이터 마이닝 KIPS_C2020A0074
..... 이주상*, 정선태, 차준엽(숭실대학교) • 393
- 112 효과음 자막 생성을 위한 딥러닝 기반의 다중 사운드 분류 KIPS_C2020A0102
..... ▶ 정현영*, 김규미, 김현희(동덕여자대학교) • 397
- 113 온라인 행동정보를 이용한 협업 필터링 KIPS_C2020A0111
..... ▶ 광지윤*, 김가영, 홍다영, 김현희(동덕여자대학교) • 401
- 114 머신러닝을 이용한 구축함 수리부속 예측 연구 KIPS_C2020A0114
..... 정연오*, 김재동(한국국방연구원) • 405
- 115 빅데이터 도구 트렌드 및 긍·부정적 인식 결정 요소 조사 KIPS_C2020A0139
..... ▶ 이명진*, 구자환, 김응모(성균관대학교) • 409
- 116 COVID-19 확산 예측 모형에 관한 연구 KIPS_C2020A0146
..... 윤석용*(명지대학교) • 413
- 117 마이데이터 서비스 활성화를 위한 분산 ID(Decentralized Identification, DID) 수용의도에 영향을
미치는 요인에 관한 연구 KIPS_C2020A0184
..... 김지영*, 신용태(숭실대학교) • 417
- 118 최근접 이웃 탐색 기반의 향상된 스카이라인 질의를 위한 전처리 기법 KIPS_C2020A0188
..... ▶ 김지현*, 이상민, 전형준, 진창균, 김지윤(삼육대학교),
..... 권진영(건국대학교), 김종완, 오덕신(삼육대학교) • 420
- 119 시공간을고려한개인맞춤형경로추천알고리즘제안 KIPS_C2020A0191
..... 추민지*, 이혜진, 박영호(숙명여자대학교) • 424



인공지능


- 120 효과적인이상진단을위한클러스터링의타당성연구 KIPS_C2020A0001
..... 이현용*, 김낙우, 이준기, 이병탁(한국전자통신연구원) • 428

121	N-grams를 사용한 CNN 기반의 악성코드탐지 기법 연구 KIPS_C2020A0002	▶ 허정원*, 문봉교(동국대학교) • 431
122	대규모 외생 변수와 Deep Neural Network를 사용한 금융 시장 예측의 성능 향상에 관한 연구 KIPS_C2020A0006 천성길*, 이주홍, 최범기(인하대학교), 송재원(주밸류파인더스) • 435
123	Actor-Critic 모델을 이용한 포트폴리오 자산 배분에 관한 연구 KIPS_C2020A0007 칼리나 바야르체쎈*, 이주홍(인하대학교), 송재원(주밸류파인더스) • 439
124	인공지능을 활용한 스트리밍 서비스/SNS 내에서의 폭력 감지 시스템 KIPS_C2020A0013 ▶ 김선민, 이석원*, 임승수, 최상일(강릉원주대학교) • 442
	125 단일 단계 검출 방법을 위한 이미지 합성기반 학습 데이터 증강에 관한 연구 KIPS_C2020A0021 이선경*(한국전자통신연구원, 부경대학교), 정치운, 문경덕(한국전자통신연구원, 김재규(부경대학교) • 446
126	형태소 임베딩과 SVM을 이용한 뉴스 기사 정치적 편향성의 자동 분류 KIPS_C2020A0033 조단비*, 이현영(국민대학교), 박지훈(다함미 커뮤니케이션즈), 강승식(국민대학교) • 451
127	신경망 모델의 편향성을 줄이기 위한 데이터 증강 연구 KIPS_C2020A0035 손재범*(한양대학교) • 455
128	전력 데이터의 특징 추출 및 XGBoost를 이용한 숙박 업소 재실 여부 판단 KIPS_C2020A0040 김에덴*, 고석갑, 손승철, 이형옥, 이병탁(한국전자통신연구원) • 458
129	시니어 사용자를 위한 언어 모델 기반 질환 증상 인식 방법 KIPS_C2020A0043 박민경*, 최진우, 황보택근(가천대학교) • 461
130	EEG, MRI와 조현병의 상관관계를 이용한 진단 시스템 연구 KIPS_C2020A0051 ▶ 성지현*, 김도연, 김지은(이화여자대학교) • 464
131	ESRGAN과 Semantic Soft Segmentation을 이용한 객체 분할의 성능 개선 KIPS_C2020A0055 윤동식, 곽노윤*(백석대학교) • 468
132	최소 클래스 분류 문제 해결을 위한 전처리 연구 KIPS_C2020A0057 류경준*, 신동규, 신동일(세종대학교) • 472
133	AI 음악 큐레이션과 AR 운동방법을 이용한 전기자극 장치 개발 KIPS_C2020A0058 김홍윤*(주식회사 제우기술), 진세한(주식회사 캐스트유), 강지영(호서대학교) • 478
134	합성곱 신경망을 이용한 동결절편의 암세포 전이 여부 자동진단에 관한 예비연구 KIPS_C2020A0060 정대일*, 강재구, 전해린, 오세중(단국대학교), 김성철, 김영곤, 공경엽(서울아산병원), 송인혜(서울성모병원), 박소연, 안수민(분당서울대학교병원), 이현나, 양동현(서울아산병원), 유원상(선문대학교) • 480
	135 임베디드 시스템을 위한 멀티태스킹 딥러닝 학습 기반 경량화 성별/연령별 추정 KIPS_C2020A0067 Huy-Tran Quoc Bao*, 정선태(Soongsil University) • 483
136	Web Radiology_CDM기반 기계학습을 위한 인공지능 학습 플랫폼 구축 KIPS_C2020A0070 노시형*, 김승진, 김지언, 이충섭, 김태훈(원광대학교), 김경원(울산대학교), 김태규(주딴노이드), 윤권하, 정창원(원광대학교) • 487
137	호스트 기반 침입 탐지 데이터 분석 비교 KIPS_C2020A0079 박대경*, 신동규, 신동일(세종대학교) • 490

	138	랜덤 탐색과 유전 알고리즘 탐색을 이용한 효율적 기계학습 방법 연구 KIPS_C2020A0080	이경태*, 권영근(울산대학교) • 494
	139	OBDII 데이터 기반의 회귀 분석을 통한 실시간 연료 소비량 예측 KIPS_C2020A0081	양희은(단국대학교), 김도현*(성균관대학교) • 497
	140	딥러닝 기반 특허의 종속 청구항 인식 개선 KIPS_C2020A0083	▶ 박주연*, 신예지, 김민수, 김동호, 김지희(동국대학교) • 500
	141	초해상도 모델의 활성화함수 변경에 따른 성능 분석 KIPS_C2020A0086	유영준*, 김대희, 이재구(국민대학교) • 504
	142	기상 인자와 대기오염 인자를 활용한 LSTM 기반의 미세먼지 농도 예측 KIPS_C2020A0088	유지훈*, 신동일, 신동규(세종대학교) • 508
	143	사전 지식에 의한 강화학습 에이전트의 학습 속도와 경향성 변화 KIPS_C2020A0092	▶ 김지수*, 이은현, 김현철(고려대학교) • 512
	144	딥러닝 기반 한국 표준 산업분류 자동분류 모델 비교 KIPS_C2020A0094	우찬균*, 임희석(고려대학교) • 516
	145	인공지능 기반의 언어 생성 모델 분석 KIPS_C2020A0095	이승철*, 장용훈, 박창현, 서영석(영남대학교) • 519
	146	Transformer-based DKN for News Recommendation KIPS_C2020A0099	Hanwei Xia*, Inwhee Joe(Hanyang University) • 523
	147	Hybrid Feature Selection과 Data Balancing을 통한 네트워크 침입 탐지 모델 KIPS_C2020A0100	민병준*, 신동규, 신동일(세종대학교) • 526
	148	가사의 감정 분석을 이용한 GAN 기반 댄스 공연 배경 생성 방법 KIPS_C2020A0115	윤혜원*,곽정훈, 성연식(동국대학교) • 530
	149	단일 LiDAR를 활용한 End-to-End 기반 3D 모델 생성 방법 KIPS_C2020A0117	곽정훈*, 성연식(동국대학교) • 532
	150	경량 딥러닝과 지식베이스를 활용한 모바일 질환별 식품 추천 시스템 KIPS_C2020A0122	현범수*, 김도현, 이상근(고려대학교) • 534
	151	비디오 감시 카메라 내 사물 추적을 통한 골목길 교차로 사고 예방 시스템 KIPS_C2020A0123	▶ 김형진*, 김준영, 박주홍, 심재욱, 고석주(경북대학교), 김정석(SK텔레콤) • 536
	152	일반 필기데이터와 CNN을 이용한 온라인 서명인식 KIPS_C2020A0124	▶ 박민주*, 윤희용(성균관대학교) • 540
	153	GAN 기반 고해상도 의료 영상 생성을 위한 연구 KIPS_C2020A0126	고재영*(성균관대학교), 조백환, 정명진(삼성서울병원) • 544
	154	기계학습 기반의 낙상 검출 KIPS_C2020A0127	김인경*, 김대희, 허성실, 이재구(국민대학교) • 547
	155	오프로드형 자율주행 로봇 구동 메커니즘에 관한 연구 KIPS_C2020A0129	▶ 정혜원*, 김상훈(한경대학교) • 551
	156	그래프 신경망과 멀티 모달 맥락 정보를 이용한 장면 그래프 생성 KIPS_C2020A0130	정가영*, 김인철(경기대학교) • 555
	157	시각-언어 이동 에이전트를 위한 모방 학습과 강화 학습의 결합 KIPS_C2020A0131	오선택*, 김인철(경기대학교) • 559

158	쌍 선형 그래프 신경망을 이용한 지식 그래프 기반 질문 응답 KIPS_C2020A0132	이상의*, 김인철(경기대학교) • 563
159	신경망 기반 음원 분리 시스템의 학습 속도 향상을 위한 음역대 강조 기법 KIPS_C2020A0138	김민석*, 최우성, 정순영(고려대학교) • 567
160	다중 구면 영상으로부터 물체의 3D 위치 추정 KIPS_C2020A0147	홍철기*, 박종승(인천대학교) • 570
 161	TensorRT 엔진과 SSD를 이용한 Face detection KIPS_C2020A0156	▶ 유혜빈*, 김상훈(한경대학교) • 574
162	DNN과 LSTM 기반의 대기질 예측 모델 성능 비교 연구 KIPS_C2020A0159	▶ 조성재*, 김준석, 김성희, 윤주상(동의대학교) • 577
163	DenseNet을 통한 얼굴 스푸핑 탐지 기술 KIPS_C2020A0165	▶ 김소희*, 유수경, 이의철(상명대학교) • 580
164	기호 실행에서의 인공 지능 적용에 대한 연구: 퍼징과 취약점 탐지에서의 활용 KIPS_C2020A0167	하회리*, 안선우, 김현준, 백윤홍(서울대학교) • 582
165	소포물 분류를 위한 그리드 타입 시스템의 강화 학습 기반 행동 제어 KIPS_C2020A0169	최호빈*, 김주봉, 황규영, 한연희(한국기술교육대학교) • 585
 166	Contextual LSTM 기반 변분 오토인코더를 이용한 이동 경로 예측 KIPS_C2020A0172	조광호*, 차재혁(한양대학교) • 587
 167	분류 복잡도를 활용한 오버 샘플링 비율 산출 알고리즘 개발 KIPS_C2020A0176	이도현*, 김경옥(서울과학기술대학교) • 591
168	IoU의 최적화에 관한 연구 KIPS_C2020A0182	서신*(한양대학교) • 595

멀티미디어처리

169	다시점 360도 영상을 사용한 자유시점 영상 생성 방법 KIPS_C2020A0034	조영광*, 안희준(서울과학기술대학교) • 600
170	Unity 엔진을 이용한 노년층을 위한 VR 멀티 시뮬레이션 게임 개발 KIPS_C2020A0113	▶ 차주영, 윤혜원*(이화여자대학교) • 604
 171	구면 PTAM의 구현을 위한 카메라 모델 설계 KIPS_C2020A0140	김기식*, 박종승(인천대학교) • 607
172	바퀴변형과 센서를 이용한 안정적 계단이동 로봇의 설계 KIPS_C2020A0148	▶ 박성현*, 김상훈(한경대학교) • 611
173	코로나 19에 대해 일일 브리핑을 하는 정부 관계자의 목소리 특징 분석 KIPS_C2020A0154	조일영(중원대학교), 이선경(한국교통대학교), 조동욱*(충북도립대학교) • 615
174	차량번호판 영역 추출 방법론 비교 분석 KIPS_C2020A0192	이은지*, 박영호(숙명여자대학교) • 617

웹사이언스

- 175 오픈 API에서의 새로운 파라미터 요청 방식 제안 KIPS_C2020A0022
..... 박재훈*, 서화정(한성대학교) • 622
- 176 사용자 정보를 이용한 Indexed DB 암호화 인증 KIPS_C2020A0121
..... 황우섭*(한국방송통신대학교), 박지수(전주대학교), 손진곤(한국방송통신대학교) • 626

인간과 컴퓨터 상호작용

- 177 고객만족 및 서비스 품질에 관한 연구 - KOSEN 사례를 중심으로 KIPS_C2020A0024
..... 김상국*, 최선희(한국과학기술정보연구원) • 631
- 178 무대 공연을 위한 제스처 인식 기반 동적 프로젝션 맵핑 프레임워크 구현 KIPS_C2020A0178
..... 고유진*, 김태원, 최유주(서울미디어대학원대학교) • 633
- 179 Unity 기반 물리 실험 교육 시뮬레이터 개발 KIPS_C2020A0190
..... 김연정*, 윤세희, 신병석(인하대학교) • 635

제53회
2020 온라인 춘계학술발표대회

컴퓨터시스템 및 이론



자바 기반의 스프링 Web MVC 와 WebFlux 성능 분석

정명교*, 서태원**

*고려대학교 컴퓨터정보통신대학원 소프트웨어공학과
mkyo@korea.ac.kr, suhtw@korea.ac.kr

A Study on Tools for Agent System Development

Myung-Kyo Jung*, Taeweon Suh**

*Graduate School of Computer & Information technology, Korea University

** Graduate School of Computer & Information technology, Korea University

요 약

논블로킹 IO 를 활용한 웹 서비스를 위한 미들웨어 구축 방법은 2009 년 발표된 Node.js 에서 도입된 이후로 여러 언어 및 프레임워크로 전파되기 시작하였다. 자바 진영에서도 Project Reactor 를 통하여 논블로킹 IO 패러다임에 대응하기 시작하였고 이를 스프링 프레임워크로 구현한 WebFlux 가 출시되었다.

본 논문은 자바 기반의 웹서비스 구축 시 스프링 프레임워크를 활용한 블로킹 기법과 논블로킹 기법 간의 차이점을 살펴보고 성능을 분석한다. 이를 통해 가장 효율적인 성능을 발휘할 수 있는 아키텍처 모델을 도출한다.

1. 서론

자바 언어는 비교적 쉬운 문법 및 사용성을 바탕으로 국내에서 수많은 IT 서비스의 사용 언어로 채택되어왔다. 이후 2000 년 초에 스프링 프레임워크가 소개된 뒤 제어 역전과 의존성 주입뿐 아니라 Web MVC 같은 편리한 도구를 통하여 웹 서비스를 쉽고 빠르게 구축하는데 큰 기여를 했다. [1]

스프링의 Web MVC 는 동시 접속 사용자 처리를 위하여 블로킹 IO 모델을 활용한다. 이는 처리 가능한 동시 접속자의 수만큼 스레드를 생성하여 각각의 스레드가 요청이 완료될 때까지 점유 되어있는 상태로 존재하며 클라이언트에게 응답을 돌려줄 때 해당 스레드가 다시 가용한 상태로 전환되는 방식이다.

하지만 클라우드 환경을 기반으로 한 IT 서비스 인프라 환경이 늘어나기 시작하면서 웹 서비스 아키텍처를 구축 시 더 적은 자원으로 더 빠르게 서비스를 제공하려는 수요가 늘어나기 시작하였고, Node.js 에서는 이벤트 루프를 활용한 논블로킹 IO 를 선보이면서 웹 서비스 아키텍처에 새로운 패러다임이 제시되었다. [2]

Node.js 의 성공을 통해 자바 진영에서도 논블로킹 IO 모델에 대한 필요성이 꾸준히 제시되기 시작하였고, Java 8 버전부터 함수형 프로그래밍 문법을 일부 지원하기 시작한 이후로 논블로킹 IO 를 자바에서 구현할 수 있는 도구를 제공하기 시작하였다. 스프링 프레임워크 5 버전부터 이를 활용한 웹 프레임워크를 구축하는 도구를 WebFlux 라는 이름으로 지원하기 시작하였다.

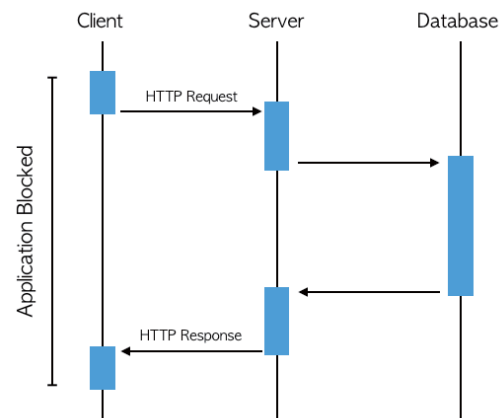
본 연구에서는 Web MVC 와 WebFlux 간의 구조적

차이에 대하여 알아보고 실험을 통하여 둘의 성능을 비교하여 그 결과를 바탕으로 웹 어플리케이션 서버 (WAS) 구축 시 최적의 성능을 위한 방법에 대하여 제안한다.

2. 관련연구

2.1 블로킹 IO 방식

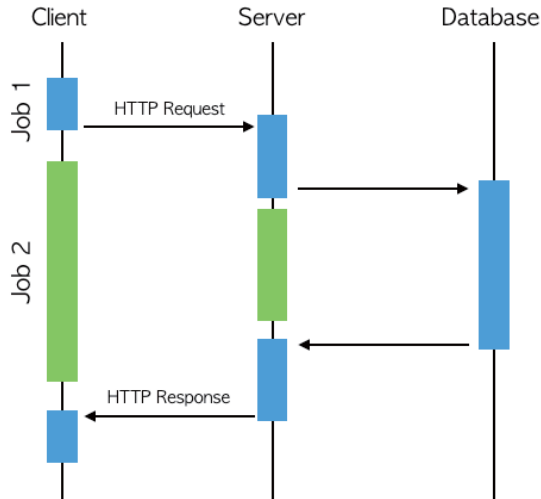
클라이언트로부터 요청이 발생한 시점부터 서버가 이를 처리하고 클라이언트에게 응답을 주기 전까지 대기하는 구조이다. 하나의 스레드가 요청을 처리하는 동안에는 다른 서비스를 수행할 수 없는 블로킹 상태가 된다.



(그림 1) 블로킹 방식의 작업 흐름

2.2 논블로킹 IO 방식

클라이언트가 서버에 요청을 전달한 뒤 대기하지 않고 다른 처리를 수행한다. 처리가 완료된 뒤에는 미리 등록된 콜백 함수를 호출하여 후처리를 진행한다. 이런 방식은 요청을 받고 해당 요청에 대한 결과를 리턴하는 과정에서 다른 태스크를 수행할 수 있기 때문에 다수의 스레드풀을 생성할 필요가 없다.



(그림 2) 논블로킹 방식의 작업 흐름

2.3 스프링 Web MVC

블로킹 방식의 웹 서비스를 구현하기 위해 제공되는 스프링 프레임워크의 라이브러리이다. MVC 는 Model-View-Controller 디자인 패턴의 약어이며 클라이언트로부터의 요청은 Dispatch Servlet 을 통하여 Controller 로 전달되며 이 때 동시 접속을 위한 사용자의 수만큼 스레드가 생성되는 구조이다.

2.4 스프링 WebFlux

논블로킹 IO 처리를 위해 제공되는 스프링 프레임워크의 라이브러리이다. 스프링 프레임워크 5 버전부터 제공되기 시작하였으며 반응형 프로그램을 위한 API 스펙을 구현하였다.

2.5 반응형 프로그래밍

반응형이라는 용어는 IO 이벤트에 반응하는 네트워크 컴포넌트, 마우스 이벤트에 반응하는 UI 컨트롤러 등 이벤트에 반응하는 프로그래밍 모델을 의미한다. 이러한 의미에서 논블로킹 IO 는 반응형이라고 볼 수 있는데, 이는 논블로킹 IO 는 작업이 완료되거나 데이터가 사용 가능한 이벤트에 반응할 수 있는 구조를 갖추기 때문이다. [3]

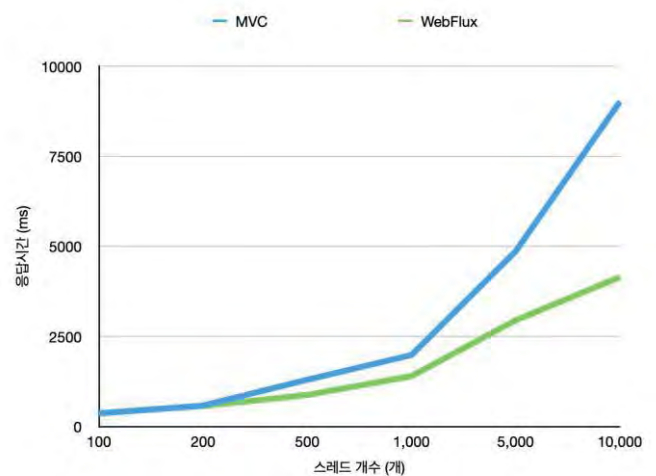
3. 성능비교

실험은 다음과 같은 방식으로 진행하였다. 스프링 Web MVC, WebFlux 각각을 사용하여 구현한 웹서비스를 구축한다. WebMVC 의 경우 동시접속자는 최대 200 명으로 설정하였다. 테스트 클라이언트에서는 다수의 동시접속자가 접속하는 상황을 가정하여 각 서

버에 동시다발적으로 요청을 발생시킨다. 각 서버별로 동시접속자 수에 따른 응답시간을 밀리초 단위로 측정한다. 숫자가 낮을수록 응답속도가 더 빠른 것을 의미한다.

<표 1> 동시접속자 수에 따른 응답시간 비교
(단위: 밀리초)

동시접속자 수	Web MVC	WebFlux
100	363	374
200	583	568
500	1,299	876
1,000	1,987	1,399
5,000	4,867	2,980
10,000	9,018	4,149



(그림 3) 블로킹 방식의 작업 흐름

4. 결과

200 개 이하의 동시 요청에 대해서는 두 서비스간의 응답속도가 동일하지만, 200 을 초과하는 요청부터는 응답속도의 차이가 관찰되었으며 동시접속자의 수가 많을수록 응답속도의 차이가 더 커지는 것을 확인할 수 있다. 이를 통해 다중 사용자에게 대한 HTTP 요청 처리시 WebFlux 가 Web MVC 보다 빠르거나 동일한 성능임을 알 수 있다. 즉 구축하는 서비스의 특성상 다량의 동시접속 사용자를 대응해야 하는 경우는 WebFlux 를 사용하여 구축을 하는 것이 성능상으로도 더 효과적이며 동시접속 사용자가 적은 서비스의 경우는 Web MVC 로 구축하더라도 동일한 성능을 발휘할 수 있다. 향후에는 실제 웹서비스 운영 환경과 동일한 구조로 데이터베이스를 구성하고 DB 커넥션풀의 논블로킹 여부에 따른 성능 차이를 분석하여 운영 환경에서의 서비스 성능 최적화가 이루어지도록 할 예정이다.

참고문헌

- [1] Johnson, Rod, et al. Professional Java development with the Spring framework. John Wiley & Sons, 2009.
- [2] Satheesh, Mithun, Bruno Joseph D'mello, and Jason Krol. Web development with MongoDB and NodeJs. Packt

Publishing Ltd, 2015.

- [3] Define “Reactive” <https://docs.spring.io/spring/docs/current/spring-framework-reference/web-reactive.html>
#webflux-why-reactive

스마트 더스트 환경을 위한 위치 기반 데이터 축소 시스템 설계

박준수*, 박기현*

*계명대학교 컴퓨터공학과

parkjoonsuu@gmail.com, khp@kmu.ac.kr (교신저자)

A Design of a Location-based Data Reduction System for a Smart Dust Environment

Joonsuu Park*, KeeHyun Park*

*Dept. of Computer Engineering, Keimyung University

요 약

매우 작은 크기의 센서들이 산악 등의 험지에 흩뿌려지는 스마트 더스트 환경은 장치들의 컴퓨팅 성능과 리소스가 매우 제한되기 때문에 각 센서들의 위치를 식별하기 매우 힘들다. 또한 초대량의 센서들이 뿌려지는 특성으로 인해 수집, 전송되는 데이터의 크기가 상상하기 힘들 정도로 커질 수 있다. 본 논문에서는 중간 매개 역할을 수행하는 디바이스의 위치와 삼변측량을 이용해 센서들의 위치를 계산하고 계산된 위치를 기반으로 동종의 센서에서 수집된 데이터를 축소, 통합하는 위치 기반 데이터 축소 시스템을 제안한다.

1. 서론

스마트 더스트(Smart Dust) 기술이란 먼지 크기의 매우 작은 센서들을 건물, 도로, 의복, 인체 등 물리적 공간에 먼지처럼 뿌려 주위의 온도, 습도, 가속도, 압력 등의 정보를 무선 네트워크로 감지, 관리할 수 있는 기술을 말한다 [1]. 즉, 스마트 더스트는 넓은 의미에서 사물 인터넷(Internet of Things) 범주에 속하며, 무선 네트워크를 통해 주변 정보를 측정하고 관리할 수 있는 기술이다 [2-4]. 스마트 더스트는 장치 주변의 정보를 쉽게 수집할 수 있지만 사람이 접근이 어렵거나 힘든 지역에 살포되는 특징으로 인해 관리 및 수리가 어려울 수 있다. 뿐만 아니라, 항공기 등을 이용해 넓은 지역에 광범위하게 살포되기 때문에 장치 하나 하나는 최소한의 컴퓨팅 성능과 리소스를 포함하는 경우가 대부분이다. 즉, 스마트 더스트는 다음과 같은 특징으로 요약될 수 있다.

- 1) 광범위한 지역에 살포
- 2) 많은 수
- 3) 낮은 컴퓨팅 파워 및 리소스

주변의 정보를 수집하는 스마트 더스트 시스템은 많은 경우 물리적 위치에 따라 유사한 데이터를 수집한다는 특성을 갖는다. 예를 들어, 근거리에서 위치한 온도, 습도 등의 환경 수집 센서들은 비슷한 온도, 습도를 수집할 것이며, 근거리에서 위치한 동작 감지 센

서들도 비슷한 시간에 비슷한 동작을 수집할 확률이 높다. 따라서 근거리에서 위치한 센서들 간의 데이터를 대표할 수 있는 데이터를 선정하거나 계산함으로써 데이터의 크기를 줄일 수 있다. 하지만 대부분의 센서들은 비용, 관리 및 수리의 문제 등의 이유로 GPS와 같은 위치를 식별할 수 있는 장치들을 포함하기 어렵기 때문에 위치 기반 데이터 축소 방법을 사용하기 어렵다.

우리는 본 연구를 통해 GPS 등의 위치 센서를 포함하지 않는 센서들의 스마트 더스트 환경에 다소 높은 컴퓨팅 센서를 갖는 릴레이 더스트 디바이스를 소규모(상대적)로 포함시키고 이를 통해 센서들의 위치를 식별함으로써 위치 기반 데이터 축소 방법을 수행할 수 있는 시스템을 제안한다.

본 논문은 2장에서 릴레이 디바이스를 제안하는 논문과 릴레이 디바이스에 관한 개요를 소개한다. 3장에서는 릴레이 디바이스를 이용하여 더스트 디바이스의 위치를 계산할 수 있는 방법에 대해 소개하고 4장에서 3장에서 소개한 계산을 통해 위치가 계산된 디바이스의 데이터 축소 방법을 소개한다. 끝으로 5장에서 결론과 향후 연구에 대해 이야기한다.

2. 릴레이 디바이스(Relay Devices)를 포함하는 시스템

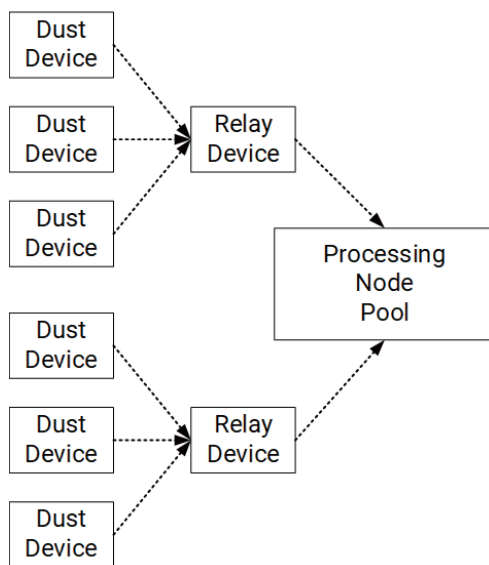
릴레이 더스트 디바이스의 개념은 사물 인터넷 환경의 스마트 더스트 환경을 위한 고속 패킷 처리 시스템을 다루는 우리의 이전 연구들[5-7]에서 패킷 고속 처리를 위한 데이터 축소를 위한 개념으로 소개되

었다.

이전 시스템들에서 릴레이 디바이스는 더스트 디바이스들의 데이터를 수집하여 처리 장치들로 연결하는 역할을 수행함과 동시에 처리 시 데이터를 합치거나 센서 종류에 따라 합칠 수 있는 데이터를 합치는 등의 일부 변환 역할을 수행했다.

이전 연구들은 위치를 기반으로 수집 데이터가 유사할 수 있다는 개념이나 이를 기반으로 합치려는 시도가 아닌 비슷한 시간에 도착한 데이터를 합치는 다소 단순한 형태의 데이터 병합이었다.

아래 그림 1 은 본 시스템에서 릴레이 디바이스의 개념적 위치와 시스템의 구성 요소들을 간략히 보인다.



(그림 1) 릴레이 더스트 디바이스의 위치 및 스마트 더스트 시스템의 개요

3. 릴레이 디바이스 주도의 위치 계산

우리는 더스트 디바이스보다 상대적으로 컴퓨팅 파워 및 리소스가 많은 릴레이 디바이스가 더스트 디바이스와 직접적으로 연결된다는 점에 착안하여 주변의 릴레이 디바이스의 위치로부터 더스트 디바이스의 위치를 계산한다.

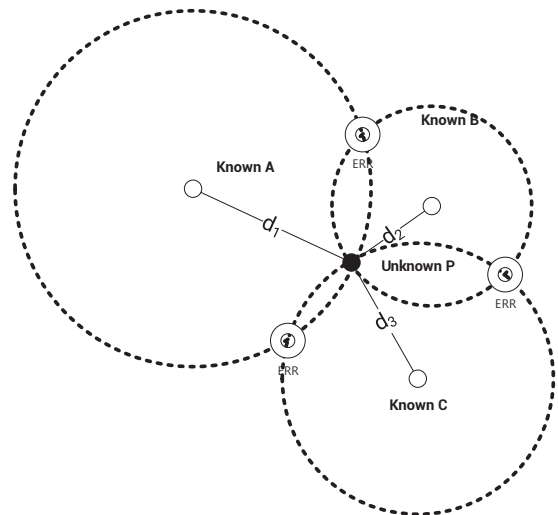
디바이스의 위치를 알아내기 위해 무선 센서 네트워크 환경에서 사용할 수 있는 첫번째 방법은 각도를 통해 위치를 측정하는 기법이다. 이런 거리 측정 기법은 TOA [8], TDOA [9], AOA [10] 기법이 있으며 이를 통해 거리나 각도를 얻을 수 있다. 이 세가지 방법은 모두 신호의 각, 신호의 도착 시간 측정 등을 사용하지만 이를 위해 센서에 구성요소들이 부착되거나 수신을 위한 별도의 장치들을 구성해야한다는 문제를 가지고 있다 [11].

거리 정보를 기반으로 위치를 인식하는 계산 방법으로 삼변측량이 있다. 삼변측량은 위치를 알고 있는 3 개의 무선 센서 노드(릴레이 디바이스)와 알고자 하

는 위치(더스트 디바이스)의 거리 정보를 토대로 위치를 계산한다. 삼변측량은 다소 오차가 발생할 여지가 있지만, 릴레이 디바이스와 더스트 디바이스 간의 비콘 (beacon)만으로 위치를 계산할 수 있다는 장점이 있으며 간단한 수식만으로 위치를 계산할 수 있다는 장점을 지닌다.

우리는 정확하고 섬세한 위치보다는 디바이스 간의 거리가 데이터를 합칠 정도로 가까운가 하는 정보를 필요로 하기 때문에 삼변측량에 의한 위치 계산을 수행한다.

아래 그림 2 는 위치를 알고 있는 3 개의 포인트와 위치를 알지 못하는 1 포인트에 대한 예를 보인다.

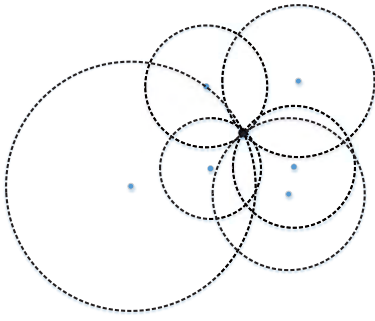


(그림 2) 알려진 노드 3 개(Known A, B, C)와 위치를 알아내고자 하는 노드 1 개(Unknown P)의 예시

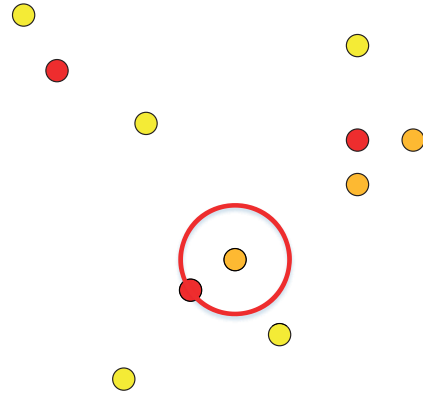
그림 2 에서 위치를 알고 있는 Known A, B, C 는 본 시스템의 릴레이 더스트 디바이스에 매핑될 수 있으며 위치를 알지 못하는 Unknown P 는 더스트 디바이스에 매핑될 수 있다. d_1, d_2, d_3 는 각각 P 의 신호 세기와 매핑되어 A, B, C 에서 측정될 수 있다. 결국 상술한 변수들을 이용하면 세 원의 교점을 찾을 수 있으며 각 교점들의 중심 위치가 P 의 위치가 된다.

다소의 오차를 포함하는 삼변측량은 일반적으로 보정 수식을 이용하여 보다 정확한 위치를 계산한다. 하지만 아주 정확한 계산이 필요하지 않으며, 여러 릴레이 디바이스를 보유한 상황을 가정하는 본 시스템은 보정 수식을 이용하기 보다는 이미 존재하는 릴레이 더스트의 개수를 이용하여 교점을 보다 정확히 보정한다.

아래 그림 3 에서 알 수 있듯 신호를 감지한 릴레이 디바이스의 수가 늘어날수록 실제 위치가 보다 정확한 위치로 보정됨을 알 수 있다.



(그림 3) 여러 릴레이 디바이스에 신호를 전달하는 더스트 디바이스 예시

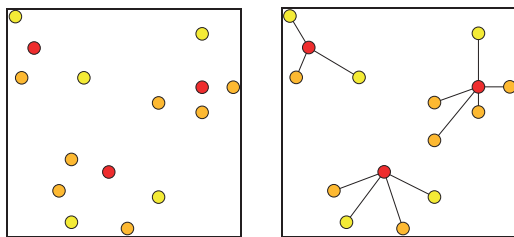


(그림 5) 축소율을 고려한 더스트 디바이스의 연결

4. 위치 기반 데이터 축소 시스템

릴레이 디바이스 주도의 위치 기반 데이터 축소 방법이 적용된 시스템은 첫번째 단계에서 각 더스트 디바이스의 위치를 상술한 바와 같이 계산한다. 위치가 결정된 디바이스들은 동종의 디바이스가 가장 많이 연결될 수 있는 릴레이 디바이스로 데이터를 송신한다. 두번째 단계에서는 그룹화를 진행한다.

아래 그림 4 는 그룹화 전의 릴레이/더스트 디바이스들과 그룹화 후의 릴레이/더스트 디바이스들을 보인다.



(그림 4) 그룹화 전(좌)의 디바이스들과 그룹화 후(우)의 디바이스들

그림 4 의 붉은색 표시는 릴레이 디바이스를 의미하며, 주황색, 노란색은 서로 다른 종류의 더스트 디바이스를 의미한다. 각각은 가장 가까운 릴레이 디바이스로 연결된다. 이 때, 경우에 따라 연결되는 릴레이 디바이스를 변경할 수 있다. 예를 들어, 아래 그림 5 에 표시된 주황색 더스트 디바이스는 거리상 하단의 릴레이 디바이스에 연결되어야 하지만, 혼자 연결될 경우 데이터의 축소 효과를 누리기 힘들기 때문에 우측의 릴레이 디바이스로 연결된다. 이 비율은 상대적으로 높을 수 있다. 따라서 본 시스템은 같은 종류의 더스트 디바이스의 비율이 높은 릴레이 디바이스를 우선 고려하도록 설계된다.

그림 4 의 우측의 그림과 같이 릴레이 디바이스에 연결된 더스트 디바이스들은 각 위치에서 정보들을 수집하여 릴레이 디바이스로 전송한다. 이를 수신한 릴레이 디바이스는 세번째 단계인 데이터 축소 단계를 수행한다. 데이터 축소 단계에서는 같은 종류의 더스트 디바이스가 같은 릴레이 디바이스로 송신한 데이터들의 평균을 계산하여 1 개의 평균 데이터 값을 서버로 전송한다. 즉, 그림 4 의 우측 그림에서 각 릴레이 디바이스 일반적인 시스템일 경우 12 개의 데이터를 전송하지만, 각각 최대 2 개의 데이터를 송신하여 6 개의 데이터만을 송신하고 평균 50% (디바이스 종류의 수가 많아 질수록 줄어듦) 데이터를 축소할 수 있다.

5. 결론 및 향후 연구

우리는 본 논문에서 스마트 더스트 환경에서 위치에 대해 알 수 없는 더스트 디바이스의 위치를 계산하고 이를 이용하여 전송 데이터의 크기를 줄일 수 있는 위치 기반 데이터 축소 시스템을 제안했다.

우리는 위치를 찾기 위해 삼변측량을 사용하여 위치를 결정했으며 데이터 통합을 위해 평균값을 취하는 방법을 사용했다. 본 시스템은 삼변측량의 오차를 보정하기 위해 많은 수의 릴레이 디바이스가 협동하지만 적은 수의 릴레이 디바이스가 있는 환경에 대해 유연하게 대처할 수 있는 시스템에 대한 연구, 개발이 필요하다. 또한, 수치 데이터에만 적용 가능한 평균값 보다 투표 방식과 같은 비수치적 데이터에 적용 가능한 대표 값 취득 방식에 관한 연구, 개발이 필요하다.

이 논문은 2020 년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. NRF-2018R1D1A1B07043982).

참고문헌

- [1] 박천교. (2004). 스마트 더스트(Smart Dust). [IITA] 정보통신연구진흥원 학술정보, (), 0-0.
- [2] Kahn, M.J.; Katz, R.H.; Pister, K.S.J. Next Century

- Challenges: Mobile Networking for Smart Dust. In Proceedings of the 5th annual ACM/IEEE International Conference on Mobile Computing and Networking, Seattle, WA, USA, 17–19 August 1999. [Google Scholar]
- [3] Brett, W.; Last, M.; Liebowitz, B.; Pister, K.S.J. Smart Dust: Communicating with a Cubic-Millimeter Computer. *Computer* 2001, 34, 44–51. [Google Scholar]
- [4] Kahn, M.J.; Katz, R.H.; Pister, K.S.J. Emerging Challenges: Mobile Networking for Smart Dust. *J. Commun. Netw.* 2000, 2, 188–196. [Google Scholar] [CrossRef]
- [5] Park, Joonsuu, and KeeHyun Park. "A Dynamic Plane Prediction Method Using the Extended Frame in Smart Dust IoT Environments." *Sensors* 20.5 (2020): 1364.
- [Park, J.; Park, K. A Study on System Architecture Design for Plane Dynamic Scaling in Smart Dust Environments. In Proceedings of the 2019 Korea Information Processing Society Conference in Spring, Seoul, Korea, 10–11 May 2019.
- [6] Park, K.; Kim, I.; Park, J. A High Speed Data Transmission method for DPDK-based IoT Systems (in Korean). In Proceedings of the International Conference on Future Information & Communication Engineering, Singapore, 23 April 2018; pp. 325–327.
- [7] Park, J.; Park, K. A Study on System Architecture Design for Plane Dynamic Scaling in Smart Dust Environments. In Proceedings of the 2019 Korea Information Processing Society Conference in Spring, Seoul, Korea, 10–11 May 2019.
- [8] J. Caffery Jr. and G. L. Stuer, "Subscriber location in CDMA cellular networks," *IEEE Trans. Veh. Technol.*, vol.47, pp. 406-416, May 1998.
- [9] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan, "The cricket location-support system," in *Proc. ACM Int. Conf. Mobile Computing Networking (MOBICOM)*, Boston, MA, Aug. 2000, pp.32-43. [3]R.J. Shupe, "Effect of Occlusal Guidance on Jaw Muscle Activity," *J Prosthet Dent*, Vol. 51, pp. 811-818, 1984.
- [10] D. Niculescu and B. Nath, "Ad Hoc Positioning System (APS) using AoA" in *Proc. IEEE Joint Conf. IEEE Computer Communications Societies (INFOCOM)*, San Francisco, CA, USA, Mar. 2003, pp.1734-1743.
- [11] 김선관, 김태훈, and 탁성우. "다중 무선센서 네트워크 환경에서 삼변측량 기법을 이용한 위치 인식 방법들에 대한 비교평가." *한국멀티미디어학회 학술발표논문집* (2010): 203-206.

스마트 컨트랙트를 활용한 공유숙박 서비스

유지성*, 김제인*, 서승현*
*한양대학교 에리카 전자공학부

wltjd1014@hanyang.ac.kr, rean5123@hanyang.ac.kr, seosh77@hanyang.ac.kr

Home Sharing Service Using Smart Contract

Ji-Sung Yoo*, Jane Kim*, Seung-Hyun Seo*

*Dept. of Electronic Engineering, Hanyang University ERICA

요 약

에어비엔비와 같은 공유숙박시스템은 하루 400 만명 이상 이용하고 있는 거대한 시장이다. 일반적으로 지출해야 할 숙박비용보다 더 저렴한 가격이나 좋은 조건으로 머물 곳을 찾을 수 있다는 점에서 많은 사람들이 이용하고 있다. 그러나 호스트와 게스트에게 부담되는 과도한 수수료 문제가 존재한다. 또한 기존의 공유숙박 시스템은 호스트가 게스트에게 직접 비밀번호나 열쇠를 전달하기 때문에 보안 상의 이슈가 발생한다. 본 연구는 공유숙박시스템에 스마트 컨트랙트 기술을 도입하여 해당 이슈들을 개선, 해결하여 더 안전하고 합리적인 공유숙박시스템을 제안한다.

1. 서론

공유 숙박이란 중개시스템을 통해 주택의 빈방을 숙박용으로 제공하는 서비스이다. 호스트, 게스트 그리고 중개사이트로 구성되는 이 시스템은 호스트와 게스트가 중개사이트에 중개수수료를 지불하게 되어 있다. 현재 에어비엔비에서 호스트와 게스트가 지불하는 중개수수료는 전체 숙박비의 8%~15% 차지한다 [1]. 또한 기존의 공유숙박 플랫폼들은 호스트가 게스트에게 직접 숙소의 비밀번호나 열쇠를 전달하는 과정을 거친다. 게스트가 숙소 사용이 허락된 시간외에 숙소를 이용할 수 있다는 부분은 보안상의 문제가 발생 할 수 있다. 최근 이러한 문제들을 해결하기 위해 또다른 공유숙박 플랫폼인 wehome 은 스마트 컨트랙트 시스템을 도입하여 중개 수수료를 절감했다. 또한 보안사고를 막기 위하여 숙소 체크인 방법을 개선하고자 하는 움직임이 있다.

위의 문제를 개선하기 위하여 본 연구에서도 이더리움(Ethereum) 블록체인 플랫폼에서 스마트 컨트랙트를 사용하여 기존 플랫폼보다 적은 중개수수료로 이용할 수 있는 서비스를 제작한다. 뿐만 아니라 게스트에게 비밀번호나 열쇠 대신 체크인 할 수 있는 일회용 QR 코드를 발급하여 보다 안전한 공유숙박시스템을 제안한다. 숙박하는 기간에만 사용할 수 있는 QR 코드는 기존의 보안상의 문제를 해결 할 수 있다. 이 시스템을 통해 더 안전하고, 중개수수료가 감면된 혁신적인 공유숙박 시스템을 이용할 수 있을 것이라 기대한다.

2. 관련 연구

2.1 스마트 컨트랙트

이더리움은 최초의 블록체인 기반의 스마트 컨트랙트 플랫폼이다[2]. 스마트 컨트랙트는 코드화 시킨 조건이 만족하면 계약이 자동으로 성사되어 '이더(ETH)' 라는 암호 화폐가 사용되는 시스템이다. 이런 자동화 시스템으로 제 3의 보증기관의 도움 없이 개인 간 거래가 원활하게 이루어질 수 있다. 'Solidity'라는 프로그래밍 언어로 작성된 스마트 컨트랙트 코드는 바이트 코드로 컴파일 되고, 블록체인 네트워크에 배포된다. 블록체인 네트워크에 기록된 바이트 코드는 이더리움 가상머신(EVM) 환경에서 작동한다. 계약을 진행중인 참여자가 발생시키는 모든 트랜잭션의 데이터는 전체 노드들에 의해서 실행되고 저장되는데, 이 노드들은 전부 이더리움 가상머신 환경 속에서 존재한다. 스마트 컨트랙트는 다수의 노드에 의해 데이터들이 공유되기 때문에 특정 공격자가 계약 결과를 조작하는 것은 불가능하고, 결과적으로 무결성을 보장한다.

2.2 메타마스크

이더리움을 송금하거나 안전하게 관리할 수 있는 이더리움 암호화폐 지갑이다[3]. 메타마스크는 크롬

웹 브라우저 환경에서 작동하는 구글 확장프로그램 중 하나이다. 이더리움 디앱(Dapp)은 이더리움 노드들 위에서 동작하므로 일반적인 웹 브라우저 환경에서는 동작하지 않는다. 메타마스크를 이용하면 이더리움 노드들이 실행되고 있지 않은 웹 브라우저 환경에서도 디앱을 동작시킬 수 있다. 또한, 블록체인 네트워크 참여자들이 만드는 트랜잭션에 대한 서명을 받을 수 있는 기능을 제공한다. 본 연구에서는 메타마스크를 이용해 웹 브라우저 환경에서 블록체인 네트워크 참여자들은 계약금을 주고받는 서명을 통해 숙박 공유 스마트 컨트랙트 디앱을 동작시킨다.

2.3 가나슈

블록체인 개발 테스트에 사용되는 프라이빗 간이 블록체인이다[4]. 가나슈는 간이 블록체인이기 때문에 별도의 네트워크 연결이 필요하지 않고 로컬에서 동작하므로 스마트 컨트랙트를 쉽게 배포할 수 있다. 블록체인 개발을 위해 geth와 같은 클라이언트를 이용하면 트랜잭션이 작동하기까지 채굴하는 시간이 소요되기 때문에 개발 속도가 느리다. 가나슈는 트랜잭션이 발생할 시 자동으로 채굴하도록 만들 수 있으며, 블록이 생성되는 시점도 초 단위로 설정할 수 있다. 가나슈는 개발 테스트를 위해 테스트 전용 계정을 만들 수 있고, 해당 계정에 스마트 컨트랙트를 위한 가상의 이더를 넣을 수 있다. 계정 잔액, 블록과 트랜잭션의 로그 정보를 가나슈 사용자 인터페이스에서 확인 가능하다. 가나슈의 테스트용 계정은 메타마스크와 연동이 되어 웹 브라우저 환경에서 실제로 스마트 컨트랙트를 테스트해볼 수 있다. 본 연구에서는 가나슈를 이용하여 10 개의 테스트 계좌를 만들고 각 계정에 100ETH를 세팅한다. 테스트용 계정을 이용해 숙박 공유 스마트 컨트랙트를 동작시키고, 가나슈 인터페이스를 통해서 해당 결과를 분석한다.

3. 제안하는 SQome 서비스



그림 1. 시스템 진행단계

SQome은 Smart QRcode home의 의미로 본 연구에서 제안하는 시스템 이름이다. SQome은 다음과 같이 총 3 단계로 진행되고 모든 숙박 시설에는 QR 코드를 통해 문을 열 수 있는 스마트 잠금 장치가 있다고 가정한다.

- 1 단계: 호스트의 숙박 등록 단계
- 2 단계: 게스트의 숙박 예약 단계

3 단계: QR 코드 확인 단계

3.1 호스트의 숙박 등록 단계

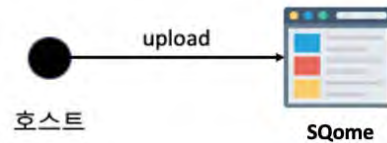


그림 2. 호스트의 숙박등록

호스트는 SQome에 숙박 정보를 게시한다. 숙박을 등록하는 트랜잭션이 발생하면 그 트랜잭션은 호스트의 비밀키로 서명한다. 트랜잭션들이 모여 블록을 생성하고, 각 노드는 해당 스마트 컨트랙트의 바이트코드를 가진다. 이후에 트랜잭션의 내용에 따라 스마트 컨트랙트를 실행하고, 다른 모든 노드가 해당 내용을 저장한다.

3.2 게스트의 숙박 예약 단계

게스트는 SQome에서 호스트가 등록한 숙박을 조회한다. SQome에서는 블록체인 네트워크에서 숙박의 상태, 즉 예약 여부를 조회하여 SQome에 표시한다. 게스트는 예약을 할 때 이름, 전화번호를 입력 후 메타마스크를 통해 계약금을 지불한다. 트랜잭션은 스마트 컨트랙트의 상태를 변경할 수 있다. 게스트가 이더를 지불함과 동시에 스마트 컨트랙트가 체결된다. 호스트는 계약이 체결됨과 동시에 이더를 제공받고 게스트는 숙박기간동안 사용할 수 있는 QR 코드를 제공받는다. 예약이 완료되면 스마트 컨트랙트의 내용을 변경시키는 트랜잭션을 발생시키고 호스트가 숙박을 등록될 때와 마찬가지로 모든 노드가 바뀐 내용을 얻게 된다.



그림 3. 스마트 컨트랙트 체결

3.3 QR 코드 확인 단계

스마트 컨트랙트 체결과 동시에 SQome에서 해당 숙박은 예약완료되며 이 결과는 SQome에 표시된다. 그 후 조회를 통하여 게스트는 자신이 예약한 숙소의 상세정보와 QR 코드를 확인할 수 있다. 해당 QR 코드를 이용하여 숙박기간동안 체크인이 가능하다.

4. SQome 구현

본 연구에서 제안한 SQome은 크게 이더리움 블록체인 네트워크의 스마트 컨트랙트 부분과 웹 페이지 부분으로 구성되어있다. SQome의 스마트 컨트랙트 부분은 솔리디티(Solidity) 언어를 통해서 구현했다. 솔리디티는 블록체인 플랫폼에서 스마트 컨트랙트 작

성과 구현에 사용되는 계약 지향 프로그래밍 언어이다. 작성된 스마트 컨트랙트는 dApp 관리 프레임워크인 트러플을 통해 컴파일과 배포가 가능하다. 시뮬레이션을 위해 간이용 블록체인인 가나슈를 통해 테스트 계좌 10 개를 생성하고, 각 계좌에 100 이더를 설정하였다. 작성한 스마트 컨트랙트를 트러플을 통해 컴파일 후에 가나슈 네트워크에 배포하였다.

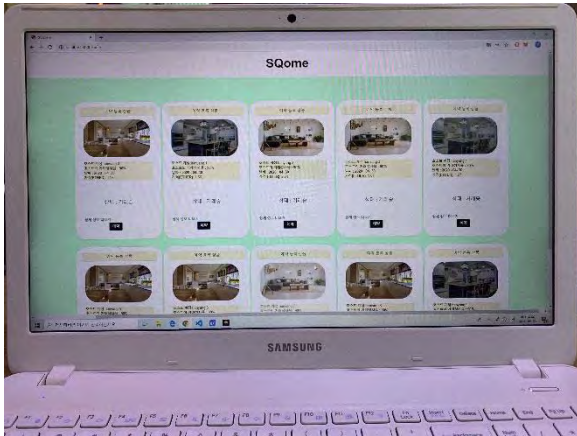


그림 4. SQome 메인 페이지

그림 4 는 실제 로컬 호스트에서 구현된 SQome 의 메인 페이지 모습이다. Node.js 의 Express 프레임워크를 이용하여 SQome 의 웹 페이지를 제작했다. 게스트는 메인 화면에서 호스트들이 등록해 놓은 거래 물품을 확인할 수 있으며, 예약 버튼을 통해 거래를 진행할 수 있다.

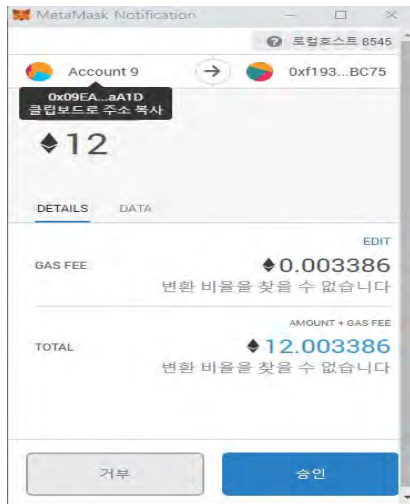


그림 5. 메타마스크를 통한 거래 과정

그림 5 는 게스트가 예약을 신청할 때 볼 수 있는 인터페이스 화면이다. 게스트는 메타마스크를 통해 거래 금액, 가스화 같은 상세 내용을 확인하고 해당 거래에 대한 서명을 할 수 있다. 게스트가 거래에 대한 승인을 마치고 호스트에게 이더를 전송하면 스마트 컨트랙트가 정상적으로 작동한다.

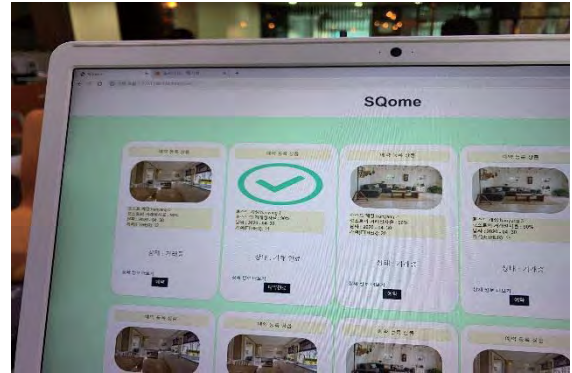


그림 6. 예약 완료된 페이지

그림 6 은 예약완료 후 결과를 확인 할 수 있는 페이지이다. 이 페이지에서 '예약 확인하기' 버튼을 통해 게스트는 예약 내역을 확인할 수 있는 페이지로 넘어갈 수 있다.

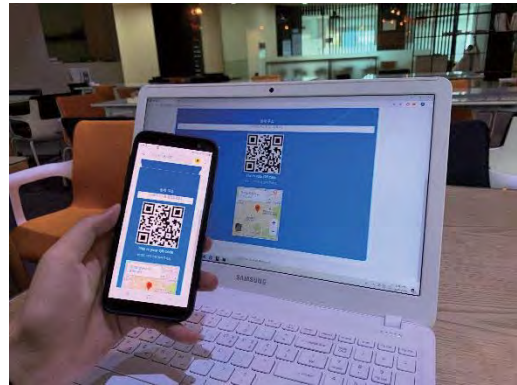


그림 7. QR 코드 확인 페이지

그림 7 은 게스트의 상세 예약 정보를 확인 할 수 있는 페이지이다. 이 페이지에서 게스트는 숙박 기간에 사용할 수 있는 일회용 QR 코드와 숙박하게 될 상세한 주소를 확인할 수 있다. 해당 페이지는 모바일 환경에서도 접속이 가능하며 게스트는 QR 코드를 통해 호스트의 숙소에 체크인 할 수 있다.

ACCOUNTS	BLOCKS	TRANSACTIONS	CONTRACTS	EVENTS	LOGS
ACCOUNT 1	0	0	0	0	0
ACCOUNT 2	0	0	0	0	0
ACCOUNT 3	0	0	0	0	0
ACCOUNT 4	0	0	0	0	0
ACCOUNT 5	0	0	0	0	0
ACCOUNT 6	0	0	0	0	0
ACCOUNT 7	0	0	0	0	0
ACCOUNT 8	0	0	0	0	0
ACCOUNT 9	0	0	0	0	0
ACCOUNT 10	0	0	0	0	0

그림 8. 가나슈 계정 정보

그림 8 은 가나슈 툴을 이용하여 미리 생성한 10 개

의 계좌 주소와 잔액 등을 보여준다. 초기 100 이더로 세팅한 다른 계좌와 달리 구매를 진행한 9 번째 계정은 거래금액만큼 줄어든 계좌잔액을 확인할 수 있다.

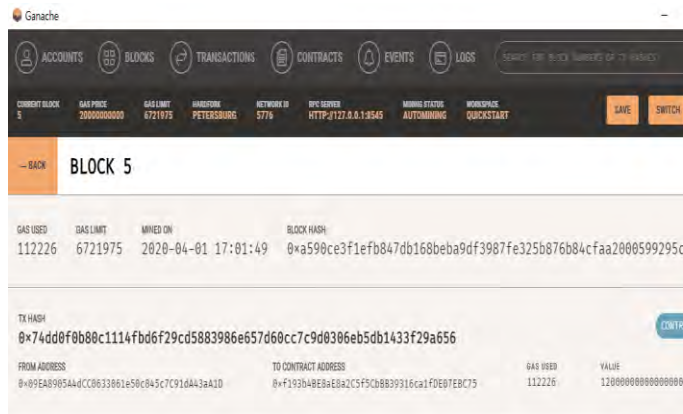


그림 9. 블록에 저장된 거래 정보

스마트 컨트랙트가 실행되면 이더리움 블록체인 네트워크에 새로운 블록을 추가하고, 해당 거래 정보를 블록에 저장한다. 그림 9 는 가나슈를 통해 앞서 진행한 스마트 컨트랙트가 체결되면서 생성된 블록 정보를 보여준다. 블록에는 거래 일시, 이더를 주고받은 계좌 주소, 거래 금액 등이 포함되어 있다.

5. 결론 및 향후 연구

기존의 공유숙박서비스는 제 3 의 보증 기관이 별도로 필요하며 추가적인 수수료가 부과되고 있다. 본 논문에서는 스마트 컨트랙트를 공유숙박 서비스에 접목함으로써 중개 기관이 필요치 않은 블록체인 활용 플랫폼을 제안하였다. 이는 블록체인 네트워크에 존재하는 전체 노드들이 네트워크 참여자들이 만드는 모든 트랜잭션을 검증하고 기록하기 때문에 가능하다. 또한 기존 공유숙박 서비스는 호스트의 개인 열쇠나 비밀번호를 게스트에게 알려주어야 하는 불필요한 과정이 필요하다. 본 논문에서 제안한 서비스는 스마트 컨트랙트의 결과로 일회용 QR 코드를 제공함으로써 이 문제를 해결하였다.

향후 연구에서는 QR 코드 뿐만 아니라 다양한 인증 수단을 스마트 컨트랙트와 연동을 시켜 접근성이 확장된 서비스 구축을 목표로 할 것이다.

참고문헌

- [1] <https://www.airbnb.co.kr>
- [2] 정효연, 임미숙, 강희조, 김윤희 "블록체인 기반 스마트 컨트랙트 기술동향", 한국정보기술학회, 2018.6, 60~62
- [3] 메타마스크, <https://metamask.io>
- [4] 가나슈, <https://github.com/trufflesuite/ganache>

적응적 상관도를 이용한 주성분 분석에 관한 연구

고명숙*

*부천대학교 경영과

kms@bc.ac.kr

A Study on PCA using Adaptive Correlation

Myung-Sook Ko*

*Dept. of Business Administration, Bucheon University

요 약

고차원의 데이터를 처리하기 위해서는 데이터의 성질을 유지하면서 특징을 잘 반영할 수 있는 특징 추출 방법이 필요하며 주성분분석 방법은 대표적인 특징 추출 방법이다. 본 연구에서는 데이터가 고차원인 경우 데이터 특징 추출을 위한 주성분 분석의 주성분 변수 선정시 적응적 상관도(Correlation)를 기반으로 한 주성분 분석 방법을 제안한다. 제안하는 방법은 입력 데이터간의 상관관계를 기반으로 상관도를 적응적으로 반영하여 데이터의 주성분을 분석함으로써 실제 데이터의 특징을 나타내는 세분화 변수 선정 시 데이터 편향성의 영향을 줄이기 위한 방법이다.

1. 서론

고차원의 데이터는 데이터 분포 형태를 알 수 없을 뿐만 아니라 많은 양의 메모리와 계산을 필요로 한다. 이러한 데이터를 처리하는 과정에서 차원을 낮추고 데이터의 특징을 추출하기 위해 사용하는 대표적인 기법 중 주성분 분석 기법이 많이 사용된다[1]. 주성분 분석(Principle Component Analysis; PCA)은 고차원의 데이터를 저차원의 데이터로 환원시켜 서로 연관 가능성이 있는 고차원 공간의 표본들의 공분산 행렬을 원 변수의 선형 결합을 이용하여 분석하는 방법으로서 선형 연관성이 없는 분산 기반 저차원 공간으로의 사상을 통하여 주요성분들을 축으로 하여 선형 변환한다[1,2]. 본 논문에서는 주성분 분석의 주성분 변수(또는 세분화변수) 선정시 상관도(Correlation)를 적응적으로 적용하여 데이터 편향성의 반영도를 낮추고 연관성을 높이는 데이터 특성을 반영하여 고 차원 데이터의 특징을 더 잘 반영한 주성분 분석의 세분화 변수를 얻을 수 있는 방법을 제안하고자 한다.

2. 주성분 분석 및 세분화변수 선정

주성분 분석은 데이터의 특성을 찾아내는 가장 대표적인 방법 중의 하나로서 고차원 데이터의 정보

손실을 최소화하는 저차원의 세분화 변수를 통하여 전체 데이터를 표현하는 방법이다[1].

x와 y의 공분산(covariance) cov는 다음과 같이 정의될 수 있다.

$$\text{cov}(x,y) = E[(x-m_x)(y-m_y)] = E[xy] - m_x m_y$$

단, m_x 는 x의 평균, m_y 는 y의 평균, E[]는 기대값

x의 분산은 x값들이 평균을 중심으로 얼마나 흩어져 있는지를 나타내고, x와 y의 공분산은 x, y의 흩어진 정도가 얼마나 서로 상관관계를 가지고 흩어져 있는지를 나타낸다. 공분산 행렬(covariance matrix) C는 데이터의 좌표 성분들 사이의 공분산 값을 원소로 하는 행렬로서 데이터의 I번째 좌표와 j번째 좌표의 공분산 값을 행렬 i행 j열 원소값으로 하는 행렬을 말한다[1].

$$x = [x_1, \dots, x_n]^T : n\text{차원 } T\text{갓수의 열벡터}$$

$$y_1 = a_{11}x + a_{12}x + \dots + a_{1p}x_p = a_1^T x$$

$$y_n = a_{p1}x_1 + a_{p2}x_2 + \dots + a_{pp}x_p = a_p^T x$$

$$C = E[(x_i - m_x)(x_j - m_{x_j})] : n \times n \text{행렬}$$

아래 식에서 주성분 분석 세분화 변수 중 제1세분화 변수는 데이터의 특성을 가장 잘 반영하는 변

수이며(고유벡터 e_1), 제2세분화변수는 e_2 로 다음과 같이 정의된다.

$$Ce_i = \lambda_i e_i$$

e_i : eigenvector of c

λ_i : eigenvalue, e_i 방향으로의 분산

$$\lambda_1 \geq \dots \geq \lambda_n \geq 0$$

e_1 : 분산이 가장 큰 방향

e_2 : e_1 에 수직이면서 다음으로 가장 분산이 큰 방향

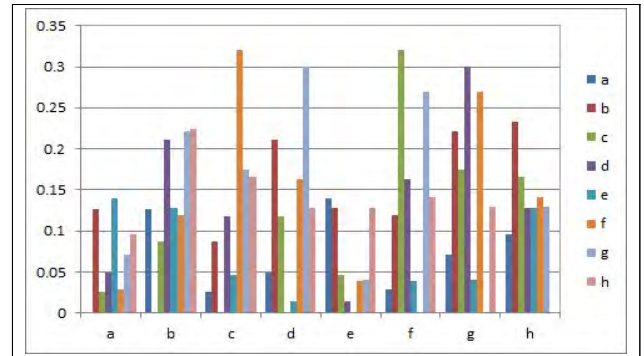
e_k : e_1, \dots, e_{k-1} 에 모두 수직이면서 가장 분산이 큰 방향

제1세분화변수 이후의 세분화변수는 제1세분화변수로 설명할 수 없는 자료의 변동을 설명하며 제k세분화변수로 갈수록 원래 데이터에 대한 특징 반영도는 낮다고 볼 수 있으며 고유값(eigenvalue) 그래프를 사용하여 세분화 변수 수를 결정한다[1-4].

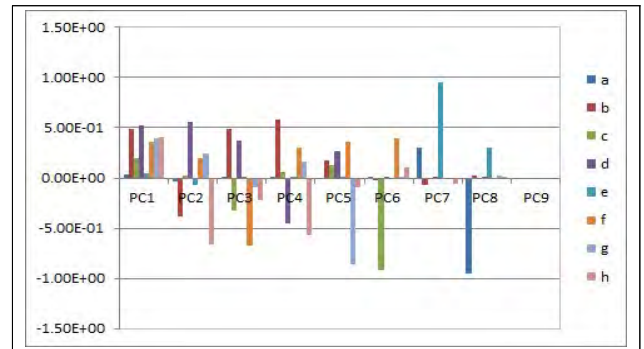
3. 상관도 기반 세분화 변수 선정

본 논문에서는 전체 데이터에 대한 주성분분석 결과에 대하여 상관도를 기반으로 하여 세분화변수를 결정하고자 한다. 또한, 변수간의 상관도를 적응적으로 고려함으로써 전체 데이터에 대한 세분화 변수를 결정하고자 한다. 먼저, 상관 분석을 수행한 후 상관도(Correlation) 결과 값을 기반으로 상관도가 높은 데이터 변수를 제거해 나간다. 세분화 변수 수를 결정하기 위하여 고유값(eigenvalue) 그래프를 사용하여 세분화 변수 결정시에 서로 밀접하게 영향을 끼칠 수 있는 변수들의 영향을 최소화하기 위하여 상관도가 높은 변수들을 차례로 제거한 후 고유값 그래프를 완성함으로써 적응적으로 세분화 변수를 개수 결정에 반영하고자 한다. 다음 그림 1은 8개 변수 1000개(변수a~변수h, generatedata.com)에 대하여 변수 간의 상관도를 계산한 결과이며, 여기에서 (b,d), (c,f), (b,g), (d,g), (f,g), (b,h)의 상관도가 높게 나타남을 알 수 있다. 상관도가 높음으로 인하여 데이터 주성분 분석의 세분화변수가 편향되게 결정되는 것을 막기 위하여 앞에서 나타난 여러 변수와 중복적으로 상관도가 높은 변수들 중 (b,d), (b,g), (b,h)쌍에서 변수 b와 (b,g), (d,g), (f,g) 쌍에서 변수 g가 세분화 변수 선정 시 편향화를 초래할 수 있으므로 이 두 변수 b와 g를 제거 대상으로 선정한다. 다음 단계로 전체 데이터에 대하여 PCA eigenvector 계수 값을 구한 후 두 데이터 변수간의 eigenvector 계수 값이 낮은 것을 차례로 제거해 나간다. 다음 그림 2는 8개의 변수에 대한 PCA 결과를 보여주는 그래프이다. 여기서 eigenvector 계수

값이 낮은 PC9, PC8 순으로 세분화 변수(변수a, 변수e)를 제거하는 방식으로 처리한다.



(그림 1) Correlation coefficient of input data



(그림 2) PCA of input data

4. 분석 및 결론

본 논문에서는 입력 데이터의 주성분 분석의 세분화변수 결정시 데이터 편향성의 영향을 줄이기 위해 여러 변수와 중복적으로 상관도가 높은 변수로 분석된 변수를 적응적으로 제거하는 방법을 제안하였다. 주성분 분석 결과인 PC1, PC2 등의 주성분(데이터 특징)을 추출 시 상관 관계를 기반으로 상관도가 높은 변수들을 차례로 제거한 후 8개 변수에 대하여 고유값(eigenvalue) 그래프를 도식하면 주성분분석의 세분화 변수는 적응적 상관도 적용 전 b,f,h,d에서 a,c,d,e로 선정되었음을 알 수 있으며 편향성 유도 변수는 세분화 변수에 포함되지 않았음을 알 수 있다.

참고문헌

- [1] I.T. Jolliffe, "Principle Component Analysis" Springer-Verlag, New York, 1986.
- [2] B. J. Kim, et al, "On-line Nonlinear Principal Component Analysis for Nonlinear Feature Extraction", The Journal of KISS, 31(3) pp.361-368, 2004.
- [3] Y. J. Kim, "Evaluation of Urban Lakes Water Quality Using Principle Component Analysis", The Journal of KSEA, 9(2) pp.197-203, 2003.
- [4] H.J. Joo, N.H. Kim et al, "A Study on Data Types and Visualization for Traffic Congestion and Accidents", Proceeding of IEIE, 2019, pp1011-1013.

제53회
2020 온라인 춘계학술발표대회

**병렬 및
분산컴퓨팅**



다기관 임상연구를 위한 의료 데이터 셋 관리 시스템

이충섭¹, 김승진¹, 김지언¹, 노시형¹, 김태훈^{1,3}, 윤권하^{1,2,3}, 정창원^{1,3}

¹원광대학교 의료융합연구센터

²원광대학교 의과대학 영상의학과

³원광대학교병원 스마트헬스 IT 사업단

e-mail : {cslee99, koch369369, kakasky112, nosij123, tae_hoonkim, khy1646, mediblue}@wku.ac.kr

Medical Dataset Management System for Multi-Center Clinical Research

Chung-Sub lee¹, Seung-Jin Kim¹, Ji-Eon Kim¹, Si-Hyeong No¹, Tae-Hoon Kim^{1,3},
Kwon-Ha Yoon^{1,2,3}, Chang-Won Jeong^{1,3}

¹Medical Convergence Research Center, Wonkwang University

²Dept of Radiology, Wonkwang University School of Medicine and Hospital

³Smart Health IT Center, Wonkwang University Hospital

요 약

본 논문은 국제표준화인 OHDSI OMOP-CDM의 확장으로 의료영상 표준기반의 R_CDM으로 변환하고 그 데이터를 기반으로 다기관 임상연구를 위한 관리시스템에 대해 기술한다. 이를 위해 기존 공통 데이터모델과 연계에 중점을 두어 DICOM 태그정보를 기반으로 의료영상 표준 모델의 스키마와 다기관 연구를 위한 Report 정보를 포함하여 모델링하였다. 이를 기반으로 머신러닝 기술개발을 위한 데이터 셋 생성과 관리를 위한 웹 기반 시스템 구조와 기능에 대해서 기술한다. 끝으로 구현된 시스템에서 제공하는 웹 서비스 수행 결과를 보인다.

1. 서론

제 4 차 산업혁명의 핵심 기술인 사물인터넷, 인공지능, 클라우드, 빅데이터는 의료 서비스의 패러다임을 변화시키고 있다[1]. 특히, 임상데이터기반의 인공지능(AI), 빅데이터 분석 관련 기업이 급성장하고 있다[2]. 최근 1 차병원과 2, 3 차병원간 진단과 처방 등 진료기록을 교류하는 시스템을 구축하는 사업을 국가적으로 추진하고 있다. 이러한 시스템 개발에 있어서 가장 중요한 요소는 표준화 연계모델 고도화를 위해 국제표준화 용어(SNOMED_CT)를 사용한다. 이와 관련하여 OHDSI(Observational Health Data Science and Informatics)에서 제안하는 공통데이터모델(CDM)[3]은 임상데이터기반 연구를 위한 의료정보의 표준화에 대한 대표적인 모델이다. 이를 기반으로 다기관 공동연구 플랫폼으로 분산형 바이오헬스 빅데이터 플랫폼(FEEDER-NET)이 개발되어 국내외 공동연구가 활발하게 진행되고 있다[3]. 그동안 우리는 OMOP-CDM을 기반으로 의료영상표준인 DICOM의 태그 정보를 추출하여 메타데이터의 표준화와 의료영상데이터의 관리에 중점을 둔 R_CDM을 제안하였다. 우리가 제안한 R_CDM은 머신러닝 연구를 위한 표준화된 의료

영상 데이터셋을 검색하여 다양한 형태로 생성할 뿐만 아니라 다기관 공동연구를 위한 표준화된 영상정보를 수집하고, 익명화된 데이터를 공유할 수 있다. 그러나 실제 활용하기 위해서는 수집된 의료영상기반의 데이터셋 뿐만 아니라 의료영상에 대한 설명을 리포트하는 기능이 요구되었다. 그리고 다기관 영상정보를 관리하기 위한 이질성 문제(DICOM 헤더 정보, 파일 확장자 등)를 해결해야 했다.

본 논문에서는 웹 기반으로 다자간 임상연구를 위한 의료영상 데이터 셋 관리 시스템에 대해서 기술한다.

2. 관련 연구

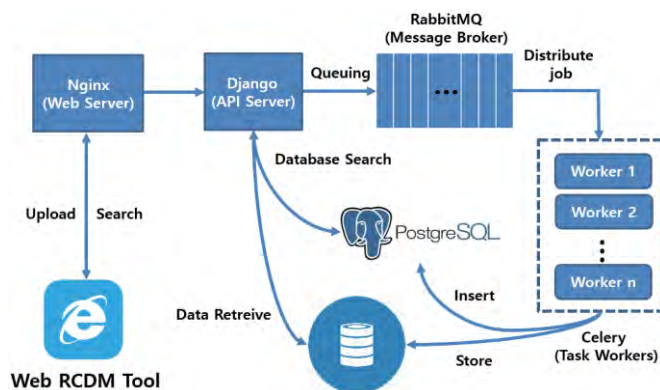
OMOP-CDM은 정형화된 임상데이터를 표준화하는데 중점을 두고 있다. 그러나 최근 유전체, 영상 그리고 생체신호와 같은 비정형 데이터의 표준화로 확장하고 있다. 특히, 현재 각 병원에서는 PACS를 사용하여 DICOM 국제 표준을 준수하여 저장하고 있으나 이러한 방대한 양의 데이터가 있더라도 실제 임상연구를 위해서는 각 질환 별로 최적화된 임상 프로토콜에 의한 선별, 핵심적인 의료영상에 저장되는 의료정보까지

¹ This study was supported by the Korea Health Technology R&D Project through the Korea Health Industry Development Institute(KHIDI), funded by the Ministry of Health & Welfare(HI18C1216, HI18C2383) and the Technology Innovation Program (or Industrial Strategic Technology Development Program(20001234)).

표준화되어 저장되어야 한다[4]. 이와 관련하여 수행된 연구는 국내외에서도 미흡하며 더욱이 의료기관별 의료영상의 표준화된 정보 없이 인공지능 학습 연구에 적용하기에는 어려움이 있다[5]. 또한 인공지능 학습을 위해서는 방대한 양의 의료영상 데이터가 요구되며, 인공지능 알고리즘의 최적화에 필요한 검증 및 테스트 데이터 수집도 매우 어렵다. 이러한 문제점을 해결하기 위해 의료영상에 대한 표준화의 요구사항을 정리하였고, 기존의 OMOP-CDM 과 연계하여 확장 모델을 제시하였다[6]. 또한 다기관 공동연구를 위한 영상데이터에 대한 리포트 기술에 대한 요구사항에 따라 기존 제시한 R_CDM 관리 시스템을 개선하고자 한다.

3. 제안 시스템

본 논문에서 제안하는 다기관 임상연구를 위한 의료 데이터 셋 관리 시스템은 각 기관에서 수집한 데이터를 R_CDM 기반의 표준화된 데이터로 변환하여 함께 공유하고 해당 영상에 대한 Report 를 작성하여 다기관 공동연구가 가능하도록 개발되었다. 본 시스템의 구조는 다음 그림 1 과 같다.



(그림 1) 다기관 의료 데이터셋 관리 시스템

React UI Library 기반의 Front-End (Web Client) 와 Python Django Rest Framework 기반의 Back-End (REST API Server)를 설계하였다. 또한, 각 기관에서 발생하는 대량의 의료 데이터를 수집하기 위해 Nginx 웹 서버와 Message Queue, Task Worker 을 통해 비동기 분산 업로드 방식을 도입하였다. 의료기관의 데이터 관리 시스템은 환자 정보를 비식별화 해야하기 때문에 익명화(Anonymize)를 지원하고 Client 와 Server 간의 통신프로토콜을 암호화하여 전송된 환자 정보 및 데이터에 대한 보안을 유지하도록 SSL:보안소켓 계층(Secure Sockets Layer) 프로토콜을 지원하고 있다.

3-1. 의료영상정보 표준화를 위한 데이터베이스 설계

본 논문에서 제안한 다기관 임상연구를 위한 의료 데이터 셋 관리 시스템의 DB 설계는 다음 그림 2 와 같다. 데이터베이스는 크게 Radiology CDM 기반의 의료영상 표준화를 위해 DICOM 태그 정보로부터 추출되는 데이터 셋의 촬영 정보를 저장하기 위한

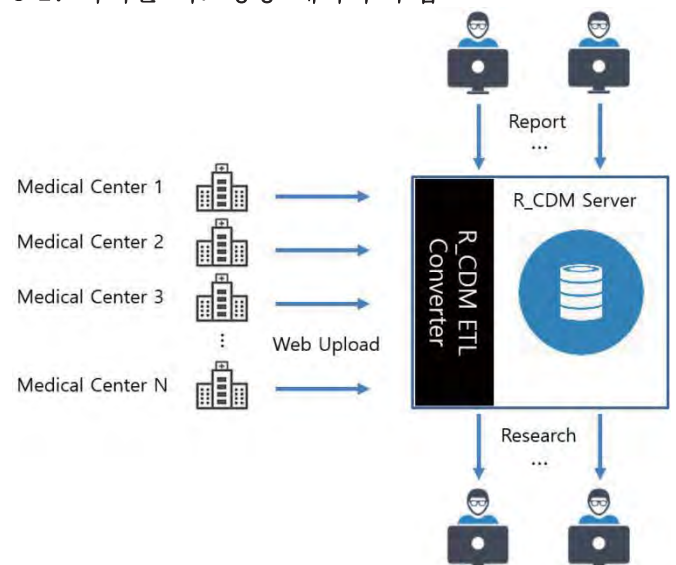
Radiology Occurrence 테이블과 각 데이터 셋에 포함된 이미지들에 대한 정보를 저장하는 Radiology Image 테이블로 설계하였다.



(그림 2) R_CDM 을 위한 데이터베이스 스키마

또한, 각 데이터 셋의 정보를 표준화하기 위해서 병원 별 촬영 조건이 담긴 Radiology Protocol, 어떤 질환에 대한 영상인지를 판단할 수 있는 Radiology Condition, 어떤 자세로 촬영된 지 판단할 수 있는 Radiology Person Position, 촬영된 Modality 를 판단할 수 있는 Radiology Modality, 의료영상의 각종 단위를 표시하는 Radiology Units, 영상에 촬영한 장비를 표시하는 Radiology Device, 영상이 촬영된 병원을 표시하는 Radiology Hospital 정보, 해당 영상의 임상적 의견을 관리하는 Radiology Report 등 임상연구에 필요한 정보를 저장하기 위한 테이블로 설계하였다

3-2. 다기관 의료영상 데이터 수집



(그림 3) R_CDM Workflow

웹 기반으로 구축된 시스템은 다 기관으로부터 의료영상 데이터를 그림 3 과 같이 R_CDM 으로 변경하여 데이터를 수집할 수 있다. R_CDM 으로 표준화하여 저장된 데이터는 관독의로부터 해당 영상의 Report 를 작성하여 소견을 작성할 수 있다. 이러한 소견을 바탕으로 특정 질환군에 세부적인 검색 조건이 되어 연구자들에 의해서 필요한 데이터셋을 생성하여 연구에 사용될 것으로 전망된다

표 1 과 같이 Radiology Report 테이블은 Radiology Occurrence Table 과의 연결성을 갖기 위해 Study Instance UID 를 Key 로 관리되고 있고 Report 생성일, Report 결과에 대한 컬럼을 포함한다.

<표 1> Report 를 위한 임상 정보

Table Name	Column	Remarks
Report Table	Study Instance UID	Occurrence Table
Report Table	Modality	Occurrence Table
Report Table	Study Date	Occurrence Table
Report Table	Report Create Date	Create
Report Table	Report Approval Date	Create
Report Table	Report Text	Create

Radiology Occurrence List 는 각 기관으로부터 수집된 데이터의 전체를 그림 4 와 같이 보인다. 또한 사용자가 원하는 조건(질환별, 디바이스, 모달리티 등)으로 검색할 수 있다. 좀더 확장된 검색 기능으로 특정 키워드의 일부분만 입력해도 해당 Occurrence 를 찾고 멀티 키워드를 입력해도 해당 키워드에 맞는 Occurrence 를 검색할 수 있는 기능을 제공한다. 또한 해당 Radiology Occurrence List 에서 검색한 결과를 데이터셋으로 생성하여 다운로드 받을 수 있다.

(그림 4) Radiology Occurrence List

3-3. 데이터 셋 생성 및 다운로드

의료영상을 기반으로 인공지능 연구를 위해서는 해당 연구목적에 맞는 데이터 셋을 확보하여 반복적인 학습을 통해 알고리즘을 개발한다. 그리고 개발된 알고리즘에 대해서 Internal/External 검증을 통해 마무리한다. 최근 임상시험을 위한 e-CRF 시스템이 자동화 패키지를 가진 시스템으로 대안이 되었으나

매번 연구 종료 함께 데이터의 재활용이 불가능하다. 또한 연구자가 원하는 형태의 데이터 포맷으로 생성하기에는 어려움이 있다. 데이터의 규모가 증가함에 따라서 사용자의 요구에 따른 데이터 셋을 자동으로 생성하는 기능이 필요하다. 그림 5 와 같이 Phase, Plane 형태에 따라 데이터 셋 다운로드 기능을 설계하였다. 분류 기준은 의료영상의 해부학적 포지션에 따라서 Plane Mode 기능을 설계하였고, 의료영상의 촬영 시간에 따라서 Phase Mode 를 설계하였다. 데이터 셋 생성 기능을 제공함으로써 인공지능 연구를 수행하기 위한 필요한 데이터 셋을 제안한 시스템을 통해서 해결할 수 있다.

(그림 5) 커스텀 데이터 셋 다운로드

3-4. 다기관 연구를 위한 Report 관리

논문에서는 다기관에서 수집된 표준화된 의료영상에 임상적 의미를 부여하기 위해서 그림 6 과 같이 Report 입력을 제공하고 있다. 또한 해당 영상을 공유한 연구자들은 해당 영상의 Report 를 확인할 수 있다.

(그림 6) Report 입력 및 뷰 다이얼로그

4. 결론

본 논문에서는 다기관 연구를 위한 의료영상정보의 표준화와 인공지능 기반의 임상연구를 위한 데이터 수집 및 커스텀 데이터 셋을 제공하는 웹 기반의 관리시스템을 제안한다. 구축된 웹 기반 관리시스템을

통해 인공지능 기반의 임상 연구에 적용하기 위한 학습 또는 검증 그리고 테스트 데이터를 위한 데이터셋을 제공할 수 있음을 보였다. 그리고 기존 CDM 과 연계하여 다 기관 임상연구를 수행할 수 있는 Report 입력을 보였다. 향후 연구내용으로는 표준화 작업을 통해 변환된 각 의료영상 이미지를 다기관 연구를 위한 각 기관별 통계를 보여주고 웹 기반 관리시스템 상에서 다양한 정량화 분석 툴들을 지원하여 다기관 분석 연구를 위한 이미지 뷰어 개발을 진행할 예정이다. 또한, 수집된 데이터를 활용하여 웹 기반 관리시스템 상에서 다양한 인공지능 학습 모델에 생성된 데이터 셋을 학습시키고 최적의 알고리즘 개발을 지원하는 실증 연구를 수행할 계획이다.

참고문헌

- [1] 4 차 산업혁명 대정부 권고안, <https://www.4th-ir.go.kr/>
- [2] 박성욱, “빅데이터 기법을 활용한 Data Technology의 키워드 분석”, 기술혁신학회지, 제 22 권, 2 호 pp. 265~281.
- [3] OHDSI Forum, <https://forums.ohdsi.org/t/oncology-radiology-imaging-integration-into-cdm/2018/7>
- [4] W.Dean Bidgood, Jr., MD, MS, Steven C. Horii, MD, Fred W. Prior, PhD, and Donald E. Van Syckle “Understanding and Using DICOM, the Data Interchange Standard for Biomedical Imaging,” Vol. 4, No. 3, pp. 199-212, May-Jun 1997.
- [5] Adrian V. Dalca, Katherine L. Bouman, William T. Freeman, Natalia S. Rost, Mert R. Sabuncu, Polina Golland, “Medical Image Imputation From Image Collections,” IEEE transactions on medical imaging, Vol. 38, No. 2, pp. 504-514, Feb 2019.
- [6] OHDSI/Radiology-CDM, <https://github.com/OHDSI/Radiology-CDM>

KVM 가상머신에서 도커를 사용하는 시스템의 호스트 메모리 부하에 따른 task 처리 성능 분석

장용현, 이재학, 유현창
고려대학교 컴퓨터학과

wkd3475@gmail.com, {smreodmlvl, yuhc}@korea.ac.kr

Analysis of task processing performance depending on the host memory load of the system using the docker in the KVM virtual machine

Yong-Hyeon Jang, Jaehak Lee, Heonchang Yu
Dept. of Computer Science, Korea University

요 약

도커는 하드웨어 가상화를 지원하는 KVM과 달리 호스트의 커널을 공유하기 때문에 보안적인 문제가 생길 수 있다. 또한, 도커는 호스트 OS에 종속적이기 때문에 다른 OS에 종속적인 컨테이너를 실행할 수 없다는 단점도 있다. 이를 보완하기 위해 KVM을 이용해 가상머신을 실행하고 가상머신에서 도커를 이용하면 도커와 KVM의 장점을 살린 시스템을 구성할 수 있다. 실제 이 시스템의 실효성과 안정성을 평가하기 위해 실험을 진행하였고, 호스트의 메모리만 충분하다면 실효성과 안정성이 보장됨을 확인하였다.

1. 서론

도커는 cgroups와 namespace를 이용하여 호스트의 커널을 공유하고 독립적인 컨테이너를 실행한다. cgroup은 리눅스 커널에서 제공하는 자원에 대한 제어를 가능하게 해주는 기능이고, namespace 역시 리눅스 커널에서 제공하는 독립적인 공간을 제공하여 충돌을 방지해주는 기능이다. 이를 통해 기존의 하드웨어를 가상화하는 KVM과 같은 하이퍼바이저를 이용한 가상화 기법보다 더 적은 용량으로 빠르게 격리된 환경을 제공할 수 있다.

하지만 컨테이너가 호스트의 커널을 공유하기 때문에 작동 중인 컨테이너 중에 하나라도 공격을 당하게 된다면 호스트 커널을 통해 다른 컨테이너 까

지 영향을 줄 수 있다. 그러나 하드웨어를 가상화하는 KVM은 완전히 분리된 환경을 제공하기 때문에 하나의 가상머신이 공격당해도 다른 가상머신에는 영향을 주지 않는다. 그리고 컨테이너는 호스트 OS 커널에 종속적이기 때문에 다른 OS 환경을 사용할 수 없지만 하드웨어 가상화를 통해서는 호스트 OS와는 다른 가상화된 OS를 사용할 수 있다.

위와 같은 이유로 도커는 기존 하드웨어 가상화를 완전히 대체할 수 없고 이를 보완하기 위해 KVM의 가상머신에서 도커 컨테이너를 실행시켜 컨테이너가 공격당해도 공격당한 가상머신에서만 타격을 입고 다른 가상머신에는 영향을 주지 않게 구성을 할 수 있다. 또한, 이렇게 시스템을 구성하면 컨테이너가 구동되는 게스트 OS가 호스트와 다른 OS를 기반으로 실행될 수 있기 때문에 다른 OS에 종속적인 컨테이너를 실행할 수 있다는 장점을 얻을 수 있다. 실제로 아마존과 구글에서 컨테이너 호스팅을 지원하지만 보안을 위해서 가상머신을 이용하여 공간을 격리시키고 그 위에서 컨테이너를 실행하게 한다[1].

본 논문에서는 KVM 가상머신에서 도커 컨테이

I "본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구 센터지원사업의 연구결과로 수행되었음" (IITP-2018-0-01405)

II 이 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2018-0-00480)

너를 실행시키는 환경의 실효성을 확인하기 위해 실제 서비스 환경에서의 성능 평가를 수행하고자 한다. 이를 평가하기 위해 기존 시스템 모델과 비교하여 KVM 가상머신에서 도커 컨테이너를 실행할 때 각 서버의 task 처리 속도에 어떤 영향이 생기는지를 평가한다. 또한, 각각의 시스템에 대해 호스트의 메모리에 부하가 늘어남에 따라 서버의 task 처리 속도에 미치는 영향을 평가하여 안정성에 대한 평가도 진행한다.

2. 관련 연구

Xuehai Tang이 2014년에 작성한 “Performance Evaluation of Light-Weighted Virtualization for PaaS in Clouds” 논문을 살펴보면 도커와 KVM에서의 Isolation Performance를 측정하였다. 메모리 stress에 대해서는 도커는 43.3% 성능 저하, KVM은 4.2%의 성능 저하를 보여주었고, Disk stress에 대해서는 도커는 34.7%의 성능 저하, KVM은 20.9%의 성능 저하를 보여주었다. 그리고 도커와 KVM 모두 CPU stress에 대해서는 0%의 성능 저하를 보여주었다[2].

위 논문의 실험을 통해 각각의 실험에 사용되는 시스템의 호스트 메모리에 부하를 주면 성능 간섭이 발생할 것을 예상해볼 수 있고, 실제로 부하를 주어 각 서버의 task 수행 시간에 어떤 영향을 미치는지를 확인하고자 한다.

3. 실험 환경 구성 및 수행 방법

3.1 실험 환경 구성

KVM 가상머신에서 도커 컨테이너를 이용해 실행 중인 서버의 성능을 기존 시스템 모델들과 비교하기 위한 실험과 KVM 가상머신에서 도커 컨테이너를 이용해 실행 중인 서버의 안정성을 평가하기 위해 메모리 부하가 있을 때 서버들 사이의 성능 균형이 유지되는지를 평가하는 실험을 진행하도록 한다.

실험에 사용되는 컴퓨터 HostA와 HostB의 사양은 <표 1>과 같다. 그리고 HostA와 HostB에서 KVM으로 실행되는 하나의 가상머신의 성능은 <표 2>와 같다.

<표 1> 실험 환경

	HostA	HostB
CPU	Intel(R) Core(TM) i5-6400 CPU @ 2.70GHz, 4 cores	Intel(R) Core(TM) i5-6400 CPU @ 3.40GHz, 4 cores

RAM	8G	32G
Disk	1TB	1TB
OS	Ubuntu 18.04 LTS	Ubuntu 18.04 LTS

<표 2> 가상머신

	HostA	HostB
vCPU	1 core	1 core
RAM	1G	2G
Disk	15GB	15GB
OS	Ubuntu server 18.04.04 LTS	Ubuntu server 18.04.04 LTS

1) 서버 및 클라이언트 구성

서버는 node.js express를 이용해서 제작하였으며, get 요청을 받으면 2,000,000번 write 작업을 수행하여 약 30MB 크기의 파일을 생성 후 저장한다. 그리고 task 수행 시간을 클라이언트에게 반환해준다. 클라이언트는 한 회차에 4개의 서버에 동시에 request를 전송하며, 수행 시간을 전부 받고 나서 task 수행 시간을 저장 한 후에 다음 회차로 넘어간다. 그리고 이런 과정을 총 50회 수행한다.

2) 메모리 부하

메모리 부하는 stress 툴[3]을 사용한다. stress 툴의 -m 옵션을 통해 부하를 주는 프로세스의 갯수를 정할 수 있고, 하나의 프로세스당 256MB 만큼의 malloc 작업을 수행하는 것이 default로 설정이 되어있다.

3.2 실험 수행 방법

본 실험은 기존 시스템 모델과 도커를 KVM 가상머신에서 실행하는 환경의 성능 비교와 도커를 KVM 가상머신에서 실행할 경우 호스트의 메모리 부하에 따라 각각의 가상머신의 도커 컨테이너의 성능이 균등하게 유지가 되는지를 평가하기 위해 총 4가지의 시스템 모델에 대하여 메모리 부하 작업을 수행한다.

메모리 부하 작업은 stress 툴의 -m 옵션으로 stress를 주는 프로세스의 갯수를 HostA는 1개씩 늘려가며, HostB는 20개씩 늘려가며 호스트의 메모리 부하가 증가함에 따라 각각의 서버에 생기는 영향을 평가한다. 4가지의 실험 유형은 3.3과 같다.

3.3 실험 유형

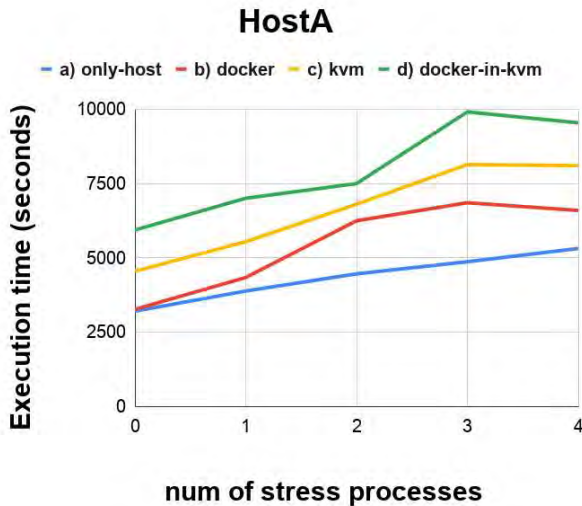
a) 호스트 컴퓨터에서 작동 중인 4개의 api 서버에 대한 성능 평가

b) 호스트 컴퓨터에서 도커 컨테이너로 격리되어 작동 중인 4개의 api 서버에 대한 성능 평가

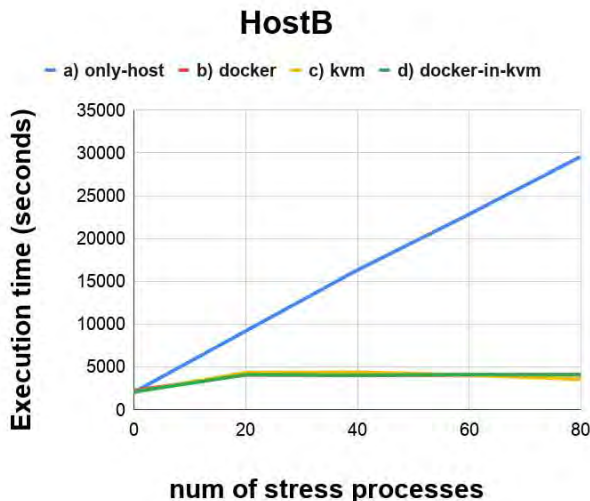
- c) 4개의 가상머신에서 격리되어 작동 중인 4개의 api 서버에 대한 성능 평가
- d) 4개의 가상머신에서 격리되어 도커 컨테이너로 작동 중인 4개의 api 서버에 대한 성능 평가

4. 실험 평가

4.1 기존 시스템 모델과 성능 비교



(그림 2) HostA, 시스템별 서버 평균 task 수행 시간



(그림 3) HostB, 시스템별 서버 평균 task 수행 시간

(그림 2) HostA에서 실험한 시스템들의 성능을 보면 평균적으로 호스트에서만 서버를 운영한 것보다 도커를 사용한 시스템에서는 1.26배, KVM를 사용하는 시스템에서는 1.53배, KVM에서 도커를 사용하는 시스템에서는 1.84배만큼 처리 속도가 느려짐을 확인할 수 있다. 그러나 (그림 3) HostB에서는 호스트에서만 서버를 운영한

시스템만 호스트의 메모리 부하가 증가함에 따라 수행시간이 비례해서 증가하고, 나머지 시스템에서는 호스트의 메모리부하가 증가해도 메모리 부하가 없을 때보다 1.9배 이상으로 처리 속도가 느려지지 않는 것을 확인할 수 있다.

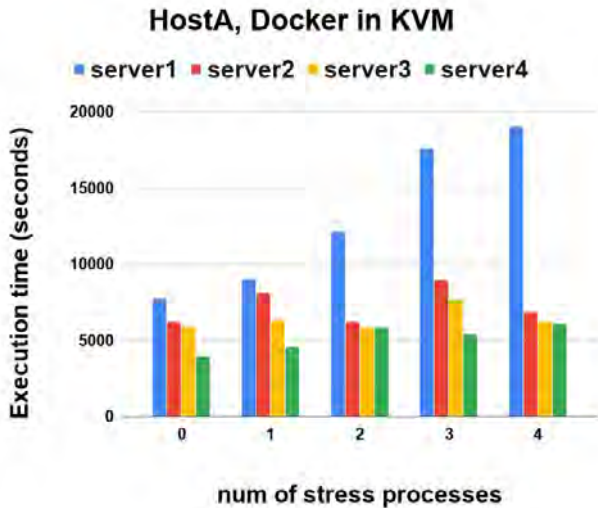
HostA와 HostB에서 실험한 결과의 차이가 생기는 이유는 HostA가 가상머신 4개를 운영하기에는 메모리 용량이 부족하기 때문이다. 호스트의 메모리 부족으로 메모리 스왑이 많이 발생하게 되고 이로 인해 도커보다 메모리를 더 많이 사용하는 가상머신이 더 많은 성능 저하를 일으켰다고 볼 수 있다.

그리고 HostA에서 메모리 스왑이 많이 발생한 원인으로 Memory Ballooning이 발생했다고 볼 수 있다. Memory Ballooning은 호스트의 메모리가 부족하고 게스트 가상머신의 메모리는 여유가 있을 때 발생한다. 이런 상황이 발생하면, Balloon Controller가 게스트 OS 내부의 메모리를 inflate시켜 메모리 스왑을 일으키고 메모리의 내용을 disk로 스왑 아웃하여 비워낸다. 이를 통해 호스트 OS의 메모리 공간을 확보하게 된다[4]. 그리고 Memory Ballooning으로 인한 가상머신의 성능 저하를 막기 위해 Memory Ballooning을 비활성화하는 시도도 존재한다[5]. 실제 본 실험 과정에서 HostA는 가상머신을 4개를 실행시키면 스왑 공간이 사용됨을 확인하였고, 이를 통해 HostA에서는 Memory Ballooning이 발생해서 성능 저하가 일어났다고 볼 수 있다.

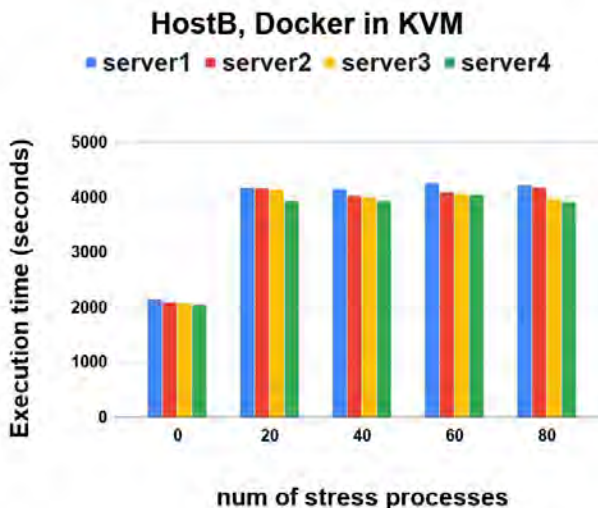
하지만 HostB처럼 호스트 OS의 물리적 메모리가 충분한 경우에는 메모리 스왑이 발생하지 않아 게스트 OS의 성능 저하가 거의 일어나지 않았음을 확인할 수 있다. 이 실험을 통해 호스트의 메모리가 충분하다면 KVM 가상머신을 사용하여도 서버의 성능은 도커만을 사용할 때와 비슷한 성능을 보여준다는 것을 확인할 수 있어 이러한 시스템의 실효성을 확인할 수 있다. 그리고 도커나 KVM과 같은 가상화를 이용하면 호스트에서 바로 서버를 운영하는 것 보다 안정적으로 성능을 유지할 수 있음을 확인할 수 있다.

4.2 메모리 부하에 따른 각 서버 사이의 간섭 현상 측정

(그림 4) HostA에서의 실험 결과를 보면, 가상머신 4대를 실행시키는 것 자체만으로도 호스트의 메모리에 부하가 심해 각 서버에서 성능 차이가 생기는 것을 확인할 수 있다. 그리고 메모리의 부하가 증가함에 따라 성능의 불균형이 더 심해지는 것을 확인할 수 있다. 이를 통해, KVM에서 실행되는 게스트 OS는 호스트 메모리에 심한



(그림 4) HostA, docker in kvm의 서버별 task 수행시간



(그림 5) HostA, docker in kvm의 서버별 task 수행시간

부하가 생기면 성능 불균형이 발생함을 확인할 수 있다,

(그림 5) HostB에서는 HostA에서와는 다르게 서버들 사이의 성능이 비교적 비슷하다는 것을 확인할 수 있다. 이런 결과나 나온 이유로 호스트의 메모리가 충분하여 Memory Ballooning과 같은 성능에 영향을 줄 수 있는 원인이 발생하지 않았기 때문이라고 유추한다. 그리고 이를 통해 호스트의 메모리가 충분하다면, 안정성을 보장함을 확인할 수 있었다.

5. 결 론

KVM을 이용해 가상머신을 실행하고 가상머신에서 도커를 이용하면 도커와 KVM의 장점을 살린 시스템을 구성할 수 있다. 그리고 실험을 통해 KVM 가상머신에

서 도커를 사용하는 시스템을 사용해도 호스트의 메모리만 충분하다면 실행되는 서버의 성능은 도커만 사용하는 시스템과 KVM만 사용하는 시스템과 동일한 성능을 보이고, 동시에 운영되는 서버 사이의 성능 균형도 보장함을 확인하였다. 그러나 호스트의 메모리가 충분하지 않으면, 성능 저하와 서버간의 성능 불균형이 발생함을 확인하였다. 그래서 도커와 KVM을 같이 사용하여 보안적인 문제를 해결하는 환경을 구축하는 것은 메모리가 적은 호스트에서는 권장되지 않으며, 메모리가 충분한 호스트에서 도커를 KVM에서 사용하는 시스템의 경우에는 운영하는 서버의 task 처리 성능 저하가 없고 동시에 운영하는 서버들 사이에 성능 균형을 보이기 때문에 실효성과 안정성이 보장됨을 확인하였다.

참고문헌

- [1] <https://xenproject.org/2015/08/11/will-docker-replace-virtual-machines/>
- [2] Xuehai Tang, Zhang Zhang, Min Wang, Yifang Wang, Qingqing Feng, and Jizhong Han, "Performance Evaluation of Light-Weighted Virtualization for PaaS in Clouds", ICA3PP Algorithms and Architectures for Parallel Processing, pp. 415 - 428, 2014
- [3] <https://linux.die.net/man/1/stress>
- [4] Chin-Hung Li, "Evaluating the Effectiveness of Memory Overcommit Techniques on KVM-based Hosting Platform", International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol.6, No.10, pp. 1218-1222, 2012
- [5] Nadav Amit, Dan Tsafir, Assaf Schuster, "VSwapper: a memory swapper for virtualized environments", ACM, pp. 349-365, March 1-4, 2014

Docker Swarm에서 컨테이너간의 메모리 자원에 대한 성능 간섭 측정

정진원, 이재학, 유헌창

고려대학교 컴퓨터학과

e-mail:{jin4812, smreodmlvl, yuhc}@korea.ac.kr

Measuring Performance Interference on Memory Resources between Containers in Docker Swarm

JinWon Jeong, JaeHak Lee, HeonChang Yu

Dept of Computer Science and Engineering, Korea University

요 약

Docker Swarm은 호스트 머신에서 여러 개의 컨테이너들을 실행할 때 발생하는 네트워크와 호스트 리소스 등을 포함한 여러 문제를 해결해 주기 위해 등장하였다. 하지만 컨테이너간의 메모리 경합으로 인한 성능 간섭 문제는 여전히 대두되고 있다. 본 논문에서는 성능 간섭 정도를 측정하기 위해 Docker Swarm을 이용하여 클러스터 환경을 구축하고 메모리 부하 작업을 수행하는 특정 스레드 개수 및 시간을 선정하여 다양한 실험을 진행하였다. 그 결과 특정 스레드 개수를 할당해 주었을 때 특정 시점에서 컨테이너간의 성능 간섭이 가장 크게 발생하였으며 그 이후의 시점부터는 성능 간섭 정도가 크게 나타나지 않는 것을 확인하였다. 이를 토대로 Docker Swarm에서 사용 중인 스케줄링 방법을 개선하여 컨테이너간의 성능 간섭을 최소화할 수 있는 향후 연구 방향을 모색할 수 있을 것으로 보인다.

1. 서론

Docker Swarm은 오픈소스 프로젝트인 Docker에서 공식적으로 만든 Docker 컨테이너를 위한 오케스트레이션 툴이다. 오케스트레이션 툴이란 여러 호스트 서버의 컨테이너들을 배포 및 관리하기 위한 툴을 의미한다. 즉, Docker Swarm을 이용하면 여러 개의 서버와 컨테이너들을 쉽게 관리할 수 있다. Docker Swarm은 manager노드와 worker노드로 구성된다. Manager노드는 Raft consensus algorithm을 이용해 클러스터에서 작동하는 다양한 서비스들이 일관된 상태를 유지할 수 있도록 관리한다. Raft consensus algorithm은 여러 서버 중 일부에 장애가 발생해도 나머지 서버가 정상적인 서비스를 제공할 수 있도록 해주는 합의 알고리즘이다. Worker노드는 manager

노드의 명령을 받아 컨테이너를 실행하는 노드를 의미한다. Docker는 호스트 OS의 커널을 공유하고 namespace를 기반으로 각각의 애플리케이션에 대한 격리된 환경을 제공한다. 사용자가 컨테이너를 실행하면, 해당 컨테이너에서 사용할 namespace를 생성하게 된다. Docker의 각 컨테이너는 자신에게 할당된 만큼의 자원을 점유할 수 있도록 격리되어야 한다. 여러 개의 컨테이너가 존재할 때 한 컨테이너가 자원을 초과해서 사용한다면 서로 간에 성능 간섭이 발생하게 되고 심각한 성능 저하 문제로 이어질 수 있게 된다[1]. 이러한 일이 발생하지 않도록 Docker는 각 컨테이너가 할당된 자원만큼만 사용하도록 조정하는데, 이때 리눅스의 cgroups를 이용해서 이 기능을 구현한다. 하지만 호스트 머신 내에서 메모리 서브시스템을 공유하는 컨테이너의 특성으로 인해 메모리 대역폭을 많이 사용하는 특정 컨테이너들이 실행되었을 때 성능이 저하되는 현상이 빈번히 발생하고 있다[2].

본 논문에서는 Docker Swarm을 이용하여 클러스

I “본 연구는 과학기술정보통신부 및 정보통신기획 평가원의 대한ICT연구센터지원사업의 연구결과로 수행되었음” (IITP-2018-0-01405)

II 이 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2018-0-00480)

터 환경을 구축한 후 각 worker노드에서 메모리 부하 작업을 수행하는 컨테이너가 작동할 때 발생하는 성능 간섭 현상을 분석한다. 이를 바탕으로 구성한 실험 환경에서 어느 정도의 부하를 주었을 때 특정 애플리케이션에 대한 작업 수행시간의 증가량을 통해 성능 저하 정도를 측정한다.

본 논문의 구성은 다음과 같다. 2장에서 실험 환경과 실험을 수행하는 방법에 대해 서술하고 3장에서는 메모리 부하 작업을 수행하는 스레드의 개수에 따라 프로그램의 성능이 저하되는 정도를 측정하는 실험을 수행 및 분석하고, 마지막 4장에서는 결론 및 향후 연구에 대해 서술한다.

2. 실험 환경 및 수행 방법

본 실험에서는 메모리 부하 작업을 수행하는 컨테이너 및 wordcount 작업을 수행하는 다수의 컨테이너를 각 worker 노드에게 동일한 개수로 배포한 뒤, 각 worker노드 내의 컨테이너들 간에 발생하는 성능 간섭 정도를 측정하기 위해 Docker Swarm을 이용한 클러스터 환경을 구축한다. 실험 환경은 <표 1>, <표 2>와 같다. Docker Swarm 클러스터는 manager 노드 1개, worker노드 5개로 구성한다. 물리 머신을 manager노드로 설정하였고, 각 worker노드는 드라이버가 virtual box로 설정된 docker-machine으로 구성하였다.

실험을 위한 애플리케이션으로 직접 구성한 특정 txt파일의 단어를 세는 작업을 총 10,000번 수행하는 wordcount 프로그램을 선정하였으며, 이를 통해 작업 수행시간의 결과 값을 도출한다. 메모리 부하 작업을 수행하는 애플리케이션으로는 리눅스 과부하 테스트 프로그램인 stress tool[3]을 이용하였다.

실험을 진행하기 위해 wordcount 프로그램의 image로 빌드된 컨테이너들이 아무런 성능 간섭 없이 동작했을 때와 메모리 부하 작업으로 인해 성능 간섭이 발생했을 때, 각 worker노드별 wordcount 컨테이너들의 작업 수행시간을 비교함으로써 성능 저하 정도를 측정한다. 각 실험마다 구분된 메모리 부하 작업을 수행하는 스레드의 개수는 1개, 5개, 10개로 구성하였으며 메모리 부하 작업의 시간(timeout)을 5초에서 시작하여 2000초까지 주었을 때 각 worker 노드 내 wordcount 컨테이너들의 작업 수행시간의 평균값을 측정하였다. 메모리 부하 작업에 따른 성능 간섭으로 인한 성능 저하 정도를 측정하기 위해 총 세 단계의 작업을 진행한다.

<표 1> 물리 머신 환경

CPU	i5-7500 CPU @ 3.40GHz x 4
RAM	32GB
HDD	1TB
OS	Ubuntu 18.04.4 LTS

<표 2> Docker Swarm 환경

구분	Manager 노드	Worker 노드
노드 수	1개	5개
RAM	27GB	1GB
HDD	924GB	20GB

가장 먼저 아무런 성능 간섭이 없었을 때 컨테이너들의 작업 수행시간을 측정한다. 5개의 worker노드에게 총 50개의 wordcount 컨테이너를 배포한다. 각 worker노드는 Docker Swarm 스케줄러에 의해 컨테이너를 10개씩 균등하게 배분받게 된다. 그 후 각 worker노드마다 배분받은 컨테이너들의 작업 수행시간을 측정한 뒤 평균값을 계산한다. 위 과정을 총 5번 수행해서 각각의 계산된 평균값을 가지고 최종적인 평균값을 계산하여 각 worker노드 내 컨테이너들의 작업 수행시간의 평균값을 나타낸다.

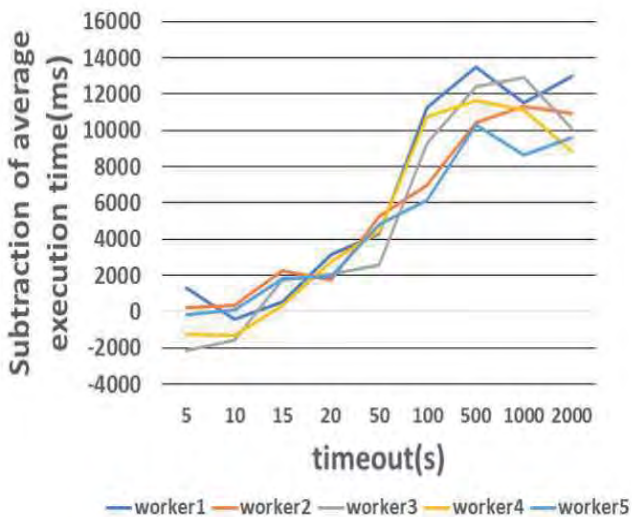
두 번째로 성능 간섭이 발생했을 때 컨테이너들의 작업 수행시간을 측정한다. 각 worker 노드가 10개의 wordcount 컨테이너를 배분 받은 상황에서 추가로 메모리 부하작업을 수행하는 컨테이너를 한 개씩 worker노드에게 배포한다. 그리고 각 worker노드 내에서 timeout마다 컨테이너들의 최종 작업 수행시간의 평균값을 위와 같은 방식으로 계산한다.

마지막으로 메모리 부하 작업을 수행하는 스레드 개수별로 timeout마다의 각 worker노드 내 컨테이너들의 작업 수행시간의 평균값에서 아무런 성능 간섭이 없었을 때 컨테이너들의 작업 수행시간의 평균값을 빼줌으로써 그 결과 값을 그래프로 나타낸다. 이를 통해 각 worker노드 내 컨테이너들 간의 메모리 경쟁으로 인한 성능 저하 정도를 측정한다.

3. 실험 결과 및 분석

[그림 1]은 메모리 부하 작업을 수행하는 스레드 개

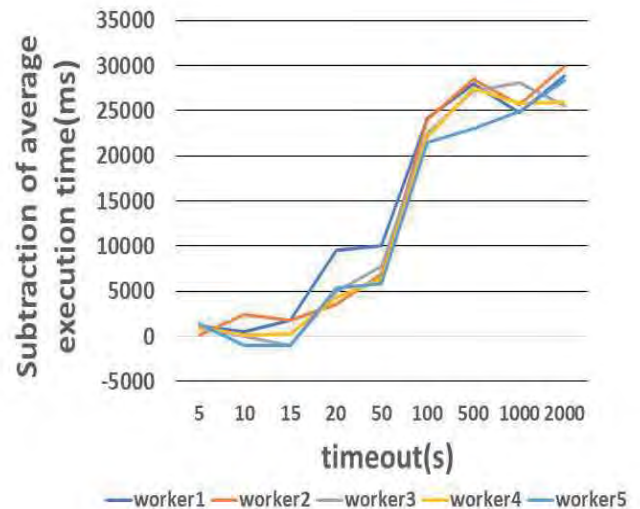
수가 1개일 때 timeout에 따른 각 worker노드마다의 작업 수행시간의 평균값 차이를 나타낸 그래프이다. Timeout이 5초 지점일 때 worker3과 worker4 그리고 worker5에서 작업 수행시간의 평균값 차이가 음수인 것을 볼 수 있다. 이는 오히려 메모리 부하 작업이 수행되었을 때의 경우가 평균적으로 작업 수행시간이 더 빨랐다는 것을 의미한다. 10초 지점일 때 도 worker1과 worker3 그리고 worker4에서 같은 상황을 보여준다. 이는 이에 해당하는 각 worker노드마다 5번의 반복 작업 중 몇몇의 경우에 컨테이너를 10개씩 배분 받았다가 Docker swarm 스케줄러에 의해 컨테이너가 재배포되어 최종적으로 작업을 수행한 컨테이너의 개수가 다른 worker노드에 비해 훨씬 더 적었던 것이다. 따라서 컨테이너들 간에 메모리 경합이 비교적 덜 일어났고 평균적으로 작업 수행을 더 빨리해낸 상황이 발생한 것으로 보인다. 15초 지점 이후부터는 각 작업 수행시간의 평균값이 점점 차이가 나면서 500초와 1000초 지점에서 각 worker노드마다 그래프가 최고점에 달성하는 것을 보였다. 그 이후의 시간부터는 그래프에 큰 변화가 없는 것을 볼 수 있으며, timeout을 더 늘려도 작업 수행시간의 평균값 차이는 더 이상 크게 나타나지 않았다.



[그림 1] 스레드가 1개일 때 수행시간의 평균값 차이

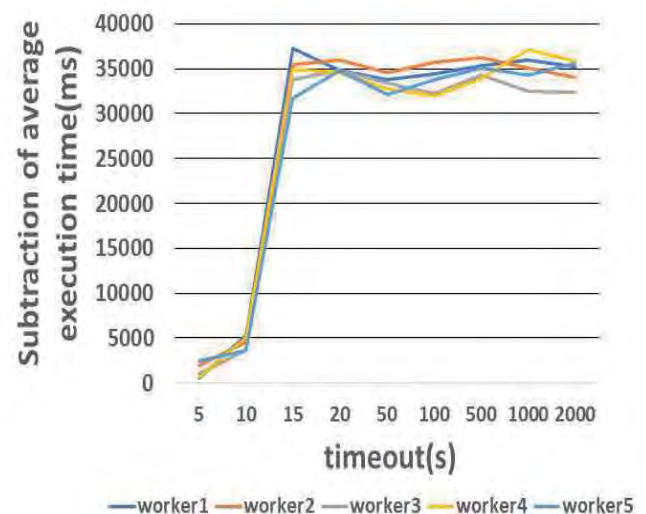
[그림 2]는 메모리 부하 작업을 수행하는 스레드 개수가 5개일 때 timeout에 따른 각 worker노드마다의 작업 수행시간의 평균값 차이를 나타낸 그래프이다. Timeout이 10초 지점일 때 worker5, 15초 지점일 때 worker3과 worker5에서 작업 수행시간의 평균값 차이가 음수인 것을 볼 수 있다. 이는 [그림 1] 설명에

서 서술한 내용과 같은 이유로 보인다. 그 이후의 시간부터는 각 worker노드마다 그래프가 증가하는 양상을 보이며 100초 지점일 때 크게 증가하는 모습을 볼 수 있다. 500초 지점 이후부터는 그래프에 큰 변화가 없는 모습을 보였다.



[그림 2] 스레드가 5개일 때 수행시간의 평균값 차이

[그림 3]은 메모리 부하 작업을 수행하는 스레드 개수가 10개일 때 timeout에 따른 각 worker노드마다의 작업 수행시간의 평균값 차이를 나타낸 그래프이다. [그림 1]과 [그림 2]를 보면 timeout이 500초와 2000초 지점 사이에서 큰 수치에 도달했고 [그림 3]은 15초 지점 일 때 모든 worker노드의 그래프가 급격하게 증가하는 것을 볼 수 있다. 이는 세 가지 실험 중에서 컨테이너들 간에 성능 간섭으로 인한 성능 저하가 가장 크게 일어난 모습을 보여준다. 그 이후부터는 그래프에 큰 변화가 없는 모습을 보였다.



[그림 3] 스레드가 10개일 때 수행시간의 평균값 차이

본 실험에서 각 worker노드마다 도출되는 컨테이너들의 작업 수행시간의 평균값을 더 정밀하게 나타내기 위해 총 5번의 반복 계산 작업을 실시하여 최종적인 평균값을 나타내었다. 이 과정에서 스레드 개수별로 메모리 부하 작업을 수행하는 컨테이너가 포함되었을 때 timeout에 따른 각각의 worker노드에서 나타난 컨테이너들의 작업 수행시간의 평균값들 중 최대값과 포함되지 않았을 때 나타난 각각의 worker노드 내 컨테이너들의 작업 수행시간의 평균값을 비교해본 결과 작업 수행시간의 증가율은 <표 3>과 같다. <표 3>을 보면 스레드 개수가 10개일 때 각 worker노드마다의 성능 저하율이 가장 크게 발생한 것으로 나타났다. 즉, 메모리 부하 작업을 수행하는 스레드 개수가 증가할수록 작업 수행시간이 더 크게 증가해 프로그램의 성능이 저하되는 현상을 확인할 수 있다.

<표 3> 수행시간 최대 증가율

스레드 개수	worker 1	worker 2	worker 3	worker 4	worker 5
1개	14.02%	11.7%	13.22%	11.92%	10.55%
5개	29.98%	30.93%	28.75%	28.17%	29.06%
10개	38.69%	37.45%	35.61%	38.11%	36.53%

4. 결론 및 향후 연구

본 논문에서는 Docker Swarm을 통해 구성된 클러스터 환경에서 메모리 부하 작업을 수행하는 컨테이너를 실행시켰을 때와 그렇지 않았을 때의 작업 수행시간을 측정 및 비교함으로써 나타난 성능 저하 현상을 관찰 및 분석하였다. 스레드 개수를 본 실험에서 사용한 개수보다 더 많이 할당하거나 timeout을 더 늘린다 하더라도 성능 저하 정도가 크게 증가하지 않았다. 이는 각각의 worker노드가 할당받은 메모리 용량에서의 한계점으로 보였으며 worker노드의 메모리 용량을 늘린다면 더 많은 스레드를 할당해 더 큰 성능 저하를 일으키는 모습을 확인할 수 있을 것으로 보인다.

본 실험에서 할당한 스레드 개수가 1개일 때와 5개일 때, 메모리 부하 작업이 수행되었을 때의 경우가 그렇지 않았을 때의 경우보다 평균적으로 컨테이너

들의 작업 수행시간이 더 빨랐던 현상이 관찰되었다. 이는 Docker Swarm 환경에서 worker노드의 자원 여유에 따라 실행되는 컨테이너의 수가 달라질 수 있기 때문에 나타난 현상이다. 이를 바탕으로 각 worker 노드마다 다른 수의 컨테이너가 실행되고 있는 상황이라도 메모리 경합을 줄일 수 있는 적절한 스케줄링 방법을 연구해 볼 수 있다.

Docker Swarm에서 기본적으로 사용하고 있는 Raft consensus algorithm은 여러 서버 중 일부에 장애가 발생해도 제 기능을 유지하도록 해주지만 메모리 경합에 대한 고려는 하지 않는다. 그러므로 worker 노드 내 메모리 경합으로 인한 여러 컨테이너들의 성능 저하를 예방하지 못한다. 따라서 향후 연구에서는 이러한 성능 간섭으로 인해 발생하는 성능 저하를 해결하고자 Docker Swarm을 이용한 클러스터 환경에서 메모리 경합을 고려한 스케줄링 기법에 대하여 연구할 계획이다.

참고문헌

- [1] Prateek Sharma et al., "Containers and Virtual Machines at Scale: A Comparative Study" 17th International Middleware Conference, 2016
- [2] Junhee Park et al., "Performance Interference of Memory Thrashing in Virtualized Cloud Environments: A Study of Consolidated n-Tier Applications" IEEE 9th International Conference on Cloud Computing (CLOUD), 2016
- [3] <https://linux.die.net/man/1/stress>

응용 프로그램 특성 분석 기반 스케줄링 최적화 기법의 확장성 연구

최지은, 박근철, 노승우, 박찬열
한국과학기술정보연구원 슈퍼컴퓨터기술개발센터
(jieun1205, gcpark, seungwoo0926, chan)@kisti.re.kr

A Scalability Study for scheduling optimization method based on application characterization

Jieun Choi, Geunchul Park, Seungwoo Rho, Chan-Yeol Park
Center for Development of Supercomputing System
Korea Institute of Science and Technology Information

요 약

한정된 고성능 자원을 여러 사용자에게 제공해야 하는 슈퍼컴퓨터와 같은 시스템은 제한된 기간 내에 보다 많은 양의 작업이 실행되도록 시스템 활용률을 높이는 방안이 필요하다. 이를 위해 시스템 관리자가 수행할 응용 프로그램에 대한 사전 정보를 파악하는 것이 유용하다. 대부분의 고성능 컴퓨팅 시스템 운영에 있어 작업을 실행할 때 사용자로부터 실행 기간, 자원 요구사항들에 대한 정보를 제공 받거나 시스템 사용 통계 값을 사용하여 필요한 정보를 생성하는 등의 프로파일링 기술을 바탕으로 시스템 활용률을 높이는데 활용하고 있다. 본 논문의 선행연구에서 하드웨어 성능 카운터를 이용하여 응용 특성 분석을 실행하고, 이 결과를 바탕으로 작업 스케줄링을 최적화하는 기술을 개발한 바 있다. 본 논문에서는 슈퍼컴퓨터 최적 실행 지원을 위한 프로파일링 테스트베드를 구축하고 단일노드를 기반으로 분석한 응용 프로그램 특성 결과를 활용한 스케줄링 최적화 기법이 확장성 있게 동작함을 보이고자 하였다. 또한 중규모 클러스터에 개발한 스케줄링 최적화 기법을 적용한 결과 전체 응용 프로그램이 실행 시간을 단축함으로써 최대 33%의 성능 향상 효과를 얻었다.

1. 서론

전세계 슈퍼컴퓨터의 계산 성능 상위 500 시스템을 공표하는 Top500[1]에 따르면 현재 상위 10위에 속하는 슈퍼컴퓨터들은 최소 788개에서 최대 40,960 개의 계산 노드로 구성되어 있으며, 100Gb/s 전송속도를 갖는 고성능 I/O 장비를 통해 대규모 클러스터 시스템 구조를 갖는다. 이와 같은 고성능 컴퓨팅 시스템은 한정된 고성능 자원을 여러 사용자에게 제공해야 하기 때문에 제한된 기간 내에 보다 많은 양의 작업이 실행되도록 시스템 생산성을 높이는 방안이 필요하다. 이를 위해 시스템 관리자가 수행할 응용 프로그램에 대한 사전 정보를 파악하는 것이 유용하다.

대부분의 고성능 컴퓨팅 시스템을 운영하는 센터들은 사용자로부터 작업 제출 시에 응용 프로그램의 실행 시간, 자원 요구사항들에 대한 기본 정보를 제공 받는다. 추가적으로 시스템 모니터링을 통해 자원 사용에 대한 모니터링 값이나 자원 상태 정보와

같은 통계 데이터를 수집하여 필요한 정보를 생성하는 등의 프로파일링 기술을 바탕으로 시스템 활용률을 높이기 위한 연구를 진행하고 있다[2, 3, 4]. 그러나 실제 사용자가 요청한 작업이 수행되어야 할 대규모 고성능 컴퓨팅 시스템에서 작업의 프로파일링 데이터를 생성하기 위한 과정은 시스템 활용률을 낮출 수 있으므로 실제 시스템과 유사하면서 적은 규모의 테스트베드 운용의 필요성이 대두된다.

한편, 본 논문의 선행연구[5]에서 하드웨어 성능 카운터를 이용하여 응용 프로그램의 시스템 활용에 대한 특성 분석으로 프로파일링 데이터를 생성하고, 생성된 데이터를 바탕으로 응용 프로그램 사이의 자원 간섭률 기반 동시 스케줄링 기법을 개발한 바 있다. 본 논문에서는 슈퍼컴퓨터 최적 실행 지원을 위한 프로파일링 테스트베드를 구축하고 단일 노드를 기반으로 분석한 응용 프로그램 특성 결과를 활용한 스케줄링 최적화 기법이 확장성 있게 동작함을 실험을 통해 보이고자 한다.

2. 관련연구

고성능 컴퓨팅 시스템에서 작업에 대한 정보 및 통계 값을 사용하여 생성된 대략적인 프로파일 데이터를 활용하는 연구[2]에서는 오프라인 스케줄링을 통해 자원 활용률 기반으로 프로파일을 재생성한 다음 수정된 프로파일을 기반으로 스케줄링 기법을 제안하였다. [2]연구의 결과로 CINECA 컴퓨팅 센터에서 운영하는 오로라(EURORA) 시스템의 PBS[7] 스케줄러의 성능을 개선시켰다.

동적 자원 관리 플랫폼을 제안한 연구[3]에서는 스케줄러가 사전에 노드수와 전력 사용 레벨의 조합에 대한 성능 프로파일 데이터 셋을 저장하도록 한다. 스케줄러는 프로파일이 없는 새로운 작업에 대해서 필수 전력특성을 바탕으로 성능 모델링을 통해 자원을 할당한다. 제안된 기법은 아르곤 국립연구소의 IBM BG/P 시스템에서 선입선출 및 backfiling 스케줄링 기법을 사용하는 Slurm[8] 스케줄러와 비교하여 성능을 최대 5.2배 향상시켰다.

전력 프로파일링 생성 방법을 연구한 논문[4]에서는 작업 모니터링 데이터 수집, cray 플랫폼을 활용한 out-of-band 데이터 수집, 하드웨어 성능 카운터를 활용한 In-band 데이터 수집 및 코드 인스트루멘테이션 기반의 코드 프로파일링 데이터 수집 방법을 비교 분석한다. 이 연구는 소규모 테스트베드에서 생성된 전력 프로파일을 이용하여 로스앨러모스 국립연구소의 Trinity 대규모 슈퍼컴퓨터를 대상으로 프로파일링 데이터의 확장성 실험을 진행하였다.

3. 슈퍼컴퓨터 최적 실행 지원을 위한 프로파일링 테스트베드 구축

2018년 도입된 국가 슈퍼컴퓨터 5호기(누리온)는 인텔 제온파이 프로세서 기반의 계산 노드 8,305대와 인텔 제온 프로세서 기반의 CPU-only 노드 132대로 구성되어 총 25.7PFlops의 계산 성능 갖추었다. 슈퍼컴퓨터 5호기는 지난 1년 여간 140개 기관과 2000여명이 넘는 연구자들을 대상으로 서비스되었으며, 본 연구에서는 누리온의 최적 실행 지원을 위해 응용 프로그램의 성능 프로파일링이 가능한 테스트베드 클러스터를 구축하였다.

프로파일링 테스트베드 클러스터는 누리온의 계산 노드와 동일한 인텔 제온파이 프로세서 기반의 'KISTI-GVP' 서버 16노드로 구축하였다. KISTI-GVP 서버는 한국과학기술정보연구원 슈퍼컴퓨터기술개발센터에서 진행 중에 있는 창의형 융합연구 사

업 과제의 연구 결과인 자체 개발 메인보드에 인텔 제온파이 프로세서를 장착한 시제품으로, <표 1>은 KISTI-GVP 서버의 하드웨어 및 소프트웨어 세부 사양을 보여준다.

<표 1> KISTI-GVP 노드 사양

플랫폼	Intel S7200AP
프로세서	Intel Xeon Phi CPU 7290@1.50GHz, 72 cores (288 cores by Hyper-threading)
메모리	19.2 GB (DDR4) 16GB (MCDRAM)
네트워크	Mellanox Infiniband 100GB/s
운영체제	CentOS 7.3
커널	3.10.0-514.el7.x86_64
클러스터 모드	Quadrant Mode
메모리 모드	Cache Mode
파일 시스템	Network File system
플랫폼	KISTI-GVP(Groveport)

4. 응용 특성 분석 기반 스케줄링 최적화 기법의 확장성 실험

본 장에서는 KISTI-GVP 단일 노드에서 응용 프로그램의 특성을 분석하고 이를 바탕으로 16개 노드의 테스트베드 클러스터 시스템에서 스케줄링 최적화 기법의 확장성 실험을 진행하였다. 실험내용을 다루기에 앞서 실험에 사용된 응용 프로그램에 대해 설명하고자 한다.

4-1. NPB 응용 프로그램

실험에 사용된 응용 프로그램은 NASA에서 개발한 전산유체역학(CFD) 분야의 계산 및 데이터 연산을 벤치마크한 Nas Parallel Benchmark(NPB)[6] 프로그램을 대상으로 하였다. NPB는 5개의 커널 프로그램(IS, EP, CG, MG, FT)과 3개의 수도 어플리케이션(BT, SP, LU)으로 구성되어있다. 또한 I/O 연산 벤치마크를 위한 프로그램(BT_epio, BT_full)등을 포함한다. 각 프로그램은 가장 작은 문제크기(class)인 S, W부터 중규모 A, B, C 클래스와 대규모 D, E, F 문제크기로 규모를 변경하여 실행 가능하다.

본 실험에서는 하나의 물리서버가 갖는 최대 물리 코어 수(72개)를 고려하여 노드 당 MPI 프로세스(ppn)를 64로 설정하였다. <표 2>는 실험에서 사용한 10개의 NPB 응용프로그램의 문제 크기와 실행

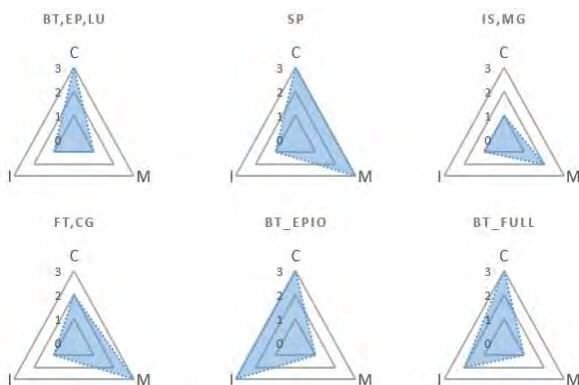
시간 측정 결과를 나타내고 있다. 단일 노드 프로파일링 실험에서 문제크기는 C 또는 D 클래스를 사용한다. 문제크기가 너무 클 경우 단일 노드에서 실행이 불가능한 경우가 있고, 응용 특성 분석에 있어 실행 시간이 미치는 영향을 줄이고자 다음과 같은 규모로 실행하였다. 클러스터 구성은 4노드, 8노드, 16노드로 확장해가며 실험하고 해당 규모의 클러스터에서 실행하기 적합한 D, E 클래스를 대상으로 하였다.

<표 2> 실험에 사용된 NPB 프로그램의 문제크기 및 실행시간

NPB	단일 노드 프로파일링		중규모 클러스터 실험 (16 nodes)	
	문제크기 (class)	실행시간 (seconds)	문제크기 (class)	실행시간 (seconds)
BT	C	51.38	D	118.55
EP	D	33.79	E	34.46
LU	C	31.09	D	47.77
SP	C	35.45	D	113.72
IS	D	34.92	E	188.97
MG	D	84.23	E	37.06
FT	C	10.39	D	151.04
CG	C	10.93	D	53.61
BT_epio	C	76.44	D	214.55
BT_full	C	120.23	D	595.93
Total	488.85 seconds		1555.66 seconds	

4-2. 하드웨어 성능 카운터를 이용한 응용 특성 분석

(그림 1)은 KISTI-GVP 단일노드에서 응용 프로그램이 실행되는 동안 하드웨어 성능 카운터를 수집하고 이후 군집분석을 수행하여 그 결과를 응용 프로그램별로 차트(kiviart chart)로 도식화한 결과이다.



(그림 1) KISTI-GVP 단일 노드에서 NPB 응용(C 또는 D 클래스) 특성 분석 결과

차트에서 삼각형의 각 꼭짓점은 CPU(C), Memory(M), I/O(I) 자원을 나타낸다. 삼각형의 크기는 응용 프로그램별 상대적인 자원 사용률에 따라 자원 사용이 낮은 군집(1), 중간 군집(2), 높은 군집(3)에 속함을 보여준다. 예를 들어 NPB의 BT, EP, LU 응용 프로그램의 경우 계산 자원의 사용이 다른 응용에 비해 상대적으로 높게 나타났으며 메모리, I/O 자원의 사용은 가장 낮은 군집에 속한 것으로 분석되었다.

응용 프로그램 특성 분석 결과를 활용하면 자원 간섭률 기반의 스케줄링 최적화 전략을 세울 수 있다[5]. 선행 연구[5]에 따르면, 응용 프로그램별 특성 결과 차트를 두 개씩 중첩시켰을 때 중첩되는 면적이 응용 프로그램 사이의 자원 간섭률로 계산되고 시스템 큐에서 대기중인 작업 간에 작업 간섭률을 고려하여 스케줄링 최적화가 가능하다.

4-3. 확장성 실험

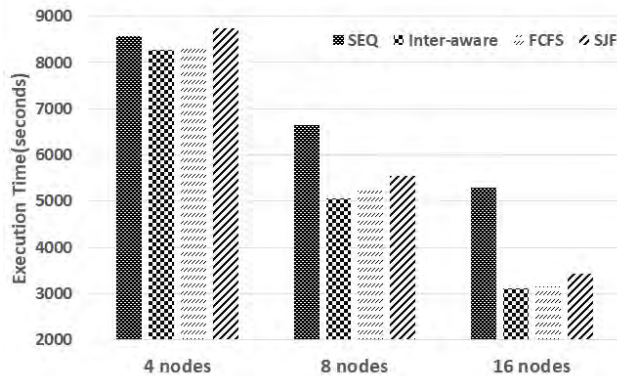
(그림 1)의 단일 노드에서 문제크기가 작은 응용 프로그램의 특성 분석 결과를 활용한 자원 간섭률 기반의 스케줄링 최적화 기법(Inter-aware)을 문제크기가 큰 응용을 대상으로 중규모 클러스터에서 스케줄링 최적화시에 시스템 실행 최적화 효과를 분석하기 위한 실험을 진행하였다.

스케줄링 실험은 랜덤으로 생성된 NPB 작업 30개가 대기중인 작업큐를 대상으로, 두개의 작업 실행 스레드(Worker)가 스케줄링 기법에 따라 작업을 실행한다. 제안된 자원 간섭 기반 스케줄링 최적화 기법(Inter-aware)은 간섭률이 낮은 작업을 동시에 우선 스케줄링한다. 이와 비교군으로 선입선출 스케줄링(FCFS) 기법과 작업 실행시간이 짧은 작업 우선 실행 스케줄링(SJF) 기법을 수행하였다. 또한 자원 간섭 없이 하나의 worker로 작업을 하나씩 순차적으로 실행한 결과는 'SEQ'으로 나타내었다.

각 스케줄링 기법은 동일한 작업큐를 사용하여 비교 실험하였으며, <표 3>과 (그림 2)는 다섯 개의 작업 큐의 평균 실행 시간을 보여준다. 가장 적은 수의 노드 4개를 사용한 경우, Inter-aware 기법은 FCFS, SJF, SEQ 대비 0.30%, 5.54%, 3.66%로 작업 실행 시간을 단축시켜 시스템 성능을 향상시켰다. 마찬가지로 8노드를 대상으로 했을 때 1.59%, 10.99%, 15.55%씩 실행 성능이 향상되었고, 16노드에서는 1.68%, 9.59%, 33.34% 성능 향상을 보였다.

<표 4> 단일 노드 프로파일링 기반의 스케줄링
최적화 확장성 실험 결과

	SEQ	Inter-aware	FCFS	SJF
4 노드	8579.01	8264.50	8289.65	8749.75
8 노드	6640.79	5069.57	5225.64	5536.06
16 노드	5285.12	3107.05	3160.09	3436.76



(그림 2) 단일 노드 프로파일링 기반의 스케줄링
최적화 확장성 실험 결과 비교

선행 연구[5]에 따르면 단일 노드에서 응용 특성 분석 후 단일 노드 스케줄링 최적화시 SEQ 대비 29.85%, FCFS 대비 6.22%, SJF 대비 9.98%의 성능 향상을 보였다. 이와 비교했을 때, 본 실험에서의 8 노드, 16노드에 비해 4노드 성능 향상률이 상당히 낮게 측정되었고, SJF 실행의 경우 SEQ 실행보다 성능이 떨어지는 것으로 보인다. 이는 NPB 프로그램 D, E 클래스의 실행이 가능한 최소 노드수인 4 노드가 응용 실행은 가능하나 시스템 부하가 상당히 기 때문으로 분석된다.

5. 결론

본 연구에서는 자체 개발한 KISTI-GVP 시스템 기반 클러스터 환경에서 응용 특성 분석 기법의 스케줄링 최적화 확장성 실험을 진행하였다. 실험 결과 프로파일링 대상 응용과 스케줄링 최적화 대상 응용 프로그램의 문제 크기가 다를지라도 시스템 성능 향상의 효과가 유지됨을 보였다.

향후 중규모 클러스터에서 실행할 응용 프로그램과 같은 문제 크기의 응용을 대상으로 최소한의 노드를 활용하여 프로파일링 정보를 생성하고 프로파일링 효과를 분석하고자 한다. 또한 중규모 클러스터에서 응용 프로그램의 런타임 전체를 프로파일링 하는 것이 아닌 일부분만 프로파일링 하는 경우의

성능 변화도 분석할 예정이다.

Acknowledgement

이 논문은 2020년도 한국과학기술정보연구원 (KISTI)의 주요사업 과제(No. K-20-L02-C08-S01) 및 정부의 재원으로 진행된 창의형 융합연구사업(No. G-19-GT-CU01-S01)의 지원을 받아 수행된 연구임.

참고문헌

- [1] (Online) Top500, <https://www.top500.org>
- [2] Bridi Thomas, "Scalable optimization-based Scheduling approaches for HPC facilities.", PhD Thesis, alama, Bologna, 2018.
- [3] Sarood Osman et al. "Maximization throughput of overprovisioned hpc data centers under a strict power budget." SC'14, New Orleans, LA, USA, 2014, pp. 807-818
- [4] Younge Andrew J. et al. "Small scale to extreme: Methods for characterizing energy efficiency in supercomputing applications." Sustainable Computing: Informatics and Systems, vol. 21, pp. 90-102, 2019.
- [5] Jieun Choi et al. "Interference-aware co-scheduling method based on classification of application characteristics from hardware performance counter using data mining." Cluster Computing, Vol. 23, No.1, pp. 57-69, 2020.
- [6] (Online) NPB, <https://www.nas.nasa.gov/publications/npb.html>
- [7] (Online) PBS, <https://www.pbspro.org>
- [8] (Online) Slurm, <https://www.slurm.schedmd.com>

실시간 데이터 분석을 위한 컨테이너 기반 가상화 성능에 관한 연구†

최보아*, 한재덕*, 오다솜*, 박현국*, 김현아*, 서민관**, 이종혁*‡

*대구가톨릭대학교 인공지능·빅데이터공학과

**티쓰리큐(주)

e-mail : jonghyuk@cu.ac.kr

A Study on Performance Evaluation of Container-based Virtualization for Real-Time Data Analysis

BoAh Choi*, JaeDeok Han*, DaSom Oh*, HyunKook Park*, HyeonA Kim*, MinKwan Seo**, JongHyuk Lee*

*Dept. of Artificial Intelligence & Big Data Engineering, Daegu Catholic University

** T3Q

요 약

본 논문은 실시간 데이터 분석을 위한 컨테이너 가상화 기술 사용에 대한 효율성을 알아보기 위해 HDP 와 MapR 배포판에 포함된 Spark 를 도커라이징 전과 후 환경에 설치 후 HiBench 벤치마크 프로그램을 이용해 성능을 측정하였다. 그리고 성능 측정치에 대해 대응표본 t 검정을 이용하여 도커라이징 전과 후의 성능 차이가 있는지를 통계적으로 분석하였다. 분석 결과, HDP 는 도커라이징 전과 후에 대한 성능 차이가 있었지만 MapR 은 성능 차이가 없었다.

1. 서론

도커[1]는 운영체제 레벨 가상화인 컨테이너 기술을 제공하는 소프트웨어로서 PaaS(Platform as a Service)의 일종이다. 컨테이너 가상화 기술은 클라우드 컴퓨팅을 가능하게 하는 중요한 기반 기술로 경량성, 성능, 이식성 등의 측면에서 하드웨어 가상화 기술 대비 우수하다. 또한 애플리케이션 실행에 대한 동일 환경 제공이 가능하여 애플리케이션의 개발, 배포, 운영의 효율화를 위해 최근 널리 활용되고 있다.

스파크[2]는 대규모 데이터 처리를 위한 통합 분석 엔진이다. 스파크는 인 메모리 캐싱 등 하둡의 배치 처리보다 최적화된 실행을 지원하여 실시간 데이터 처리 및 분석에 많이 활용된다.

본 논문은 컨테이너 가상화 기술을 이용한 실시간 데이터 분석의 성능을 분석하여 컨테이너 가상화 기술의 효율성을 알아보고자 한다. 이를 위해 본 논문은 하둡 배포판 중 HDP[3]와 MapR[4] 내 포함된 스파크를 도커 적용 전과 후 환경에 각각 구축하고 벤치마킹 프로그램인 HiBench[5]를 이용하여 성능을 측정한다. 스파크 도커라이징 환경의 적용 전과 후의 비교를 위해 실행 시간과 처리량에 대해 통계적 검증 방법인 T-test 로 가설을 세워 성능 차이 유무를 비

교 분석하여 컨테이너 가상화 기술의 효율성을 판단한다.

본 논문의 2 절에서는 HDP 와 MapR 기반 스파크 환경 도커라이징 전과 후의 성능 차이 존재 여부를 확인하기 위해 이용한 대응표본 t 검정을 설명하고 3 절에서는 실제 데이터를 이용하여 도커라이징 전과 후의 성능 차이가 있는지 통계 분석한 결과를 설명한다. 마지막으로 4 절에서는 결론을 맺는다.

2. 관련연구

t 검정은 t 분포에 의존하여 두 집단 간의 평균이 통계적으로 유의미한 차이를 보이는지 판별한다. 대응표본 t 검정은 한 집단내에 두 개의 변수를 비교하기 위해 일반적으로 한 집단의 사전, 사후에 대한 차이를 분석할 때 사용하는 통계적 기법이다. 본 논문은 HDP 와 MapR 기반으로 스파크 도커라이징 환경 적용 전과 후의 성능 차이를 분석하기 때문에 대응표본 t 검정(paired t-test) 사용이 적합하다.

3. 실험 환경 및 결과

본 논문은 스파크 도커라이징 환경 적용 전과 후

† 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 SW 중심대학지원사업의 연구결과로 수행되었음(2019-0-01056).

‡ 교신저자

성능의 차이가 존재하는지 분석하기 위해 Host OS 와 Docker 에 HDP 와 MapR 기반 Spark 환경을 <표 1>과 같이 각각 구축하였다. 그리고 HiBench 벤치마크 프로그램을 사용하여 각각의 워크로드를 10 번 실행 후 실행시간과 처리량을 수집하였다. HiBench 는 Micro, ML, SQL, Graph, Websearch 및 Streaming 의 6 가지 범주로 총 27 개의 워크로드로 구성되어 있다. 본 논문에서는 Micro 의 WordCount 와 Sort 워크로드를, Websearch 의 PageRank 워크로드를 사용하였다.

<표 1> 실험 환경

구분	상세 스펙 및 버전 Host OS / Docker
Hardware	AWS EC2 instance: t2.large (vCPUs: 2, RAM: 8GB, General Purpose SSD)
Software	Ubuntu 16.04 HDP 2.6.5 MapR 5.2.2 OpenJDK 1.8.0_222 Docker 18.09.7 HiBench 7.0

본 논문은 도커라이징 전과 후의 실행 시간과 처리량 성능에 대한 차이를 알아보기 위해 다음과 같이 가설을 세우고 대응표본 t 검정을 실행하여 분석하였다.

- H_0 : 도커라이징 전과 후의 성능에 대한 차이가 없다.
- H_1 : 도커라이징 전과 후의 성능에 대한 차이가 있다.

3.1 HDP 기반 Spark 의 도커라이징 전, 후 실행시간 차이 분석

HDP 기반 Spark 의 도커라이징 전과 후의 WordCount, Sort, PageRank 의 실행시간을 대응표본 t 검정 수행 결과, <표 2> 와 같이 HDP 기반 Spark 의 도커라이징 전 WordCount, Sort, PageRank 실행시간 평균은 각각 7.521, 7.294, 7.623 이고, 후의 평균은 각각 8.965, 8.838, 9.424 이다. 유의수준 $\alpha=0.05$ 에서 전과 후의 차이에 대한 유의확률을 검정 하였을 때, 유의확률은 각각 $5.645e-07$, $1.798e-07$, $1.616e-06$ 이므로 모두 H_1 을 채택한다. 따라서, 도커라이징 전과 후의 성능에 대한 차이가 있다고 할 수 있다.

<표 2> HDP 기반 Spark 의 도커라이징 전, 후 실행시간 차이 분석 결과 (단위: 초)

	전 평균	후 평균	유의확률
WordCount	7.521	8.965	$5.645e-07$
Sort	7.294	8.838	$1.798e-07$
PageRank	7.623	9.424	$1.616e-06$

3.2 HDP 기반 Spark 의 도커라이징 전, 후 처리량 차이 분석

HDP 기반 Spark 의 도커라이징 전과 후의 처리량을 대응표본 t 검정 수행 결과, <표 3>과 같이 도커라이징 전 처리량 평균은 각각 4909.5, 4900.5, 1408.7 이고, 후의 평균은 각각 4054.1, 4098.6, 1149.5 이다. 유의수준 $\alpha=0.05$ 에서 전과 후의 차이에 대한 유의확률을 검정 하였을 때, 유의확률은 각각 $4.543e-06$, $3.695e-07$, $2.663e-05$ 이므로 모두 H_1 을 채택한다. 따라서, 도커라이징 전과 후의 성능에 대한 차이가 있다고 할 수 있다.

<표 3> HDP 기반 Spark 의 도커라이징 전, 후 처리량 차이 분석 결과

	전 평균	후 평균	유의확률
WordCount	4909.5	4054.1	$4.543e-06$
Sort	4900.5	4098.6	$3.695e-07$
PageRank	1408.7	1149.5	$2.663e-05$

3.3 MapR 기반 Spark 의 도커라이징 전, 후 실행시간 차이 분석

MapR 기반 Spark 의 도커라이징 전과 후의 실행시간을 대응표본 t 검정 수행 결과, <표 4>와 같이 도커라이징 전 실행시간 평균은 각각 10.957, 10.987, 10.7481 이고, 후의 평균은 각각 10.803, 10.848, 10.930 이다. 유의수준 $\alpha=0.05$ 에서 전과 후의 차이에 대한 유의확률을 검정 하였을 때, 유의확률은 각각 0.4082, 0.3689, 0.3193 이므로 모두 H_0 을 채택한다. 따라서, 도커라이징 전과 후의 성능에 대한 차이가 없다고 할 수 있다.

<표 4> MapR 기반 Spark 의 도커라이징 전, 후
실행시간 차이 분석 결과 (단위: 초)

	전 평균	후 평균	유의확률
WordCount	10.957	10.803	0.4082
Sort	10.987	10.848	0.3689
PageRank	10.7481	10.930	0.3193

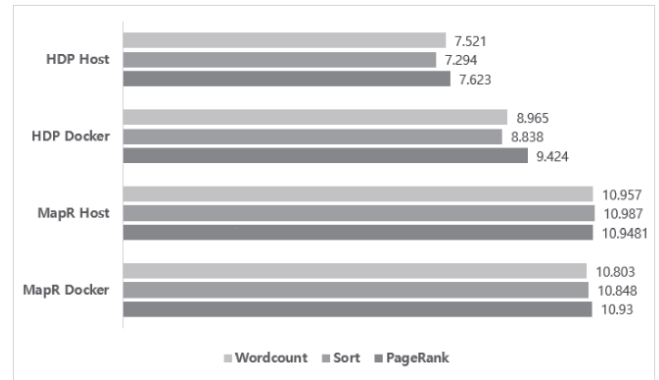
3.4 MapR 기반 Spark 의 도커라이징 전, 후 처리량 차이 분석

MapR 기반 Spark 의 도커라이징 전과 후의 처리량을 대응표본 t 검정 수행 결과, <표 5>와 같이 도커라이징 전 처리량 평균은 각각 3394.7, 3384.9, 1007.6 이고, 후의 평균은 각각 3296.5, 3318.1, 989.6 이다. 유의수준 $\alpha=0.05$ 에서 전과 후의 차이 대한 유의확률을 검정 하였을 때, 유의확률은 각각 0.1606, 0.1999, 0.2485 이므로 모두 H_0 을 채택한다. 따라서, 도커라이징 전과 후의 실행시간에 대한 차이가 없다고 할 수 있다.

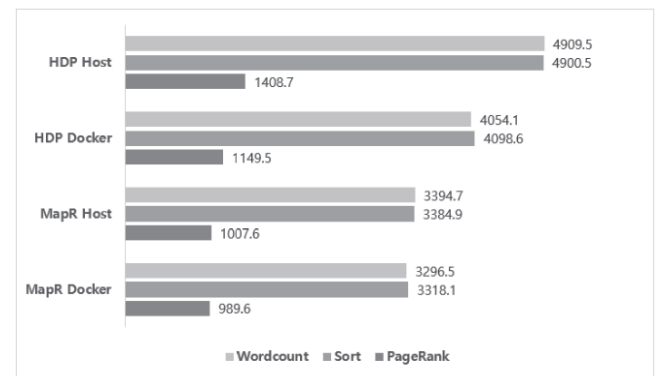
<표 5> MapR 기반 Spark 의 도커라이징 전, 후
처리량 차이 분석 결과

	전 평균	후 평균	유의확률
WordCount	3394.7	3296.5	0.1606
Sort	3384.9	3318.1	0.1999
PageRank	1007.6	989.6	0.2485

위의 분석 결과에 따르면 HDP 기반의 스파크 도커라이징 환경 적용 전과 후에는 성능에 대한 차이가 있는 반면 MapR 기반의 스파크 도커라이징 환경 적용 전과 후에는 성능에 대한 차이가 없다. (그림 1)은 도커라이징 환경 적용 전과 후의 실행시간 평균을 보여준다. (그림 1)에서 보듯이 HDP 는 도커라이징 환경 적용시 실행시간에 차이가 크지만 MapR 은 작음을 알 수 있다. (그림 2)는 도커라이징 환경 적용 전과 후 처리량의 평균을 보여준다. (그림 2)에서 보듯이 HDP 가 MapR 보다 처리량 평균 차이가 큼을 알 수 있다.



(그림 1) 도커라이징 전과 후의 실행시간 평균
(단위: 초)



(그림 2) 도커라이징 전과 후의 처리량 평균

4. 결론 및 향후 과제

본 논문은 컨테이너 가상화 기술을 이용한 실시간 데이터 분석의 효율성을 알아보고자 실제 HDP 와 MapR 기반 스파크 도커라이징 환경 적용 전과 후의 성능 데이터 분석을 통해 성능에 차이가 존재하는지 알아보았다. 분석 결과, HDP 는 오픈소스라는 강점이 있지만, 도커라이징 환경을 적용하였을 때 처리량은 감소하고, 실행 시간은 늘어나는 것을 알 수 있었다. 즉 HDP 는 도커라이징 환경을 적용했을 때 성능적인 부분에서 오버헤드가 존재함을 의미한다. MapR 은 하둡 배포판의 상용 버전으로 서비스 이용시에 비용이 발생하지만, 도커라이징 환경을 적용했을 때에 처리량과 실행 시간의 성능 저하가 발생하지 않는다. 따라서 도커라이징 환경을 적용하고자 한다면 MapR 이 HDP 보다 성능적인 면에서 더 효율적이라고 할 수 있다.

본 논문은 계속해서 성능 차이 여부에 대한 원인을 분석하고자 한다.

참고문헌

- [1] Dirk Merkel. Docker: lightweight Linux containers for consistent development and deployment. Linux Journal,

2014.

- [2] Matei Zaharia, Mosharaf Chowdhury, Michael J. Franklin, Scott Shenker, and Ion Stoica. Spark: cluster computing with working sets. In Proc. HotCloud '10, 2010.
- [3] Hortonworks Data Platform (HDP), <https://www.cloudera.com/downloads/hdp.html>
- [4] MapR, <https://mapr.com/>
- [5] HiBench, <https://github.com/Intel-bigdata/HiBench>

제53회
2020 온라인 춘계학술발표대회

모바일컴퓨팅 및 통신시스템



모바일 결제 및 정보제공 플랫폼을 활용한 결식아동 급식지원 사업 개선 제안

전현지*

*삼육보건대 의료정보학부

e-mail : hgcy118@naver.com

A proposal for improvement of the business supporting poorly-fed children using mobile payment and information delivery platform

Hyun Ji Jeon *

*Dept. of Medical Information, Shamyook Health University

요 약

결식아동 급식지원 사업은 소년소녀 가장 등 결식우려가 있는 미성년 아동/청소년에게 꿈나무 카드를 활용하여 급식을 지원하는 사업이다. 여기서 꿈나무 카드란, 학교 바깥에서 급식에 준하는 식사를 할 수 있도록 서울시에서 발급하는 결식아동용 카드로 2017년 기준 317,234명이 사용하고 있다. 그러나 잔액조회 기능 등이 없어 사용이 불편하고, 카드 사용에 대한 사람들의 시선으로 아동/청소년이 카드 사용을 꺼려 하고 있다. 또한 카드 사용이 가능한 가맹점 정보의 미제공으로 카드 이용이 활성화되지 않고 있어, 이에 대한 개선으로 모바일 결제와 가맹점 정보를 제공하는 플랫폼 개발을 제안하게 되었다. 따라서, 본 논문에서는 저자가 실제 개발하여 테스트 중인 모바일 결제와 가맹점 정보제공 서비스, 향후 제로페이 연동에 대한 기술 검토 내용, 관리자 계정/시스템 구축을 통해 원활한 정보처리를 제안한다. 향후 연구 과제인 지자체별 결식아동 카드와의 통합을 제안하기 위해 플랫폼 개념을 기능 구성도에 반영하였다.

1. 서 론

꿈나무 카드는 학교 바깥에서 급식에 준하는 식사를 할 수 있도록 서울시에서 발급하는 결식아동용 카드로 2017년 기준 317,234명이 사용하고 있다. 현재 한 끼 5000원의 식사 보조금(서울시 기준)을 한 달 단위로 꿈나무 카드에 지급하고 있으나, 카드를 사용하는 아동/청소년은 제한적인 결제 기능과 사용이 가능한 가맹점 정보의 미 제공으로 불편함을 겪고 있다. 또한 카드를 사용하는 아동/청소년에 대한 사람들의 시선으로 카드를 보이지 않고 바로 계산을 할 수 있도록 한 음식점(주로 분석집)에 맡겨 놓고 쓰는 아이들이 많다. 식당을 이용하는 시간마저 사람들의 시선을 비교적 덜 받을 수 있는 새벽 시간 대에 찾아가서 식사를 하곤 한다. 이러한 아동/청소년의 실태에 대해 꾸준히 문제 제기되어 왔고, 서울시는 아이들의 낙인감을 최소화하기 위해 꿈나무 카드 디자인을 바꿨다. (2019.9.1. 변경된 카드 지급 실시)

하지만 바뀐 디자인 역시 아동급식카드라는 고유성이 남아있어 본질적인 문제가 해결되지 않고 있다. 아래의 표는 일부 지자체별로 진행되고 있는 결식아동 사업에 대한 내용으로 지정 카드사와 제공되는 보조금 규모가 모두 상이하고 각각의 지자체별로 개발 및 운영을 하고 있어 예산이 낭비되는 문제가 있다.

표 1. 지자체별로 상이한 결식아동 사업 기준

지역	카드 이름	은행 (지정 카드사)	내용
서울	꿈나무 카드	신한 은행	1식 5000원
경기도	G-드림 카드	농협	1식 4500원 1회 최대사용 30,000원
대구	컬러풀 카드	대구 은행	횟수제한 없음 1일 최대한도 15,000원

따라서 지자체별로 운영중인 결식아동 급식지원 사업 관련 결제 시스템과 가맹점 정보제공 서비스를 통합할 수 있는 플랫폼의 필요성이 요구된다. 또한 이용 가능한 가맹점 정보와 저소득층 아이들에게 공짜로 음식을 제공하겠다는 식당들이 늘고 있으나, 정작 해당 정보가 필요한 아동/청소년들은 관련 정보를

* 본 논문은 과학기술정보통신부 정보통신창의인재 양성사업의 지원을 통해 수행한 프로보노 ICT멘토링 자율형 프로젝트 결과물입니다.

접하기 어려우며 한 끼 5000원의 식사 보조금으로 여러 식당을 돌아다니면서 5000원 이하 가격대의 식사 메뉴를 확인해야만 하는 불편함을 겪고 있다. 이와 같은 문제를 해결하기 위해 본문에서 모바일 결제와 가맹점 정보제공 서비스 개발 사례, 향후 제로페이 연동에 관한 기술 검토 방안을 구체적으로 제시하고자 한다. 이에 앞서, 서비스를 사용하게 될 아동/청소년들에게 친근하게 다가가 이용을 활성화하기 위해 캐릭터를 제작하였다. ‘찬솔 매장’과 ‘해솔 어린이’라는 순우리말의 의미가 담긴 명칭으로 각각 ‘알차게 잘 자란 소나무’, ‘해처럼 밝고 소나무처럼 바르게’라는 뜻을 부여했다.

2. 본 론

2.1 모바일 결제 방식 도입 제안

실물 카드로 결제를 하는 기존의 결제 방식과 달리 모바일 QR코드 결제 방식을 제안하고자 한다. 모바일 QR코드 결제 방식은 고유성을 가진 실물 카드를 사용하지 않기 때문에 아동/청소년들이 결식아동용 카드를 사용한다는 부담감을 벗어나게 할 수 있다. 이에 따른 모바일 결제 플랫폼 기능 구성도는 아래와 같다.

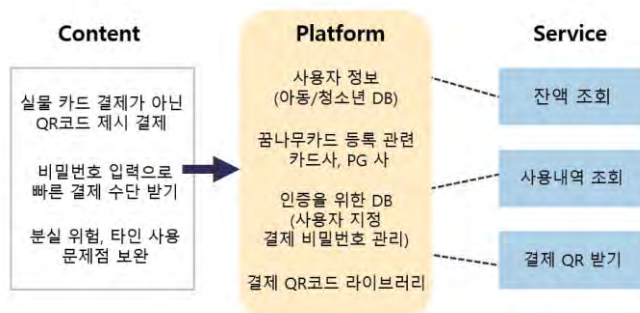


그림 1. 모바일 결제 플랫폼 기능 구성도

결제 수단인 QR코드를 받기 위해서는 1차로 기존에 발급받은 곱나무 카드를 등록해야 한다. 이때, 빠르게 결제 수단을 부여받기 위해 2차로 비밀번호를 입력하게 되는데, 이 과정을 한 번 거치면 그 이후에는 결제 비밀번호 입력만으로 간편하게 결제 수단을 부여받을 수 있다. 또한 지정한 비밀번호를 입력하면 잔액 조회와 사용내역 조회도 간편하게 할 수 있다. 추가적으로 스마트폰이 없는 경우와 QR코드 분실

위험 및 타인 사용 문제점에 대해서도 고려하였다. 스마트폰이 없는 아동/청소년의 경우 근처 주민센터 또는 지역아동센터를 방문, QR코드를 출력/발급받는 방안이 있다. QR코드는 제공 유형을 3가지(일회성 코드는 하루에 하나, 일주일 단위 7개, 한 달권)로 나누어 부여하고, QR코드에 사용 가능 시간을 설정하여 분실로 인한 타인 사용의 위험성을 최소화한다.

2.2 서비스 이용 활성화를 위한 가맹점 정보 제공 제안

가까운 매장 찾기 기능의 제공으로 사용자가 500M 이내 가맹점 정보를 제공받을 수 있게 하였다. 기존에는 가맹점 정보의 미제공으로 매번 같은 곳에서 식사하는 아동/청소년의 비율이 높았으나, 앞으로는 다양한 매장의 이용을 기대할 수 있게 되었다. 추가로 결식아동에게 무료로 음식을 제공하고 싶어 하는 매장을 ‘찬솔 매장’이라고 브랜드화하여 관련 정보 조회 서비스를 제공한다. 무료로 식사를 제공하고자 하는 매장의 DB는 한국결식아동청소년지원협회로부터 제공받아 관련 정보를 조회할 수 있게 하였다. 이에 따른 전반적인 가맹점 정보 제공 기능 구성도는 아래와 같다.

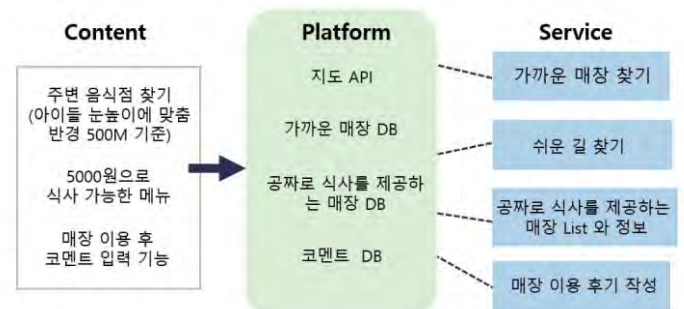


그림 2. 매장 정보 제공 기능 구성도

지도 API를 이용하여 가까운 매장과 찬솔 매장의 정확한 위치를 나타내 주고, 아동/청소년들이 쉽게 매장을 방문할 수 있도록 ‘쉬운 길 찾기’라는 기능을 추가하였다. 매장을 이용한 후 불편사항이나 좋았던 점을 코멘트할 수 있는 기능을 추가하여 다른 아동/청소년이 해당 매장을 이용할 때 참고할 수 있도록 한다.

2.3 제로페이 연동에 대한 기술검토

현재 서울시에서 운영하는 제로 페이는 고정된 MPM (Merchant Presented Mode) QR코드를 사용 중으로 가맹점에 부착된 고정형 QR코드를 촬영함과 동시에 결제가 진행되는 방식이다. 하지만 향후 변동형 CPM

(Customer Presented Mode) 이라는 QR코드를 도입하기 위해 현재 테스트 중으로 본 논문에서는 CPM 방식과 연동을 가정 했을 때를 대상으로 기술검토를 하였다. 아래는 CPM 방식으로 연동을 가정했을 때의 다이어그램이다.

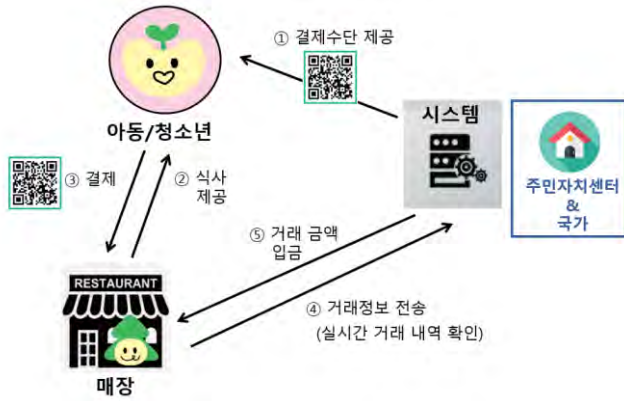


그림 3. CPM 방식의 연동을 고려한 다이어그램

향후 변동형 CPM 방식이 도입된다면 결식아동/청소년은 부여받은 QR코드로 매장에서 쉽게 스캔하게 될 것이다.

2.4. 가맹점 정보 관리에 따른 관리자 시스템 도입

결식아동들에게 무료로 식사를 제공하고 싶어 하는 매장이 늘고 있는 반면, SNS 활용도가 떨어지는 비교적 어린 연령대의 아이들은 해당 정보를 쉽게 접할 수 없는 상황이다. 따라서 ‘찬솔 매장 찾기’ 서비스를 통해 위 정보를 제공한다. 찬솔 매장 중 하나를 선택하면 그 매장의 위치, 운영시간 등 간단한 소개가 나온다. 사장님 한마디, 식사 가능한 메뉴, 음식 사진, 포장 여부 등의 정보들에 관해서는 주기적인 변동 가능성이 고려되기 때문에 Admin 시스템을 구축하여 사장님들의 수월한 페이지 관리를 도모한다. 이에 따라 정확하고 신속한 관리를 통해 정보 수용자인 아동/청소년들의 원활한 이용을 참여시킬 수 있다.

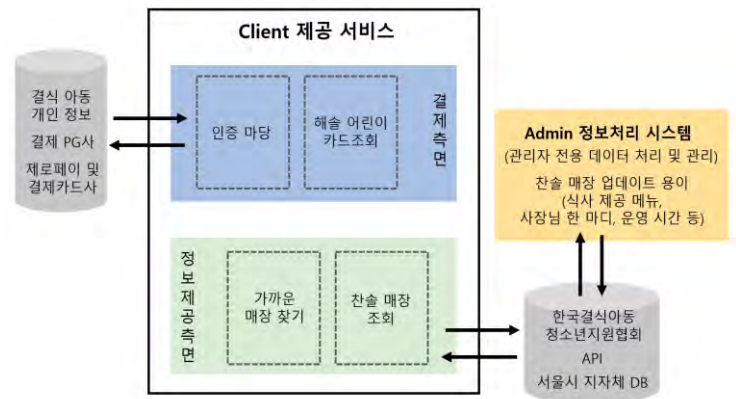


그림 4. Admin 시스템 도입에 따른 전체 기능도

추가적으로, 평균 한 끼 식사 지원금은 5000원으로 가격대가 낮은 편이기 때문에 먹고 싶은 메뉴를 선택하기가 거의 불가능한 상황이다. 이 상황을 해결해보고자 사장님의 재량으로 5000원대 이상의 식사 금액을 5000원으로 식사를 할 수 있게끔 하는 메뉴의 정보도 더불어 제공할 것이다. 이 부분은 사장님의 재량이기 때문에 매장 상황에 따라 음식 메뉴 변동, 제공 유/무에 관해서는 관리 시스템을 통해 수월한 업데이트를 가능하게 한다.

2.5. 국가사업의 지자체 통합 관리 부분

결식아동 급식지원 사업은 각 지자체별로 관련 기준이 매우 상이하다. 지정 카드사가 달라 예산을 지자체별로 배분하여 각 주민자치센터로 지급하는 연속된 과정을 줄이는 등 사업 예산의 통합 관리를 제안한다.

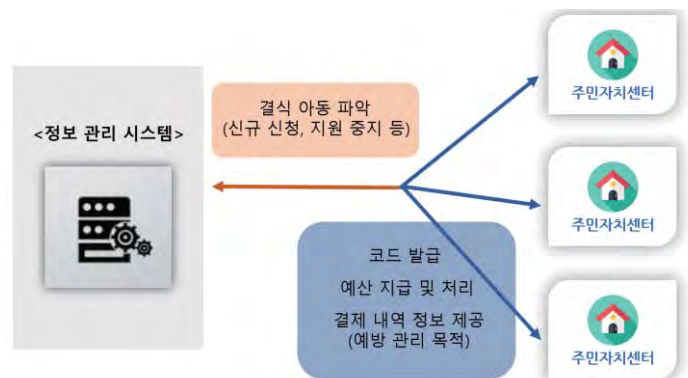


그림 5. 지자체 통합 예산 시스템 흐름도

결식아동들을 지역별로 코드화 하여 체계적인 신규 신청 관리를 하며, 결식아동 급식지원 사업의 대상이 아닌(성인이 된 경우 등) 코드를 시스템상으로 파악하여 각 지자체에 알리고자 한다. 2~3일

이상으로 결제 내역이 없는 경우의 결식아동 코드에 관해서는 결제 현황 및 정보 내역을 주민자치센터 담당자에게 신속하게 신고하여 불의의 상황을 예방하고, 균형적인 식사를 잘 하고 있는지에 대한 모니터링을 하는 등 데이터를 기반으로 한 통합 관리를 할 수 있다.

3. 결론 및 향후 연구

모바일 결제와 가맹점 정보 제공 서비스는 개발 완료 후 테스트 중이며, 지도 API와 매장 DB를 이용한 정보 제공의 정확성을 높이고 있다. 또한 제로페이 연동을 위한 결제 로직 사전 검토는 완료되었고, 연동 개발의 필요성을 서울시에 제안 예정이다. 실제 구현되는 결과물을 확인하기 위해서는 서울시 API, 결제 PG사 등 정부/지자체 차원의 지원이 필요하기 때문에 현재 이론적 개념을 반복하여 검토하고 있다. 이를 위해 한국정보보호학회, 한국통신학회 등에서 주관하는 학술대회 참석하여 보안, 간편결제 웹서비스, 서버 설계 등과 관련된 논문, 발표 내용을 토대로 연구 중이다.

참 고 문 헌

- [1] 경희대학교 산학협력단 전종식 교수,
꿈나무카드 분석 보고서, 2017
- [2] 부산여성가족개발원 박금식,
결식우려아동에 대한 효율적 급식지원방안 연구, 2012
- [3] 한국마케팅연구원 신주연,
QR코드 시장에서 제대로 활용하려면, 2012
- [4] 한국지능정보시스템학회 이준엽/이경전,
스마트카드 가상화(ViSCa)플랫폼 기반 모바일 결제 서비스 제안 및 타 사례와의 비교분석, 2014
- [5] 남광우/하수옥, Awarematics/WMServer:
오픈소스 웹맵 서비스 서버의 설계와 구현,
한국공간정보시스템학회 논문지, 2009
- [6] 김영의/문현실/김재경,
모바일 결제 서비스 시장의 경쟁구도 분석,
한국경영정보학회 학술대회, 2015

사용자의 활동성을 장려하는 AR 콘텐츠 게임¹

김다은*, 배민주, 유채현, 이유진, 박수이**, 강승석**

서울여자대학교 디지털미디어학과

shalo1040@gmail.com, itsfromj@gmail.com, ismy123@naver.com, leeyj7988@gmail.com,

spark44@swu.ac.kr, msukang@swu.ac.kr

The AR Game to Promote User Activities

Da-Eun Kim*, Min-Joo Bae, Chae-Hyeon You, Yu-Jin Lee, Sue Park**, Seung-Seok Kang**

Dept. of Digital Media Design and Applications, Seoul Women's University

요 약

항상 앉아서 게임을 하는 9~12 세 청소년들의 활동성 장려를 위해 만들어진 모바일 게임으로, 걸음 수와 연동하여 청소년들의 신체활동을 조성한다. 또한, 청소년들의 흥미를 유발하기 위해 외계 생명체로부터 지구를 지키는 스토리 요소를 접목한 AR 및 3D 모바일 게임이다.

1. 서론

기술이 발전하면서 스마트폰은 청소년들에게도 필수 전자기기가 되었다. 그에 따라 언제 어디서나 할 수 있는 스마트폰 플랫폼의 모바일 게임이 많이 등장하고 있다. 성장기 청소년들은 쉽게 게임 중독에 노출되고, 이는 비만이나 건강 악화로 이어진다. 하지만 게임의 중독성 때문에 스마트폰 게임에서 쉽게 헤어 나오지 못하는 청소년들이 많다.

따라서 우리는 청소년들의 유희적 요소인 게임을 놓치지 않으면서도 이들의 외부 활동을 장려해 재미 있는 신체활동을 조성하는 AR 및 3D 모바일 게임 <무빙무빙>을 기획하게 되었다.

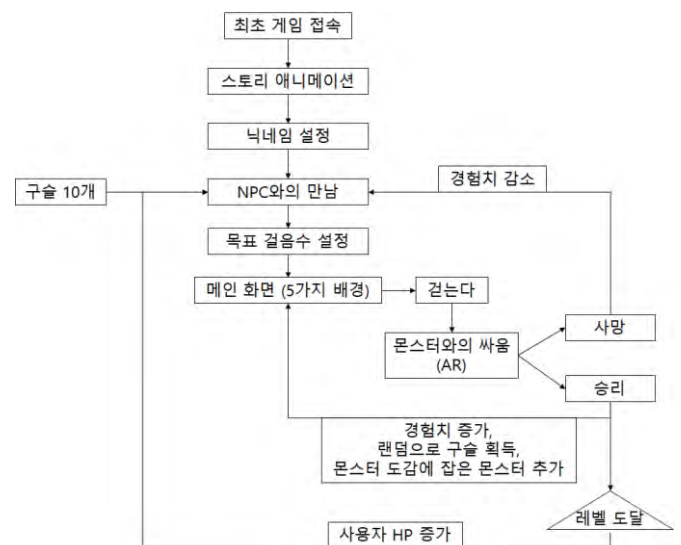
게임의 모든 진행은 사용자의 활동성 장려를 위해 모바일 기기의 걸음 수와 연동되어 작동된다. 게임에 필요한 아이템을 수집하고 몬스터를 물리치기 위해 사용자는 걸어야만 한다. 또한 걷기 활동의 동기부여를 위해 매일 목표 걸음 수를 설정하여 많이 걸을수록 다양한 테마의 배경들을 볼 수 있다.

2. 콘텐츠 가치

이 게임은 사용자에게 두 가지의 가치를 준다. 먼저, 사용자가 신체활동을 하고자 하는 욕구의 의미를 갖는 활동적 가치를 제공한다. 활동적 가치의 요소로는 걸음 수를 통한 구슬과 아이템 획득, 몬스터 사냥, 목표 걸음 수 달성에 따라 여러 테마를 즐길 수 있다.

두 번째 가치는 사용자가 즐거움을 얻고자 하는 욕구인 유희적 가치이다. 유희적 가치의 구성요소에는 레벨 업, 아이템 획득과 몬스터 도감이 있고 AR 과 3D 콘텐츠를 통해 이 두 가지 가치를 얻을 수 있다.

3. 콘텐츠 진행 과정



<표 1> 전체적인 게임 진행 흐름도

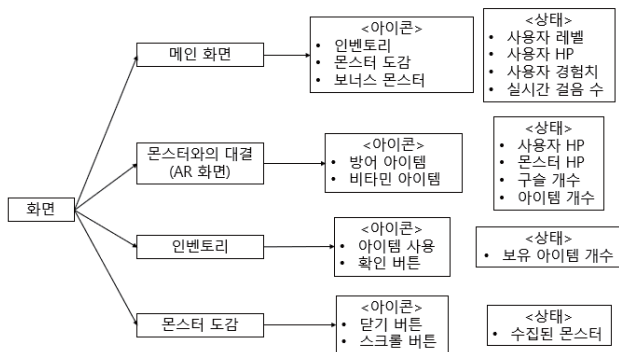
¹ 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 SW 중심대학지원사업의 연구결과로 수행되었음 (2016-0-00022)

This research was supported by the MISP(Ministry of Science, ICT & Future Planning), Korea, under the National Program for Excellence in SW(2016-0-00022) supervised by the IITP(Institute of Information & communications Technology Planing & Evaluation)(2016-0-00022)



<표 2> 사용자 걸음 수에 따른 예상 게임 동작 그래프

사용자가 스마트폰을 들고 걷기 시작하면 스마트폰의 기울기 변화 속도에 따라 걸음 수를 센다. 게임의 메인 화면에서 사용자가 걷기 시작하면 화면 속의 길이 움직여 마치 직접 그 길을 걸어가는 듯한 느낌을 준다. 사용자가 151~200 걸음을 걸었을 때마다 사용자의 레벨에 맞는 몬스터가 출현한다. 처음 게임이 시작될 때 사용자는 목표 걸음 수를 설정하게 되고 목표 걸음 수를 달성하게 되면 다섯 가지 테마 속에서 플레이를 할 수 있어 사용자에게 걸어야 하는 동기를 부여한다. 이 목표 걸음 수는 자정이 되면 초기화되며 다음 날 새로운 목표 걸음 수를 설정할 수 있다. 또한 몬스터와의 싸움에서 필요한 구슬도 80 걸음마다 길 위에 등장하는 구슬 박스를 열어 얻을 수 있기 때문에 게임이 진행되기 위해서 사용자의 활동성을 유도한다.



<표 3> 화면 구조도

1) 구슬

사용자는 게임을 처음 시작할 때 NPC로부터 총 10 개의 구슬을 받게 되며, 이후에는 몬스터를 제거하거나 걸음 수를 채워야 구슬을 더 모을 수 있다. 또한, 사용자는 지구를 지키기 위해 획득한 구슬로 몬스터를 무찌른다. 추가로, 사용자는 게임을 진행하면서 하루에 걸은 걸음 수만큼 구슬을 보상받을 수 있다.

2) 아이템

비타민(사용자 HP 15 만큼 충전), 구슬 (몬스터 공격 시 사용), 방어 아이템 (몬스터 공격으로부터 5 초 간 방어 역할)이 있다.

3) 걸음 수

사용자는 걸음 수에 대한 보상으로 구슬과 아이템을 지급받는다. 또한, 사용자는 게임을 시작할 때 하루에 걷고자 하는 목표 걸음 수에 따라 다섯 가지 테마 속에서 게임을 플레이할 수 있다.

4) 게임 방법

사용자의 걸음 수에 따라 몬스터가 등장하고, 그 몬스터를 클릭해 AR 화면으로 이동하면 몬스터가 등장한다. 몬스터는 주기적으로 사용자를 공격하며 이를 피하지 않고 공격을 맞게 되면 사용자의 HP 가 감소한다. 이때, 방어 아이템을 사용하면 5 초 동안 몬스터의 공격을 방어할 수 있다. 사용자가 몬스터를 공격하기 위해 화면 하단부에 위치한 세 개의 구슬 버튼을 클릭해 어떤 구슬을 발사할지 선택한다. 이때, 버튼에는 사용자가 보유한 만큼의 숫자가 표기되어 있으며 보유한 구슬이 없으면 발사되지 않는다. 구슬이 몬스터에게 닿으면 몬스터의 HP 가 감소하며 몬스터는 공격받은 모션을 취한다. 게임을 플레이한 후 사용자 또는 몬스터의 체력이 0 이 되는 순간 승 또는 패의 결과 화면이 나타나며, 그 결과에 따른 보상이 주어진다. 사용자가 확인 버튼을 누르면 게임은 완전히 종료되고 다시 메인 화면으로 이동한다.

사용자 레벨	사용자 HP	경험치
1	100	1000
2	200	1500
3	300	2000

<표 4> 사용자 레벨에 따른 HP 와 경험치

구슬	1 회 타격 시 데미지 (몬스터의 hp 감소)
1	8
2	16
3	34

<표 5> 구슬 레벨에 따른 타격 데미지

구슬의 데미지는 몬스터의 hp 와 사용자의 걸음 수를 고려했다. 사용자에게 구슬은 게임에 참가할 수 있는 중요한 요소이기 때문에 구슬의 데미지가 크면 사용자의 흥미가 떨어질 수 있고, 데미지가 작으면 사용자가 어려움을 느낄 수 있기 때문이다.

몬스터 레벨	몬스터 HP	몬스터 공격 데미지
1	50	10
2	100	20
3	240	40

<표 6> 몬스터 레벨에 따른 HP 와 공격 데미지

4. 결론 및 기대 효과

<무빙무빙>은 게임의 유희적인 요소를 고려한 것에서 더 나아가 사용자의 신체활동 또한 장려하는 게임이다. <무빙무빙>을 플레이하면 실내에서만 게임을 하던 청소년들이 밖으로 나와 활동적으로 게임을 하게 된다. 게임을 즐기는 동시에 걸음 수를 장려하는 요소들을 통해 신체 활동을 함으로써 기존의 비만과 같은 건강 악화 문제가 완화되는 효과를 기대한다.

더욱이, 게임은 여러 방면에서 이롭지 않다는 편견

을 가진 사람들에게 <무빙무빙>을 통해 게임을 다양한 요소와 접목할 수 있고, 개인 혹은 사회적인 문제점의 해결에도 긍정적인 효과를 보여줄 좋은 사례가 될 수 있을 것이다.

MWSN에서 채널 및 타임 슬롯 공동 스케줄링 데이터 집계를 위한 제안 계획 : 알고리즘 설계

Vi Van Vo*, 김문성**, 추현승*

*성균관대학교 소프트웨어대학

**서울신학대학교 교양학부

vovanvi@skku.edu, moonseong@stu.ac.kr, choo@skku.edu

A Proposed Scheme for Channel and Timeslot Co-Scheduling Data Aggregation in MWSNs: An Algorithm Design

Vi Van Vo*, Moonseong Kim**, Hyunseung Choo*

*College of Software, Sungkyunkwan University

**Dept. of Liberal Arts, Seoul Theological University

요 약

Aggregating data with an optimal delay, which is a critical problem in Wireless Sensor Networks applications, is proven as NP-hard. In this paper, we focus on optimizing the aggregation delay by presenting an idea for channel and timeslot co-scheduling data aggregation in MWSNs. The proposed scheme, which names Break and Join, maximizes the number of sensor nodes to be scheduled in a working period, so that the overall number of working periods and data collection delay are reduced.

1. Introduction

In Wireless Sensor Networks (WSNs), data aggregation is essential in many application scenarios which are limited in energy resources such as spatial exploration, battlefield surveillance, or environment monitoring, etc. to save the energy of sensor nodes. The energy conserving approaches are used by switching sensor nodes between active and dormant modes [1]. The sensor nodes only receive data when they are in active mode, this is one of interesting challenges for proposing some delay efficiency data aggregation algorithms.

Data aggregation is one of two terms named data aggregation convergecast along with raw data convergecast [2]. The convergecast is a many-to-one pattern where one node in a sensor network as a sink node role collects data from others in the network by using wireless communication links. Data aggregation is the process that intermediate nodes will maximize, summarize or moderate data before sending it to their parent nodes. Whereas raw data convergecast transfer the data directly to the next hop without modification.

Scheduling by using multi-channel technique in multi-channel wireless sensor network (MWSNs) helps conflict links can communicate to each other simultaneously. This overcomes the drawback of single channel scheduling, that when two nodes in the network communicate, other neighbor nodes cannot transmit their data until those nodes above complete. With multi-channel allocation, nodes are assigned

in different channels, so that while two nodes are communicating, other their surrounding nodes can also transmit or receive the data from other nodes without worrying about collisions occur if they are assigned channels in properly ways. Moreover, while single channel scheduling only considers timeslots conflict, multi-channel needs to take care both channel and timeslot conflicts when scheduling.

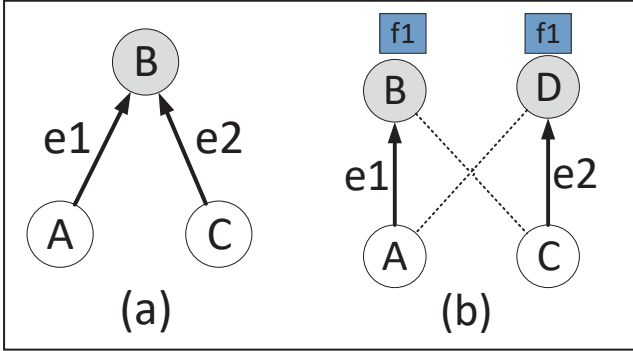
In this paper, we design an improvement scheme to reduce the aggregation delay. The structure of this paper is organized as follows: In the section 2, we provide the model and problem statement. We present the relate work and our proposed idea in section 3. Finally, we summarize our scheme and outline the future research direction.

2. Model and Problem Statement

A WSN model consists a number of sensor nodes and a sink node which aggregates data from all others. All nodes in the network are randomly deployed in a limited field, and they have a limited transmission range and omnidirectional antennas. The network topology is represented as an undirected graph $G = (V, E)$ whereas V is a set of nodes in the network and E is a set of edges in the network. This network topology is connected, in the other hand there is always a path connecting any node to a sink node in the network. The transmission range between nodes is their Euclidean distance.

Nodes in the network can transmit and receive data in designated channels and timeslots, they cannot communicate simultaneously. There are two types of collision happens that

should be avoided while scheduling which are primary collisions and secondary collisions as shown in figure 1 (a) and (b) respectively. One node receives data from two or more nodes at the same time causing primary conflicts. The secondary conflicts happen when a node is unintended to receive data from its neighbor while the node is receiving data from its child node.

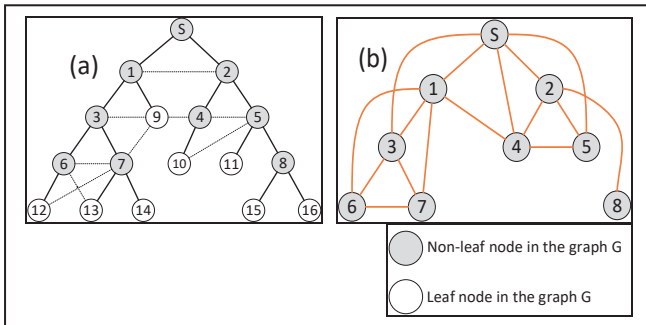


(Figure 1) (a) Primary collision between edges e1 and e2. (b) Secondary collision between edges if they transmit data on the same channel, one of the receiver nodes is unintended to receive the data.

3. Proposed Scheme

A. Related work

In the paper [3], the authors proposed a scheme to allocate channels and timeslots to reduce used channels and minimize the data aggregation delays in a multichannel WSNs. The scheme consists of two stages which are channel allocation to avoid the secondary collisions and timeslot assignment to avoid primary collisions.



(Figure 2) (a) Aggregation tree; (b) Constraint graph built for the receiver nodes from the tree

In the channel allocation stage, determine all subtrees in which the number of descendent nodes is fewer than or equal to the number of timeslots in a working period L (L is given). Allocating channels to all subtrees one by one from the largest subtree. The channel allocation work based on the constraint graph (CG) which is proposed in [4]. All nodes in a specific subtree is assigned in the same channel. The constraint graph is used to avoid the secondary collisions. The CG, which is created from the original graph G , contains all non-leaf nodes of graph G . Any two nodes in the CG connects to each other when their edges that cause secondary collisions as illustrated in the figure 2. In the other word, a node in the CG graph connects to others if it finds secondary

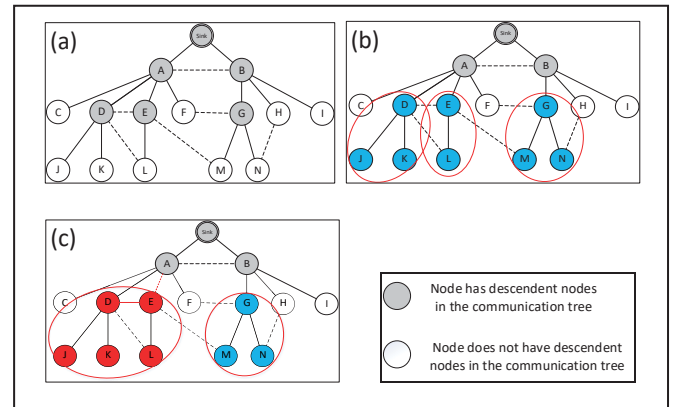
collisions with its child and neighbor nodes. The figure 2 shows how the CG works and how the channel allocation operates based on the CG. Assume that the aggregation tree is given in the figure 2 (a), the constraint graph is built from the aggregation tree in the figure 2 (b). Any two adjacent nodes in the constraint graph must not be assigned same channel.

In the timeslot assignment stage, the subtree is assigned the timeslot in a bottom-up manner starting from 1 to L right after the channel allocation completes. Because all nodes in the subtree has the same channel, the scheme assigns different timeslots to each node in the that subtree to avoid the primary collisions.

B. Proposed idea

In this section, we apply the Break and Join method to the reference scheme aiming to reduce the aggregation delay of the network. Given a tree and a feasible aggregation schedule, in which each node is scheduled to transmit its data to the parent node at a specific timeslot. The Break and Join scheme operate on node u and its neighbor v consists of two actions: First, node u breaks its edge with its parent; Second, the node u joins as a child of node v .

There are two reasons that we apply the Break and Join method to the reference scheme. We want to maximize the number of descendent nodes in a subtree (equal or approximate to L). So that the number of subtrees to be scheduled is reduced, this lead reducing the number of channels using to allocate all nodes in the network. The second reason, when number of descendent nodes in subtrees is maximized, parallel transmissions in a timeslot increase also, the aggregation delay of the network, therefore, is reduced.



(Figure 3) Break and Join scheme operation

As follow the procedure of reference scheme, in each iteration, a subtree is chosen to schedule in which the number of descendent nodes is equal or less than the length of timeslots in one working period. If the selected subtree having number of descendent nodes is equal to the length of timeslots in the working period, the scheme works follow as the procedure. If the selected subtree having number of descendent nodes is fewer than the length of timeslots in the working period, the Break and Join scheme is executed aiming to increase the number of descendent nodes in that subtree as well as increase number of nodes in the network can be scheduled in a working period.

An example run below in the figure 3 is to illustrate how

the Break and Join scheme works and somehow show that how it increases a subtree in one iteration.

Assume that a communication tree is built by using Short Path Tree algorithm (Figure 3 (a)), and there are 4 timeslots in a working period ($L = 4$). In the first iteration, three subtrees rooted at D (two descendent nodes), E (one descendent nodes) and G (two descendent nodes) are candidates (Figure 3 (b)). If following procedure of the reference scheme, the subtree rooted at D is selected due to maximum descendent nodes and D has a lower ID than G. However, because number of descendent nodes is lower than L, the Break and Join scheme is executed in this case. D has two neighbor nodes E and L. If node E breaks its parent (A) then joins as a child of node D, the subtree rooted at D has 4 descendent nodes. Similar for node L, the subtree rooted at D has 3 descendent nodes. Therefore, the node E is chosen as the child of node D. After applying the Break and Join scheme, the selected subtree now has 4 descendent nodes (as maximizing the number of descendent nodes) to be assigned channel and timeslots nodes in that subtree. So on and so forth, with the Break and Join scheme, after a number of iteration to do the scheduling for all nodes in the network the aggregation time can be reduced.

4. Conclusion

In this paper, we present an idea of improving aggregation delay for channel and timeslot co-scheduling data aggregation in MWSNs. The idea, named Break and Join, maximizes the number of descendent nodes in a selected subtree if the length of node number in the subtree is smaller than the timeslot number in a working period. The robust feature of our proposed idea is the scheme can run if there is any chance to maximize nodes in a working period so that the delay performance can be improved too. The performance evaluation of our proposed idea compared with the reference scheme is performed in our future research.

Acknowledgement

본 논문은 과학기술정보통신부 및 정보통신기획평가원의 Grand ICT연구센터지원사업 (IITP-2020-2015-0-00742), 2020 년도 정부(과학기술정보 통신부)의 재원으로 정보통신 기획평가원의 지원(No.2019-0-00421, 인공지능대학원지원) 과 2020년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원(NRF-2020R1A2C2008447, 딥적대적러닝 기반의 버추얼 엣지: 자가감독형 엣지 이동성, 리소스 배치 및 할당)의 연구결과로 수행되었음

References

- [1] X. Jiao *et al.*, "Delay Efficient Scheduling Algorithms for Data Aggregation in Multi-Channel Asynchronous Duty-Cycled WSNs," in *IEEE Transactions on Communications*, vol. 67, no. 9, pp. 6179-6192, Sept. 2019.
- [2] Van Vo V., Nguyen D.T., Le DT., Tran MH., Kim M., Choo H. (2019) A Top-Down Scheduling for Time Efficient Data Aggregation in WSNs. In: Dang T., Küng J., Takizawa M., Bui S. (eds) Future Data and Security Engineering. FDSE 2019.
- [3] Yeoum S, Kang B, Lee J, Choo H. Channel and Timeslot Co-Scheduling with Minimal Channel Switching for Data Aggregation in MWSNs. *Sensors (Basel)*. 2017;17(5):1030. Published 2017 May 4. doi:10.3390/s17051030
- [4] Ghosh, A.; Incel, O.D.; Kumar, V.S.A.; Krishnamachari, B. Multichannel Scheduling and Spanning Trees: Throughput-Delay Tradeoff for Fast Data Collection in Sensor Networks. *IEEE/ACM Trans. Netw.* 2011, 19, 1731–1744.

추가적인 백업 가상 네트워크 기능 배치 없이 서비스 체인 생존성을 보장하는 상호보완적 백업 시스템

이도경*, 장영훈**, 샤이드 무함마드 라자**, 김문성***, 추현승*

*성균관대학교 소프트웨어학과

**성균관대학교 전자전기컴퓨터공학과

*** 서울신학대학교 교양학부

dokyunglee@skku.edu, jang0h@skku.edu, s.moh.raza@skku.edu, moonseong@stu.ac.kr, choo@skku.edu

Cooperative Backup System to Ensure Survivability of Service Chain Except Provisioning Additional Backup VNFs

Dokyung Lee*, Syed Muhammad Raza**, Moonseong Kim***, Hyunseung Choo*

*Dept. of Software, Sungkyunkwan University

**Dept. of Electrical and Computer Engineering, Sungkyunkwan University

***Dept. of Liberal Arts, Seoul Theological University

요 약

네트워크 기능 가상화와 소프트웨어 정의 네트워킹의 융합은 현재의 네트워크를 대체할 새로운 매커니즘으로써 대두되고 있다. 특히 서비스 기능 체인은 네트워크에 유연성을 효율적으로 부여할 수 있다는 장점으로 인해 부각되고 있다. 그러나 서비스 기능 체인은 그 특유의 체인형 구조로 인해 생존성에 큰 약점을 갖고 있기도 하다. 이에 기존 방법들은 별도의 백업 가상 네트워크 기능을 배치하는데, 이는 자원 효율적이지 못하다. 본 논문에서는 추가적인 백업 가상 네트워크 기능 배치 없이 서비스 기능 체인의 생존성을 보장하는 백업 시스템을 제안한다.

1. 서론

네트워크 기능 가상화(NFV)와 소프트웨어 정의 네트워킹(SDN)의 융합은 현재의 네트워크를 대체할 새로운 매커니즘으로써 대두되고 있다. 소프트웨어 정의 네트워킹은 기존 네트워크에서는 개별적으로 수행하던 제어 평면의 기능들을 컨트롤러가 중앙 집중적으로 관리하는 차별점을 갖는다. 이로 인해 네트워크 설정 및 커스터마이징 측면에서 훨씬 유연하다는 장점이 있다. 소프트웨어 정의 네트워킹에서 스위치들 상에는 가상 네트워크 기능(VNF)들이 배치되어 사용자들에게 각 기능들을 제공한다. 이 때 가상 네트워크 기능들은 개별적으로 존재하는 것이 아니라, 하나의 커다란 서비스를 제공하기 위한 서비스 기능 체인(SFC)의 형태를 이룬다. 사용자는 하나의 서비스 기능 체인을 구성하는 가상 네트워크 기능들을 순차적으로 통과하며 각각에 탑재된 기능들을 제공받는다.

서비스 기능 체인은 효율적인 커스터마이징이 가능하도록 유연성을 부여하는 장점으로 인해 각광받고 있다. 그러나 그 특유의 체인형 구조로 인해 치명적인 약점을 보유하고 있기도 하다[1]. 서비스 기능 체인을 사용하는 유저는 트래픽을 각 가상 네트워크 기

능을 통과시킴으로써 서비스를 제공받는다. 따라서 단 하나의 가상 네트워크 기능이라도 장애가 발생하게 되면 전체 체인의 서비스가 마비되는 문제가 있다.

기존 연구들은[2][3] 장애 발생에 대비하여 별도의 백업 가상 네트워크 기능을 배치하여 문제를 해결하고 있다. 각 백업 가상 네트워크 기능은 평소에는 트래픽을 소화하지 않고 배치만 되어 있다가 가상 네트워크 기능에 장애가 발생할 경우에만 트래픽을 이전 받는다. 이러한 방법은 서비스 기능 체인의 생존성을 높이는 데에 큰 도움이 되지만, 백업 노드를 배치하고 유지하는 비용을 추가로 발생시킨다.

따라서 본 논문에서는 백업 가상 네트워크 기능을 추가로 배치하지 않고 가상 네트워크 기능들의 생존성을 보장하는 백업 시스템을 제안한다. 제안하는 백업 시스템은 두 개 이상의 서비스 기능 체인들이 있는 환경에서 같은 타입의 가상 네트워크 기능들이 서로의 백업으로써 작용하도록 한다. 여기서 타입은 가상 네트워크 기능이 제공하는 서비스를 의미한다. 가상 네트워크 기능에 장애가 생기면 컨트롤러는 해당 컨트롤러로 향하는 트래픽을 같은 타입의 다른 가상 네트워크 기능으로 이전시킨다. 본 시스템은 기존 방

법에 비해 노드 배치 및 유지 비용을 효과적으로 줄일 수 있을 것으로 보인다.

2. 관련 연구

[2] Overload and Failure Management (OFM) 모듈은 서비스 기능 체인의 공급 장애를 방지하기 위해 제안된 소프트웨어 정의 네트워킹 컨트롤러 모듈이다. OFM 모듈은 과부하를 방지하기 위한 Overload Management (OM) 모듈과 장애를 방지하기 위한 Failure Management (FM) 모듈로 구성되어 있다. 본 아이디어는 서비스 기능 체인을 이루는 가상 네트워크 기능들에 대하여 평소에 트래픽이 지나지 않는 백업 가상 네트워크들을 배치한다. 각 가상 네트워크 기능들은 컨트롤러에게 현재 로드 정보를 주기적으로 전송한다. 이 때 OM 모듈은 로드가 일정한 쓰레스홀드보다 클 경우, 백업 가상 네트워크 기능으로 트래픽을 이주시킨다. FM 모듈은 가상 네트워크 기능의 장애가 감지되면, 백업 노드로 트래픽을 우회한다. 위와 같이 OFM 모듈은 서비스 기능 체인의 과부하와 장애를 동시에 관리하도록 제시되었으나, 자원 사용은 고려되지 않았다.

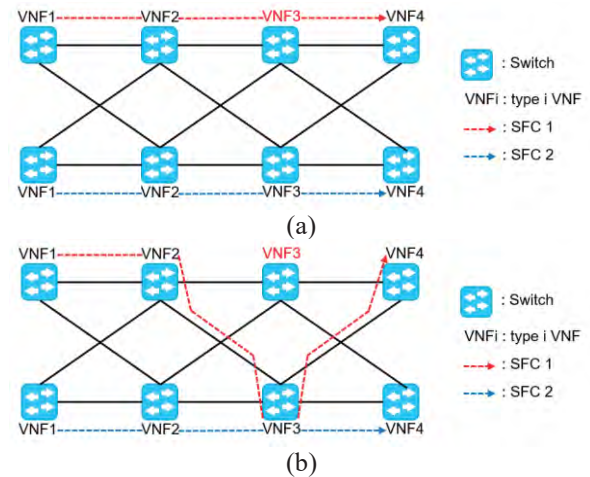
[4] Saifeddine et al.은 네트워크 상의 모든 서비스 기능 체인들에 대한 안정성 문제를 프로액티브한 방법으로 풀어내는 프레임워크를 제안한다. 서비스 기능 체인들로 이루어진 네트워크는 같은 타입인 가상 네트워크 기능이 여러 개 존재함을 가정한다. 제안하는 아이디어는 하나의 노드 장애에 대한 백업을 지원하는 동시에 자원 사용량도 고려하는 백업 공유 방식이다. 따라서 가능한 적은 백업 가상 네트워크 기능을 배치하여 모든 노드들에게 백업을 제공하기 위한 휴리스틱 알고리즘을 제안한다. 본 알고리즘은 백업 가상 네트워크 기능 배치를 효과적으로 절감했지만 휴리스틱 알고리즘으로써 안정성이나 자원 사용량 측면에서 개선의 여지가 있다.

3. 제안 시스템

제안하는 시스템은 서비스 기능 체인을 구성하는 어떠한 타입의 가상 네트워크 기능에서 장애가 발생했을 때, 해당 트래픽을 다른 서비스 기능 체인의 같은 타입 가상 네트워크 기능으로 이전시킨다. [4] 서비스 기능 체인들로 구성된 네트워크 상에는 같은 타입의 가상 네트워크 기능들이 여러 개 존재한다. 따라서 기능들을 쌍으로 엮어 각 가상 네트워크 기능들이 서로의 백업으로 작용하는 상호보완적 백업 시스템을 제시한다.

그림 1은 두 개의 서비스 기능 체인이 서로의 백업 체인으로써 존재하는 상황을 가정한 백업 시스템 예시이다. 각 스위치들 상에는 가상 네트워크들이 설치되어 있으며 이들은 각각 1, 2, 3, 4 기능을 제공하는 두 개의 서비스 기능 체인들을 구성하고 있다. 또한 스위치들은 링크로 연결되어 있다. 이 때 (b)에서는 서비스 기능 체인 1의 타입 3 가상 네트워크 기능에 장애가 발생한 상황을 보여준다. 컨트롤러는 스위치로부터 장애를 보고받으면 체인 1의 타입 3 가상 네트워크 기능으로

향하는 트래픽이 체인 2의 타입 3 가상 네트워크 기능으로 우회되도록 경로를 조정한다.



(그림 1) 본 백업 시스템의 예시. (a)는 평소 상태이며 (b)는 서비스 기능 체인 1의 타입 3 가상 네트워크 기능에 장애가 발생한 상황.

4. 결론

본 논문에서는 추가적인 백업 가상 네트워크 기능 배치 없이 서비스 체인의 생존성을 보장하는 백업 시스템을 제안하였다. 본 방법을 통해 노드 배치 및 유지에 사용되는 자원량을 효과적으로 줄일 수 있을 것으로 보인다. 본 시스템은 네트워크 전체로 확장 적용하는 과정에서 추가 개선될 수 있을 것으로 보인다.

사사문구

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 Grand ICT 연구센터지원사업(IITP-2020-2015-0-00742), 과학기술정보통신부 및 정보통신기획평가원의 글로벌핵심인재양성지원사업(IITP-2019-0-01579), 정보통신기술 진흥센터 (No.2015-0-00567, 유무선 통합 네트워크에서 접속 방식에 독립적인 차세대 네트워크 기술 개발)의 연구결과로 수행되었음.

참고문헌

- [1] Rashid Mijumbi, Joan Serrat, Juan-Luis Gorricho, Niels Bouten, Filip De Turck and Raouf Boutaba, "Network Function Virtualization: State-of-the-Art and Research Challenges," IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 236-262, 2016.
- [2] Jaewook Lee, Haneul Ko, Dongeun Suh, and Sangheon Pack, "Overload and failure management in service function chaining", IEEE Conference on Network Softwarization (NetSoft), Bologna, Italy, 2017, pp. 1-5.
- [3] Sara Ayoubi, Yiheng Chen, and Chadi Assi, "Towards Promoting Backup-Sharing in Survivable Virtual Network Design", IEEE/ACM Transactions on Networking, vol. 24, no. 5, pp. 3218-3231, 2016.
- [4] Saifeddine Aidi, Mohamed Faten Zhani, and Yehia Elkhatab, "On Improving Service Chains Survivability Through Efficient Backup Provisioning", International Conference on Network and Service Management (CNSM), Rome, Italy, 2018, pp. 108-115.

블루투스 비콘을 사용한 고객 관리와 결제 플랫폼 서비스

고혁준*, 한성수**, 전유부***, 정창성****

*고려대학교 영상정보처리협동과정

**강원대학교 자유전공학부

***순천향대학교 컴퓨터소프트웨어공학과

****고려대학교 전기전자공학부

e-mail : doltwo@hanmail.net*, sshan1@kangwon.ac.kr**, jeonyb@sch.ac.kr***, csjeong@korea.ac.kr****

Practical Implementation Customer management and payment platform service using Bluetooth beacon

Hyug-Jun Ko*, Seong-Soo Han**, You-Boo Jeon***, Chang-Sung Jeong****

*Dept. of Visual Information Processing, Korea University

**Dept. of Division of Liberal Studies, Kangwon National University

***Dept. of Computer Software Engineering, Soonchunhyang University

****Dept. of Electrical Engineering, Korea University

요 약

인터넷 상거래의 발전으로 온라인 쇼핑몰은 간편 결제와 같은 다양한 페이들을 지원하며 결제 방식에 있어서 다양한 방법들을 제공하고 있다. 한편, 경쟁 우위에 있는 다양한 온라인 앱들은 O2O(Online-to-Offline) 서비스를 기반으로 오프라인 매장에도 진출하고 있다. 반면, 기존의 오프라인 사업장을 가진 소상공인들은 ICT 적용과 활용을 위한 개발에 어려움을 겪고 있을 뿐만 아니라 고객 관리와 광고 등에서도 상대적인 열세로 인하여 오프라인 사업장의 수익은 점점 줄어드는 실정이다. 이러한 문제를 해결하기 위하여 본 논문에서는 블루투스 비콘 기술을 사용하여 고객 관리와 광고 등이 가능하며, 오프라인 사업장에도 적용이 가능한 방법을 제안한다. 제안 방법을 통하여 오프라인 매장에서 온라인 쇼핑몰처럼 관리가 가능하다.

1. 서론

인터넷의 발전은 다양한 분야에서 혁신을 가져왔다. 그 중에서도 인터넷을 활용한 온라인 쇼핑몰은 급격한 성장을 보이고 있으며, 결제 방식에 있어서도 간편 결제의 대표적인 스마트 페이의 사용을 비롯하여 다양한 방식을 지원하고 있다. 또한 인터넷 쇼핑몰에서 비롯된 결제 분야는 커다란 사업영역을 확보해 가고 있다. 한편, 경쟁 우위에 있는 다양한 온라인 앱들은 온라인에서의 제품 및 서비스 정보검색과 결제, 그리고 오프라인에서의 제품 수령이 혼합된 새로운 상거래 방식인 O2O(Online-to-Offline) 서비스를 기반으로 오프라인 매장에도 진출하며, 사업 영역을 점점 확대해 나가고 있다. 이에 반하여 오프라인 사업장을 가진 소상공인들은 ICT 활용을 위한 개발에 어려움을 겪고 있을 뿐만 아니라 고객 관리와 광고 등에서도 상대적인 열세로 인하여 오프라인 사업장의 수익은 점점 줄어드는 실정이다. 이들의 고객 유치와 고객

관리 활동은 블로그를 통한 온라인 광고나 SNS 에 등록된 회원들에게 문자 광고를 발송하여 고객의 유입을 유도하는 것이 대부분이다. 그러나 최근 위치기반 GPS 와 블루투스 비콘을 기반으로 하는 새로운 방법이 사용되고 있다. 특정 앱을 사용하여 고객이 사업장 근처에 접근했을 때 광고 푸쉬(push)를 보내어 매장 방문을 유도하는 방식이다. 비콘(beacon)은 블루투스를 기반으로 하는 무선 기술로써 페어링 없이 특정 정보를 지속적으로 전송할 수 있는 저전력 무선 통신 기술이다. 최근 블루투스는 무선 블루투스 이어폰과 자동차 내 블루투스 활용 및 스마트폰 등에서 활용이 늘어나고 있기 때문에 비콘의 활용도는 더 높아질 것으로 예상된다.

본 논문에서는 기존의 오프라인 사업장을 가진 소상공인들의 어려움을 해결하기 위하여 일반 매장에서 온라인 매장과 같이 고객 관리와 광고를 할 수 있는 방법을 제안하고자 한다. 제안 방법은 BLE 비콘

기술을 사용하여 단순 방문과 회원을 나누어 관리할 수 있는 방식이다. 또한, 고객과 매장 간에 상호작용을 통하여 매장에서는 고객을 인식할 수 있고 고객은 매장을 인식할 수 있는 방식의 서비스를 설계하고자 한다. 오프라인 매장에서든 온라인 쇼핑몰처럼 고객을 회원 및 비회원으로 구분하여 관리할 수 있다. 제안 플랫폼을 통하여 오프라인 사업장을 운영하는 소상공인들도 편리하게 고객 관리와 광고 등에 사용할 수 있을 것으로 기대한다.

2. 관련 연구

2.1. 핑거프린트(Fingerprint) 방식의 위치 추적

핑거프린트 방식은 위치 추적을 위한 정보로 신호 간섭과 주위의 환경 정보를 활용하는 방식으로써 무선 신호 기반의 위치 추적 시스템에서 가장 많이 사용되는 방식이다. 측정 위치 대상 공간에 기준점의 위치 정보를 데이터베이스에 저장한 뒤 위치 정보와 함께 AP(Access Point)로부터 스마트폰에 도달한 신호 세기를 측정하여 해당 정보를 저장한다. 이 작업을 모든 기준점에서 수행한다.

데이터베이스에 기준점에 대한 정보를 모두 저장한 뒤 스마트폰을 가진 사용자가 측정 위치를 요청하면 스마트폰에 수신되는 신호 세기를 측정한 후 데이터를 서버로 전송한다. 서버에서는 사용자로부터 전송된 신호와 데이터베이스에 저장된 신호의 정보를 비교하여 사용자의 위치를 판단하여 해당 위치 정보를 사용자의 스마트폰에 전송한다[2].

2.2. BLE(Bluetooth Low Energy) 비콘(Beacon)

비콘(beacon)은 근거리에서 있는 스마트 기기를 자동으로 인식하여 필요한 데이터를 전송할 수 있는 무선 통신 장치로써 블루투스 비콘(Bluetooth Beacon)이라고도 한다. 근거리 무선 통신인 NFC가 10cm 이내의 근거리에서만 작동하는 반면, 비콘은 최대 50m 거리에서 작동할 수 있다. 이러한 비콘 기술을 이용하면 쇼핑센터, 음식점, 박물관, 미술관, 영화관, 야구장 등을 방문한 고객의 스마트폰에 할인 쿠폰이나 상세 설명 등의 데이터를 전송할 수 있다[3].

또한, 비콘은 비콘 신호 송출 범위 안으로 스마트폰을 가진 사람이 들어오면 특정 ID 값을 전달한다. 이러한 값을 수신한 스마트폰 애플리케이션은 서버로 해당 정보를 전달한다. 서버는 전달 받은 ID 가 등록된 ID 인지 확인한 후 등록되어 있다면 해당 비콘이 설치된 위치에 대하여 설정된 이벤트나 서비스 정보를 스마트폰으로 전송한다[4].

이러한 비콘 기술을 사용하여 애플은 2013 년 12 월 미국 전역 254 개 애플스토어에서 iBeacon 서비스를

시작하였다. 애플스토어를 방문한 고객은 iBeacon 서비스를 통해 iPhone 이 진열된 테이블 옆을 지나갈 때 현재 자신이 사용하고 있는 iPhone 이 업그레이드 가능한지, 어떠한 보상판매 옵션을 제공받을 수 있는지 등의 정보를 제공받을 수 있다[5].

3. 구현

본 논문에서는 구글의 Eddystone 방식을 활용하였고, 라즈베리파이의 비콘 메시지를 작성하기 위해서 다음과 같은 명령어 셋(command set)을 만들 수 있다. 예를 들어 Eddystone-URL 인 `http://yoica.net/uid`의 메시지를 전송하기 위해 라즈비안의 셸에서 <그림 1>과 같은 메시지를 입력하면 라즈베리파이 4가 비콘처럼 주기적으로 Eddystone-URL 패킷 메시지를 전송한다[5].

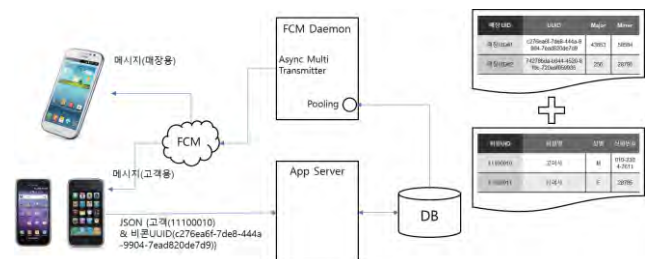
<그림 1. 라즈비안 셀 입력 메시지>

```

Your commands for " http://yoica.net/uid" are:
$ sudo hciconfig hci0 up
$ sudo hciconfig hci0 leadv 3
$ sudo hcitool -i hci0 cmd 0x08 0x0008 17 02 01 06
03 03 aa fe 0f 16 aa fe 10 00 02 79 6f 69 63 61 03 75
69 64 00 00 00 00 00 00 00 00

```

이를 수신하기 위해 비콘 스캐너가 해당 비콘 송신기를 발견했을 경우 이를 곧바로 서버에 질의를 하여 해당 서버가 판단하여 사용자에게 알림이 필요한 경우 클라우드 메시징 서비스를 이용하여 알림을 전송한다. 해당 사용자는 알림을 받고 클릭하면 해당 앱의 인텐트(intent)로 동작하여 안드로이드 결제 액티비티(Activity)를 실행하게 되며, 이때 앱은 공유 프리퍼런스(Shared Preference)[6]를 읽어 사용자를 특정하게 된다. 전송된 JSON 정보를 이용하여 소규모 매장 점주는 사용자 방문을 알 수 있으며, 매장 회원 정보와 매칭하여 고객을 식별할 수 있다. <그림 2>와 같이 고객과 매장 간에 상호작용 시스템의 구성을 설계하여 고객이 매장에 방문했을 때 <그림 3>과 같은 예시처럼 고객에게는 환영메시지 및 혜택을 JSON 형식으로 전송하여 FCM(Firebase Cloud Messaging)[7]을 통해 전송된 메시지를 앱에서 확인 후 알림 메시지를 띄워준다. 또한 <그림 4>와 같이 매장 관리자에게는 고객정보 및 통계정보를 발송하여 고객을 관리할 수 있다.



<그림 2. 비콘을 사용한 고객 관리 플랫폼 구성도>

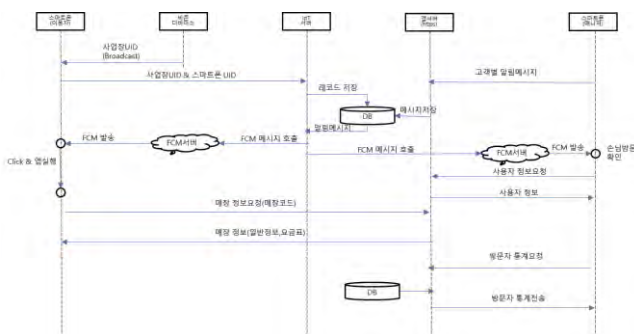

```
{
  "type": "system",
  "alarm": 1,
  "noti_id": "11100010",
  "title": "[주유소] GS칼텍스 카닥일산주유소",
  "content": " 휘발유: 1380원/L, 경유: 1280원/Lwn,
  5만원 주유시 2천 원 할인 쿠폰을 이용하면 커피나
  핫도그 등을 1천 원의 가격으로 이용할 수 있습니다.wn
  방문 클릭 http://yoica.net/uid=c276ea6f-7de8-444a-9904-7ead820de7d9"
}
```

<그림 3. 고객용 JSON 메시지 예시>

```
{
  "type": "system", "alarm": 1, "noti_id": "매장UID#1 ",
  "title": "[요이카] 고이사님이 3회 방문.",
  "content": "고이사님이 2020년 3회차 방문하였습니다."
}
```

<그림 4. 매장용 JSON 메시지 예시>

이를 전체적인 흐름으로 표현하면 <그림 5> 와 같은 메시지 흐름도로 표현할 수 있다.



<그림 5. 메시지 흐름도>

4. 결론

본 논문에서는 일반 매장에서든 온라인 매장과 같이 광고와 고객 관리를 할 수 있는 방법으로 BLE 비콘을 사용하여 단순 방문과 회원을 나누어 관리할 수 있는 플랫폼을 제안하였다. 제안 플랫폼은 매장에서 방문객에게 매장에 대한 정보를 제공하고, 앱을 통하여 수집된 단말 정보를 통해 단순 방문객과 매장 회원을 구분이 가능하다. 플랫폼을 통하여 스마트폰에서 매장 UUID(Universally Unique Identifier)를 받아서 앱을 통해 해당 매장 정보를 확인하고 해당 사용자와 매장 간의 관련정보를 확인하여 회원임을 특정함과 동시에 방문객들의 동향을 파악할 수 있는 방법이다.

향후에는 고객과 매장을 연결하는 결제 시스템 또는 간편 페이를 이용한 결제와 마일리지 제공을 통한 공유 경제 모델을 연구하고자 한다.

참고문헌

- [1] JaeKyung Kim, HyeJin Jeong, YuRi Jang, Yun Ji Moon, "Success Factors of O2O(Online-to-Offline) Commerce" Proceedings of the Korean Institute of Information and Communication Sciences Conference, pp.374 - 377, 2015.
- [2] Jeon H.S et al., "A Study on Algorithm for Efficient Location Tracking in Indoor Environment", Journal of information technology applications & management, Vol.13, No.3, 2006, 59-74
- [3] Tae-Woo Byeon, Seong-Yong Jang, "A Study on the Technological and Environmental Factors Affecting the Accuracy of Beacon Based Indoor Positioning System", Journal of the Korea Society for Simulation, Vol. 25, No. 2, pp. 21-29 (2016. 6)
- [4] "비콘, 위치기반 서비스의 핵심 인프라로 급부상", 한국방송통신전파진흥원, 2014.04.04, p31-39
- [5] 최주호, 김재범, 정동진, "IoT 사물인터넷을 위한 라즈베리파이 4 정석", 앤써북, 2019-11
- [6] Oglaza, Arnaud; Laborde, Romain; Zarate, Pascale; Benzekri, Abdelmalek; Barrere, Francois, "Difficulties to enforce your privacy preferences on Android? Kapuer will help you", Consumer Communications & Networking Conference (CCNC), 2016 13th IEEE Annual 2016 Jan, pp. 315- 316, 2016.
- [7] <https://firebase.google.com/>, 2017.2.

만물 접속 네트워크의 소셜 그룹 관리를 이용한 블록체인 프로토콜 운영 방안

김수연*, 강현국**

*계명대학교 산학협력단, **고려대학교 전자정보공학과
e-mail : sykim388@gmail.com

The Operation of Blockchain Protocol using Social Group Management of Network of Everything.

Suyeon Kim*, Hyun K. Kahng**

*Dept. of Industry Cooperation, Keimyung University

**Dept. of E&I Engineering, Korea University

요 약

본 논문에서는 분산 원장의 미들웨어 플랫폼으로 예상되는 블록체인 시스템의 실질적인 운영과 관련하여 블록체인 그룹 구조의 단점에 대하여 연구하고 이를 해결하기 위한 해결책으로 현재 ISO/IEC JTC1 SC6 에서 표준화가 진행중인 만물 네트워크 프로토콜의 사물 유저 소셜 그룹 관리기능을 이용한 블록체인의 운영 방법을 제시하였다. ISO/IEC JTC1 SC6 에서 표준화가 진행중인 만물네트워크의 사물 유저 소셜 그룹 관리기능은 안정적인 프로토콜 기능과 데이터 전송 관리를 제공하고 있으며 멤버 디스커버리기능, 데이터 전송 통로 관리기능 등의 그룹 관리 기능을 제공하고 있다. 이러한 기능을 블록체인 플랫폼에 활용할 수 있어서 블록체인 멤버 관리 및 그룹 관리 기능에 도움이 될 것으로 예상하며 표준화가 진행되고 있는 ISO/IEC JTC1 SC6 의 미래 네트워크 기능과 구조에 적극 반영하고자 한다.

1. 서론

블록체인 기술은 신뢰할 수 있는 중앙 서버의 제어 없이 P2P 기반의 네트워크에서 거래가 가능한 시스템으로 4 차 산업혁명의 기반 기술로 관심을 모으고 있다. 최근에는 PC 와 스마트폰을 이용한 O2O(Online to Offline) 거래가 증가하면서 해킹과 위·변조가 불가능한 블록체인 기술을 핀테크 산업전반에 적용하려는 새로운 비즈니스 모델이 증가하고 이를 위한 다양한 응용프로그램들이 개발되고 있다. 또한 글로벌 금융기관들은 파트너십을 통해 블록체인 시스템 구축과 표준 개발을 추진하고 있으며 이를 통한 블록체인의 활성화가 전 세계적으로 이루어질 것으로 예상된다.

한편 블록체인 기술은 비트코인같은 암호 화폐의 구현 기술로 탄생했기 때문에 데이터 구조나 프로토콜 방법이 범용적이지 못하다. 따라서 최근에는 다른 영역에서도 적용이 가능하도록 다양한 종류의 블록체인 플랫폼이 만들어져 운영되고 있어서 상호간의 호환성 문제는 해결되기 어렵다. [1][2]

블록체인 기술은 일반적인 P2P 네트워크를 사용하고 있어서 해결해야 할 과제가 아직 많다. 특히 참여하는 노드의 신뢰성과 브로드캐스트의 불확실성에 관한 문제가 있다. [3] 어떤 노드가 장시간 P2P 그룹에

참여하고 있다면 노드의 신뢰성은 높다고 할 수 있지만 P2P 그룹에 참여와 해제를 빈번히 하는 노드는 신뢰하고 확실한 통신을 하기 어렵다. 신뢰성자체를 측정하는 방법도 다양하기 때문에 검토가 필요하고 브로드캐스트에 대해서는 블록체인 네트워크 전체에서 동기화가 가능한지 데이터에 대한 신뢰성 있는 도착 보장은 어떻게 할 것인지에 대한 과제가 남아있다.

국제표준화 기구인 ISO/IEC JTC1 SC6 에서는 미래에 다가올 다양한 상위 프로그램을 지원하기 위한 미래 네트워크 하부 구조에 대한 연구를 진행하고 있으며 예상되는 요구사항을 바탕으로 프로토콜 표준화가 현재 진행 중이다. 미래 네트워크의 요구사항에 대한 세부적인 내용은 “ISO/IEC TR 29181-series, Problem statements and Requirements” 문서에서 정의가 되어 있으며 이를 바탕으로 ISO/IEC 21558 미래 네트워크 구조에 대한 표준화와 ISO/IEC 21559 미래 네트워크에 대한 프로토콜과 메커니즘을 표준화하고 있다. [4][5]

최근에 CD(Committee Draft)로 등록되었고 DIS(Draft International Standard) 등록을 추진하고 있는 ISO/IEC 21558 미래 네트워크 구조 문서와 ISO/IEC 21559 미래 네트워크 프로토콜 문서는 [표 1]과 같은 영역으

본 논문은 산업통상자원부의 ‘국가표준기술력향상사업’의 지원에 의해 작성되었습니다.(No. 20002532)

로 세분화되어 구성되었다.

문서번호	제목
ISO/IEC 21558-1	Architecture Part 1: Switching and Routing
ISO/IEC 21558-2	Architecture Part 2: Proxy model based Quality of Service
ISO/IEC 21558-3	Architecture Part 3: Network of Everything
ISO/IEC 21559-1	Protocol Part 1: Switching and Routing
ISO/IEC 21559-2	Protocol Part 2: Proxy model based Quality of Service
ISO/IEC 21559-3	Protocol Part 3: Network of Everything

[표 1] 미래 네트워크 표준화 영역

본 논문에서는 [표 1]의 표준화 영역 중 ISO/IEC 21558-3 Network of Everything (만물네트워크, NoE) 아키텍처 구조에 블록체인 데이터 전송 관리 모델을 프로토콜 능력 세트(Capability Set)로 구성하여 적용하려 한다. [6] 그리고 현재의 네트워크 시스템에서 다양한 블록체인 응용플랫폼이 운영될 경우에 필요한 멤버 관리와 그룹 관리 방법에 대하여 분석하였다. 이러한 분석을 바탕으로 ISO/IEC JTC1 SC6 에서 표준화가 추진중인 미래네트워크의 그룹 관리 방안과 블록체인 운영에 필요한 프로토콜 기능을 융합하여 표준화에 적용하고자 한다. 이러한 내용을 기반으로 미래네트워크에 대한 표준화가 이루어진다면 블록체인과 함께 최적의 미래 네트워크가 새로운 플랫폼으로 제공되어 사용자에게 최적의 안전 거래 시스템을 제공할 수 있을 것이라 생각한다.

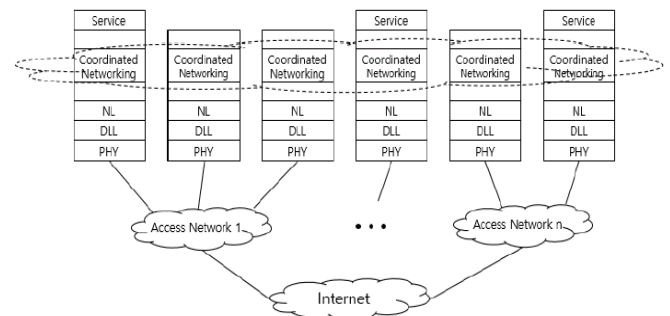
이를 위하여 본 논문의 2 장에서는 만물네트워크 표준화 항목 중 ISO/IEC 21558-3 만물네트워크 구조 및 그룹 관리 기능에 대하여 소개하고 3 장에서는 미래 네트워크의 그룹 관리 기능상에서 블록체인 운영 방법을 제시하고 ISO/IEC JTC1 SC6 의 미래 네트워크 표준화에 이러한 요구사항을 적용하기 위한 필요성을 언급할 예정이다. 마지막으로 4 장에서 블록체인의 운영을 위해 미래 네트워크에 적용할 요구사항에 대한 결론을 논하고 앞으로의 연구계획을 제시하고자 한다.

2. 만물 네트워크 프로토콜 소개 및 그룹 관리 기능

ISO/IEC 21558-3 만물네트워크 구조 문서에 따르면 만물 네트워크는 만물 네트워크를 사용하고자 하는 사용자들 사이에 두가지 서비스를 제공하는데 사물 유저 소셜 네트워킹(Thing-user social networking)과 사물 유저 중심 통신 서비스(Thing-user centric communication service)이다. 사물 유저 소셜 네트워킹이 형성되면 형성된 소셜 네트워킹에 포함된 사물 유저(Thing-user)는 자신의 능력을 감지할 수 있는 지적인 능력을 소유하고 있으며 이러한 지적 정보를 다른 사물 유저와 서로 공유하고 또한 다른 사물 유저에 의해 제공된 능력들을 활용할 수 있다. 사물 유

저 중심 통신 서비스는 사물 유저들 사이에 협의된 규약에 의해 다양한 정보나 필요한 결정에 대한 반응을 주고 받음으로써 공동작업을 수행할 수 있는 서비스를 제공해 준다.

만물 네트워크에서는 이중 망간의 연결상에서도 서비스가 정해진 규약으로 동작할 수 있도록 구성하기 위하여 사물 유저 소셜 네트워킹 서비스를 제공하는 Coordinated Networking Layer 를 OSI 수송 계층 위에 규정하였다. 아래 (그림 1)에서 보는 바와 같이 Coordinated Networking Layer 는 OSI 응용 계층에 위치하고 있고 사물 유저의 정보교환 및 경험 정보 공유, Discovery 동작을 수행하게 된다.



(그림 1)만물접속네트워크 계층구조

만물네트워크를 지원하기 위하여 Coordinated Networking Layer 는 [표 2]에서 보는 바와 같이 여러 개의 기능 블록으로 구성되는데 thing-user management 블록, thing-user social networking 블록, coordinated experience management 블록, coordinated peer discovery 블록, proximal path management 블록, thing-user centric networking control 블록으로 구성된다. 각 기능 블록의 역할은 다음과 같다.

기능 블록	역할
thing-user management 블록	각 사물 유저가 가진 자원과 능력 세트의 프로파일을 유지하고 필요한 네트워크 자원들을 관리한다.
thing-user social networking 블록	사물 유저의 그룹을 만들거나 해체함으로써 그룹을 관리하고 사물 유저사이의 연결을 설정한다.
coordinated experience management 블록	사물 유저의 요청에 적합한 기능을 보유한 다른 사물 유저를 검색하고 찾아준다.
coordinated peer discovery 블록	공동작업을 수행하기에 적합한 사물 유저를 발견하기 위한 프로세스를 처리한다.
proximal path management 블록	필요한 사물 유저를 찾기 위하여 최고 근접한 사물 유저와의 근접 경로를 만들어준다.
thing-user centric networking control 블록	사물 유저의 관계망을 만들어주고 연결을 설립해준다

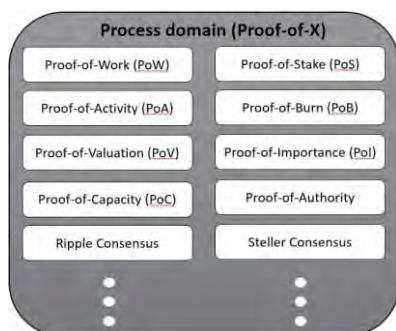
[표 2] Coordinated Networking Layer 의 기능 블록

3. 만물네트워크의 사물 유저 관리 기능과 블록체인

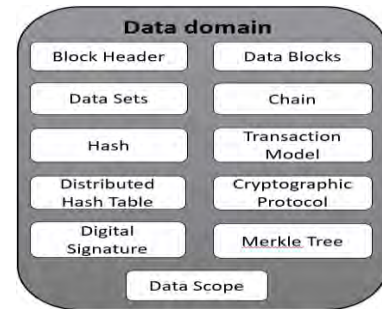
데이터 전송 기능

만물네트워크 플랫폼에서 블록체인 프로토콜을 지원하기 위해서 2장에서 언급된 6개의 기능 블록 중에 thing-user management 블록의 사물 유저 프로파일에 블록체인 관련 기능들을 적용하여 능력 세트(Capability Set)로 구축하고자 한다. 만물네트워크에서 사물 유저 소셜 네트워킹을 구축할 때 블록체인 프로토콜이 동작하는 사물 유저 소셜네트워킹을 지원하기 위하여는 두가지 절차가 필요하다. 첫째는 특정한 블록체인 기능을 이용하고자 하는 사물 유저가 소셜 네트워킹에 참여하고자 할 때 원하는 블록체인 프로토콜 능력 세트에 구성된 소셜 네트워킹을 검색하고 적절한 블록체인 능력 세트를 가진 소셜네트워킹이 발견되면 참여하게 된다. 둘째로 참여가 완료되면 참여하고 있는 다른 사물 유저와 블록체인 프로토콜 관련된 능력 정보를 공유하게 된다. 목적에 따라서 하나의 사물 유저는 동시에 두개 이상의 소셜네트워킹에 연결도 가능하다. 연결되어 공동작업을 수행하는 동안에도 소셜네트워킹내에서 정보를 주고 받으면서 더 많은 정보를 요청할 수 있다.

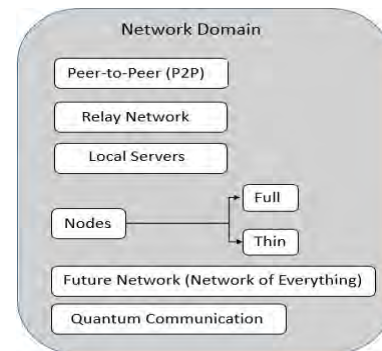
사물 유저 소셜네트워킹을 형성한 사물 유저는 그들의 통신 능력과 소셜네트워킹에 참여한 동기, 경험, 초현실적 지능 정보를 전달하기 위한 협업의 의도까지도 공유하게 된다. 기본적으로 전달되는 이름, 주소, URI, URL 과 보안 정보뿐만 아니라 다양한 블록체인 관련된 정보도 교환하여 블록체인 플랫폼을 지원하는 소셜네트워킹을 구축하게 된다. 중앙집중형 서버의 중개없이 블록체인 트랜잭션을 처리하는 각 사물 유저 소셜 네트워킹은 거래에 참석하는 사물 유저들의 연결된 소셜 네트워킹 상에서 동작한다. 그리고 참여한 노드들이 보유한 자원(프로세싱 파워, 디스크 용량, 네트워크 대역폭 등)을 이용하여 트랜잭션이 가능하다. 이러한 운영을 지원하기 위하여 블록체인 기술을 능력 세트로 구성하여야 하는데 본 논문에서는 3개의 기술 도메인으로 분류하여 사물 유저의 능력 세트로 구분하였다. (그림 2)에서 보는 바와 같이 Process 도메인에서의 능력 세트는 블록체인의 중요한 기능인 컨센서스 프로토콜의 기능을 집합으로 가지고 있고 (그림 3)의 Data 도메인에서는 블록체인 데이터 처리 기능을 집합체로 가지고 있다.



(그림 2) Process Domain 상의 능력 세트



(그림 3) Data Domain 상의 능력 세트



(그림 4) Network Domain 상의 능력 세트

(그림 4)에서는 블록체인이 운용될 하부 네트워크의 능력 세트를 표시하고 있다. 블록체인의 프로토콜에 적합한 네트워크 환경을 협상하고 선택하기 위해 존재한다. 이러한 블록체인 기능과 관련된 능력 세트를 보유한 사물 유저는 필요한 서비스 기능에 따라 적절한 능력 세트 서비스를 협상하여 블록체인 사물 유저 소셜 그룹에 참여하고 참여가 완료되면 블록체인 데이터를 다른 사물 유저와 교환할 수 있다. 이러한 세부적인 과정은 다음과 같다.

- 1) 블록체인 사물 유저 소셜 그룹의 형성: 최초로 블록체인 사물 유저 소셜 그룹을 형성할 필요가 있을 때 필요로 하는 사물 유저가 블록체인 그룹을 형성하기 위한 최초의 사물 유저가 된다. 정당한 승인절차를 거쳐서 사물 유저 소셜 그룹의 서버 역할을 수행할 노드는 필요한 보안 기능과 블록체인 능력 세트를 가지고 정보를 교환할 수 있는 그룹을 형성하게 된다.
- 2) 블록체인 그룹에 참여하기: 사물 유저가 블록체인 사물 유저 소셜 그룹에 등록하고자 한다면 기본적인 블록체인 능력 세트를 교환 협상하고 의도와 동기를 포함한 정보를 교환하게 된다. 소셜 그룹에서 참여를 허락한다면 참여를 할 수 있게 되고 참여한 사물 유저의 의도를 그룹내 모든 사물 유저가 공유하게 된다. 이렇게 함으로써 블록체인 사물 유저 소셜 그룹의 멤버가 되고 공동작업에 참여하게 된다.
- 3) 블록체인 사물 유저 소셜 그룹에서 작업 경험 공유하기: 사물 유저 소셜 그룹이 형성되면 블록체인 능력을 기반으로 경험이나 지식이 사물 유저 멤버들 사이에 공유된다. 참여하는 멤버들사이의 프로세싱 파워나 메모리 양 같은 자원의 차이에

의해 공유하는 것은 제한될 수 있고 블록체인 능력 세트를 지원하기 위해 특정 자원 또는 능력을 요청하는 멤버에게 적절한 자원과 기능을 할당할 수 있어야 한다.

- 4) 블록체인 사물 유저 소셜 그룹에 참여할 노드의 발견: 블록체인 사물 유저 소셜 그룹에 특정의 사물 유저가 필요하다면 소셜 그룹의 서버 역할을 수행하는 사물 유저가 참여 요청 대상의 사물 유저에 대한 순결성을 확인하기 위하여 절차를 시작한다. 서버 사물 유저는 보유한 능력 세트 profile 을 통하여 확인절차를 걸쳐서 그룹에 참여시키게 된다.

4. 결론

블록체인 기술은 전자화폐를 비롯한 스마트 계약 등 앞으로 다른 영역에서도 적용이 가능하도록 다양한 플랫폼의 형태로 만들어질 것이다. 따라서 증권회사, 은행, 거래솔루션기업, O2O 를 포함한 전자상거래 기업의 영역으로 확대될 것이 분명하며 다양한 개발 기관들이 함께 참여하여 국제적으로 운영되는 새로운 생태계를 구축할 것으로 예상된다.

본 논문에서는 이와 같이 다양한 블록체인 플랫폼이 혼재되어 운영될 것으로 예상됨에 따라 블록체인 플랫폼 간에 호환성을 제공하고 블록체인 프로토콜 기능이 필요한 사물의 그룹 관리 기능을 제공하는 방법을 연구하였다. 또한 하부 네트워크 구조로써 ISO/IEC 21558-3 만물네트워크 아키텍처 구조에 블록체인 데이터 전송 관리 기능을 프로토콜 능력 세트 (Capability Set)로 구성하고 그룹 관리 방안과 블록체인 운영에 필요한 프로토콜 기능을 적용하였다.

이러한 내용을 기반으로 만물네트워크에 대한 표준화가 이루어진다면 블록체인과 함께 최적의 미래 네트워크가 새로운 플랫폼으로 제공되어 사용자에게 최적의 안전 거래 시스템을 제공할 수 있을 것이라 생각한다.

참고문헌

- [1] Satoshi Nakamoto, "Bitcoin: A Peer-to Peer Electric Cash System", www.bitcoin.org, 2008. 10. 31.
- [2] C. Decker, R. Wattenhofer, "Information propagation in the bitcoin network", 13th IEEE International Conference on Peer-to-Peer Computing, 2013, pp. 1-10
- [3] 아카하네 요시하루, 아이케이 마나부, "블록체인 구조와 이론", 2017 년 6 월 23 일, 위키북스, ISBN 979-11-5839-066-2
- [4] ISO/IEC 21558-3 - Information Technology - Telecommunications and information exchange between systems - Future Network - Architecture
- [5] ISO/IEC 21559-3 - Information Technology - Telecommunications and information exchange between systems - Future Network - Protocols and mechanisms
- [6] Claudio Lime, "DLT/Blockchain Architectures and Reference Frameworks", Blockchain Engineering Council

5G 네트워크에서 기계학습 기반 트래픽 예측을 통한 네트워크 슬라이싱 자원 예약 기법

이필원*, 이아름*, 박수용*, 신용태**

*숭실대학교 컴퓨터학과

**숭실대학교 컴퓨터학부

pwlee@soongsil.ac.kr

Machine Learning-based Network Slicing Resource Reservation Scheme in 5G Network

Pil-Won Lee, Soo-Yong Park, Yong-Tae Shin

Department of Computer Science, Soongsil University

요 약

최근 초저지연, 초고속, 초연결 네트워크를 요구하는 기술들이 급속하게 발전하고 있다. 기존 4G 네트워크는 위 요구사항을 만족할 수 없었기 때문에 5G 네트워크가 등장했다. 5G 네트워크는 네트워크 가상화 기반 네트워크 슬라이싱을 통해 각각의 서비스마다 독립적인 네트워크 환경을 제공한다. 그러나 네트워크에 참여하는 서비스가 다양해질수록 트래픽 부하가 폭발적으로 증가할 것으로 예상되며 트래픽 부하에 따른 병목현상이 발생할 가능성이 여전히 존재한다. 본 논문에서는 인공 신경망 알고리즘 RNN을 활용하여 트래픽을 예측하고 예측 결과를 기반으로 네트워크 슬라이싱의 자원을 선제적으로 조절하는 기계학습 기반 네트워크 슬라이싱 자원 예약 기법을 제안한다.

1. 서론

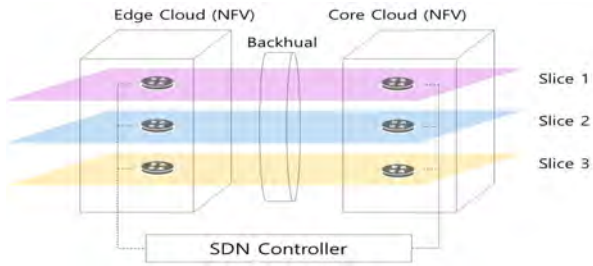
최근 사물인터넷, 가상현실 및 자율주행 등의 네트워크에 초저지연, 초고속, 초연결을 요구하는 다양한 기술이 급속하게 발전하고 있다. 기존 4G 네트워크 기술은 이러한 요구사항을 만족할 수 없기 때문에 5G 네트워크 기술이 등장했다. 5G 네트워크의 핵심 기술인 네트워크 슬라이싱(network slicing)은 네트워크 가상화를 통해 각각의 서비스에 특화된 네트워크 환경을 제공한다[1]. 그러나 5G 네트워크를 적용하는 기술의 종류가 다양해질수록 네트워크에 트래픽 부하가 폭발적으로 증가할 것으로 예상되기 때문에 여전히 트래픽 부하로 인한 병목현상이 발생할 가능성이 존재한다. 따라서 본 논문에서는 트래픽 추적 데이터를 기계학습 알고리즘을 활용하여 학습하고 시간에 따른 서비스별 트래픽 사용량을 예측한다. 그리고 예측한 트래픽 사용량에 따라 네트워크 슬라이싱을 통해 서비스별로 가상화된 네트워크의 자원을 예약하는 시스템 구조를 제안한다. 본 논문의 구성은 다음과 같다. 2장에서는 기존에 활용되는 5G 네트워크 슬라이싱 기법에 대해 살펴보고 요구사항을 분석한다. 3장에서는 본 논문에서 제안하

는 기계학습 기반 네트워크 슬라이싱 자원 예약 기법을 제안한다. 4장에서는 제안하는 기법의 성능을 분석하고, 마지막 5장에서는 결론을 제시한다.

2. 관련 연구

2-1.SDN 및 NFV를 적용한 5G 네트워크

SDN(Software-defined Networking)[2],[3]은 기존 네트워크의 한계를 뛰어넘을 수 있는 새로운 네트워킹 패러다임이다. SDN의 개념 및 특징은 첫째, 라우터 및 스위치의 데이터 영역과 제어 영역을 분리하여 수직적 통합을 제거한다. 둘째, 기존의 수직적 통합을 분리함에 따라 라우터는 데이터 영역의 단순한 데이터 전달 기능만 담당하는 장치가 되고 제어 영역의 경로 연산 기능이 중앙 집중화된 원격의 컨트롤러에 위임되며 네트워크 정책 구성과 집행이 단순화된다[4]. NFV(Network Functions Virtualization)은 소프트웨어 가상화 기술을 통해 기존 네트워크 하드웨어 기능을 구현하고 가상화된 범용 서버 및 스위치로 네트워크를 구현하는 기술이다[5]. 이러한 네트워크 기능 가상화는 새로운 서비스에 대해 네트워크 하드웨어를 추가로 설치하지 않고 온디맨드 방식으로 네트워크 인스턴스를 생성할 수 있다.



(그림 1) NFV와 SDN이 적용된 네트워크 구성도

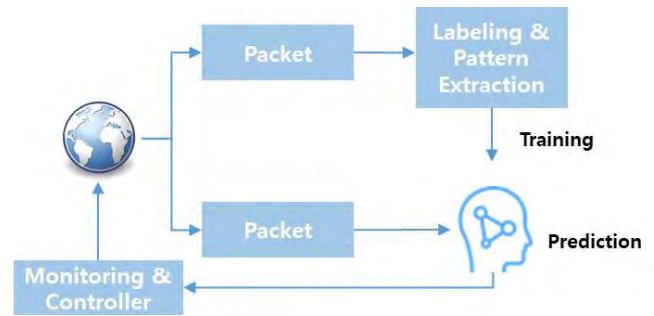
[그림 1]은 SDN과 NFV이 적용된 네트워크를 표현한 그림이다. NFV는 5G 네트워크에서 다양한 조건을 가진 서비스를 상황에 맞게 유연한 네트워크 인스턴스를 제공할 수 있게 한다. SDN은 NFV를 통하여 만들어진 가상 스위치 기능을 제어하여 가상 네트워크 환경을 구성한다.

2-2.네트워크 슬라이싱(Network Slicing)

네트워크 슬라이싱은 서로 다른 서비스들의 네트워크 요구사항을 모두 수용하고 각각의 서비스 별로 다른 네트워크 환경을 제공한다[6]. [그림 1]에서처럼 나누어진 세 개의 슬라이스는 각각 서로 다른 네트워크 환경을 제공한다. 따라서 네트워크 슬라이싱 기능이 구현되기 위해서는 5G 네트워크에서 엣지 클라우드 및 코어 클라우드를 NFV를 활용한 가상화가 선행되어야 한다. 각 슬라이스는 가상화된 자원을 할당 받으며 하나의 슬라이스에서 오류가 발생하여도 다른 슬라이스에 영향을 미치지 않는다. 5G 네트워크는 각기 다른 서비스에 대해 독립적이고 안정적인 네트워크를 제공해야하므로 네트워크 슬라이싱을 활용한다.

2-3.네트워크 머신러닝(Network Machine Learning)

네트워크 머신러닝의 주된 목적은 네트워크 데이터를 기반으로 지식(Knowledge)을 구성하고 이를 이용하여 자동으로 네트워크의 제어 및 관리를 하는 것이다[7]. 기존에는 네트워크의 오류를 유발하는 데이터의 패턴을 분류하여 특정 패턴의 네트워크 데이터를 입력되면 네트워크가 오류에 대처할 수 있는 조치를 취하도록 시스템을 구성하였다. 기존 패턴 인식은 지도학습(supervised learning)을 이용해서 과거 데이터 패턴을 학습하고 학습 모델을 구축하여 네트워크 오류를 예측한다.

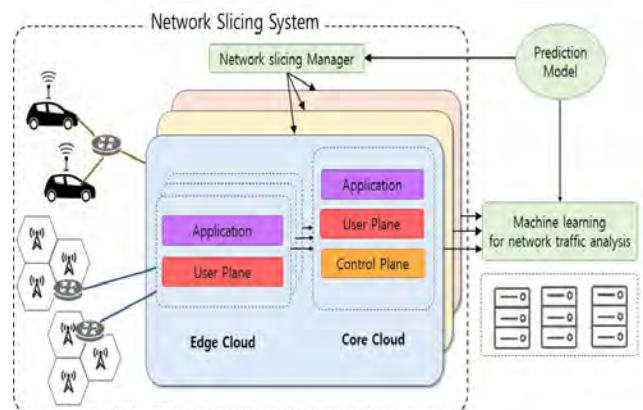


(그림 2) 네트워크 머신러닝 시스템 구성도

[그림 2]는 네트워크 패킷을 분석하여 라벨링 및 패턴 추출을 통해 기계학습을 하고 학습된 모델을 통해 예측을 하고 네트워크를 모니터링 및 컨트롤하는 시스템의 구성도이다. 그러나 5G 네트워크에서는 데이터의 종류가 시간이 흐를수록 다양해지기 때문에 오류를 유발하는 패턴의 변화를 지속적으로 학습해야만 새로운 오류에 대처할 수 있다[8].

3. 제안하는 기계학습 기반 네트워크 슬라이싱 자원 예약 기법

제안하는 기계학습 기반 네트워크 슬라이싱 자원 예약 기법은 크게 네트워크 슬라이싱에서 발생하는 트래픽 데이터를 분석 및 학습하는 부분과 네트워크 슬라이스의 자원을 제어하는 네트워크 슬라이스 관리자로 구성된다.



(그림 3) 제안하는 기계학습 기반 네트워크 슬라이싱 자원 예약 기법 구조도

3-1.트래픽 데이터 분석 및 학습

트래픽 데이터를 분석하여 학습하는 알고리즘은 시계열 데이터를 학습하는데 특화된 RNN(Recurrent Neural Network)을 활용하여 학습 모델을 구축한다.

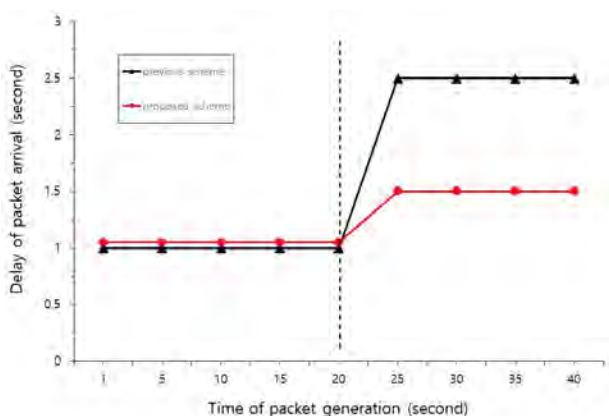
RNN은 학습 데이터를 통해 학습 모델 내 가중치를 결정한다. 이 때 과거의 가중치를 활용하여 현재 학습에 반영하므로 다양한 패턴의 변화를 지속적으로 학습하기에 적합하다. 제안하는 기법의 전략은 초기에 트래픽 데이터를 수집하여 학습 모델을 구축하고 이후 네트워크를 운영한다. 운영을 할 때 발생한 트래픽 데이터는 분석 서버에서 수집하게 되며 수집한 데이터는 다시 학습에 활용하여 예측 모델이 패턴이 변화되어도 정확히 예측할 수 있게 한다.

3-2. 네트워크 슬라이스 자원 관리자

네트워크 슬라이스는 NFV를 통해 가상화된 범용서버의 물리적 자원을 활용한다. 따라서 네트워크 슬라이스 자원 관리자는 앞서 분석 서버에서 예측한 트래픽 사용량에 의존하여 가상화된 자원을 할당한다. 할당하는 자원의 종류는 정량화 가능한 CPU, 메모리, 네트워크 대역폭이 있다. 자원을 할당하는 기준은 자원 할당에 따른 트래픽 포화 상태를 측정하여 정의한다. 따라서 자원 관리자는 분석 서버에서 전달하는 시간에 따른 트래픽 예측을 자원 할당 기준과 비교하여 이미 할당 되어 있는 자원이 예측된 트래픽을 처리할 수 있는지 판단하고 자원을 조정한다.

4. 성능평가

본 논문에서 제안하는 기법의 성능을 평가하기 위해 자원이 고정된 시스템과 제안하는 기법이 적용된 시스템에 기존에 할당된 자원으로는 원활한 처리가 불가능한 만큼의 인위적인 트래픽을 부하했다.



(그림 4) 기존 기법과 제안하는 기법의 패킷 지연시간 비교

제안하는 기법은 기존의 자원이 고정된 시스템과

비교해 패킷 지연 시간이 감소하였으며 안정적으로 트래픽을 처리할 수 있는 것을 확인하였다.

5. 결론

5G 네트워크에 참여하는 서비스의 다양화에 비례하여 네트워크 트래픽 또한 폭발적으로 증가될 것으로 예상된다. 이에 따라 5G 네트워크는 NFV 기반의 네트워크 슬라이싱 기법을 활용하여 각각의 서비스마다 독립적인 네트워크 환경을 제공하지만 트래픽 과부하 상황에서의 네트워크 병목현상 발생 가능성이 여전히 존재한다. 본 논문에서는 트래픽 데이터를 인공지능망의 종류 중 하나인 RNN을 활용하여 예측모델을 구축하고 예측 결과를 기반으로 네트워크 슬라이스 관리자가 선제적으로 자원을 조절하는 기법을 제안하였다.

ACKNOWLEDGMENT

이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.IITP-2017-0-00724, 셀룰러 기반 산업 자동화 시스템 구축을 위한 5G 성능 한계 극복 저지연, 고신뢰, 초연결 통합 핵심기술 개발)

참고문헌

- [1] "NGMN 5G White Paper", Tech Rep., vol. 1, Feb. 2015.
- [2] N. Mckeown, How SDN will shape networking. Invited talk at Open Networking Summit. Oct. 2011.
- [3] S. Schenker, The future of networking and the past of protocols, Invited talk at Open Networking Summit. Oct. 2011.
- [4] H. Kim, N. Feamster, "Improving network management with software defined networking", IEEE Commun. Mag., vol. 51, no. 2, pp. 114-119, Feb. 2013.
- [5] B. Han, V. Gopalakrishnan, L. Ji and S. Lee, "Network function virtualization: Challenges and opportunities for innovations," in IEEE Communications Magazine, vol. 53, no. 2, pp. 90-97, Feb. 2015.
- [6] X. Foukas, G. Patounas, A. Elmokashfi and M. K. Marina, "Network Slicing in 5G: Survey and Challenges," in IEEE Communications Magazine, vol. 55, no. 5, pp. 94-100, May 2017.

- [7] H. Lim, J. Kim and Y. Han, "Research Trend on Network Machine Learning," Journal of Advanced Technology Research, vol. 2, no. 2, pp. 13-20, 2017.
- [8] S. Jiang, B. Liu, P. Demestichas, J. Francois, G. M. Moura, P. Barlet, "Applying machine learning mechanism with network traffic", IETF Internet Draft (Work in progress), <https://tools.ietf.org/html/draft-jiang-nmlrg-traffic-machine-learning-00>, Dec. 2016.

Apache Kudu와 Impala를 활용한 Lambda Architecture 설계

황윤영*, 이필원*, 신용태**

*숭실대학교 컴퓨터학과

**숭실대학교 컴퓨터학부

doublewhy@soongsil.ac.kr, pwlee@soongsil.ac.kr, shin@ssu.ac.kr

Lambda Architecture Design using Apache Kudu and Impala

Yun-Young Hwang, Pil-Won Lee, Yong-Tae Shin
Soongsil University, Science of Computer

요 약

데이터의 양은 기술의 발전으로 발생하는 크게 증가하였고 다양한 빅데이터 처리 플랫폼이 등장하고 있다. 이 중 가장 널리 사용되고 있는 플랫폼이 Apache 소프트웨어 재단에서 개발한 Hadoop이며, Hadoop은 IoT 분야에도 사용된다. 그러나 기존에 Hadoop 기반 IoT 센서 데이터 수집 분석 환경은 Hadoop의 코어 프로젝트인 HDFS의 Small File로 인한 네임노드의 과부하 문제와 Import된 데이터의 Update나 Delete가 불가능하다는 문제가 있다. 본 논문에서는 Apache Kudu와 Impala를 활용해 Lambda Architecture를 설계한다. 제안하는 Architecture는 IoT 센서 데이터를 Cold-Data와 Hot-Data로 분류해 각 성격에 맞는 스토리지에 저장하고 Batch를 통해 생성된 Batch-View와 Apache Kudu와 Impala를 통해 생성된 Real-time View를 활용해 기존 Hadoop 기반 IoT 센서 데이터 수집 분석 환경의 문제를 해결하고 사용자가 분석된 데이터에 접근하는 시간을 단축한다.

1. 서론

데이터의 발생량은 5G의 등장으로 초고속, 초저지연을 이용한 새로운 IoT 기술이 등장하고 발전하면서 폭발적으로 증가하고 있다. 다양한 빅데이터 처리 플랫폼이 이를 처리하기 위해 등장하고 있다. Hadoop은 이 중 가장 널리 사용되고 있는 플랫폼 중 하나로 Apache 소프트웨어 재단에서 개발했다. Hadoop은 빅데이터를 수집, 저장, 처리, 분석, 시각화하는 다양한 서브 프로젝트를 프레임워크로 제공한다. Hadoop의 코어 프로젝트인 HDFS(Hadoop Distributed File System)는 블록 기반의 대용량 데이터 저장소로 최소 64MB에서 256MB 크기의 블록 단위에 데이터를 저장하기 때문에 설정된 블록의 사이즈를 최대한 활용해야 효율성이 좋아진다.

그러나 작은 단위의 데이터를 지속적으로 생성하는 IoT 센서 데이터 수집 분석 환경의 경우 HDFS에 구성된 최소 크기의 블록만큼 데이터가 생성되기 전에 저장되는 Small File 문제로 인해 네임노드에 과부하가 발생해 전체적인 시스템의 성능을 저하시키는 문제가 있다.[1] HDFS는 블록에 파일 형식으

로 데이터를 저장하기 때문에 Import된 데이터의 Update나 Delete가 불가능하다. Apache Kudu는 이와 같은 문제를 해결하기 위해 개발되었다.

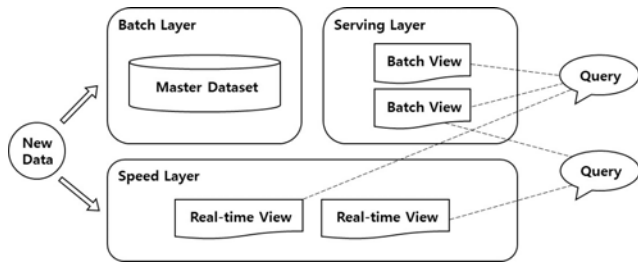
제안하는 Apache Kudu와 Impala를 활용한 Lambda Architecture는 Hadoop 기반의 IoT 센서 데이터 수집 분석 환경에서 발생하는 Small File 문제를 해결한다. 제안하는 Architecture는 Hadoop에서 불가능한 Import된 데이터의 수정 문제를 Apache Kudu와 Impala를 활용하여 해결한다. 갱신 주기가 짧으며 크기가 작은 실시간 데이터와 갱신 주기가 긴 저장되어 있는 대용량 데이터를 빠르게 분석하는 환경을 제공한다.

본 논문의 구성은 다음과 같다. 2장에서는 Lambda Architecture의 정의와 특징, Apache Kudu와 Apache Impala에 대해 살펴본다. 3장에서는 제안하는 Apache Kudu와 Impala를 활용한 Lambda Architecture를 설계한다. 4장에서는 결론 및 향후 연구 방향을 제시한다.

2. 관련 연구

2-1. Lambda Architecture

Lambda Architecture는 오래된 데이터를 보관하는 배치(Batch) 테이블과 실시간 데이터를 가진 실시간 테이블을 JOIN하여 결과값을 얻을 수 있도록 구성된 Architecture이다.[2] [그림 1]은 Lambda Architecture의 구조를 나타낸다.



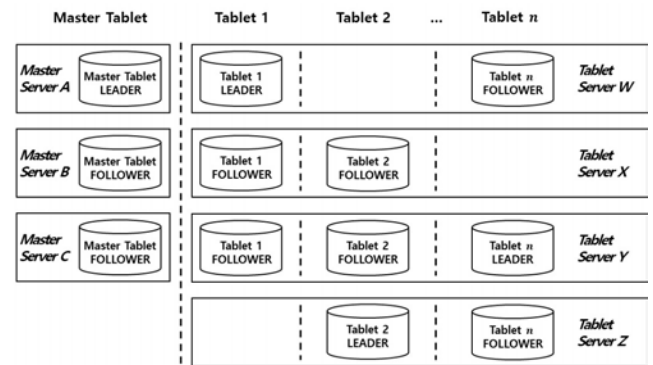
[그림 1] Lambda Architecture의 구조

Lambda Architecture는 Batch Layer, Speed Layer, Serving Layer로 구성되어 있다. Batch Layer에서는 Batch를 이용해 데이터를 미리 계산하여 저장소에 raw 데이터를 보관한다. Batch View의 데이터가 부정확할 때 저장소의 raw 데이터를 통해 복구가 가능하다. 기존의 raw 데이터는 새로운 View를 제공하고자 할 때 통계 분석이 가능하다. Speed Layer는 데이터를 실시간으로 집계해 별도의 테이블에 저장하여 Batch가 실행되는 동안 발생하는 조회에 대한 공백 문제를 해결한다. Serving Layer는 Batch Layer 및 Speed Layer의 출력을 저장한다. 클라이언트는 Serving Layer에 저장된 데이터를 조회하기 때문에 빠른 응답이 가능하다.

2-2. Apache Kudu

Apache Kudu는 Apache 소프트웨어 재단에서 개발한 컬럼 지향 데이터 스토리지이다. Apache Kudu는 Hadoop 기반의 프레임워크 대부분과 호환되며 Hadoop의 범용 하드웨어 사용성, 확장성, 데이터 가용성 보증의 특성을 지원한다. Apache Kudu는 블록 기반의 스토리지가 아닌 NoSQL OLAP 데이터베이스로 HDFS에서 불가능한 Update와 Delete 명령문을 지원한다. Apache Kudu는 데이터를 칼럼 기반으로 저장하여 특정 칼럼만 읽을 때는 디스크에서 읽는 데이터의 양을 줄여 성능을 높인다. Apache Kudu는 일반 DBMS처럼 Primary Key를 제공하며, Primary Key는 내부적으로 B+트리로 저장되어 대규모 데이터에서 빠르게 원하는 데이터에 접근한다.

Apache Kudu는 데이터 저장소 역할만 하는 플랫폼으로 이를 사용하기 위해 서버가 필요하다.[3] [그림 2]는 Apache Kudu의 서버 구성을 나타낸다.

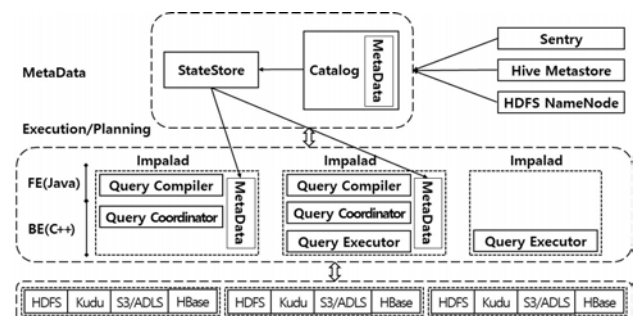


[그림 2] Apache Kudu의 서버 구성

Apache Kudu 내 데이터는 구조화되어 테이블에 저장되며, 테이블은 Tablet이라는 단위로 세분화되어 Tablet 서버에 저장된다. 스토리지 시스템은 메타데이터를 관리하는 마스터 노드와 사용자 데이터인 Tablet을 저장하는 Tablet 서버로 구성된다. Apache Kudu는 하나 이상의 마스터 노드와 Tablet 서버로 구성된다. Apache Kudu는 단순한 CRUD만 제공하기 때문에 복잡한 질의를 실행하기 위한 별도의 질의 처리기가 필요하다.

2-3. Apache Impala

Apache Impala는 HDFS를 위해 Apache 소프트웨어 재단에서 개발한 분산 병렬 질의 처리 엔진이다. Apache Impala는 스토리지에 저장되어 있는 데이터를 SQL을 통해 실시간으로 분석하는 시스템으로 스토리지 엔진이 제공하지 않는 연산을 실행한다.[4] Apache Impala는 MapReduce를 이용하지 않는 분산 질의 엔진을 통해 SQL을 실행하여 낮은 지연시간으로 결과를 제공한다. [그림 3]은 Apache



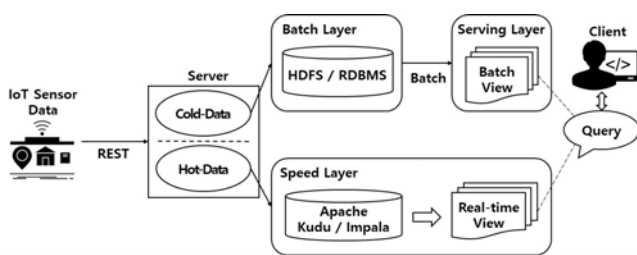
[그림 3] Apache Impala의 구성

Impala의 구조를 나타낸다.

Apache Impala는 Daemon, Catalog Service, Statestore로 구성된다. Daemon은 데이터 노드에서 실행되는 프로세스로 사용자의 요청을 수용하고, Coordinator와 Executor 역할을 한다. Catalog Service는 메타데이터의 동기화를 위한 프록시 역할을 하며 Daemon에서 직접 메타데이터를 변경하면 자동으로 동기화된다. Statestore는 Daemon의 상태를 확인하고 메타데이터를 동기화한다.

3. 제안하는 Lambda Architecture 설계

제안하는 Architecture는 기존의 HDFS 기반 IoT 센서 데이터 수집 분석 환경을 Apache Kudu와 Impala를 활용해 Lambda Architecture로 구성한다. 제안하는 Apache Kudu와 Impala를 활용한 Lambda Architecture는 발생하는 데이터를 자주 사용되지 않고 갱신이 적은 대용량의 Cold-Data와 자주 사용되고 갱신주기가 짧고 크기가 작은 실시간 Hot-Data로 분류한다. 데이터가 크기에 따라 분류되어 각 성격에 맞는 스토리지에 저장됨으로써 HDFS의 Small File 문제를 해결할 수 있다. Speed Layer에서는 Real-time View를 끊임없이 생성해 Batch가 실행될 때 발생하는 공백 문제를 해결할 수 있다. [그림 4]는 제안하는 Apache Kudu와 Impala를 활용한 Lambda Architecture의 구성을 나타낸다.



[그림 4] 제안하는 Lambda Architecture의 구성

제안하는 Architecture는 IoT 센서 데이터를 Rest 통신으로 서버에 전송하며, 서버는 이를 Cold-Data와 Hot-Data로 분류한다. Cold-Data는 HDFS에 저장되고, HDFS는 Batch를 통해 주기적으로 Batch View를 생성한다. Hot-Data는 Apache Kudu에 저장되는 동시에 누락된 데이터를 삭제하거나 갱신하여 데이터의 무결성을 보장하며 Impala를 통해 Real-time View를 생성한다. 클라이언트는 SQL 질의를 통해 Batch View와 Real-time View의 JOIN 결과를 제공받는다.

4. 결론

본 논문에서 제안하는 Apache Kudu와 Impala를 활용한 Lambda Architecture는 Batch View와 Apache Kudu와 Impala로 생성된 Real-time View를 통해 클라이언트가 결과까지 접근하는 시간을 단축하며, Hadoop 기반 데이터 수집 분석 환경에서 발생하는 Small File로 인한 네임노드의 과부하 문제를 해결할 수 있다. 향후 본 논문에서 제안하는 Apache Kudu와 Impala를 활용한 Lambda Architecture의 구축이 필요하며, Cold-Data와 Hot-Data를 운영환경에 맞춰 자동으로 분류하는 알고리즘의 연구가 필요하다.

Acknowledgement

이 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.IITP-2019-0-00135, ICT 기반 환경 모니터링 센서 신뢰성 검증 및 평가 플랫폼)

참고문헌

- [1] Bende, Sachin, and Rajashree Shedge. "Dealing with small files problem in hadoop distributed file system." *Procedia Computer Science* 79 pp. 1001-1012, 2016.
- [2] KIRAN, Mariam, et al. Lambda architecture for cost-effective batch and speed big data processing. In: 2015 IEEE International Conference on Big Data (Big Data). IEEE, p. 2785-2792, 2015.
- [3] Lipcon, Todd, et al. "Kudu: Storage for fast analytics on fast data." Cloudera, inc 28, 2015.
- [4] KORNACKER, Marcel; ERICKSON, Justin. Cloudera impala: Real time queries in apache hadoop, for real. Ht Tpblog Cloudera Combog201210cloudera-Impala-Real-Time-Queries --Apache-Hadoop--Real, 2012.

대용량 스토리지 기반의 데이터 전송 노드 클러스터 설계 및 구축

홍원택*, 안도식**, 이재국**

*한국과학기술정보연구원 과학기술연구망센터

**한국과학기술정보연구원 슈퍼컴퓨팅인프라센터

{wthong, dsan, jklee}@kisti.re.kr

Designing and building a DTN cluster based on massively scalable storage

Wontaek Hong*, Dosik An**, Jaekook Lee**

*Advanced Kreonet Center, KISTI

**Supercomputing Infrastructure Center, KISTI

요 약

과학응용분야의 원활한 협업 지원을 위해서는 원거리간 대용량 연구데이터의 고속 전송이 반드시 요구된다. 이와 관련하여, 본 논문은 기 구축된 대용량 파일 시스템을 다수의 데이터 전송 노드(DTN)에 연동하기 위해 필요한 요구사항들을 정리하고, 이에 기반하여 DTN 클러스터를 설계하고 구축한 사례를 제시한다. 추가적으로, 종단간 왕복지연 시간이 약 130ms에 달하는 원거리 종단 포인트와 대용량 실험데이터를 송수신함으로써 구축된 결과물의 전송 성능을 측정하고 확인한다.

1. 서론

대용량 데이터의 고속 전송이 요구되는 과학응용 분야를 위한 특화된 네트워크를 제공하기 위해 제안된 미국 에너지과학연구망(ESnet)의 Science DMZ 개념은 최근 천문학, 기상기후 분야 등의 대용량 데이터 전송이 필요한 국내외 연구망 커뮤니티에서 활발히 적용되어 오고 있다. [1][2] 이러한 Science DMZ 개념을 실현화하기 위해서는 일반 망과는 차별화된 고품질의 고성능 네트워크 경로 확보, 전용의 데이터 전송 노드(DTN) 및 전송 상태를 모니터링할 수 있는 시스템 등이 요구된다. 특히, 핵심 요소인 DTN을 적용하기 위해서는 RAID 컨트롤러를 기반의 내부 스토리지 연계 또는 확장성이 우수한 외부 스토리지 연계 모델의 구현이 필요하다. [3] 이와 관련하여 본 논문에서는 고성능 컴퓨팅(HPC) 환경과 같이 대용량 데이터 전송이 요구되는 분야에서 Science DMZ 구축 모델에 기반하여 기 구축된 병렬 파일 시스템을 연계할 수 있는 DTN 클러스터를 설계하고 구축한다.

2. 본론

대용량 스토리지들을 Science DMZ 환경에 적용하기 위해 고속 마운트 기반의 외부 스토리지 연계

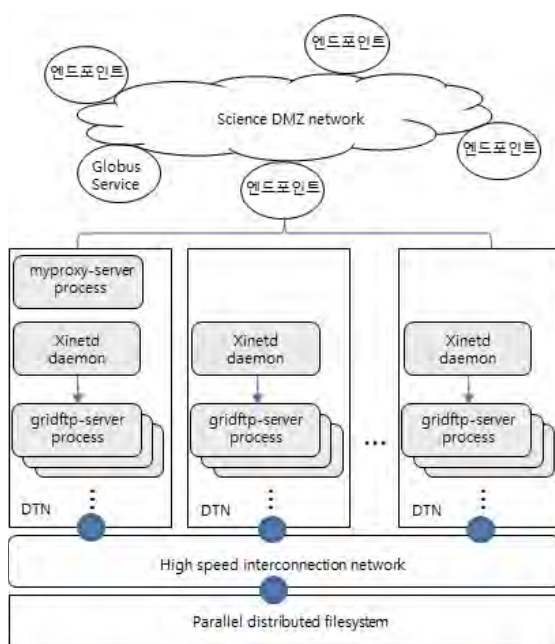
모델에 기초하여 DTN 클러스터를 구축한다. 이러한 접근 방법은 기 구축된 병렬 파일시스템을 다수의 DTN 서버에 마운트하여 확장성을 높일 수 있다. HPC 환경에서 계산 노드들과 스토리지 시스템들을 연결해 주는 인터커넥션 네트워크 기술이 DTN과 외부 파일시스템을 연동하기 위해 동일하게 적용될 수 있다. 특히, DTN 기반의 고속 마운트를 위해 병렬 파일시스템의 서버/클라이언트 모듈의 튜닝이 필요하고, 이러한 과정은 외부 스토리지에 적용된 파일시스템 프로토콜에 의존하여 서버/클라이언트 간의 성능 최적화 과정이 요구된다.

DTN을 하드웨어적으로 구성하는 측면에서 개별 DTN 시스템은 제한된 기능만을 수용할 수 있도록 최대한 단순하게 구성하는 것이 중요하다. 특히, 고속 마운트 기반의 파일시스템 연계를 위해서는 외부 망 트래픽을 위한 단일 네트워크 인터페이스와 파일 시스템으로 향하는 단일 네트워크 인터페이스로 분리하여 DTN을 구성해야 하고, 이러한 인터페이스들은 Ethernet, InfiniBand, Intel Omni-Path와 같은 인터커넥션 네트워크에 연결되어야 한다. 또한, DTN 하드웨어 성능 최적화와 더불어 원거리 전송에 적합한 TCP 알고리즘의 선택, 소켓버퍼 크기, 점보 프레임 지원을 위한 MTU 크기 세팅 등을 포함한 DTN 운영체제 및 전송 프로토콜에 대한 소프트

웨어 최적화가 선행되어야 한다.

병렬 파일시스템 내의 다수의 대용량 파일들을 Science DMZ 환경에서 고속으로 전송하기 위해서는 DTN 서버들 또한 확장 가능한 병행성(Concurrency)와 병렬성(Parallelism)을 지원해야 한다. 병행성은 전송하고자 하는 DTN 서버의 수 및 CPU 코어 수의 증가를 의미하고, 이러한 증가된 자원들은 각각의 전송 프로토콜 프로세스에 매핑되어 전송 성능을 향상시킬 수 있다. 또한, 하나의 파일을 전송하는데 있어서 다수의 TCP 스트림들로 나누어 전송할 수 있는 병렬성을 지원함으로써 전송 효율을 향상시킬 수 있다. 이러한 병행성과 병렬성은 전송하고자 하는 파일의 크기, 파일의 수 등의 전송 환경에 따라 최적 값이 변할 수 있음을 추가적으로 고려해야 한다.

DTN 클러스터가 연결된 외부 전송망은 네트워크 패스 프로비저닝 등을 통해 병목이 없는 전용 경로를 확보한다. 또한, DTN 서버에 설정된 점보프레임 지원을 위한 MTU 설정과 더불어 상대방 DTN 서버들 또한 동일한 MTU 크기의 설정이 필요하다. 이러한 MTU 크기의 세팅은 DTN 네트워크 인터페이스 뿐만 아니라, 종단 목적지까지의 모든 경로 상에 있는 네트워크 장비 상의 In/Outbound에 대해 동일하게 설정해야 한다. 추가적으로 더 엄격한 망 분리를 고려하는 경우에는 데이터 전송 프로토콜의 제어 채널을 위한 제어 망과 데이터 채널을 위한 전송망을 분리한다.



(그림 1) DTN 클러스터 구축

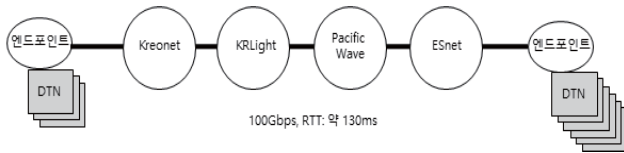
그림 1은 위에서 언급된 요구사항들을 반영하여 병렬 파일시스템 내의 파일들을 고속 전송하기 위해 Globus Connect Server(GCS) 소프트웨어 [4]를 활용하여 다수의 DTN 서버들을 클러스터링한 구축 환경을 보여준다. GCS에서는 DTN과 같은 다수의 I/O 노드들을 하나의 종단 포인트로 표현할 수 있는 메커니즘을 제공하고, 이러한 메커니즘에 기반하여 원격 전송에 적합하게 하드웨어, 소프트웨어들이 성능 튜닝된 다수의 DTN 서버들을 대상으로 클러스터링화 한다.

다수의 파일들을 동시에 전송하기 위해서는 Xinetd 데몬에서 fork된 gridftp-server 프로세스들이 각각의 파일들을 전송하기 위해 생성되어 전송에 참여한다. 이렇게 생성된 각각의 gridftp-server 프로세스들은 DTN에서 제공하는 다수의 CPU 코어들로 매핑되어 병행성을 증가시킨다. 추가적으로 각각의 gridftp-server 프로세스들은 하나의 파일을 전송하는데 있어서, 다수의 TCP 스트림들을 생성하여 병렬성을 높이게 된다. 예를 들어, L개의 DTN 서버에서 M개의 CPU 코어를 갖고, 각 전송 프로세스당 N개의 TCP 스트림들을 생성한다면 산술적으로 최대 $L \times M \times N$ 개의 TCP 스트림을 생성할 수 있게 된다. 이렇게 병렬 파일시스템을 고속 마운트하는 DTN 클러스터를 바탕으로 설정된 단일의 종단 포인트는 Globus 전송 기반의 협업에 참여하고자 하는 다른 종단 포인트들과 상호 검색 및 고속 전송이 가능하다.

그림 1에서와 같이 슈퍼컴퓨터 5호기 누리온의 약 20PB 용량의 Lustre 파일시스템을 연계하기 위해 3 대의 고성능 DTN 서버를 활용하여 DTN 클러스터를 구축하였다. 각 DTN 서버는 2*Intel Xeon Gold 3.5GHz 8 코어 CPU, 12*32GB 메인메모리, 1.92TB SSD 디스크, 100Gbps Ethernet NIC, 100Gbps 인터커넥션 NIC 등으로 구성된다. 추가적으로 각 DTN에는 CentOS v7.5.1804, Globus connect server v4, Lustre client v2.10.7이 설치되어 적용된다.

그림 2는 Lustre 파일시스템을 기반으로 구축된 DTN 클러스터의 전송 성능을 측정하기 위한 실험 환경을 보여준다. DTN 클러스터는 다수의 대용량 파일들에 대해 병행성과 병렬성을 극대화하기 위한 접근 방법이므로, 실험 환경의 구성 시에도 이러한 점을 충분히 고려해야 한다. 즉, 구축된 DTN 클러스터의 종단 포인트와 더불어 전송에 참여하는 상대

편 종단 포인트도 DTN 클러스터로 구성되어야 자원들을 충분히 활용할 수 있다. 이러한 맥락에서 미국 에너지성 슈퍼컴센터(NERSC)의 Cori 파일시스템과 연동되어 있는 DTN 클러스터 종단 포인트와의 전송 테스트를 수행한다.



(그림 2) 전송 실험 환경

NERSC DTN 종단 포인트는 6대의 DTN 서버들로 구성되어 있고, 그림 2에서처럼 두 종단 포인트들 간의 네트워크 경로는 한국의 국가과학기술연구망(KREONET), ESnet 등을 통해 제공되고, RTT가 약 130ms, 종단간 대역폭은 100Gbps으로 제공된다. 이러한 환경에서 종단간 Disk-to-Disk 전송 테스트를 위해 ESnet Read-Only DTN에서 제공하는 약 250GB의 데이터 set들을 대상으로 송수신 실험을 진행한다. 표 1은 실험에 이용되는 데이터 set에 대한 세부 정보를 보여준다.

<표 1> 전송 파일 정보

종류	크기	구성
Climate-Small	246GB	29MB에서 425MB의 크기로 분포된 1,496개의 파일들로 구성
Climate-Large	244GB	10개의 21.5GB의 파일과 1개의 28.8GB 파일로 구성

약 250GB 크기의 Climate-{Small, Large} 데이터 set을 대상으로 송수신 실험을 한 결과, Climate-Small 데이터 set의 경우 송수신시 각각 14.4Gbps, 25.76Gbps의 전송 성능을 기록하였고, Climate-Large 데이터 set의 경우 각각 22.48Gbps, 36.08Gbps의 전송 성능을 기록하였다.

3. 결론

본 논문에서는 병렬 파일시스템의 대용량 데이터를 효율적으로 전송하기 위해 Globus 기반의 DTN 클러스터를 설계하고 구축하였다. 또한, 한미간 원거리 전송 환경에서 실험 데이터를 송수신함으로써 DTN 클러스터링에 따른 전송 성능을 측정하였다. 향후, DTN 클러스터링의 효과를 면밀히 확인하기

위해 전송 규모, 파일의 크기 등 다양한 전송 환경을 고려한 성능 분석에 대한 연구가 필요하다.

ACKNOWLEDGMENT

본 연구는 2020년도 한국과학기술정보연구원(KISTI) 주요사업 과제로 수행한 것입니다.

참고문헌

- [1] J. Crichigno, E. Bou-Harb, and N. Ghani, "A Comprehensive Tutorial on Science DMZ", IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 2041-2078, 2019.
- [2] Z. Liu et al., "A Comprehensive Study of Wide Area Data Movement at a Scientific Computing Facility", IEEE International Conference on Distributed Computing Systems, Vienna, Austria, Jul. 2018.
- [3] E. Dart et al., "The Science DMZ: A Network Design Pattern for Data-Intensive Science", SC'13 Proceedings of the International Conference on High Performance Computing, Networking, Storage and Analysis, Denver, USA, Nov. 2013.
- [4] Globus Connect Server, <https://docs.globus.org/globus-connect-server-installation-guide/>.

비콘과 홍채인식 기반의 의료진 신분확인 시스템 제안

임세진*, 권혁동**, 서화정**

*한성대학교 컴퓨터공학부

**한성대학교 IT융합공학부

tpwls834@naver.com, korlethean@gamil.com, hwajeong84@gmail.com

A Proposal of Beacon and Iris Recognition Based Medical Identification System

Se-Jin Lim*, Hyeok-Dong Kwon**, Hwa-Jeong Seo**

*Dept. of Computer Engineering, Han-sung University

**Dept. of IT Convergence Engineering, Han-sung University

요 약

최근 대리수술 (무면허의료행위)과 같이 환자의 안전을 위협하는 사건들이 언론에 보도되고 있다. 대리수술 방지를 위한 수술실 감시카메라 장치 도입 등의 대안이 등장하고 있지만, 의료계의 거센 반발로 인해 시행되기에는 현실적인 어려움이 있다. 하지만 대리 수술과 같은 사건이 빈번히 발생함에 따라 의사에 대한 사회적 신뢰도가 추락하고 있다. 본 논문에서는 근거리 무선 통신 장치인 비콘(Beacon)과 생체인식 중 안전하고 신뢰할 수 있는 홍채인식을 결합한 의료진 신분 확인 시스템을 제안한다. 이 시스템은 홍채인식을 통해 사용자 인증을 수행함으로써 1차적인 신분확인을 하고 비콘을 통해 의료진이 수술실에 있다는 것을 증명한다. 또한 무작위 주기로 홍채인증을 수행하여 의료진이 초기 인증만 수행하고 수술실을 떠나는 경우를 방지함으로써 집도의에 대한 환자의 신뢰를 보장한다.

할 수 있을 것이다.

1. 서론

최근 의료계에서는 <표 1>과 같이 의사면허를 가지지 않은 자가 불법적으로 수술이나 시술을 진행하는 등 환자의 안전이 보장받지 못하는 사건이 빈번히 발생하고 있다.

<표 1> 3년간 의료인 행정처분(무면허 의료행위) 현황[1]

구분	2015	2016	2017	총계
	자격정지	자격정지	자격정지	
의사	41	13	19	73
치과의사	8	5	6	19
한의사	17	26	11	54
간호사	10	3	6	19
계	76	47	42	165

대리수술 방지를 위해 수술실 CCTV 설치 및 운영 의무화에 대한 법제화가 요구되었지만 의료계의 거센 반발로 인해 시행되기에는 현실적인 어려움이 있다. 본 논문에서는 CCTV 없이도 대리수술이 아님을 증명할 수 있는 의료진 신분확인 시스템을 제안하고자 한다. 홍채인식을 통해 의료진의 신분확인을, 비콘(Beacon)을 통해 의료진이 수술실에 있다는 것을 증명한다. 본 시스템은 대리수술 감소에 기여

2. 관련 연구

2.1 비콘(Beacon)

비콘은 페어링과 같은 별도의 과정 없이 근거리 내에 있는 블루투스가 활성화된 스마트 기기를 자동으로 인식하여 통신할 수 있는 무선 통신 장치이다[4]. 주파수를 활용하여 단말기 정보를 전송하며, 최대 50m 거리를 인식할 수 있고 측위 오차 5cm 이내라는 특성이 있어 특정 장소의 세부적인 위치 정보를 얻기에 적합하다[3]. NFC 기술과 비교했을 때 비콘은 직접 모바일 기기를 태그하지 않아도 되고 좀 더 먼 거리에서 자동 감지할 수 있다는 장점이 있다.

2.2 홍채인식

생체인식에는 지문인식, 홍채인식, 얼굴인식 등 다양한 종류가 있다. 본 시스템에서 지문인식을 적용할 경우, 의사가 수술실에서 사용자 인증을 위해 지문인식을 할 때 세균감염이 초래될 수 있으므로 적합하지 않다. 또한 얼굴인식의 경우도 수술 마스크와 모자 등 수술 복장을 갖춘 상태에서는 오류율이 높기 때문에 적합하지 않다. 따라서 본 시스템에

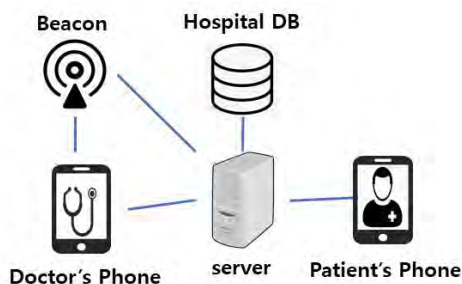
서는 접촉이 필요 없고 오류율이 낮은 홍채인식을 활용한다.

3. 시스템 구조

본 시스템은 의료진과 환자에게 모바일 애플리케이션으로 제공된다. 본 시스템의 구조를 크게 시스템 설계 구조와 시스템 동작 시나리오로 나누어 설명하고자 한다.

3.1 시스템 설계 구조

<그림 1> 전체 시스템 구조



본 시스템은 <그림 1>의 구조를 가진다.

환자정보와 수술실정보, 의사정보와 같이 병원에서 관리하는 정보는 서버가 병원DB를 통해 알아낸다.

비콘은 UUID(Universally Unique Identifier), Major ID, Minor ID와 같은 세 종류의 식별자를 가진다. UUID 안에 수술실 정보와 정해진 시간마다 일정 규칙에 따라 변하는 수를 넣어 브로드캐스트한다. UUID 값을 유추할 수 없게하여 고정 UUID 값을 사용했을 때 발생 가능한 부정 인증을 방지한다[3]. 비콘 신호의 세기는 수술실의 크기에 맞게 조절하여 다른 수술실의 비콘 신호에 대한 간섭이 없도록 한다. 동작 시에는 의료진과 환자 측의 애플리케이션이 서버와 통신하며 진행된다.

3.2 시스템 동작 시나리오

의료진은 <그림 2>의 흐름도[2]와 같이 애플리케이션 가입 시 개인정보를 입력한다. 서버를 통해 입력한 정보가 병원 DB와 일치하는지를 확인한다. 일치하면 홍채정보를 받아 서버에 의사정보와 함께 저장한다. 이때 홍채정보는 가입 시에만 등록할 수 있으며 가입 후에는 수정이 불가능하도록 한다. 이는

추후 대리인의 홍채정보로 수정하는 경우를 방지하기 위함이다. 일치하지 않으면 가입이 종료된다.

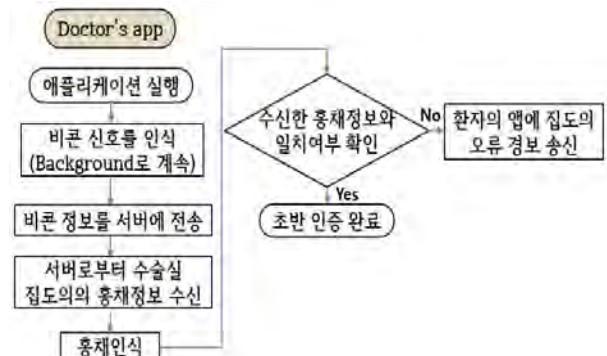
환자 측의 경우 가입 없이 환자와 집도의의 이름을 입력하면 집도의의 일치여부를 확인할 수 있는 권한으로 로그인된다. 만약 집도의가 일치하지 않는다면 환자에게 알림이 간다.

<그림 2> 의료진 가입 흐름도



본 시스템이 수술 시에 동작하는 시나리오[2]에 대해 설명하겠다. <그림 3>처럼 의료진은 수술실에 들어가 애플리케이션을 실행한다. 실행시점에서 블루투스 기능이 활성화되어있지 않으면 자동으로 활성화되도록 한다. 수술실의 비콘 신호를 인식하여 서버에게 전송한다. 서버는 비콘의 UUID를 통해 수술실의 위치를 확인하고 병원DB를 통해 해당 수술실에 수술이 예정되어있는 집도의의 정보를 얻는다[3]. 해당하는 집도의의 홍채정보를 서버에서 찾아 앱에 전송한다. 담당 의료진이 홍채를 인식하여 사용자 인증이 되면 초반 인증이 완료되고 수술이 시작된다. 홍채 인식은 최대 3회 시도할 수 있다.

<그림 3> 의료진 앱 기준, 수술 시 동작 시나리오



수술실에서 초기 인증이 완료된 후에도 동작은 끝난 것이 아니다. 이후의 부정인증을 방지해야한다. 모바일 기기가 수술실에서 벗어나게 되면 비콘 신호를 인식하지 못하게 되어 환자의 애플리케이션으로 오류 경보가 송신된다. 또한 초기 인증만 마치고 대리인으로 교체하는 경우가 있을 수 있다. 이를 방지하기 위해서 환자의 수술을 진행하는 동안 무작위 주기로 3회 이내의 홍채인증을 진행한다. 홍채인증이 진행되지 않으면 해당 집도의가 수술실에 존재하지 않는 것으로 판단해 환자의 애플리케이션으로 경보알림이 간다.

4. 결론

본 논문에서는 비콘과 홍채인식 기술을 기반으로 한 의료진 신분확인 시스템을 제안하였다. CCTV를 운영하기 어려운 현 상황의 대안으로 고안해 낸 방법이다. 하지만 본 시스템에는 수술실에 대리인과 의료진이 같이 있는 상태에서 대리수술을 진행할 경우에는 판별할 수 없다는 한계점이 존재한다. 본 논문의 시스템에 대한 추가적인 연구가 필요하다.

참고문헌

- [1] MEDI:GATE NEWS [Internet]. Available: <https://www.medigatenews.com/news/1896439862>
- [2] H.I.Hwang, S.W.Seo, W.Y.Kim, H.G.Lim, Y.S.Park, M.H.Lee, C.Y.Keum, H.G.Je, and I.K.Kim “Healthcare Professional Identification Process using Fingerprint” Korea Information Science Society, pp 251-253, Dec, 2018.
- [3] J.H.Lee, G.H.Chae, G.Y.Lim, J.H.Seol, S.M.Choi, and S.U.Lim “Attendance Check System combining Beacons and Biometrics” Korean Institute of Next Generation Computing, Vol. 14, No. 2, pp 24-32, April, 2018.
- [4] K.N.Kang, C.W.Kim, G.J.Bang, Y.J.Oh, L.Kwon, and E.C.Park “Smart Attendance Management, Indoor Positioning and Prepayment System using Beacon” Korea Information Science Society, pp 1650-1652, Dec, 2018.

무선 센서 네트워크에서 장애 검출을 위한 결합 주성분분석과 적응형 임계값

Thien-Binh Dang*, Vi Van Vo*, Duc-Tai Le*, Moonseong Kim**, Hyunseung Choo*

*성균관대학교 전자전기컴퓨터공학과

**서울신학대학교 교양학부

e-mail: {dtbinh, ldati, choo}@skku.edu

moonseong@stu.ac.kr

Joint PCA and Adaptive Threshold for Fault Detection in Wireless Sensor Networks

Thien-Binh Dang*, Vi Van Vo*, Duc-Tai Le*, Moonseong Kim**, Hyunseung Choo*

* Dept. of Electrical and Computer Engineering, Sungkyunkwan University

**Dept. of Liberal Arts, Seoul Theological University

Abstract

Principal Component Analysis (PCA) is an effective data analysis technique which is commonly used for fault detection on collected data of Wireless Sensor Networks (WSN). However, applying PCA on the whole data make the detection performance low. In this paper, we propose Joint PCA and Adaptive Threshold for Fault Detection (JPATAD). Experimental results on a real dataset show a remarkably higher performance of JPATAD comparing to conventional PCA model in detection of noise which is a popular fault in collected data of sensors.

1. Introduction

In Wireless Sensor Networks (WSN), the limitation on size and cost of a sensor make it a weak device, such as low computational speed, small memory, limited energy and restricted communication bandwidth [1]. Thus, the WSN are highly vulnerable to random faults and cyber-attacks. The faulty data collected from sensors can leads data analysts to improper decisions. To ensure accuracy and reliability of the sensory data, an efficient fault detection algorithm needs to be developed. Principal Component Analysis (PCA) is an important method to analyze multivariate data obtained from WSN. It was used in many existing works to detect faulty data such as [1], [2]. However, the conventional PCA is not sensitive enough to recognize small faults whose data has small differences to the normal data. In this paper, we propose Joint PCA and Adaptive Threshold for Anomaly Detection (JPATAD) which focuses on improving the sensitiveness of conventional PCA by splitting data into small segments.

2. Joint PCA and Adaptive Threshold for Anomaly Detection

The key idea is that the data is split into smaller segments and the detection threshold adapt to the variation of data from segment to segment. The proposed scheme has two phases: training phase and testing phase. In training phase, considering the data matrix $\mathbf{X} = \{\mathbf{x}^1, \mathbf{x}^2, \dots, \mathbf{x}^M\}$ where column i contains N data samples $\mathbf{x}^i = \{x_0^i, x_1^i, \dots, x_{N-1}^i\}$ of sensor i collected from normal operation, M is the number of sensors. Then the data \mathbf{X} is split into $\frac{N}{S}$ segments where S is the length of a segment (or the number of samples of a segment). Then, PCA is applied on these segments independently to compute Square Prediction Error (SPE) threshold. In testing phase, the incoming data s is first identified the segment it resides in by its collected time and the interval of $\frac{N}{S}$ segments which are established in training phase. PCA is then applied on s to calculate its SPE value. The data s is normal if its SPE value is less or equal to the SPE threshold of identified segment, otherwise s is detected as faulty data.

The advantage of PCA is that it can capture the

correlation of by projecting sensors' data into a lower dimension space which still preserves maximum variance of the original data in minimum number of dimensions. In order to apply PCA, the data matrix is normalized to zero-mean and scaled to unit variance. Let \mathbf{Y}_s is the normalized data of a, \mathbf{Y}_s can be expressed as:

$$\mathbf{Y}_s = (\mathbf{Y} - \bar{\mathbf{Y}})D^{-\frac{1}{2}}$$

where $\bar{\mathbf{Y}} = \frac{1}{N}(\mathbf{1}^T \mathbf{X})$ and $D = \frac{1}{N-1}[(\mathbf{X} - \bar{\mathbf{X}})^T(\mathbf{X} - \bar{\mathbf{X}})] \circ I_M$ where \circ denoting the Hadamard multiplication and I_M is the identity matrix. Then, the covariance matrix \mathbf{R} of matrix \mathbf{Y}_s is constructed by $\mathbf{R} = \mathbf{Y}_s^T \mathbf{Y}_s$ where \mathbf{Y}_s^T is the transpose matrix of matrix \mathbf{Y}_s . In next step, Singular Value Decomposition (SVD) is performed on \mathbf{R} as $\mathbf{R} = \mathbf{V} \mathbf{\Lambda} \mathbf{V}^T$ where $\mathbf{\Lambda}$ is the diagonal matrix containing M eigenvalues of matrix \mathbf{R} in descending order ($\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_M \geq 0$) and matrix \mathbf{V} is the collection of M eigenvectors of \mathbf{R} . SPEs of data samples are calculated for fault detection based on the loading matrix $\hat{\mathbf{P}}$ which is formed by l smallest eigenvectors. SPE statistics can be calculated by the following equation: $SPE = \|(\mathbf{I} - \hat{\mathbf{P}}\hat{\mathbf{P}}^T)\mathbf{Y}_s\|$. The data is considered normal if its $SPE \leq \delta^2$, where δ^2 is expressed as follows:

$$\delta^2 = \theta_1 \left[\frac{C_\alpha \sqrt{2\theta_2 h_0^2}}{\theta_1} + 1 + \frac{\theta_2 h_0 (h_0 - 1)}{\theta_1^2} \right]^{\frac{1}{h_0}}$$

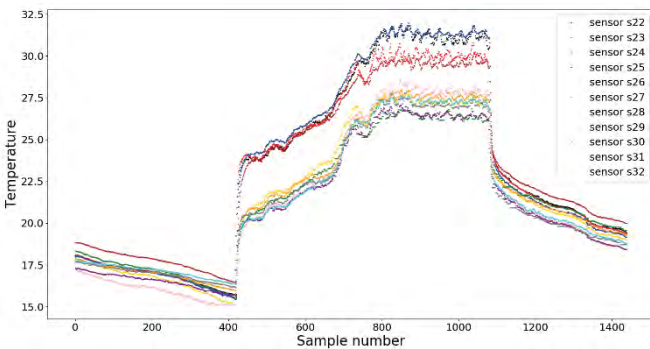
$$h_0 = \frac{2\theta_1 \theta_3}{\theta_2^2},$$

$$\theta_i = \sum_{j=l+1}^L \lambda_j^i,$$

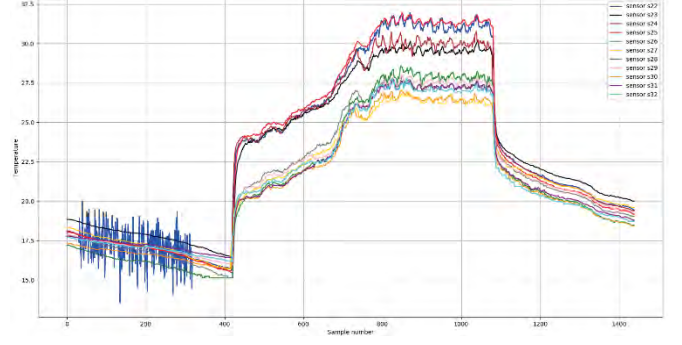
where λ_j is the eigenvalue associated with j_{th} the eigenvector, C_α is the standard normal deviation corresponding to the confident level of standard normal distribution.

3. Performance Evaluation

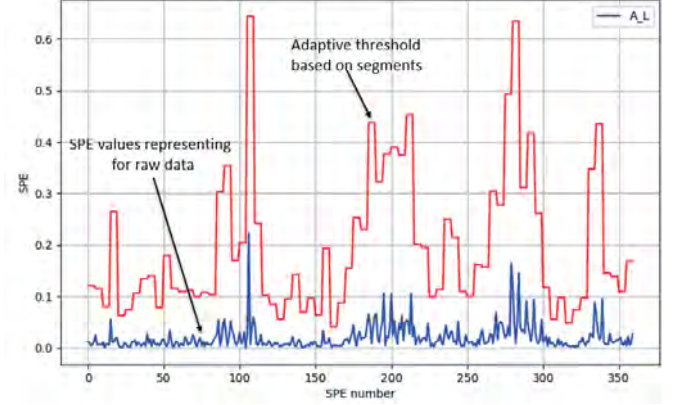
In this research, a real WSN from Intel Berkeley Research lab (IBRL) is used for evaluating the



(Figure 1) Training data



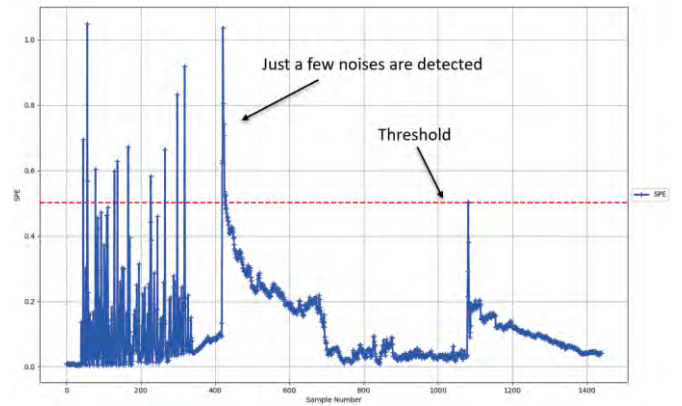
(Figure 2) Training data



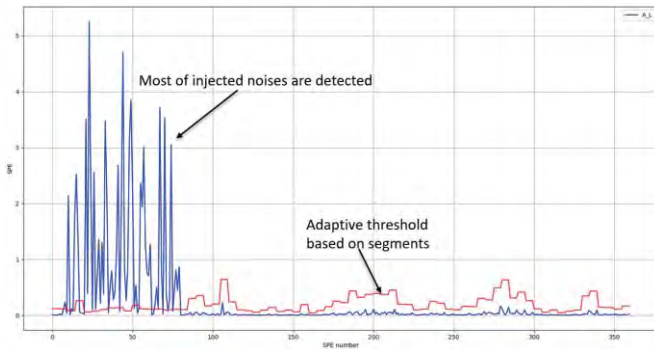
(Figure 3) Noise in sensor 22

efficiency of JPATAD. Without loss of generality, we only choose temperature measurements from eleven sensors whose IDs are 22, 23, ..., 32 for experiment. In our experiment, temperature readings from these eleven sensors are re-sampled every minute so a total of 1440 samples are taken in one day. We use 1400 samples of March 1st for training (Figure 1), the segment length S is set to 20 samples and we consider this training data is normal. The adaptive threshold of the training data is shown in Figure 2.

For testing, we inject noise into this normal data (i.e. an example of injected noise is shown in Figure 3) and comparing the performance of conventional PCA and JPATAD.



(Figure 4) Detection result of conventional PCA with noise



(Figure 5) Detection result of JPATAD with noise

The experiment results in the Figure 4 and 5 shown that the conventional PCA cannot detect well the injected noise but the noise is shown clearly in JPATAD depicted by the number of SPE points higher than the SPE threshold (the red dot line).

4. Conclusion

In this work, we proposed Joint PCA and Adaptive Threshold in WSN. The experiment results show that the JPATAD outperforms the conventional PCA in detection noise.

ACKNOWLEDGEMENT

본 논문은 과학기술정보통신부 및 정보통신 기술평가원의 Grand ICT연구센터지원사업 (IITP-2020-2015-0-00742), 정보통신기술진흥센터 (No.2015-0-00567, 유무선 통합 네트워크에서 접속 방식에 독립적인 차세대 네트워킹 기술 개발), 과학기술 정보통신부 및 정보통신기술평가원의 글로벌핵심인재 양성지원사업 (2019-0-01579)의 연구결과로 수행되었음.

References

- [1] D. W Carman, P. S Kruus, and B. Matt, "Constraints and approaches for distributed sensor network security (final)," 10 2000.
- [2] M. Livani and M. Abadi, "Distributed pca-based anomaly detection in wireless sensor networks," in Internet Technology and Secured Transactions (ICITST), 2010 International Conference.
- [3] X. L. Zhang, F. Zhang, J. Yuan, J. lan Weng, and W. h. Zhang, "Sensor fault diagnosis and location for small and medium-scale wireless sensor networks," in 2010 Sixth International Conference on Natural Computation.

클라우드 환경에서 오토 스케일링이 가능한 센서 데이터 수집 시스템 설계

박수용*, 최수민*, 신용태**

*승실대학교 컴퓨터학과

**승실대학교 컴퓨터공학부

tndyd5390@naver.com

A Study on Tools for Agent System Development

Soo-Yong Park*, Su-Min Choi*, Yong-Tae Shin**

*Dept of Computer Science, Soongsil University

요 약

센서 네트워크의 센서 개수가 늘어나고 데이터 수집 주기가 짧아지며 데이터의 용량도 늘어남에 따라 데이터를 수집하는 중앙서버의 과부하가 걸리는 현상이 발생할 수 있다. 본 논문에서 제안하는 시스템은 센서 데이터를 수집하는 모듈을 컨테이너화 하여 쿠버네티스로 관리한다. 또한 쿠버네티스의 오토 스케일링 기능을 이용하여 데이터 수집 모듈의 과부하가 발생할 경우 자동으로 수집 모듈을 복사하여 scale out 할 수 있다.

1. 서론

센서 네트워크는 특정 지역에 분산하여 배치된 센서로부터 데이터를 수집하는 네트워크를 의미한다. 센서 네트워크는 환경 모니터링, 보안 및 감시, 스마트 홈, 스마트 그리드 등의 다양한 분야에서 사용되고 있다. 센서 네트워크는 센서가 수집한 데이터를 게이트웨이를 통하여 중앙의 서버로 전송하는 방식을 사용하고 있다. 센서 네트워크를 사용하는 분야가 다양해지고 측정하고자 하는 지역이 넓어짐에 따라 센서의 수가 늘어났다. 따라서 중앙 서버로 전송되는 트래픽과 데이터의 양이 증가하고 중앙 서버에 과부하가 걸리는 현상이 발생하게 된다[1].

제안하는 시스템은 클라우드 환경에서 다수의 서버를 이용하여 클러스터링을 수행한다. 각각의 서버에는 도커를 이용하여 데이터 수집 시스템을 구축하고 센서로부터 전송되는 트래픽과 데이터의 양을 지속적으로 모니터링한다. 센서 네트워크에서의 어떠한 이벤트로 인해 트래픽 또는 데이터의 양이 증가하여 도커의 자원이 부족해지면 클러스터에서 동일한 도커를 하나 더 생성하여 부하를 분산시킬 수 있다.

본 논문의 구성은 다음과 같다. 2장 관련 연구에서는 시스템 설계에 필요한 기반 기술인 도커와 쿠

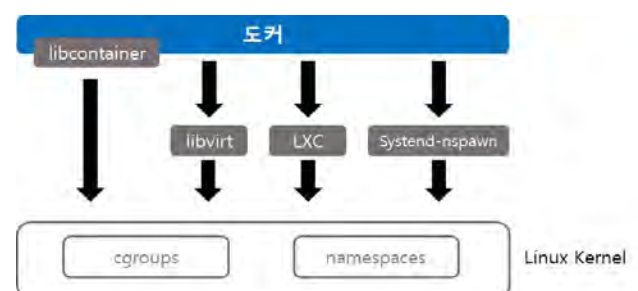
버네티스에 대해 연구한다. 3장 시스템 설계에서는 관련 연구를 기반으로 시스템을 설계한다. 4장 결론에서는 설계된 시스템에 기초하여 결론을 제시한다.

2. 관련 연구

본 장에서는 클라우드 환경에서 오토스케일링이 가능한 센서 데이터 수집 시스템 설계에 필요한 기반 기술인 도커와 쿠버네티스에 대해 연구한다.

2.1. 도커

도커는 클라우드 환경에서 애플리케이션을 처리할 수 있는 컨테이너 플랫폼을 의미한다. 도커는 운영체제에서 namespace와 cgroup 기능을 이용하여 프로세스에서 사용하는 자원을 분리하여 컨테이너라는 공간에 할당한다[2]. (그림 1)은 도커에서 사용하는 자원 분리 방식을 나타낸다.

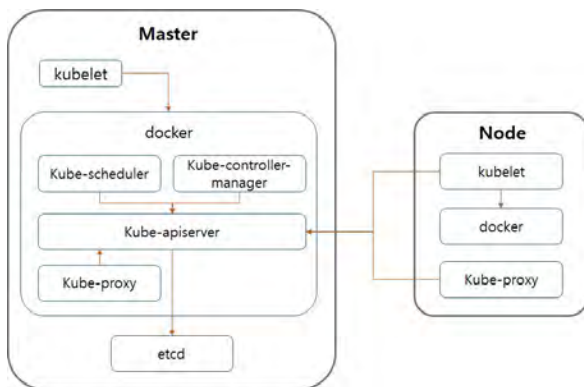


(그림 1) 도커에서 사용하는 자원 분리 방식

컨테이너에서는 할당된 자원을 활용하여 애플리케이션을 실행할 수 있고 애플리케이션의 실행 상태를 이미지로 저장하여 사용자가 원할 때 바로 실행이 가능하다. 이미지로 저장하고 원할 때 실행한다는 점에서 다른 오픈소스 가상화 소프트웨어와 비슷하지만 오픈소스 가상화 소프트웨어는 운영체제를 가상화하고 도커는 자원을 격리시킨다는 점에서 분명한 차이가 있다. 오픈소스 가상화 소프트웨어는 가상화된 머신에 항상 게스트 OS를 설치해야 하기 때문에 용량이 많이 필요하다. 도커는 실행파일을 호스트에서 직접 실행하기 때문에 가상화에 비해 저장공간이 적게 필요하다.

2.2. 쿠버네티스

쿠버네티스는 구글에서 개발하고 배포한 컨테이너 작업을 자동화하는 컨테이너 오케스트레이션 오픈소스 플랫폼이다. 도커를 이용하여 컨테이너를 작성하고 실행하는데 필요한 수동 프로세스를 자동으로 전환할 수 있다. (그림 2)는 쿠버네티스의 아키텍처를 나타낸다.



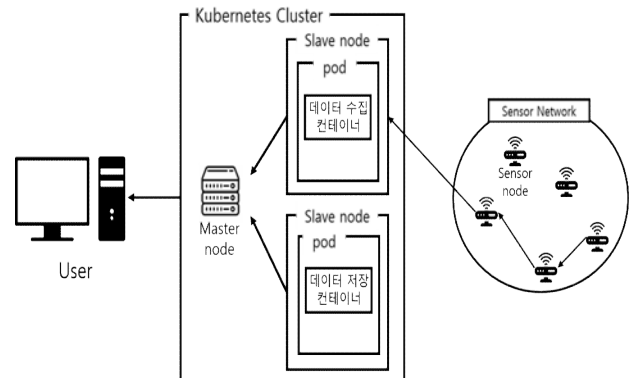
(그림 2) 쿠버네티스의 아키텍처

쿠버네티스는 마스터 노드와 슬레이브 노드로 구성된다[2]. 마스터 노드는 컨테이너를 생성하고 슬레이브 노드에 배포하며 관리하는 역할을 한다. 슬레이브 노드는 마스터 노드로부터 명령을 전달받고 실제 실행해야 할 애플리케이션이 담긴 컨테이너를 실행하는 노드이다. 또한 슬레이브 노드는 현재 실행 상태인 컨테이너의 정보를 마스터 노드로 전송하는 역할을 한다. 마스터 노드는 슬레이브 노드의 자원 사용량을 정할 수 있고 자원 사용량을 넘어서는 컨테이너를 자동으로 복사해서 다른 노드에 실행시키

고 로드밸런싱을 수행하는 오토스케일링 기능을 가지고 있다.

3. 시스템 설계

제안하는 시스템은 센서로부터 생성되는 트래픽의 양과 데이터에 따라 수집 서버를 scale out 할 수 있어야 한다. (그림 3)은 제안하는 시스템의 아키텍처를 나타낸다.



(그림 3) 제안하는 시스템의 아키텍처

3개 이상의 서버를 이용하여 쿠버네티스 클러스터를 구축한다. 3개 이상의 서버를 사용하는 이유는 마스터 서버가 과부하 되어 제 기능을 수행하지 못할 경우 다른 마스터 서버를 선출해야 하기 때문이다. 클러스터 구축이 완료되면 센서 네트워크의 데이터 수집 모듈과 저장 모듈을 도커를 사용하여 컨테이너로 생성한다. 생성된 컨테이너는 마스터 노드에 의해 슬레이브 노드로 배포되고 데이터 수집 및 저장을 시작한다. 슬레이브 노드는 데이터를 수집하고 있는 컨테이너의 상태를 지속적으로 마스터에게 전송한다. 마스터 노드는 데이터 수집 컨테이너의 자원 사용량이 일정 수준을 넘어서면 데이터 수집 컨테이너를 복사하고 다른 슬레이브 노드에 배포한다. 이때 마스터 노드에서는 동일한 작업을 수행하는 컨테이너를 여러 개 생성하기 때문에 로드밸런싱이 필요하다[3].

쿠버네티스에서 오토스케일링 및 로드밸런싱 기능을 사용하기 위해서는 metrics-server를 설치해야 한다. metrics-server는 컨테이너의 자원 사용량을 지속적으로 모니터링하는 서버로 전체 클러스터의 특성을 검사하여 클러스터 내의 애플리케이션의 성능을 검사할 수 있다. metrics-server 서버 설치 후에 컨테이너의 메트릭 데이터를 수집하기 위하여

metrics-server-deployment.yaml 파일을 수정해야 한다. (그림 4)는 수정된 설정 파일을 나타낸다.

```

1 containers:
2   #수정하고자 하는 인스턴스의 이름
3   - name: metrics-server
4     image: k8s.gcr.io/metrics-server-amd64:v0
5     args:
6       #데이터 수집을 위한 인증서가 저장된 폴더
7       - --cert-dir/tmp
8       #메트릭 데이터 수집시 사용하는 포트
9       - --secure-port=4443
10      #인증서로 인한 오류방지
11      - --kubelet-insecure-tls
12      #마스터 노드가 InternalIP를 사용하여 다른
13      #노드를 검색할 수 있도록 함
14      - --kubelet-preferred-address-types=Internal

```

(그림 4) 수정된 metrics-server의 설정파일

metrics-server는 메트릭 데이터의 수집만을 담당하고 실제로 컨테이너는 scale out하지 않는다. 실제 컨테이너의 scale out을 위해서는 autoscaling.yaml 파일을 생성하여 적용시켜야 한다. (그림 5)는 autoscaling.yaml 파일을 나타낸다.

```

1 #생성된 인스턴스의 종류 여기서는 autoscaler
2 kind: HorizontalPodAutoscaler
3 metadata:
4   #autoscaler의 이름
5   name: autoscaler
6 #autoscaler의 세부 설정
7 spec:
8   #컨테이너의 최대 복사본의 개수
9   maxReplicas: 10
10  #컨테이너의 최소 복사본의 개수
11  minReplicas: 1
12  scaleTargetRef:
13    kind: Deployment
14    name: <데이터 수집 컨테이너의 이름>
15  #cpu 사용률이 30%가 넘으면 스케일링 함
16  targetCPUUtilizationPercentage: 30

```

(그림 5) autoscaling.yaml 파일의 내용

autoscaling.yaml 파일을 적용시키면 마스터 노드는 데이터 수집 컨테이너의 cpu 사용률이 30%가 넘을 경우 복사본을 생성하여 다른 슬레이브 노드로

scale out 할 수 있다.

4. 결론

본 논문에서는 도커와 쿠버네티스를 이용하여 센서 네트워크에서 수집하는 데이터의 양이 많아질 경우 자동으로 수집 모듈을 scale out 하여 더 안정적으로 데이터를 수집할 수 있는 시스템을 설계하였다. 데이터를 저장하기 위한 저장 모듈 또한 같은 방식으로 scale out 가능하다. 그러나 데이터의 저장소가 scale out 되어 복사가 될 경우 같은 데이터가 중복되기 때문에 저장소를 제외한 모듈만 복사하는 연구가 추가적으로 이루어져야 한다. 또한 본 논문에서는 시스템의 cpu 사용률이 30%가 넘을 경우 오토 스케일링을 실행하도록 설정하였으나 추후 실험을 통하여 가장 효율적인 오토스케일링 시점을 찾아야 한다.

Acknowledgement

본 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.IITP-2019-0-00135 ,ICT 기반 환경 모니터링 센서 신뢰성 검증 및 평가 플랫폼)

참고문헌

- [1] 장시웅, 김지성 "대규모 센서 네트워크에서 센서 데이터 수집을 위한 효율적인 통신 시스템 설계 및 구현", 한국정보통신학회논문지, 제24권, 제1호, pp113-119, 2020
- [2] 장현준, 임인구, 진현욱, "도커 컨테이너 자원 활용률 모니터", 한국정보과학회 학술발표논문집, 2019, pp1086-1088
- [3] 김경일, "클라우드 서비스를 위한 쿠버네티스 구조", 한국통신학회지, 제35권, 제11호, pp11-19, 2018
- [4] Ilseok Han, Jonggyu Park, Wonyoul Bae, Hagbae Kim, "Development of an Optimal Load Balancing Algorithm based on ANFIS modeling in a Clustering Web Server", 한국통신학회 학술대회 논문집, 2003, pp1215-1218

노인 일자리 플랫폼 개발에 관한 연구

김상오* 공인복** 이해임*** 서정연**** 한보현****

*상명대학교 식품영양학과

**링크플러스 사업단, 상명대학교

***상명대학교 가족복지학과

****상명대학교 휴먼지능정보공학과

sangoh51@naver.com, kib@smu.ac.kr, kateli1004@naver.com,
sjo5525@naver.com, hbh0604@naver.com

A study on the Development of Job platfom for the Elderly

Sang-oh kim*, In-bog kong** Hye-lm Lee*** Jeong-youn Seo**** Bo-hyun Han****

*Dept. of Food and Nutrition, Sangmyung University

**Leaders in INdustry-universty Cooperation, Sangmyung University

***Dept. of Family Welfare, Sangmyung University

****Dept. of Human Intelligence Information Engineering, Sangmyung University

노인 일자리 분야의 플랫폼 연구는 초고령 사회를 맞이하는 대한민국 사회에 필수 불가결한 요소이다. 현재 고령인구, 향후 고령인구들에 대한 대책이 마련되지 않고 단순 보조금 지급과 같은 형식의 해결책으로는 실질적인...

1. 서론

최근 플랫폼 산업 관련 많은 이슈 중 노인 일자리 플랫폼 관련 수요는 나날이 증가하고 있는 추세다. 노령인구의 일자리 재창출을 위한...

2. 노인 일자리 분야의 선행 연구와 요구사항

고령사회, 초고령사회로 진입하는 한국사회에서 노인 일자리 부문 연구는 꾸준히 진행되어 왔다. 하지만 지금의 방식은 단순히 보조금 형식(현금 지원 방식)으로 진행되고 있으며, 일자리를 공급한다하더라도 직업 훈련 교육과 같은 프로그램 없이 단순 직종에만 편중되어 있다. 이는 실효성 측면에서 문제가 제기되었으며, 장기적인 관점에서 한계점이 있다는 문제가 있다. 이제는 보다 실질적인 노인 일자리 분야에 대한 진지한 고찰이 필요하며, 지금의 4050 세대에도 향후 직면할 중요한 이슈이다.

3. 노인 일자리 분야 플랫폼 연구

본 플랫폼 개발 연구에서 시니어들이 가지고 있는 경험 및 노하우를 어떻게 전달 할 수 있는가, 그 전달 방식을 보다 효율적으로 할 수 있는 플랫폼은

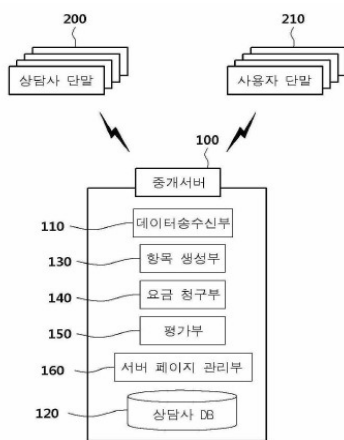
무엇인가 진지하게 고민하게 되었다. 시니어들이 단순 노무, 단순 직종에만 편중되는 것이 아니라 그들이 가지고 있는 전문지식, 경험을 보다 쉬운 방식, 간편한 플랫폼을 통해 전달할 수 있다면 젊은 층이 효율적으로 일처리를 할 수 있을 것이다. ‘시니어 노



(그림1) 플랫폼 사업 구상도

하우 중개 서비스 제공 시스템'은 이를 해소할 수 있는 방안이 될 수 있다. 본 내용은 고령의 시니어 상담사가 주니어 사용자에게 상담사의 경험을 바탕으로 해당 분야에 대한 노하우를 전달, 전수 할 수

있는 시스템에 관한 것이다. 해당 직종에서 은퇴한 고령의 전문가를 대상으로 상담자인 전문가 집단을 구성함으로써 은퇴한 고령의 시니어에게 일자리를 제공함은 물론이고, 삶의 경험을 기반으로 한 노하우를 주니어 사용자에게 제공 할 수 있는 중개 서비스 제공 시스템을 개발하는 것이다. 이 플랫폼에 구축된 시스템은 중개 서버와 데이터 송수신부, 평가부 등 데이터를 처리 가공할 수 있는 시스템이 포함된다. 또한, 정보를 DB에 기록하여 데이터를 구축한다. 데이터 시각화를 통해 쉽게 제공함으로써 노인 일자리 창출 효과와 젊은 세대들이 이 플랫폼을 이용할 수 있도록 유도한다.

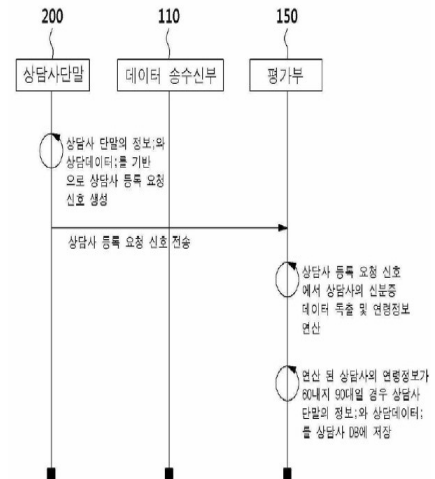


(그림2) 유무선 네트워크망

4. 플랫폼 기술 개발 관련 연구

근래에는 유무선 인터넷을 이용하여 사용자가 원하는 전문 영역의 질문을 접수하고, 해당 질문 영역에 적합한 전문가 집단을 통해 답변을 얻을 수 있는 전문가 상담 중개 시스템이 제공되고 있다. 일 예로 종래 출원 특허 제 10-2015-0053333호에 의하면, 사용자가 상담 신청 정보 및 개인 정보에 따라 자동적으로 추천된 상담자의 정보를 제공받음으로써 만족도 높은 상담을 받을 수 있도록 하는 네트워크 상의 상담자 중개 서비스 제공 방법을 제공하고 있다. 종래의 방법에 의하면, 상담자인 전문가 집단은 특정 전문적 분야에서 근로하고 있는 주니어 세대 또는 중장년층이 주를 이루며 질문에 대한 답변은 전문 지식을 바탕으로 이루어지기 때문에 전문 지식에 대한 답변을 요하는 사용자에게 적합하다. 상기 목적을 달성하기 위하여, 유무선 네트워크망을 통해 적어도 하나 이상의 상담사 단말과 사용자 단말 사이에 유/무선으로 연결시킴으로써 해당 분야에 대한 상담

서비스를 제공하는 중개 시스템에 있어서, 상담 서비스를 제공하는 상담사 단말과 유/무선 네트워크 연결 서비스를 제공하는 중개 서버와 상기 중개서버를 통해 상담사 단말과 연결되어 상담 서비스를 이용하는 사용자 단말을 포함하되, 상기 상담사 단말은 상담사의 경험을 기반으로 해당 분야에 대한 노하우 정보를 상기 사용자 단말에 제공한다.



(그림3) DB 서식도

5. 기대 효과

초고령 사회로 진입하는 대한민국에서 젊은 세대의 노인 부양부담은 날이 갈수록 증가한다. 이는 젊은 세대의 노동 효율이 저하되고, 국가 경쟁력 또한 저하되는 문제점을 야기한다. 이는 국내에서 세대간 갈등으로 이어져 문화적 갈등, 세대 간 갈등으로 점철 될 수 있다. 노인 일자리 플랫폼을 사용함으로써 노인들은 경제적 소득 창출을 통한 삶의 질을 향상할 수 있고 사회참여의 기회를 제공받게 된다. 능력 있는 시니어들의 인력활동은 노동 효율의 극대화를 불러오며 일자리 확대를 통한 경제적 성장과 같은 선순환적 구조를 해결할 수 있는 노인 일자리 문제의 하나의 해결책이 될 수 있다.

6. 결론

2020년 현재 플랫폼 산업에서 패권을 쥐고 있는 기업들이 세계를 이끌고 있다. 하지만 플랫폼 기반 사업들은 대부분 최신식 기술에 국한되어 있기에 일자리 관련, 특히 노인 일자리 관련 플랫폼 개발은 더딘 것이 현실이다. [1]노인 일자리사업이 사회적 요구와 정책적 검토의 과정을 단계적으로 거쳐 생산된 정책적 결과물이라기보다 정치적 고려에 따라 일

방적으로 도입된 성격이 강하며 이 때문에 정책도입 이전에 충분한 철학적, 윤리적 논의가 충분히 이루어지지 않은 한계에 기반한 결과로 이해된다. 현재 개발되고 있는 노인 일자리 플랫폼은 노인의 풍부한 경험에 기반한 플랫폼이므로 노인 일자리 분야에 있어서 실질적인 도움이 될 것이며, 시니어가 사회에 기여 할 수 있는 보다 효율적인 플랫폼 사업이 될 것이다.

참고문헌

- [1] 김대건. (2019). 노인일자리사업 연구경향 분석. 한국산학기술학회 논문지, 20(4), 197-206.

도시 도로 환경에서의 적용 가능한 동적 군집주행에 관한 연구

최수민*, 박수용**, 신용태*
*승실대학교 융합소프트웨어학과
**승실대학교 컴퓨터학과

suumn1538@soongsil.ac.kr, tndyd5390@naver.com, shin@ssu.ac.kr

A Study on the Applicable Dynamic Platooning in Urban Road Environment

Su-Min Choi*, Soo-Yong Park**, Yong-Tae Shin*

*Dept. of Computer Science, Soong-Sil University

**Dept. of Convergence Software, Soong-Sil University

요 약

최근 자율주행차량의 기술 개발이 확대되면서 이를 기반으로 운전자, 인프라 등 다양한 관점에서 효과를 기대할 수 있는 군집주행에 대한 관심도 점차 높아지고 있다. 현재 고속도로에서만 적용 가능한 군집주행 기술이 상용화 되면서 교차로가 많은 도시 도로 환경에서도 이를 적용하기 위해 여러 자동차 업체에서 시스템을 개발 중이다. 하지만 기존 군집주행 방식은 군집이 해체될 경우 차량이 다시 군집을 형성하고 다른 군집에 가입하는 과정에서 발생하는 시간이나 비효율적인 측면에서 도로 처리량과 시간 단축이라는 본래 군집주행의 목표에 미치지 못한다. 따라서 본 논문은 차량 간에 주고받는 메시지를 개선하여 군집주행 알고리즘을 새롭게 설계해 도시 도로 환경에서도 적용 가능한 동적 군집주행에 대해 제안하였다.

1. 서론

현재 고속도로에서만 제한적으로 적용되는 군집주행을 교차로가 많은 도시 도로까지 확대시키기 위해 보완되어야 할 부분이 많다. 기존 군집주행 방식에서는 군집이 해체되는 경우에 리더 차량을 재선출하여 군집을 재형성 하거나 다른 군집에 합류 요청을 하여 군집에 가입할 수 있다. 이러한 과정으로 인해 군집주행을 하는 데 시간이 지연되고 도로 사용 측면에서도 비효율적이므로 도로 사용 처리량을 최대화한다는 본래 군집주행 목표에 미치지 못한다.

따라서 본 논문은 군집 해체 시 도로 처리량과 시간 단축의 효율성을 높이고 도로에서 발생하는 문제 상황에 대해 신속하게 대응할 수 있도록 리더 차량에서 후보 리더에 대한 목록을 추가하였다. 이는 고속도로뿐만 아니라 교차로가 많은 도시 도로 환경에서도 유연하게 군집의 분리 및 재형성이 가능하도록 주행 중에 차량 간에 주고받는 메시지의 표준인 SAE J2735 Message Protocol 을 개선하여 군집주행 통신 알고리즘을 새롭게 설계하는 방안에 대해 연구를 진행하였다.

2. 관련 연구

본 장에서는 제안하는 연구의 기반이 되는 군집주행과 차량 간 통신 메시지인 SAE J2735 Message Protocol 에 대해 서술한다.

2.1 군집주행

군집주행(Platooning)은 두 대 이상의 차량이 하나로 연결된 로드 트레인을 구성하여 운행하는 기술로 자율주행 기술과 함께 차량 연결 기술이 복합적으로 적용된 주행 방법이다. 군집주행 시 각각의 차량들은 하나의 세트로 연결되어 서로 가까운 거리를 유지한 채 마치 기차와 같은 행렬로 이동하게 된다. 군집주행의 선두에 위치한 차량은 리더 역할을 수행하며, 뒤따르는 차량들은 리더 차량의 경로를 그대로 따라 주행한다.

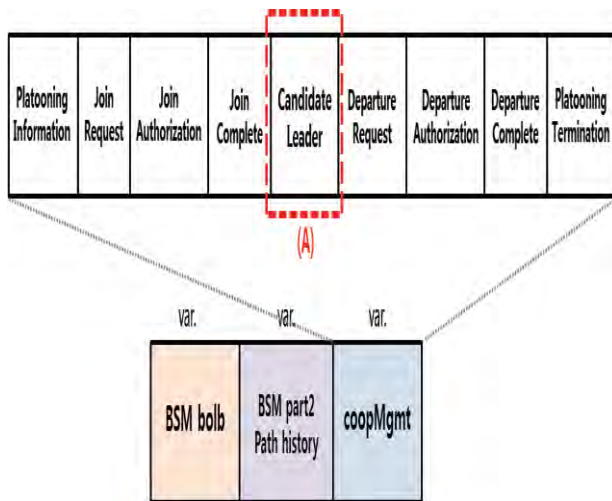
일반 모드로 주행하는 차량들이 많을 때 보다 군집 모드로 주행하는 차량이 많을수록 도로를 효율적으로 사용할 수 있다. 또한 운송이나 목적지 도착 시간을 단축시킬 수 있으며, 자율주행기술을 기반으로 하므로 운전자들이 주행 중 전화, 여가 생활 등 다른 업무가 가능해졌다.

2.2 SAE J2735 Message Protocol

WAVE(Wireless Access in Vehicular Environment) 통신 기반의 어플리케이션에서 사용되는 데이터 요소와 데이터 프레임으로 구성된 메시지셋의 표준이다[1]. 이는 WAVE 통신 기반으로 정의되어 있지만 다른 무선 통신 기술에서도 사용이 가능하도록 정의되어 있다.

3. 동적인 군집주행을 위한 메시지 프로토콜 설계 및 시나리오

도시 도로 환경에서도 적용 가능한 동적인 군집주행을 위해 기존의 메시지 구조에서 하나의 필드를 더 추가하여 후방 차량에서 리더 차량에게 군집의 다음 리더가 될 수 있게 우선순위를 정하는 데 필요한 상태 정보들을 메시지에 담아 보내게 된다.



(그림 1) 후보 리더 선정을 위한 메시지 프레임 추가

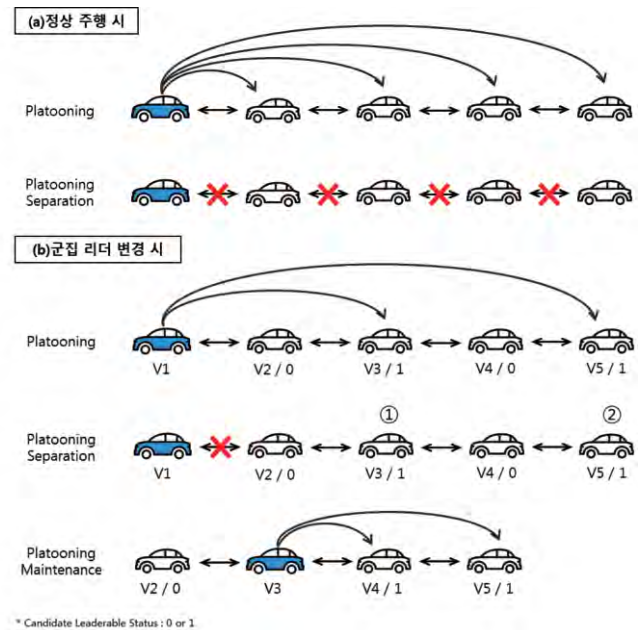
운전자가 이미 형성되어 있는 군집에 가입하려고 할 때 군집 리더에게 합류 요청을 하게 되고 리더가 합류를 승인하면 군집 합류가 완료된다. 그 후에 운전자가 군집 해체 시에 차기 리더가 가능한지에 대한 상태를 결정한다. 선택은 차량의 센터 패시아에서 스크린 통해 군집에 합류할 때뿐만 아니라 운전자가 직접 설정의 상태를 변경할 수 있다. 이 상태 정보는 그림 1에서 데이터 요소 (A)에 0 또는 1의 형태로 저장되며 0은 후보 리더 불가능, 1은 후보 리더 가능을 의미한다.

군집을 가입되어 있는 후행 차량 중에서 여러 대의 차량이 후보 리더 가능 상태일 경우가 존재한다. 이러한 경우에는 리더 차량에서 후행 차량들에게 전송 받은 메시지의 후보 리더 데이터 요소를 확인하고 해당 차량들의 차량 상태 정보를 기반으로 후보 리더

차량들의 우선순위를 정한다.

후보 리더 차량의 우선순위를 정해 놓게 되면 교차로가 많은 도시 도로 환경에서도 군집주행이 가능해진다. 교통 신호 등의 여러 가지 변수로 인해 군집의 중간이 분리되더라도 우선순위 정보를 통해 유동적으로 리더를 재선출하여 군집을 유지한다

제안한 메시지 프로토콜을 기반으로 한 군집주행 시나리오는 (그림 2)와 같다.



(그림 2) 군집주행 시나리오

그림 2에서 ‘(a)정상 주행 시’의 경우 기존 군집주행 방식에서 주행 중 여러 가지 변수로 인해 군집주행 해체되는 과정을 보여준다. 리더 차량이 군집 모드에서 일반 모드로 변경하면 군집을 이루고 있는 모든 후행 차량들까지도 일반 모드로 변경되고 이로 인해 군집은 해체된다. 군집을 계속해서 유지하고 차량이 있어도 리더 차량이 떠나는 순간 해체되는 것이다.

다시 군집을 형성하려면 그 후행 차량 중에서 누군가가 군집 리더로 설정을 해야 한다. 다른 후행 차량들도 군집에 가입하려면 리더 차량에게 합류 요청을 보내고 리더 차량에서 승인을 받아서 가입을 완료한다. 이와 같은 과정은 군집에 가입하길 원하는 차량이 있을 때마다 반복된다.

교차로가 많은 도시 도로 환경에서는 실시간으로 변하는 교통신호 또는 정보를 전송 받아야 하기 때문에 군집 재형성 과정으로 인한 시간 지연이 발생하지 않아야 한다.

그림 2에서 ‘(b)군집 리더 변경 시’의 경우 후보 리더 차량을 추가하여 군집을 유지하는 과정을 보여준

다. 일반 차량이 처음 군집에 가입할 때 후보 리더 가능 상태를 설정하여 0 또는 1 의 형태로 리더 차량에게 전송한다. 군집 내의 후보 리더 가능 차량이 다수일 경우 리더 차량에서 각각의 차량이 가입할 때 전송한 차량의 상태 정보를 파악하여 후보 리더 우선순위를 정한다. 이 우선순위 정보를 후보 리더 가능 차량들에게 전송하고 해당 차량들은 이 정보를 유지하면서 주행한다.

군집주행 중에 군집이 해체되기 직전의 상황일 때 후보 리더 가능 차량들은 리더 차량으로부터 받은 우선순위에 따라 1 순위 차량을 새로운 리더 차량으로 파악한다. 새로운 리더는 군집의 리더 차량 ID 를 자신의 차량 ID 로 변경한다. 변경된 리더 차량 ID 가 포함된 메시지를 나머지 후보 리더 가능 차량에게 전송한다.

후보 리더 차량의 우선순위를 정해 놓게 되면 교차로가 많은 도시 도로 환경에서도 군집주행을 적용하는 것이 가능해진다. 교통 신호 등의 여러 가지 변수로 인해 군집의 중간이 분리되더라도 우선순위 정보를 기반으로 지연 없이 리더를 교체하여 군집을 유지한다.

4. 결론

본 논문에서는 기존 군집주행 방식에서 발생하는 트래픽 과부하, 시간 지연 문제점을 개선하기 위해 군집 후보 리더 차량의 우선순위를 추가하였다. 이를 기반으로 교차로가 많은 도시 도로 환경에서도 군집주행을 적용할 수 있는 방안에 대해 제안하였다.

교통 상황이나 리더 차량의 변수로 인해 리더가 변경되어야 하는 경우에 기존과 달리, 군집을 분리하지 않고 신속하게 리더를 변경하여 유연한 군집주행이 가능해졌다. 이로 인해 고속도로 환경에서만 적용이 가능했던 군집주행을 신호등과 교차로가 많은 도시 도로 환경에서도 적용할 수 있게 되었다.

차량과 차량 간에는 차량의 ID 와 주행에 필요한 여러 가지 정보가 패킷에 담겨 데이터 전송이 이루어진다. 그러므로 보안을 강화하여 차량 운전자 또는 군집을 이루고 있는 차량들의 안전을 보호할 수 있는 차량 정보 해킹 방지 또는 탐지 알고리즘을 개발하는 연구가 필요하다.

ACKNOWLEDGMENT

이 논문은 2017 년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.IITP-2017-0-00724, 셀룰러 기반 산업 자동화 시스템 구축을 위한 5G 성능 한계 극복 저지연, 고신뢰, 초연결 통합 핵심기술 개발)

참고문헌

- [1] TTAS, "Communication Protocol for Group Driving ," "TTAK.KO-06.0439 "
- [2] Inès Ben Jemaa. "Multicast communications for cooperative vehicular systems ." "Robotics [cs.RO]" Ecole Nationale Supérieure des Mines de Paris, 2014

제53회
2020 온라인 춘계학술발표대회

사물인터넷



얼굴인식을 이용한 드론의 위치제어 구현

권기환, 짜오 차오란, 권지승, 김수연
지도교수 정순호
부경대학교 컴퓨터공학과
e-mail : rlghks786@gmail.com

Drone position control using face recognition

Gi-Hwan Kwon, Chao-Ran Zzao, Ji-Seung Gwon, Su-Yeon Kim
Prof. Soon-Ho Jung
Dept of Computer Engineering, Pukyung University

요 약

드론을 활용한 산업이 많은 관심을 받고 있다. 군집비행 연구는 산업 분야, 군사 분야에서 주요작업 성공확률을 높일 수 있다. 본 논문에서는 전파 음영지역에서의 드론의 군집비행 제어를 위해 얼굴인식을 바탕으로 위치제어를 수행한다. 이러한 기능의 구현을 통해 드론의 효과적인 군집비행이 가능할 것이며 정밀한 제어가 요구되는 분야에서 이용 가능할 것으로 기대된다. 향후 추가적인 제어방식으로 개선할 것이다.

1. 서론

최근 드론을 활용한 산업이 많은 관심을 받고 있고 활용 분야 또한 늘어나는 추세이다. 특히 다수의 드론을 동시에 제어하는 군집비행 연구는 산업 분야, 군사 분야에서 주요작업 수행시 성공확률을 높일 수 있다.[1]

군집비행을 위해서는 드론 사이의 간격을 보정할 필요가 있는데 일반적으로 GPS/RTK 등의 전파정보를 활용한다. 하지만 실내 또는 건물이 밀집된 지역의 경우 위성전파에 대한 음영지역이 발생하기 때문에 이에 의존하지 않는 새로운 위치 보정 방법이 필요하다.

본 논문에서는 전파 음영지역에서의 드론의 간격을 보정하기 위한 다양한 방법 중 인체를 기준으로 삼는 얼굴인식을 이용한 위치제어 방식을 구현하고자 한다.

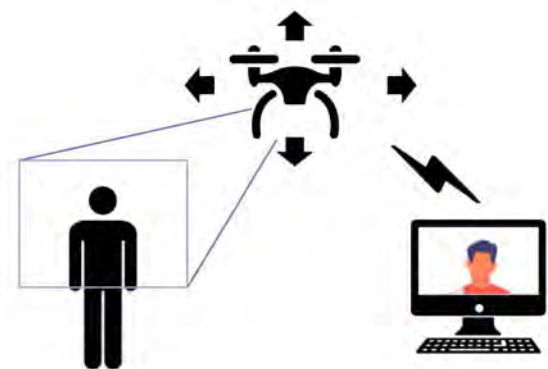
이어지는 2장에서 드론 위치제어 시스템의 구성을 소개하고 3장에서 구현 및 실험하겠다.

2. 드론 위치제어 시스템

시스템은 드론과 서버로 구성된다. 드론은 서버와 연결되어 제어를 받고 카메라에서 촬영된 영상을 송신한다. 서버는 영상을 처리하여 얼굴인식을 수행하며 드론에 명령을 내리는 역할을 한다.

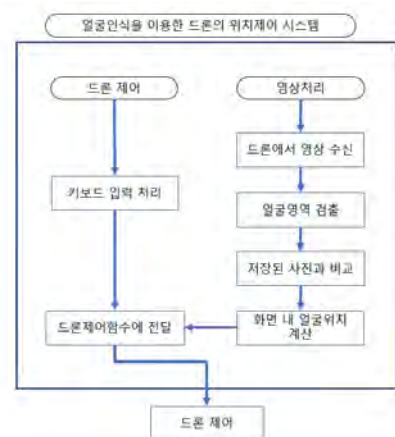
(그림 1)과 같이 드론이 비행 중 서버에 얼굴 정보가 등록된 사람이 나타난다면 얼굴인식을 통해 확인 후 고도와 거리를 조정한다. 또한, 사용자가 직접 드론의 위치를 세부적으로 제어하는 것이 가능하다.

다수의 인원이 화면 내에 있을 경우, 얼굴이 등록된 사람 또는 가장 먼저 얼굴이 식별된 사람만을 기준으로 하도록 하였다.



(그림 1) 얼굴인식을 통한 드론의 위치제어

시스템의 전반적인 흐름은 (그림 2)와 같다.



(그림 2) 시스템 흐름도

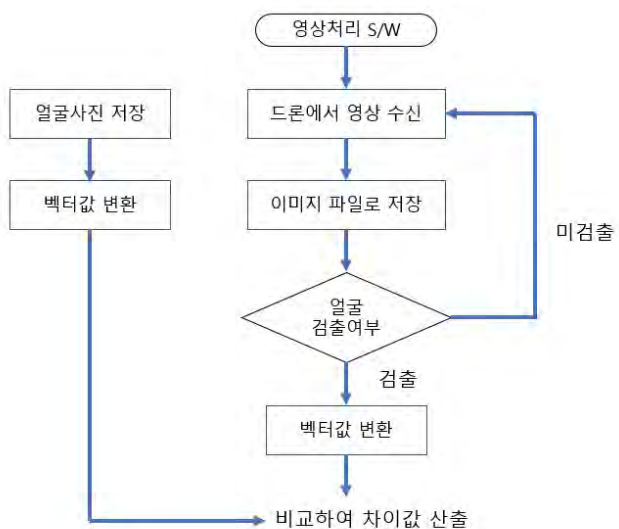
프로그램은 드론의 제어와 영상처리를 각각 처리하며 제어 함수는 키보드 입력과 드론 제어, 영상처리 함수는 얼굴인식과 화면 내 얼굴의 위치를 계산하는 역할을 한다.

2.1 얼굴인식과 영상처리

얼굴인식은 드론에서 촬영한 영상을 이미지로 저장하기 위한 VLC 미디어 플레이어와 얼굴 검출을 위한 모듈인 dlib, 영상을 통해 드론의 상대적 위치를 계산하기 위한 Opencv를 사용한다.

얼굴인식 함수는 인식할 사용자의 얼굴 사진을 서버에 미리 저장해두고 미디어 플레이어로 드론에서 영상을 전송받아 실시간으로 처리하는 방식이며 얼굴인식 모듈을 사용하여 촬영된 이미지에서 얼굴이 검출될 경우 서버에 저장된 얼굴 이미지와 비교한다.[2]

드론에서 촬영한 이미지와 서버에 저장된 두 이미지의 비교는 유클리드 거리 계산방식을 이용하며 계산과정은 (그림 3)와 같다. 서버 내에 저장되어 있는 얼굴이미지와 촬영된 얼굴 이미지를 벡터값으로 변환 후 두 이미지 간 차이 값이 기준 수치보다 작다면 일치한다고 판단한다.



(그림 3) 영상처리 S/W 흐름도

검출된 얼굴은 리스트에 저장되어 얼굴인식 과정 중 다수의 얼굴이 검출될 경우에도 리스트의 첫 번째에 저장된 사람의 얼굴을 기준으로 드론 제어가 가능하게 하였다.

해당 얼굴은 Opencv 영상 출력창에서 사각형 프레임을 덧씌워 나타나며 사각형 프레임은 화면 내 얼굴의 상대적인 위치를 계산하는 데 쓰인다. 영상처리 함수는 (그림 4)과 같이 사각형 프레임이 화면 중앙에 오도록 드론의 위치를 제어하는 값을 반환한다.[3]



(그림 4) 드론의 위치 제어방식

2.2 드론 제어

드론 제어는 Pyparrot, Pygame 모듈을 사용하며 드론 제어와 키보드 이벤트 발생을 기록하는 역할을 한다.[4] [5]

드론 제어함수는 영상처리 함수에서 반환된 인식 결과를 받아 화면 내에서 인식된 얼굴이 중앙에 오도록 드론의 위치를 조정하게 된다.

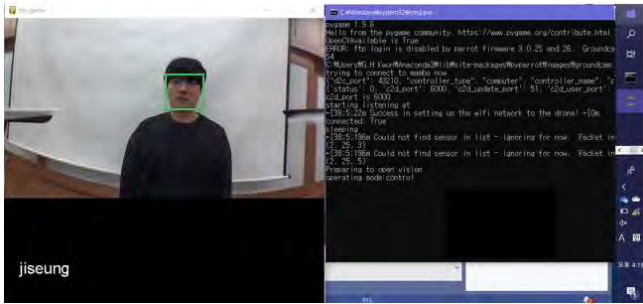
자동으로 조종되는 것 외에도 사용자가 드론의 위치를 미세조정할 필요가 있다고 생각되어 키보드로도 조종할 수 있도록 구성하였다. 드론은 상하 이동, 전후좌우 이동, 제자리 방향전환이 필요하기 때문에 키보드의 8개 키 입력을 받는다.

3. 구현 및 실험

(그림 5)와 (그림 6)는 프로그램이 동작하는 모습이다. (그림 5)와 같이 드론 조종을 통해 얼굴인식이 필요한 대상의 근처로 드론을 이동시킨다. 이후 (그림 5)와 같이 드론이 대상을 인식하고 자동으로 위치제어를 수행한다.



(그림 5) 사용자의 드론 제어



(그림 6) 영상처리 프로그램의 동작

4. 결론

본 논문에서는 전파 음영지역에서의 효율적인 드론 제어를 위해 제안한 얼굴인식을 통한 드론의 위치제어 방식을 소프트웨어 설명, 흐름도를 통해 기술하였다.

영상처리를 이용하여 드론을 제어하는 방식을 통해 위치 식별이 불가능하여 제어되지 않는 드론도 효과적으로 제어할 수 있을 것이며 산업분야, 군사분야와 같은 고가의 드론을 사용하고, 정밀한 제어가 요구되는 분야에서 이용 가능할 것으로 기대된다.

향후 연구계획으로는 드론 외부에 존재하는 카메라를 통하여 드론을 인식 후 제어할 수 있도록 기능을 개선하고 작동의 편의성을 위하여 UI를 추가하고자 한다.

참고문헌

- [1] “드론의 공공임무 활용”, 이상춘, 윤병철, 김동억, 채지인, 한국통신학회지(정보와통신), 제 33권, 제 2호, pp 100-106
- [2] Florian Schroff, Dmitry Kalenichenko, James Philbin, “FaceNet – A unified Embedding for Face Recognition and Clustering”
- [3] “Opencv”, <https://opencv.org>
- [4] “Pygame”, <https://pygame.org>
- [5] “Pyparrot 1.5.3 Documentation”
<https://pyparrot.readthedocs.io/en/latest/index.html>

차량 인포테인먼트 장치 통합관리 모듈 설계 및 개발

이채현*, 오현경*, 박소연*, 김성우*, 정중화*, 고석주*, 김재수*, 김지인**

*경북대학교 컴퓨터공학과

**㈜엠케이오토텍

dlcoguswkd@naver.com, hyeony1070@gmail.com, thdus1487@naver.com,
sw960703@naver.com, godopu16@gmail.com, sjkoh@knu.ac.kr,
kjs@knu.ac.kr, jiin16@gmail.com

Design and Development of Integrated management module in In-Vehicle Infotainment System

Chae-Hyun Lee*, Hyun-Kyung Oh*, So-Yeon Park*, Seong-Woo Kim*,
Jung-Hwa Jung*, Seok-Ju Go*, Jae-Soo Kim*, Ji-in Kim**

*Dept. of Computer Science and Engineering, KyungPook National University

**MK Autotech

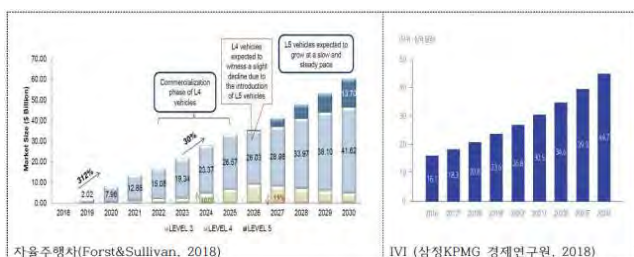
요 약

우리 생활 속에 사물인터넷이 확산하면서 상호작용이 가능한 스마트 기기들이 증가하고 있다. 차량은 인간에게 친숙한 이동수단으로, 현재 차량 인포테인먼트(Infotainment) 시스템의 관심이 급증하고 있다. 하지만 해당 시스템은 기업마다 개발요소와 기준이 다르다. 본 논문에서는 차량 인포테인먼트 장치들을 통합적으로 관리하는 모듈을 설계 및 개발하고, 미래 인포테인먼트 서비스의 방향을 제시하고자 한다. 본 논문의 모듈은 스마트폰과 마스터 디바이스(Device), 그리고 센서들을 사용해 제작되었으며, 모듈의 실제 차량의 적용 및 확장을 통해 더 나은 인포테인먼트 관리 모듈을 개발할 수 있을 것으로 기대한다.

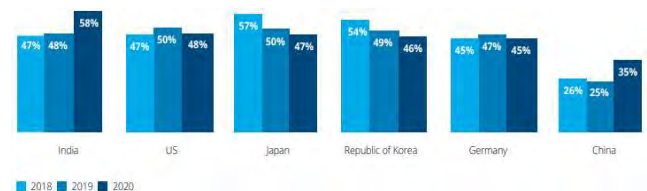
1. 서론

차량 인포테인먼트(In-Vehicle Infotainment, 이하 IVI)란 차체의 상태를 관리하고, GPS를 이용한 길 안내 등을 의미하는 인포메이션(Information)과 비디오 및 오디오 서비스 등 운전자의 엔터테인먼트(Entertainment) 요소들을 결합한 서비스를 말한다. 자동차는 AI, VR Camera 등의 기술과 접목되는 추세지만 특히 자율주행과 깊은 연관이 있다.

IVI 시장은 매년 지속적으로 성장 중이며, 자율주행차 성장곡선과 유사한 형태를 가지고 있다. 자율주행차 시장이 도래하면서 커질 것으로 예측된다[1].



(그림 1) 세계 자율주행차 및 IVI 시장 규모



(그림 2) 자율주행차의 불안전성에 대한 긍정적 답변

하지만 자율주행차에 대해 소비자들의 반응은 엇갈리는 편이다. 'Deloitte'의 소비자 조사결과에 따르면 자율주행차에 대한 불안전성에 동의하는 의견이 중국을 제외하면 거의 50%에 육박한다[2].



(그림 3) 자율주행차 사고를 미디어로 접한 후 위험을 느낀 비율

또한, 자율주행차에 의한 사고를 미디어를 통해

접한 사람들이 지속적으로 해당 기술에 대한 위험을 느낀다고 반응한 비율이 모든 조사국에서 55% 이상을 차지했다[2].

위와 같이 IVI 시스템은 많은 관심을 받고 있고, 많은 기업이 자신들만의 IVI 시스템을 만들어내고 있지만, 그만큼 소비자들은 그 위험성에 대한 우려를 나타낸다. 자율주행의 편리성과 오락, 콘텐츠뿐만 아니라 지금은 자율주행을 상용화하기 위해서 소비자들이 납득할 수 있는 IVI 시스템의 기준을 정해야 할 것으로 생각되어 해당 프로젝트를 진행했다.

2. 관련 적용 사례

2.1 CES 2019 : 아우디

세계 최대 규모의 전자 제품 박람회인 CES에서 2019년에 많은 자동차 제조 회사들이 자율주행 콘텐츠를 소개했다. 그 중 아우디는 디즈니와 협력해 이머시브 인카 엔터테인먼트(Immersive In-Car Entertainment)와 아우디 익스피어리언스 라이드(Audi Experience Ride)라는 2개의 프로젝트를 소개했다.

이머시브 인카 엔터테인먼트는 영상, 소리와 자동차 움직임, 공조 시스템 등을 결합하는 콘텐츠로 4D 영화관 같이 차량이 움직이는 효과를 제공했다.

아우디 익스피어리언스 라이드는 주행 정보를 VR 콘텐츠 정보와 동기화 시킬 수 있었는데, 주행 경로에 따라 VR 콘텐츠의 체험이 달라지게 하는 방식이다. 이를 통해 영화, VR 콘텐츠 등을 더욱 생생히 느낄 수 있다[3].



(그림 4) 아우디 익스피어리언스 라이드

2.2 안드로이드 오토와 애플 카플레이

안드로이드 오토와 애플 카플레이는 안드로이드 혹은 iOS를 설치 가능한 기기를 차량에 연결하여 차량 - 스마트 기기 - 탑승자 간의 상호작용을 가능하게 했다.

해당 앱은 차량 내부의 디스플레이에 맞는 안드로이드 UI를 띄워주는 형식으로 구동되며, 음성을 통한 조작, 내비게이션, 통화 및 메시지 전송, 오디오 및 비디오 콘텐츠 등 다양한 기능을 사용할 수 있으

며, 현재 국내에서 현대, 기아, 쌍용, 쉐보레 등 다양한 기업의 차량에 지원이 되고 있다.

3. 시스템 설계 및 구현

3.1 전체 시스템 개요



(그림 5) 시스템 설계 개요도

시스템은 CCIS Device 및 CCIS Master와 어플리케이션이 사용가능한 스마트 기기로 구성된다. CCIS란 Configurable Car Infotainment Services의 약자로 IVI가 제공하는 서비스를 통칭한다. CCIS Device(이하 디바이스)는 차량 내부를 구성하는 요소들로 에어컨, 내비게이션, 안전장치와 기타 센서들을 포함한다. CCIS Master(이하 마스터)는 디바이스들과 연결되어 있으며, 마스터에 의해 제어된다.

본 논문에서는 차량 내부의 장치들을 모방한 일부 센서들을 CCIS Device로 설정하였으며, 마스터와 User 어플리케이션을 안드로이드 어플리케이션 형태로 구성하였다. 디바이스들은 항상 마스터에 의해 제어되며, 사용자의 권한이 만족될 때 마스터는 사용자의 명령을 디바이스에 전달하게 된다.

3.2 사용자 권한 설계

해당 시스템을 사용하기 위한 사용자는 보안을 위해 총 3개의 등급으로 분류하였다.

구분	설명
(1) Car Owner	실질적인 차량 소유자
(2) Temporary Owner	임시 소유자로 (1)로부터 권한 위임 (3)에게 기능 권한 부여 가능 기한 만료 시, (1)의 요청 시 권한 박탈 가능
(3) Private/Public User	Owner로부터 일부 기능에 대한 권한을 받아 사용 상위 권위자의 권한 박탈 시, 자신의 권한도 박탈

<표 1> 사용자 등급 3단계

Car Owner는 기본적으로 차량 내부의 센서 및 기기들의 상태확인 및 제어 권한을 소유하고 있다. 해당 권한을 Temporary Owner 혹은 User에게 부여할 수 있고, 부여한 권한은 Car Owner에 의해 언

제든지 박탈당할 수 있다.

Temporary Owner는 권한을 일정 기간 소유하는 대여자로서 이 권한을 다른 User에게 부여할 수 있고, 권한의 기한만료, 혹은 반납을 원할 때 자신이 가진 권한을 없앨 수 있다. 또한, 다른 User에게 할당했던 권한들도 사라진다.

Private/Public User는 Owner들로부터 일부 권한을 할당받아 기능을 사용한다. User는 Owner에게서 부여받은 권한 외 기능은 사용할 수 없으며, 상위 등급자의 권한 만료 시, 자신의 권한도 동시에 사라진다.

3.3 시스템 구현

구분	상세
OS	Windows 10 Education
Device	Galaxy A9
Device OS	Android 9.0
Framework	Android studio
Language	Java

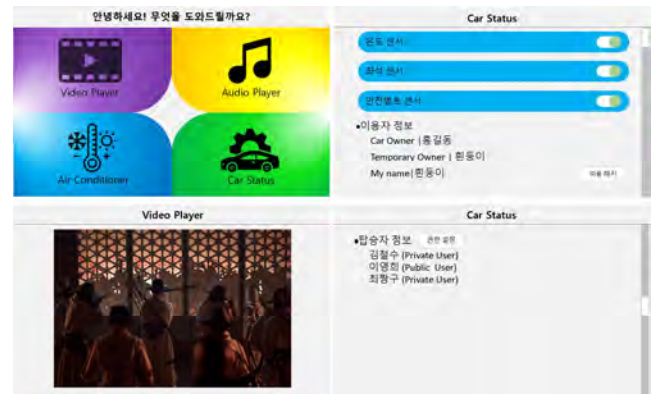
<표 2> 시스템 개발 환경

구분	설명
온도 센서	차량 내부의 온도 감지 감지 후 에어컨 작동 등 적절 기능 추천
적외선 센서(2)	송신 좌석 탑승 여부 확인용 수신 수신 시 미탑승, 미수신 시 탑승
리드 스위치 센서 모듈	안전 벨트의 사용 여부 감지 미착용 시 어플리케이션에 알림 전송
와이파이 모듈	스마트폰 - 센서와의 통신을 담당

<표 3> 사용 센서 및 설명



(그림 6) CCIS App for Client



(그림 7) CCIS App for Master

본 시스템의 개발 환경은 <표 2>와 같으며, 사용된 센서와 그 사용처는 <표 3>에서 확인할 수 있다.

클라이언트 어플리케이션에서는 현재 탑승한 차량의 마스터 기기에 접속하여 마스터에서 보내오는 정보들을 받아 확인하고 마스터에게 적절한 명령을 보낼 수 있다. 또한, 현재 탑승자들의 목록을 받아 관리할 수 있다.

마스터 어플리케이션에서는 다른 인증 없이 클라이언트 어플리케이션으로 사용자가 마스터에 접속 시 권한에 따라 적절한 기능을 사용할 수 있도록 메인 메뉴를 구성하여 마스터에서 직접 제어가 가능하도록 했다. CCIS Device(센서)와 직접 연결되어 센서에서 보내는 신호를 상황에 따라 클라이언트 어플리케이션에 전송하는 매개체 역할을 수행한다.

4. 테스트 결과

본 시스템에서는 <표 4>의 영역별 진단표를 작성하여 결과를 정리했다.

영역	상세	여부(Pos, Neu, Neg)
보안	등록/로그인 시 정보 무결성 유지	Pos
보안	하위 권한자가 상위 권한자의 권한 수정	Neg
보안	적절한 권한을 가진 사용자의 기능 사용	Pos
인증	클라이언트->마스터 접속 시 인증 여부	Pos
인증	탑승자 정보의 올바른 유지	Pos
연결	마스터에서 센서 작동 On/Off 기능	Neu
연결	센서의 올바른 작동 여부	Neu
연결	클라이언트-마스터 연결 해지	Pos
기능	미디어(비디오, 오디오) 기능	Pos
기능	온도에 따른 기능 추천	Pos

<표 4> 영역별 진단표

먼저 사용자 및 차량의 정보를 서버에 저장할 때와 변경 및 접속 시 모든 정보의 무결성이 유지되는 것을 확인했으며, 하위 권한자가 상위 권한자의 권한을 수정하는 권한 역전 현상은 발견하지 못했다.

하지만 센서의 연결 및 통신이 일부 미흡한 점이 발견되었다. 해당 부분은 안드로이드 기기와 센서의 통신환경과 호환성 여부를 재확인 시 해결할 수 있을 것으로 보인다.

클라이언트-마스터 간의 통신은 적절하게 이루어졌고, 클라이언트 요청에 대한 마스터의 프로세스 처리가 올바르게 처리되었으며, 기타 기능에 대해서는 문제를 발견하지 못하였다.

5. 결론

현재 차량 시장은 5G, 인공지능, 자율주행 등 여러 기술이 결합된 제3의 생활공간으로 진화하는 과정이다. IT 기술이 발전함에 따라 자동차는 인간의 명령에 따라 스스로 처리하는 스마트 공간으로 진화할 가능성이 높아지고 있다. 따라서 자동차라는 공간 안에서 사람은 더욱 자유로워지고, 이동하는 동안 스마트폰 등 스마트 기기를 통해 집, 직장 등 다른 공간의 전자기기들을 제어할 수 있게 될 전망이다. 그렇기에 IVI 시장 확장, 플랫폼 개발에 자동차 제조 기업은 더 많은 투자를 진행하고 있다. 하지만 기준과 프로토콜이 존재하지 않는 무분별한 투자와 개발은 기기 및 서비스의 비호환성, 비효율을 초래할 수 있다.

본 논문에서는 IVI 서비스를 제어할 수 있는 통합 관리 모듈의 한 예시를 보여주었다. 해당 시스템은 대부분의 차량에 적용할 수 있도록 진행되었으며, 또한 각각의 사용자 등급을 부여하여 기능 사용에 대한 구분 및 권한도 구별하도록 하였다. 이를 통해 차량 대여 서비스, 차량 도난 방지 서비스 등의 서비스로도 확장할 수 있을 것으로 기대하며, 사용자 안전과 보안, 그리고 엔터테인먼트를 충족시킬 수 있는 기준을 제시할 수 있을 것이라 예상한다.

현 시스템은 차량을 가정한 일부 센서 및 서비스와 스마트폰을 이용한 프로젝트로 진행하였다. 하지만 IoT의 가속화로 스마트 기기들도 증가하는 추세이며, 스마트폰을 넘어 스마트 워치, 스마트 가전, 스마트 홈(Home)마저 등장하고 있다. 그렇기에 오픈소스 플랫폼, 사물인터넷 표준의 활용을 통해 개발한 현재 통합관리 시스템의 모듈을 확장한다면, 차량 - 사람뿐만 아니라, 사람과 상호작용이 가능한 모든 스마트 기기 안에 스마트 카(Car)도 포함시킬 수 있는 기회가 될 것이다.

참고문헌

- [1] 신현국, '자율주행차 시대, 인포테인먼트 발전방향', NIPA 이슈리포트, 2019-33호, 6쪽, NIPA(정보통신산업진흥원), 2019년
- [2] Joseph Vitale, '2020 Deloitte Global Automotive Consumer Study', 9쪽, Deloitte, 2020년
- [3] 정구민, 'CES 2019 자율주행 주요 동향', KISA REPORT, 2019 Vol.1, 28~29쪽, KISA(한국인터넷진흥원), 2019년

※ 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 SW중심대학사업의 연구결과로 수행되었음 (2015-0-00912)

VR 콘텐츠를 응용한 로잉머신 시스템의 설계 및 구현

반현진*, 윤다영*, 김재림*, 백세연*, 이나영*, 장영현*, 김정민**

*배화여자대학교 스마트IT과

e-mail: bhj0212@naver.com

Design and Implementation of Rowing Machine System using VR Contents

Hyun-Jin Ban*, Da-young Yun*, Jae-rim Kim*, Se-yeon Baek*,

Na-young Lee*, Young-hyun Chang*, Jung-min Kim**

*Dept of Smart IT, Baewha Women's University

**KT

요 약

본 연구에서는 4차 산업혁명의 핵심 분야인 가상현실을 헬스 엔터테인먼트 서비스에 응용하는 시스템을 개발하였다. 스마트폰에 내장된 GPS와 GYRO 센서를 활용하여 로잉머신의 동작 상태를 이중 데이터로 측정하고, 분석한 값을 활용해서 Unity를 사용하여 AR 어플리케이션을 설계, 구현하였다. 어플리케이션을 AR 글라스를 통해 실행한 결과, 생동감 넘치는 운동 환경을 사용자에게 제공한다. 그러나 사용자의 시각적 부담 과다로 인하여 로잉머신 운동효과 경험에 부분적 장애를 유발할 수 있어 2차적 개선으로 VR 콘텐츠로 전환을 적용하여 안전한 운동효과를 검증하였다. 본 연구의 VR 콘텐츠 개선기술을 적용하면 사용자 안전에 우선하는 헬스 엔터테인먼트 시장의 활성화가 기대된다.

1. 서론

4차 산업혁명에 대한 관심도가 높아지는 가운데 세계 경제포럼은 4차 산업혁명을 디지털, 바이오산업, 물리학 등의 경계를 융합하는 기술혁명이라고 정의하였다. [1] 미래창조과학부는 4차 산업혁명을 선도하는 핵심기술 중 하나로 가상현실을 선정하고 육성하기 위한 정책과 관련 사업을 시행한다고 밝혔다. 현재 가상현실은 다양한 분야에서 연구개발 및 여러 산업에 활용되고 있다. [2]

가상현실(Virtual Reality, 이하 VR)은 사실이 아니거나 사실이 분명하지 않은 것을 사실이라고 가정해서 생각하는 것을 의미한다. [3] 가상현실은 컴퓨터 그래픽으로 창조되는 가상의 공간이며, 가상의 공간을 현실이라 느끼며 실제로 활동할 수 있게 만드는 기술이다.

VR의 가장 큰 특징은 인위적인 세계로 끌어들여 자신도 모르는 사이에 가상의 세계에서 생활하고 있다는 것이다. 컴퓨터가 만들어낸 가상의 세계와 '나' 또는 'AI'가 상호작용을 하며 활동하는 것을 말한다. [4]

현재 VR 콘텐츠는 단순한 게임의 영역뿐 아니라 현실 세계의 환경과 접목하는 새로운 시장을 개척하고 있으며 화두는 '스포츠' 영역이다. 단순히 컴퓨터그래픽을 마우스를 통해 조정, 제어하는 것이 아니라 사용자 동작을 인식하여 사용자 동작에 따라 미리 계산된 운동 부하가 전달된다. 또한 다양한 가상현실 환경을 구현하여 가상의 세계에서 실제 사용자가 스포츠를 하고 있음을 체감시켜주는 엔터테인먼트라고 할 수 있으며, VR 콘텐츠가 발달함에 따라 실제 스포츠 상황을 재현하여 생동감 있는 체험이 가능해지고 있다.

VR 스포츠 시스템은 이용자를 컴퓨터 모션에 의해 개

발된 가상 환경에 몰입시킨 뒤, 실제 장비와 같은 형태를 사용함으로 신체의 근육을 이용해 운동 효과를 불러일으키는 행위를 의미한다.

증강현실(Augmented Reality, 이하 AR) 또한 실제 환경에 가상의 개체가 있는 것처럼 보이는 반 가상현실이다. 눈으로 보이는 실제 환경에 눈으로 보지 못한 컴퓨터 그래픽을 겹쳐서 보여주는 개념이다. VR 스포츠는 우리가 체험하지 못하는 가상의 세계라면 AR 스포츠는 사용자에게 실제 존재하는 환경과 가상의 그래픽을 합성한 기술이라고 할 수 있다. [5]

다양한 스포츠 종목들이 VR, AR과 접목되고 진화됨에 따라 경기장 및 경기 환경과 같은 제약이 사라지고, 다양한 공간에서도 경기장에 있는 듯한 효과를 얻을 수 있으며 사용자에게 생동감을 느낄 수 있는 신체활동을 가능하게 한다.

수많은 스포츠 중에서 다수의 사람이 애용하고 있는 헬스 엔터테인먼트는 VR, AR의 기술을 접목하여 비즈니스 활성화가 가능한 콘텐츠에서 빼놓을 수 없는 한 영역이다.

본 연구에서는 AR, VR 콘텐츠를 기반으로 신체적 안전 상태를 효율적으로 보장하는 헬스 엔터테인먼트 로잉머신 기반 AR, VR 어플리케이션을 설계, 구현한다.

2. AR, VR 로잉머신의 기능과 효과 분석

2.1 로잉머신 요구사항

헬스 엔터테인먼트의 종류는 다양하나 본 논문에서는 로잉머신을 기반으로 연구, 개발한다.

로잉머신은 조정선수들이 동계 혹은 악천후 시 실제 배

를 타지 못할 경우 실내에서 훈련을 할 수 있게 만든 실내 조정기구로, 날씨와 장소에 구애받지 않고 훈련을 할 수 있는 운동기구다. 최초에는 훈련을 주목적으로 개발되었으나, 운동 효과가 검증되면서 일반인에게도 확대되고 있다.

국내 로잉머신 헬스 엔터테인먼트 시장은 소규모이며 실제 헬스 엔터테인먼트를 즐기는 국내 이용자들은 외국 회사의 로잉머신과 자체 지원하는 어플리케이션을 사용한다. 그러나 해외에서 개발된 어플리케이션인 관계로 언어의 장벽과 현지인 대상 공지사항과 이벤트 등에 참여가 어려운 관계로 100% 효율적인 사용과 활용 면에서 다수의 단점이 존재한다.

<표 1> 로잉머신 지원기능 비교

모델	가격	어플리케이션 연동	VR/AR 지원
컨셉2	130만원	○	○
샤오미 스마트 로잉머신	80만원	○	○
xr pro 2000	20만원	X	X

<표 1>은 다양한 로잉머신의 장단점에 대한 비교 분석이다. 대중적인 로잉머신을 비교, 분석하여 자체적인 제공 기능은 부족하나 보통의 사용자 환경을 고려하고 가성비를 최우선 조건으로 하여 상대적 가치가 우수한 "xr pro 2000"을 연구개발 장비로 선정하였다. 시중에서 시판 중인 VR을 응용한 로잉머신의 장단점과 기능을 분석한 후 xr pro 2000 로잉머신을 이용한 VR/AR 콘텐츠를 설계, 구현하였으며, 연구 결과 저렴한 가격에서도 질적 만족도와 신체적 안전도가 높은 품질을 보증하는 가성비 효과를 도출하였다.

2.2 로잉머신의 효과

로잉머신은 조정 선수들이 실내에서 조정을 연습하는 것을 목적으로 제작이 되었으나, 운동 연습뿐 아니라 다양한 효과를 지니고 있다.

첫 번째, 로잉머신을 활용하는 것은 무릎이나 발목에 무리를 최소화하는 저 충격 운동임에도 사용자가 높은 칼로리를 소모하도록 한다는 장점이 있다. 전신의 근력을 이용하는 운동으로 지방 연소에 뛰어난 유산소운동의 효과를 볼 수 있다. 로잉머신은 심폐기능, 근력, 근지구력이 요구되며, 전신 근육을 사용하기에 신체 일부분의 근력이 아닌 전신 근력에 영향을 준다는 강점을 지닌다.

두 번째는 동일한 동작을 반복적으로 실행하며, 올바른 자세를 유지하면서 재활 측면에서도 도움이 된다는 강점을 지닌다. [6]

3. VR 로잉머신의 설계 및 구현

3.1 개발환경

본 논문에서는 로잉머신 기반 어플리케이션(Application)을 개발하고 사용자에게 가상의 세계, VR 환경을 제공한다. VR/AR을 사용하는 효율적 개발환경을 구성하기 위하여 아래의 <표2>를 통하여 Unity, Android Studio, Smart Maker에 대한 8가지 개념을 비교 분석하였다.

<표 2> VR 로잉머신 개발환경 비교

구분	Unity	Android Studio	Smart Maker
개요	3D/2D 게임 개발엔진	안드로이드 어플리케이션 개발 엔진	쉬운 앱 개발 엔진
언어	C#	JAVA, C#	자연어
오픈 소스	많음	많음	적음
디자인 자유도	높음	높음	낮음
지원 플랫폼	ios, Andriod 등 27개	Android 등	Android, ios
AR/VR 구현 개발	쉬움	어려움	불가능
난이도	보통	어려움	쉬움
최종안	○	△	X

VR/AR에 유연한 개발환경을 제공하는 Unity를 기반으로 어플리케이션을 제작하여 패키징 후 스마트폰에 배포하여 사용자에게 VR 환경을 제공한다. Unity는 세계 1위의 VR/AR 개발도구이며 Youtube와 Git hub 등 다양한 매체에서 Unity를 활용한 VR 기술 구현 방법론을 공유할 수 있으며, <표 2>와 같이 타 개발환경보다 양호한 개발 작업이 가능하다.

어플리케이션 개발환경 최상의 특징은 가상세계에서 중요한 역할을 하는 그래픽 처리 수준이 타 개발환경보다 탁월하다는 것이며 개발환경 내에서 존재하는 예셋 스토어를 활용하면 다양한 3D 모델, 텍스처와 파티클을 받을 수 있고, 튜토리얼을 통해 부족한 부분에 대한 보완이 가능하다.

3.2 어플리케이션 설계 방안

2개의 어플리케이션을 제작하여 로잉머신 VR을 구현한다. 첫 번째는 로잉머신에 부착하여 데이터 측정을 목적으로 하는 어플리케이션과 두 번째는 VR 글라스와 연결하여 사용자에게 VR 그래픽 이미지를 제공하는 어플리케이션이다. Unity를 이용하여 제작되며, 측정 어플리케이션에

서는 데이터를 송수신하기 위한 센서를 사용하므로 Unity 에 센서를 연동하여 구현한다.

본 연구에서는 <표 3>의 4가지 센서 중 로잉머신이 적용 기능상 비교우위를 가진 GPS와 GYRO, 2개의 센서를 사용하며 GPS의 로잉머신의 팔운동에 의한 이동 위치와 운동 중 신체의 수평 기울기의 차이를 이용하는 GYRO 센서를 응용하여 적용한다. 2개의 센서는 송신데이터 수집의 상호 보완 차원에서 비교, 분석하며 적용된다. 사용자가 로잉머신을 기준으로 이동성향의 데이터와 기울기를 기반으로 하는 수평 차이 자료를 동시에 측정하고 상호 보정하여 운동 상태 데이터를 확정하고 적용하여 시간에 따른 속도와 칼로리를 계산한다.

<표 3> 로잉머신 센서 기능 비교

센서	자이로 센서	GPS 센서	와이파이 무선 센서	유선 센서
개요	사용자의 움직임을 인식하기 위한 핵심 역할	위치를 좌표값으로 계산하므로 복잡한 계산이 필요 없음	거리 측정이 어려움	운동할 때 선으로 인해 불편할 것으로 예상되며 거리 측정 어려움
특징	이미 상용화가 많이 됨	GPS 센서를 장착한 스마트 기기가 보편화 됨	많은 데이터 송수신과 빠른 속도가 필요한 경우 사용	전력선이 존재함
장점	1) 앱 활용에 유용 2) 효과적인 시뮬레이션 가능	사용자의 위치를 좌표값을 이용해 간단한 계산이 가능	선없이 인터넷이나 상호간 통신이 가능	유선에 비해 가격이 저렴 전력선 외에 통신선로가 필요 없음
단점	1) 실제 값과 비슷하지만 누적오차가 발생할 수 있음 2) 데이터 처리가 힘들	1) 건물 내부와 지하에서는 전파를 받지 못함 2) 사용자의 위치를 타인에게 노출시킬 수 있어 정보 보안 측면에서 위험	1) 비용이 높음 2) 하드웨어와 소프트웨어 구성이 필요함	1) 보이는 선의 정리가 필요 2) 움직임의 제한이 있음
비고	△	○	×	×

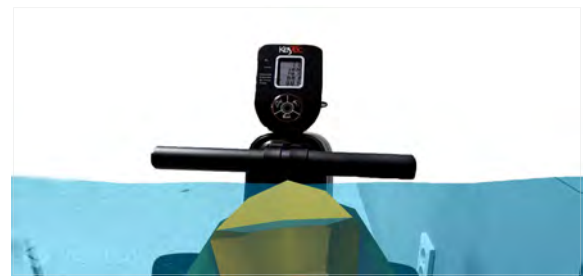
GPS 센서로 로잉머신의 시작 전 위치를 스타트 위치로 잡고, 사용자가 로잉머신의 손잡이를 잡아당기고 멈춘 위치를 라스트 위치로 잡아 거리를 계산하며, 계산된 거리를 누적하여 최종 거리를 계산하는 방식으로 어플리케이션을 구현하였다. 1차 측정값의 오차범위를 축소하기 위하여 GYRO 센서의 기울기 값을 적용하여 운동 횟수를 측정하고 적용한다. GPS와 GYRO 센서의 이중화 측정값의 상호 작용으로 정확한 운동 상태만을 제어하여 측정할 수 있으므로 다양한 운동 환경에서 발생할 수 있는 로잉머신의 이동과 충격에 따른 임의의 값의 송수신을 방지 할 수 있다.

두 번째 개발 기능은 가상세계를 연결하는 어플리케이션으로 VR 글라스에 스마트폰을 연결하여 사용자에게 가상의 공간을 보여주어 실제 존재하는 환경에서 운동하는 감각과 느낌을 인식할 수 있다. 스마트폰의 카메라 기능을 활용하여 이미지를 인식한 후, 인식된 이미지에 설정되어 있던 가상의 공간을 제공하고 보여준다.



(그림 1) 연구용 AR 글라스

위의 (그림 1)과 같이 어플리케이션을 설치한 스마트폰을 AR 글라스에 연결, 착용하여 사용자에게 가상의 환경에서 로잉머신 운동을 할 수 있게 한다.



(그림 2) AR 글라스 기반 로잉머신 AR 동작 화면

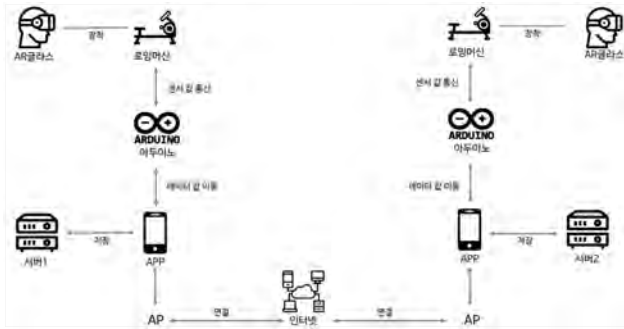


(그림 3) AR 글라스 기반 로잉머신 VR 동작 화면

AR 글라스에 스마트폰을 연결하여 설정된 이미지를 인식하면 위의 (그림 2)와 같은 가상의 공간을 사용자에게 제공된다. 그러나 오브젝트와 달리 배경이 현실이기에 사용자에게 시각적으로 빠르게 지루함을 느낄 수 있어 사용자 경험에 장애가 발생할 확률이 높아진다. 따라서 장애적 요소의 문제점을 해결하기 위하여 임시로 VR로 전환하여 인간 신체의 시간 요소에서 발생하는 장애적 요소를 제거하면 (그림 3)의 동작 화면으로 눈의 컬러 보정에 정상적으로 적용한다.

3.3. NEXT VR 로잉머신 개발

NEXT VR 로잉머신은 (그림 4)와 같이 서버를 연계하여 사용자가 AR 글라스를 착용한 상태에서 가상의 환경을 보며 로잉머신을 이용하고, 아두이노 센서를 통해 측정값을 휴대폰 어플리케이션으로 전송한다.



(그림 4) NEXT VR 로잉머신 구성도

전송데이터를 분석하여 로잉머신의 운동 시간, 소모 칼로리 등을 확인할 수 있으며 인터넷 AP로 연결하여 다른 사용자와 함께 게임 상태로 운동할 수 있도록 개발할 계획이다.

4. 결론

본 논문에서는 VR 콘텐츠를 기반으로 하여 헬스 엔터테인먼트를 이용 시 생동감을 주는 시스템을 설계 및 구현하고 데이터를 측정, 분석하였다.

다소 아쉬운 점은 완벽한 VR을 기반으로 어플리케이션을 설계, 구현하고자 하였으나, 세미 AR 기반 어플리케이션으로 연구를 마무리하였다는 점이다. 이는 향후 추가적인 환경 개발을 통해 VR로 변경해 나갈 것이다. VR 환경으로 변경될 경우, 더욱 다양한 가상의 공간을 설계, 구현할 것이며, 이를 통해 어플리케이션을 이용하는 사용자가 원하는 가상공간의 형태를 선택하여 운동에 참여가 가능해질 뿐 아니라 많은 사용자의 참여를 유도할 수 있을 것이다.

또한 리듬에 맞춰 로잉, 다른 사용자와 연결하여 진행하는 로잉 게임, 데이터 기록의 시각화 기능을 추가 구현하게 되면 엔터테인먼트로서의 활용도가 증가 될 것이며 시간의 변화에 따른 사용자의 신체 능력의 향상을 확인할 수 있을 것이다. 이는 다른 어플리케이션과 차별화된 점을 두어 하나의 획기적인 서비스가 될 것을 예측해 볼 수 있다. 이와 같은 추가적인 기능을 설계 후 구현하는 것이 앞으로 보완해야 할 과제이다.

참고문헌

- [1] 김가람, "효과적인 VR 연동 액추에이터 제어를 위한 가이드라인 제안 및 구현", 숭실대학교 석사학위논문, 2017
- [2] 네이버 뉴스, <https://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=105&oid=029&aid=0002394451>, 2017
- [3] 표준국어대사전
- [4] 이수직, "가상현실 스포츠 이용 동기 및 서비스요인이 여가만족에 미치는 영향:스크린골프 중심으로", 세종대학교 석사학위논문, 2011
- [5] 신동경, "VR/AR 스포츠 참여동기, 지각된 가치 만족: 스크린테니스 이용자를 대상으로", 고려대학교 석사학위논문, 2019
- [6] Azuma, R.T, "A survey of augmented reality. Teleoperators and Virtual Environments", 1997
- [7] 백은채, "실내조정 운동 프로그램이 발달장애 학생의 건강체력에 미치는 효과", 한국체육대학교 석사학위논문, 2017

본 논문은 과학기술정보통신부 정보통신창의인재양성사업의 지원을 통해 수행한 ICT멘토링 프로젝트 결과물입니다.

스마트홈 환경에서 AR기술을 활용한 슬립테크 제어 방법

차성민⁰, 배수민*, 박현주*, 이재동*

⁰단국대학교 소프트웨어학과

*단국대학교 소프트웨어학과

32154579@dankook.ac.kr⁰, 32152076@dankook.ac.kr*, 32152006@dankook.ac.kr*,

letsdoit@dankook.ac.kr*

Method of Sleeptech control using AR in Smart home environment

Seong-Min Cha⁰, Su-Min Bae*, Hyeon-Ju Park*, Jae-Dong Lee*

⁰Dept. of Software Engineering

*Dept. of Software Engineering

요 약

최근 스마트 홈에서 슬립테크를 제어할 수 있는 어플리케이션 개발 및 연구의 필요성이 높아지고 있다. 기존 스마트 홈 제어 어플리케이션들은 텍스트 형식의 UI, 직관적인 정보 제공의 부재, 스마트 스위치 수준의 서비스 제공 등의 문제점을 가지고 있다. 이러한 문제점을 개선하기 위해 본 논문에서는 증강현실과 3D 모델링을 통해 스마트 홈을 보다 직관적이고 편리하게 사용할 수 있는 슬립테크 제어 방법을 제안한다.

▶ Keyword : 증강현실(Augmented Reality), 스마트 홈(Smart home), 슬립테크(Sleep Tech)

I. Introduction

4차 산업혁명 시대가 도래함에 따라 AI, IoT, VR/AR 등의 기술 발전이 이루어지고 있으며 특히 스마트 홈 시장 규모는 나날이 커져가고 있다. 이제 스마트 홈은 가전제품과 사물인터넷 연결에서 더 나아가 고도화된 기술로 사용자 맞춤형 서비스로 진화하고 있다.

따라서 본 논문에서는 현재 기존의 스마트 홈 제어 어플리케이션이 가지는 직관성, 편의성 등의 문제점을 해결하고 사용자에게 보다 친숙한 스마트홈 환경을 제공할 수 있는 AR를 활용한 슬립테크 제어 방법을 제안하였다. 또한 증가하는 수면 장애 환자들을 위해 수면에 도움이 될 수 있도록 슬립테크 기능을 증강현실과 모션 베드를 이용해 제어할 수 있는 스마트 홈 어플리케이션 시스템을 제안한다.

II. Background

2.1 스마트홈(Smart home)

주거 환경에 정보 기술이 융합되어 거주자의 편리, 복지, 그리고 안전 중심의 생활을 가능하게 하는 스마트

라이프 환경을 스마트 홈(Smart Home)이라고 정의한다. 스마트 홈 네트워크와 연결된 가전제품들을 통해 제공되는 다양한 맞춤형 콘텐츠와 스마트 홈 서비스는 지속적으로 확대되고 있다.[1]

2.2 슬립테크(Sleep tech)

슬립테크(Sleeptech)란 ‘Sleep(수면)’과 ‘Technology(기술)’의 합성어로, 첨단 기술을 활용해 수면관련 데이터를 분석하고 수면을 돕는 기술을 일컫는다. 현재 성인의 하루 적정 수면 시간은 8시간이지만 실제로는 약 40%가 이보다 적은 7시간미만의 잠을 자고 있는 실황이다.[2]

2.3 증강현실(Augmented Reality)

AR은 실제 환경에 컴퓨터 모델링을 통해 생성한 가상의 물체(물체, 텍스트, 비디오)를 겹쳐 보이게 하여 공간과 상황에 관한 가상정보를 제공하는 시스템 및 기술이다. AR은 다음과 같은 특징들을 가지고 있다.

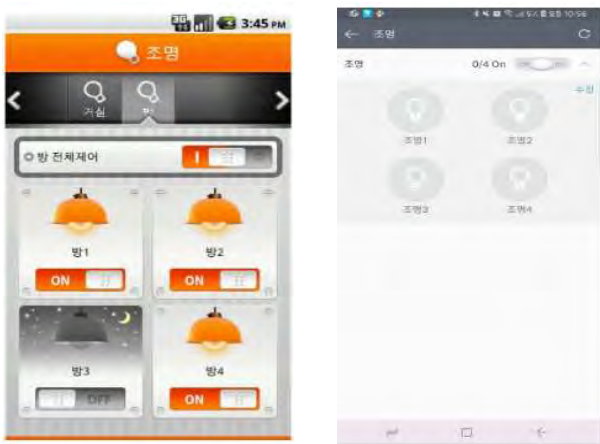
먼저, 사용자가 촉각과 후각 등의 감각을 확장하고 참여자로서 이용할 수 있고 사물을 직접 체험하고 싶은 인간의 원초적 욕구를 가장 잘 충족시켜줄 수 있다는 점이 있고[3], 다음으로, 다양한 사물들에 대한 추가적인 정보를 제공할 수 있다는 점과 높은 몰입도를 요구하는 공간구성에서의 콘텐츠로 활용이 가능하다는 점이 있다[4].

III. Proposed method of Sleeptech control using AR

3.1 Necessity of research

본 논문에서는 스마트홈과 슬립테크를 증강현실을 통해 제어할 수 있는 어플리케이션을 만들어 3가지의 문제점을 해결하는 것을 목표로 한다.

첫 째, <그림 1>과 같이 가장 큰 문제점인 텍스트 형식의 UI와 이에 따른 직관적인 정보 제공의 부재를 모델링을 통해 관리할 수 있게 하여 해결한다.



<그림 1> 기존 스마트폰 어플리케이션

둘 째, 늘어나는 수면장애 환자들로 인해 나날이 중요해지는 슬립테크를 스마트홈에 접목시키고, 이를 증강현실을 통해 제어할 수 있는 환경을 만들어 수면장애 문제를 해결한다.

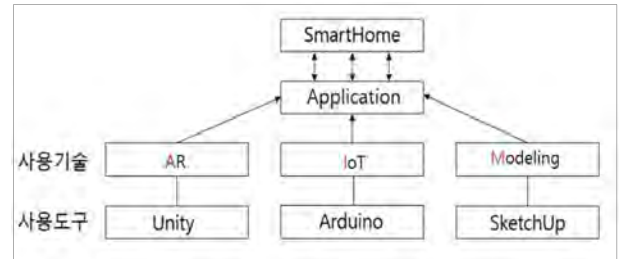
마지막으로, 카메라 화면을 통해 인식만 시키면 정보들이 그래픽으로 화면 UI에 나타나 전 연령대 모두가 사용하는데 불편함이 없는 체험 및 실감형 콘텐츠를 만든다.

위와 같은 3가지의 문제점을 증강현실 기술을 사용하여 해결하는 것을 목표로 하며, 증강현실을 사용하는 이유는 다음과 같다.

1. 다양한 사물들에 대한 추가적인 정보를 제공해줄 수 있다.
2. 높은 몰입도를 요구하는 공간구성에서의 콘텐츠로 활용이 가능하다.
3. 사용자가 촉각과 후각 등의 감각을 확장하고 참여자로서 이용할 수 있다.
4. 사물을 직접 체험하고 싶은 체험형, 실감형 콘텐츠를 제공한다.

이처럼 크게 4가지 증강현실의 특징 점을 활용하여 이를 스마트홈과 슬립테크에 적용시켜 제어하는 어플리케이션을 개발한다.

3.2 Development Environment



<그림 2> 스마트 홈 구조도

<그림 2>는 스마트 홈 시스템에 사용되는 구조도이다. 사용하는 기술은 크게 AR, IoT, Modeling 3가지로 구분된다. 조명, 침대 등을 카메라 화면을 통해 스캔을 하면 각종 정보가 UI에 그래픽으로 제공되는 AR을 Unity를 이용하여 구현하고, 스마트 홈 모형에 부착되는 각종 센서들(IoT)은 Arduino를 이용하여 구현한다. 또한, 3D 기반의 집 모델링이 화면에 나와야하기 때문에 이를 3D 설계 소프트웨어인 SketchUp 툴을 이용하여 제작 및 구현한다.

3.3 Development Process

3.3.1 Production of 3D modeling

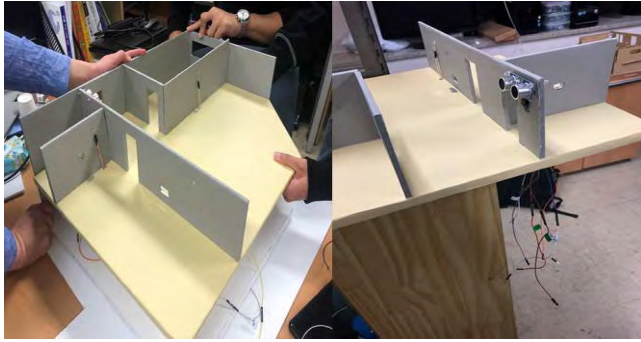


<그림 3> 스마트 홈 모델링

본 논문에서는 스마트 홈을 어플리케이션을 통해 제어할 수 있도록 실제 스마트 홈 모형과 같은 모델을 스마트폰 어플리케이션 안에 구현하기 위해서 3D 설계 소프트웨어인 SketchUp 툴을 이용하여 스마트 홈 내부 구조를 3D 모델링으로 <그림 3>과 같이 제작한 후에 스마트폰 어플리케이션에 적용하였다.

3.3.2 Producing of Real model

어플리케이션을 제작한 후 단순히 어플리케이션 상에서만 구동되는 것이 아니라 실모형에서도 작동함을 보여주기 위하여 우드락과 폼보드와 아두이노와 센서들을 이용하여 실제모형을 제작한다.



<그림 4> 실제 모형 제작과정

<그림 4>는 우드락, 폼보드, 아두이노를 이용하여 실제모형을 제작하는 모습이다.

효율적인 배선을 위하여 사전에 미리 수치를 측정하고 공간에 여유가 있도록 설계한다. 이후 설계한 장소에 맞춰 아두이노와 센서들 배선 및 설치한다.

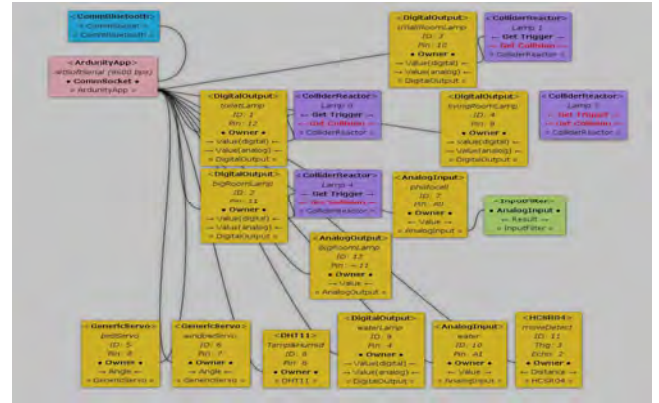
3.3.3 Producing of Application



<그림 5. 유니티 제작 화면>

<그림 5>는 유니티를 통해 어플리케이션을 제작하는 모습이다. 3D모델링과 증강현실 기술의 사용을 위해 유니티를 기반으로 어플리케이션을 제작한다. 유니티를 통해 UI제작, 3D 모델링 제어, 아두이노 센서 제어 등을 구현한다.

Sketchup을 이용해 만든 3D 모델링을 유니티로 가져오고 실제 모형에 부착되어 있는 아두이노 센서들을 제어하기 위해 ‘아두니티’ 툴을 사용한다.



<그림 6> 아두니티 구성 화면

<그림 6>은 아두니티의 구성모습을 나타낸 화면이다. 그림 6.을 이용하여 유니티 상에서 아두이노를 제어할 수 있게 한다. 마지막으로 유니티를 이용해 안드로이드 앱 빌드를 하여 안드로이드 환경에서 어플리케이션이 구동될 수 있도록 한다.

3.4 User Interface



<그림 7. 어플리케이션 UI>

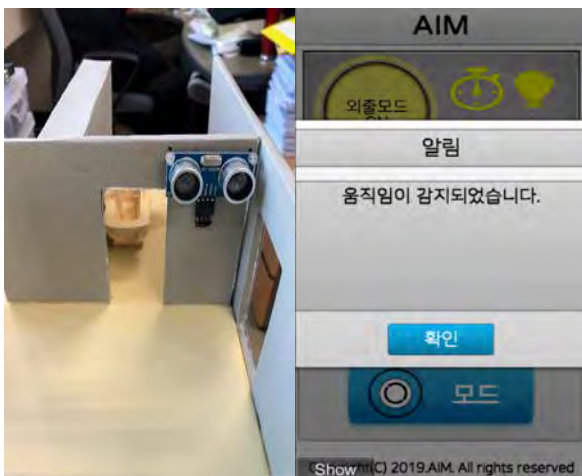
<그림 7>은 어플리케이션을 실행했을 때 가장 먼저 나오는 화면으로, 블루투스를 연결하여 로그인을 통해 홈 화면인 가운데 보이는 UI로 이동을 하게 된다. 홈 화면에서 모드 변경을 통해 재택모드와 외출모드로 변경을 할 수 있고, 스캔을 눌러 카메라로 화면을 전환시킬 수 있다. 모델을 누르면 오른쪽에 보이는 UI와 같이 3D 모델링을 통해 만든 집 모델이 화면에 나타나게 되고 조명, 창문 등 각종 센서들을 터치를 통해 제어할 수 있다.

3.5 Control of Smart home & Sleep tech



<그림 8> 어플리케이션을 통해 제어

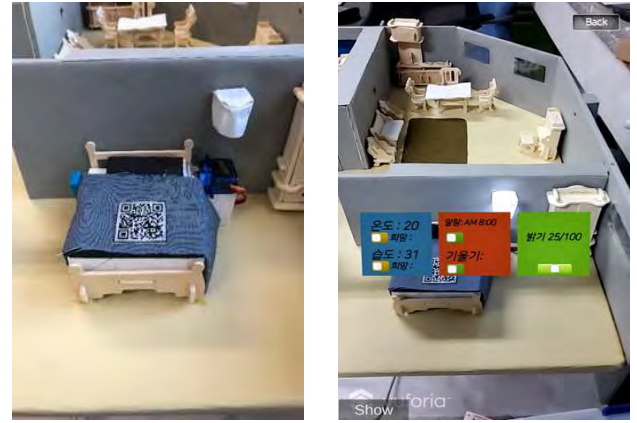
<그림 8>은 창문에 서보모터와 조도센서를 결합해 구현한 모습이다. 오른쪽 앱 실행화면에서 창문을 터치하면 자동조절 및 수동조절 창이 뜨게 되고 밑의 스크롤바를 조절하여 창문을 열거나 닫을 수 있다. 자동 조절을 터치하게 되면 설치된 조도 센서가 활성화되어 빛의 양에 따라 창문이 자동으로 열리거나 닫히게 된다.



<그림 9> 움직임 감지 센서와 알림

<그림 9>는 움직임 감지 센서이며 앱의 홈 화면에서 모드 선택을 통해 제어할 수 있다. 모드에는 재택 모드와 외출 모드가 있으며, 외출 모드 선택 시 움직임 감지 센서가 활성화되어 움직임이 감지되었을 경우 앱에 알림이 뜨게 된다.

<그림 10>은 침대에 온습도센서, 서보모터, LED를 결합하여 구현한 모습이다. 침대의 경우 증강현실 기술을 이용해 제어할 수 있으며 침대 스캔 시 오른쪽에 보이는 화면처럼 온습도, 알람, 기온기, 밝기를 제어할 수 있는 그래픽이 나오게 된다. 원하는 항목을 터치하여 세부 조절을 할 수 있다.



<그림 10> 증강현실 기반 제어

데모영상 URL :

https://drive.google.com/open?id=1nk3fGGsJ5YBfdQDTCVqhGX_nHF8viTp2

IV. Conclusions

증강현실을 활용하여 스마트 홈 및 슬립테크를 제어하는 어플리케이션을 제작함으로써 기존 스마트 홈 어플리케이션의 문제점인 직관성 부족의 문제를 해결하였다. 또한, 모션베드 제어를 하는 슬립테크 기술을 도입하였고, 이 과정에서 증강현실을 사용하여 스캔만 하면 필요한 정보가 화면에 나타나도록 하여 전 연령대가 사용할 수 있는 체험 및 실감형 콘텐츠를 제작하였다.

이를 기반으로 하여 향후엔 신분이 인증이 된 관리자들이 유용하게 사용할 수 있을 스마트빌딩 관리 시스템을 만들고 실제 업체들과의 협업을 통하여 실 적용까지 해볼 계획이다.

"본 연구는 과학기술정보통신부 및 정보통신기획평가원의 글로벌핵심인 재양성지원사업의 연구결과로 수행되었음(2019-0-01577)"

References

- [1] Ji-One Park. "A Study on the Product Use Patterns and Smart Hub of Smart Home User in the Near Future" (2020)
- [2] Hyeong-Min Lee, "Technology and innovation". Vol. 426, pp.69-71, (2019)
- [3] Ji-Sun Yang, "A Study on the Improvement of User Experience in the Mobile AR Interior Content according to the Theory of Attendance"(2019)
- [4] Jung-Yeob Han, 'Features of Types and Content-design of Mixed-reality-based Devices', Journal of the Korea Institute of the Spatial Design, vol. 10,no. 2, pp. 63-72, (2015)

규칙엔진 기반 인터랙티브 디지털 사이니지 서비스 시스템 설계 및 구현

신은규* 정선태** 이주호*

*송실대학교 대학원 정보통신공학과

**송실대학교 스마트시스템소프트웨어학과

tlsdmsrb0427@soongsil.ac.kr, cst@ssu.ac.kr, juho1504@soongsil.ac.kr

Design and Implementation of Interactive Digital Signage Service System based on Rule Engine

Eun-kyu Shin*, Sun-Tae Chung**, Ju-ho Lee*

*Dept. of Information and Telecommunication Eng., Graduate School, Soongsil University

**Dept. of Smart Systems Software, Soongsil University

요 약

센서/외부사건 연동을 지원하는 인터랙티브 디지털 사이니지(Interactive Digital Signage)가 활발히 전개되고 있다. 그런데, 현재 전개되고 있는 대부분의 인터랙티브 사이니지 시스템은 정해진 인터랙션에만 맞추어 설계되어 지원되기 때문에, 추가적인 인터랙션 기능이 요구되는 경우에 재프로그래밍하여야 한다. 다양한 센서 입력, 외부사건 발생 등에 대한 반응을 유연하게 지원하는 데 있어서 규칙엔진 지원이 유용하다. 본 논문에서는 규칙 메타데이터 변환 및 이의 규칙엔진과의 동기화 방안을 제시하고, 이를 활용하여 다양한 센서/외부사건 연동 인터랙션을 유연하게 지원하는 규칙엔진 기반 인터랙티브 디지털 사이니지 시스템의 설계 및 구현을 보고한다.

1. 서 론

디지털 사이니지(Digital Signage)는 네트워크를 통해 원격제어가 가능한 디지털 디스플레이 기기를 공장소나 상업 공간에 설치하여 정보, 엔터테인먼트, 광고 콘텐츠 등을 제공하는 디지털 미디어를 뜻한다. 디지털 사이니지 기반의 콘텐츠는 블루투스, NFC, 영상처리 기술들의 발달에 따라 사용자와의 양방향 커뮤니케이션(Communication)이 강화되고 있으며, 또한 사용자의 성별, 나이, 위치 등을 인식하여 사용자 맞춤형 서비스를 제공하는 콘텐츠(Contents)가 증가하고 있다. 디지털 사이니지가 지속적인 경쟁력을 가지기 위해서는 단순한 콘텐츠 재생 지원을 넘어 시간과 공간 그리고 다양한 고객 상황에 맞는 인터랙티브 맞춤형 콘텐츠 재생 서비스를 제공해야 할 필요가 있다[1]. 그런데, 현재에 전개되고 있는 대부분 센서 연동 지원 인터랙티브 디지털 사이니지 시스템에서는 센서가 연동되었을 경우, 센서의 값과 센서값에 따라 실행될 액션을 고정적으로 대응(Mapping)시키는 방식으로 프로그래밍이 되어 구현하고 있다. 이 방식은 센서 연동 액션의 변경이나 새로운 센서의 추가적 연

동을 지원하기 위해 재프로그래밍하여야 하는 한계가 있어 유연한 시스템 운용이 힘들다.

인터랙션은 센서 입력 및 외부사건 알림이 발생했을 때 적절한 반응(액션)을 제공하는 것인데, 다양한 경우의 사건 발생과 해당 반응을 'if(등록 지정 센서/외부사건 입력 발생), then(상응하는 액션(함수) 수행)'이라는 규칙으로 기술하고 이러한 규칙들이 수행하도록 지원하는 규칙엔진[2]을 활용하면, 기존 인터랙티브 디지털 사이니지 시스템의 고정된 방식을 벗어나 사이니지 시스템이 설치된 장소 및 여러 고려 사항에 맞는 인터랙션을 지원할 수 있다.

본 논문에서는 다양한 인터랙션 동작 환경을 유연하게 지원하는 인터랙티브 사이니지 시스템을 규칙엔진을 활용하여 구현한 개발 내용을 보고한다.

2. 배경이론

2.1 규칙엔진

조건부 및 루프가 포함된 일련의 명령으로 구성된 명령형 프로그래밍 모델과는 다르게, 규칙엔진은, 시스템이 수행하여야 할 작업을 데이터에 대해 'if(조

건)-then(액션)'으로 구성되는 규칙(rule)을 수행함으로써 이루어지도록 지원한다. 규칙이 서술된 순서에 상관없이 규칙엔진이 언제 어느 규칙이 수행되어야 하는지를 결정해서 수행해준다. 규칙이 충돌 날 때는 이를 해결하여 어느 규칙이 먼저 수행되어야 하는지 또는 어느 규칙만을 수행하여야 하는지도 결정해준다. 규칙엔진의 중요한 특성은 체인닝(chaining)이다. 한 규칙의 액션 부분이 다른 규칙의 조건 부분 값을 변경하는 방식으로 시스템 상태를 변경한다. 체인은 더 복잡한 행동을 지원하기 때문에 매력적으로 들리지만 추론하고 디버그하기가 매우 어려울 수 있다.

2.2 JSON JavaScript Rule Engine ;

“json-rules-engine”

본 논문에서 채택한 규칙엔진은 가볍지만 강력한 “json-rules-engine”[3]으로 웹브라우저와 node.js 에서 모두에서 수행될 수 있다. 본 논문에서 사용하는 사이니지 플레이어는 chromium 과 node.js 로 구성되는 Electron 플랫폼 기반의 응용으로, “json-rules-engine”과의 통합 적용은 어렵지 않다.

“json-rules-engine”에서의 규칙은 일련의 조건과 단일 이벤트(액션의 역할을 함)가 포함되며, 이들 규칙은 JSON으로 기술된다. 엔진이 실행될 때 각 규칙 조건이 평가되며 평가결과가 사실이면 등록된 이벤트가 트리거된다. 시스템은 해당 이벤트에 따라 정해진 액션을 수행하도록 처리할 수 있다.

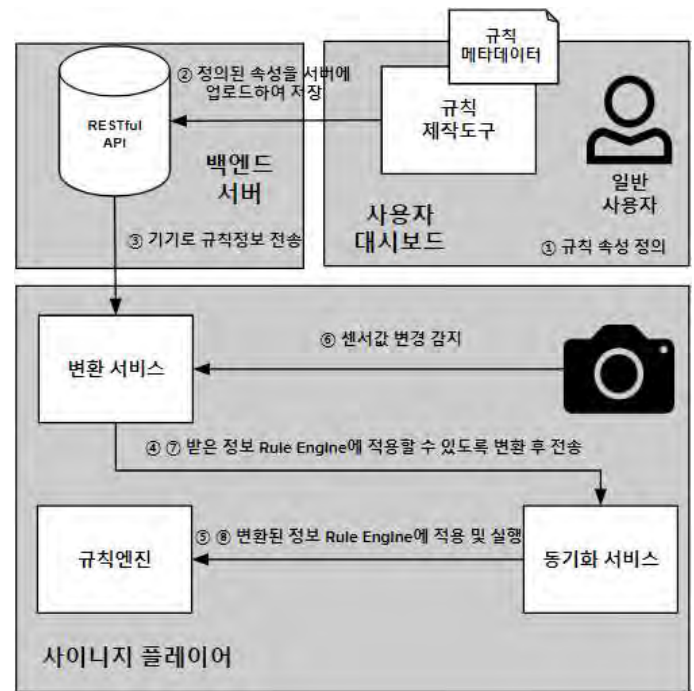
3. 제안 규칙엔진 기반 인터랙티브 사이니지

3.1. 동작 구조

〈그림 1〉은 대시보드에서부터 규칙 설정 및 사이니지 플레이어로 설정된 규칙과 이벤트들이 어떻게 적용이 되고 실행이 되는지를 보여주는, 본 논문의 규칙엔진 기반 인터랙티브 디지털 사이니지 시스템 동작 구조 개념도이다.

사이니지 시스템 사용자가 원하는 인터랙티브 상황 처리를 규칙과 이벤트를 웹 대시보드에서 설정하면, 대시보드는 이를 위한 규칙 메타데이터를 생성하고 (①) 이를 백엔드 서버(CMS)로 업로드한다(②).

서버는 연동된 사이니지 플레이어 기기로부터



<그림 1> 규칙엔진 기반 인터랙티브
디지털 사이니지 시스템 동작 구조

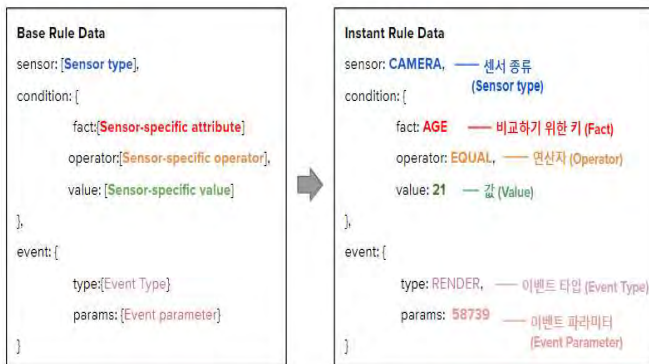
요청 시에 이를 전송한다(③). 전송된 메타데이터들은 규칙엔진에 적용하기 위한 형식으로 변환하기 위해 변환 서비스를 거쳐(④) 동기화 서비스에서 실질적으로 규칙엔진에 규칙으로 세팅한다(⑤). 이런 방식으로 규칙엔진에 사용자가 원하는 규칙과 이벤트가 설정되며 센서값 변동을 감지하였을 때(⑥), 변환 서비스는 이를 맞게 변환 후에 동기화 서비스로 전달하고(⑦), 동기화 서비스는 전달받은 변환된 정보를 규칙엔진에 전달하고(⑧), 규칙엔진에서는 전달받은 정보가 기설정된 규칙과 일치할 시 해당 액션(여기서는 주로 연관된 콘텐츠 렌더링)을 수행한다.

3.2. 규칙 메타데이터 생성

사이니지 시스템의 사용자 맞춤형 규칙과 이벤트를 작성하여 사이니지 시스템의 규칙엔진에 적용하기 위해서 대시보드가 필요하다. 본 논문에서는 대시보드를 웹으로 구현하였다.

구현된 웹 대시보드에서는 <그림 2>와 같이 백엔드 서버(CMS)의 Database에 저장되어있는 Base Rule Data를 기반으로 센서 종류, 센서의 변경된 값과 비교할 값, 값들을 비교하는 속성을 자유롭게 작성할 수 있으며, 이벤트에는 특정 광고화면을 표출하거나 웹 기반 디지털 사이니지를 기반으로 하였기 때문에 CSS 선택자(CSS Selector)를 변경시켜 현재 보이는

광고의 이미지 및 동영상 등이 크기 전환, 변경 등을 지정해 Instant Rule Data를 생성한다.



<그림 2> DB 데이터 기반
규칙 메타데이터 생성

3.3. 인터랙티브 사이니지를 위한 규칙엔진

동기화 구현

사이니지 시스템의 더욱 유연한 인터랙션을 지원하기 위한 규칙엔진 활용을 위해서 규칙엔진이 기존 사이니지 시스템과 동기화되어야 한다. <그림 1>의 동작 환경에서 동기화 구현 내용을 다음과 같은 인터랙션 시나리오를 통해서 설명하기로 한다.

- 획득된 고객의 얼굴의 성별과 나이가 판별되면 해당 고객에게 맞는 광고 내용을 디지털 사이니지 디스플레이 화면에 표출한다 -

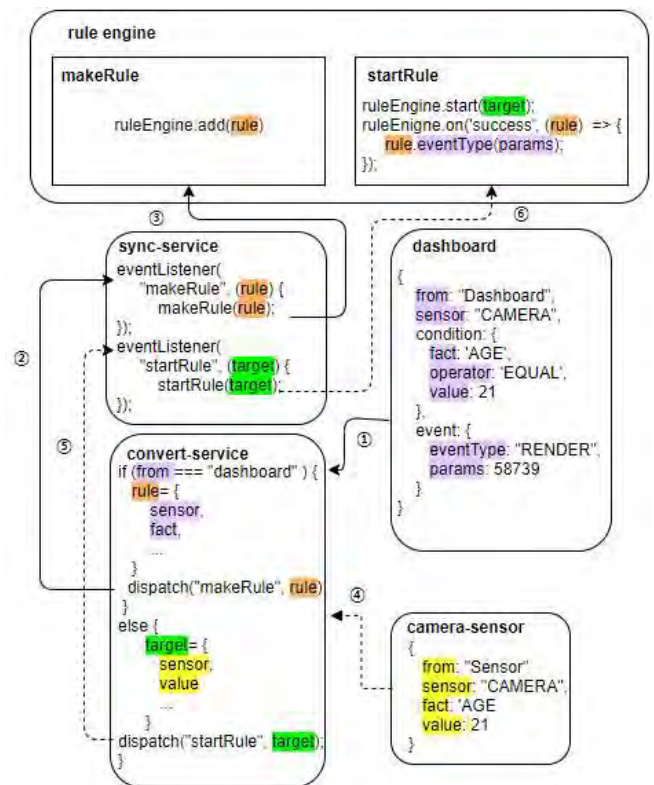
이러한 시나리오의 인터랙티브 사이니지를 지원하기 위해서는, 1) 획득한 얼굴 이미지로부터 성별과 나이를 추정하는 모듈과의 인터페이싱을 지원하는 센서연동 모듈, 2) 센서 입력값(여기서는 고객의 성별 및 나이 값)에 대해 적용할 규칙 및 이벤트처리 설계, 3) 설계되는 규칙과 이벤트처리를 설정할 대시보드 인터페이스, 4) 설정된 규칙과 이벤트 및 센서값의 변화를 사이니지 플레이어의 규칙엔진에 적용될 수 있도록 변환하는 변환 서비스 모듈, 5) 센서 입력 및 이벤트에 동기를 맞추어 규칙엔진을 실행시킬 동기화 서비스 모듈 등의 구현이 필요하다. 이 가운데, 본 논문에서는 규칙엔진 동기화 구현에 중요한 4) 변환 서비스 5) 동기화 서비스의 핵심 부분만을 간단히 기술한다.

규칙 메타데이터 및 센서 데이터의 효과적 전달을 위해 Web API인 CustomEvent[4]를 활용하였다. 변환 서비스 구현에서는 규칙 설정 메타데이터 및 센서 입력 처리 규칙 메타데이터 등을 CustomEvent로 구성하고, 'Dispatch'로 배포하도록 하였고, 동기화 서비스에서는 'eventListener'를 통해 캐치하고 해당

이벤트에 상응하는 규칙엔진의 규칙들을 구동되도록 한다. 이후 규칙엔진에서는 해당 규칙을 수행한다.

<그림 3>은 상기 시나리오에 따른 구현 및 동작 과정을 보여준다.

대시보드에서 센서에 맞는 규칙과 이벤트를 설정하면 변환 서비스(convert-service)에서 규칙과 이벤트를 규칙엔진에 적용할 수 있도록 변환하고 동기화 서비스를 통해 규칙엔진에 전달되어 규칙으로 등록되게 한다. 이후, 센서의 값에 변화가 발생하게 되면 동기화 서비스(sync-service)에서 센서의 값을 사이니지 시스템상의 값과 동기를 맞추어 규칙엔진이 구동되도록 하고, 규칙엔진은 해당 규칙을 실행한다. 해당 규칙은 해당 콘텐츠를 재생되도록 사이니지 플레이어의 렌더러가 호출되게 한다.



<그림 3> 사이니지 시스템과 규칙엔진 간 데이터
변환 및 동기화 구조

4. 구현 결과

상기 시나리오에 따라 사이니지 시스템과 규칙엔진의 통신 및 동기화를 구현하였으며, 최종적인 결과는 <그림 4>는 이를 보여준다. 대시보드 상에서 자유롭게 규칙과 이벤트가 설정한 후 사이니지 시스템에서 그 규칙이 일치할 시 설정된 이벤트가 표출된 것을 확인할 수 있다.

(대시보드)

(사이니지 시스템)



<그림 4> 규칙엔진 기반 인터랙티브 디지털 사이니지 시스템 서비스 구현 결과

향후 연구에서는 본 논문에서 가능한 내용뿐만 아니라 기존 사이니지 시스템에 연동되어있지 않은 센서와 이벤트라도 규칙엔진에 적용하기 위한 변환 및 동기를 맞출 수 있도록 설계를 하여 유연성 있는 사이니지 시스템에 맞는 연구가 진행될 것이다. 그리고 더 나아가 본 논문에 제안된 기술이 적용된 사이니지 시스템들이 배포되고 사용될 수 있도록 응용 이벤트 및 다양한 규칙들을 적용할 수 있는 대시보드 설계 방법에 관한 연구 및 개발을 진행할 예정이다.

참 고 문 헌

- [1] 채송화, “디지털 사이니지(Digital Signage) 기반 콘텐츠 산업의 현황과 전망”, 한국콘텐츠진흥원 코가포커스 통권 54호, pp.1~22, 2012
- [2] Rule-based System, https://en.wikipedia.org/wiki/Rule-based_system
- [3] json-rules-engine, <https://www.npmjs.com/package/json-rules-engine>
- [4] MDN, CustomEvent, <https://developer.mozilla.org/ko/docs/Web/API/CustomEvent/CustomEvent>

5. 결론 및 향후 연구

본 논문에서는 규칙엔진 기반 인터랙티브 디지털 사이니지 시스템 설계 및 구현 방안을 제안하였다. 다양한 동작 환경에서의 인터랙션을 보다 유연하게 지원하기 위하여 규칙엔진을 활용하였으며, 활용한 규칙엔진과 기존 사이니지 시스템과의 연동을 위한 대시보드 인터페이스, 플레이어에서의 규칙 메타데이터의 기존 사이니지 플레이어에서의 효과적 처리를 변환 및 동기화 구조 설계를 제시하였다. 본 논문에서 제안한 규칙엔진 기반 인터랙티브 디지털 사이니지 시스템의 효과적 동작을 확인하였다.

환경 모니터링을 위한 EDA 기반 데이터 분석

강윤희*, 조재혁**

*백석대학교 ICT학부

**숭실대학교 전자정보공학부

yhkang@bu.ac.kr, chojh@ssu.ac.kr

EDA based Data Analysis for Environmental Monitoring

Yunhee Kang*, JaeHyuk Cho**

*Div. of ICT, Baekseok University

**Dept. of Electronic Eng., Soongsil University

요 약

최근 센서데이터 활용 영역이 넓어지면서 데이터 분석 서비스가 활성화되고, 분석을 용이하게 할 수 있는 환경으로 진화하고 있다. 이에 따라 센서데이터의 신뢰성 보장이 필요하다. 신뢰성을 갖는 환경모니터링을 위해서는 센서로부터 수집된 환경 데이터의 분포 및 값을 살펴본 후 데이터가 표현하는 현상을 더 잘 이해하고, 센서 및 센서데이터에 대한 잠재적인 특이점을 발견을 진행하여야 한다. 이를 위해 EDA를 통해 수집된 센서 값을 시각화하고 분석에 주어진 데이터의 개별 속성의 특징 및 상관관계를 도출한다. 본 연구의 EDA 분석 결과는 센서데이터의 신뢰성을 평가하기 위해 사용한다.

1. 서론

최근 센서 데이터 활용 영역이 넓어지면서 데이터 분석 서비스가 활성화되고, 분석을 용이하게 할 수 있는 환경으로 진화하고 있다[1]. 아마존 AWS IoT은 데이터 수집을 지원하는 플랫폼으로 데이터 분석 활용 영역이 넓어지면서 빅데이터 분석 서비스가 활성화되고, 분석이 용이해지고 한다.

탐색적 데이터 분석(EDA, Exploratory Data Analysis)는 데이터의 구조적 특성을 알아내기 위한 기법이다[2,3]. EDA는 수집한 데이터에 대한 다양한 각도에서 관찰하고 이해하는 과정으로 상세한 데이터를 분석하기 전에 그래프나 통계적인 방법으로 자료를 직관적으로 바라보는 과정이다[4].

기존 센서평가는 주로 내구성 시험과 전자파 인증 및 친환경 제품 인증과 같은 위해성 검사에 한정되어 있으며 센서 데이터의 신뢰성 검사는 제한적이다. 이를 해결하기 위해서는 ICT 기반 센서 데이터의 신뢰성 제고를 위한 환경구축이 요구된다.

신뢰성을 갖는 환경모니터링을 위해서는 센서로부터 수집된 환경 데이터의 분포 및 값을 살펴본 후 데이터가 표현하는 현상을 더 잘 이해하고, 센서 및 센서데이터에 대한 잠재적인 특이점을 발견을 진행

하여야 한다.

이 논문에서는 신뢰성 평가에 필요한 센서특성을 이해하는 것을 목적으로 한다. 이를 위해 EDA를 통해 수집된 센서 값을 시각적하고 분석에 주어진 데이터의 개별 속성의 특징 및 상관관계를 도출한다. 이는 측정인자에 따른 출력 특성을 알고 있는 센서를 이용하여 현재 시간과 공간에서 측정하고자 하는 환경인자 값을 도출하고 동일공간 및 동일시간대의 다른 센서에 대한 출력을 비교하여 비교군 센서의 특성을 관찰함으로써 EDA 분석 결과는 센서 데이터의 신뢰성을 평가하기 위해 사용한다.

2. 실험결과 및 분석

본 실험은 실내 공기질 모니터링을 위해 2020년 4월 2일부터 2020년 4월 19일까지 PM2.5, PM10.0, 온도, 습도, TVOC, CO2 센서로부터 전달된 센싱데이터(sensory data)를 기반으로 한다. 미세먼지 측정을 위해 PM2.5와 PM10.0을 사용하며, 공기품질 측정을 위해 TVOC, CO2를 사용한다.

EDA를 수행한 후 센서간의 상관관계를 도출한다. 기초적인 데이터 분석은 파이썬의 Pandas 라이브러리를 사용하여 수행한다. 표 1은 실험에 사용한 센서 데이터 중 습도와 CO2의 통계정보 (descriptive

statistics)를 보인 것이다. 225919의 전체 관측치를 가지며, 1초에 6개의 센서데이터를 획득하여 수집 서버에 전달한다.

<표 1> 데이터셋의 통계 값

	습도	CO2
count	225919	225919
mean	26.715375	4.709173
std	13.300000	1.380514
min	19.600000	1.880000
25%	22.300000	3.870000
50%	25.500000	4.540000
75%	30.500000	5.180000
max	43.400000	8.310000

<표 2>와 <표 3>은 5개의 최저 및 최고 습도 측정값에 따른 다른 5 센서값과의 측정값을 기술한 것으로 습도값은 CO2 과 연관성이 있음을 관찰할 수 있다.

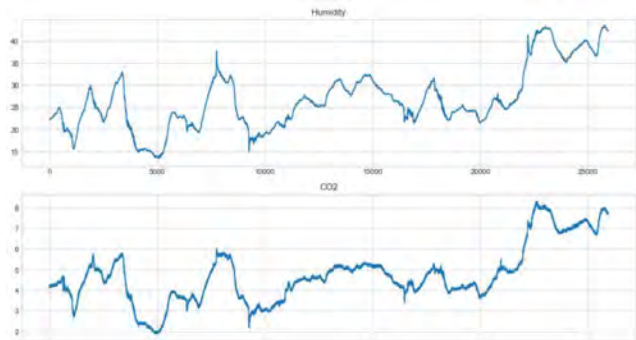
<표 2> 최저습도값의 타 센서 측정값

	REG_DATE	PM25	PM100	Temperature	Humidity	TVOC	CO2
5071	2020-04-05 12:31	15.38	18.57	19.5	13.3	1.55	1.92
5072	2020-04-05 12:32	16.54	18.57	19.5	13.4	1.56	1.98
5073	2020-04-05 12:33	15.67	18.57	19.6	13.4	1.53	1.90
5074	2020-04-05 12:34	15.09	12.38	19.6	13.4	1.55	1.98
5070	2020-04-05 12:30	15.67	18.57	19.5	13.5	1.54	1.98

<표 3> 최고습도값의 타 센서 측정값

	REG_DATE	PM25	PM100	Temperature	Humidity	TVOC	CO2
25735	2020-04-19 20:55	10.25	10.25	20.7	43.4	1.88	7.95
25736	2020-04-19 20:56	10.01	10.01	20.7	43.4	1.88	7.98
25737	2020-04-19 20:57	9.38	9.38	20.7	43.4	1.86	7.97
25740	2020-04-19 21:00	8.97	8.97	20.7	43.4	1.89	7.92
25741	2020-04-19 21:01	9.67	9.67	20.7	43.4	1.87	7.93

<그림 1>은 습도와 CO2의 측정값을 시각화하여 연관성을 플롯팅한 것을 보인 것으로 시각화를 통해 두 센서의 변화추이를 관찰할 수 있다.



<그림 1> 습도(Humidity) 와 CO2 관측값 플롯팅

<표 4>은 5개 센서값을 기반으로 센서간의 연관성

을 측정하였다. S4(습도) 는 S6(CO2)와 상호 높은 연관성(0.978920) 을 갖고 있음을 보인다.

<표 4> 센서값의 연관성(correlation) 결과

	S1	S2	S3	S4	S5	S6
S1	1.000000	0.978462	0.126186	0.086916	0.355466	0.106732
S2	0.978462	1.000000	0.121493	0.071399	0.346467	0.091029
S3	0.126186	0.121493	1.000000	0.179200	0.549721	0.369453
S4	0.086916	0.071399	0.179200	1.000000	0.250780	0.978920
S5	0.355466	0.346467	0.549721	0.250780	1.000000	0.349379
S6	0.106732	0.091029	0.369453	0.978920	0.349379	1.000000

3. 결론 및 향후 연구

이 논문에서는 실내 환경 모니터링을 위해 PM2.5, PM10.0, 온도, 습도, TVOC, CO2 센서로부터 측정값을 획득하였으며 센서특성을 이해하였다. 이를 위해 EDA를 통해 수집된 센서 값을 시각적으로 표현한 후 분석에 주어진 데이터의 개별 속성에 서로 의미 있는 상관관계를 도출한다. EDA 분석 결과는 센서데이터의 신뢰성을 평가하기 위해 사용한 후 스마트 시티, 스마트 국가 등 대규모 영역의 복잡한 사회 인프라를 최적화하기 위한 기술로서 활용예정이다.

감사의 글

본 논문은 과학기술정보통신부(정보통신기획평가원, 2019-0-00136) ICT 혁신선도 인프라 구축 사업의 ICT 기반 환경 모니터링 센서 검증 플랫폼 과제 의 지원을 받아 수행된 연구임

참고문헌

- [1] Ali, H., Soe, J. K., and Weller, S. R.. "A real-time ambient air quality monitoring wireless sensor network for schools in smart cities," in Proceedings of the 2015 IEEE First International Smart Cities Conference (ISC2)
- [2] Tukey J.W. "Exploratory Data Analysis. Addison Wesley, Reading" MA
- [3] Andrienko, N & Andrienko, G "Exploratory Analysis of Spatial and Temporal Data. A Systematic Approach" Springer.
- [4] Chen, Daniel Y. "Pandas for Everyone : Python Data Analysis" Addison-Wesley

자율주행차 서비스를 위한 차량 엣지 컴퓨팅 모델 연구

윤주상
동의대학교 산업ICT기술공학과
e-mail:jsyoun@deu.ac.kr

A Study on Vehicle Edge Computng Model for Autonomous Vehicle Service

Joosang Youn
Industrial ICT Engineering
Dong-Eui University

요 약

최근 엣지 컴퓨팅을 활용한 자율주행차 서비스 개발 연구가 진행 중이다. 특히, 최근 개발 중인 차량 엣지 컴퓨팅 기술은 도로 상황 및 교통 정보를 실시간으로 수집하여 빠른 처리를 통해 안정된 차량 및 교통 서비스를 제공할 수 있는 기술로 평가받고 있다. 따라서 본 논문에서는 자율주행차 서비스를 위해 차량 엣지 컴퓨팅 간, 엣지-클라우드간 협업 모델을 제안하고 차량 안전 메시지와 같은 긴급 메시지의 빠른 전달을 위한 초지연 메시지 전달 기법을 제안한다.

1. 서론

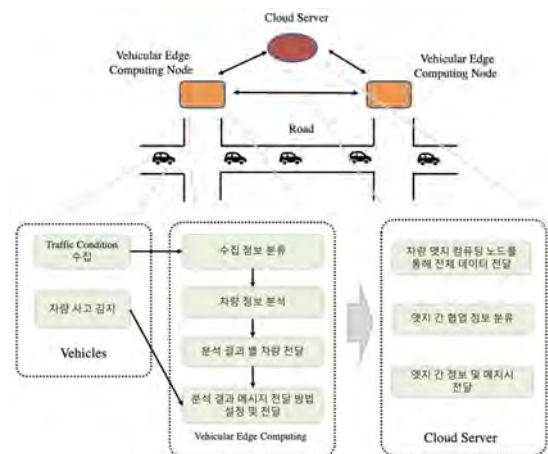
최근 자율 주행차량의 협업 서비스 제공을 위해 Internet of Vehicles (IoV)과 엣지 컴퓨팅 기술을 결합하는 새로운 연구가 진행 중이다. 자율주행차량간 협업 서비스를 제공하기 위한 네트워크 구축 기술인 기존 VANET을 활용하며 자율주행차량간 협업 서비스 제공은 엣지 컴퓨팅 기술을 활용한다. 또한, 협업 서비스 제공을 위해 엣지 노드 간 협업 기능을 제공한다[1, 2]. 엣지 노드에서 자율주행차량은 멀티 센서를 갖춘 지능형 이동 단말로 간주하며 주변 상황에 대한 유용한 정보를 수집할 수 있으며 통신 기능을 통해 엣지 노드에 관련 정보를 전달하고 엣지 노드에서 수집된 정보를 분석하여 그 결과를 다시 자율주행차량에 전달하여 차량간 협업 서비스가 가능하도록 차량 엣지 컴퓨팅 모델 및 기능을 본 논문에서 제안한다. 특히, 차량에서 엣지로 전달되는 정보는 차량 내부뿐만 아니라 차량과 관련된 외부 정보도 모두 포함된다. 예를 들어 주변 차량 사고 정보를 수집한 경우 사고 정보를 엣지 노드에 전달하여 차량 사고에 영향을 줄 수 있는 주변 차량에 관련 정보를 제공하는 역할을 엣지 노드에 역할로 정의한다. 차량 엣지 컴퓨팅 구조에서 엣지 노드는 자율주행차량 네트워크의 엣지에 위치하며 실시간으로 데이터 저장, 처리, 수집 등의 기능을 효과적으로 수행한다. 특히, 혼잡한 도시 내 도로와 고속도로 환경으로부터 많은 데이터를 수집하고 처리해야 할 경우에 차량 엣지 컴퓨팅 노드에서는 스마트 교통, 향상된 차량 안전 서비스 등과 같은 기능을 제공한다. 또한, 클라우드 기반 차량 서비스 제공에 비해 차량 엣지 컴퓨팅 노드는 오프로딩 서비스를 통해 컴퓨팅

오버헤드를 줄일 수 있는 기능을 제공한다. 본 논문에서는 차량 엣지 컴퓨팅 구조를 정의하고 교차로 상황에서 차량 엣지 컴퓨팅 기능을 가진 엣지 노드를 활용하여 빠른 정보 전달 및 긴급 메시지 전달 서비스가 요구되는 빠른 지연 메시지 전달기법을 제안한다.

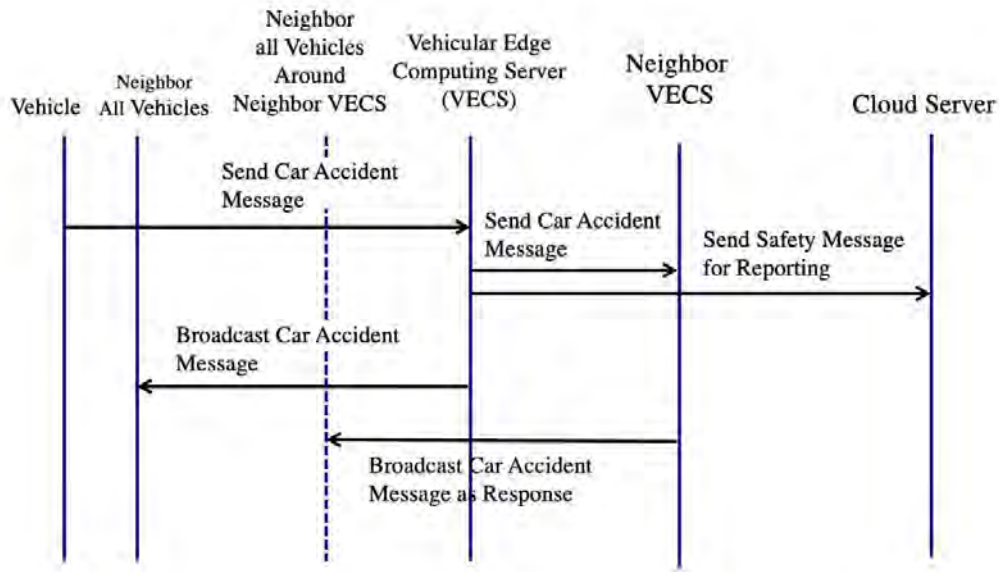
본 논문은 2장에서 차량 엣지 컴퓨팅 모델을 정의하고 3장에서 차량 엣지 컴퓨팅 노드 내 초저지연 메시지 전달 기법을 제안하고 마지막으로 4장에서 결론을 맺는다.

2. 자율주행차량의 협업 지원 차량 엣지 컴퓨팅 모델

[1]에는 엣지 컴퓨팅 기반 차량 서비스 제공을 위해 차량, 엣지 서버, 클라우드 서버 등으로 구성된 서비스 모델



(그림 1) 차량 엣지 컴퓨팅 모델



(그림 2) 차량 엣지 컴퓨팅 노드 간 초지연 메시지 전달 기법 (차량 안전 메시지 전달 시)

을 제안하고 있다. 본 논문에서는 [1]에서 제안된 구조를 기반으로 차량 엣지 컴퓨팅 모델을 제안한다. 그림 1은 본 논문에서 제안하고 있는 모델을 제안하고 있다. 우선, 차량은 데이터를 수집하고 수집한 데이터를 통해 차량 레벨의 컴퓨팅 및 결정 등의 역할을 수행한다. 차량 엣지 컴퓨팅 노드는 교차로 또는 도로에 위치하며 여러 차량으로부터 다양한 데이터를 수집하고 수집한 데이터 분류 및 분석을 실시하고 분석 결과를 관련된 차량에 전달하는 역할을 수행한다. 마지막으로 클라우드 서버는 데이터 분석 및 도시 레벨의 컴퓨팅 및 특정 상황에 대한 결정 등을 수행한다.

3. 차량 엣지 컴퓨팅 노드 내 초지연 메시지 전달 기법

초지연 차량 안전 데이터 메시지 전달을 위해 본 연구에서는 그림 2에 도시되어 있다. 자율주행차량의 경우 안전 및 위급상황과 관련된 시급한 안전 데이터 메시지는 빠른 데이터 전달이 매우 중요하다. 따라서 엣지 컴퓨팅 노드 간 네트워크 데이터 전달을 위한 자원 할당 지시와 엣지 노드 간 협업을 통해 빠르게 데이터를 전달하는 방법이다.

4. 결론

본 논문에서는 차량 엣지 컴퓨팅 기반 모델 및 초저지연 차량 정보 메시지 전달기법을 제안하였다. 제안한 기법은 교차로 내에 설치된 엣지 노드를 통해 교차로에서 발생한 위급상황을 주변 차량 및 이웃한 교차로의 엣지 노드에 빠르게 전달할 수 있는 기술이다. 특히, 제안하는 기법은 차량 안전 메시지와 같은 빠르 전달 서비스를 제공해야 하는 지연에 민감한 데이터 메시지를 빠르게 전달할 수 있다. 추후 연구로는 제안하는 기법의 성능 평가를 수행할 예정이다.

ACKNOWLEDGMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) (NRF-2017 R1D1A1B0 3034689)

참고문헌

- [1] C. Huang, R. Lu, and K. R. Choo, "Vehicular Fog Computing: Architecture, Use Case, and Security and Forensic Challenges," IEEE Communications Magazine, November 2017.
- [2] J. Youn, "Latency-Sensitive Message Broadcasting Scheme Based on Vehicular Fog Computing for Connected Self-Driving Cars," in processing of NGCIT 2018, Aug. 2018.

LoRa 네트워크를 활용한 주차정보 서비스 시스템 설계

김유찬, 문남미
호서대학교 컴퓨터공학과
dbcks2033@gmail.com, nammee.moon@gmail.com

Design of parking information service system using LoRa network

YuChan Kim, Nammee Moon
Dept. of Computer Engineering, Hoseo University

요 약

모든 주차 면수에 대해 감지하는 시스템은 큰 비용이 필요하여 주차정보 제공을 위해 필요한 스마트 주차장의 설치를 부담스럽게 하므로 애플리케이션을 통한 주차정보 제공을 어렵게 한다. 본 논문에서 제안하는 시스템은 외부 디바이스, 서버, 애플리케이션으로 구성된다. 주차장 출입로에 아두이노를 활용한 IOT 디바이스를 설치하여 센서를 통해 출입 차량을 감지하고 소량의 데이터를 장거리 전송할 때 적합한 LoRa(Long Range) 네트워크를 통해 주차정보를 서버로 전송하며 사용자의 요청이 있을 때 주차정보를 제공한다. 기존 시스템보다 감지범위를 줄이고 LoRa 네트워크를 활용한 시스템을 통해 주차공간 탐색으로 인한 사회적 비용과 시스템 구축비용을 절감하는 효과를 기대할 수 있다.

1. 서론

차량의 대수는 꾸준히 증가하고 있지만, 주차공간은 차량의 증가에 발을 맞추지 못해 주차공간의 부족이 사회적 문제가 되고 있으며 이로 인해 주차공간을 찾지 못해 주차장을 배회하여 주차장 내부의 혼잡과 사용자의 불편이 야기된다[1]. 애플리케이션을 통해 주차정보를 제공하여 주차공간을 찾는 시간을 줄여 편의를 도모할 수 있으나 기존의 센서를 매설하는 형태의 시스템은 시공을 위한 인력과 비용이 필요하며 시설물의 이용이 통제되고 설치하는 형태는 시공 없이 설치할 수 있으나 두 형태 모두 주차면수 별로 모니터링하여 센서의 비용이 크고 주차장 내부의 차량을 계수해 잔여 주차공간을 파악할 수 있는 스마트 주차장 시스템의 보급이 미흡하여 애플리케이션을 통한 주차정보 제공이 어렵다[2].

IoT 시장의 다양한 네트워크 분야 중 저전력 장거리 통신기술(Low Power Wide Area Network, LPWAN)은 스마트 시티, 스마트 미러링 등 다양한 분야에 적용 가능하며, 이러한 LPWAN의 요구사항을 만족하는 대표적인 IoT망으로 LoRa가 있다

[3][4]. 본 논문에서는 소량의 데이터를 장거리 전송하는데 적합한 LoRa 네트워크를 아두이노를 활용한 IOT기반 주차정보 시스템에 적용하여 구성한다.

2. 관련연구

기존 주차관리 시스템과 차량 감지 센서를 살펴보면 다음과 같다.

2.1 주차관리 시스템

2.1.2. 전자 주차 시스템

전자 주차 시스템은 사용자가 다른 서비스 및 센서로부터 주차장의 현재 공석에 대한 정보를 전자적으로 얻을 수 있는 시스템이다[5]. 스마트폰 또는 웹 기반 응용 프로그램을 통해 시스템을 이용할 수 있는 주차공간 예약과 이익 또는 주차공간 활용을 극대화하기 위한 주차공간 할당을 포함하는 개념이다[6].

2.1.1. 주차예약 시스템

주차예약 시스템(Parking Reservation System, PRS)은 사용자가 원하는 시간에 주차 장소를 예약할 수 있는 시스템이다. 사용자는 스마트폰 또는 웹

기반 응용 프로그램과 같은 통신 서비스를 사용하여 주차공간을 예약할 수 있다. PRS의 구현을 위해서는 주차장에 대한 실시간 모니터링 시스템이 필요하지만, 사용자가 시스템을 사용하고 주차 공석을 신고하도록 장려하는 클라우드 소싱을 통해 구현하기도 한다[7].

2.2 차량 감지 센서

2.2.1. 적외선 센서

적외선 센서는 물체와 주변 환경 사이의 온도 차이를 감지하여 작동한다[8]. 차량 또는 도로에서 방출되는 온도 차이를 측정하여 주차공간의 공석을 식별하며 벽이나 바닥에 매설할 필요 없이 주차장의 천장에 설치할 수 있다. 또한, 적외선 센서는 기상 조건 영향을 받기 쉬워 주차 시스템 성능을 저하할 수 있다.

2.2.2. 초음파 센서

초음파 센서는 음파를 사용하여 25~50kHz의 주파수로 에너지를 전송하고 차체에서 반사될 때 주차장의 상태를 감지할 수 있습니다. 유사하게, 그것은 차량의 속도와 주어진 거리에 있는 차량의 수와 같은 다른 유용한 정보를 제공합니다. 적외선 센서와 마찬가지로 온도와 환경에 민감합니다. 그러나 설치가 간단하고 투자 비용이 적기 때문에 전자 주차 시스템에서 주차공간을 식별하는 데 널리 사용됩니다.

2.2.3. CCTV 및 이미지 처리

이미지 처리를 위한 감지는 차량의 유무를 판단하기 카메라로 촬영한 데이터는 이미지 처리 기술을 사용하여 프레임별로 분석할 수 있다[9]. CCTV는 이미 감시 목적으로 여러 주차장에서 사용되고 있으므로 이러한 시스템의 구현이 쉽다. 단일 카메라로 둘 이상의 주차 지점을 분석할 수 있으므로 넓은 영역을 감지할 때 훨씬 효율적이다. 하지만 기상 조건에 따라 시스템의 성능이 영향받을 수 있다.

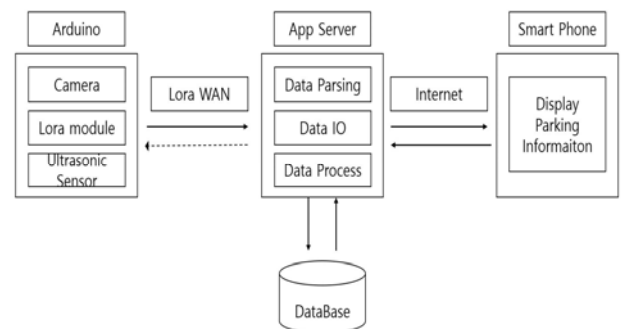
2.2.4. LDR 센서

LDR(Light Depended Resister)은 빛에 의존하는 센서로 광도의 변화를 감지한다. 차량은 태양과 같은 1차 광원과 다른 주변 빛과 같은 2차 광원을 할당하여 그림자를 통해 빛 센서가 광도 변화를 감지하여 주차 장소에 차량이 있음을 감지한다[10]. 기상 조건에 따라 성능이 영향받을 수 있다.

3. 본론

기존의 스마트 주차장 시스템은 설치형과 매설형 모두 센서를 통해 주차 면수 별로 모니터링하여 센서의 비용이 크기 때문에 부담이 된다. 따라서 주차장 출입로에 시스템을 설치하여 카메라와 장거리 통신을 위한 LoRa모듈로 구성된 시스템을 통해 출입 차량을 계수하여 주차 정보 시스템의 핵심적인 개념인 잔여 주차공간과 주차 회전을 평균 주차 지속시간과 같은 정보에 초점을 맞춰 수집 및 제공하여 시스템 구축비용을 절감한다.

시스템의 전체적인 구성은 그림 1과 같다. 카메라, 초음파 센서, LoRa 모듈, 아두이노, 네트워크 서버, 앱 서버로 구성된다. 차량 계수에 사용되는 하드웨어에는 카메라, LoRa 모듈, 초음파 센서가 포함되며 센싱을 통해 차량이 감지되면 카메라를 통해 차량의 번호판이 포함된 원본 이미지를 수집한 뒤 아두이노를 이용한 Open CV 기반 이미지 프로세싱으로 출입 차량의 차량번호를 추출하고 차량 출입시간과 이에 따른 잔여 주차공간의 데이터를 LoRa WAN을 통해 LoRa 네트워크 서버로 전송한다. 전송된 데이터는 앱 서버에서 파싱하여 데이터베이스에 업데이트하며 서버는 클라이언트의 위치를 기반으로 주차 가능한 인근의 주차장을 추천하거나 요청에 따라 잔여 공간, 주차 지속시간, 주차 회전을, 리뷰정보를 애플리케이션을 통해 시각적으로 제공한다.

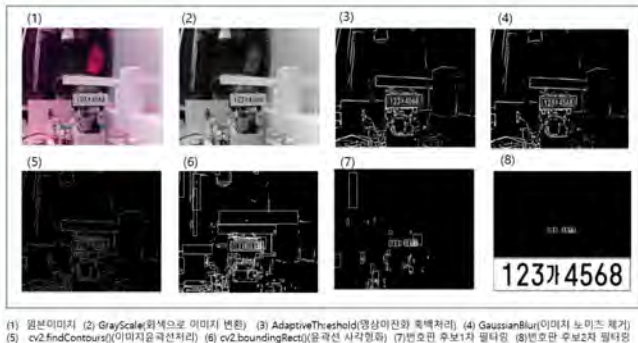


<그림 1> LoRa기반 주차정보 서비스 시스템 구성도

3.1 출입 차량 검출

출입 차량을 검출하기 위하여 초음파 센서와 카메라를 사용한다. 초음파 센서를 통해 출입 차량이 감지되면 카메라를 이용해 출입 차량의 번호판을 추출한다. Open CV 라이브러리로 원본 이미지에서 번호판 후보를 추출한 뒤 OCR(Optical Character

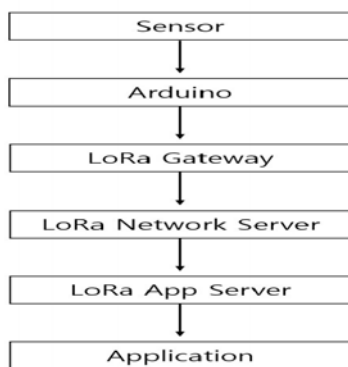
Recognition) 엔진으로 텍스트를 추출하여 출입 정보와 번호판 데이터 서버로 전송한다. 그림 2는 Open CV를 활용한 차량번호 인식 과정의 예시과정을 나타낸 것이다. [11]



<그림 2> Open CV를 활용한 주차장 차량번호 인식 과정의 예시

3.2 Lora 네트워크

LoRa는 Long Range의 약자로 최대 도달거리가 10km 이상으로 장거리 통신이 가능하고 저전력으로 유지보수 비용이 저렴하며 낮은 구현 복잡성을 가지고 양방향 통신을 지원하는 소량의 데이터를 장거리 전송할 때 적합한 모듈이다. 본 논문에서는 LoRa WAN 규격에 따라 통신하며 규격에 맞춰 수집된 데이터를 스택으로 쌓아 두었다가 10초마다 네트워크 서버로 송신한다. 수집된 데이터는 LoRa 게이트웨이에서 UDP 패킷의 형태로 송수신되며 게이트웨이가 브릿지에서 UDP를 MQTT프로토콜을 통해 JSON으로 추상화하여 LoRa 네트워크 서버로 전송한다. 각 과정은 암호화되어있기 때문에 디코딩하여 전송된 데이터를 활용한다.



<그림 3> 시스템 아키텍처 블록 다이어그램

3.3 서버

서버는 구글 파이어 베이스를 기반으로 구축하며 LoRa 네트워크 서버로 전송된 데이터를 파싱하고

데이터를 기반으로 주차 회전율과 평균 주차 지속시간을 계산하여 해당 주차장의 데이터베이스를 업데이트한다. 서버는 클라이언트의 요청에 따라 애플리케이션을 통해 데이터를 제공하며 클라이언트는 애플리케이션 UI를 통해 GPS를 기준으로 잔여 주차공간이 있는 가장 가까운 주차장을 추천받거나 특정 주차장을 선택하여 해당 주차장의 잔여 주차공간이나 리뷰, 회전율, 평균 주차시간과 같은 주차정보를 시각적으로 제공받을 수 있다.

4. 결론 및 기대효과

본 논문에서는 기존 주차정보 시스템에 저전력 저비용의 특성을 가진 LoRa 네트워크를 활용하고 모니터링 범위 감소를 통해 시스템 구축비용을 절감하며 이용자에게 핵심적인 주차정보만을 제공하는 시스템의 설계를 제안하였다. 이를 통해 스마트 주차장의 보급에 기여하고 주차공간 탐색으로 인해 발생하는 사회적 비용감소의 효과를 기대하며 추후 스마트 결제나 주차공간 예약, 개인화 추천 같은 기능을 주차정보 서비스와 융합시켜 이용자의 편의성을 높이는 것을 목표로 한다.

참고문헌

- [1] Graham Cookson. "Smart Parking - A Silver Bullet for Parking Pain". <https://inrix.com/blog/2017/07/parkingsurvey/>.
- [2] Tahon, Mathieu, et al. "Parking sensor network: Economic feasibility study of parking sensors in a city environment is well." 2010 9th Conference of Telecommunication, Media and Internet. IEEE, (2010).
- [3] 이리나, 이가람, 김호원. "LoRa 기술 분석." 한국통신학회. 학술대회논문집. pp. 217-218. (2017).
- [4] Georgiou, Orestis, and Usman Raza. "Low power wide area network analysis: Can LoRa scale?." IEEE Wireless Communications Letters 6.2. pp. 162-165. (2017).
- [5] Rao, Y. Raghavender. "Automatic smart parking system using Internet of Things (IOT)."

Int J Eng Technol Sci Res 4.5 (2017).

[6] Shao, Chaoyi, et al. "A simple reservation and allocation model of shared parking lots." *Transportation Research Part C: Emerging Technologies* 71. pp. 303-312. (2016).

[7] Yan, Tingxin, et al. "Crowdpark: A crowdsourcing-based parking reservation system for mobile phones." *University of Massachusetts at Amherst Tech. Report* 1-14. (2011).

[8] Someswar, G. M., et al. "DESIGN & DEVELOPMENT OF AN AUTONOMIC INTEGRATED CAR PARKING SYSTEM." *Compusoft* 6.3. pp. 2309-2312. (2017).

[9] Zhang, Lin, et al. "Vision-based parking-slot detection: a benchmark and a learning-based approach." *Symmetry* 10.3. pp. 64. (2018).

[10] Bachani, Mamta, Umair Mujtaba Qureshi, and Faisal Karim Shaikh. "Performance analysis of proximity and light sensors for smart parking." *Procedia Computer Science* 83. pp. 385-392. (2016)

[11] <https://www.youtube.com/watch?v=apJ97MA1IU>

제53회
2020 온라인 춘계학술발표대회

정보보호



적외선통신 암호화 연구

김민철*, 서태원**

*고려대학교 정보보호학과

**고려대학교 컴퓨터학과

e-mail: betamc@korea.ac.kr, suhtw@korea.ac.kr

A Study on Secure Infrared Communication

Minchul Kim*, and Taeweon Suh**

*Graduate School of Information Security, Korea University

**Dept of Computer Science and Engineering, Korea University

요 약

적외선통신은 리모컨이나 하이패스와 같이 주변에서 흔히 보이는 디바이스에서 사용하는 방법이다. 적외선통신을 이용하여 전송을 하게 되는 경우 전파를 이용한 통신에 비해 비용과 유지의 효율성 면에서 이점을 가진다. IoT환경에서 적외선통신은 민감하고 중요한 데이터까지 보내는 수단으로까지 사용되고 있다. 본 논문에서는 이러한 적외선통신을 IoT환경 하에서 안전하게 사용할 수 있도록 두 가지 관점을 제시한다. 적외선통신의 키를 사용하는 방법과 카운터를 사용하는 두 가지의 관점을 설명하고, 이에 대한 평가를 병행한다.

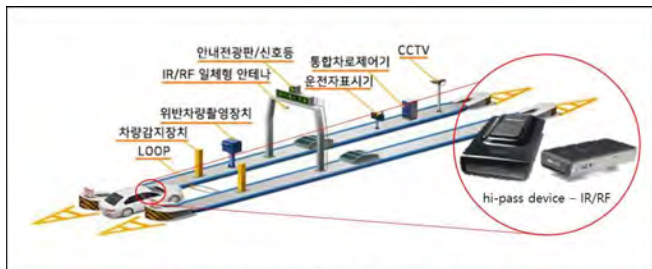
1. 서론

적외선통신은 TV, 에어컨, 오디오, 빔프로젝터 등 무선으로 기기를 조작하기 위해 사용되는 통신 방법이다. 적외선통신을 위해, 송신하는 쪽은 IRED로 수신하는 쪽은 Photodiode로 구성한다. 송신부와 수신부의 구성요소만 보아도 다른 통신 방법들에 비해 회로구성이 간결하고 저렴하며, 유지보수가 간편하다는 점을 알 수 있다. 소비전력이 낮으므로 상대적으로 긴 시간 사용도 가능하다. 빛 중에서도 적외선을 사용하기 때문에, 라디오 주파수를 이용하는 통신(예: Wi-Fi, Bluetooth, 5G와 같은 모바일 통신 등)과 충돌이 발생하지 않고, 전파 규제도 일어나지 않는다. 충돌되는 통신이 없고 전파 규제가 없으므로 적외선으로 통신을 할 경우 사용 가능한 채널의 대역폭이 넓고 채널을 자유롭게 이용할 수 있다. 널리 쓰는 방법임에도 불구하고 적외선통신에 있어 보안에 대한 연구는 찾아보기 매우 어려운데, 적외선 통신은 한계를 확실하게 가지고 있는 통신 방법이기 때문이다. 자연광이나 인공광, 대기 중의 먼지에 민감하며 통신을 위해서는 송신기와 수신기가 마주 놓여야 한다. 통신거리도 짧고, 통신 시야각이 좁다는 제한점까지 가지고 있다[1-5]. 바로 이 점들 때문에 이제까지 적외선통신과 관련한 보안연구는 단 한 번

도 이루어진 적이 없다. 일정반경 외에서는 통신을 할 수 없고, 송신기와 수신기의 각도가 일정수준을 벗어나면 통신이 되지 않는다. 따라서 제한된 환경 내에서 통신이 일어나는 것에 대해 보안이 필요하지 않다고 생각하여 적외선 통신의 보안 영역을 간과하게 된다. 과거에는 리모컨으로 디바이스의 단순한 기능만을 사용했다면, 지금에 와서는 리모컨 한 개로 결제사항이나 개인정보, 혹은 금융이나 기타 민감한 사항까지 입력하는 경우가 많아졌다. 이 때문에 보안을 위협하는 몇 가지 상황이 발생한다. 첫째는 동일한 공간에 존재하는 사람에 의한 위협이다. 동일한 공간 내에 여러 사람이 함께 있을 때는 송신기가 어디 있는지 알 수 없다. 중요한 회의가 열리고 있는 상황에서, 보조 장치인 빔프로젝터를 인가된 사람이 아닌 공격자가 마음대로 조작할 수 있다. 또한 공격자는 오디오 장치를 악의적으로 이용하여 회의를 방해할 수도 있다. 둘째는 적외선이 투명한 매질을 통과 할 수 있는 성질을 이용한 보안 위협이다. 이를테면 외부에서 창문이나 유리벽을 통해 집 안에 있는 IPTV를 볼 수 있다. 사회 공학적 기법을 통해, 설정해놓은 비밀번호나 결제관련 정보를 유추할 수 있게 되면 금전적인 피해를 입을 확률이 커진다. 셋째는 첫 번째와 두 번째 항목과 관련하여, 적외선 레이저를 이용하여 다른 장소에서 디바이스를 마음대로 조작할 수 있다는 원거리 위협이다. 넷째는 공개된 공간에서 적외선 통신을 사용하는 경우에

이 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2019-0-00533, 컴퓨터 프로세서의 구조적 보안 취약점 검증 및 공격 탐지 대응)

서 발생하는 오픈 데이터에 의한 위협이다. 그림 1의 (a)와 같이, 고속화도로에서 상용화된 하이패스는 적외선을 사용하는 IR방식과 라디오 주파수를 사용하는 RF방식이 있다[6]. IR방식의 디바이스를 사용하는 사용자에게는 주차가 되어 있더라도 상시 배터리로 디바이스가 동작할 경우이거나 도로를 주행하는 경우 모두 공격에 노출되어있다. IR방식은 누구든 볼 수 있게 열려있기 때문에, 데이터 수집이 쉽기 때문이다. 본 논문에서는 이러한 공격이 가능하게 된 배경으로, 2장에서 적외선통신 프로토콜에 대해 살펴본다. 3장에서는 이러한 공격을 방지하기 위한 방어 방법에 대해 소개하면서, 공격 방법에 따른 취약점을 분석한다. 이를 토대로 4장에서는 적외선통신에 대한 보안을 총체적으로 분석하며 결론을 내린다.



(a) 국내 고속도로 자동결제 시스템 (hi-pass)



(b) IPTV

(그림 1) 실생활 적외선통신

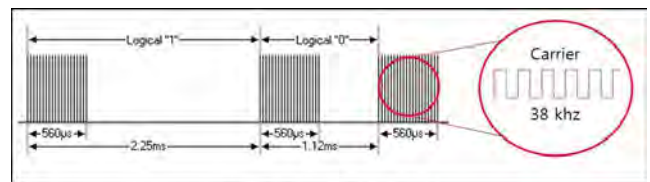
2. 선행연구

2.1. 적외선통신 프로토콜

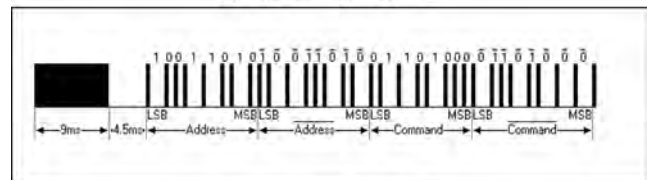
적외선통신은 회사마다 다른 프로토콜을 사용한다. 본 논문에서는 대표적인 프로토콜인 NEC 방식[4]을 분석한다. 그림 2의 (a)에서와 같이 데이터 '1'과 데이터 '0'이 나타난다. 데이터 '1'은 560 μ s 동안 38kHz의 캐리어를 이용하여 신호를 보낸 뒤, 1690 μ s 동안 아무 신호도 보내지 않는다. 데이터 '0'은 560 μ s 동안 38kHz의 캐리어를 이용하여 신호를 보내고 나서 560 μ s 동안 아무 신호도 보내지 않는다. 이렇게 데이터 '1'과 '0'이 구분된다.

적외선통신은 비대칭통신이므로 데이터를 구분 짓

기 위해 선행비트(Start bit)가 필요하다. NEC 프로토콜에서는 선행비트로 9ms동안 캐리어를 이용하여 신호를 보낸 후 4.5ms동안 아무 신호도 보내지 않는다. 데이터를 구분한 다음 데이터를 보낼 수 있다. 데이터는 기기를 식별할 수 있는 주소(address)와 명령(command) 부분으로 나뉜다. 두 부분의 데이터 사이즈는 각각 8bit으로, 주소와 명령 데이터는 수신이 잘 됐는지 판별하기 위해 데이터 '0'과 '1'을 서로 바꾸는 토글 과정을 거쳐 보낸다. 총 주소를 보내는데 16bit, 명령을 보내는데 16bit, 선행비트를 제외한 총 32bit의 데이터를 보낸다.



(a) 데이터 '1'과 '0'의 표현

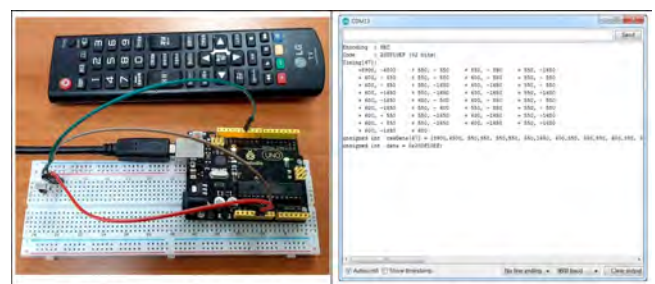


(b) NEC 프로토콜 구조

(그림 2) NEC 프로토콜 적외선통신 방법

2.2. 적외선통신 도청방법

적외선통신은 그림 3의 (a)와 같이 적외선수신센서와 마이크로컨트롤러만 있으면 손쉽게 도청할 수 있다. 그림 3의 (b)는 LG 리모컨을 분석한 것이며, 데이터를 보낼 때 NEC 방식을 사용하는 것을 알 수 있다.



(a) 리모컨과 마이크로컨트롤러와 적외선센서

(b) 리모컨 데이터

(그림 3) 적외선통신 도청방법

3. 적외선통신 보안방법

적외선통신에서 보호하고자 하는 부분은 주소(address)부분이다. 명령(command)부분에 비밀번호와 같이 민감한 데이터가 들어 있음에도 불구하고 이를 보안하지는 않는다. 명령부분을 도청한다고 해

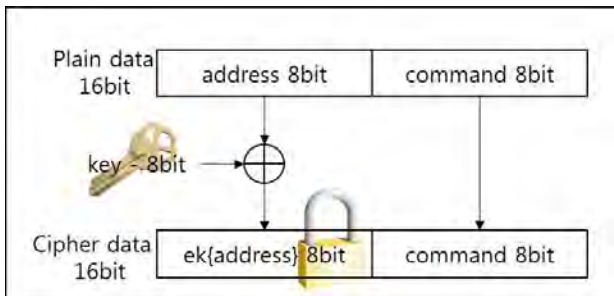
도 주소가 일치하지 않으면 적외선통신이 동작하지 않기 때문이다. 여기에서 더 고려해야 할 사항은 통신에 대한 보안을 기본으로 하되, 빠른 반응속도를 유지할 수 있도록 디자인해야 한다는 것이다. 과한 암호화는 사용자관점에서 작업을 저해하는 요인으로 작용하므로 업무 효율을 낮춘다.

3.1. 키를 사용한 보안

적외선통신에서 데이터 '1'과 '0'으로 인코딩되기 전 키를 이용하여 암호화하는 방법이다. 이를 위해 블록암호 전반을 사용할 수 있다. 블록암호 중 가장 간단한 데이터와 키를 XOR연산 하는 치환암호를 소개하면 다음과 같다.

$$8\text{bit data} \oplus 8\text{bit key} = 8\text{bit encrypted data} \quad (1)$$

(1)의 키를 이용한 보안은 고유한 주소를 숨기는데 도움이 된다. 그러나 주소와 동일한 키를 이용해 안전하게 사용하기 위해선 키 관리가 중요하다. 키가 항상 같다면 재전송 공격이 가능해지기 때문에 결국 문제가 발생할 수 있으므로 키를 주기적으로 바꾸어 주어야 한다. 어떠한 블록암호에서도 시간에 따라 값이 바뀌지 않으면 재전송 공격에 취약할 수밖에 없다. 그럼에도 불구하고 키를 이용한 보안을 사용하기 좋은 이유는 적외선통신이 도청하기 힘든, 홈 IoT 환경에서 사용할 수 있기 때문이다.



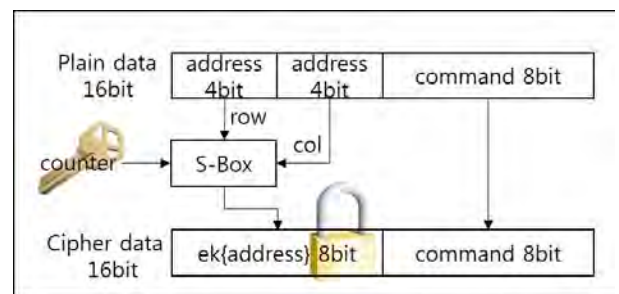
(그림 4) 키를 사용한 보안

3.2. 카운터를 사용한 보안

카운터는 송신부와 수신부가 일치되었을 때만 정상적인 데이터로 판단하는 목적으로 사용한다. 따라서 카운터를 사용하는 보안은 사전에 카운터 동기화가 필요하다. 카운터를 위해 보안에 사용된 테이블은 미국의 NIST 표준인 AES(Advanced Encryption Standard) 암호[7]의 S-Box를 이용하였다. S-Box를 사용하는 이유는 전단사함수를 이용하여 복호화하는데 짧은 시간이 소요되기 때문이다. 또한 S-Box를 이용하면 선형분석(LC: Linear Cryptanalysis)에 대해 안전함을 보인다[8-10]. 그림 6의 표는 S-box이

며 그림 5와 같이 행에 주소 4bit과 열에 주소 4bit을 이용한다. 카운터는 총 2개를 사용하며 행 카운터, 열 카운터를 사용한다. 초기에 카운터를 동기화하며 카운터의 시프트 연산을 통해 매번 입력할 때마다 값을 변경한다. 연산 후 최종 값을 주소로 사용한다. 그림 6을 보면 주소가 a7일 때, 카운터를 사용하지 않으면 5c로 고정된 출력을 가진다. 카운터를 사용할 때, 카운터에 의해 초기 주소가 6c가 되며 S-Box의 출력인 50을 주소로 사용한다. 또한, 카운터가 증가됨에 따라 출력이 바뀐다. 이전 카운터를 사용한 것과 다음에 사용한 카운터의 연관성은 S-Box에 의해 없으며 두 개의 카운터를 알지 못하면 복호화하기 어렵다. S-Box와 카운터 연산 후 결과인 50 (0101 0000)을 주소로 사용하여 IRED를 통해 데이터를 보낸다.

카운터를 이용한 보안의 경우 하드웨어와 소프트웨어가 오픈되어있다는 전제 하에서 카운터 값을 찾으면 공격자에게 기기의 주도권을 박탈당하게 된다. 이 때, 인가된 사용자의 리모컨은 더 이상 기능하지 못하게 된다. 따라서 카운터를 사용했을 때 일정 횟수 실패하면 카운터를 다시 동기화 할 수 있게 디자인해야 한다.



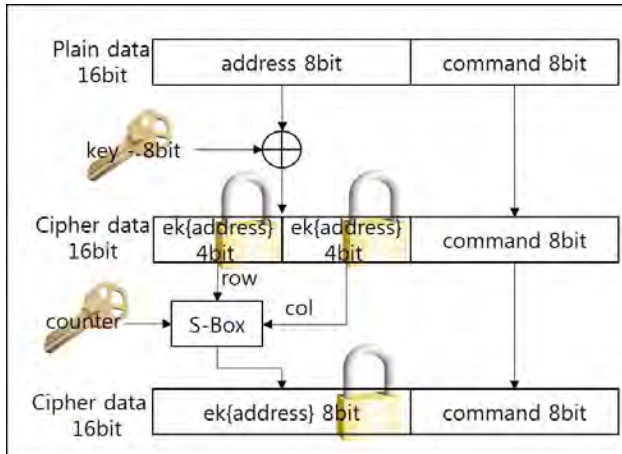
(그림 5) 카운터와 S-Box를 이용한 보안

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	5e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	d6	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	93
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

(그림 6) S-Box와 카운터를 이용한 연산

3.3. 키와 카운터를 사용한 보안

3.1.키를 이용한 보안과 3.2.카운터를 이용한 보안을 믹스하여 둘의 단점을 보완한 것으로 주소값이 키에 의해 보호되며 키를 일정 시기마다 변경하게 되면 S-Box에 의해 전혀 다른 값이 나오게 되어 안전해진다. 그림 7은 그림 4와 그림 5의 융합된 형태로 구성되어 있으며 주소를 암호화한 후 S-Box와 카운터를 이용하여 암호화한다.



(그림 7) 키와 카운터, S-Box를 사용한 보안

4. 결론

빛을 사용하는 적외선 통신은 라디오 주파수에 비해 혼선이 발생하지 않는다. 빛을 사용하는 방식으로 통신하기 때문에 채널을 제한 없이 사용할 수 있다. 통신에 필요한 송/수신 센서도 저렴하기 때문에 설계와 보수의 비용이 저렴하다. 또한 소비전력이 낮기 때문에 유지비용도 낮다는 장점까지 가지고 있다. 이러한 적외선통신은 우리가 의식하지 못하는 사이 리모컨이라는 이름으로 익숙하게 사용되고 있다. 그러나 이에 대한 보안 연구는 정작 이루어지지 않고 있다. 적외선통신으로 개인정보나 자산에 영향을 주는 데이터를 주고받는 상황이 늘어났으므로, 이를 효과적으로 보안할 수 있는 방법 또한 고안되어야 한다. 단순히 데이터를 암호화하는 것에 그칠 것이 아니라, 환경을 고려하여 보안 할 수 있는 방법을 찾는 것이 중요하다. 보안의 효율성과 사용자의 편리성은 반비례한다. 어느 쪽을 더 중요하게 여기는가에 따라 보안의 방향이 결정된다. 본 논문에서 제시한 보안 방법은 다소 보안에 치우친 것처럼 보이지만, 사용자의 편리성을 위해 하드웨어의 처리를 고려하여 최소의 보안으로 최대의 효과를 내기에 적합하다. 보안의 정도를 높이면서도 사용자에게 편

리한 환경을 제공할 수 있는 보다 발전된 연구가 필요하다.

참고문헌

- [1] H. Du and G. Xu, "Infrared indoor wireless MIMO communication system using 1.2GHz OOK modulation," in China Communications, vol. 16, no. 5, pp. 62-69, May 2019.
- [2] M. Sugimoto, K. Aoyama and A. Kongoh, "Improvement of traffic control system by means of infrared beacon two-way communication," ITSC2000. 2000 IEEE Intelligent Transportation Systems. Proceedings (Cat. No.00TH8493), Dearborn, MI, USA, 2000, pp. 258-263.
- [3] F. Arvin, K. Samsudin and A. R. Ramli, "A Short-Range Infrared Communication for Swarm Mobile Robots," 2009 International Conference on Signal Processing Systems, Singapore, 2009, pp. 454-458.
- [4] S. Ohtsuka, S. Hasegawa, N. Sasaki and T. Harakawa, "Communication System between Deaf-Blind People and Non-Disabled People Using Body-Braille and Infrared Communication," 2010 7th IEEE Consumer Communications and Networking Conference, Las Vegas, NV, 2010, pp. 1-2.
- [5] Wang Xianzhen, Yan Huan, Miao Changyun and Zhang Cheng, "The design of locomotive alarm and parking system based on infrared communication," 2010 Second Pacific-Asia Conference on Circuits, Communications and System, Beijing, 2010, pp. 5-8.
- [6] 한국도로공사, Available: <https://www.ex.co.kr/>
- [7] Standard, NIST-FIPS. "Announcing the advanced encryption standard (aes)." Federal Information Processing Standards Publication 197.1-51 (2001): 3-3.
- [8] Keliher, Liam. "Refined analysis of bounds related to linear and differential cryptanalysis for the AES." International Conference on Advanced Encryption Standard. Springer, Berlin, Heidelberg, 2004.
- [9] Musa, Mohammad A., Edward F. Schaefer, and Stephen Wedig. "A simplified AES algorithm and its linear and differential cryptanalyses." Cryptologia 27.2 (2003): 148-177.
- [10] Matsui, Mitsuru. "Linear cryptanalysis method for DES cipher." Workshop on the Theory and Application of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1993.

원자력시설 핵심디지털자산에 대한 코드 난독화 적용에 관한 연구

김상우, 김시원, 변예은, 권국희
한국원자력통제기술원

kjoey@kinac.re.kr, swkim@kinac.re.kr, hibye@kinac.re.kr, vivacita@kinac.re.kr

Applying Code Obfuscation to Vital Digital Assets at the Nuclear Facilities

Sangwoo Kim, Siwon Kim, Yeeun Byun, Kookheui Kwon
Korea Institute of Nuclear Nonproliferation and Control (KINAC)

요 약

원전에 대한 사이버위협이 지속됨에 따라 IAEA 및 각국에서는 원전 사이버보안 강화를 위해 노력하고 있다. 그 일환으로 국내에서는 규제기준 KINAC/RS-015를 통해 원전 내 안전·보안·비상대응 기능과 관련된 필수디지털자산에 대한 사이버보안 규제를 수행하고 있으나 원전 사고와 직접적으로 관련된 자산에 대해서는 보다 강화된 보안조치를 적용하여 보안성을 높이하고자 한다. 이러한 강화 조치의 하나로 ‘코드 난독화 적용’이 있으며 이에 대해 상세히 살펴보고자 한다.

1. 서론

원전 제어시스템의 디지털화가 지속되고 원전에 대한 사보타주를 목적으로 한 악성코드들이 점차 늘어나고 있다. 대표적인 예로 2010년 이란 원자력시설을 대상으로 한 스텝스넷 사건이 있었으며, 이를 통해 산업제어시스템을 폐쇄망 구조로 운영하는 것만으로는 사이버공격으로부터 완전히 자유로울 수 없음이 드러났다. 이러한 원자력시설 대상 사이버공격에 대비하기 위해 국제원자력기구(IAEA)의 NSS 17과 미국 원자력규제위원회(NRC)의 RG 5.71 등이 발간되어 원자력시설의 주요 디지털자산에 사이버보안조치를 수행하도록 권고 및 규제하고 있다[1][2]. 국내에서는 규제기준 KINAC/RS-015에서 제시한 101개의 보안조치 항목을 통제하는 방식으로 대응하고 있다[3]. 만약 규제대상인 디지털자산 내에서도 원전의 노심 손상을 유발하여 심각한 영향을 가져올 수 있는 자산을 도출해 보다 강화된 보안조치를 적용한다면 원전의 보안성을 한층 높일 수 있을 것이다. 이에 본 연구에서는 원전의 노심 손상을 유발할 수 있는 디지털자산인 핵심디지털자산[4]에 대해 차등적으로 적용 가능한 강화된 보안조치를 찾고자 한다.

2. 핵심디지털자산 보안 요구사항 분석

핵심디지털자산을 위한 보안조치를 도출하기 위

해 우선 원전의 디지털자산 중 사고를 직접적으로 일으키거나 사고완화 실패를 유발할 수 있는 제어시스템들의 하드웨어, 소프트웨어 및 네트워크 특성을 분석하여 이를 기반으로 핵심디지털자산의 공격 벡터를 식별하였다. 그리고 식별된 공격 벡터들을 예방하기 위해 사이버보안 기술, NIST 800-53, IAEA NSS 17 등의 국제 사이버보안 가이드라인 등을 분석하여 핵심디지털자산을 위한 보안 요구사항을 도출한 후 KINAC/RS-015에서 요구하는 보안 요구사항과 비교 및 분석한 결과, 핵심디지털자산을 위한 보안 요구사항이 KINAC/RS-015에서 요구하는 보안조치에 의해 대부분 만족되고 있음을 확인하였다[1][3][5]. KINAC/RS-015의 보안조치를 통해 완벽히 예방되지 않는 일부 보안 요구사항에 대해서는 기존 보안조치 중 일부를 강화하거나 추가적인 보안조치를 적용해 보안을 보다 강화하는 것이 필요하다. 이러한 추가 보안조치의 하나로 ‘코드 난독화(obfuscation) 적용’이 있으며, 동 보안조치는 공급망 통제, 신뢰성 확보 등의 보안조치가 포함되어 있는 KINAC/RS-015의 시스템 및 서비스 획득 관련 보안조치로 분류할 수 있다[3].

3. 역공학에 의한 제어시스템 위협

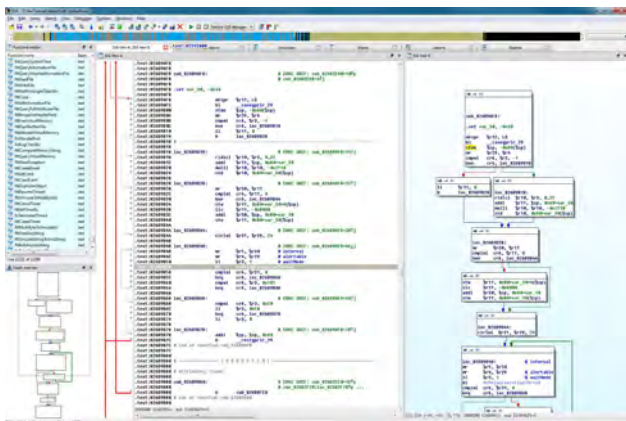
소프트웨어 공격 벡터 측면에서 분석한 결과, 소

소프트웨어 역공학(reverse engineering) 또는 퍼징(fuzzing) 등을 통한 제어시스템 관련 신규 취약점 발견이 늘어나고 있다. 소프트웨어 소스코드를 어셈블리 파일로 변환하기 위해 컴파일 과정을 거치며, 어셈블리 파일을 최종적으로 바이너리 파일로 만들기 위해 어셈블 과정을 거치게 된다. 이러한 과정을 거쳐 생성된 바이너리 파일은 실행 파일의 구조를 이해하더라도 코드 섹션의 기계어를 분석하기 쉽지 않아 거의 블랙박스로 취급되고 있다. 그러나 많은 공격자들은 기계어로 생성된 바이너리 파일을 대상으로 디스어셈블러와 디컴파일러를 활용해 간소화된 소스코드를 추출하고 있으며, 이러한 소스코드를 바탕으로 코드들의 계층 구조 및 제어 흐름을 분석하고 있다. 이를 소프트웨어 역공학이라 하며, 아래 그림은 역공학을 통한 소스코드 추출 과정을 보여주고 있다[6].



(그림 1) 역공학을 통한 소스코드 추출 과정

악성코드 분석, 소프트웨어 보안성 테스트 등 다양한 목적을 위해 역공학이 사용되고 있으며, 이를 지원하기 위해 다양한 디스어셈블 및 디컴파일 도구들이 사용되고 있다. 대표적인 역공학 도구로는 IDA Pro, OllyDbg 등이 있으며, 아래는 IDA Pro를 이용하여 소프트웨어의 기계어 함수 구성 및 흐름을 분석하는 화면이다[7][8].



(그림 2) IDA Pro를 이용한 분석 예시 화면

산업제어시스템에서 사용되는 바이너리 파일 중 제조사에서 공개하고 있는 일부 파일들은 공격자가 역공학을 통해 소스코드를 추출하는데 사용되기도 한다. 원자력시설에서 사용되는 제어시스템의 경우에는 전용시스템으로 만들어지거나 보안 상의 문제로 일반적인 산업제어시스템 대비 외부 공개가 훨씬 제한적인 상황이다. 그럼에도 동일 제조사가 만든 제어시스템의 경우 유사하거나 동일한 라이브러리를 사용하는 경우가 있기 때문에 이를 공격자가 파악하여 분석하게 된다면 원자력시설의 제어시스템에 대한 사이버공격에 사용될 가능성도 있다.

4. 코드 난독화

앞서 설명한 바와 같이 공격자는 특정 시스템의 바이너리 파일을 확보한 후 역공학을 수행하여 어셈블리 코드나 소스코드를 추출하고 이를 분석해 해당 시스템의 취약점을 찾아낸다. 이러한 공격을 예방하기 위해서 코드 난독화를 적용할 수 있다. 코드 난독화는 프로그램 변환 기법의 일종으로 역공학을 사용해 소프트웨어의 행위를 분석하는 것을 어렵게 만들기 위해 프로그램의 원래 의미는 보존하면서 코드의 일부 혹은 전체를 변형하는 프로그램 보호 기법을 말한다. 프로그램의 원래 의미를 보존하기 위해서는 반드시 코드 변형 후에도 변형 전과 동작이 동일해야 한다[9].

코드 난독화는 난독화 대상에 따라 바이너리 난독화와 소스코드 난독화로 분류할 수 있다. 바이너리 난독화는 컴파일 후에 생성된 바이너리 자체에 대해 역공학을 통해 분석하기 어렵도록 변형하는 것이다. 대표적으로 예로 프로그램 언어 특성에 맞게 심볼 정보를 제거하거나 심볼 이름을 변경하는 방법을 통해 공격자가 바이너리를 이해하고 분석하는데 지장을 주는 것이 있다. 소스코드 난독화의 경우 프로그램의 소스코드를 알아보기 힘들게 변형하는 것으로서 특정 코드를 과도하게 복잡하게 만들거나 아무 것도 수행하지 않는 코드를 추가하는 방법, 서로 관련이 없는 다양한 함수들을 섞는 방법, 데이터를 알아보기 어렵게 변경하거나 변수명에 의미가 포함되지 않도록 일반화하는 방법, 주석의 정보를 제거하는 방법 등이 이에 해당한다[10][11]. 이러한 방식을 통해 소스코드를 난독화한 후 컴파일을 통해 바이너리를 만들게 되면 해당 바이너리를 분석하기가 어려워지며, 소스코드 자체가 유출되는 경우에도 분석에 많은 지장을 줄 수 있게 된다.

5. 코드 난독화 적용을 위한 고려사항

이러한 코드 난독화 기법을 핵심디지털자산의 소프트웨어에 적용하기 위해서는 다음의 조건들을 적용하는 것이 필요하다. 난독화는 공격자가 핵심디지털자산의 취약점을 분석하는데 보다 많은 시간과 비용을 소모시켜 공격을 어렵게 만들지만 침투 자체를 완벽히 불가능하게 할 수는 없으며, 난독화를 높은 수준으로 적용할수록 시스템의 성능을 저하시키고 비용이 증가하게 된다. 따라서 난독화에 투입되는 비용과 효과를 분석하여 난독화의 범위와 수준을 결정하는 것이 필요하다. 또한, 난독화로 인해 변형된 코드는 변형 전과 동일하게 동작해야 하며[6], 높은 수준의 난독화는 시스템에 부하를 발생시켜 성능을 저하시킬 수 있으므로 난독화가 적용된 후에도 시스템에 요구되는 최소 성능을 보장할 수 있어야 한다. 디버깅 및 유지보수에 영향을 주지 않기 위해서 심볼, 주석 등의 정보가 제거되더라도 추적 가능하도록 해당 정보들을 별도로 보관하는 등의 추가적인 조치가 필요하다. 이러한 조건들을 통해 난독화로 인한 부작용을 방지할 수 있을 것이다.

핵심디지털자산의 소프트웨어에 코드 난독화 기법을 적용한다면 공격자들이 핵심디지털자산의 취약점을 분석하는데 보다 많은 시간과 비용이 소모될 것이며 이를 통해 사이버공격을 예방하고 완화시키는데 도움을 줄 수 있을 것으로 기대한다. 다만, 프로그램 업데이트가 자주 일어나지 않는 환경에서는 효과가 저하될 수 있기 때문에 현재의 원자력시설 환경에서 코드 난독화 만으로는 취약점 분석을 통한 사이버공격을 원천적으로 막기 어려울 수도 있다는 점도 같이 고려되어야 한다. 또한, 코드 난독화를 적용하는 보안조치들은 대부분 설계단계에서만 적용이 가능하며 시스템의 성능과 이에 따른 안전 요건에 영향을 줄 수도 있기 때문에, 신규 원자력시설 건설 혹은 기존 시설의 설비 개선 시 시스템 설계 단계에서부터 보안요건과 안전요건을 모두 고려하여 진행되어야 할 것이다.

5. 결론

본 연구에서는 원전 사고와 직접적으로 관련된 핵심디지털자산에 대해 기존의 KINAC/RS-015 대비 추가적으로 적용이 필요한 보안 요구사항 중 하나로 코드 난독화를 제시하였다. 이러한 코드 난독화와 몇 가지 추가적인 보안조치를 핵심디지털자산에 적용한다면 원자력시설의 보안성을 보다 강화할

수 있을 것으로 기대된다.

ACKNOWLEDGMENT

본 연구는 원자력안전위원회의 재원으로 한국원자력안전재단의 지원을 받아 수행한 원자력안전연구사업의 연구결과입니다. (No. 1605007)

참고문헌

- [1] IAEA, "Computer Security at Nuclear Facilities," Nuclear Security Series(NSS) 17, 2011.
- [2] U.S.NRC, "Cyber Security Program for Nuclear Facilities," Regulatory Guide 5.71, 2010.
- [3] 한국원자력통제기술원, "원자력시설의 컴퓨터 및 정보시스템 보안," KINAC/RS-015, 2016.
- [4] Kookheui Kwon, "Research on Vital Assets for Nuclear Cyber Security," ANS 2017 International Topical Meeting on Probabilistic Safety Assessment and Analysis, 2017.
- [5] NIST, "Security and Privacy Controls for Federal Information Systems and Organizations," NIST 800-53 Revision 4, 2013.
- [6] C. Cifuentes, "An environment for the reverse engineering of executable programs," 2nd Asia-Pacific Software Engineering Conference(APSEC), 1995.
- [7] IDA, <https://www.hex-rays.com/products/ida>
- [8] OllyDbg, <http://www.ollydbg.de/>
- [9] C. Collberg, C. Thomborson, and D. Low, "A Taxonomy of Obfuscating Transformations," Technical Report #148, The University of Auckland, 1997.
- [10] J. Viega, "Building Secure Software: How to Avoid Security Problems the Right Way," Addison-Wesley, 2011.
- [11] S. Banescu, C. Collberg, V. Ganesh, Z. Newsham, and A. Pretschner, "Code Obfuscation Against Symbolic Execution Attacks," 32nd Annual Conference on Computer Security Applications, ACM, 2016.

코드기반암호를 활용한 IoT 환경 보안 프로토콜 설계

장경배*, 심민주*, 서화정* †

*한성대학교 IT 융합공학과

starj1023@gmail.com, minjoos9797@gmail.com, hwajeong84@gmail.com

Design of IoT Environment Secure Protocol Using Code-Based Cryptography

Kyung-Bae Jang*, Min-Joo Sim*, Hwa-Jeong Seo*†

*Dept. of IT Convergence Engineering, Hansung University

요 약

IoT(Internet of Things) 시대가 활성화되면서 개인정보를 포함한 많은 정보들이 IoT 디바이스들을 통해 전달되고 있다. 정보보호를 위해 암호화하여 통신하는 것이 중요하며 성능의 제한으로 인해 경량 보안 프로토콜 사용이 요구된다. 현재 많은 암호 시스템들은 인수분해 그리고 이산대수의 어려움에 기반하고 있다. 하지만 양자 알고리즘이 실현 가능한 양자 컴퓨터가 개발된다면 앞선 문제들을 쉽게 해결할 수 있다. 이에 본 논문에서는 양자내성암호 중 코드기반암호를 사용한 경량 보안 프로토콜을 제안한다. 기존 프로토콜과 비교 분석해보고 안전성 분석 또한 실시하였다.

1. 서론

현대에 있어 IoT[1] 기술의 중요성은 점차 부각되지만 사용자의 개인정보를 보장하고 민감 데이터를 보호하는데 있어 많은 문제와 위험도 따른다. 만약 헬스케어 시스템 이용자에 대한 거짓 의료정보를 의사에게 전송한다면 의사는 잘못된 처방을 내릴 수 있다.

이러한 보안 위협에 대처하기 위해서는 서로의 신원을 올바르게 확인하고 통신할 수 있는 보안 프로토콜이 필요하다. 이때 IoT 디바이스의 제한된 성능 탓에 경량 설계가 요구되므로 사용하는 암호화 방식도 경량 암호화 방식을 사용해야 한다.

현재 ECC(Elliptic Curve Cryptography)를 많은 곳에서 경량 공개키 암호로 사용하고 있으며 대표적으로 2017년 Wang의 프로토콜[2] 또한 그렇다. 하지만 양자 컴퓨터가 개발된다면 더이상 사용할 수 없다는 문제점이 있다.

이에 기존 암호시스템들을 무너뜨릴 수 있는 양자 컴퓨터의 계산 능력에 내성을 가진 양자내성암호 연구가 이루어지고 있다. 미국 NIST(National Institute of Standards and Technology)에서는 2016년 양자내성암호 표준화 공모전을 주최 하였고 세계 여러 각국에서 양자내성암호 알고리즘을 제출하였다. 현재 26개 후보들이 살아남아 Round2에 대한 평가를 진행 중이며 코드, 격자, 다변수다항식, 아이소제니 기반암호들로

구성되어 있다.

이에 본 논문에서는 NIST 양자내성암호 공모전을 진행중인 코드기반암호 중 ROLLO를 활용하여 경량 보안 프로토콜을 설계하였다. IoT 환경을 대상으로 하기 때문에 암호화 횟수를 최소로 수행하고, 상대적으로 연산이 적은 해시 연산과 XOR 연산을 사용하여 설계하였다. 또한 통신과정에서 가능한 다양한 공격들을 가정하여 안전성 분석을 실시하였다.

2. 관련 연구

2.1 코드기반암호

코드기반암호의 원리는 송신자가 메시지에 고의로 수정 가능한 오류를 첨부한다. 그리고 올바른 수신자는 오류수정코드를 알고 있어 첨부된 오류를 손쉽게 수정할 수 있다. Robert J. McEliece는 1978년, 최초의 코드기반암호 McEliece[3]를 제안하였다.

McEliece에서는 Goppa 코드라는 오류수정코드를 사용하는데 현재 NIST 양자내성암호 공모전 Round 2, 7개의 코드기반암호 중 Classic McEliece와 NTS-KEM이 Goppa 코드를 그대로 사용하고 있다. Goppa 코드는 역사가 길어 뛰어난 보안성을 자랑하지만 키 사이즈가 매우 크다는 단점이 있다. 하지만 한계점인 키 사이즈를 줄이기 위해 Goppa 코드가 아닌 새로운 코드를 사용하는 연구가 진행중이며 Quasi Cyclic, Rank metric 코드에 기반한 5개의 암호가 Round 2를 진행중

이다.

2.2 ROLLO

ROLLO[4]는 양자내성암호 표준화 공모전 Round2를 진행중인 코드기반암호이다. Goppa 코드가 아닌 효율성을 증시한 Rank Metric 코드(1991)를 기반으로 하여 키 사이즈와 계산 복잡도 측면에서 매우 효율적이다. Goppa 코드를 사용하는 Classic McEliece 와 NTS-KEM 과의 성능 비교를 위해 저전력 모바일 프로세서인 ARM 에서 속도를 측정하였다. 실험 환경과 연산 속도 비교 결과는 표 1, 표 2 와 같다.

<표 1> 실험 환경

	Raspberry Pi B+
CPU	ARM Cortex-A53@1.4 GHz
Memory	1GB LPDDR2 SDRAM
OS	Raspbian

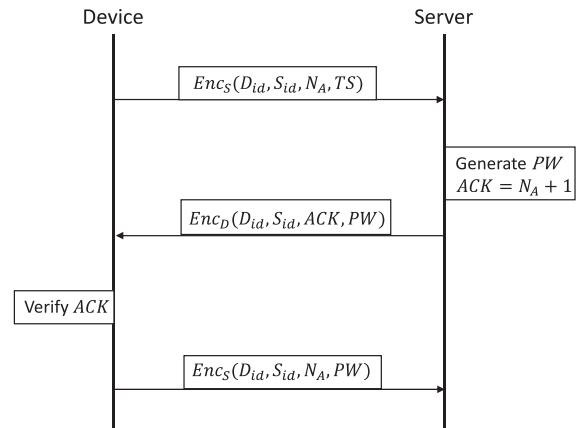
<표 2> 연산 속도(ms) 비교

	Key Gen	Enc	Dec
mcEliece348864	1780.94	0.84	247.94
mcEliece460896	3864.43	2.52	630.32
nts kem 12 64	291.66	1.28	9.8
Rollo-I-128	8.19	1.21	4.27
Rollo-II-128	73.94	6.89	19.84
Rollo-III-128	1.67	2.62	3.98

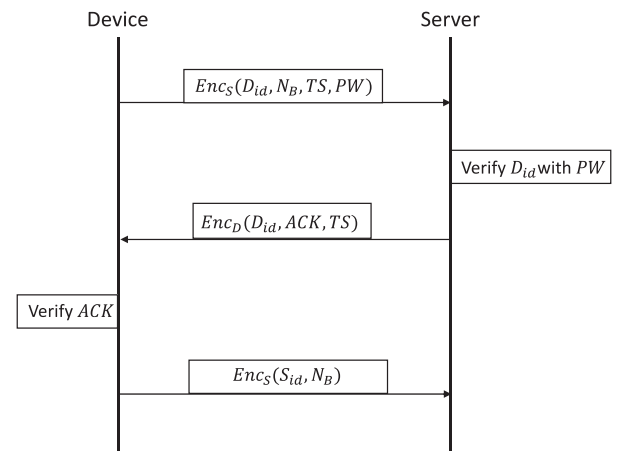
40 년의 역사를 가지고 있는 Goppa 코드에 비하여 Rank Metric 코드는 상대적으로 짧은 검증 시간을 가지고 있지만 높은 성능을 보여준다. 128-bit 보안 레벨 기준으로 Classic McEliece 의 공개키는 261120 바이트, 개인키가 6452 바이트인 반면, ROLLO 의 공개키는 634 바이트, 개인키는 40 바이트로 훨씬 작은 키 사이즈를 제공한다. 본 논문에서 제안하는 프로토콜의 암호화 기법은 ROLLO-I, II, III 중 II 을 선택하였다. ROLLO-I, ROLLO-III 는 KEM(Key Encapsulation Mechanism) 방식으로 자체적으로 세션 키를 설립하지만 ROLLO-II 는 메시지 암호화에 적합한 PKE(Public Key Encryption) 방식을 제공하기 때문이다.

2.3 Kumar S. Roy's Protocol

2019 년 Kumar S. Roy 는 코드기반암호 McEliece 를 사용하여 경량 보안 프로토콜[5]을 제안하였다. 등록과 인증 2 가지 절차로 구성되며 그림 1, 그림 2 와 같다. 암호화는 등록 과정에서 3 번, 인증 과정에서 3 번 수행된다. Kumar S. Roy 의 프로토콜은 5 장에서 보다 세부적으로 살펴보면 제안하는 프로토콜과 성능 및 안정성 측면에서 비교 분석하고자 한다.



(그림 1) 등록 절차



(그림 2) 상호 인증 절차

3. 제안 프로토콜

제안하는 보안 프로토콜은 다음 두가지로 구성된다. 적합 디바이스를 서버에 등록하는 절차와 등록된 디바이스가 서버와 상호 통신하기 위한 인증 절차로 이루어진다. 암호화 기법으로는 양자컴퓨터의 공격에 내성을 가질 수 있도록 코드기반암호 ROLLO-I, II, III 중 II 을 사용하였다.

ROLLO-I, ROLLO-III 는 KEM(Key Encapsulation Mechanism) 방식으로 자체적으로 세션 키를 설립하지만 ROLLO-II 는 PKE(Public Key Encryption) 방식이기 때문이다. 또한 경량 설계를 위해 암호화 횟수를 최소로 수행하고 나머지 연산들은 해시 함수와 XOR 연산 만을 사용하였다. 프로토콜 설명을 위한 표기법은 표 3 과 같다.

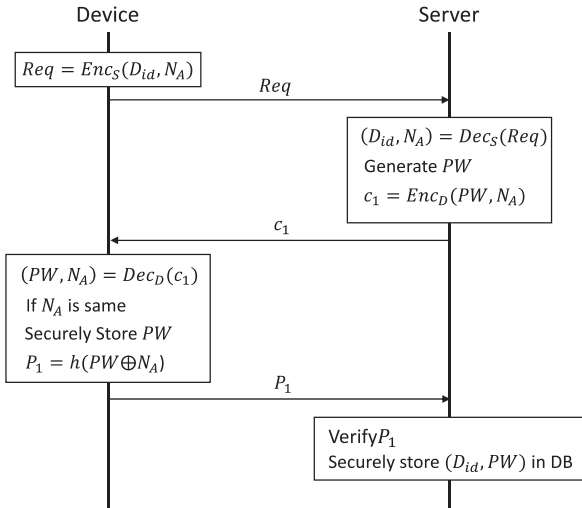
<표 3> 표기법

Notation	Meaning
Req	Request message for registration
Enc_S	Encrypt with server's public key
Dec_S	Decrypt with server's private key
D_{id}	Device id
S_{id}	Server id
N_A, N_B	Nonce value

TS	Time stamp
PW	Password
PW_{temp}	Temporary password
h	Hash function
DB	Database
SK	Session key

3.1 디바이스 등록

디바이스가 서버에 등록되는 단계는 총 4 단계로 구성되며 그림 3 과 같다.



(그림 3) 등록 절차

첫번째, 서버에 등록을 원하는 디바이스는 자신의 디바이스 id 와 nonce 값을 서버의 공개키로 암호화하여 전송한다.

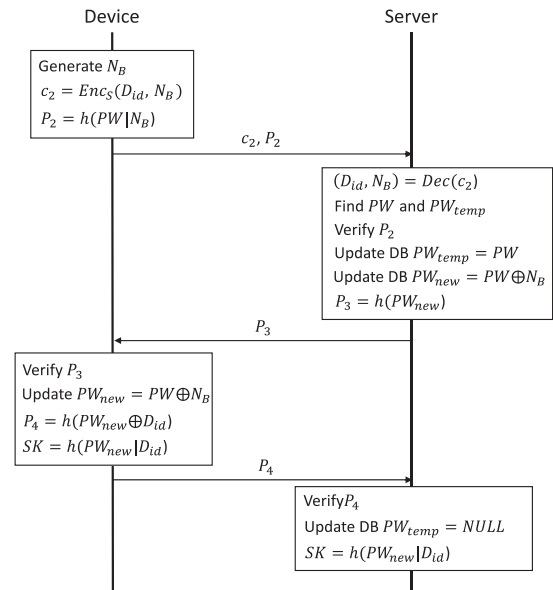
두번째, 서버는 수신한 메시지 Req 를 자신의 개인키로 복호화 하여 디바이스 id 와 nonce 값을 확인한 뒤 해당 디바이스를 위한 패스워드를 생성한다. 그리고 서버의 신원확인이 가능한 nonce 값과 생성한 패스워드를 해당 디바이스의 공개키로 암호화하여 전송한다.

세번째, c_1 을 수신한 디바이스는 자신의 개인키로 복구한 nonce 값이 일치한다면 패스워드를 안전하게 저장한다.

마지막으로 $P_1 = h(PW \oplus N_A)$ 를 계산하여 서버에 전송한다. 해시의 입력 값을 알고있는 서버는 P_1 의 검증 수행한 뒤, 데이터베이스에 디바이스 id 와 패스워드를 저장한다.

3.2 디바이스 서버간 상호 인증

등록절차를 거친 디바이스가 서버와 통신하기 위한 상호 인증은 총 4 단계이며 그림 4 와 같다.



(그림 4) 상호 인증 절차

첫번째, 생성한 nonce 값과 자신의 디바이스 id 를 서버의 공개키로 암호화한 c_2 그리고 등록 시 부여 받은 패스워드와 nonce 값으로 $P_2 = h(PW | N_B)$ 를 계산하여 서버에 전송한다.

수신한 서버는 자신의 개인키로 복호화 한 디바이스 id 와 데이터베이스를 대조하여 해당 디바이스의 패스워드와 임시 패스워드를 조회한다. nonce 값과 두 가지 경우의 패스워드 해시 값 P_2 가 검증된다면 기존 패스워드를 임시 패스워드로 바꾸고 새로운 패스워드를 $PW_{new} = PW \oplus N_B$ 로 업데이트한다. 그리고 새로운 패스워드를 해시 한 값을 전송한다.

디바이스는 자신의 패스워드와 자신이 생성했던 nonce 값으로 P_3 를 검증한다. 검증이 완료되면 서버와 같이 자신의 패스워드를 새로 갱신한 뒤, $P_4 = h(PW_{new} \oplus D_{id})$ 를 계산하여 전송하고 세션 키 $SK = h(PW_{new} | D_{id})$ 를 설립한다.

마지막으로 서버는 동일하게 해시의 입력 값을 구성하여 P_4 가 검증되면, 임시 패스워드를 삭제하고 디바이스와 동일하게 세션 키를 설립한다.

4. 안전성 분석

4.1 디바이스 익명성 및 정보 기밀성

제안하는 프로토콜의 등록, 상호 인증 초기에 디바이스의 신원을 추측할 수 있는 디바이스 id 를 암호화하고 nonce 값으로 인해 암호문도 항상 변한다. 때문에 어떤 디바이스가 어느정도 통신하고 있는지 추적이 불가능하다.

또한 적합한 사용자만이 송수신되는 정보를 알 수

있어야 한다. 제안하는 프로토콜에서는 중요 정보들이 암호 기법, 해시 함수를 통해 암호화 되기 때문에 적합하지 않은 사용자는 디바이스 id, nonce 값, 패스워드와 같은 정보에 접근할 수 없다.

4.2 중간자 공격, 재전송 공격

제안하는 프로토콜에선 디바이스를 등록하고 세션을 설립하는 과정 모두에서 인증 메시지 P 를 통해서로의 통신 사실을 확인하고 있기 때문에 중간자 공격에 대한 보안성을 확보할 수 있다.

재전송 공격에 대해서는 세션 초기에 생성한 nonce 값이 암호화 되어 전송되거나, 전송되는 해시 입력 값에 영향을 주기 때문에 모든 메시지에 nonce 값이 관여하게 된다. 따라서 이전 세션에서 사용된 메시지의 내용이 그대로 사용 된다면 재전송 공격이라 판단하여 방어할 수 있다.

4.3 PFS(Perfect Forward Secrecy)

PFS 의 달성을 위해선 개인키가 노출되어도, 과거에 도청당한 통신 기록들의 보안이 지켜져야 한다. 제안하는 프로토콜에선 디바이스가 탈취되어 패스워드가 노출된다 해도 nonce 값을 알아내지 못하면 갱신되기 전의 패스워드를 추적할 수 없기 때문에 이전 통신 기록을 해킹할 수 없다. 따라서 최종적으로 PFS 를 달성할 수 있다.

5. 비교 분석

5.1 프로토콜 성능

Kumar S. Roy 의 프로토콜은 암호화 기법으로 Goppa 코드 기반의 McEliece 를 사용한다. McEliece 의 연산 속도는 빠르지만 키 사이즈가 매우 크다. 대표적으로 Round2 를 진행중인 Classic McEliece 는 8-bit AVR 프로세서에는 저장할 수 없을 만큼 키 사이즈가 크다. 하지만 제안하는 프로토콜에서는 적합한 키 사이즈를 제공하며 연산 속도 또한 준수한 ROLLO 를 사용하였다. ARM 프로세서에서 프로토콜의 성능을 측정하였으며 표 4 와 같다.

<표 4> 성능 측정(ms)

	Registration	Authentication
Proposed Protocol	82	41

암호화에는 많은 연산이 요구되기 때문에 경량 프로토콜 설계를 위해서는 수행되는 암호화 횟수가 중요하다. Kumar S. Roy 의 프로토콜은 등록 과정에서 3 번, 인증 과정에서 3 번의 암호화가 수행되는 반면 제안 프로토콜에서는 등록 과정에서 2 번, 인증 과정에

서는 1 번만 수행된다. 등록 과정은 초기에 각자의 신원을 확인해야 하기 때문에 디바이스에서 1 번, 서버에서 1 번, 총 2 번의 암호화를 수행하였다. 인증 과정에서는 패스워드와 익명성을 위한 디바이스 id 암호화 1 번만을 수행하고 이후로는 인증된 패스워드와 해시 함수를 활용하여 서로의 신원을 밝혔다.

5.2 프로토콜 안전성

PFS 달성의 측면에서 바라보았을 때, Kumar S. Roy 의 프로토콜은 통신과정에서 패스워드, 개인키를 정적으로 사용한다. 때문에 디바이스가 탈취되어 개인키와 패스워드가 노출되었을 때, 과거의 통신 기록이 해킹 당할 수 있다. 하지만 제안하는 프로토콜은 통신 후 패스워드를 업데이트 하기 때문에 과거의 통신 기록 해킹에 필요한 패스워드를 알 수 없다.

6. 결론

본 논문에서는 다가오는 양자컴퓨터 시대를 대비하여 코드기반암호를 활용한 경량 보안 프로토콜을 설계하였다. 키 사이즈가 작고 연산 속도가 빠른 ROLLO 를 사용하였으며 암호화 수행 횟수를 줄이고 해시 함수와 XOR 연산을 사용하였다. 제안 프로토콜의 구현 코드는 Github[6]에 공개되어 있으며 향후 연구 방향으로 프로토콜 안전성 분석에 범용적으로 사용되는 AVISPA 툴[7]을 활용한 자동화 분석과 경량 설계를 위한 개선을 진행할 예정이다.

참고문헌

- [1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (IoT): A vision, architectural elements, and future directions ", Future Gen. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, 2013.
- [2] Wang KH, Chen CM, Fang W, Wu TY "A secure authentication scheme for internet of things" Pervasive Mobile Comput 42:15–26, 2017.
- [3] R. J. McEliece "A Public-Key Cryptosystem Based On Algebraic Coding Theory", Technical report, NASA, 1978.
- [4] C. A. Melchor, etc "ROLLO –Rank-Ouroboros, LAKE & LOCKER", Submission to the NIST post quantum standardization process, Round 2, 2019.
- [5] K. S. Roy, H. K. Kalita, "A Code based Light-weight Authentication Scheme for IoT in Fog Computing Environment", Jour of Adv Research in Dynamical & Control Systems, vol. 11, 06-Special Issue, 2019.
- [6] Github: source code (Internet). Available: <https://github.com/starj1023/Code-Based-Protocol-ROLLO->
- [7] Armando A, etc, "The AVISPA tool for the automated validation of internet security protocols and applications. In: International Conference on Computer Aided Verification", Springer, pp 281–285, 2005.

공동 현관 비밀번호 유출 방지를 통한 블록체인 기반의 안전한 배송 시스템

김현지*, 권용빈*, 최승주*, 서화정*[†]

*한성대학교 IT융합공학부

khj1594012@gmail.com, vexyoung@gmail.com, bookingstore3@gmail.com,

Hwajeong84@gmail.com

Secure delivery system based on blockchain through preventing leakage of common entrance password.

Hyun-Ji Kim*, Yong-Been Kwon*, Seung-ju Choi*, Hwa-Jeong Seo*[†]

*Dept. of IT convergence engineering, Hansung University

요 약

최근 변화하는 소비패턴으로 인해 당일 및 새벽 배송 등의 서비스가 보편화되고 있다. 해당 서비스는 배송 정보를 입력 시 건물에 자유롭게 출입할 수 있는 공동 현관 비밀번호를 기입해야 한다. 이는 이미 빈번하게 발생하고 있는 무단 주거 침입 등의 범죄에 더 쉽게 노출되도록 할 수 있는 위험 요소이다. 본 논문에서는 신뢰할 수 있는 사용자만이 참여 가능한 프라이빗 블록체인 네트워크에서의 차량 번호판 인식 및 스마트 컨트랙트를 통해 랜덤한 마스터 비밀번호를 제공하여, 보안적으로 취약한 비밀번호 기입 절차를 없애고 검증 받은 사용자에게만 출입을 허가하는 방식을 제안한다.

1. 서론

최근 발생한 코로나 바이러스 감염증-19 (COVID-19)로 인해 생활 및 소비패턴이 변화하고 있다. 특히, 일상생활에서 거를 수 없는 요소인 배달 음식과 신선식품 전자상거래의 수요가 가파르게 증가하였으며, 당일 및 새벽 배송 업체는 최근 평균 300만개의 주문량을 기록했다.

관련 어플리케이션을 사용해보면 빠른 배송 서비스를 제공하기 위해 새벽 배송을 하고 있으며 이를 위해 공동현관 비밀번호를 직접 명시하도록 되어있다. 해당 비밀번호는 각 세대별 비밀번호와 마스터 비밀번호로 구성되어 있으며, 초기 설정 후 거의 바꾸지 않기 때문에 노출되면 외부인의 자유로운 출입이 가능해진다. 이러한 배송 시스템은 관련 범죄들에 더 쉽게 노출될 수 있다.

최근 5년간의 경찰청 범죄 통계에 따르면, 택배기사를 사칭하여 무단으로 주거침입을 하는 등의 관련 범죄들이 1600건 이상 발생하였고, 배송 업체 직원들 간에 공동 현관 비밀번호를 공유하고 심지어 이를 악용하는 사례도 있다.

따라서 앞으로 보편화 될 전망인 배송 서비스는 더욱 안전하게 운영되어야 할 필요가 있다.

2. 관련 연구

2.1 스마트 컨트랙트

스마트 컨트랙트는 실행 조건과 계약 내용을 구현한 코드이며 해당 조건을 만족하면 자동으로 계약 내용을 수행한다. 디지털 데이터의 경우 위변조의 문제가 존재하지만 이를 블록체인 플랫폼에서 적용할 경우 정보의 무결성이 보장되어 제 3자의 개입 없이 신뢰할 수 있는 거래가 가능하다[1].

트랜잭션 발생 시 블록체인 상의 모든 노드는 해당 트랜잭션을 공유하여 블록을 생성한 후 브로드캐스팅한다. 블록을 전달 받은 노드들은 해당 블록을 각자의 블록체인에 추가한 후 동기화한다. 이러한 과정을 통해 모든 데이터가 공유 및 기록되기 때문에 계약 내용을 조작할 수 없다. 또한 추적이 가능하며 실행 조건 만족 시 자동 이행되므로 거래 비용을 줄일 수 있다.

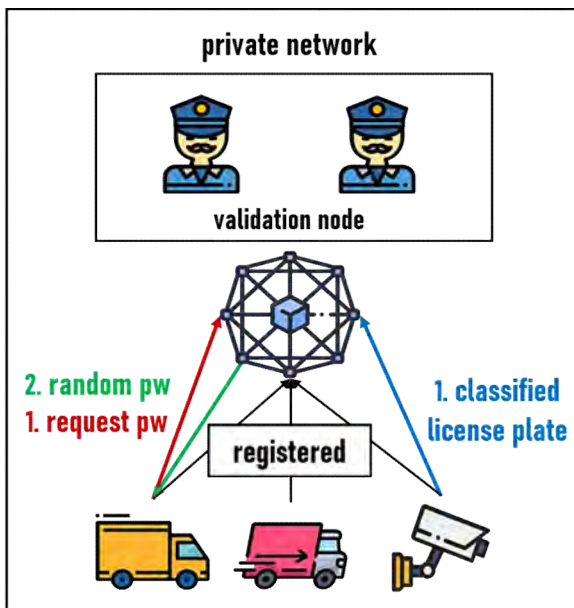
2.2 차량 번호판 인식

노이즈 필터링과 외곽선 검출 등의 영상 처리 과정을 거쳐 차량 번호판을 검출해낼 수 있다. 또한, Convolutional Neural Network 등의 딥 러닝 모델을 통해 번호판 이미지를 학습하여 검출해낼 수도 있으며 현재 상용화 되어 사용되고 있는 기술이다.

3. 시스템 제안

본 논문에서 제안하는 시스템은 프라이빗 블록체인 네트워크를 활용하여 허가 받은 노드만이 참여 가능하며 배송 차량 노드, 차량 인식 카메라 노드, 경비실 노드로 구성된다. 합의 알고리즘으로는 권한 증명(Proof of Authentication, PoA)을 사용하여 신원이 검증된 경비실 노드를 검증 권한이 있는 노드로 사전 승인한다.

그림 1은 제안 시스템의 동작과정을 나타낸 구성도이다. 해당 시스템을 이용하기 위해 배송 차량 노드와 차량 인식 카메라 노드를 해당 블록체인 네트워크에 사전 등록한다. 배송 차량이 아파트 입구에 들어서면 차량 인식 카메라 노드는 해당 차량의 번호판을 인식하고 배송 차량은 랜덤 마스터 비밀번호를 요청한다. 사전 등록된 정보와 일치하는지 확인한 후 랜덤 마스터 비밀번호를 제공하며, 해당 비밀번호는 일정 시간 후 폐기된다.



(그림 1) 시스템 구성도.

3.1 노드

제안 시스템은 신원이 확인된 차량 및 차량 인식 카메라만이 프라이빗 블록체인 네트워크에 노드로서 참여할 수 있고, 사전에 등록된 정보와의 비교를 통해 인증을 받아야 마스터 패스워드를 얻을 수 있다.

3.1.1 배송 차량 노드

대부분의 배송 시스템은 각 배송 차량에 할당된 지역이 있으므로 프라이빗 블록체인 네트워크에 신원이 확인된 배송 차량의 정보가 사전 등록되어 있으며 항목은 표1과 같다. 배송 차량의 번호판, 계정

주소, 트랜잭션 생성 시 입력할 비밀번호가 등록되어 있으며 해당 비밀번호를 입력하여 랜덤 마스터 패스워드를 요청한다.

<표 1> 배송 차량 노드의 사전 등록 정보

registered infomation
license plate
account address
key

3.1.2 차량 인식 카메라 노드

차량 인식 카메라 노드 또한 신원이 확인된 기기를 사용하며 표2와 같은 해당 기기의 정보를 프라이빗 블록체인 네트워크에 사전 등록한다.

<표 2> 차량 인식 카메라 노드의 사전 등록 정보

registered infomation
device id
account address

배송 차량이 입구에 들어오면 블록체인에 사전 등록된 차량 인식 카메라는 광학 문자 인식(Optical Character Recognition)을 통해 차량의 번호판을 검출한다. 검출 결과는 해당 기기의 아이디, 계정 주소, 타임 스탬프와 함께 블록체인 네트워크로 전송된다.

3.1.3 경비실 노드

신뢰할 수 있는 데이터를 통해 신원이 검증되어 사전에 권한을 얻은 노드로서, 권한증명(PoA) 합의 알고리즘을 통해 배송 차량 노드와 카메라 노드로부터 발생한 트랜잭션의 유효성을 검증하고 블록체인 네트워크에 반영하는 역할을 한다.

3.2 스마트 컨트랙트

배송 차량 노드에서 서버에 저장된 값과 동일한 비밀번호를 입력하여 랜덤 마스터 비밀번호를 요청하는 트랜잭션이 생성되고, 동시에 차량 인식 카메라 노드에서는 카메라를 통해 검출한 차량 번호판 정보를 전송하는 트랜잭션이 생성된다. 생성된 두 트랜잭션은 각각 다른 컨트랙트 어카운트로 전송되며 해당 컨트랙트들은 내부 코드를 실행한다.

배송 차량 노드로부터 발생한 트랜잭션은 랜덤 마

스터 패스워드를 생성하는 컨트랙트(컨트랙트 A)로 전송된다.

차량 인식 카메라 노드로부터 발생한 트랜잭션은 디바이스 정보와 번호판 검출 결과를 저장하는 컨트랙트(컨트랙트 B)로 전송된다.

컨트랙트A가 컨트랙트 B를 호출하여 차량 인식 카메라의 디바이스 아이디, 계정 주소, 번호판 검출 결과를 얻는다. 사전에 해당 배송 차량 계정에 등록된 정보들을 비교하여 등록된 차량임이 인증될 경우 마스터 랜덤 비밀번호를 전송한다.

<표 3> 스마트 컨트랙트에 저장될 데이터

contract A	contract B
key	account address (camera)
account address	device ID
account address (camera)	license plate
device ID	
license plate	

따라서 자주 갱신하지 않고 공동으로 사용하는 현관 비밀번호를 허가 받지 않은 사용자에게 노출하지 않을 수 있게 되고 발급 받은 랜덤 마스터 비밀번호는 일정 시간 후, 트랜잭션 발생 시 랜덤으로 다시 생성된다. 또한, 출입에 관련된 정보가 블록체인 상에 기록되며 프라이빗 블록체인의 특성 상 책임소재를 파악할 수 있다. 이는 서론에서 언급한 어플리케이션 등을 통해 노출된 현관 비밀번호를 사용하여 택배기사를 사칭하는 등의 악의적인 무단 침입 범죄를 방지할 수 있다.

4. 구현

본 시스템의 구현은 go language를 기반으로 한 go-ethereum(eth)를 사용하여 프라이빗 블록체인 네트워크를 구성한 후 remix와 연동하여 배포하며 솔리디티 언어로 스마트 컨트랙트를 작성한다. 또한 python과 openCV 라이브러리를 활용하여 차량 번호판 인식을 진행하였다.

4.1 네트워크 구성

go language와 geth를 설치한 후 총 5개의 노드 디렉터리와 계정을 생성하여 프라이빗 네트워크를 구성하였다. 해당 네트워크의 노드는 3개의 일반 노드(배송 차량 노드 2개, 차량 인식 카메라 노드 1개)

와 2개의 검증자 노드(경비실 노드)로 구성된다.

genesis 파일을 생성 및 네트워크 설정은 그림2와 같이 puppeth를 통해 진행하였다. 합의 알고리즘은 프라이빗 네트워크에서 더 효율적인 권한증명(PoA)인 clique를 사용하며, 검증자 역할을 할 노드의 계정에 블록 생성을 권한을 승인하였다.

```
INFO [03-30]15:06:44.704] Administering Ethereum network
WARN [03-30]15:06:44.704] No previous configurations found
imhyunji/.puppeth/test2

What would you like to do? (default = stats)
1. Show network stats
2. Configure new genesis
3. Track new remote server
4. Deploy network components
> 2

What would you like to do? (default = create)
1. Create new genesis from scratch
2. Import already existing genesis
> 1

Which consensus engine to use? (default = clique)
1. Ethash - proof-of-work
2. Clique - proof-of-authority
> 2

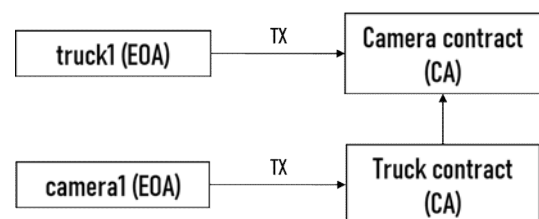
How many seconds should blocks take? (default = 15)
> 15

Which accounts are allowed to seal? (mandatory at least one)
> 0xf84F9D228d7Eb23B6c6EF2AEC1a6e28F8dD6580d
> 0xDe4C256DEd44514F782f4c467b1E7803980b1ca5
> 0x
```

(그림 2) puppeth를 이용한 블록체인 네트워크 설정

4.2 스마트 컨트랙트 구성

본 시스템을 위해 두 개의 스마트 컨트랙트를 작성하였다. 배송 차량이 아파트 입구에 진입할 경우 각 노드는 트랜잭션을 발생시키고 그림 3과 같이 진행된다. 또한, 각 컨트랙트는 표 4, 표 5와 같이 구성된다.



(그림 3) 노드 계정과 스마트 컨트랙트

<표 4> Camera contract

Camera contract	
constructor (생성자)	<pre> constructor(string _plate, string _deviceId) public { camowner = msg.sender; licenseplate = _plate; deviceId = _deviceId; } </pre>
function (함수)	setfromcam

<표 5> Truck contract

Truck contract	
constructor (생성자)	<pre> constructor(uint32 _privatekey) public { truckowner = msg.sender; privatekey = _privatekey; } </pre>
function (함수)	setAddress
	setInfo
	genPW

Camera 컨트랙트의 경우, 차량 인식 카메라로부터 검출한 번호판 데이터와 해당 카메라의 디바이스 식별자를 매개변수로 받아온다. 스마트 컨트랙트 실행 시 가장 먼저 실행되는 생성자를 통해 표 4의 변수에 저장하며 트랜잭션을 발생시킨 계정의 주소는 camowner로 설정한다. 해당 정보들은 setfromcam 함수를 통해 camowner를 키값으로 하는 구조체 배열(Infocams)의 각 멤버변수에 저장된다.

Truck 컨트랙트는 배송 차량이 사전에 등록한 비밀번호를 입력하여 트랜잭션을 발생시키면 생성자를 통해 트랜잭션을 생성한 계정과 입력한 비밀번호를 저장한다.

해당 계정에 등록된 정보가 현재 인식한 정보와 동일한지 비교해야하므로 그림 4와 같이 setAddress 함수를 통해 Camera 컨트랙트를 호출한다. 호출한 컨트랙트로부터 번호판 검출 결과와 디바이스 식별자 및 계정 정보를 참조하여 키값이 truckowner인 구조체 배열(trucks)의 각 멤버변수에 저장한다. 이 과정은 그림 5를 통해 확인할 수 있다.

```

Camera c;
function setAddress(address _address){
    c = Camera(_address);
}

```

(그림 4) Camera 컨트랙트 호출

infocams 0x14723A09ACff6D2A60DcF7aA4AFf308FDdC160C 0: address: camaddr 0x14723A09ACff6D2A60DcF7aA4AFf308FDdC160C 1: string: deviceID 1234:5678 2: string: plate 12A3456	trucks 0xCA35b7d915458EF540aDe6068dFe2F44E8fa733c 0: uint32: privatekey 9876 1: address: truckaddr 0xCA35b7d915458EF540aDe6068dFe2F44E8fa733c 2: address: camaddr 0x14723A09ACff6D2A60DcF7aA4AFf308FDdC160C 3: string: plate 12A3456 4: string: deviceID 1234:5678
---	--

(그림 5) 카메라로부터 수신한 정보 저장(왼쪽) 및 Camera 컨트랙트 호출하여 두 트랜잭션에 대한 정보 저장(오른쪽)

이 과정에서 그림 6과 같이 이벤트로그로 기록되므로 차량의 출입에 관한 정보가 남게 되며 이상 트랜잭션 발생 시 추적이 가능하다.

이 후 배송 차량의 계정 주소에 해당하는 정보들을 사전에 등록된 정보와 비교하여, 동일한 경우 genPW 함수를 통해 그림 7과 같은 랜덤 마스터 비밀번호를 발급한다.

```

"tprivatekey": 9876,
"taddr": "0xCA35b7d915458EF540aDe6068dFe2F44E8fa733c",
"cadddr": "0x14723A09ACff6D2A60DcF7aA4AFf308FDdC160C",
"licensePlate": "12A3456",
"dID": "1234:5678",
"length": 5

```

(그림 6) 이벤트로그

```
"uint256: 7860"
```

(그림 7) 발급된 랜덤 마스터 비밀번호

5. 결론

본 논문에서는 프라이빗 블록체인과 차량 번호판 인식 기술을 활용하여 건물 출입에 필요한 마스터 비밀번호를 랜덤하게 발급하는 방법을 제안하였다. 허가 받지 않은 사용자의 경우 비밀번호를 발급 받을 수 없으며, 이를 통해 건물에 자유롭게 출입할 수 있는 비밀번호의 노출 가능성을 줄여 무단 주거 침입 등의 범죄를 예방할 수 있을 것으로 기대된다.

그러나 현재 특별한 신원 확인 절차 없이 관련 업체에 배송 기사로 등록이 가능한 경우가 있어 본 시스템의 적용을 위해서는 신원 확인 절차가 필요하다. 또한 손으로 눌러야 하는 비밀번호는 뒤에서 훑쳐보는 경우 노출될 위험이 있다. 따라서 QR 코드 등을 통해 허가된 사용자만 이용할 수 있도록 하여 보안성을 강화하는 방법 등을 고려할 필요가 있다.

참고문헌

- [1] Jun-hyeok Yun, Mihui Kim. Private Blockchain and Smart Contract Based High Trustiness Crowdsensing Incentive Mechanism. Journal of The Korea Institute of Information Security and Cryptology (JKIISC), 28(4), 999-1007. (2018).
- [2] Chul-Jin Kim. A Static and Dynamic Design Technique of Smart Contract based on Block Chain. Journal of the Korea Academia-Industrial cooperation Society(JKAIS), 110-119. (2018.6)

가상화폐기반 P2P 전기자동차 전력거래 시스템

한예지, 신수정
전북대학교 IT정보공학과
e-mail: yeji5281@gmail.com, ssj4980@hanmail.net

Charging Management based on blockchain for electric vehicles

Ye-Ji Han, Su-Jeong Shin
Department of Information Technology and Engineering,
Jeonbuk national University

요 약

기존의 중앙 집중형 에너지 거래 방식을 블록체인 기반의 분산형 거래방식으로 변경하여 누구나 공급자나 수요자(프로슈머)가 될 수 있고, 투명하고 신뢰성있는 에너지 거래가 이루어지도록 한다. 이러한 거래가 이루어지기 위해 공급자와 수요자를 연결하고, 공급 및 수요를 효율적으로 관리하여 새로운 부가가치를 창출하는 시스템을 개발한다.

1. 서론

파리기후협약 이후 전 세계는 친환경 에너지 개발에 맞춰 기술력을 키우고 있다. 이에 따라 화석 연료를 사용하는 내연기관 자동차를 대신하여 전기자동차가 주목을 받고 있다. 전기자동차가 미래 시대에 적합하다고 여겨지는 이유는 리튬 전고체 배터리의 상용화로 배터리 용량이 늘어날 것으로 전망되기 때문이다. 또한, 가격적 측면에서도 전기자동차는 일반 자동차보다 더 큰 효율성을 가지고 있다. 전기자동차의 배터리 충전 비용은 일반 자동차의 유류값의 절반에도 못 미칠 정도로 저렴하고, 주택가에 충전소를 설치한다면 집에서 전력을 충전하고 바로 출근할 수 있는 생활이 가능하다.

이를 바탕으로 최근에는 개인 간 전력을 공유하는 전력 거래가 해외에서 진행되고 있다는 사례를 찾을 수 있었으며 우리는 이 개인 간의 전력 거래가 자동차라는 매개체를 가진다면 거래를 더 쉽고 활발하게 만들 것이라고 판단했다. 더불어 거래 시스템에 블록체인 기술을 융합하여 중앙 집중형으로 이루어지던 거래를 블록체인 기반의 분산형 거래방식으로 변경할 때 나타나는 이점을 활용하고자 한다.

블록체인은 네트워크에 참여하는 모든 사용자가 관리 대상이 되는 모든 데이터를 분산하여 저장하는 데이터 분산처리기술을 말한다. 따라서 본 논문에서는 투명하고 신뢰성있는 에너지 거래 시스템을 구축하고 수요 및 공급을 효율적으로 관리하여 새로운 부가가치를 창출하는 시스템을 제안한다.

2. 전력 거래 시스템

2-1. EVT 토큰 발행

블록체인 기술의 특징 중 하나인 가상화폐 즉 토큰이라는 개념을 도입한다. 가상화폐는 전기자동차 간의 전력 거래를 위해 정의된 EVT 토큰이며, 전기자동차 간의 전력 거래는 오직 EVT 만을 이용하여 수행될 수 있다. 가상화폐거래는 블록체인 앱(Decentralized application, DAPP) 상에서 이루어지며, 필요할 때 현금화하는 방식으로 진행된다.

EVT는 전세계 토큰의 기준 ERC-20(Ethereum Request for Comment)을 바탕으로 개발되어 화폐 거래뿐만 아니라 자동차 정보와 전력 거래 정보를 기록할 수 있다. 상기 정보는 블록 생성 정보와, 거래하는 전기자동차의 현재 전력 상태, 거래 완료시 전력 상태, 자동차 번호, 차주 이름을 포함한다.

거래 시세에 따라서 1 EVT의 값이 변동될 수 있지만, 개발 단계이기 때문에 1 EVT은 0.1 ether와 같은 가치라고 전제하겠다. 또한, 현재는 전력 거래에 사용하기 위해 발행되는 전체 EVT의 개수를 1,000,000개로 제한한다.

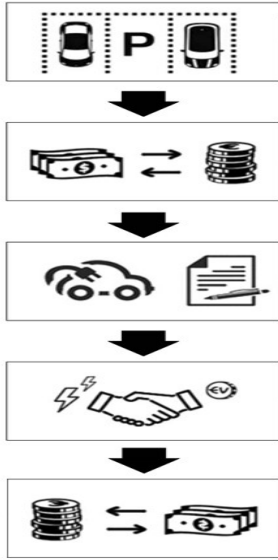
2-2-1. 시스템 개요

공급 전기자동차와 수요 전기자동차 각각으로부터 현재 배터리 용량과 충전 전력의 판매 또는 구매 후의 배터리 용량에 대한 정보를 수신한다.

현재 배터리 용량과 충전 전력의 판매 또는 구매 후의 배터리 용량에 기초하여 전기자동차들의 상태를 고려한 가장 효율적인 공급 전기자동차와 수요 전기자동차를 매칭하거나, 거래 상대 선택 권한을 부여한다.

공급 전기자동차와 수요 전기자동차 간에, 소정 단가에 기초하여 충전 전력의 유상 거래가 성립된다.

유상 거래에 대한 정보를 포함하는 블록을 생성하고,

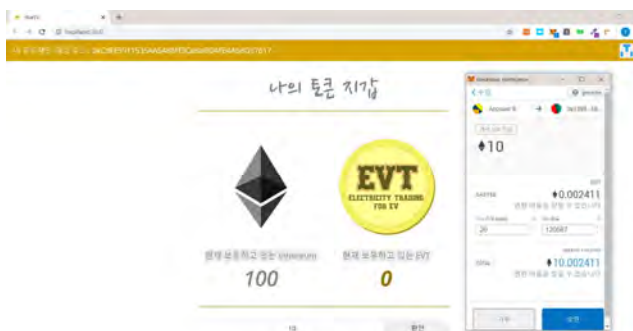


[그림 1] 전력거래 흐름도
생성된 블록을 전력 거래 시스템에 등록된 복수개의 전기 자동차에게 분산하여 전송한다.

2-2-2. DAPP 구현



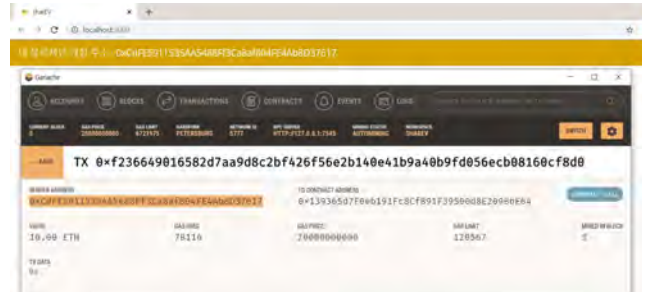
[그림 2] 명령 프롬프트, Genesis block 정보



[그림 3] Dapp 화면, Ethereum과 EVT 환전

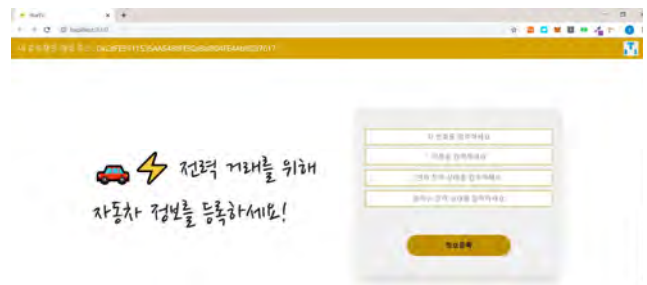
Dapp을 구동하기 위해 Ev Contract를 배포한다. [그림 2]에서 해당 컨트랙트의 블록 정보를 확인 할 수 있다. EVT와 Ether를 동시에 이용하기 위해 사용자(프로슈머)는 블록체인 코인을 관리하는 Metamask 지갑 계정이 요

구된다. [그림3]은 사용자가 ether를 EVT로 환전하는 화면이다. 사용자는 메타메스크 계정으로 로그인 후 웹에 접속하여 원하는 만큼의 환전 금액을 입력한다. 우측 창은 블록에 기록하기 위해 트랜잭션을 승인하는 내용이다. 트랜잭션은 정보를 등록하기 위한 모든 과정에 동일하게 발생된다.



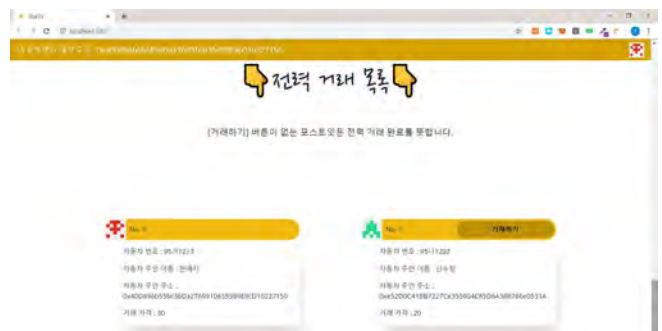
[그림 4] Ganache, 10Eth - 100EVT 환전 내역

[그림 4]처럼 명령프롬프트 뿐만 아니라 Ganache 가상 네트워크 상에서도 실시간으로 블록에 기록된 정보와 이벤트들을 확인 할 수 있다.



[그림 5] 자동차 정보 등록

사용자는 가상 네트워크 상에서 만들어진 계정에 전기자동차의 정보를 입력한다. [그림 5]는 사용자로부터 전기자동차 정보를 받아 블록에 등록하는 화면이다. 본 시스템은 차주 정보(차 번호, 이름)와 현재 전력 상태, 원하는 전력 상태를 수신한다. 현재 전력 상태와 원하는 전력 상태에 기초하여 현재 보유한 전력량보다 원하는 전력량이 적으면 판매자로 등록하고 반대일시 소비자로 등록하여 자동으로 판매자와 소비자를 구분한다.



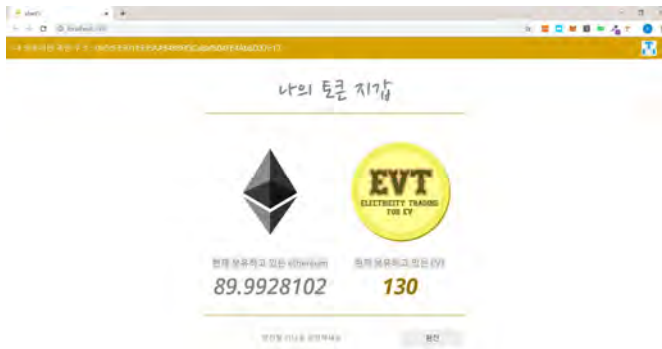
[그림 6] 거래 목록, (좌)거래 완료 (우)거래 가능

입력된 정보는 [그림 6]과 같이 거래 플랫폼에 등록되어 사용자 모두가 확인 할 수 있다. 소비자가 판매자의 정보를 확인하고 자신이 거래하고 싶은 판매자를 선택하여 거래를 진행한다. 혹은 매칭 알고리즘을 통해 판매자와 소비자가 매칭되어 전력을 교환하며 EVT를 이용하여 해당 금액을 전송한다. 현재 알고리즘은 선입선출 알고리즘을 사용하고 있으나 사용자의 요구 전력량을 고려하도록 알고리즘을 보완할 수 있다.



[그림 7] 블록에 등록된 차량 정보

[그림 7]은 사용자 계정의 해시 값과 블록 생성 해시 값이 가지고 있는 정보를 보여준다. 전력 거래가 이루어진 후 거래 내역은 전기자동차 전력 거래 블록체인 시스템 상에 기록이 남게 됨을 증명한다. 블록체인의 거래 내용이 한번 블록에 기록되면 과반수의 동의 없이는 수정될 수 없다는 특성상 거래자 간의 신뢰 형성을 기대할 수 있다.



[그림 8] 거래 완료 후 지갑

[그림 8]을 통하여 전력량 30을 판매 하여 거래가 성립된 후 30 EVT가 나의 토큰 지갑으로 들어 온 모습을 볼 수 있다. 이후 필요한 재환전은 위에서 언급된 환전 방법과 같다.

2-3. 기대 및 전망

본 시스템은 기존의 중앙 집중형 에너지 거래 방식을 블록체인 기반의 분산형 거래방식으로 변경함으로써, 누구나 전력의 공급자나 수요자(프로슈머)가 될 수 있게 한다.

블록체인에 기초하여 전력 거래를 수행함으로써, 투명하고 보안성이 높은 에너지 거래가 이루어질 수 있고, 직접 수요 및 공급을 효율적으로 관리하여 새로운 부가가치를 창출할 수 있다.

전력 거래 시 가상화폐를 사용함으로써, 현금거래 시 필요한 잔돈이나 카드거래 시 필요한 단말기를 없애 빠른 정산이 가능해지고 거래 비용도 감소된다.

나아가, 정부는 전기자동차 사용을 장려하여 친환경 에너지 사업에 도움이 될 수 있다. 전기자동차의 전력뿐 아니라, 탄소 배출권이나 태양광 발전 시설 공유시스템 등 다양한 신재생 에너지의 공유 시스템에도 적용될 수 있다.

플랫폼 제공자는 토큰(가상화폐)을 발행하여 거래 수수료로 이윤을 창출할 수 있으며 거래가 성립될 때 마다 내부에서 자동으로 발생하는 정해진 비율만큼의 수수료를 받을 수 있다.

전기자동차의 차주는 시간대별 전력 가격 차이를 이용하여 이윤을 창출할 수 있다. 현재 한국전력 전기자동차 충전 서비스에 의하면 시간대별 충전 요금(경부하 시간대, 중간부하 시간대, 최대부하 시간대)이 다르게 나누어져 있다.

구분	여름철	봄철 및 가을철	겨울철
경부하 시간대	23~9시	23~9시	23~9시
중간부하 시간대	9~10시, 12~13시, 17~23시	9~10시, 12~13시, 17~23시	9~10시, 12~17시, 20~22시
최대부하 시간대	10~12시, 13~17시	10~12시, 13~17시	10~12시, 17~20시, 22~23시

[표 1] 계절별 적용 시간대

구분	여름철	봄철 및 가을철	겨울철
경부하 시간대	83.6원	84.1원	95.5원
중간부하 시간대	129.0원	90.3원	120.2원
최대부하 시간대	174.3원	92.8원	152.6원

[표 2] 시간대별 충전요금(원/kWh, 부가세 별도, 2020-05 기준)

이와 같이 전기는 시간대마다 가격이 다르다. 따라서, 본 발명에 따른 전력거래 시스템을 이용하여 전기가 저렴할 때 집에서 전기를 충전하고, 전기가 비쌀 때 전력을 필요로 하는 다른 전기자동차에게 전기를 판매할 수 있다.

예를 들어, 여름철을 기준으로 경부하 시간대에 100kWh 충전 시 8360원이 소요된다. 만일, 충전한 전력을 사용하지 않고 다른 전기자동차에 판매한다고 가정하면, 최대부하 시간대에 80kWh 판매 시 13,944원(=174.3원 × 80kWh)의 판매 이득을 얻게 된다. 이 경우, 순이익은 13,944원 - 8360원 = 5584 이 된다.

따라서, 늦은 밤에 집에서 배터리를 완충시키고 필요한 만큼만 남긴 후, 최대부하 시간대에 가지고 있는 전기를 판다면 전력 거래로 수익을 창출할 수 있을 것이다.

3. 결론 및 고찰

본 논문에서 제안하는 시스템은 공급 전기자동차와 수요 전기자동차 간의 이더리움 기반의 토큰 및 전력 거래가 가능하게 하는 프로그램이다. 이더리움 기반의 토큰을 도입하여 수수료 기반의 토큰 경제를 설계할 수 있고, 스마트 계약을 활용하여 거래정보뿐만 아니라 전기자동차의 정보 또한 블록에 저장되는 이점은 앞으로 발생할 무수한 거래의 보안성을 향상시키는데 기여할 것이다.

블록체인 특성상 거래가 발생했을 때 블록이 생성되어야 하고 작업증명을 처리하는 시간이 필요하기 때문에 오랜 시간이 소요된다는 점, 자동차와 자동차 간의 전력 거래를 가능하게 하는 물리적 충전 장치가 개발되어야 한다는 점 등에서 향후 연구가 필요하다.

참고문헌

- [1] 우청원, “에너지블록체인 도입방안 연구”, 과학기술정책연구원, STEPI Insight, 제 222호 2018. 4. 9, pp.8-22
- [2] 이승문, 김재경, “네트워크 기반의 전기자동차 충전인프라 구축 방안 연구”, 에너지경제연구원, 기본연구보고서 16-08, pp.75-113
- [3] 박찬국, “우리나라 P2P 전력거래 가능성 연구”, 에너지경제연구원, 수시연구보고서 15-10, pp.3-7
- [4] 와타나베 아츠시, “블록체인 애플리케이션 개발 실전 입문”, 위키북스, 2017

오픈소스 보안 취약점 및 패치 현황 실시간 알림 시스템

최지은*, 구예림**, 전선진*** 박우인**** 이병희*****

*덕성여자대학교 컴퓨터공학과

**경기대학교 컴퓨터과학과

***송실대학교 소프트웨어학부

****수원대학교 정보보호학과

*****네이버(주)

skskje312@naver.com, hoyu210@gmail.com, seonjinjeon.12@gmail.com, shionista@gmail.com, flittermouse@naver.com

OpenSource Security Vulnerability Real-Time Notification System

Ji Eun Choi*, Ye Lim Koo**, Seon Jin Jeon***, Woo In Park****, Byoung Hee Lee*****

* Dept. of Computer Engineering, Duksung Women's University

** Dept. of Computer Science, Kyonggi University

*** Dept. of Software, Soongsil University

**** Dept. of Information Security, Suwon University

*****Naver

요 약

기업 내에서는 다양한 오픈소스를 활용하고 있다. 이런 환경에서 해당 오픈소스의 취약점 및 패치 현황을 실시간으로 제공하여 빠르게 대처하는 것이 중요하다. 먼저 기업 내에서 많이 사용하는 오픈소스를 조사한 후 Top 70 오픈소스를 선정하여 보안 취약점 및 패치 현황을 파악한다. 실제 크롤링을 통해 취약점을 수집한 후, 필요한 정보를 가공하여 웹 서비스로 시각화 하여 제공한다. 또한 취약점이 발생했을 때 기업에서는 실시간 메일 알림 서비스를 받아볼 수 있는 과정을 제시한다.

1. 서론

1.1 개발 배경 및 필요성

IT 현업의 소프트웨어 엔지니어들은 다양한 오픈소스를 활용해 개발하고 있다. 이때 사용하는 오픈소스의 취약점 및 패치현황을 항상 모니터링할 수 없다는 현실적인 한계가 존재한다. 이러한 한계를 극복하기 위해 자주 사용되는 상위 70 개의 오픈소스의 취약점 및 패치 현황을 실시간으로 점검할 수 있는 어드바이저 프로그램 개발의 필요성이 있다. 따라서, 실시간으로 오픈소스의 보안 위협과 패치의 알람을 보낼 수 있는 자동화된 프로그램을 개발하여 IT 실무에 효율을 증진하고 낭비되는 시간과 비용을 최소화하고자 했다.

1.2 기존 서비스와의 차별점

기업 내에서 사용 빈도가 높은 오픈소스 파악 및 취약점을 확인할 수 있다. 실제 크롤링을 통해 필요한 정보를 시각화하여 제공할 수 있다. 또한, 등록해 놓은 이메일로 당일 오픈소스의 취약점 리스트를 전송 받을 수 있다.

2. 본론

2.1 시스템 개요

오픈소스를 활용해 개발이 진행되는 있는 상황에서 해당 오픈소스의 취약점 및 패치 현황을 실시간으로 제공하여 빠르게 대처하는 것이 중요하다. 따라서 본 프로젝트에서는 기업에서 자주 사용하는 오픈소스를 선정하여 보안 취약점 및 패치 현황을 실시간으로 확인할 수 있도록 한다.

2.2 기능 설계

사용자가 보안 취약점 및 패치 현황을 실시간으로 확인할 수 있도록 5 가지의 기능을 설계했다.

표 1 주요기능

기능	설명
크롤링	선별된 오픈소스 보안 패치 현황에 대한 크롤링
데이터 분석 및 가공	크롤링 데이터를 분석 및 가공하여 DB 저장

실시간 알람	오픈소스 보안 중요도에 따른 메일을 이용한 실시간 알람
데이터 시각화	오픈소스에 관한 CVE 통계 및 실시간 모니터링
데이터 번역	오픈소스 정보 영한번역

2.3 서비스 흐름도 설계

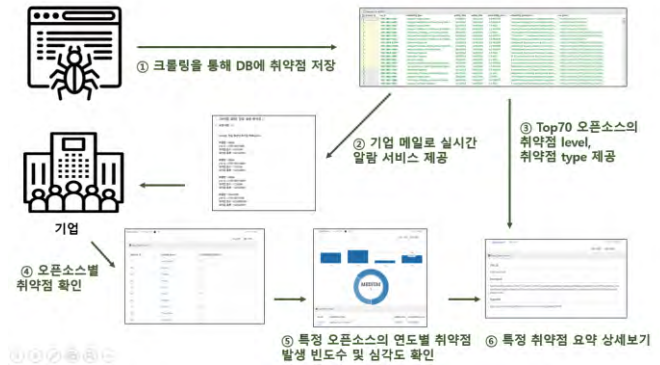


그림 1 동작 흐름도

3. 구현 결과

3.1 크롤링

CVE 취약점 사이트인 NVD 에서 오픈소스의 취약점을 크롤링하여 DB 에 저장했다. 해당 크롤링은 하루에 한번의 주기로 실행되어 데이터를 추출해 저장한다. 이 때, 기존에 확인된 취약점에 대해서는 다시 확인하지 않도록 설계하여 성능 측면의 리스크를 최소화 하였다.

그림 2 DB에 저장된 취약점 리스트

3.2 실시간 알람

크롤링 데이터 중 당일 발생한 오픈소스의 취약점을 추출하여, 등록된 사용자의 이메일로 당일 오픈소스 취약점 리스트를 전송한다.

☆ [취약점 알림] 당일 발생 취약점

보낸사람 VIP
받는사람

name1님, 12/17/2019 발생한 취약점 목록입니다.

제품명 : OpenShift
cve id : CVE-2014-3496
취약점 점수 : 10.0 HIGH
취약점 종류 : Improper Control of Generation of Code ('Code Injection')

제품명 : Puppet
cve id : CVE-2019-10694
취약점 점수 : 9.8 CRITICAL
취약점 종류 : Use of Hard-coded Credentials

제품명 : OpenShift
cve id : CVE-2015-5254
취약점 점수 : 9.8 CRITICAL
취약점 종류 : Improper Input Validation

제품명 : Git
cve id : CVE-2019-19604
취약점 점수 : 9.8 CRITICAL
취약점 종류 : Improper Input Validation

그림 3 메일로 전송된 오픈소스 취약점 실시간 알람

3.3 데이터 시각화

CVE 통계 및 실시간 모니터링을 위해 취약점 데이터를 시각화 한다. 시각화의 핵심은 직관적으로 알 수 있어야하고 위험 레벨에 따른 구분이 가능하도록 설계하였다.



그림 4 오픈소스 취약점 데이터 시각화

4. 결론 및 향후 연구

최근 다양한 산학연에서 오픈소스의 활용이 증가하고 있다. 해당 시스템은 이러한 곳에서 오픈소스 취약점에 대한 실시간 알람을 통한 신속한 대응 가능할

것으로 기대된다. 또한, 최신 보안 취약점 경향 파악으로 오픈소스 활용에 대한 보안 위협 최소화에 도움을 줄 수 있을 것이다. 마지막으로 Threat Intelligence으로 보안 위협에 대한 자동화된 대응 체계 확립할 것을 기대한다.

향후 크롤링한 오픈소스 취약점 데이터의 심층 분석 및 위협 레벨에 대한 가공을 진행할 것이다. 번역 API 를 이용한 영한 번역을 통해 담당자가 쉽게 위협을 판단 할 수 있도록 확장할 예정이다. 또한 오픈소스의 확장을 통해 좀 더 많은 오픈소스 취약점을 실시간으로 탐지하고 반영할 수 있도록 할 것이다.

참고문헌

- [1] 송석리, 이현아. “모두의 데이터 분석 with 파이썬”, 2019
- [2] 사카타 코이치. “예제로 쉽게 배우는 스프링 프레임워크 3.0”, 2012

본 논문은 과학기술정보통신부

정보통신창의인재양성사업의 지원을 통해 수행한

ICT멘토링 프로젝트 결과물입니다.

개인정보보호를 위한 영상 암호화 아키텍처 연구

김정석***, 이재호*

*서울시립대학교 전자전기컴퓨터공학부

**에스케이텔레콤 AIX 센터 시큐리티랩스

justinkim@uos.ac.kr, jaeho@uos.ac.kr

A Study of video encryption architecture for privacy protection

Jeongseok Kim***, Jaeho Lee*

*Dept. of Electrical and Computer Engineering, University of Seoul

**Security Labs, AIX Center, SK Telecom

요 약

영상 감시 시스템은 광범위한 영역에서 쉽게 설치되고 있으며, 감시 지역을 녹화한 영상 정보는 대개 인터넷을 통한 클라우드 상의 저장소에서 관리하는 중앙 관리 방식을 사용하고 있다. 그러나 이러한 시스템의 주요한 문제점은 저장 영상의 전송 과정과 저장 대해서 객관적으로 신뢰할 수 있는 방법이 제공되지 않고 있으며, 개인정보보호를 위한 장치 유무와 별개로 모든 권한을 서비스 제공자에게 위임한 상태에서 운영하고 있다는 점이다.

본 연구에서는 공개키 기반 암호화와 블록체인 기반의 키 관리 시스템을 조합한 아키텍처를 이용하여 민감한 정보를 사용자가 안전하게 보호할 수 있는 방안을 제시한다. 제안하는 아키텍처에서는 대칭키를 사용한 블록 암호화(block-cipher) 과정을 통해 영상 정보를 암호화하고, 이때 사용하는 대칭키를 사용자의 공개키로 암호화하여 블록체인의 레저(ledger)로 기록하는 기법을 사용한다. 영상 정보를 암호화하는 과정을 블록체인 네트워크의 특성(분산, 투명성, 데이터 변조 불가)을 활용하여 개인정보 영상의 생성부터 소멸까지 사용자가 추적이 가능하도록 한다.

1. 서론

영상 감시 시스템은 지정한 장소를 상시 녹화하고 있고 불특정 다수의 정보를 수집하는 특성을 가지고 있다. 감시 시스템을 통해 녹화된 영상은 개인정보 혹은 장소에 대한 민감 정보를 저장하고, 시스템 사용자나 서비스 제공자 사이의 개인정보 오남용 방지를 위한 객관적인 관리 시스템 또는 서비스는 부재인 상태이다. 현존하는 클라우드 기반 비디오 영상 감시 서비스들은 공통적으로 영상을 카메라에서 취득한 뒤, 인터넷 구간을 통해 영상 스트림을 전송하여 저장하는 방식을 취하고 있다. 이 때 전송하는 구간에 대해서는 SSL 을 적용하여 안전하게 보호하려 하지만, 서비스 내부에 저장된 영상에 대해서는 방화벽 등을 이용한 접근 차단 외에는 데이터 이동, 복사를 통한 유출에 대해서는 고려하고 있지 못하는 실정이다.

본 연구에서 제안하는 아키텍처는 영상을 저장할 때 영상 암호화 방법을 사용하여, 주어진 키를 알고 있는 경우에만 해당 영상을 재생할 수 있도록 한다. 따라서 본 연구의 목적은 영상 정보를 전송하거나 저

장하는 순간부터 이동, 복사, 그리고 삭제할 때까지 일련의 과정을 추적할 수 있는 장치를 마련하여 전체 시스템에서 사용자 신뢰도를 향상시키는데 있다.

2. 관련 연구

영상 감시 시스템은 본질적으로 운영되는 시간 동안 끊임없이 자동적으로 특정 구역을 실시간으로 모니터링하거나 발생한 이벤트를 사건 이후 확인하기 위하여 녹화하는 것을 기반으로 구현 되어있다. 저장된 영상 파일은 카메라가 설치된 장소의 정보와 해당 위치에 방문한 인물들에 대한 정보를 담고 있으며, 경우에 따라서는 개인 정보 혹은 설치된 공간의 민감 정보를 내포하게 된다. 이러한 이유로 저장된 영상 파일에 대한 접근 통제는 대개 시스템에서 권한을 부여 받은 특정 사용자로 한정되도록 설계되어 있다.

개인정보보호를 위한 대표적인 아키텍처로는 G. Zyskind et al.[1]이 블록체인 아키텍처를 기반으로 하는 개인 데이터 보호 방안을 제시하고 있다. 영상과 음성 데이터를 보호하기 위한 방법으로는 MPEG-CENC 표준[2]으로 제시되고 있으며, 단일 혹은 여러 개의

AES Key 를 이용하여 멀티미디어 데이터를 암호화하는 방법으로 통용되고 있다. 이러한 멀티미디어 데이터 암호 기법은 데이터 자체의 보호보다는 Widewine, PlayReady 등과 같은 디지털 저작권 관리(Digital Right Management)의 관점에서 발전하고 있다. Vishwa et al.[3]은 블록체인 기반의 DRM 을 연구하여 저작권을 보호하는 방법을 제시하고 있다.

분산 환경에서 콘텐츠를 암호화하고 사용자의 키를 관리하는 방법에 대해서는 블록체인 기반의 PKI(Public Key Infrastructure)[4]를 사용자-서비스 간의 신원확인 및 데이터 보호에 사용하는 방안이 제시되고 있다. 또한 민감한 데이터를 보호하는 방법에 대한 연구는 EMR(Electronic Medical Records)처럼 정보의 소유자가 아닌 제 3 자가 데이터를 수집하고 처리할 때 발생할 수 있는 정보 보호 이슈[5]를 해결하고자 새로운 아키텍처를 수립하기도 하였다.

또한 실질적인 데이터를 관리하는 상황에 있어서, 블록체인 기반의 접근 방법은 위변조가 불가능하고 개인정보보호에 사용이 가능하다는 것을 이야기하지만, 시스템을 설계할 때 보호하려는 데이터의 크기보다는 기록하는 데이터의 수에 따라 전체 시스템의 성능이 좌우된다는 연구 결과[6]를 고려하여 영상 암호화 아키텍처를 제안하고자 한다.

3. 영상 스트림 접근 제어

데이터를 보호 방법은 데이터에 허가된 사용자가 접근하는 것을 제어하는 것과 위변조를 방지하는 두 가지 측면에서 접근할 수 있다. 그러나 본 제안 아키텍처에서는 영상을 획득하는 카메라가 설치된 장소와 획득한 영상을 서비스 제공자가 구성한 클라우드 기반의 저장소로 자동적으로 전송되는 특성을 고려하여 EMR 의 경우와 비슷하게 제 3 자에 의하여 생성된 데이터를 관리하는 방안을 제시하고자 한다.

또한 네트워크 단절 상황에서도 영상 유실을 막고자 카메라 내부에 일정 시간 동안 저장하는 경우에도 해당 데이터를 보호하기 위하여 서비스 전반에 걸쳐 영상 암호화 방법을 적용하도록 설계하였다.

4. Compound Identity 의 복잡성

비대칭 암호화는 둘 이상의 관련자간의 공개키와 개인키를 사용하고 있으며, 암호화 데이터 전송 이전에 공개키의 교환은 필수적인 절차이다. 그렇기 때문에 서로간의 공개키를 통하여 서로를 식별하는 *Compound Identity* 를 구성하게 된다. Compound 집합은 공개키(pk)와 개인키(sk)의 2-tuple 혹은 완전한 식별 데이터를 요구하는 경우 5-tuple(공개키, 개인키, 상대방 공개키와 개인키, 공유하는 대칭키)로 구성된다. 그러나 이러한 집합은 단순히 양방향 데이터 교환을 위해서는 강력한 암호화 메커니즘을 제공하는 기반이 되지만, 사용자와 다수의 서비스간의 경우로 환산한다

면, Compound Identity 자체의 복잡도는 $O(n!)$ 으로 수렴하게 된다.

$$\begin{aligned} \text{Compound}_{u,s_1,s_2,\dots,s_n}^{(public)} = & \text{Compound}_{u,s_1}^{(public)} + \dots + \text{Compound}_{u,s_n}^{(public)} + \\ & \text{Compound}_{s_1,u}^{(public)} + \dots + \text{Compound}_{s_1,s_n}^{(public)} + \\ & \dots \\ & \text{Compound}_{s_n,u}^{(public)} + \dots + \text{Compound}_{s_n,s_{n-1}}^{(public)} \end{aligned}$$

Equation 1 Complexity of Compound Identity

영상 감시 시스템은 사용자가 직접 콘텐츠를 생성하는 것이 아니라, 카메라와 시스템이 자동적으로 생성하는 구조이기 때문에, 사용자-서비스 혹은 사용자-카메라간의 Compound Identity 를 구성한다고 하면, 이러한 복잡도의 증가는 시스템의 구성을 저해하는 요소가 된다.

5. 제안 아키텍처

Compound Identity 의 복잡도는 공개키를 공유를 필요로 하는 양방향의 데이터 보호 채널을 구성하기 때문에 발생하게 된다. 영상 감시 시스템에서는 카메라와 사용자간의 관계상 사용자만이 카메라의 영상을 확인할 수 있도록 한정하여 Compound Identity 의 복잡도를 획기적으로 낮추도록 하였다.

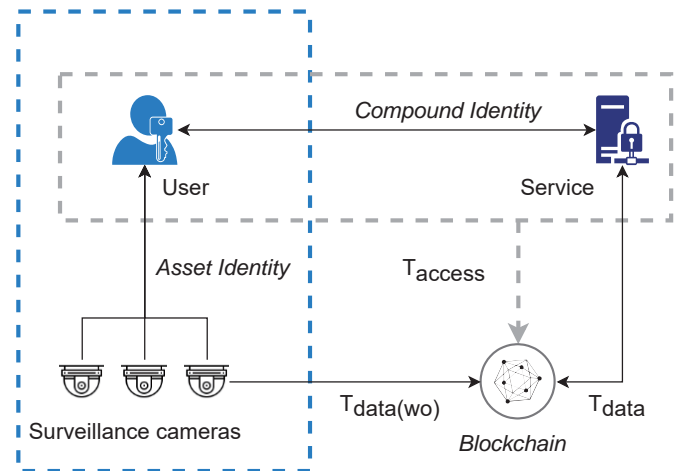


Figure 1 Overview of privacy protection architecture for surveillance system

1) *Asset Identity*: Algorithm 1에서는 사용자-카메라 혹은 사용자-암호화된 비디오의 관계를 설정하여 사용자의 공개키와 영상 암호화에 사용할 대칭키만을 조합하는 *Nonce* 개념을 소개하고 있다.

카메라 혹은 서비스가 생성한 *Nonce* 를 기반으로 영상 파일을 암호화하는 경우 대칭키 정보는 사용자만이 알 수 있게 된다. 그렇기 때문에 영상 파일을 공개된 공간으로 전송하거나 사고에 의하여 유출된다고

하더라도 사용자의 개인키에 대한 어떠한 정보도 얻을 수 없게 되며, 이는 영상 정보를 복호화 할 수 없다는 것을 의미한다.

$$\begin{aligned} Asset_{u,a} &= (pk_{sig}^u, Nonce_{pk(enc)}^a) \\ Asset_{u,a_1,a_2,\dots,a_n} &= (pk_{sig}^u, Nonce_{pk(enc)}^A) \end{aligned}$$

Equation 2 Asset Identity

Nonce 는 사용자가 정보의 소유권을 가진 장치나 서비스 등 사용자의 공개키를 획득할 수 있는 제 3 자에 의해서 생성이 가능하며, 사용자는 대칭키를 관리해야하는 부담에서도 동시에 벗어날 수 있다. 또한 Nonce 생성에는 단지 사용자의 공개키만을 요구하기 때문에 사용자와 암호화 채널을 구성해야하는 영상 감시 카메라 혹은 영상 정보를 처리하는 서비스가 증가함에도 그 복잡도는 여전히 $O(n)$ 으로 수렴한다.

Require: $A \neq \emptyset$

```

1: procedure ASSETIDENTITY( $U, A$ )
2:   if  $(pk_{sig}^U, sk_{sig}^U) = \emptyset$  then ▷  $U$  executes
3:      $(pk_{sig}^U, sk_{sig}^U) \leftarrow \mathcal{G}_{sig}()$ 
4:      $sk_{enc}^U \leftarrow \mathcal{G}_{enc}()$  ▷ only  $U$  keeps
5:   end if
6:   for each  $a_k \in A$  do
7:      $Nonce \leftarrow \mathcal{G}_{nonce}()$  ▷ only  $a_k$  keeps
8:      $Nonce_{enc}^{a_k} \leftarrow Encrypt(pk_{sig}^U, Nonce)$ 
9:   end for
10:  return  $(pk_{sig}^U, Nonce_{enc})$ 
11: end procedure

```

Algorithm 1 Generating Asset Identity

2) **Protocol:** 개인정보보호를 위해 생성하는 일련의 정보는 블록체인 메모리(L)에 저장하는 것을 기본 전제로 한다. 영상 스트림의 경우, 영상 정보를 대개 그 사이즈가 크기 때문에 L 에 저장하는 것보다는 일반적인 저장소(ds)에 저장하고, 해시 함수(H)를 통해 매핑한 정보를 L 에서 관리하도록 한다. Nonce 에 대한 공유 혹은 허가 정보를 L 에 기록하여, 개인정보보호 관점에서 저장된 영상의 접근 제어뿐만 아니라 영상 정보의 생성부터 소멸까지 전반적인 라이프 사이클에 대한 추적이 가능하도록 한다.

3) **Data Transaction:** Asset Identity 절차를 통하여 Asset 으로 분류되는 카메라는 Nonce 정보를 가지고 있기 때문에, $Nonce_{enc}$ 와 Asset 정보(a)를 암호화된 미디어 파일(M_{enc}) 내의 메타데이터로 기록하여 암호화된 미디어 파일 단독으로 off-chain 을 통해 공유 가능한 상태가 된다.

Algorithm 2 는 StoreSecureDataTX 를 이용한 데이터 저장소와 블록체인 메모리간의 상호 운영에 대한 절차를 설명하고 있다. 위에서 언급한대로 암호화된 미디어에 기록된 Nonce 는 아무런 제약없이 추출이 가능한 메타데이터이기 때문에 본 연구에서 제안하는 시스템은 카메라 내부 혹은 클라우드 기반의 데이터 저장 서비스를 블록체인 네트워크 혹은 암호/복호화 과

정과 분리하여 수행할 수 있도록 하여 시스템의 확장성을 고려하고 있다.

Require: $M_{enc} \neq 0$

```

1: procedure STORESECUREDATATX( $pk_{sig}^k, M_{enc}$ )
2:    $(a_p, Nonce_{enc}^p) \leftarrow Parse(M_{enc})$ 
3:   if  $ValidateAsset(pk_{sig}^k, a_p, Nonce_{enc}^p) \neq True$  then
4:     return  $\emptyset$ 
5:   end if
6:    $h_{M_{enc}} \leftarrow \mathcal{H}(M_{enc})$ 
7:    $L[\mathcal{H}(pk_{sig}^k)] \leftarrow L[\mathcal{H}(pk_{sig}^k)] \cup h_{M_{enc}}$ 
8:    $ds[h_{M_{enc}}] = M_{enc}$ 
9:   return  $h_{M_{enc}}$ 
10: end procedure

```

Algorithm 2 Storing secure data

StoreSecureDataTX 내에서 수행하는 ValidateAsset 은 트랜잭션 내에서 비즈니스 로직이 개입할 수 있는 보조적인 장치로 사용되고 있으며, 이를 통하여 사용자, Asset, Nonce 정보가 일치하는지 확인할 때 블록체인 네트워크에 M_{enc} 에 대한 접근 상황을 추적할 수 있다.

암호화된 미디어의 저장이 완료된 이후 Algorithm 3 은 ds 와 H 를 이용하여 M_{enc} 를 획득한 후 복호화를 수행하는 과정을 설명하고 있다. 또한 제 3 자에 의한 복호화 요청에도, CheckPolicy 를 정의하여 본래 Asset 의 소유자인 사용자에게 요청을 허가할지 결정할 수 있도록 하여, M_{enc} 의 복호화 과정을 블록체인 네트워크에 기록할 수 있도록 한다. 또한 사용자가 허가할 수 있는 권한의 종류는 downloadable, readable 등으로 세분화하여 세밀한 권한 제어가 가능하도록 한다.

요청자가 M_{enc} 를 획득한 이후에도 ValidateAsset 을 수행하여 사용자가 허가한 경우에 한하여 평문의 대칭키를 획득 가능하도록 하여 미디어 파일의 획득과 복호화 과정을 분리하여 추적할 수 있다.

Require: $m \neq 0$

```

1: procedure LOADSECUREDATATX( $pk_{sig}^k, m$ )
2:    $(h_{M_{enc}}, x_p) \leftarrow Parse(m)$ 
3:   if  $CheckPolicy(pk_{sig}^k, x_p) \neq True$  then
4:     return Error
5:   end if
6:   if  $h_{M_{enc}} \in L[\mathcal{H}(pk_{sig}^k)]$  then
7:      $M_{enc} \leftarrow ds[h_{M_{enc}}]$ 
8:      $(a_p, Nonce_{enc}^p) \leftarrow Parse(M_{enc})$ 
9:     if  $ValidateAsset(pk_{sig}^k, a_p, Nonce_{enc}^p) \neq True$ 
then
10:      return  $\emptyset$ 
11:    end if
12:  end if
13:  return  $(pk_{sig}^k, h_{M_{enc}}, a^p, Nonce_{enc}^p)$ 
14: end procedure

```

Algorithm 3 Loading secure data

4) **Tracing Transaction:** 영상 정보의 생성 이후 M_{enc} 의 소유권 이전과 소멸에 대한 관리를 위한 트랜잭션으로 대용량의 미디어 파일의 반복적인 암호/복호화 과정

없이 Nonce 정보를 추가하여 off-chain 상에서도 전달 과정을 Algorithm 4 를 통해 제시하고 있다.

제시된 알고리즘의 6 번째 라인에서 설명하듯 M_{enc}^t 는 $Nonce_{enc}^k$ 와 $Nonce_{enc}^t$ 의 정보를 모두 가지고 있기 때문에 사용자 k 와 t 는 M_{enc}^t 를 복호화 할 수 있으나, 이 과정에서 M_{enc}^t 를 복호화는 필요로 하지 않는다.

Require: $T \neq \emptyset \vee m \neq 0$

```

1: procedure TRANSFERSECUREDATATX( $pk_{sig}^k, T, m$ )
2:   ( $pk_{sig}^k, h_{M_{enc}}, a^p, Nonce_{enc}^p$ )  $\leftarrow$ 
   LoadSecureDataTX( $pk_{sig}^k, m$ )
3:    $M_{enc} \leftarrow ds[h_{M_{enc}}]$ 
4:   if  $M_{enc} \neq \emptyset$  then
5:     ( $pk_{sig}^t, Nonce_{enc}^t$ )  $\leftarrow$  AssetIdentity( $T, a^p$ )
6:      $M_{enc}^t \leftarrow M_{enc} \cup Nonce_{enc}^t$ 
7:      $h_{M_{enc}^t} \leftarrow$  StoreSecureDataTX( $pk_{sig}^t, M_{enc}^t$ )
8:   end if
9:   return  $h_{M_{enc}^t}$ 
10: end procedure

```

Algorithm 4 Transferring secure data

영상 감시 시스템에서 또다른 주요 이슈는 생성된 영상 정보를 영구히 제거하는 것이다. 제안된 시스템에서도 임의로 저장한 M_{enc} 의 복사를 제한할 수 있는 방법은 없으나, Algorithm 5 는 Nonce 자체를 무효화하여 결과적으로는 M_{enc} 의 복호화 방법을 차단하는 간접적인 절차를 통해 해당 영상 정보에 접근을 영구히 제거하는 방안을 제안한다.

물론 Nonce 조차도 임의의 공간에 별도로 보관하는 경우 무효화된 M_{enc} 를 복호화 하려는 시도는 가능하나 일반적으로 난수 생성기(Random Number Generator)를 통해 생성된 값으로 공격의 대상이 되는 모든 M 에 대하여 무효화 이전에 예측 불가능한 Nonce 를 별도의 시스템에서 관리하는 것은 사실상 불가능에 가깝다.

```

1: procedure INVALIDATESECUREDATATX( $pk_{sig}^k, h_{M_{enc}}$ )
2:    $M_{enc} \leftarrow ds[h_{M_{enc}}]$ 
3:   ( $a^p, Nonce_{enc}^p$ )  $\leftarrow$  Parse( $M_{enc}$ )
4:    $M_{enc} \leftarrow M_{enc} - Nonce_{enc}^p$ 
5:   if  $M_{enc}$  has no Nonce then
6:      $ds[h_{M_{enc}}] = \emptyset$ 
7:   end if
8: end procedure

```

Algorithm 5 Invalidating secure data

6. 결론

사회 안전을 위하여 널리 사용되고 있는 영상 감시 시스템의 시스템 자체가 개인정보보호를 위해 보호되어야 하는 대상이 되고 있다. 시간이 지남에 따라 더 많은 사용자와 시스템이 관련되기 때문에 악의적인 접근과는 상관없이 실수에 의해서도 민감한 영상이 공유되는 상황은 발생할 수 있으나 시스템에 대한 접

근 차단 외에는 뚜렷한 보호장치는 없는 상태이다. 본 연구에서 제안한 아키텍처는 영상 정보에 보다 중점을 두어 사용자의 제어권 안에서 영상 정보 제공이 가능하도록 하여 개인정보를 보호하는데 목적을 두고 있다. 그러나 제안된 아키텍처는 영상 감시 시스템 뿐만 아니라 추후 연구를 통하여 데이터의 생성과 소유가 분리되는 일반적인 경우에도 적용할 수 있을 것으로 기대된다.

참고문헌

- [1] G. Zyskind, O. Nathan, and A. Pentland. Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops*, pages 180–184, May 2015.
- [2] ISO/IEC 23001-7:2016, Part 7: Common encryption in ISO base media file format files In *Information technology – MPEG systems technologies* Retrieved from <https://www.iso.org/standard/68042.html>
- [3] Alka Vishwa and Farookh Hussain. A blockchain based approach for multimedia privacy protection and provenance. In *2018 IEEE Symposium Series on Computational Intelligence (SSCI)*, pages 1941–1945, Nov 2018.
- [4] R. Wang, J. He, C. Liu, Q. Li, W. Tsai, and E. Deng. A privacy-aware pki system based on permissioned blockchains. In *2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS)*, pages 928–931, Nov 2018.
- [5] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman. Medrec: Using blockchain for medical data access and permission management. In *2016 2nd International Conference on Open and Big Data (OBD)*, pages 25–30, Aug 2016.
- [6] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla. Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In *2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, pages 468–477, May 2017.

실시간 모니터링을 이용한 캐시 부채널 공격 탐지 프레임워크

임미옥, 김수진, 신영주
광운대학교 컴퓨터정보공학부 정보 및 사이버보안 연구실
e-mail: mo981014@gmail.com, kipper152@naver.com, yjshin@kw.ac.kr

Framework on Cache Side-channel Attack Detection Using Real-time Monitoring

Miok Im, Soojin Kim, Youngjoo Shin
Information and Cyber Security Lab, School of Computer and Information Engineering
Kwangwoon University

요 약

캐시 부채널 공격은 캐시 기반의 공격 기법으로 개인정보 유출에 대한 위협성이 큰 보안 취약점이다. 해당 취약점을 막기 위해 실시간 공격 탐지 기법에 관한 연구들이 진행되고 있지만 사용자에게 이벤트값과 탐지 결과를 빠르고 편리하게 보여줄 필요성이 있다. 본 논문은 효율적인 캐시 부채널 공격 탐지를 위해 Intel PCM 과 기존의 탐지프로그램을 개선하여 탐지에 필요한 데이터들을 실시간으로 모니터링 및 경고를 보내주는 프레임워크를 제작했다. 해당 프레임워크는 캐시 부채널 공격을 실시간 탐지 및 관련 데이터들을 대시보드로 보여준다.

1. 서론

프로세서는 캐시를 사용하여 CPU 가 메모리에 저장된 데이터를 읽어올 때 빠르게 접근할 수 있다. 캐시는 프로세서의 성능 향상에 기여하며 오늘날 대부분의 프로세서에서 사용되고 있다. 하지만 캐시 취약점은 캐시 부채널 공격에 이용되어 개인정보를 유출할 수 있다는 문제점이 있다. 캐시 부채널 공격은 캐시 기반의 공격 기법으로 공격자와 희생자가 공유하는 LLC(Last Level Cache)를 사용한다. 해당 공격을 막기 위해 탐지 기법에 관한 많은 연구가 진행됐지만 사용자에게 이벤트 값(Cache Miss, IPC, Branch 등)과 어떠한 공격이 들어왔는지 시각적으로 보여줄 필요성이 있다.

우리는 Intel PCM 과 기존의 탐지 프로그램[7]을 활용하여 이벤트값과 탐지 결과를 실시간 모니터링함으로써 캐시 부채널 공격 여부를 쉽게 확인할 수 있도록 프레임워크를 제작했다. 해당 프레임워크는 데이터 수집도구인 Telegraf 를 통하여 이벤트 값과 탐지 프로그램 결과값을 수집한 후 시계열 데이터베이스 Influxdb 에 저장함으로써 최종적으로 Grafana 대시보드에 그래프로 보여주도록 만들었다. 기존 탐지 프로그램에서 모니터링 및 경고 수단을 추가하여 사용자가 편리하고 빠르게 공격 여부를 확인할 수 있었다.

본 논문의 구성은 다음과 같다. 2 장에서는 Grafana, PCM, 캐시 부채널 공격, Softmax Classification 에 대한

배경지식을 설명한다. 3 장에서는 프레임워크 제작 방법에 대해서 데이터 수집 및 저장, 대시보드 설정 및 알람에 대해 말한다. 4 장에서는 3 장의 실험과 결과를 설명한다. 5 장에서는 향후 계획, 마지막 6 장에서는 결론에 대해 기술한다.

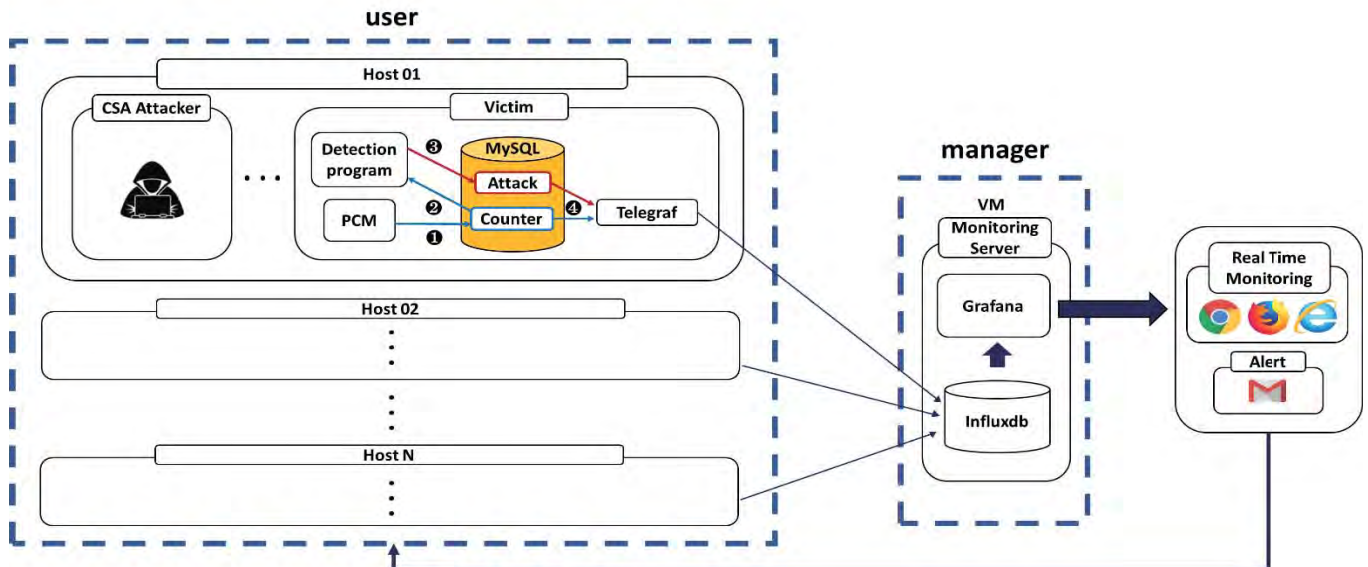
2. 배경지식

2.1 Grafana

Grafana 는 데이터소스(e.g., Cache Miss)를 모니터링 및 관찰하기 위한 오픈 소스 플랫폼이며 시각화를 위해 Graphite, Prometheus, Elasticsearch, OpenTSDB 및 Influxdb 등을 지원한다[1]. 특히, 본 논문에서는 실시간 시각화를 위해 가장 널리 사용되는 시계열 데이터베이스 Influxdb 와 데이터 수집 방법으로 입력 플러그인(e.g., MySQL)과 출력 플러그인(e.g., Influxdb)을 간단한 설정으로 사용 가능한 Telegraf 를 활용하였다[2]. 즉, Telegraf 에서 데이터 수집한 것을 Influxdb 에 저장하여 Grafana 대시보드에 나타낼 수 있다. 또한, Grafana 는 시각화뿐만 아니라 특정 지표에 대한 경고 규칙을 정의하고, 지속적으로 Slack, SMS 와 Email 같은 시스템에 알람을 보낼 수 있다.

2.2 Performance Counter Monitor (PCM)

Performance Counter Monitor(PCM)는 인텔 프로세서 내부의 특수 레지스터를 이용하여 이벤트 값(e.g., Cache Miss)을 실시간으로 관찰할 수 있는 도구이다[3].



(그림 1) 모니터링 시스템 구조

프로세스의 이벤트 변화율은 캐시 부채널 공격을 탐지하는 데 사용된다. Intel PCM은 컴파일되지 않은 소스코드를 제공하기 때문에 내부 동작을 사용자가 변경할 수 있으며 간단하게 컴파일하여 실행파일로 이용할 수 있다.

2.3 캐시 부채널 공격(Cache Side Channel Attack)

2.3.1 FLUSH+RELOAD 공격

FLUSH+RELOAD[4] 공격은 공격자와 희생자가 공유하는 L3 캐시 라인을 대상으로 하는 공격이다. 공격은 크게 3단계로 이루어져 있다. 첫 번째로, 공격자는 공격자와 희생자가 공유하는 캐시 라인을 `clflush` 명령어를 사용하여 L1, L2, L3 캐시에서 모두 비워준다. 두 번째로, 공격자는 희생자가 해당 캐시 라인에 접근할 때까지 기다린다. 마지막으로, 공격자는 다시 해당 캐시 라인에 접근하여 데이터를 로드 한다. 프로세서는 최근에 사용한 데이터를 캐시에 저장한다. 데이터가 캐시 메모리에 존재한다면 프로세서는 메인 메모리에 접근하지 않고 캐시 메모리에서 데이터를 바로 가져올 수 있다. 따라서 데이터를 가져오는 데 있어서 메인 메모리보다 더 짧은 시간 내에 가져온다. 공격자가 데이터를 로드 하는 시간이 느리다면 희생자가 해당 캐시 라인에 접근한 것이고, 반대로 시간이 빠르다면 희생자가 접근하지 않은 것이다. FLUSH+RELOAD 공격은 이러한 시간 차이를 통하여 희생자의 데이터를 알아낼 수 있다.

2.3.2 FLUSH+FLUSH 공격

FLUSH+FLUSH[5] 공격은 FLUSH+RELOAD 공격과 방식이 유사하다. 하지만 세 번째 단계에서 로드를 하는 대신 다시 `clflush` 명령어를 실행하여 캐시 라인을 비워준다. 캐시 라인에 데이터가 존재한다면 데이터가 존재하지 않을 때보다 캐시를 비우는 데 오랜 시간이 걸린다. 따라서 세 번째 단계에서 시간이 오래 걸린다면 희생자가 해당 캐시 라인에 접근한 것이

고, 시간이 오래 걸리지 않는다면 희생자가 접근하지 않은 것이다. FLUSH+FLUSH 공격도 이러한 시간차를 통하여 희생자의 데이터를 알아낼 수 있다.

2.3.3 PRIME+PROBE 공격

PRIME+PROBE[6] 공격은 앞서 설명한 2 개의 공격과 달리 공격자와 희생자가 공유하는 L3 Cache Set을 대상으로 공격한다. PRIME+PROBE 공격은 크게 3 단계로 이루어져 있다. 첫 번째로, 공격자는 자신의 데이터로 공유 Cache Set 들을 채운다. 두 번째로, 공격자는 희생자가 실행하는 동안 기다린다. 마지막으로, 공격자는 다시 자신의 데이터를 실행하여 로드 하는 시간을 측정한다. 이때 희생자가 Cache Set에 접근했다면 Cache Set은 희생자의 데이터로 채워지면서 공격자의 데이터는 `evict` 된다. 따라서 공격자가 다시 로드 하였을 때 시간이 오래 걸린다. 반면에 희생자가 접근하지 않았다면 시간이 오래 걸리지 않는다. PRIME+PROBE 공격은 이러한 시간 차이를 통하여 희생자의 데이터를 알아낼 수 있다.

2.4 Softmax Classification

여러 공격 중에서 어떠한 공격이 진행되었는지 판단하기 위해 다중 클래스 분류인 Softmax Classification을 사용하였다. Softmax Classification의 가설 함수 $H(x)$ 는 입력 데이터 x 에 대하여 가중치(W)를 곱하고 편향(b)을 더한 값이다. $H(x)$ 가 Softmax 함수 S_i 의 입력 값이 되어 나온 값이 예측값이 된다. Softmax 함수란 분류해야 하는 클래스의 총 개수를 k 라고 하면, k 차원의 벡터를 입력받아 각 클래스에 대한 0~1 사이의 확률값을 구한다. 이와 같이 확률적인 결과 값을 가지고 높은 확률을 가지는 클래스가 예측값이 된다. 가설 함수를 통하여 구한 예측값과 실제 값을 기반으로 비용 함수 Cost(W)를 구한다. Softmax Classification의 비용 함수는 각 클래스에 대한 예측값과 실제값의 차이를 모두 더한다. 따라서 비용 함수는 예측값이



(그림 2) Grafana 를 통한 각 호스트 별 캐시 부채널 공격 전과 후의 이벤트 값들과 탐지 결과값 변화

실제값과 유사할수록 0 에 가까워지고, 다를수록 값이 커지게 된다. 비용 함수가 최소가 되도록 W, b 의 값을 찾음으로써 가장 적절한 예측을 할 수 있는 가설 함수를 구할 수 있다.

$$H(x) = Wx + b$$

$$S_i = \frac{e^{y_i}}{\sum_{j=1}^n e^{y_j}} \text{ for } i = 1, 2, \dots, k$$

3. 프레임워크

효율적으로 캐시 부채널 공격 탐지를 위해 Intel PCM 과 기존의 탐지 프로그램[7]을 개선하고 Telegraf, Influxdb, Grafana 를 사용하여 실시간 모니터링이 가능하도록 프레임워크를 제작하였다.

(그림 1)과 같이 관리자 서버는 가상 머신이며 Influxdb 와 Grafana 로 이루어져 있고, 사용자 서버는 MySQL, Telegraf, Intel PCM 그리고 탐지 프로그램으로 구성되어 있다. 프레임워크는 사용자와 관리자 서버로 구분되며, 관리자 서버를 통해 호스트간 접근이 불가하여 보안상 안전하다.

3.1 데이터 수집 및 저장 방법

탐지 프로그램은 PCM 을 동작시키고, (그림 1)과 같이 MySQL 로부터 이벤트값들을 읽어와 어떠한 공격을 받았는지에 대한 결과를 MySQL 에 저장한다. 구체적으로 탐지 프로그램이 PCM 을 실행시키면 MySQL 의 'Counter' 테이블에 이벤트값들이 저장된다. 탐지 프로그램은 탐지에 필요한 데이터들을 읽어 오기

위해 반복문을 통하여 'Counter' 테이블에서 실시간으로 값을 가져온다. 해당 데이터들은 Softmax Classification 기법으로 훈련된 머신러닝 모델의 입력값으로 넣어 주어 예측 결과를 출력한다. 모델은 이벤트값들을 토대로 어떠한 공격도 하지 않은 상태를 0, FLUSH+RELOAD 공격은 1, FLUSH+FLUSH 공격은 2, PRIME+PROBE 공격이 진행된 경우는 3 으로 출력하며 이를 MySQL 의 'Attack' 테이블에 저장한다. 최종적으로 MySQL 은 저장된 값들(Attack, Counter)을 Telegraf 를 통하여 대시보드에 나타낼 데이터들을 수집한다.

Telegraf 는 input plugin 으로 MySQL 을 사용하여 Intel PCM 의 이벤트 값과 탐지 프로그램의 결과값을 수집하였다. 이때, Telegraf 의 설정파일을 통해 데이터 수집 주기 1 초, 데이터 전송주기 1 초로 정해주었으며 수집한 데이터를 저장하기 위해 output plugin 은 시계열 데이터베이스 Influxdb 로 설정해주었다.

각 사용자 서버는 (그림 1)과 같이 Telegraf 또는 데이터 수집에 필요한 프로그램 등을 백그라운드로 실행하여 모니터링 서버의 Influxdb 에 데이터를 보낸다. Influxdb 는 데이터를 HTTP 로 받아들이기 때문에 Telegraf 설정 파일 중 output plugin 의 URL 부분을 Influxdb 주소로 변경해주어야 한다. 관리자 서버는 가상 머신이기 때문에 브릿지를 통해 네트워크 대역을 재설정해준 후 모든 사용자가 데이터를 전송할 수 있도록 포트 포워딩이 필요하다.

3.2 대시보드 설정 및 알람

Grafana 는 데이터소스로 Influxdb 를 선택함으로써

이벤트값과 탐지프로그램 [7] 결과값을 대시보드에 나타낼 수 있다. (그림 2)와 같이 여러 쿼리를 만들어 주어 다양한 값들을 대시보드에 그래프로 나타내 주었다. 하나의 호스트당 4 개의 대시보드를 가지도록 구성하였으며 Grafana 의 alert 기능을 사용하여 캐시 부채널 공격이 들어왔을 때 사용자 메일로 관리자 서버에서 경고 메시지를 보내도록 설정했다. 또한, 관리자 서버의 Grafana 대시보드를 모든 사용자가 웹 브라우저로 확인할 수 있도록 브릿지 설정과 포트 포워딩해 주었다.

4. 실험

4.1 캐시 부채널 공격에 따른 PCM 값의 변화

Intel PCM 값들의 변화를 통하여 캐시 부채널 공격들을 탐지할 수 있었다. 캐시 부채널 공격들은 수행하는 명령어에 비해 많은 cycle 이 소요되기 때문에 IPC(Instruction Per Cycle) 값이 감소하지만 공격 코드가 수행하는 반복문으로 인해 Branch 값은 증가한다. 하지만 캐시 부채널 공격들은 Cache Miss 로 구분될 수 있다. 첫 번째, FLUSH+RELOAD 공격은 공격자가 희생자와 공유하는 L3 캐시 라인을 비우고 reload 를 반복한다. 따라서 공격이 진행되는 동안 모든 Cache Miss 값들이 급격하게 증가한다. 두 번째, PRIME+PROBE 공격은 PROBE 시 대부분 자신의 코드와 데이터들로 이루어진 Cache Set 들을 reload 하기 때문에 L3 Cache Miss 값 변화는 크게 없다. 하지만 L1, L2 Cache 는 구조상 L3 에서 reload 하고자 하는 Cache Set 들을 한 번에 가져올 수 없으므로 L1, L2 Cache Miss 값은 급격하게 증가한다. 마지막 FLUSH+FLUSH 공격은 공격자가 희생자와 공유하는 L3 캐시 라인을 reload 하지 않고 비워주기만 하므로 Cache Miss 값에는 큰 변화가 없다. 따라서 해당 이벤트값들로 공격을 탐지하고 Cache Miss 를 통해 분류할 수 있다.

4.2 실험 결과 및 관찰

Intel® Core™ i5-7400, Intel® Xeon® E5-2620, Intel® Core™ i9-9900KF 총 3 개의 프로세서에서 각각 Intel PCM 값들을 읽어와 탐지 프로그램의 입력 값으로 넣어주고, 탐지 프로그램이 출력한 값을 가지고 어떠한 공격이 들어왔는지를 탐지하였다. (그림 2)는 캐시 부채널 공격 전과 후의 PCM 값들과 탐지 결과를 각각의 호스트별로 Grafana 에서 나타낸 것으로 공격이 10 초간 지속되는 경우 빨간색 라인이 생기며, 이를 기준으로 공격 전과 후를 구분할 수 있다. E5-2620 프로세서는 FLUSH+RELOAD 공격을, i9-9900KF 프로세서는 FLUSH+FLUSH 공격을, i5-7400 프로세서는 PRIME+PROBE 공격을 진행하였다. (그림 2)에서 E5-2620 프로세서를 보면 FLUSH+RELOAD 공격이 진행되는 동안 모든 Cache Miss 값들이 급격하게 증가하는 것을 볼 수 있다. 또한 i5-7400 프로세서를 보면 PRIME+PROBE 공격이 진행되는 동안 L3 캐시와 달리 L1, L2 의 Cache Miss 값이 증가하는 것을 볼 수 있다. 하지만 i9-9900KF 프로세서는 FLUSH+FLUSH 공격이 진행되는 동안 Cache Miss 값은 변화가 없는 것을 볼 수 있다. 또한 모든 캐시 부채널 공격들이 진

행되는 동안 Branch 값은 증가, IPC 값은 감소하는 것을 볼 수 있으며 Attack 값의 경우 FLUSH+RELOAD 공격이 진행된 경우 1, FLUSH+FLUSH 공격이 진행된 경우 2, PRIME+PROBE 공격이 진행된 경우 3 으로 변경되는 것을 확인할 수 있다. 이를 기반으로 Counter 값들의 변화에 따라서 어떠한 공격을 받았는지를 알아낼 수 있었다. (그림 2)에서와 같이 호스트별로 Intel PCM 값들과 탐지한 공격을 Grafana 에서 실시간으로 나타내 주고 공격이 탐지될 경우 사용자에게 경고 메일을 보내준다.

5. 향후계획

현재 탐지 프로그램은 L1, L2, L3 Cache Miss 값들을 기반으로 캐시 부채널 공격들을 탐지하기 때문에 실제로 공격을 하지 않아도 Cache Miss 값이 증가하면 공격으로 탐지하는 경우가 있다. 따라서 이러한 오탐률을 줄일 수 있도록 현재 탐지 프로그램을 개선하려 한다.

6. 결론

본 논문에서는 각 호스트별로 Intel PCM 값들과 FLUSH+RELOAD, FLUSH+FLUSH, PRIME+PROBE 중에서 어떠한 캐시 부채널 공격이 실행되었는지에 대한 데이터들을 실시간으로 Grafana 를 통하여 나타내어 주고 공격을 받은 호스트에게 메일을 통하여 알려주는 방법에 대해서 설명하였다. 또한 Intel PCM 값들을 기반으로 어떠한 캐시 부채널 공격이 실행되었는지를 머신러닝을 통하여 탐지하는 기술에 대하여 설명하였다.

Acknowledgement

이 논문은 2019 년도 정부 (과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (2019-0-00533, 컴퓨터 프로세서의 구조적 보안 취약점 검증 및 공격 탐지 대응)

참고문헌

- [1] <https://grafana.com/oss/grafana/> - Grafana Labs
- [2] <https://github.com/influxdata/telegraf/> - telegraf
- [3] Intel® Performance Counter Monitor - A Better Way to Measure CPU Utilization
- [4] Yarom Yuval, and Katrina E. Falkner. "Flush+Reload : a High Resolution, Low Noise, L3 Cache Side-Channel Attack". USenix Security, 2014.
- [5] Daniel Gruss, Clémentine Maurice, Klaus Wagner, Stefan Mangard. "Flush+Flush : A Fast and Stealthy Cache Attack". DIMVA, 2016.
- [6] Liu, F.; Yarom, Y.; Ge, Q.; Lee, R.B. "Last-Level Cache Side-Channel Attacks are Practical". IEEE Symposium on Security and Privacy, 2015.
- [7] Jonghyun Cho, Taehun Kim, Soojin Kim, Miok Im, Taehyun Kim, and Youngjoo Shin "Real-Time Detection for Cache Side Channel Attack using Performance Counter Monitor". Applied Sciences-Basel, 2020.

블록체인을 활용한 공공기관 정보시스템에서의 개인 정보 유출 방지 시스템 제안

최승주*, 박재훈*, 서화정**

*한성대학교 IT 융합공학과

bookingstore3@gmail.com, p9595jh@gmail.com, hawjeong84@gmail.com

A proposal of preventing the leakage of personal information from public institution information system using blockchain

Seung-Joo Choi*, Jae-hoon Park*, HwaJeong Seo**

*Dept. of IT Convergence Engineering, Hansung University

요 약

보건 복지부, 병원, 동사무소 등의 공공기관에서는 업무 처리를 위해 사람들의 주민등록번호, 연락처, 주소 등 수많은 개인정보를 업무 처리를 위해 각 기관마다 사용하는 정보 시스템을 통해 다룬다. 그런데 이러한 정보 시스템을 통한 내부 정보 유출 사건이 지속적으로 발생하고 있다. 이와 같이 유출된 정보는 단순 유출자의 호기심으로 끝나기도 하지만 다른 영리 기관들에 팔려 악용되기도 한다. 이에 본 논문은 정보 시스템을 통한 개인 정보 유출을 방지하기 위해 블록체인을 활용한 시스템을 제안한다.

1. 서 론

최근 잇따른 개인정보 유출 사건이 지속적으로 발생함에 따라 개인정보에 대한 사회적 관심이 증가하고 있다. 지난 10년간 국내에서 발생한 개인정보 유출 사례는 60억 건이 넘으며[1] 이러한 개인정보 유출이 발생하는 주된 경로 중 하나는 공공 기관에서 사용되는 정보 시스템이다[2].

정보 시스템은 각 부서에서 업무를 처리할 때 사용되는 시스템으로서 보건복지부와 같은 경우 사회보장 정보시스템을 사용하며 이를 통해 각종 복지 혜택을 제공할 때 정부 부처나 지자체에서 심사목적 등으로 연락하는 통합 망을 사용하고 있으며 병원과 같은 경우 병원 정보 시스템을 통해 환자의 정보 및 신체에 대한 정보들을 공유하는 시스템을 사용하고 있다. 정보 시스템은 이름만 입력을 하면 해당 사람의 연락처, 주소 정보, 학력 정보, 건강 정보, 계좌 정보 및 상담 내역 등의 민감한 개인 정보를, 각 기관마다 사용되는 정보시스템에 따라 표시되는 정보의 차이는 있지만, 손쉽게 열람할 수 있다. 이처럼 공공기관에서 업무 처리를 진행할 수 있게 도와 국민들의 삶에 도움을 줘야하는 시스템이 오히려 공공기관 내부자에 의해 개인정보가 유출이 되는 주된 경로가 되고 있다.

이와 같은 개인정보 유출의 원인으로는 단순한 다른 사람의 상담 내역에 대한 호기심, 팬의 유명 연예인에 대한 호기심과 같이 단순 호기심과 같은 이유도 있지만 건강 관련 정보를 빼내어 해당 사람들에게 요양원 시설 등을 홍보하는 등 악용하기 위한 원인도 존재한다.

이와 같은 정보 시스템에 등록되어 있는 사람의 수는 천

백만 명이 넘으며 이를 열람할 수 있는 공무원의 숫자는 약 3만 7천명임을 감안하였을 때 정보 통신을 통한 개인정보 유출은 심각한 문제이며 해결책이 반드시 필요하다. 이에 본 논문에서는 블록체인을 활용하여 개인정보 사용 시 해당하는 개인에게 허락 및 알람이 가며 조회 기록을 변조되지 않고 유지할 수 있기 위한 블록체인을 활용한 정보 시스템을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 블록체인 기반 개인 정보 보호 정보 시스템을 위한 블록체인, 스마트 컨트랙트 등 관련 연구에 대해 살펴보고, 3장에서는 본 논문에서 제안한 시스템에서 사용되는 스마트 컨트랙트의 알고리즘을 간략히 구현하여 실제 시스템을 재현한 결과를 살펴본다. 마지막으로 5장에서는 제안 시스템에 대한 분석과 향후 필요한 연구 과제에 대하여 논의하며 결론을 맺도록 한다.

2. 관련 연구

2.1 블록체인

블록체인이란 동일한 전자 장부에 대한 데이터를 네트워크에 참여하고 있는 노드들이 함께 공유하고 검증하는 네트워크 시스템이다. 블록체인에서 사용되는 전자 장부의 내용은 다수의 노드가 함께 공유하고 해당 장부 기록이 동일하지 검증하기 때문에 공유 장부에 적힌 내용을 하나의 노드가 단독으로 위조 및 변조하기 어렵다는 특징이 있다. 이와 같은 블록체인의 특징을 이용하여 가상 화폐 개념을 도입하여 제 3의 공인기관이나 중개자의 개입 없이 익명간의 거래

를 진행할 때 사용되기도 한다.

블록체인에서 사용되는 공유 전자 장부가 위조 되지 않을 수 있었던 이유는 그림 1과 같은 구조를 통해 장부 내용의 위변조를 방지하기 때문이다. 블록체인 상에 기록을 남기는 행위를 트랜잭션이라 하며 이러한 트랜잭션은 블록이라는 구조에 담겨 블록체인 네트워크에 기록이 된다. 이때 블록에는 트랜잭션의 내용과 함께 시간, 논스 값 그리고 이전에 생성되었던 블록의 해시 값 정보 등이 같이 저장된다. 해시 함수란 임의의 길이의 데이터를 고정된 길이의 데이터로 만들어주는 함수로서 하나의 데이터만 달라져도 완전 다른 결과의 데이터가 도출이 되기 때문에 무결성을 증명하기 위한 용도로 많이 사용이 된다. 블록체인에서는 이런 해시의 특징을 이용해 공유 장부의 무결성을 보장하기 위해 블록 간에 이전 블록 해시 값을 저장해 각 블록이 해시 값으로 연결된 형태를 구성한다.

이와 같은 블록은 네트워크 참여자 중 블록을 형성하고 형성한 대가로 소량의 가상 화폐와 수수료를 받는 채굴자(miner)에 의해 형성이 된다. 이때 네트워크 참여자 중 가장 많은 블록이 형성된 장부의 기록을 검증 과정을 통해 네트워크 공식 장부로 인정을 하게 되고 해당 기록을 바탕으로 다른 기록들을 무효화해 모두가 같은 기록을 갖는 공유 장부를 소유할 수 있게 만든다.

만약 악의적인 네트워크 참여자가 특정 블록의 데이터를 위조 및 변조를 하려고 시도했을 때 변조된 블록 이후의 모든 블록들에 대한 해시 값을 다시 연산을 하고 다른 네트워크 참여자보다 더 많은 블록을 형성해야한다. 그러나 이러한 전체 네트워크의 연산 능력의 절반을 넘는 연산 능력을 악의적인 참여자 한명 또는 소수의 그룹이 보유하는 것은 사실상 불가능하기 때문에 블록체인 공유 장부는 위조 및 변조에 대한 내성을 지닐 수 있게 된다.

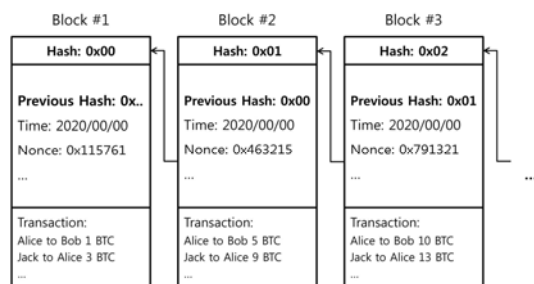


Fig. 1 Blockchain network's block structure

최초의 블록체인은 가명의 인물 사토시 나카모토가 2008년에 발표한 비트 코인[3]으로 공개형 블록체인 형태를 띠고 있다. 이는 해당 네트워크에 누구나 참여하고 싶은 주체는 누구나 참여할 수 있으며 누구나 블록을 형성하는 채굴자가 될 수 있는 구조이다. 그러나 최근에는 공개형 블록체인의 한계점[4]을 고려하여 기업형 또는 허가형 블록체인 형태도 출시되고 있다. 허가형 블록체인의 특징은 블록체인 네트워크에 참여할 수 있는 대상이 정해져있으며 해당 네트워크에 참여하기 위해서는 네트워크를 운영하고 있는 주체의 허락

을 받아야 참여할 수 있다는 점이다. 허가형 블록체인의 특징을 블록 형성을 위한 컴퓨터 연산 과정을 투표 형식으로 대체하거나 블록 생성 시간을 단축하는 등 기업과 같이 블록체인 네트워크를 공개한 상태로 운영할 필요가 없는 기관에서 사용된다.

2.2 스마트 컨트랙트

스마트 컨트랙트는 디지털로 만들어진 계약서를 의미하며 1994년 최초로 제안되었다. 이와 같이 디지털 상으로 존재하는 스마트 컨트랙트는 작성된 계약 조건이 만족되면 3자의 개입 없이도 즉각 이행될 수 있으며 해당 이행에 대한 결과가 명확하게 도출된다는 특징을 갖고 있다. 이와 같은 무결성과 정확성의 특징을 갖고 있는 스마트 컨트랙트의 개념을 2세대 블록체인이라고 불리는 이더리움에서 최초로 블록체인 네트워크에 가져와 적용하였다[5].

이와 같은 스마트 컨트랙트를 통해 많은 탈중앙화 어플리케이션(DApp, Decentralized Application)이 제작이 되고 있으며 대표적인 공개형 블록체인인 이더리움 뿐만 아니라 기업형 블록체인인 하이퍼레저[6] 등 다른 여러 종류의 블록체인 네트워크에서도 많이 제작 및 배포가 되어 여러 서비스에서 사용이 되고 있다.

이와 같은 스마트 컨트랙트를 이용하여 본 논문에서는 정보 시스템을 통한 개인 정보 열람 시 처리되어야 할 절차들 및 스마트 컨트랙트의 구조를 3장에서 제안한다.

3. 시스템 제안

개인 정보 유출이 발생해도 알기 어려운 것은 공공 기관에서 정보 시스템을 통해 해당 정보를 조회해도 일반적인 업무에 참조하는 자료로서 사용되기 때문에 별다른 조치가 이뤄지지 않기 때문이다. 조회를 위해서는 신청이 이뤄져야 하지만 해당 정보를 갖고 실제로 어디에 쓰였는지 등에 대한 처리는 이뤄지지 않고 있다.

이를 해결하기 위해서는 우선 개인 정보의 소유는 엄연히 개인에게 존재하기 때문에 이를 바탕으로 개인의 정보를 조회 시 해당 사람에게 그 사실을 알려주는 시스템을 정보시스템에 적용하는 것이 우선이다. 가장 좋은 방법은 공공 기관에서 개인 정보를 이용한 업무를 처리해야 할 때 개인 정보 조회 민원뿐만 아니라 해당하는 개인에게 사용하는 때마다 동의를 구하는 것이다. 그러나 현실적으로 업무 처리에 있어 해당하는 사람이 연락이 되지 않을 수도 있으며 답변이 없다면 무한정 업무가 처리되지 않을 수 있기 때문이며 이는 시간적으로 너무 소요가 되는 방법이다. 하여 조회를 할 때마다 동의를 받지 않고 조회 사실과 조회 목록에 대한 알림을 해당 사용자에게 실시간으로 전송하는 할 것을 제안한다. 이와 유사한 시스템으로는 구글의 알림 서비스를 볼 수 있다. 구글에서는 다른 컴퓨터에서 계정에 대한 새로운 접근이 발생하면 접근을 시도한 아이피 주소와 시간대 그리고 해당 접근의 주체에 대한 질문을 이메일과 알림을

통해 계정 소유자에게 전달한다. 이와 마찬가지로 개인 정보에 대한 조회가 정보 시스템을 통해 일어날 때마다 어떠한 기관에서 어떤 개인 정보에 대한 조회가 일어났는지를 개인 정보 주체에게 알람을 보낼 것을 제안한다. 해당 시스템은 미리 작성된 스마트 컨트랙트를 통해 일어나며 순서는 다음과 같다.

먼저 개인 정보를 정보 시스템을 통해 조회하고자 하는 기관에서 조회하고자 하는 정보의 종류와 사유 그리고 기관명을 스마트 컨트랙트에 트랜잭션을 보내 요청한다. 그럼 해당하는 정보를 요청할 수 있는지 트랜잭션 요청자에 대한 권한을 검증하고 만약 권한이 있는 자라면 각 기관에서 해당 정보를 볼 수 있게 허락하는 권한을 가진 사람의 동의를 기다린다. 해당 동의가 일어나면 요청한 정보가 전송이 되며 이때 정보에 해당하는 개인에게 개인 정보 조회 사실이 앞서 말한 사유와 기관 등의 정보와 함께 알람이 전송된다.

제안하는 시스템에서 사용되는 스마트 컨트랙트 구조는 그림 2 와 같다.

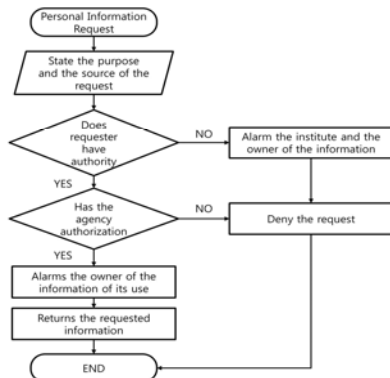


Fig. 2 Structure of Information system smart contract

기관에서 업무를 처리하기 위해 개인 정보 조회 요청을 블록체인에 등록되어 있는 스마트 컨트랙트에 요청을 보낸다. 이때 조회하고자 하는 정보에 대한 자세한 명세와 요청을 보낸 기관 등에 대한 구체적인 정보를 함께 전송한다. 해당 요청을 받은 스마트 컨트랙트에서는 요청을 보낸 사람이 개인 정보를 취급할 수 있는 인물로 스마트 컨트랙트에 등록이 되어있는 사람인지 확인을 한다. 만약 허가되지 않은 사람이라면 해당 기관과 개인 정보의 주인에게 해당 사실에 대한 알람을 전송하고 요청을 거부한다. 요청 권한이 있는 사람이라면 해당 요청에 대한 기관의 상부의 허가를 기다린다. 만약 상부에서 허가를 해 주지 않는다면 요청을 기각하며 이때는 알람을 보내지는 않는다. 허가가 난 경우 요청 정보의 주체에게 해당 개인 정보가 어느 기관에서 어떠한 목적으로 언제 조회가 되었는지 알람을 보내고 요청을 보냈던 사람에게 해당 개인 정보의 정보를 전송한다.

이와 같은 블록체인 네트워크는 각 기관의 정보 시스템을 통합하여 공개형 블록체인으로 구성하여 기록에 대한 조작을 각 기관에서 견제하여 정보의 무결성을 보장할 수 있다. 또한 개인 정보 조회에 대한 사실을 실시간으로 전달함으로써 개인 정보의 사용 사실을 명확히 할 수 있으며 만일 개

인 정보가 불분명한 이유로 조회가 되면 바로 알 수가 있어 조치가 가능하다.

4. 시스템 구현

4.1 제안 기법 구현

본 논문에서 제안하는 기법을 구현하여 동작을 확인하였다. 구현은 이더리움에서 제작한 스마트 컨트랙트 언어 솔리디티(Solidity)를 사용했으며 개발 IDE는 리믹스(Remix) 환경을 사용하였다.

스마트 컨트랙트는 컨트랙트 배포자의 주소, 조회 권한이 있는 직원의 주소의 값을 저장하며 추가로 이름, 주민등록번호, 전화번호 그리고 집 주소에 대한 값을 배열로 저장하게 구현하였다. 이때 스마트 컨트랙트 배포자의 주소는 리믹스에서 임의로 생성한 주소 0xca3로 시작하는 주소를 사용했으며 직원의 주소는 0x147로 시작하는 주소 값을 지정하였다. 해당 값들을 이용해 구현한 결과는 그림 3과 4와 같다.



Fig. 3 Personal information request permitted

그림 3의 from, 즉 정보 요청을 보낸 주소를 보면 0x147, 즉 정보 시스템에 등록된 직원의 주소임을 알 수 있다. 해당 직원의 요청에 대한 허가가 나면 decoded output 부분을 보면 임의로 입력해 놓은 홍길동에 대한 이름, 주민등록번호, 전화번호 그리고 집 주소가 반환된 것을 알 수 있다. 또한 logs를 보면 개인 정보가 현재 허가 받은 직원으로부터 조회되고 있다는 로그가 성공적으로 뜬 것을 볼 수 있다.



Fig. 4 Personal information request denied

그림 4와 같은 경우 from, 즉 정보 요청을 보낸 주소를 보면 0x4b0으로 시작하는, 즉 정보 시스템에 등록되지 않은

주소로부터 개인 정보에 대한 조회 요청이 온 것을 볼 수 있다. 허가되지 않았기에 decoded output 부분을 보면 반환된 값이 없음을 알 수 있으며 logs에서 해당 개인 정보가 노출 되었으니 즉시 해당 기관에 연락을 취하라는 알람이 보내진 것을 볼 수 있다.

4.2 성능 평가

기존 정보 시스템과 같은 경우 접근 기록은 남지만 정보 주체에게 조회 사실이 알려지지는 않았고 이 때문에 개인 정보 유출에 대한 대응이 늦어질 수밖에 없었다. 그러나 본 논문에서 제안한 방식을 통하면 실시간으로 이러한 유출 사태를 알 수 있다 또한 각 개인 정보에 대한 관리는 각각의 기관에서 진행하였지만 본 논문에서 제안한 블록체인을 활용하면 정보에 대해 같이 공유하여 관리하기 때문에 저장된 정보들에 대한 무결성 또한 보장이 된다. 표 1에서 본 논문의 제안 기법과 기존 조회 기법의 비교를 정리한다.

Table 1. Comparison between conventional and proposed personal information referencing method

	Conventional	Proposed
Send notification to information owner	None	Real time
Manipulation possibility	Possible through internal operation	Impossible
Data integrity	Unverified	Verified by network

5. 결 론

본 논문에서는 블록체인의 스마트 컨트랙트를 활용하여 정보 시스템의 개인 정보 유출을 방지하는 시스템을 제안하였다. 개인 정보 주체에게 조회 사실이 전송되게 하는 구조를 통해 어떤 기관에서 무슨 사유로 인해 개인정보를 열람하는지 알 수 있는 구조를 제안하였다. 이를 통해 개인의 엄연한 자산인 개인 정보가 어디에서 사용되는지 실시간으로 알 수 있을 것으로 판단된다.

개인 정보 유출은 정보화시대가 가속화 되면서 앞으로 더욱 심각한 사건으로 받아들여져야 하는 요소이다. 그러나 개인 정보의 유출에 관한 불감증은 여전히 낮은 상태이다 [7]. 앞으로 개인 정보에 대한 보호는 기술적인 측면에서도 접근이 필요하지만 무엇보다 정보들의 주체가 개인 정보의 중요성을 인지하고 적극적으로 보호할 필요가 있을 것으로 보인다.

References

- [1] The Radio News. "6 billion unauthorized leaks of personal information over 10 years" [Internet]. Available: <http://www.jeonpa.co.kr/news/articleView.html?idxno=59734>
- [2] United News, "Welfare officials continue to illegally access personal information". [Internet], <https://www.yna.co.kr/view/AKR20181010043300017>
- [3] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic cash System" metzdowd.com, Oct. 2009.
- [4] Jae Young Lee, Cheong Won Woo, Prospects, "Limitations and Implications of Blockchain Technology", FUTURE HORIZON, vol. 38, no. 4, Dec. 2018.
- [5] Ethereum. A Next-Generation Smart Contract and Decentralized Application Platform [Internet]. Available: https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf
- [6] Hyperledger. An Introduction to Hyperledger [Internet]. Available: <https://www.hyperledger.org/>.
- [7] United News. "Hana Tour penalty 30 million won, Personal information protection insensitivity" [Internet]. Available: <https://www.yna.co.kr/view/AKR20180206100300004?input=1195m>

단일 부채널 전력 파형을 사용한 마이크로컨트롤러 상에서 소프트웨어 표절 탐지

김현준*, 장경배*, 김경호*, 서화정*

*한성대학교 IT융합공학부

khj93072004@gmail.com

Similar Software Code Detection Using Side Channel Leakage in Microcontrollers

Hyun-Jun Kim*, Kyung-Bae Jang*, Kyung-Ho Kim*, Hwa-Jeong Seo*

*Division of IT convergence engineering, Hansung University

요 약

부채널 정보를 사용하여 마이크로 컨트롤러 상에서 표절 된 코드를 탐지하는 새로운 방법을 제시한다. 제안 기법은 애플리케이션을 보호하기 위해 추가로 워터 마킹 할 필요가 없이 코드를 실행하는 마이크로 컨트롤러의 유출데이터를 워터 마크로서 사용 할 수 있다. 두 가지 다른 구현의 각각 하나의 부채널 파형에 대한 절대 상관 계수를 기반으로 분석 한다. 어셈블리 언어로 작성된 다양한 테스트 응용 프로그램을 사용 Xmagal28 마이크로 컨트롤러에서 평가하였다. 제안 기법은 어셈블리 코드를 수정하는 공격자에게도 강력하며 코드에 대한 정보와 입력에 대한 접근이 불가능 하여도 탐지가 가능하다.

1. 서론

임베디드 시스템에서 작동하는 소프트웨어는 지적 재산권으로 보호받을 수 있으며 일반적으로 개발자가 지적 재산권 (IP) 코어라고 하는 타사 디자인을 구매하고 사용한다. Marketsandmarkets의 연구에 따르면 임베디드 시스템은 2020년 865억 달러에서 2025년 1,110억 달러로 성장할 것으로 예상된다. 2020 년에서 2025년까지 연평균 6.1 % 증가할 것으로 예상하고 있다[1]. 이와 함께 IP 코어 판매에 대한 시장도 커지며 IP 도용 또한 중요한 위협이 되었다.

IP는 리버스 엔지니어링을 통해 해킹하고 디자인을 불법 복제하여 판매하거나 사용 할 수 있다. 이런 문제는 제품 수익에 큰 영향을 끼치는 만큼 임베디드 시스템 제조업체의 큰 관심 사항이며 IP 불법 복제를 방지하기 위해 다양한 기술이 제안되었다.

이러한 IP 불법 복제를 방지하기 위한 방법으로 워터마킹 기술을 활용하는 방법이 있다. 소프트웨어 워터마크는 공격자가 프로그램을 복사하는 것을 막지는 않지만, 복제를 탐지하는 데 사용된다. 워터 마킹은 리버스 엔지니어링 분석보다 저렴한 비용으로 불법 복제물을 탐지할 수 있다.

워터마크 기법에는 감지하는 소프트웨어나 실행 중인 메모리에 대한 접근이 필요하다. 그러나 코드

복사가 관련 위협이 있는 시스템의 경우에는 대부분 메모리가 무단 읽기 작업으로부터 보호되기 때문에 임베디드 환경에서는 의심스러운 코드에 접근하기가 쉽지 않다. 이 문제를 해결하기 위해 최근 연구에는 프로그램 코드에 접근하지 않고 감지 할 수 있는 부 채널 정보 기술을 사용한 워터마킹 방법이 제안되고 있다.

관련된 가장 최근의 연구에서는 공격자가 IP 표절 탐지를 막기 위해 마이크로 컨트롤러 상에서 코드가 작동할 때 나타나는 전력 파형을 비교하여 표절 여부를 판단한다[2, 3, 4, 5]. 이때 분석을 위해 10만 개 이상의 파형과 같은 입력값을 사용하나 입력이 알려지지 않거나 입력 데이터를 조작할 수 없는 경우에는 이러한 분석이 불가능하다[5]. 본 논문에서는 다른 입력값에서도 적용되며 하나의 파형으로도 분석 가능한 새로운 기법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 제안하는 기법에 대해 설명한다. 3장에서는 제안 기법에 대한 실험을 통해 성능을 평가한다. 4장에서는 본 논문의 결론과 추후 연구 방향에 대해 기술한다.

2. 제안기법

kocher의 부채널 공격에 대한 개척 이후 마이크로컨트롤러에서 코드가 실행되는 동안 전력 소비,

전자기 방출에서 사이드 채널 누설을 유발한 다는 것이 잘 알려졌다[6]. 마이크로 컨트롤러에서 수행되는 명령어들은 각각의 다른 전력 소비를 갖는다. 제한 기법에서는 IP 보호를 구현된 프로그램 코드와 구현된 미지의 의심스러운 코드의 전력 파형을 사용한다. 두 코드의 파형의 상관 계수를 계산하면 두 코드의 유사도가 높을수록 상관계수가 높게 나타난다. 만약 공격자가 코드를 복사 할 경우 코드 상에서 동일한 부분은 높은 상관계수를 나타낼 것이다. 제한 기법에서는 원본파형을 일정길이의 구간으로 나누어 원본파형이 드러나는 부분을 탐색하여 IP 탐지에 적용하였다.

공격 공격은 두 가지의 경우로 나눌 수 있다. 첫 번째로는 공격자가 도난한 IP를 그대로 사용하는 경우이다. 두 번째는 공격자가 도난한 IP를 수정하여 사용하는 방법이다. 첫 번째의 경우는 일반적인 워터마킹의 기법으로 IP복제의 여부를 판단 할 수 있지만 두 번째의 경우에는 워터마킹으로 사용된 코드 부분을 수정하여 IP탐지를 방해 할 수 있다. 제한 기법에서는 공격자가 이 두 가지의 공격에 대한 방어를 중점으로 두었다.

추출 데이터의 추출은 정품의 프로그램과, 알려지지 않은 프로그램의 파형을 수집하여야한다. 정품 코드의 파형을 워터 마킹으로 사용하며 대상장치에서 사용되는 입력값을 선택 할 수 없다고 가정하여 해당코드는 알려지지 않은 입력에 대한 입력을 사용한다. 측정은 유사성을 비교하기 쉽도록 두 프로그램은 동일한 측정 설정을 사용한다.

전처리 동일한 파형이라도 노이즈로 인해 변경될 수 있다[4]. 데이터의 압축과 노이즈에 대한 필터링을 위해 FFT (Fast Fourier Transform)를 적용한다.

탐지 탐지는 추출한 두 개의 데이터에서 4개의 행렬을 생성한다. 이 4개의 행렬을 사용하여 상관계수를 계산하고 최대값으로 사영하고 이 값을 비교한다.

추출 데이터 기반으로 행렬 생성 추출한 정품코드의 파형 데이터를 N의 길이로 나눈 $N \times M1$ 행렬 T_{genuine} 과 추출한 의심코드의 파형 데이터를 N의 길이로 나눈 $N \times M2$ 행렬 T_{unknown} 을 생성한다. M은 각 데이터 샘플의 길이를 N으로 나눈 값이다.

추출한 코드의 파형 데이터의 길이 l을 N만큼 추출한 값을 모든 구간에서 추출하여 FFT 적용

$$T' = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-2} & a_{n-1} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ a_{l-n} & a_{l-n+1} & \cdots & a_{l-n+1} & a_{l-1} \end{pmatrix}$$

를 생성한다. 정품 파형의 데이터로 $N \times M1'$ 행렬 T'_{genuine} 과 의심 파형의 데이터로 $N \times M2'$ 행렬

T'_{unknown} 을 만든다.

피어슨 상관계수 계산 제안기법에서는 전력 기반 암호 분석 분야에서 많이 사용되고 있는 피어슨 상관관계를 사용한다. 정품 코드와 미지의 코드에 데이터 누출 간의 유사성을 계산 하기 위해 행렬 T_{genuine} 와 T'_{unknown} 의 상관계수로 이루어진 $M1 \times M2'$ 행렬 S1 그리고 행렬 T_{unknown} 와 T'_{genuine} 의 상관계수로 이루어진 $M2 \times M1'$ 행렬 S2를 구한다.

Maximum Projection 구간으로 나눈 파형이 비교하는 파형과 유사한 지점이 있다면 해당 구간은 그 지점에서 높은 상관계수를 갖는다. 이러한 값을 찾기 위해 S1와 S2의 열에서 최대값으로 이루어진 $p1_{\text{col}}$ 와 $p2_{\text{col}}$ 를 구한다.

이 $p1_{\text{col}}$ 와 $p2_{\text{col}}$ 의 평균치로 표절 여부를 판단하고 각 구간에 대한 값을 사용하여 해당 구간에 대한 유사성을 판단하여 표절 후 수정 여부를 평가한다.

3. 실험

실험에서 장치의 수집은 입력이 알려지지 않은 단일 파형이 사용되며 소스 코드 또한 알려지지 않았다. 측정에는 동일하게 ChipWhispererLite XMEGA (8-bit processor)[7] 사용하며 7.38 MS/s 샘플링으로 모두 동일한 설정을 사용한다.

3.1 같은 암호에 다른 구현 비교

같은 알고리즘에도 구현에 따라 속도와 구조가 다르다. IP의 구분에 있어서도 서로 다른 IP로 간주 해야한다. 또한 코드의 일부가 유사하거나 동일하다는 것을 확인하기 위해 3가지의 AES 암호화 구현에 대한 테스트를 진행한다.

<표 1> Furious와 다른 AES암호구현과의 제안기법을 사용한 n에 따른 절대 상관계수

	400	200	100	50
Furious	0.99213	0.99170	0.99287	0.99486
	0.99216	0.99194	0.99320	0.99507
Fast	0.83707	0.88271	0.92129	0.96302
	0.88861	0.92829	0.95482	0.98099
Fantastic	0.84027	0.88468	0.91259	0.94188
	0.88577	0.91963	0.94888	0.96943

<표 1> 은 모든 테스트 AES 구현에 대한 평균 절대 상관 계수를 보여준다. 라운드의 반복으로 같은 구간에 대한 비교로 유사한 파형이 반복됨을 알 수 있다. (그림 1)과 같이 같은 구현을 비교할 경우 N의 값이 작아지더라도 0.99 이상의 비교적 높은 상관계수를 나타낸다.

다른 구현의 경우에는 N의 값이 클수록 높은 상관 계수를 나타내며 N의 작을 경우 (그림 2)와 같이 동일한 코드의 부분에서는 높은 상관계수를 나타내고 그렇지 않은 부분에서는 낮은 상관계수를 드러낸다. 그래프를 통해 코드의 어느 부분이 유사하거나 동일한 지 알 수 있다.

3.2 표절 후 수정된 구현 비교

코드를 적극적으로 조작하는 공격자를 시뮬레이션 하기 위해 Furious를 실제 구현으로 선택하고 6개의 방식으로 수정한다.

주소변경 구현에서 사용되는 레지스터와 SRAM 주소를 변경한다.

명령어변경 가능한 경우 클럭 사이클의 변경 없이 명령의 순서나 명령어를 바꾼다.

주소와 명령어 변경 구현에서 사용되는 레지스터와 SRAM 주소 그리고 명령의 순서를 바꾼다.

NOP 더미 추가 더미로 NOP명령어를 삽입한다. 실험에는 570 사이클을 추가 하였다.

Smart 더미 추가 더미로 NOP 명령어를 사용시에는 전력 소비가 적기 때문에 구별이 쉽다. 전력소비를 보다 정교하게 보이기 위해 Smart 더미[5]를 사용한다. 실험에는 570 사이클을 추가 하였다.

주소와 명령어 변경과 Smart 더미 추가 레지스터와 SRAM 주소 그리고 명령의 순서를 변경하고 Smart 더미[5]를 추가한다.

<표 2> 실제 구현과 수정한 코드의 제안기법을 사용한 n에 따른 절대 상관계수

	400	200	100	50
addr	0.98174	0.98092	0.98204	0.98700
	0.98230	0.98124	0.98272	0.98786
swap	0.99026	0.98946	0.98998	0.99198
	0.99023	0.98943	0.99021	0.99218
addr+swap	0.98123	0.98073	0.98243	0.98707
	0.98168	0.98176	0.98338	0.98773
dummy (nop)	0.88323	0.92220	0.93959	0.96058
	0.88191	0.92733	0.96737	0.98681
dummy (smart)	0.78183	0.85451	0.91320	0.95578
	0.81031	0.91686	0.96328	0.98745
addr+swap+ dummy(smart)	0.79846	0.85621	0.91140	0.95135
	0.81913	0.91282	0.95799	0.98227

<표 2>는 수정한 코드의 평균 절대 상관 계수를 보여준다. 레지스터 수정과 명령어 교환에서는 수정과 무관하게 높은 평균의 상관계수를 나타내 표절하여도 탐지가 가능하다.

더미를 추가 하였을 경우에는 더미의 추가가 상관

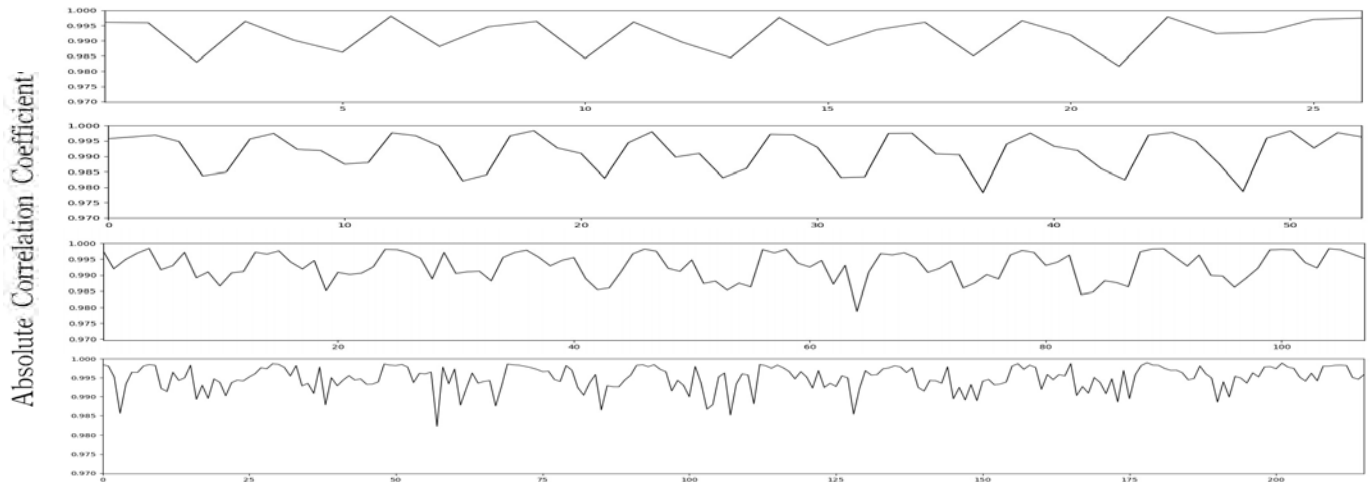
계수를 낮추는 것을 알 수 있다. 그러나 더미 추가의 경우 N의 크기를 줄이면 (그림3), (그림4)와 같이 수정 전 코드구간을 수정코드에 탐색할 경우에는 전체적으로 높은 상관계수를 나타내지만 반대의 경우는 더미를 추가한 구간의 상관계수가 낮게 나와 이를 구분할 수 있다. 그림 과 같이 유사성을 나타내는 그래프에서 차이로 더미를 추가하였음을 알 수 있어 더미 코드를 추가 하였어도 탐지가 가능함을 확인할 수 있다.

4. 결론

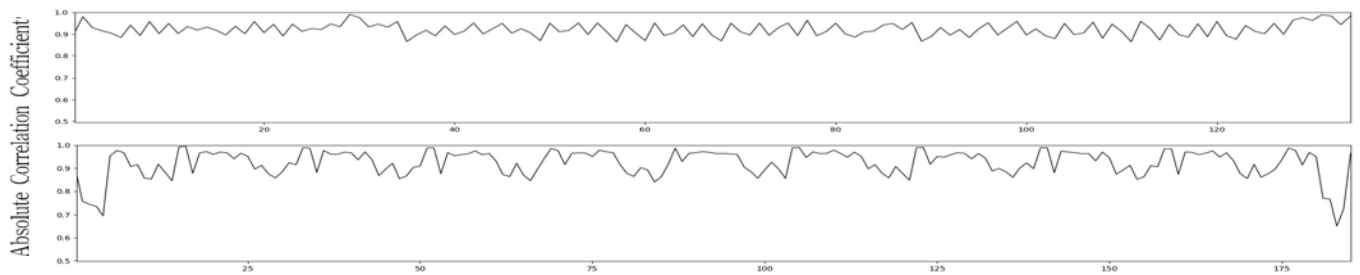
마이크로 컨트롤러 플랫폼에서 소프트웨어 표절을 탐지하기 위한 새로운 방법을 제시하고 평가하였다. 소스 코드와 입력이 데이터가 알려지지 않은 까다로운 시나리오에서 IP를 식별 할 수 있었다. 또한 실험에서 제안하는 방법이 여러 가지 코드 변환에 강력 함하며 코드에 추가적인 작업이 필요 없이 적은양의 마이크로 컨트롤러의 데이터 유출만으로 IP 식별이 가능함을 보였다

참고문헌

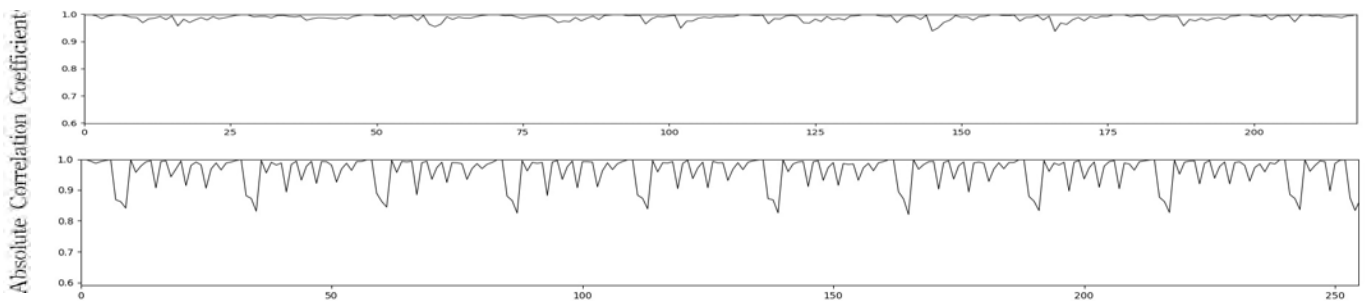
- [1] Embedded System Market by Hardware, Software, System Size, Functionality, Application, Region - Global Forecast to 2025. <https://www.marketsandmarkets.com/Market-Reports/embedded-system-market-98154672.html>
- [2] Becker, G., Strobel, D., Paar, C., Burleson, W.: Detecting software theft in embedded systems: a side-channel approach. IEEE Trans. (2012)
- [3] Strobel, D., Bache, F., Oswald, D., Schellenberg, F., Paar, C.: SCANDALee: a sideChANnel-based DisAssembLer using local electromagnetic emanations. In: Design, Automation, and Test in Europe (DATE), 9 - 13 March 2015 (2015)
- [4] Durvaux, F., Gérard, B., Kerckhof, S., Koeune, F., Standaert, F.-X.: Intellectual property protection for integrated systems using soft physical hash functions. In: Lee, D.H., Yung, M. (eds.) WISA 2012. (2012).
- [5] Peter Samarin, Kerstin Lemke-Rust: Detecting Similar Code Segments Through Side Channel Leakage in Microcontrollers. ICISC 2017: 155-174
- [6] Kocher, P., Jaffe, J., Jun, B.: Differential power analysis. In: Wiener, M. (ed.) CRYPTO 1999. (1999).
- [7] NewAE Technology Inc. ChipWhisperer-Lite. https://wiki.newae.com/CW1173_ChipWhisperer-Lite.



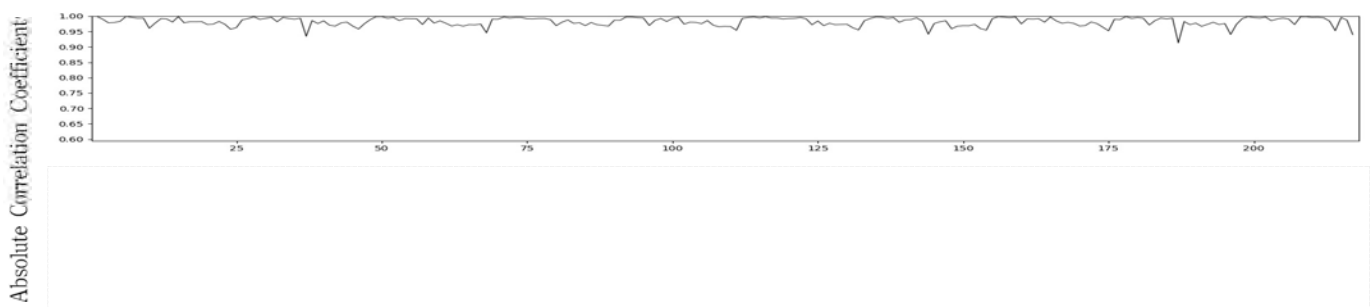
(그림 1) Furious와 Furious의 n=400, 200, 100, 50에서 p1col 그래프 n의 개수와 상관없이 높은 상관계수를 나타낸다.



(그림 2) 위 Furious와 Fast의 n=100에서 p1col 그래프와 아래 AES암호 구현 Furious와 Fantastic의 n=100에서 p1col 그래프 Furious와 Furious 비교 보다 낮은 상관계수를 나타낸다.



(그림 3) Furious와 dummy(nop)을 추가한 Furious의 n=50에서 p1col 그래프와 p2col 그래프. p1col 그래프와 다르게 p2col 그래프는 추가된 더미 코드 부분에서의 상관계수가 높게 나오는 것을 확인 가능하다.



(그림 4) Furious와 Dummy(smart)을 추가한 Furious의 n=50에서 p1col 그래프와 p2col 그래프. p1col 그래프와 다르게 p2col 그래프는 추가된 더미 코드 부분에서의 상관계수가 높게 나오는 것을 확인 가능하다.

정규표현식을 이용한 시스템 로그 분석

김홍경*, 이정현**

*부경대학교 일반대학원 정보보호학협동과정
khk009@kamco.or.kr, khrhee@pknu.ac.kr

An Analysis of System Log using Regular Expressions

Hong-Kyung Kim*, Kyung-Hyune Rhee**

*Dept. of Information Security, Pukyong-National University

요 약

보안업무를 수행하는 담당자로서 사이버 피해 여부를 파악하기 위한 가장 중요한 업무 중의 하나는 피해를 입은 시스템과 서비스에서 발생하는 다양한 로그들을 정확하게 분석하는 것이다. 그러나 해당 기관이 보안로그를 전문적으로 분석하는 SIEM(Security Information and Event Management)과 같은 솔루션이 없을 경우, 보안업무 담당자가 피해 시스템에서 추출된 로그만 가지고 직접 분석하여 공격여부를 판단하기는 쉽지 않다. 따라서 본 논문에서는 정규표현식을 이용하여 다양한 시스템의 로그를 쉽고 정확하게 분석하는 방법을 제시한다.

1. 서론

해커가 시스템의 취약점을 공격하기 위해서 가장 쉽게 접근하는 경로는 인터넷과 접점을 두고 있는 웹서버라 할 수 있다. 웹서버의 사이버 침해 여부를 확인하기 위해서는 웹서버의 로그파일을 정확하게 분석하여야 한다. 기업에서 운영하는 웹서버의 운영체제는 다양하지만, 본 연구에서는 현재 가장 많이 사용하고 있는 리눅스 운영체제 시스템과 Apache 웹서버에 대한 로그를 분석하고자 한다.

본 논문에서는 기업용 로그 분석솔루션이 없는 경우 보안업무 담당자가 직접 웹서버의 access_log 파일을 분석하는 과정에서 공격패턴을 정확하게 확인하기 위하여 정규표현식(Regular Expressions)을 이용하는 것에 목적이 있다.

이를 위하여 웹서버의 사이버 침해 여부를 확인하기 위한 웹서버의 로그파일을 선별하여 추출하고 그 로그파일의 내용에서 특정 문자열을 대상으로 조건을 지정하여 검색/치환/검사를 실행하는 방법[1]으로 정규표현식을 활용하여 웹서버 로그파일의 분석결과를 정확하게 추출하고자 한다.

2. 로그파일 분석 요구사항

2-1. 로그파일의 수집

본 논문에서는 시스템에서 생산되는 다양한 로그들이 있지만 해커의 침해위험에 대비하기 위하여 보안업무 담당자가 우선 수집하여 분석해야 할 로그 유형들을 <표 1>과 같이 몇 가지 선별하여 정의한다.

<표 1> 사이버 침해 분석에 필요한 로그 유형

로그파일명	저장데이터
access_log	웹서버 접속정보
error_log	웹서버 error정보
messages	콘솔 화면에 출력되는 메시지 정보
secure	사용자 인증에 관련된 정보

물론 <표 1> 이외의 로그 유형도 많이 있고 침해사고 유형에 따라 분석해야 하는 로그파일은 다를 수 있다.

2-2. 정규표현식 문법

보안업무 담당자는 침해사고가 발생한 시점의 로그파일을 수집하여 정규표현식을 통하여 분석하고자 할 경우 정규표현식의 문법규칙을 이해해야 한다.

그 이유는 로그유형마다 문자열 집합이 다를 수 있고 로그 내용에서 꼭 확인해야 하는 정보만 선택적으로 분류해서 재 정의하고 분석결과를 추출해야 할 필요도 있기 때문이다.

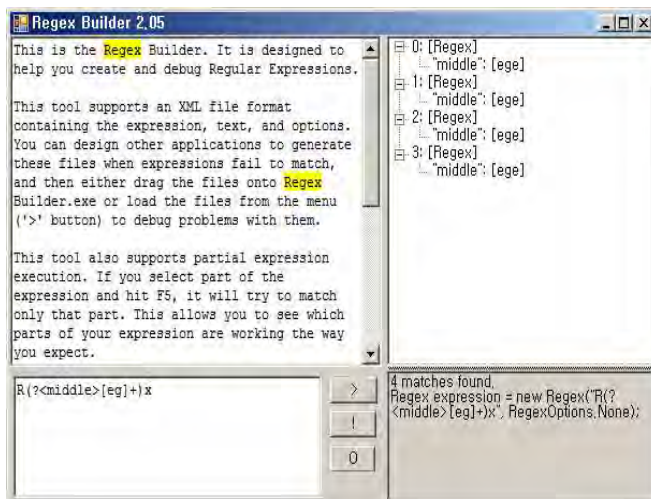
이를 위하여 사이버 침해 분석에 필요한 로그 유형에서 선별한 로그파일을 분석하기 위한 Symbol[2]을 <표 2>와 같이 선별하여 정의한다.

<표 2> 정규표현식 Symbol 과 Meaning

Symbol	Meaning
Wd	숫자만 매치(문자·특수문자 제외)
Ww	영숫자 문자나 밑줄과 일치(특수문자 제외)
Ws	공백 문자와 일치
+	문자 하나 이상 찾기
*	문자가 없거나 하나 이상 연속문자 찾기
W	문자열로 사용할 때 사용
()	찾은 값 중 원하는 값을 캡처
[]	대괄호 안의 문자를 or조건으로 찾을
^	문자열의 첫시작과 일치
\$	문자열을 끝냄
(?<alias명>)	캡처한 값에 alias명을 부여
값?	? 앞에 지정한 값의 유무의 조건 지정
(?:)	괄호 안에 내용은 캡처 안함

2-3. 분석 프로그램

본 논문에서는 Apache 웹서버의 access_log를 정규표현식으로 분석하기 위한 프로그램인 Regex Builder[3]을 활용한다. Regex Builder 프로그램은 C#으로 작성된 WinForm 응용프로그램으로써 개발자가 정규표현식을 쉽고 빠르게 작성하고 테스트 할 수 있도록 돕는 프로그램이다.[4]



(그림 1) Regex Builder 프로그램

3. 로그파일 분석

아래의 (그림 2)는 Apache 웹서버의 원본 access_log 에서 사이버 위협이 의심되는 로그내용만 추출하기 위하여 정규표현식 문법규칙을 적용하

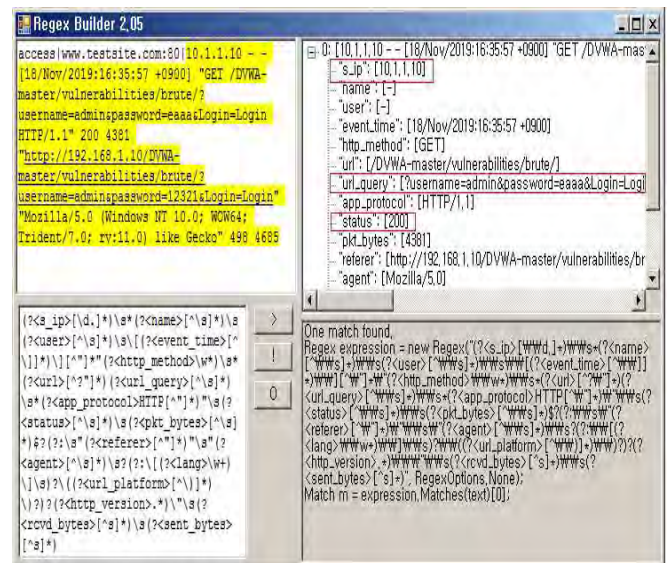
여 치환한 결과이다.

```
=====원본로그=====
access/www.testsite.com:80|10.1.1.10 - - [18/Nov/2019:16:35:57 +0900] "GET
/DVWA-master/vulnerabilities/brute/?username=admin&password=eaaa&Login=Login
HTTP/1.1" 200 4381
"http://192.168.1.10/DVWA-master/vulnerabilities/brute/?username=admin&password
=12321&Login=Login" "Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0)
like Gecko" 498 4685

=====정규표현식=====
(?<s_ip>[d.]*\s*(?<name>[^\s]*)\s*(?<user>[^\s]*)\s*(?<event_time>[^\s]*)\s*(?<ht
tp_method>[w]*\s*(?<url>[^\s]*)\s*(?<url_query>[^\s]*)\s*(?<app_protocol>HTTP[^\s]*)\s(
?<status>[^\s]*)\s*(?<pkt_bytes>[^\s]*)$?(?:\s*(?<referrer>[^\s]*)\s*(?<agent>[^\s]*)\s*(?:
\\(?:<lang>[w-]*\s*)\s*(?<url_platform>[^\s]*)\s*)\s*(?<http_version>[^\s]*)\s*(?<rcvd_bytes>
[^\s]*)\s*(?<sent_bytes>[^\s]*)
```

(그림 2) Apache access_log 정규표현식 치환

아래의 (그림 3)은 Apache 웹서버의 원본 access_log 와 정규표현식을 Regex Builder 프로그램 을 이용해서 분석한 결과를 나타낸다.



(그림 3) Regex Builder 프로그램 분석결과

위의 Regex Builder 분석 결과를 통해 해커의 ip 주소는 “s_ip”:10.1.1.10, 공격은 “url_query”로 username=admin, password=eaaa를 전송하여 관리자 권한으로 로그인을 시도하였고 “status”: 200을 볼 때 공격이 성공한 것으로 판단할 수 있다.

4. 결론

본 논문에서는 Apache 웹서버의 access_log 파일에서 일부분의 로그를 정규표현식 문법규칙을 활

용하여 피해를 정확하게 분석하였다. 하지만 개선된 방안으로, 시스템의 Log Format을 공통로그형식으로 설정한다면 표준 형식의 로그파일로 별도 생산할 수 있고, 웹 페이지 형태의 정규표현식 검사기 애플리케이션을 개발[5]한다면 표준 형식의 로그파일을 웹 페이지에 업로드 하여 로그파일 분석결과를 자동으로 얻을 수 있다.

참고문헌

- [1] Young-Bo Kim, "Regular Expression with JavaScript", ITC, 2010, Page 1.
- [2] Junghoo Cho and Sridhar Rajagopalan, "A Fast Regular Expression Indexing Engine", IEEE, San Jose in USA , 2002, Page 3.
- [3] Regex Builder Program Download Path "<http://www.sourceforge.net/projects/regexbuilder/>"
- [4] Dimitar and George Totkov, "Visual Parser Builder", RANLP , 2005, Page 4.
- [5] Joonseon Ahn and Yeong-Min Kim and Jang-Wu Jo, "Development of a String Injection Vulnerability Analyzer for Web Application Programs", KIPS Transactions:PartA, Volume 15A Issue 3, 2008, Page 187

사이버 전투 피해평가를 위한 긴급 CAS 임무 자산 스코어링 연구

김재근, 김성중, 김국진, 이동환, 신동일, 신동규
세종대학교 컴퓨터공학과

{jaekeun0310, tjdwnd2004, kjkim, dhwlee}@sju.ac.kr, {dshin, shindk}@sejong.ac.kr

Research on Emergency CAS Mission asset scoring for cyber battle damage assesment

Jaekun Kim, Seongjung Kim, Kookjin Kim, Donghwan Lee,
Dongil Shin, Dongkyoo Shin
Dept. of Computer Engineering, Sejong University

요 약

사이버 공격은 조직과 국가에 큰 피해를 주려는 목적으로 정보를 가로채고 파괴하는 의도적인 행동으로 빚어지는 경우가 많다. 이에 따라 국제 표준화 기구(ISO)는 ISO/IEC 27000 시리즈 등 정보 자산의 보호를 위한 표준 문서를 지침으로 제공한다. 하지만 지침만 제공할 뿐 자산 보호를 위한 구체적인 방법이나 절차가 포함되어 있지 않다. 본 연구에서는 공군의 긴급 CAS(Close Air Support) 작전을 대상으로 추후 사이버 전투 피해평가를 위해 사이버 공격에 의한 정보 자산에 대한 점수를 가산화 한다. 긴급 CAS 작전 시뮬레이션 진행 후 도출된 요소를 가지고 객관적인 수치라고 할 수 있는 CIA(Confidentiality, Integrity, Availability)지표들과 군 정보를 접목시켜 자산의 중요성을 계산하고 나아가 가중치를 주어 차별성을 가지게 된다.

1. 서론

오늘날의 정보 통신 기술 분야의 발전 추세로 볼 때 미래에는 사이버 전쟁 양상으로 나아 갈 것이 필연적이라 판단된다 [1]. 사이버 전쟁 양상으로 나아감으로써 사이버 공격 위협이 국내외를 불문하고 점점 지능적이고 고도화되고 있다. DDoS 공격이나 악성코드, 랜섬웨어, APT공격 등에 의해 네트워크, 시스템 피해를 받게 되는 경우 조직 및 국가가 정상적으로 운영이 어려울 정도로 마비가 되거나 국가 및 군 기밀자료 등이 빠져나갈 수 있다. 2017년 사이버 공격으로 인해 국내의 경제적 손실액이 약 77조 원으로 막대한 피해가 있었지만, 기업의 임원들 중 17%가 사이버 보안 투자를 비즈니스적 차별화 요소로만 생각한다 [2].

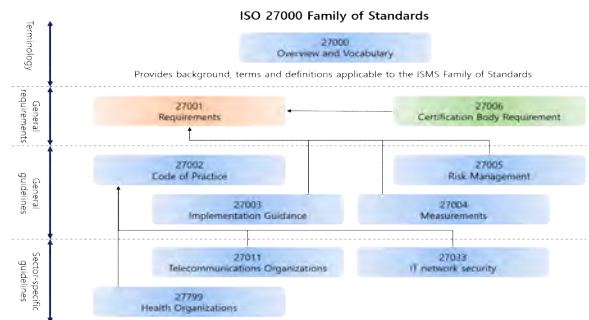
국제 표준화 기구인 ISO/IEC에서 자산을 보호하기 위한 가이드라인 문서들을 내놓았다 [3]. 하지만 ISO/IEC의 경우 지침만 제공하고 구체적인 자산 보호를 위한 방안을 제시하지는 않았다. 국내의 경우 ISO/IEC에서 내놓은 가이드라인을 가지고 다양한 연구가 이루어 지지만 정량적인 평가가 이루어질 수 없다는 문제를 가지고 있다 [4].

본 논문에서는 공군의 근접 항공 지원 작전 중 긴급 CAS 작전에 대한 시뮬레이션이 끝난 후 피해평가를 하기 위해 작전에서 사용되는 문서 및 자산 요소들을 가지고 점수를 책정하고 가 산화한다. 객관적인 수치인 CIA지표와 각 자산들을 군에 맞게 가중치를 줌으로써 차별성을 준다.

2. 관련 연구

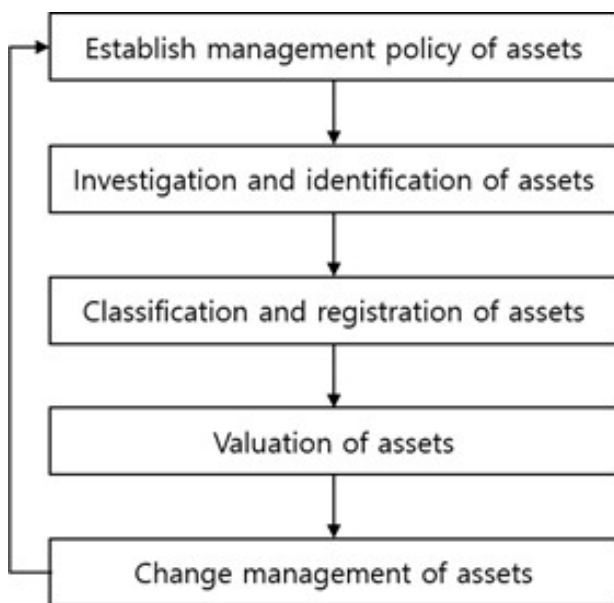
2.1. ISO/IEC 27000 시리즈

ISO/IEC 27000 시리즈는 ISO/IEC 정보보안 관리 시스템(ISMS) 표준 계열의 일부이다. ISO/IEC 27000 표준에는 ISMS를 수립과 인증에 관련된 여러 가지 약속 그리고 용어들이 정의되어있다.



(그림 1) ISO/IEC 27000 표준 시리즈 상호 관계도[5]

ISO/IEC 27001 표준은 ISMS를 수립, 구현, 운영, 모니터링, 검토, 유지 그리고 개선하기 위한 요구사항들이 명시돼 있다 [5]. ISO/IEC 27002 표준은 27001 표준을 기반하고 있다. 27002 표준은 ISMS를 구현하는 과정에서 통제를 선택하거나 일반적으로 수용되는 정보보안 통제를 구현하는 조직을 위한 지침 문서로 사용될 수 있도록 고안되었다 [6]. 또한 ISO/IEC 27000 시리즈 중 ISO/IEC 27002 표준은 ISMS의 구현을 위한 지침 문서이기 때문에 여러 자산관리 방안에 관한 연구나 논문들에서 원용하는 경향이 있다. 하단의 그림2는 27002에 정의된 자산관리 절차이다.



(그림 2) ISO/IEC 27002에 정의된 자산관리 절차[6]

ISO/IEC 27002 이외에도 ISO/IEC 27003은 구체적인 구현 권고사항 규정, ISO/IEC 27004는 개선하는 방안, ISO/IEC 27005는 위험 관리 과정을 6개의 프로세스로 구분, ISO/IEC 27006은 ISMS 인증기관 및 심사인의 자격요건, ISO/IEC 27011은 통신분야의 특화된 ISM 적용 실무지침, ISO/IEC 27033은 네트워크 시스템의 보안 관리와 운영에 대한 실무지침이다 [7].

2.2. CAS

근접항공지원(CAS : Close Air Support, 이하 CAS) 작전은 공대지 작전 중 하나로, 아군과 근접하게 대치 중인 적을 항공기로 공격하는 작전이다. 이는 지상/해상 군의 유리한 작전 여건을 조성하거나, 작전을 지원하여 군사 목표 달성에 핵심적인 임

무를 수행하는 작전으로 정의한다 [8].



(그림 3) 긴급 CAS 운용 절차

그림 3은 한국에서 운용중인 긴급 CAS 운용 절차의 간략한 도식이다 [9, 10]. 적과 대치하고 있는 대대 혹은 연대 지휘관의 CAS 요청이 발생하면 항공지원 작전본부(ASOC: Air Support Operation Center)에서 요청을 종합하여 사용 가능한 CAS 자산을 각 부대에 분배한다. 그 후 명령을 지시받은 항공기가 목표를 공격하는 흐름으로 작전이 진행된다. 긴급 CAS는 요청 시간과 공격 시간 사이는 2~5분으로 틈이 짧아 빠른 의사결정이 요구된다. 이를 위하여 지휘관 결심에 근거할 지표 분석이 신뢰도를 가져야 하며 분석에 대한 명령체계의 신속한 전산처리 역시 동반되어야 한다.

3. 긴급 CAS 임무 자산 스코어링 방안

본 논문의 연구는 긴급 CAS 작전 시뮬레이션을 진행한 후 피해평가를 하기 전 임무에 관련된 자산 요소들의 중요도를 가 산화 하는 것이다. 긴급 CAS 작전을 시뮬레이션 중 자산으로 뽑은 것 중 문서는 첩보 보고서, 대대 or 연대 지휘관의 CAS 요청서, TACP의 CAS 요청서, ASOC의 CAS 승인서, ASOC의 MSN Info이다. 그중 대대 지휘관의 긴급 CAS 요청서를 가지고 기밀성, 무결성, 가용성 지표와 가중치를 통하여 자산의 중요도를 가 산화 한다. 대대 지휘관의 긴급 CAS 요청서 안 요소는 적 병력(규모), 적 전투력 수준(보병, 탱크), 적 표적 위치, 아군 소속 및 관등성명, 첩보한 위치, 긴급 CAS 작전 실시 여부, 항공기의 생존도이며 총 8개의 요소가 포함된다 [11].

가중치 지표의 경우 ISO/IEC 27002 표준을 토대로 군 정보와 접목시켜 산출하였다. 대대 지휘관의 긴급 CAS 요청서로 산출된 기밀성, 무결성, 가용성 가중치 가 산화 지표 예시는 다음과 같다.

<표 1> 기밀성 지표

기밀성 지표	1	2	3	4	5	점수	가중치
<기밀성 지표>							
정보의 노출 방지 필요 수준					✓	5	상
정보의 열람 수준이나 열람 대상을 제한할 필요성			✓			3	상
정보의 내·외부 노출 시 예상할 수 있는 악용범위				✓		4	상
정보의 무단 노출 시 피해 발생 가능성				✓		4	상
정보를 열람한 사실을 확인하는 감사기록의 필요성		✓				2	상
정보의 비인가 노출이 군 업무수행에 미치는 영향					✓	5	상
정보와 군의 인사정보에 대한 관련성			✓			3	상
정보의 무단 노출 시 군의 재정에 미치는 영향	✓					1	상
정보와 군이 국민에게 제공하는 서비스에 대한 관련성	✓					1	상
정보와 시스템 개발에 대한 관련성		✓				2	상
<공동 지표>							
정보와 진행 중인 연구 및 개발 프로젝트에 대한 관련성		✓				2	하
정보와 군의 재정에 대한 관련성			✓			3	하
정보와 재난 감시 및 예측에 대한 관련성					✓	5	하
정보와 에너지에 대한 관련성		✓				2	하
정보와 군 관계자의 개인 정보에 대한 관련성		✓				2	하

기밀성 분류 지표의 경우 표1에 제시한 바와 같이 기밀성 지표 10개, 공동지표 5개로 구성된다. 기밀성 지표의 가중치를 "상"으로 공동지표 5개의 경우 가중치는 "하"로 적용한다.

<표 2> 무결성 지표

무결성 지표	1	2	3	4	5	점수	가중치
<무결성 지표>							
정보의 수정·삭제를 감시하는 감사기록의 필요 수준					✓	5	상
정보가 무단으로 변조·삭제될 경우 악용범위					✓	5	상
정보의 무단 변조·삭제를 방지하기 위한 특정한 도구 및 방법의 필요 수준				✓		4	상
정보에 접근하기 위해 공인 인증서를 사용해야 할 필요성	✓					1	상
정보가 무단 변조·삭제될 경우 정상적인 업무 수행에 미치는 영향					✓	5	상
정보와 지적재산권·개인정보 등과의 관련성			✓			3	상
정보와 군의 비상계획과의 관련성				✓		4	상
정보와 안보 및 외교와의 관련성	✓					1	상
정보와 국가 주요 인프라 정보와의 관련성					✓	5	상
정보가 군 외부로 공개될 시 요구되는 신뢰도 수준			✓			3	상
<공동 지표>							
정보와 진행 중인 연구 및 개발 프로젝트에 대한 관련성		✓				2	하
정보와 군의 재정에 대한 관련성			✓			3	하
정보와 재난 감시 및 예측에 대한 관련성					✓	5	하
정보와 에너지에 대한 관련성		✓				2	하
정보와 군 관계자의 개인 정보에 대한 관련성		✓				2	하

무결성 분류 지표의 경우 표2에 제시한 바와 같이 무결성 지표 10개, 공동지표 5개로 구성된다. 무결성 지표의 가중치를 "상"으로 공동지표 5개의 경우 가중치는 "하"로 적용한다.

<표 3> 가용성 지표

가용성 지표	1	2	3	4	5	점수	가중치
<가용성 지표>							
정보의 상시 접근 및 사용이 보장될 필요성		✓				2	상
군의 고유 업무를 지속적으로 지원하기 위한 정보의 필요성				✓		4	상
정보에 접근하고 사용하는 범위					✓	5	상
정보의 사용·접근의 방해 시 예상 가능한 악용범위					✓	5	상
제해 및 공격의 발생 시 예상되는 정보의 복구 우선 순위				✓		4	상
정보의 사용·접근 방해 시 군의 정상적인 업무 수행에 미치는 영향				✓		4	상
정보의 사용·접근 방해 시 재정에 미치는 영향		✓				2	상
정보의 사용·접근 방해에 대비하여 정보에 대한 접근 방식을 이중화할 필요성					✓	5	상
정보의 백업 필요성	✓					1	상
정보의 재무 및 회계와의 관련성	✓					1	상
<공동 지표>							
정보와 진행 중인 연구 및 개발 프로젝트에 대한 관련성		✓				2	하
정보와 군의 재정에 대한 관련성			✓			3	하
정보와 재난 감시 및 예측에 대한 관련성					✓	5	하
정보와 에너지에 대한 관련성		✓				2	하
정보와 군 관계자의 개인 정보에 대한 관련성		✓				2	하

가용성 분류 지표의 경우 표3에 제시한 바와 같이 가용성 지표 10개, 공동지표 5개로 구성된다. 가용성 지표의 가중치를 "상"으로 공동지표 5개의 경우 가중치는 "하"로 적용한다.

기밀성, 무결성, 가용성 가중 점수는 각 지표별 척도와 가중치를 곱한 값의 항목 가중치를 나누어 산출한다. 표4의 임무 자산 중요도 점수의 경우 각 가중 점수를 더해서 지표 수 만큼 나누게 된다. 가중 점수와 임무 자산 중요도는 "상","중","하"로 구분하며 각각의 범위로는 "상"등급은 3.30~4.89, "중"등급은 1.70~3.29, "하"등급은 0~1.69로 규정한다.

가중치 공식은 다음과 같다.

$$\text{가중평점} = \frac{\sum(\text{지표척도} \times \text{가중치})}{\sum(\text{항목의가중치})}$$

"상"등급 정보 : $3.30 \leq \text{가중 평점} \leq 4.89$

"중"등급 정보 : $1.70 \leq \text{가중 평점} \leq 3.29$

"하"등급 정보 : $0 \leq \text{가중 평점} \leq 1.69$

가중치 공식을 적용한 결과는 다음과 같다.

<표 4> 대대 지휘관의 CAS 요청서 임무 자산 중요도

구 분	기밀성	무결성	가용성
평균 점수	2.93	3.33	3.13
가중 점수	2.96	3.44	3.20
등급	중	상	중
임무 자산 중요도	3.20(중)		

표 4의 결과를 보면 대대 지휘관의 CAS 요청서에 대한 임무 자산 중요도는 3.20으로 (중) 등급에 들어가게 된다. 이처럼 임무 자산 중요도 점수를 책정하고 등급화한다면 사이버 공격에 대한 자산 관련 피해평가는 수월해질 것이다. 다만 가중치가 있는 만큼 모든 지표 척도를 중요하다고 판단하게 되면 임무 자산 중요도가 상향될 가능성이 있다는 점은 보완해야 할 문제이다.

4. 결론

본 논문에서는 긴급 CAS 시나리오 중 대대 지휘관의 CAS 요청서를 ISO/IEC 27002 기반의 기밀성, 무결성, 가용성 임무 자산 가중치 지표를 산출하였다. 산출한 임무 자산 가중치 지표들을 이용하여 임무 자산 중요도 점수 산출하는 방법을 제시하였다.

기밀성, 무결성, 가용성 가중치 지표의 가중치 공식을 적용하여 영향도를 "상", "중", "하"로 등급화 하였으며, 최종적으로 문서가 가진 등급과 점수를 결정하게 된다.

이를 발전시켜 가중치 조정과 모든 지표 척도를 중요하다고 판단하게 되면 임무 자산 중요도 점수가 상향될 가능성이 있는 점을 보완할 예정이다. 추후가 산출한 임무 자산 중요도 점수를 가지고 사이버 공격 피해평가에 반영하여 사이버 공격 별 얼마나 임무 자산피해를 받는지 산출할 예정이다.

ACKNOWLEDGMENT

“본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다(UD190016ED).”

참고문헌

- [1]오제상, “미래 사이버전 능력 필요”, 국방과 기술, 272호, 52-57, 2001
- [2]Frost&Sullivan, Microsoft, “Understanding the Cybersecurity Threat Landscape in Asia Pacific: Securing the Modern Enterprise in a Digital World,”Frost&Sullivan and Microsoft Corp., Korea,

Jun. 2018.

- [3]Disterer, G. (2013) ISO/IEC 27000, 27001 and 27002 for Information Security Management. Journal of Information Security, 4, 92-100.
- [4]나관식, “정보 보호 관리 체계(ISMS)의 국제 표준과 국내 표준 비교”, 과학과 문화, 제 8권 27호, 23-36, 2011. 2
- [5]Information technology-Security techniques-Information security management systems-Requirements, ISO/IEC 27001, 2013.
- [6]Information technology-Security techniques-Code of practice for information security controls, ISO/IEC 27002, 2015.
- [7]윤현수. “사이버 정보 자산의 분류 및 정량적 중요도 산출에 최적화된 지표 설계”, 세종대학교 석사학위논문(2019)
- [8]Joint Chiefs of staff. Close Air Support., Joint Publication 3-09.3, Jul. 2009
- [9]공군본부, 공군 기본교리, 2007.
- [10]장용진; 이태공; 김영동. 긴급 근접항공지원작전 전력 분배 방법. 한국통신학회논문지, 39.11: 1050-1067, 2014.
- [11]장용진. “긴급 근접항공지원작전 전력 분배 모델”, 아주대학교 석사학위논문(2015)

8-bit AVR 프로세서 상의 Revised CHAM 어셈블리 최적 구현

권혁동*, 김현지**, 박재훈**, 심민주**, 서화정**†

*한성대학교 정보컴퓨터공학과

**한성대학교 IT융합공학부

korlethean@gmail.com, khj1594012@gmail.com, p9595jh@gmail.com,

minjoos9797@gmail.com, hwajeong84@gmail.com

The Optimal Assembly Implementation of Revised CHAM on 8-bit AVR Processor

Hyeok-Dong Kwon*, Hyun-Ji Kim**, Jae-Hoon Park**,

Min-Joo Sim**, Hwa-Jeong Seo**†

*Dept. of Information Computer Engineering, Hansung University

**Dept. of IT Convergence Engineering, Hansung University

요 약

경량 암호는 컴퓨팅 파워가 부족한 저사양 프로세서를 위해 개발되었다. CHAM은 국산 경량 암호 중 하나로, 세 가지의 규격을 제공하며 ARX 구조를 사용한 암호이다. CHAM 발표 이후, 라운드 수를 조절하여 성능을 향상시킨 Revised CHAM이 제안되었다. 기존 CHAM은 8-bit AVR 프로세서 상에서 최적 구현이 이루어졌지만, 최신 기술인 Revised CHAM은 해당 구현물이 존재하지 않는다. 따라서 8-bit AVR 프로세서를 대상으로 Revised CHAM-64/128을 최적 구현하여 최상의 성능으로 연산이 진행되도록 한다. 본 논문에서는 최적 구현에 사용한 기법들을 소개하며, 기존에 제안된 기법과 성능 비교를 통해 본 기법의 우수함을 서술한다.

<표 1> CHAM의 파라미터

	n	k	w	k/w	r
CHAM-64/128	64	128	16	8	80(88)
CHAM-128/128	128	128	32	4	80(112)
CHAM-128/256	128	256	32	8	96(120)

1. 서론

CHAM은 저사양 프로세서를 대상으로 개발된 국산 경량 암호로 ARX 연산을 사용한다. 이후 CHAM의 라운드 수를 변경한 Revised CHAM이 제안되었다. 본 논문에서는 Revised CHAM의 규격 중 하나인 64/128의 최적 구현을 시도한다. 대상 프로세서는 8-bit AVR 프로세서인 Atmega128 프로세서이다. 논문의 구성은 다음과 같다. 2장에서 CHAM에 관한 내용과 기존 최적화 구현물에 대해 확인하며 3장에서 제안 기법에 적용된 최적화 기법을 확인한다. 4장에서 기존 기법과의 성능비교를 진행하고 5장에서 결론을 맺는다.

2. 국산 경량 암호 CHAM

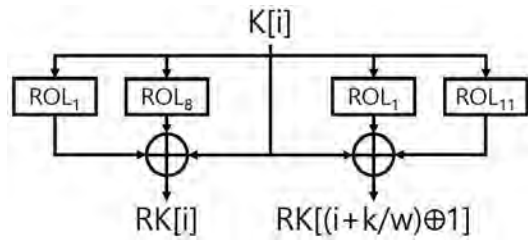
2.1 Revised CHAM[1][2]

Revised CHAM의 원형인 CHAM은 ICISC'17에서 발표된 경량 암호이다. CHAM은 Addition, Rotation, eXclusive-or의 세 가지 연산을 사용한다. CHAM에서 사용하는 파라미터는 표 1로 명시한다.

이후 ICISC'19에서 CHAM의 개량형인 Revised CHAM이 발표되었다. Revised CHAM은 CHAM과 동일한 구조 및 규격을 지니지만, 라운드 수만 다르다. 표 1의 괄호 부분이 Revised CHAM의 파라미터이다.

Revised CHAM은 키 상태를 저장하지 않는 스테이트리스 기법을 사용하며, 그림 1과 같은 키 스케줄링을 통해 라운드 키를 생성한다. Pseudo 코드 형태로 표현하면 다음과 같다.

```
for (i = 0; i < k/w; i++) {
    RK[i] ← K[i] ⊕ (K[i] ≪ 1) ⊕ (K[i] ≪ 8)
    RK[(i + k/w) ⊕ 1] ← K[i] ⊕ (K[i] ≪ 1) ⊕ (K[i] ≪ 11)
}
```



(그림 1) Revised CHAM의 키 스케줄링

이후 평문을 4개의 블록으로 나눈 후, 라운드 함수를 반복하여 암호화를 진행한다. 라운드 함수의 구조는 전체적으로 동일하지만 짝수, 홀수 라운드 별로 회전 연산의 횟수만 다르다. 라운드 함수는 그림 2와 같으며 Pseudo 코드로 표현하면 다음과 같다.

```
for (i = 0; i < r; i++) {
    (xi+1, yi+1, zi+1, wi+1) ← (yi, zi, wi, \
    (((xi ⊕ i) + ((yi ≪ αi) ⊕ RKi mod 2k/w)) mod 2w ≪ βi))
}
```

코드에서 α, β는 i값에 따라 달라진다. 만약 i가 짝수라면 α = 1, β = 8이며 반대로 홀수라면 α = 8, β = 1이 대입된다.

2.2 기존 제안 기법

[3]은 CHAM을 8-bit AVR 프로세서 상에서 최적 구현하였다. [3]에 적용된 기법은 다음과 같다.

첫째로 라운드 키 접근이다. CHAM-64/128의 라운드 키는 32바이트이다. 즉, 메모리에 대한 최대 범위는 32이므로, 레지스터 하나로 모든 메모리 접근이 가능하다. 이를 구현하기 위해서는 상위 주소를 고정된 채, 하위 주소에 0x00값을 설정한다. 따라서 1바이트 오프셋 연산으로 메모리 접근이 가능하다.

둘째는 카운터 최적화이다. CHAM은 라운드 카운터와 XOR하는 부분이 있다. 64-128 규격은 80라운드를 거치는데, 레지스터 하나의 표현 범위가 256이므로 레지스터 하나로 카운터 관리가 가능하다.

마지막은 메모리 접근 최적화이다. 후 증가 명령어를 활용하여 메모리 접근 이후, 다음에 연산할 메

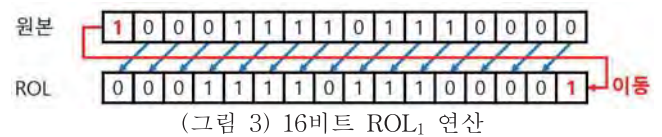
모리 주소로 자동으로 이동하도록 한다.

3. 제안 기법

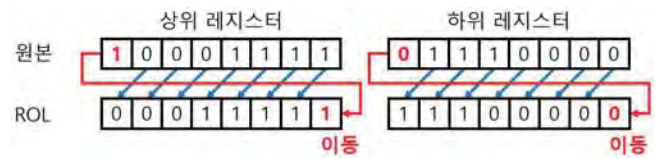
[3]은 CHAM에 대한 최적 구현이므로 Revised CHAM-64/128에 대한 최적 구현을 한다. 본 장에서는 [3]의 기법을 포함한 채로, 추가적으로 적용한 기법을 서술한다.

3.1 회전 연산 최적화

Revised CHAM-64/128의 블록 크기는 16비트이며, 회전 연산을 취한 결과는 그림 3과 같다.

(그림 3) 16비트 ROL₁ 연산

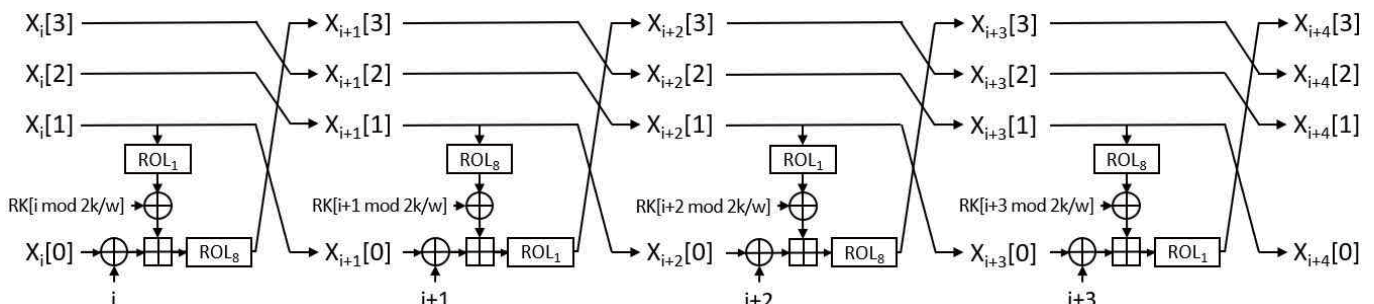
하지만 대상 프로세서는 8비트 레지스터를 사용하므로 블록 하나를 두 개의 레지스터에 나누어 저장한다. 때문에 단순히 회전 연산을 적용하면 그림 4와 같이 의도하지 않은 결과가 도출된다.

(그림 4) 8비트 레지스터 상의 16비트 ROL₁ 연산

정상적인 회전 연산을 위해서는 ROL 외에 추가적인 명령어가 필요하다. 최소한으로 구현하기 위해서 표 2 좌측의 명령어 모음을 사용한다.

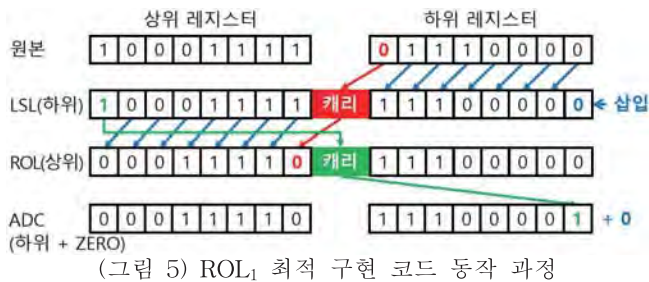
<표 2> 회전 연산 최적화 코드

ROL ₁		ROL ₈	
LSL	LO	MOV	TEMP, LO
ROL	HI	MOV	LO, HI
ADC	LO, ZERO	MOV	HI, TEMP

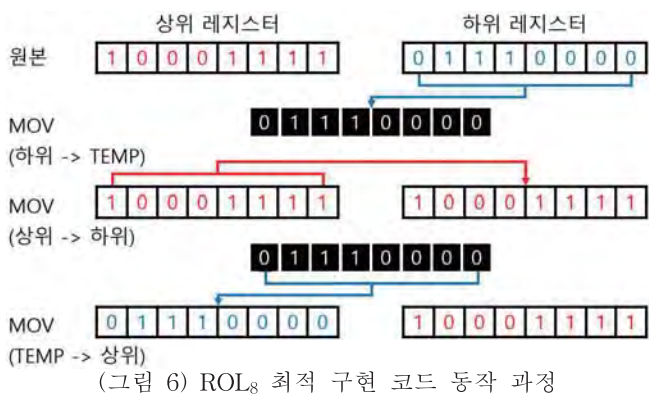


(그림 2) CHAM의 라운드 함수

가장 먼저, 하위에 LSL 명령어를 사용하여 모든 비트를 좌측으로 1비트씩 옮긴다. 이때 좌측 끝 비트는 캐리에 저장된다. ROL 명령어는 상위에 사용하며, 캐리에 있는 하위의 좌측 끝 비트를 상위의 우측 끝 비트에 저장한다. ROL 명령어로 인해 상위의 좌측 끝 비트는 캐리에 저장된 채로 종료된다. 마지막으로 ADC 명령어로 하위와 제로 레지스터를 더해준다. ADC 명령어는 캐리를 최하위 비트에 더해줄 수 있기 때문에 캐리에 저장된 상위의 좌측 끝 값을 하위의 우측 끝에 저장하여 회전 연산을 3사이클로 완성한다. 이 과정은 그림 5와 같다.



Revised CHAM에는 8회전 연산도 존재한다. 블록 하나는 16비트이며 이를 8회전 한다면, 중앙을 기준으로 앞뒤의 값이 반전된다. 대상 레지스터는 8비트 레지스터를 사용하므로 본 특징을 활용 가능하다. 구현에는 표 2 우측의 코드를 사용한다. 레지스터 값을 교차하여 8회전 연산을 구현한다면 3사이클이 소요되며 동작은 그림 6과 같다. 추가로 본 연산을 두 번 연속 연산할 경우, 초깃값으로 복구된다.



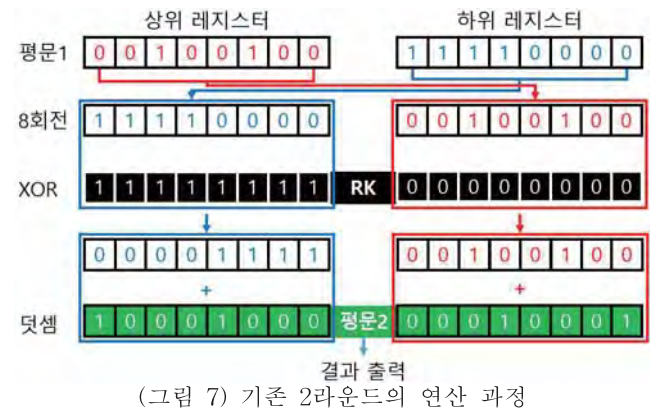
3.2 회전 연산 횟수 최적화

그림 2에서 $X_i[0]$ 의 1라운드, 그리고 $X_i[2]$ 의 2라운드에서 8회전 연산을 제거할 수 있다. 우선 $X_i[0]$ 의 경우 1라운드의 마지막에서 8회전 연산을 거친다. 하지만 4라운드에서 $X_i[0]$ 가 입력 값으로 사용

될 때, 다시 8회전 연산을 거친다. 3.1절에서 서술하였듯, 8비트 레지스터 상에서 8회전 연산을 두 번 거치면 값이 원상으로 돌아온다.

따라서 1라운드의 8회전 연산을 생략한다면 4라운드에서도 생략 가능하다[4]. 다만 $X_i[0]$ 에는 8회전된 값이 있어야 이후 연산 결과가 정상적이므로 4라운드 종료 직전에 $X_i[0]$ 에 8회전 연산을 취해준다.

$X_i[2]$ 의 일반적인 연산 과정은 그림 7과 같다.



하지만 $X_i[2]$ 는 XOR와 덧셈 연산 시에, 표 3의 코드와 같이 레지스터를 교차해서 연산하는 것으로 자체적으로 8회전 연산을 포함시킬 수 있다. 동작을 묘사한다면 그림 8과 같이 표현 가능하다. 그림 8의 동일 색상의 음영끼리 연산을 수행한다.

<표 3> 레지스터 교차 연산 코드

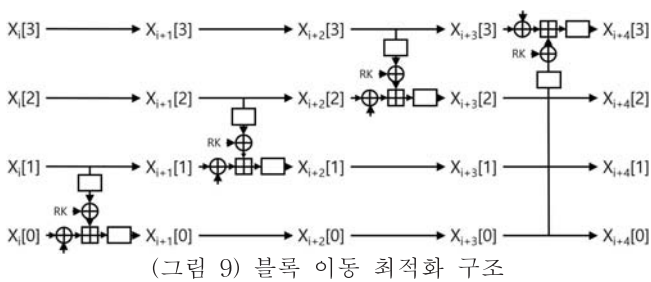
Register reverse method	
LPM	RK, Z+ // RK 하위 8비트
EOR	HI2, RK
LPM	RK, Z+ // RK 상위 8비트
EOR	LO2, RK
ADD	LO1, HI2
ADC	HI1, LO2



이것으로 Revised CHAM-64/128의 전체 88라운드 중 44회의 8회전 연산이 생략되며, 132사이클을 줄일 수 있다.

3.3 블록 이동 최적화[5]

Revised CHAM-64/128은 평문을 4개의 블록으로 나누고 라운드의 종료 직전 모든 블록은 좌측방향으로 이동한다. 이때 각 블록은 4라운드 이후 제자리로 돌아오는 것을 알 수 있다. Revised CHAM-64/128은 4의 배수인 88라운드로 동작한다. 때문에 1라운드 시작 시의 블록 위치와 88라운드 종료 시의 블록 위치는 동일하다. 즉, 블록 위치를 이동하지 않더라도 최종 출력은 동일하다. 이것으로 라운드 함수 구조를 그림 9의 형태로 변형할 수 있다. 블록 이동을 생략하면 라운드별 5개의 MOVW 명령어가 생략되며, 동작 사이클 관점에서는 880사이클이 감소된다.



4. 성능 평가

본 장에서는 구현물의 성능 비교를 한다. 구현에는 Atmega128 프로세서를 사용한다.

8-bit AVR 프로세서에 대한 CHAM 최적 구현은 [3]이 존재하나, 해당 구현물은 Revised CHAM에는 대응하지 않는다. 그러므로 본 논문의 구현물과 비교하기 위해 해당 구현물을 Revised CHAM 버전으로 이식하여 비교한다. 결과는 표 4와 같다.

<표 4> 성능 평가 결과

구현물	ROM	RAM	cpb
[3] + Revised	152	3	232
This Work	198	3	209

제안기법이 [3]에 비해 다소 큰 코드 사이즈를 가진다. 하지만 속도 면에서 [3]은 232cpb로 동작하는 반면, 제안하는 구현물은 209cpb로 동작한다. 이는 9.9%의 속도 향상에 해당된다.

5. 결론

본 논문에서는 Revised CHAM-64/128을 8-bit AVR 프로세서를 대상으로 최적 구현하였고, 기존 구현에 비해 9.9%의 속도 향상을 달성했다.

향후 과제로는 Revised CHAM의 남은 규격 두 가지에 대해서 최적 구현을 진행할 예정이다. 또한 본 구현물의 성능을 보다 더 개선할 수 있는 사항에 대해 확인해본다.

참고문헌

- [1] Bonwook Koo, Dongyoung Roh, Hyeonjin Kim, Younghoon Jung, Dong-Geon Lee, and Daesung Kwon, "CHAM: A Family of Lightweight Block Ciphers for Resource-Constrained Devices," *International Conference on Information Security and Cryptology*, Seoul, Korea, pp 3-25, 2017.
- [2] Dongyoung Roh, Bonwook Koo, Younghoon Jung, IlWoong Jeong, Dong-Geon Lee, Daesung Kwon, and Woo-Hwan Kim, "Revised Version of Block Cipher CHAM," *International Conference on Information Security and Cryptology*, Seoul, Korea, pp 1-19, 2019.
- [3] Hwajeong Seo, "Memory-Efficient Implementation of Ultra-Lightweight Block Cipher Algorithm CHAM on Low-End 8-Bit AVR Processors," *Journal of the Korea Institute of Information Security & Cryptology*, Vol. 28, No. 3, pp 545-550, 2018.
- [4] Sujin Lee, Junyoung Kang, Dowon Hong, and Changho Seo, "Research for Speed Improvement Method of Lightweight Block Cipher CHAM using NEON SIMD," *Journal of KIISE*, Vol. 46, No. 5, pp 485-491, 2019.
- [5] Taeung Kim, and Deukjo Hong, "Software Implementation of Lightweight Block Cipher CHAM for Fast Encryption," *Journal of the Korea Society of Computer and Information*, Vol. 23, No. 10, pp 111-117, 2018.
- [6] Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers, "The SIMON and SPECK Block Ciphers on AVR 8-bit Microcontrollers," *International Workshop on Lightweight Cryptography for Security and Privacy*, Istanbul, Turkey, pp 3-20, 2014.

코사인 유사도 측정을 통한 행위 기반 인증 연구

길선웅

인천대학교 정보통신공학과

swgil009@inu.ac.kr

Behavior-based Authentication Study By Measuring Cosine Similarity

Seon-Woong Gil

Dept. of Information and Communication Engineering,

Incheon National University

요 약

사용자 행위 기반 인증 기술은 다른 인증 기술들에 비해서 인증의 인식률을 높이는데 많은 데이터의 장기간 추출이 필요하다. 본 논문은 터치 센서와 자이로스코프를 이용하여 그동안의 행위 기반 인증 연구에서 사용되었던 행위 특징 데이터들 중에서 핵심적인 최소한의 데이터들만을 사용하였다. 측정된 데이터들의 검증에는 그간 사용자 행위 기반 인증 연구에서 이용되지 않고 문서 검색의 유사도 측정에 사용되었던 코사인 유사도를 사용하였다. 이를 통해 최소한의 특징 데이터와 기준이 되는 데이터의 코사인 유사도 비교 검증만을 통해서도 인증 범위에 적용되는 임계값을 조절하는 방식을 통해서 최초 EER 37.637%에서 최종 EER 1.897%의 높은 검증 성능을 증명하는데 성공하였다.

1. 서론

행위 기반 인증 기술은 다른 인증 기술들에 비해서 인증에 필요한 사용자의 행동을 추출하는데 많은 데이터가 필요하고 인식률마저 부족하다는 문제점이 존재한다. 본 논문에서는 행위 기반 인증의 정확도 향상을 위해서 인증 기반으로 설정하는 사용자 행위 패턴 데이터를 다량으로 수집 하는 기존의 연구들을 분석하여 인증에 필요한 핵심적인 데이터를 선정해 최소한의 데이터 수집으로 기존에 행위 기반 인증에 사용되지 않던 코사인 유사도 측정 방법을 통해서 최대한의 사용자 인증 정확도를 얻을 수 있는 방법에 대해 연구하였다.

본 논문은 2장에서는 기존의 연구들을 분석하여 인증에 사용할 핵심적인 사용자 특징 데이터를 선정한다. 3장에서는 코사인 유사도를 이용한 사용자 행위 기반 인증 기술을 설계한다. 4장에서는 설계한 사용자 행위 기반 인증 기술을 실험하고 이를 분석한다. 마지막으로 5장에서 결론을 맺는다.

2. 기존 행위 기반 인증 기술들의 특징 데이터

행위 기반 인증 기술에 대한 다양한 연구가 진행

되고 있는 가운데 최근 2013년도부터의 가시적인 결과를 보여준 연구결과를 정리해보면 아래 <표1>과 같다.

<표 1> 행위 기반 인증 기술 연구 동향

저자	특징 데이터	알고리즘	정확도(%)
Meng et al. (2013)	싱글 터치, 터치 이동, 멀티 터치 상황에서 터치 타입, 좌표, 시간, 방향, 행동 횟수	Neural Network	EER : 2.92
Xu et al. (2014)	키스트로크(크기, 시간, 압력), 슬라이드(위치, 크기, 압력, 속도, 길이), 서명(크기, 압력, 위치, 방향, 속도, 여백), 펀치(위치, 크기, 압력, 속도, 길이, 방향)	SVM	EER : 10
Meng et al. (2014)	터치 이동 수, 싱글 터치 수, 멀티 터치 수, 터치 이동 시간, 싱글 터치 시간, 멀티 터치 시간, 터치 이동속도, 터치 압력	Neural Network	EER : 2.46
Shen et al. (2015)	슬라이드(상하좌우 각 방향별 위치, 길이, 각도, 시간, 속도, 가속도, 압력)	One-class SVM	FAR : 0.03 FRR : 0.05
Sitova et al. (2016)	탭(시간, 크기, 속도), 키스트로크(누른 시간, 입력 간 시간), 쥐는 형태 (가속계, 중력계, 자력계)	one-class SVM	EER : 7.16(이동) EER : 10.05(정지)

각 연구의 특징 데이터와 사용한 알고리즘, 정확도를 보여준다. 지금까지 살펴본 행위 기반 인증 기술 연구들의 대부분이 터치와 각종 센서를 이용하여 사용자의 특징 데이터를 추출 하고 있다.[1][6]

본 논문에서는 기존 연구들에서 사용한 데이터들 중 핵심적인 특징 데이터로 터치 센서를 이용하여 터치 좌표와 시간, 모션 센서인 자이로스코프를 이용하여 스마트폰의 회전벡터를 사용한다.

3. 행위 기반 인증 기법 설계

본 논문에서는 안드로이드 스마트폰의 터치, 모션 센서로 추출한 사용자의 스크린 터치시의 좌표, 시간, 회전벡터를 검증에 사용하기 위해 코사인 유사도 값으로 가공한다.

코사인 유사도란 다차원의 양수 공간에서의 유사도 측정에 이용되며 벡터의 크기 값은 결과에 영향을 미치지 않고 차원의 개수가 많은 다차원의 벡터일수록 유사도를 뚜렷이 구분할 수 있는 장점이 있다. 그런 특징 때문에 벡터의 원소나 비교 벡터의 원소와의 크기 값이 차이가 많이 나는 경우에도 다른 가공 없이도 유사도를 비교할 수 있다. 또한 두 벡터의 내적과 외적을 통해서 아래 (그림 1)과 같이 간단한 공식만으로도 연산이 가능하다는 장점이 있다.[7]

$$\text{similarity} = \cos(\theta) = \frac{\mathbf{A} \cdot \mathbf{B}}{\|\mathbf{A}\| \|\mathbf{B}\|} = \frac{\sum_{i=1}^n A_i B_i}{\sqrt{\sum_{i=1}^n A_i^2} \sqrt{\sum_{i=1}^n B_i^2}},$$

(그림 1) 코사인 유사도 공식

본 논문에서 제안하는 인증 기법은 사용자가 다섯 번의 터치를 시도 할 때 본인만의 리듬으로 화면 좌표를 터치하고 스마트폰을 기울이며 측정을 마친다. 이렇게 한 차례의 측정을 마친 사용자에게 다섯 차례의 측정을 요구한다. 한 차례의 측정을 마친 사용자의 데이터는 아래 <표 2>과 같이 터치 X좌표, Y좌표, 측정 때의 스마트폰의 회전벡터 값 X, Y, Z, 터치시의 시간으로 한 차례의 측정 때마다 30개의 데이터가 측정된다.

<표 2> 한 차례의 측정 때 수집되는 데이터

터치 X좌표	터치 Y좌표	회전벡터 X	회전벡터 Y	회전벡터 Z	시간
touch X.1	touch Y.1	round X.1	round Y.1	round Z.1	T1

touch X.2	touch Y.2	round X.2	round Y.2	round Z.2	T2
touch X.3	touch Y.3	round X.3	round Y.3	round Z.3	T3
touch X.4	touch Y.4	round X.4	round Y.4	round Z.4	T4
touch X.5	touch Y.5	round X.5	round Y.5	round Z.5	T5

이 30개의 데이터에서 각 터치 사이를 구간으로 두면 총 4개의 구간이 생기게 된다. 각 구간 사이의 값은 터치 X좌표, Y좌표, 측정 때의 스마트폰의 회전벡터 X, Y, Z, 터치시의 시간 값으로 사용자가 측정을 할 때의 특징 데이터 값이다. 아래 <표 3>과 같이 다음 터치 횟수의 데이터 값에 현재 터치 횟수의 데이터 값을 차감하여 다음 터치로 이동 할 때의 각 데이터 항목의 변화량을 이용한다.

<표 3> 네 가지 구간별 사용자 행위 특징 데이터

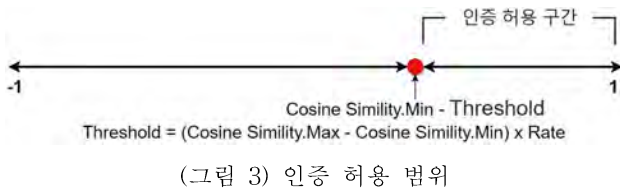
터치 X좌표	터치 Y좌표	회전벡터 X	회전벡터 Y	회전벡터 Z	시간
touch X.2 - touch X.1	touch Y.2 - touch Y.1	round X.2 - round X.1	round Y.2 - round Y.1	round Z.2 - round Z.1	T2 - T1
touch X.3 - touch X.2	touch Y.3 - touch Y.2	round X.3 - round X.2	round Y.3 - round Y.2	round Z.3 - round Z.2	T3 - T2
touch X.4 - touch X.3	touch Y.4 - touch Y.3	round X.4 - round X.3	round Y.4 - round Y.3	round Z.4 - round Z.3	T4 - T3
touch X.5 - touch X.4	touch Y.5 - touch Y.4	round X.5 - round X.4	round Y.5 - round Y.4	round Z.5 - round Z.4	T5 - T4

이렇게 구한 각 구간별 특징 데이터 값의 1회부터 5회까지 측정에서의 평균값을 구하고 이 평균값과 각 측정시도의 구간 값을 (그림 1)에서 보았던 코사인 유사도 공식에 사용되는 벡터로 사용하면 사용자의 검증을 위한 코사인 유사도 값을 구할 수 있다. 총 5차례의 측정이 있었으므로 각 구간 당 5개의 코사인 유사도 값 총 20개의 코사인 유사도 값이 생성된다. 아래 (그림 2)는 실제 실험자들의 각 구간별 최소 코사인 유사도 값을 보여준다.

name	valid1min	valid2min	valid3min	valid4min
1 a	0.997980015039642	0.994509343848845	0.992790538067006	0.989612523883865
2 b	0.988631548602581	0.986413805561361	0.995784860427118	0.993264592615508
3 c	0.985034300848266	0.981012263583957	0.990947984281981	0.979339312302176
4 d	0.996949306283853	0.994489861082515	0.998624731776395	0.996652134175104

(그림 2) 사용자의 각 구간별 최소 코사인 유사도 값

다섯 차례의 사용자 측정을 통해 구한 최소 코사인 유사도 값을 그대로 범위로 사용하면 FRR(False Rejection Rate)의 비율이 너무 높아져 버릴 것이기 때문에 최소 코사인 유사도 값에 특정한 임계값을 차감하는 형태로 아래 (그림 3)과 같이 인증 허용 범위를 늘리거나 줄여야 한다.

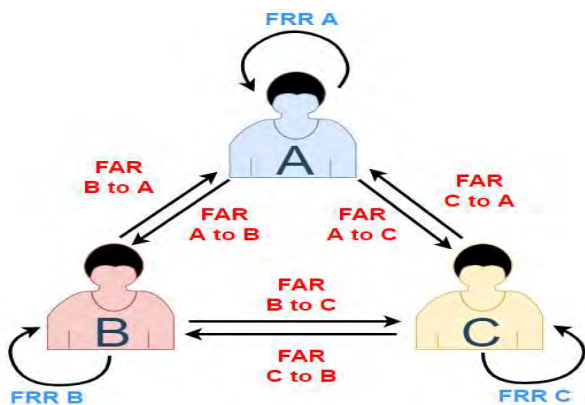


이때 차감할 임계값(Threshold)에 사용하는 값을 각 구간별로 구한 최대 코사인 유사도 값(Cosine Similitiy.Max)에서 최소 코사인 유사도 값(Cosine Similitiy.Min)을 빼준 값에 특정 임계 상수(Rate)를 곱한 값을 사용한다.

이러한 방법으로 최소 코사인 허용 범위를 설정하는 이유는 각 구간별로 최소, 최대 코사인 유사도 값이 다르기 때문에 FRR 비율이 높게 나올 수 있는 특정 구간에서는 최소, 최대 코사인 유사도 값의 차이가 크다. 이 때문에 사용자마다 각 구간별로 유연한 허용 범위 설정이 측정과 동시에 가능하기 때문이다.

4. 실험 및 분석

본 실험에서 사용할 데이터 셋을 모으기 위해서 실험자 세 명이 실험에 참여하였다.



실험자들은 위 (그림 4)처럼 스마트폰 화면이 서로에게 보이지 않도록 삼각형 모양으로 마주보며 앉아 실험자 A부터 FRR 데이터 셋을 수집하기 위해 곧 바로 50회 가량의 본인에 대한 행위

기반 인증을 실시하였고, 이때 나머지 실험자 B와 C는 그 행위를 지켜보며 실험자 A의 인증 행동을 관찰하도록 하였다.

실험자 A의 FRR 측정이 끝난 후에는 실험자 A에 대한 FAR(False Acceptance Rate) 데이터 셋 수집을 위하여 실험자 A의 행동을 관찰하던 실험자 B와 C가 곧바로 실험자 A에 대한 침입자의 행위 기반 인증을 각각 25회 가량 진행하여 이전에 실험자 A의 인증 행동을 계속해서 따라 해보는 방식으로 실험하였다. 이렇게 실험자 A에 대한 FRR, FAR 데이터 셋을 수집한 후에는 실험자 B와 C 순서대로 같은 방식의 실험을 진행하였다.

이와 같이 실험한 결과 실험자 A와 B, C는 FRR에 대한 데이터 수집을 각각 53회, 57회, 72회 총 182회 진행하였고 이를 바탕으로 데이터 수집 1회당 1구간부터 4구간까지의 인증에 시도한 코사인 유사도 값 4개의 데이터가 수집되어 총 728개의 데이터 셋을 모을 수 있었다. 실험자 A와 B, C의 FAR에 대한 데이터 수집은 각 53회, 71회, 67회의 총 191회의 시도를 통해 총 764개의 데이터 셋이 모였다.

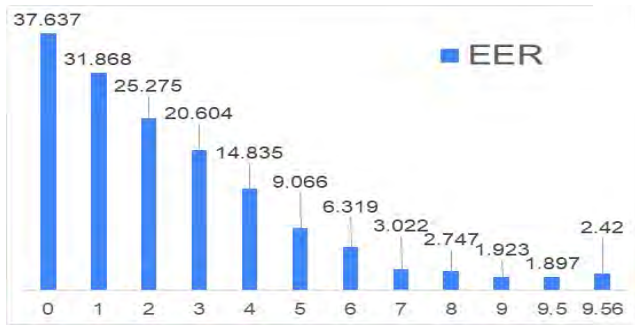
실험자 A와 B, C가 진행한 FRR, FAR 실험에서 측정한 인증 시도시의 각 네 가지 구간별 코사인 유사도 값 데이터 셋이 아래 (그림 5)와 같이 728개, 764개 총 1,492개의 데이터 셋이 모였다.

	_id	name	mnum	rate	tester
	필터	필터	필터	필터	필터
1487	1487	c	3	9.0	-0.00816233046606713
1488	1488	c	4	9.0	0.166972501599505
1489	1489	c	1	9.0	0.979234207482881
1490	1490	c	2	9.0	0.999786227953024
1491	1491	c	3	9.0	0.706970177023108
1492	1492	c	4	9.0	0.0736266626927253

(그림 5) 1,492개의 FAR, FRR 데이터 셋

이렇게 모인 데이터 셋을 가지고 사용자 행위 기반 인증을 허용하는 범위 조절에 사용하는 임계값(Threshold)의 임계 상수(Rate)값을 변화시키며 실험자 A와 B, C의 평균 EER을 구하여 임계 상수(Rate)에 따른 평균 EER을 서로 비교 분석하는 방법으로 실험을 분석하였다.

아래 (그림 6)은 임계 상수(Rate)의 변화에 따른 실험자 A와 B, C의 EER 값을 평균한 본 논문에서 제안하는 행위 인증 기법의 EER 수치이다. 본 실험 결과 최대, 최소 코사인 유사도 값의 차에 곱해지는 임계 상수(Rate) 값이 증가함에 따라 EER 수치가 점점 줄어드는 결과가 나타났다.



(그림 6) 임계 상수(RATE)에 따른 EER 그래프

최초 임계 상수(Rate)를 0으로 설정하여 임계값 없이 측정된 사용자 최소 코사인 유사도 값만으로 인증을 진행 할 시 평균 FRR은 75.275%, 평균 FAR은 0%로 평균 EER은 37.637%를 나타냈고, 최종적으로 임계 상수(Rate)가 9.5인 지점에서 평균 FRR은 2.747%, 평균 FAR은 1.047% 그리고 최종 EER은 1.897%로 가장 낮은 값을 나타내었다. 그 후에는 EER 수치가 증가하는 추세를 보였다.

본 실험에서 임계 상수(Rate) 값이 9.5 일 때 가장 성능이 좋은 인증이 되었던 이유는 실험자에 따라서 또 그 구간에 따라서 FAR, FRR 수치가 각기 다르며 코사인 유사도의 최대, 최소 값이 모두 다르기 때문에 이번 실험에 참여한 실험자 A와 B, C의 데이터 셋에서 각 구간 별 인증 범위를 가장 정확도 있게 설정할 수 있는 임계 상수(Rate)가 9.5였고 이 값은 유동적인 값이라고 분석한다. 즉 본 행위 기반 인증 기법의 EER수치를 변동시키는 임계 상수(Rate)값은 실험자의 수가 더 많아지거나 실험자가 인증 값을 생성할 때 5회 이상의 더 많은 측정 횟수를 시도하게 되거나 실험자의 제안 인증 기법의 숙련도에 따라 수치로 변동 할 수 있는 수치라고 분석한다.

5. 결론

본 논문을 통해서 안드로이드 스마트폰에 내재되어있는 터치 센서와 자이로스코프를 이용하여 최소한의 행위 특징 데이터들을 코사인 유사도 측정 비교 방식을 이용하여 행위 기반 인증을 설계 및 실험하였다. 사용자에게 다섯 차례의 측정을 요구하여 터치시의 X, Y좌표와 스마트폰 기울기에 해당하는 회전벡터 X, Y, Z와 터치 시간 값을 이용하여 총 6가지의 행위 특징 데이터를 수집하였고 다음 터치 측정으로 넘어가는 동안의 데이터들의 변화 값을 통해서 사용자를 특정 할 수 있는 데이터로 가공하였다. 측정 데이터의 유사도를 검증하기 위해서는 코

사인 유사도를 이용한 비교 방식을 선택하였고 많은 수의 수집 데이터나 오랜 시간의 실험 없이도 수집한 데이터와 기준이 되는 데이터의 코사인 유사도 비교만을 통해서도 적은 수의 실험자와 특정 데이터의 환경에서도 인증 범위에 적용되는 임계값을 조절하는 방식을 통해서 최초 EER 37.637%에서 최종 EER 1.897%의 높은 성능을 증명하는데 성공하였다. 향후에는 사용자의 측정 횟수의 제한을 없애고 사용자의 수가 늘어날 때마다 EER 수치가 가장 낮은 임계값을 시스템 스스로 설정하여 변경하는 방식으로 보완하여 본 논문에서 제안하는 사용자 행위 기반 인증 기법의 신뢰도를 검증해 나갈 것이다.

참고문헌

- [1] T. Feng, X. Zhao, B. Carbunar, and W. Shi, "Continuous mobile authentication using virtual key typing biometrics." 2th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. IEEE, 2013.
- [2] H. Xu, Y. Zhou, and M.R. Lyu, "Towards continuous and passive authentication via touch biometrics:An experimentalstudy on smartphones,," Symposium On Usable Privacy and Security (SOUPS 2014). 2014.
- [3] Y. Meng, and D.S. Wong, "Design of touch dynamics based user authentication with an adaptive mechanism on mobile phones,," Proceedings of the 29th Annual ACM Symposium on Applied Computing. ACM, 2014.
- [4] C. Shen, Y. Zhang, Z. Cai, T. Yu, and X. Guan, "Touch-interaction behavior for continuous user authentication on smartphones,," 2015 International Conference on Biometrics (ICB), IEEE, 2015.
- [5] Z. Sitová, J. Šeděnka, Q. Yang, G. Peng, and G. Zhou, "HMOG: NewBehavioral Biometric Features for Continuous Authentication of Smartphone Users." IEEE Transactions on Information Forensics and Security, Vol. 11, No. 5, pp. 877-892, 2016.
- [6] 김민우(2016), "안드로이드에서 앱 사용과 터치 정보를 이용한 행위 기반 사용자 인증 기술 연구", 석사학위 논문, pp.8 ~ 42
- [7] <https://www.ibric.org/myboard/cosinesimilarity>

독립된 데이터셋을 활용한 효율적인 딥러닝 기반 비프로파일링 부채널 분석 방안

김주환^{**}, 문혜원^{*}, 김연재^{*}, 박아인^{*}, 한동국^{*}, ^{***}

^{*}국민대학교 정보보안암호수학과

^{**}국민대학교 수학과

^{***}국민대학교 금융정보보안학과

zzzz2605@kookmin.ac.kr, qwerty25879@kookmin.ac.kr, duswo0024@kookmin.ac.kr,

applepai28@kookmin.ac.kr, christa@kookmin.ac.kr

Efficient Non-Profiled Deep Learning-based Side-Channel Analysis with Independent Dataset

Ju-Hwan Kim^{**}, Hye-Won Mun^{*}, Yeon-Jae Kim^{*}, A-In Park^{*}, Dong-Guk Han^{*}, ^{***}

^{*}Dept. of Information Security, Cryptology, and Mathematics, Kookmin University

^{**}Dept. of Mathematics, Kookmin University

^{***}Dept. of Financial Information Security, Kookmin University

요 약

비프로파일링 부채널 분석은 프로파일링 장비가 없는 환경에서 부채널 정보를 이용해 비밀정보를 분석하는 방법이다. 기존에 알려진 Timon의 비프로파일링 분석은 학습 데이터 집합만을 이용해 공격하므로 전력 파형의 수가 제한된다면 과적합이 발생하여 키 분석 성능이 떨어질 수 있다. 본 논문에서는 비프로파일링 환경에서의 딥러닝 기반 부채널 분석 성능을 향상시키기 위해 학습 데이터 집합과 독립적인 검증 데이터 집합을 활용해야 하는 실증적 근거를 제시한다. 이에 대한 실험으로 기존 기법과 제시한 기법의 성능을 비교해 봤을 때, 검증 데이터를 활용하면 더 적은 데이터로 비밀키 추출이 가능함을 보인다.

1. 서론

사물 인터넷 기술이 보편화됨에 따라, 수학적인 안전성과 더불어 사물에 가해지는 물리적인 공격에 대한 안전성도 중요하게 여겨지고 있다. 이때 공격자가 수행할 수 있는 대표적인 물리적인 공격으로는 암호 알고리즘이 동작할 때 발생하는 물리적인 정보(동작 시간, 소비 전력, 전자파 등)를 이용하여 비밀정보를 분석하는 방법인 부채널 분석[1]이 있다.

부채널 분석은 크게 프로파일링 부채널 분석과 비프로파일링 부채널 분석으로 나눌 수 있다. 먼저 프로파일링 부채널 분석은 분석자가 공격 대상 기기와 동일한 기기에 접근할 수 있음을 공격 가정으로 하며, 대표적으로 템플릿 공격[2]과 스토캐스틱 모델[3] 등이 있다. 반면에 비프로파일링 부채널 분석은 공격자가 모르는 비밀키에 대해 암호 알고리즘의 동작 결과만을 얻을 수 있음을 공격 가정으로 하며, 대표적으로 차분 전력 분석[1], 상관 전력 분석[4] 등이 있다. 프로파일링 분석의 경우 비교적 강한 공격 가정이 필요하므로 실제 환경에서의 적용이 현실적으로 제한될 수 있다. 따라서 공격 가정이 완화된

비프로파일링 분석이 많이 연구되고 있다.

최근에는 딥러닝을 이용한 비프로파일링 부채널 분석 방법이 제시되었다. Timon은 딥러닝 학습 결과를 구별자로 이용하여 파형을 라벨에 따라 분류했을 때, 학습 결과가 손실값, 정확도, 가중치의 측면에서 다르게 나타난다는 사실을 통해 비밀키를 분석하는 차분 딥러닝 분석을 제시했다[5]. 그러나 신경망의 용량에 비해 적은 수의 단일 데이터 집합으로 학습시킬 경우, 신경망이 데이터의 분포를 학습하지 못하고 단지 입출력을 외우는 문제가 발생할 수 있다. 따라서 본 논문에서는 학습 데이터 집합과 독립적인 데이터 집합을 활용하여 Timon의 방법보다 더 효과적인 비프로파일링 분석을 제시하고 이를 실험적으로 증명하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 제시한 방안을 이해하기 위한 소비전력모델, 딥러닝과 차분 딥러닝 분석을 소개한다. 3장에서는 독립적인 데이터셋을 사용해야 하는 근거를 제시하고, 4장에서는 실험을 통해 기존 방법[5]과 제시한 방법을 비교한다. 마지막 5장에서는 결론을 제시하면서 마친다.

2. 관련 연구

2.1 소비전력모델

소비전력모델은 소비 전력과 중간값과의 관계를 수학적으로 나타내기 위해 사용되며, 대표적으로 해밍웨이트 모델과 해밍디스턴스 모델이 있다. 해밍웨이트는 데이터의 이진 표현 시 1의 개수를 의미하며 일반적으로 소프트웨어로 구현된 암호 알고리즘은 해밍웨이트 모델을 따른다고 알려져 있다. 아래 수식은 해밍웨이트 모델을 나타낸 것이다.

$$P_{total} = \epsilon \cdot HW(y) + P_{noise}$$

(P_{total} : 총 전력소비, P_{noise} : 잡음, ϵ : 상수,
 HW : 해밍웨이트, y : 중간값)

2.2 딥러닝

인공 신경망은 사람의 신경망으로부터 영감을 얻어 뇌의 구조를 모델로 삼은 통계학적 학습 알고리즘이다. 층을 겹겹이 쌓은 인공 신경망을 사용하여 학습하는 기계 알고리즘의 집합을 딥러닝[6]이라고 한다. 학습이란 주어진 입력을 정확한 기댓값에 사영시키기 위해 적합한 가중치를 구하는 과정이다. 일반적으로 학습은 손실함수를 통해 신경망의 출력이 기댓값에서 벗어난 정도를 계산한 후, 최적화함수를 통해 손실함수가 감소하는 방향으로 가중치를 반복 수정한다. 손실함수는 평균 제곱 오차, 오차 제곱합, 교차 엔트로피 오차 등이 있고, 최적화함수는 경사하강법, Adam, RMSProp 등이 있다.

2.2.1 다층 퍼셉트론

다층 퍼셉트론(Multi-Layer Perceptron, MLP)[7]은 퍼셉트론으로 이루어진 여러 층을 붙여 놓은 계층구조를 갖는다. 퍼셉트론은 입력에 대해 가중치 곱과 편향의 합을 계산한 후, 활성화함수를 거치는 구조로 이루어진다. 그러나 퍼셉트론의 경우, 선형 분류만이 가능하므로 이를 보완하기 위해 입력층과 출력층 사이에 여러 개의 중간층을 두어 비선형 분류가 가능하도록 MLP를 구성한다. 이때 여러 개의 중간층을 은닉층이라고 부르며, 사용하는 활성화함수로는 Sigmoid, ReLU, Softmax 등이 있다.

2.2.2 일반화 성능

모델의 일반화 성능이란 학습에 사용하지 않은 데이터에 대한 예측의 정확도를 의미한다. 그런데 일반적인 학습 데이터 집합으로 모델을 훈련하고 평가

하는 방식은 모델의 일반화 성능을 보장할 수 없다. 학습 데이터의 양에 제한이 있는 경우, 모델이 데이터의 분포를 학습하지 않고 단순히 학습 데이터를 외워버리는 문제로 인해 과적합이 일어날 수 있기 때문이다. 이때 과적합이란 모델이 실제 데이터의 분포보다 주어진 학습 데이터의 분포에 더 근접하게 학습되는 현상을 의미한다. 즉 학습 데이터만으로는 새로운 데이터에 대해 일반화가 잘 이루어졌는지를 판단할 수 없다. 따라서 학습 데이터 집합을 훈련 데이터 집합과 그와 같은 분포를 가지는 독립적인 검증 데이터 집합으로 랜덤하게 나누어 모델의 일반화 성능을 검증한다[8]. 모델의 일반화 성능을 검증하는 방법에는 홀드아웃, K-겹 교차검증 등이 있다.

2.3 차분 딥러닝 분석

차분 딥러닝 분석(Differential Deep Learning Analysis, DDLA)[5]은 차분 전력 분석을 딥러닝에 적용한 것이다. 공격 대상 기기에서 수집한 파형들을 학습의 입력 데이터로 사용하여 딥러닝 학습을 수행하는데, 이때 모델의 라벨은 중간값의 최상위 비트, 최하위 비트 혹은 해밍웨이트를 사용한다. 학습의 성능 지표로는 손실값, 정확도 혹은 가중치를 이용하는데, 만약 성능 지표로 손실값을 사용했다면 딥러닝 모델이 학습을 잘 수행했다고 가정했을 때 옳은 라벨에 대한 손실값이 틀린 라벨에 대한 손실값보다 작을 것이라고 예상한다. 따라서 가장 작은 손실값을 가지는 라벨을 계산할 때 사용된 키를 비밀키라고 추측할 수 있다.

3. 신경망의 일반화성능 비교를 통한 효율적인 딥러닝 기반 비프로파일링 부채널 분석 방안

본 논문에서는 신경망의 일반화 성능을 비교함으로써 기존 방법보다 더 적은 정보로도 비밀키를 찾는 방안을 제시하고, 논리적 타당성을 실증적으로 보인다.

기존 방법은 하나의 데이터 집합에 대한 학습 결과를 기반으로 추정한 키가 비밀키인지를 검증한다. 이 방법에서는 파형과 추정한 키로 계산한 라벨이 관련 없더라도 신경망이 단순히 입출력을 외워서 손실값이 감소하는 문제가 있다. 즉, 옳은 키와 틀린 키 모두 손실값이 감소한다. 우리는 이를 해소하기 위해 일반화 성능을 기반으로 신경망의 학습 여부를 판정한다. 신경망이 데이터의 분포를 학습하지 못했다면 새로운 데이터에 대해서는 정확한 라벨을 예측

할 수 없으므로 검증 데이터 집합에 대한 손실값은 감소하지 않는다. 반면, 분포를 학습했다면 새로운 데이터에 대한 라벨을 높은 정확도로 예측할 수 있으므로 손실값이 감소한다.

기존 방법은 비밀키를 찾기 위해 신경망이 입출력을 외울 수 없을 정도로 많은 데이터가 필요하다. 한편, 제시한 방법은 분포를 학습할 수 있을 정도의 데이터만 있으면 비밀키를 찾을 수 있으므로 기존 방법보다 더 적은 정보로도 분석이 가능하다.

4. 실험 결과

본 장에서는 기존 방법과 제시된 방법을 비교한다. 실험은 Atmel XMEGA128D4 (8-bit 프로세서) 칩을 사용하는 ChipWhisperer-Lite 전력 수집 보드에서 부채널 대응기법이 적용되지 않은 8-bit 단위 AES-128 암호 알고리즘[9]이 10,000번 동작할 때 발생하는 소비전력을 Sampling Rate 29.538MS/s로 수집하였다. 신경망은 TensorFlow 2.0.0 버전을 백엔드로 하는 Keras 2.3.1 버전을 이용해 구현하였다.

신경망의 입력은 1라운드 SubBytes를 수행할 때의 소비전력 696포인트이고, 출력은 바이트별 1라운드 SubBytes 출력의 해밍웨이트이다. 과적합을 방지하기 위해 은닉층이 1개인 MLP를 구성하였으며, 은닉층은 8개의 노드를 가진다. 학습은 200에포크만큼 수행했다. 제시한 방법에서 학습 데이터 집합과 검증 데이터 집합의 비율은 7 : 3으로 지정했다. 성능 지표로는 Timon이 제시한 손실값, 정확도, 가중치 중 손실값을 활용한다.

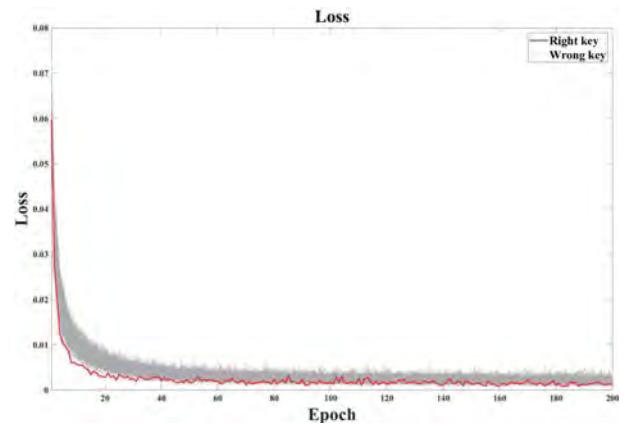
신경망의 목표가 중간값의 해밍웨이트를 찾는 회귀 문제를 해결하는 것이므로 손실함수는 평균 제곱 오차를 채택하였으며, 손실값이 가장 낮을 때의 키를 비밀키라고 추정하였다.

학습 결과를 비교하기 위해 *ratio*를 다음과 같이 정의한다.

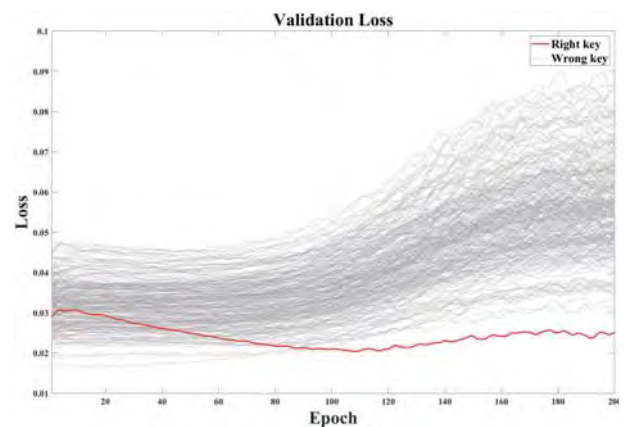
$$ratio = \frac{(\text{틀린 키의 손실값 중 최솟값})}{(\text{옳은 키의 손실값})}$$

올바르게 추측했다면 옳은 키의 손실값이 가장 작으므로 *ratio*는 1보다 커야 한다.

(그림 1), (그림 2)는 200개의 파형을 이용해 첫 번째 바이트 키를 각각 기존 방법, 제시한 방법으로 분석했을 때의 손실값을 나타낸 것이다.



(그림 1) 기존 방법을 이용했을 때의 에포크별 손실값

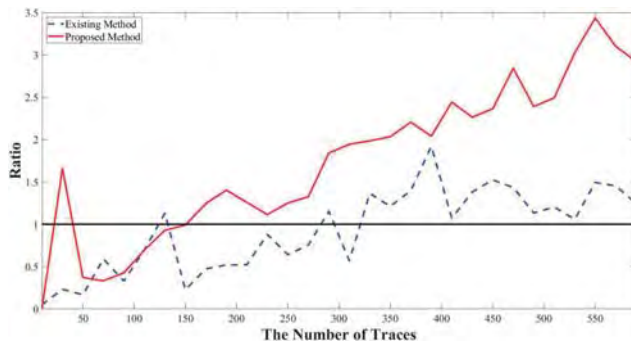


(그림 2) 제시한 방법을 이용했을 때의 에포크별 손실값

기존 방법의 경우 틀린 키를 이용해 라벨을 계산했다 해도 신경망이 입출력을 외우기 때문에 모든 키의 손실값이 낮아지며 $ratio \approx 0.77$ 으로 비밀키 분석에 실패했다.

반면, 제시한 방법은 틀린 키를 이용해 라벨을 계산할 경우 신경망이 데이터의 분포를 학습하지 못하므로 틀린 키의 손실값은 증가하지만, 옳은 키의 손실값은 감소한다. 또한, $ratio \approx 1.22$ 로 비밀키 분석에 성공했다.

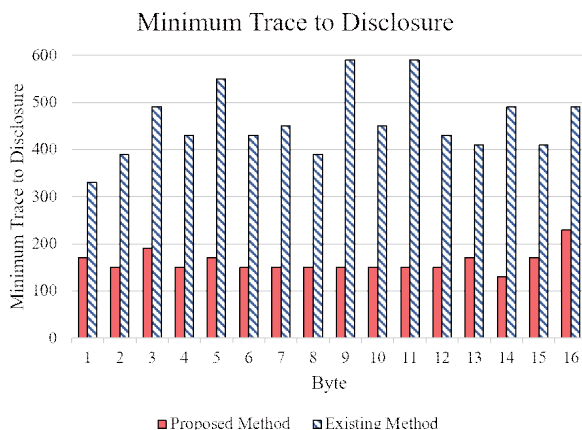
(그림 3)은 데이터 수에 따른 *ratio*의 변화를 나타낸 것이다.



(그림 3) 데이터 수에 따른 ratio

기존 방법은 비밀키 분석을 위해 330개 이상의 데이터가 필요하지만, 제시한 방법은 170개의 데이터만으로도 비밀키 분석에 성공했다.

(그림 4)는 바이트별 비밀키 분석을 위해 필요한 과형의 수를 도식화한 것이다. 기존 방법은 전체 비밀키 분석을 위해 590개의 과형이 필요하지만, 제시한 방법은 230개의 과형으로도 비밀키 분석에 성공했다. 따라서 제시한 방법을 사용하면 기존 방법의 약 1/3의 데이터만으로도 비밀키 분석이 가능하다.



(그림 4) 기존 방법과 제시한 방법의 최소 분석 과형 수

5. 결론

본 논문에서는 비프로파일링 환경에서 학습 데이터 집합과 독립적인 검증 데이터 집합을 활용하여 딥러닝 기반의 부채널 분석 성능을 향상할 수 있는 방법을 제시하였다. 제시한 방법은 신경망의 일반화 성능을 검증함으로써 입력 데이터와 라벨 사이에 규칙이 존재함을 보인다는 점에서 기존 방법보다 논리적 타당성을 갖는다. 실험 결과, 기존 방법으로는 키 분석에 590개의 과형이 필요했지만 제시한 방법을 이용하면 230개의 과형으로 비밀키 분석이 가능했다.

사사

본 논문은 산업통상자원부 국제공동기술개발사업으로 지원된 연구임. (P0011922, 딥러닝을 이용한 RI SC-V 기반 하드웨어 보안성 검증 도구 개발)

참고문헌

- [1] Paul Kocher, Joshua Jaffe, and Benjamin Jun "Differential power analysis" Annual International Cryptology Conference. Springer, Berlin, Heidelberg, 1999.
- [2] Suresh Chari, Josyula R. Rao, and Pankaj Rohatgi "Template attacks" International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg, 2002.
- [3] Werner Schindler, Kerstin Lemke, and Christof Paar "A stochastic model for differential side channel cryptanalysis" International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg, 2005.
- [4] Eric Brier, Christophe Clavier, and Francis Olivier "Correlation power analysis with a leakage model" International workshop on cryptographic hardware and embedded systems. Springer, Berlin, Heidelberg, 2004.
- [5] Benjamin Timon, "Non-profiled deep learning-based side-channel attacks with sensitivity analysis" IACR Transactions on Cryptographic Hardware and Embedded Systems (2019): 107-131.
- [6] Yann LeCun, Yoshua Bengio, and Geoffrey Hinton "Deep learning" nature 521.7553 (2015): 436-444.
- [7] Marius-Constantin Popescu et al. "Multilayer perceptron and neural networks" WSEAS Transactions on Circuits and Systems 8.7 (2009): 579-588.
- [8] Ron Kohavi, "A study of cross-validation and bootstrap for accuracy estimation and model selection" Ijcai Vol. 14. No. 2. 1995.
- [9] Federal Information Processing Standards Publication (FIPS 197), "Advanced Encryption Standard(AES)", 2001

IoT 환경에서 물리적 복제 방지 기술 기반 인증 프로토콜 취약점 분석 및 개선방안 제안¹⁾

최재현*, 정익래*, 변진욱**

*고려대학교 정보보호대학원 정보보호학과

**평택대학교 정보통신학과

93jamie@korea.ac.kr, irjeong@korea.ac.kr, jwbyun@ptu.ac.kr

A proposal of countermeasure and security analysis on the PUF based authentication protocol in IoT network

Jae Hyun Choi*, Ik Rae Jeong*, Jin Wook Byun**

*Graduate School of Information Security, Korea University

**Dept. of Information and Communication, Pyeongtaek University

요 약

사물인터넷의 사용이 급격히 증가함에 따라 관련 보안 기술의 개발이 매우 중요하게 되었다. 사물인터넷이 지니는 근본적인 자원 제한 요소 환경을 극복하기 위해, 최근 Chatterjee 기타 등은 경량화된 질의 응답 기반의 PUF를 활용한 인증 프로토콜을 최근 IEEE Transactions on Dependable and Secure Computing 저널에 제안하였다. 그러나 장치 간 세션 키를 주고받는 과정에서 공개된 채널에서 값을 한번 획득한 공격자는 누구나 세션 키를 만들 수 있는 치명적인 취약점이 존재한다. 본 논문에서는 이러한 취약점을 설명하고 정당한 장치만 세션 키를 만들 수 있는 방법을 제시한다.

1. 서론

최근 사물인터넷(IoT)의 활용도와 접근성이 증가함에 따라 IoT 기기들은 일상생활에서 다양한 영역에서 사용되고 있다. IoT 환경에서 보안 프로토콜을 설계할 때 가장 큰 이슈는 낮은 계산 능력과 적은 메모리를 고려하여 인증 및 보안 프로토콜을 설계해야 한다는 점이다. 이로 인해, 물리적인 복제 기능을 갖춘 PUF(Physical Unclonable Function) 기술에 주목하게 되었다. PUF는 제조 시 동일한 과정을 거치더라도 반도체의 미세한 구조 차이를 이용하여 물리적으로 복제 불가능한 기능으로 보안키를 생성하는 기술이다. 마치 사람의 지문과 같이 장치의 고유한 정보를 갖고 있고, 이 고유한 값은 외부로 유출되지 않는 특징을 갖고 있다[1]. PUF를 사용하면 질의 응답 기반의 경량화된 인증 설계가 가능하여 IoT 장비의 보안 요구사항에 대한 부담을 줄일 수 있다[2][3][4].

2018년에 Chatterjee 기타 등[5]은 IoT 환경에서 PUF를 사용하여 장치 간 비밀 통신을 위한 프로토

콜을 제시했다. 그런데 세션 키를 생성하는데 사용될 값을 공유할 때, 정당하지 않은 장치가 임의의 값으로 세션키를 형성할 때 필요한 값을 만들 수 있는 문제점이 존재한다. 본 논문에서는 Chatterjee 기타 등에서 장치 간 세션 키 형성에 있어서 정당한 장치임을 인증하는 개선방안을 제안한다.

2. 암호 프리미티브

- 타원 곡선 암호 (Elliptic Curve Cryptography)

공개키 암호 시스템으로 타원 곡선 이론에 기반한 이론이다. 타원 곡선은 유한체 $E: y^2 = x^3 + ax + b$ 상의 정수로 이뤄진 점들의 집합이다. 타원 곡선에서의 곱셈은 타원곡선 상에서의 정의된 덧셈 연산의 반복 수행하는 것이다.

- Bilinear paring operation

큰 소수 q 에 대해 타원 곡선과 군 G_1, G_2, G_3 가 있다. Bilinear paring operation은 bilinear map $e: G_1 \times G_2 \rightarrow G_3$ 이고 다음을 만족한다.

$$(1) \text{ Bilinearity : } \forall a, b \in F_q^*, \forall P \in G_1, \forall Q \in G_2 \\ : e(aP, bQ) = e(P, Q)^{ab}.$$

1) 이 논문은 2017년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. 2017R1D1A1B03032424)

(2) Non-degeneracy : $e(P, Q) \neq 1$.

(3) Computability : e 를 계산하는데 효율적인 알고리즘이 존재한다.

• Elliptic curve discrete logarithm problem

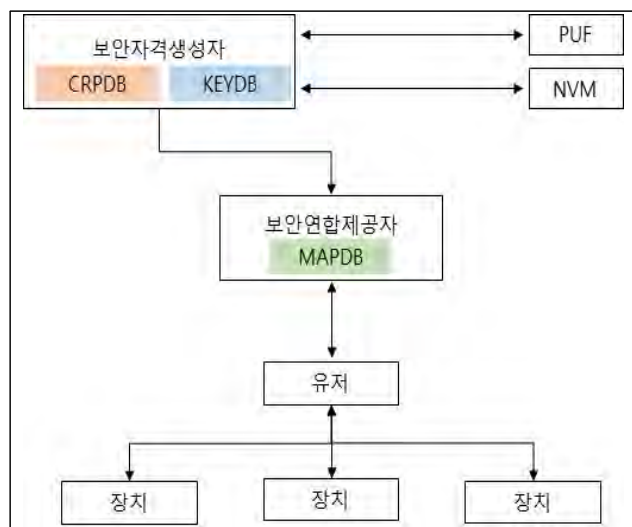
타원곡선 위의 점 P 와 생성원 Q 가 존재할 때, $P = t \cdot Q$ 를 만족하는 스칼라 t 를 다항 시간 내에 구하는 것은 어렵다.

3. Chatterjee 기타 등의 프로토콜 분석

인증프로토콜은 일반적으로 등록 단계와 인증 및 키 교환 단계로 나뉜다. 등록단계는 안전한 채널을 가정하고 인증 및 키교환 단계는 공개된 채널에서 수행됨을 가정한다. 전체적인 프로토콜에서 사용되는 표기와 그에 대한 설명은 <표 1>, 시스템 구조는 <그림 1>에서 정리하였다. <그림 2>, <그림 3>는 Chatterjee 기타 등[5]의 프로토콜을 직접 이미지화 시켜서 표현한 것이다.

표기	설명
C_A, R_A	PUF의 질의, 응답 값
HLP_A	PUF값의 헬퍼데이터
C_S, K_S	유저의 질의 값, 비밀 값
H_1, H_2, H_3	암호학적으로 안전한 해시 함수 단, H_2 는 키를 이용한 해시 함수
e	타원곡선 pairing 연산
BCH_{Enc}, BCH_{Dec}	헬퍼데이터 값을 위한 인,디코딩
a, x, t	임의의 수
KA_{PUB}, KA_{PRV}	장치 간 사용되는 A 의 공개,개인키

<표 1> 표기 및 설명에 대한 소개



<그림 1> 시스템 구조

1) 등록 단계

• 보안 자격 생성자는 IoT 장치 A 에 PUF 입력값에 해당하는 질의 값 C_A 를 전송하고 장치 A 는 $R_A = PUF_A(C_A)$ 를 계산하여 응답한다. 보안 자격 생성자는 받은 R_A 로부터 인코딩을 통해 HLP_A 를 생성하고 이 값을 저장한다.

• 보안 자격 생성자는 유저 S 에게 비밀 값 K_S 를 전달한다.

• 보안 자격 생성자는 유저 S 와 장치 A 를 연결하는 프로세스를 실행한다. 이때 C_S 를 생성하고, $P_A = H_1(R_A), P_S = H_2(K_S), aIN_R Z_q^*, B = P_A - aP_S, d = H_3(H_1(C_A || C_S || HLP_A || a || H_3(P_S)) + B)$ 를 계산 후 보안 연합 제공자에게 $C_A, C_S, a, HLP_A, B, d_1$ 을 건네 주고 보안 연합 제공자는 이를 저장한다.

2) 인증 및 키 교환 단계

장치 A 는 장치 B 와 비밀통신하기 위해 유저와 상호 인증 과정을 마치고 유저에게 받은 값들을 활용하여 장치 간 통신을 위한 세션키를 생성한다.

• 장치 A 가 유저에게 장치 A, B 의 ID를 보낸 후 유저는 각 장치가 본인의 것인지 확인을 위해 보안 연합 제공자에게 유저와 장치의 ID를 보낸다. 보안 연합 제공자는 저장된 값을 확인 후 유저에게 C_A, C_S, HLP_A, a, B, d 를 전송한다.

• <그림 2>에서는 유저가 보안 연합 제공자로부터 값을 전달받은 이후 장치 A 와 유저간의 인증 과정을 나타낸다. 장치 B 역시 유저와 같은 과정을 동일하게 수행하므로 장치 A 에 대한 프로토콜만 표기하였다.

(1) 유저의 질의값을 키를 사용한 해시함수로 P_S 를 생성하고, 해시함수를 통해 보안 연합 제공자로부터 전달받은 값의 무결성을 검증한다. P_A 를 계산 후 난수 x 와 함께 Q_A 값을 생성하고, 나중에 검증값으로 사용될 V_A 를 계산한다.

(2) 유저는 ID_B , 장치 A 의 질의 값, A 의 헬퍼데이터와 자신이 생성한 Q_A 값을 장치 A 에게 전달한다.

(3) 장치 A 는 유저로부터 받은 질의 값에 대한 PUF를 이용한 응답 값에 헬퍼데이터를 디코딩하여

R 값을 구한다. R 값을 해시한 후 인증에 사용될 값을 생성하고 난수 t 와 임의의 생성원 Y_A 를 만든다. 난수와 생성원을 기반으로 공개키와 개인키를 생성한다.

(4) 장치 A 는 인증하기 위해 생성한 값들을 유저에게 전송한다,

(5) 유저는 장치 A 에게 받은 값을 이용하여 장치 A 가 정당한지 여부를 확인한다.

(6) 유저는 장치 A 와 동일한 과정을 거친 인증된 장치 B 로부터 받은 값을 장치 A 에게 전달한다. 이때 정당한 유저라고 인증할 값으로 해시된 P_A 값을 해시하여 함께 보낸다.

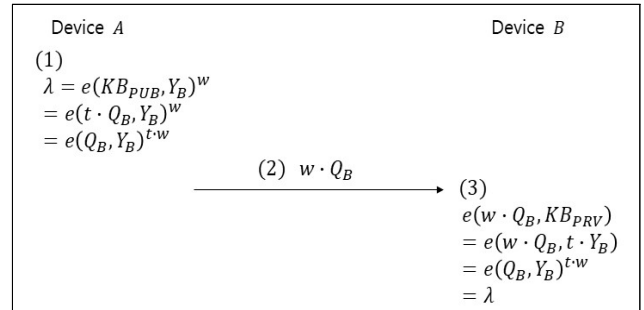
• 장치 간 세션키를 형성하는 과정은 <그림 3>과 같다.

(1) 장치 A 는 유저로부터 받은 장치 B 에 대한 값인 KB_{PUB} , Y_B 와 임의로 생성한 난수 w 를 사용하여 세션키로 사용될 λ 를 계산한다.

(2) 장치 A 는 장치 B 가 λ 를 생성할 수 있도록 $w \cdot Q_B$ 를 건네준다.

(3) 장치 B 는 장치 A 에게 받은 값 $w \cdot Q_B$ 와 자신의 비밀정보 KB_{PRV} 를 사용하여 세션키로 사용할 λ 를 생성한다.

통해 건네주게 된다. 장치 A 뿐 아니라 악의적인 사용자가 KB_{PUB} , Q_B , Y_B 를 얻을 수 있음을 의미한다. 악의적인 사용자가 얻은 값과 임의의 값 w' 을 생성하여 세션키 λ' 을 생성할 수 있다.



<그림 3> 장치 간 세션키 형성 과정

4. 해결 방안

본 논문에서 KB_{PUB} , Q_B , Y_B 를 얻은 임의의 장치가 세션키 λ 를 생성하는 문제를 해결하고자 한다. 제안하는 해결 방안은 세션키 λ 를 생성할 때, 유저와 상호 인증을 마친 정당한 장치 A 가 가진 개인키 값 KA_{PRV} 를 활용하여 세션키를 만들도록 설계하는 것이다.

1) 세션키 형성 과정

제안하는 장치 간 세션키 형성 과정은 <그림 4>와 같다.

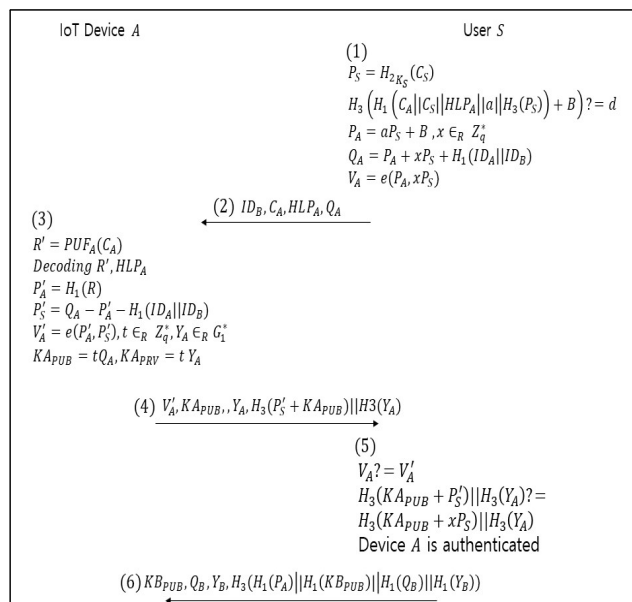
(1) 장치 A 는 자신이 생성한 KA_{PRV} , 유저로부터 건네 받은 KB_{PUB} , 난수 w 를 활용하여 타원곡선 paring 연산을 통해 세션키 λ ($= e(KA_{PRV}, KB_{PUB})^w$)를 생성한다.

(2) 장치 A 는 장치 B 에게 세션키 λ 를 만들기 위해 사용될 $w \cdot t_a \cdot Q_B$ 를 건네준다.

(3) 장치 B 는 유저에게 받은 Y_A , 자신이 가진 비밀 값 t_b 과 장치 A 에게 받은 값 $w \cdot t_a \cdot Q_B$ 를 사용한다. $e(Y_A, w \cdot t_a \cdot Q_B)$ 에 t_b 를 거듭제곱 한 후 paring 연산 방법에 따른 계산을 완료하면 λ 를 생성할 수 있다.

2) 안전성 분석

본 논문에서 제안한 프로토콜에서는 세션키를 만들 때 장치 A 의 개인키 KA_{PRV} 와 장치 B 의 공개키 KB_{PUB} 와 임의의 난수 w 가 사용된다. 이때, 개인키는 장치 A 가 임의로 생성한 난수 t_a 와 임의의 생성



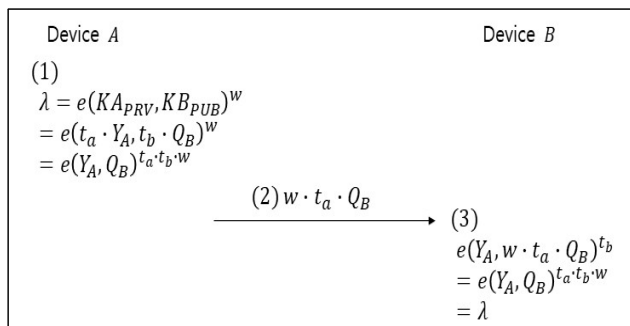
<그림 2> Chatterjee 기타 등의 프로토콜

3) Chatterjee 기타 등의 프로토콜 취약점

Chatterjee 기타 등의 프로토콜에서 장치간 세션키 λ 를 생성할 때 사용되는 인자들이 공개된 채널을

원 Y_A 를 사용하여 만든다. 이전의 장치 및 유저 간 인증 과정에서 유저를 통해 Y_A , KA_{PUB} , Q_A 가 전달되어 노출되더라도 타원 곡선 이산대수 문제의 어려움에 따르면, 공격자는 $KA_{PUB}(=t_a \cdot Q_A)$ 와 Q_A 값을 통해서 t_a 를 다항 시간 내에 계산하는 것이 어렵다. 마찬가지로 타원 곡선 이산대수 문제에 따라 Q_B 를 알고 있더라도, 세션키 형성 중 건네주는 $w \cdot t_a \cdot Q_B$ 의 값을 통해서도 t_a 뿐 아니라 w 값도 얻어 낼 수 없다. 따라서 t_a 를 모르는 공격자는 장치 A 의 개인키 값인 KA_{PRV} 를 만들 수 없다. 장치 B 는 이를 근거로 오로지 t_a 값을 알고있는 장치 A 가 세션키를 만들었음을 알 수 있다.

또한 공격자가 장치 B 인척 $w \cdot t_a \cdot Q_B$ 를 탈취하여 장치 A 와 세션키를 공유하려고 할지라도 마찬가지로 이유로 장치 B 의 비밀 값인 t_b 를 알지 못하므로 세션키 λ 를 생성할 수 없다. 따라서 정당한 장치 A 와 정당한 장치 B 만 안전하게 세션키를 주고 받을 수 있게 된다.



<그림 4> 제안하는 세션키 형성 과정

5. 결론

사물인터넷(IoT)의 사용의 증가에 따라 보안 문제도 함께 해결되어야 함에 있어서 자원 문제 등 많은 제한사항이 있는 환경에서 Chatterjee 기타 등은 PUF를 활용하여 보안성을 높이고 보안 요구사항에 적합한 프로토콜을 제시했다. 그러나 장치 간 세션키 형성 과정에서 사용되는 값이 공개된 채널에서 전달되고 이를 탈취한 공격자가 정당한 장치인 척 세션키를 만들 수 있는 문제점이 발견되었다. 본 논문에서는 이를 해결하고자 세션키를 생성할 때, 타원 곡선 이산대수 문제의 어려움에 기반한 유저와 상호 인증을 마친 정당한 장치만 갖고있는 개인키를 사용함으로써 장치 간 상호 인증을 가능하도록 방법을 제안하였다.

참고문헌

- [1] M. Potkonjak and V. Goudar, "Public Physical Unclonable Functions," in Proceedings of the IEEE, vol. 102, no. 8, pp. 1142-1156, Aug. 2014.
- [2] K. Zhao and L. Ge, "A Survey on the Internet of Things Security," 2013 Ninth International Conference on Computational Intelligence and Security, Leshan, 2013, pp. 663-667.
- [3] A. P. Johnson, R. S. Chakraborty and D. Mukhopadhyay, "A PUF-Enabled Secure Architecture for FPGA-Based IoT Applications," in IEEE Transactions on Multi-Scale Computing Systems, vol. 1, no. 2, pp. 110-122, 1 April-June 2015.
- [4] Y. Yilmaz, S. R. Gunn and B. Halak, "Lightweight PUF-Based Authentication Protocol for IoT Devices," 2018 IEEE 3rd International Verification and Security Workshop (IVSW), Costa Brava, 2018, pp. 38-43.
- [5] U. Chatterjee et al., "Building PUF Based Authentication and Key Exchange Protocol for IoT Without Explicit CRPs in Verifier Database," in IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 3, pp. 424-437, 1 May-June 2019.

네트워크 패킷 레벨에서 알려진 실행 파일 식별 및 차단 연구

조용수*, 이희조*

*고려대학교 컴퓨터정보통신대학원 소프트웨어보안학과
e-mail: emptyskycho@korea.ac.kr

Research on the identification and blocking of known executalbe files at the network packet level

Yongssoo Jo*, heejo Lee*

*Dept. of Information Technology, Korea University

요 약

최근의 사이버 침해 사고는 공격 대상을 지정하여 지속적으로 공격을 시도하는 APT(Advanced Persistent Threat)와 랜섬웨어(Ransomware) 공격이 주를 이룬다. APT 공격은 dirve by download 를 통하여 의도하지 않은 파일의 다운로드를 유도하고, 다운로드 된 파일은 역통신채널을 만들어 내부 데이터를 외부로 유출하는 방식으로, 공격에 사용되는 악성 파일이 사용자 모르게 다운로드 되어 실행된다. 랜섬웨어는 스피어 피싱(Spear-phishing)과 같은 사회공학기법을 이용하여 신뢰 된 출처로 유장 된 파일을 실행하도록 하여 주요 파일들을 암호화 한다. 때문에 사용자와 공격자 사이 네트워크 중간에 위치한 패킷 기반의 보안 장비들은 사용자에게 의해 다운로드 되는 파일들을 선제적으로 식별하고, 차단하여 침해 확산을 방지 할 수 있는 방안이 필요하다. 본 논문에서는 네트워크 패킷 레벨에서 알려진 악성파일을 식별하고 실시간 차단하는 방안에 대하여 연구하고자 한다.

1. 서 론¹⁾

대부분의 기업들은 내부 네트워크를 외부의 불법적인 사용자의 침입으로부터 안전하게 보호하기 위한 네트워크 보안 장비, 방화벽(Network FireWall), IPS(Intrusion Prevention System) 등을 사용한다. 이러한 보안 장비들은 모두 패킷(packet)을 기반으로 검사하는 방식으로, 1Kbyte-2Kbyte (ethernet 기준 1518 byte) 패킷 정보로 보안 정책을 판단하여 차단 할 것인지, 전달 할 것인지를 판단하게 된다. 때문에, 1.5Kbyte 의 패킷 사이즈 보다 훨씬 큰 파일 기반 공격으로 이루어진 APT 와 랜섬웨어는 패킷 기반 보안 장비로 대응하기 어렵다. 시그니처 기반으로 각 파일들의 signature, pattern 를 찾아 등록 할 수 있지만, 모든 파일을 각각 분석하여 unique signature 찾아야 하기 때문에, 패킷 기반 보안 장비에서는 거의 사용하지 않는다. (패킷 fragment 에 의한 시그니처의 분리도 시그니처 탐지 방식 사용을 어렵게 한다.) 이러한 문제를 해결하기 위해 네

트워크 패킷 단위를 기반으로 악성 파일을 식별할 수 있는 방안에 대해 연구하였으며, 제안 방식을 시험을 통하여 연구 결과를 살펴보고자 한다. 본 논문에서는 악성파일을 식별하고 탐지 및 차단하는 것을 목표로 하며, APT 공격과 랜섬웨어 이용되는 파일들이 EXE, DLL, SCR 같은 실행파일, 즉 PE(Portable Executable) 파일 형식을 사용하고 있으므로, PE(Portable Executable) 형태의 실행 가능한 파일을 대상으로 범위를 한정한다.

2. 관련 연구

알려진 악성 파일을 식별하기 위해 자주 사용되는 기술은 해시(hash)이다. 파일 해시 기술은은 파일의 전체 내용을 SHA1이나 MD5와 같은 해시 연산을 통해 하나의 해시 값으로 생성하는 방식으로, 완전한 파일 전체를 대상으로 해쉬하여 나온 값을 통하여 식별한다. 해시를 이용한 다른 파일 식별 방법으로는 파일 부분 해시 기술로, 파일을 나누는 기준에 따라 FLC(Fixed Length Chunking)과 VLC(Variable Length Chunking)으로 나뉜다. 이러한 방식은 파일의 유사

성을 비교하기 위하여 주로 사용되고, 이 역시 완전한 파일 전체를 대상으로 block 단위와 위치에 따라 나누어 해시 한 후 대표값을 통하여 파일을 식별한다.

인터넷 사용자와 서버 사이에 위치하는 네트워크 보안 장비는 그 위치와 서비스를 지원하는 특성상 속도에 민감하다. 때문에 기존 전체 파일 해시 방식을 활용하여 악성파일을 식별한다면 네트워크 처리 성능에 많은 영향을 미치게 된다. 다음은 악성파일 탐지를 위한 검사 시간 영향도이다.

$$\text{Scanning Time} = \frac{\text{Packet of the file recombination} \times \text{Size of the file objects} \times \text{Hash Time}}{\text{Speed of Processor}}$$

Fig 1. 파일전체 해시를 이용한 검사 시간

검사 대상 파일의 모든 패킷을 수집하여 완전한 파일로 재조합 한 후 해시 검사를 완료하여 탐지하고 차단한다면, 네트워크 중간의 보안 장비는 패킷을 수집 할 많은 메모리 공간과 파일 재조합 비용으로 많은 네트워크 딜레이가 발생하게 될 것이다.

3. 제안 방안

서론에서 언급한 것과 같이 악성 파일들이 EXE, DLL, SCR 와 같은 PE(Portable Executable) 파일 형식을 사용하고 있으며, PE(Portable Executable) 은 PE header 에 파일을 특정 지을 수 있는 많은 정보들이 들어있다. PE 파일의 대표적인 정보로는 TimeDate Stamp, Size of Code, Address of EntryPoint, CheckSum, Size Of File, Certificate address 등이 포함되며, 이 모든 정보는 파일의 첫 1Kbyte 안에 존재하게 된다.

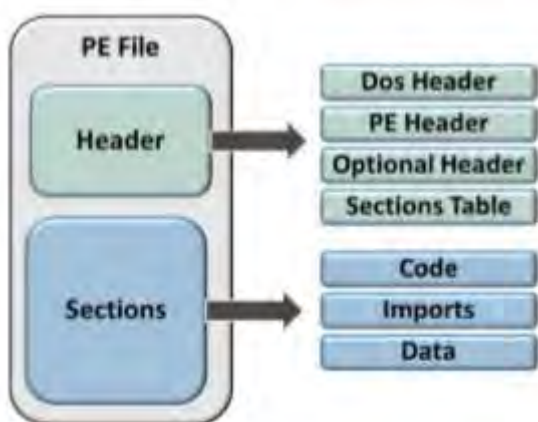


Fig 2. PE 파일 구조

즉, MS-DOS 2.0 Section, PE File Header, Windows Specific Fields, Data Diorectories, Certificate Table 정보 등 PE 파일을 특정 지을 수 있는 정보의 대부분이 파일

의 첫 번째 패킷에 들어있게 된다. 이것은 PE 파일 전체 해시를 첫 번째 패킷 데이터로 대체 할 수도 있다는 가정을 하게 되었다.아래는 하나의 패킷 해시로 대응 했을 때 탐지를 위한 검사 시간 영향도 이다.

$$\text{Scanning Time} = \frac{\text{One piece of packet} \times \text{Hash Time}}{\text{Speed of Processor}}$$

Fig 3. PE헤더 해시를 이용한 검사 시간

4. 시험 및 결과

VirusTotal 에서 2020년 1월부터 3월기간 동안 악성파일로 탐지(20개 이상의 백신에 탐지) 된 1천개의 파일과 인터넷에서 무작위로 수집 된 인터넷 실행 파일(정상) 9천개를 대상으로 파이썬 스크립트를 통하여 네트워크로 전송하였다. 네트워크 중간의 보안 장비에서 패킷을 모니터링하여, PE 파일의 경우 첫번째 패킷을 해쉬하여 로깅하였고, 이를 이용하여 충돌물을 비교 검사하였다.



Fig 4. 해시 충돌 시험 환경

시험 결과,

바이러스 토탈 악성 1000 파일 - 충돌파일 0 | 인식 1000
네트워크 임의 정상 9000 파일 - 충돌파일 3 | 인식 8994

총 1만개의 악성, 정상 파일을 분석 한 결과 악성파일에서 0건, 정상 파일에서 1건의 충돌이 있었다. 정상파일 1건의 경우 분석결과 뺑깍으로 압축 된 실행파일 형태였으며, 동일한 압축 포맷, 즉 동일한 뺑깍 PE 헤더를 통하여 내부 서로 다른 파일을 감싸고 있었다.

5. 결 론

시험을 통하여 PE (Portable Executable) 파일 기반 실행파일은 PE 헤더 정보를 해쉬하는 것만으로도 충분히 파일 인식이 가능하며, 이를 통하여 알려진 악성 파일의 확산을 FireWall 과 IPS 같은 패킷 기반 네트워크 보안 장비에서 선 차단 할 수 있을 것을 기대한다. 시험에서 예외로 발생 하였던 실행파일 뺑깍 PE 포맷은 해당 프로그램의 특징으로 파일 패킹(file packing) 기술로 봐야 할 것이다. 다만, 뺑

집의 경우 모두 동일 특징을 가지고 있어 예외처리가 가능하다. 이 후 시험에는 더 많은 파일들을 대상으로 시험하여 해시 충돌률을 면밀히 비교해 볼 예정이다.

참고문헌

- [1] Breitingner, F. & Baggili, I. "File detection on network traffic using approximate matching.", Journal of Digital Forensics, Security and Law. Special Issue: 2014 ICDF2C / SADFE. 9(2): 23-36, 2014.
- [2] Y. J. Cho, "Unknown Malware Detection Using File Reputation", Proceedings of the Korea Information Processing Society Conference, 376-379, 2015
- [3] S. J. Oh, Ko and Y. W. Ko, "Triple Fixed Length Hashing Scheme for Similarity Search", Proceedings of KIIT Conference, 339-342, 2013
- [4] Y. J. Yoo and S. J Kim and J. Kim, and Y. W. Ko, "File Similarity Evaluation System Using Rate-based Representative Hash Scheme", Korean Institute of Information Technology, 81-88, 2014
- [5] Virustotal statistics, "virustotal malware statistics", (<https://www.virustotal.com/ko/statistics>)

지터에 내성을 갖는 딥러닝 기반 부채널 분석 방안

김주환**, 김수진*, 우지은*, 박소연*, 한동국*, ***

*국민대학교 정보보안암호수학과

**국민대학교 수학과

***국민대학교 금융정보보안학과

zzzz2605@kookmin.ac.kr, suzin22@kookmin.ac.kr, dnwldms928@kookmin.ac.kr,

soyeonp@kookmin.ac.kr, christa@kookmin.ac.kr

Deep Learning-based Side-Channel Analysis Method with Resistance to Jitter

Ju-Hwan Kim**, Soo-Jin Kim*, Ji-Eun Woo*, So-Yeon Park*, Dong-Guk Han*, ***

*Dept. of Information Security, Cryptology, and Mathematics, Kookmin University

**Dept. of Mathematics, Kookmin University

***Dept. of Financial Information Security, Kookmin University

요 약

물리적 정보를 이용해 암호 알고리즘의 비밀정보를 분석하는 부채널분석 분야에서도 딥러닝을 접목한 분석방법들이 활발히 제안되고 있다. 본 논문에서는 소비전력이 시간축상으로 흐트러지는 현상인 지터가 있는 파형을 신경망의 특성을 기반으로 효과적으로 분석하는 방법을 제안한다. 제안한 방법을 실험적으로 검증하기 위해 지터가 있는 AES-128 파형을 Convolutional Neural Network와 Multi-Layer Perceptron을 기반으로 분석한 결과 제안한 방법을 적용한 신경망은 모든 바이트 키 분석에 성공했으나, 이외의 신경망은 일부 혹은 모든 바이트 키 분석에 실패했다.

1. 서론

부채널분석(Side-Channel Analysis)이란 암호 알고리즘이 실제 디바이스에서 동작할 때 발생하는 전력이나 전자파와 같은 부채널 정보를 이용하여 비밀정보를 분석하는 방법이다[1]. 그중 대표적인 분석방법인 전력분석공격은 디바이스가 동작할 때의 소비전력을 이용하여 비밀정보를 분석한다[2]. 따라서 공격자는 데이터와 소비전력 사이의 관계를 찾거나 소비전력에서 유의미한 분석 지점인 PoI(Point of Interest)를 찾아내야 하는 등 공격자에게 높은 분석능력이 요구된다.

최근 딥러닝이 여러 분야에 활용되면서 부채널분석 분야에서도 딥러닝을 접목한 공격방법들이 연구되고 있다. 프로파일링 환경에서 딥러닝 기반 부채널분석은 공격자가 평문과 비밀키를 알고 있는 프로파일링 장비를 확보했다는 가정 하에서의 공격이다. 비밀키를 알고 있다면 파형에 대응되는 중간값을 계산할 수 있으므로, 신경망이 파형으로부터 중간값을 예측하도록 학습시킬 수 있다. 공격자는 학습된 신경망을 이용하여 공격 대상의 소비전력으로부터 중간값을 복구해 비밀정보를 찾을 수 있다. 딥러닝은 데이터의 특징을 알아서 학습하므로 전통적인 전력

분석공격에 비해 공격자의 분석 능력에 크게 의존하지 않는다.

실제 부채널 정보에는 데이터가 시간축상으로 흐트러지는 현상인 지터가 있거나, 노이즈가 발생하는 문제가 있으므로 데이터의 특성에 맞게 적합한 신경망을 채택하는 것이 중요하다. 데이터의 이동에 민감한 MLP(Multi-Layer Perceptron)의 경우 별도의 전처리를 수행하지 않으면 부채널분석에 활용하기에 적합하지 않다. 반면, CNN(Convolutional Neural Network)은 컨볼루션층과 풀링층의 연산적 특성 덕분에 변동을 감내할 수 있으므로 CNN을 활용하면 지터가 있는 파형을 효과적으로 분석할 수 있다. 따라서 본 논문에서는 CNN을 활용해 지터에 내성을 갖는 신경망을 구성하는 방안을 제안하고 이를 실험적으로 검증한다.

본 논문의 구성은 다음과 같다. 2장에서는 부채널분석과 신경망을 설명하고 3장에서는 지터에 내성을 갖는 신경망 구성 방안을 제안한다. 4장에서는 실험을 통해 제안한 방법을 검증한다. 마지막으로 5장에서 결론을 제시하며 마친다.

2. 관련 연구

2.1 프로파일링 공격

전력분석공격이란 암호 알고리즘이 디바이스에서 동작할 때의 소비전력과 중간값의 관계를 이용하여 비밀정보를 알아내는 공격 방법이다. 프로파일링 기반의 전력분석공격은 공격자가 사전에 공격 대상과 동일하며 비밀키, 평문, 소비전력을 알고 있는 장비를 조작할 수 있다고 가정한다. 프로파일링 공격은 다음과 같이 학습 단계와 공격 단계로 나눌 수 있다.

가. 공격자는 프로파일링 장비의 비밀키를 알고 있으므로 소비전력에 대응되는 중간값을 계산할 수 있다. 이를 통해 신경망이 소비전력을 입력받아 중간값을 예측하도록 학습시킨다.

나. 학습된 신경망을 이용해 공격 대상의 소비전력으로부터 중간값을 계산할 수 있다. 공격자는 평문과 계산한 중간값을 이용해 비밀키를 찾을 수 있다.

예를 들어, AES 암호 알고리즘[3]에 대한 비밀키 복구 방안은 다음과 같다. 중간값을 SubBytes 변환의 출력으로 했을 때, T, M, I, P, K, S 를 각각 소비전력, 신경망, 중간값, 평문, 비밀키, SBox라 하자. 공격자는 T, M, I, P 를 알고 있고 K 를 찾아야 한다. 미리 학습시킨 M 을 이용하면 T 로부터 비밀키와 관련된 중간값 $I = M(T)$ 를 계산할 수 있다. 이때 $I = S[P \oplus K]$ 이므로 공격자는 다음 수식을 이용해 비밀키를 찾을 수 있다.

$$K = S^{-1}[M(T)] \oplus P$$

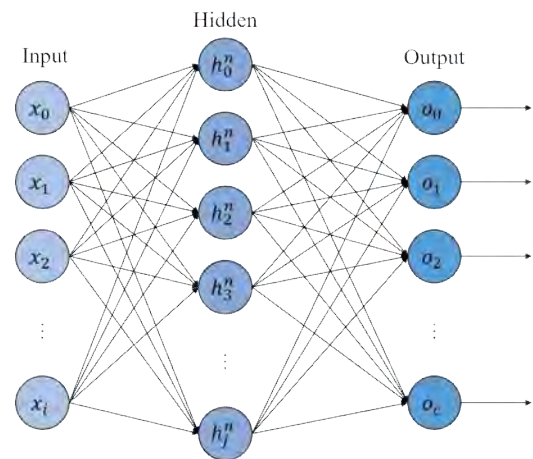
신경망이 잘못된 중간값을 예측할 수 있으므로 여러 파형에 대한 중간값을 예측한 뒤 가장 많이 예측된 키를 비밀키라 추정한다. 이때 신경망의 성능을 측정하기 위해 비율 $ratio$ 를 정의한다.

$$ratio = \frac{(\text{옳은 키의 수})}{(\text{틀린 키 중 가장 많이 나온 키의 수})}$$

분석결과 예측한 키가 비밀키라면 옳은 키의 수가 가장 많아야 하므로 $ratio$ 는 1보다 커야한다.

2.2 Multi-Layer Perceptron

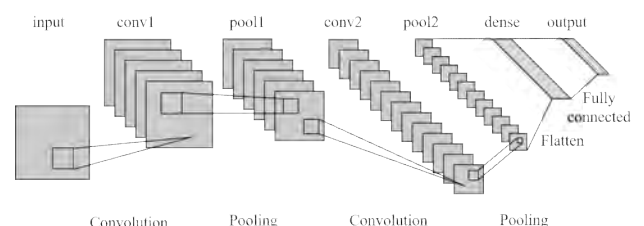
퍼셉트론(Perceptron)이란 인공 신경망의 한 구조로 고차원의 데이터를 입력받아 가중치 벡터를 곱한 후 비선형함수인 활성화 함수를 통과시켜 일차원 데이터를 출력한다[4]. 이러한 퍼셉트론을 여러 개 결합하여 비선형적인 데이터에 대해서도 분류가 가능하도록 하는 Multi-Layer Perceptron(MLP)이 제안되었다[5]. MLP는 (그림 1)과 같이 입력층, 은닉층, 출력층 총 세 가지 계층으로 이루어져 있다. 은닉층에서는 데이터의 특징을 학습한다. 활성화 함수로는 Sigmoid, Tanh, ReLU 등을 사용한다. MLP는 각 벡터의 원소마다 다른 가중치를 곱하므로 특징 벡터의 이동에 민감한 특성이 있다.



(그림 1) MLP의 구조

2.3 Convolutional Neural Network

Convolutional Neural Network(CNN)은 영상처리나 신호처리 분야에서 일반적으로 사용하는 신경망이다[6]. CNN은 (그림 2)와 같이 컨볼루션 연산과 풀링 연산을 이용해 특징 맵을 생성하고 마지막에 완전연결층을 통해 데이터를 분류한다. 컨볼루션 연산은 이동에 동변이고 풀링 연산은 특징 벡터를 압축하므로 MLP와 달리 CNN은 이동에 내성을 갖는다.



(그림 2) CNN의 구조

3. 신경망의 특성에 기반한 지터에 내성을 갖는 신경망 구성 방안

본 절에서는 신경망의 특성을 기반으로 지터가 심한 파형에 내성을 갖는 신경망 설계 방법을 제안한다.

MLP는 특징 벡터의 차원별로 가중치를 가지므로 데이터의 이동이 심하고 데이터가 적으면 데이터의 분포를 제대로 학습할 수 없다. 반면, CNN의 컨볼루션 연산은 이동에 동변이고, 풀링 연산은 특징 벡터를 압축하므로 CNN은 데이터의 이동을 감내할 수 있다. 따라서 CNN을 이용하면 지터가 심한 파형을 다른 신경망에 비해 효과적으로 데이터의 분포를 학습할 수 있다.

컨볼루션 연산과 풀링 연산은 특징 벡터의 이동에 영향을 받지 않지만, 완전연결 층은 특징 벡터의 이동에 영향을 받는다. 따라서 지터에 내성을 갖는 신경망을 구성하기 위해서는 충분히 많은 풀링층을 거치도록 구성해야 한다. 즉, 특징 벡터가 이동하더라도 마지막 풀링층에서는 유사한 특징 벡터가 나오도록 구성해야 한다. 풀링층의 커널의 크기를 p 라 했을 때, 보폭이 커널의 크기와 같다면 풀링층을 한번 거칠 때마다 p 차원 정보가 1차원으로 요약된다. 유사하게 신경망의 층의 수를 l 이라 했을 때, 마지막 풀링 결과 신경망의 입력의 p^l 차원의 정보가 1차원으로 집약된다. 수집된 파형의 위상의 차의 최대값을 z 라 하면, 즉 동일한 데이터와 관련된 파형 정보가 최대 z 포인트 이동한다면, 해당 정보와 관련된 특징 벡터가 마지막 풀링 결과 1차원으로 집약되기 위해서는 수식 (1)과 같은 관계를 만족하도록 신경망을 구성해야 한다.

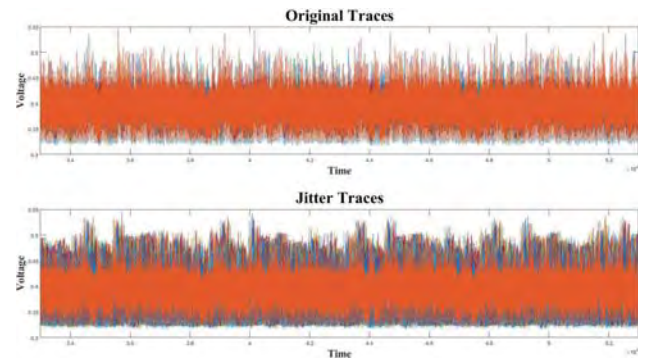
$$p^l > z \Leftrightarrow l > \log_p z \quad \dots (1)$$

4. 실험 결과

본 장에서는 MLP와 CNN을 기반으로 지터가 있는 파형에 대한 프로파일링 분석을 수행한다. 실험은 TrusThings에서 제공하는 공개 데이터셋을 활용했다. 해당 데이터는 AVR ATmega 128 (8-bit 프로세서)에서 부채널 대응기법이 적용되지 않는 AES-128 암호 알고리즘이 동작할 때의 소비전력을 SCARF 전력수집 보드에서 수집한 것이다. 학습을 위한 임의의 키로 암호화를 5,000번 수행할 때의 데이터, 공격을 위한 고정된 키로 암호화를 2,000번 수행할 때의 데이터로 나누어져 있다. 신경망은 Tensor

Flow 2.0.0 버전을 백엔드로 하는 Keras 2.3.1 버전을 이용해 구현하였다.

TrusThings의 파형은 지터가 거의 없는 파형이므로 실험을 위해 임의로 파형의 위치를 변환한다. 우리는 집합 $[-250, 250]$ 에서 균등분포로 임의의 정수를 선택한 뒤, 선택된 정수만큼 파형을 이동시켰다. (그림 3)은 각각 원본 파형과 변환된 파형을 나타낸다.



(그림 3) TrusThings의 원본 파형과 변형된 파형

본 실험에서는 7개의 CNN과 2개의 MLP로 분석한 결과를 비교한다. 실험한 CNN은 신경망의 입력, 컨볼루션 출력, 완전연결층 사이에 배치정규화를 수행한다. 신경망의 컨볼루션층(C), 풀링층(P)의 커널의 수와 완전연결층(FC)의 노드의 수는 다음과 같다.

$$[CNN - 2^i] := C(2^1) - P(2^1) - C(2^2) - P(2^2) - \dots - C(2^i) - P(2^i) - FC(2^9) - FC(2^8) \quad (5 \leq i \leq 11)$$

신경망을 위와 같이 구성한 이유는 모델의 용량을 유사하게 하기 위함이다. CNN의 전체 파라미터 중 대부분은 완전연결층과 관련된 파라미터이므로 모델의 용량을 유사하게 만들기 위해서는 평탄화된 특징 벡터의 차원이 비슷해야 한다. 위의 신경망은 풀링으로 인해 압축되는 비율만큼 커널의 개수가 증가하므로 평탄화된 특징 벡터의 차원이 유사하다.

CNN의 컨볼루션 커널의 크기는 3, 풀링 커널의 크기는 2로 지정했다. 각 $[CNN - 2^i]$ 는 풀링 연산을 i 번 수행하므로 수식 (1)의 $2^i > 500$ 를 만족하려면 i 는 9보다 커야한다.

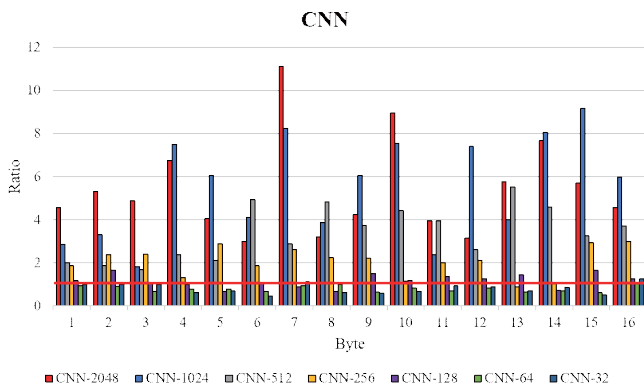
MLP는 신경망의 입력, 완전연결층 출력에 배치정규화를 수행한다. 각 층의 노드의 수는 다음과 같다.

$$[MLP - 0] := 2^{10} - 2^{10} - 2^9 - 2^9 - 2^8 - 2^8 - 2^8 - 2^8$$

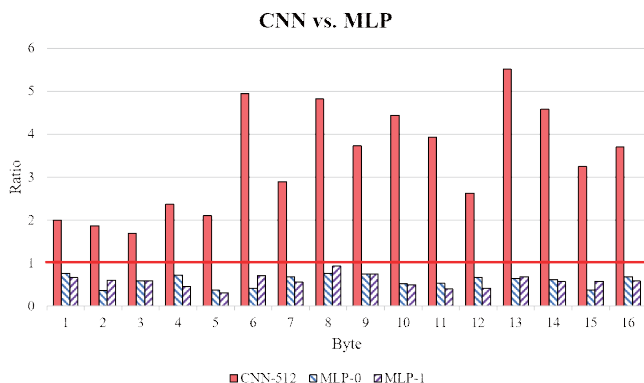
$$[MLP - 1] := 2^9 - 2^9 - 2^9 - 2^9 - 2^8 - 2^8 - 2^8 - 2^8$$

CNN과 MLP는 모두 최적화함수는 Adam, 손실함수는 categorical cross entropy, 활성화함수는 ReLU를 사용하며, 레이블은 바이트별 SubBytes 출력값이다. 데이터는 총 4,500개의 학습파형과 500개의 검증파형을 사용하여 50 에포크만큼 학습했다.

(그림 4)는 CNN의 구조별 *ratio*를 도식화한 것이다. 수식 (1)을 만족하는 신경망 [CNN-2048], [CNN-1024], [CNN-512]는 모든 바이트 키 분석에 성공했지만, [CNN-256]은 16바이트 중 15바이트 비밀키만 복구했고, [CNN-128]은 11바이트, [CNN-64]는 1바이트, CNN-32]는 2바이트 비밀키를 복구했다.



(그림 5)는 수식 (1)을 만족하는 가장 얇은 신경망인 [CNN-512]와 두 구조의 MLP의 *ratio*를 비교한 것이다. 특징 벡터의 이동에 민감한 MLP는 모든 바이트에서 키 분석에 실패했지만, CNN은 전체 비밀키를 복구했다. 이는 데이터의 특성을 기반으로 적합한 신경망을 채택하는 것이 분석의 성공 여부를 결정할 정도로 중요함을 시사한다.



(그림 5) [CNN-512]와 MLP 구조별 실험 결과

5. 결론

본 논문에서는 프로파일링 환경에서 파형이 흔들려서 나타나는 노이즈, 즉 지터가 있는 파형에 대한 효과적인 분석방법을 제안했다. 이를 실험적으로 보이기 위해 다양한 구조의 CNN, MLP로 지터가 있는 파형을 분석한 결과, 제안된 조건을 만족하는 CNN은 모든 바이트 키 분석에 성공했지만, 그렇지 않은 신경망과 MLP는 분석에 실패했다. 따라서 제안된 조건을 이용하면 지터가 있는 파형을 효과적으로 분석할 수 있다.

사사

본 연구는 고려대 암호기술 특화연구센터(UD170109ED)를 통한 방위사업청과 국방과학연구소의 연구비 지원으로 수행되었습니다.

참고문헌

- [1] Kocher, Paul, Joshua Jaffe, and Benjamin Jun. "Differential power analysis." Annual International Cryptology Conference. Springer, Berlin, Heidelberg, 1999.
- [2] Mangard, Stefan, Elisabeth Oswald, and Thomas Popp. Power analysis attacks: Revealing the secrets of smart cards. Vol. 31. Springer Science & Business Media, 2008.
- [3] Brier, Eric, Christophe Clavier, and Francis Olivier. "Correlation power analysis with a leakage model." International workshop on cryptographic hardware and embedded systems. Springer, Berlin, Heidelberg, 2004.
- [4] Rosenblatt, Frank. "The perceptron: a probabilistic model for information storage and organization in the brain." Psychological review 65.6 (1958): 386.
- [5] R. Collobert and S. Benjio, "Links between perceptrons, MLPs and SVMs," Proceedings of the twenty-first international conference on Machine learning, ICML'04, 2004
- [6] O'Shea, Keiron, and Ryan Nash. "An introduction to convolutional neural networks." arXiv preprint arXiv:1511.08458 (2015).

실시간 동영상에서의 인물 선별 송출 시스템

우채운, 박나형, 백지윤, 정유진, 김명주

서울여자대학교 정보보호학과

eogkr2017@daum.net, nhpark326@naver.com, pottery030@naver.com,

yujinj96@naver.com, mjkim@swu.ac.kr

Person Selectable Transmission System in Real-Time Video Conference

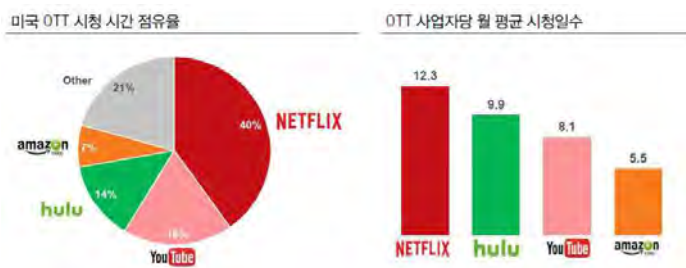
Chae-Yoon Woo, Na-Hyung Park, Ji-Yoon Beak, Yu-Jin Jung, Myuhng-Joo Kim
Dept. of Information Security, Seoul Women's University

요약

본 논문에서는 실시간 얼굴인식 기술을 활용한 인물 선별 송출 시스템을 제안한다. 실시간 동영상 안에 등장하는 다수의 인물 객체 얼굴을 검출하고 인식하기 위해 Haar 특징 정보 기반의 다단계 (Cascade) 학습 알고리즘을 사용한다. 이 시스템은 다수의 인물을 인식하고 학습할 수 있으며 인식된 각 인물의 송출 여부를 사용자가 직접 선택할 수 있는데 이 모든 선택 송출 과정을 실시간으로 처리할 수 있다. 여기에서 제시한 기술은 다자간 화상 채팅이나 다자간 화상 회의에서 특정인의 프라이버시 보호를 위한 기술로 활용될 수 있다.

1. 개발배경

정보통신기술의 발달과 인터넷의 대중화가 이뤄지면서, 개인이 직접 다양한 콘텐츠를 생산 및 공유하는 1인 미디어 사업이 확산되고 있다. 그중에서도 스마트폰이 현대인들의 필수품이 되면서, 스트리밍 방식으로 언제 어디서든 영상 콘텐츠를 볼 수 있는 서비스인 OTT(Over The Top)의 시장 규모가 계속해서 성장하고 있다.



(그림1) 미국 OTT 시장점유율 및 사업자당 월 평균 시청일수(정보통신산업진흥원 디지털콘텐츠산업기획팀, “2017년 CG/VFX 산업 주간 이슈페이퍼 8월호”, p.13, 2017)

하지만 이러한 1인 미디어와 관련된 개인정보 보호에 대한 인식과 규제가 아직 명확하지 않아, (그림 2)와 같이 이에 대한 소비자의 보안위협 및 사생활 침해에 대한 불안함을 가지고 있는 것으로 분석됐다.



(그림2) 디지털 보안 및 프라이버시 안전 수준(DMC MEDIA M.U.D 연구팀, “디지털 미디어 정보 침해에 대한 소비자 보고서”, p.6, 2013)

특히 1인 미디어 플랫폼 중 하나인 실시간 스트리밍 서비스에서의 개인 정보 노출 사고가 문제 되고 있다. 사용자 본인이 아닌 타인의 얼굴이 노출되는 등 초상권 침해에 대한 우려가 커지고 있는 상황이다[1]. 본 논문에서는 Python 3.6, opencv, PyQt5 을 사용하여 실시간 동영상에서의 인물 선별 송출 시스템 프로그램을 구현하였다. 이를 통하여 개인의 프라이버시와 타인의 초상권을 보호해 줄 수 있다. 본 논문에서 구현한 프로그램은 windows 10 (64비트), windows 7 (64비트)에서의 운영환경을 지원하고 있다.

2. 유사 프로그램과의 비교



(그림3) 기존 프로그램과의 비교

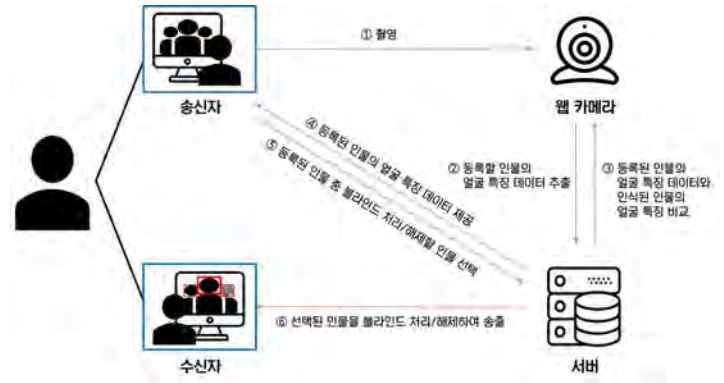
(그림3)은 실시간 스트리밍에서 사용되는 프로그램들을 비교한 것이다. 기존 프로그램들은 실시간 통신 서비스만 제공하는 반면 본 논문에서는 프라이버시 보호에 초점을 맞춰 보안이 강화된 실시간 통신 서비스를 제공한다. 등록된 사용자 이외의 모든 인물을 보이지 않도록 하여 타인의 프라이버시를 보호하고, 사용자에게 객체의 송출 여부를 선택할 수 있도록 하는 자율성을 제공한다. 따라서 본 연구는 사용자에게 자율성을 부여하고 보안 측면을 강조함으로써 기존 프로그램들과 차별성을 제시한다.

3. Haar based Cascade의 활용

실시간 컴퓨터 비전을 목적으로 한 프로그래밍 라이브러리인 OpenCV에서는 Haar Feature를 기반으로 한 Cascade Classifiers를 제공하고 있다. Haar 기능 기반 캐스케이드 분류기를 사용한 객체 탐지는 2001년 Paul Viola와 Michael Jones가 "단순한 기능의 강화된 캐스케이드를 사용한 빠른 객체 탐지"에서 제안한 객체 탐지 방법이다[2].

영역 간의 밝기 차이인 haar 모양의 특징으로 특징값을 계산하고, 적분 영상을 적용한다. 그리고 AdaBoost를 이용하여 약 분류기 중 물체 검출에 크게 기여하는 강 분류기를 만들고, 여러 개의 강 분류기를 사용하여 Cascade 구조로 구성한다. 그리고 조건에 만족하는 이미지를 분류하여 조건에 맞지 않을 경우 버리고, 조건이 맞다면 다음 조건으로 넘어간 뒤 최종 검출로 출력한다[3]. 검출기 분류를 통하여 검색 속도를 향상시킬 수 있는 장점을 제공한다. 본 논문에서는 이상에서 제시한 내용을 포함하여 구현을 진행하였다.

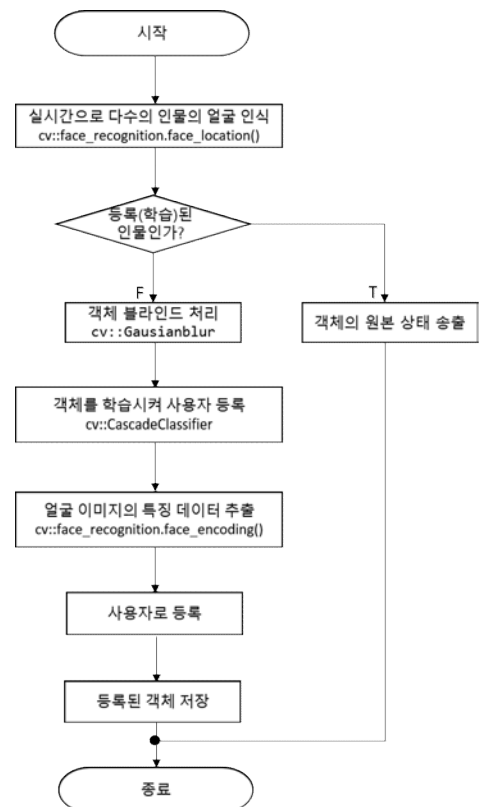
4. 시스템 구성도



(그림4) 시스템 구성도

본 논문에서 개발한 프로그램의 사용자는 (그림4)가 보여주는 것과 같이 송신자 역할과 수신자 역할을 모두 할 수 있다. 송신자는 웹캠으로 촬영 중인 영상에서 송출할 인물 객체를 선택적으로 등록할 수 있으며 이 기능은 서버에서 실행된다. 서버는 등록된 인물 객체의 데이터를 송신자에게 반환하며, 등록된 객체 중 송신자가 선택한 객체를 블라인드 또는 해제 처리한다. 수신자는 서버에서 처리된 영상을 수신한다.

5. 얼굴인식 과정



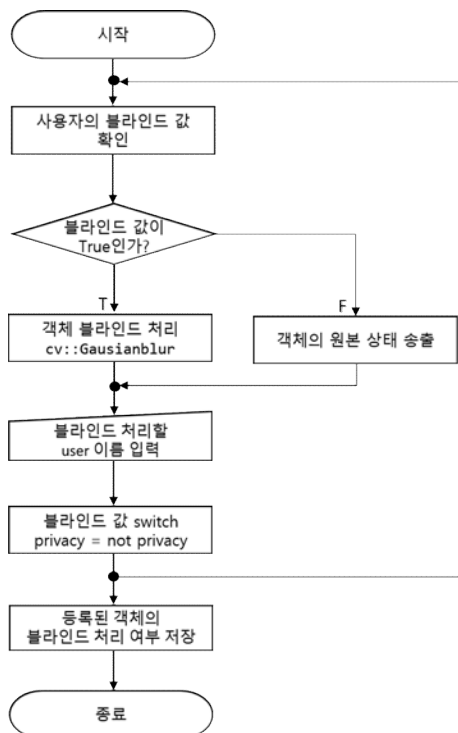
(그림5) 얼굴인식 및 학습 알고리즘

얼굴인식 및 학습 과정은 (그림5)와 같이 진행된다. 먼저 프로그램이 실행되면 OpenCV에서 제공하는 cv::face_recognition 클래스의 face_location 메서드를 사용하여 카메라 촬영 영상 frame에서 얼굴 영역과 특징을 추출한다.

다음으로 cv::face_recognition 클래스의 distance 메서드를 사용하여 frame에서 추출한 얼굴 특징을 기존에 등록(학습)된 얼굴 특징과 비교하여 거리 척도를 환산한다. 거리가 0.6 이하일 시 동일 인물로 인식하여 원본 상태의 frame을 송출하며, 등록된 인물이 아닐 시 해당 인물을 블라인드 처리하여 송출한다.

haarcascade 방식으로 cv::CascadeClassifier 메서드를 이용하여 객체의 얼굴 영역을 식별하며 cv::face_recognition.encoding 메서드로 식별된 얼굴 영역에서 68개의 얼굴 특징 위치를 분석하여 데이터로 추출한다. 추출된 데이터는 등록된 객체의 정보로 저장된다.

6. 블라인드 처리 과정



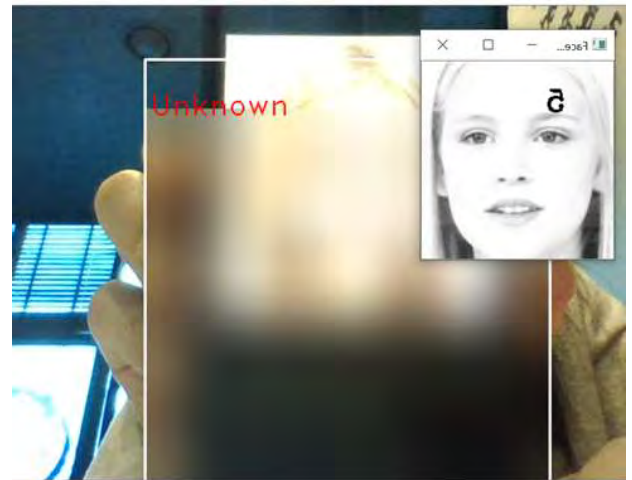
(그림6) 블라인드 처리 알고리즘

인식된 객체에 대한 블라인드 처리 과정은 (그림6)과 같이 진행된다. cv::rectangle 메서드를 이용하여 인식된 객체의 얼굴에 박스를 그리고 사용자가 등록된(학습된) 객체의 블라인드 처리 여부를 결정한다. cv::Gaussianblur 메서드로 해당 객체의 박스를 블라

인드 처리 또는 해제한다. 등록된 사용자에 대한 블라인드 값은 기본적으로 False로 되어있어, 사용자의 원본 상태를 출력한다. 이때, 사용자가 블라인드 처리하고 싶은 사용자의 이름을 입력하면 해당 사용자의 블라인드 값을 True로 전환시킨다. 사용자가 블라인드 처리 및 해제를 적용하고 싶을 때마다 이와 같은 과정을 반복한다.

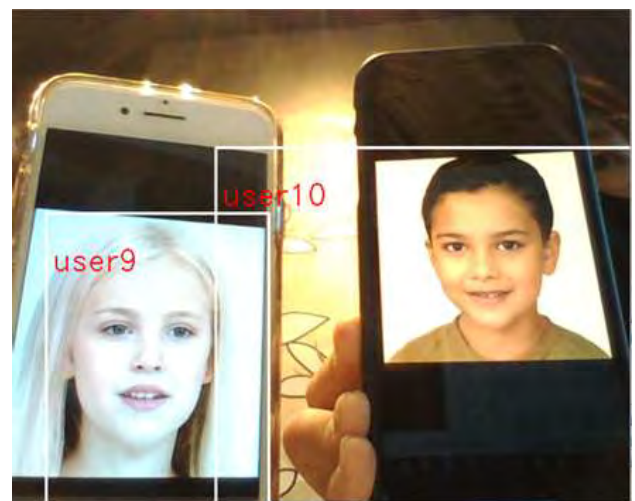
7. 실행 결과

각 얼굴 사진은 Generated Photos 사이트에서 제공하는 무료 AI 생성 인물사진을 활용했다[4].



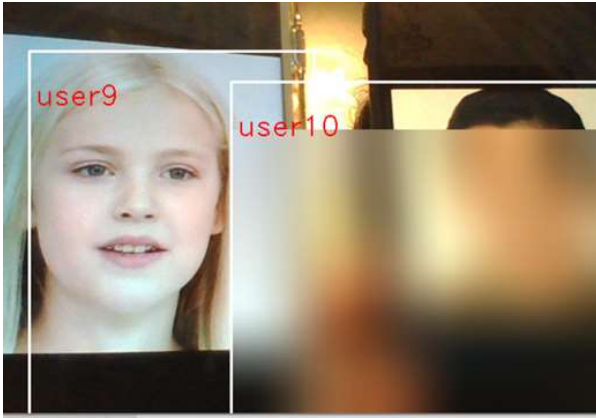
(그림7) 인물 학습 모듈

(그림7)은 학습되지 않은 인물을 학습하는 과정이다. 새로운 인물의 사진을 학습하여 사용자로 인식시킨다.



(그림8) 다수 객체 인식 모듈

(그림8)은 동시에 다수의 객체를 각각 다른 인물로 인식하는 것을 확인할 수 있다.



(그림9) 개별 블라인드 모듈

(그림9)에서와 같이 인식된 사용자 각각을 구별하고, 사용자의 송출 여부 선택에 따라 송출되지 않는 인물은 블라인드 처리가 적용된다.

8. 보안 요소

1) 사용자 프라이버시 보호

프로그램이 처음 실행될 때 사용자의 얼굴을 학습하여 등록한다. 등록된 사용자만 보여주고, 등록되지 않으면 모두 블라인드 처리해 송출한다. 이로써 별도 처리 과정 없이 타인의 얼굴이 노출되는 것을 방지한다. 만약 등록되지 않은 사용자의 얼굴을 송출하고 싶다면 이를 등록하고 송출한다. 등록된 인물의 얼굴 송출 여부는 사용자가 변환할 수 있다. 이처럼 등록되지 않은 객체는 모두 블라인드 처리하고, 등록된 객체의 블라인드 여부를 결정하게 하여 사람들의 프라이버시를 보호한다. 또한, 학습된 얼굴 데이터는 프로그램이 종료될 때 삭제하여 개인 정보를 파기한다.

2) 암호화 통신

Frame을 jpg 이미지로 인코딩을 한 후 raw images를 통해 연속적으로 반환시켜서 다른 사용자에게 프레임을 송출한다. raw images를 보낼 때, 암호화 과정을 거쳐서 영상을 송출한다. 따라서 수신자는 영상을 수신할 때, 복호화 과정을 거친 후 프레임을 볼 수 있다. 실시간으로 통신을 해야 하므로 상대적으로 속도가 빠른 AES256 알고리즘을 사용했다. 시스템 상에 임의로 key 값을 설정한다. 송신자는 raw images를 시스템 상 정의되어있는 비밀키로 암호화하여 수신자에게 실시간으로 보낸다. 수신자 역시 시스템 상에 정의되어있는 비밀키로 복호화하여 실시간으로 동영상을 수신한다.

9. 기대 효과

본 논문에서는 실시간으로 송출해야 할 얼굴을 사용자가 직접 선별함에 따라 사용자들에게는 개인의 프라이버시를 보장해주며, 타인의 초상권 또한 보호해 주는 시스템을 제안하였다. 이를 통해 시스템 카메라 화면에 들어오는 모든 사람의 개인정보를 보호하는 핵심 기술로 자리 잡을 수 있다. 또한, 이 기술을 사용하면 스트리밍 서비스 등에서 타인의 초상권 보호를 위한 별도의 영상 편집 과정을 거치지 않아도 되므로 경제적으로 인적 자원 비용이 절감되는 기대효과를 제공한다.

영상 콘텐츠 시장이 점점 확대되고 있는 1인 미디어 시장뿐 아니라 화상 회의, 방송 영상 등 다양한 분야로의 발전 가능성이 무한하다고 볼 수 있다. 원하는 객체를 선별적으로 송출해야 하는 사람들을 대상으로 선제적인 시장 창출을 할 수 있을 것이라 예상된다.

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 SW중심대학지원사업의 연구결과로 수행되었음(2016-0-00022)

참고문헌

- [1] “노숙인도 방송소재 삼는 1인 미디어들…서울시 “초상권 침해는 범죄”, 스포츠경향. 2019년 3월 5일 수정, 2020년 4월 7일 접속, http://m.sports.khan.co.kr/view.html?art_id=201903050831003&sec_id=561101#c2b.
- [2] opencv, 2019, https://docs.opencv.org/4.1.0/d7/d8b/tutorial_py_face_detection.html
- [3] 유제훈, 심귀보, Cascade 안면 검출기와 컨볼루션 신경망을 이용한 얼굴 분류, 한국지능시스템학회 논문지, 26(1), 70-75. (2016).
- [4] “Generated Photos”, 2020년 5월 9일 접속, <https://generated.photos/faces>

원자력시설의 무선통신 사이버보안을 위한 접근통제 방안 연구

김상우*

*한국원자력통제기술원

kjoey@kinac.re.kr

A Study on Access Control for Wireless Communication at Nuclear Facilities

Sangwoo Kim*

*Dept. of Nuclear Security, Korea Institute of Nuclear Non-proliferation And Control

요 약

최근 4차 산업혁명과 더불어 센서 네트워크와 같은 최신 무선통신 기술들의 기반시설 적용을 위한 연구들이 활발하게 이루어지고 있다. 원자력시설 또한, 보안 및 비상대응 시스템에 무선통신을 적용하기 위한 연구들이 진행되고 있으며, 미국과 UAE의 경우 이미 원자력시설에 무선통신을 적용하여 사용하고 있다. 그러나 무선통신의 경우, 물리적인 네트워크 접근 경로가 존재하지 않기 때문에 통신 경로에 대한 접근통제가 불가능하며 광범위한 지역에 네트워크를 설치하는 경우 중계 단말 수량의 증가로 인한 접근통제 취약점이 발생할 가능성이 있다. 이와 같은 무선통신의 특성 때문에 원자력시설의 필수디지털자산에 무선 네트워크를 적용 시 현재의 통신 경로 접근통제 등의 유선 통신을 기준으로 작성된 접근통제 규제기준으로는 무선통신에 대한 접근통제를 이행하기에는 부족함이 있다. 이에 본 논문에서는 무선 네트워크 접근통제를 위한 규제 기준 개선안을 제시한다.

1. 서론

최근 4차 산업혁명이 이슈화됨에 따라 기반시설에도 주파수 통신을 활용하는 센서 네트워크와 같은 최신 기술을 도입하기 위한 연구들이 활발하게 이루어지고 있다. 원자력시설 또한, 무선통신 적용을 통해 비용 절감 및 효율 극대화를 위한 노력들이 지속적으로 이루어지고 있으며, 실제 미국의 경우 원자력발전소의 비상대응, 비안전 시스템 등에 무선통신을 활용하고 있다[1, 2, 3]. 국내 원자력시설의 필수디지털자산에 무선통신을 적용하기 위해서는 원자력시설의 컴퓨터 및 정보시스템 보안 기준인 KINAC/RS-015에 따라 디지털자산에 대한 기술적·운영적·관리적 보안조치를 반드시 수행해야 한다[4]. 그러나 무선 주파수를 대기 중으로 방사하는 무선통신의 특성 상 규제기준에서 요구하는 통신경로 접근통제, 네트워크 접근통제의 수행이 불가능하다. 이에 본 논문에서는 무선통신의 특성을 고려한 원자력시설 무선통신 장비에 대한 접근통제 규제 요건을 제안한다.

2. 국내 규제 기준 현황

국내 원자력시설의 필수디지털자산은 KINAC/RS-015에 따른 기술적·운영적·관리적 보안조치를 적용해야 한다. 기술적 보안조치에서는 원자력시설에 대한 무선통신 사용은 원칙적으로 금지하고 있으나, 필요시 보안성 평가 및 규제기관의 승인 후 사용하도록 하고 있다. 네트워크를 사용하는 필수디지털자산들은 반드시 기술적보안조치인 네트워크 접근통제와 운영적 보안조치인 통신경로 접근통제를 적용해야 한다. 그러나 운영적 보안조치의 통신경로 접근통제의 경우, 물리적 형태가 존재하는 유선 통신을 기준으로 작성되어 무선 네트워크를 사용하는 장치에는 해당 보안조치를 적용하기 어렵다. 네트워크 접근통제 또한 망 분리를 통해 원격에서 네트워크의 물리계층에 접근하는 것이 불가능한 상태를 기본 전제로 하고 있기 때문에 현재 명시된 보안조치 만으로는 원자력시설의 무선통신에 대한 규제에 활용하기에는 부족함이 있다[5].

3. 원자력시설 무선통신 접근통제 규제 기준 제안

2장에서 제시한 현재 규제기준의 무선통신 적용시 발생 가능한 문제점을 해결하기 위해 본 논문에서는 기존의 규제기준 일부 항목을 수정/보완한 원자력시설의 무선통신을 위한 접근통제 규제 기준을 제안한다.

<표 1> 무선통신 네트워크 접근통제 규제기준 제안

네트워크 접근통제	
기존	원자력사업자는 다음이 수행되도록 보장한다. 가) MAC(Media Access Control) 주소 잠금 나) 물리적 혹은 논리적 네트워크 분리 다) 정적 테이블 주소 유지 라) 패스워드 등 중요정보 전송 시, 암호화 마) 모니터링
추가 항목	바) 네트워크 장비 및 무선통신 장치는 초기에 서로를 식별하고 인증하여야 함 사) 무선 네트워크 구성 이전에 접근통제를 위해 허용 가능한 기기 목록을 작성 및 보유 아) 무선 네트워크 구성 이전에 접근통제를 위해 인가된 주파수 호핑 알고리즘 및 네트워크 ID 사용 자) 무선통신 시스템 설계 및 설치 시 무선 네트워크 접근통제 정책의 미적용 구간이 발생하지 않도록 장치의 설치 위치 및 개수 등을 지정하고 문서화

표 1은 기존 KINAC/RS-015에 존재하는 원자력시설의 필수디지털자산을 위한 네트워크 접근통제 규제기준에 무선통신 네트워크에 대한 접근통제를 위한 항목을 추가한 것이다. 무선통신 네트워크의 주파수가 방사되는 대기에 대한 접근통제는 불가능함으로 우선 주파수 접근 후 실제 네트워크 통신 사용하기 전의 인증 과정을 추가하여야 한다. 또한 네트워크 활용 시 쉽게 구입이 가능한 상용기기로 쉽게 접근이 불가능하도록 특화된 주파수 호핑 알고리즘 또는 네트워크 식별자를 통해 비인가 장비의 네트워크 접근을 통제해야 한다.

<표 2> 무선통신 통신경로 접근통제 규제기준 제안

통신 경로 접근통제	
기존	원자력사업자는 필수디지털자산 통신케이블 및 장비에 대한 물리적 접근을 통제하고 문서화하여야 한다.
신규	원자력사업자는 무선통신 사용 시 방호구역 외부에서는 통신 접근이 불가능 하도록 주파수 범위 및 중계기 설치 구역을 제한하고 문서화해야 한다.

표 2는 기존 KINAC/RS-015의 통신 경로 접근통제 항목과 무선통신을 위한 신규 규제 항목이다.

기존 규제기준은 표 2와 같이 통신케이블이 존재하는 유선 통신을 대상으로 적용 가능한 기준이기 때문에 유선통신에는 적용이 불가능 하다. 이에 상기 규제 기준에 준하는 무선 통신 네트워크의 물리적 계층에 대한 접근을 통제하기 위해 위와 같은 신규 항목을 제시하였다.



(그림 1) 무선통신 통신 경로 접근통제 적용 예시

본 논문에서 제시하는 무선통신 통신경로 접근통제를 적용할 경우 그림 1과 같이 무선통신 범위는 방호 구역 내부로 한정될 것이다. 방호 구역은 원자력시설의 물리적방호 규정에 따라 기본적인 물리적 접근통제가 이루어지고 있으며, 이에 따라 무선통신 경로에 대한 접근통제를 만족할 수 있다.

4. 결론

최근 원자력시설의 무선통신 사용 요구 및 연구가 증가함에 따라 사이버보안 규제에 대한 필요성도 증가하고 있다. 이에 본 논문에서는 현재의 원자력시설에 대한 사이버보안 규제기준에 따른 보안조치를 무선통신 장치에 적용하였을 경우 접근통제와 관련하여 발생 가능한 문제점을 도출하였다. 도출된 문제점을 해결하고자 네트워크 접근통제를 위한 추가 항목과 무선통신 경로 접근통제를 위한 신규 항목을 제안하였다. 본 연구는 원자력시설에 무선통신을 적용하고자 하는 연구자들과 규제기준을 개발하고자 하는 규제자를 위한 선행 연구로 활용이 가능하다. 또한, 상기 항목들이 실제 규제 기준에 반영 될 경우, 원자력시설의 무선통신 설치로 인해 발생 가능한 신규 공격 경로에 대한 접근통제를 기대할 수 있다.

참고문헌

- [1] 고도영, 이재곤, 임재현 & 김만우. "원전 기기상 태감시 무선기술 적용 타당성 조사". 대한기계학회 춘추학술대회(2017)
- [2] Deng, Zhiguang, et al. "Application Analysis of Wireless Sensor Networks in Nuclear Power Plant." International Symposium on Software Reliability, Industrial Safety, Cyber Security and Physical Protection for Nuclear Power Plant. Springer, Singapore, 2019.
- [3] Electric Power Research Institute, "implementation guideline for wireless networks and wireless equipment condition monitoring", 2009, TR1019186.
- [4] 송동훈, et al. "원자력시설 사이버보안 강화를 위한 관리적 보안조치 검증 방법론 연구." 한국통신학회 학술대회논문집 (2018): 1048-1049.
- [5] KINAC/RS-015, "원자력시설의 컴퓨터 및 정보시스템 보안", 2016

대학생들을 위한 블록체인 기반의 신뢰성 있는 중고 책 거래 플랫폼 구현

김윤채, 이지혜, 조운재, 김명주

서울여자대학교 정보보호학과

somniumseio128@gmail.com, sugarden98@gmail.com, ynj3126@swu.ac.kr

Implementation of Blockchain-based Used-Book Trading Platform for College Students

Yoon-Chae Kim, Ji-Hye Lee, Yoon-Jae Jo, Myuhng-Joo Kim

Dept. of Information Security, Seoul Women's University

요 약

본 연구에서는 안전하면서도 쉽게 사용할 수 있는 블록체인 기반의 중고 책 거래 플랫폼을 개발하였다. 이 플랫폼은 블록체인의 특성을 이용해 거래 제품 및 거래내역을 공유원장에 기록하여 거래 내역을 투명하게 공개하며 누구나 열람 가능하다. 이는 데이터의 무결성과 투명성을 보장하며 신뢰성 있는 거래 환경을 제공한다. 이를 사용할 경우, 기존 중고거래 시스템에서 발생 가능한 데이터의 위조, 변조의 문제점과 불확실한 신뢰 문제가 해결되어 중고거래 사기사건을 예방할 수 있다.

1. 제작 배경

국내에서 인터넷을 통한 중고거래시장의 규모는 갈수록 커지고 있다[1]. 이와 비례하여 허위매물과 반복적인 중고거래로 인한 사기 사건들이 점점 늘어나고 있다[2].

이러한 문제점을 해결하기 위해서 보다 안전한 거래를 할 수 있는 중고거래 플랫폼이 필요하다고 판단된다. 이러한 사기사건이 발생하는 이유는 판매자 본인의 게시글 관리를 자유롭게 할 수 있기 때문인데 이 문제는 블록체인 기술을 이용하면 위조, 변조가 불가능해져서 해결이 가능해진다. 또한 블록체인 기술의 특징인 분산형 데이터 저장기술[3]을 활용한다면 삭제가 불가능하기 때문에 발생하는 중고거래 사기사건을 줄일 수 있다.

블록체인 기술은 신뢰할 수 있는 제 3자인 중개인이 없는 상황에서도 금융거래를 가능하게 해주는 특징을 갖는다. 이 기술은 다수의 개인 간 합의과정을 통해 데이터를 검증하고, 검증된 내용은 블록체인 구조의 장부에 저장하는 방식으로 중개인의 역할을 대체한다[2].

따라서 블록체인을 이용한 중고거래 플랫폼에서는 중간매체 없이 간편하게 판매자와 구매자가 안전하게 거래할 수 있게 된다[2][3].



(그림 2) 최근 1년간 중고거래 제품

본 연구에서는 허위매물과 중고거래 사기를 미연에 방지하기 위해서 블록체인의 복잡하면서도 다양한 서비스들을 간단하면서도 안전하게 사용할 수 있는 웹사이트를 구현하였다.

2. 유사 앱들의 비교



(그림 3) 주요 중고거래 앱 사용자 현황

(그림 3)은 앱 시장에서 나온 기존 앱들 중에서 주요 중고거래 앱 사용자 현황을 비교한 것이다[5]. 3 위를 차지한 네이버 카페 ‘중고나라가 가장 먼저 출시되었지만, 허위 매물이나 반복적인 거래 사기가 빈번하게 일어나 중고나라보다는 조금 비싸도 새로운 방법을 택한 소비자들이 많았다.

주요 중고거래 앱 사용자 현황에서 1 위는 ‘당근마켓이 331 만으로 사용자가 161% 증가했다[5]. 기존 앱인 중고나라보다 더 늦게 출시된 당근마켓은 등록 수수료가 없는 대신 최대 6 km 내의 이용자끼리 거래할 수 있다.

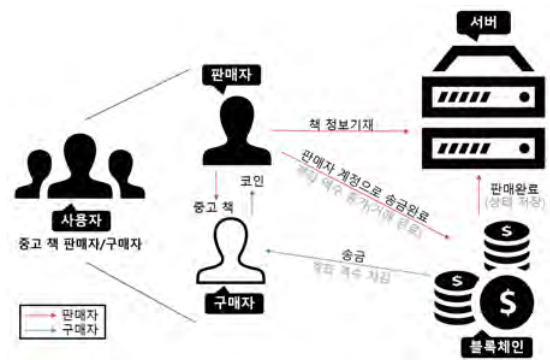
서울처럼 거래 매물이 많이 올라오는 지역은 3~4 km 반경으로 거래를 제한했다. 이용자는 자신의 주거 지역을 휴대전화로 인증해야만 가입할 수 있다. 덕분에 택배대신 만나서 거래를 하게 된다. 길가다 지하 철에서 마주칠 수 있을 정도로 가까운 거리에 사는 사람들 간의 거래이다 보니 사기 거래일 가능성도 낮아지는 효과가 있다.

이상과 같은 유사 앱들의 특징들을 참고하여 본 연구에서는 사용자가 구매자와 판매자 중에서 선택함으로써 구매자일 때는 서버에 정보를 저장해 웹페이지에 해당 정보를 송수신할 수 있도록 한다.

판매자일 때는 웹페이지에 원하는 정보를 선택해서 가까운 지역내에서만 직접 거래를 할 수 있도록 설정한다. 뿐만 아니라 구매자와 판매자가 거래를 직접 제어할 수 있도록 채팅이나 게시판, 댓글 기능들을 제공한다.

아울러 이러한 거래 서비스가 안전하게 운영되도록 블록체인 기술을 이용한 보안 기능을 제공해서 웹사이트를 설계하였다.

3. 시스템 구성도

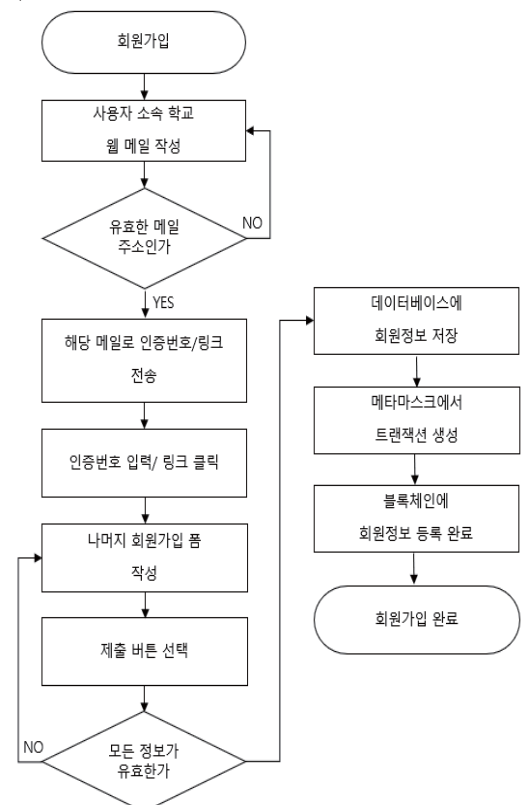


(그림 4) 시스템 구성도

본 연구에서 개발한 웹사이트의 사용자는 (그림 4)가 보여주는 것과 같이 구매자 역할과 판매자 역할을 모두 할 수 있다. 판매자는 서버에 본인이 판매하려는 중고 책 정보를 등록할 수 있으며 이러한 기능은 서버로부터 부여 받는다. 구매자는 앞서 등록되어있는 책을 구매함으로써 메타마스크를 통해 송금 서비스를 받게 된다.

4. 회원가입과 로그인

이 앱은 대학생들 사용대상으로 하기에 대학생임을 입증할 수 있는 소속 학교 웹메일을 인증 방식으로 채택했다.



(그림 5) 회원가입을 통해 데이터베이스 및 블록체인에 회원 정보를 등록하는 과정

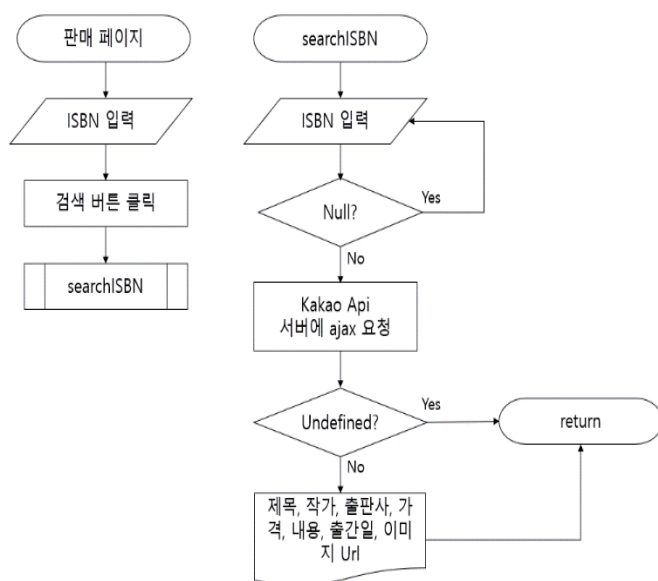
회원이 가입 시, 가장 먼저 소속 학교의 웹메일을 작성해야 하며 해당 웹메일로 전송된 인증번호를 입력하거나 인증링크를 클릭해야 인증이 완료된다. (그림 5)는 회원가입 절차를 거쳐 데이터베이스 및 블록체인에 회원 정보를 등록하는 과정을 나타낸다. 인증이 완료되면 이중가입 및 범죄 예방을 위하여 이름, 소속학교 등 중요정보가 자동완성 되고, 나머지 칸은 사용자가 직접입력 하도록 한다. 가입이 완료되면 회원 정보(이메일, 이름, 패스워드, 학교, 학과 등)가 데이터베이스에 저장된다. 데이터베이스에 회원정보를 저장하는데 그치지 않고 블록체인에 회원정보를 저장함으로써 이중가입이나 사기이력이 존재하는 회원의 재가입 방지에 효과적일 것으로 예상된다. 따라서, 회원정보를 기존에 작성해둔 회원관리 스마트 컨트랙트에 저장하기 위해서 메타마스크를 활성화시키고 트랜잭션을 생성해 회원정보를 블록체인에 저장한다[6].

웹사이트의 로그인 버튼을 누르면 로그인 화면으로 넘어가고 회원 정보를 입력한다. 로그인 화면에서 회원가입을 누르면 회원가입 창으로 넘어간다. 만약 회원가입 하지 않고 회원정보(ID, PW)를 입력하면 데이터베이스 안의 데이터 비교해 ID와 PW가 맞는지 판별한다. 데이터가 일치한다면 해당 ID의 회원 정보를 화면에 띄워준다.

5. 판매

판매 페이지에서 판매하고자 하는 책의 정보를 폼 형식으로 입력하고 게시물을 등록할 수 있다. 본 절에서는 판매 절차로서 게시물 등록 과정을 구체적으로 살펴본다.

5.1. ISBN 검색



(그림 6) isbn 검색을 통한 품 자동 입력 과정

본 연구에서는 isbn, 책 제목, 정가, 판매가, 작가, 출판사, 출간일, 내용, 상태, 사진 정보를 모두 기입해야 하는 일련의 과정을 단순화하기 위해 ISBN 검색 기능을 도입한다.

(그림 6)는 사용자가 ISBN 검색 기능을 이용하여 품의 일부 정보를 자동 입력하는 과정을 보여준다. 판매할 책의 ISBN을 입력한 후 검색 버튼을 클릭하면 searchISBN 함수가 호출된다. 해당 함수는 실질적으로 Kakao Rest API를 통해 ISBN으로 책을 검색하고 정보를 받아오는 기능을 수행한다. 함수가 호출되면 입력된 내용이 Null인지 점검하고, Null이 아니면 Kakao API 서버에 ISBN을 질의어로 하는 비동기 요청을 보내 해당 책의 정보를 받아온다. 응답 바디는 meta, documents로 구성된 JSON 객체이다[7].

사용하고자 하는 실질적인 데이터는 result.documents[0]에 존재하는데, 만약 올바르게 않은 ISBN을 입력하는 경우 이 데이터의 값이 'undefined'이 되므로 함수를 리턴하고 위 과정을 다시 처음부터 진행한다. 올바른 ISBN을 입력한다면 책 제목, 작가, 출판사, 가격, 내용, 출간일, 이미지 URL 필드가 자동으로 입력된다.

따라서 사용자는 2개의 필드만 입력하면 되기 때문에 보다 쉽게 게시물을 등록할 수 있다.

5.2. 게시물 등록

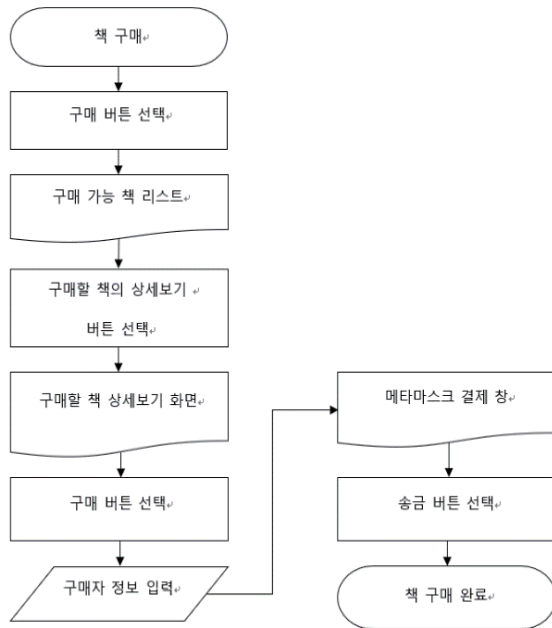
판매 페이지에서 모든 필드에 대해 입력을 완료했다면 등록 버튼을 눌러 게시물을 데이터베이스에 업로드할 수 있다. Form에 입력된 책 정보들과 0부터 시작되는 index 값을 DB에 저장하게 된다. index 값은 책이 하나 등록될 때마다 1씩 증가하며, 해당 책의 구매자 정보를 저장하고 불러올 때 사용하게 된다.

본 연구에서는 몽고 DB를 이용하여 웹서비스를 구현한다. 몽고 DB는 기존 RDBMS의 행 개념 대신 문서를 사용한다는 의미로 최근 빅 데이터 처리에 사용되는 유연한 데이터 처리 모델이다. 스키마 없이 동작하며 구조에 대한 정의도 변경을 필요로 하지 않으며 레코드에 자유롭게 필드 추가가 가능하다[7].

또한 몽고 DB는 사전에 정의된 스키마와 관계없이 임의의 JSON Document 형태로 레코드를 DB에 삽입할 수 있어, 데이터를 모델링하고 모델을 변경하기 용이하다[8]. 관계형 데이터베이스와 달리 테이블이 미리 정해진 고정된 스키마를 가지고 있지 않지만 모델을 정의할 때 Schema 메서드를 이용하면 관계형 데이터베이스와 같이 Key-Value 형태의 스키마 형태로 데이터를 운용할 수 있다.

따라서 본 연구에서는 폼 형식이 고정되어 있는 게시물의 성격에 맞게 스키마 형태로 모델을 정의하고 데이터를 관리한다.

6. 구매



(그림 7) 메타마스크를 통한 책 구매 과정

(그림 7)은 판매절차를 거쳐 등록된 책들 중 원하는 책을 구매하는 과정이다. 메인 화면에서 구매 버튼을 클릭 시, front-end에서는 ajax 함수를 통해 서버에 데이터베이스에 저장된 책 리스트를 요청하고, 서버는 라우팅 함수를 통해 데이터 베이스에 접근한다. 서버는 response 로서 얻은 리스트를 JSON 형태로 front-end에 전달하고 이를 사용자가 front-end 상에서 리스트로 확인할 수 있다. 구매자가 원하는 책을 선택 후, 상세보기 버튼을 클릭하면 데이터베이스에 저장된 해당 책의 판매가, 상태 등의 상세정보를 확인할 수 있다. 상세정보를 확인 후, 구매 버튼을 클릭하면 web3.js 를 통해 해당 계정(구매자-판매자) 주소, 결제 금액, 해당 책의 index 값을 얻을 수 있으며 송금 계좌와 금액이 입력된 메타마스크 결제창이 활성화된다[9]. 결제 주소와 결제 금액(ether)은 구매자가 임의로 변경 불가하며 가스 비용만 별도 조정이 가능하다. 송금이 완료되면 solidity 코드 상에 구현한 구매자 배열의 해당 index 위치에 구매자 정보(계좌, 이메일)가 저장되며, 서버에서 구매자 배열에 접근할 수 있다. 이후, 해당 책의 중복구매를 막기 위하여 구매자 배열에 구매자 정보가 존재하는지 확인한 다음, 구매버튼을 선택 불가하도록 하고 해당 책의 구매자 정보를 언제든지 확인할 수 있도록 구매 페이지 GUI를 업데이트 한다.

7. 기대효과

본 연구에서 제시했듯이 중고 책 거래 플랫폼에 공공 거래 장부 기술인 블록체인을 도입함으로써 여러 가지 효과들을 기대할 수 있다.

고유 해시 값을 포함한 모든 회원 정보가 원장에 분산, 공개되어 무결성이 유지되고 관리에 용이하며 특

정 회원의 사기 이력 등을 비교적 손쉽게 확인할 수 있다. 회원 정보와 더불어 모든 거래 내역 또한 투명하게 공개되므로 서비스에 대한 신뢰도가 향상되고, 추후 문제가 발생했을 때 거래 사실을 입증하는 과정이 간단 해진다. 특히 메타마스크를 통해 거래를 진행하면 계좌번호 및 이름과 같은 신상 정보를 공개할 필요가 없어 사용자 측면에서 보다 안전하게 서비스를 이용할 수 있다. 물론 이를 원하지 않는 경우 현금 결제를 선택하여 거래를 진행하면 된다.

본 연구에서 제시한 플랫폼은 대학생들을 대상으로 한 중고 책 거래를 염두에 두고 개발된 것이지만, 일반적인 거래로 확장될 수 있다. 이 경우 블록체인 기반의 신뢰가능한 거래 플랫폼으로 활용될 수 있다.

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 SW중심대학지원사업의 연구결과로 수행되었음(2016-0-00022)

참고문헌

- [1] 박유진, 이보성, 김범수, 이애리. (2017). 온라인 중고물품 재구매의도 영향요인 분석: “중고나라” 사이트를 중심으로. e-비즈니스연구, 18(1), 123-140.
- [2] 이경남, 전계형, 블록체인을 이용한 중고거래 플랫폼 개선방안 연구, 한국디지털정책학회 2018
- [3] 다고모리 테루히로 “엔지니어를 위한 블록체인 프로그래밍: 이더리움 기반 신뢰성 높은 스마트 계약 개발하기”
- [4] 한국리서치, 컨슈머 리포트, “중고나라의 사람들” (2018)
- [5] 앱/리테일 분석서비스 와이즈앱/와이즈리테일 (2019.10) 전국 40,000 명의 안드로이드 스마트폰 사용자 표본조사
- [6] 최낙훈, 김희열, “메타마스크와 연동한 블록체인 기반 사용자 인증모델”, 인터넷정보학회논문지, 제 20 권, 제 6 호, pp. 119-127, 2019
- [7] 김현주. (2014). 몽고 DB를 이용한 웹 서비스 데이터 처리. 한국산학기술학회 학술대회논문집, (), 233-236.
- [8] 윤중성, 정두원, 강철훈, 이상진. (2014). MongoDB에 대한 디지털 포렌식 조사 기법 연구. 정보보호학회논문지, 24(1), 123-134.
- [9] 조원삼, 최준혁, 황해인, 안병구, “블록체인을 이용한 중고거래 시스템”, 한국통신학회 학술대회논문집, pp. 481-482, 2019

FSR Array 마우스 패드를 이용한 사용자 인증 시스템

권승호*, 김태연*, 서승현*
한양대학교 ERICA 전자공학부
rnjs9232@hanyang.ac.kr, kty24898@hanyang.ac.kr

User Authentication System using FSR Array Mouse Pad

Seung-Ho Gwon*, Tae-Yeon Kim*, Seung-Hyun Seo*

*Division of Electrical Engineering, Hanyang University ERICA Campus

요 약

현재 PC 환경에 대한 보안시스템은 PIN 번호 인증 방식과 지문, 홍채와 같은 생체정보 인증방식에 머물러 있다. 하지만 취약한 PIN 번호는 도용이 쉽고, 생체정보는 누출되었을 경우 갱신이 불가능하다는 단점을 가지고 있어 이를 악용한 해킹 사례가 발생하고 있다. 기존 인증방식의 문제점을 개선하기 위해 최근, 개인의 행동습관을 통해 사용자를 인증하는 ‘행위적 특징 기반 인증기술’이 주목받고 있다. 본 논문에서는 사용자마다 마우스 사용습관이 다르다는 특성에 기반한 PC 사용자 인증 방식을 제안한다. 인증 성공률을 높이기 위하여 Mouse dynamics 방식에 압력의 분포, 모양과 같은 새로운 특징적 요소를 추가한다. 또한, 마우스 사용 시 손의 모양, 압력의 분포 등을 수집하여 특징점을 추출할 수 있도록 FSR Array로 마우스패드를 구현하여 새로운 PC 인증 시스템의 프로토타입을 구현하였다.

1. 서론

PC, 스마트폰과 같이 다량의 개인정보를 저장하고 있는 전자기기들이 늘어나면서 자연스럽게 개인정보에 대한 보안의 중요도가 증가하고 있다. 스마트폰의 경우 PIN 번호를 이용한 인증방식부터 홍채, 지문과 같은 보다 높은 안전성을 지닌 생체정보를 이용한 인증방식까지 꾸준히 개발되고 있다. 하지만 PIN 번호는 도용이 쉽고 개인정보를 통해 추측이 가능하다는 점에서 보안 위협에 굉장히 취약한 모습을 보인다. 또, 생체정보의 경우 임의로 갱신할 수 없어서 한번 유출되면 악의를 가진 타인도 쉽게 도용 가능하다는 치명적인 단점을 가지고 있다. 이에 걸음걸이, 키 스트로크와 같이 모방하기 어려운 사용자의 행동 습관을 기반으로 한 ‘행위적 특징 기반 인증기술’이 주목받고 있다. 실제로 2016년 구글은 사용자의 걸음걸이, 말하는 속도 등을 종합적으로 수집하여 분석을 거쳐 신뢰 점수를 측정하는 스마트폰 보안 인터페이스, ‘Trust API’를 발표하였다. [1]

반면, PC 환경에서는 행위적 특징 기반 인증 기술에 관한 연구가 비교적 활발하지 않고, 여전히 PIN 번호 인증방식에 머물러 있다. 본 논문에서는 PC에 적용 가능한 행위적 특징 중 하나인 Mouse

dynamics를 이용한 기존의 특징점 추출방식에 압력이라는 새로운 특징적 요소를 추가하여 사용자 인증 성공률을 높이는 방안을 제안한다. PC 환경에서 각 개인이 마우스를 사용하는 습관을 새로운 특징점으로 활용하는 시스템을 구현하기 위하여 FSR(Force-Sensing Resistor) Array를 마우스 패드로 제작하였다. 제작한 마우스 패드에 가해지는 압력의 분포, 모양 등을 감지하여 특징점을 추출하는 방법을 제시하고 실험을 통해 시스템의 상용화 가능성을 검증한다.

2. 관련 연구

PC 환경에서 행위적 특징 기반 인증기술에 관한 연구는 크게 키보드를 눌렀다 떼는 시차를 행동특징으로 수집하는 Keyboard Stroke[2]와 마우스의 움직임의 기반으로 하는 Mouse dynamics[3],[4]로 나뉜다. 그러나 Keyboard Stroke의 경우, 사용자의 몸 상태 등에 따라 많은 편차가 있어 오류율이 다소 크다는 단점을 가진다. 반면, Mouse dynamics의 경우 다양한 특징점을 추출할 수 있어 인증 오류율이 비교적 작다는 장점이 있어 관련 특허도 꾸준히 출원되고 있다. 2019년 Victor Gorelik가 등록한 특허[5]

에서는 마우스에 카메라와 마이크를 내장하여 사용자의 손바닥 사진을 촬영하고, 맥박 소리를 등록하여 특징으로 추출한다. Clint Feher가 발표한 논문 [6]에서는 마우스의 이동, 버튼 클릭, 드래그 등과 같은 움직임을 4가지 종류로 규정하여 종류마다 평균 이동 거리, 방향, 횟수 등을 통계적으로 분석하여 특징점을 추출하는 알고리즘을 제시하였다. 하지만 이러한 연구들도 상용화할 만큼 완벽한 인증 성공률을 보이지는 못하였다.

본 연구는 기존의 Mouse Dynamics 인증방식에 압력이라는 특징적 요소를 추가하여 더 많은 특징점을 추출하고 인증 성공률을 높이는 것을 목표로 한다.

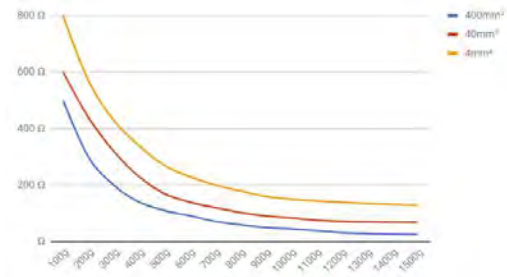
3. FSR Array를 이용한 마우스 패드 설계

본 논문에서 제안하는 방식은 FSR Array를 통해 압력의 분포, 모양 등의 특징점을 얻는 방식으로 현재 문제가 되는 원격해킹방식의 침입을 인지하고 예방한다는 점에서 차별된 장점이 있다. 실제 재택근무가 활발히 시행되는 요즘, 원격 상황에서 기업 내부망으로 접속하여 개인정보를 빼내는 해킹 사고 [7]가 발생하고 있다. 마우스패드에서는 마우스의 움직임이 인식되지 않는데, 마우스 커서가 움직이는 등 특이점이 생기면 PC 사용을 자동으로 중단시키거나 본 소유자에게 위험 메시지를 전송하는 방식 등으로 응용될 수 있다.



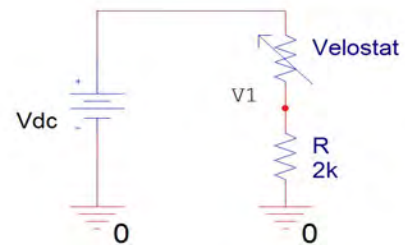
(그림 1) 시스템 구성도

3.1 Velostat을 활용한 FSR Array 설계



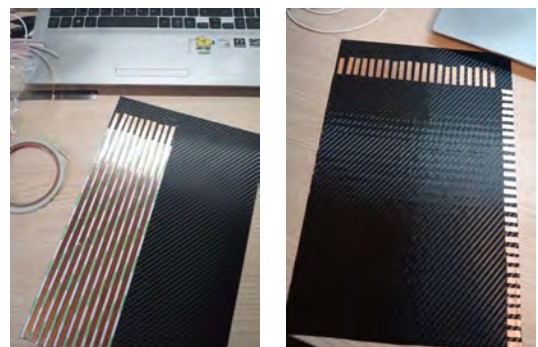
(표 1) Velostat 압력에 대한 저항의 크기 변화[8]

전도성 필름 Velostat의 성질을 이용해 Voltage Divider 회로(그림 2)를 설계하였다. Velostat은 (표 1)과 같이 가해지는 압력이 클수록 저항의 크기가 작아지는 일종의 가변저항이다. 가변저항으로 달라지는 전압 V1을 수치로 나타내도록 설계하였다.



(그림 2) Voltage Divider

구리테이프를 top layer에 가로로, bottom layer에 세로로 각각 배열하고, 그 사이에 Velostat을 부착하는 방식으로 FSR Array를 구현하였다. 구리테이프가 겹치는 면적이 하나의 압력 센서가 되며, Velostat에 압력이 전해지면 저항이 변하여 센서값도 변하는 원리로 작동한다.



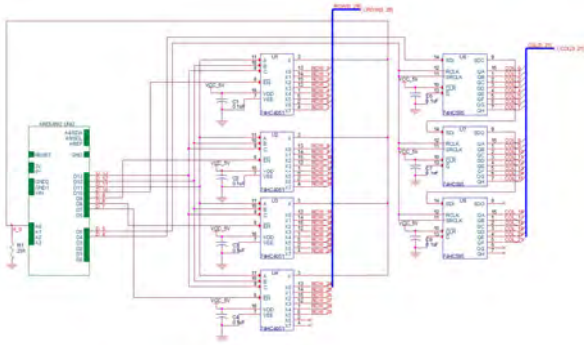
(그림 3) 29×20 센서 Array

3.2 FSR Array 구동을 위한 아두이노 기반 회로

아두이노를 통해 FSR Array를 제어하며, 압력 센서의 각 행과 열의 값을 얻기 위해 Shift Register와 Multiplexer를 이용해 회로를 구성한다.

Shift Register에 Clock 신호를 인가하여 Column

layer에서 검출된 29개의 전압값을 차례로 Multiplexer에서 받고, 다음 Column으로 넘어가도록 회로를 설계하였다.

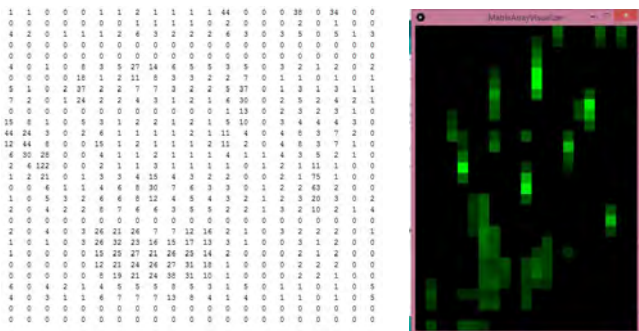


(그림 4) 4개의 MUX(74HC4051), 3개의 SR(74HC595)를 활용한 회로도



(그림 5) 완성된 FSR Array

가해지는 압력에 따라 변하는 압력센서의 값들을 그림 6과 같이 29×21의 숫자 행렬 형태로 아두이노 시리얼 모니터에 출력하도록 코드를 작성하였다. 그림 7과 같이 센서값의 크기를 색깔의 밝기로 나타내도록 java 코드를 작성하였다.



(그림 6) 시리얼모니터 (그림 7) Processing 출력

	센서값의 크기
압력이 가해지지 않았을 때	0 ~ 15
마우스를 올렸을 때	30 ~ 50
압력이 세게 가해질 때 (손목 등)	50 이상

(표 2) 센서값의 크기

4. 실험 결과



(그림 8) 사용자 A



(그림 9) 사용자 B



(그림 10) 사용자 C

- A : 마우스의 왼쪽과 아래쪽으로 압력이 분포
- B : 손목 부위에 집중적으로 압력이 분포
- C : 사용자의 약지, 소지가 패드에 닿아 압력이 가해진다

3명의 사용자가 평소에 마우스를 사용하듯이 마우스 패드 위에서 마우스를 사용하였다. 사용자 A는 마우스의 좌측 하단에 무게가 실리는 것을 확인할 수 있었고, 사용자 B의 경우, 마우스보다는 잡은 손의 손목 부위에 비교적 큰 센서값이 출력되었다. 사용자 C는 잡은 손의 약지, 소지가 패드에 닿아 그림 10과 같은 센서값이 확인되었다. 이 같은 실험을 통해 압력의 세기, 모양, 위치 등이 개인마다 차이가 있고, 행위적 특징 기반 인증 방식에 특징적 요소로 활용이 가능한 것을 확인했다.

5. 특징점 추출 - 유클리드 거리변환

FSR Array에서 출력한 센서값은 29×21의 숫자 행렬로 단순한 숫자 행렬끼리의 유사도를 판별하는데 자주 쓰이는 '유클리드 거리변환'을 본 시스템에 적용하려고 한다.

유사도란 두 데이터가 얼마나 같은지 나타내는 척도이다. 어떤 데이터가 n차원 상의 벡터로 표현된다면, 두 데이터의 유사도는 n차원 상에서 두 벡터 사이의 거리라고도 볼 수 있다. 만약 거리가 가깝다면 두 데이터는 꽤 유사하다고 생각할 수 있다.

$$d(\mathbf{p}, \mathbf{q}) = d(\mathbf{q}, \mathbf{p}) = \sqrt{(q_1 - p_1)^2 + (q_2 - p_2)^2 + \dots + (q_n - p_n)^2}$$

$$= \sqrt{\sum_{i=1}^n (q_i - p_i)^2}.$$

이와 같은 방식으로 마우스패드의 센서값과 미리 학습한 사용자의 센서값 사이의 유클리드 거리를 계산한다. 거리가 일정 수준 이상 가까운 센서값이라면 PC를 사용할 수 있도록 하고, 차이가 크게 발생하면 침입자로 판단해 PC 사용을 중단시키도록 하는 등의 사용자 인증 시스템을 구현할 수 있다.

5.1 유클리드 거리 측정을 위한 코드 작성

위와 같은 알고리즘으로 작동하는 파이썬 코드를 작성하였다. 인증단계에서는 학습된 데이터와 실시간으로 패드를 통해 얻어지는 센서값의 유클리드 거리를 계산한다. 기준 거리 이상의 값이 입력될 경우 유클리드 거리와 에러 메시지를 출력한다.

```
4rd Euclidean distanceEuclidean distance is :
2.23686797749979

5rd Euclidean distanceEuclidean distance is :
79.41832678436729
Warning! You are Unauthorized! Please Go Away!!!

6rd Euclidean distanceEuclidean distance is :
98.37682653958786
Warning! You are Unauthorized! Please Go Away!!!
```

(그림 11) 결과 출력값

5.2 적절한 유클리드 기준 거리 조정

사용자 인증의 기준이 되는 적절한 유클리드 거리를 찾기 위해 기준 거리를 바꿔가며(40 ~ 80) 실험을 진행하였다. 각각 FAR(False Accept Rate, 비등록자를 등록자로 인식하여 잘못 수락하는 확률), FRR(False Rejection Rate, 등록자를 비등록자로 인식하여 접근을 거부하는 확률)을 측정하였다.



(표 3) 기준거리에 따른 FAR, FRR

기준 거리 70 이상에서 FAR, FRR 모두 5% 미만으로 만족스러운 인식률을 얻을 수 있었다.

6. 결론 및 향후 연구

본 논문에서는 마우스 패드를 FSR Array로 제작하여 센서에 가해지는 압력의 분포를 특징점으로 추출하여 사용자를 인식하는 Secondary 인증 시스템을 제안한다. 직접 하드웨어를 구상하고 제작하여 센서값을 얻을 수 있도록 하였고, 실험을 통해 개인마다 마우스 사용습관에 차이가 있고, 이를 특징점으로 활용할 수 있다는 가능성을 보였다. 제안한 시스템은 기존에 연구되어 온 Mouse dynamics 기반 인증 시스템에 추가적인 Secondary 인증방식으로써 정확도를 높이고 더욱 강력한 보안 시스템을 구현하는 데 도움이 될 것으로 기대된다. 향후 연구내용으로는 유클리드 거리변환을 적용한 인증 소프트웨어를 발전시킬 예정이다. 이외에도 여러 알고리즘을 적용하여 인식 성공률을 분석하고 가장 정확한 알고리즘을 찾아 활용해 완성도를 높이려 한다. 또, 하드웨어에서 노이즈를 줄이는 방안을 찾을 계획이다.

참고문헌

- [1] 기사 “Google aims to kill passwords by the end of this year”, The Guardian, <https://www.theguardian.com/technology/2016/may/24/google-passwords-android>, 2016.05.24
- [2] 김원겸, “행위적 특징 기반 바이오 인증 기술 동향”, 정보통신기술진흥센터, 2017
- [3] Chao Shen, “User Authentication Through Mouse Dynamics”, IEEE Transactions on Information Forensics and Security, 2013
- [4] Maja Pusara, “User Re-Authentcation via Mouse Movements”, Vizsec/DMSEC’04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, 2004
- [5] 등록번호 : 10210375 B2, 2019.02, Victor Gorelik, Alexander Fursenko
- [6] Clint Feher, “User Identity Verification via Mouse Dynamics”, 2012
- [7] 기사 “코로나19로 위장한 각종 해킹 공격 증가, '주의 필요'”, IT dongA, <http://it.donga.com/30345/>, 2020.04.07
- [8] REPS.CC, <https://reps.cc/?p=50>

이 조사결과에 따르면 가장 많은 취약점이 발견된 언어는 C언어였다. 오픈소스는 프로그래밍시 구글 혹은 다른 사이트를 통해서 참고할 수 있는 중요한 자료이다. 하지만 시큐어코딩을 거치지 않고 바로 사용하게 될 경우 시스템에 치명적인 취약점을 입힐 가능성이 있다.

본 논문에서 설계하고 구현한 모바일 애플리케이션은 개발자들에게 시큐어 코딩 개념 원리에 대한 설명을 제공하고, 객관식 문제를 풀어보며 취약점에 대한 정보를 인식할 수 있도록 하고 있다. 문제에 대해서 완벽하게 이해했을 때 사용자에게 인증서를 제공하며 시큐어 코딩에 대한 자신의 이해도를 점검하는 방식을 도입했다. 실습 문제를 통해서 안전하지 않은 코드를 안전한 코드로 바꾸는 방향성을 제시하며 결과만을 중요시하는 코딩이 아니라 프로그래밍을 안전하게 구현하며 개발자가 본인의 코드를 이해하는 것이 가장 이상적인 코딩임을 인식할 수 있도록 목적을 두고 있다.

현재 앱스토어 시장에서는 코딩 교육에 대한 앱들은 많지만 시큐어 코딩을 교육하는 앱은 설계되어 있지 않다. 또한 시큐어 코딩 방법을 습득할 수 있는 교육기관이 부족해 기술 습득 기회가 많지 않은 것이 사실이다[4]. 앞으로도 소프트웨어 개발보안과 시큐어 코딩 적용의 중요성은 증가할 것이다[5].

본 애플리케이션은 KISA에서 제공하는 C 시큐어 코딩 가이드를 참고하여 앱으로 만들어 실용성을 높였다. 웹 서비스와 비교했을 때 실제 코딩을 하는 창을 블록으로 구현하였기 때문에 프로그래밍할 때도 보다 편리하게 사용할 수 있도록 기획하였다.

2. 관련 연구 및 관련 기술

2.1 시큐어 코딩과 취약점

소프트웨어를 개발하기 위한 과정에서 프로그래머가 코딩한 프로그램에 많은 오류가 발생한다. 이러한 오류는 검증에 의해 발견이 되지만, 발견되지 않은 오류가 존재하며, 프로그램을 사용하는 중에 발견되는 경우가 있다. 이러한 경우에는 수정에 많은 시간과 비용이 소모된다. 이러한 오류는 사용 중인 프로그램이 내재한 기능성의 문제를 발생시킬 뿐만이 아닌 보안성에 중요한 문제인 프로그램 취약성을 발생시킨다[6]. 위 문제를 해결할 수 있는 것이 시큐어 코딩이다. 시큐어 코딩은 소프트웨어 개발 단계(Software Development Life Cycle : SDLC)에서 보안 약점을 제거함으로써 소프트웨어의 취약점과 해킹의 위험성을 줄여주는 방어적 프로그래밍 기법이다[7]. 시큐어 코딩

은 입력데이터의 검증 및 표현, 보안 기능, 시간 및 상태, 오류 처리, 코드 오류, 캡슐화, API 오용 등 다양한 취약점에 대응할 수 있게 되어 있지만, 주로 웹 서버 혹은 웹 애플리케이션이 직접적으로 가지는 취약점에 대해 조치하는 것이 일반적이다[8]. 특히, 소스코드 보안취약점을 이용한 사이버 공격은 침입차단 및 침입방지 시스템 등 일반적인 보안 장비로는 대응이 어려운 특징이 있다[9].

2.2 사용한 개발 프레임 워크 Flutter

플러터는 한 번 코딩으로 여러 플랫폼용 앱을 만드는 크로스 플랫폼 개발 프레임워크다. 안드로이드와 iOS뿐 아니라 웹, 데스크 톱, 앱 개발도 가능하다. 장점으로 낮은 진입장벽, 높은 네이티브 성능, 훌륭한 개발 도구지원을 들 수 있다[10]. 플러터 언어인 Dart를 사용할 경우 iOS와 안드로이드를 모두 호환하는 앱을 개발할 수 있다.

플러터의 주요 구성요소는 다음과 같다:

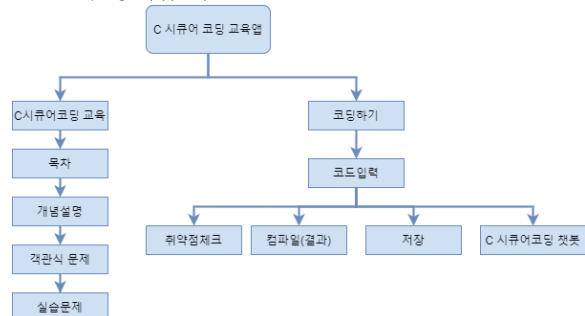
- 다트 플랫폼
- 플러터 엔진
- 파운데이션 라이브러리
- 디자인 특화 위젯 [11]

본 애플리케이션 앱을 설계하기 위해서 하나의 언어로 안드로이드와 iOS 운영체제를 모두 포괄할 수 있는 flutter를 선택하였다.

3. 설계 및 구현

3.1 구조적 설계

본 애플리케이션은 C 시큐어 코딩 교육과 코딩하기를 주요 기능으로 초점을 두고 있다. 그림 3은 애플리케이션의 전체 시스템 구성도로써 인터페이스별 핵심 기능을 중심으로 구성하였다.



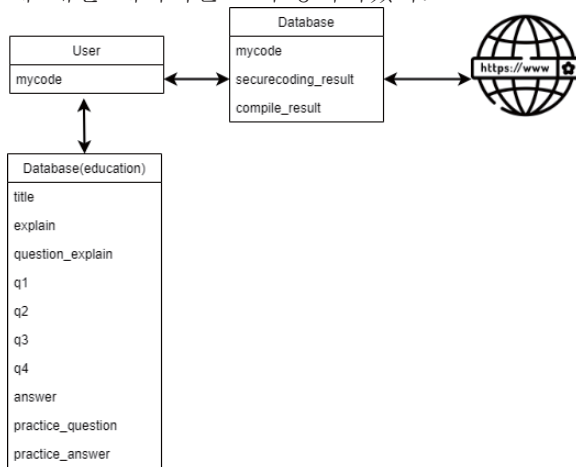
[그림 3] 앱의 시스템 구조도

아래 그림 4는 데이터베이스 구조도를 보여준다. 이 중에서 'Secure Studying'은 User, Database, Database(education)로 설계되어있다.

User는 입력한 mycode를 database로 보내 저장을 하고 해당 코드를 컴파일한 결과들

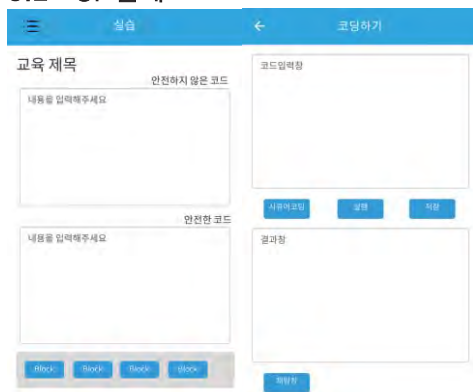
을 securecoding_result와 compile_result에 크롤링하여 저장한다.

Databases(education)은 C 시큐어 코딩 교육에 필요한 개념설명, 개념문제, 실습문제에 대한 데이터들로 구성되어있다.



[그림 4] 데이터베이스 구조도

3.2 UI 설계



[그림5] 교육하기 실습 문제 UI

[그림6] 코딩하기 실행 UI

그림 5와 6은 ‘Secure Studying’의 사용자 인터페이스를 나타낸 그림이다. 코딩하기와 실습하기의 기본적인 기능을 화면에 보여준다.



[그림 7] OWASP 표준 2017 빈도수가 큰 취약점 TOP 10

메인페이지에서는 로고 레이블과 코딩하기, 실습하기 버튼 2개를 가진 기본적인 인터페이스라 따로 그림을 첨부하지 않았다. 실습하기 창에서는 취약점 별로 문제와 개념을 정리해 놓았으며 문제는 그림 7에 나와 있는 OWASP에서 정의한 빈도수 별 취약점을 토대로 정리하였다.

코딩하기는 사용자가 코드를 입력할 코딩 창, 결과를 보여주는 결과 창을 토대로 구성하였다. 시큐어 코딩, 결과, 저장하는 버튼을 코딩 창과 결과 창 사이에 배치하였다.

3.3 구현

본 어플리케이션 ‘Secure Studying’은 별도의 로그인 없이 사용 가능하다. 메인 화면에서 ‘C 시큐어 코딩 교육’ 버튼과 ‘코딩하기’ 버튼 중 원하는 버튼을 클릭하면 해당 인터페이스로 이동한다. ‘시큐어 코딩 교육’을 클릭하면 교육 목차들이 나열되어 있고 원하는 목차를 선택하면 해당 목차에 대한 개념 설명을 볼 수 있다. 문제는 객관식과 실습 문제로 구성되어 있다. 실습 문제는 블록코딩으로 이루어진다. 잘못된 코드 부분을 보여주고 빈칸으로 둔다. 해당 코드를 블록으로 표시하고 사용자는 블록을 드래그 하여 알맞게 배치하면 된다. 정답에 맞게 배치하면 자동으로 넘어간다. ‘코딩하기’ 버튼을 클릭하면 ‘코드 입력 창’과 ‘시큐어 코딩’, ‘실행’, ‘저장’, ‘채팅 창’으로 이루어진 인터페이스로 이동한다. ‘시큐어 코딩’은 입력된 코드에 대한 보안적 문제들을 cppCheck 사이트에서 웹 크롤링을 통해 결과 창에 출력하여 개발자가 보안적인 취약점에 대해 인식할 수 있도록 한다. ‘실행’은 사용자가 입력한 코드를 서버가 컴파일러 사이트에 전송한다. 컴파일된 결과를 웹 크롤링을 통해 ‘결과 창’에 출력한다. ‘채팅 창’은 컴파일 결과에 오류가 출력되었을 때, 해당 오류를 복사하여 채팅 창에 붙여넣으면 문제 해결에 도움을 주는 웹사이트들의 URL을 보여준다.

4. 결론

본 논문에서는 개발자들이 실생활에서 시큐어 코딩에 대한 이해도를 높이고 교육을 더욱 쉽고 간편하게 이용할 수 있도록 블록 형태의 교육 애플리케이션을 설계하고 구현하였다. 본 논문에서 구현한 애플리케이션은 웹 서비스보다는 일상생활에서 간편하게 사용하고 교육할 수 있도록 스마트 폰에 초점을 두어 모바일 애플리케이션으로 구현하여 사용자의 편의성과 학습효과를 높일 수 있을 것으로 기대된다.

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 SW 중심대학지원사업의 연구결과로 수행되었음(2016-0-00022)

참고문헌

- [1] 2019 년 대학 SW 특기자 전형 사진
<https://blog.naver.com/wlrhks815/221876328288>
- [2] LG CNS 공식 블로그
<https://m.post.naver.com/viewer/postView.nhn?volumeNo=16691275&memberNo=3185448&vType=VERTICAL>
- [3] 최문정, 최준성, 정익래, “시큐어 코딩 관련 국내 연구 동향”, 한국통신학회 학술대회논문집, 한국통신학회, 2015, 790-791
- 사진[2] <https://byline.network/2019/03/27-42/>
- [4] “파수닷컴, SW 개발자 대상 시큐어코딩 교육”, 디지털 타임즈, 2014.07.11,
http://www.dt.co.kr/contents.html?article_no=2014071102109960800002
- [5] 최문정, 최준성, 정익래, “시큐어 코딩 관련 국내 연구 동향”, 한국통신학회 학술대회논문집, 한국통신학회, 2015, 790-791
- [6] 김슬기, 박대우, SW 취약점의 보안성 강화를 위한 진단원의 교육 양성 연구, 한국정보통신 학회논문지, 한국정보통신학회, 2017, 945-950
- [7] A. John. R. Peter, “Electric Communication Development,” Communications of the ACM, 40, PP. 71-79, May. 1997.
- [8] S. M . C ho, H. L ee, “A Countermeasure against the Abatement Attack to the Security Server,” Journal of the Korea Institute of Information and Communication Engineering, vol. 20, no. 1, pp. 94-102, Jan. 2016
- [9] 김슬기, 박대우, SW 취약점의 보안성 강화를 위한 진단원의 교육 양성 연구, 한국정보통신 학회논문지, 한국정보통신학회, 2017, 945-950
- [10] 오준석, “오준석의 플러터 생존코딩”, 한빛 미디어, p25
- [11] <https://ko.wikipedia.org/wiki/%ED%94%8C%EB%9F%AC%ED%84%B0>

SDN 환경에서 DDoS 공격에 대한 방어 기법

지승훈*, 박지수**, 손진곤**

*한국방송통신대학교 대학원 정보과학과

**전주대학교 컴퓨터공학과

mayets@knou.ac.kr, jisupark@jj.ac.kr, jgshon@knou.ac.kr

Defense Techniques against DDoS Attack in SDN Environment

Seung Hun Jee*, Ji Su Park**, Jin Gon Shon*

*Dept. of Computer Science, Korean National Open University

**Dept. of Computer Science and Engineering, Jeonju University

요 약

소프트웨어 정의 네트워크(Software-Defined Networking; SDN) 기술은 기존 네트워크 기술의 폐쇄성과 복잡성의 한계를 극복하고, 중앙 집중적 관리 및 프로그래밍 기반의 네트워크 서비스를 제공할 수 있는 장점이 있다. 그러나 SDN 환경에서도 다른 네트워크 환경처럼 악의적인 DDoS 공격으로 인해 전체 네트워크 서비스가 마비될 수도 있는 문제가 있다. 이러한 문제를 해결하기 위한 기존의 연구들은 공격이 인입되는 스위치 포트를 차단하거나, 공격자의 출발지 주소 자체를 차단하는 기법 등이 있으나 공격 트래픽과 함께 정상 트래픽까지 차단하는 문제가 있다. 본 논문에서는 SDN 환경에서 DDoS 공격 발생 시 악의적인 트래픽만 방어하고, 정상적인 트래픽은 최대한 허용하는 서비스 Flow 기반의 방어 기법을 제안한다. 제안 기법은 SDN 환경에서 Flow 분석을 통해 DDoS 공격을 탐지한 후 이를 접근제어 리스트 방식을 통해 공격 트래픽만을 차단하는 것이 가능하다. 실험 결과를 통해 공격자의 악의적인 트래픽은 차단하고, 정상적인 트래픽은 허용하는 것이 확인되었다.

1. 서론

최근 네트워크 기술은 몇 가지 변화된 특징이 있다. 네트워크 장비는 하드웨어와 소프트웨어가 통합된 블랙박스 형태에서 하드웨어와 소프트웨어가 분리된 화이트박스 형태로 변화하고 있다. 네트워크 운영체제는 제조사 별로 상이하게 관리가 필요한 폐쇄적인 형태에서 범용 프로그래밍 언어로 관리가 가능한 개방적인 형태로 발전하고 있다.

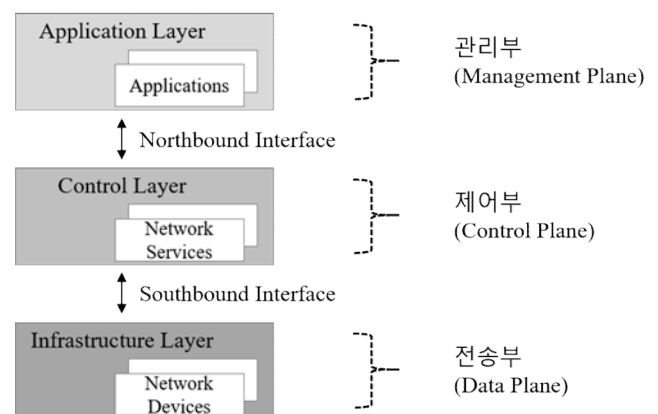
이런 변화를 주도하고 있는 기술인 소프트웨어 정의 네트워크(Software-Defined Networking; SDN)는 네트워크 가상화의 핵심 기술로 활용되고 있다. 하지만 SDN의 구조는 분산 서비스 거부 공격(Distributed Denial of Service; DDoS) 발생 시 치명적인 서비스 단절 현상을 초래할 수 있는 단점이 있어 이를 방어하기 위한 기법이 필요하다.

본 논문에서는 SDN 환경에서 DDoS 공격에 대한 방어 기법을 연구한다. 특히 TCP SYN Flooding 공격 유입 시 제안 기법은 해당 공격 Flow만 탐지 후 차단하고 나머지 정상 Flow는 모두 허용한다.

2. 관련 연구

2.1. SDN과 DDoS의 구조

SDN이란 기존 네트워크 장비에서 하드웨어와 소프트웨어의 기능을 분리한 새로운 네트워크 기술을 의미한다[1]. SDN은 (그림 1)과 같이 관리 및 모니터링을 담당하는 관리부, 경로 설정 및 통제를 담당하는 제어부, 전송을 담당하는 전송부로 구성된다.

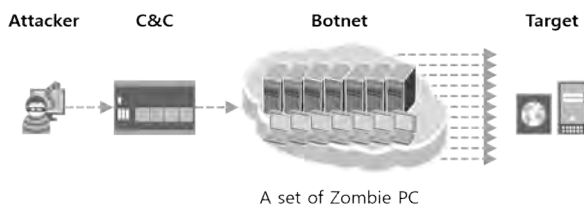


(그림 1) SDN의 구조

+ 교신저자

SDN을 통해 기존 네트워크 한계를 극복하기 위한 다양한 연구 성과에 비해 SDN 환경에서 보안을 강화하기 위한 연구는 상대적으로 부족하다. 이에 SDN 환경에서 악의적인 공격 발생 시 네트워크를 보호하기 위한 기법에 대한 연구가 필요하다[2].

한편 DDoS 공격이란 인터넷 상에 있는 악성 코드에 감염된 다수의 단말을 악용하여 공격 시스템에 대량의 트래픽을 전송하여 시스템의 정상적인 서비스를 마비시키는 공격을 말한다. DDoS 공격의 구조는 (그림 2)와 같이 공격자가 C&C 서버를 통해 다수의 좀비 PC로 이루어진 Botnet으로부터 대량의 트래픽 전송을 수행하게 하는 구조로 이루어진다[3].



(그림 2) DDoS 공격의 구조

2.2. 관련 논문 연구

SDN 환경에서 DDoS 공격에 대한 방어 기법에 대한 기존 연구는 탐지 기법에 대한 연구와 차단 기법에 대한 연구로 분류할 수 있다. 첫 번째로, SDN 환경에서 DDoS 공격 탐지 기법에 대한 연구를 3가지 기준으로 분류하였다.

정적 임계치 기반의 탐지는 설정된 임계값을 초과 시 초과 시 이를 탐지 시점을 판단하는 기법이다 [4]-[5]. 이 경우 임계값 이하에서는 DDoS 공격 트래픽에 대한 탐지 자체를 할 수 없는 문제가 있다.

정책 기반의 탐지는 정형화된 DDoS 공격에 대해서는 효과적으로 탐지 가능하다[6]. 다만 비정형화된 새로운 DDoS 공격에 대해서는 탐지가 어렵다.

동적 학습 기반의 탐지는 인공 지능 기술을 활용하여 일정 기간 평시 사용량에 대한 학습 결과를 기반으로 이를 초과하는 트래픽 발생 시 탐지를 수행하는 기법으로 현재까지 연구에서 가장 지능적이고 효과적인 방안이다[7]-[8]. 다만 이 기법의 경우에도 평시와 다른 이벤트로 인한 대용량 트래픽과, DDoS 공격으로 인한 대용량 트래픽을 구별할 수 있는 기술적 방안에 대한 연구가 필요하다.

공격 탐지 기법을 정리하면 <표 1>과 같다.

<표 1> DDoS 공격 탐지 관련 연구

탐지 기준	탐지 대상	관련 논문
정적	네트워크 이용률	M. Nugraha[4]
임계치	서버 큐 이용률	방기현[5]
정책	정의된 패턴 위반	조승진[6]
동적 학습	K-Means 기반	신동혁[7]
	SVM 기반	오대명[8]

두 번째로, SDN 환경에서 DDoS 공격 차단 기법에 대한 연구를 3가지 기준으로 분류하였다.

Port 기반의 차단은 공격 트래픽이 유입되는 스위치 Port 자체를 차단하는 기법으로[9], 해당 Port로부터 유입되는 정상 Flow를 포함한 모든 Flow를 차단하는 문제가 있다. Flow 기반의 차단은 공격자 주소 IP가 포함된 Flow 전체를 차단하는 기법으로 [10], 해당 IP로부터 유입되는 정상 Flow까지 차단하는 문제가 있다. Host 기반의 차단은 공격자 단말 자체를 네트워크에서 격리 후 치료하는 기법으로 [11], 공격 시도를 자체를 차단할 수 있으나 공격자는 대부분 외부 네트워크에 존재하고 있어 사실상 격리 및 치료가 어렵다. 공격 방어 기법을 정리하면 <표 2>과 같다.

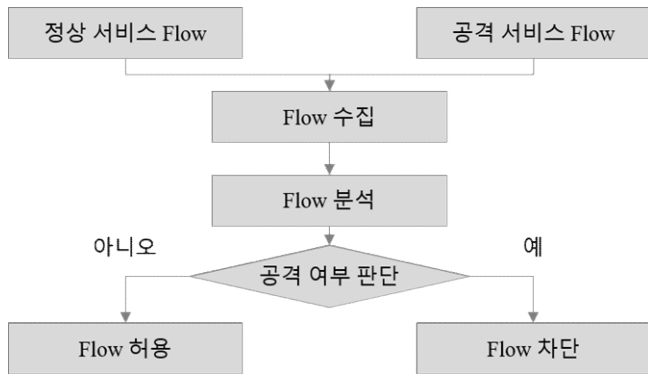
<표 2> DDoS 공격 방어 관련 연구

방어 기준	방어 대상	관련 논문
Port	공격 유입 Port 차단	박종환[9]
IP Flow	공격자 IP Flow 차단	김정훈[10]
Host	좀비 PC 격리/치료	배효빈[11]

기존 연구의 한계점을 극복하기 위해 전체 트래픽 Flow 중에서 비정상적인 Flow만 차단하고 나머지 정상적인 Flow는 허용하여, 오탐율을 최소화하고 공격 트래픽에 대해서만 최소한으로 방어하는 기법에 대한 연구가 필요하다.

3. 서비스 Flow 기반 DDoS 방어 기법

본 연구에서 제안된 서비스 Flow 기반 DDoS 방어 기법은 서비스 Flow 기반 DDoS 탐지 기법과 서비스 Flow 기반 DDoS 차단 기법으로 구성되어 있다. 첫 번째, 서비스 Flow 기반 DDoS 탐지 기법은 (그림 3)과 같이 서비스 SDN 스위치를 통해 수집된 Flow를 기반으로 SDN 애플리케이션에서 각각의 서비스 Flow 분석하여 DDoS 공격 여부를 탐지한다.



(그림 3) 제안 기법의 동작방식

제안 탐지 기법은 DDoS 공격 중 하나인 TCP SYN Flooding 공격 유입 시 <표 4>와 같이 의사 코드 형태로 표현된 알고리즘으로 동작한다.

<표 4> TCP SYN Flooding 공격 탐지 기법

```

D ← empty dictionary
max_syn ← 60 // can be modified
timer ← 60 sec // can be modified
while True :
  get TCP packet
  if protocol is "TCP" :
    get tcp_flag
    if tcp_flag is syn :
      if source_ip ∈ key(D) :
        D[source_ip] [0] ++
      else :
        start_time ← get current time
        D[source_ip] ← [0, start_time]
    if D[source_ip] [0] > max_syn :
      time_difference = current time -
        D[source_ip] [1]
      if time_difference < timer :
        print "TCP SYN Flooding attack"
  
```

두 번째, 제안된 서비스 Flow 기반 DDoS 차단 기법은 탐지된 공격 서비스 Flow는 SDN 컨트롤러를 통해 SDN 스위치에 접근 제어 리스트(Access Control List)를 추가하여 해당 Flow만 차단한다.

제안 기법은 Port 기반 또는 IP Flow 기반의 기존 연구와는 달리 공격자의 모든 Flow를 차단하는 것이 아니라, DDoS 공격 Flow만 차단한다. 공격자의 단말이 자신도 모르게 악성 코드에 감염되어 악의적인 공격에 참여할 경우 공격자 주소 자체가 네

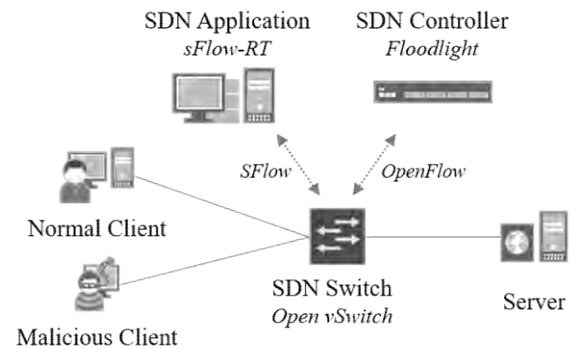
트워크 환경에서 차단되어, 향후 단말에 대한 방역이 끝난 이후에도 네트워크 통신이 불가능한 문제를 해결할 수 있다.

4. 실험 및 평가

제안 기법을 검증하기 위해 <표 5>와 같은 실험 환경과 (그림 4)와 같은 실험 구성을 기반으로 제안 기법에 대한 실험을 수행하였다.

<표 5> 실험 환경

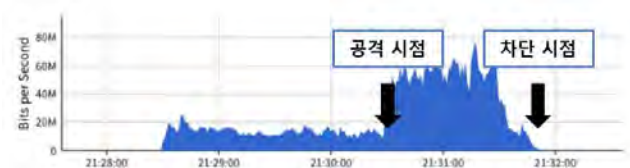
구분	실험 도구	버전
에뮬레이터	Mininet/Miniedit	2.3.0d6/2.2.0.1
컨트롤러	Floodlight	1.2
스위치	Open vSwitch	2.9.5
Flow 수집	sFlow-RT	3.0



(그림 4) 실험 구성

실험 환경에서 정상 사용자는 정상적인 ICMP 및 TCP 트래픽 전송하고, 공격자는 정상적인 ICMP 트래픽과 TCP SYN Flooding 공격 트래픽을 전송한다. 기존의 차단 기법과 제안된 차단 기법에서 각각 허용되는 트래픽과 차단되는 트래픽 검증을 위해 실험을 수행하였다.

Port 기반 차단 기법을 적용한 결과 (그림 5)와 같이 공격 탐지 후 차단 시점에 다른 모든 정상 트래픽도 차단되어 차단 시점 이후 트래픽 유입이 전혀 없는 것을 알 수 있다.



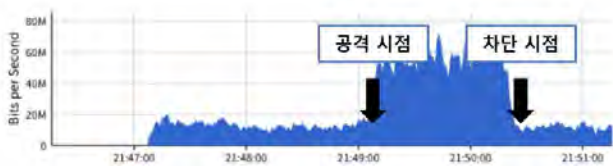
(그림 5) Port 기반 차단 기법 적용 결과

IP Flow 기반 차단 기법을 적용한 결과 (그림 6)과 같이 공격 탐지 후 차단 시점에 공격자의 정상 트래픽까지 차단되어 공격 시점 전과 차단 시점 이후 트래픽 유입량이 차이가 나는 것을 알 수 있다.



(그림 6) IP Flow 기반 차단 기법 적용 결과

이에 비해 제안된 서비스 Flow 기반 차단 기법은 (그림 7)과 같이 공격 탐지 후 차단 시점에 공격자의 공격 트래픽만을 차단하고 나머지 트래픽은 정상적으로 허용되어, 공격 시점 전과 차단 시점 이후 트래픽 유입량이 차이가 없는 것을 알 수 있다.



(그림 7) 서비스 Flow 기반 차단 기법 적용 결과

실험 결과는 아래 <표 6>과 같이 정리하였다.

<표 6> 차단 기법에 따른 실험 결과

차단 기법	정상 사용자		공격자	
	정상 ICMP	정상 TCP	정상 ICMP	공격 TCP
Port 기반	차단	차단	차단	차단
IP Flow 기반	허용	허용	차단	차단
서비스 Flow 기반	허용	허용	허용	차단

5. 결론

본 논문에서는 SDN 환경에서 DDoS 공격 발생 시 SDN 스위치에서 수집된 Flow 정보를 기반으로 SDN 애플리케이션에서 공격 Flow를 탐지하고, 해당 Flow에 대해서만 SDN 컨트롤러를 통해 차단하는 서비스 Flow 기반 DDoS 방어 기법을 제안하였다. 기존 연구 기법에 비해 제안 기법은 공격 Flow만을 탐지 후 차단함으로써 차단 범위를 최소화하고, 공격자 IP로부터의 정상적인 트래픽은 계속 허용하는 것을 확인하였다.

서비스 거부 공격에는 TCP 자원 고갈 공격 외에

도 다양한 공격이 있다. 향후 연구에서는 SDN 환경에서 다양한 DDoS 공격 발생 시 이를 탐지하고 차단할 수 있는 방어 기법에 대해 연구한다.

참고문헌

- [1] M. Casado et al., "Ethane: taking control of the enterprise," ACM SIGCOMM Computer Communication Review, Aug. 2007.
- [2] Y. Liu et al., "A survey: typical security issues of software-defined networking," China Communications, vol. 16, no. 7, pp. 13-31, Jul. 2019.
- [3] J. Mirkovic et al., "A taxonomy of DDoS attack and DDoS defense mechanisms," ACM SIGCOMM Computer Communications Review, vol. 34, no. 2, Apr. 2004.
- [4] M. Nugraha et al., "Utilizing openflow and sflow to detect and mitigate SYN flooding attack," 멀티미디어학회논문지, vol. 17, no. 8, pp. 988-994, Aug. 2014.
- [5] 방기현 외 2명, "SDN 환경에서의 목적지 주소별 패킷 샘플링을 이용한 SYN Flooding 공격 방어 기법," 멀티미디어학회논문지, vol. 18, no. 1, pp. 35-41, Jan. 2015.
- [6] 조승진 외 1명, "Cookie 기반의 HTTP DDoS attack 방어 시스템," 한국통신학회 학술대회논문집, pp. 464-465, Jan. 2016.
- [7] 신동혁, "Malicious traffic detection using k-means," 성균관대학교 대학원 석사학위논문, 2016.
- [8] 오대명, "SDN 환경의 플로우 테이블 특징 기반 DDoS 공격 완화 기법," 서울과학기술대학교 대학원, 석사학위논문, 2016.
- [9] 박종환 외 1명, "SDN 환경에서 소스의 입력 포트를 기반으로 한 DDoS 탐지 및 대응 방법," 한국통신학회 학술대회논문집, Jan. 2019.
- [10] 김정훈, "SDN 및 sflow를 활용한 이동통신사 IP망 환경에서 DDoS 공격 대응 개선방안," 연세대학교 공학대학원, 석사학위논문, 2016.
- [11] HB. Bae et al., "Zombie PC detection and treatment model on software-defined network," Computer Science and its Applications, pp. 837-843, Jan. 2015.

개인정보 문서 노출과 가명정보 조합을 통한 개인정보 관련 피해 위험성 연구

김민주*, 김영은**, 이준민**, 이창현**, 하정희**,
정재완***, 강대명****, 김영철****, 허원석****
*서울여자대학교 정보보호학과
**한국정보기술연구원 Best of the Best
***광운대학교 정보융합학부
****한국정보기술연구원 Best of the Best 멘토
mjkim3715@swu.ac.kr

A Study on the Risk of Personal Information-related Damage through the Exposure of Personal Information Documents and the Combination of pseudonym Information

Min-Ju Kim*, Young-Eun Kim**, Jun-Min Lee**, Chang-Hyun Lee**, Jeong-Hee Ha**
Jae-Wan Jeong***, Dae-Myung Kang****, Yung-Chul Kim****, Won-Seok Heo****
*Dept. of Information Security, Seoul Women's University
**KITRI Best of the Best
***Dept. of Information Convergence, KwangWoon University
****KITRI Best of the Best Mentor

요 약

대부분의 공공기관과 기업에서 개인정보가 포함된 문서를 마스킹 처리하여 온라인상에 게재하고 있다. 이 때, 여러 검색 엔진에서 특정 키워드를 통한 검색 결과를 통해 개인정보가 포함된 문서들이 대량으로 노출되고 있으며 마스킹 처리가 된 정보라 하더라도 2 개 이상의 부가 정보들을 조합해서 개인을 특정할 수 있는 문제가 발생할 수 있다. 이를 통해 얻은 개인정보와 개인을 특정할 수 있는 정보는 다양한 범죄 피해를 발생시킬 우려가 있다. 따라서 본 논문은 검색 엔진과 온라인상에서 노출되고 있는 개인정보가 포함된 문서들을 탐지한다. 그 후 발견된 문서들의 통계와 조사를 통해 온라인상에 노출 중인 개인 정보와 가명정보 등이 초래하는 피해의 심각성을 재고하고, 대안을 제시하고자 한다.

1 서론

제 4 차 산업혁명 시대의 도래에 따른 세계 각국의 데이터 경제 활성화 추진과 현대 사회 트렌드를 빠르고 정확하게 예측해 정보를 추출하는 일은 수많은 기업의 과제가 되고 있다 [1]. 이에 따라 텍스트, 이미지, 동영상 등 데이터에서 추출한 정보의 부가가치가 높아지고 있다. 최근 개인정보보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 그리고 신용정보의 이용 및 보호에 관한 법률 (이하

데이터 3 법) 은 데이터를 효율적으로 활용하고 안전하게 이용할 수 있도록 정책을 마련하기 위해 개정이 되었다. 데이터 3 법이 개정되면서 가명정보를 활용하고 이를 정보주체의 동의 없이 적절한 안전 조치 하에 통계, 연구, 기록, 보존 등 다양한 분야에서 활용 가능하게 되었다. 여기서 가명정보의 정의는 '가명 처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보(이하 가명정보)[2]이다.

일반적으로 개인정보의 유·노출 방지 및 보호를 위해 개인정보의 일부를 특정 문자나 기호로 치환하는 방식인 마스킹 처리 방법을 사용한다[3]. 마스킹 처리란, 주민등록번호의 경우 ‘200410-4*****’ 처럼 주민등록번호의 뒤 7 자리의 일부를 ‘*’ 과 같은 특수 기호로 치환하는 방식으로 마스킹 처리할 수 있다. 마스킹 처리는 비교적 쉽게 개인을 식별할 수 없도록 하는 방법 중 하나로 많은 게시판이나 첨부파일에 활용되고 있다.

하지만, 마스킹 처리되지 않고 온라인상에 게시된 개인정보를 포함하는 문서(이하 개인정보 문서)가 특정한 검색 키워드를 통해 검색 엔진에서 수집되어 노출되는 경우가 발생하고 있다. 이를 통해 취득한 개인정보와 관련된 피해가 우려된다.

본 논문에서는 검색 엔진 상에서 개인정보문서와 마스킹 처리를 했음에도 불구하고 개인정보를 유추할 수 있는 문서를 탐지하고 문서들의 정보를 결합하여 개인 특정 가능 여부를 조사하고자 한다.

그 후 탐지된 문서들의 개인정보 노출 여부와 통계를 통해 심각성을 파악하고, 향후 데이터 3 법이 시행되었을 때 개인정보 유·노출 및 가명정보 조함으로 우려되는 피해를 줄일 수 있는 방안을 제시하고자 한다.

2 본론

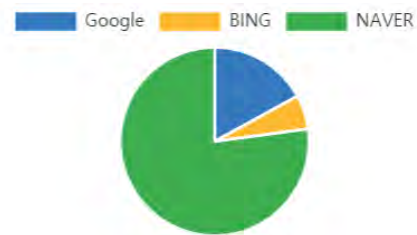
2.1 현황 조사 및 개인정보 노출 현황

서론에서 언급한 개인정보 문서가 노출되는지 여부를 확인하기 위해 검색 엔진 선정을 진행하였다. 검색 엔진 점유율과 특성을 하단의 <표 1>과 같이 비교하여 대상 검색엔진을 선정하였다.

	.hwp 검색	국내 검색 엔진 점유 순위	고급 검색 지원 여부	검색 결과 마스킹 여부
네이버 (NAVER)	O	1 위	O	O
구글 (Google)	X	2 위	O	X
다음 (Daum)	O	3 위	△	X
줌 (ZUM)	X	4 위	X	X
빙 (Bing)	X	5 위	O	X

<표 1> 검색 엔진 비교[4]

해당 논문에서는 아래와 같은 검색 엔진을 선정했는데, 그 이유는 국내 이용자들이 가장 많이 사용하는 검색 엔진인 네이버와 타 검색 엔진에 비해 방대한 정보를 캐시(Cache) 서버에 저장하는 구글(Google), 관련 직종 종사자와 경력자들의 조언을 바탕으로 기관과 기업에서 정보 유출이 다수 발견되는 Bing) 또한 개인정보의 접근 가능성이 높아 대상으로 삼았다.

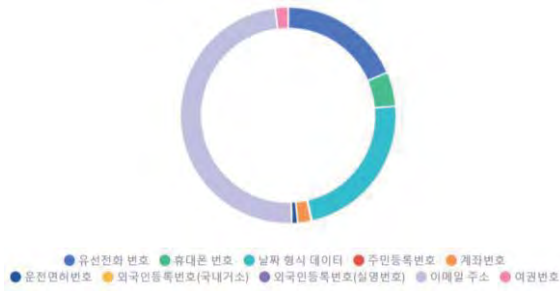


(그림 1) 검색 엔진 별 개인정보 노출 문서 통계표

상단의 (그림 1)은 위에서 언급한 3 가지 검색 엔진에 대해 유·노출 데이터를 수집한 결과이며, 네이버 1,868 건, 구글 412 건, Bing 142 건으로 총 2,422 건이 탐지되었다. 특히 엑셀 파일의 경우 단순 '숨기기' 기능이나 글자 색을 바꾸는 등의 처리만 하여 개인정보가 노출되는 경우가 다수 발견되었다.

이들을 대상으로 각 정규표현식을 통해 해당되는 개인 정보가 포함된 문서 및 게시글을 수집하여 개인정보 유·노출 현황 통계 작업을 진행했다. 개인정보종류는 ‘개인정보보호법’ 및 KISA 에서 제공한 ‘홈페이지 개인정보 노출방지 안내서’에 작성되어 있는 기준으로 고유식별정보(주민등록번호, 여권번호, 외국인등록번호, 운전면허번호), 개인식별정보(휴대폰 번호, 전화번호, 이메일, 생년월일(이하 날짜형식 데이터)), 신용정보(계좌번호) 등으로 9 가지를 선정하였다[3].

하단의 (그림 2)는 위에서 설명한 방법을 통해 36 시간가량 네이버와 구글, Bing에서 탐지한 문서 내의 개인정보의 총 개수이다.



(그림 2) 개인정보 노출 현황 통계 자료

위에서 탐지한 노출된 개인정보가 담긴 문서에서 아래의 <표 2>와 같이 개인 정보의 건 수를 추출할 수 있었다.

개인정보 종류	발견 건 수
이메일	2,714
날짜 형식 데이터	1,272
전화 번호	1,034
휴대전화 번호	286
계좌 번호	114
여권 번호	106
운전 면허 번호	48
주민 등록 번호	8
외국인 등록 번호	0

<표 2> 탐지된 문서에서 발견한 개인정보 건 수

이 지표를 통해 마스킹 되지 않은 개인정보들이 상당수 온라인상에 노출되어 있으며, 이 개인정보들이 충분히 악용될 소지가 있다고 판단된다.

2.2 가명정보 조합을 통한 개인 특정

위 기법을 사용해 수집한 결과 가명정보들을 포함하는 문서들을 탐지할 수 있었다. 보통 개인정보가 포함된 문서를 게시하기 전 마스킹 처리를 실시한다. 일부를 가린 개인정보라고 해도 문서 내 함께 존재하는 소속 정보 및 직업 등과 같은 부가 정보와 별도의 문서에서 발견한 마스킹 된 개인정보들을 조합하면 충분히 개인을 특정할 수 있다.

다음은 가명정보를 포함하는 문서들 속에 존재하는 개인정보를 활용하여 개인을 특정한 예시이다.

선발캠프 대상자 명단(초등)

수험번호	이름	생년월일	휴대폰 번호	수험번호	이름	생년월일	휴대폰 번호	수험번호	이름	생년월일	휴대폰 번호
40	구*우	060712	010-****-5589	31	문****소	080423	010-****-8884	47	문*우	060927	010-****-2880
10	김*진	070803	010-****-1979	44	서*재	060621	010-****-6420	14	문*호	080121	010-****-2886
1	김*아	080508	010-****-8583	12	황*영	070331	010-****-1807	22	황*우	081130	010-****-1343
5	김*영	070326	010-****-1586	20	홍*우	070108	010-****-0335	48	황*현	060611	010-****-7674
41	김*진	060708	010-****-7885	13	오*희	081205	010-****-8522	33	홍*호	070207	010-****-4796
2	김*용	080623	010-****-8133	45	오*영	060111	010-****-8829	34	황*현	071016	010-****-6051
27	김*진	071121	010-****-4676	37	홍*우	070702	010-****-7991	38	조*재	071015	010-****-8311
42	김*진	060309	010-****-4676	46	홍*우	061230	010-****-7719	23	조*익	081019	010-****-2588
28	노*민	070521	010-****-6187	16	문*진	081015	010-****-7046	35	조*호	070306	010-****-0420
6	박*진	080529	010-****-1439	9	박*나	080302	010-****-4392	24	안*호	080415	010-****-3424
29	박*진	070603	010-****-4986	4	박*진	080521	010-****-8448	49	한*현	080222	010-****-9587
7	박*영	080825	010-****-2915	18	박*영	030628	010-****-3585	37	박*우	070720	010-****-4856
43	박*영	060311	010-****-4684	17	박*영	080605	010-****-7207	38	박*남	071018	010-****-5778
3	박*영	080510	010-****-7710	26	박*지	071231	010-****-2348	25	박*현	080107	010-****-9079
10	박*영	070326	010-****-3416	32	박*현	070719	010-****-3712	39	홍*호	080322	010-****-7220
15	박*영	071028	010-****-6822	19	박*호	080811	010-****-1137				
8	박*영	081121	010-****-5817	21	황*현	081118	010-****-0254				

(그림 3) 가명정보가 포함된 문서

(그림 3)의 경우 특정 기업에서 실시하는 선발 캠프 참가 대상자의 개인정보를 마스킹 처리하여 게시하고 있다. 이 중 한 명의 가명정보를 검색 엔진의 고급검색 기법 이용하여 검색을 진행하였다. 검색 결과는 다음 (그림 4)와 같다.



(그림 4) 고급 검색 기법을 통한 검색 결과

(그림 4)의 결과를 통해 같은 홈페이지에 게시되어 있는 것으로 확인되는 별도의 문서 한 건을 발견했다. 이 문서는 하단의 (그림 5)와 같다.

이름	학번	휴대폰 번호	아이디	비밀번호	이름	학번	휴대폰 번호	아이디	비밀번호
김*아	초4	010-****-8593	5101	S****@lg	이*원	초4	010-****-7207	5119	S****@lg
김*애	초4	010-****-7603	5102	S****@lg	이*호	초4	010-****-1137	5120	S****@lg
김*용	초4	010-****-8133	5103	S****@lg	이*희	초4	010-****-5747	5121	S****@lg
박*건	초4	010-****-1439	5104	S****@lg	이*희	초4	010-****-1134	5122	S****@lg
박*승	초4	010-****-2915	5105	S****@lg	임*빈	초4	010-****-0254	5123	S****@lg
박*연	초4	010-****-2219	5106	S****@lg	양*윤	초4	010-****-2688	5124	S****@lg

(그림 5) 검색을 통해 얻은 별도의 문서

(그림 3)과 (그림 5)를 비교 분석했을 때 개인의 이름, 생년월일, 나이, LMS 아이디 및 비밀번호 일부를 수집할 수 있게 된다. 이 결과로 한 명을

특정할 수 있다는 것을 확인했다.

마스킹 처리가 된 가명정보라도 2 개 이상의 가명정보가 있거나, 직장, 나이, 소속 등 부가 정보들을 조합하면 개인을 특정할 수 있었다.

3 결론

기업과 기관에서는 개인정보 문서들을 게시하는 경우 검색 엔진 등이 게시판이나 첨부파일의 정보를 수집할 수 없도록 robot.txt 를 올바르게 설정할 필요가 있다. robot.txt 를 활용함으로써 기업이나 기관의 개인정보 문서를 일차적으로 보호할 수 있게 된다.

또한, 검색 엔진의 캐시 서버에 개인정보 문서가 존재하는지, 혹은 검색 엔진 상에 노출되어 있는 개인정보 문서가 없는지 주기적으로 점검할 수 있게 시스템 구축이 요구되며, 이미 노출된 문서들은 삭제 조치가 필요하다.

국내에서 가장 보편적으로 사용하는 검색 엔진인 네이버의 경우 타 검색 엔진에 비해 카페나 블로그의 게시글이나 첨부파일의 형태로 개인정보가 많이 노출될 가능성이 있으므로 관리상 주의가 필요하다.

타 검색 엔진과 달리 네이버는 개인정보가 존재하는 검색 결과를 탐지하여 마스킹 처리 후 검색 결과 페이지에서 보여주고 있다. 구글 등의 타 검색 엔진은 개인정보가 있더라도 검색 결과 페이지에서 마스킹 처리가 되지 않은 정보를 바로 확인할 수 있어 더 위험할 수 있다. 그러므로 국내에서 서비스하고 있는 검색 엔진들이 검색 결과에서 일차적으로 개인정보의 유출을 막을 수 있는 방안이 필요하다. 또한, 각 기관이나 기업, 개인은 개인정보를 온라인상에 게시하기 전 최소한 마스킹 처리를 하고 부가 정보를 삭제하는 것이 바람직하다.

위와 같은 사전 조치 방법을 시행했음에도 불구하고 개인정보의 유·노출 여부가 탐지된 경우, 이를 탐지한 시점에서 최대한 그 정보와 관련 없는 타인이 악용할 수 없도록 해당 문서나 웹 서비스의

담당자(이하 담당자)는 빠르게 조치해야 할 필요가 있다.

따라서 개인정보 문서나 개인정보를 포함한 게시물이 탐지되면 이를 조치할 권한이 있는 담당자에게 즉시 연락을 통해 조치를 취할 수 있도록 한다.

탐지 결과를 레포팅하는 방식은 본 논문에서 활용한 프로젝트에 등록된 각 기관 담당자의 이메일 주소나, 온라인상에 게시된 담당자의 이메일 주소를 통해 개인정보 유·노출 여부 탐지 시 바로 조치를 취할 수 있도록 탐지 및 통계 결과와 게시된 곳의 링크 등을 첨부하여 이메일을 발송한다.

또한, 웹 사이트의 경우 담당자의 이메일 주소 등의 연락처를 온라인 상에 게시하거나 개인정보 포함 내용을 빠르게 조치하기 위해 자체적으로 신고 게시판 제도를 운영하는 방법 등이 필요하다.

결과적으로 담당자는 연락처로 제공받은 정보와 신고 게시판을 통해 얻은 정보를 활용하여 보다 빠른 조치를 취해 타인이 해당 정보를 악용할 수 없도록 할 수 있다.

마지막으로 데이터 3 법이 개정된 시점에서 가명정보라 해도 부가 정보가 있거나, 두 가지 이상의 가명정보를 포함하는 별도의 문서가 함께 존재할 경우 개인이 특정될 가능성이 있다. 따라서 이와 관련한 법률과 명확한 가이드라인이 필요하다.

참고문헌

- [1] 데이터 3 법 개정의 주요 내용과 전망, 2020 KISA REPORT 2 월호, KISA, 2020
- [2] 개인정보보호법 제 2 조제 1 항다목
- [3] 홈페이지 개인정보 노출방지 안내서, KISA, 2018
- [4] <http://www.internettrend.co.kr/trendForward.tsp>
- [5] 2010 인터넷상 개인정보 노출의 문제점 및 대응방안, KISA, 2018
- [6] 개인정보 노출예방 교육, 개인정보보호 종합 포털, 2017
- [7] 2019 년 개인정보 보호법 위반사례 및 대응방안, 개인정보보호 종합 포털(건양대 차건상 교수), 2019
- [8] 홈페이지 개인정보 유출 위반사례 및 후속조치, KISA, 2019

블록체인을 통한 키오스크 스마트 체크인 방식 제안

심민주*, 최승주*, 서화정*[†]

*한성대학교 IT융합공학부

minjoos9797@gmail.com, bookingstore3@gmail.com, hwajeong84@gmail.com

Proposal of a Kiosk Smart Check-in Method with Block Chain

Min-Joo Sim*, Seung-Ju Choi*, Hwa-Jeong Seo*[†]

*Division of IT Convergence Engineering, Han-Sung University

요 약

최근 키오스크 사용 비중이 커짐으로써 그에 따른 사용자들의 개인 정보에 대한 보안 위협이 증가하였다. 호텔과 같은 숙박업소에서 이용하는 키오스크의 경우 체크인을 하기 위해 사용자들의 개인 정보를 입력하는 것은 물론 숙박하는 호실의 정보도 가지고 있다. 이 경우 정보 유출 시 개인 정보 유출 이외의 다른 범죄가 발생할 수 있다. 이와 같은 키오스크 보안의 한계점을 보완하기 위해 본 논문에서는 Tendermint 기반의 블록체인을 이용하여 기존 일방향적인 결제 시스템을 지닌 기존 키오스크 체크인 시스템의 단점을 보완하고 키오스크 체크인의 보안성 및 신뢰성을 강화하는 방법을 제안한다.

1. 서론

최근 언택트 문화(Untact Culture)를 바탕으로 우리 사회에서 무인화 기계인 키오스크를 쉽게 찾아볼 수 있다. 키오스크의 사용이 점점 늘어남과 동시에 보안 위협도 증가하였다. 무엇보다도 키오스크를 이용하는 숙박업소에 제공되는 이용자의 개인 정보는 물론 이용하는 호실까지 유출되어 다른 범죄가 발생할 수 있다.

본 논문에서는 현재 호텔 등의 숙박업소에서 키오스크를 이용해 스마트 체크인할 때 발생하는 단점인 결제 시스템을 보완하고, 숙박업소에서 사용되는 키오스크에 저장된 정보를 안전하게 보호할 수 있는 새로운 키오스크 체크인 시스템을 제안한다.

2. Tendermint 기반 블록체인

Tendermint는 Cosmos에서 사용하는 합의 알고리즘이다.[1] Cosmos 블록체인이 블록체인으로 동작할 수 있도록 만들어주고, 모든 것을 올바르게 처리하는 역할을 한다.[2] 기존 합의 알고리즘과 달리 '선(先) 합의, 후(後) 블록 생성'하는 메커니즘을 가지고 있어 포크가 발생하지 않는다. 이 때문에

Tendermint 기반의 블록체인은 가장 최근에 생성된 블록에 기록된 정보를 가져와도 안전하다.

3. 기존 키오스크

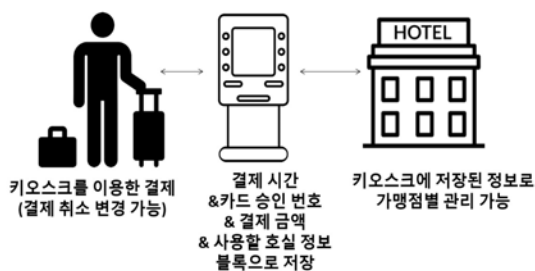
기존의 키오스크 결제 시스템은 사용자가 키오스크로 결제 시 결제 정보가 관계자에게 넘어가기 때문에 사용자가 결제 후 결제 취소를 하거나 변경을 하고 싶어도 키오스크에서는 해당 결제의 변경이 불가능하다. 이 경우 관계자에게 문의가 필수적인 불편함이 발생한다. 키오스크의 이용이 늘어나는 것은 주문과 결제의 회전율이 빠른 이유가 있다. 하지만 기존 키오스크의 결제 시스템은 회전율에 영향을 준다.

또한, 키오스크 이용률이 늘어남에 따라 보안 취약성도 보안 위협도 증가하였다. 보안이 중요한 숙박업소 키오스크는 사용자들의 개인 정보뿐만 아니라 사용자들이 특정 호수에 몇 박 이용하는지의 정보가 저장되어 있다. 이는 숙박업소 키오스크의 경우 보안이 취약하다면 사용자들의 개인 정보 유출, 숙박 호수 변경 등은 물론 다른 범죄까지 노출되는 환경을 제공한다.

따라서 키오스크 이용 시 결제 변경 및 결제 취소가 가능하고 키오스크 체크인의 보안성과 신뢰성을 강화한 새로운 시스템이 필요하다.

4. 시스템 제안

사용자가 키오스크를 이용하여 결제하면, 결제 정보는 즉시 블록으로 생성된다. 이 결제 정보에는 결제 시간, 사용자가 사용한 카드의 승인 번호, 사용하는 호실, 금액 등의 정보가 저장되어 있다. 블록에 저장된 정보는 사용자, 모든 가맹점에서 언제든지 데이터 열람을 하거나 저장할 수 있다.



[그림 1] 키오스크를 이용한 스마트 체크인

키오스크를 통해 저장된 블록 정보는 키오스크에 저장되고, 사용자는 결제 직후, 앱으로도 블록에 저장된 해당 데이터 열람이 가능하며 데이터 저장 또한 가능하다. 영수증이 따로 없더라도 모바일에 저장된 데이터를 이용하여 결제 취소, 변경이 가능하다.



[그림 2] 앱으로 결제 확인, 변경 가능

Tendermint 기반의 블록체인을 활용하여 본사는 가맹점의 매출 관리와 고객들의 선호도 조사가 가능하다.

사용자, 키오스크, 숙박업소의 가맹점은 각각 고유의 코드를 갖는다. 키오스크에서 결제된 정보는 가맹점, 사용자, 키오스크 순서대로 저장되어 블록에

저장된다. 이 블록 정보의 공유가 가능하여 본사에서도 블록 확인이 가능하고, 동일 숙박업소의 다른 가맹점을 찾는 사용자의 이전 정보를 확인하여 사용자가 선호하는 호실을 추천해 주거나 포인트를 적립해주는 등의 마케팅 효과를 얻을 수 있다.

	기존 키오스크	제안 키오스크
결제 변경&취소	불가능	가능
가맹점 간의 호환성	불가능	가능
개인 정보 유출 위험성	높음	매우 낮음
결제 금액 위조 가능성	높음	매우 낮음
배정된 호수 위조 가능성	높음	매우 낮음
결제 회전을	높음	기존보다 높음

[표 1] 기존 키오스크와의 비교

5. 결론

본 논문에서는 Tendermint 기반의 블록체인을 활용한 키오스크 스마트 체크인을 제안하였다. 기존 키오스크의 경우 단순히 주문과 결제 정보만을 관계자에게 넘겨주는 역할을 하여 사용자가 결제를 취소하거나 변경하고 싶어도 키오스크에서 결제를 정정할 수 없었다. 이는 키오스크의 장점 중 결제 회전에 영향을 주는 것을 Tendermint 기반의 블록체인을 활용하여 키오스크 자체에서 결제를 변경하거나 취소할 수 있다. 또한, 앱을 이용하여 사용자가 결제 정보 확인이 가능하며 앱에서도 결제를 취소하거나 변경이 가능한 시스템을 제안하였다. 보안에 취약했던 키오스크를 블록체인을 활용하여 새로운 키오스크 시스템을 제안하여 스마트 체크인을 하였을 때 개인 정보와 숙박할 호수에 대한 정보는 보안성을 강화하였고, 결제 정보를 블록에 저장함으로써 결제 금액이나 숙박할 호수에 대한 정보 위조 가능성이 낮은 효과로 키오스크 스마트 체크인의 신뢰성을 강화하였다.

본 제안 시스템은 키오스크를 이용한 스마트 체크인뿐 아니라 키오스크를 이용하는 다양한 분야에

적용될 수 있어 안전하고 결제 회전율이 높은 키오스크 이용이 가능해질 것이다.

참고문헌

- [1] S.M.Lee, S.Y.Shin, Y.S.Kang, S.W.Jeong, S.K.Han, and M.G.Lee, Shared kiosk payment platform based on blockchain Tendermint algorithm, The Korean Institute of Information Scientists and Engineers, 2019, pp 2043-2045.
- [2] S.Nakamoto, "Bitcoin A Peer-to-Peer Electronic Cash System," 2008, Accessed 2017.

블록체인 분산신원증명에 기반한 공적마스크 중복구매 확인 시스템에 대한 연구

노시완*, 장설아*, 이경현**

*부경대학교 일반대학원 정보보호학과

**부경대학교 IT융합응용공학과

nosiwan@pukyong.ac.kr, seolahh1020@gmail.com, khrhee@pknu.ac.kr

A Study on Face Masks Distribution System based on the Blockchain Decentralized Identity

Siwan Noh*, Seolah Jang*, Kyune-Hyune Rhee**

*Department of Information Security, Graduate School,
Pukyong National University

**Department of IT Convergence and Application Engineering,
Pukyong National University

요 약

2020년 1월 국내에 신종 코로나 바이러스의 확산으로 인해 보건 마스크의 수요가 급증하고 이에 따라 마스크의 가격이 폭등하자 정부가 건강보험정보를 기반으로 보건용 마스크 판매에 관여하는 공적 마스크 5부제를 시행해 왔다. 하지만 건강보험 가입정보에 의존적인 신원 인증 시스템으로 인해 유학생 등 건강보험 미가입자의 경우 마스크의 구입이 어렵고 개인정보 접근 문제 등으로 판매채널의 확장이 어려운 문제가 있었다. 본 논문에서는 건강보험과 같은 특정 신원정보 시스템에 의존하지 않고 중앙기관이 발행하는 신뢰할 수 있는 모든 신원정보(여권, 외국인등록증 등)에 기반하여 사용자가 스스로 자신의 신원정보 속성을 블록체인을 통해 관리하는 방법을 제안한다. 또한 제안 방법에 대해 디지털신원 기법을 평가할 수 있는 지표를 기반으로 자체 평가를 수행한다.

1. 서론

2020년 1월 국내에서 첫 번째 코로나 바이러스 감염증(COVID-19) 환자가 발생하고 점차 확진자가 증가함에 따라 보건 마스크 수요가 급증하였고 이에 따라 시중의 마스크의 가격이 폭등하는 상황에서도 여전히 마스크 품귀현상이 빚어질 정도로 공급이 수요를 쫓아가지 못하는 상황이 발생하였다. 이 과정에서 지나친 매점매석으로 시중에서 보건 마스크를 구하기 더욱 어렵게 되자 정부가 개입하여 마스크 공급량을 대폭 늘리고 판매 채널을 제한하는 공적마스크를 도입하였다. 초기에는 농협 하나로마트와 우체국을 공적판매처로 마스크를 판매하였으나 곧 출생년도에 따른 마스크 5부제를 도입하여 현재까지 시행 중에 있다. 마스크 5부제는 기존에 건강보험심사평가원에서 제공하던 의약품안전사용서비스(Drug Utilization Review, DUR)를 사용하여 공적마스크 구매를 1인당 1주일 2매로 제한하여 중복구매를 방지한다. 본래 의사 및 약사가 환자에게 처방된 의약품의 정보를 제공받아 부적절한 약물사용을 사전에

방지하는 것을 목표로 하는 서비스이나 정부에서는 이 항목에 마스크를 추가하여 사용하고 있다.

하지만 현재 사용하고 있는 공적마스크 판매에는 몇 가지 문제점이 존재한다. 첫째, DUR은 건강보험 심사평가원에 등록된 건강보험 가입자 DB에 의존하기 때문에 외국인 등과 같이 건강보험에 가입되지 않은 사용자에게 적용이 어렵다. 둘째, DUR 시스템에 접근하기 위한 권한을 약사 외에 다른 일반인에 부여하기에는 많은 문제가 발생할 수 있기에 판매처를 확장하기 어렵다. 공적마스크 판매 초기에 판매 물품의 유통관리가 효율적인 편의점을 판매처로 추가하는 것에 대한 논의가 있었으나 마스크 수급이 불안정한 시점에서 판매처를 늘리는 것은 의미가 없다고 판단되어 불발되었다. 하지만 편의점을 판매처로 추가하였더라도 DUR과 편의점의 POS(Point of Sales) 시스템의 연동이 어렵고 편의점 직원에게 건강보험 가입자 정보에 접근할 수 있는 DUR 시스템의 관리를 맡기기는 어렵기 때문에 문제가 되었을 것으로 보인다. 마지막으로 마스크 구매자의 프라이버시 노출 문제가 있다. 현재 DUR에 기록된 정보를

확인하기 위해 개인 신분증(주민등록증, 여권, 면허증 등)을 제시하여야하나 이 과정에서 출생년도를 확인하고 DUR에 등록하기 위한 주민등록번호를 제외한 나머지 정보(주소 등)가 판매자에게 노출되는 문제가 존재한다.

본 논문에서는 언급한 문제점들을 해결하고 차후 유사한 상황이 발생 시에 빠르게 구축 및 적용이 가능한 분산신원증명 시스템에 대한 연구를 제안한다.

2. 분산신원증명(DID)

신원(Identity)은 개인을 식별하는 유일한 값으로 주민등록증, 여권 등은 개인의 신원과 속성(Attribute)의 관계에 대해 발급기관이 정의한 전통적인 오프라인 신원인증 수단이다. 반면에 온라인 신원인증은 신뢰기관이 보증한 사용자의 공개키와 오프라인 신원 정보의 결합인 공인인증서를 기반으로 이루어지는데 인증서 발급과정의 불편함이 존재하고 인증과정에서 서비스제공자에게 제공되는 정보에 대한 통제가 발급기관에 존재하는 문제가 있었다.

이에 따라 탈중앙화된 시스템에 대한 관심이 높아지는 가운데 블록체인을 이용한 탈중앙화된 신원(Decentralized Identity, DID)이 제안되었다[1-3]. DID는 사용자의 신원정보를 신뢰기관 없이 스스로 비가역적인 블록체인을 통해 관리하고 신원증명을 중앙화된 기관을 거치지 않으면서도 가능하도록 하여 다양한 분야에서 사용자인증을 제공할 수 있다

<표 1> [5]에서 정의한 신원관리 기법 평가기준

평가기준	설명
사용자 자기제어	사용자를 식별할 수 있는 신원정보는 사용자의 동의하에서만 공개되어야함
제한된 사용	인증에 필요한 정보만 수집되어야 함
정당한 취급자	신원정보는 적합한 접근권한을 가진 사용자들 사이에서만 공유되어야함
신원의 방향성	시스템은 공적인 개체에 대한 단방향 식별자와 사적인 개체에 대한 양방향 식별자를 모두 지원해야 함
다원화 설계	시스템은 다른 신원관리·자격증명 기법과 상호 작용할 수 있어야함
사용자 통합	명확한 인간-기계 통신 메커니즘을 통해 사용자를 시스템의 컴포넌트로 정의해야 함
일관된 사용자 경험	시스템은 사용자에게 간단하면서 일관적인 사용자 경험을 제공해야함

[4]에서 Paul과 Fabien은 블록체인 기반 신원관리 기법 중 ShoCard[1], Sovrin[2], uPort[3]를 선택하여

[5]에서 정의하는 신원관리 기법의 평가기준에 기반하여 각각을 평가하였다. 정의된 평가기준은 표 1과 같다. 3장에서는 기존의 신원관리 기법을 기반으로 한 공적마스크 중복구매 확인 시스템을 설계하고 [5]의 평가기준을 토대로 자체 평가를 실시한다.

3. DID 기반 중복구매 확인 프로토콜

[4]에서 Paul과 Fabien은 분산신원관리 기법을 중앙 기관 없이 사용자가 스스로 자신의 신원과 속성을 정의하고 관리하는 자기주권신원(Self-sovereign Identity)과 기존에 존재하는 중앙 기관이 발급한 신원(여권 등)에 대해 블록체인을 이용한 검증 서비스를 제공하는 분산된 신뢰 신원(Decentralized trusted Identity)으로 구분하였다. 제안하는 시스템은 중앙 기관인 정부가 마스크와 같은 공적 판매가 필요한 물품의 판매과정에서 사용자가 가진 특정 속성(마스크 구매여부)를 탈중앙화된 방식으로 검증하는 것이 목적이므로 분산된 신뢰신원 형태의 설계가 적절하다.

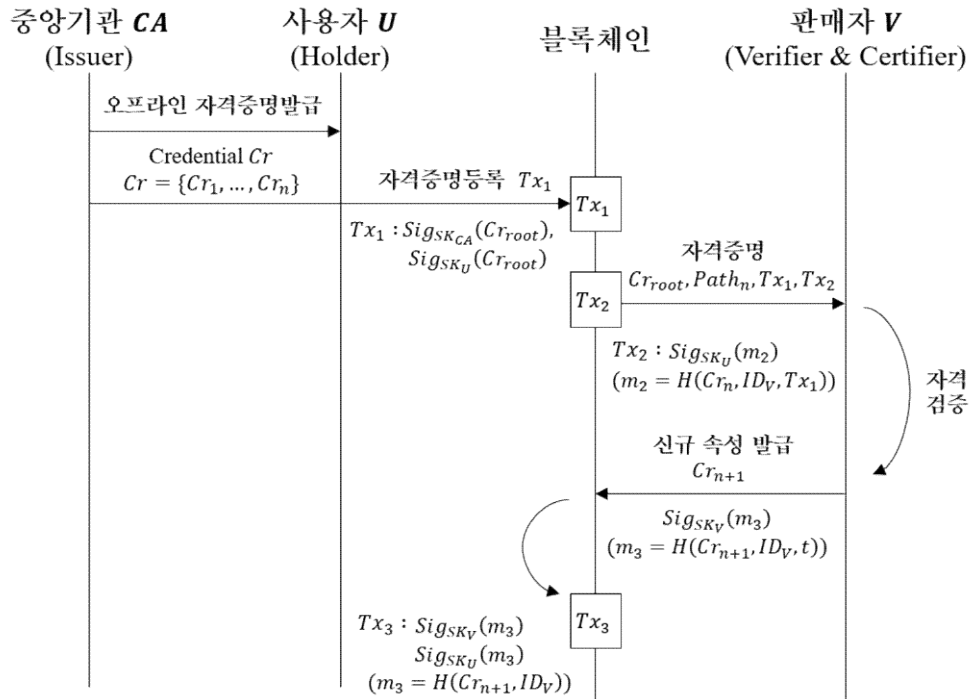
제안시스템에서 중앙기관(정부, Issuer)은 사용자(Holder)에게 신뢰할 수 있는 자격증명을 부여한다. 사용자는 발급받은 자격증명을 블록체인에 기록하고 중앙기관이 인가한 판매자(Verifier)를 통한 마스크 구입 시 신원에 대한 검증 및 새로운 속성(마스크 구매여부)을 신원정보에 추가한다. 여기서 판매자는 사용자에게 대한 새로운 속성을 부여하는 기관(Certifier)의 역할을 수행한다. 제안시스템의 세부적인 절차는 그림 1과 같다.

■ 자격증명등록

사용자(U)는 여권, 운전면허증과 같이 중앙기관(CA)에서 발급하는 오프라인 자격증명을 가지고 있다는 가정 하에 오프라인 자격증명에 있는 각 속성(이름, 주민번호, 주소 등)에 대한 부분집합들(예:[이름],[이름,주소],...)을 선택하고 선택된 부분집합들을 이용하여 머클트리(Merkle tree)를 생성, 머클 루트 값 Cr_{root} 를 계산한다. 사용자와 중앙기관은 Cr_{root} 에 대한 서명을 생성하여 블록체인에 기록한다(Tx1).

■ 자격증명검증 및 신규속성 발급

사용자는 Tx1의 서명에 사용된 비밀키와 동일한 키를 사용하여 마스크 구매를 시도한다. 이 과정에서 마스크 구매에 필요한 자격증명 부분집합 Cr_n 과



(그림 1) 제안시스템 세부 과정

이를 검증하기 위한 Cr_{root} 및 머클경로(Merkle path) $Path_n$ 을 제시하고 이에 대한 서명을 비밀키로 생성하여 마스크 판매자에게 전달한다. 판매자는 Tx1에 사용된 비밀키와 제시된 서명에 사용된 비밀키의 동일성 및 자격증명의 유효성을 검증한다.

<표 2> 제안 시스템 평가결과

평가기준	설명
사용자 자기제어	사용자만이 신뢰기관으로부터 자신에게 발급된 자격에 대한 권한을 가지며 이는 스마트계약에 해당하는 비밀키로 관리됨
제한된 사용	사용자는 오프라인 자격증명에 포함된 자격을 부분집합으로 구성하여 공개하고 싶은 자격만 증명에 사용할 수 있음
정당한 취급자	자격정보는 블록체인 상에서는 해시값으로 기록되고 정보취급자에게만 자격검증을 위한 원본값이 제공됨
신원의 방향성	단방향(unidirectional) 신원만을 제공
다원화 설계	시스템은 비트코인, 이더리움과 같은 퍼블릭 블록체인 상에서 동작하는 것을 가정하여 상호운용성을 보장하는 기술을 사용하여 다른 신원관리 시스템과 연동 가능
사용자 통합	모바일 앱 형태로 서비스 제공 가능, 사용자 인증은 신분증을 보고 입력하는 과정없이 간편하게 이루어지며 타인의 신분증 도용 불가능
일관된 사용자 경험	모바일 앱에서 QR코드를 이용한 인증 등을 통해 자격증명 과정을 간소화하여 간편하게 서비스를 제공할 수 있음

자격검증 후 판매자는 마스크 판매 및 사용자의 속성에 마스크 구매에 대한 속성 Cr_{n+1} 을 자신의 서명을 통해 추가한다.

각 과정은 별도의 스마트계약을 통해 이루어지며 사용자의 초기 자격증명을 관리하는 계약 A와 이 계약과 연동되어 사용자의 속성을 관리하는 계약B의 연동으로 동작한다. 제안 시스템에 대한 자체평가 결과는 표 2와 같다.

4. 결론

본 논문에서는 최근까지도 이슈가 되고 있는 공적 마스크 구입에 필요한 자격증명에 대해 블록체인을 이용한 방식을 제안하였다. 제안 시스템은 이더리움 블록체인과 같은 퍼블릭 블록체인 상에서 구현이 가능하고 비밀키 관리 및 서명용 모바일 애플리케이션과 스마트계약만으로 구축이 가능하고 사용자에게 부여가능한 속성에 대해 제약이 없으므로 좀더 유연하게 다양한 상황에 대응할 수 있을 것으로 기대한다.

사사표기

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음(IITP-2020-2015-0-00403)으며 일부는 2018년도 정부(과학기술정보통신부)의 재원으로 한

국연구재단의 지원을 받아 수행된 연구임 (No. NRF-2018R1D1A1B07048944)

참고문헌

- [1] “Identity Management Verified Using the Blockchain,” ShoCard Whitepaper, 2017.
- [2] A. Tobin and D. Reed, “The Inevitable Rise of Self-Sovereign Identity,” The Sovrin Foundation, 2016.
- [3] C. Lundkvist et al., “uPort: A Platform for Self-Sovereign Identity,” 2017.
- [4] P. Dunphy and F. A. Petitcolas, “A first look at identity management schemes on the blockchain,” IEEE Security & Privacy, vol. 16, no. 4, pp. 20 - 29, 2018.
- [5] K. Cameron, “The laws of identity,” Microsoft Corp, vol. 12, pp. 8 - 11, 2005.

블록체인 기반의 디지털 신원증명 동향

이정현*, 서화정**

*한성대학교 컴퓨터공학부

**한성대학교 IT융합학부

sjeonghyeonz@gmail.com, hwajeong@hansung.ac.kr

Trends of Blockchain-based Digital Identity

Jeong-Hyeon Lee*, Hwa-Jeong Seo**

*Dept. of Computer Engineering, Hansung University

**Dept. of IT convergence Engineering, Hansung University

요 약

개인 정보의 유출은 유출된 당사자에게 단순 정보 유출을 넘어서 2차적인 피해를 주기 때문에 개인 정보 보호에 대한 중요성은 높아지고 있지만 오늘날까지 개인 정보 유출 사고는 끊임없이 발생하고 있다. 현재 널리 사용되고 있는 디지털 신원인 중앙 집중형 ID(Centralized Identity)는 사용자가 스스로 신원을 생성, 제어, 관리할 수 없어 개인 정보 유출 및 오남용이 쉬운 구조이다. 이러한 문제를 해결하기 위해 개인이 스스로 자신의 신원을 관리 및 통제할 수 있는 블록체인 기반의 디지털 신원의 필요성이 제기되었다. 본 논문에서는 디지털 신원(Digital Identity)의 종류와 현재 국내외에서 연구하고 있는 블록체인 기반의 신원증명 기술에 대한 동향을 살펴본다.

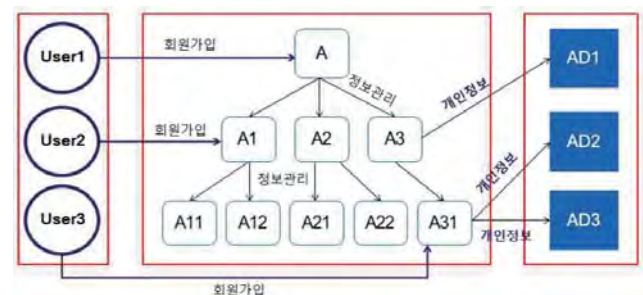
1. 서론

인터넷의 발전에 따라 단순히 정보를 공유하는 것을 넘어서 오늘날에는 실질적인 가치나 콘텐츠를 제작하고 공유한다. 이러한 변화를 통해 시간적, 공간적 제약이 따랐던 이전과 달리 인터넷을 통해 비교적 제약 없이 서비스 이용이 가능해졌다.

사용자는 각 서비스마다 회원가입 시 신원 정보를 입력한다. 이 때, 비밀번호는 보안을 위해 복잡한 형식으로 설정할 것을 요구한다. 대다수의 사용자는 계정 정보를 기억에 의존하기 때문에 ID와 비밀번호를 유사하게 설정한다. 그리고 서비스 이용을 위해 개인정보 수집 및 활용, 위탁 관리와 같은 필수약관에 동의한다. 이로 인해, 사용자는 원하는 서비스를 위해 특정 서비스에 가입하지만 사용자의 정보는 해당 회사의 계열사 및 위탁관리업체에 넘어가기 때문에 사용자가 서비스에 가입할수록 개인정보는 더 많은 곳에 제공된다.[1] 이러한 구조는 해킹하기 쉽게 만들고 한 사이트에서 개인 정보가 유출되면 타 사이트의 계정도 영향을 미쳐 보안성을 저하시킨다. 유출된 개인 정보는 단순히 유출에 그치지 않고 범죄에 이용되거나 경제적 피해를 주기도 한다.[2]

또한 World bank의 데이터에 따르면 약 10억 명이 법적 신원 없이 살고 있다.[3] 자신의 신원을 증

명하지 못하면 삶의 질과 기회에 있어 매우 제한적이고 최악의 경우, 기본권조차 보장받지 못한다. 국가 차원에서도 세금을 징수하거나 정책을 이행하고 범죄자를 식별하는 등 안정적인 사회 운영과 관리를 위해 신원확인도 중요하다.



(그림 1) 개인정보 보안 및 관리에 대한 문제점[4]

본 논문에서는 위와 같은 문제를 해결하기 위한 블록체인 기반의 디지털 신원과 연구되고 있는 ID 관리 기술에 대한 동향을 살펴보도록 한다.

2. 블록체인

블록체인(Blockchain)은 P2P(Peer-to-peer) 기술을 기반으로 중앙 기관 없이 모든 참여자가 거래 정보를 검증하여 원장에 기록하고 공유하여 데이터의 무결성과 신뢰를 보장하는 기술이다.

트랜잭션들에 해시 함수를 적용해 생성한 해시 값을 블록에 저장하고, 추가로 생성한 해시 값은 다음 블록에 저장한 후 이전 해시 값과 연결 지어 체인을 형성한다. 이를 통해 하나의 거래 정보가 변경되면 연달아 뒤에 있는 블록체인의 해시 값이 모두 변경되므로 특정 노드가 임의로 정보를 조작하는 것을 어렵게 함으로써 정보의 무결성을 유지한다. 또한 모든 노드들은 모든 트랜잭션에 대한 전체 기록을 공유하게 된다. 블록체인의 구조적인 특징으로 인해 체인이 길어질수록 임의의 참여자에 의해 데이터 위변조가 불가하며, 참여자 간 P2P 네트워크를 통해 완전히 정보가 공유되기 때문에 전체 시스템이 중단되는 단일 장애점 위험에 대비할 수 있고 데이터 보호 비용을 감소시킨다는 장점을 가진다.

3. 블록체인 기반의 디지털 신원

3.1 신원

신원(Identity)은 한 사람이 누구인지 정의하는, 다른 사람들과 구분되는, 개개인을 식별하는 이름, 직업, 주소와 같은 정보를 의미하며, 디지털 신원(Digital Identity)은 컴퓨터 시스템 상에서 개인 및 그룹 사용자들 각각을 구분하고 이에 따른 권한 부여 및 서비스를 제공하기 위해 사용되는 정보를 의미한다. 기존 신원정보를 포함하여 아이디와 패스워드 등이 디지털 신원에 해당한다.[1]

3.2 종류

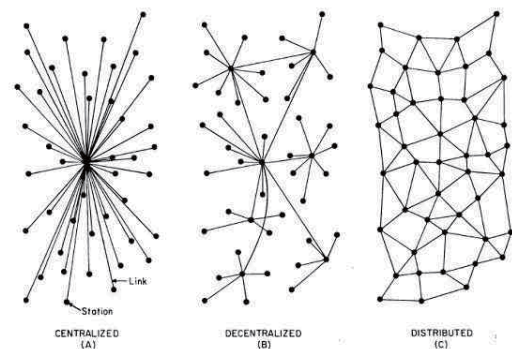
디지털 신원은 중앙 집중형 ID(Centralized Identity), 연합형 ID(Federated Identity), 사용자 중심형 ID(User-centric Identity), 자기주권형 ID(Self-sovereign Identity)로 진화하고 있다.[5]

중앙 집중형 ID는 사용자가 각 사이트에 계정을 만들 때 정보를 일일이 입력하며 이 정보를 기업이 개인 정보 제공 및 활용 동의를 받아 서버에 저장하고 관리한다. 이러한 구조에서는 사용자 스스로 개인 정보를 관리하고 통제하기 어렵고 개인 정보 유출 및 오남용 문제가 발생하기 쉽다.

연합형 ID는 OpenID, OAuth 등을 기반으로 기존 사용자의 소셜 미디어 계정으로 다른 애플리케이션이나 사이트에 로그인하는 형태이다. 계정 생성의 번거로움이 줄어들었지만 특정 대기업이나 서비스에 의존하기 때문에 개인 정보 유출 위험이 여전히 존재한다.

사용자 중심형 ID는 신원 입증을 요구하는 자와 신원을 입증하고자 하는 두 당사자 사이에 신분증, 여권과 같은 기존의 신뢰할 수 있는 신원증명 제공자가 신원증명을 수행하고, 추후 제3의 기관에 의한 유효성을 검증하기 위해 입증 내용을 분산 원장에 기록하는 방식이다. 탈중앙형 네트워크의 모형과 유사한 구조로 연합형 ID와 비슷하지만 특정 기업이나 서비스가 아닌 기존의 신원증명 방식을 사용하기 때문에 일반적으로 오프라인에서의 신원 확인을 병행한다.

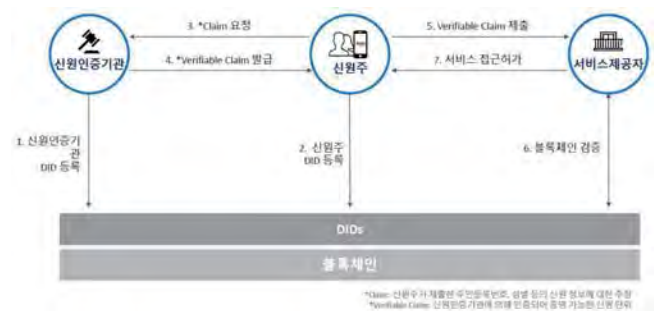
자기 주권형 ID는 사용자 스스로 자신의 정보를 저장하고 소유하기 때문에 중앙기관이 필요 없으며, 스스로 통제하기 때문에 유출 가능성이 없는 신원이다. 분산 네트워크의 모형과 유사한 구조를 가지며 신원은 분산 ID 공개키, 신원 소유자가 공개하고자 하는 기타 모든 공개 자격 증명 및 상호작용을 위한 네트워크 주소를 포함하는 분산 ID 문서와 함께 블록체인에 저장된다.



(그림 2) 디지털 신원의 종류에 따른 모형[6]

3.3 신원증명 시스템

국내외로 블록체인을 기반으로 한 신원 증명 서비스를 제공하기 위해 연합체를 형성하고 많은 기업들이 파트너로써 참여하고 있다. 다양한 시스템과 연합들이 존재하지만 대표적인 서비스 위주로 살펴보고자 한다.



(그림 3) DID 서비스 흐름[7]

3.3.1 해외

3.3.1.1 ShoCard

ShoCard는 사용자가 신원을 주민등록증, 여권, 운전면허증 같은 기존의 신뢰할 수 있는 자격 증명으로 생성하여 데이터를 단말기에 저장하게 한다. 사용자는 직접 생성한 신원의 공개 범위를 제어할 수 있으며 초대받은 관련 당사자에게만 신원을 공개한다. 많은 데이터 중 공유할 데이터 일부를 선택함으로써 검증할 데이터를 최소화한다. 개인 식별 정보의 해킹을 방지하기 위해 ShoCard 시스템은 개인 식별 정보는 블록체인이 아닌 단말기에 저장하고 검증 정보만 블록체인에 저장함으로써 이동성을 가진다. 또한, ShoCard 알고리즘은 다양한 블록체인에 독립적으로 존재해 투명성을 확보하였으며 다른 블록체인에서도 동작하기 때문에 일부 블록체인이 동작하지 않더라도 신원은 유효하게 남는 지속성을 가진다.[8][9]

3.2.1.2 Sovrin

Sovrin은 허가된 분산 원장을 기반으로 구축된 분산 신원 네트워크다. 공개 표준과 오픈 소스인 Hyperledger Indy 프로젝트를 기반으로 하여 공개적인 네트워크지만 크리덴셜(Credential)이라 불리는 은행, 대학, 정부 등과 같은 신뢰할 수 있는 기관들만이 보안성과 확장성에 초점을 둔 분산 합의 프로토콜에 참여하는 노드를 실행함으로써 원장이 허가된다. 사용자는 어떤 신원을 사용할지 선택할 수 있고, 속성에는 사용자가 지정한 사람이나 사용자에게 위임을 받은 대리인만 접근하며, 영지식 증명을 기반으로 전체 속성 중 공개하고 싶은 속성을 선택함으로써 데이터를 최소화한다. 모든 상황이나 관계에 대해 별도의 신원을 부여하는 양방향 식별자를 지원하기 때문에 제3자가 사용자의 신원에 접근하여 유출시키더라도 다른 곳에서 해당 신원을 사용할 수 없게 되고, 사용자는 문제 상황을 감지해 신원을 변경할 수 있다. 처음부터 이 관계에서만 유효한 신원을 당사자 간에 공유했기 때문에 변경한 신원은 다른 관계에는 영향을 미치지 않는다. ShoCard와 달리 신원들은 제3자인 재단이 소유하기 때문에 이동성은 없다.[8][10]

3.2.1.3 uPort

uPort는 모든 사람들에게 분산 신원을 제공하는 것이 목표인 오픈소스 분산 신원 프레임워크로, 이더리움 분산 원장에 차세대 DApp과 이메일, 은행과

같은 기존의 중앙 집중식 애플리케이션용 신원 관리에 사용된다.

uPort는 모바일 애플리케이션, 개발자 라이브러리, 스마트 컨트랙트로 구성된다. 모바일 애플리케이션에는 신원 관련 데이터와 사용자의 키를 보관하여 사용자가 중앙기관 없이 스스로 신원을 생성, 제어 및 접근하고 다른 사람이 정보를 사용하기 전에 동의 여부를 확인한다. 개발자 라이브러리는 타사의 개발자가 uPort에 대한 지원을 자신의 앱에 통합하는 방법을 지원한다. 스마트 컨트랙트에는 컨트롤러와 프록시가 있다. 컨트롤러는 신원 형성의 주요 부분을 담당하며, 친구나 가족 같은 개인이나 은행, 신용조합 같은 기관이 복구 대리인 명단에 등록되어 있다가 사용자가 모바일 기기를 분실했을 경우 복구 대리인들이 투표해 정족수가 넘으면 사용자 신원을 복구하는 로직을 관리한다. 오직 다른 uPort 신원만 입증할 수 있기 때문에 이동성이 부족하다.

속성 데이터 구조 내 특정 속성은 개별적으로 암호화되지만, 신원 제공자, 이용자와의 관계나 특정 속성에 대한 메타 데이터가 유출될 수 있는 전체 JSON 데이터 구조가 표시되기 때문에 레지스트리에 과도하게 의존하면 정보가 유출될 수 있다. 또한 스마트 컨트랙트에 대량의 데이터를 저장하는 것은 비효율적이므로 JSON 속성 구조의 해시만 레지스트리에 저장하고 데이터 자체는 오픈 분산 원장 데이터 저장소인 IPFS에 저장하여 레지스트리로 저장된 데이터를 참조한다.[8][11]

3.2.2 국내

3.2.1 MyID

마이아이디(MyID)는 개인정보를 자신의 단말기에 저장하고, 인증할 때 필요한 정보만 골라 제출할 수 있게 하는 블록체인 기반 전자 신원증명 플랫폼이다. 통합된 ID 플랫폼을 사용함으로써 신원증명절차를 간소화하여 하나의 신원으로 다양한 곳에서 증명할 수 있게 되었고, 신원 정보는 생체인증을 통해 활성화함으로써 보안성을 강화하였다.

금융위원회 샌드박스를 통해 독점적 라이선스를 획득함에 따라 금융 서비스에 특화된, 국내에서 유일하게 금융실명법과 전자금융법에서 요구하는 금융권 실명 신원 확인이 가능한 분산 ID이다. 또한 국내 최초로 분산 ID 관련 W3C Method Registry를 등록하고 실 서비스를 오픈함으로써 검증된 안정적 기술력을 가졌다.[12]

3.2.2 Initial

국내 주요 통신사들을 중심으로 한 컨소시엄형 블록체인 네트워크로 각종 증명서 등을 담을 수 있는 지갑 형태의 앱을 개발하여 출시 예정에 있다. 규모는 다른 두 연합체보다 제일 작지만, 중소기업이 중심인 타 연합체와는 달리 대기업이 주도하고 파트너사도 대기업들이기 때문에 빠른 대중화가 용이하다.

3.2.3 DID Alliance Korea(DAK)

분산형 ID 서비스를 표준화된 한 체계 안에서 만들어야 한다는 필요성이 제기됨에 따라 2019년, 미국과 한국이 공동 주도하여 DID Alliance를 출범시키면서 국내에서 진행되는 활동을 담당하기 위한 DID Alliance Korea도 생겼다. 앞서 살펴본 두 협의체는 특정 기업이 주도하여 분산 ID 서비스를 제공한다면, DAK는 상위 개념인 디지털 신원증명이나 분산 ID 표준화 제정과 운영체계 구축 등을 논의한다.

4. 결론

본 논문에서는 디지털 신원의 진화 과정을 살펴보고 기존의 중앙 집중식 신원관리 시스템의 문제점을 해결하기 위해 연구되고 있는 블록체인 기반의 디지털 신원과 시스템에 대해 살펴보았다.

분산 ID를 사용하면 신원증명 절차 간소화로 간편함을 제공하고 인증과 관련한 시간적, 물질적 비용을 절감함과 동시에 기업에서도 개인 정보 관리에 대한 부담과 비용을 줄일 수 있다는 경제적인 효과와 동시에 스스로 신원을 관리해 개인 정보 유출 및 오남용과 그에 따른 2차적 피해를 줄일 수 있다.

이러한 장점 때문에 현재 다양한 디지털 신원 중 사용자가 중앙기관의 개입 없이 신원을 생성 및 제어할 수 있는 자기 주권형 ID가 세계적으로 활발하게 연구 및 개발되고 있다. 해외에서는 이미 실생활에 분산 ID를 적용한 사례가 있지만[13], 국내에서는 지난 2020년 3월 31일에 분산 ID의 금융보안표준이 제정되었으며, 현재 서비스를 앞두고 있거나 서비스는 출시되었지만 사용자 확보가 미흡한 상황이다. 대한민국의 잘 갖춰진 신원확인 시스템을 바탕으로 분산 ID에서도 금융권을 비롯한 다양한 산업과 해외 서비스와의 상호운용성이 확보된다면 글로벌 분산 ID 시장을 선점할 수 있을 것이다.

참고문헌

- [1] Han-Jae Jeong. "Design and Implementation of Blockchain Based Digital Identity Management System", Soongsil University, Dec. 2017.
- [2] "개인정보 유출 뭐가 문제죠?", JoongAng Ilbo, 2014.03.26.
<https://news.joins.com/article/14259415> (2020.01.23.)
- [3] "ID4D Data: Global Identification Challenge by the Numbers", World bank, June, 2018.
<https://id4d.worldbank.org/global-dataset> (2020.01.23.)
- [4] Kwang-Hee Jang. "Design of Personal Information Security and Utilization System Structure Using Blockchain Technology", Hanyang University, Aug, 2019.
- [5] Jae-Hoon Na. "Blockchain Identity Management and Privacy Standard Trend", Journal of the Korean Telecommunications Society, vol. 36, no. 7, pp.20-25 Jun, 2019.
- [6] Paul Baran. "Centralized, Decentralized and Distributes Systems", Rand Corporation, Sep, 1962.
- [7] Sun-Kyu Park, "Digital Signature-Based Digital Identification System Implementation and Use Cases", IconLoop, Aug, 2019.
- [8] van Bokkem, D., Hageman, R., Koning, G., Nguyen, L., & Zarin, N. "Self-sovereign identity solutions: The necessity of blockchain technology", arXiv preprint arXiv:1904.12816., Apr, 2019.
- [9] ShoCard Whitepaper, "Identity Management Verified Using the Blockchain", Jan. 2018.
- [10] Sovrin Whitepaper, "A Protocol and Token for Self-Sovereign Identity and Decentralized Trust", Jan. 2018.
- [11] uPort Whitepaper, "A Platform for Self-Sovereign Identity", Oct. 2016.
- [12] MyID Alliance Intorduction, "MyID Alliance Introduction", Apr, 2020.
- [13] "英서는 DID로 담배 구매... "한국도 표준화 작업 서둘러야"", The Block Post, 2019.12.18.,
<https://www.fnnews.com/news/201912181715015337> (2020.01.23.)

로컬 특징 기반 글로벌 이미지를 사용한 CNN 기반의 악성코드 분류 방법

장세준, 성연식*
동국대학교 멀티미디어공학과
sejun@dongguk.edu, sung@dongguk.edu

Convolutional Neural Network-based Malware Classification Method utilizing Local Feature-based Global Image

Sejun Jang, Yunsick Sung*
Dept. of Multimedia Engineering, Dongguk University-Seoul

요 약

최근 악성코드로 인한 피해가 증가하고 있다. 악성코드는 악성코드가 속한 종류에 따라서 대응하는 방법도 다르기 때문에 악성코드를 종류별로 분류하는 연구도 중요하다. 기존에는 악성코드 시각화 과정을 통해서 생성된 악성코드의 글로벌 이미지를 사용해 악성코드를 각 종류별로 분류한다. 글로벌 이미지를 악성코드로부터 추출한 바이너리 정보를 사용해서 생성한다. 하지만, 글로벌 이미지를 사용해서 악성코드를 각 종류별로 분류하는 경우 악성코드의 종류별로 중요한 특징을 고려하지 않기 때문에 분류 정확도가 떨어진다. 본 논문에서는 악성코드의 글로벌 이미지에 악성코드의 종류별 특징을 나타내기 위한 로컬 특징 기반 글로벌 이미지를 사용한 악성코드 분류 방법을 제안한다. 첫 번째, 악성 코드로부터 바이너리를 추출하고 추출된 바이너리를 사용해서 글로벌 이미지를 생성한다. 두 번째, 악성 코드로부터 로컬 특징을 추출하고 악성코드의 종류별 핵심 로컬 특징을 단어-역문서 빈도(Term Frequency Inverse Document Frequency, TFIDF) 알고리즘을 사용해 선택한다. 세 번째, 생성된 글로벌 이미지에 악성코드의 패밀리별 핵심 특징을 픽셀화해서 적용한다. 네 번째, 생성된 로컬 특징 기반 글로벌 이미지를 사용해서 컨볼루션 모델을 학습하고, 학습된 컨볼루션 모델을 사용해서 악성코드를 각 종류별로 분류한다.

1. 서론

최근 다양한 기술들의 발달로 인해 정보 보호의 중요성이 높아지고 있다. 해커는 특정 컴퓨터에 대한 권한을 악성코드를 사용해서 탈취한다. 해커는 획득한 권한을 사용해 특정 컴퓨터에 저장되어 있는 중요 정보를 변조하거나 탈취한다. 예를 들어, 슈퍼인텔리전스 기반의 XR SW 플랫폼으로부터 발생한 K-pop 통합 데이터를 해커로부터 보호하기 위해서 악성코드의 탐지 및 분류 과정이 필요하다.

글로벌 이미지는 악성코드의 전체 바이너리 정보를 사용해 악성코드 자체를 시각화한 이미지다. 악

성코드로부터 추출한 바이너리 정보를 8bit 단위로 나누고 나뉜 8bit를 하나의 픽셀로 사용한다. 8bit는 0에서 255까지의 수를 표현할 수 있기 때문에 그레이스케일 이미지의 픽셀로 사용하기 적합하다. 악성코드의 바이너리 정보는 연산 코드, 응용 프로그램 프로그래밍 인터페이스 그리고 동적 링크 라이브러리 등의 정보를 포함하기 때문에 악성코드의 글로벌 이미지를 사용하면 악성코드의 전체적인 구조와 함께 작은 변화를 감지할 수 있다. 변종 악성코드 분류가 가능하다. 하지만, 악성코드의 글로벌 이미지만 사용해서 악성코드를 분류할 경우 패밀리별 악성코드의 행위를 고려할 수 없는 단점이 있다.

이 논문에서는 로컬 특징 기반의 글로벌 이미지를 사용한 악성코드 분류 방법을 다음과 같이 제안한다: 첫 번째, 악성코드로부터 바이너리 정보를 추출해서 악성코드의 글로벌 이미지를 생성한다. 두 번째, 악성 코드로부터 로컬 특징을 추출하고 단어-역문서 빈도

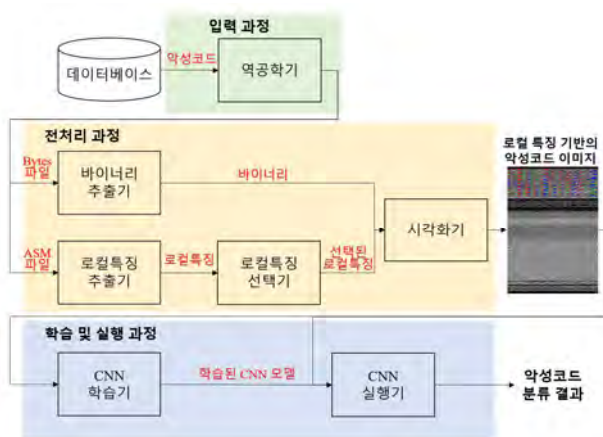
* 교신저자: 성연식 (sung@dongguk.edu)

"본 연구는 과학기술정보통신부 및 정보통신기획평가원의 글로벌핵심인재양성지원사업의 연구결과로 수행되었음(2019-0-01585)"

(Term Frequency Inverse Document Frequency, TFIDF) 알고리즘을 사용해서 악성코드의 패밀리별 중요 로컬 특징을 선택한다. 세 번째, 악성코드의 글로벌 이미지에 선택된 로컬 특징을 RGB 픽셀화해서 적용한다. 제안하는 로컬 특징 기반의 글로벌 이미지를 사용한 악성코드 분류 방법은 악성코드의 글로벌 이미지에 악성코드의 종류별 핵심 특징을 포함한다. 악성코드의 전체 구조와 로컬 특징을 고려하는 동시에 악성코드의 종류별 중요 특징을 한 장의 이미지에 포함할 수 있다.

2. 로컬 특징 기반 글로벌 이미지를 사용한 악성코드 분류 방법

(그림 1)은 제안하는 방법인 로컬 특징 기반 글로벌 이미지를 사용한 악성코드 분류 방법의 개요를 보여준다. 제안하는 방법은 입력 과정, 전처리 과정 그리고 학습 및 실행 과정으로 나뉜다.



(그림 1) 제안하는 방법 개요.

입력 과정에서는 역공학기가 데이터베이스로부터 악성코드를 입력받아서 역공학 소프트웨어를 사용해 바이트 파일과 ASM 파일을 출력한다.

전처리 과정에서는 입력 과정으로부터 입력된 바이트 파일과 ASM 파일을 사용해서 로컬 특징 기반의 악성코드 이미지를 생성한다. 바이너리 추출기는 바이트 파일을 입력 받아서 바이너리를 출력한다. 로컬특징 추출기는 입력 과정으로부터 입력된 ASM 파일을 입력 받아서 로컬 특징을 추출한다. 로컬 특징은 CPU 명령어인 연산 코드다. 추출된 로컬 특징은 로컬 특징 선택기에 입력된다. 로컬 특징 선택기는 TFIDF 알고리즘을 사용해서 악성코드의 각 패밀리

리별 중요 특징을 선택한다[1]. 바이너리, 로컬 특징, 그리고 선택된 로컬 특징은 시각화기에 입력된다. 시각화기는 입력받은 바이너리, 로컬 특징, 그리고 선택된 로컬 특징을 사용해서 로컬 특징 기반 글로벌 이미지를 출력한다. 시각화기는 바이너리를 8bit 단위로 분할하고, 분할된 8bit 단위의 바이너리를 하나의 픽셀로 사용해서 글로벌 이미지를 생성한다[2]. 8자리의 2진수는 0부터 255까지의 값을 표현할 수 있기 때문에 그레이스케일 이미지의 픽셀로 사용하기 적합하다. 바이너리를 사용해 생성한 글로벌 이미지에 로컬 특징과 선택된 로컬 특징을 사용해서 악성코드의 각 종류별 중요한 특징을 RGB 픽셀로 적용한다.

3. 결론

이 논문에서는 로컬 특징 기반 글로벌 이미지를 사용한 악성코드 분류 방법을 다음과 같이 제안했다. 첫 번째, 데이터베이스로부터 역공학을 사용해서 바이트 파일과 ASM 파일을 추출했다. 두 번째, 바이트 파일로부터 바이너리를 추출하고 8bit 단위로 나눴다. 8bit의 바이너리는 하나의 픽셀로 사용해서 글로벌 이미지를 생성했다. 세 번째, ASM 파일로부터 로컬 특징인 opcode를 추출하고, TF-IDF 알고리즘을 통해 악성코드의 각 종류별 중요한 특징을 선택했다. 추출된 로컬 특징과 선택된 로컬 특징을 사용해서 시각화 과정을 통해 로컬 특징 기반 글로벌 이미지를 생성했다. 네 번째, 로컬 특징 기반 글로벌 이미지를 통해서 악성코드를 각 종류별로 분류했다.

사사표기

"본 연구는 과학기술정보통신부 및 정보통신기획평가원의 글로벌핵심인재양성지원사업의 연구결과로 수행되었음(2019-0-01585)"

참고문헌

- [1] H Zhang, X Xiao, F Mercaldo, S Ni, F Martinelli, A K Sangaiah, "Classification of Ransomware Families with Machine Learning based on N-gram of Opcodes", Computers & Electrical Engineering, 77, 366-375, 2019.
- [2] Kesav K, Srinivas M, "Image Visualization based Malware Detection", 2013 IEEE Symposium on Computational Intelligence in Cyber Security (CICS). IEEE, Singapore, Singapore, 2013.

IoT 센서를 이용한 블록체인 기반 식품 공급망 개발

심재익*, 김왕록*, 전미현*, 오동의*, 정병규**, 신상욱*

*부경대학교 IT융합응용공학과

**부경대학교 대학원 정보보호학과

wodlr2007, korgnawmik, jmh3850@naver.com, deo1915@gmail.com,

holine0622@pukyong.ac.kr, shinsu@pknu.ac.kr

Development of Blockchain-based Food Supply Chain Using IoT Sensors

Jae-Ik Sim*, Wang-Rok Kim*, Mi-Hyeon Jeon*, Dong-Eui Oh*,

Byeong-Gyu Jeong**, Sang Uk Shin*

*Dept. of IT Convergence and Application Engineering, Pukyong National University

**Dept. of Information Security, Graduate School, Pukyong National University

요 약

현 식품 공급망은 중앙 집중화되어 있고, 투명하지 않으며 복잡한 시스템으로 인해 많은 문제점이 존재한다. 판매자는 싼값에 팔고 소비자는 비싼 값에 구매하는 문제가 지속적으로 대두되고 있으며 유통 과정에서 생기는 문제에 대한 책임 추적이 어렵다. 본 논문에서는 각 유통 단계에서 생성되는 IoT 센서 데이터를 블록체인 기술에 적용하며 이를 활용하는 방안에 대해 제안한다. 제안 모델을 통해 유통 과정과 데이터에 대한 신뢰성을 확보하고 제품의 원산지, 배송 과정, 보관 상태를 비롯한 유통 정보들을 추적할 수 있다.

1. 서론

현재의 식품 공급망은 중앙 집중화되어 있고, 투명하지 않은 시스템으로 인해 많은 문제점이 존재한다. 그 예로 2018년 5월 미국 캘리포니아 로메인 상추 대장균 검출 사건이 있다. 이는 복잡한 유통과정 때문에 책임 추적이 있어서 2주 이상의 시간이 소요됐다[1]. 이러한 식품 공급망 때문에 상품에 대한 신뢰성을 확보하기 어렵고, 판매자는 싼값에 팔고 소비자는 비싼 값에 구매하는 문제가 지속적으로 대두되고 있다.

블록체인은 탈중앙화라는 특성을 가지고 있어 신뢰기관 없이 거래가 가능하다[2]. 또한 거래 정보를 다수가 공동으로 관리하는 구조로써 거래에 대한 신뢰성과 투명성을 보장한다. 이러한 블록체인을 현 식품 공급망에 적용한다면 거래에 대한 신뢰도를 높일 수 있다. 또한 제품의 출처, 배송 과정, 보관 상태 등에 대한 유통 정보들을 투명하게 공유할 수 있고 유통 과정에서 문제가 발생했을 경우 신속하게 추적할 수 있다.

본 논문에서는 허가형 프라이빗 블록체인 플랫폼인 하이퍼레저 패브릭(Hyperledger Fabric)을 채택하여

블록체인 기반 식품 공급망을 제안한다. 하이퍼레저 패브릭의 채널을 활용해 동일한 비즈니스 목적을 가진 허가 받은 참여자만 데이터를 공유할 수 있다[3]. 이로 인해 데이터에 대한 프라이버시를 보장하고 암호화해 없이 합의를 이룰 수 있다. 또한 ‘최초 1마일’의 문제를 해결하기 위해 IoT 센서를 라즈베리파이가 전처리하고 하이퍼레저 패브릭의 체인코드에 의해 올바른 데이터만 자동 저장되도록 한다.

논문의 구성은 다음과 같다. 2장에서는 관련 연구로 하이퍼레저 패브릭에 대해 살펴본다. 3장에서는 본 논문에서 제안하는 모델의 구성과 데이터 처리에 대해 설명하고, 4장에서 제안 모델에 대해 분석한다. 마지막으로 5장은 본 논문의 결론이다.

2. 하이퍼레저 패브릭

하이퍼레저 패브릭은 허가형 프라이빗 블록체인으로써, MSP(Membership Service Provider)라고 하는 인증 관리 시스템에 등록된 사용자들만 네트워크에 참여할 수 있다[3]. 참여자들은 비즈니스 목적에 알맞은 형태로 블록체인 플랫폼을 구축할 수 있으며 적합한 블록 생성 알고리즘이나 트랜잭션 보증 정책을 직접 구현할 수 있다. 하이퍼레저 패브릭에서는

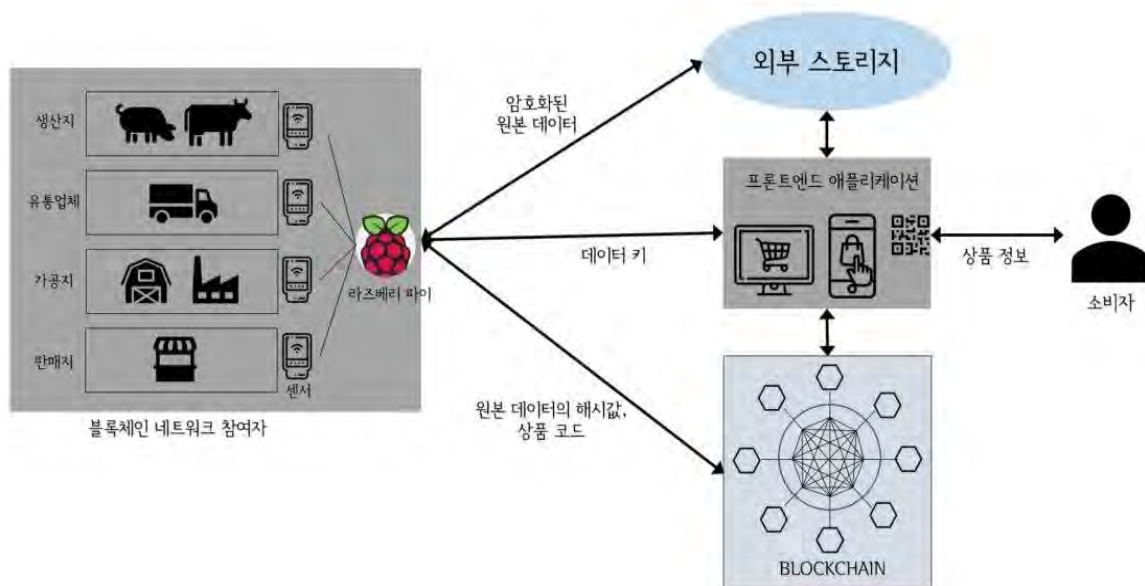
기존 블록체인과 달리 스마트 컨트랙트를 체인코드라고 하며 블록이 생성되고 연결되기까지 실행(Execute), 정렬(Order), 검증(Validation)의 단계를 합친 과정이라고 정의한다.

하이퍼레저 패브릭 네트워크는 MSP, 오더러, 피어로 구성되며, 이들은 채널을 이용하여 통신을 수행한다. 피어는 분산원장과 체인코드를 저장, 실행하는 엔티티이다. 블록체인의 참여자는 피어에 설치된 체인코드를 호출하여 분산원장에 저장된 정보에 접근할 수 있다. 채널은 그룹 간 커뮤니케이션을 가능하게 하는 메커니즘으로 각 채널마다 하나의 분산원장이 존재한다. 이로 인해 기업간의 데이터 프라이버시 보호를 유지할 수 있다. 오더링 서비스(Ordering Service)는 블록 내 트랜잭션의 순서를 정하고 연결된 노드들에게 블록을 전달하는 기능을 한다. 오더러(Orderer)는 오더링 서비스의 주체이며 트랜잭션을 시간 순으로 정렬한 후 최신 블록을 생성한다. MSP는 하이퍼레저 패브릭의 멤버십 관리 기술이며 이를 통해 조직(그룹)의 구조를 설계한다. MSP를 이용하여 참여자들의 권한을 관리하며 디지털 증명서를 발급하는 기능을 수행한다.

3. 제안 모델

본 절에서는 IoT 센서 데이터 처리 방법과 제안 모델의 구조와 특징, 그리고 블록체인 네트워크 구성에 대해 설명한다.

3.1 IoT 센서 데이터 처리



(그림 1) 블록체인 네트워크 구조

유통과정에서 생산지, 가공지, 운송, 판매지에는 IoT 센서가 설치되어 있고 외부의 공격으로부터 안전하다고 가정한다. 생성되는 IoT 센서 데이터의 종류에는 온도, 시간, 위치, 상품 등급, 담당자 정보, 가격, 상품 코드 등이 있다. 유통과정의 각 단계들마다 조금씩 다르게 생성되는 데이터들은 엣지 컴퓨팅이 가능한 라즈베리파이로 수집되고 하나의 트랜잭션으로 생성된다. 블록체인 시스템 계산능력의 과부하를 방지하고 트랜잭션 포맷을 맞추기 위해 라즈베리파이에서 전처리 작업을 수행한다.

기존 공급망 블록체인은 ‘최초 1마일 문제’, 즉 블록체인과 사람이 접촉하는 지점에서 생기는 데이터 신뢰성에 대한 문제가 있다[4]. 제안 모델은 이를 위해 IoT 센서 데이터의 자동입력을 통해 해결한다. IoT 센서에 대한 물리적인 보안과 중간 매개체 역할을 하는 라즈베리파이에 대한 시스템 보안, 데이터를 전송하는 네트워크 보안, 데이터를 처리하는 블록체인의 신뢰가 보장되어야 한다.

3.2 블록체인 네트워크

[그림 1]은 블록체인 네트워크의 구조를 나타낸다.

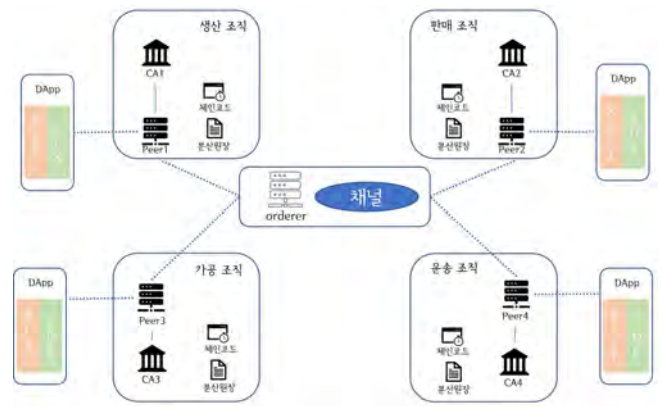
블록체인 시스템 참여자는 식품 유통과정의 각 단계를 표현한 생산지, 가공지, 운송업체, 판매지이다. 각 시스템 참여자들은 하나의 채널로 연결되고, 유통 데이터를 공유한다. 시스템에 참여하기 위해 하이퍼레저 패브릭 MSP로부터 인증을 받아야 한다. 상품을 구매하는 소비자는 블록체인 시스템에 참여하지 않는 클라이언트이다. 따라서 소비자는 블록체

인에 저장된 데이터에 접근할 수 없으며, 체인코드에 의해 지정된 데이터만 별도의 애플리케이션을 통해 확인할 수 있다. 왜냐하면 블록체인에는 추적을 위한 각 단계의 담당자 개인정보가 있는데, 이는 외부로부터 보호되어야 하기 때문이다. 소비자는 상품에 있는 QR코드를 통해 이러한 애플리케이션에 접근이 가능하고, 애플리케이션은 블록체인에 저장된 상품코드를 추적하여 상품의 신뢰성을 판단할 수 있는 최소한의 데이터만 제공한다.

블록체인은 비가역적이다[2]. 따라서 블록체인 시스템 설계에 있어서 높은 전송률과 성능 향상을 위해 블록체인에 저장되는 데이터의 크기는 매우 중요한 요소이다[2]. 제안 모델에서는 최소한의 데이터만 블록체인에 저장하며 용량이 큰 원본 데이터는 외부 스토리지에 저장하는 방식을 취했다. 여기서 외부 스토리지는 클라우드 스토리지이다. 외부 스토리지에는 IoT 센서로부터 생성된 모든 데이터를 암호화해서 저장한다. 암호화에 사용되는 키는 하이퍼레저 패브릭 MSP에 의해 블록체인 시스템의 참여자인지 확인하고 프론트엔드 플랫폼을 통해 분배된다. 여기서 키는 공개키 기반 구조로써 데이터 암호화뿐만 아니라 데이터의 소유권을 주장할 수 있는 디지털 서명의 기능을 한다. 블록체인에는 외부 스토리지에 저장된 원본 데이터의 위치와 무결성 검증을 위한 해시값, 그리고 추적을 위한 상품 코드가 저장된다. 이렇게 데이터를 분리 저장함으로써 데이터에 대한 프라이버시 보호와 안정성을 기여할 수 있다.

4. 제안 모델 개발 및 분석

기존 공급망 관련 블록체인 모델은 [5], [6] 등이 제안되었다. 기존 모델과는 다르게 제안 모델은 ‘최초 1마일’의 문제를 해결할 수 있는 방안과 프라이빗 블록체인에서 상품을 구매하는 소비자와 같은 외부 개체들에 대한 데이터 제공 방법을 제안한다. 또한, 블록체인 네트워크 참여자의 프라이버시 보호를 위해 블록체인과 외부 스토리지로 저장기능을 분리하고, 블록체인에 저장되는 데이터에 대한 프라이버시 보호를 위해 공개키 기반 구조로 암호화하여 저장한다. 거래 당사자의 신뢰성을 위해 이미 인증되고 검증된 노드들만 참가하는 허가형 프라이빗 블록체인을 채택한다. 이로 인해 소비자들은 식품을 구매하는데 있어 신뢰성을 확보할 수 있다. 또한 식품 유통과정 중 발생한 제품 손상이나 사고에 대한 책임 추적도 가능하다.



(그림 2) 하이퍼레저 패브릭 네트워크 구조

하이퍼레저 패브릭 네트워크에는 생산, 가공, 판매, 운송의 4개의 조직이 있으며 각 조직에는 한 개의 peer가 있다고 가정한다. [그림 2]는 하이퍼레저 패브릭 네트워크 구조를 나타낸다. 각 피어는 하나의 채널을 통해 데이터를 공유하고 있으며 동일한 분산 원장을 보유하고 있다. 각 피어들은 DApp(Distributed Application)을 통해 트랜잭션을 생성하고 Orderer 노드에게 전달한다. Orderer 노드는 트랜잭션들을 정렬하고 블록을 생성하면 다시 각 조직의 peer에게 블록을 전달한다. 각 조직의 peer는 받은 블록을 검증하여 각자 보유한 분산원장에 블록을 연결한다.

프론트엔드 개발은 VScode 1.44 버전, 센서 데이터 저장 서버로 ThingSpeak 클라우드 서버와 웹페이지 서버로 netlify를 사용하고 개발 언어로는 HTML 5.0, CSS 2.1, Javascript 1.5 버전을 사용했다. 판매자의 각 상품마다 붙어있는 QR코드를 인식하면 [그



(그림 3) 프론트엔드 웹 애플리케이션

럼 3]과 같은 웹 애플리케이션이 실행된다. 이를 통해 소비자 평점과 식품의 신선도 변화를 수치 및 그래프로 확인할 수 있다.

해당 모델의 전체적인 보안 매커니즘은 블록체인 사용에 기인한다. 데이터 해시를 통해 무결성을 보장한다. 원본 데이터의 해시값이 블록체인에 저장되어 있기 때문에 데이터 참여자는 원본 데이터에 대한 무결성을 검증할 수 있다.

5. 결론

본 연구에서는 IoT를 이용한 블록체인 기반 식품 공급망 모델을 제안하고 적용 방안을 제시했다. 블록체인의 무결성, 안전성, 투명성, 추적성이라는 특징은 안전하고 신뢰성 있는 식품 유통을 가능하게 하고 QR코드를 통해 네트워크 참여자가 아닌 소비자의 블록체인 데이터를 확인할 수 있게 했다. 따라서 소비자들도 안심하고 제품을 구매할 수 있으며 시스템 참여자들은 유통시 발생하는 제품 손상이나 사고에 대한 책임 추적도 가능하다. IoT 센서 데이터를 이용한 자동화된 트랜잭션 처리로 저장되는 데이터에 대한 신뢰성을 달성할 수 있다. 이로 인해 기존 공급망 블록체인에 존재했던 ‘최초 1마일’의 문제를 해결한다. 블록체인 플랫폼으로 허가형 프라이빗 블록체인인 하이퍼레저 패브릭을 채택함으로써 사용자 프라이버시를 보호하고 저장 공간을 블록체인 및 외부 스토리지로 분리함으로써 데이터 프라이버시 보호 및 저장의 효율성을 극대화했다.

향후 운송단계에서의 데이터 전송을 위한 무선 네트워크 환경을 구축하고 IoT 센서와 라즈베리파이의 물리, 시스템 보안구현이 연구 과제로 남아있다.

Acknowledgments

이 논문은 2020년 해양수산부 재원으로 해양수산과학기술진흥원의 지원을 받아 수행된 연구임 (미래수산물 연구센터)

참고문헌

- [1] Astill, G. M., Kuchler, F., Todd, J. E., & Page, E. T. "Shiga Toxin - Producing Escherichia coli (STEC) O157: H7 and Romaine Lettuce: Source Labeling, Prevention, and Business." *American Journal of Public Health*, 110(3), 322-328, 2020.
- [2] Viriyasitavat, W., & Hoonsopon, D. "Blockchain characteristics and consensus in modern business processes." *Journal of Industrial Information Integration*, 13, 32-39, 2019.
- [3] Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Muralidharan, S. "Hyperledger fabric: a distributed operating system for permissioned blockchains" In *Proceedings of the Thirteenth EuroSys Conference*, 1-15, 2018.
- [4] 커넥팅랩, 블록체인 트렌드 2020, 비즈니스북스, 2019.
- [5] Ren, C, Shao, B., Sun, N., & Zhang, B. "Blockchain-based food product shelf-life management." *U.S. Patent Application No. 15/380,476*, 2018.
- [6] Baralla, G., Ibba, S., Marchesi, M., Tonelli, R., & Missineo, S. "A blockchain based system to ensure transparency and reliability in food supply chain." *European conference on parallel processing*. Springer, Cham, 379-391, 2018.

Merging Collaborative Learning and Blockchain: Privacy in Context

Sandi Rahmadika and Kyung-Hyune Rhee*

Department of ITConvergence of Information Security, Graduate School
Pukyong National University, Republic of Korea

*Department of ITConvergence and Application Engineering
Pukyong National University, Republic of Korea

Abstract

The emergence of collaborative learning to the public is to tackle the user's privacy issue in centralized learning by bringing the AI models to the data source or client device for training. Collaborative learning employs computing and storage resources on the client's device. Thus, it is privacy preserved by design. In harmony, blockchain is also prominent since it does not require an intermediary to process a transaction. However, these approaches are not yet fully ripe to be implemented in the real world, especially for the complex system (several challenges need to be addressed). In this work, we present the performance of collaborative learning and potential use case of blockchain. Further, we discuss privacy issues in the system.

1. Introduction

Collaborative learning and blockchain technology are widely discussed recently. These technologies count on the top of the decentralized form as a part of the distributed system. Both can be interpreted as an intersection of on-device AI, decentralized ledger, and edge computing. The main objective of this approach is to cover the weaknesses in the centralized architecture.

Collaborative learning is a breakthrough in the machine learning. It turns the centralized raw data into a decentralized form. The raw data owned by clients are never leaving the devices [1]. Thus, the issues of privacy in centralized learning can be tackled.

Blockchain appears with the merits of offering solutions that are faced in the centralized model. The core idea behind it is a chain-shaped data structured as known as a chain of blocks [2]. Due to the merits, blockchain can be used for many purposes such as storing data, managing data, and incentive mechanisms [3]. Therefore, the application of the blockchain has reached many aspects such as finance, healthcare, supply chain, and to name a few.

In this work, we briefly show the performance of collaborative learning where the users train the model on the devices using their dataset (built-in training). Once the training is completed, the user sends the upgraded model back to the global or aggregation server. This sort of activity is carried out continuously for as long as necessary to improve the AI model.

The users are incentivized since they provide the valid upgraded model and train the model using their resources. The rewards are propagated by relying on the blockchain technology. Eventually, blockchain with its merits offered can be used in the collaborative learning as an incentive mechanism. However, this paper only presents the initial approach of collaborative learning and incentive mechanism. Further research is a necessity, especially related to potential attacks.

2. Collaborative Intelligence

One of the most prominent benefits of utilizing blockchain technology is not involving a middleman nor intermediaries to manage the transactions [4]. This feature is also useful for

collaborative intelligence where data is not concentrated. The data is scattered among the user devices in the same application. In the collaborative learning algorithm, there is a set of users with a distinct local dataset.

$$f(w) = \frac{1}{n} \sum_{i=1}^n f_i(w) \quad (1)$$

$$\sum_{n=1}^n \frac{c_n}{c} w_{t+1}^n \quad (2)$$

Intuitively, $f_i(w) = (x_i, y_i, w)$ can be defined as a loss of the prediction on example (x_i, y_i) which is managed by model parameters w as shown in (1). It also can be interpreted as IoT devices send gradients or parameters $\Delta w_1 + \Delta w_2 + \Delta w_3 + \dots + \Delta w_n$ to the cloud server, which is partitioned homogeneously [5]. Finally, the aggregated server computes the model received and applies it to the new parameters as defined in (2).

3. Blockchain Incentive Structure

A blockchain-based loyalty rewards system can reduce management costs with smart contracts that are secure, trackable, transparent, and lower costs. A smart contract can be utilized further such as merging with AI as shown in Figure 1. This combination can provide a more resilient and efficient path for a decentralized system. By implementing this, the reliance on the middleman to take care of the transaction can be eliminated, so that many benefits are obtained.

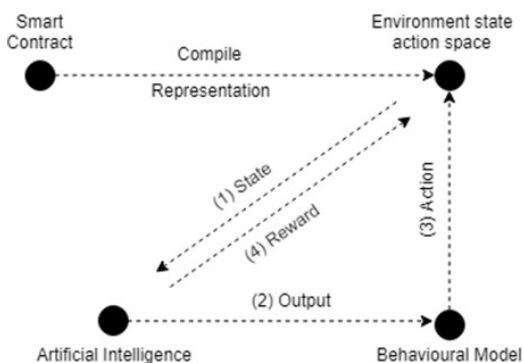


Fig. 1. The basic high-level structure of the AI smart contract scheme.

Figure 1 presents a smart contract that handles

the training of AI agents with an interpretable result. As the transition model towards the blockchain economy space, this could become a critical tool in offering safer decentralized application (DApps) [6].

4. Results and Discussion

For the presentation and implementation, we use five devices acting as clients in the collaborative system. Afterward, the clients download the first global model from the aggregated server. The devices train the model using their dataset. When training is completed, the client sends the updated model back to the aggregation server.

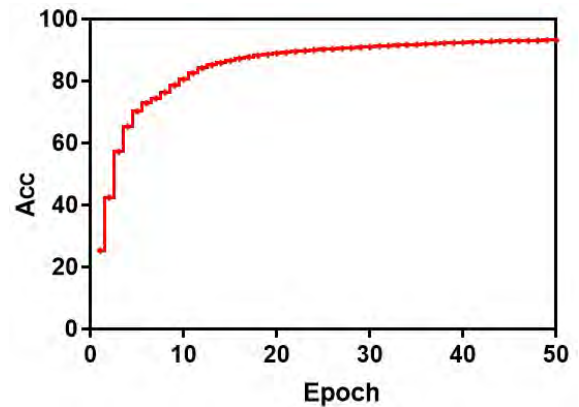


Fig. 2. Average accuracy of training data
We use a standard convolutional neural network (CNN) as the model installed within devices. The model trains the letter and number images.

Table 1. Inference attacks for different fractions

Property / % parameters update	10%	50%	100%
Top region (Antwerpen)	0.84	0.86	0.93
Gender	0.90	0.91	0.93
Veracity	0.94	0.99	0.99

Based on the implementation, the accuracy increased over time (see Fig 2). The average loss is around 0.23 and the accuracy reaches 93%. Nevertheless, we find that the number of devices affects the training time. The more devices within the collaborative system, the slower the training time it gets. When the transaction is conducted and verified by the aggregated server, then the rewards are delivered to the clients by using

smart contracts. Nevertheless, in this paper, we do not elaborate on the smart contract in detail.

Even though the combination of decentralized learning and blockchain brings a lot of benefits, but it is also still vulnerable to attacks such as inference attacks as shown in Table 1 [7]. Roughly speaking, in a certain way, the malicious can leak the training dataset of the clients. Thus, the main objective of decentralized learning has been disrupted by malicious clients. The bright side is the performance of the malicious decreases with the increasing number of honest clients (a large number of clients) in the same decentralized network. In short, the attempt from malicious is negligible.

5. Conclusion

The collaboration of decentralized learning and blockchain brings a lot of merits that overcome many issues in the centralized system. We presented the model as well as the performance which needs to be developed further in all aspects. Even though this combination provides goodness in the real world, the privacy of the users is still an issue. The malicious with a certain condition can gather the training dataset of the users. For future work, we plan to analyze the data protection policies with the appropriate incentives by leveraging blockchain.

Acknowledgments

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. NRF-2018R1D1A1B07048944) and partially was supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program (IITP-2020-2015-0-00403) supervised by the IITP(Institute for Information & communications Technology Planning & Evaluation)

[References]

- [1] Weng, Jiasi, et al. "Deepchain: Auditable and privacy-preserving deep learning with blockchain-based incentive." *IEEE Transactions on Dependable and Secure Computing* (2019).
- [2] S. Wu, Y. Chen, Q. Wang, M. Li, C. Wang, and X. Luo, "CReam: A Smart Contract Enabled Collusion-Resistant e-Auction," *IEEE Transactions on Information Forensics and Security*, 2018.
- [3] Wang, Jingzhong, et al. "A blockchain based privacy-preserving incentive mechanism in crowdsensing applications." *IEEE Access* 6 (2018): 17545-17556.
- [4] G. A. Montes and B. Goertzel, "Distributed, decentralized, and democratized artificial intelligence," *Technological Forecasting and Social Change*. 2019.
- [5] Jakub Konecny, H Brendan McMahan, Daniel Ramage, and Peter Richtarik. "Federated optimization: Distributed machine learning for on-device intelligence", *arXiv preprint arXiv:1610.02527*, 2016.
- [6] "Incentivai." [Online]. Available: <https://incentivai.com/product/>. [Accessed: 12-Oct-2019].
- [7] Melis, Luca, et al. "Exploiting unintended feature leakage in collaborative learning." 2019 *IEEE Symposium on Security and Privacy (SP)*. IEEE, 2019.

Empowering Blockchain For Secure Data Storing in Industrial IoT

Muhammad Firdaus* and Kyung-Hyune Rhee**

*Department of Information Security, Graduate School
Pukyong National University

**Department of IT Convergence and Application Engineering
Pukyong National University

e-mail: mfirdaus@pukyong.ac.kr, khrhee@pknu.ac.kr

Abstract

In the past few years, the industrial internet of things (IIoT) has received great attention in various industrial sectors which have potentially increased a high level of integrity, availability, and scalability. The increasing of IIoT is expected to create new smart industrial enterprises and build the next generation smart system. However existing IIoT systems rely on centralized servers that are vulnerable to a single point of failure and malicious attack, which exposes the data to security risks and storage. To address the above issues, blockchain is widely considered as a promising solution, which can build a secure and efficient environment for data storing, processing and sharing in IIoT. In this paper, we propose a decentralized, peer-to-peer platform for secure data storing in industrial IoT base on the ethereum blockchain. We exploit ethereum to ensure data security and reliability when smart devices store the data.

1. Introduction

The integration of IoT and industry, also known as the industrial internet of things (IIoT) has received great attention in various industrial sectors which has potential increasing a high level of integrity, availability, and scalability. The increasing IIoT is expected to produce extraordinary economic growth opportunities by conducting digital transformation to create new smart industrial enterprises and build the next generation smart system in many areas, including manufacturing, energy, transportation, agriculture, retail, and many more.

However existing IIoT systems rely on centralized servers for data storing, processing and sharing are vulnerable to a single point of failure and malicious attack, which exposes the data to security risks and storage [1]. Therefore, data security becomes critical concerns for IIoT [2]. To address the above issues, blockchain is widely considered as a promising solution, which

can build a secure and efficient environment for data storing, processing, and sharing in IIoT [3], [4]. Blockchain can be a decentralized cloud storage network that has been introduced with many advantages over the datacenter-based storage.

In this paper, we propose a decentralized, peer-to-peer platform for secure data storing in industrial IoT base on ethereum blockchain. We exploit ethereum to ensure data security and reliability when smart devices store the data since ethereum can effectively maintain a tamper-proof ledger shared by the participating smart devices without the need of a trusted third central organization. The rest of this paper is organized as follows. We present the related works concerning the IIoT system and blockchain technology. Then, we describe the system that empowering blockchain for securing data storage in the IIoT system. Finally, we conclude this paper.

2. IIoT and Blockchain

The past years have witnessed the rapid development of the IIoT, which is reshaping various industrials such as agriculture, environmental monitoring, and security surveillance [5]. The IIoT system which consists of smart devices is adequate for using sensors to collect data around or using embedded cameras to capture the images or videos, which should be captured and stored or processed securely. In [6], the authors provided several research opportunities and challenges such as using cryptography and other techniques to ensure privacy and security in IIoT. Shrouf et al. [7] presented a reference for IoT-based smart factories' architecture and they decide the main characteristics of the factories especially from the perspective of sustainability.

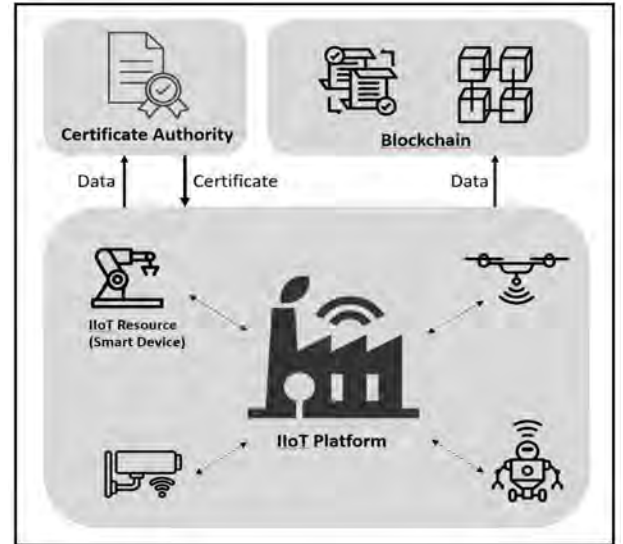
In 2008, Nakamoto proposed a peer-to-peer (P2P) digital currency system named bitcoin for economic transactions based on blockchain technology [8]. Blockchain can guarantee data security and efficiency by enabling anonymous and trustful transactions and removing all kinds of intermediaries. Refers to [9], authors discuss the possibilities of integrating blockchain into IoT applications, called BIoT. They provide a detailed analysis of the important aspects of the development of BIoT applications.

3. Blockchain-based for Secure Data Storing in IIoT

We consider a blockchain-enabled IIoT system, which consists of two stages, the authentication of the IIoT smart devices which will collect the data with sensing tasks and blockchain system that guarantees data storing in a distributed ledger and secure manner.

3.1 Smart Devices Authenticated in IIoT Network

In this scheme, each smart device registers to the certificate authority (CA) and obtains its public and private keys (pk^m, sk^m) , $\forall m \in M$, to



(Figure 1). System Model

become an authenticated smart device. The private key is used to encrypt data to ensure that collected data sent to the blockchain network is valid and can not be forged. Next, the smart device will send it to the CA, which will check whether the data come from a legitimate smart device and data is real. After verification, the signature of CA and encrypted data will return to the smart device, and can be sent to the blockchain as a storage request.

3.2 Blockchain-Enabled Secure Data Sharing

The blockchain is capable to securely exchange and store the data from components in IIoT systems without the need for an intermediary. Smart devices generate transactions using its sensor to collect data, which should be captured and stored securely. Eventually, these transactions are relayed to blockchain systems for storing the data into/from the distributed ledger, i.e. the underlying blockchain. We exploit ethereum as required data storage service and build a private blockchain, which includes $N \{n = 1, 2, N\}$ Ethereum nodes for storing and sharing data. We then classify them into the following two categories.

1) *Mining Nodes*: They are used to verify data sharing transactions and compile them into

Algorithm 1: Blockchain-Enabled Secure Data Storing Among Smart Devices

```

1. Initialize private blockchain and setup  $N$ 
   Ethereum nodes;
2. Deploy smart contract on blockchain;
3. Blockchain start mining;
4. for SD  $m$  in  $M$  do
5.   Run  $Gen(1^n)$  to obtain  $(pk^m, sk^m)$ ;
6.   CA stores identity  $(m, pk^m)$ ;
7. end for
8. for SD  $m$  in  $M$  do
9.   Collect data ;
10.  Generates data collection  $(U_m)$ ;
11.  Hash collected data  $H(U_m)$ ;
12.  Send  $\{U_m, Sign sk^m H(U_m)\}$  to CA ;
13.  if  $Vrfy pk^m\{U_m || Sign sk^m H(U_m)\} == 1$  then
14.    if  $U_m == collection[m]$  then
15.       $U_m^* = Sign sk^m\{H(U_m)\}$ ;
16.      Return  $\{U_m, Sign sk^{CA}(U_m^*)\}$  to SD  $m$ ;
17.    end if
18.  end if
19.  if SD  $m$  receives signature from CA then
20.    Send transaction request
       $\{U_m, Sign sk^{CA}(U_m^*), pk^m\}$  to blockchain;
21.    if verify signature and identity is
      true then
22.      Upload transaction to blockchain
      and wait for confirmation ;
23.    end if
24.  end if
25. end for

```

blocks. They need to consistently use machine computing resources to solve computing problems and submit blocks to the blockchain network.

2) *Non-mining Nodes*: Since the non-mining node is only responsible for receiving and broadcasting data sharing transaction request, it does not need the same amount of resources if compared to a mining one.

4. System Model

We explain the whole process of secure data storing among smart devices by using pseudo-code in Algorithm 1. As shown in Algorithm 1, to be more specific, we first run $Gen(1^n)$ to generate public and private keys pair (pk^m, sk^m) for each smart device (SD), where 1^n

is a security parameter (Line 5). And CA would store SD m id and public key (m, pk^m) in a list (Line 6). SDs starts to collect data using different kind of sensors. After the end of collecting data, SDs will send their data collection (U_m) and signature to CA (Line 9–12). CA can decrypt it and judge whether it is the SDs m data according to the result $Vrfy pk^m\{U_m, Sign sk^m H(U_m)\}$. If the result is 1, the request is sent by SD m , otherwise not. Besides, after decryption, it is also necessary to compare U_m with the data on the device itself to avoid fake data. Therefore, if $Vrfy pk^m\{U_m, Sign sk^m H(U_m)\} = 1$ and $U_m = collection[m]$, then CA will add its signature to the request and return it to the SD m (Line 13–18). SD can package the request $\{U_m, Sign sk^{CA}(U_m^*), pk^m\}$, then send it to the blockchain. After non-mining nodes receive transaction requests from SD, blockchain will verify the signature on the request and decide whether to submit the transaction to the blockchain network based on the verification results (Line 26–28). The submitted transaction will be mined and written in a new block by mining nodes.

5. Conclusions

We presented a blockchain platform for secure data storing in industrial IoT. Smart devices generate transactions by collecting data using its sensors. These transactions are relayed to blockchain systems for storing the data into the distributed ledger. We propose ethereum as the required data storage service and build a private blockchain, which includes mining nodes to verify data sharing transactions and non-mining nodes for receiving and broadcasting sharing transactions.

Acknowledgment

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. NRF-2018R1D1A1B07048944) and partially was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information

Technology Research Center) support program (IITP-2020-2015-0-00403) supervised by the IITP (Institute for Information & communications Technology Planning & Evaluation)

[References]

- [1] Do, H.G. and Ng, W.K., 2017, June. "Blockchain-based system for secure data storage with private keyword search," in 2017 IEEE World Congress on Services (SERVICES) (pp. 90-93). IEEE.
- [2] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial Internet of Things," IEEE Trans. Ind. Inform., vol. 14, no. 8, pp. 3690 - 3700, Aug. 2018.
- [3] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in Proc. IEEE Int. Congr. Big Data, Honolulu, HI, USA, Jun. 2017, pp. 557 - 564.
- [4] W. Chen, M. Ma, Y. Ye, Z. Zheng, and Y. Zhou, "IoT service based on jointcloud blockchain: The case study of smart traveling," in Proc. IEEE Symp. Service-Oriented Syst. Eng., Bamberg, Germany, Mar. 2018, pp. 216 - 221.
- [5] H. Liu, Y. Zhang, and T. Yang, "Blockchain enabled security in electric vehicles cloud and edge computing," IEEE Netw. Mag., vol. 32, no. 3, pp. 78 - 83, May/Jun. 2018.
- [6] K. K. R. Choo, S. Gritzalis, and J. H. Park, "Cryptographic solutions for industrial internet-of-things: Research challenges and opportunities," IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 3567 - 3569, Aug. 2018.
- [7] F. Shrouf, J. Ordieres, and G. Miragliotta, "Smart factories in industry 4.0: A review of the concept and of energy management approached in production based on the internet of things paradigm," in Proc. IEEE Int. Conf. Ind. Eng. Eng. Manage., 2015, pp. 697 - 701.
- [8] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2009. [Online]. Available: <http://www.bitcoin.org/bit-coin.pdf>
- [9] Fernández-Caramés TM, Fraga-Lamas P. "A Review on the Use of Blockchain for the Internet of Things." in IEEE Access. 2018 May 31;6:32979-3001.

해킹메일 대응을 위한 기술 표준 분석

변예은*

*한국원자력통제기술원

hibye@kinac.re.kr

Analysis of Technical Standards for Hacking Mail

Ye-Eun Byun*

*Korea Institute of Nuclear Nonproliferation and Control

요 약

해킹메일로 인한 피해는 꾸준히 발생하고 있으며, 최근에는 정부나 공공기관을 사칭하는 메일로 인한 피해 사례가 증가하고 있어 정부에서는 사칭메일을 대응하기 위한 기술을 적용하도록 요구하고 있다. 2017년부터 한국인터넷진흥원에서는 이메일 주소를 사칭하는 메일을 차단하기 위해서는 SPF(Sender Policy Framework) 기술을 적용해야 한다고 밝혔으며, 2019년에 정부에서는 SPF 뿐만 아니라 DKIM(Domain Keys Identified Mail)과 DMARC(Domain-based Message Authentication, Reporting, and Conformance)까지 적용을 확대할 것을 요구하고 있다. 이에, 본 논문에서는 해킹메일 대응을 위해 적용하고 있는 세 가지 기술의 기술 표준을 분석함으로써 해당 기술을 적용하여 나가기 위한 발판을 마련하고자 한다.

1. 서론

최근에 해킹메일로 인한 피해가 꾸준히 증가하고 있으며, 그 중에서도 정부나 공공기관을 사칭한 메일로 인한 피해가 증가하고 있어 정부에서는 이러한 사칭메일을 대응하기 위하여 각 기관에서 보안 기술을 적용하도록 요구하고 있다. 2017년부터 이미 한국인터넷진흥원에서는 이메일 주소를 사칭하는 메일을 차단하기 위해서 이메일 발신 서버의 진위 여부를 판단하는 SPF(Sender Policy Framework) 기술을 적용해야 한다고 밝혔으며, 2019년부터 정부에서는 SPF 뿐만 아니라 전자서명 방식의 DKIM(Domain Keys Identified Mail)을 통해 발신자가 발송한 메일의 위변조 여부를 확인할 수 있는 기술을 적용하여야 한다고 밝힌 바 있다. 또한 SPF와 DKIM을 모두 적용한 DMARC(Domain-based Message Authentication, Reporting, and Conformance)까지 적용을 확대할 것을 요구하고 있다. 이에, 본 논문에서는 최근 이슈가 되고 있는 해킹메일 대응을 위하여 적용하고 있는 기술인 SPF, DKIM, DMARC의 기술이 어떠한 표준 문서와 체계에 의해 마련되었는지를 살펴보기 위해 해당 기술 표준에 대해 분석하고자 한다.

2. 본론

우선, 기술 표준 관련 문서들의 체계를 살펴보기 위하여 먼저 기술 표준을 만드는 협회와 기술 표준 문서 체계에 대해 살펴보고, 각 기술에 관련된 기술 표준에 대해 살펴보하고자 한다.

2.1 IETF RFC

국제인터넷표준화기구(Internet Engineering Task Force, IETF)에서는 인터넷 관련 기술 표준을 만드는 데, 이 과정에서 생산되는 문서를 RFC(Request For Comments)라 하고 이는 인터넷에서 기술을 구현할 때 필요한 절차 등을 제공하는 문서로 활용된다.

2.2 SPF 관련 기술 표준 분석

SPF(Sender Policy Framework)와 관련한 RFC 문서를 분석한 결과는 다음과 같다. SPF에 대해서 주로 다루고 있는 문서는 RFC 7208로, 이는 RFC 4408을 검토하고 개정하여 표준(Standard)으로 정해진 문서이다.[1] 이전 버전으로 볼 수 있는 RFC 4408은 실험적인(Experimental) 문서로 분류되었으며, 이는 검증되거나 범용적으로 활용되기 전 단계의 문서로서의 성격을 띤다.[2] 또한, RFC 6686은 정보 전달(Informational)의 문서로, 해당 문서에서

언급하고 있는 두 가지 메일 인증 프로토콜 중 하나인 Sender ID 프로토콜은 RFC 4406(Sender ID : Authenticating E-Mail)에서 제안하고 있는 실험적인(Experimental) 것으로, SMTP 서버가 수신된 메일의 주소가 해당 메일 주소의 DNS의 검증을 받았는지 여부를 판별할 수 있는 기술에 대해 설명한다.[3]

<표 1> SPF 관련 기술 표준

문서번호	제목	주요 내용
RFC 4408 ('06.04)	Sender Policy Framework(SPF) for Authorizing Use of Domains in E-Mail, Version 1	- 보내는 사람이 도메인 네임을 사용할 수 있는지를 검증하고, 받는 사람도 그 검증을 확인하는 SPF 프로토콜에 대해 설명
RFC 7208 ('14.04)		- Administrative Management Domains(ADMDs)가 상기 내용을 검증하는 프로토콜에 대해 설명
RFC 6652[4] ('12.06)	SPF Authentication Failure Reporting Using the Abuse Reporting Format	- 메시지 인증 실패 시, 상세하게 보고할 수 있는 방식에 대해 설명 - 본 문서를 통해 RFC 4408 업데이트. 표준(Standard)
RFC 6686 ('12.07)	Resolution of the SPF and Sender ID Experiments	- SPF와 Sender ID 두 가지의 메일 인증 프로토콜의 차이점 등에 대해 설명

2.3 DKIM 관련 기술 표준 분석

다음으로 DKIM(Domain Keys Identified Mail)와 관련한 RFC 문서를 분석한 결과는 다음과 같다. DKIM 기술을 설명할 때 일반적인 표준 기술은 RFC 4871이며, 이 문서는 도메인 별로 이메일에 디지털 서명을 하기 위한 프레임 워크를 정의한 RFC 4870을 업데이트 하여 작성되었다.[5]

<표 2> DKIM 관련 기술 표준

문서번호	제목	주요 내용
RFC 4871 ('07.05)	Domain Keys Identified Mail (DKIM)	- 공개키 암호화와 키 서버 기술을 사용하는 도메인

	Signatures	수준의 인증 프레임워크 설명
RFC 5672 ('09.08)	RFC 4871 Domain Keys Identified Mail (DKIM) Signatures -- Update	- RFC 4871을 업데이트 - 제안된 기술(Proposed Standard)
RFC 6376[6] ('11.09)	DomainKeys Identified Mail (DKIM) Signatures	- DKIM 서명을 유지하는 방식을 통해 메일이 전송되는 방식에 대해 설명 - RFC 4871을 업데이트하여 작성된 표준(Standard)
RFC 8301[7] ('18.01)	Cryptographic Algorithm and Key Usage Update to DomainKeys Identified Mail(DKIM)	- DKIM이 설계되었을 때, 포함된 암호 알고리즘과 키 크기 요구사항에 대한 부분을 수정 - RFC 6376을 업데이트
RFC 8463[8] ('18.09)	A new Cryptographic Signature Method for DomainKeys Identified Mail(DKIM)	- RFC 6376을 업데이트

또한, RFC 4871은 RFC 5672를 통해 업데이트 되는데, 문서를 살펴보면 RFC 4871에서 언급한 내용의 한 문장씩을 수정하기도 하고 SDID(Signing Domain Identifier)라는 새로운 개념을 도입하기도 한다.[9]

2.4 DMARC 관련 기술 표준 분석

마지막으로 DMARC(Domain-based Message Authentication, Reporting, and Conformance)와 관련한 RFC 문서를 분석한 결과는 다음과 같다.

<표 3> DMARC 관련 기술 표준

문서번호	제목	주요 내용
RFC 7489 ('15.03)	Domain-based Message Authentication, Reporting, and Conformance	- 정보 전달(Informational)의 문서

	(DMARC)	
RFC 7960 (‘16.09)	Interoperability Issues between Domain-based Message Authentication, Reporting, and Conformance (DMARC) and Indirect Email Flows	- 정보 전달(Informational)의 문서

RFC 7489에서는 메일 발신자가 도메인 수준의 정책 및 기본 설정을 처리할 수 있는 메커니즘인 DMARC에 대해 설명을 하고 있다.[10] 또한, RFC 7960에서는 DMARC 메커니즘을 사용하였을 때, 메시지가 발신자의 도메인에서 수신자에게 직접 전달되지 않는 경우 발생할 수 있는 상호 운영성의 문제를 ‘간접 이메일 흐름’이라 정의하고 이를 해결하기 위한 방안을 제시하고 있다.[11]

3. 결론

최근 메일 수신자가 관심을 가지는 내용의 제목으로 클릭을 유도하는 피싱 메일이나 특정 집단을 타겟으로 하여 정부기관 등을 사칭하는 해킹 메일 등 다양한 기법을 통해 해킹 메일이 사용자들에게 유포되고 있다. 이에, 정부에서도 각 기관에서의 피해를 방지하기 위해 SPF·DKIM·DMARC의 기술을 적용할 것을 요구하고 있고, 보안 업체에서도 갈수록 발전하고 있는 공격 기법에 대응하기 위한 제품들을 출시하고 있다. 본 논문에서는 이러한 사회적인 환경에서 요구하고 있는 보안 기술들의 체계와 해당 기술들의 표준 문서에 대해 살펴보았다. 보안 기술을 적용하기 위해 해당 기술이 제안되거나 적용되고 있는 문서의 흐름을 파악하는 것은 기술 도입 전 이해를 돕기 위한 발판이 되었으며, 이를 통해 보다 폭 넓은 기술적인 이해를 할 수 있을 것이라 기대해본다. 물론 다양한 보안 기술을 적용함으로써 기관 내 보안대책을 강화하는 것도 중요하지만 무엇보다 중요한 것은 의심되는 메일은 열어보지 않고, 기본적인 보안 수칙을 준수하는 사용자들의 보안 의식이 가장 중요할 것이다.

참고문헌

- [1] S. Kitterman, “Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1”, 2014
- [2] M. Wong, W. Schlitt, “Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1”, 2006
- [3] M. Kucherawy, “Resolution of the Sender Policy Framework (SPF) and Sender ID Experiments”, 2012
- [4] S. Kitterman, “Sender Policy Framework (SPF) Authentication Failure Reporting Using the Abuse Reporting Format”, 2012
- [5] E. Allman, J. Callas, M. Delany, M. Libbey, J. Fenton, M. Thomas, “DomainKeys Identified Mail (DKIM) Signatures”, 2007
- [6] D. Crocker, Ed., T. Hansen, Ed., M. Kucherawy, Ed., “DomainKeys Identified Mail (DKIM) Signatures”, 2011
- [7] S. Kitterman, “Cryptographic Algorithm and Key Usage Update to DomainKeys Identified Mail (DKIM)”, 2018
- [8] J. Levine, “A New Cryptographic Signature Method for DomainKeys Identified Mail (DKIM)”, 2018
- [9] D. Crocker, Ed., “RFC 4871 DomainKeys Identified Mail (DKIM) Signatures – Update”, 2009
- [10] M. Kucherawy, Ed., E. Zwicky, Ed., “Domain-based Message Authentication, Reporting, and Conformance (DMARC)”, 2015
- [11] F. Martin, Ed., E. Lear, Ed., T. Draegen, Ed., E. Zwicky, Ed., K. Andersen, Ed., “Interoperability Issues between Domain-based Message Authentication, Reporting, and Conformance (DMARC) and Indirect Email Flows”, 2016

클라우드 하이퍼바이저 구조의 취약점 개선을 위한 고찰

김태우*, 석상기*, 박종혁*
 *서울과학기술대학교 컴퓨터공학과
 e-mail:{tang_kim, sksuk, jhpark1}@seoultech.ac.kr

Consideration for Improving the Vulnerability of the Cloud Hypervisor Architecture

Tae Woo Kim*, Sang Kee Suk*, Jong Hyuk Park*
 *Department of Computer Science and Engineering, Seoul National University of Science and Technology

요 약

클라우드 컴퓨팅 (Cloud Computing)은 언제 어디서든 인터넷을 통하여 필요한 컴퓨팅 자원을 원하는 시간만큼 활용할 수 있는 최신 컴퓨팅 방식으로 사용자에게 효율적인 컴퓨팅 자원을 제공한다. 또한 빅데이터 및 인공지능 분야에서의 활용도가 높아 4차 산업혁명의 기초 인프라로 부각되고 있다. 클라우드의 독립적인 컴퓨팅 자원을 하이퍼바이저 (Hypervisor)를 통해 효율적으로 관리한다. 본 논문에서는 클라우드 하이퍼바이저에 대한 공격 기법인 커널 기반 루트킷, 캐시 기반 부 채널 공격, ROP (Return oriented Programming) 공격의 공격 방법과 대응 방안을 분석한다. 이후 기존에 연구된 하이퍼바이저 보안을 위한 클라우드 컴퓨팅 아키텍처를 소개하고, 하이퍼바이저 구조의 취약점에 대해 고찰한다. 마지막으로 하이퍼바이저 기반 클라우드 컴퓨팅 아키텍처의 문제점과 해결방안을 고찰한다.

1. 서론

인터넷 통신망의 빠른 발전과 IoE의 활성화에 따라 사용자에게 효율적으로 컴퓨팅 서비스를 제공하기 위해 새로운 컴퓨팅 패러다임을 고안했다. 클라우드 컴퓨팅 (Cloud Computing)이란 언제 어디서나 인터넷 통신망을 통하여 언제 어디서든 컴퓨팅 자원을 필요한 시간에 필요한 만큼 활용할 수 있는 컴퓨팅 방식이다[1]. 인터넷 통신망 접속이 가능하다면 시간과 장소 그리고 접속기기에 따른 제약이 발생하지 않아 연결성이 뛰어나다. 또한, 사용자가 원하는 만큼의 컴퓨팅 자원을 하이퍼바이저를 사용하여 컴퓨팅 자원 공유가 가능하여 효율성이 높다[2]. 빅데이터와 인공지능의 중요성이 부각된 4차 산업혁명에서 대규모 데이터 관리 및 처리가 용의하여, 빅데이터 기반의 인공지능을 위한 방대한 컴퓨팅 자원으로 활용 가능한 하이퍼바이저 기반의 클라우드 컴퓨팅이 주목받고 있다[3].

하이퍼바이저 (Hypervisor)란 클라우드 상의 분할된 컴퓨팅 자원을 관리하는 중간관리자이다[4]. 하나의 컴퓨팅 자원에서 다수의 VM (Virtual Machine)을 구동시켜 독립성을 가지고 있는 다수의 컴퓨팅

자원으로 활용하게 되며 이때 VM을 관리하는 중앙 관리자 역할을 한다. 하이퍼바이저는 각 VM의 상위 계층에 위치하여 관리자 권한을 가지고 있어 하이퍼바이저가 감염되면 인증 과정의 무력화가 가능하다.

클라우드의 사용자 인증과정은 다수의 정보가 저장되어있는 클라우드 데이터베이스의 접근을 위한 필수적 요소이다. 인증 (Authentication)이란 비인가된 접속자가 접근하지 못하도록 인가된 사용자만이 알고 있는 정보를 이용해 자신을 증명하는 것이다 [6]. 공격자는 사용자의 권한을 획득하기 위해 인증 과정을 공격하거나 인증을 우회하는 방법을 사용하며, 권한을 획득하여 데이터에 접근하거나 악의적인 프로그램 설치를 통해 2차 공격이 가능하여 사용자 인증에 대한 지속적인 연구가 필요하다.

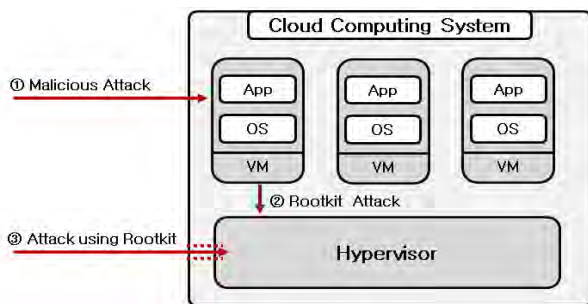
본 논문에서는 클라우드 컴퓨팅에서 발생하는 보안 위협인 VM 커널 기반 루트킷, 캐시 기반 부 채널 공격, ROP 공격을 사용자 인증 측면에서 분석한다. 사용자 인증을 무력화 목적의 하이퍼바이저 감염을 방지하기 위한 클라우드 보안 아키텍처를 소개한다. 마지막으로 클라우드 보안 아키텍처의 문제점을 분석하고 해결방안에 대해 고찰한다.

2. 관련연구

클라우드 컴퓨팅은 뛰어난 연결성, 컴퓨팅 자원의 효율성을 장점으로 빠른 발전이 이뤄졌다. 그러나, 그만큼 다방면의 보안위협이 존재한다는 문제점을 가지고 있다. 본 장에선 하이퍼바이저를 목표로 하는 공격에 대해 분석한다.

2.1 VM 커널 기반 루트킷 공격

VM 커널 기반 루트킷 공격이란 (그림 1)과 같이 하이퍼바이저가 관리하는 VM을 이용하여 커널 기반의 루트킷을 생성하는 공격이다[7]. 루트킷은 시스템 내부의 다른 위치를 공격하는 다양한 방식을 가지고 있다. VM에 루트킷이 설치되면 클라우드의 OS 및 응용 프로그램에서 공격자의 시스템 로그를 보이지 않게 하며, 일반적으로 원격 제어 또는 자동화 데이터 수집 등의 공격 경로를 제공한다. 따라서 공격자는 VM의 일반 권한 수준을 관리자 권한으로 수정할 수 있어 모든 데이터에 접근 가능하다.



(그림 1) VM 커널 기반 루트킷 공격 형태

VM 커널 기반 루트킷 공격을 방어하기 위해 강력한 사용자별 권한 분리가 필요하다. 또한 주로 시스템 명령어를 통해 사용자 권한이 변경된다는 점을 주목하여 사용자 권한 관련 명령어에 대한 시큐어 프로그래밍 기법, 명령어 난독화 기법 등을 사용하여야 한다. 그러나 방어 기법에 대한 우회 방법이 연구됨에 따라 루트킷 방어를 위해 추가적인 연구가 필요하다.

2.2 캐시 기반 부 채널 공격

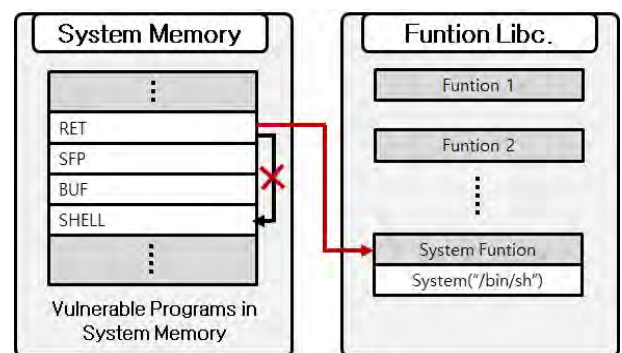
캐시 기반 부 채널 공격은 AES과 같은 암호화 알고리즘에 대한 암호화 키를 획득하는 정교한 공격이다. 공격자는 주로 공유 캐시 메모리 타이밍 분석, 프로세스 캐시 사용량 분석 등을 통해 얻은 정보를 통해 사용자 권한을 획득한다[8]. 클라우드의 프로세스의 캐시 사용량을 관찰하기 위해 스파이 프로세스

를 병렬로 실행시키는 Prime-Probe 공격기법과 공유 메모리 페이지를 모니터링하는 Flush-Reload 공격 기법을 사용한다.

캐시에 대한 부 채널 공격은 정적 소스 코드 분석과 CPU 성능 카운터를 사용하여 탐지할 수 있다. 이외에도 교차 VM 부 채널 공격 탐지, 캐시메모리에 대한 부 채널 누출 감지 아키텍처 등 여러 대응 방안이 연구 중이다[9]. 그러나 변형되고 발전된 모든 부 채널 공격을 방어할 수 없으며 부 채널 공격에 대한 예방 기법으로 인해 메모리의 성능 감소 문제가 발생할 수 있다.

2.3 Return oriented Programming 공격

ROP 공격은 (그림 2)와 같이 취약한 프로그램 내부에 있는 기계어 코드 섹션을 이용해 시스템 메모리에 대한 BOF (Buffer OverFlow) 공격을 응용한 공격법이다[10]. ROP 공격기법에는 스택에 있는 Return Address를 통해 라이브러리의 시스템 명령어를 실행시키는 RTL (Return to Libc) 공격, RTL을 연속적으로 발생하게 스택을 구성하여 공격하는 Chaining RTL Calls 공격, 그리고 함수 주소를 저장해 놓은 공간을 변경하는 GOT (Global Offset Table) 공격 등이 존재한다. ROP 공격을 통해 접근 권한을 획득하여 VM 초기화를 실행해 데이터를 삭제시키거나, 다른 VM에 접속할 수 있는 접근 권한을 획득할 수 있다. 따라서 데이터 및 사용자 접근 권한에 대한 심각한 문제가 발생한다.



(그림 2) VM 셸프롬프트 ROP 공격

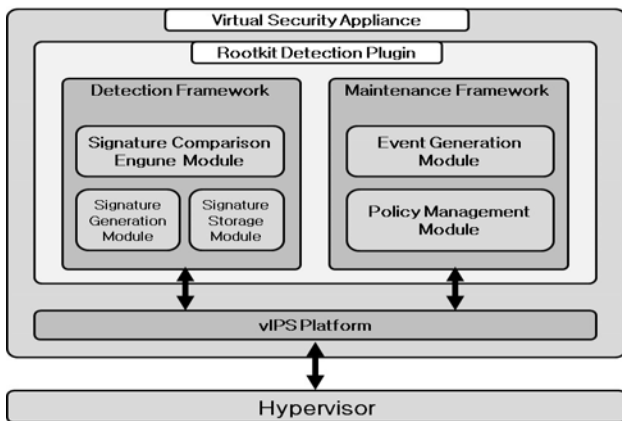
클라우드에서 시스템 메모리에 대해 ROP 공격이 발생한다. 시스템 메모리에서 프로그램이 의도한 대로 return 구문이 동작하는지 탐지하는 Shadow Stack 기법을 사용하거나, 프로그램 실행 중 지속해서 주소 공간을 난수화 하는 Shuffler 기법을 사용하여 시스템 메모리에 대한 보안을 강화할 수 있다[11].

3. 하이퍼바이저 보호를 위한 아키텍처

클라우드 전체를 감염시키기 위해 시도되는 공격들은 클라우드내의 중간관리자 역할인 하이퍼바이저를 목표로 하고 있다. 본 장에서는 커널 기반 루트킷 공격을 방어하기 위한 Virtual Security Appliance, 비정상적인 접근을 차단하고, 데이터 보호를 위한 Hypervisor Security Framework에 대해 소개하고 아키텍처의 취약점에 대해 분석한다.

3.1 Virtual Security Appliance의 약점

VSA (Virtual Security Appliance)는 (그림 3)과 같이 탐지 프레임워크, 관리 프레임워크 그리고 vIPS 플랫폼으로 구성되어 있다[11]. 탐지 프레임워크는 VSA의 핵심요소로 루트킷 탐지 엔진 및 서명 데이터베이스로 작동한다. 관리 프레임워크는 vIPS 플랫폼과의 통신을 관리하며, 주로 정책 관리 및 침입 알림을 처리한다. 마지막으로 vIPS 플랫폼은 가상 시스템의 내부 검사를 위해 클라우드에 영향을 받지 않는 독립적인 가상 네트워크 IPS (Intrusion Prevention System) 플랫폼이다. vIPS 플랫폼은 관리 프레임워크를 통해 탐지 프레임워크에서 진행한 VM 내부 검사 정보를 하이퍼바이저에게 제공하여 클라우드에 대한 침입에 대해 대응 하게 한다.

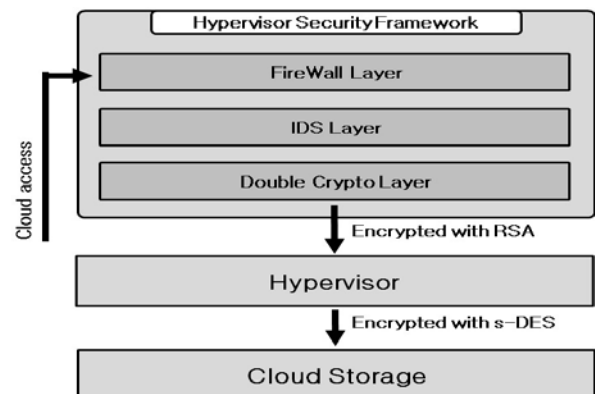


(그림 3) 제안된 VSA 아키텍처[11]

VSA는 하이퍼바이저와 독립되어 운영되는 어플리케이션으로 VM 커널 기반 루트킷 공격으로 안전하며, VM 커널 기반 루트킷 공격에 대한 루트킷 탐지가 가능하다[11]. 그러나 루트킷 탐지에 대한 탐지 정확도 측면에 대한 검증이 되지 않았으며, API기반의 사용자 인증에 대한 직접적인 공격에 대해서는 보안성이 취약하다는 문제점이 있다.

3.2 Hypervisor Security Framework의 약점

HSF (Hypervisor Security Framework)는 개인 클라우드에 대한 비정상적인 액세스 요청 시 방화벽, IDS (Intrusion Detection System)을 사용하여 통제하고 클라우드에 데이터 저장할 경우 이중 암호레이어를 사용하여 데이터를 보호한다[12]. HSF는 (그림 4)와 같이 3계층으로 각각 방화벽 레이어, IDS 레이어, 이중 암호 레이어로 구성되어 있다. 방화벽 레이어는 제한된 회원만 액세스 할 수 있게 하며, IDS 레이어에서는 클라우드 액세스 요청 중 액세스 권한이 올바른 사람에게만 부여되도록 작동한다. 마지막으로 이중 암호화 레이어는 데이터에 대해 하향식 정책 기반 보안 관리를 시행하며, RSA를 첫 번째 암호화 단계로 사용하고 s-DES를 두 번째 암호화 단계로 사용해 데이터를 저장한다. 제안된 보안 프레임 워크는 비정상적인 외부 접속과 데이터에 대한 수준 높은 보안 환경을 제공한다.



(그림 4) 제안된 HSF 아키텍처[12]

제안된 HSF는 클라우드에 대한 비정상적인 접근을 통제하고, 이중 암호 레이어를 통한 하향식 보안 정책을 채택하여 데이터를 암호화한다. 비인가된 접근 방식을 통해 데이터가 유출될 경우 2중 암호화가 되어있어 데이터를 보호 할 수 있다. 그러나 공격자가 비정상적인 방법으로 사용자 권한을 획득한다면 암호화된 데이터에 대한 접근 권한이 생기므로 암호화는 무력화 된다는 문제점을 가지고 있다. 또한 중간자공격 (Man-in-the-middle attack)을 통해 암호화를 우회할 수 있어 완전하다고 볼 수 없다.

4. 하이퍼바이저 취약점에 대한 고찰 및 결론

하이퍼바이저 기반의 클라우드 컴퓨팅에서는 VM 커널 기반 루트킷 공격, 캐시 기반 부 채널 공격, 시스템 메모리에 대한 ROP 공격 등이 존재한다. 공격

자는 하이퍼바이저를 감염을 통해 사용자 인증 과정을 우회하여 관리자 권한을 획득하는 것을 목적으로 하고 있다. 이러한 공격을 방어하기 위해 VSA, HSF와 같은 클라우드 내부적 문제 해결을 위한 보안 아키텍처에 대한 연구가 진행되고 있다.

VSA는 하이퍼바이저와 독립적으로 구성되어 운영하므로 하이퍼바이저 감염에 영향을 받지 않으며, VM 커널 기반 루트킷 공격에 대한 루트킷 탐지, 이상 동향탐지가 가능하다. 루트킷 탐지 정확도에 대한 정확도가 증명되지 않았으며, API기반의 접근과정에서 사용자 인증에 대한 직접적인 공격에 대해서는 보안성이 취약하다는 문제점을 가지고 있다.

HSF는 방화벽 레이어, IDS 레이어를 통해 비정상적인 접근을 차단하며, 이중 암호 레이어를 통해 데이터를 이중으로 암호화하여 데이터를 보호한다. 그러나 사용자 인증 우회, 중간자 공격등을 통해 비정상적인 방법으로 사용자 권한을 획득하게 될 경우 암호화된 데이터에 대한 접근 권한이 생기므로 이중 암호화가 무력화 된다는 문제점을 가지고 있다.

본 논문에서 소개한 클라우드 보안 아키텍처는 내부적으로 하이퍼바이저 감염을 방어하고, 비정상적인 접근을 차단하여 클라우드를 보호 한다. 그러나 사용자 인증에 대한 고려를 하지 않아 공격자가 관리자 권한을 획득하게 될 경우 데이터에 접근 할 수 있어 완전하다고 볼 수 없다. 이러한 문제를 해결하기 위해 사용자 인증 강화를 위해 다수의 인증 과정을 사용하는 Multi-factor 인증, 통합적인 보안 정책 관리를 위해 사용하는 Software Defined Security 등에 관한 연구 및 개발이 필요하다고 전망한다.

Acknowledgement

- This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (NRF-2019R1A2B5B01070416).

참고문헌

[1] S. Singh, Y. S. Jeong, and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions" *Journal of Network and Computer Applications*, Vol.75, pp.200-222, 2016.

[2] N. H. Hussein, and A. Khalid, "A survey of Cloud Computing Security challenges and solutions" *International Journal of Computer Science and Information Security*, Vol.14, No.1, pp.52-56, 2016.

[3] F. Zafar, et al, "A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends" *Computers & Security*, Vol.165, pp.29-49, 2017.

[4] M. S. Dildar, et al, "Effective way to defend the hypervisor attacks in cloud computing" In 2017 2nd International Conference on Anti-Cyber Crimes, IEEE, Saudi Arabia, 2017, pp.154-159.

[5] L. Ran, R. F. Yu, and X. S. Wang, "Information Resources Sharing Security in Cloud Computing" *Journal of Applied Science and Engineering Innovation*, Vol.5, No.3, pp.65-68, 2018.

[6] M. Yaici, A. Oussayah, and M. A. Takerrabet, "Trust-based Context-aware Authentication System for Ubiquitous Systems" *Procedia computer science*, Vol.134, pp.35-42, 2018.

[7] S. W. Ahn, et al, "A Study on Development of Code Reuse Attacks and Defenses." *Proceedings of the Korea Information Processing Society Conference*, 2017, Korea, pp.275-278.

[8] A. Shahzad, and A. Litchfield, "Virtualization technology: Cross-VM cache side channel attacks make it vulnerable" In *Australas Conf Inf Syst*, Australia, 2015, pp.1-16.

[9] D. Gruss, et al, "Strong and efficient cache side-channel protection using hardware transactional memory" In 26th {USENIX} Security Symposium, Canada, 2017, pp.217-233.

[10] S. R. Krishna, and B. P. Rani, "Virtualization security issues and mitigations in cloud computing" In *Proceedings of the First International Conference on Computational Intelligence and Informatics*, Singapore, 2017, pp.117-128.

[11] T. H. Hwang, et al, "Design of a hypervisor-based rootkit detection method for virtualized systems in cloud computing environments" In *AASRI Winter International Conference on Engineering and Technology*, USA, 2013, pp.27-32.

[12] S. Talasila, et al, "HSF-HYPERVISOR SECURITY FRAMEWORK FOR ACHIEVING DATA SECURITY IN A CLOUD ENVIRONMENT" *International Journal of Pure and Applied Mathematics*, Vol.115, No.6, pp.73-79, 2017.

확장성이 고려된 Bitcoin-NG 프로토콜 고찰 및 연구

김수현*, 차정훈*, 박종혁*

*서울과학기술대학교 컴퓨터공학과

e-mail: {ryun71380, ckwjdgns, jhpark1}@seoultech.ac.kr

Consideration and Research of Bitcoin-NG Protocol Considering Scalability

Soo Hyeon Kim*, Jeong Hun Cha*, Jong Hyuk Park*

*Department of Computer Science and Engineering, Seoul National University of Science and Technology

요 약

최근 IT 기술의 발전에 따라 블록체인 기술과 융합하려는 다양한 시도를 보인다. 비트코인(Bitcoin)의 탄생으로 알려지게 된 블록체인은 P2P (Peer-to-Peer) 네트워크에서 데이터의 무결성 조건을 만족할 수 있게 되면서 보안 기술에 대해 많은 연구가 진행 중이다. 데이터의 무결성을 증명하기 위해 합의 알고리즘을 사용하는데, 합의 알고리즘의 처리속도 및 저장 공간 문제 등으로 인해 다른 분야로 확장에 어려움을 겪고 있다. 따라서 블록체인을 구성하는 환경이나 목표에 따라서 적절한 합의 알고리즘을 선택하는 것이 중요하다. 본 논문에서는 확장성 문제를 해결할 수 있는 Bitcoin-NG 합의 알고리즘을 비롯하여 다양한 합의 알고리즘의 원리와 장단점을 소개한다. 블록의 합의에 참여하는 범위, 리더를 선정하는 방법 등의 기준으로 Bitcoin-NG 알고리즘이 확장성 문제에 긍정적인 합의 알고리즘으로서 갖춘 특징을 살펴보고 앞으로 합의 알고리즘의 발전 방향에 대해 고찰한다.

1. 서론

최근 다양한 종류의 네트워크 장치들이 개발되면서 하나의 네트워크에 P2P 연결이 많아지고 있다. 2008년 ‘사토시 나카모토’에 의해 처음으로 세상에 알려지게 된 블록체인은 분산 데이터베이스 시스템이다[1]. 블록체인 기술은 블록이 체인에 결합하게 되면 블록의 내용을 수정할 수 없다는 점에서 무결성 조건을 만족하게 되어 보안 기술로 인기를 얻었다. 세계 경제 포럼에서는 12대 유망 기술 중 하나로 블록체인을 선정하였으며, 나아가 약 10년 뒤 전 세계 GDP의 10%가 블록체인 기술에 기반을 둘 것으로 예측한다[2].

블록체인은 P2P 네트워크에서 완전한 정보 공유로 인해 특정 노드를 목표로 하는 해킹 시도를 무력화할 수 있으며, 단일 장애 점 (Single Point Failure) 발생에 대비할 수 있다. 하지만 분산 네트워크를 기반으로 하는 블록체인은 네트워크에 참여하는 노드가 증가하게 되었을 때, 검증해야 하는 거래의 수와 합의해야 하는 대상의 수가 증가하게 되어 네트워크 참여자 간의 합의에 도달하는 시간이 증가하게 된다. 시간이 지날수록 길어지는 체인을 저장하는

점과 블록의 크기가 1MB로 제한되어 큰 데이터를 저장하는 데 어려움이 있다는 점에서 기술적 한계를 보인다.

네트워크 참여자 간의 합의 도달 시간이 증가하는 한계를 극복하기 위해서 속도가 빠른 합의 알고리즘을 사용하고 하나의 프로세스가 처리해야 하는 데이터의 크기를 줄여 동일한 알고리즘에서 빠르게 처리할 수 있도록 한다. 다중 블록체인이나 샤딩 (Sharding) 방법, 병렬처리 또는 분할처리 방식을 이용하여 처리해야 하는 데이터의 크기를 줄일 수 있다. 저장 공간으로 인한 블록체인의 기술적 한계를 극복하기 위해서는 다중 블록체인을 이용하거나 외부에 저장 후 가리키는 키를 이용하는 등의 방법이 있다[3].

본 논문은 비트코인 등의 암호 화폐에서 사용 중인 합의 알고리즘 중 PoW, PoS, DPoS 합의 알고리즘의 원리 및 장단점에 관해서 서술하고, 블록체인의 확장성 문제를 해결할 수 있는 Bitcoin-NG의 구조 및 원리에 대해 소개한다. 마지막으로 처리 속도 및 보안성의 측면에서 합의 알고리즘을 분석하여 확장성을 해결하기 위한 조건에 대해 고찰한다.

2. 다양한 종류의 합의 알고리즘

P2P 연결을 기반으로 하는 블록체인은 거래의 신뢰를 보증해주는 제 3자가 없고, 신뢰할 수 없는 노드들로 네트워크가 구성된다. 발생하는 트랜잭션이 올바른 것인지 증명하고 신뢰 있는 데이터임을 증명하기 위해서 합의 알고리즘이 요구된다. 합의 알고리즘을 통해 블록체인 네트워크에서 모든 노드가 동일한 데이터를 공유하게 된다.

다음은 현재 암호 화폐에서 많이 사용되는 합의 알고리즘에 소개 및 장점과 단점에 대한 설명을 한다.

2.1 Proof-of-Work 합의 알고리즘

비트코인에서 사용하고 있는 합의 알고리즘으로 1993년 DDos 공격과 같은 사이버 공격을 막기 위해서 처음으로 정의되었다. 이후 ‘사토시 나카모토’에 의해 블록의 합의를 이끌어 내는 합의 알고리즘으로 이용된다.

PoW는 생성하고자 하는 블록의 해시값에 맞는 논스 (Nonce) 값을 찾는 방법으로 0부터 1씩 증가시키면서 찾는다. 블록 생성 주기는 해시 난이도를 통해 조절하는데, 평균적으로 소요 시간을 10분으로 설정했다. 주기적으로 해시 난이도 조절을 통해 블록 생성 주기를 제어한다[4].

작업 증명 방식 합의 알고리즘은 더 큰 네트워크를 구성할수록 안정성이 증가하고, 간단한 구조로 누구나 참여 가능하다는 장점이 있다. 하지만 네트워크 자원의 51%를 차지하게 되면 네트워크 전체 합의를 좌우할 수 있다는 점과 불필요한 컴퓨터 자원을 많이 사용한다는 한계점을 보인다.

2.2 Proof-of-Stake 합의 알고리즘

PoW가 에너지 소비에 의존한다는 점을 지적하며 Coin age라는 개념을 도입하여 합의에 이용되는 불필요한 컴퓨터 자원 사용을 줄이고자 했다.

PoS는 통화의 소유권 증명 형식을 의미하며, 새로운 블록을 추가하기 위해서는 자신이 보유한 코인을 자신의 블록에 등록함으로써 다음 블록 생성자로 선택될 확률을 높이는 방법이다[5]. (수식 1)은 PoS의 해시 함수와 채굴 난이도 사이의 관계를 나타낸다[6].

$$\text{hash}(\text{hash}(B_{prev}), A, t) \leq \text{bal}(A)M/D \quad (1)$$

B_{prev} 은 이전 블록의 Target 값, A는 주소 (Address), t는 해당 블록의 타임스탬프, bal(A)은 A가 가진 지분에 비례하는 Balance, D는 암호 퍼즐의 난이도, M은 암호 퍼즐이 가질 수 있는 난이도의 최댓값을 의미한다. 블록 B의 해시값은 A가 소유한 Balance와 난이도의 영향을 받게 된다. A가 소유한 Balance가 클수록 M의 값은 작아지게 됨으로 많은 지분을 가진 노드가 낮은 난이도의 문제를 풀게 되어 채굴의 확률을 높여준다[7].

모든 노드가 채굴에 참여하지 않음으로써 생성 주기를 단축할 수 있으며, PoW에서 문제가 되었던 컴퓨팅 낭비를 줄일 수 있다. 하지만 초기 지분이 많은 사람이 다음 블록 생성에 더 유리하다는 단점이 있다. 이를 해결하기 위해 코인의 양 및 코인 소유일수 기반으로 생성되는 수치를 통해 초기 지분이 많은 사람들이 블록 형성을 독점하는 것을 막는 Coin age 개념을 도입했다. 그러나 PoS는 Nothing at Stake가 발생하여 하나의 블록체인을 형성하는 것에 문제를 겪을 수 있다.

2.3 Delegated Proof of Stake 합의 알고리즘

DPoS 합의 알고리즘은 위임 지분 증명 알고리즘을 의미하며, 암호 화폐 소유자들이 각자의 지분율에 따라 투표를 하여 각 네트워크의 대표자를 선정하고 대표자들끼리 합의하여 의사결정을 내리는 방법이다. 대표자가 되고 싶은 노드의 경우 자신을 공개키와 함께 등록하면 네트워크를 구성하는 노드들의 투표를 통해 대표자로 선출될 수 있다.

합의는 네트워크를 대표하는 대표자에 의해서 이루어지기 때문에 합의에 걸리는 시간 및 비용이 적게 사용되고, 단위 시간 동안 생성되는 블록의 개수 또한 많아진다. 실제로 이더리움은 545,224Tx (Total Transactions) 처리속도를, DPoS 합의 알고리즘을 이용하는 스팀 (Steam)은 1,169,182Tx 처리속도를 가진다[8]. 하지만 블록 생성을 대표하는 대표자들 사이에 블록 생성 권한을 계속 유지하기 위해서 서로가 서로에게 투표하는 상황이 발생 할 수 있다. 일반 노드들이 대표자 선출에 있어 적극적으로 투표를 하지 않은 경우, 대표자들 소수의 담합으로 인해 소수 노드에 의해 블록체인의 전부가 지배될 수 있다.

3. 확장성이 고려된 합의 알고리즘 Bitcoin-NG

Bitcoin-NG (Next Generation)는 확장성을 고려

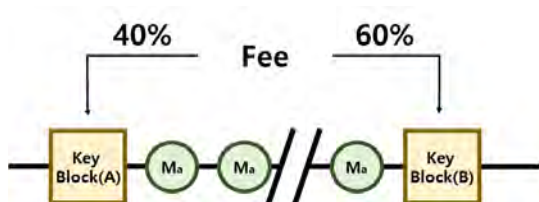
한 새로운 블록체인 알고리즘으로 블록체인 연산을 작업 증명을 이용한 ‘리더 선택’과 ‘트랜잭션 직렬화’ 두 부분으로 구분한다. 비트코인의 경우 트랜잭션의 처리 시간과 보안성이 반비례 관계를 가졌지만, Bitcoin-NG에서는 보안성을 감소시키지 않고 트랜잭션의 처리 시간을 향상한다.

3.1 Bitcoin-NG 프로토콜의 구조

Bitcoin-NG는 리더를 선출하기 위한 Keyblock과 장부의 역할을 하는 Microblock으로 구성된다. Keyblock은 현재 Unix 시간과 이전 블록에 대한 참조, 논스값 등으로 구성되며 Microblock을 검증할 수 있는 Keyblock 리더의 공개키를 포함한다. Microblock의 헤더에는 이전 블록에 대한 참조, 현재 Unix 시간, 최신 Keyblock의 개인키로 서명된 내용 등으로 구성된다. Keyblock 생성에 성공한 노드를 리더 노드라고 하고, 리더 노드는 다음 리더가 선정되기 전까지 Microblock을 생성할 수 있는 권한을 가지게 된다. Keyblock의 개인키로 한 서명을 통해 Microblock의 유효성을 입증하게 된다.

3.2 Bitcoin-NG 프로토콜의 작동 원리

시간을 에폭 (Epoch)으로 나누어, 각 에폭마다 하나의 리더를 가지게 된다. PoW와 동일하게 Keyblock 헤더의 해시는 Target value보다 작도록 논스값을 변경하며 암호 퍼즐을 푼다. (그림 1)는 Bitcoin-NG의 체인 구조로 노드 A에 의해 생성된 Microblock은 노드 A의 개인키로 서명되어 있으며, 생성되는 Microblock의 수수료는 해당 Keyblock에게 40%, 다음 생성되는 Keyblock에게 60%로 나눈다.



(그림 1) Bitcoin-NG의 체인 구조 [9]

새로운 Keyblock을 생성한 노드가 보다 트랜잭션 처리를 통한 이득을 증가시키기 위해 이전 Keyblock을 생성한 노드가 생성한 Microblock을 일부러 배제하는 것이 가능하다. 이것을 막기 위해 현재 Keyblock이 생성한 Microblock에서의 수수료를 다음 Keyblock과 나눈다.

Bitcoin-NG는 Microblock에서는 PoW 작업을 포함하지 않음으로 쉽고 빠르게 생성될 수 있다는 장점이 있다. 하지만 포크 발생 및 이중 지불 문제 (Double-Spending)가 발생하기 쉽다는 문제점을 가진다.

4. 확장성이 고려된 합의 알고리즘에 대한 고찰

블록의 합의에 참여하는 범위, 리더를 선정하는 방법 등에 따라서 다양한 합의 알고리즘이 존재한다는 것을 확인했다. PoW는 모든 노드가 채굴의 대상이 될 수 있으며 채굴을 통해 더 빠르게 논스 값을 찾아내는 노드가 블록을 생성하여 모든 노드가 합의에 참여하는 방법이다. PoS는 자신이 가진 지분에 의해 암호 퍼즐의 난이도가 반비례로 조정되어, 많은 지분을 가질수록 논스를 찾아내는 것이 쉽다. 지분에 따라 채굴할 노드를 결정하고 채굴을 통해 생성된 블록은 네트워크를 구성하는 모든 노드의 합의를 통해 체인에 연결되게 된다. DPoS는 네트워크에 포함된 모든 노드들이 지분 등록을 통해 대표자를 선정함으로써 블록의 합의에 참여하는 노드를 대표자 집합으로 제한한다. 대표자들에 의해 합의 과정에 진행되기 때문에 블록을 생성하여 체인에 연결하는 속도는 빠르지만, 탈중앙화로부터 멀어지게 된다. Bitcoin-NG는 PoW의 방법을 이용하여 네트워크에 포함된 모든 노드들이 리더 선출에 참여한다. 특정 노드가 리더로 선정된 후 공개키 기반 암호 기술을 이용하여 여러 개의 Microblock을 생성하게 되고, 네트워크에 포함된 모든 노드들이 공개키로 확인함으로써 합의를 이루게 된다. 공개키 암호를 이용하여 시간이 오래 걸리고 자원을 많이 사용하는 채굴을 한 번만 실행하고 여러 개의 블록을 체인에 연결하는 방법을 통해 트랜잭션의 처리속도를 증가시켰다.

모든 노드가 블록을 생성하는 과정과, 합의를 이끌어 내는 과정에 참여하여 많은 검증을 거치는 방법이 보안성에 이득을 보인다. 하지만 모든 노드가 참여함으로써 거쳐야 할 과정이 늘어나 처리 시간이 증가한다. 네트워크의 규모가 커지는 경우 적합하지 않을 수 있다. Bitcoin-NG는 블록체인의 암호기술에 채굴보다 처리속도가 비교적 빠른 공개키 암호 기술을 결합하여 처리속도와 보안성을 모두 고려한 합의 알고리즘이다. 확장성을 고려하였을 때, 가장 적합하다. 하나의 리더 노드를 선정하는 과정에 모든 노드가 참여함으로써 특정 노드의 독점을 막을 수 있으

며, 공개키 암호 기술을 이용하여 하나의 리더 노드가 여러 개의 신뢰 블록을 생성하는 것이 처리속도를 줄임으로서 보안성과 확장성을 가진 합의 알고리즘이다. 다른 분야로 확장성을 고려하였을 때, 여러 다른 보안 기술과 블록체인 기술을 융합하여 안전성을 고려한 리더 선출을 통해 보안성을 결여 시키지 않도록 여러 개의 신뢰 블록을 생성하는 방법이 효율적일 것이라 사료된다.

5. 결론

블록체인은 P2P 연결에서 신뢰하지 않는 노드들 사이에 신뢰를 합의하는 데이터베이스 시스템이다. P2P 연결을 기반으로 하는 IoT를 비롯한 다양한 분야와의 결합 가능성이 기대되는 기술이다. 합의에 도달하는 시간이 오래 걸리는 등의 문제로 인해 융합에 어려움을 겪고 있다. 하지만 Bitcoin-NG와 같은 보안성의 감소 없이 트랜잭션 처리량을 증가시킬 수 있는 합의 알고리즘을 이용한다면 확장성에 긍정적인 것이라 사료된다. 아직 Bitcoin-NG 또한 완벽한 기술은 아니지만 앞으로 블록체인과 다른 암호 기술의 융합이 시도되다 보면 한계점을 극복할 수 있는 다양한 방법들이 제시될 수 있을 것이라 기대된다.

Acknowledgement

- This study was supported by the Advanced Research Project funded by the SeoulTech(Seoul National University of Science and Technology)

참고문헌

- [1] Nakamoto. Satoshi, "Bitcoin: A peer-to-peer electronic cash system", <https://git.dhimmel.com/bitcoin-whitepaper/>, Access by Mar. 2020.
- [2] 광현, "블록체인(BlockChain)기술의 산업동향 및 특허동향", https://www.kiip.re.kr/board/report/view.do?bd_gb=data&bd_cd=4&bd_item=0&po_item_gb=5&po_item_cd=dgb_20&po_no=12351, Access by Mar. 2020.
- [3] 이제영, 우정원, "블록체인 기술의 전망과 한계 그리고 시사점", FUTURE HORIZON, Future Horizon:2018 제38호, 12-15, 2018.
- [4] 가사키 나가토, "처음 배우는 블록체인", 한빛미디어, 2018. (2판)
- [5] Sunny. King and Scott. Nadal, "PPcoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake", <https://www.chai.nwhy.com/upload/default/20180619/126a057fef926dc286acc>

b372da46955.pdf, Access by Apr. 2020.

- [6] BitFury Group, "Proof of Stake Versus Proof of Work White Paper", <https://www.semanticscholar.org/paper/Proof-of-Stake-versus-Proof-of-Work-White-Paper/69900bac4097a576414f69f1998c11089fb5bb94>, Access by Apr. 2020.
- [7] 임종철, 유현경, 광지영, 김선미, "블록체인과 합의 알고리즘", 전자통신동향분석, 제33권, 1호, 45-56, 2018.
- [8] steam, "An incentivized, blockchain-based, public content platform", <https://steem.com/SteemWhitePaper.pdf>, Access by Apr. 2020.
- [9] Eyal. Ittay, et al, "Bitcoin-NG: A Scalable Blockchain Protocol", 13th {USENIX} symposium on networked systems design and implementation ({NSDI} 16), Santa Clara, USA, 2016, pp.45-59.

컨소시움 블록체인을 이용한 내부자 이상행위 탐지의 관한 연구*

최용철, 이덕규**

**서원대학교 정보보안학과

cho6nt@gmail.com, deokgyulee@gmail.com

A Study on Insider Anomaly Detection Using Consortium Blockchain *

Yong cheol Choi, Deok Gyu Lee**

**Dept of information security, Seowon University.

요 약

첨단 기술이 나날히 발전하면서 매년 내부자에 의한 기밀 유출 또한 증가함에 따라 기업에 피해가 발생하고 있다. 기업비밀이 유출될 경우 기업 입장에 막대한 손실을 미칠 수 있으며, 핵심 기술 유출은 해마다 지속적으로 증가하는 추세이다. 본 논문은 기존 기계학습을 이용한 내부자 이상행위 탐지 시스템에 컨소시움 블록체인을 이용하여 꾸준한 기록 관리를 통해 내부자의 이상행위를 탐지하는 솔루션을 제안하여 내부자 유출을 방지하고자 한다.

I. 서론

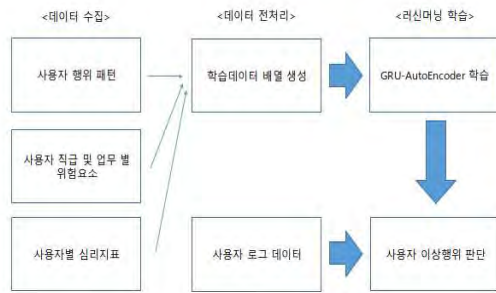
산업기밀유출범죄는 매년 증가하고 있다. 2013년을 기점으로 해외로 유출하려는 건수가 급격하게 증가하고 있으며 2014년 피해건수는 472건, 피해금액은 50조원으로 중소기업 4,700여 개의 연 매출과 맞먹는 금액이다. 이러한 손실을 최소화하기 위한 범 국가적인 대응체계 마련과 중소기업의 보안체계 구축을 위한 회사의 관심과 의식향상이 필요하다. 산업기밀보호센터의 기술유출 분야별현황을 보면 우리나라가 높은 경쟁력을 가지고 있는 정밀 기계(34%), 전기 · 전자(26%),

정보통신(14%) 분야에서 많은 산업기밀 유출사건이 일어나고 있다.[1] 산업스파이의 표적 기술은 점점 대기업의 IT 분야 기술에서 중소기업의 정밀기계 분야로 이동 및 확대 되고 있다는 것을 알 수 있다. 이를 방지하기 위해 본 논문에서 기존 내부자 이상행위 탐지를 위한 시스템에 블록체인 사용을 제안하고, 목차로는 2장에서는 본 논문에서 제안하는 시스템을 다루며, 3장에서 결론으로 마무리 짓는다.

II. 제안 방식

2.1 시스템 구성

*본 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No. 2020-0-00326, 블록체인 기반 물류정보의 실시간 트래킹을 통한 스마트 항만 응용 플랫폼 개발)



[Fig. 1] Schematic diagram of existing systems

기존 시스템의 시스템 구성은 사용자의 비정상행위를 탐지하기 위해 사용자의 정상행위를 학습한 후 사용자가 정상행위인지 아닌지를 판별하게 된다. 이 때 판별하는 기준이 사용자별로 하루 업무는 순서가 있고, 매일 비슷한 흐름으로 업무를 진행하게 될 것이다. 또한 각 개인마다 일정한 패턴을 갖고있는데 이 데이터를 학습해 기준으로 잡아 정상행위로 판단할 것이다. 이 외에 내부자 위협에 이상행위에 대해서 2가지로 나눌수 있는데 첫 번째론 행동적 이상행위로 평소 업무시간 이외에 네트워크 접근과 불필요한 파일에 복사 USB 과다횟수 연결등 평소 업무에 크게 빗나가는 행동을 할 경우와 두 번째론 심리적 요인인데 해당 사용자의 취약한 심리상태와 적대적인 행동이다. 이를 기준삼아 머신러닝에 정상행위를 학습시킨다.

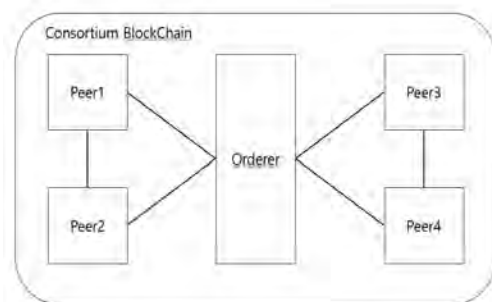
성향	요소
행위적 요인	로그인/로그오프 기록
	웹 활동
	파일 액세스 활동
	전자 메일 사용
	Device 사용
상황적 요인	업무시간 외 컴퓨터 사용
	직위
	부서
	근무기간
심리적 요인	참가 프로젝트
	직무만족도
	심리지표

[Fig. 2] Example of data target by user

기계학습을 하기 위해서는 데이터 분석이 필요하다. 데이터 분석을 통해 불필요한 정보를 제거하고 기계학습의 효과를 최대한으로

할 수 있다. 수집 데이터로서는 시간행 순서로 사용자 로그인/로그오프 기록, 웹 활동, 파일 액세스 활동, 전자 메일 사용, 장치 사용 및 사용자들의 직위, 부서, 근무 기간, 참가 프로젝트, 직무 만족도등을 담은 데이터를 수집할 것이고 그 외에도 각 사원에 대한 심리적 성향 지표도 함께 데이터 배열을 생성할 것이다. 여기서 컨소시엄 블록체인을 이용하여 기존의 사용자 데이터를 공유함으로써 기계학습의 데이터량을 더 늘리고 학습범위도 늘려서 탐지율을 더욱 높일 수 있고, 이상행위 점수 공유에 따른 초기 탐지에도 도움이 될 수 있는 블록체인을 이용한 공유 시스템을 제안한다.

2.2 컨소시엄 블록체인 적용



[Fig 3.] Consortium BlockChain Principle



[Fig 4.] Insider abnormality score inside the blockchain

기존의 내부자 이상행위 탐지를 위한 데이터들을 합산하여 내부자 이상행위에 대한 점수를 계산하고, 각 사용자에게 대한 점수를 사용자 가상지갑에 저장시키는 방식으로 제안한다. 일종의 가상거래를 통한 평가점수를 저장하며, 사용자 가상지갑을 통해 기존의 내

부자 이상행위에 대한 정보를 파악 할 수 있으며, 마치 신뢰도 평가와 같은 방식으로 작동 할 수 있다. 기업입장에서는 이력서 이외에 기업 비밀 유출에 관한 확률또한 계산 할 수 있으며, 신입사원 혹은 경력직을 모집 할 때에 좀 더 유용한 정보로 사용 할 수 있다. 또한 여럿이서 공유함으로써 기존에 있던 내부자 이상행위 평가 점수에 관한 검증도 할 수 있으므로 더욱 유용한 정보로 사용 될 수 있다.

2.3 제시되는 문제점

기존 시스템에 블록체인을 적용하여 평가점수를 이용한 내부자 이상행위 탐지 및 평가에 관한 문제점은 기존 사용자들의 프라이버시가 문제가 될 수 있다. 자신의 평가점수가 기업을 통해 공유됨으로써 과거의 평가점수가 어디에서든지 공유되고 문제가 제시될 수 있고, 또한 개인정보로 분류 될 수 있기 때문에 개인정보에 관한 문제가 있다. 따라서 블록체인 서비스에 관한 개인정보 관리에 대한 연구가 더욱 진행되어야 하는 과제가 남아 있다.

2.4 제안 방식 평가

	기존 방식 (GRU를 이용한 내부자 이상행위 탐지)	제안 방식 (기존 시스템에 블록체인을 활용한 평가점수 도출)
학습데이터 축적량		
지속적인 기록 관리	X	O
내부자 이상행위 검증	X	O

[표 1.] Evaluate proposed method

기존 시스템과의 비교에서 기존 시스템을 유지한다고 할 때, 학습데이터에 관한 축적량은 블록체인을 이용하여 공유하였을 때 더욱 높다. 또한 지속적인 시스템 사용으로 기록관리를 할 때 블록체인을 이용한 방식이 더욱 수월하다는 것을 볼 수 있다. 블록체인을 이용하였을 때 내부자 이상행위의 오탐 및 검증에 관한 문제를 해결 할 수 있으며, 타 기업들과의 컨소시움을 통하여 초기 탐지에

관한 문제도 해결 할 수 있다. 정보가 없을 경우 탐지에 문제가 생길 수 있지만 컨소시움을 맺은 기업들간의 정보가 공유될 시에 더욱 많은 데이터량을 가지고 탐지 할 수 있기 때문이다.

III. 결론

첨단 기술이 나날이 발전하면서 매년 산업스파이에 의한 기밀 유출 또한 증가함에 따라 기업들이 막대한 피해가 발생하고 있다. 이에 사내에서는 이상 행위 탐지 도구를 사용해도 사용초기에는 사용자에게 대한 데이터가 없을시와 신입사원이 새로 회사에 입사할 시 보안 도구에 변경으로 데이터가 추가될 경우 데이터의 부족으로 어떤 사원이 내부 유출자인지 정확한 판단이 힘들어 질 수 밖에 없다. 이러한 문제점을 개선하기 위해 본 논문에서는 사용자 행위를 탐지하는 기존 시스템에 블록체인을 이용하여 더욱 넓은 탐지 환경을 제공 할 수 있는 환경을 만드는 시스템을 제안하여 기업의 내부자를 통한 비밀 유출을 방지하고자 한다.

[참고문헌]

- [1] 한국산업기술보호협회,
http://www.kaits.or.kr/front/bmt/bbs/list.act?bbs_config_nid=2
- [2] 박정홍, 'Private 블록체인 특성이 의료분야 수용의도에 미치는 영향' 성균관대학교 일반대학원.
- [3] Jerald Lee, "SSDT Hooking", November 2006.
- [4] 이기영, '기록관리시스템 블록체인 기술 적용 방안 연구' 명지대학교, [2019]
- [5] 고필성, '블록체인을 이용한 의료정보시스템 활용방안에 관한 연구' 숭실대학교,

- [2019] 김혜리 , 강희정 , 홍승필
보안공학연구논문지 ,pp. 139 - 154 , 2018 ,
- [6] 구동균 ‘Deep Learning을 이용한 택시 승객 승차 예측에 관한 연구’ 서울시립대학교 [2018]
- [7] 여강국 ‘H-CNN 알고리즘을 이용한 이미지 데이터 학습과 정확도 측정 및 학습 속도 비교’ 동아대학교 [2017]
- [8] Keji Zheng, Wei Qi Yan, and Parma Nand, “Video Dynamics Detection Using Deep Neural Networks”, Journal of IEEE, pp. 1-11, Dec. 2017.
- [9] S. N. Danilin and S. A. Shchanikov, "Neural Network Algorithms for Determining the Values of Signal Parameters in Radio-Electronic Hardware", Journal of IEEE, Vol. 14, Nov. 2017.
- [10] 조영복 ‘딥러닝 기반의 R-CNN을 이용한 악성코드 탐지 기법’ 디지털콘텐츠 학회 논문지, 대전대학교 [2018]
- [11] 정예나 ‘블록체인 기반 영상 정보 관리 시스템’ 아주대학교 [2019]
- [12] 효율적인 이더리움 스마트 콘트랙트에 관한 연구
김대한 (아주대학교 사이버보안학과) , 최광훈 (아주대학교 컴퓨터공학과) , 김강석 (아주대학교 사이버보안학과) , 김재훈 (아주대학교 사이버보안학과)
한국정보처리학회 2018년도 추계학술발표대회 2018 Oct. 31 ,pp. 82 - 84 , 2018
- [13] 핀테크를 위한 스마트 컨트랙트 보안
신다혜 (가천대학교) , 이종협 (가천대학교)
정보처리학회지 = Korea information processing society review v.22 no.5 ,pp. 54 - 62 , 2015 , 1226-9182 ,
- [14] 개인정보보호를 고려한 스마트 컨트랙트 설계 방안 연구

이종 장치간 전송 파일의 추적 정보 연구

조을한*, 김지선**, 조태남***

*기전대학교 디지털포렌식학과

**우석대학교 정보보안학과

***우석대학교 IT전자융합공학과

joedulhan@gmail.com, rlawltjs122@gmail.com, tncho@ws.ac.kr

Research on tracking information of file transferred between heterogeneous devices

Eulhan Jo*, Jisun Kim**, Taenam Cho***

*Dept. of Digital Forensics and Information Security, Kijeon University

**Dept. of Information Security, Woosuk University

***Dept. of IT and Electronics Engineering, Woosuk University

요 약

파일 추적은 디지털 포렌식에서 매우 중요한 요소이며, 파일 추적에는 파일의 원본 확인과 이동 경로 분석이 수반된다. 본 논문은 다양한 매체를 통해 이미지 파일이 전송될 때 변화하는 시각정보와 원본 확인에 사용되는 해시값의 변화를 분석함으로써 파일 추적 시 고려해야 할 사항을 연구하였다.

1. 서론

디지털 포렌식에서 중요한 요소 중의 하나인 파일 추적은 기밀 파일의 배포 여부와 배포경로를 알아내는 것이다. 이를 위해서는 어떤 파일이 원본 파일로부터 배포된 것이며 배포경로를 입증할 수 있어야 한다. 파일 추적은 한 가지 기술로만 해결하기 어려우며 시스템 로그, 워터마크, 이동 매체 확인 등 많은 기술이 복합적으로 요구된다.

두 파일이 동일하다는 것은 두 파일의 해시값을 비교함으로써 확인할 수 있으며, 파일에 연관된 시간 정보는 파일의 원본과 사본을 구분 및 배포경로를 파악하는 중요한 정보가 된다[1]. 그러나 파일의 시간 정보와 해시값은 매체를 통해 다른 단말장치에 저장될 경우 매체나 단말장치에 따라 시간 정보가 달라지기도 하고[2][3] 파일이 변형되기도 한다[4]. 최근에는 PC와 이메일 뿐만 아니라 스마트폰, USB, 클라우드 등 다양한 저장 매체가 존재하며, 이들 저장 장치 간의 이동 수단도 USB, 이메일, 클라우드 저장소 등 매우 다양해졌다.

본 논문에서는 특히 아이폰의 이미지 파일이 대표적인 여러 매체를 통해 전달될 때 나타나는 시간 정보의 변화와 해시값의 변화를 분석하였다.

2. 관련 연구

(1) 파일 시간 정보

파일에는 파일시스템이 제공하는 정보와 파일 자체가 보유하고 있는 메타정보가 존재한다.

널리 사용되고 있는 FAT과 NTFS 파일시스템의 메타정보에서 파일의 생성, 수정, 접근시간 정보를 확인할 수 있으며 이 정보는 파일 자체에 포함되지 않고 파일시스템이 제공하는 정보이다. FAT과 NTFS 파일시스템에서 시간 정보를 가지고 있는 영역은 각각 표 1과 표 2 와 같다.

<표 1> FAT의 DATA 영역

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
		Name						Extension		Attr	Reserved		Created Time		
Created Date	Last Accessed Date		Starting Cluster HI	Last Written Date		Last Written Date		Starting Cluster Low		File Size					

<표 2> NTFS 의 \$STANDARD_INFORMATION

Attribute Header			
Created Time		Modified Time	
MFT Modified Time		Accessed Time	
Flag	Max Number Of Version	Version Number	Class ID
Owner ID	Security ID	Quota Charged	
Update Sequence Number (UCN)			

이미지 파일의 경우에는 EXIF(Exchangeable Image File Format)라고 하는 이미지 파일 메타데이터 포맷을 통해 사진에 대한 정보가 메타데이터로 제공되며 이 정보는 파일 일부로 포함된다.

EXIF에는 카메라 제조사(Maker), 카메라 모델(Model) 등 매우 많은 정보가 수록되어 있으며, 우리가 관심 있는 시간정보로는 생성, 수정, 접근시간 외에도 다양한 세부적인 시간 정보를 담고 있다.

(2) 해시함수

해시함수(hash function)는 데이터의 무결성을 증명하는 가장 널리 쓰이는 효율적인 방법이다. 해시 함수 $h(x)$ 는 함수값 $y=h(x)$ 로부터 x 를 알아낼 수 없다는 일방향성과 동일한 해시값을 가지는 서로 다른 입력값을 알아낼 수 없다는 충돌 회피성을 가진다. 따라서 두 파일이 해시값이 같으면 동일한 파일이라고 인정할 수 있으며, 주어진 해시값을 이용하여 원본 파일을 생성해 낼 수 없다. 이러한 성질에 근거하여 해시함수는 파일의 무결성과 원본 확인에 사용된다. 가장 널리 사용되는 해시함수로는 MD5, SHA1, SHA2(SHA128, SHA256, SHA512) 등이 있다.

3. 실험 환경 및 방법

이미지의 전달 매체에 따라 달라지는 파일 정보를 실험하기 위해서 그림 1과 같이 아이폰으로 촬영한 jpg 타입의 사진 파일을 여섯 가지 전송 매체를 통해 전송한 후 수신 단말기에서 해시값과 시간 정보를 확인하였다. 원본 파일을 원격 드라이브에 업로드할 때는 선택자에 따라 여러 가지 파일 타입으로 업로드하였다(표 3 참조). 안드로이드, 아이폰에 있는 jpg의 해시값은 PC에 연결하여 HashCalc 프로그램[5]을 이용하여 SHA256 값을 계산하였다.



(그림 1) 실험 방법

<표 3> 실험 환경

Source		전달 매체	확장자	Destination	
Device	확장자			Device	해시함수
iPhone Xs, iPhone 11 Pro	jpg	USB	jpg	PC, Android (Galaxy A5), iPhone	SHA256
		Gmail			
		카카오톡	jpg		
		네이버			
		클라우드	heic		
		구글	jpg		
드라이브	heic				

4. 실험 결과

(1) 시간 정보

아이폰에 저장된 원본 사진 파일을 PC나 안드로이드로 전송했을 때, 파일시스템이 제공하는 시간정보는 모두 수신/다운로드한 시간으로 변경된다. 아이폰으로 이메일을 통해 전송했을 때도 모두 수신한 시간으로 변경된다. 그 외의 방법으로 아이폰으로 전달했을 때는 생성시간이 원본과 그대로 유지된다.

EXIF에 저장된 다양한 시간 정보도 전송 방식에 따라 삭제되기도 하였다. 그러나 삭제되지 않은 경우에는 원본과 동일한 시간정보로 유지된다. 표 4는 각각의 수신 단말에 사본이 만들어 졌을 때 시간정보가 유지되는지를 나타낸 것이다.

<표 4> 파일 전송으로 인한 시간 정보의 유지 여부

Source	전송 매체	Destination		
		PC	안드로이드	아이폰
아이폰	USB	○	-	-
	Gmail	×	×	×
	카카오톡	○	×	○
	네이버 클라우드	○	○	○
	구글 드라이브	○	○	○

(2) 해시값

아이폰 단말장치 사이에서 전송 방식을 달리하여

사본을 생성하고, 원본 이미지와 사본 이미지의 해시값을 비교하였다. SHA256 결과값이 커서 동일한 값만 구분하기 위하여 알파벳으로 표기하였다.

파일을 전송 방법은 아이폰 갤러리에서 전송 프로그램으로 공유하는 방법과 전송 프로그램에 접속하여 업로드하는 방법이 존재하는데, 전송 방법에 따라 각각 다른 해시 패턴을 보이기 때문에 표 5와 같이 6개로 나누어 실험하였다. 실험 결과의 일관된 분석을 위해, 여러 개의 파일에 대하여 동일한 실험을 실행하였으며, 하나의 파일에 대해서도 3번 이상 동일한 실험을 실행하여 항상 같은 결과가 나타나는지 관찰하였다.

<표 5> 사진 파일 공유 방법

실험 구분	전송 파일	전달 방법
실험 1	원본 파일 f0	프로그램에서 업로드
실험 2		갤러리에서 업로드
실험 3	사본 파일 f1	프로그램에서 업로드
실험 4		갤러리에서 업로드
실험 5	사본 파일 f2	프로그램에서 업로드
실험 6		갤러리에서 업로드

표 6은 실험 1에 대한 결과로서, 원본 파일 f0을 전송 프로그램에 접속하여 파일을 업로드/다운로드했을 때 해시값을 비교한 결과이다. 네이버 클라우드에 heic로 업로드하여 아이폰에서 다운로드했을 때만 원본 해시값과 같고, 다른 경우에는 해시값을 가진다.

<표 6> 전송 프로그램에서 원본 파일 업로드(실험 1)

Source		전송 방식	확장자	Destination		
단말	해시			PC	안드로이드	아이폰
아이폰	A	USB	jpg	A	-	-
		Gmail	jpg	B1	B1	B2
		카카오톡	jpg	B3	B3	B4
		네이버 클라우드	jpg	B5	B5	B5
			heic	B6	B6	A
		구글 드라이브	heic	B6	B6	B7

표 7은 원본 파일 f0을 아이폰 갤러리에서 공유 버튼을 이용하여 jpg 파일을 업로드했을 때의 결과이다. 여섯 가지 전송 방식 모두 jpg 확장자로 업로드되며 모두 원본과 다른 해시값을 가진다.

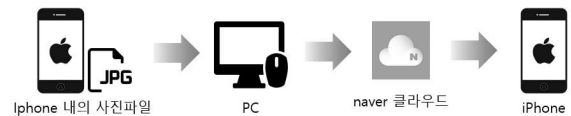
<표 7> 갤러리에서 원본 파일 업로드(실험 2)

Source		전송 방식	확장자	Destination		
단말	해시			PC	안드로이드	아이폰
아이폰	A	USB	jpg	A	-	-
		Gmail	jpg	C1	C1	C2
		카카오톡	jpg	C1	C1	C3
		네이버 클라우드	jpg	C1	C1	C3
		구글 드라이브	jpg	C1	C1	C1

표 6에서 본 바와 같이 2가지 경우에서 원본과 해시값이 동일하게 나타난다. 우리는 이 사본들을 이용하여 다시 실험을 수행하였다. 2번째 전송 방식에서 생성된 사본을 f1이라고 하고(그림 2), 첫 번째 전송 방식에서 생성된 사본을 가지고 2번째 전송 방식을 이용하여 생성된 파일을 f2라고 하자(그림 3).



(그림 2) 사본 파일 f1 생성 방법



(그림 3) 사본 파일 f2 생성 방법

f1을 가지고 표 6과 표 7의 실험을 수행한 결과 결과는 각각 표 8 및 표 9와 같다. 표 6은 표 8과 동일하고 표 7은 표 9와 동일한 것으로 나타난다. 즉, 예상대로 원본을 가지고 실험했을 때와 동일한 결과를 보인다.

<표 8> 전송 프로그램에서 f1 업로드(실험 3)

Source		전송 방식	확장자	Destination		
단말	해시			PC	안드로이드	아이폰
아이폰	A	USB	jpg	A	-	-
		Gmail	jpg	B1	B1	B2
		카카오톡	jpg	B3	B3	B4
		네이버 클라우드	jpg	B5	B5	B5
			heic	B6	B6	A
		구글 드라이브	heic	B6	B6	B7

<표 9> 갤러리에서 f1 업로드(실험 4)

Source		전송 방식	확장자	Destination		
단말	해시			PC	안드로이드	아이폰
아이폰	A	USB	jpg	A	-	-
		Gmail	jpg	C1	C1	C2
		카카오톡	jpg	C1	C1	C3
		네이버 클라우드	jpg	C1	C1	C3
		구글 드라이브	jpg	C1	C1	C1

f2를 가지고 표 6과 표 7의 실험을 수행한 결과 결과는 각각 표 10 및 표 11과 같다. 이 경우에는 예상과 달리 f2가 원본과 해시값이 동일한 사본임에도 불구하고 실험 결과가 원본에 대한 실험 결과와 전혀 다른 결과를 보이고 있다.

<표 10> 전송 프로그램에서 f2 업로드(실험 5)

Source		전송 방식	확장자	Destination		
단말	해시			PC	안드로이드	아이폰
아이폰	A	USB	jpg	A	-	-
		Gmail	jpg	D1	D1	D2
		카카오톡	jpg	A	A	D3
		네이버 클라우드	jpg	D4	D4	D4
			heic	A	A	A
		구글 드라이브	heic	A	A	A

<표 11> 갤러리에서 f2 업로드(실험 6)

Source		전송 방식	확장자	Destination		
단말	해시			PC	안드로이드	아이폰
아이폰	A	USB	jpg	A	-	-
		Gmail	jpg	A	A	B3
		카카오톡	jpg	A	A	B4
		네이버 클라우드	jpg	A	A	A
		구글 드라이브	jpg	A	A	A

5. 결론

본 논문에서는 아이폰에 저장된 이미지 파일이 다양한 매체를 통하여 다른 장치로 전송되었을 때 발생 되는 시간 정보의 변화와 해시값의 변화를 조사하였다. 저장 단말장치나 전송 매체에 따라 시간 정보가 달라지고, 파일의 해시값도 달라지는 것을 확인하였다. 해시값은 원본과 동일함을 확인하는 중요한 수단으로서, 해시값이 다를 경우 동일한 파일이라고 단정하기 어렵다. 원본에 아무 수정이 가해지지 않은 사본에 대해서 해시값이 달라지기 때문에 단순히 해시값의 비교로서 원본을 확인하는 것은 위험한 일이다.

향후에는 다양한 이미지 타입의 파일과 동영상 및 다양한 전송 방식에 대해 분석할 것이다. 또한 해시값의 변화를 야기시키키는 원인에 대해 조사하고, 원본 확인을 위한 방법을 연구하고자 한다.

Acknowledgement

이 논문은 2017년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(NRF-2017R1D1A3B03032637).

참고문헌

- [1] J. Kim, Mo. Kwak, S. Lee, and T. Cho, "File Tracking Technique with Active Directory Event Log," World IT Congress, paper no. 23, 2020.
- [2] K. Jin, J. Yang, S. Lee, S. Han, T. Cho, "A Study on the File Trace using File Metadata," Journal of KICS, Republic of Korea, 2018, pp.873-874.
- [3] J. Bang, B. Yoo, S. Lee, "Timestamp Analysis of Windows File Systems by File Manipulation Operations," Journal of KIISC, 20(3), pp.79-91, 2010.
- [4] S. Han, Practice on Digital Forensics, BOOKK, 2019.
- [5] HashCalc, <https://www.slavasoft.com/hashcalc/>.
- [6] naver Cloud, www.cloud.naver.com.
- [7] Google Drive, www.google.com/drive/.

GRU를 활용한 악성코드 탐지의 관한 연구^{*)}

류경근, 최용철, 이덕규**

**서원대학교 정보보안학과

ryu8340@gmail.com cho6nt@gmail.com, deokgyulee@gmail.com

A Study on Malicious Code Detection Using GRU**

Ryu Kyeong Geun, Yong cheol Choi, Deok Gyu Lee

**Dept. of information Security, Seowon University

요 약

최근 악성코드에 의한 피해사례가 매년 증가하고 있다. 전통적인 시그니처 기반 안티바이러스 솔루션은 제로데이 공격이나 랜섬웨어처럼 전례가 없는 새로운 위협에 속수무책일 정도로 취약하다. 그럼에도 불구하고 많은 기업이 다중 엔드포인트 보안 전략의 일환으로 시그니처 기반 안티바이러스 솔루션을 유지하고 있다. 이에 응하고자 다양한 악성코드 분석기술이 출현해왔으며, 최근의 연구들은 부분 머신러닝을 이용하여 기존에 진행했던 시그니처 기반의 한계를 보완하고 노력하고 있다. 본 논문은 머신러닝을 이용한 바이러스 분석 모델과 머신러닝 알고리즘 중 GRU를 이용한 솔루션 시스템을 제안한다. 기존 DB Server를 통해 머신러닝을 학습 시키며 다양한 샘플과 형식을 이용하여 머신러닝을 학습하고 이를 이용해 새로운 악성코드, 변조된 악성코드의 탐지율을 높일 수 있다.

1. 서론

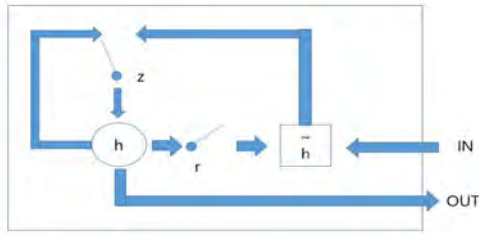
최근 기업 사용자는 데스크톱 PC뿐만 아니라, 노트북, 태블릿, 스마트폰, 그리고 수많은 이동식 저장장치를 사용한다. 또한 최근에는 IoT, 클라우드 컴퓨터등이 실사용화 되면서 새로운 악성코드들이 대량 발생하며 신종 악성코드는 20% 미만이라고 한다. 나머지는 기존에 있던 악성코드들이 변형되어 사용된다. 진화하는 악성코드와 취약점은 주로 이런 엔드포인트 기기들을 노리고 있어 보안 상태는 나날이 위험해지고 있다. 카스퍼스키 통계에 따르면, 2018년에 탐지된 전체 신종 악성 파일 중에서 백도어로 밝혀진 악성 파일의 수는 44% 증가했으며 랜섬웨어의 규모도 43% 증가했다고 발표 했다.

이는 사이버상에서 심각한 위협이 되며, 이러한 악성코드는 나날히 발전하여 더욱 정교해지고 복잡해지고 있다. 50% 이상의 악성코드가 안티바이러스 제품에 탐지되지 않는 경우가 발생한다.[1] 기계 학습 방법은 데이터로부터 알고리즘을 지속적으로 학습하여 갱신할 수 있기 때문에 변칙적인 침입에 유연하게 대응할 수 있는 장점을 가지고 있다.[2] 이러한 측면에서 바이러스 발생 초반 바이러스에 대한 적은 데이터로 머신러닝을 학습시켜 초기 데이터로도 변종 악성코드를 탐지할 수 있도록 하는 GRU를 활용한 머신러닝 탐지 모델을 제안한다.

*) 본 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No. 2019-0-00326, 블록체인 기반 물류정보의 실시간 트래킹을 통한 스마트 항만 응용 플랫폼 개발)

2. 관련연구

2.1 GRU(Gated Recurrent Unit)

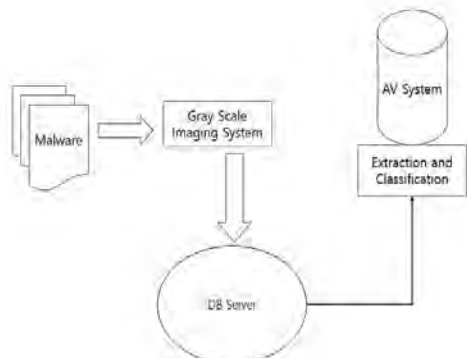


(그림 1) GRU 모델 구조

GRU(Gated Recurrent Unit)는 2014년 발표된 모델로 LSTM의 구조를보다 단순하게 처리한 LSTM 변형모델의 하나이다. GRU의 구조는 LSTM과 마찬가지로 gate를 이용하여 정보의 양을 조절하는 것은 같지만, gate의 제어 방식에는 차이가 있음을 알 수 있다. GRU는 LSTM의 forget gate와 input gate를 update gate로 통합하고, 이를 기준으로 상호작용하는 네 개의 층이 존재한다. 입력데이터를 선택적으로 학습시키기 위해 세 개의 셀 상태의 게이트에서 정보를 더하거나 지우는 구조를 가지고 있다.[3] 셀 상태와 은닉 상태를 하나로 통합하였다. LSTM보다 단순한 구조로 가중치 수가 작으므로 또한 학습이 더 빠르지만, LSTM과 거의 같은 성능을 보인다.[4]

3. 제안방식

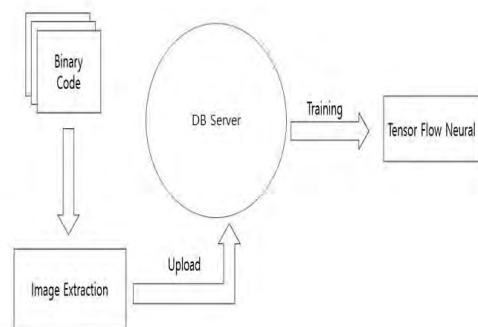
3.1 시스템 구성



(그림 2) 시스템 흐름도

이 그림은 본 논문에서 제안할 방식 시스템의 흐름과 AV(Anti-Virus) System의 분류하여 학습하는 과정을 나타낸다. 먼저 DB Server에는 이미지가 등록된다. 사용자들이 파일의 그레이스케일을 추출해주는 모듈에서 파일에 특정 특징을 배열화 시켜 DB Server에 등록 하면 머신러닝을 통하여 그레이스케일 화 된 이미지를 가져오고 이미지 파일에서 배열을 추출하여, 분류 작업을 통하여 악성코드와 정상파일 등을 분류한다. 본 논문에서 사용한 머신러닝은 LSTM의 한 종류인 GRU를 사용하며 제안하는 방식은 기존 머신러닝 모델보다 게이트 수가 적으며 구조가 간단하여[5] 빠르고 많은 데이터를 실시간성으로 추가할 수 있고, 다양한 데이터셋을 통해 더 수준 높은 기계학습이 가능하여, 기존 Deep Learning 방식의 전수조사의 다양성 또한 보장 할 수 있다.

3.2 악성코드 분류 및 탐지



(그림 3) 악성코드 이미지화

악성코드를 이미지화 시키는 분류 시스템의 흐름은 [그림 3.]과 같다. 먼저, 악성코드 바이트코드를 이미지화 하는 작업을 수행한다. 이 과정을 통해 일정크기의 이미지로 변환시키고, 이미지의 크기에 따라 분류정확도가 영향을 받는다. 이미지화 된 악성코드의 이미지를 학습시킨다.

3.3 데이터 전처리

기계학습을 하기 위해서는 데이터 분석이 필요하다. 데이터 분석을 통해 불필요한 정보를 제

거하고 기계학습의 효과를 최대한으로 할 수 있다. 수집 데이터로서는 악성코드 분석에 사용되는 Feature들은 PE header, Strings, Sequences, DLL/API, Entropy, Instructions, Visualization, Memory 정보, File 정보, Registry 정보, CPU Register, Network 속정보, Anti-Virus 분석정보[6]등 다양하지만, 그 중 분석에 주요한 정보를 가진 5가지인 PE Header, Printable Strings, Sequences, DLL/API, Entropy에 관한 데이터를 수집할 것이고 이 정보와 그 파일이 악성코드인지 여부를 통해 배열을 만들어 머신러닝으로 학습을 시킨다.

3.4 머신러닝의 비정상 행위 탐지

학습 행위를 마치면 각각의 파일들에 대한 정상파일에 대한 출력 시퀀스를 가지고 있다. 이를 이용해 가중치를 계산한다.[7] 또한 이 가중치를 임계치로 설정하여 후에 다른 파일로부터의 정보를 계속 받아와 분석을 하여 분석 정보를 추출하고 가지고 있던 정상파일과 비교하여 이를 정상파일과 동일하거나 유사한 패턴의 형태를 가지면 가중치가 임계치를 넘지않으니 평소와 비슷함으로 정상파일로 간주하며 비정상 패턴이면 가중치가 정상패턴과 크게 다르게 되므로 임계치를 초과하여 비정상파일로 탐지한다.

3.5 Dropout 적용에 따른 성능 차이

인공신경망의 학습은 가중치를 일정 범위 내에서 골고루 분포하도록 초기화 할 경우 좋은 결과를 보이며 Dropout 기법을 통해 과다학습을 방지할 수 있다.[7] 일반적인 신경망 모델에서는 Dropout을 적용할 때 더 좋은 성능을 보인다. 하지만 RNN 계열의 모델들을 정규화 하는 방법은 많이 적용되지 않고 RNN 모델을 확장하고 보완하여 만든 GRU 모델 역시 Dropout을 적용하면 오히려 성능이 떨어진다. [9]

3.6 머신러닝 모델 비교

<표 1> 머신 러닝 모델 비교

	데이터 의존도	정확도	과적합 빈도
RNN	○	△	○
LSTM	○	○	△
GRU	△	○	X

<표 1> 은 기존에 있던 RNN과 LSTM을 활용하여 만든 사용자 행위 분석과 본 논문에서 제안하는 시스템간의 비교를 나타내고 있다. 데이터 의존도 측면에서는 기존의 RNN과 LSTM은 사용자 분석의 데이터 의존도는 매우 높다. 이에 반해 GRU는 LSTM에서 데이터 의존도를 낮추어 제안된 모델로서 데이터가 부족한 경우에도 기존 방식보다 빠르게 이상 행동을 유추해낼 수 있다. 정확도 측면에선 RNN과 GRU 모델에 큰 차이는 없다. 하지만 GRU 모델에선 적은 데이터로와 짧은 학습 시간으로도 높은 정확도를 얻을 수 있다. LSTM은 적은 데이터에선 GRU보단 낮은 정확도를 가지지만 충분한 수의 데이터가 있을시 우수한 결과를 보여주었다. 과적합 빈도 측면에서 보자면 RNN은 히든 노드가 순환하는 방식으로 망각 게이트가 없어 과적합이 일어나기 쉽다. LSTM은 RNN에서 메모리셀을 더한 구조로서 과적합 비율을 줄였다. 여기서 GRU는 셀상태와 은닉상태를 통합하여서 더욱 메모리에 적재를 줄이고 과적합 빈도를 낮췄다. 분석한 내용을 보자면 RNN을 이용한 사용자 행위 분석보단 다른 LSTM과 GRU를 사용한 사용자 행위 분석이 월등한 성능을 갖고 있다. 여기서 LSTM은 많은 데이터를 가질 시 더욱 높은 정확도를 보여주었고 GRU는 많은 데이터를 학습할 시 LSTM보단 낮은 정확도를 가지게 되지만 GRU는 적은 데이터와 짧은 시간으로 단기간에 높은 정확도를 보여주었다. 제로데이 공격 이후 초반 적은 데이터에 대한 학습에 더 유용하다. 초기 보안 측면을 위해 본 논문에선 GRU 방식을 제안한다.

4. 결론

최근 악성코드에 의한 피해사례가 매년 증가하고 있다. 전통적인 시그니처 기반 안티바이러스 솔루션은 제로데이 공격이나 랜섬웨어처럼 전례가 없는 새로운 위협에 속수무책일 정도로 취약하다. 본 논문에서는 차세대 안티바이러스 솔루션 대책으로 머신러닝 알고리즘 중 GRU를 이용한 솔루션 시스템을 제안한다. 기존 머신러닝을 사용한 안티바이러스 소프트웨어와 비교하며 변종 악성코드를 탐지할 때 더욱 적은 데이터를 사용해서 탐지할 수 있을 것이다. 탐지하는 부분에서 다양한 샘플과 형식을 이용하여 머신러닝을 학습하고 이를 이용해 새로운 악성코드 및 변종 악성코드의 탐지율을 높일 수 있고 또한 기존의 Deep Learning 방식의 다양한 학습 및 전수조사가 필요한 부분을 GRU 알고리즘으로 보완할 수 있지만 현재 실험 데이터가 없으며 명확한 성능을 기대하기 어렵고 적용시에도 머신러닝의 문제점인 높은 오답률에 대한 개선해야한다. 최근 CNN과 GRU를 함께 사용하여 이미지에 대한 학습도를 향상 시키는 연구도 이루어지고 있으니 이에 맞춰 적용할 여지도 충분히 있다.

[참고문헌]

- [1] M. Sharif, A. Lanzi, J. Giffin, W. Lee, 'Automatic Reverse Engineering of Malware Emulators', 2009 30th IEEE Symposium on Security and Privacy, pp. 94-109.
- [2] Joe cheolhee "Research on An efficient Insider Threat Detectionbased on LSTM Autoencoder using user attribute information", Sungkyunkwan University Doctor's Thesis, Aply 2018
- [3] Seo Jihye, Yong hawnseung, 'EPerformance Evaluation of LSTM and GRU using TensorFlow,' 2014. Korea Information Science Society 2016 Winter Conference, 2016, pp. 211 - 213 (3 pages)
- [4] J. Chung, C. Gulcehre, K. H. Cho, and Y. Bengio, 'Empirical evaluation of gated recurrent neural networks on sequence modeling,' 2014.
- [5] Junyoung Chung and Çağlar Gülçehr, 'Empirical Evaluation of Gated Recurrent Neural Networks on Sequnce Modeling', Newyork Univ. ArXiv, December 2014
- [6] Tae-jin Lee, 'Trend of Intelligent Malware Analysis Technology Using Machine Learning, KIISC review v.28 no.2, April 2018
- [7] Dong-wook Ha, 'A Study on a Machine Learning Model for Detecting Insider Anomaly Behaviour', February 2018
- [8] hoe-hyeon KIM, 'Forecasting Time-series Data Using LSTM/GRU Recurrent Neural Networks', Korea National Open University Master's Thesis, July 2017
- [9] Ye-seul Lee, 'The Judgement System for the Risk Classification of Internal Data Leakage using GRU Model', soongsil University Master's Thesis, December 2017

사이버위협 동향 분석을 통한 내부망 대응 방안

변예은*

*한국원자력통제기술원
hibye@kinac.re.kr

Internal Network Response Plan through Cyber Threat Trend Analysis

Ye-Eun Byun*

*Korea Institute of Nuclear Nonproliferation and Control

요 약

한국인터넷진흥원에서는 2020년 사이버 공격에 대한 7대 전망을 일상 속 보안 취약점, 공공기관·기업 대상 랜섬웨어, 가상통화 거래소를 통한 해킹 사고, 문자 메시지·이메일을 통한 악성코드 감염, 지능형 표적 공격, 소프트웨어 공급망 공격, 융합 서비스 보안 위협으로 제시하였다. 이에 본 논문에서는 신규 사이버위협에 대한 동향 분석을 통하여 기관의 정보보안을 위해 대응할 수 있는 방안에 대해 살펴보고자 한다.

1. 서론

국내·외에서 정보보안에 대한 필요성과 인식이 높아지면서 기업들의 보안 수준도 많이 향상되고 있지만, 여전히 새로운 사이버위협들은 계속해서 발전하고 있다. 작년에도 망분리 환경에서의 제로데이 취약점으로 인한 유출 사고, 공공기관 서버에 암호화폐 채굴 악성 프로그램이 깔리는 등 새로운 위협이 등장하였으며, 랜섬웨어가 끊임없이 기승을 부리는 와중에 소디노키비, 갠드크랩 등 새로운 랜섬웨어도 생겨나고 있다. 또한, 여전히 각종 기업에서 정보유출 사고도 다양한 경로를 통해 발생하고 있다. 이러한 상황에서 기업에서는 새로운 보안 이슈가 발생할 때마다 대책을 마련하는 것도 중요하지만, 사전에 위협에 대한 분석을 통해 대응 방안을 마련해 가는 것 또한 매우 중요하다고 할 수 있다. 이에, 본 논문에서는 한국인터넷진흥원에서 발표한 국내 주요 보안 업체에서 제시한 사이버위협 7대 전망을 살펴본 후에 이에 대해 기업의 입장에서 어떠한 대응 방안을 마련할 수 있는지에 대해 살펴보고자 한다.

2. 사이버위협 분석

우선, 한국인터넷진흥원에서 발표한 2020년 사이버 공격 7대 전망에 대해 살펴보고자 한다.[1] 첫 번째로 한국인터넷진흥원에서 발표한 위협은 일상 속으로 파고든 보안 취약점에 관한 내용이다. 이는 지

능형 CCTV, AI 스피커 등 IoT 결합 서비스를 대상으로 한 사이버 위협이 증가하고 있다는 것이다. 국내 IoT 시장이 확대되는 만큼, 보안 문제에 대한 우려 또한 증가하고 있다. 통신 암호화 문제, 원격 셀 접근 문제, IoT 기기를 대상으로 한 서비스 거부 공격 문제 등 다양한 보안 문제가 대두되고 있다.[2] 다음으로, 안랩에서는 공공기관·기업으로 사칭한 랜섬웨어가 APT와 결합되어 유포됨으로써 이로 인한 피해가 확대될 것이라 발표하였다. 작년에 미국에서는 텍사스 주의 행정망에 랜섬웨어가 침투되어 이로 인한 피해는 발생하지 않았지만, 주 정부의 비상관리 대응 중 두 번째로 높은 등급인 2단계 대응조치가 이루어진 사례가 있었다.

세 번째로, 가상통화 탈취 및 가치 조작을 목적으로 하는 가상통화 거래소 관련 해킹 사고가 꾸준히 증가하고 있다. 작년에 한 공공기관의 서버가 사용자 몰래 가상화폐 채굴 프로그램 악성코드를 심는 크립토재킹에 활용된 사실이 밝혀졌다. 이와 같이 피해를 눈치 채기 어려운 채굴형 악성코드가 지속적으로 유포되어 사용자의 감염을 시도할 것으로 전망하고 있다. 다음으로는 문자메시지나 이메일 속 링크를 이용하여 악성 앱을 감염시키는 모바일 표적 공격이 증가하고 있다. 웹 페이지를 통해 소프트웨어를 다운받을 때, 소프트웨어에 대한 무결성 검증과 배포자에 대한 인증을 제공해주는 것이 코드서명

기술이다.[3] 이러한 유효한 코드서명 인증서에 대해 탈취를 시도하고 이로 서명된 악성코드를 유포·감염시키는 공격이 증가하고 있다.

다섯 번째로, 문서 파일을 위·변조한 스피어피싱, 소프트웨어 자체 보안 기능을 통한 위협 탐지 시스템 회피, 정상 서비스를 활용한 악성코드 통신 기법 활용 등 다양한 지능형 표적 공격이 증가하고 있다. 정상 문서 파일을 위·변조하거나 암호화된 문서 파일을 이용하여 사용자에게 접근하는 방식이 보다 정교화되고 있다. 또한, 모바일 앱이나 스마트폰 제조사를 대상으로 한 소프트웨어 공급망 공격이 확대되고 있다. 이는 소프트웨어의 특정 사용자만을 선별하여 표적으로 하는 악성코드를 유포하여 공격한다. 마지막으로, 스마트시티나 스마트공장 등을 위협하거나 의료 시스템을 해킹하는 등 융합 서비스를 노리는 새로운 보안 위협이 등장할 것으로 예상하고 있다.

3. 보안 대응 방안

이번 장에서는 각 사이버위협에 대한 대응 방안에 대해 살펴보고자 한다. 우선, IoT 결합 서비스와 보안 강화를 위해서는 기관에서 사물인터넷 결합 제품을 도입할 경우, 가급적 기관망과는 별도의 망을 활용할 수 있도록 하여 사물인터넷을 통한 기관의 망에 피해가 발생하지 않도록 하는 것이 가장 중요할 것이다. 또한, Windows7/XP 등의 지원이 중단된 혹은 예정인 운영체제를 통한 취약점이 대두되고 있는 만큼, 해당 운영체제를 업그레이드하여 취약점에 노출되지 않도록 하는 정책 적용이 필요하다.

공공기관·기업을 표적으로 한 랜섬웨어 감염 시, 파일 암호화 및 금전 요구 등의 피해가 발생할 수 있으므로 랜섬웨어가 가장 쉽게 유입될 수 있는 통로인 메일을 통한 감염에 유의해야 한다. 기술적으로 랜섬웨어 차단 솔루션 등을 도입하여 차단하는 것도 필요하겠지만, 무엇보다 의심스러운 메일을 열람하지 않는 등 사용자가 유의하는 것이 가장 필수적이라고 할 수 있다. 이러한 보안 대응 방안은 문자메시지나 이메일을 통한 악성코드 공격 대응 방안에도 동일하게 적용될 수 있을 것이다. 물론 기관에서 업무용 모바일 앱을 활용할 때는 개발 시에 보안 대책을 마련하여 추진하여야 한다.

또한, 가상통화 거래소 관련 해킹 사고를 방지하기 위해서도 악성 프로그램이 설치되지 않도록 기술적 보안대책을 마련하는 것 뿐만 아니라 작년 공공

기관 사례에서는 용역업체 직원에 대한 관리 부족으로 사건이 발생한 만큼 제도적인 측면을 보완하는 것도 중요하다. 다음으로 지능형 지속위협(APT) 공격이 네트워크, 이메일 등 다양한 경로를 통해 증가하고 있는 만큼 유입되는 악성코드에 대해 분석 및 차단할 수 있는 시스템을 통해 근본적인 대응을 할 필요가 있다. 이를 통해 기업 내 사용자 PC들에 대한 감염 여부를 분석하여 외부 위협으로부터의 원 내 전산망에 대한 안전성을 확보할 필요가 있다.

4. 결론

최근 메일 수신자가 관심을 가지는 내용의 제목으로 클릭을 유도하는 피싱 메일이나 특정 집단을 타겟으로 하여 정부기관 등을 사칭하는 해킹 메일 등 다양한 기법을 통해 이러한 해킹 메일이 사용자들에게 유입되고 있다. 이에, 정부에서도 각 기관에서의 피해를 방지하기 위해 SPF·DKIM·DMARC의 기술을 적용할 것을 요구하고 있고, 보안 업체에서도 발전하고 있는 공격 기법에 대응하기 위한 제품들을 출시하고 있다. 본 논문에서는 이러한 사회적인 환경에서 요구하고 있는 보안 기술들의 체계와 기술 문서에 대해 살펴보았다. 보안 기술을 적용하기 위해 해당 기술이 제안되거나 적용되고 있는 문서의 흐름을 파악하는 것은 기술 도입 전 이해를 돕기 위한 발판이 되었으며, 이를 통해 좀 더 폭 넓은 기술적인 이해를 할 수 있을 것이라 기대해본다. 물론 다양한 보안 기술을 적용함으로써 보안을 강화 시키는 것도 중요하지만 무엇보다 중요한 것은 의심되는 메일은 열어보지 않고, 기본적인 보안 수칙을 준수하는 사용자들의 보안 의식이 가장 중요할 것이다.

참고문헌

- [1] 한국인터넷진흥원, “2020년 7대 사이버 공격 전망”, 2019
- [2] 이동혁, 박남제, “IoT 기기의 보안성 확보를 위한 제도적 개선방안”, 한국정보보호학회 논문지 VOL.27, NO.3, 2017
- [3] 이래, 이동훈, “코드 서명 기술의 국내 PKI 적용 방안 비교 연구”, 정보보호학회논문지 14권, 3호, 2014

ARM TrustZone 기반 신뢰실행환경의 취약점과 방어기법에 대한 연구

유준승*, 서지원*, 방인영*, 백윤홍*

*서울대학교 전기정보공학부, 반도체공동연구소

jsyou@sor.snu.ac.kr, jwseo@sor.snu.ac.kr, iybang@sor.snu.ac.kr, ypaek@snu.ac.kr

A Study on Vulnerabilities and Defense Systems of ARM TrustZone-assisted Trusted Execution Environment

Jun-Seung You*, Jiwon Seo*, In-young Bang*, Yunheung Paek*

*Dept. of Electrical and Computer Engineering and Inter-University
Semiconductor Research Center (ISRC),
Seoul National University

요 약

현재 전 세계 수많은 모바일 기기들은 보안에 민감한 애플리케이션들과 운영체제 요소들을 보호하기 위하여 ARM TrustZone 기반 신뢰실행환경 (Trusted Execution Environment) 을 사용한다. 하지만, 신뢰실행환경이 제공하는 높은 보안성에도 불구하고, 이에 대한 성공적인 공격 사례들이 지속적으로 확인되고 있다. 본 논문에서는 이러한 공격들을 가능하게 하는 ARM TrustZone 기반 신뢰실행환경의 취약점들을 소개한다. 이와 더불어 취약점들을 보완하기 위한 다양한 방어 기법 연구에 대해 살펴본다.

1. 서론

신뢰실행환경(Trusted Execution Environment)은 최근 애플리케이션들의 무결성과 기밀성을 보호하기 위한 핵심 보안 기법으로 떠오르고 있다. 해당 기법은 전용 하드웨어를 사용하여 보안에 민감한 애플리케이션들을 시스템의 운영체제로부터 격리된 보호구역에서 실행하는 기능을 제공한다. 다양한 프로세서 제조사들(AMD, ARM, Intel, IBM 등)이 신뢰실행환경 기능을 제공하는 가운데, 모바일 및 IoT 시장에서 가장 많이 사용되는 ARM 프로세서의 ARM TrustZone[1] 기술이 모바일 기기들에 신뢰실행환경을 제공하기 위해 활발히 도입되고 있다.

ARM TrustZone 기반 신뢰실행환경이 제공하는 높은 보안 수준에 힘입어 해당 기술은 사용자 인증, 온라인 뱅킹 등 보안에 민감한 다양한 애플리케이션들을 보호하기 위해 채택되었다. 안타깝게도, ARM TrustZone 기반 보안 시스템들에 대한 성공적인 공격 사례들은 지난 몇 년 동안 지속해서 발견되고 있다. 이러한 공격들은 ARM TrustZone 기반 시스템들이 지니는 취약점들(신뢰실행환경의 큰 코드 베이스, 격리된 보호구역의 관리 방법 등)에 기인한다.

본 논문에서는 ARM TrustZone 기반 신뢰실행환경이 지니는 취약점들을 분석한다. 이와 함께 취약점들을 해결하기 위해 사용되고 있는 방어 기법들을 살펴본다.

2. 배경이론

2.1 신뢰실행환경과 ARM TrustZone

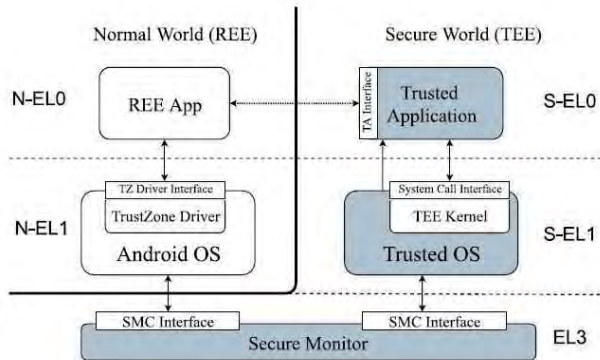
신뢰실행환경은 본래 기존 운영체제를 통하는 민감한 데이터를 격리된 환경에서 처리한다. 즉, 신뢰실행환경은 TA(Trusted Application)라고 불리는 프로그램들의 안전한 실행 보장을 목표로 한다. 신뢰실행환경은 하드웨어 기술을 기반으로 하며, 해당 기술 중 하나인 ARM TrustZone은 2004년부터[2] ARM Cortex-A 프로세서들에 제공되었으며, 최근 Cortex-M[3] 프로세서들에 제공을 위해 재개발되었다.

TrustZone은 ‘secure world(SW)’와 ‘normal world(NW)’라는 두 구역으로 운영된다. 각 물리적 프로세서는 하드웨어를 통해 구역별로 가상 프로세서를 할당하고 다른 구역으로의 안전한 전환을 가능케 한다. 시스템의 상태는 프로세서의 NS 비트를

통해 어느 구역에 있는지 확인되며, SW에 있는 자원들은 NW에서 접근할 수 없다.

2.2 ARM TrustZone의 소프트웨어 구조

ARM TrustZone의 기본적인 소프트웨어 구조는 그림1과 같다. 앞서 언급되었듯이 기본적으로 두



(그림 1) ARM TrustZone의 소프트웨어 구조

구역(normal world와 secure world)으로 운영되며, 각 구역은 3가지 실행 레벨(Execution Level; EL)을 가진다. 실행 레벨이 높을수록 구역에서 더 높은 권한을 가지며, 보통 EL0에서 애플리케이션들이 실행되며, EL1에서는 해당 구역의 운영체제가 실행된다. Secure world의 운영체제는 해당 구역에서 애플리케이션이 실행되기 위한 기본적인 기능들뿐만 아니라 암호 라이브러리, 신뢰 I/O 등의 신뢰실행환경 동작에 필요한 기능들을 제공한다. 가장 높은 실행 레벨인 EL3에는 secure monitor이라 불리는 소프트웨어가 존재하여 두 구역 간의 안전한 전환을 제공하며, 이는 SMC(Secure Monitor Call) 명령어를 통해 두 구역에서 접근할 수 있다. Secure world의 운영체제와 secure monitor를 합쳐 신뢰실행환경 시스템의 TCB(Trusted Computing Base)라 일컫는다.

3. ARM TrustZone 기반 신뢰실행환경 취약점들

3.1 신뢰실행환경 공격 반경

신뢰실행환경은 기본적으로 작은 TCB를 가정한다. 다시 말해 격리된 보호구역에서 작동하는 요소들을 최대한 줄이고자 한다. 격리된 구역(secure world)에 많은 요소가 들어갈수록 해당 구역 내에서 작동하는 애플리케이션들이 공격할 수 있는 부분들이 증가할 뿐만 아니라, 다른 구역(normal world)에서 격리된 구역으로 접근할 통로들도 증가하기 때문이다. 하지만 현재 ARM TrustZone 기반 신뢰실행환경 시스템들은 너무 큰 TCB를 지닌다. 즉,

secure world에서 작동하는 애플리케이션들 및 운영체제의 크기가 공격하기에 충분하다. 이는 다양한 ARM TrustZone 기반 신뢰실행환경 시스템들의 크기와 시스템에서 발견된 취약점들의 개수(표1)를 통해 확인할 수 있다.

<표 1> 다양한 신뢰실행환경 크기 및 취약점 개수

신뢰실행환경	바이너리	CVE
Qualcomm TEE	1.61 MB	92
Trustonic TEE	350 KB	5
Huawei TEE	744 KB	3
Nvidia TEE	97 KB	10
Linaro TEE	365 KB	3

3.2 Secure, normal world 간의 격리

신뢰실행환경은 SW와 NW 사이를 강력하게 격리함과 동시에 두 구역 사이의 안전한 통신을 제공해야 한다. 하지만 격리 체계는 secure world에서의 시스템 콜 등에 의해서 우회될 수 있다. 문제는 SW에서 실행되는 애플리케이션들이 NW의 물리 메모리를 변조시킬 수 있다는 점이다. 즉, 두 구역 간의 통신을 위해 공유 메모리가 있을 때, SW에서 실행되는 프로그램이 NW의 프로그램보다 더 높은 권한을 지니고 공유 메모리를 변조시킬 수 있다. 예를 들어, Qualcomm TEE에서는 SW에서 실행되는 프로그램이 특정 시스템 콜을 사용하여 NW의 OS 커널이 관리하는 물리 메모리 할당을 허용한다. 그뿐만 아니라 신뢰실행환경 디버깅 메커니즘의 허점을 통해 두 구역 간의 격리가 우회될 수 있다. 디버깅 과정에서 나오는 중요 정보들(스택 트레이스, 로그 등)이 NW의 메모리로 전달되어 시스템 관련 중요 정보들이 취약해진다.

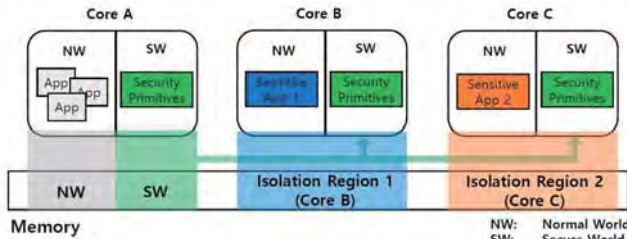
3.3 메모리 보호 메커니즘

많은 신뢰실행환경 시스템들은 취약한 메모리 보호 메커니즘을 지니고 있거나, 아예 보호 장치가 없다. 대표적으로 기본적인 메모리 보호 기법인 ASLR(Address Space Layout Randomization)은 많은 신뢰실행환경 시스템에 제대로 구현되어 있지 않다. 이와 더불어 스택 쿠키나 guard pages 등의 추가적인 메모리 보호 기법들 또한 구현되어 있지 않다.

4. ARM TrustZone 기반 신뢰실행환경 보호기법

4.1 다중 격리 환경

3.1에서 분석한 신뢰실행환경의 넓은 공격 반경에 의한 취약점의 근본적인 문제점은 하나의 구역(security world)에 너무 많은 애플리케이션 및 신뢰실행환경 구성 요소들이 밀집되어 있다는 점이다. 이를 해결하기 위한 보호 기법은 그림2처럼 현재 하나의 거대한 구역으로 운영되고 있는 격리 보호 구역을 나누어 다중 격리 환경으로 운영한다. 즉,



(그림 2) 다중 격리 환경의 기본적인 구조

여러 개의 애플리케이션과 운영체제가 한 구역에서 같이 실행되지 않고, 애플리케이션별로 서로 다른 격리 보호구역에서 실행된다. SANCTUARY[4]는 ARM TrustZone이 제공하는 TZASC(TrustZone Address Space Controller)를 사용하여 다중 격리 환경을 구현하며, vTZ[5]는 잘 사용되지 않는 실행 레벨(EL2)과 하드웨어 가상화 기법을 사용하여 이를 구현한다.

4.2 구역 간 안전한 통신 채널 및 격리

3.2에서 소개한 두 구역(security, normal world)간의 격리 우회는 근본적으로 두 구역간의 통신 채널의 허점에 기인한다. 즉, NW에서 SW의 메모리에 접근할 때 충분한 인증 작업이 이루어지지 않고, 두 구역간의 메모리 공유 메커니즘이 불안전하다. 이러한 두 구역 간의 통신 취약점은 normal world에 있는 애플리케이션과 secure world에 있는 애플리케이션이 통신할 때마다 세션 키를 사용하여 보호할 수 있다. 즉, 특정 애플리케이션들만 알고 있는 키를 사용하여 상호 통신을 암호화하여 외부 공격을 방어한다. 또 다른 방어 기법은 구역 간 통신을 공유 메모리 없이, 즉 데이터 복사로, 구현한다.

4.3 암호화된 메모리

3.3에서 소개한 메모리 보호 기법의 부재는 기본적으로 기존의 보호 기법을 구현하여 해결할 수 있다. 메모리 보호 기법이 오작동하기보다는 구현이 되어있지 않기 때문이다. 하지만 이와 함께 추가로 구현할 수 있는 방어 기법도 있다. 해당 기법은 secure world에서 보호되고 있는 데이터를 암호화한

다. 이는 이미 다른 신뢰실행환경 기술 (Intel SGX)에서 구현되어 있지만, ARM TrustZone에서는 제공되지 않는 기능이다. Secure world에 있는 데이터를 모두 암호화하여 보관하고, 데이터를 처리할 때만 격리 보호구역 안에서 해독하면 normal world에서 secure world의 메모리에 접근할 수 있더라도 데이터들은 안전하다.

5. 추가 취약점들 및 보안 강화 방안

앞서 분석한 ARM TrustZone 기반 신뢰실행환경의 취약점들은 가장 대표적인 약점들 및 방어 기법들이며, 다른 취약점들도 존재한다. 대표적으로는 부채널 공격으로부터의 취약점들이다. 해당 취약점들은 근본적으로 하드웨어 설계 자체의 문제인 경우가 많아 큰 비중을 두고 다루지 않았지만, 캐시나 분기 예측기, DRAM을 이용한 부채널 공격들[6-8]이 존재한다. 이를 방어하기 위해서 하드웨어 명령어를 추가하거나 캐시를 빈번하게 플러시하는 방어 기법들이 존재하지만, 최적화되어 설계된 하드웨어를 변형시키기 때문에 감수해야 하는 오버헤드가 크다.

이와 더불어 ARM TrustZone이 제공하지 않는 신뢰실행환경 기능들에 의한 취약점들이 존재한다. 예를 들면, 앞서 언급한 데이터 암호화 기능이나 원격 증명(remote attestation) 기능의 부재가 있다. 원격 증명이란 원격 신뢰실행환경끼리 상호 간의 신뢰를 형성하는 메커니즘인데, Intel SGX는 제공하지만, ARM TrustZone은 제공하지 않는 기능이다. 즉, 원격에 있는 ARM TrustZone 기반 신뢰실행환경은 상대방도 신뢰실행환경이라고 착각하고 민감한 데이터들을 통신할 수 있다. 이를 방어하기 위해서는 ARM 프로세서의 고유 키나 특성을 가지고 상호 인증할 수 있는 메커니즘을 고안해야 할 것이다.

6. 결론

본 논문에서는 ARM TrustZone 기반 신뢰실행환경이 지니는 취약점들을 분석하고, 이에 대한 방어 기법들을 살펴보았다. ARM TrustZone의 통합적 격리 메커니즘으로 인한 공격 반경 증가, 격리 보호구역과 일반 구역간의 안전한 통신 메커니즘 부재, 그리고 메모리 보호 기법 부재로 인한 취약점들이 존재한다. 이를 방어하기 위해 다중 격리 환경, 세션 키를 활용한 안전한 통신 메커니즘, 메모리 암호화 등의 방어 기법을 사용한다. 많은 취약점에 대한 방

어 기법이 존재하지만, 하드웨어 부채널 공격이나 제공되지 않는 신뢰실행환경 기능으로 인한 취약점들은 아직 ARM TrustZone 기반 신뢰실행환경에 위협적이다. 이를 위해 오버헤드를 줄여 실용적인 방어 기법 연구 및 제공되지 않는 신뢰실행환경 구현 연구가 계속되어야 할 것이다.

7. ACKNOWLEDGEMENT

본 연구는 2020년도 정부(과학기술정보통신부)의 재원으로 한국연구재단 (NRF-2017R1A2A1A17069478), 2020년도 두뇌한국21플러스사업, 2020년도 정부 과학기술정보통신부의 재원으로 정보통신기술진흥센터 (No.2017-0-00213, 능동적 사전보안을 위한 사이버 자

Shadowing,” in 26th USENIX Security Symposium (USENIX Security 17). Vancouver, BC: USENIX Association, 2017, pp. 557 - 574.

[8] V. van der Veen, Y. Fratantonio, M. Lindorfer, D. Gruss, C. Maurice, G. Vigna, H. Bos, K. Razavi, and C. Giuffrida, “Drammer: Deterministic Rowhammer Attacks on Mobile Platforms,” in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York, NY, USA: ACM, 2016, pp. 1675 - 1689.

참고문헌

- [1] Arm, “ARM Security Technology. Building a Secure System using TrustZone Technology ARM,” Arm whitepaper, p. 108, 2009.
- [2] T. Alves and D. Felton, “TrustZone: Integrated Hardware and Software Security,” Tech. In-Depth, vol. 3, no. 4, pp. 18 - 24, 2004.
- [3] S. Pinto, H. Araújo, D. Oliveira, J. Martins, and A. Tavares, “Virtualization on TrustZone-enabled Microcontrollers? Voilà!” in 25th IEEE Real-Time and Embedded Technology and Applications Symposium, Montreal, Canada, 2019.
- [4] F. Brasser, D. Gens, P. Jauernig, A.-R. Sadeghi, and E. Stäpf, “SANCTUARY: ARMing TrustZone with Userspace Enclaves,” in Network and Distributed Systems Security (NDSS) Symposium, 2019.
- [5] Z. Hua, J. Gu, Y. Xia, H. Chen, B. Zang, and H. Guan, “vTZ: Virtualizing ARM TrustZone,” in USENIX Security Symposium. Vancouver, BC. 2017, pp. 541 - 556.
- [6] M. Lipp, D. Gruss, R. Spreitzer, C. Maurice, and S. Mangard, “ARMageddon: Cache Attacks on Mobile Devices,” in USENIX Conference on Security Symposium. Denver: 2016, pp. 549 - 564.
- [7] S. Lee, M.-W. Shih, P. Gera, T. Kim, H. Kim, and M. Peinado, “Inferring Fine-grained Control Flow Inside SGX Enclaves with Branch

클라우드 컴퓨팅 환경에서의 동형암호기술 적용에 대한 연구

장지원*, 남기빈*, 조명현*, 백윤홍*

*서울대학교 전기·정보공학부, 반도체공동연구소

jwchang@sor.snu.ac.kr, kvnam@sor.snu.ac.kr, mhcho@sor.snu.ac.kr, ypaek@snu.ac.kr

A Study on the Applying Fully Homomorphic Encryption in the Cloud Computing Environment

Jiwon Chang*, Kevin Nam*, Myunghyun Cho*, and Yunheung Paek*

*Dept. of Electrical and Computer Engineering and Inter-University Semiconductor Research Center (ISRC),

Seoul National University

요 약

클라우드가 보편적으로 활용되면서 클라우드 서버에 정보를 저장하거나 연산을 하는 일은 일상이 되었다. 그러나, 이러한 클라우드 컴퓨팅 서비스가 급격히 증가하면서, 개인정보보호와 데이터 보안성, 기밀성 및 시스템의 안정성에 대한 우려가 높아지고 있다. 클라우드는 데이터를 위탁받아 연산하는 과정에서 사용자들의 개인정보를 유출시킬 수 있는 문제점이 있다. 이러한 문제점을 해결하기 위한 방법 중 현재 가장 각광받고 있는 해결책은 바로 동형암호기술이다. 동형암호는 이전 암호체계와 다르게 사용자의 암호화된 데이터를 복호화하지 않고서도 연산할 수 있어서, 이를 이용하게 되면 사용자 데이터의 기밀성을 보장하면서도 원하는 결과를 얻을 수 있다. 그러나, 동형암호를 클라우드 컴퓨팅 환경에 적용하는데 가장 큰 장애물은 바로 연산 오버헤드가 대단히 크다는 점이다. 본 연구에서는 최신 동형암호 기술을 소개하고 연산속도를 증가시키기 위한 솔루션들에 대해 알아보하고자 한다.

I. 서론

4차 산업 혁명 시대를 맞이하며 인공지능, IoT, 빅데이터, 클라우드는 현대 컴퓨팅 환경에서의 대표적인 연산 주체이자 객체가 되어가고 있다. 이들은 데이터의 활용 및 분석을 통해 여러 응용 분야에 적용되고 있다. 최근 급부상하고 있는 엣지 컴퓨팅과도 연관이 있는데, 이러한 컴퓨팅 환경이 이루어지기 위해서는 원격 연산 기술이 필요하다. 빅데이터를 관리하기 위해 데이터 센터를 가진 많은 기업들은 데이터 센터에 수집된 빅데이터와 개인으로부터 제공받은 데이터를 기반으로 클라우드와 엣지 노드들을 통해 사용자들에게 편리한 서비스를 제공하고

있다. 이러한 빅데이터 시대에는 수많은 데이터들이 이곳저곳을 오가며 처리되고 있다. 때문에, 계속해서 더 많은 기업들이 클라우드 컴퓨팅 환경을 통해 고객의 데이터를 수집하여 서비스를 제공하려 할 것이다. 클라우드 컴퓨팅 환경은 원격으로 연산이 이루어져 개인이 처리할 수 있는 데이터양보다 훨씬 더 많은 방대한 양의 데이터를 효율적이고 경제적으로 처리할 수 있다.

그러나, 클라우드 컴퓨팅 환경은 여러 문제점 [1]을 지니고 있는데, 개인정보와 같은 민감한 데이터에 대한 보안성이 취약하다는 가장 큰 문제를 갖고 있다. 대량의 데이터 수집 및 처리

과정이 클라우드 내에서 이루어지기 위해서 사용자로부터 전달받은 데이터를 암호화하지 않은 상태에서 연산을 수행해야 한다, 이러한 과정에서 클라우드 내의 민감한 데이터의 변조 및 유출 위험성은 상시 존재한다. 즉, 내부자 위협(Insider Threat)이나 부채널 공격(Side-channel Attack)에 취약한 클라우드 컴퓨팅 환경을 사용자들이 직접 통제하거나 감시할 수 없기 때문에, 클라우드 서비스를 전적으로 믿어야 한다. 이러한 상황이 계속해서 증가하므로, 최근 EU에서는 GDPR(General Data Protection Regulation), 미국 캘리포니아 주에서는 CCPA(California Consumer Privacy Act) 소비자 프라이버시 보호법을 제정하는 등 국제적으로 개인정보보호에 대한 관심이 증대되고 있는 추세이다.

이러한 추세에 발맞추어 안전한 클라우드 컴퓨팅 환경을 제공하기 위한 많은 연구가 이루어지고 있다. 현재 가장 많이 적용되는 기술은 바로 Intel과 ARM에서 사용하고 있는 신뢰실행환경(Trusted Execution Environment) 기술이다. 가장 대표적인 예로, Intel 6세대 프로세서인 ‘스카이레이크’에서부터 포함된 Intel SGX는 Enclave 라는 격리된 신뢰실행환경을 하드웨어적으로 제공하여 소프트웨어적으로 구축된 보안 기법보다 더 강력한 보호 환경을 제공한다. 하지만, Intel SGX가 캐시 부채널 공격에 취약하다[2]는 연구결과가 발표되었다.

부채널 공격뿐만 아니라 내부자 위협에도 데이터의 안정성을 보장하는 기술은 바로 차세대 암호체계인 동형암호(Homomorphic Encryption) 기술이다. 동형암호는 데이터를 암호화한 상태에서도 복호화 없이 연산이 가능 암호기술로 양자컴퓨터 시대에도 안전한 암호 기술이다.

동형암호는 클라우드 서비스에 대한 어떠한 신뢰 가정 없이 데이터 보안을 보장한다. 클라우드 서비스는 단순히 계산능력만 사용자들에게 제공하고 데이터에 대한 정보는 암호화되어 있어 알 수 없다. 때문에, 동형암호는 프라이버시를 보장하는 클라우드의 솔루션으로 적용하

기에 가장 적합한 기술이다. 예를 들어, MLaaS(Machine Learning as a Service)에서 동형암호 기술은 Oblivious 뉴럴 네트워크 추론에 적용될 수 있다. 사용자들은 개인의 데이터를 암호화하여 클라우드로 전송하고, 클라우드 서버에서는 암호화된 데이터들을 암호화된 채로 머신러닝 모델을 이용한 연산을 통해 결과값을 다시 사용자들에게 보내준다. 이때 모든 중간 및 최종 결과에 대한 데이터 값들은 암호화되어있고 오직 비밀키를 가지고 있는 사용자에 의해서만 복호화될 수 있다.

하지만, 동형암호기술을 실제 클라우드 컴퓨팅에 상용화하기에는 아직 연산속도가 일반연산보다 50만배 이상 느리다는 문제점이 존재한다. 현재 이러한 동형암호의 연산 오버헤드를 줄이기 위해, Software 최적화, Hardware를 이용한 연산 가속, 새로운 scheme 제시 등 많은 연구가 이루어지고 있다.

본 연구에서는 동형암호에 대한 기본적인 설명과 연산속도를 빠르게 하기 위한 연구들을 소개하며 향후 연구 방향을 제시하고자 한다.

II. 동형암호기술 소개

기존 암호화 기술은 데이터가 암호화된 상태에서 연산, 탐색, 분석 등의 작업이 불가능하였다. 반면에, 1978년 Rivest, Adleman and Dertouzos[3]에 의해 처음 제안된 동형암호는 암호화된 상태에서도 데이터의 연산이 가능하여 이상적인 암호 기술로 인식되었으나, 안전성 문제를 해결하지 못한 채 30여 년간 미제로 남아있었다. 2009년 Gentry[4]가 암호문에 대한 임의의 연산이 가능하고 안전성을 보장하는 동형암호가 제안되었고, 이를 토대로 많은 연구가 발전되고 있다.

Gentry가 제안한 동형암호는 암호문에 대해 제한된 횟수의 연산만을 수행할 수 있었는데, 이는 암호문에 대한 연산이 수행된 후 암호문 안에 존재하는 노이즈(noise)가 커져 일정 노이즈 임계치를 넘게 되면 암호문을 평균으로 복호화가 불가능해지기 때문이다. 이를 제한동형암호(SHE, Somewhat Homomorphic

Encryption)라고 부른다. 이와 달리, 무제한으로 암호문에 대한 임의의 연산이 가능한 암호를 완전동형암호(FHE, Fully Homomorphic Encryption)라 부른다. 완전동형암호는 연산이 수행된 후 암호문에 대한 노이즈를 줄이는 재부팅(Bootstrapping) 과정을 통해 무한히 암호문에 대한 연산을 노이즈 임계치를 넘지 않으면서 수행한다.

이러한 완전동형암호를 바탕으로 발전된 여러 방안(Scheme) 중 가장 대표적인 3가지 방안은 BGV[5], BFV[6], CKKS(HEAAN)[7]이다. 이들의 가장 큰 차이점은 연산 가능한 수의 범위이다. BGV와 BFV 방안은 오직 정수에 대한 동형암호연산이 가능하기에 많은 제약이 존재한다. 이러한 제약에서 벗어날 수 있도록, 2017년 실수에 대한 동형암호연산이 가능한 CKKS 방안이 우리나라에서 최초로 제안되었다. 이전까지는 많은 동형암호 라이브러리들이 주로 BFV 방안을 활용하여 개발되었는데, CKKS의 등장 이후로 CKKS 방안을 채택한 라이브러리들이 다수 등장하고 있으며, 많은 연구진들이 CKKS 방안을 활용한 연구를 진행 중이다. 대표적인 예로 Microsoft Research에서 개발 중인 SEAL[8] 동형암호 라이브러리는 최근에 CKKS 방안을 주로 제공하며 BFV 방안 같은 경우는 선택적으로 사용할 수 있도록 제공하고 있다.

앞서 소개한 것과 같이, 완전동형암호는 여러 연구를 통해 많은 성능향상을 일궈냈다. 하지만, 여전히 소프트웨어로만 구현한 동형암호는 실용화하기에 연산속도가 너무 느리다. 이 때문에 최근에는 하드웨어를 도입하여 동형암호의 연산 오버헤드를 감소시키기 위한 많은 연구가 진행되고 있다.

III. 하드웨어 기반 동형암호 가속기

동형암호기술이 많은 발전을 이뤘음에도 불구하고 여전히 연산 오버헤드가 상당하다. 소프트웨어 구현만으로는 한계가 존재하기 때문에, 최근 많은 연구진들은 GPU나 FPGA와 같은 하드웨어를 사용하여 동형암호의 연산속도를 몇 백배 이상 줄일 수 있었다. 하드웨어 가속기는

병렬처리에 강하며 에너지 효율성이 높기 때문에 이와 같은 성능 개선을 이뤄낼 수 있었다. 하지만, 대부분의 연구들은 시뮬레이션을 통한 결과들뿐이다. 실제 하드웨어를 구현한 연구는 추가적인 블록을 설계한다거나 코어들의 동기화를 고려해야 하는 등 굉장히 복잡하고 도전적인 작업이 필요하다.

Operation type	Message	Ciphertext	Slowdown
Addition	2.1 ns	348.2 ns	168.2×
Multiplication	4.3 ns	155883.8 ns	36112.7×

<표 1> 동형암호 연산 속도 비교[9]

<표 1>에서 볼 수 있듯이, 동형암호연산에서 가장 오래 걸리는 연산은 암호문 간의 곱셈 연산이다. 그래서 대부분의 연구진들은 이 동형암호 곱셈 연산을 가속화 하는 방안을 연구하고 있다. 가장 대표적인 3가지 예를 확인해보면, 먼저 2019년 발표된 [10]에서는 FPGA를 활용하여 동형암호 곱셈 연산을 블록 단위의 파이프라이닝과 병렬처리를 통해 가속화 하였다. 하지만, BFV 방안을 사용하여 실수에 대한 연산이 어려우며, 하나의 고정된 동형암호 파라미터에 대한 연구로 확장성이 부족하다.

반면, 2020년 Microsoft Research에서 발표한 [11]에서는 CKKS 방안을 채택하여 실수에 대한 연산이 가능하며, FPGA를 활용해 이전보다 많은 단계의 파이프라이닝과 모듈화를 통해 동형암호 곱셈 연산을 가속화 하였으며, 뿐만 아니라, 여러 동형암호 파라미터 세트를 제공하여 이전 연구보다 더 높은 병렬성과 확장성을 보였다.

마지막으로 [12] 연구에서는 GPU를 활용하여 동형암호기술을 뉴럴 네트워크 연산에 적용하여 가속화 하였다. 이 연구에서는 BFV 방안의 동형암호를 적용한 합성곱(CNN) 연산을 통해 MNIST 데이터 집합과 CIFAR-10 데이터 집합을 높은 성능으로 분류해내었다. MNIST의 경우 99%의 높은 정확도를 보이지만, CIFAR-10의 경우 77.55%의 낮은 정확도를 보여 앞으로 더 많은 연구가 필요하다.

IV. 결론

본 논문에서는 동형암호에 대한 기본적인 개념과 클라우드 컴퓨팅 환경에 적용되기 위한 여러 가지 연구에 대하여 알아보았다. 차세대 암호체계인 동형암호에 관한 연구는 앞으로도 많은 연구가 필요한 분야이며, 뉴럴 네트워크 연산을 포함하면서 하드웨어 가속기를 이용하는 연구가 향후 이어질 것으로 본다.

V. ACKNOWLEDGEMENT

이 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구(NRF-2017R1A2A1A17069478)이며, 2020년도 두뇌한국21플러스사업에 의하여 지원되었음. 또한, 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2018-0-00230, (IoT 총괄/1세부) IoT 디바이스 자율 신뢰보장 기술 및 글로벌 표준기반 IoT 통합보안 오픈 플랫폼 기술개발 [TrusThingz 프로젝트]).

[참고문헌]

- [1] T. Dillon, C. Wu, and E. Chang, "Cloud Computing: Issues and Challenges," in IEEE International Conference on Advanced Information Networking and Applications, 2010.
- [2] O. Oleksenko, B. Trach, R. Krahn, M. Silberstein, and C. Fetzer. Varys: Protecting SGX enclaves from practical side-channel attacks. In 2018 USENIX Annual Technical Conference (USENIX ATC), 2018.
- [3] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On Data Banks and Privacy Homomorphisms," Foundations of Secure Computation, vol. 4, no. 11, 1978.
- [4] C. Gentry, "Fully homomorphic encryption using ideal lattices," in Proceedings of the 41st ACM Symposium on Theory of Computing (STOC 2009), pp. 169 - 178, 2009.
- [5] Z. Brakerski, C. Gentry, and V. Vaikuntanathan. "Fully homomorphic encryption without bootstrapping." In Innovations in Theoretical Computer Science (ITCS'12), 2012
- [6] J. Fan and F. Vercauteren, "Somewhat Practical Fully Homomorphic Encryption," The International Association for Cryptologic Research Cryptology ePrint Archive, vol. 2012, 2012
- [7] J. Cheon, A. Kim, M. Kim, and Y. Song, "Homomorphic Encryption for Arithmetic of Approximate Numbers," in International Conference on the Theory and Application of Cryptology and Information Security, 2017
- [8] SEAL 2020. Microsoft SEAL (release 3.5.0). <https://github.com/Microsoft/SEAL>. Microsoft Research, Redmond, WA.
- [9] W. Jung, E. Lee, S. Kim, K. Lee, N. Kim, C. Min, J. Cheon and J. Ahn, "HEAAN Demystified: Accelerating Fully Homomorphic Encryption Through Architecture-centric Analysis and Optimization," arXiv:2003.04510, 2020
- [10] S. S. Roy, F. Turan, K. Jarvinen, F. Vercauteren, and I. Verbauwhede, "FPGA-Based High-Performance Parallel Architecture for Homomorphic Computing on Encrypted Data," in IEEE International Symposium on High Performance Computer Architecture (HPCA), 2019.
- [11] M. S. Riazi, K. Laine, B. Pelton, and W. Dai, "HEAX: HighPerformance Architecture for Computation on Homomorphically Encrypted Data in the Cloud," arXiv:1909.09731, 2019
- [12] A. A. Badawi, J. Chao, J. Lin, C. F. Mun, S. J. Jie, B. H. M. Tan, X. Nan, K. M. M. Aung, and V. R. Chandrasekhar, "The AlexNet moment for homomorphic encryption: HCNN, the first homomorphic CNN on encrypted data with GPUs," arXiv:1811.00778, 2018.

부분적 동형암호 HW 가속기 설계에 관한 연구

남기빈*, 장지원*, 조명현*, 방인영*, 백윤희*

*서울대학교 전기정보공학부, 반도체공동연구소

{kvnam, jwchang, mhcho, iybang}@sor.snu.ac.kr, ypaek@snu.ac.kr

Partially Homomorphic Encryption HW accelerator

Kevin Nam*, Jiwon Chang*, Myunghyun Cho*, Inyoung Bang*,
and Yunheung Paek*

*Dept. of Electrical and Computer Engineering and Inter-University
Semiconductor Research Center(ISRC), Seoul National University

요 약

최근 동형암호에 대한 관심이 높아진 가운데, 이를 활용한 Cloud Computing 서비스를 구축하기 위한 시도가 이어지고 있다. 기존 동형암호 HW에 대한 연구는 수학적 기능 구현 자체에 중점을 두고 있다. 본 논문에서는 동형암호 CNN inference 모델 설계 과정에서 HW 구현 한계점과 bottleneck들을 수학적 기법이 아닌 HW 특징을 이용해서 극복하는 과정을 서술하였다.

FHE와 그 이전 형태들을 비교하고, 대표적인 최신 scheme들을 간단히 비교하여 설명할 것이다.

1. 서론

동형암호는 암호화 전 연산과 암호화한 상태에서의 연산 결과가 복호화할 시 같다는 특징을 지니고 있다. 사용자는 암호화한 데이터를 서버에 전송하여 처리하여 돌려받아, 본인이 복호화하여 값을 확인할 수 있어, 차세대 Cloud Computing Interface의 주요 feature로 주목받고 있다. 이에 최근 FPGA와 GPU를 이용한 동형암호 가속기를 구현하고자 하는 시도가 이어지고 있으나, 수학적 기능 구현에 중점을 두어 구현되어 과도한 resource 사용으로 인한 timing 문제, 지나친 bottleneck의 한계로 성능 제한을 받고 있다.

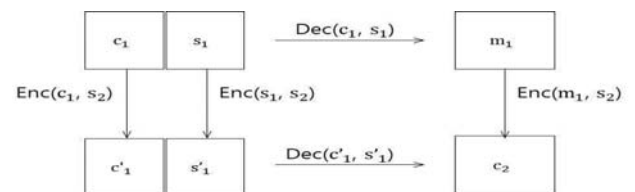
본 연구는 수학적 분석 없이 주어진 동형암호 체계를 부분적으로만 활용하여 데이터 이동, resource, configurability와 같은 HW 특징에 중점을 두고 원하는 기능에 맞게 더 좋은 성능의 HW 체계를 구현하였다. 본 논문은 그 과정에서 이루어지는 선택과 정들에 관해 서술하여 가이드라인을 제공하고자 한다.

2. 동형암호의 분류

동형암호 개념이 등장한 것은 1997년이지만[1] 실제 구현 가능한 동형암호는 2009년 Gentry의 BFV scheme을 통해 소개되었다[2]. 본 장에서는

2.1 Somewhat/Fully Homomorphic Encryption

곱셈이 이루어지면, 암호문에 noise bits가 증가하게 된다. 이에 허용 최대 수를 벗어나면, overflow가 발생하여 가용하지 않은 상태가 된다. 이러한 이유로 Somewhat이라는 단어가 붙어 SHE라고 부른다. SHE의 한계를 극복한 FHE는 noise bits를 줄이는 bootstrap이라는 방법과 함께 등장했다. (그림 1)에 나타나듯, m_1 을 암호화한 암호문 c_1 과 s_1 을 새로운 암호키 s_2 을 통해 각각 암호화한 값들을 c'_1 과 s'_1 이라 하자. c'_1 을 s'_1 을 통해 복호화한 문장은, m_1 을 s_2 를 통해 암호화한 새로운 암호문 c_2 가 된다. 즉, 암호문을 새로운 암호키를 이용하여 새로운 암호문으로 전환하면서, 아직 어느 곱셈도 하지 않은 상태의 새로운 암호문이 되는 것이다.



(그림 1) Bootstrap procedure

2.2 BGV, BFV, CKKS

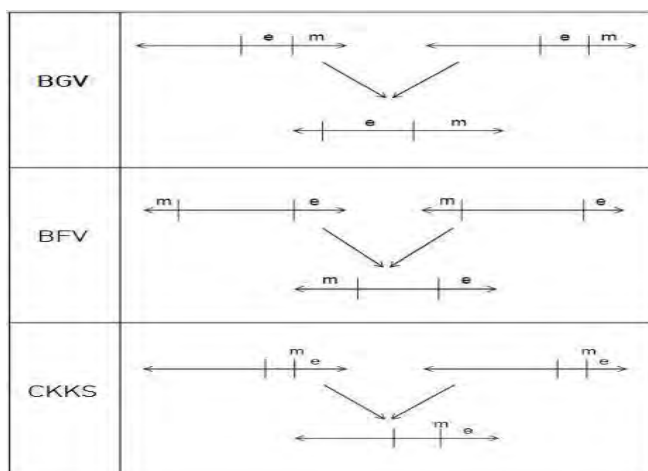
같은 원리를 통해 다양한 scheme들이 등장한 가운데, 가장 자주 언급되고 연구되는 세 가지 scheme들이 있다. 각각 BGV[3], BFV[4], CKKS[5]라 불리며, 이들에 대해서 필요한 부분들을 간단히 정리해서 서술하면 다음과 같다.

BGV scheme은 $ct = Enc_{sk}(m) = (a, as + te + m)$ 의 꼴을 통해 암호화가 이루어진다. (그림 2)에 나타나듯, 문장의 상위비트에 noise를 추가하여 연산이 이루어진다. 곱셈이 이루어질 때마다 noise가 곱해지며 점점 증가하기 때문에, 이를 줄이는 방법이 필요하였기에 modulus switching이라는 기법을 도입하였으나, modulus가 줄어든다는 단점을 지니고 있다.

BFV scheme의 경우 LSB에 noise를, MSB에 문장을 넣어 암호화를 진행한다.

$ct = Enc_{st}(m) = (a, as + e + \frac{q}{t}m)$ 의 꼴을 따라 진행되는데 이 경우 scale-invariant하여 noise를 줄이는 과정 진행시 modulus가 줄지 않는다는 장점을 지니고 있었다. 그럼에도 noise자체는 점점 증가하여 최대 비트 수를 넘길 수 없기에, FHE를 이루기 위해서는 재부팅이 불가피하다.

CKKS는 approximate 형태로 실수를 표현가능한 scheme이다. Noise를 추가로 첨가하는 이전 scheme들과 다르게, 실수 중 오차 허용 범위를 벗어난 값들을 noise로 추가하는 형태로 연산을 진행한다. CKKS의 경우도 마찬가지로 noise와 문장의 길이가 곱할수록 커지는데, 이 오차 허용 범위를 동일하게 하기 위해 rescaling을 활용한다.



(그림 2) BGV, BFV, CKKS

이러한 scheme들을 통해 FHE 구현을 실현할 수

있는 library들이 존재한다. 이후 서술될 내용은 MS의 SEAL[6]을 활용하여 실험하였다.

3. 동형암호 HW 체계 한계점

이러한 동형암호 체계를 실용화하기 위한 단계로써 HW 가속기 설계에 관한 연구가 최근 많이 진행되고 있다. BFV scheme을 활용한 연구[7]와 CKKS를 활용한 HEAX[8]가 full module을 구현한 사례이며, 이 외에도 맞춤형 SHE 체계를 구현한 연구들이 진행됐다. 이러한 연구들은 최고 성능의 FPGA와 GPU를 활용하였음에도 불완전하다는 한계점을 지니고 있는데, 그러한 이유에 관해서 서술하겠다.

3.1 Bootstrapping(rescaling) Complexity

위에서 언급된 재부팅 과정을 다시 살펴보면, 원래 크기의 암호문으로 변경하는 기능을 이루었지만, 이를 해독하기 위해서는 두 번의 해독과정이 필요하다. 즉 재부팅이 이루어질수록 해독과정이 복잡해진다. 이 과정은 FHE 연산 과정에 있어 매우 큰 bottleneck이 되고 있다. 이를 해소하기 위해 재부팅이 필요한 상태를 예측하여 buffer에 미리 추가, 시간을 단축하고자 하는 시도 등이 있었지만, 아직 충분히 해소되지 않았다.

이에 SHE지만 필요한 기능은 수행할 수 있는, 즉 구현하고자 하는 기능이 요구하는 multiplicative depth를 만족하는 SHE 체계를 구현하기 위한 시도가 있었으며, 이들 시도는 re-scalability를 포기한 시도들이라 정리할 수 있다.

3.2 Parameter Selection

동형암호는 다른 암호체계와 마찬가지로 기반이 되는 parameter들을 설정해야 한다. HW 설계 시 이러한 modulus 기저들의 크기를 고려하여 i/o 비트 수를 정해야 한다. 문제는 HEAX와 같이 높은 차수의 다항식을 다룰 수 있도록 설계할 경우 과한 복잡도로 timing 문제가 발생할 수 있으며, 일부 resource는 거의 쓰지 않게 될 수 있다. 일부 정보는 사용자만 알고 있으므로 노출 위험이 적지만, 많은 사용자가 서로 다른 설정 하에 활용하기 위해서 정보를 저장한다면 error 발생 빈도가 높아질 수 있어 이를 고려하여 설계하여야 한다.

3.3 연산 종류의 한계

동형암호의 장점은 암호화한 상태에서 연산이 이

루어진 후 복호화하더라도 같은 결과를 만들어 준다는 점이다. 덧셈과 곱셈을 할 수 있지만, 다른 연산이 불가능하다. 지수 함수같이 다항식으로 근사가 가능한 방법이 있지만, comparator와 같은 비교 연산은 암호화 상태에서 불가능하다.

직접 비교 연산 없이 같은 기능을 할 방법들에 관한 연구 시도가 있었지만, 단순 부호 판단만 하더라도 zero 값에 대한 암호문이 알려져야 하는 등 조건들이 필요하며, 특정 case들에 대한 암호문을 공개하는 것은 암호체계의 confidentiality를 해치기에 위험한 접근으로 여겨진다.

4. Homomorphic CNN HW 구현

2, 3장서 서술한 내용을 바탕으로 HW 구현 솔루션을 설계하는데 고려해야 할 점들이 많다. 본 장은 CNN의 inference 과정을 동형암호 체계로 구현하기 위한 일련의 선택과정을 서술하고, 이들에 대한 비교 자료를 제시할 것이다. MNIST dataset을 활용하였고, C++과 MS의 SEAL을 통해 CKKS scheme을 구현하였다. SW 구현이지만 HW 설계 시뮬레이션을 이루기 위해 각 component 별 비트 수를 고정하였고, 이를 초과할 경우 error가 발생하도록 만들고 진행하였다.

4.1 SHE vs FHE

SHE와 FHE에 대한 선택은 HW 구현에 있어 큰 trade-off를 일으킨다. FHE는 제한 없는 곱셈 횟수를 이루어 낼 수 있지만 많은 양의 resource가 필요하여 값비싼 솔루션인 만큼 최적화를 목적으로 하는 HW 설계 면에서 한계를 지니고 있다. HEAX의 경우 Stratix 10 보드의 90%가 넘는 resource를 활용하여 연산자를 구현했음에도 bootstrap이 많은 연산을 진행시 speedup이 4.8에 불과한 결과를 보여주었다. 이에 FPGA를 활용하여 parameter를 조절해서 재부팅 없이 사용자 필요에 맞는, 기능을 수행할 수 있도록 설계하여 FHE와 같은 형태를 구현하는 방법이 성능 면에서 효율적일 것이라 판단된다.

4.2 Modulus Switch / Relinearization

곱이 반복되며 noise 증가 폭이 늘어나는데, 이를 줄이기 위한 기법들 역시 HW 구현 시 충분히 포함할 수 있는 기능들이다. <표 1>는 CNN inference과정을 동형암호 체계에서 구현한 시뮬레이션 코드 결과이다. 곱이 지속할수록, 가용 비트 수가 줄어드는

데, relinearization을 사용할 경우 가용 비트 수 감소량이 줄어들었다. 한편, 시간 지연이 발생하는데, 이 둘의 trade-off는 병렬화, threading, buffer의 활용 등 다른 설계 특징들에 의해 상호 관계가 많이 변하기 때문에, 직접 실험을 통해 최적의 case를 찾아내는 것이 바람직하다고 판단된다.

<표 1> CNN inference 과정 중 data

No# mult.	no relin.	with relin.
0	338 bits left	338 bits left
1	283 bits left	283 bits left
2	224 bits left	245 bits left
3	194 bits left	211 bits left
total time	22sec/img	48sec/img

4.3 사용자 PC와 서버 간 인터페이스

암호화한 상태에서 불가능한 연산들을 다른 방법으로 구현할 수도 있으나, 사용자 PC로 되돌려 복호화한 후 연산을 진행하는 것 역시 방법이 될 수 있다. 데이터를 전송하는 과정이 오랜 시간을 요구하지만, 필요한 기능에 따라 후자가 더 좋은 성능을 나타내기도 한다. 즉, 모든 과정을 암호화한 상태로 진행할 필요가 없다는 것이다.

CNN의 경우 비교 연산은 ReLu 활성화 함수와 마지막 label 선택할 때 softmax값들 중 가장 큰 값을 고르기 위해 활용한다. 따라서 처음 사용자 PC에서 서버, 마지막 서버에서 PC로의 데이터 전송 외 추가 전송이 발생하지 않아, 추가 지연이 필요하지 않다. 따라서 비교 연산을 암호화 상태에서 구현할 필요 없이 PC로 받아 복호화하여 연산할 수 있다.

활성화 함수의 경우, 다른 함수로 대체하여 진행할 수 있다. 시간 지연을 고려한 시뮬레이션 결과 accuracy는 차이가 없었기에, 따로 기능을 구현하지 않는 것으로 선택하였다. 그 결과는 아래 <표 2>를 통해 확인할 수 있다.

<표 2> 활성화 함수에 따른 결과

	ReLu at PC	Linear Activation
time	36sec/img	22sec/img
accuracy	96%	96%

5. 채택한 HW 구현 방향 (CHCNN)

본 연구를 통해 구현한 Partially Homomorphic CNN(PHCNN)은 MS SEAL을 이용하여 CKKS 체계로 구현했으며 요약하면 <표 3>와 같다. 이전 연

구와 다르게 FHE 구현을 위해 과도한 재부팅과 rescale을 진행하지 않고, parameter를 필요에 따라 조정하였고, 이에 Modulus Switch와 Relinearization도 고려하지 않았다. 필요할 때마다 Normalize를 통해 data 범위를 정정하였고, 사용자 PC와 서버와의 통신을 최소화하기 위해 두 번(시작, 끝)만 data를 주고받을 수 있도록 모델을 구현하였다. 표에 나타나지 않은 값들은 중요하지 않거나 SEAL에서 자동으로 설정해주는 값들로, HW 구현할 시 값들을 확인해서 메모리에 사전 저장해주어야 한다.

<표 3> Parameters for CNN model

Parameter Name	Value
poly modulus degree	16384
plain modulus	5522259017729
Max bits	540
multiplicative depth	11
Normalization	Linearized

6. 결론

이전 연구들의 접근과 본 논문을 통해 구현한 체계와의 비교 분석은 아래 <표 4>와 같다.

<표 4> Performance Comparison

HW Approach	inference (sec/img)
Raw approach	1759
Rescaling CKKS	344
HCNN approach	121
PHCNN	22

실험 결과 수학적 접근에 중점을 둔 완전 구현보다, 필요에 따라 scale을 변경하여 제 기능을 수행할 수 있도록 SHE를 조절하는 것이 훨씬 좋은 성능을 보여주었다.

완전한 체계 구현을 위한 과한 설정은 지나친 resource 남용과 bottleneck으로 이어질 수 있으며, 잘못된 설정은 multi-user 인터페이스 구현에 제한 사항을 유발한다. 현재까지 알려진 연구들은 불완전한 구현을 최적화 없이 HW로 구현한 것이 대부분이다. HW 특징을 고려했다는 하나만으로도 본 연구가 이전 결과들보다 좋은 성능을 나타낼 수 있음을 충분히 설명해줄 수 있다. 물론 재부팅과 같은 동형암호 체계의 기능들에 대한 분석, 이에 따른 효율적인 가속기 구현이 이루어진다면 더 좋은 가속기 설계가 가능하리라 생각한다.

추후 본 논문보다 좋은 결과를 위해 위와 같은 연구가 이루어져야 할 것이다.

7. ACKNOWLEDGEMENT

이 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구(NRF-2017R1A2A1A17069478)이며, 2020년도 두뇌한국 21플러스사업에 의하여 지원되었음. 또한, 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2018-0-00230, (IoT 총괄/1세부) IoT 디바이스 자율 신뢰보장 기술 및 글로벌 표준기반 IoT 통합보안 오픈 플랫폼 기술개발 [TrusThingz 프로젝트]).

참고문헌

- [1] R. Rivest, L. Adleman, and M. Dertouzos, "On data banks and privacy homomorphisms," Foundations of secure computation, 1978.
- [2] C. Gentry, "Fully homomorphic encryption using ideal lattices," Proceedings of the 41st ACM Symposium on Theory of Computing 2009, pp. 169 - 178, 2009.
- [3] Z. Brakerski, C. Gentry, V. Vaikuntanathan, "Fully Homomorphic Encryption without Bootstrapping", Electronic Colloquium on Computational Complexity Report No.111 (2011)
- [4] S. Halevi, Y. Polyakov, & V. Shoup, "An Improved RNS Variant of the BFV Homomorphic Encryption Scheme", The Cryptographers' Track at the RSA Conference 2019
- [5] J. Cheon, A. Kim, M. Kim, Y. Song, "Homomorphic Encryption for Arithmetic of Approximate Numbers", ASIACRYPT 2017
- [6] N. Dowlin et al. "Manual for Using Homomorphic Encryption for Bioinformatics", Microsoft Research, 2015
- [7] S. Sinha Roy et al. "FPGA-Based High-Performance Parallel Architecture for Homomorphic Computing on Encrypted Data", 26th International Symposium on high-Performance Coputer Architecture (HPCA, 2019)
- [8] M. Sadegh Riazi et al. "HEAX: An Architecture for Computing on Encrypted Data", 25th The International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS, 2020)

최근 퍼징 기법들과 발전에 관한 연구

전소희*, 이영한*, 김현준*, 백운흥*
*서울대학교 전기·정보공학부, 반도체공동연구소

shjun@sor.snu.ac.kr, yhlee@sor.snu.ac.kr, hjkim@sor.snu.ac.kr, ypaek@snu.ac.kr

A Study of fuzzing techniques and their development

So-Hee Jun*, Young-Han Lee*, Hyun-Jun Kim*, and Yun-Heung Paek*

*Dept. of Electrical and Computer Engineering and Inter-University Semiconductor Research Center (ISRC),

Seoul National University

요 약

최근 컴퓨터 프로그램의 크기가 증가하고 목적이 다양해지면서 프로그램의 취약점에 대한 위협이 증가하고 있다. 공격자 보다 먼저 프로그램 취약점을 찾아내기 위한 여러 기법들이 있다. 그 중 프로그램의 취약점을 보다 효율적으로 찾아내기 위한 기법 중 하나인 퍼징 (Fuzzing) 은 프로그램에 무작위로 입력 데이터를 입력하여 프로그램의 정의되지 않은 영역을 검증하는 기법이다. 이러한 입력 데이터를 최대한 적은 시간과 자원을 소모하여 생성하기 위해 인공지능과 퍼징을 결합하는 연구가 활발히 진행 중이다. 본 논문에서는 퍼징의 개념 및 종류에 대해 설명하고 퍼징과 인공지능이 결합된 최신 연구에 대해 서술한다.

1. 서론

최근 다양한 목적을 가진 여러 종류의 프로그램들이 요구되고 개발되면서, 프로그램의 크기 및 복잡도가 매우 증가하고 있다. 그에 따라, 프로그램의 취약점 또한 증가하게 되며 이런 프로그램의 취약점은 공격자에게 공격 대상이 될 수 있기 때문에 반드시 공격자보다 먼저 알아내어 보완되어야 한다. 마이크로소프트, 페이스북 등과 같은 IT 대기업 회사에서는 자사 프로그램의 취약점을 찾아낸 사람에게 포상금을 지급하는 버그바운티 (Bug bounty) 제도가 있을 정도로 프로그램의 취약점을 찾는 것은 중요한 작업이다. 하지만 개발자가 프로그램을 개발하면서 직접 취약점을 찾아내는 것은 사실상 불가능에 가까우며, 전문가를 통한 역공학 (Reverse engineering) 기법, 동적 테스트와 같은 기법들이 사용되고 있지만 많은 인력, 시간과 자원이 소모된다. 이를 보완하기 위해 취약점 자동화 테스트 기법들이 활발히 연구되고 있으며 대표적으로 퍼징 (Fuzzing) 기법이 있다. 본 논문은 이러한 퍼징 기법에 대해 알아보고 최근 기존 퍼징 기법의 단점을 보완하기 위해 퍼징과 인공지능을 결합하는 연구에 대해 서술한다.

2. 퍼징이란?

퍼징 (Fuzzing)이란, 소프트웨어 테스트 기법으로 프로그램에 대해 무수한 여러 데이터를 입력하여 프로그램의 충돌이 발생하는 프로그램 취약점의 위치를 찾아내는 기법이며 주로 소프트웨어나 컴퓨터 시스템들의 보안 취약점을 파악하고 정의되지 않은 영역을 검증하기 위해 사용된다. 이러한 퍼징 기법의 기원은 매우 우연적이다. 장마철 전자기 간섭으로 인해 프로그램에 임의의 값들이 무작위로 입력되어 프로그램의 충돌이 발생하였고 이를 통해 무작위로 생성된 입력이 프로그램의 취약점을 발현 시킬 수 있다는 것이 발견되었다 [1]. 퍼징은 주어진 시간 동안 최대한 많은 프로그램의 취약점을 찾아내는 입력 데이터를 찾아내는 최적화 문제이지만 취약점이 프로그램 내에 드문드문하게 위치하기 때문에 퍼징의 성능은 주로 프로그램의 코드를 커버한 정도로 평가된다.

2.1 퍼징 기법의 분류

퍼징 기법은 프로그램의 정보를 활용하는 정도에 따라 블랙박스 (black-box) 퍼징, 화이트박스 (white-box) 퍼징, 그레이박스 (gray-box) 퍼징으로 분류할 수 있다. 블랙박스 퍼징은 대상 프로그램의 내부 정보를 사용하지 않고 대상 프로그램의 입력과 출력 데이터

만 사용하는 퍼징 기법이다. 대표적으로 SPIKE [2], BFF (Basic Fuzzing Framework) [3], FOE (Failure Observation Engine) [4] 등이 있다. 화이트박스 퍼징은 대상 프로그램의 내부 구조와 실행 중 발생하는 정보들을 사용하는 퍼징 기법이다. 대표적으로, 그레이박스 퍼징은 블랙박스와 화이트박스의 중간적인 특성을 가지며 대상 프로그램의 내부 정보와 실행 중 발생하는 정보 일부를 사용하는 퍼징 기법이다. 대표적으로, AFL (America Fuzzy Loop) [5], VUzzer [6] 등이 있다.

또한, 퍼징 기법은 입력 데이터를 생성하는 법에 따라 두가지로 구분할 수 있다. 생성 기반 (Generation-based) 퍼징은 데이터의 구조 및 프로토콜을 이해하여 프로그램에 적합한 입력 데이터를 생성하는 기법이다. 생성될 입력 데이터의 구조 및 프로토콜을 이해하기 때문에 유효한 입력 데이터를 잘 구성할 수 있지만 많은 시간이 소요될 수 있다. 변이 기반 (Mutation-based) 퍼징은 입력 데이터를 특정하여 그 입력 데이터에 대해 조금씩 변이를 주어 새로운 입력 데이터를 생성하는 기법으로 여기서 특정된 입력 데이터는 주로 씨드 (seed) 데이터라 통칭된다. 변이 기반 기법은 씨드 데이터에 무작위적으로 변형을 주는 기법이기에 때문에 많은 시간이 소요되지 않지만 유효하지 않은 입력 데이터가 생성되는 경우가 많아 멍청한 (dumb) 퍼징이라 불리기도 한다.

3. 인공지능을 활용한 퍼징

퍼징 기법의 시초는 데이터를 무작위로 생성하는 것이었지만, 임의의 값을 무작위로 생성하는 것은 많은 시간과 비용을 소모하며 유효하지 않은 입력 데이터를 만들 가능성이 매우 높아 비효율적이다. 그렇기에 다수의 퍼징 기법은 진화 알고리즘 (Evolutionary algorithm)을 사용한다. 진화 알고리즘은 세대에 걸쳐 입력 데이터를 생성하는 방법으로 이전 세대에서 유용하게 사용되었던 입력을 골라 다음 세대에서 재사용하여 무작위 생성 방법보다 효율성을 높일 수 있고 시간도 절약할 수 있다.

최근에는 퍼징 기법에 인공지능을 결합하여 보다 효율적으로 프로그램 취약점을 검증하는 연구가 활발히 진행되고 있다. 기존 진화 알고리즘 (Evolutionary Algorithm)을 사용하는 방법은 시간적 이점을 가지지만 무작위적으로 변형을 진행하면서 유효하지 않은 입력 데이터를 다수 생성할 가능성이 높다는 단점을 가진다. 이러한 단점을 보완하기 위해, 데이터의 패턴을 학습할 수 있는 인공지능 기술과 퍼징을 결합하는 연구가 많이 진행되고 있다. 그 중 인공 신경망을 통해 입력 데이터와 출력 데이터 간의 관계를 파악하는 Neuzz [7]와 퍼징에 효과적인 입력 데이터를 생성하기

위해 인공 신경망을 사용하는 Learn & Fuzz [8]과 강화 학습 (Reinforcement learning)을 퍼징에 활용하는 Deep Reinforcement Fuzzing [9]에 대해 서술한다.

3.1 Neuzz

Neuzz는 프로그램의 엣지 커버리지 (Edge coverage) 데이터를 사용하는 그레이박스 퍼징 기법으로 신경망 (Neural Network)을 통해 출력 데이터 간의 관계를 이해하여 입력 데이터가 출력 데이터에 끼치는 영향력을 분석하여 입력 데이터에서 출력 데이터에 높은 영향력을 끼치는 부분을 변이하여 보다 효과적으로 프로그램의 취약점을 찾는다. 신경망은 대상 프로그램의 브랜치 행동 (Branch behavior)과 관련된 입력 데이터 간의 관계를 비선형 함수로 근사화하여 입력 데이터에 따른 대상 프로그램의 컨트롤 플로우 엣지 (Control flow edge)를 예측한다. 학습된 신경망을 활용하여 입력 데이터에서 되면 출력 데이터에 큰 변화를 줄 수 있는 부분을 변이하여 취약점 탐지를 위한 입력 데이터를 생성한다. 또한 생성된 새로운 입력 데이터로 다시 신경망을 학습시켜 신경망이 기존 입력 데이터와 생성된 입력 데이터에 대한 학습을 증진시켜 높은 성능을 보였다.

3.2 Learn & Fuzz

Learn & Fuzz는 신경망과 샘플 입력 데이터를 사용해 문법 기반 (Grammar-based) 퍼징을 위한 입력 데이터를 생성하는 기법이다. Learn & Fuzz의 목표는 대상 프로그램의 코드 커버리지를 최대화하기 위한 입력 데이터를 생성하는 것과 대상 프로그램의 정의되지 않은 영역을 검증하기 위한 입력 데이터를 생성하는 것이다. 이를 위해 Learn & Fuzz는 새로운 입력 데이터를 생성하기 위해 다음에 올 값을 예측할 수 있는 신경망의 한 종류인 RNN (Recurrent Neural Network)을 사용하며 대상 프로그램과 입력 데이터는 PDF (Portable Documents Format)가 대상이다. Learn & Fuzz는 세가지 방법을 통해 새로운 PDF 데이터를 생성한다. 첫번째 방법은 뒤에 이어질 가장 높은 확률의 문자를 선택하는 것이고, 두번째 방법은 뒤에 이어질 문자를 확률적으로 선택하는 것이고, 세번째 방법은 위의 두 방법을 합친 것으로 앞의 문자가 공백으로 끝날 때는 두번째 방법을 사용하고 아닐 경우에는 첫번째 방법을 사용하는 것이다. 이러한 Learn & Fuzz는 처음으로 신경망 기반 확률적 학습 기법을 사용하여 문법 기반의 퍼징을 위한 프로그램 입력 데이터를 생성하였으며 학습된 신경망 모델을 통해 유효하며 프로그램의 커버리지를 높일 수 있는 입력 데이터를 생성하였다.

3.2 Deep Reinforcement Fuzzing

Deep Reinforcement Fuzzing 은 강화 학습을 퍼징에 사용한 방법으로 강화 학습은 환경 (Environment), 행위 (Actions), 보상 (Reward)를 기본 요소로 가지며, 환경과 소통하며 행위를 하여 보상을 얻는 에이전트 (Agent)가 존재한다. 에이전트의 목적은 최대한 많은 보상을 얻는 것이다. 이러한 에이전트가 입력 데이터에 대해 행위를 수행하여 새로운 입력 데이터를 생성하고 생성된 데이터가 프로그램의 취약점을 많이 찾아내거나 프로그램의 코드 커버리지를 증가시킬수록 높은 보상을 받는 과정을 따른다. 이 과정을 통해 에이전트는 최대한 많은 보상을 얻기 위해 유효하고 퍼징 성능이 좋은 입력 데이터를 생성하게 된다. 강화 학습은 인공지능 분야 중에서도 최근 활발하게 연구되고 있는 분야로 앞으로 더욱 발전하여 퍼징과 결합된다면 높은 성능을 보일 수 있을 것으로 기대된다.

4. 결론

우리의 삶 가까운 곳에서 함께하고 있는 컴퓨터 프로그램의 목적과 기능이 다양해지면서 그에 따른 보안의 필요성 또한 크게 증가하고 있다. 이로 인해, 프로그램의 취약점을 검증하기 위한 기법들에 대한 연구가 진행 중이며 특히 자동화 소프트웨어 테스팅 기법인 퍼징에 대한 연구가 활발히 진행되고 있다. 최근에는 전통적인 퍼징 기법의 한계점을 인공지능 기술을 통해 보완하는 기법이 연구되고 있으며 높은 효율성과 좋은 성능을 보이고 있어 큰 발전이 기대되고 있다.

5. ACKNOWLEDGEMENT

이 논문은 2020 년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원 (NRF-2017R1A2A1A17069478), 2020 년도 두뇌한국 21 플러스 사업에 의하여 지원되었고 2020 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2018-0-00230, (IoT 총괄/1 세 부) IoT 디바이스 자율 신뢰보장 기술 및 글로벌 표준 기반 IoT 통합보안 오픈 플랫폼 기술개발 [TrusThingz 프로젝트])

참고문헌

- [1] Barton P. Miller, Louis Fredriksen, Bryan So, "An Empirical Study of the Reliability of UNIX Utilities." Communications of the ACM, 33(12):33-44, December 1990.
- [2] D. Aitel, "An introduction to SPIKE, the fuzzer creation kit," in Proceedings of the Black Hat USA, 2001.
- [3] CERT, "Basic Fuzzing Framework," <https://www.cert.org/vulnerability-analysis/tools/bff.cfm>.
- [4] "Failure Observation Engine," <https://www.cert.org/vulnerability-analysis/tools/foe.cfm>
- [5] M. Zalewski, "American Fuzzy Lop," <http://lcamtuf.coredump.cx/afl/>.
- [6] S. Rawat, V. Jain, A. Kumar, L. Cojocar, C. Giuffrida, and H. Bos, "VUzzer: Application-aware evolutionary fuzzing," in Proceedings of the Network and Distributed System Security Symposium, 2017.
- [7] Dongdong She, Kexin Pei, Dave Epstein, Junfeng Yang, Baishakhi Ray, Suman Jana. "Neuzz: Efficient fuzzing with neural program learning." In 2019 IEEE Symposium on Security and Privacy (SP). IEEE, 2019.
- [8] P. Godefroid, H. Peleg, and R. Singh, "Learn&fuzz: Machine learning for input fuzzing," CoRR, vol. abs/1701.07232, 2017.
- [9] Konstantin Bottinger, Patrice Godefroid, Rishabh Singh. "Deep reinforcement fuzzing." 2018 IEEE Security and Privacy Workshops, SP Workshops 2018, San Francisco, CA, USA, May 24, 2018, pages 116-122, 2018.

Multi-Variant Execution Environment 연구 동향

조명현*, 장지원*, 남기빈*, 황동일*, 백윤흥*

*서울대학교 전기정보공학부, 반도체공동연구소

{mhcho, jwchang, kvnam, dihwang}@sor.snu.ac.kr, ypaek@snu.ac.kr

A Study on Multi-Variant Execution Environment

Myunghyun Cho*, Jiwon Chang *, Kevin Nam*, Dongil Hwang*, Yunheung Paek*

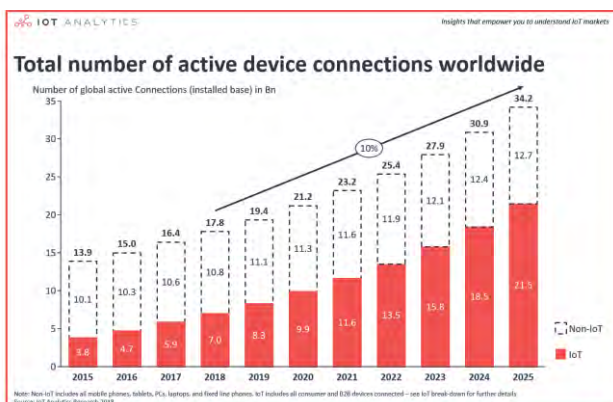
*Dept. of Electrical and Computer Engineering and Inter-University
Semiconductor Research Center (ISRC), Seoul National University.

요 약

C 와 C++은 비교적 자유로운 코딩 환경으로 많은 프로그래머들에게 사랑받는 프로그래밍 언어이다. 또한, 빠른 속도와 호환성 덕분에 현재 많은 IOT, 임베디드 시스템에 적용되고 있다. C 와 C++은 자유로운 환경을 가지고 있는 반면에 프로그래머의 부주의한 코딩 방식에 의해 여러 취약점을 발생시켜 공격 범위를 증가시킬 수 있다. 다음은 외부 침입자에게 공격에 필요한 좋은 소스를 제공할 수 있으므로 이러한 공격을 막기 위한 범용적인 기술이 필요하다. 본 연구에서는 다음 취약점에 대한 공격을 막을 수 있는 기술 중 하나인 Multi-Variant Execution Environment(MVEE) 기술을 소개하고 다음 기술의 핵심인 다양한 Variant 생성 방식과 기존 연구 분석을 통해 한계점을 고찰하고자 한다.

1. 서론

최근 IOT, 임베디드 기기의 증가에 따라 많은 사물들이 연결된 시대가 도래했다. 스마트 홈은 가스레인지, 냉장고, 컴퓨터, IP 캠 등과의 통신을 통해 사용자가 본인 휴대전화로 원격 제어가 가능하지만, 해킹에 대한 취약점을 갖고 있는 것이 화두가 되고 있다. 취약점을 제공하고 있는 원인 중 하나는 많은 임베디드 기기들이 C 와 C++을 기반으로 애플리케이션을 돌리고 있다는 점인데 다음 프로그래밍 언어의 특성으로 인해 공격 가능한 면적이 넓어질 수 있다.



(그림 1) IOT 트렌드.[1]

C 와 C++은 자유로운 코딩 환경과 빠른 실행 환경으로 임베디드 기기뿐만 아니라 많은 애플리케이션

제작에 사용되고 있는 범용적인 프로그래밍 언어이다. 자유로운 코딩 환경을 제공하는 특성을 가지지만 프로그래밍 개발자의 부주의로 인해 여러 가지 보안 문제를 가질 수 있다. 전 세계적으로 많이 사용하는 모놀리식 커널인 Linux, Windows, BSD 등은 프로그래머들이 코딩 방식에 많은 주의를 기울이고 있지만 여전히 안전하지 않은 프로그래밍 언어를 사용하므로 많은 버그가 존재한다. 예를 들어 보편적인 취약점에는 1) Uninitialized read, 2) Use-after-free, 3) Out-of-bounds 등이 있는데 다음을 이용해 공격자들은 민감한 커널 포인터 탈취, 암호화 키 탈취 등을 통해 Privilege escalation과 같은 차후의 공격으로 연결할 수 있다. 만약 공격을 통해 공격자가 Root 권한을 탈취한다면 중요한 데이터에 대한 접근 권한을 가질 수 있고 IOT 기기들(IP 캠 등)을 통해 사용자의 개인정보가 유출될 수도 있다.

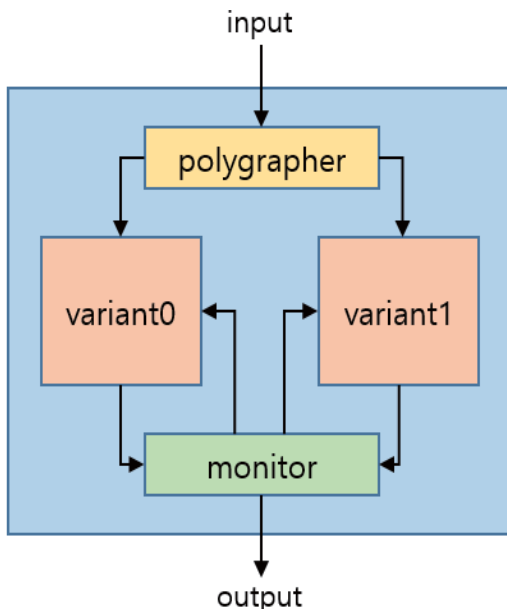
안전하지 않은 프로그래밍 언어를 사용할 때 개발자의 세밀한 코딩 방식으로는 한계가 있다. 그러므로 여러 가지 보안 기법들이 필요한데 다음 기법에는 정적 분석을 통한 변수 초기화, Bound check, 비정상적인 행동 모니터링 등과 같이 공격자에게 소스를 제공하는 것을 막는 기법들이 있고, ASLR(Address Space Layout Randomization), KASLR(Kernel Address Space Layout Randomization)와 같이 확률적인 방어 기법들이 존재한다. Fine-grained 기법에서는 여러 공격에 대한 높은 방어율을 보여주지만 높은 성능 저하를 발생시

키고 Coarse-grained 기법에서는 낮은 성능저하와 낮은 비용 등을 보여주지만 한정된 공격에 대한 방어만 가능하다.

많은 보안 기법들 중 본 논문에서는 MVEE(Multi-Variant Execution Environment)에 대해 2장에서 설명하고 3장에서는 여러 MVEE 기법에 대한 분석 마지막으로 4장에는 결론과 MVEE 기법에 대해 고찰을 할 예정이다.

2. MVEE(Multi-Variant Execution Environment) 개념

NVP(N-Version Programming)는 1970년 Chen and Avicenis[2]에 의해 고안되었다. NVP의 아이디어는 여러 프로그래머로 이뤄진 팀마다 각각 독자적인 똑같은 프로그램을 만들어 병렬적으로 돌림으로써 버그를 찾아내는 방식에 의해 출발하였다. 하지만 업데이트가 필요할 때 모든 독자적인 프로그램들을 다시 업데이트해야 하므로 높은 유지비용을 발생시켰다.



(그림 2) N-variant System Framework.[3]

초기 NVP의 높은 유지비용을 해결하기 위해 Variant[3]라는 개념을 도입하였다. Variant란 본질적으로 동일한 행위를 하지만 방식을 Variant마다 정해진 규칙에 따라 다각화하여 비정상적인 행동이나 버그가 생길 시 다른 행동을 하도록 만든 개체이다. MVEE의 Variant들은 동일한 소스 코드에서 자동적으로 생성되기 때문에 수동적으로 다시 업데이트할 필요가 없어 초기 NVP의 단점인 높은 유지비용을 감소시켰다.

MVEE(Multi-variant execution environment) 기술은 악의적인 공격 시 프로세스의 상태가 달라지는 특성을 모니터링하므로 프로그램의 버그 탐지뿐만 아니라 보안에도 적절하다. MVEE의 동작은 (그림 2)와 같이 폴리그래퍼가 입력을 받으면 다음 입력을 복사하여

각각의 Variant들에게 똑같이 전달한다. 여기서 Variant들은 본질적으로 동일한 행위를 하지만 내부의 구조가 다르므로 내부 상태에 맞게 알맞은 입력을 줘야 한다. 예를 들어, 각 입력에 해당하는 포인터의 위치는 다를 수 있지만, 본질적인 내용은 같아야 하고 버퍼를 사용할 시 위치가 다르더라도 버퍼 안의 내용은 같아야 한다. 다음과 같이 각 Variant은 동일한 행위를 수행하고 결과값을 모니터로 전달하는데 이 때 모니터는 각각의 모니터의 값을 비교하여 같은 값이 나왔는지 비교한다. 만약에 동일한 입력에 대해 다른 출력값이 나왔다면 다음을 공격으로 간주하고 민감한 데이터를 0으로 만들어 유출을 막거나 프로그램을 종료시키는 등 미리 정해진 규칙에 따라 동작하도록 만든다.

다음과 같이 MVEE는 Multi-Variant들을 동시에 실행시키므로 현대 멀티코어 시스템에서 매우 적합하다. 또한, 특정 환경에 맞게 출력 값만 볼 것인지 아니면 내부 진행상태를 정해진 범위내에서 볼 것인지 정하여 granularity를 조절할 수 있으므로 각각의 디바이스에 맞는 보안 수준을 제공할 수 있다.

3. MVEE(Multi-Variant Execution Environment) 연구 동향

MVEE는 런타임 모니터링 기술로써 Lock-step 방식을 통해 동일한 입력을 동기화하여 각각의 Variant에 넣는다. 보안성을 위해 각각의 Variant들은 메모리 Isolate 기술을 사용하여 모니터와 물리적으로 분리되어 있다. 또한, 성능향상을 위해 Salamat B, Jackson T, Wagner G, et al[4]은 각각의 Variant의 메모리 블록을 공유시키는 방식을 고안했는데 모니터가 Variant들에게 데이터를 제공할 때는 공유된 메모리에 써서 Variant들이 읽은 뒤 자신의 할당된 주소에 쓰도록 하였고, 동일하게 모니터가 각각의 데이터를 요청할 때는 자신의 주소에서 읽어 공유된 메모리에 쓰도록 하였다.

현재 연구된 MVEE는 다양한 모니터의 구현과 Variant 방식을 가지고 있다. 대부분의 MVEE는 User-space에서 구현되는데 그 이유는 User-space 프로그램들은 엄격하게 정의된 Syscall이라는 I/O 인터페이스를 가지고 있기 때문이다. 그러므로 각각의 Variant들은 Syscall을 통해 동일한 시간 값과 네트워크 트래픽을 가질 수 있다. 하지만 Kernel-space에서는 그러한 인터페이스가 없으므로 추가적인 동기화 구조를 만들어야 한다. 최신 연구인 kMVX[5]는 Kernel-space에 동기화 구조를 추가적으로 만들어 MVEE를 구현할 수 있음을 보여줬다.

MVEE의 단점 중 하나는 다음 기술을 적용 시 큰

성능 저하를 발생시킨다는 점이다. 특히 I/O 에 관련된 Syscall 이 연속적으로 요청되었을 때 더 큰 성능저하를 보여주었다. 대부분 모니터의 구현은 Syscall 을 감지하는 ptrace 인터페이스에 의해 구현되는데 4byte 씩 읽는 특성 때문에 느리다는 단점이 있다. 그러므로 성능 저하를 줄이기 위해 여러 기법들의 구현이 필요하다. VARAN[6]같은 경우에는 Fast shared memory ring buffer 를 이용하여 ptrace 인터페이스의 오버헤드를 감소시켰고, ReMon[7]은 모니터로 Context switching 이 일어날 때 큰 성능 저하가 발생하는 것을 대상으로 하여 Syscall 중 민감한 Syscall 은 cross-process 모니터를 이용하여 외부에서 안전하게 처리하고 민감하지 않은 Syscall 은 in-process 모니터를 이용하여 빠르게 처리하여 성능 저하를 감소시켰다. 하지만 다음 노력에도 불구하고 몇 가지 벤치마크에서는 아직도 큰 성능 저하를 보여주었다.

MVEE 의 핵심적인 요소는 Variant 의 설정이다. 어떻게 Variant 를 정할지에 따라 보안 수준과 성능이 달라지므로 적절한 매커니즘을 고안해야 한다. Variant 를 통한 보안 수준 향상을 위해 주의할 점은 Variant 자체의 엔트로피보다는 공격에 대해 각각의 Variant 마다 서로 다른 행동을 보여줌으로써 공격에 대한 탐지를 가능하게 하는 것이다. 예를 들면 KASLR 같은 경우 커널 메모리의 레이아웃에 대한 복잡도가 증가하므로 자체 엔트로피는 크지만, 공격에 대한 Variant 마다의 상이함을 잡아낼 수 있는 능력이 높다고는 말할 수 없다.

<표 1> 취약점 및 대응하는 Variant 기법들

취약점	Variant 기법
포인터	1) 주소공간 파티셔닝
초기화 안된 변수	2) 리버스 스택
초기화 안된 변수	3) 스택 패딩
초기화 안된 변수	4) 스택 구조 랜덤화
코드 삽입	5) 명령어 세트 랜덤화
포인터	6) 시스템 콜 번호 랜덤화
버퍼 오버 플로우	7) 데이터 공간 랜덤화
Use-after-free	8) Type-based SLAB allocator

현재 연구된 Variant 방식은 1)주소 공간 파티셔닝, 2)리버스 스택, 3)스택 패딩, 4)스택 구조 랜덤화, 5)명령어 세트 랜덤화, 6)시스템 콜 번호 랜덤화, 7)데이터 공간 랜덤화, 8)Type-based SLAB allocator 등 여러 가지가 있다. 1)주소 공간 파티셔닝 기법은 가장 보편적으로 쓰이는 방식으로 Variant 마다 다른 절대 주소 공간을 할당하여 공격자가 민감한 포인터에 악의적인 목

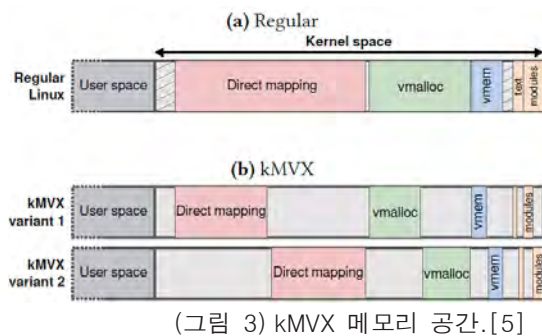
적으로 접근 시 알람을 울리게 하는 방법이다. 한 Variant 주소 공간에 적법한 민감한 포인터가 다른 Variant 주소 공간에서는 적법하지 않을 수 있는 것을 이용한다. 스택의 포맷을 바꾸는 방식은 초기화가 안된 변수를 통한 데이터 유출을 막는 데 도움이 된다. 예를 들어 스택 프레임이 pop 되고 새로운 스택 프레임이 push 되었을 때 새로운 스택 프레임에 초기화가 안된 변수가 있으면 이전 프레임의 값을 가지고 있을 수 있다. 2)리버스 스택은 스택이 자라는 방향을 다르게 하는 기법이고, 3)스택 패딩은 프레임마다 랜덤하게 공간을 만들어 타겟이 되는 데이터 값을 읽지 못하게 하는 방법이다. 또한, 4)스택 구조 랜덤화를 이용해 필드의 저장 순서를 랜덤화 하여 원하는 데이터의 위치를 알기 어렵게 만들 수 있다. 5)명령어 세트 랜덤화는 명령어에 각각의 Variant 에 맞는 랜덤한 값을 추가해 악의적인 목적의 명령어 실행 시 특정 Variant 에서는 가능하지만 다른 Variant 에서는 불가능하게 만들어 모니터가 탐지하게 만드는 기법이다. 6) 시스템 콜 번호 랜덤화는 실행마다 시스템 콜번호에 해당하는 서비스 루틴을 랜덤화 하여 공격자가 포인터 탈취를 통해 악의적인 서비스 루틴을 실행하지 못하도록 막는다. 7)데이터 공간 랜덤화[8]는 버퍼 오버플로우를 탐지하는 기법으로 각 Variant 의 버퍼와 민감한 데이터마다 다른 키를 할당하여 XOR 연산을 하게 만든다. 만약에 버퍼 오버 플로우가 발생한다면 민감한 데이터 앞의 버퍼의 키 값이 민감한 데이터와의 연산으로 올라와 다른 Variant 와 다른 결과를 야기할 것이다. 8)Type-based SLAB allocator 은 kmalloc 의 수정을 통해 SLAB allocator 을 타입 기반으로 바꿔 use-after-free 를 방지하는 기법이다. 다음과 같이 다양한 기법들이 존재하지만, 상황에 맞지 않은 적용들은 오히려 성능 저하를 발생시킬 수 있다.

<표 2> MVEE 연구 동향[9]

Technique	Synchronization	Defense	Implementation	Privilege	Security Benchmark
GHUMVEE	program points		ptrace	user space	
DCL	program points	control flow hijacking exploits	ptrace	user space	CVE-2013-2028 CVE-2010-4221 CVE-2012-4409 CVE-2014-0749
ReMon	syscall	unknown attacks and low-level memory errors	ptrace	kernel space	logical argument
MvArmor	syscall	memory error exploits	ptrace	user space	CVE-2004-0488 CVE-2014-0160
KMVX	I/O and syscall	kernel information leaks		kernel space	CVE-2014-0195 CVE-2016-4569 CVE-2013-2237 CVE-2016-0728
Varan	syscall		binary rewriting	context	

여러 모니터링 기법, Variant 기법, Memory-space 기법 등을 통해 MVEE 에 관한 연구들이 진행되어 왔다. Petr Hosek 은 Bionic C 라이브러리 기반의 자신만의 C library function 을 구현한 'VARAN[6]'을 발표해 성능

향상을 보여줬고, K. Koning 은 hardware-assisted 가상화 기반의 ‘MvArmor[10]’을 구현함으로써 성능 개선에 도움을 주었다. S.Volckaert 는 주소 파티셔닝 기법을 이용해 ROP (Return Oriented Programming) 공격을 막는 ‘DCL[11]’을 보여주었고 중요한 Syscall 만 cross-process 모니터를 통해 선별적으로 안전하게 검사하는 ‘ReMon[7]’을 고안하여 성능 향상을 보여주었다. 최근에는 S. Osterlund 가 초기화가 안 된 변수를 통한 민감한 정보의 유출을 타겟으로 Kernel-space 에서 두 커널을 Variant 로 설정하여 주소 파티셔닝, 스택과 힙 영역의 다각화 등을 통해 MVEE 시스템을 구현했다. 두 커널에 시간과 네트워킹을 동기화할 수 있는 I/O sync 와 Copy_to_user 와 같은 커널 정보가 유저에게 유출될 수 있는 상황을 탐지할 수 있는 Syscall sync 를 구현해 Kernel space 에서 공격을 탐지할 수 있는 ‘kMVX[5]’를 발표했다.



4. 결론 및 고찰

본 논문에서는 C 와 C++의 취약점을 보완할 수 있는 MVEE 에 대한 개념과 핵심 기법인 Variant 를 소개했고, 과거 MVEE 기법부터 최신 MVEE 기법까지 분석을 했다. 모든 보안 기법에도 그렇듯 성능과 보안은 Trade-off 관계에 있다. 최신 연구인 kMVX[5]도 20~50%의 높은 성능 저하를 보여주는데 앞으로 다음 문제점을 개선하기 위해서는 공격이 가해질 때 포괄적으로 반대 행동을 하는 Variant 에 대한 연구, 병렬적인 연산을 해결할 수 있는 하드웨어 모니터링, 필요한 방어 기법들만 유동적으로 적용할 수 있는 모듈화에 관한 연구 등이 필요할 것이다.

5. ACKNOWLEDGEMENT

본 연구는 2020 년도 정부(과학기술정보통신부)의 재원으로 한국연구재단(NRF-2017R1A2A1A17069478), 2020 년도 두뇌한국 21 플러스사업, 2020 년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터(No.2017-0-00213, 능동적 사전보안을 위한 사이버 자가변이 기술 개발)의 지원을 받아 수행된 연구임.

참고문헌

- [1] <https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/>
- [2] Liming Chen., Algirdas V. Avizienis. “N-version programming: A fault-tolerance approach to reliability of software operation” in Annual International Conference on Fault-Tolerant Computing, Toulouse, 1978, pp.3-9.
- [3] B. Cox et al. “N-variant systems: A secretless framework for security through diversity” in *USENIX Security*, Canada, 2006, pp. 105-120
- [4] Salamat, B., Jackson, T., Wagner, G., Wimmer, C., Franz, M., “Runtime defense against code injection attacks using replicated execution” in Department of Computer Science, United States, 2011, pp. 588-601.
- [5] S. Österlund., K. Koninh., P. Olivier., A.Barbalace., H.bos., C. Giuffrida. “kMVX: Detecting Kernel Information Leaks with Multi-variant Execution” in ASPLOS, United States, 2019, pp. 559.
- [6] Hosek, P., & Cadar, C. “Varan the unbelievable: An efficient n-version execution framework.” in International Conference on Architectural Support for Programming Languages and Operating Systems – ASPLOS, Istanbul, 2015, Vol. 50, No. 4, pp. 339-353
- [7] Volckaert, S., Coppens, B., Voulimeneas, A., Homescu, A., Larsen, P., De Sutter, B., & Franz, M. “Secure and efficient application monitoring and replication” in *USENIX Annual Technical*, United States, 2016, pp. 167-179
- [8] Hwang, Shin, et al. "Data Randomization for Multi-Variant Execution Environment.", in International SoC Design Conference (ISOCC), Jeju, 2019, pp. 291-292
- [9] Zhenwu Liu, Zheng Zhang, Jiexin Zhang and Hao Liu. “Multi-Variant Execution Research of Software Diversity” in *Journal of Physics: Conference Series*, China, 2019, Volume 1325.
- [10] Koning, K., Bos, H., & Giuffrida, C. “Secure and efficient multi-variant execution using hardware-assisted process virtualization.” in 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), France, 2016, pp. 431-442.
- [11] Volckaert, S., Coppens, B., & De Sutter, B. “Cloning your gadgets: Complete ROP attack immunity with multi-variant execution” In *IEEE Transactions on Dependable and Secure Computing*, 2015, 13(4): 437-450.

스마트 컨트랙트를 사용한 IoT 서비스 접근제어 설계

김미선*, 서재현*

*국립목포대학교 정보보호학과

misun@mokpo.ac.kr, jhseo@mokpo.ac.kr

A Design of IoT Service Access Control using the Smart Contract

Mi-Sun Kim*, Jae-Hyun Seo*

*Dept of Information Security Engineering, Mokpo National University

요 약

IoT 서비스는 이기종의 다양한 IoT 장치들로부터 수집된 데이터를 목적에 맞게 가공, 저장, 처리하여 사용자에게 서비스를 제공한다. 본 연구에서는 이기종의 IoT 서비스에서 공유 가능한 접근 제어를 위해 스마트 컨트랙트를 사용하고자 한다.

이를 위해 IoT 데이터 공유를 위하여 탱글 네트워크 환경에서 실행되는 스마트 컨트랙트(Smart Contract)를 사용한 IoT 서비스 접근 제어를 설계하였다. 본 연구를 통해 이기종의 다양한 사물인터넷 서비스들이 탱글 네트워크를 통해 스마트 컨트랙트를 공유함으로써, 중앙 제어 없이 IoT 데이터 접근이 안전하게 이루어질 수 있다.

1. 서론

IoT 산업은 지속적으로 성장하여 더 많은 IoT 센서가 만들어지고, 다양한 분야에서 사용되고 있다. IoT 센서의 수가 증가함에 따라 해당 센서에서 생성된 데이터의 가치를 극대화하는 방법을 찾는 것이 점점 더 중요해지고 있다[1]. IoT 서비스는 다양한 IoT 장치들로부터 수집된 데이터를 목적에 맞게 가공, 저장, 처리하여 사용자에게 서비스를 제공한다. IoT 장치들로부터 수집된 데이터는 사물인터넷 서비스들에 의해 공유되어지며, 이 과정에서 보안 이슈가 발생할 수 있다.

기존 연구에서 사물 인터넷에 적합한 접근 제어를 위해 토큰을 이용하여 인증 및 권한 관리를 하고 모든 작업을 분산 원장 형태로 공유할 수 있는 기술을 제안하였으며[2,3], 본 연구에서는 이기종의 IoT 서비스에서 공유 가능한 접근 제어를 위해 스마트 컨트랙트(Smart Contract)를 사용하고자 한다.

스마트 컨트랙트는 접근 권한 토큰 발급, 서비스 및 리소스 접근 수행을 위해 사용되며 탱글네트워크의 분산 원장에 트랜잭션으로 저장, 공유된다.

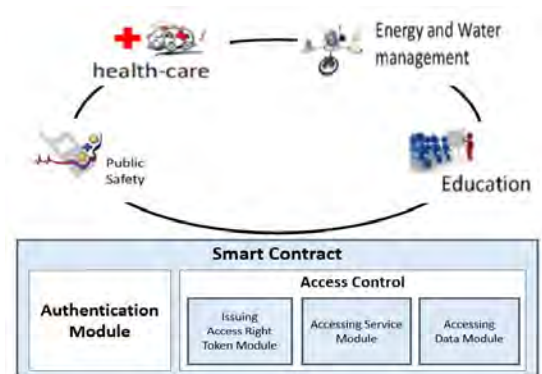
본 연구를 통해 이기종의 다양한 사물인터넷 서비스들이 탱글 네트워크를 통해 스마트 컨트랙트를 공유함으로써, 중앙 제어 없이 IoT 데이터 접근이 안

전하게 이루어질 수 있다.

2. 스마트 컨트랙트를 사용한 IoT 서비스 접근 제어 설계

2.1 IoT 서비스 접근 제어 시스템 구성

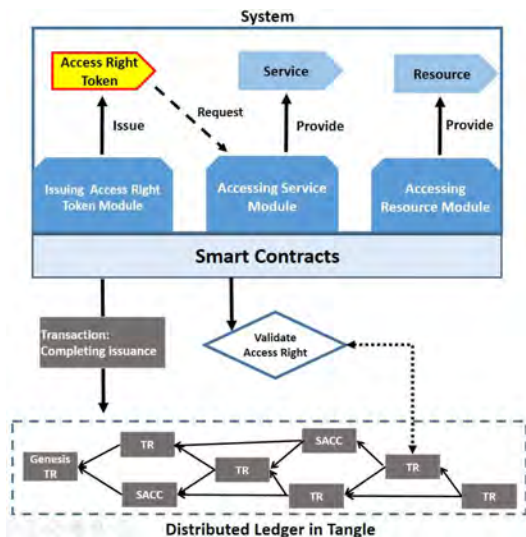
본 논문에서는 IoT 서비스에 대하여 토큰 기반의 접근 제어를 수행하고 탱글 및 스마트 컨트랙트를 이용하여 분산화된 접근 제어를 수행하는 시스템을 제안하고자 한다. 이기종의 IoT 서비스에서 Smart Contract를 이용하여 접근 제어를 수행하는 시스템의 구성도는 (그림 1)과 같다.



(그림 1) 시스템 아키텍처

본 시스템은 IoT 서비스를 제공하기 위하여 다음과 같은 접근 제어 과정을 수행한다.

- i. 접근 제어에 대한 정책을 스마트 컨트랙트로 정의한다.
 - ii. 탱글의 분산 원장에 스마트 컨트랙트를 트랜잭션으로 저장하여 공유한다.
 - iii. 공유한 스마트 컨트랙트를 기반으로 토큰을 발급함으로써 접근 권한을 부여하고 토큰에 대한 발급 사실을 원장으로 공유한다.
 - iv. 발급한 토큰을 통하여 주체 기반의 접근 제어를 수행하여, 사물 인터넷 서비스에 대한 접근 제어를 수행한다.
- 접근 제어 수행을 위해 (그림 2)와 같이 모듈을 구성한다.



(그림 2) 시스템 모듈 구성도

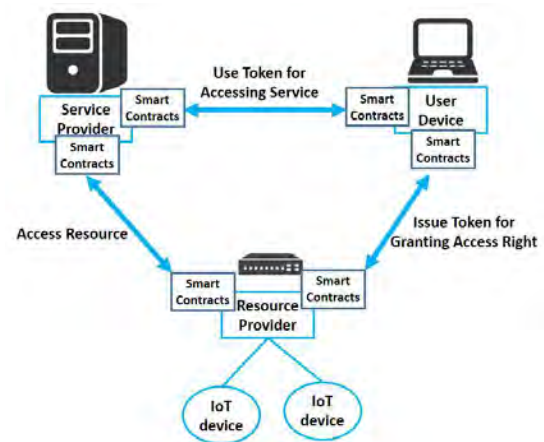
접근 권한 토큰 발급 모듈에서는 스마트 컨트랙트를 이용하여 접근 권한 토큰을 발급함으로써 접근 권한을 부여한다.

서비스 및 리소스 접근 모듈에서는 스마트 컨트랙트를 이용하여 토큰에 대한 검증을 수행함으로써 서비스에 대한 접근 제어를 수행한다.

본 시스템에서는 토큰 발급에 대한 트랜잭션을 생성하여 발급 사실을 원장으로 공유한다. 원장으로 공유함으로써 다른 노드들은 토큰 검증을 위해 발급자에 요청을 수행하지 않고 토큰을 검증할 수 있다. 또한 한번 발급된 토큰을 재사용할 수 있으므로 반복적인 권한 부여 과정을 수행하지 않아 접근 제어 프로세스를 최소화 할 수 있다[2].

IoT 서비스 접근 제어 시스템은 (그림 3)와 같이 서비스 제공자, 리소스 제공자, IoT 디바이스, 유저

디바이스로 구성한다. IoT 디바이스를 제외한 나머지 노드들은 접근 권한 토큰에 대한 트랜잭션을 공유하며, 트랜잭션을 저장하기 위한 각자의 Wallet을 소유한다.

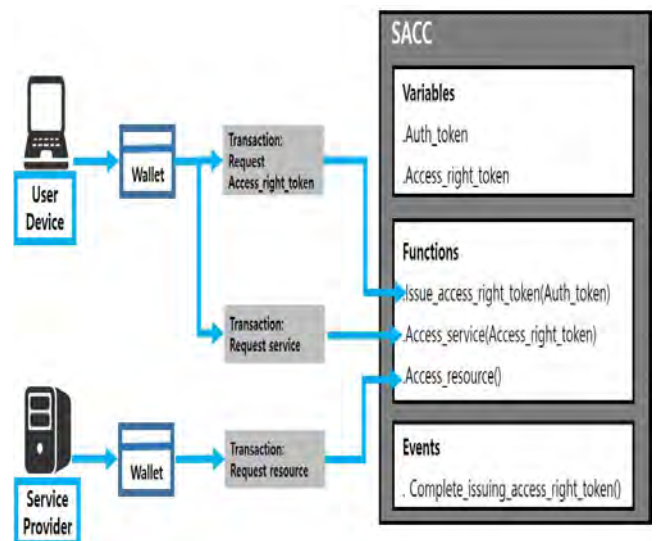


(그림 3) 서비스 구성도

2.2 서비스 접근 제어 컨트랙트(SACC, Service Access Control Contract)

본 논문에서 스마트 컨트랙트는 IoT 서비스를 이용하고자 하는 주체와 IoT 서비스 데이터를 제공하는 객체 사이에 접근제어를 수행하기 위해 인증 및 권한 부여를 위한 디지털 계약으로 정의하며, 서비스 접근 제어 컨트랙트(SACC, Service Access Control Contract)라고 명명하였다. SACC는 디지털 계약을 위한 함수들, 데이터, 각 스마트 컨트랙트간 메시지 전달을 위한 인터페이스 및 이벤트로 구성하였다.

본 논문에서 IoT 서비스 접근 제어를 위해 정의한 SACC의 구조는 (그림 4)와 같다.



(그림 4) SACC 구조

IoT 서비스 시스템에서 접근 제어를 위한 SACC의 주요 함수는 다음과 같다.

- **Issue_access_right_token()** : 요청자의 인증 토큰을 파라미터로 입력받아 디바이스의 접근 권한 요청을 처리하여 접근 권한 토큰을 발행하는 함수이다. 인증 토큰에 대한 무결성 및 유효성을 검증하여 실패시 해당 요청을 거부하거나, 성공시 해당 유저 디바이스에게 접근 권한 토큰을 생성하여 송신한다.
- **Access_service()** : 요청자의 접근 권한 토큰을 파라미터로 입력받아 유저 디바이스의 서비스 요청을 처리하는 함수이다. 접근 권한 토큰의 생성자가 서비스에 대한 리소스를 소유하고 있는 리소스 제공자임을 확인하고 무결성을 확인한 다음, 원장에서 해당 토큰에 대한 발급 사실을 확인함으로써 유효성 검증을 수행한다. 검증이 실패하였을 경우, 해당 접근 요청을 거부한다. 검증이 성공하였을 경우에는 리소스 요청에 대한 트랜잭션을 생성하고 송신함으로써 **Access data()**를 호출한다. 인가된 유저 디바이스가 서비스를 요청했음을 전달하고 서비스에 필요한 리소스를 요청하여 수신한다. 또한 수신한 리소스를 이용하여 해당 유저 디바이스에게 서비스를 제공한다.
- **Access_resource()** : 서비스 제공자의 리소스 요청을 처리하는 함수이다. 요청을 수신한 리소스 제공자는 서비스에 필요한 리소스를 서비스 제공자로 송신한다.

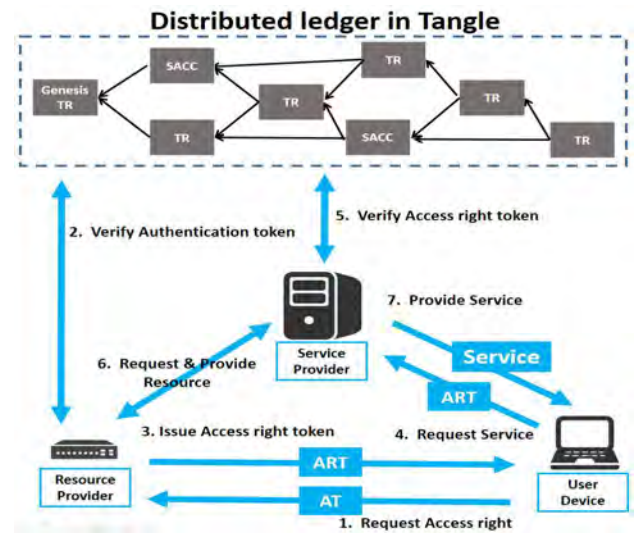
SACC는 컨트랙트의 수행 이후 발생 가능한 이벤트(Events)를 정의한다. SACC에서 이벤트는 컨트랙트의 함수를 수행한 다음, 함수 수행 결과에 대한 트랜잭션을 생성하여 다른 노드들에게 송신하는 기능을 갖는다.

SACC에서 정의한 이벤트는 다음과 같다.

- **Complete_issuing_access_right_token()** : 이 이벤트는 **Issue_access_right_token()**를 수행하여 접근 권한 토큰을 정상적으로 발급하였을 경우에 수행된다. 토큰 발급 완료에 대한 트랜잭션을 생성하여 시스템 노드들에게 송신함으로써 발급 사실을 노드들과 공유한다.

2.3 SACC를 사용한 IoT 서비스 접근 제어 프로세스

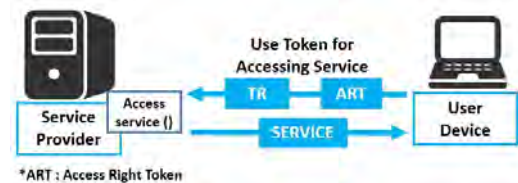
SACC를 사용하는 IoT 서비스 접근 제어의 전체적인 흐름도는 (그림 5)와 같다.



(그림 5) IoT 서비스 접근 제어 프로세스

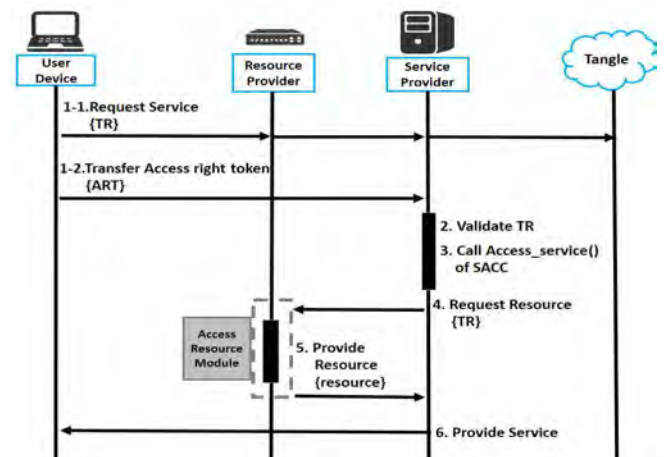
본 논문에서는 IoT 서비스 접근 제어 시스템 모듈 중 서비스 접근 모듈에서 정의된 SACC를 사용하는 과정을 설명한다.

유저 디바이스는 서비스 제공자에게 소유하고 있는 리소스에 대한 접근 권한을 증명함으로써 서비스를 요청하여 이용할 수 있다. 서비스 요청 프로세스는 (그림 6)과 같다.



(그림 6) 서비스 요청 프로세스

유저 디바이스는 소유하고 있는 접근 권한 토큰을 이용하여 서비스 제공자에게 서비스를 요청할 수 있다. 서비스 요청 프로세스의 절차는 (그림 7)과 같다.



(그림 7) SACC를 사용한 서비스 요청 프로세스 절차

참고문헌

- [1] Y.Zhang, S.Kasahara, Y.Shen, X.Jiang and J.Wan, "Smart Contract-Based Access Control for the Internet of Things", IEEE Internet of Things Journal, Vol. 6, No. 2, April, 2019.
- [2] Hwan Park, Mi-sun and Jae-hyun Seo, "Token-based IoT access control using distributed ledger", Journal of The Korea Institute of Information Security & Cryptology, Vol. 29, No. 2, pp.377-391, 2019.
- [3] Hwan Park, Mi-sun Kim and Jae-hyun Seo, "Token-based Rights Management Using IoT Blockchain", CISC-W18, 2018.
- [4] I. Karamitsos, M. Papadaki, N. Baker Al Barghuthi, "Design of the Blockchain Smart Contract: A Use Case for Real Estate", Journal of Information Security, No. 9, pp. 177-190, 2018.

유저 디바이스는 서비스를 이용하기 위해 접근 권한 토큰 사용 요청에 대한 트랜잭션을 생성하여 시스템 노드들에게 송신한다. 또한 서비스 제공자에게 소유하고 있는 접근 권한 토큰을 송신함으로써 서비스 요청을 수행한다.

서비스 제공자는 수신한 트랜잭션에 대한 전자서명을 검증한다. 트랜잭션에 대한 검증이 완료되면, 서비스 제공자는 소유하고 있는 Wallet에서 SACC를 불러오고 서비스 접근에 대한 함수인 Access_service()를 호출한다.

Access_service()를 통해 수신한 접근 권한 토큰에 대한 전자서명을 검증하여 리소스 제공자가 발급했음을 확인한다. 소유하고 있는 원장에서 해당 접근 권한 토큰의 ID를 조회하여 비교함으로써 발급 사실 여부를 확인함으로써 검증을 수행한다. 검증이 실패하였을 경우 프로세스를 중단한다. 검증이 성공하였을 경우, 서비스 제공자는 서비스를 요청한 유저 디바이스에게 서비스를 제공함으로써 프로세스를 완료한다.

3. 결론

본 논문에서는 이기종 IoT 서비스의 접근제어를 위하여 스마트 컨트랙트를 이용하여, 접근 제어 토큰 발행 및 사용 관리 정보를 공유할 수 있는 시스템을 설계하였으며, 시스템 구성 및 SACC 구조를 정의하였다. 또한 IoT 서비스 접근 제어 시스템 모듈 중 서비스 접근 모듈에서 정의된 SACC를 사용하는 과정을 제시하였다.

추후 상세 아키텍처 설계 및 시스템 구현에 대한 연구를 진행하고자 한다.

Acknowledgement

본 논문(연구)은 교육부의 재원으로 이공분야기초연구사업의 지원을 받아 수행된 연구임 (No. NRF-2018R1D1A1B07051203).

보안 하드웨어 모니터링 기법에 관한 연구

김현준*, 조명현*, 장지원*, 오현영*, 백윤홍*

*서울대학교 전기·정보공학부, 반도체공동연구소

hjkim@sor.snu.ac.kr, mhcho@sor.snu.ac.kr, jwchang@sor.snu.ac.kr, hyoh@sor.snu.ac.kr,
ypaek@sor.snu.ac.kr

A Survey on Hardware Monitoring Technique for Security

Hyun-Jun Kim*, Myung-Hyun Cho*, Ji-Won-Chang*, Hyun-young Oh*,
Yun-Heung Paek*

*Dept. of Electrical and Computer Engineering and Inter-University
Semiconductor Research Center (ISRC), Seoul National University

요 약

본 논문에서는 시스템이 비정상적인 상태에 진입하였는지를 판단하여 공격에 대한 탐지를 효율적으로 수행할 수 있는 하드웨어 기반 보안 모니터링 기술에 대해 소개한다. 먼저 이벤트 기반으로 커널을 보호하는 모니터링 기법들에 대해 알아볼 것이다. 최종적으로 다양한 이벤트를 유연하게 모니터링할 수 있는 기법을 살펴보고, 이를 바탕으로 보안 하드웨어 모니터링 기법의 향후 연구방향을 모색하고자 한다.

1. 서론

4차 산업시대를 맞이하게 되면서 빅데이터, 인공지능, 클라우드와 같은 첨단 디지털 기술들이 다발적으로 개발되고 이들을 활용한 서비스들이 널리 제공되고 있다. 이 기술들이 발전함에 따라 충분한 컴퓨팅 파워를 제공할 수 있는 디바이스에 대한 수요가 증가하고 있다. 또한 이러한 디바이스들에 대한 공격 위협 또한 점점 커지고 있다.

모니터링 기법은 이러한 디바이스들에 대해 보안을 제공해줄 수 있는 효과적인 솔루션이다. 모니터링 기법은 감시의 대상이 되는 디바이스로부터 얻어낸 정적/동적 정보를 활용해서 시스템이 비정상적인 상태에 진입하였는지를 확인하고, 시스템 관리자 혹은 보안 정책에 의해 시스템의 정지 또는 정상적인 상태로의 복구를 시도할 수 있다.

소프트웨어 기반 모니터링 기법 중 대표적인 방식으로는 가상화 머신 모니터(VMM)를 활용하여 시스템을 감시하는 기술이 있다. 가장 상위층에 있는 모니터링 엔진이 하위 계층의 게스트 운영체제의 동작을 감시하며 시스템의 상태를 체크한다. 하지만 이 방식은 여러 가지 단점을 가지고 있다. 첫 번째는 VMM도 소프트웨어이기 때문에 취약점을 가지고 있다는 문제가 있다. 가상머신의 취약점에 의해 정

상적으로 동적 정보를 추출하지 못하거나 모니터링 엔진이 공격당할 수 있다. 두 번째로 악성 행위를 일으키는 프로그램이 가상 환경을 인식하여 모니터링을 회피할 가능성이 있다. 마지막으로 소프트웨어 기반 방식이기 때문에 오버헤드가 크다는 단점이 있다.

하지만 하드웨어 방식 모니터링 엔진은 운영체제와 격리되어 있어 물리적인 공격이 아닌 한 공격당하기 힘들며, 모니터링 엔진이 존재하는지 알 수 없다. 그리고 별개의 하드웨어를 사용하므로 오버헤드가 거의 없다. 따라서 하드웨어 기반 모니터링 솔루션은 효율적으로 타겟 디바이스에 보안을 제공해 줄 수 있다.

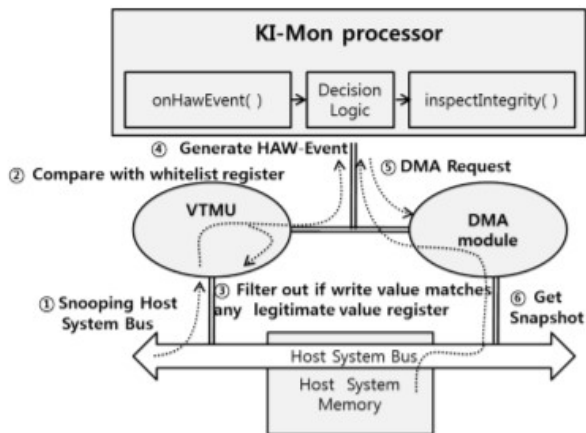
본 연구에서는 이러한 보안 하드웨어 모니터링 기법들에 대해 살펴보고, 이를 기반으로 향후 보안 하드웨어 모니터링 기법의 방향을 모색하고자 한다.

2. 보안 하드웨어 모니터링 기법

2-1. KI-Mon [1]

본 기법은 시스템에 영향을 미칠 수 있는 동작에 대해 이벤트를 생성한 다음, 하드웨어 로직으로 분석하여 커널이 비정상상태인지를 확인한다. 그 대상은 커널 내 특정 오브젝트가 메모리 내에서 변경될

경우 그 쓰기 주소와 변형(mutation)된 값을 이벤트로 형성한다. 일차적으로 화이트리스트 기법을 사용하여 커널 내 불변 오브젝트 (invariant)가 변경되었는지 확인한다. 그 외의 변형 가능한 자료 구조에 대해서는 콜백 검증 (callback verification)을 호출하여 문맥적(Semantically)으로 올바른 변형인지를 소프트웨어적으로 체크한다. 이를 위해 변경되는 값들을 전용 메모리에 기록해두고 이를 가속기로 해싱한 값을 제공하여 문맥을 파악할 수 있게 해준다. 모니터링에 사용되는 메모리의 버스 트래픽은 VTMU (Value Table Managment Unit)을 통해 하드웨어적으로 모니터링하고, 필요할 때에만 이벤트를 생성하여 적은 오버헤드로 모니터링이 가능하다. 해당 연구는 하드웨어를 활용하여 고속으로 커널 내 오브젝트를 모니터링하고, 콜백을 통해 유연하게 복잡한 추가 검증을 수행할 수 있다는 점에 의의가 있다.



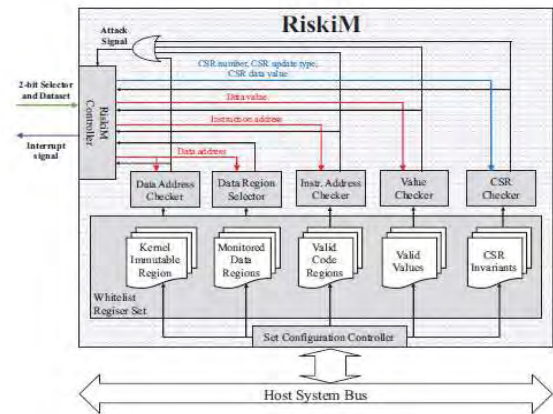
(그림 1) KI-Mon 동작 흐름도

2-2. RiskiM [2]

본 기법은 오픈 소스로 공개된 RISC-V 프로세서를 수정하여 코어 내부 정보를 추출해낼 수 있는 인터페이스를 구축하고, 코어 외부의 모니터링 엔진을 통해 커널이 비정상상태인지를 확인하고, 커널의 무결성을 보장한다.

모니터링에 필요한 정보를 얻으면서도 RISC-V, 소프트웨어 스택과의 호환성을 보장하기 위해 코어의 RTL 코드를 최소한으로 수정하였다. 이를 통해 추가한 인터페이스에서는 메모리 쓰기에 대해 명령어 주소, 데이터 주소, 데이터 값을 추출하고, 코어 내부 정보를 저장하는 CSR 값의 변화할 경우 CSR 숫자, 업데이트 타입, CSR 값을 추출해낸다. 이들이 묶여서 데이터 셋의 형태로 코어 외부로 전달되고, 외부의 모니터링 엔진에서는 주소, 값에 대한 전용 검증 모듈이 있어 이들에 대한 검증을 순서대로 수

행한다. 해당 연구는 기존에 존재하던 Intel PT, ARM PTM와 같은 디버그 인터페이스에 의존하지 않고, RISC-V를 조금 수정하여 전용 인터페이스를 추가하여 기존에 사용하지 못하던 코어 내 정보를 추출하여 모니터링을 수행할 수 있는 엔진을 개발했다는 점에서 그 의미가 있다.

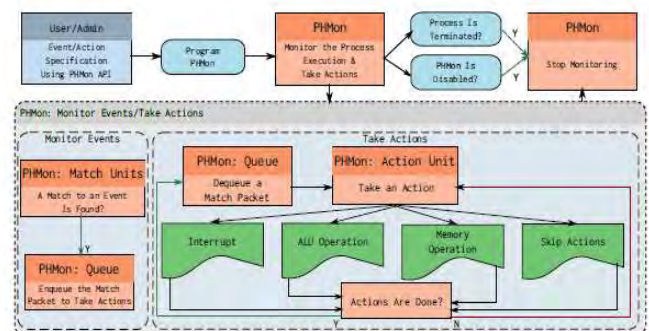


(그림 2) RiskiM 구조

2-3. PHMon [3]

본 기법은 이벤트를 여러 개의 모니터링 룰(rule)과 행동 (action)의 집합으로 나타낸다. 추출한 동적정보에 룰을 적용하여 이벤트를 인식하고, 이에 대응되는 행동을 수행하는 프레임워크를 개발하였다.

본 모니터링 엔진은 RISC-V 코어를 수정하여 명령어 트레이스를 얻을 수 있다. 이에 는 명령어, 주소, 데이터 값, 인터럽트, 메모리 리퀘스트 등의 다양한 정보들을 포함하고 있다. 또한 Linux OS를 수정하여 각 프로세스에 대해 다양한 보안 정책을 적용할 수 있다. 해당 프레임워크를 통해 커널과 같은 시스템의 무결성을 보장하는 것도 가능하며, 가속화된 퍼징 (Fuzzing), 디버깅 (Debugging)에도 사용 가능하다. 해당 연구는 코어 내 내부 정보를 하드웨어적으로 특정 룰과 매칭시키고 이에 대응되는 행동을 정의하여 다양한 보안 정책을 적은 오버헤드로 구현했다는 점에서 의미가 있다.



(그림 3) PHMon 동작 흐름도

3. 차후 하드웨어 모니터링 연구 방향

모니터링에 필요한 정보를 추출하고 사용하는 부분에 있어서 충분히 많은 연구가 진행되어 왔다. 하지만 이 정보를 통해 시스템의 비정상적인 시스템을 진단하는 방식은 대부분 화이트리스트 방식에 치중되어 있어 이에 대한 더 많은 연구가 필요하다.

이에 대한 솔루션으로 머신러닝을 들 수 있다. 머신러닝을 사용하면 여러 이벤트들의 패턴을 좀 더 추상화된 벡터 형태로 추출해낼 수 있고, 해당 벡터를 사용해 특정 보안 태스크를 수행하는 모델을 생성할 수 있다. 또한 머신러닝은 하드웨어 기술을 통해 가속을 할 수 있기 때문에 효율적으로 하드웨어 모니터링을 수행할 수 있을 것으로 예상된다.

4. 결론

본 논문에서는 보안 하드웨어 모니터링 기법을 다룬 3개의 연구를 살펴보고, 각각의 논문에서 어떤 방식을 통해 하드웨어 기술을 모니터링에 사용했는지 알아보았다. 차후의 연구에서는 정보를 추출하고 처리하는 것뿐만 아니라 이를 활용해 어떻게 시스템의 비정상적인 상태를 진단하거나 기타 보안 목적의 기능을 수행할 수 있는지가 중요할 것이다.

5. Acknowledgement

본 연구는 2020년도 정부(과학기술정보통신부)의 재원으로 한국연구재단 (NRF-2017R1A2A1A17069478), 2020년도 두뇌한국21플러스사업, 2020년도 정부 과학기술정보통신부의 재원으로 정보통신기술진흥센터 (No.2017-0-00213, 능동적 사전보안을 위한 사이버 자가변이 기술 개발)의 지원을 받아 수행된 연구임.

참고문헌

- [1] Lee, Hojoon, et al., "Ki-mon: A hardware-assisted event-triggered monitoring platform for mutable kernel object", USENIX Security Symposium, Washington D.C., U.S.A, 2013
- [2] Hwang, Dongil, et al., "RiskiM: Toward Complete Kernel Protection with Hardware Support", DATE, Florence, Italy, 2019
- [3] Delshadtehrani, Leila, et al. "PHMon: A Programmable Hardware Monitor and Its Security Use Cases", USENIX Security Symposium, 2020

Open IDS 및 CVE 기반의 OpenIOC가 결합된 CTI 프레임워크 설계

윤경찬, 유지훈, 신동일, 신동규
세종대학교 컴퓨터 공학과

keoungchan@gamil.com, yoojihoon@sju.ac.kr, dshin@sejong.ac.kr, shindk@sejong.ac.kr

Design of CTI framework that combines Open IDS and CVE based OpenIOC

Keoungchan Yoon, Jihoon Yoo, Dongkyoo Shin

*Dept. of Computer Engineering, Se-jong University

요 약

정보통신 기술의 발달로 무분별한 사이버 공격에 노출되어 있기 때문에 정보보안의 기술이 중요해지고 있다. 이중 침입 탐지 시스템은 방화벽과 더불어 시스템 및 네트워크 보안을 위한 대표적인 수단으로, 현재까지 네트워크 기반인 NIDS와 호스트 기반인 HIDS에 대한 많은 연구가 이루어졌다. 이러한 침입탐지에 대한 CTI(Cyber Threat Intelligence)를 공유하기 위해 다양한 CTI 프레임워크를 사용하여 CTI 정보를 공유하는 연구가 진행되고 있다.

이에 본 논문에서는 CVE기반의 OpenIOC와 Snort 및 OSSEC에서 생성된 Raw Data를 결합하여 새로운 CTI 프레임 워크를 제안한다. 제안된 시스템을 테스트하기 위해서는 CVE 분석을 기반으로한 Kali Linux로 공격을 진행한다. 이를 통해 생성된 데이터는 시간이 지남에 따라 축적된 데이터를 저장 및 검색을 위해 대규모 분산 처리 시스템과도 결합이 필요할 것으로 예상되며 추후 딥러닝 기술을 활용하면 지능형 지속 위협을 분석하는데 용이할 것으로 예상된다.

1. 서론

전 세계적으로 인터넷이 활성화 된 21세기는 정보통신 기술의 발달로 무분별한 사이버 공격에 노출되어 있기 때문에 정보보안기술이 더욱 중요해지고 있다. 이에 따라 정보보호 서비스 및 보호 기술에 대한 수요가 확대되고 있으며, 이중 침입탐지 시스템(IDS, Intrusion Detection System)은 방화벽(Firewall)과 더불어 시스템 및 네트워크 보안을 위한 가장 대표적인 수단이다. 침입 탐지 시스템은 네트워크 기반의 NIDS(Network based Intrusion Detection System)와 호스트 기반인 HIDS(Host based Intrusion Detection System)으로 구분되며, NIDS의 경우 네트워크 공격인 DoS, Port Scan 등의 네트워크 트래픽 공격 탐지와 관련해서 많은 연구가 주를 이룬다 [1, 2]. 이에 반해 호스트 기반의 HIDS는 시스템 내부에서 발생하는 시스템 호출, 이벤트 로그 등의 시스템 내부 행위 및 로그에 대한 분석을 통해 이상 여부를 탐지한다. 이와 더불어 사이버 공격에 대한 위협정보를 공유하기 위해

CTI(Cyber Threat Intelligence)플랫폼을 사용하여 최신의 공격과 기존 운영 체제의 취약성에 관련된 위협 정보를 수집 및 분석하여 공유하는 연구가 진행되고 있다 [3].

본 논문에서는 Raw Data와 OpenIOC가 결합된 CTI 프레임워크를 제안한다. 이 프레임워크는 CVE(Common Vulnerabilities and Exposures)기반의 OpenIOC와 연관된 오픈 IDS(Snort, OSSEC) 규칙을 설정하고, 해당 원시(Raw) 데이터를 생성하기 위해서 위협 도구로 Kali Linux를 사용한다.

2. 관련 연구

Satyendra Kumar Patel, Abhilash Sonker 는 네트워크 보안을 개선하기 위해 규칙 기반의 Snort을 제안하였다. 해당 연구에서는 Port Scan 공격을 실시간을 감지하기 위해 자체적으로 EPSDR(Efficient Port Scan Detection) 규칙을 생성하였다. 이러한 새로운 EPSDR 기반 IDS는 새로운 오탐을 줄이는 데 좋은 성과를 달성했다 [4].

RaviTeja Gaddam ,Dr. M. Nandhini는 Snort를 통해 생성된 대량의 트래픽을 처리하기 위하여, 여러 가지 문제를 극복하기 위해 즉각적인 정보에 반응하는 계층 기반 설계를 구상하였다. 이 설계를 통합하기 위하여 Snort 코드를 재구성 한 다음 Kali Linux 환경에 수정된 Snort를 배포하여 성능 평가를 진행하는 방식을 제안하였다 [5].

Guangming Yang 외 3명은 트래픽이 많이 발생하는 네트워크 환경에서 침입 탐지의 효율성을 높이기 위해 시그니처 커스텀 마이징 방법을 제안하였다. 이 방법은 취약성 스캐너, 상태보고서, 서명 선택, 호스트로 구성되고 CVE번호 선택과 포트 선택의 방식으로 구성된다. 해당 연구에서는 불필요한 경고를 줄이고 탐지 효율을 향상시킨 것을 볼 수 있었다 [6].

3. CTI 프레임워크 구성

본 연구에서 제안한 CTI 프레임워크 구성은 그림 1에 나타내었으며, 핵심 어플리케이션은 아래에서 설명한다. CVE기반의 OpenIOC와 연관된 공개 IDS(Snort, OSSEC) 규칙을 설정하고, 해당 원시 데이터를 생성하기 위해서 위협 도구로 Kali Linux를 사용하며, 원시 데이터 및 관련정보를 Anomali STAXX에 축적하여 CTI Feed를 구성한다.

3.1 CVE (Common Vulnerabilities and Exposures)

CVE는 알려진 취약점을 식별하는 방식을 표준화하는 것으로 표준 ID를 통해 다양한 CVE 정보 소스에서 특정 위협에 대한 기술적 정보를 찾아 활용

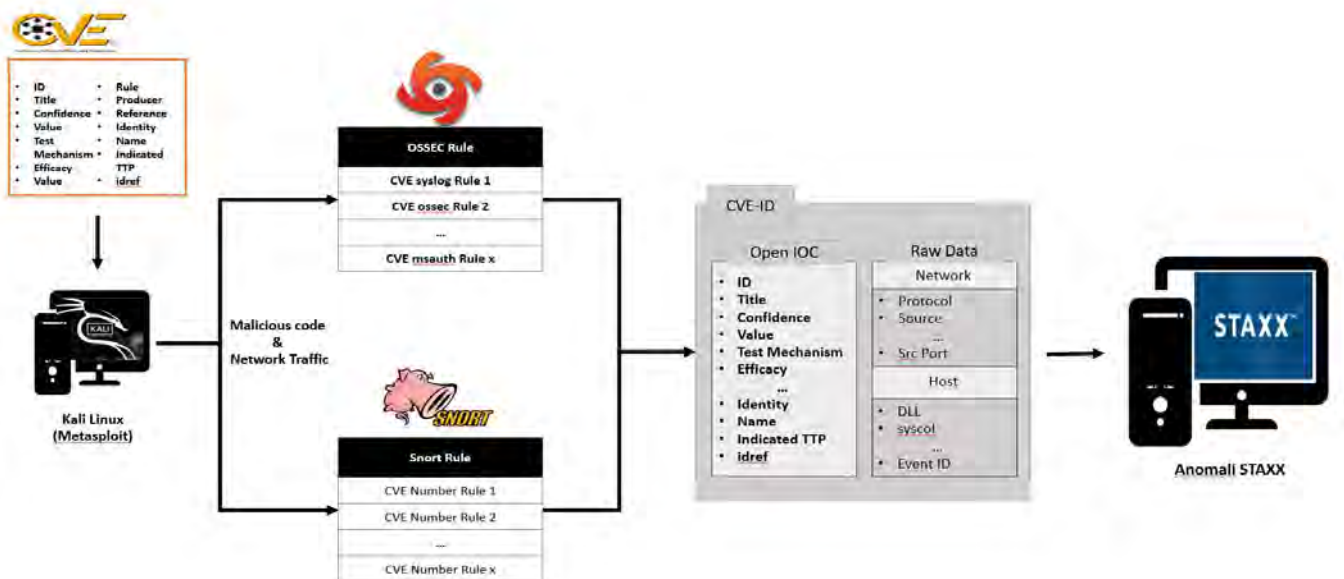
하는데 사용한다. CVE의 구성요소를 그림 2에 나타내었다. 본 논문에서는 Snort와 OSSEC에서 나온 RAW데이터와 CVE 기반의 OpenIOC를 매핑시키는 것이 목표이다.



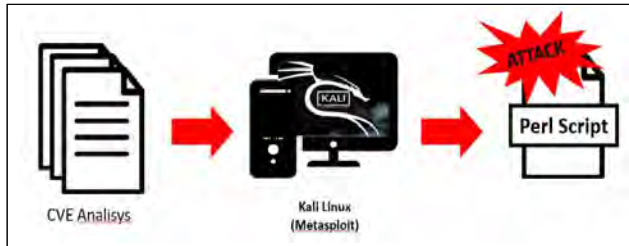
(그림 2) CVE 구성요소

3.2 Kali Linux(Metasploit)

Kali Linux는 침투 테스트를 위해 만들어진 데비안 계열의 리눅스로, 취약점과 관련한 모든 메타 데이터를 관리하는 프레임워크인 MetaSploit를 통해 보안 취약점 분석에 많이 사용된다. 본 연구에서는 이 MetaSploit 및 Perl Script기반의 취약점 공격을 통해 Open IDS에 원시 데이터를 생성하는데 사용한다. 그림 3은 Kali Linux의 취약점 공격 구조를 나타낸다.



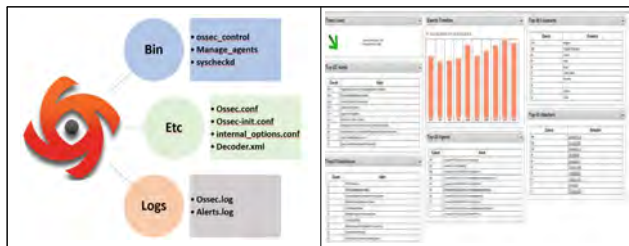
(그림 1) 제안된 프레임 워크 흐름도



(그림 3) Kali Linux의 취약점 공격 구조

3.3 OSSEC (Open Source HIDS Security)

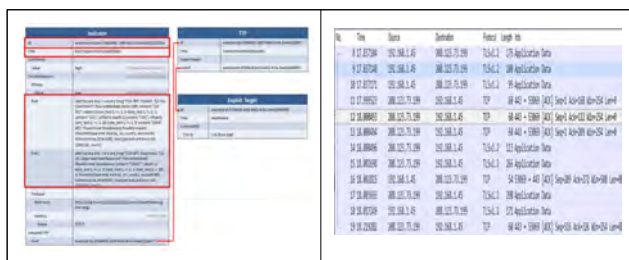
OSSEC는 오픈 소스 기반의 호스트 침입탐지 시스템이다. OSSEC는 로그를 분석 가능한 로그 분석 엔진이 있고, 중앙 집중식 아키텍처로 구성된 플랫폼이기 때문에 여러 시스템을 관리하기 용이하다. 본 연구에서는 호스트 기반 침입 탐지에서 발생할 수 있는 원시 데이터를 CVE와 매핑시키는 것이 목적이다.



(그림 4) OSSEC 구성요소

3.4 Snort

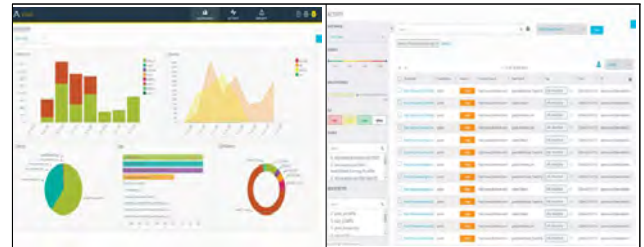
Snort는 실제 취약점 탐지를 기반으로 하고 IP 네트워크에서 프로토콜 분석 실시간 트래픽 분석 작업을 수행하여 다양한 공격을 탐지하는 네트워크 기반의 침입 탐지 시스템이다. 본 연구에서는 Snort Rule을 활용해 CVE 분석을 기반으로 생성된 Kali Linux의 공격을 스캔하여 축적된 Raw Data와 CVE 기반의 OpenIOC와 매핑을 시키는 것이 목표이다.



(그림 5) Snort Rule

3.5 Anomali STAXX

Anomali STAXX는 STIX/TAXII 서버에 연결하여 위협 피드를 발견 및 구성하고 위협 정보를 폴링 가능하게 한다. 또한 사용자에게 IOC(Indicator of Compromis)연구 도구를 제공한다. 본 연구에서는 CVE 기반의 데이터와 OSSEC 및 Snort가 매핑된 데이터를 Anomali STAXX에 정보를 축적하여 CTI Feed를 구성하는 것이 목표이다.



(그림 6) Anomali STAXX

4. 결론

본 연구를 통해서 OSSEC 및 Snort에서 생성된 Raw Data와 CVE 기반의 OpenIOC를 매핑한 CTI를 축적할 수 있는 프레임 워크를 제안할 수 있었다. 제안된 프레임 워크는 시간이 지남에 따라 축적된 CTI정보들을 처리하기 위해서 대규모 분산 처리 시스템을 통해 효율적인 저장 및 검색을 필요 할 것으로 예상하며, 추후 축적된 데이터를 딥러닝 기술을 이용하여 지능형 지속 위협(APT, Advanced Persistent Threat)을 분석 하는데 활용 가능할 것으로 예상된다.

ACKNOWLEDGMENT

“본 연구는 국방과학연구소의 지원으로 수행되었습니다(위탁연구계약번호:UD200014ED)”

참고문헌

- [1] ROESCH, Martin, et al. Snort: Lightweight intrusion detection for networks. In: Lisa. 1999. p. 229-238.
- [2] SABOOR, Amtul; AKHLAQ, Monis; ASLAM, Baber. Experimental evaluation of Snort against DDoS attacks under different hardware configurations. In: 2013 2nd National Conference on Information Assurance (NCIA). IEEE, 2013. p. 31-37.
- [3] KIM, Eunsoo, et al. CyTIME: Cyber Threat Intelligence ManagEment framework for automatically generating security rules. In:

Proceedings of the 13th International Conference on Future Internet Technologies. 2018. p. 1-5.

[4] PATEL, Satyendra Kumar; SONKER, Abhilash. Rule-based network intrusion detection system for port scanning with efficient port scan detection rules using snort. International Journal of Future Generation Communication and Networking, 2016, 9.6: 339-350.

[5] GADDAM, RaviTeja; NANDHINI, M. An analysis of various snort based techniques to detect and prevent intrusions in networks proposal with code refactoring snort tool in Kali Linux environment. In: 2017 International Conference on Inventive Communication and Computational Technologies (ICICCT). IEEE, 2017. p. 10-15.

[6] YANG, Guangming, et al. Research of intrusion detection system based on vulnerability scanner. In: 2010 2nd International Conference on Advanced Computer Control. IEEE, 2010. p. 173-176.

Binary lifting을 이용한 안드로이드 라이브러리 취약점 분석*

이성원, 윤종희
영남대학교 컴퓨터공학과
noke15@ynu.ac.kr, youn@yu.ac.kr

Android library vulnerability analysis using binary lifting

Sung-Won Lee, Jonghee Youn
Computer Engineering, Yeungnam University

요 약

안드로이드 OS 는 대중적이고 중요한 시스템으로 자리 잡았고, 이에 따른 다양한 연구도 진행 중이다. 본 논문에서는 보안측면에서의 취약점 분석 방법을 제시하여, 각종 보안 위협을 예방하는데 기여하고자 한다. 안드로이드 라이브러리를 대상으로 Binary Lifting 기술을 사용하여 코드기반(LLVM IR) 퍼징을 진행하는, 취약점 분석 과정을 설계 수행한다.

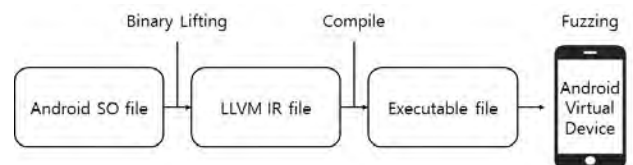
1. 서론

스마트 폰과 IoT제품들 중 안드로이드 시스템은 높은 비중을 차지하고 있으며, 용도에 맞는 다양한 어플리케이션이 등장하고 개발되고 있다. 사용자의 편의를 제공할 뿐만 아니라 핵심적인 역할을 담당하는 만큼 보안사고가 발생했을 경우 개인이나 집단에 매우 치명적일 수 있으며, 이를 방지하기 위한 노력과 연구가 반드시 필요하다. 본 논문에서는 안드로이드 시스템 중 라이브러리를 대상으로 Binary Lifting(본 논문에서는 바이너리를 LLVM IR[1]로 변환하는 과정을 의미한다) 하여 취약점을 발견하고 분석하는 방법을 제안한다.

2. 분석 프로세스 설계

안드로이드 라이브러리를 효율적으로 분석하기 위해 기존의 오픈소스 도구들을 결합하는 방식으로 진행되었다. MCSEMA[2], LLVM, Libfuzzer[3], Android Studio[4] 도구들을 중점적으로 사용하며, 취약점을 찾는 방식으로는 퍼징을 사용한다. 코드가 없는 바이너리 상태인 라이브러리를 LLVM IR 이라는 코드레벨로 변환하고, 이를 통해 소스코드를 사용하는 Libfuzzer로 퍼징 할 수 있게 된다. 그림 1은

전체적인 취약점 분석과정을 나타낸다.



<그림 1> 전체 취약점 분석 과정

각 도구마다 다양한 버전이 존재하고, LLVM과의 의존성 문제도 존재하기에 버전에 따라 각 도구들이 호환이 안 되는 상황이 발생하기도 한다. 본 논문에서 사용하는 환경과 도구의 버전과 표 1 과 같다.

<표 1> 분석에 사용된 환경과 도구의 버전

대상	환경 및 버전
Host	Ubuntu 18.04 x86_64
Guest	AVD - Android Pie x86_64
MCSEMA	LLVM 8
NDK	r21 Ver.
	x86_64 linux android clang

분석 프로세스는 Lifting, Compile, Fuzzing 3단계로 이루어진다.

Lifting 단계에서, 지원하는 도구들은 다양하게 개발되고 있으며, 그 중 안드로이드 시스템을 대상으로 하기에 x86_64 와 aarch64 아키텍처를 지원하

*이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF-2018R1D1A1B07050647)

는 MCSEMA를 사용하였다. MCSEMA에서 Lifting 하는 과정은 바이너리를 대상으로 Control Flow를 뽑고 Lifting 하는 2단계로 거쳐 bc 확장자를 가진 LLVM IR 을 생성한다.

Compile 단계에서, 생성된 LLVM IR 을 다시 실행 파일로 만들기 위해선 Clang이 필요하고, Host PC의 리눅스 환경에서 안드로이드 환경의 실행파일을 생성하기 위해 크로스 컴파일방법을 사용한다. 크로스 컴파일을 지원하는 Android Studio의 Ndk 도구를 사용하여 Guest 환경인 안드로이드 Pie x86_64 에서 실행 가능한 바이너리를 생성한다. r21 Ndk 버전에서 Clang 버전은 9.0.8로 설정되어 있으며, Libfuzzer를 사용하기 위한 옵션으로 -fsanitize=fuzzer,address를 인자로 적용하여 컴파일 한다. 안드로이드 시스템에 대한 또다른 컴파일 방법으로는 AOSP[5]를 사용하여 빌드 후 크로스 컴파일 하는 방법이 있다. 해당 방법의 경우 가장 높은 Clang의 버전이 6 버전으로(AOSP Android Pie 기준) 사용 하는 다른 도구와 LLVM 버전이 다르고, Libfuzzer 관련 라이브러리 또한 지금은 사용하지 않는 Libfuzzer.a를 사용한다.

Fuzzing 단계에서, 생성한 바이너리를 실행시킬 환경으로는 가상머신을 사용한다. Android Studio의 Android Virtual Device(AVD)를 사용하여 안드로이드 Pie x86_64 가상환경을 구축한다. 각 단계를 거쳐 생성된 바이너리를 실행시켜 퍼징을 통한 라이브러리 취약점 분석이 가능하다.

3. 실험 및 결과

실제 스토어에서 다운 가능한 어플리케이션을 대상으로 설계한 취약점 분석 프로세스를 진행하였다.

대상 어플리케이션의 APK파일 내부에서 분석하고자 하는 SO를 추출. 안드로이드 기기에서 작동하는 어플리케이션이라 추출된 SO 파일의 아키텍처는 aarch64로 확인된다. Lifting 후 Compile 과정 중에서 컴파일 되어 나오는 파일은 x86_64시스템으로 변경된다. MCSEMA에서 핵심 과정에 사용하는 라이브러리인 libmcsema_rt가 원인으로 x86, x86_64만 지원하고 있기 때문에 크로스 컴파일 과정 중 x86_64 아키텍처로 컴파일 한다. 다른 아키텍처로 크로스 컴파일 시 컴파일러가 incompatible target 에러를 출력한다.

완성된 실행파일을 AVD 환경에서 실행시키면

Libfuzzer를 사용하여 퍼징, 취약점을 분석한다. 그림 2와 3은 AVD환경에서 실행 했을 때 출력되는 결과 분석의 일부이다.

```
generic_x86_64:/ # /data/local/tmp/...fuzz
==5847==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602c67ff410
WRITE of size 28 at 0x602000000060 thread T0
#0 0x569ea8d87a58 (/data/local/tmp/...fuzz+0xae58)
#1 0x569ea8d45134 (/data/local/tmp/...fuzz+0xc134)
#2 0x569ea8d705b2 (/data/local/tmp/...fuzz+0x975b2)
#3 0x79654d90578c (/system/lib64/libc.so+0xc278c)
```

<그림 3> 취약점 분석 결과 1

```
SUMMARY: AddressSanitizer: heap-buffer-overflow (/data/local/tmp/...fuzz+0xae58)
Shadow bytes around the buggy address:
0x0c047fff7fb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c047fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c047fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c047fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c047fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c047fff8000: fa fa 00 fa fa fa 00 fa fa fa 00 00 fa fa fa fa
0x0c047fff8010: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c047fff8020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c047fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c047fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c047fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
Addressable: 00
```

<그림 2> 취약점 분석 결과 2

실행결과 Heap buffer overflow를 발생시키는 부분을 확인할 수 있다. 실제 어플리케이션에서 해당 라이브러리의 함수를 호출할 때 공격에 대한 방어가 존재할 수도 있지만, 라이브러리의 특성상 이후에도 계속 사용될 가능성이 높기 때문에 라이브러리 자체의 보안 취약점을 개선하는 것이 안전하다.

4. 결론

본 논문에서는 안드로이드 시스템의 라이브러리를 대상으로 하며 Binary Lifting을 통해 Libfuzzer로 퍼징하는 방법을 제안했다. 이러한 방식은 안드로이드 기본라이브러리를 대상으로 진행할 수 있을 뿐만 아니라 소스코드가 주어지지 않은 APK를 대상으로도 코드 기반(LLVM IR) 테스트를 통해 취약점 분석이 가능하다. 안드로이드 어플리케이션이 급증하고 다양한 기능을 위해 자체 제작한 라이브러리들이 포함되기 때문에 본 논문에서 제안하는 방식으로 취약점을 분석하고 개선하여 보안 위협을 줄일 수 있다.

참고문헌

- [1] <https://llvm.org/docs/LangRef.html>
- [2] <https://github.com/lifting-bits/mcsema>
- [3] <https://llvm.org/docs/LibFuzzer.html>
- [4] <https://developer.android.com/studio>
- [5] <https://source.android.com/>

원전 다양성보호계통 사이버보안 테스트베드 설계

정성민*

*한국원자력연구원

smjung@kaeri.re.kr

The Design of a Cybersecurity Testbed for Diverse Protection System in NPPs

Sungmin Jung*

*Korea Atomic Energy Research Institute

요 약

원자력 발전소의 계측제어시스템에 디지털 관련 기술이 적용되면서 사이버보안 위협이 증가하였고, 이에 따라 사이버보안 위협의 대응은 중요한 현안이 되었다. 하지만, 실제 운영중인 원자력 발전소에 침투 시험은 불가능하기 때문에 테스트베드를 구축 및 활용하여 사이버보안 위협을 분석해야 한다. 계측제어시스템의 비안전계통은 디지털 기반의 제어기와 통신망이 사용되기 때문에 안전계통보다 많은 사이버보안 취약점이 존재한다. 본 연구에서는 비안전계통인 다양성보호계통을 위한 테스트베드의 구성과 취약점 확인을 위한 공격, 그리고 대처 방안에 대해 논의한다.

1. 서론

원자력 발전소의 계측제어시스템은 보수적인 특성에 따라 아날로그 기술이 일반적으로 사용되었지만, 최근 디지털 기술이 사용되면서 사이버보안 위협이 증가하였다[1]. 사이버보안 위협에 대한 취약점을 확인하기 위해 계측제어시스템을 대상으로 침투 시험이 필요하지만 운영중인 원자력 발전소에서는 잘못된 결과에 대한 위협이 크기 때문에 직접적인 침투 시험은 불가능하다. 따라서 위협을 분석하기 위해 테스트베드를 이용해야 한다. 테스트베드를 통해 사이버보안 공격의 영향을 간접적으로 확인하고 방화벽이나 암호화 장비와 같은 보안 도구들의 적합성을 평가하여야 한다. 테스트베드를 구축하기 위해 안전과 관련 사항, 설치 비용 및 규모, 그리고 시험의 용이성을 고려하여 비안전계통인 다양성보호계통에 대해 테스트베드의 구성과 시험 및 사이버보안 대응 방안에 대해 논의한다.

2. 다양성보호계통 테스트베드 구성

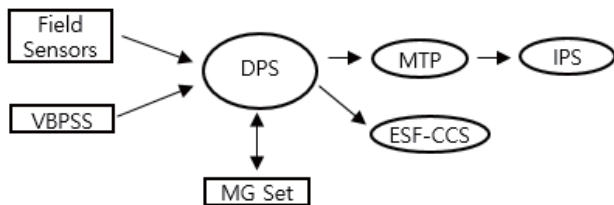
원자력 발전소 계측제어시스템은 기능과 규제 등급에 따라 안전계통과 비안전계통으로 나눌 수 있다[2]. 안전계통은 원자력 발전소의 사고를 방지하고 사고 결과를 완화하기 위한 계통이고, 비안전계통은 원자

력 발전소 운전을 위해 계측, 감시, 제어 기능을 수행하는 계통이다. 다양성보호계통(DPS, Diverse Protection System)은 비안전계통으로 원자로가 정지되어야 할 조건임에도 정지되지 않는 과도상태의 위협을 줄이기 위해, 원자력 발전소의 상태 정보를 입력 받아 설정치와 비교하여 원자로 정지, 터빈 정지, 그리고 보조급수 작동 기능을 수행한다[3].

다양성보호계통은 디지털 기반의 제어기와 통신망이 사용되기 때문에 사이버보안 위협에 취약하고, 안전계통인 원자로보호계통(RPS, Reactor Protection System)과 다양성을 위하여 설계된 계통이기 때문에 사이버보안 공격으로 인한 오작동 또는 간단히 조작된 정보의 입력만으로 원자로 정지와 같은 잘못된 결과를 가져올 수 있다. 따라서 다양성보호계통에 대한 사이버보안의 위협을 분석하여 대응 방안을 마련하는 것은 중요하고 침투 시험이 불가능한 원자력 발전소는 테스트베드를 활용하는 것이 최선의 방법이다. 테스트베드를 이용한 침투 시험을 수행하기 위해 먼저 다양성보호계통의 연계 사항을 파악해야 한다. 그리고 취약한 구간을 선정하여 가능한 취약점을 확인하기 위한 시험을 수행하고 분석된 결과를 바탕으로 사이버보안 위협에 대한 대응을 마련해야 한다.

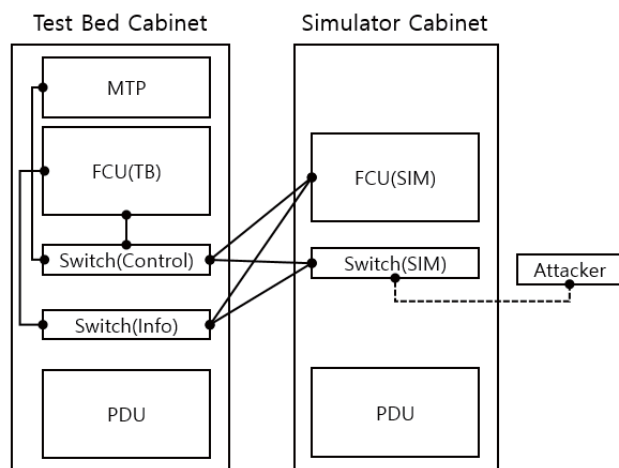
(그림 1)은 다양성보호계통과 다른 계통과의 주요한 연계 사항을 보여준다[4]. 여러 계통과 단방향 또

는 양방향으로 데이터를 송수신 하는데, 일부 구간은 독자적인 통신망이나 아날로그 실배선을 사용하기 때문에 보안상 영향이 거의 없지만 정보처리계통(IPS, Information Processing System)같은 일부 시스템 사이에 디지털 기반의 통신망을 사용하기 때문에 시스템의 취약점이 될 수 있으므로 해당 구간에서 사이버보안 위협을 분석해야 한다.



(그림 1) 다양성보호계통 주요 연계 사항

(그림 2)는 다양성보호계통의 테스트베드 구성을 보여준다. 테스트베드는 테스트베드 캐비닛과 시뮬레이터 캐비닛으로 구성될 수 있다. 다양성보호계통은 센서 데이터 수집과 공정제어 수행을 위해 비안전 제어기인 FCU(Field Control Unit)를 사용한다. 테스트베드 캐비닛에는 MTP(Maintenance and test panel), FCU(Field Control Unit), PDU(Power Distribution Unit), 그리고 제어망, 정보망을 위한 스위치로 구성된다. 시뮬레이터 캐비닛은 타 계통 및 현장 센서의 입력신호를 모사하기 위한 FCU 와 PDU, 그리고 로깅과 시험을 위한 스위치로 구성된다.



(그림 2) 다양성보호계통 테스트베드 구성안

3. 다양성보호계통 취약점 분석

테스트베드를 통해 예상되는 취약점을 확인하여 다양성보호계통의 사이버보안 위협을 분석할 수 있다.

먼저 테스트베드에서 스위치 장비의 취약점을 확인해야 한다. 테스트베드에 정보망과 제어망을 위한 스위치에 보안 기능이 없거나 기본적인 설정만 적용되어 있는 경우에 취약점이 될 수 있다. 스위치 장비에 대해 MAC 플러딩(Flooding)이나 ICMP 리다이렉트(Redirect) 공격을 확인한다. MAC 플러딩의 경우에 변조된 대량의 ARP relay 패킷을 발생시켜 공격 목표인 정보망 또는 제어망 스위치의 MAC 테이블에 오버플로우(Overflow) 공격을 수행하여 패킷을 강제로 플러딩(Flooding)한다. 이후 스위치의 Fail Open 정책에 따라 허브(Hub)와 같은 방식으로 동작하게 된다. 이 취약점은 네트워크에서 스니핑(Sniffing)이 가능하게 하여 운영과 관련한 패킷 정보가 노출될 수 있다. 또한, ICMP 리다이렉트는 공격 목표 IP 주소를 획득하고 이를 공격자의 IP 주소로 변조된 ICMP 리다이렉트 메시지를 브로드캐스트한다. 이 취약점에 의해 다른 네트워크의 제어기기 사이에 송수신 되는 패킷이 노출될 수 있다.

스위치 장비 이외에 디지털 기반의 통신망을 사용하는 FCU(TB)와 FCU(SIM), MTP 와 FCU(TB), 그리고 MTP 와 FCU(SIM) 구간에서 취약점을 확인해야 한다. 즉, 제어기기와 제어기기 간, 그리고 제어기기와 MTP 사이의 데이터 송수신시 해당 구간에서 ARP 스푸핑(Spoofing)과 스니핑(Sniffing)과 같은 취약점을 확인한다. ARP 스푸핑의 경우에 공격 목표인 FCU 또는 MTP의 IP 와 MAC 주소를 파악한다. MAC 주소가 변조된 ARP relay 패킷을 지속적으로 네트워크에 브로드캐스트 하면 공격 대상이 되는 FCU 나 MTP 는 변조된 정보를 이용하여 내부의 ARP 캐시를 업데이트 한다. 이후 해당 정보는 공격자에게 전송되기 때문에 공격 목표의 송수신 패킷을 가로채거나 중간자(MITM) 공격을 통하여 FCU 제어명령 등이 노출될 수 있다. 그리고, 스니핑의 경우에는 무차별(Promiscuous) 모드 혹은 ARP 스푸핑이나 MAC 플러딩을 이용하여 스위치 장비를 오버플로우시켜 패킷을 강제로 플러딩시킬 수 있다. 이 취약점을 이용하여 제어 명령 등 중요 정보를 습득할 수 있다.

4. 결론

원자력 발전소 계측제어시스템의 사이버보안 위협의 분석과 대응을 위해 테스트베드의 구축은 중요하다. 본 논문에서는 비안전계통인 다양성보호계통에서 테스트베드의 구성과 취약한 구간과 대상 및 취약점 확인이 필요한 공격을 알아보았다. 다양성보호계통에서 사이버보안 위협에 대응하기 위해 네트워크 장비에 대한 접근권한 관리, 송수신 데이터의 암호화, 정

적 ARP 테이블 관리, 스위치의 동작상태 확인, VLAN 을 이용한 네트워크 분리, 스위치 보안 설정, ICMP 리다이렉트 기능의 비활성화 등이 사이버보안 위협에 대한 대응 방법이 될 수 있다. 추후 침투 시험 결과와 해당 대응 방법을 분석하여 단방향 통신과 같은 기본적인 보안 대응 방안과 함께 계통에 최적화된 선별적 사이버보안 대응 방안을 마련하고자 한다.

참고문헌

- [1] Seungmin Kim, Gyunyoung Heo, EnricoZio, Jinsoo Shin, Jae-gu Song, "Cyber attack taxonomy for digital environment in nuclear power plants," Nuclear Engineering and Technology, Volume 52, Issue 5, pp.995-1001, 2020.
- [2] 이철권, "원전 계측제어시스템 사이버보안 기술 동향," 한국정보보호학회, 정보보호학회지, 제 22 권, 제 5 호, 2012, pp.28-34.
- [3] 원자력안전위원회규칙 제 24 호, "원자로시설 등의 기술기준에 관한 규칙," 2020.
- [4] Oh, Y.G., Jeong, J.K., Lee, J.J., Lee, Y.H., Baek, S.M., Lee, S.J., "Fault-tolerant design for advanced diverse protection system," Nuclear Engineering and Technology, Volume 45, Issue 6, pp.795-802, 2013.

제53회
2020 온라인 춘계학술발표대회

ICT융합



빅데이터를 통한 약 성분명 처방 활용을 위한 시스템 개발

김한예슬*, 김소연*, 문유진*

*한국의국어대학교 경상대학

e-mail : {khys0079, 201604054, yjmoon}@hufs.ac.kr

System Development for Utilizing Nonproprietary Medicine Name of Prescription through Big Data

Hanyeseul Kim*, Soyeon Kim*, Yoo-Jin Moon*

*College of Economics and Business, Hankuk University of Foreign Studies

요 약

이 논문은 공공 의료 빅데이터를 통해 약 처방 데이터베이스시스템을 구축하고 활용하는 방안을 제시하는 데 목적이 있다. 이를 위하여 약 처방 데이터베이스시스템 이용자가 원하는 목적에 따라 검색하여 처방 성분 별 제품, 기업 정보 및 약국운영 정보를 확인하여 의사결정을 도울 수 있는 데이터베이스 시스템을 구축하였고 정보의 비대칭 문제로 약품 시장에서 불리한 입지에 놓인 수요자 측면의 권익을 향상하는 방안으로 권익 확대 및 정책 방향을 제시한다. 더 나아가 고령인구를 고려한 정책 방향에 대해서도 제안한다.

1. 서론

최근 정부가 국제일반명제도 (International Nonproprietary Names, INN) 도입 방안을 검토하면서 약성분명 처방 제도에 대한 논의가 재 점화되었다. 성분명처방은 의약품의 특정 제약사의 제품명이 아닌 의약품의 일반명칭으로 기재 및 처방하는 것을 말한다. 현재 「의료법」 제 18 조에서 제품명과 성분명 처방 모두 허용되고 있으나, 제품명 처방이 보편화되어 있다. 제품명 처방에서는 의사가 환자가 복용해야 하는 약을 정해주면 약사는 원칙적으로 해당 약만 조제할 수 있다. 해당 약이 없을 경우 대체 조제 제도에 따라 약사가 복제약을 조제할 수 있지만 사전 또는 사후에 의사에게 의무적으로 보고해야 한다. 세계보건기구(WHO)에서도 의료기관이나 제약회사의 변경 등으로 인한 혼란과 의료 과오를 방지할 수 있어 성분명 처방의 중요함을 강조하고 있다.[1] 건강보험 재정부담을 줄이고, 약국마다 수십 종의 동일 성분을 보유해야 하는 불합리성을 개선하여 총 관리비용을 줄일 수 있다. 소비자는 자신이 복용하는 성분을 파악하게 되고, 약품의 선택권이 강화된다. 해외 사례로는 영국은 약 83%(2009 년 기준)가 성분명 처방을 하고 동일 성분으로 분류된 의약품 중 제네릭 의약품 사용을 늘리기 위한 프로그램도 있다. 프랑스에서는 비율 25%이상인 경우 처방 인센티브를 지급하고 있다.[2] 이러한 장점과 추세에도 우리나라에서는 각 단체의 이해관계가 상충하면서 약을 처방 받는 소비자의 권익은 고려되지 않고 있다. 한국의 진료비 중

약품비 차지 비율이 OECD 국가 평균보다 4%나 더 높은 수준이다. [3] 연구도 공급자 측면에서 제도의 실효성에 초점이 맞춰 있다.

본 논문에서는, 성분명 처방 시 소비자들이 약정보에 대한 낮은 인식과 비대칭문제로 겪고 있는 어려움을 완화시키기 위하여 약 처방 데이터베이스시스템 구축을 통해 의사결정에 도움이 되고자 하며 처방전 내역 데이터를 통해 제도의 방향성을 제공하고자 한다. 정보의 비대칭 문제로 약품 시장에서 불리한 입지에 놓인 수요자 측면의 권익을 향상하는 활용방안으로 권익 확대 및 정책 방향을 제시하고자 한다.

2. 관련 공공데이터 및 도구

약 처방 데이터베이스시스템 구축을 위한 데이터의 출처는 건강보험심사평가원의 약제 급여 목록 및 급여 상한 금액표, 의약품 안전성 정보, 국민건강보험공단의 의약품처방정보, 국립중앙의료원의 중앙응급의료센터의 약국 데이터 등 비식별 처리된 공공데이터이며, 이 데이터를 전처리하여 사용하였다.

공공데이터 외에도 Naver Open API 를 이용하여 뉴스 기사를 웹 스크래핑(Web Scraping)을 이용하여 json 형식의 파일을 Jupyter Notebook 과 Python3 을 이용하여 태깅에 맞추어 테이블 형식으로 변환하여 사용하였다. 각 기사 내용에 대한 평가는 <표 1>의 키워드 중심으로 처리하였다. 각 기사 내용에 대한 평가는 키워드 중심으로 분류하여 강한 긍정 2, 긍정 1, 중립 0, 부정 -1, 강한 부정 -2 로 각각 가중치를

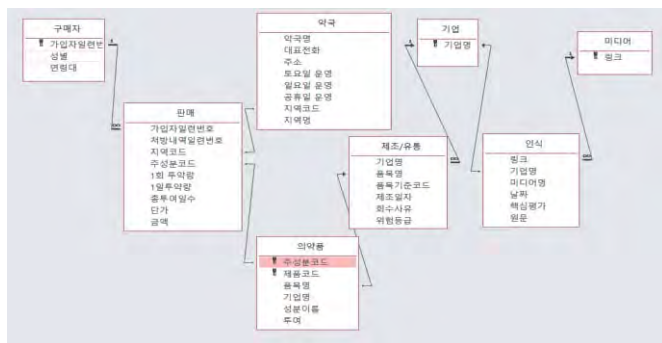
주었다.

<표 1> 스크래핑 데이터 극성 분류 기준

분류	키워드
강한 부정	발암물질, 건강에 치명적, 판매 중지
부정	비교적 덜 심각한 리콜 사유
중립	정보성 뉴스(Public Relation)
긍정	행사 개최, 봉사, 기부, 신약개발 추진
강한 긍정	R&D 실적, 연구논문, 매출 증가

3. 시스템 아키텍처

해당 데이터 세트를 이용하여 약처방 데이터베이스 시스템을 설계하기 위하여 (그림 1)과 같은 Entity-Relation Diagram (E-R Diagram)을 사용하였다.[4][5] 약국, 구매자, 의약품, 판매를 기본 개체로 두고 다른 약국 데이터베이스와 차별화를 두기 위해 제약 기업 개체를 추가하여 기업별 약품의 위험도, 핵심 평가, 이슈를 통해 제품, 성분, 기업을 평가할 수 있고 약국명, 주소, 지역을 통해 약국의 운영 여부 등 다양하고 유용한 정보를 제공하려고 한다, 처방 내역을 바탕으로 특정 연령대의 특징을 파악할 수 있도록 설계하였다.




(그림 1) E-R Diagram

(그림 1)에서 개체와 속성을 설정 한 후 각 개체에 맞는 관계 스키마를 생성, 다대다 (M:N) 관계를 설정한다. 조인 유형은 원하는 데이터형식에 맞게 도출하기 위해 Inner Join, Left Outer Join 과 Right Outer Join 을 활용하였다.

4. 소비자 측에 유용한 약처방 데이터베이스 조회

소비자들이 처방전에 적혀있는 성분 코드를 입력하면 기업, 품목별로 리콜 횃수와 사유, 미디어 종합평가, 위험 등급, 판매량, 금액 등을 조회하고 일목요연하게 비교하여 선택할 수 있다. 회사의 미디어 평가 쿼리를 생성하여 또 다른 쿼리에 중첩하였다. (그림 2)에서는 예시로 해열소염진통제 성분인 텍시부로펜(14230) 주성분코드의 일부인 142 를 입력 한 후 시럽(ASY)과 알약(TAB)중 알약 형태 중 선택 입력하였다. 해당 의약품을 기준으로 기업 개체에 대하여

Left Join 하여 해당 주성분 의약품을 판매한 기업들만 조회되도록 하였고, 처방 기록을 바탕으로 비교하도록 Inner Join 을 교집합하도록 중첩한 후 Right Join 을 이에 중첩하여 안전성 정보 데이터내의 리콜 여부가 없는 기업부분만 반환하도록 하였다. 이 쿼리에서는 안정성이 있는 제품을 가격 비교하고 구매할 수가 있다.



주성분코드	성분이름	기입명	1일 투약 예상액(㎍)
142301ATB	dexibuprofen 0.18g	하원제약	37
142301ATB	dexibuprofen 0.20g	고려제약	37
142301ATB	dexibuprofen 0.21g	안국약품	37
142301ATB	dexibuprofen 0.25g	삼남제약	37
142301ATB	dexibuprofen 0.29g	경보제약	37
142301ATB	dexibuprofen 0.4g	크리스탈생명	37
142302ATB	dexibuprofen 0.15g	안국약품	37
142303ATB	dexibuprofen 0.19g	보령바이오파	42
142303ATB	dexibuprofen 0.22g	안국약품	42
142303ATB	dexibuprofen 0.23a	경동제약	42

(그림 2) 리콜 여부 없는 성분별 기업에 따른 가격 비교

반대로 약품 안정성에서 위험 등급이 있는 성분의 제품을 검색을 하기 위하여, 웹 스크래핑(Web Scraping)으로 모은 미디어 평가를 기업별로 합한 쿼리를 다른 쿼리에 호출하였다. 예를 들어, 텍스부로 쉐 시럽 형태를 입력하여 위와 비슷한 원리를 이용하여 병합하고 종합 평가 시행하였으며 성분, 품목, 기업별 위험등급, 리콜 사유 등을 선택하여 반환하였다. 특정 제품의 회사에 대해서 어느 정도 위험한지 왜 리콜 했는지 알 수 있게 되어 구매 시 유의하게 된다.

[illegible]

(그림 3) 리콜이 있는 회사들의 평가와 해당 제품 성분명 검색

약국 이용에 있어서 처방 받는 사람들 중 오후 늦게 혹은 주말이나 공휴일에 약국 방문이 필요한 소비자들을 위해서, 자신이 원하는 시간, 위치를 선택하여 주말, 공휴일에도 전체 약국 운영시간을 알 수 있도록 설계하였다. 지역명과 지역 코드로 검색하고 와일드 카드를 이용하여 늦은 오후와 공휴일에 운영하는 지와 해당 약국 명, 주소, 전화번호와 함께 공휴

일에 운영하는지 여부를 확인할 수 있었다. (그림 4)에서는 역삼역 코드를 입력하여 공휴일과 주말에 늦게까지 운영하는 약국들만 반환하였다.

역삼약국명	주소	토요일 운영	일요일 운영	공휴일 운영
국약국	서울특별시 중구 명동길 45, 1, 2층 (명동1가)	12:00~22:00	12:00~22:00	12:00~22:00
새원약국	서울특별시 중구 명동길 52, (명동2가)	10:00~22:00	10:00~21:00	11:00~21:00
신세계약국	서울특별시 중로구 중로 1241	09:30~23:00	13:00~21:00	13:00~21:00
태약국	서울특별시 중로구 중로 1991, (중로4가)	09:00~20:00	09:00~20:00	09:00~20:00

(그림 4) 약국 운영 여부 - 공휴일과 주말

5. 취약계층에 유용한 약 처방 데이터베이스 조회

의약품 처방 내역을 바탕으로 어떤 연령대가 가장 많이 처방 받고 지출을 많이 했는지 알아보기 위해 (그림 5)에서 처방자 연령별 비율 비교와 (그림 6)에서 연령별 평균 지출액과 복용량을 비교하였다. 연령별 비율을 백분율(%)값으로 보면 고령자들이 처방한 비율(47%)이 압도적으로 많음을 알 수 있다. 각 연령별 처방 성분별 일평균 지출액수는 60대에서 평균적으로 최소값인 미성년자보다 8 배 이상 많았고 연령대별 평균 총복용량에서도 압도적으로 많이 소비하는 것을 알 수 있었다. 노령인구는 다른 연령 인구에 비해서 약을 많이 처방 받고 지출한다는 것을 알 수 있었다.

미성년자비율	20대비율	30대비율	40대비율	50대비율	60대이상비율
15	7	7	11	13	47

(그림 5) 연령대별 처방 비율

연령	평균 총지출(₩)	평균 총복용량(정)
60대이상	8309	25
50대	4631	17
40대	2891	12
30대	2825	12
20대	1808	12
미성년	1135	19

(그림 6) 연령별 일 평균 지출액과 총 평균 복용량

이 결과는 소비자들의 고령 소비자 권익 강화방안 연구 수행 결과와 성분명 처방을 경험한 비율이 적은 고령소비자의 권익 강화의 필요성을 뒷받침한다.[6] 특히, 만성 질환을 갖고 있고 개인·국가적 부담으로 돌아오기 때문이며 주로 동네 병원을 이용 비율이 높다. 따라서, 의약품 선택권 강화를 위한 정책 대안의 필요성이 커짐에 따라 이와 같은 성분 별 안정성과 가격 비교 가능한 서비스는 더욱 유용할 것으로 기대되어진다.

6. 결론

이 논문에서 구축한 약처방 데이터베이스 시스템은, 다양한 약품 관련 공공데이터의 통합을 통하여 회사 평판, 주성분 코드 검색을 통한 안전한 기업별 주성분, 의약품 리콜 기록, 미디어 평가를 통한

기업이나 품목의 안정성과 심야 및 공휴일에 근무하는 약국 운영 여부를 선택 검색하여 소비자들에게 유용한 의약 정보를 제공할 수 있었다. 즉, 환자가 처방전의 의약품 가격 등 정보로 동일 성분 제품을 스스로 선택할 수 있도록 하는 것뿐 아니라 미디어 평가와 회수에 대한 부가적 정보를 보고 기업을 평가 선택할 수 있도록 소비자에게 선택권을 확대할 수 있는 정보를 제공하고 있다. 또한, 과거 처방 내역을 바탕으로 연령별 처방 내역이 있는 환자들의 특성을 파악하여 소비량과 지출량 모두 가장 많은 연령층은 고령 소비자임을 보여주었고 이를 통해서 고령 소비자들의 선택권을 위하여 정부는 더욱 노력해야 함을 알 수 있다. 특히, 고령소비자들의 의약품 선택권 강화와 함께 의약비 부담 완화에 대한 필요성을 데이터를 통해 고취하며 이와 같은 서비스의 필요성을 제기하고 있다.

이 논문에서 구축한 약 처방 데이터베이스 시스템의 확장성 측면에 있어 앱, 웹개발을 통해서 서비스를 제공할 수 있으며 또한 GPS 를 이용하여 실시간으로 사용자와 약국의 위치를 확인하여 가장 가까운 약국의 운영 정보를 보내어 줄 수 있다. 또한 웹 크롤링을 자동화하여 최신 정보를 의사결정에 활용할 수 있음이 기대된다.

하지만, 기업평가 방법은 발제 되는 기사를 토대로 한 오피니언 마이닝에서 활용하고 있는 극성 분류를 사용하였으므로 기업과 미디어 간의 리베이트 부분이 간과되었다. 따라서 더욱 신뢰성 있는 평가를 위해 사실에 근거한 다양하고 정확한 데이터를 기준으로 분류하여 평가에 있어서 척도의 기준을 더 객관적이고 명확하게 세우고 기사 외에 다른 소셜 미디어도 고려해 보아야 한다.

참고문헌

- [1] World Health Organization (WHO), Guidance on INN <https://www.who.int/medicines/services/inn/inn-guidance/en/>, 2019.
- [2] 건강보험심사평가원, 정책 동향 11 권 6 호 2017, 국외 저가의약품 사용 장려 정책 고찰
- [3] 서울대학교, 성분명 처방 시범사업 평가를 위한 연구, 2009.
- [4] 김연희, 데이터베이스개론, 2019.
- [5] David Kroenke and David Auer, Database Concepts, Pearson, 2015
- [6] 한국소비자원, 고령 소비자 문제 종합 대응체계 구축방안 연구, 2016.

독거노인 이중케어 시스템 개발 연구

임유빈*, 추은정*, 한지민**
*성공회대학교 소프트웨어 공학과
**성공회대학교 글로벌IT학과
e-mail : qorn3574@naver.com

A Study on the Development of Double Care System for the Elderly Living Alone

You-Bin Lim*, Eun-Jeong Chu*, Ji-Min Han**
*Software Engineering , Sungkonghoe University
**Glocal IT, Sungkonghoe Universeity

요 약

본 연구에서는 독거노인의 사회적 단절 문제 해결을 위해 방문후원자-독거노인, 독거노인-독거노인이라는 지속적인 방문 관계를 만들고 웹, 모바일 어플리케이션과 방문 기록 리더기를 이용하여 관리하는 돌봄 솔루션을 제안한다.

1. 서론

늘어나는 노인군에 의해 노인을 위한 복지 서비스들이 제공되고 있다. 그 중, 우리나라 독거노인을 위한 사회 복지 제도에는 독거노인 돌봄 서비스가 있다. 독거노인 돌봄 서비스는 사회복지사가 방문 서비스를 원칙으로 하여 일상생활, 안전 확인 서비스를 진행하고 있다. 하지만 사회복지사가 하루에 방문하는 가구가 정해져있고, [1]사회복지사의 수 또한 정해져 있어 많은 이들을 돌보기 힘들다. 게다가 장애등급과 소득분위로 나누어 모든 독거노인이 혜택을 받기 힘든 상황이다. 그래서 본 연구는 해당 문제점을 고려하여 ‘독거노인-방문후원자’, ‘독거노인-독거노인’의 이중 관계를 만들고, 웹, 모바일 어플리케이션과 방문 기록 리더기를 이용한 독거노인 돌봄 서비스 관리 솔루션을 제안한다.

2. 관련연구

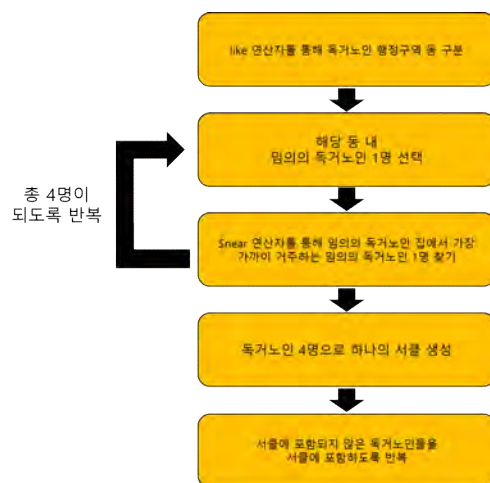
2.1몽고디비의 geospatial query 이용한 근거리 계산

해당 시스템에서는 독거노인들의 서클을 이루어 매칭하기 위해 근거리의 독거노인을 찾기 위해 근거리 계산이 필요하다. mongoDB 쿼리를 이용하여 계산할 수 있는데, mongoDB 쿼리 중 geospatial query [2]\$near 연산자는 GeoJSON 점 또는 레거시 좌표 점을 지정할 수 있고, 가장 가까운 곳에서 가장 먼 곳까지 반환한다.

먼저, 사용자 정보로부터 추출된 위도와 경도 데이터를 데이터베이스에서 접근하여 지리정보와 관련된 어트리뷰트 index를 2dsphere로 설정 (공간 쿼리 연산자를 사용하기 위해서는 위치 정보 필드의 index를 2d나 2dsphere로 지

정해야 함)한다.

근거리의 독거노인을 찾기 위해 근거리 계산 순서는 다음과 같다



1. 현재 도로명 주소 개정으로 주민센터 내에서도 도로명 주소와 행정동 주소를 둘 다 가지고 관리하는 실정을 바탕으로 해당 시스템에는 행정동을 기준으로 한 주소 데이터를 삽입하여 간단한 정규식을 이용하여 동 구분 검색이 가능하게 하였다.

2. random 함수를 통해 임의의 한 독거노인 데이터를 선택한다.

3.mongoDB 내장 geospatial 쿼리 \$near를 이용하여 반경 2km 이내 선택된 노인 데이터와 가장 가까운 노인데이터를 찾는다.

4.그 다음 near을 통해 검색된 노인을 기점으로 하여 다시

\$near 쿼리를 수행한다. 이를 정해진 수(4명)가 채워질 때까지 반복하여 하나의 서클을 생성한다. 서클에 포함되지 않은 노인을 대상으로 위의 1,2,3,4 과정을 반복한다.

2.2 Spring Data MongoDB을 이용한 DB조회

Spring Data MongoDB 프로젝트는 MongoDB 도큐먼트 데이터베이스와의 통합을 제공한다. Spring Data MongoDB의 주요 기능 영역은 MongoDB DBCollection과 상호 작용하고 리포지토리 스타일 데이터 액세스 계층을 쉽게 작성할 수 있는 POJO 중심 모델¹⁾으로 MongoDB 쿼리 사용

```
<dependency>
  <groupId>org.springframework.boot</groupId>
  <artifactId>spring-boot-starter-data-mongodb</ar
tifactId>
</dependency>
```

이 손쉽게 가능하다.

```
public interface LocationRepository extends MongoRepository<Sponsor,String>{

    List<Sponsor> findByAddressLocationNearAndMatch(Point p,Distance d,int match);

}
```

maven을 이용하여 dependency추가(pom.xml)

앞에서 말한 방문후원자(Sponsor)객체를 주소(Address) 객체 내 어트리뷰트인 위치(Location) 객체를 기준으로 가장 가까운(near) 순으로 조회

```
List<Sponsor> sponsors =locationRepository.findByAddressL
ocationNearAndMatch(new Point(location.getLat(),location.ge
tLng()), new Distance(0.5,Metrics.KILOMETERS),0);
```

위에서 작성된 repository를 controller 내에 DI(Dependency Injection)하여 특정 위치 포인트 기준 500미터 내 위치한 방문후원자를 조회함

3. 독거 노인 이중케어 시스템 구성

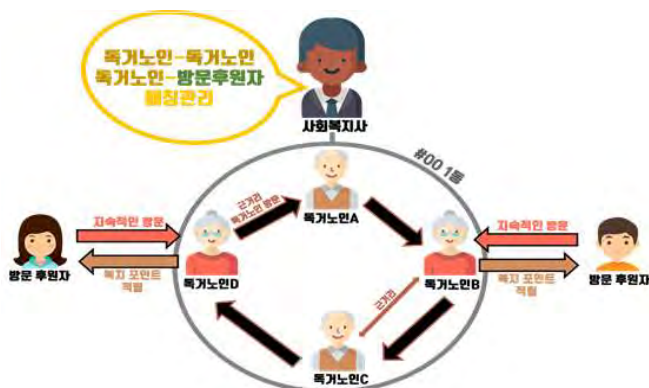


그림 1 독거노인 이중케어시스템 구성도

해당 시스템은 사람들의 방문이 그리운 독거노인과 도움의 손길을 내밀고 싶은 근거리의 방문 후원자를 매칭하여 매 주마다 일정 횟수를 서약하고 독거노인과 후원자와의 만남을 보장하도록 한다. (독거노인-방문후원자 관계) 또한, 근거리에 거주하고 있는 이웃 독거노인들의 서클을 이루어 매칭하고 해당 서클을 담당 사회복지사가 관리한다. 방문관계는 후원자와의 관계, 이웃노인과의 관계로 이중으로 연결되어 기존 사회복지사가 일대일로 독거노인을 관리하여 생겼던 사각지대를 보완한다.

4. 웹/모바일 어플리케이션을 이용한 돌봄 서비스



그림 2 시스템 이용 구성도

웹 어플리케이션은 관리자 페이지, 방문후원자 페이지로 나뉘어진다. 관리자 페이지는 관리자들의 공지사항 관리, 독거노인 서클 관리, 노인과 후원자 조회 등이 가능하다. 웹 어플리케이션에서 관리자가 독거노인 정보 등록시, 주소등록은 좌표변환 API를 이용하여 등록하고 등록된 주소값은 위도와 경도로 표현되어 데이터베이스에 저장된다. 이 값을 바탕으로 몽고디비 근거리연산자를 사용하여 근거리에 있는 독거노인과 썬클을 구성한다. 조회페이지는 몽고디비에 저장되어 있는 데이터베이스를 조회 영역에 따라 쿼리를 작성하여 보여주도록 구현했다. 방문후원자 페이지에서는 방문 일지 작성, 사각지대 신고, 직접 후원 등이 가능하다.

모바일 어플리케이션은 안드로이드로 개발하여 배포된다. 방문후원자가 독거노인의 집에 방문하여 모바일 기기에 독거노인의 NFC카드를 접촉하게되면, 서버에 저장되어있는 방문후원자-독거노인 정보와 일치한지 확인하게 된다. 일치하면 방문이 확인되어, 데이터베이스에 방문 정보가 기록되고 포인트가 적립된다.

그림 2의 과정을 거쳐 방문후원자의 방문이 확인되면, 모바일 어플리케이션에 있는 일지작성 기능이 활성화된다. 방문 인증이 확인된 날짜에만 빨간색 점으로 일지 작성 가능 표시가 나타나 해당 날짜에만 일지 작성이 가능하도록

1) <https://spring.io/projects/spring-data-mongodb#overview>

록 구현했다. 일지 작성은 해당 날짜에 구체적인 돌봄 내용을 기록한다.

5. 독거노인을 위한 NFC 리더기

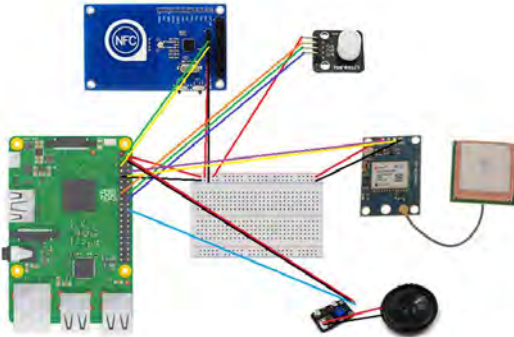


그림 3 라즈베리파이 회로 구성도

독거노인 스마트폰 사용의 어려움을 고려하여 간단히 리더기에 카드를 태그하여 방문기록을 수행할 수 있도록 한다. NFC 리더기는 라즈베리파이, NFC 모듈, LED 모듈, GPS 모듈, 앰프모듈, 스피커로 구성된다. 작동 방식은 다음과 같다. NFC카드를 접촉하기 전 데이터를 읽기 위해 대기하고 있는 상태에서, 리더기에 NFC 카드를 접촉하면 카드에 포함된 사용자 정보와 GPS모듈로부터 받아온 위치 정보가 서버로 전송된다. 서버에서 전송하는 응답 메시지를 통해 검증 결과를 사용자에게 알리고 성공 여부를 LED 색상을 통해 통지한다. 빨간색일 경우 실패, 초록색은 성공을 나타낸다. 스피커에서도 성공음, 실패음이 출력된다.

6. 결론

독거노인 이중케어 시스템은 1인 가구 고령자의 사회적 단절 해소를 위해 사용되기 위함이다. 기존에 1인 가구 고령자의 문제를 해결하기 위해 시스템이 있지만 문제점이 많다. ‘노노케어’같은 경우에는 노인들의 수기작성에 의존하는 경향이 있는데 이중케어시스템은 ICT를 융합한 체계적인 기록 관리를 통해 관리를 보다 용이하게 한다. 기존에는 사회복지사에게 과중한 업무가 주어지고 관리에 대한 한계가 있었는데 본 연구에서는 방문후원자와 노인, 노인과 노인 간의 방문활동으로 사회복지사의 업무 효율을 증대시킨다. 이외에도 블록체인 기술에 기반하여 후원금과 복지포인트를 관리하여 중간 관리자 없이 후원금 및 복지포인트 관리를 투명하게 한다. 뿐만 아니라 지역 복지포인트를 이용하여 지역화폐가 활성화되는 효과가 있다.

현재까지는 웹과 모바일 어플리케이션과 NFC 리더기가 모두 개발된 상황이다. 블록체인은 일부 개발 진행 중이

며 블록을 채굴하고 사용자가 지갑생성과 토큰을 transfer하는 단계까지 완료하였다. 향후 연구방향으로 데이터베이스와 블록체인을 연결해서 후원금과 포인트 관리를 블록체인으로 관리하는 방법에 대한 연구가 필요하다

참고문헌

- [1] 황경란·박혜선·이미영(2017), 『경기도 독거노인 보호 사업 활성화 방안』, 경기복지재단
- [2] MongoDB Documentation Reference: near operator

원자력시설 사이버사건 대응훈련 정책 개선을 위한 규제방안 연구

류진호* 김상우*

*한국원자력통제기술원 사이버보안실
halloyu@kinac.re.kr, kjoey@kinac.re.kr

A Study on the Improvement of Cybersecurity Exercise Policy for the Nuclear Facilities

Jinho Ryu*

*Cyber Security Division, Korea Institute of Nuclear Nonproliferation and Control

요 약

정보처리기술이 발달함에 따라 원자력시설에 대한 사이버침해 가능성이 갈수록 높아지고 있다. 방사능방재법 및 관련 법령에 의거하여 국내 원자력시설은 각 시설 별 사이버사건 비상대응 절차를 수립하고 절차의 유효성 및 비상대응조직의 대응역량을 제고하기 위한 목적의 주기적인 사이버사건 대응훈련을 실시하고 있으며, 규제기관의 독립적인 훈련평가 결과를 통해 많은 개선사항이 도출되고 있다. 본 논문에서는 현행 원자력시설의 사이버사건 대응훈련 체계를 분석하여 사이버사건대응 훈련 정책의 개념에 대해, 국내·외 기준에 따른 사이버사건 대응훈련 정책의 요소를 식별하여 이를 개선하기 위한 구체적인 규제방안을 제시한다.

1. 서론

전 세계적인 정보처리기술의 발달은 산업제어시스템을 활용하는 원자력시설 계측 및 제어분야에 대해 디지털화된 기기들의 도입들을 촉발하며 많은 변화를 가져왔다. 이러한 변화가 적시성, 효율성을 증대시킨 반면, 사이버보안의 관점에서는 또 다른 대책이 요구되었다. 2015년 원자력시설 등의 방호 및 방사능 방재 대책법의 개정으로 원자력시설에 대한 전자적침해행위에 대한 대책이 수립되도록 법령체계가 정비되었다.

2016년 한국원자력통제기술원에서 발행한 *원자력 시설의 컴퓨터 및 정보시스템 보안 심·검사 기준서*[1]는 각 원자력시설별 사이버보안조치 이행의 기준이 되는 “정보시스템 보안규정 (Cyber Security Plan, CSP)”의 지침을 제시하며, 이에 따라 해당 계획의 단계별 이행에 대한 특별검사가 2019년 완료된 바 있다.

아울러 원자력시설에 발생할 수 있는 사이버사건에 대한 대응체계를 시험하고 대응역량을 제고하기 위한 사이버사건 대응훈련(이하, 사이버보안 훈련)이 관련 법령에 근거하여 2016년부터 실시되고 있다. 그러나 사이버보안 필수디지털자산 식별, 휴대용 저장매체 통제, 침입방호 적용 등 주요 보안조치들이 앞서 언급한 CSP에 따라 이행되고 있는 것과는 달리 사이버

보안 훈련은 주로 관련 법령 및 고시에 근거하여 수행되고 있다. 이에 따라 원자력시설 사이버보안 이행의 기준이 되는 CSP와 사이버보안 훈련과의 관계성이 모호하고, 사이버보안 훈련의 내용이 KINAC/RS-015에 따른 훈련 지침의 내용을 적절히 반영될 수 없는 구조로 생각되고 있다.

이에 본 논문에서는, 원자력시설 사이버보안 훈련의 수준을 제고하기 위해서 CSP 수준의 정책이 개발될 필요가 있음을 관련 문헌조사를 통해 뒷받침하고, 이에 대한 구체적인 방안에 대해 논의하고자 한다.

2. 원자력시설 사이버보안 훈련 규제체계 현황

동법 제9조의3(물리적방호 훈련) 및 원자력안전위원회 고시 제2017-1호에 따라 원자력시설은 물리적방호 훈련의 일환으로 사이버보안 훈련을 실시하도록 요구받고 있으며, 이에 따라 국내 원자력시설은 2016년부터 현재까지 각 시설별로 연 3회(전체훈련 1회/부분훈련 2회)의 훈련을 수행하고 있다. 각 원자력시설은 훈련을 실시하기 위해 연간훈련계획 및 훈련 세부계획을 수립하여 원자력안전위원회의 승인을 받은 뒤 실시하여야 한다. 관련 법령간의 상관관계를 도식화하면 아래 그림과 같다.



(그림 1) 방사능방재법에 따른 사이버보안 훈련 관련 법령

3. 원자력시설 사이버보안 훈련 정책 현황

3.1 원자력시설 사이버보안 훈련 정책의 정의

행정학사전[2]에 따르면 정책이란 "공공문제를 해결하고자 정부에 의해 결정된 행동방향을 말하며, 법률·정부방침·정책지침·결의와 같이 여러 형태로 표현"되며 "합법적 강제력을 수반하는 권위가 부여되고 이에 따르지 않을 경우 벌금·제재 등의 조치"를 받는 것을 의미한다.

방사능방재법 제 9 조(물리적방호에 대한 원자력사업자의 책임)에 따라 원자력사업자는 CSP 를 수립하여 이를 원자력안전위원회(정부)의 승인을 받아야 한다. 승인받은 CSP 를 위반하였을 경우 동법 제 12 조(검사) 제2항에 따라 정부는 시정을 명할 수 있다. 마지막으로 동법 제 50 조(벌칙)에 따라 정부는 검사에 따른 시정 명령을 위반할 경우 1년 이하의 징역 또는 1천만원 이하의 벌금을 부과할 수 있다.

이러한 법률구조를 종합할 때, 원자력시설의 CSP 는 행정학사전에서 정의하는 정책의 조건을 충족한다고 볼 수 있다.

3.2 원자력시설 사이버보안 훈련 정책 현황

원자력안전위원회 고시 제 2017-51 호(물리적방호규정 등의 작성내용의 항목별 세부작성기준) 별표 4(정보시스템 보안규정의 세부작성기준)은 원자력사업자의 CSP 가 작성되어야 할 세부기준을 제시한다. 동 고시의 “전자적 침해행위에 대한 원자력시설 컴퓨터 및 정보시스템 대응조치계획에 관한 사항”에서는 본 논문에서 다루고자 하는 사이버사건 대응과 관련한 교육 및 훈련에 관한 사항을 기술하도록 명시하고 있다.

이러한 요건은 KINAC/RS-015 부록 2에 근거하여 수립된 원자력시설별 CSP 에 반영되어 있다. 따라서 현재 원자력시설은 사이버사건 대응을 위한 최소한의 정책이 존재한다고 볼 수 있다. 원자력시설별 CSP 수립 시 참조된 KINAC/RS-015의 해당 대목은 아래와 같다.

3.3 교육 및 훈련에 관한 사항

3.3.1 교육 및 훈련

3.3.1.1 비상사건 대응 훈련

(원자력사업자)는 비상사건대응 교육 및 훈련과 관련하여 다음을 이행한다

- 가. 사이버공격 비상사건대응 인력에 대하여 주기적으로 교육 제공
- 나. 개발된 비상사건대응 절차 및 가상 시나리오를 기반으로 원자력시설 운영에 영향을 주지 않는 범위 내에서 주기적인(최소 년 1회 이상) 모의 훈련 실시(비공식 훈련 포함)
- 다. 교육훈련 결과에 대한 문서화

3.3.1.2 비상 복구계획 점검 및 훈련

(원자력사업자)는 다음이 수행되도록 보장한다.

- 가. 비상복구계획에 대한 주기적 점검 및 훈련(최소 년 1회 이상)을 통해 효과성 입증
- 나. 훈련을 실제 백업될 장소에서 수행하여 관련자로 하여금 그러한 상황에 익숙해 질 수 있도록 하며, 해당 장소가 비상 복구계획을 지원할 능력을 갖추었는지 확인
- 다. 훈련은 미리 설정된 실제 발생될 수 있는 현실적인 시나리오를 기반으로 수행
- 라. 훈련 시 필수디지털자산에 대한 복구 및 재구성 포함
- 마. 점검 및 훈련 결과를 검토하여 보완사항에 대한 적절한 조치 이행 및 비상 복구계획 개정
- 바. 비상 복구계획 훈련이 필수디지털자산 본래의 SSEP 기능 성능 및 신뢰성에 악영향을 미쳐 수행이 불가할 경우에는 다른 대안적인 대책 수립
- 사. 계획예방정비 기간 등을 활용하여 비상 복구계획에 대한 점검 및 훈련 수행 가능

(그림 2) KINAC/RS-015의 전자적 침해행위에 대한 원자력시설 컴퓨터 및 정보시스템 대응조치계획에 관한 사항 중 사이버사건대응 교육 및 훈련에 관한 사항

4. 국내·외 기준에 따른 사이버 훈련 정책 요구사항

4.1 KINAC/RS-015 비상사건 대응에 관한 사항

KINAC/RS-015 2.3(비상사건 대응 및 복구)에 따르면 원자력사업자는 비상사건에 대응하기 위한 목적, 범위, 역할, 책임 및 관리적인 사항을 기술하는 비상사건 대응 정책을 개발해야 한다. 이는 사이버 비상사건에 대한 훈련에 관한 사항을 포함하기 때문에 사이버보안 훈련에 대한 원자력사업자의 상위 문서에 해당한다. 따라서, 이러한 요구사항은 훈련에 관한 정책의 필요성을 언급하고 있는 것으로 간주될 수 있다.

4.2 美 국립표준기술연구소(NIST) SP 800-84

미 국립표준기술연구소 표준문서인 NIST SP 800-84 [3]는 기관의 사이버사건대응을 위한 IT 전략 계획에 대한 가이드를 제공하는 문서이다. 본 문서에서는 종합적인 교육 및 훈련에 대한 정책을 개발할 것을 명시하고 있으며, 정책 항목으로 제안하는 사항은 아래와 같다.

- 목적
- 유효일자

- 달성하고자 하는 목표들
- 적용 대상 및 범위
- 관련 법령 및 규제요건
- 책임 조직 및 담당자
- 훈련 정책 요구사항
- 훈련 정책에 대한 검토 및 승인

4.3 美 국토안보부의 훈련 평가 프로그램(HSEEP)

미국 국토안보부(DHS)의 국토안보훈련 및 평가 프로그램(Homeland Security and Evaluation Program, HSEEP)[4]는 미국의 9.11 테러 이후 발간된 지침 및 가이드 성격의 문서로 다양한 비상대응분야(재난, 테러, 사이버공격 등)에서 적용 가능한 훈련 설계, 실시 및 평가에 대한 기준을 제시한다.

HSEEP는 가장 먼저 훈련 프로그램 관리(program management)에 관한 사항을 다룬다. 여기서 "프로그램"이라 함은 특정 장기목표에 대한 체계화된 행동/조치들을 의미하며, 따라서 훈련 프로그램은 훈련의 계획, 수행 및 평가에 대한 일관된 접근방법을 뜻한다.

훈련 프로그램 관리는 훈련 프로그램 중점사항(priorities)들이 달성되도록 중점사항 그 자체를 식별하고, 필요한 자원을 배분하고, 훈련이 지속되기 위한 조직/부처/기관을 통합하는 활동을 의미한다. 이를 통해 일련의 훈련활동을 지속적으로 감독하고 중점사항을 일관성 있게 추구해 나가는 것을 보장한다. 이에 따라 훈련 프로그램 중점사항 역시 훈련의 정책에 반영되어야 할 중요한 요소로 간주될 수 있다.

또한, HSEEP를 통해 제시되는 훈련의 유형에 관한 정의는 대표적으로 훈련 정책에 포함되어야 할 요소로 볼 수 있다. 현행 사이버보안 훈련의 경우, 훈련을 실시하는 방법 및 종류에 대한 기준이 모호한 반면, HSEEP에 근거한 훈련 유형 분류체계는 향후 훈련의 실시 목적에 적합한 형태의 훈련을 수행할 수 있는 근거로 활용될 수 있을 것이다.

NIST SP 800-84와 HSEEP에 따른 훈련의 유형 분류체계를 종합하면 아래 그림과 같이 표현할 수 있다.



(그림 3) NIST SP 800-84 및 DHS HSEEP에 따른 사이버보안 훈련 유형분류 체계[5]

5. 상세 규제방안

5.1 CSP 개정을 통한 사이버보안 훈련 정책 개선

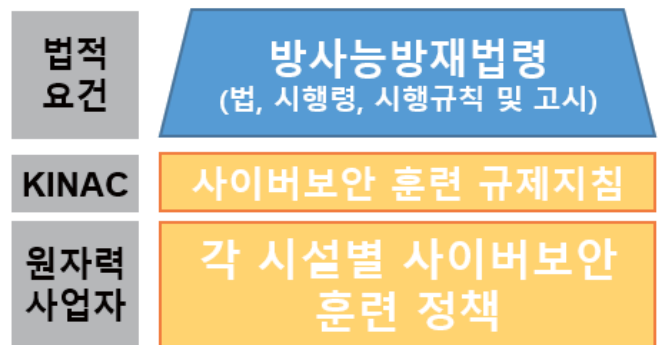
원자력사업자의 사이버보안 이행 활동의 최상위 문서가 되는 CSP 개정을 통해 훈련 정책을 수립할 수 있다. 물리적방호의 관점에서 원자력시설 규정 중 방사능방재법상 CSP에 상응하는 규정인 "원자력시설 등의 물리적방호를 위한 규정"에 따르면 물리적방호 교육 및 훈련과 관한 사항의 기술이 관련 훈련 고시와 연동되어 전체훈련 및 부분훈련의 실시에 관하여 적시되어 있다.

이러한 사례를 참조할 때, CSP의 "전자적 침해행위에 대한 원자력시설 컴퓨터 및 정보시스템 대응조치계획에 관한 사항"에 따른 교육 및 훈련에 관한 사항에서도, 해당 훈련이 방사능방재법 및 관련 고시에 따라 수행한다는 기술이 필요하다.

또한, 해당 규제요건을 만족시키기 위한 훈련의 실시 유형에 대하여 본 논문에서 제시한 바와 같이 NIST SP 800-84 및 HSEEP에 따른 다양한 형태의 훈련 형태에 대해 정의하는 것이 필요하다.

기타 NIST SP 800-84 및 HSEEP에 따른 훈련 정책의 주요 요소(정책 수립 과정에서 중견 간부의 참여 보장, 훈련의 중점사항(priorities) 등)에 대해서도 CSP에 반영되어야 할 것이다.

이러한 CSP의 개정방안은 결국 개정방향과 그 내용에 대한 규제지침을 제공하는 사이버보안 훈련 규제지침의 필요성을 역설한다. 규제기관은 현행 관련 규제요건 및 KINAC/RS-015의 내용을 보다 상세화 및 보충하는 수준의 규제지침을 개발하여 본 논문에서 제안하는 바와 같이 국내·외 기준에 따른 사이버보안 훈련에 관한 정책을 수립하는 기준을 제시해야 할 것이다. 관련 법령체계와 연계된 규제 개선방안은 아래 그림과 같이 도식화 할 수 있다.

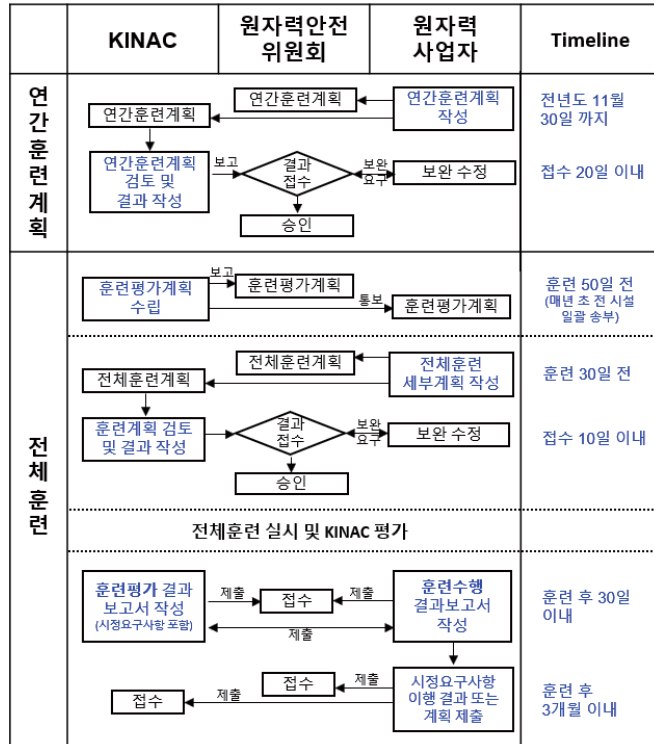


(그림 4) 사이버보안 훈련 규제요건에 따른 규제지침 및 시설 별 사이버보안 훈련 정책의 관계도

5.2 연간훈련계획 심사를 통한 사업자 정책 수립 유도

사이버보안 훈련 정책의 요소 중 시설 규정에 반영되기 어려운 수준의 정책이 존재할 수 있다. 예를 들어 정기 인사를 통해 바뀔 수 있는 정책 담당자, 또는 보다 단기간에 달성하고자 하는 정책 등의 경우에는 관련 규제기관의 승인을 받아야 하는 사업자 규정이 아닌 주기적으로 갱신되는 문서를 통해 구현하는 것이 바람직할 것이다.

현 사이버보안 훈련 규제 체계에는 이러한 성격의 문서로 사이버보안 연간훈련계획이 존재한다. 연간훈련계획은 전년도 11월 말까지 관련 규제기관에 제출되어 심사 및 승인을 받는 원자력시설의 당해년도 훈련계획에 관한 사항으로 매년 변동될 수 있는 성격의 정책을 기술하기에 적합하다. 연간훈련계획을 통해 구현된 정책은 각 부분/전체훈련 세부계획 심사 및 훈련 평가를 통해 그 이행여부가 점검될 것이다. 이러한 사이버보안 훈련 수행과 관련된 규제 절차는 사무편람[1]에 기술되어 있으며, 이를 도식화하면 아래 그림과 같다



(그림 5) 원자력시설별 연간훈련계획 및 전체훈련 세부계획에 대한 심사 및 훈련평가 절차도

6. 결론

정보보안 및 사이버보안에 있어서 정책을 수립하고 이를 이행하는 것은 조직의 보안 관점에서의 목표를 지속적으로 달성하는데 중요한 요소이다. 본 논문에서는 원자력시설 사이버보안 훈련 분야에 대해서 기존 규제체계하에서 수행된 노력들을 살펴보고, 훈련 정책의 개선이 필요함을 진단하였으며, 그 개선방안으로 정보시스템 보안규정(CSP) 차원의 훈련 정책 및 연간훈련계획의 보완을 통한 정책의 수립을 제시하였다. 또한, 수립될 훈련 정책에 들어갈 요소들에 대해서도 국내·외 기준을 근거로 열거하였다.

사이버보안 사건대응훈련은 일반적인 조직에서 사이버사건대응 계획의 일환으로 사건대응조직 구성원의 역량을 제고하기 위해 실시되는 활동이다. 이에 따라, 사이버보안 훈련 정책은 결과적으로 사이버사건대응 정책의 한 부분으로 자리잡을 수 있으며, 이

는 실제 KINAC/RS-015 에서 제시하는 바와 일치한다. 본 논문에서 제시하는 사이버보안 훈련 정책의 개선 활동은 연관된 사이버보안분야 정책의 수립 및 개선에 파급되어 전반적인 원자력시설 사이버보안 체계가 개선되는 것이 바람직 할 것이다.

참고문헌

- [1] "원자력시설의 컴퓨터 및 정보시스템 보안 (KINAC/RS-015)", 한국원자력통제기술원, 2016.
- [2] 하동석 외 1 인, "이해하기 쉽게 쓴 행정학용어사전", 새정보미디어, 2010.
- [3] Tim Grance et al., "Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities", NIST, 2006
- [4] "Homeland Security Exercise and Evaluation Program (HSEEP)." US Department of Homeland Security, 2013.
- [5] T. Aoyama et al., "On the complexity of Cybersecurity Exercises Proportional to Preparedness", Journal of Disaster Research, Vol. 12, No.3, 1081, 2017.
- [6] "원자력시설등의 물리적방호 관련 사무편람", 한국 원자력통제기술원, pp.22-26, 2016.

리멤버 어플리케이션에 기반한 배송관리 시스템에 관한 연구

정기혁*, 한울**

*고려대학교, **상명대학교

e-mail: knp6464@korea.ac.kr

A Study on the Order Management System Based on the Remember Application

ki-hyeok Jeong* , Wol Han**

*Dept of Computer and Information Science, Korea University

**Dept of Historical Contents, Sangmyung

요 약

최근에는 비교적 상황이 나아졌지만, 한때 코로나19로 오프라인 매장에서 마스크를 쉽게 구할 수 없었다. 대신 마스크에 대한 수요와 ‘사회적 거리 두기’와 함께 온라인 구매가 급격히 증가했다. 온라인 구매가 갈수록 증가하고 있지만, 여전히 소비자는 각각의 홈페이지에서 배송상태를 확인하고 있다. 본 연구는 코로나19 후에도 활발히 이루어질 온라인 유통에 주목하면서, 종합적으로 소비자 개인이 자신이 주문한 상품을 조회하는 방안을 제시하였다. 따라서 본 연구에서는 스마트폰 카메라로 명함을 찍어 비즈니스를 돕는 리멤버의 운영방식처럼 휴대폰 카메라로 명세서를 찍어 정보를 종합한 뒤, 자신의 소비량과 예상 배송기간을 바탕으로 상품 보유량을 확인하는 방법을 제안하였다.

1. 서론

코로나19로 인해 마스크 공급이 사회적인 문제로 대두되었다. 정부는 마스크 5부제 및 마스크 알리미 서비스를 도입했고, 굿닥, 똑닥, 웨어마스크 등의 서비스도 제공되었지만, 마스크 대란을 완전히 해결하지는 못했다. 근본적으로 시중에 유통되는 마스크의 수량이 부족했기 때문이다. 이에, 관세청에서는 한시적으로 마스크의 해외 반출을 제한하고 마스크 해외 직구 절차도 간소화했다.

정부와 기업의 여러 노력 덕분에 현재 마스크 품절 사태는 벗어났지만, 여전히 마스크를 한 번에 대량으로 구매하는 것은 어렵다. 마스크 업체가 하루 생산량의 80%를 정부에 납품하고 나머지 20%의 물량이 시중에서 판매되기 때문이다. 마스크의 수요는 해외에서도 높아 해외 직구로도 한 번에 대량으로 구입하기 어렵다는 점도 문제다. 해외 직구의 특성상, 불량품에 대한 환불과 교환이 어렵고, 안정성이 보장되어 있지 않다. 따라서 소비자는 더욱 마스크를 소량으로 자주 구매할 수밖에 없다.

이에 본 연구에서는 다수의 온라인 사이트에서 구입한 상품배송을 현재 본인의 재고와 비교하여 살펴볼 수 있는 시스템을 고안했다. 코로나19가 계속 이어지며 마스크는 계속 소비해야 하지만, 오프라인에서 구하기는 어려워 수시로 온라인에서 주문해야 하는 상황에 부응하기 위해서이다. 이를 통해 소비자는 물품 고갈을 예방하고 재고예상을 통해 불필요한 구매를 피하는 것은 물론, 다른 물품에도 이 시스템을 적용할 수 있을 것이다.

2. 명함 어플리케이션 리멤버의 운영방식

사실 이미 온라인에서 배송추적은 가능하다. 우체국, 네이버 쇼핑, CJ대한통운, 알라딘, 쿠팡, 티몬 등 대부분의 온라인 쇼핑몰은 결제 후 상품 출하, 배송, 도착까지 모든 과정을 제공하고 있다.



(그림 3) 도착 여부만 파악할 수 있는
기존 배송지킴이의 샘플화면과 네이버 쇼핑 배송조회

실제로 스마트택배나 배송지킴이와 같은 어플리케이션을 이용하면 온라인 배송조회를 통합적으로 살펴볼 수 있다. 그러나 위와 같은 서비스는 단순 배송현황만 제공할 뿐, 소비자의 보유량, 배송기간, 상품 물량까지 고려하고 분석하지는 않는다. 따라서 소비자가 현재 보유한 재고와 비교하며 주문한 상품을 전체적으로 조회하기는 어렵다.

이러한 한계점을 극복하기 위해, 본 연구는 명함 어플

리케이션에서에서 그 방법을 찾았다. 2010에 실시된 명함 어플에 대한 연구가 이루어진 이후, 현재는 다양한 어플리케이션이 제작되며 대중적으로 이용되고 있다. [1] 원리는 이렇다. 우선 어플을 실행하여 휴대폰 카메라로 명함을 찍는다. 그 후 찍힌 사진에서 정보가 추출된다. 취합된 정보는 분야에 따라 보기 쉽게 정리되고 필요에 따라 토론 및 구인 구직과 같은 부가적인 기능까지 제공한다. [2]



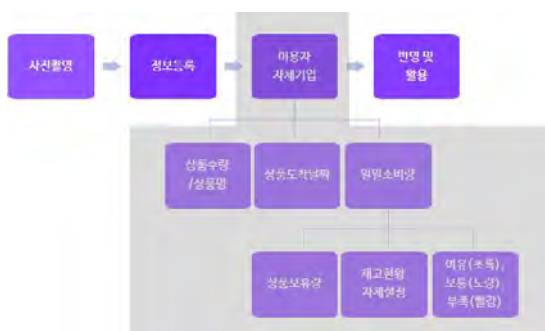
(그림 3) 명함 어플 리멤버의 구성원리

비슷한 기능을 제공하는 다른 명함 어플도 많다. 그러나 리멤버는 타이프스트를 고용, 사람이 직접 주요정보를 확인하여 정확성을 높이는 방식으로 경쟁력을 확보했다. 실제로 리멤버에서 이용자가 휴대폰에서 카메라로 사진을 찍더라도 바로 정보가 등록되지 않는다. 리멤버 소속의 타이프스트가 오류 여부를 점검한 후 후에야 정보가 등록된다. 타이프스트가 점검하기 때문에 정보를 등록할 때 다소 시간이 소요되지만, 대신 리멤버는 명함에 자필로 수정한 정보나 메모까지 정확하게 기록할 수 있는 장점을 갖췄다.

본 연구는 이 방식에 주목하여, 사용자가 직접 주요 정보를 기입하는 방식으로 타이프스트 점검 단계를 배송관리 시스템에도 적용하였다. 온라인에서 상품을 주문한 후 받는 명세표도 명함처럼 정형화된 단어와 숫자로 이루어져 인식하기 쉽기 때문이다. [3] 실제로 네이버쇼핑, 쿠팡, 티몬, G마켓, YES24에서 물품을 배송하면, 명세서 형태는 다르더라도 주요 용어는 비슷하거나 같다.

다만 사이트별로 용어 명칭이 조금씩 다르고, 배송정보와 도착 날짜가 적혀있지 않는 경우가 있어 도착 날짜 외에 일률적으로 정보를 등록하기는 어렵다. 이와 같은 어려움을 극복하기 위해, 타이프스트 점검 단계처럼 본 배송관리 시스템은 이용자가 자체적으로 주요정보를 입력하여 정확한 정보가 취합되도록 하였다.

3. 배송관리 시스템 운영방안



(그림 4) 배송관리 시스템 운영방안

배송관리시스템에서 정보를 추출하는 기본적인 방식은 리멤버나 기존의 배송관리 어플처럼 같다. 우선 명세표를 촬영하거나, 배송코드를 바탕으로 정보를 등록할 수 있도록 하였다. 다만 본 배송관리시스템에서는 정보등록 단계 후, 이용자 자체기입 단계에서 몇 가지 사항을 추가했다.



(그림 5) 이용자 자체기입단계 시안

우선 현재 상품 보유량과 상품명, 상품 도착 날짜와 일일 소비량을 적도록 하였다. 일일 소비량과 상품소비량을 바탕으로 재고 현황도 이용자가 자체적으로 설정할 수 있도록 하였다. 재고 현황은 여유(초록), 보통(노랑), 부족(빨강)으로 나누었으나 범위는 개인에 따라 자유롭게 조정할 수 있도록 하였다. 이 시스템은 배송되는 마스크 수량만 파악하는 것이 아니라 소비자의 재고량과 일일 소비량에 기반하여 재고 현황을 산출하기 때문이다.



(그림 6) 쿠팡(왼쪽)과 네이버쇼핑(오른쪽)에서 결제한 마스크 수량과 도착 날짜



(그림 7) 쿠팡과 네이버쇼핑에서 결제한 정보를 입력하는 과정

그러하여 실제 결제 후 발급받은 명세서에서 추출한 주요 정보를 입력하는 과정은 위으며, 이때에는 예상 도착 날짜와 구입수량 등의 정보를 기입한다.

실제 상황에 적용해본다면 다음과 같다. 3월 초에 보유한 마스크가 15개밖에 없다는 것을 알게 된 한 소비자는 3월 8일에 온라인에서 마스크 25개를 결제한 후 11일에 상품을 받았다. 이 소비자는 3월 14일에 마스크를 50개를 또 주문했다. 두 번째로 주문한 마스크는 주문량이 밀려 23일에 도착할 예정이다. 그동안 이 소비자는 마스크를 더 구입해야 하는지, 구입하지 않아도 된다면 언제까지 비축분을 사용할 수 있는지를 파악해야 한다.

이에 소비자는 물품을 결제하고 받은 명세표를 스마트폰 카메라로 촬영하여 우선 기본정보를 등록했다. 그리고 소비자는 이용자 자체 기입 단계에서 상품명을 마스크로, 보유한 마스크 수량에 도착한 25개를 추가로 입력했다. 도착 날짜는 예정된 23일로 입력했다. 주문한 상품과 보유한 마스크는 모두 일회용이기 때문에 일일 사용량은 한 개로 설정했다. 그리고 소비자는 재고수량을 설정할 때, 여유를 21개~50개, 보통을 11~20개, 부족을 10개 이하로 설정했다. 이를 바탕으로 구현된 소비자는 쉽게 자신의 마스크 보유량을 파악할 수 있다.



(그림 8) 현황을 살펴볼 수 있는 배송관리 시스템

그림 8에서 확인할 수 있는 것처럼, 소비자는 스마트폰에 구현된 배송관리시스템에서 3월 첫 주가 노란색 화면으로 나타난 것을 확인할 수 있다. 이때에는 아직 주문한 두 곳에서 모두 마스크가 도착하지 않았고, 25개가 남아있던 마스크를 하루에 하나씩 소비하면서, 마스크 재고가 소비자가 설정한 11~20개 내외로 떨어졌기 때문이다.



(그림 9) 현황을 살펴볼 수 있는 배송관리 시스템

그러던 것이 3월 둘째 주부터는 변화를 보인다. 그림 9에서 살펴볼 수 있는 것처럼 우선 8일부터 3월 11일까지 재고현황이 빨간색으로 변경되었다. 그 후 재고 현황 상태는 다시 초록색으로 변했다. 동시에 재고 현황 상태 위에 별도로 검은색이 생성되어, 주문한 상품이 배송 중이라는 사실도 파악할 수 있다.

이 모든 지표는 소비자가 설정한 일일 소비량과 현재 보유량을 반영한 수치다. 따라서 3월 1주 차의 노란색은 주문한 마스크가 도착하지 않아 마스크 보유량이 11개~20개였기 때문에 이를 반영한 수치다. 그러다가 3월 2주차부터 재고 현황 상태는 11일까지 빨간색으로 변했다가 12일부터는 다시 초록색으로 변했는데, 이는 결제한 마스크 중 25개가 도착하여 보유량이 여유 기준(21~50개)에 도달했기 때문이다.

그다음부터 재고는 꾸준히 초록색을 유지하고 있다. 또한, 3월 2주 차 토요일부터 3주 차 내내 검은색 표시가 다시 한번 나타나는데, 이는 두 번째로 결제한 마스크가 배송되고 있기 때문이다. 3월 12일부터 21개 이상의 마스크가 재고량으로 집계되고 있고, 23일까지 추가로 50개가 도착한다면 소비자는 마스크 재고량이 아직 여유가 있다고 손쉽게 파악할 수 있다.

만약 23일 이후 배송이 제때 도착하지 않는다고 하더라도 소비자는 적절하게 마스크 구매를 조절할 수 있다. 앞서 언급한 것처럼, 본인의 마스크 보유량과 일일 소비량을 쉽게 파악하고 있고, 배송날짜와 배송 후 마스크 수량도 확인할 수 있기 때문이다. 결론적으로 소비자는 종합적으로 정보를 파악할 수 있어 무리하게 마스크를 확보하려 애쓰거나, 불안함을 느낄 필요도 없을 것이다.

4. 결론

이상으로 여러 곳에서 소량으로 주문된 마스크의 수량과 수령일을 종합적으로 살펴보는 시스템 방안을 제시하였다. 본 연구에서는 일단 마스크에 집중했지만, 이 서비스는 앞으로 여러 곳에서 적은 양의 상품을 구매할 때에도 도움이 될 것으로 보인다.

비교적 쉽고 중장년 세대 사이에서도 이용되는 명함 어플 시스템을 활용한 점도 주목할 만한 요소다. 온라인 유통의 성장과 함께 대두되는 문제가 바로 정보 격차다. 오프라인에서 물품을 사기 위해 줄을 서는 중장년 세대와 대조적으로 젊은이들은 상대적으로 온라인으로 수월하게 마스크를 확보하는 상황이 보도되기도 했다. 만약 본 연구가 더 구체적으로 이루어진다면, 누구나 자신의 주문정보를 쉽게 살펴볼 수 있는 서비스를 제공한다는 점에서 의의가 찾을 수 있겠다.

개인을 대상으로 제안한 시스템이지만, 소규모 중소기업이나 개인사업자가 사무용품을 관리할 때에도 유용하게 활용될 수 있을 것이다. 다만 실시간으로 업데이트되는 배송상태와 연계하여 정확한 정보를 제공하는 등, 앞으로도 많은 보강과 연구가 이루어져야 하겠다.

다만, 매크로를 활용하여 마스크를 독점적으로 구입한 다면, 순차적으로 구입한 물품을 관리하는 시스템은 무용할 것이다. 이와 같은 우려는 실제로 발생했다. 3월 3일 쿠팡에서 마스크 자동구매 매크로를 사용하여 마스크 수천 장을 한 번에 구매한 사례가 발견된 것이다. 이 사건에 활용된 매크로 프로그램을 제작하고 판매하여 다른 이들도 매크로 프로그램을 활용, 총 10만여 장의 마스크를 불법적으로 구입하기까지 하였다. 따라서, 일반 소비자가 안심하고 배송관리시스템을 이용하여 자신의 물품을 언제든 구입할 수 있도록, 국회 차원에서 매크로 활용금지에 관한 입법과 홍보, 정책 개선이 요구된다.

이러한 우려에도 불구하고 본 연구는 코로나 19 이후 다가오는 삶의 변화에 선제적으로 대응하고자 노력했다는 점에서도 의의가 있다. 뉴스핌에서 카이스트 이병태 교수가 “경제적으로 무인점포, 온라인 유통이 활성화될 것.”이라고 언급한 것처럼, 온라인 유통은 앞으로도 증가한다면, 빈번한 이루어지는 배송정보를 효율적으로 관리하고 파악하는 방안에 대한 수요도 증가할 것이기 때문이다.

리멤버에서 이용자가 이직과 구직 정보까지 공유하는 것처럼, 향후 개개인의 소유 물량을 공유하거나 적정 가격을 합의하는 형태도 가능하다. 이에 따라 유통뿐 아니라 한 상품의 가격, 생산, 공급을 유연하게 소비자 수요에 맞게 조정되는 방안도 고민할 수 있을 것이다.

참고문헌

- [1] 장정관, 이호중, 이종현, 김태우, 김수동, 모바일 명함 교류를 위한 어플리케이션 설계, 한국정보과학회 학술발표 논문집, 27(2C), 103-108.
- [2] 서민교, [스마트폰 어플리케이션 소개] 명함관리도 이제는 어플로 간편하게! 리멤버, 기계저널, 57(8), 64-65, 2017.
- [3] 석정한, 윤준서, 박창우, 김동호, . 딥 러닝을 이용한 명함 인식 시스템. 대한전자공학회 학술 대회, 2018,6, 1160-1163

실버 모빌리언, 노년층의 디지털 소외 해결을 위한 앱

서진아, 오송희, 오수현, 이영현, 차승민, 호준원, 김명주

서울여자대학교 정보보호학과

staryj255@gmail.com, wuxongxi@gmail.com, dhtngus20@gmail.com, younghyun317@gmail.com,
vega2828@naver.com, jwcho@swu.ac.kr, mjkim@swu.ac.kr

Silver Mobilian, an application for solving the digital alienation of senior generation

Jin-A Seo, Song-Hee Oh, Su-Hyeon Oh, Young-Hyun Lee, Seung-Min Cha,
Joon-won Ho, Myuhng-Joo Kim

Dept. of Information Security, Seoul Women's University

요 약

디지털 시대에서 스마트폰은 없어서는 안 될 존재가 되었다. 스마트폰이 단순한 통신 기능 뿐만 아니라 다양한 서비스업의 기능까지 수행하면서, 빠르게 발전하였다. 이러한 빠른 발전 속도를 따라가지 못한 노년층은 스마트폰의 사용에 어려움을 겪고 있다. 본 연구는 노년층이 디지털 시대에서 소외되지 않고, 스마트폰을 쉽게 사용할 수 있도록 돕는 애플리케이션을 제안한다. 애플리케이션은 전화 및 메시지 기능의 사용 방법을 안내하고, 위급 상황을 빠르게 알리며 보이스피싱의 위험으로부터 보호하는 기능을 가지고 있다.

1. 서론

1-1. 연구의 배경 및 목적

최근 들어 빠르게 대중화되고 있는 것은 바로 스마트폰이다. 남녀노소 누구나 하나 또는 그 이상으로 소지하고 있으며, 스마트폰의 사용은 없어서는 안 될 정도로 큰 비중을 차지하고 있다. 이처럼 디지털 시대에서 스마트폰의 사용은 매우 보편화되었지만 디지털 소외 계층인 노년층이 겪는 어려움 중 ‘스마트폰 사용의 어려움’이 가장 크다는 것을 직면하게 되었다[1]. 이러한 문제를 해결하기 위해 개발한 애플리케이션 ‘실버 모빌리언’은 디지털 소외 계층이 스마트폰의 사용에서 필수적인 기능인 전화 및 메시지 기능을 보다 쉽고 간편하며 빠르게 사용할 수 있도록 해주며, 각 기능마다 사용하는 방법에 대해 안내해 준다. 또한 장·노년층 사용자가 위급 상황 발생 시 사용자의 위치정보를 보호자에게 보내주는 동시에 전화를 연결해주는 SOS 기능과 보이스피싱 위험에 쉽게 노출될 수 있는 사용자를 고려하여 이를 예방하기 위해 위험 번호에 대해 경고를 주는 기능을 제공한다.

1-2. 기존 애플리케이션에 대한 고찰

정보화 시대가 되면서 주목받고 있는 문제 중 하나는 정보격차이다. 한국 정보화 진흥원에서 조사한 2019 디지털정보격차 실태조사에 따르면 정보취약 4대 계층 중 고령자의 디지털정보화 활용 수준이 가장 떨어진다. 특히 고령자끼리 생활하는 경우, 문자 메시지를 작성하여 타인에게 발송할 수 있는 비율이 절반도 되지 않는다[2]. 전화와 문자는 스마트폰의 가장 기본적인 기능이라 할 수 있지만 현재 노년층을 위해 제공되고 있는 많은 애플리케이션들 중 이를 안내해 주는 서비스는 존재하지 않는다. 또한 위급 상황 시 노년층의 안전을 위해 사용되는 ‘응급 안전 알림 서비스’의 경우 다수의 문제점이 존재한다. 노후화된 장비로 인해 기기의 오작동 및 데이터 전송 오류 등의 서비스 문제뿐만 아니라 서비스 관리 인력 부족으로 사용자들이 제대로 된 서비스를 제공받지 못하고 있다[3]. 또한 화재 및 가스 감지센서를 이용하기 때문에 더 다양한 응급상황에서 대처할 수 없다. 따라서 본 애플리케이션에서는 스마트폰의 사용이 매우 활성화되고 있는 디지털 시대에서 노년층들의 정보격차를 줄이고 동시에 일상생활에서 발생할 수 있

는 모든 긴급상황으로부터 안전한 생활을 보장하기 위해 안내와 SOS 기능이 필요하다.

2. 본론

2-1. 주요기능

2-1-1. 안내

실버 모빌리언은 노년층의 디지털 소외 해결을 위한 애플리케이션이다. 정보화와 IT가 발전함에 따라 정보격차가 발생하고 있으며 전화와 문자는 스마트폰에서 가장 대표적인 기능이지만 고령층에서 많은 어려움을 겪고 있다[4]. 디지털 시대를 살아온 세대에게 모바일 기기의 기본이 되는 전화 기능과 문자 기능은 너무 당연하고 직관적인 기능이다. 하지만 디지털 세대에게 익숙한 방식이 모든 세대에게도 통하는 것은 아니며 이로 인해 디지털 소외가 발생한다. 실버 모빌리언은 이를 해결하여 디지털 소외 계층인 노인에게 도움이 되고자 기능 안내 서비스를 제공한다.



<그림 1> 기능 안내 실행 모습

안내 서비스는 애니메이션 효과와 안드로이드의 Toast 메시지를 통해 사용자가 실행하고자 하는 기능의 이용 방법을 순차적으로 안내한다. 주 사용자가 노년층임을 고려하여 안내 서비스에 보다 쉽게 접근할 수 있도록 화면 오른쪽 하단에 플로팅(Floating) 버튼을 배치하였다. 플로팅 버튼의 visibility 속성을 이용하여 사용자가 버튼을 클릭하였을 때, 각 기능 메뉴가 보이도록 하였고, 사용자가 안내 받고자 하는 메뉴를 클릭하면 id 값을 받아와, 해당하는 안내를 수행한다. 이는 정확한 안내를 제공하여 노년층의 혼선을 방지하며 손쉬운 스마트폰 사용을 가능하게 한다. 그뿐만 아니라 사용자는 기능 실행 방법을

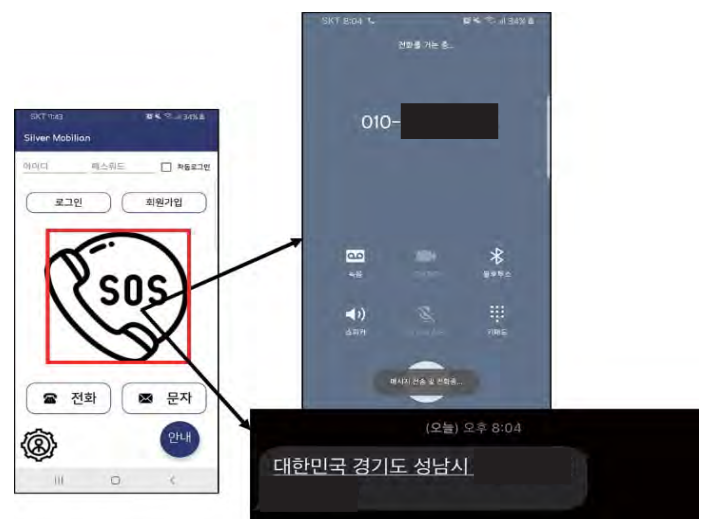
안내 받음과 동시에 기능을 실행할 수 있다. 이것은 서비스 전반에 적용되어 사용자는 애플리케이션과 상호작용 할 수 있다는 장점이 있다. 이는 스마트폰 주요 기능에 대한 이해가 부족하고 사용에 미숙한 노년층이 기능의 목적을 명확히 인지할 수 있도록 도와준다.

애플리케이션은 전화를 거는 방법부터 주소록 검색 및 저장과 즐겨찾기 목록 기능을 안내하며, 메시지 전송 및 답장 기능에 대한 안내와 메시지 내역 검색 기능 또한 안내한다. 이외에도 긴급 호출 서비스 및 마이 페이지에 대한 안내를 제공한다. 사용자는 안내 서비스를 통해 어려움 없이 특정 기능을 수행할 수 있으며, 누군가가 방법을 알려줄 때까지 기다려야 하는 일 없이 상시로 애플리케이션 서비스에 접근할 수 있다.

2-1-2. SOS

실버 모빌리언의 주 사용자들은 고령층이며 이들의 1인 가구 비율은 2015년 24.5%에서 2045년 45.9%로 증가할 전망이다. 고령화 사회로 접어들고 독거노인의 비율이 증가할수록 응급 상황에 대한 노출이 늘어나고 있으며 응급 상황이 발생했을 때 적절한 조치가 이루어지지 않은 경우가 허다하다. 따라서 애플리케이션은 이를 해결하기 위해 응급 상황 시 SOS 기능을 제공한다.

SOS 기능은 긴급 호출 서비스로 사용자가 위급 상황에서 보호자에게 연락을 취하고 사용자의 현재 위치를 자동으로 전송하는 기능이다. 이를 제공하기 위해서 사전에 보호자의 연락처를 필요로 하며 보호자의 연락처는 마이 페이지에서 등록할 수 있다. 또한 사용자의 모바일 기기의 위치 서비스를 활성화하여 사용자의 현재 위치를 출력하게 한다.

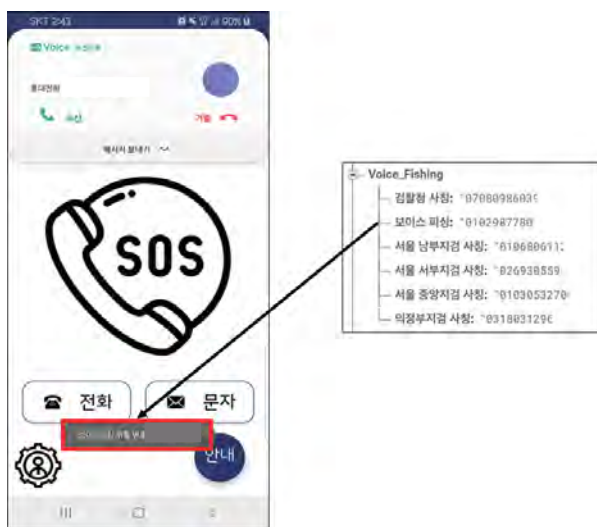


<그림 2> SOS 실행 모습

<그림 2> 를 통해 SOS 기능의 실행 모습을 확인할 수 있다. 사용자가 위급 상황이라고 판단을 하면 애플리케이션의 메인 화면에서 [SOS] 버튼을 클릭한다. 버튼을 클릭하면 미리 저장해 두었던 보호자의 연락처를 가져와 자동으로 전화를 연결하고, 사용자의 위치 정보를 수집하여 보호자에게 문자를 발송한다. 이는 보호자의 신속하고 적절한 대처를 가능하게 한다.

2-1-3. 보이스피싱 예방

보이스피싱이란 주로 금융 기관이나 유명 전자 상거래 업체를 사칭하여 불법적으로 개인의 금융 정보를 빼내 범죄에 사용하는 불법 행위를 말한다. 현재 금융사기에 노출되는 중고령자의 수가 증가하는 데 비하여 사기 예방을 위한 대응책은 충분하지 않으며, 학계에서도 실질적 해결책을 제시하는 데 필요한 기초적인 실증연구조차 아직 제대로 이루어지지 않은 실정이다[5]. 따라서 실버 모빌리언에서는 보이스 피싱을 예방하기 위한 기능을 제공한다. 사전에 많이 사칭 되는 스캠 번호를 Firebase에 넣어 둔다. 이후 사용자에게 수신되는 번호와 비교하여 같을 경우 보이스 피싱 위험 번호라는 경고를 주어, 피해 위험을 사전에 예방할 수 있게 된다.



<그림 3> 보이스피싱 예방 실행 모습

2-2. 주요 기능을 위한 구현

2-2-1. 데이터베이스

애플리케이션에서는 사용자 별 아이디 및 비밀번호 정보, SOS 보호자 연락처, 전화 즐겨찾기, 보이스 피싱 의심 번호를 저장할 수 있는 데이터베이스가 필요하다. 따라서 쉽게 연결이 가능하며 서버 프로그램 없이 데이터베이스에 바로 접근하고 데이터를 용이하게 조작할 수 있도록 Firebase를 사용했다.

2-2-2. 전화 및 문자



<그림 4> 전화 및 문자 구현 모습

애플리케이션에서 제공하는 안내 기능을 구현하기 위해서는 <그림 4>와 같은 별도의 전화 기능 및 메시지 기능이 필요하다. 왜냐하면 애플리케이션이 사용자가 클릭할 부분을 알려주고 사용자의 클릭 이벤트를 확인할 수 있어야 하기 때문이다. 따라서 주요한 전화 및 메시지 기능을 선정하여, 한 화면 내에서 사용하고자 하는 기능과 안내를 함께 이용할 수 있도록 구현하였다.

일반적인 전화 애플리케이션은 그 기능이 단순함에도 불구하고 사용이 꽤 복잡하다. 예를 들어, 전화를 걸 수 있는 방법은 키패드에 직접 번호 입력하기, 키패드 상단의 검색 아이콘 이용하기, 주소록 리스트 스크롤하여 검색하기 등 여러 가지이다. 이는 애플리케이션 사용에 익숙한 노년층이 전화 기능 자체를 이해하는 데에 있어 혼란을 주며, 기능 안내가 더욱이 필요함을 보여준다. 이에 따라 실버 모빌리언은 ‘전화 걸기’, ‘주소록 저장 및 검색’, ‘즐거찾기’를 주요 전화 기능으로 선정하여, 사용자에게 손쉬운 기능 안내를 제공한다.

모바일 기기마다 메시지 기능의 UI(User Interface)는 다르지만 메시지 기능에 공통으로 적용할 수 있는 몇 가지 핵심 요소는 분명히 존재한다. 가령 메시지를 주고받는 상대의 연락처와 메시지 내용이다. 실버 모빌리언은 이러한 핵심 요소에 초점을 맞춰서 화면 구성을 간소화하였다. 이는 노년층이 제공되는 정보에 대해 혼란스러워하지 않고 메시지 기능을 명확히 인지하도록 설계한 것이다. 실버 모빌리언은 노년층

이 주로 사용하는 ‘메시지 전송’, ‘메시지 답장’, ‘메시지 검색’ 기능을 제공한다.

3. 결론

본 애플리케이션에서는 스마트 시대에 따라 고령자들도 사용하기 쉬운 모바일 서비스를 제공한다. 이를 통하여 실버 세대는 보다 쉽게 스마트 기기를 사용할 수 있고 디지털 장비로 인한 사회적 소외감을 극복할 수 있으며, 젊은 세대와 소통할 수 있는 기회가 생김으로써 궁극적으로는 세대 차이를 해결하는데 도움을 줄 것으로 기대된다. 특히 예측이 불가능한 위급상황에 대비하여 실버 세대에게 손쉬운 SOS 서비스를 제공함으로써 긴급 대처를 도울 수 있다. 또한 스마트폰의 기본 기능에 대한 안내를 제공하고, 버튼 클릭만으로 보호자에게 SOS 를 호출하며, 수신과 동시에 보이스피싱 관련 번호임을 인지하도록 안내한다. 그 외에도 사용자를 고려해 UI 를 간소화하는 등 기존 애플리케이션과의 차별화에도 노력도 기울였다.

본 애플리케이션은 노년층의 디지털 소외와 그로 인한 정보 격차 문제점을 시간과 공간에 구애 받지 않고 해결한다는 점에서 실용성이 높다. 다만 주요 기능은 최소한 한 번의 애플리케이션 실행 후에야 사용할 수 있도록 구현되어 애플리케이션 최초 실행에 대한 안내가 있어야 한다는 점이 불편할 수 있다. 이에 따라 사용자가 스마트폰 사용 시작과 동시에 애플리케이션이 실행될 수 있는 방법에 대한 연구가 추가되면 더욱 실용적일 것이다.

Acknowledgement

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 SW중심대학지원사업의 연구결과로 수행되었음. (2016-0-00022)

참고문헌

- [1] 안아주, 심우현, 소효정. 인간중심디자인 방법론을 적용한 노인 대상 모바일 어플리케이션 개발. 한국 HCI 학회 학술대회. 452-460. (2014)
- [2] 오윤석, 가족구성에 따른 고령자들의 미디어 활용 능력, 18, 02, 1-7, 2018
- [3] 김지연, 고영준, 고령자의 안전생활을 위한 ICT 융합 서비스디자인 시나리오 제안, Journal of Digital Interaction Design, 17, 3, 129-139, 2018
- [4] 김정언, 노용환, 최두진, 정부연, 김재경. 고령화와 정보격차: 정보격차의 결정요인 분석. 연구보고 07-10. 1-103. (2007)
- [5] 김민정, 김은미. 금융사기 유형과 피해 유형험자의 특성. 소비자문제연구. 45(2). 23-46. (2014)

실시간 모니터링 및 생체정보 수집 가능한 환자 케어시스템 구현

김세정^{*1}, 윤서빈^{*1}, 변정훈^{*1}, 오예은^{*1}, 유종현^{**}, 전홍영^{**}, 정길환^{**}, 김규겸^{**1)}

^{*}원광대학교 컴퓨터소프트웨어공학과

^{**}원광대학교 의료융합연구센터

sejeong98105@naver.com, shinebin123@naver.com, sa_8001@naver.com,
548621@naver.com, jhryu@wku.ac.kr, zip80@wku.ac.kr, jeongkh1@wku.ac.kr,
kgkim@wku.ac.kr

The Implementation of a Patient Data Management System with Real-time Vital Signs Monitoring

Sea-Jung Kim^{*1}, Seo-Bin Yoon^{*1}, Jung-Hun Byeon^{*1}, Ye-eun O^{*1}, Jong Hyun
Ryu^{**}, Hong Young Jun^{**}, Kil Hwan Jeong^{**}, Kou Gyeom Kim^{**}

^{*}Dept. of Computer Software Engineering, Wonkwang University

^{**}Medical Convergence Research Center, Wonkwang University

요 약

환자의 생체신호 측정 및 관찰, 영상, 위생 등을 포함하는 직접간호는 간호사들의 총 간호활동 시간 중 내과는 48%, 외과는 40% 로 간호사들의 업무 부담이 되고 있다. 또한 의료기관에서 사용되는 의료기기들은 여러 회사에서 구매하여 사용되기 때문에 각 회사마다 상이한 프로토콜을 가지고 있어 하나의 시스템으로 생체신호를 모으기가 쉽지 않다. 따라서 여러 장비에서 생체신호를 실시간으로 취득하여 통합 관리할 수 있는 시스템 개발을 통해 간호사의 직접간호 업무량을 줄여 간호사의 근무환경 개선뿐만 아니라 중증환자의 경우 환자 생체신호에 대한 실시간 원격감시가 가능하고 환자에게서 발생된 모든 생체신호가 데이터베이스 시스템으로 기록관리 됨으로 인해, 환자의 생체 신호에 대한 이력 추적관리가 가능함으로써, 양질의 의료 서비스가 가능한 환자케어시스템을 개발하고자 한다.

1. 서론

우리나라의 간호인력 수는 OECD 평균의 절반 수준이며, 간호사 1인이 담당해야 하는 환자 수는 미국 등 의료 선진국과 약 3배 정도 차이가 난다. 즉 우리나라 간호사들은 적은 간호 인력과 양질의 의료 서비스에 대한 요구 증가로 발생한 과다한 업무량으로 높은 신체적 부담감과 정신적 스트레스에 시달리고 있다[1]. 다른 연구에 따르면 간호사가 수행한 직접 간호활동의 영역별 구성 비율에서 내과는 총 13496시간 중 6484시간으로 48%, 외과는 10589시간 중 4164시간으로 40%를 나타내며 내, 외과 모두 측정 및 관찰이 가장 많은 비율을 차지했다. 이때 직접간호는 환자에게 직접 제공되는 활동으로, 59개의 직접 간호 항목 중에서 영양, 위생, 운동, 측정 및 관찰, 의사소통, 투약, 처치, 배설 및 세척, 흡인, 산소 투여, 열요법의 간호 활동 시간을 측정한

것을 말한다[2]. 이는 직접간호에 간호사들의 업무시간 중 많은 시간이 할당되고 있고, 이는 간호사들에게 업무 부담이 되고 있음을 알 수 있다.

통상 의료기관에서 사용되는 의료기기들은 여러 회사에서 구매하여 사용되고 있는데, 각각의 의료기기 회사마다 각자의 프로토콜로 생체신호를 제공할 수 있도록 하고 있어 하나의 시스템으로 생체신호를 모으기가 어렵다는 단점을 가지고 있다. 또한 의료기관에서 의료기기 공급 업체를 선택할 때는 제품품질과 함께 유지, 보수 서비스 및 가격 등을 가장 중요하게 고려하지만[3] 기존 의료기기들은 높은 가격에 판매되고 있다.

본 연구에서는 생체신호를 실시간으로 취득하여 통합 관리할 수 있는 시스템의 개발을 통해 간호사의 직접간호 업무량을 줄여 간호사의 근무환경 개선뿐만 아니라 중증환자의 경우 환자 생체 신호에 대한 실시간 원격감시가 가능하고 환자에게서 발생된 모든 생체 신호가 데이터베이스 시스템으로 기록관리 됨으로 인해, 환자의 생체 신호에 대한 이력 추

1. 첫 네 명의 저자는 이 논문을 작성하기 위해 동일한 역할을 수행하였음.

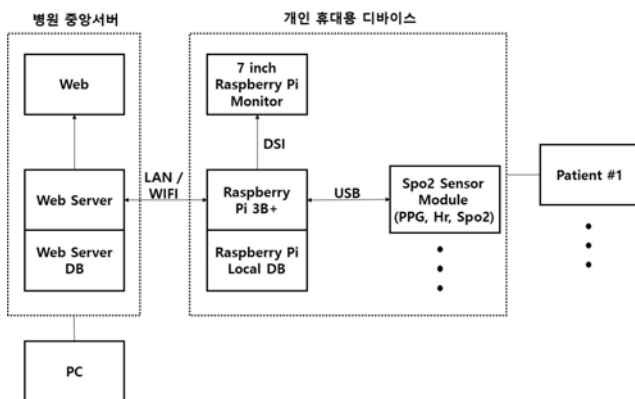
적관리가 가능함으로써, 양질의 의료 서비스가 가능한 환자케어시스템을 개발하고자 한다.

2. 본론

2.1. 시스템 구성

생체신호 수집 시스템은 크게 생체신호를 취득하여 로컬 데이터베이스에 저장하고 메인 데이터베이스에 전송하는 생체 모니터링 디바이스, 생체신호 취득 센서, 생체신호를 전송받아 데이터베이스에 저장하고 결과를 화면으로 출력해 주는 출력부로 이루어져 있다.

환자 모니터링 시스템은 그림 1과같이 구성되어 있다. 환자 실시간 모니터링의 기능은 크게 생체 모니터링 디바이스와 센서 간의 통신, 생체신호 값을 웹서버 데이터베이스와 생체 모니터링 디바이스의 로컬 데이터베이스에 저장하고 모니터링 디바이스의 모니터와 웹페이지에서 실시간 모니터링할 수 있도록 출력하는 기능을 포함한다.



(그림 1) 시스템 다이어그램

2.2 생체 모니터링 디바이스

생체 모니터링 디바이스는 데이터베이스 서버와의 통신을 위해 IoT 기술이 포함되어야 하며, 여러 개의 생체신호 센서 데이터를 취득하기 위해 여러 개의 통신 포트와 가격이 저렴해야 유리하다. 이에 응용할 수 있는 제품은 Arduino와 Raspberry Pi가 있으며 이는 다양한 센서들을 연결할 수 있을 뿐만 아니라 오픈소스코드를 활용하여 더욱 쉽게 확장시키고 발전시킬 수 있으며 일반 컨트롤러에 비해 가격이 저렴하다.

Raspberry Pi는 Arduino에 비해 리눅스와 같은 운영체제 설치가 가능하여 운영체제 내에서 직접 프로그래밍을 하여 외부기기 제어가 가능하며

Application 프로그램 사용이 가능하다. 또한 인터넷 연결을 지원하는 WIFI 모듈이나 LAN 포트, USB 포트, 화면을 표시하는 HDMI 포트 등 외부 하드웨어를 쉽게 연결할 수 있는 확장 I/O 핀이 많아 쉽게 다른 H/W와 연결이 가능한 장점을 가지고 있다[4].

Raspberry Pi는 또한 다양한 기능을 구현함에 있어서 소비하는 노력과 시간을 줄일 수 있으며, 추후 센서를 추가, 제거하는데 매우 용이하며 특정 회사의 제품으로 센서를 한정하지 않고 사용할 수 있다는 점 등을 고려하였을 때 환자 생체신호 모니터링 시스템을 개발하기에 가장 적합하다고 판단하여 Raspberry Pi를 선정하였다.

생체 모니터링 디바이스는 그림 2와 같이 Raspberry Pi 3B+(Raspberry Pi 3B+, Raspberry Pi Foundation, United Kingdom)와 Raspberry Pi 공식 7인치 터치스크린(Raspberry-Pi 7inch Touch Screen Display, Raspberry Pi Foundation, United Kingdom), 생체신호 수집 센서(SPO2 Sensor Module, APMKorea, Republic of Korea)로 구성하였다.



(그림 2) 시스템의 구성

2.3 생체신호 취득

생체신호 취득은 SPO2 Sensor Module ICOM2를 Raspberry Pi에 UART 통신을 이용해 연결하여 PPG, Hr, Spo2 생체신호를 취득하도록 한다.

생체 모니터링 디바이스는 취득한 데이터를 로컬 데이터베이스에 저장하고 디바이스에 장착된 터치스크린에 PPG 그래프와 Hr, Spo2 값을 화면에 표시한 후 TCP/IP를 통해 웹서버 데이터베이스에 전송한다. 웹서버에서는 데이터베이스에 접속하여 가장 최근에 수신된 값을 Ajax 비동기 통신을 통해 실시간으로 가져와 PPG 그래프와 Hr, Spo2 값을 갱신하며 웹페이지에 표시한다.

생체신호 센서와의 통신을 위한 프로토콜은 표 1과 같이 STX, Wave, Hr, Spo2, Status, ETX로 구성한다. STX는 시작 비트로 0xFA를, ETX는 종료 비트로 0xFB를 설정하였다. Wave는 PPG 파형의 수치를, Hr은 심박수 수치를, Spo2는 산소포화도 수치를, Status는 Sensor와 Finger 상태를 나타낸다.

센서 데이터는 0.5초 간격으로 취득하여 로컬 데이터베이스에 저장한다. 이때 손가락이 센서에 인식된 경우에만 측정되어야 의료 현장에서 오류를 줄일 수 있기 때문에 Status 값이 0x03일 때 측정되도록 한다.

<표 1> 생체데이터 취득을 위한 프로토콜

STX	Wave	Hr	Spo2	Status	ETX
0xFA	PPG wave	Heart rate	Oxygen saturation	sensor, finger	0xFB

Status Value		
Bit	Showing	
Bit0	0	Sensor Open
	1	Sensor In
Bit1	0	Finger Open
	1	Finger In
Bit2 ~ 7	0	Reserve
	1	Reserve

2.4 데이터베이스 구조

개발된 환자 모니터링 시스템은 그림 3과 같이 디바이스에서 수집한 환자들의 실시간 생체신호 값을 데이터베이스에 저장하고, 인터넷을 통해 웹서버에 접속하여 원격 조회하는 기능을 담당한다.

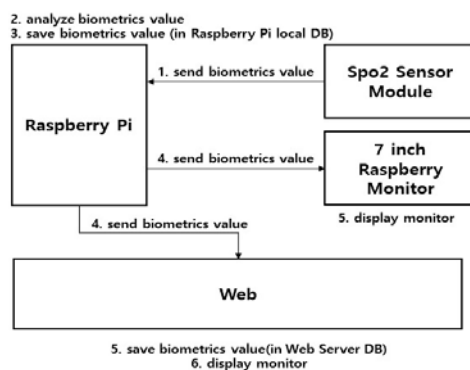
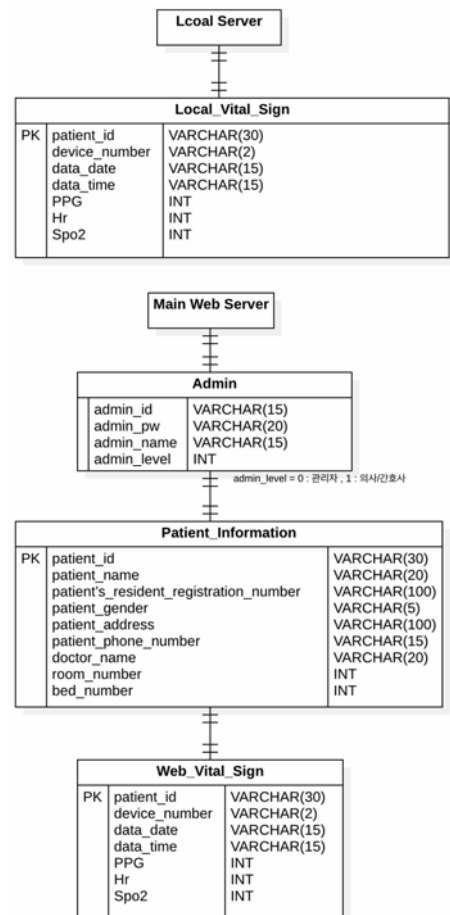


그림 3 데이터베이스 블록 다이어그램

구축한 전체 시스템은 여러 대의 디바이스에서 송신하는 데이터를 종합적으로 관리하는 웹서버, 생체 모니터링 디바이스의 로컬 서버가 있다. 각각의 서버에는 환자 정보를 저장하는 데이터베이스가 연동되어 있으며 데이터베이스는 Mysql을 이용하였다.

웹서버와 로컬 서버는 Nodejs의 express Module을 이용하여 구축하였다.

메인 웹서버 데이터베이스에는 서버 접근자 통제를 위한 Admin 테이블, 환자 정보를 담고 있는 Patient_Information 테이블과 환자의 생체신호를 실시간으로 저장하는 Web_Vital_Sign 테이블로 구성되어 있다. Patient_Information 테이블과 Web_Vital_Sign 테이블은 환자별로 테이블을 생성한다. 각 테이블은 환자 식별 번호인 patient_id를 primary key로 사용하며 이를 통해 환자를 식별한다. 이때 해당 환자 디바이스에서도 primary key를 동일하게 세팅해 주어 디바이스에서 측정된 센싱 값을 중앙 서버 데이터베이스에 저장할 때 해당 환자를 식별하고 해당 환자의 테이블에 생체신호정보가 저장된다.



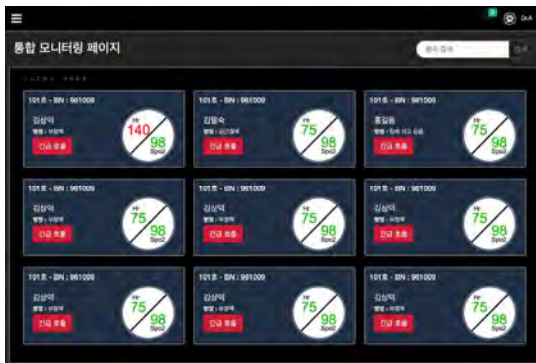
(그림 4) DB 구조

로컬 데이터베이스는 Local_Vital_Sign 테이블로 구성되어 있으며, device_number, patient_id를 초기에 설정해서 환자 구별과 기기를 식별한다. 특히 네트워크가 중단됐을 때 데이터 백업 및 생체신호 모니터링이 중단되지 않도록 구성하였다.

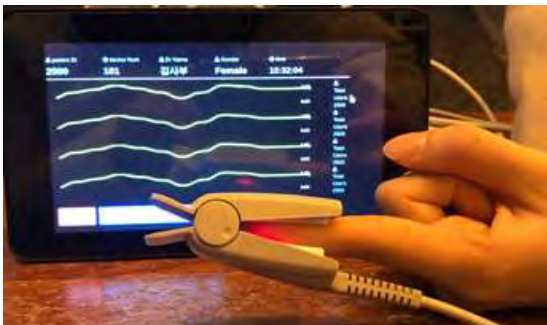
2.5 실시간 모니터링

사용자는 그림5의 (a)와 같이 웹 모니터링 화면을 통해 환자별로 디바이스에서 송신되고 있는 생체신호를 확인할 수 있으며, 정상 범위 수치는 녹색으로, 위험 범위에 속하는 범위는 붉은색 표시 및 경고음이 울리도록 하였다. 또한 환자 목록에서 선택하면 환자의 자세한 정보와 실시간 생체신호 정보를 출력하여 환자 상태를 한눈에 확인할 수 있다.

생체 모니터링 디바이스는 그림 5의 (b)와 같이 디바이스에 장착된 터치스크린에 PPG 그래프와 Hr, Spo2 값을 출력해준다.



(a)



(b)

(그림 5) 모니터링 화면

(a) 웹 모니터링, (b) 디바이스 모니터링

3. 결론

본 연구에서는 Raspberry Pi와 센서를 활용하여 환자들의 생체신호를 수집하고, 웹을 통해 실시간으로 통합 관리하는 기능을 제공하는 환자 생체신호 실시간 모니터링을 구현하였다.

환자 생체신호 실시간 모니터링 시스템은 간호사들의 직접간호 시간을 줄여 업무의 부담을 줄일 수 있을 뿐만 아니라 고가의 의료장비를 구입하고도 유지 보수에 많은 비용을 소비하고 향상된 기술 장비를 교체 적용하기 위해 전체 장비를 바꾸어야 하

는 문제 등에 상황을 겪는 의료기관의 여건 개선에도 도움이 되어 업무처리를 향상시킬 수 있으며, 환자에게는 양질의 의료서비스를 제공함으로써, 모두의 부담을 줄이면서 향상된 의료 서비스 제공 및 수혜를 받을 수 있게 할 것이라고 사료된다.

환자케어시스템은 병실 환자베드에서 환자마다 개인 단말기를 통해 모든 생체정보가 실시간으로 수집되고 데이터베이스 서버로 전송되어 기록관리됨과 동시에 원격으로 의료진이 휴대한 스마트기기 또는 PC를 통해 웹서버에 접속하여 환자의 실시간 감시가 가능하고, 기록된 생체정보는 데이터베이스를 통해 광범위한 자료검색과 열람이 가능함으로써, 환자의 생체정보 기반의 병력 추적관리가 가능하게 됨으로써 양질의 의료서비스가 가능해지며, 각 병실을 돌며 환자의 상태를 체크해야 했던 직접간호의 시간을 단축할 수 있으며 환자별 생체신호를 통합적으로 확인할 수 있어 문제 발생 시 빠른 대처가 가능하

4. Acknowledgements

본 연구는 원광대학교 현장실습지원센터 및 과학기술정보통신부 의료기관 창업 캠퍼스 연계 원천기술개발사업(No. NRF-2016M3A9E9941569)의 지원에 의하여 이루어진 것임.

참고문헌

- [1] Ji Eun Lee, Eunjoo Lee. "The influence of the burden of nurse's work and health problems on presenteeism". Journal of the Korean Data & Information Science Society, vol. 28, pp.769-781, 2017.
- [2] Jung Ho Park, Hyeoun Ae Park, Hyon Joe, Hye Rah Han. "Measurement of the Nursing Workload by Patient Classification System in a Secondary Hospital". Korean Academy of Nursing Administration, vol. 1, pp.132-146, 1995.
- [3] Yeo, Jin Dong, Kim, Hye Sook, Kim, Mi Sook. "A Study on the Effect of Medical Device Purchase Decision Making". 의료경영연구 (보건의료산업학회), vol. 2, pp.28-36, 2008.
- [4] 차승범, 유대환, 나지은, 이예랑, 김준호, "사물인터넷을 위한 안드로이드와 아두이노의 무선통신 개발환경 설정 그리고 스마트 도어락", 한국정보과학회 학술발표논문집, pp.98-100, 2016.

증강현실 기반 전자회로 교육 시스템 개발

오도봉*, 심승환*, 최한고**

*코아원

**금오공과대학교 전자공학과

dboh@coreonetech.com, shshim@coreonetech.com, hgchoi@kumoh.ac.kr

Augmented Reality Based Electronic Circuit Education System Development

Do-Bong Oh*, Seung-Hwan Shim*, Han-Go Choi**

*Coreonetechnology

**Dept. of Electronic Engineering, Kumoh National Institute of Technology

요 약

본 논문은 ICT 융합 기술 분야의 기초가 되는 전자회로의 이론 및 실습을 위한 방법으로 증강현실 기반 전자 회로 교육 시스템을 제안 하였다. 제안된 시스템은 기본 전자 소자가 탑재된 하드웨어 모듈과 증강현실 기술을 적용한 모바일 교육 콘텐츠로 실제 회로를 실물로 동작 확인이 가능하며, 증강현실 기반에서 전류의 흐름, 입·출력값, 측정값등에 대한 정보를 제공한다. 이에 각 이론 및 실습단계에서 기초 전자 소자 및 전자 회로에 대한 교육을 자기 주도 학습이 가능하도록 하였다.

1. 서론

최근 정보통신기술(ICT)의 융합의 발전 인한 관련 기술 중 전자 회로는 전문계 고등학교 이상 공학계열 전공으로 시행되고 있으며, 이론 강의 후 실습시 사용하는 교구는 만능기판, 브레드보드가 대표적이다. 이들은 안전에 유의해야 하며, 회로가 잘못 구성되었거나, 회로의 Open이나 Short등 회로의 오류를 찾기 힘들며 수정은 더 힘든 단점이 있다.

본 논문에서는 이러한 단점을 해결하고자 자석을 이용한 하드웨어 모듈을 제작하여 다양한 형태의 회로를 입체적으로 구성 할 수 있으며, 증강현실을 이용하여 회로 구성, 측정 및 디버깅 흥미 유발로 인한 수업의 효율성 및 학생의 이해도를 높일 수 있으며 언제든지 스스로 학습 할 수 있는 교육 시스템을 제안한다.

2. 관련 연구

증강현실의 교육적 활용은 능동적 학습, 구성주의적 학습, 의도적 학습, 실제적 학습 및 협동 학습을 촉진시키며[1], 몰입의 유발, 경험중심, 이동성 협력 학습 강화라는 측면에서 효과적인 학습을 기대할 수 있다[2].

기존 전자 회로 실습 교육을 위하여 사용하는 교구는 대표적으로 네 가지로 구분할 수 있다[3]. 그

첫 번째가 만능기판위에 납땜으로 회로를 구성하는 방법이고, 이는 안전에 유의 하여야 하며, 잘못 결선시 디버깅이 힘들다는 단점이 존재한다. 두 번째는 브레드보드를 이용한 실습 방법으로 파워 서플라이 등과 같은 부가적인 장치가 필요하며, 피 교육자는 회로 연결 방법을 이해할 필요가 있고, 회로연결 후 브레드 보드 내부에서 결선 또는 단선등이 발생한다는 단점이 존재한다. 세 번째는 블록 키트를 이용한 실습 방법으로 소자가 모듈형태의 방법으로 구성되어 있으나 3개 이상의 배선이 만날 경우 배선이 어렵다는 단점이 존재한다. 마지막은 전자 회로 실습장비를 이용하는 방법으로 회로가 대부분 구성되어 있어 학생이 회로를 확인 하는 장비이다.

본 논문에서는 이들의 단점을 보완하기 위해 잘못된 회로 구성 시 앱에서 메시지 알려 주고, 자석을 활용하여 납땜이 필요하지 않으며, 회로 연결이 눈으로 확인 되어 회로 디버깅에 용이한 AR 전자 회로 실습 시스템을 제안한다.

3. 증강현실 전자회로 교육 콘텐츠 시스템

본 논문에서 제안하는 증강현실 전자 회로 교육 시스템 그림 1과 같이 전자 회로 모듈을 이용한 하드웨어와 하드웨어로 구성된 콘텐츠의 학습 이론 및 실습으로 구성되는 AR 전자 회로 교육 소프트웨어를 제안한다. 또한, 본 논문에서 제공하는 교육 콘텐츠

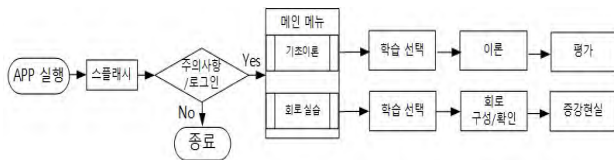
츠의 경우 공학계열 교육 과정에 주로 사용되는 저항, 콘덴서, 반파정류, 전파정류, 평활, 정전압, 트랜지스터 증폭회로, 연산증폭회로로 구성된다.



(그림 1) 교육 콘텐츠 시스템 구성

하드웨어의 경우 회로 접촉 불량에 대한 실습 오류의 최소화와 잘못된 회로 구성 시 빠른 수정을 목적으로 자석 블록 접속 방식과 소자의 모듈화를 적용하였고, 자석 블록 접속 방식은 하드웨어 모듈간의 회로 연결을 목적으로 모듈 내부에 자석을 활용하는 방법이고, 소자의 모듈화는 하나의 소자를 하나의 모듈로 적용하는 방법이다(그림 1 좌측 참고).

소프트웨어의 경우 교육을 목적으로 이론 및 실습으로 구성되고, 이론의 경우 이론 선택 및 이론학습, 평가 문제, 문제 풀이 등을 제공한다. 실습의 경우 실습 선택 및 회로학습, 증강현실로 구성되며 본 논문의 소프트웨어 설계는 그림 2와 같다.



(그림 2) 소프트웨어 설계

4. 개발 결과

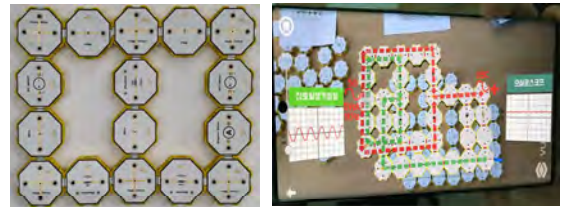
본 논문에서 개발한 교육 시스템은 그림 3과 같이 구성하였고, 피 교육자의 학습 방법은 먼저 앱에서 이론 및 문제 풀이등 선행 학습을 진행 한 후 실습을 수행할 수 있도록 하였다.



(그림 3) 이론 학습

하드웨어의 경우 그림 4 좌측과 같이 구성하였고, 피 교육자는 이를 이용하여 회로에 대한 이론, 입-

출력값, 측정값 등을 실습할 수 있도록 하였다. 마지막으로 증강현실 실습을 실행한 화면은 그림 4 우측과 같고, 실제 구성한 하드웨어의 실제 동작을 증강현실기반에서 확인 할 수 있도록 하였고, 회로 및 전류의 흐름과 입력, 출력, 측정값등의 정보를 화면에 오버랩 하여 제공하였다. 또한 편의성을 목적으로 화면 확대, 축소, 각종 정보표시 ON/OFF 기능을 제공한다.



(그림 4) 실물 회로 및 3D 증강현실 실습

5. 결론

본 논문에서는 전자 회로 교육에 대한 효율성을 높이기 위한 방법으로 실제 전자 소자 하드웨어 모듈을 이용하여 회로를 구성하여 동작을 확인 할 수 있으며, 기본 이론 학습, 문제풀이등 전자 회로에 대한 전반적인 지식을 습득 후 이를 증강현실 기술을 이용하여 회로에서 필요한 각종 정보를 표시 해 주는 증강현실을 이용한 전자 회로 실습 교육 콘텐츠를 개발 하였다.

향후 증강현실을 이용한 전자 회로 교육 콘텐츠를 더 많은 실물을 조작 할 수 있으며, 공학계열에 사용되는 전문 교과 분야로 범위를 확장하여 효과적인 교육 콘텐츠로 활용할 계획이다.

본 연구는 2019년도 중소벤처기업부의 기술개발 사업지원에 의한 연구임[과제 번호 : S2729399]

참고문헌

- [1] B. E. Shelton, "How Augmented Reality Helps Students Learn Dynamic Spatial Relationships," Unpublished doctoral dissertation, University of Washington, 2003.
- [2] 류지현, 조일현, 허희옥, 김정현, 계보경, 고범석 "증강현실기반 체험형 학습모형 연구", 한국교육학술정보원, 2006.
- [3] 박병진, "E.B.S를 이용한 전자 회로의 이해력 신장", 제43회 전국교육자료전 실과교육분야 설명서, 2012.

딥러닝 기반 이미지 인식 기술을 활용한 동전 자동분류 스마트 저금통

유연승*, 장영진*, 심현정*, 이슬비*, 김정길*

*남서울대학교 컴퓨터소프트웨어학과

yys400037@gmail.com, tmfql4428@naver.com, v_v33s@naver.com,

juangexn@gmail, comcgkim@nsu.ac.kr

Implementation of Automatic Coin Sorting Smart Piggy Bank using Deep Learning based Image Recognition Technology

Yeon Seung Yu*, Young Jin Jang*, Seul Bi Lee*,
Hyeon Jeong*, Cheong Ghil Kim*

*Dept. of Computer Science, Namseoul University

요 약

기계학습은 인공지능의 한 클래스로 최근 이미지 및 음성인식, 지능적 웹 검색, 자율 주행 자동차 등의 영역에서 성공적 발전을 바탕으로 우리의 일상에 폭넓게 이용되고 있다. 본 논문에서는 Keras 오픈소스 라이브러리를 이용해 딥러닝을 이용한 기계학습 기반의 동전 인식 소프트웨어를 구현하였고, 이를 이용해 동전 자동분류 스마트 저금통을 설계하였다. 동작 검증을 위하여 스마트 저금통의 모든 발생 이벤트는 Parse-server와 mongoDB를 이용하여 시각화 및 어플리케이션 및 웹사이트를 연결하였다.

1. 서론

인간 지능을 모사하려는 인공지능 기술은 계속적 발전으로 최근에는 해당 분야의 전문 지식에 의존하는 대신 빅데이터에 기반을 두어 지식을 자동으로 축적한다는 면에서 인간 수준의 인공지능을 향하여 진일보하고 있다. 이러한 배경으로 딥러닝(deep learning)은 최근 음성인식과 영상인식을 비롯한 다양한 패턴인식 분야의 성능향상을 이끄는 중요한 인공지능 기술이다[1].

본 논문에서는 Keras[2] 오픈소스 라이브러리를 이용한 딥러닝 기계학습 기반의 동전 인식 소프트웨어를 구현하였고, 이를 이용해 동전 자동분류 스마트 저금통을 설계하였다. 동작 검증을 위하여 스마트 저금통의 모든 발생 이벤트는 Parse-server와 mongoDB를 이용하여 시각화 및 어플리케이션 및 웹사이트를 연결시스템을 구현하였다. 논문의 구성은 다음과 같다. 2장에서는 기계학습 기반의 이미지 인식을 위한 오픈소스 플랫폼을 소개한다. 3장에서는 제안 시스템을 설계하고, 4장에서는 구현 결과를 소개한다. 마지막 5장에서 결론을 맺는다.

2. 관련 연구

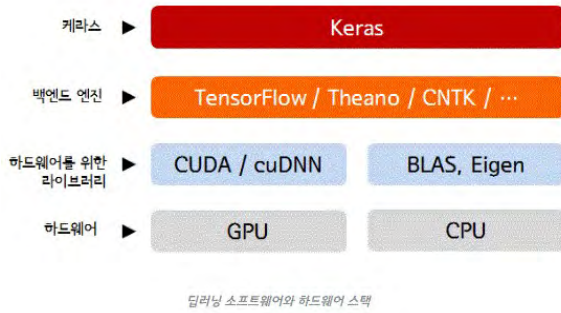
(그림 1)은 제안 시스템의 구현 도구들을 보여주고 있으며, 인공신경망 API인 Keras[2], TensorFlow[3], OpenCV[4] 이미지프로세싱 라이브러리로 구성되어 있다.



(그림 1) 오픈소스 라이브러리 및 API

2.1 TensorFlow

TensorFlow는 기계학습 시스템으로 이미지 인식, 반복 신경망, 기계 번역, 자연어 처리, 필기 글씨 인식 등의 분야에서 신경망 학습을 실행하며, 이미지 분석에 일반적으로 적용되는 합성곱 신경망(Convolutional Neural Network, CNN)[5]을 위하여 Data Flow Graph를 사용하여 연산한다. 특히, Multi-GPU를 쉽게 구현 가능하며, 별도의 코드 없이 GPU를 인식하고 동작한다. (그림 2)는 TensorFlow 이용을 위한 딥러닝 소프트웨어와 하드



(그림 2) 딥러닝 소프트웨어와 하드웨어 스택

웨어 스택을 보여준다.

2.2 Keras

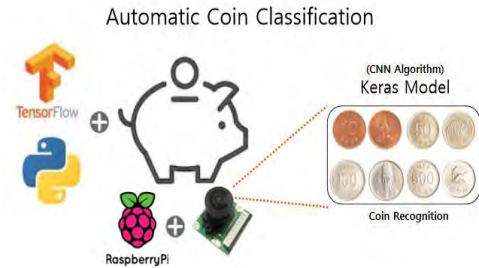
Keras는 파이썬으로 작성된 신경망 API로 TensorFlow와 함께 사용한다. 일반적으로 Keras 모델링은 Dataset 생성, Convolution2D Layer와 maxPooling Layer, Dense Layer, Flatten Layer 등 여러 Layer로 신경망이 구성된 Sequence 모델 생성, 모델의 학습 과정 설정, Training Dataset을 이용하여 구성된 모델로 학습, 모델 학습 시 손실 및 정확도 측정, Test Dataset을 이용하여 모델 평가, 학습결과 생성된 모델을 이용한 예측 단계로 진행된다.

2.3 OpenCV

OpenCV는 컴퓨터 비전을 목적으로 한 오픈소스 라이브러리로 CV(이미지프로세싱과 비전 알고리즘), MLL(통계 분류기와 집단화 도구), HighGUI(그림, 비디오 입출력), CXCORE(기본구조와 알고리즘) 이 4가지로 분류된다[4].

3. 시스템 설계

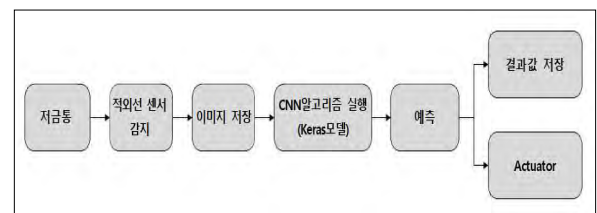
(그림 3)은 스마트 저금통의 전체 구성도를 보여준다. 라즈베리파이와 220도 초광각 카메라를 이용하여 이미지 촬영을 진행하여 만든 이미지 Dataset을 PC에서 Python을 이용해 TensorFlow의 Keras API를 이용하여 동전의 학습과 분석을 한다.



(그림 3) 시스템 구성도

3.1 하드웨어 설계

스마트 저금통은 내부에 장착된 라즈베리파이와 카메라를 이용해 자동으로 동전을 분류한다. (그림 4)는 전체 동작 과정을 보인다. 적외선 모듈에 동전이 인식되면 이미지 촬영이 이루어지며 폴더에 저장된 사진을 이용하여 이미지 분석을 한다. 학습되어 있던 모델을 토대로 결과를 예측하게 된다. 예측이 끝나면 결과에 따라서 서보모터가 작동되어 동전이 분류된다.



(그림 4) 동전 분석 및 예측 과정

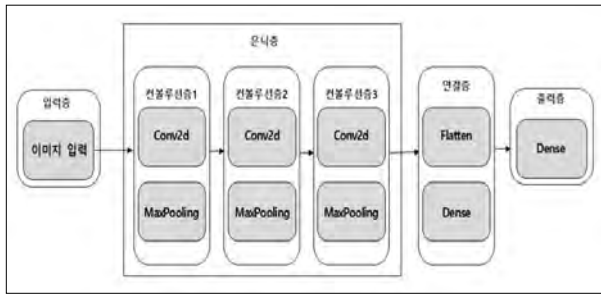
3.2 학습 데이터 추출

양면으로 디자인된 동전은 저금통 내에서 촬영 때 다양한 각도에 따라 그림자 방향이 일정하지 않은 환경에서 특징 추출을 해야 한다. 따라서 다양한 각도의 동전 학습 데이터 구성을 위하여 분류에 필요한 여러 동전을 여러 각도로 촬영을 하여 학습 데이터 10,000장을 추출하였다. 다음은 OpenCV를 이용한 이미지 전처리 과정을 거쳐 96*96 크기로 resize 된 10,000장의 이미지 데이터는 동전별로 2500개씩, 동전의 앞뒤를 구분하기 위해 각 동전 면마다 1250개씩 총 8개의 카테고리로 나뉘어 Scikit-learn 라이브러리를 이용해 numpy 배열형태의 Dataset을 생성하였다.

3.3 학습모델 설계

학습모델은 TensorFlow 라이브러리 Keras를 이용하여 CNN 알고리즘을 구현하였다. 은닉층에서 3개의 Convolution Layer, 3개의 maxPooling Layer, 연결층에서 1차원 벡터로 변환시키기 위한 Flatten

Layer, Dense Layer를 설계하였으며, 출력층에서 다시 Dense Layer를 이용하여 8개의 카테고리과 일치되게 설계하였다(그림 5). 각 Layer의 활성화 함수로 역전파 시에 좋은 성능을 내는 ReLU(Rectified Linear Unit) 함수를 사용하였다. 위의 sequential 모델을 통해 만들어진 학습모델을 'cnn_CoinBox.h5'로 저장한다.



(그림 5) 학습모델 설계 블록도

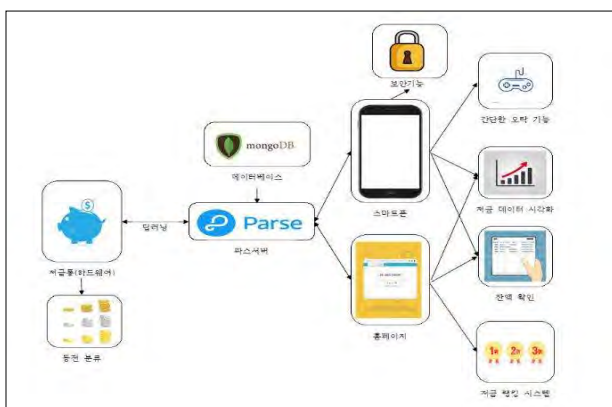
3.4 학습결과 예측

(그림 4)는 라즈베리파이에서 실행하는 부분으로 저장된 이미지는 학습된 모델을 가져와 비교 후 예측을 한다. 예측 결과는 Parse-server에 저장되며 동전 분류에 따른 해당 동전함으로 이동을 위하여 서보모터를 구동한다.

4. 시스템 구현 및 결과

4.1 시스템 구조

전체 시스템 구조는 (그림 6)과 같이 하드웨어로부터 Parse-server를 통해 사용자의 어플리케이션 또는 웹페이지로 각종 데이터를 주고받는다.



(그림 6) 시스템 구조 블록도

4.2 TensorFlow-Keras Model

<표 1>의 학습 환경에 사용된 시스템 사양을 보여준다. Keras 모델을 이용하여 100%에 가까운 학습 결과를 추출한다.

(그림 7)의 테스트 이미지를 통해, (그림 8)과 같이 테스트한 8개의 이미지가 정확하게 구분되는 결과를 보인다.

<표 1> 학습 환경

CPU	AMD Ryzen 2 2600
Clock	3.4GHz
Core	6
Thread	12
Memory	16GB



(그림 7) 검증 데이터

```
test (1).jpg : 100back
test (2).jpg : 100front
test (3).jpg : 50back
test (4).jpg : 50front
test (5).jpg : 500front
test (6).jpg : 500back
test (7).jpg : 100back
test (8).jpg : 100back
```

(그림 8) 검증 결과

5. 결론

본 논문에서는 Keras 오픈소스 라이브러리를 이용해 딥러닝을 이용한 기계학습 기반의 동전 인식 소프트웨어를 구현하였고, 이를 이용해 동전 자동분류 스마트 저금통을 설계하였다. 동작 검증을 위하여 스마트 저금통의 모든 발생 이벤트는 Parse-server와 mongoDB를 이용하여 시각화 및 어플리케이션 및 웹사이트를 연결하였다. 추후 클라우드 컴퓨팅을 활용하여 사용자들의 저금으로 인해 쌓이는 빅데이터를 분석하는 기술을 구현할 계획이다.

참고문헌

- [1] 최희열, 민윤홍, 딥러닝 소개 및 주요 이슈, 정보처리학회지, 제22권 제1호, 2015
- [2] <https://keras.io3>
- [3] <https://www.tensorflow.org>
- [4] <https://opencv.org>
- [5] L. Kang, P. Ye, Y. Li, and D. Doermann, "Convolutional neural networks for no-reference image quality assessment," in Proceedings of the IEEE conference on computer vision and pattern recognition, 2014, pp. 1733 - 1740

조건부 랜덤 포레스트 기반의 설명 가능한 일사량 예측

문지훈, 황인준
고려대학교 전기전자공학과
johnny89@korea.ac.kr, chwang04@korea.ac.kr

Explainable Solar Irradiation Forecasting Based on Conditional Random Forests

Jihoon Moon, Eenjun Hwang
School of Electrical Engineering, Korea University

요 약

태양광 발전은 이산화탄소 배출로 인한 기후 변화에 대응하는 주요 수단으로 인식되어 수요와 필요성이 급격하게 증가하고 있다. 최적의 태양광 발전 시스템의 운영을 위해서는 정교한 전력수요 및 태양광 발전량 예측 모델이 요구되며, 온도 및 일사량은 태양광 발전량 예측 모델의 필수적인 입력 변수이다. 하지만, 한국 기상청의 동네예보는 일사량에 관한 예측값을 제공하지 않아 정교한 태양광 발전량 예측 모델을 구축하는 것은 어렵다. 이를 위해 일사량 예측 기법에 관한 많은 연구 사례가 보고되고 있지만, 다수의 연구들은 충분한 데이터 셋을 이용하여 일사량 예측 모델을 개발하였다. 초기 태양광 발전 시스템 운영을 위해서는 불충분한 데이터 셋을 이용한 예측 모델 개발이 필요하나 이에 대한 사례는 불충분하다. 본 논문은 실제 태양광 발전 시스템에서 수집된 불충분한 데이터 셋을 이용한 단기 일사량 예측 기법을 제안한다. 먼저, 기상청 동네예보의 다양한 기상 요인들을 이용하여 일사량 예측 모델을 위한 입력 변수를 구성한다. 다음으로, 조건부 랜덤 포레스트를 이용하여 일사량 예측 모델을 구성하며, 설명 가능한 일사량 예측뿐만 아니라 더욱더 많은 데이터 셋을 학습하기 위해 시계열 교차검증을 수행한다. 실험 결과, 제안한 기법은 다른 예측 기법들보다 높은 예측 정확도를 보일 뿐만 아니라 설명 가능한 예측 결과를 제시할 수 있음을 보여준다.

1. 서 론

최근 기후 변화 및 에너지 부족 문제를 대비하기 위해 신재생 에너지(Renewable Energy)를 적극 활용한 스마트 그리드 기술의 관심이 커지고 있다[1]. 스마트 그리드(Smart Grid)는 정보통신기술(ICT: Information and Communication Technologies)을 기존의 전력망과 접목하여 에너지 효율을 최적화하는 기술이다[1,2]. 신재생 에너지는 스마트 그리드의 핵심 요소 중 하나이며, 태양광(PV: Photovoltaics), 풍력 등과 같은 천연 자원을 통해 목적에 따라 전기 생산이 가능하다[3]. 태양광 발전은 공간 제약 없이 설치할 수 있는 장점이 있어, 이와 관련된 기술이 빠르게 발전하고 있다[1,3].

태양광 발전 시스템은 다양한 기상 요인으로 인해 발전에 크게 영향을 받으며, 일사량(Solar Irradiation)은 태양광 발전의 중요한 요인이다[4]. 그러나 기상청의 동네예보는 기온, 습도 등과 같은 기상 요인의 예측값은 제공하지만 일사량의 예측값은 제공하지 않는다[5]. 따라서, 국내 태양광 발전 시스템의 운영을 위해서는 정확한 일사량 예측 모델이 필요하다. 그리하여,

인공지능(AI: Artificial Intelligence) 기술 기반의 일사량 예측 기법에 관한 많은 연구가 수행되었다[3-5].

다수의 연구들은 일정 기간 이상의 충분한 데이터 셋을 사용하여 예측 모델 구성 및 예측 성능 평가를 수행하였으나, 불충분한 데이터 셋을 사용하여 인공지능 기술을 기반으로 일사량을 예측한 사례는 미미하다. 따라서, 초기 태양광 발전 시스템의 효율적인 운영을 위해서는 불충분한 데이터 셋을 통해 정교한 예측 모델을 구성할 필요가 있다. 의사결정나무 기반 알고리즘들은 작은 데이터 셋에서도 만족스러운 예측 성능이 가능하다[6,7].

본 논문은 불충분한 데이터 셋을 이용하여 조건부 랜덤 포레스트(CRF: Conditional Random Forests) 기반의 일사량 예측 기법을 제안하고, 예측 성능을 다중선형 회귀(MLR: Multiple Linear Regression) 및 다양한 의사결정나무 기반의 알고리즘들과 비교한다. 본 논문의 주요 기여도는 아래와 같다.

- 조건부 랜덤 포레스트를 기반으로 예측 모델을 구축하여 다중 단기 일사량 예측을 수행한다.
- 국내 태양광 발전 시스템의 적용 가능성을 위해

기상청의 동네예보에 포함된 7 가지 기상 요인을 모두 고려한다.

- 예측 모델의 변수 중요도(Variable Importance)와 시계열 교차검증을 이용하여 예측값을 도출하는 과정을 설명한다.

본 논문의 나머지 부분은 아래와 같다. 2 장에서는 일사량 예측 모델을 위한 입력 변수 및 모델 구성에 대해 자세히 기술한다. 3 장에서는 예측 모델의 예측 성능을 비교 및 평가하기 위한 실험 과정을 기술하고 이를 논의한다. 4 장에서는 결론과 향후 연구 방향을 제시함으로 본 논문의 끝을 맺는다.

2. 일사량 예측 모델 구성

불충분한 데이터 셋을 이용하여 예측 모델을 구성하기 위해, 실제 대전에 있는 태양광 발전 시스템의 일사량 데이터를 수집하였다. 수집된 데이터 기간은 2018 년 6 월로 1 달 치의 데이터이며, 오전 6 시부터 저녁 8 시까지의 실측값으로 구성되어 있다. 표 1 에 수집된 데이터의 통계적 분석 결과를 나타내었다.

<표 1> 수집된 데이터의 통계적 분석 결과(단위: W/m²)

기술 통계법	통계량 값
평균	330.07
표준 오차	12.93
중앙값	254.50
표준 편차	274.35
범위	805
최소값	0
최대값	805
합	148529.40
관측수	450

2.1. 입력 변수 구성

예측 모델을 위한 입력 변수를 구성하기 위해 기상청의 동네예보에서 제공하는 강수형태, 습도, 강수량, 하늘상태, 기온, 풍향, 풍속의 실측값을 기상자료개방포털에서 수집하였다. 여기서, 강수형태와 하늘상태는 범주형 데이터로 이루어지며, 강수형태는 비가 왔을 때에는 1, 그렇지 않으면 0 인 명목형 데이터로 구성되어 있다. 하늘상태는 맑음, 구름 조금, 구름 많음, 흐림을 각 1 부터 4 까지로 표기한 순서형 데이터로 구성되어 있다. 나머지 실측값인 습도, 강수량, 기온, 풍향, 풍속은 연속형 데이터의 특징을 가지고 있다.

시간 정보를 반영하기 위해, 6 시부터 20 시까지 총 15 시간 간격에 대해 명목 척도로 데이터 셋을 구성하였다. 이는 아침과 저녁에는 일사량이 적고 오후 시간대에는 일사량이 많은 일사량의 특정 시간대의 특징을 더욱 효과적으로 반영할 수 있다.

이뿐만 아니라, 과거 일사량 패턴 및 추세를 반영하기 위해, 예측 시점에서 과거 2 일의 일사량과 습도, 강수량, 하늘상태, 기온, 풍속, 풍향으로 총 14 개의

입력 변수를 구성하였다. 본 논문에서 고려한 입력 변수는 총 36 개이며 표 2 에 기술하였다.

<표 2> 예측 모델의 입력 변수 구성 및 특징

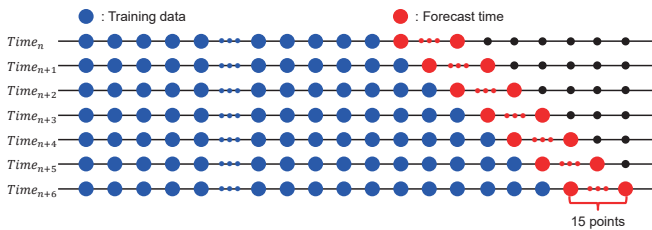
IV #	입력 변수 (특징)	IV #	입력 변수 (특징)
IV01	6 시 (명목형)	IV19	2 일 전 기온 (연속형)
IV02	7 시 (명목형)	IV20	2 일 전 풍향 (연속형)
IV03	8 시 (명목형)	IV21	2 일 전 풍속 (연속형)
IV04	9 시 (명목형)	IV22	2 일 전 일사량 (연속형)
IV05	10 시 (명목형)	IV23	1 일 전 습도 (연속형)
IV06	11 시 (명목형)	IV24	1 일 전 강수량 (연속형)
IV07	12 시 (명목형)	IV25	1 일 전 하늘상태 (순서형)
IV08	13 시 (명목형)	IV26	1 일 전 기온 (연속형)
IV09	14 시 (명목형)	IV27	1 일 전 풍향 (연속형)
IV10	15 시 (명목형)	IV28	1 일 전 풍속 (연속형)
IV11	16 시 (명목형)	IV29	1 일 전 일사량 (연속형)
IV12	17 시 (명목형)	IV30	강수형태 (명목형)
IV13	18 시 (명목형)	IV31	습도 (연속형)
IV14	19 시 (명목형)	IV32	강수량 (연속형)
IV15	20 시 (명목형)	IV33	하늘상태 (순서형)
IV16	2 일 전 습도 (연속형)	IV34	기온 (연속형)
IV17	2 일 전 강수량 (연속형)	IV35	풍향 (연속형)
IV18	2 일 전 하늘상태 (순서형)	IV36	풍속 (연속형)

2.2 예측 모델 구성

본 연구는 랜덤 포레스트와 유사하지만 다른 접근 방식을 갖는 조건부 랜덤 포레스트를 이용하여 단기 일사량 예측 모델을 구성한다. 이러한 이유로 조건부 랜덤 포레스트의 나무 구조는 랜덤 포레스트의 나무 구조보다 데이터를 편향적으로 학습하지 않으므로, 평가 집합(Test Set)에서 출력 변수를 예측할 때, 훈련 집합(Training Set)에서 모델 학습의 과적합(Overfitting) 문제 해결에 더 적합하기 때문이다[6]. 이뿐만 아니라 예측값을 평균화하는 랜덤 포레스트의 나무 구조와 달리, 조건부 랜덤 포레스트는 입력 변수의 가중치를 평균화하여 예측값을 도출하기 때문에 변수 중요도를 나타내었을 때, 더욱 효과적으로 모델 구조에 관해 설명이 가능하다. 본 논문에서는 적은 데이터 셋을

다루므로, 많은 데이터 셋을 요구하는 심층 신경망(DNN: Deep Neural Network)이나 Boosting 계열의 알고리즘들(예: XGBoost, LightGBM)을 고려하지 않았다[7].

또한, 본 연구는 점차 많은 데이터 셋을 학습하기 위해 시계열 교차검증(TSCV: Time Series Cross-Validation)을 적용한다. 시계열 교차검증은 그림 1 과 같이 각 예측 시점에서 예측 모델의 훈련 집합은 첫 시점부터 이전의 관측 시점까지 구성된다. 그리하여 각 예측 시점에 구성된 예측 모델은 1 시점 뒤부터 15 시점 뒤까지 다중 시점의 일사량을 예측하며, 각 시점의 예측 정확도를 계산하고 이를 평균값을 계산하여 예측 모델의 성능을 평가한다.



(그림 1) 다중 시점 예측을 위한 시계열 교차검증

3. 실험 및 평가

본 논문에서 제안한 예측 모델의 성능을 평가하기 위해, 전체 데이터 셋을 일자별로 분리하였으며, 6 월 1일부터 2 일은 입력 변수를 위해 데이터를 이용하며, 3일부터 23 일 총 3 주의 기간은 훈련 집합으로 24 일 부터 30 일 총 1 주는 평가 집합으로 선정하여 실험을 진행하였다. 예측 기법으로 조건부 랜덤 포레스트와 예측 성능을 비교하기 위해, 다중선형회귀, 의사결정 나무(DT: Decision Tree), GBM(Gradient Boosting Machine), 랜덤 포레스트(RF: Random Forest)로 총 4 가지의 기법 들을 이용하였다. 실험 환경은 R 3.5.1 버전의 RStudio 1.1453 버전에서 진행하였다. Grid Search 를 통해 각 예측 기법에 관한 최적의 초매개변수(Hyperparameter) 값을 선정하였으며, 이는 표 3 과 같다.

<표 3> 각 예측 기법에서 선정된 초매개변수의 값

예측 기법	패키지	초매개변수의 값
GBM	<i>gbm</i>	<ul style="list-style-type: none"> <i>distribution</i>: gaussian <i>shrinkage</i>: 0.001 <i>interaction.depth</i>: 5 <i>bag.fraction</i>: 0.5 <i>n.trees</i>: 3000 <i>cv.folds</i>: 5
RF	<i>randomForest</i>	<ul style="list-style-type: none"> <i>mtry</i>: 12 <i>ntree</i>: 128
CRF	<i>party</i>	<ul style="list-style-type: none"> <i>mtry</i>: 6 <i>ntree</i>: 500

예측 모델의 예측 정확도를 평가하기 위해, 제공된 평균제곱오차(RMSE: Root Mean Square Error) 및 평균 절대오차(MAE: Mean Absolute Error)를 사용하였으며, 이는 식 1, 2 와 같다. A' 와 F' 는 실제 관측된 일사량과 일사량 예측값을 나타내며, n 은 관측치의 수이다.

$$RMSE = \sqrt{\sum (F' - A')^2 / n} \quad (1)$$

$$MAE = 1 / n \times \sum |F' - A'| \quad (2)$$

표 4 와 5 는 각 예측 시점에 관한 예측 모델들의 RMSE 와 MAE 의 결과이다. 표에서 붉게(Red) 표기된 것은 낮은 예측 성능을 나타내며 푸르게(Blue) 표기된 것은 우수한 예측 성능을 나타낸다. 아래의 표에서 나타난 것과 같이, 현재 시점과 예측 시점의 간격이 멀어질수록 예측 성능이 저하된다는 것을 확인할 수 있다. 또한, 조건부 랜덤 포레스트는 다른 예측 기법 보다 더욱 우수한 예측 성능을 보인다는 것을 확인할 수 있었다.

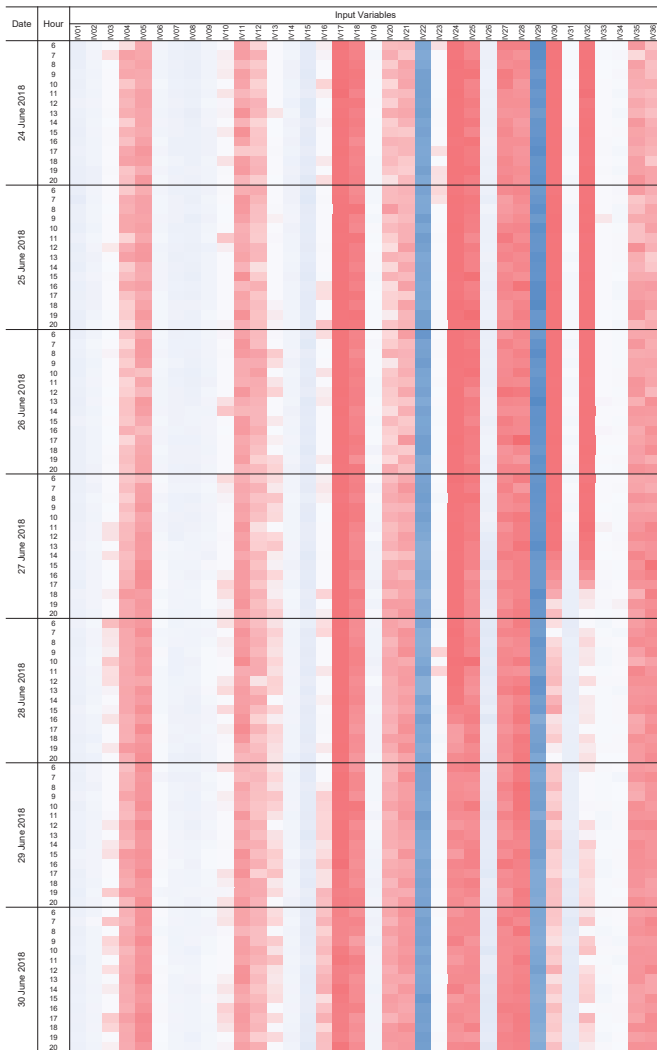
<표 4> 각 예측 시점에서 예측 모델들의 RMSE

예측 시점	MLR	DT	GBM	RF	CRF
1	199.56	189.08	147.68	169.40	138.77
2	227.03	195.91	160.56	174.92	153.06
3	250.22	207.50	168.36	178.94	163.00
4	265.22	214.04	173.87	182.27	165.88
5	300.24	221.01	177.73	183.52	166.68
6	306.06	230.33	179.54	183.64	170.06
7	318.77	232.26	181.25	183.21	171.35
8	321.69	229.44	182.22	184.24	171.60
9	323.54	231.31	183.02	185.12	169.67
10	327.85	231.13	182.91	185.64	171.43
11	336.13	226.83	182.85	186.79	171.05
12	335.62	221.47	182.48	186.10	171.01
13	336.86	216.80	182.86	185.64	169.37
14	338.19	210.27	182.79	185.73	169.13
15	338.87	201.23	183.03	186.10	169.21

<표 5> 각 예측 시점에서 예측 모델들의 MAE

예측 시점	MLR	DT	GBM	RF	CRF
1	140.54	127.58	106.27	125.20	100.52
2	154.92	134.67	114.79	129.16	110.15
3	167.05	141.21	119.83	132.11	118.38
4	175.09	145.18	123.58	133.02	119.93
5	188.80	148.93	125.83	133.94	120.51
6	196.21	154.29	126.05	134.08	122.53
7	205.31	156.23	126.66	133.10	122.15
8	209.63	153.40	126.96	133.89	121.71
9	210.26	155.30	127.28	134.59	120.23
10	212.71	155.57	127.40	134.74	122.07
11	217.35	151.59	127.19	135.25	121.61
12	218.11	146.59	127.15	135.36	120.44
13	219.39	142.56	127.35	134.71	119.67
14	219.95	136.87	126.84	134.96	120.35
15	220.54	132.34	127.02	134.99	118.54

그림 2 는 단기 일사량 예측 모델을 구성하기 위해, 조건부 랜덤 포레스트를 시계열 교차검증을 이용해 학습 시켜 구성된 예측 모델의 변수 중요도를 히트맵 그래프를 통해 시간대별로 나타낸 것이다. 그림에서 붉게(Red) 표기된 것은 낮은 변수 중요도를 나타내며, 푸르게(Blue) 표기된 것은 높은 변수 중요도를 나타낼 뿐만 아니라 주요 변수라고 판단할 수 있다.



(그림 2) 각 예측 시점에서 예측 모델의 변수 중요도

그림 2에서 확인할 수 있듯이, 과거 2일의 일사량 관측치는 예측 모델에서 매우 중요한 입력 변수이며, 실제 단기 일사량을 예측할 때 주요 요인이라는 것을 알 수 있다. 또한, 2018년 6월 27일 이후로 강수형태 및 강수량의 변수 중요도가 높아졌다는 것을 확인할 수 있다. 이는 2018년 6월 1일부터 27일 오후까지 비가 오지 않아 값이 0으로 측정되어 예측 모델을 학습할 때 중요한 변수라는 것을 판단하지 못했으나, 비가 온 시점부터는 비로 인해 일사량이 없다는 것을 예측 모델 학습에 인지하고 이에 관한 가중치를 높임으로 변수 중요도가 높아졌다는 것을 확인하였다. 그 외에도 하늘상태와 기온은 일사량 예측 모델의 주요 변수라는 것을 확인하였다.

4. 결론

본 논문은 불충분한 데이터 셋에서 정확한 일사량 예측을 수행하기 위해, 조건부 랜덤 포레스트 기반의 다중 단기 일사량 예측 기법을 제안하였다. 태양광 발전 시스템에 적용 가능성을 높이기 위해, 기상청의 동네예보에서 제공하는 정보를 이용하여 예측 모델의 입력 변수를 구성하였다. 다음으로 적은 데이터 셋에서도 효과적으로 모델을 학습할 수 있는 조건부 랜덤

포레스트를 이용하여 예측 모델을 학습하고, 더욱더 많은 데이터의 학습과 최근 일사량 패턴 및 추세를 반영하기 위해 시계열 교차검증을 적용하였다. 예측 모델은 점 예측 방식이 아닌 다중 예측 방식으로 1시점 뒤 시점부터 15시점 뒤 시점까지 총 15시점을 예측하여 예측 불확실성을 대비하는 데 도움을 줄 수 있었다. 제안한 예측 기법은 다양한 예측 기법들과 비교하여 더욱 우수한 예측 성능을 보였으며, 변수 중요도를 통해 과거 일사량과 기온, 하늘상태 등이 향후 일사량을 예측할 때 주요 변수라는 것을 확인할 수 있었다.

본 논문에서는 실제 수집된 태양광 발전 시스템의 일사량 데이터가 한 달 치만 수집되어 다양한 환경의 일사량 데이터를 통해 실험을 진행하기가 어려웠다. 향후, 일사량 데이터를 수집하여 다양한 기간, 지역 등을 고려하여 범용성을 가질 수 있는 일사량 예측 모델을 개발할 계획이다.

사사문구

이 연구는 2019년도 정부(과학기술정보통신부)의 재원으로 한국연구재단-에너지클라우드기술개발사업(No. 2019M3F2A1073184) 및 한국전력공사의 2018년 착수 에너지 거점대학 클러스터 사업(No. R18XA05)의 지원을 받아 수행된 연구임.

참고문헌

- [1] X. Huang, J. Shi, B. Gao, Y. Tai, Z. Chen, and J. Zhang, "Forecasting Hourly Solar Irradiance Using Hybrid Wavelet Transformation and Elman Model in Smart Grid," *IEEE Access*, Vol. 7, pp. 139909-139923, 2019.
- [2] J. Kim, J. Moon, E. Hwang, and P. Kang, "Recurrent inception convolution neural network for multi short-term load forecasting," *Energy and Buildings*, Vol. 194, pp. 328-341, 2019.
- [3] M. Paulescu and E. Paulescu, "Short-term forecasting of solar irradiance," *Renewable Energy*, Vol. 143, pp. 985-994, 2019.
- [4] Y. Kwon, A. Kwasinski, and A. Kwasinski, "Solar Irradiance Forecast Using Naïve Bayes Classifier Based on Publicly Available Weather Forecasting Variables," *Energies*, Vol. 12, p. 1529, 2019.
- [5] S. Jung, J. Moon, S. Park, and E. Hwang, "A Probabilistic Short-Term Solar Radiation Prediction Scheme Based on Attention Mechanism for Smart Island," *KIISE Transactions on Computing Practices*, Vol. 25, No. 12, pp. 602-609, 2019.
- [6] C. Strobl, A.-L. Boulesteix, A. Zeileis, and T. Hothorn, "Bias in random forest variable importance measures: Illustrations, sources and a solution," *BMC Bioinformatics*, Vol. 8, p. 25, 2007.
- [7] J. Moon, J. Kim, P. Kang, and E. Hwang, "Solving the Cold-Start Problem in Short-Term Load Forecasting Using Tree-Based Methods," *Energies*, Vol. 13, p. 886, 2020.

클라우드 기반의 실험실정보관리시스템 구축 및 SaaS 제공 방안에 관한 연구

임복출*, 류기상**

*주식회사 위컴즈

**주식회사 호원소프트

wiseaman.lim@wecom.com, wondboy@naver.com

A Study on How to Build a Cloud-based Laboratory Information Management System and Provide SaaS(Software as a Service)

Bock-Chool Lim*, Ki-Sang Ryu**

*Wecom Inc.

**Howonsoft Inc.

요 약

실험실정보관리시스템(LIMS)은 실험실 데이터를 저장, 가공, 검색 그리고 분석하기 위한 중앙화된 데이터베이스로서 정유, 석유화학, 정밀화학, 제조업, 금속, 제철, 식품, 의약, 연구소, 보건환경, 검사소 등 다양한 분야에 말라하여 적용이 가능한 시스템이다. LIMS를 재고 관리, 임상 연구, 프로젝트 관리 및 환자 데이터 관리를 위한 강력한 IT도구라고 하면서 특히 의료 분야에서 환자 치료가 향상되고 서비스 효율성이 높아질 것이라고 하고, 운영 비용의 절감이 가능하다. 확장성 및 비용절감과 핵심 기능을 위주로 제공하는 클라우드 및 웹 기반 솔루션의 발전으로 제4차 산업혁명의 핵심기술의 산증인의 분야로 기대가 된다.

1. 서론

실험실정보관리시스템(LIMS, Laboratory Information Management System, 이하 LIMS)은 실험실 데이터를 저장, 가공, 검색 그리고 분석하기 위한 중앙화된 데이터베이스로서 검사, 분석, 시험 업무를 수행하는 실험실을 위해 특별히 고안된 컴퓨터 시스템 또는 시스템을 의미한다[1].

2015년 중반에 프로스트 앤 설리번은 2000년 중반부터 LIMS는 높은 비용과 긴 수명으로 큰 성장을 하지 못했다고 하면서 앞으로 몇 년간 클라우드 기반 솔루션들이 도입돼 비용 절감과 특정 실험실들에서 요구되는 설정 기능들이 향상되면서, 성숙단계에 접어든 LIMS 시장에 다시 한번 성장하게 될 것이라고 예측하였다[2].

2. 관련연구

2.1. 실험실정보관리시스템(LIMS)

LIMS는 실험실의 목적에 따라서 다양한 LIMS 제품이 존재하며, 실시간 품질정보 공유에 따른 공

정별 정보를 조기에 반영 가능하도록 하고, 품질지향 모니터링을 통해 공정의 안정화를 꾀하며, 과학적 품질 통계 관리를 통하여 품질개선 효과를 기대할 수 있다. 정유, 석유화학, 정밀화학, 제조업, 금속, 제철, 식품, 의약, 연구소, 보건환경, 검사소 및 기타 관련 분야를 망라하여 실험실내 시험 분석 업무에는 어느 곳이든 적용이 가능하다[2].

LIMS가 가지고 있는 장점에도 불구하고 업무 목표와 업무 절차를 명확하게 분석하지 않은 채, 외국 패키지 LIMS를 막연한 기대와 기능 중심으로 검토 및 도입하여 제한적으로 커스터마이징을 함으로써 실험 데이터의 데이터베이스화에 그친 경우가 대부분이다. 설치와 관련한 높은 비용 및 On-premise LIMS 장점으로 영국과 미국, 그리고 서유럽 국가와 같은 선진국에서의 시장 집중도가 높았다. 그러나 확장성 및 비용절감과 핵심 기능을 위주로 제공하는 클라우드 및 웹 기반 솔루션의 확산과 홍보로 인해 시장은 클라우드 기반 솔루션에 대한 수요가 전체적으로 증가하면서 LIMS 도입의 패러다임 변화가 목격되고 있다[3].

2.2. 클라우드 기반의 SaaS

Cloud service는 서비스이용자가 정보 자원(SW, Platform, Storage, Server, NW 등)을 필요한 만큼 빌려서 사용하고, 서비스 부하에 따라서 실시간 확장성(scalability)을 지원받으며, 필요한 순간에 접속하여, 사용한 만큼 비용을 지불하는 서비스로 공유된 컴퓨팅 자원이 신속히 제공되고, 회수되는 서비스를 의미한다[4].

SaaS를 기존의 ASP와 비교해 보면, 소프트웨어를 인터넷을 통해 사용하는 점에서는 차별성이 없으나 사용자를 위한 커스터마이징을 ASP와 다르게 사용자가 직접 할 수 있다는 점과 사용자들 또는 사용자 그룹으로 표현되는 테넌트들을 하나의 소프트웨어 인스턴스로 지원(single instance multitenant)한다는 점에서 차별성을 갖는다. 이는 커스터마이징에 많은 비용이 들고 인스턴스를 개별적으로 띄우기 때문에 규모의 경제를 실현하지 못했던 ASP의 단점을 해결한다[5].

SaaS 플랫폼의 핵심 기술은 멀티테넌시를 지원하여 테넌트별 요구사항이 반영되도록 하는데 있다. 플랫폼은 테넌트들에게 테넌트별로 구성 변경된 서로 다른 서비스와 독립된 서비스 개발 환경을 제공한다[6].

3. SaaS 제공을 위한 실험실정보관리시스템 설계 및 구현

3.1. 사용자 DB 공유 구조 기반의 SaaS 설계

SaaS 플랫폼의 핵심 기술인 멀티테넌시는 (1)다수의 테넌트가 동일한 리소스에 접근, (2)데이터, 환경설정 및 세션의 독립성 보장, (3)다양한 SLA (Service Level Agreement)에 따른 실행 환경 구조 선택이 가능해야 한다. TTA의 표준안에서는 멀티테넌시를 제공하기 위하여, (1)계정 강제(Identity Enforcement) 기법, (2)설정 분리(Configuration Isolation) 기법, (3)데이터 및 세션 분리(Data & Session Isolation) 기법 등을 제안하였다[7].

본 논문에서는 데이터 및 세션 분리를 위한 방안으로 서비스 사용자 DB 공유 구조 기반의 SaaS를 설계하여 LIMS를 클라우드를 통하여 제공시 각 사용자별로 독립된 서비스를 제공하고자 한다.

서비스 사용자 DB 공유 구조는 분리 데이터베이스(Separate Physical Database), 공유 데이터베이스-분리 스키마(Shared Database, Separate Schema),

공유 데이터베이스-공유 스키마(Shared Databases, Shared Schema)로 분류할 수 있다[7].



(그림 1) 서비스 사용자 DB 공유 구조

3.2. LIaaS 구현 : LIMS as a Service

클라우드 기반 서비스 SaaS를 사용하고자 할 경우에는 ‘서비스 신청 -> 제품 선택 -> 결제 -> 서비스 사용’의 단계로 진행되는 정액제 형태의 서비스와 ‘서비스 신청 -> 서비스 사용 -> 사용량에 따른 비용 청구 -> 결제’의 단계로 진행되는 후불제 서비스의 형태가 일반적이다.

LIMS를 SaaS에서 제공하는 형태는 ‘기능별로 컴포넌트를 구매 및 결제 후 사용하는 방식’으로 정액제 형태로 제공하며, 이를 위하여 LIaaS를 신청하고 사용료를 결제하기 위하여 클라우드 샵(SaaS를 신청 및 결제하기 위한 스토어)을 구성하며, 이를 통하여 해당 서비스를 신청 및 사용할 수 있다.



(그림 2) 회원가입 및 제품 구매

LIaaS의 서비스 신청은 ‘회원가입’시 서비스 레벨에 따라 테넌트에서 사용하는 서비스 사용자 DB를 (1)독립실행형, (2)독립DB형, (3)독립데이터형으로 제공한다. 독립실행형은 별도의 가상 이미지로 제공되는 형태이며, 독립DB형은 테넌트별 독립적인 DB공간을 제공하는 형태이며, 마지막으로 독립데이터형은 테넌트구분자를 통하여 동일한 DB에 독립된 서비스로 제공되는 형태이다. 또한 테넌트의 생성시점을 회원가입 시점이 아닌 회원가입을 완료한 뒤에 가입시 기입한 이메일로 서비스 인증을 완료하여야 테넌트가 생성되며, 이를 사용하기 위하여 제품

구매 및 결제를 완료하면 서비스 이용이 가능하다.

LIaaS는 실험실정보관리를 위한 기능을 제공하며 해당 기능의 상세 설명은 다음과 같다.

(표 1) Lims as a Service 기능

	상세 기능 설명
LIMS 공통기능	<ul style="list-style-type: none"> • 행정자치부에서 보급하는 개방형 전자정부표준 프레임워크 적용 개발 • 실험실정보관리 업무를 분석하여 최적의 지원 프로세스 구축 • 편리한 표준 화면 레이아웃 설계 • Web(NginX 등), WAS(Web Application Server, Tomcat 등), DB(Maria DB 등)을 지원 • HTML5 표준 준용으로 non-ActiveX 환경으로 멀티 브라우저 지원 • 기존에 관리되는 실험실정보데이터 활용을 위하여 import 기능 지원
시험성적서 관리	<ul style="list-style-type: none"> • 성적서 발급 및 재발급 이력관리 • 조건별 의뢰건수 및 부적합 등 실적 조회 및 자동 출력 양식 • 관련법규 및 관리업무상에서 요구되는 산출물 양식 자동 출력 지원 • 시험성적서 바코드 등록, 검사원 및 결재자 인(sign) 등록 기능 • 국문, 영문 일괄 자동 출력 기능 구현, 필요시 중문 성적서 • 성적서 업체별 일괄 이메일 발송 기능
시험장비 및 자원관리	<ul style="list-style-type: none"> • 연구원의 시험장비 관리 기능 • 등록 장비에 대한 부서별, 품목별, 가격별, 기간별 조회 및 엑셀출력 기능 • 관리 대상의 지정양식 출력 기능 • 필요시 시약관리기능 구현 및 지정양식의 엑셀 출력 기능
LIMS 일반	<ul style="list-style-type: none"> • 실험실정보관리시스템 일반기능, 화면별/사용자별 권한관리 기능 • 실험실정보관리시스템 사용 조직의 부서 등의 관리 기능 • 실험실정보관리시스템에서 사용할 코드성 데이터 관리 기능
시험검사	<ul style="list-style-type: none"> • 업체 관리 기능, 검사관리 기능 • 시험(검사)결과 입력 및 첨부파일(i.e.)제한용량 : 50MB) 업로드 기능 • 시험(검사)결과 통합 조회 기능 구현

LIaaS는 멀티테넌시를 제공하고 관리하기 위하여 LIaaS 관리자 포털을 제공한다. 관리자 포털은 서비스 사용자를 관리할 수 있으며, 사용자별 테넌트를 관리할 수 있다. 사용자별 테넌트가 1개인 1:1 서비스 모델 제공이 가능하며, 사용자별 테넌트가 2개 이상인 1:N 서비스 모델도 제공이 가능하다.



(그림 3) 클라우드 샵 관리자 - 사용자/테넌트

4. 결론

본 논문에서는 클라우드 기반의 SaaS 환경에서 실험실정보관리시스템(LIMS)을 제공하기 위하여 사용자 DB 공유 구조를 활용한 클라우드 샵을 통한 서비스 제공의 관점에서 연구하였다. 향후 연구로는 실험실에서 이루어지는 검사, 분석, 시험 업무에 대한 유사한 데이터를 저장, 가공, 검색 그리고 분석하기 위하여 빅데이터 플랫폼 기술을 활용하여 클라우드

환경에서 빅데이터 기술 기반의 실험실정보관리 시스템을 설계하고 구현할 것이다.

ACKNOWLEDGMENT

본 연구는 중소벤처기업부와 한국산업기술진흥원의 “지역기업 개방형혁신 바우처(R&D, P0010684)”사업의 지원을 받아 수행된 연구결과임.

This research was financially supported by the Ministry of Small and Medium-sized Enterprises(SMEs) and Startups(MSS), Korea, under the “Regional Enterprise Open-Innovative Voucher Program(R&D, P0010684)” supervised by the Korea Institute for Advancement of Technology(KIAT).

참고문헌

- [1] 열린기술, LIMS/LAS개요, <http://www.yullin.com/Lims>
- [2] 약업닷컴, LIMS(실험실정보관리시스템) 시장 3년뒤 큰 폭 확대-프로스트앤설리반 “클라우드 기반 솔루션이 새로운 활력”, <http://www.yakup.com/news/index.html?nid=185665>, 2015년 5월
- [3] Coherent Marker and from Overblog, “Laboratory Information Management Systems(LIMS) Market Driving Factors, Industry Analysis, Investment Feasibility and Trends”, <http://coherent4484.over-blog.com/2019/02/laboratory-information-management-systems-lims-market-driving-factors-industry-analysis-investment-feasibility-and-trends.html>, February 2019
- [4] 중소기업 기술로드맵 2018-2020, 중소벤처기업부
- [5] 김형환 외 12, SaaS 기술 개발 동향, 전자통신동향분석 제24권, 제4호, 2009년 8월
- [6] 이지현 외 10, SaaS 플랫폼 기술 및 개발 동향, 전자통신동향분석 제26권, 제5호, 2011년 10월
- [7] 한국정보통신기술협회, ‘개방형 플랫폼서비스 - 제3부 : 멀티테넌트 실행 환경 구조’, TTA.KO-10.0696, 2013년 12월

이어핀 삽입 자동화 시스템을 위한 템플릿 매칭 기반 홀 판별 방법

백중환*, 이재열*, 정명수*, 장민우*, 신동호*, 서갑호*, 홍성호*

*한국로봇융합연구원 HRI연구센터

hong6286@kiro.re.kr

Hole Identification Method Based on Template Matching for Ear Pins Insertion Automation System

Jonghwan Baek*, Jaeyoul Lee*, Myungsoo Jung*, Minwoo Jang, Dongho Shin
Kapho Seo*, Sungho Hong

*KOREA INSTITUTE OF ROBOTICS & TECHNOLOGY CONVERGENCE
Dept. Human-Robot Interaction Research Center

요 약

장신구 산업은 인건비의 비중이 높고 노동자의 역량에 따라 제품의 제작 작업 시간 및 품질의 편차가 심하다. 이에 산업계의 수요에 맞추어 실리콘 금형 표면 지름 0.75mm 홀에 이어핀을 삽입하는 공정을 자동화하기 위하여 삽입 자동화 시스템이 개발되고 있다. 본 논문에서는 이어핀 삽입 자동화 시스템에서 적용할 수 있는 템플릿 매칭 방법과 관심 영역 레이블링을 통한 홀 판별 방법을 제안한다. 제안한 방법의 안정성을 확보하기 위하여 실험을 통해 최적의 매칭 방법과 이진화 기법을 적용하였으며 이어핀 홀의 좌표를 확보하여 X-Y 정밀 이송 시스템에 적용할 수 있다.

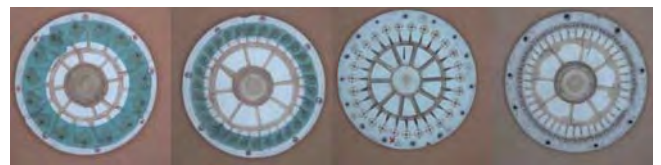
1. 서론

장신구 산업의 공정은 대부분이 수작업으로 이루어지는 노동집약적 산업으로 제조원가 중 인건비의 비중이 가장 높으며 노동자의 역량에 따라 작업 시간 및 품질의 편차가 심하다. 이에 산업계는 고객 수요에 맞추어 공정 자동화 시스템을 통해 편차가 심하지 않은 안정된 품질의 제품을 소비자에게 제공하려 하고 있다. 그러나 소비자 수요에 맞추어 빠르게 변화하는 특성상 장신구들을 주조하는 실리콘 금형상의 이어핀 삽입 위치가 다르게 나타날 수 있다.

이러한 문제점을 해결하기 위하여 본 논문에서는 정밀제어 이어핀 삽입 자동화 시스템에 적용할 수 있는 비전 기반의 이어핀 삽입 좌표 추출 방법을 제안하고, 사용할 수 있는 다른 방법과의 비교를 통한 정밀도 측정 결과를 나타내었다. 제안하는 비전 기반의 삽입 좌표 추출 방법은 템플릿 매칭-ROI 영역 레이블링을 통하여 정확도를 높였다. 제안하는 비전 기반 삽입 좌표 추출 방법을 통한 X, Y축 정밀 이송 시스템을 사용한다면 원가절감 및 품질 안정성, 생산성 향상 등을 확보할 수 있을 것이다.

2. 이어핀 삽입 자동화 시스템

기존 이어핀 삽입 작업은 주조 공정을 위해 실리콘 금형 표면 구멍에 작업자가 직접 지름 0.75mm의 핀을 삽입하는 과정으로 진행된다. 즉, 첫째로 인간의 눈으로 보고, 둘째로 삽입 위치를 인식한 후, 셋째로 손을 움직여 삽입 위치에 삽입하는 과정으로 작업을 세분할 수 있다. 본 연구에서 사용한 이어핀 자동화 시스템은 이러한 인간의 작업 방식과 유사한 작업 방식을 갖는다.



(그림 1) 다양한 모습의 실리콘 금형들

첫째로 산업용 카메라로 그림 1과 같은 다양한 금형을 보고, 둘째로 비전 시스템으로 금형의 이어핀 삽입 좌표 데이터를 추출한다. 셋째로, 추출한 데이터를 통해 자동 작업지시가 가능한 세 가지의 작업이 가능하다. 그림 2는 본 연구에서 사용한 자동화

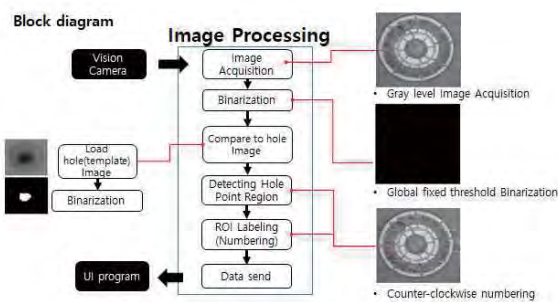
시스템을 나타낸다.



(그림 2) 이어핀 삽입 자동화 시스템

3. 이어핀 삽입 좌표 데이터 추출

3. 1. 흐름도



(그림 3) 이어핀 삽입 자동화 시스템

삽입 좌표 인식을 위한 비전 시스템의 흐름도는 그림 3과 같다. 산업용 카메라는 실리콘 금형을 촬영하여 RGB 색상 모델로 영상을 얻어오며, 영상처리 후 획득한 좌표 데이터 및 결과 이미지는 자동작업지시 공정을 위해 사용자 인터페이스 프로그램 단으로 송신된다.

3. 2. 이진화

이진화(Binarization)는 특정 경계값을 두고 두 개의 클래스 분류 문제로 0 아니면 1, 흑 아니면 백으로 분류하여 관심 객체를 분류하는 작업을 의미한다.

$$dst(x,y) = \begin{cases} 255 & src(x,y) > T \\ 0 & otherwise \end{cases} \quad (1)$$

영상에서의 이진화는 식 (1)과 같이 특정 경계값 T 를 기준으로 픽셀값을 255나 0으로 분류한다. 이진화는 입력 영상의 환경, 특히 조명의 영향을 다소 받게 되어 대비가 낮고 잡음이 심하며 객체의 패턴이 복잡한 입력 영상에서는 이진화 결과가 원하는 성능이 나오지 않아 객체 분리가 어려운 모습을 보

인다. 이에 더 나은 성능을 위하여 많은 논문이 발표된 바 있다.[1][2][3] 그러나 논문들에서 사용한 적응형 이진화 방법을 사용할 경우, 금형 표면에 여러 무늬가 있는 실리콘 금형의 특성상 잡음까지 인식해 버리는 문제가 있다. 본 논문의 이어핀 삽입 자동화 시스템은 덮개로 인하여 금형 표면에 균일한 조명을 비출 수 있으며, 그로 인해 표면의 홀이 음각으로 뚜렷하게 드러나기 때문에 전역 고정 경계값 이진화를 사용하는 편이 유리하다.

3. 3. 템플릿 매칭을 통한 관심 영역 획득

템플릿 매칭은 입력 영상에서 템플릿 이미지와 일치하는 이미지의 작은 부분을 찾기 위한 이미지 처리 기술이다. 템플릿 매칭은 찾으려는 객체의 이동 문제에 강인한 편이지만 회전 및 크기가 조절된 물체의 매칭은 어려운 편이다. 입력 영상의 이진화와 마찬가지로 이어핀 삽입 자동화 시스템은 카메라 높이가 고정되어 있으며 균일한 조명을 비추기 때문에 홀 영역을 찾는 작업에 템플릿 매칭 방법을 사용한 것이 적합하다. 실리콘 금형 표면의 홀 영역을 찾기 위하여 아래 그림 4와 같은 템플릿을 입력시키고 이진화하여 탐색하고 일치되는 영역을 관심 영역 (Region of Interest, ROI)으로 지정한다.



(그림 4) 템플릿 및 이진화 템플릿

이진화 템플릿 영상은 그 자체가 슬라이딩 윈도우가 되어 이진화 입력 영상 왼쪽 위에서 오른쪽 아래까지 탐색을 시도하며 매칭 방법에 따라 매칭을 시도한다. 입력 영상과 템플릿 영상 간의 비교 계산 방법에 따라 매칭 결과는 조금씩 달라진다.[4]

$$R(x,y) = \sum (T(x',y') - I(x+x',y+y'))^2 \quad (2)$$

$$R(x,y) = \sum (T(x',y') \times I(x+x',y+y')) \quad (3)$$

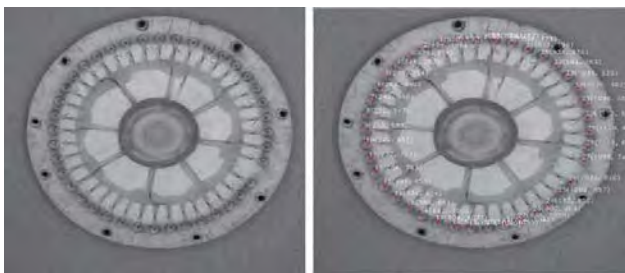
$$R(x,y) = \sum (T'(x',y') \times (I'(x+x',y+y'))) \quad (4)$$

매칭 방법은 제곱차 매칭, 상관관계 매칭, 상관계수 매칭이 있는데 각각의 수식은 식 (2), (3), (4)와 같다. I 는 탐색영역의 영상이며, T 는 템플릿, R 은 결과행렬이다. 제곱차 매칭은 일치할수록 값이 높게

나오고, 상관관계와 상관계수 매칭은 일치할수록 값이 낮게 나온다. 상관계수 매칭 방법은 일반적으로 제곱차 매칭보다 시간이 더 걸리지만 더 정확한 결과를 보인다.

3. 4. ROI 영역 레이블링을 통한 좌표 검출

레이블링은 관심 객체에 꼬리표(label)를 붙이는 작업을 의미한다. 템플릿 매칭을 통해서 홀의 대략적인 영역을 획득 할 수 있으나 홀의 정확한 좌표 획득을 위한 방법이 필요하다. 이진화된 영상의 분석에 있어서 레이블링 기법은 요소들에 대한 연결성을 제공하고 각각의 픽셀을 하나의 관심 객체로 묶는 기법이다. 일반적으로 레이블링 알고리즘은 두 번의 탐색을 통하여 재귀적으로 입력 영상 이미지에 레이블을 붙이는 작업을 하거나 비재귀적으로 한 번의 탐색을 통해 레이블링하는 기법을 사용한다.[5] 그러나 제안하는 방법에서는 템플릿 매칭을 통하여 관심 영역을 획득하고 그 영역 내에서만 레이블링 작업을 수행하기 때문에 복잡한 레이블링 알고리즘을 사용하지 않고 관심 영역 내에서 흰색 화소만을 찾는 간단한 알고리즘을 사용하였다. 이후, 관심 영역에서 레이블링된 객체의 중간 화소와 관심 영역의 위치를 합하면 홀의 좌표가 검출된다. 검출된 관심 영역 및 좌표들은 반시계 방향 순서로 번호가 매겨진다. 이후 영상의 픽셀 좌표계를 실 좌표계로 변환하고 그림 5와 같은 결과 영상과 좌표를 사용자 프로그램에 송신한다.

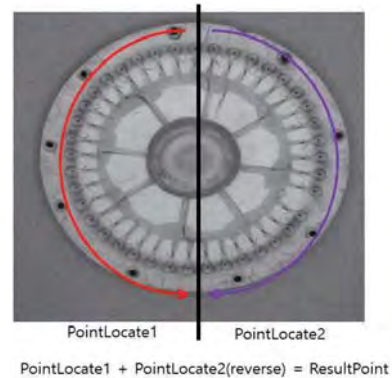


(그림 5) 홀 좌표 검출

3. 5. 템플릿 매칭에 의한 중복 검출 문제

템플릿 매칭은 슬라이딩 윈도우 기반이기 때문에 윈도우의 픽셀 이동 간격이 너무 미소하면 하나의 홀이 중복 검출되는 문제가 있다. 이를 해결하기 위한 방법으로 검출된 좌표의 y 좌표를 오름차순으로 정렬하고 y 좌표끼리 비교하여 5픽셀 이내라고 판단이 되면 좌표를 삭제하는 기법을 사용하였으며 같은 y좌표 내의 두 개의 홀이 삭제되는 것을 방지하기

위하여 그림 6과 같이 입력 영상의 절반씩 탐색하여 두 그룹을 합쳐 레이블하는 기법을 사용하였다.

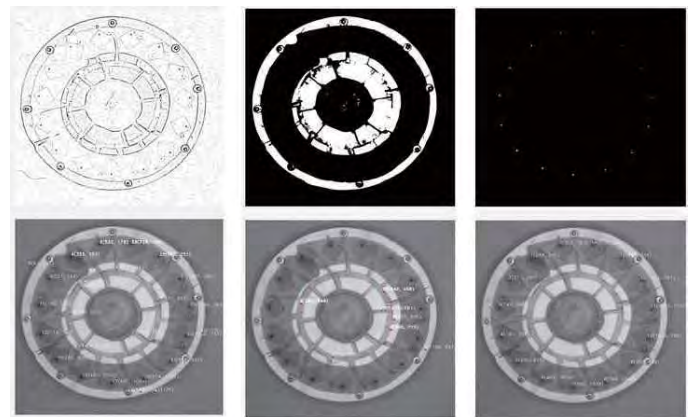


(그림 6) 레이블링 순서

4. 실험

제안한 비전 기반 삼입 좌표 추출 시스템에 사용한 방법들을 검증하기 위해 입력 영상에 각 방법을 적용하였을 때 결과 영상들을 나타내었다. 실험 환경은 산업용 머신 비전 카메라를 실리콘 금형 표면을 촬영하는 방향으로 30cm 떨어져서 촬영하였으며 덮개를 이용하여 암실을 만들고 외경 48cm, 내경 36cm의 링 형태의 조명을 사용하여 균일한 조명 환경을 만들었다. 입력 영상은 1280px×1280px이며 잡음의 영향이 없도록 무늬가 없는 바닥을 사용하였다. 사용한 전역 이진화 경계값은 50으로 고정하였으며 템플릿 매칭 유사도는 0.5로 고정된 후 실험하였다.

4. 1. 이진화 방법에 따른 매칭 결과



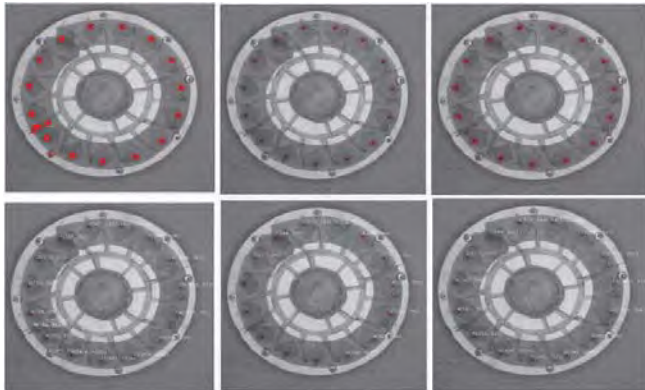
(a) 적응형 이진화 (b) Otsu 이진화 (c) 전역 이진화

(그림 7) 이진화 방법에 따른 결과

그림 7은 이진화 방법에 따른 결과를 나타내었다. 템플릿 매칭 방법은 상관계수 매칭 방법을 각각 사

용하였다. 그림 7의 a에서 적응형 이진화 방법을 사용하였을 때, 홀 검출은 비교적 잘 되었으나 잡음을 이어핀 홀로 인식하는 모습을 보인다. 그림 7의 b에서 Otsu 이진화 방법을 사용하였을 때 홀을 이진화하지 못하여 검출을 못하는 모습을 보인다. 그림 7의 c에서는 홀을 100% 검출하였으며 좌표 출력이 되는 모습을 보인다.

4. 2. 템플릿 매칭 방법에 따른 매칭 결과



(a) 제곱차 매칭 (b) 상관관계 매칭 (c) 상관계수 매칭

(그림 8) 템플릿 매칭 방법에 따른 결과

그림 8은 템플릿 매칭 방법에 따른 결과를 나타낸다. 이진화 방법은 전역 경계값 이진화를 모두 수행하였다. 그림 8의 a에서 제곱차 매칭 방법은 홀 검출 영역을 잘 잡아내었으나 잡음 역시 홀 검출 영역으로 판단하는 모습을 보인다. 그림 8의 b에서 상관관계 매칭에서는 홀 영역의 4분의 1을 잃는 모습을 보인다. 그림 8의 c에서 상관계수 매칭에서는 홀 영역 탐색을 완료한 모습을 보인다.

5. 결론

급변하는 현대 사회에서 자동화되지 않은 노동집약적 산업 분야들은 품질 안정성 및 작업 시간의 효율성을 위하여 자동화 시스템을 요구하고 있다. 본 논문에서는 주얼리 산업의 이어핀 삽입 홀 검출 자동화 시스템에 적용할 수 있는 산업용 카메라 기반의 템플릿 매칭 및 ROI 레이블링을 이용한 검출 알고리즘을 제안하였다. 실험 결과로서 최적의 검출 알고리즘을 찾아내어 적용하였으며 본 방법을 통해 비전 기반 이어핀 삽입 자동화 시스템에서 원가 절감 및 작업 시간 절감의 효과를 누릴 수 있을 것이다.

참고문헌

- [1] Sauvola, Jaakko, and Matti Pietikäinen. "Adaptive document image binarization." *Pattern recognition* 33.2 (2000): 225-236.
- [2] Liu, Ying, and Sargur N. Srihari. "Document image binarization based on texture features." *IEEE Transactions on Pattern Analysis and Machine Intelligence* 19.5 (1997): 540-544.
- [3] Pak, Myeongsuk, Jaehan Park, and Sanghoon Kim. "The Implementation of Defect Detector Using Efficient Thresholding Method." *Computer Science and its Applications*. Springer, Berlin, Heidelberg, (2015): 1085-1091.
- [4] Brunelli, Roberto. "Template matching techniques in computer vision: theory and practice." John Wiley & Sons, (2009): 43-71.
- [5] 김도현, 강동구, and 차의영. "화상 및 음성처리: 비재귀 Flood-Fill 알고리즘을 이용한 적응적 이미지 Labeling 알고리즘." *정보처리학회논문지 B* 9.3 (2002): 337-342.

코로나 바이러스 확진자 데이터 기반 시뮬레이션 모델 학습 방법 제안

장미*, 이복주**, 강봉구***, 서경민****

*한국기술교육대학교 에너지신소재응용화학공학부 **한국기술교육대학교 컴퓨터공학부

한국생산기술연구원 *한국기술교육대학교 융합학과

dntdmami@koreatech.ac.kr, bokju618@koreatech.ac.kr, bgkang@kitech.re.kr, kmseo@koreatech.ac.kr

Suggestion of Corona Virus Infection Data-based Simulation Model Update Method

Mi Jang*, Bok-Ju Lee**, Bong-Gu Kang***, Kyung-Min Seo****

*School of Energy Materials and Chemical Engineering, Korea University of Technology and Education

**School of Computer Science and Engineering, Korea University of Technology and Education

*** Korea Institute of Industrial Technology

****Dept. of Future Technology, Korea University of Technology and Education

요 약

코로나감염-19, 사스, 메르스 등 바이러스성 질병이 전세계적으로 확산되어 많은 인구가 감염되어 왔다. 바이러스성 질병의 확산 예측 및 종결을 위해 실제 감염자 데이터를 기반으로 한 시뮬레이션 연구는 반드시 필요하다. 본 연구는 지역 내 클러스터 감염 시뮬레이션을 위한 바이러스 감염 모델을 제안한다. 제안하는 모델은 여러 개의 셀로 구성되어 있으며, 각 셀은 군집을 표현하고 있다. 본 논문에서 제안한 모델은 실제 데이터를 기반으로 하여 정확도가 높으며, 이를 바탕으로 향후 지역의 특성을 반영한 전파 시뮬레이션 혹은 지역 간의 전파를 예상하는 시뮬레이션의 기초로 사용될 수 있다.

1. 서론

전세계적으로 코로나감염-19의 유행이 지속적으로 확산되고 있다. 중국 이외의 지역에서는 코로나감염-19로 인한 사망률이 낮아 국민 건강에 미치는 영향이 크지 않을 것이라고 판단했으나, 대구·경북 지역에서 31번째 확진자 발생 이후 예상하지 못한 클러스터 감염이 발생하면서 상황이 급변하였다. 그 결과 코로나감염-19 유행의 종결 시점을 정확하게 예측하기 어려워졌으며, 특정 집단에서 감염자 수가 폭등하는 현재와 같은 상황에서는 추이를 예측하는 것이 불가능하다[1].

코로나감염-19 발생 이전에도 사스, 메르스 등과 같은 바이러스성 질환의 전파에 대해 많은 데이터 기반의 분석이 이루어졌다. 데이터 기반의 모델의 경우 실제로 제공된 데이터가 바탕이 되므로 정확한 분석이 가능하다는 장점이 있다. 본 연구는 시뮬레이션 모델을 구성을 위한 이전 과정으로서 실제 발생한 일별 감염자 수 데이터를 바탕으로 바이러스 전파 모델을 설계하였다. 뿐만 아니라 클러스터 감염에 대한

표현이 가능하도록 각 행정구역을 셀로 나타내고, 각 셀의 내부에 군집 표현하였다.

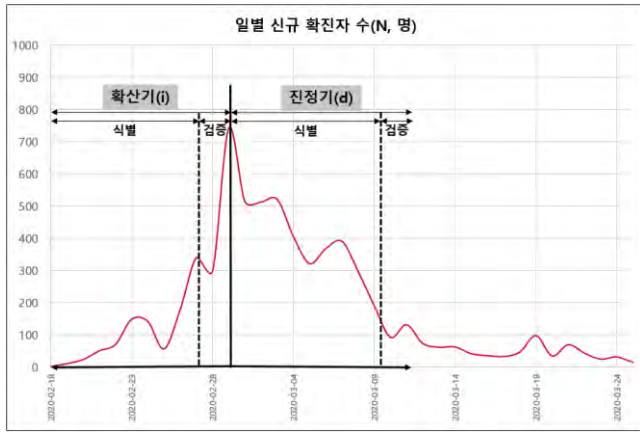
본 연구에서 제시한 모델을 통해 지역 내 클러스터 감염의 추이를 예측할 수 있게 된다. 현재 모델에서는 각 셀을 일반화하여 표현하였으나, 추후 진행될 연구에서는 각 셀에 인구 밀도, 단체 시설의 개수와 같은 지역적 특성을 반영하여 더 현실적인 전파 모델의 구현이 가능해질 것이다. 또는 지역 간의 연결을 통해 넓은 범위에 대한 분석이 가능할 것으로 보인다.

2. 모델 설계

2.1 시나리오 분석

모델 설계에 앞서 바이러스 전파 시나리오 분석을 위해 선정한 지역은 가장 많은 감염자가 발생한 대구광역시이다. 그림 1은 실제 대구에서 발생한 일별 신규 확진자의 수를 나타낸 표이다. 질병관리본부에서 발표한 바에 따르면 대구광역시에서 2월 18일 처음 1명의 확진자가 발생하였다. 확진자 발생 첫날부터 40일이 지난 3월 28일까지의 일별 신규 확진자 추이를 살펴보면 12일째에 확진 판정을 받은 사람이 741

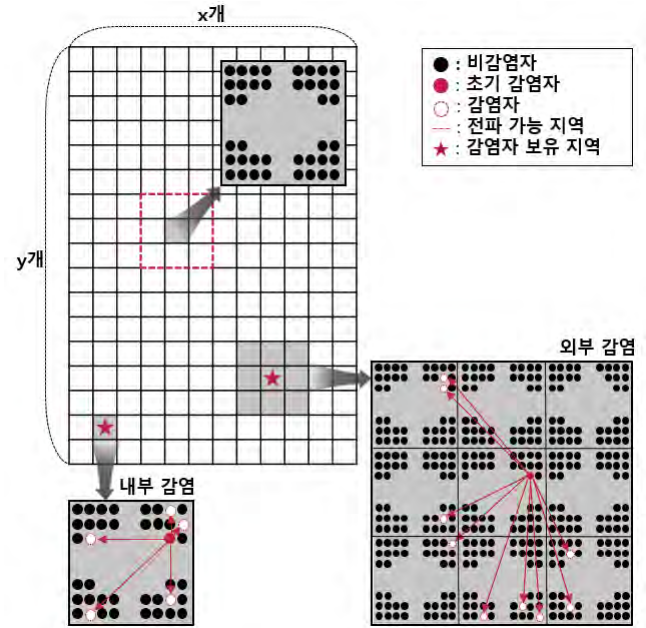
명으로 가장 높았다. 12 일째를 기준으로 이전에는 신규 확진자의 수가 점점 증가하여 바이러스가 감염이 확산되는 추세였으며, 그 이후에는 점차 확진자의 수가 줄어들어 바이러스 감염이 진정되는 경향을 확인할 수 있다. 본 논문에서는 상반되는 경향을 보이는 두 시기를 각각 확산기와 진정기로 구분하였다.



(그림 1) 대구 광역시 일별 확진자 수 현황

2020년 2월 행정안전부에서 발표한 KOSIS에 따르면 대구광역시에는 총 204개의 행정구역(읍, 면, 동)으로 이루어져 있으며, 약 243만 2천명이 거주 중이다. 모든 구성원을 하나의 모델로 간주할 경우, 모델의 개수가 굉장히 많아지므로 구현하는데 한계가 있다. 이러한 점을 반영하여 모든 구성원을 각각 모델로 나타내는 대신 행정구역을 모델 단위로 설정하였다. 연구 대상을 셀 단위로 분할하여 분석하는 방법을 셀룰러 오토마타(이하 CA)라고 한다. 모든 셀의 상태를 각각 설정할 수 있으며, 각 셀들의 관계를 나타내는 규칙에 의해 동작이 이루어지는 동적 계산 시스템이다. CA를 사용할 경우 수치적으로 분석하기 어려운 대상을 단순화하여 직관적으로 계산할 수 있다 [2].

대구 지역을 CA로 표현하기 위해 1개의 행정구역을 1개의 셀로 설정하였으며 각 셀에는 동일한 인구가 거주 중이라고 가정하였다. 즉, 지역 내 전체 인구의 수가 M 이고, 행정구역의 수가 D 일 때, 각 셀에 표현되는 인구의 수는 D/M 이다. 초기 단계에서 전체 셀 중에 임의의 하나의 셀에 한 명의 감염자를 발생시킨다. 그리고 그 감염자는 감염자가 위치한 셀 내부와 그 셀을 중심으로 인접한 8개의 셀에 거주 중인 구성원을 확률적으로 감염시킬 수 있다. 그림 2과 같이 감염자와 같은 셀 안에 포함된 인구를 감염시키는 경우를 내부 감염, 인접 셀에 포함된 인구를 감염시키는 경우를 외부 감염이라고 지칭하였다.



(그림 2) 셀룰러 오토마타를 이용한 각 행정구역 별 거주 인구 및 감염 모사

2.2 실 데이터 기반 모델 설계

2.2.1 확산기

확산기의 감염자는 내부 감염과 외부 감염이 가능하고 각각의 전파율은 α , β 이다. 그리고 확산기의 내부 감염을 나타내는 방정식을 $f_{i,in}$ 로, 외부 감염을 나타내는 방정식은 $f_{i,out}$ 으로 표기한다. 또한 $f_{i,in}$ 과 $f_{i,out}$ 을 통해 도출한 p 번째 날 각 셀의 신규 감염자 수를 $N_{p,x,y}$, p 번째 날의 전체 신규 감염자 수를 $N_{p,tot}$ 라고 표기한다. p 번째 날 (x,y) 셀의 신규 감염자 수는 (x,y) 셀 내부의 $(p-1)$ 번째 날까지의 누적 감염자로 인한 내부 감염자 수와 (x,y) 셀의 인근의 셀에 존재하는 감염자로 인한 외부 감염자 수의 합이다. 그리고 p 번째 날 신규 감염자 수의 합은 모든 셀에서 발생한 신규 감염자 수를 합한 값이다. 식으로 나타내면 다음과 같다.

$$\begin{aligned} \Delta N_{p,x,y} = & f_{i,in} \left(\sum N_{p-1,x,y}, \alpha \right) \\ & + f_{i,out} \left(\sum N_{p-1,(x-1),(y-1)}, \beta \right) \\ & + f_{i,out} \left(\sum N_{p-1,(x-1),y}, \beta \right) \\ & + f_{i,out} \left(\sum N_{p-1,(x-1),(y+1)}, \beta \right) \\ & + f_{i,out} \left(\sum N_{p-1,x,(y-1)}, \beta \right) \\ & + f_{i,out} \left(\sum N_{p-1,x,(y+1)}, \beta \right) \\ & + f_{i,out} \left(\sum N_{p-1,(x+1),(y-1)}, \beta \right) \\ & + f_{i,out} \left(\sum N_{p-1,(x+1),y}, \beta \right) \\ & + f_{i,out} \left(\sum N_{p-1,(x+1),(y+1)}, \beta \right) \end{aligned} \quad \text{식(1)}$$

$$N_{p,tot} = \sum_{x=1} \sum_{y=1} (\Delta N_{p,x,y}) \quad \text{식(2)}$$

그리고 각 셀의 신규 감염자 수는 각 셀의 인구 수를 넘을 수 없으며, p 번째 날 전체 신규 감염자 수는 지역의 총 인구 수를 넘을 수 없으므로 다음과 같은 조건을 따르게 된다.

$$0 < \alpha, \beta \leq 1 \quad \text{식(3)}$$

$$\Delta N_{p,i,j} \leq \frac{M}{D} \quad \text{식(4)}$$

$$N_{p,tot} \leq M \quad \text{식(5)}$$

2.2.2 진정기

진정기에도 확산기와 동일한 메커니즘으로 바이러스가 전파가 된다. 확산기의 전파 확률에 계수 k 와 t 를 각각 곱하여 진정기의 전파 확률을 나타낸다. 내부 감염과 외부 감염의 확률을 각각 $k \cdot \alpha$ 와 $t \cdot \beta$ 로 표기하고, 감염자를 구하는 방정식은 $f_{d,in}$ 과 $f_{d,out}$ 로 표현한다.

$$\begin{aligned} \Delta N_{q,x,y} = & f_{d,in} \left(\sum N_{q-1,x,y}, k \cdot \alpha \right) \\ & + f_{d,out} \left(\sum N_{q-1,(x-1),(y-1)}, t \cdot \beta \right) \\ & + f_{d,out} \left(\sum N_{q-1,(x-1),y}, t \cdot \beta \right) \\ & + f_{d,out} \left(\sum N_{q-1,(x-1),(y+1)}, t \cdot \beta \right) \\ & + f_{d,out} \left(\sum N_{q-1,x,(y-1)}, t \cdot \beta \right) \\ & + f_{d,out} \left(\sum N_{q-1,x,(y+1)}, t \cdot \beta \right) \\ & + f_{d,out} \left(\sum N_{q-1,(x+1),(y-1)}, t \cdot \beta \right) \\ & + f_{d,out} \left(\sum N_{q-1,(x+1),y}, t \cdot \beta \right) \\ & + f_{d,out} \left(\sum N_{q-1,(x+1),(y+1)}, t \cdot \beta \right) \end{aligned} \quad \text{식(6)}$$

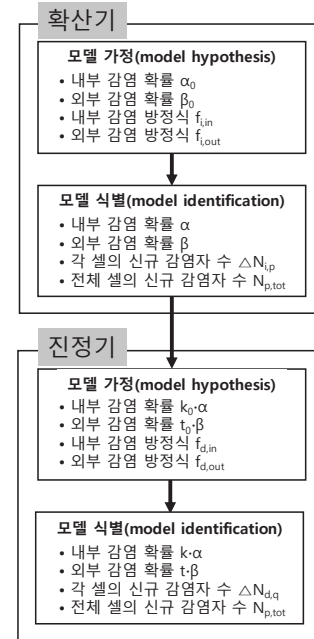
$$N_{q,tot} = \sum_x \sum_y (\Delta N_{q,x,y}) \quad \text{식(7)}$$

마찬가지로 감염 확률과 감염자 수는 다음과 같은 조건을 가지게 된다.

$$0 < k \cdot \alpha, t \cdot \beta \leq 1 \quad \text{식(8)}$$

$$\Delta N_{p,i,j} \leq \frac{M}{D} \quad \text{식(9)}$$

$$N_{p,tot} \leq M \quad \text{식(10)}$$



(그림 3) 바이러스 전파 시뮬레이션 식별 과정

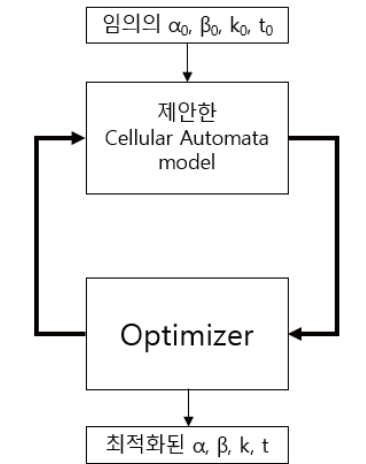
3. 모델 학습 프로세스

3.1 확산기 갱신 및 검증

그림 1의 확산기 중 모델을 학습하여 최적의 α 와 β 를 구하기 위한 구간을 식별, α 와 β 의 타당성을 판단하기 위한 구간을 검증이라고 구분하였다. 2.2에서 제시한 식(1)에 임의의 감염 확률 α_0, β_0 를 대입하여 그림 1의 확산기 중 식별 구간과 유사한 결과를 내는 찾는다. 앞서 구한 α 와 β 가 타당한지 판단하기 위해 식(1)과 α, β 를 사용해 구한 일별 감염자 수와 그림 1의 검증 구간의 감염자 수가 유사한지 비교한다. 그림 4는 임의의 감염 확률을 적용하여 최적화된 감염 확률을 찾기위해 반복되는 과정을 도식화한 모습이다.

3.2 진정기 갱신 및 검증

3.1에서 확산기의 최적화된 감염 확률을 구하는 방법과 동일하게 한 방법으로 진정기의 감염 확률을 도출한다. 진정기의 식별 구간을 통하여 $k \cdot \alpha$ 와 $t \cdot \beta$ 를 찾는다. 찾은 $k \cdot \alpha$ 와 $t \cdot \beta$ 가 최적의 전파 확률인지 진정기 검증 구간의 실제 감염자 수와 비교하여 판단한다.



(그림 4) 감염 확률 최적화 과정

4. 결론

실 데이터를 기반으로 한 시뮬레이션 모델이므로 정확도가 높다는 장점을 가진다. CA 를 사용하여 각 각의 셀에 고유한 특성을 입력할 수 있다는 특징을 바탕으로 각 셀에 지역적 특성을 반영하여 좀 더 해상도가 높은 시뮬레이션 구현이 가능하다. 특히 인구 밀도, 구성원들의 행정 구역 간의 이동, 단체 시설 등 클러스터 감염의 확률을 높이는 특성들을 도입할 경우, 폭발적이고 돌발적인 클러스터 감염에 대한 영향력을 미리 예측하고 대비할 수 있다. 더 나아가 현재는 하나의 지역을 분석 대상으로 설정하였으나, 여러 개의 지역을 결합한 모델을 구현하여 더 현실적인 감염 경로 및 감염자 수를 예측할 수 있다.

참고문헌

- [1] 김남순, 코로나바이러스감염증-19 현황과 과제, 보건·복지 Issue & Focus, 373 호, 1-13, 2020
- [2] Mohammad R. G., Kinetic of Hepatitis B Virus Infection : A Cellular Automaton Model Study, Journal of Paramedical Sciences, Vol.3, No.3, 1-8, 2012

GPS-Spoofing을 이용한 Anti-Drone

권준우, 오형석, 서승현
한양대학교 에리카 전자공학부

kjw9628@hanyang.ac.kr, tjrguddh@hanyang.ac.kr, seosh77@hanyang.ac.kr

Anti-Drone System using GPS-Spoofing

Jun-Woo Kwon, Hyeong-Seok Oh, Seung-Hyun Seo
Division of Electrical Engineering, Hanyang University ERICA Campus

요 약

최근 무인이동체 기술과 IoT(사물인터넷)의 발전에 따라 드론에 대한 관심과 사용이 꾸준히 증가하고 있다. 드론은 취미용으로 사람들에게 재미를 주는 것에서 나아가 긴급서비스, 조기경보, 모니터링 등 이용되는 분야가 다양하고 사람들의 편의에 맞게 분야와 활용목적이 점점 늘어나고 있는 추세이다. 하지만 이에 따라 불법물카나 드론을 사용한 테러 등 악의적으로 드론을 악용하는 사례 역시 빈번하게 발생하고 있다. 이를 예방하고 사전에 차단하기 위하여 본 논문에서는 주파수 송수신기인 Hack-RF One과 라즈베리파이, 안테나를 활용하여 Anti-Drone 시스템 프로토타입을 구현하였다.

1. 서론

드론은 생활속에서 많은 편의와 서비스를 제공하고 있다. 무인이동체 관련 기술과 IoT(사물인터넷)의 발전에 따라 실종자 수색, 고층빌딩 모니터링, 택배서비스, 재난 모니터링 등 드론을 이용한 서비스 역시 많이 증가하고 있다. 정부 역시 드론 산업 육성에 속도를 내면서 공공정책 분야에 드론의 활용도를 높이고 있다. 드론 산업은 항공, 정보통신기술(ICT), 소프트웨어 등 파생되는 관련 산업이 다양해 성장 잠재력이 크며, 드론 관련기술들이 발달함에 따라 2016년 700억원 규모에서 2019년 3천500억원의 시장규모가 형성된 상태이다.

그러나 사생활침해 문제(몰카)와 드론테러 등 드론을 불법적인 목적으로 사용하는 문제가 대두되고 있다. 예를 들면, 실제로 우리나라에서도 드론에 카메라를 장착하여 타인의 건물 내부 주거환경을 몰래 관찰하거나 공용 샤워장을 촬영하는 등 그 악용사례가 빈번하게 적발되고 있다. 뿐만 아니라, 해외에서는 드론을 이용하여 교도소 내부로 마약이나 휴대전화를 전달하거나 테러용으로 드론을 이용하는 등 각종 범죄에 드론이 악용되고 있다. 따라서 승인받지 않은 드론이 특정지역에 들어올 수 없게 하기 위해

서 Anti-Drone 기술이 필요하다.

본 논문에서는 허가되지 않은 지역에 드론을 이용한 악의적이고 불법적인 행위나 드론테러 등의 공격에 대응하고자 한다. Raspberry Pi 3B+와 주파수 송수신기인 Hack-RF One, 안테나를 사용하여 불법 침입 드론의 GPS좌표를 교란시키는 기술인 GPS-Spoofing 기술을 구현하고 GPS-Spoofing 기술을 Anti-Drone에 접목시켜 Anti-Drone 시스템의 프로토타입을 구현하고자 하였다.

2. GPS-Spoofing 관련연구

본 논문의 Anti-Drone 시스템은 GPS-Spoofing 기술을 기반으로 한다. Spoofing이란 승인을 받지 않은 사용자가 승인을 받은 사용자인 것처럼 위장하여 시스템에 접근하거나 네트워크상에서 허가된 주소로 가장하여 접근제어를 우회하는 공격행위이다.

GPS-Spoofing은 공격자가 공격대상의 GPS신호를 임의로 조작하여 원래 가고자 하는 목적지가 아닌, 공격자가 원하는 목적지로 가게 하는 것을 목표로 한다. 아직 GPS Spoofing에 대한 공격 가능성이 명확하지 않고, 경각심이 부족하기 때문에 대부분의 민간 시스템은 방어 메커니즘을 제대로 갖추고 있지 않다. 따라서 대부분의 민간 시스템이나 무인이동체

등은 GPS-Spoofing 공격에 노출되어 있다.

(그림 1)은 GPS-Spoofing의 진행 단계이다. 첫 번째 단계는 GPS-Spoofing을 하기 위한 장치인 GPS-Spoofers를 구성하는 것이다. 두 번째 단계는 구성된 GPS-Spoofers를 통하여 공격대상의 GPS신호보다 더 강한 신호를 발생시켜 공격대상의 GPS신호를 takeover 시키는 단계이다. 세 번째 단계는 takeover된 공격대상의 GPS의 좌표를 교란하는 단계이다.

takeover는 앞서 구성된 GPS-Spoofers를 통하여 상대방의 GPS 수신기를 원래의 신호에서 거짓신호인 Spoofing신호로 바꾸는 것으로 시작된다. takeover 단계는 빠르고 강압적인 방법과 천천하고 은밀한 방법으로 나뉜다. 전자의 경우 공격자는 단순히 강한 거짓 신호를 전송해 공격대상이 위성을 추적하지 못하게 하고, 공격대상의 GPS 신호를 더 강한 Spoofing신호에 고정 시킨다. 이와는 대조적으로, 후자의 경우 원초적 신호와 거짓된 신호를 함께 공격대상에 전송하고 그 후에 점차적으로 거짓신호의 세기를 높여 원래의 신호를 Spoofing신호로 천천히 이동 시킨다. 후자방식의 장점은 수신된 신호강도에 비정상적인 점프를 일으키지 않기 때문에 높은 은밀성을 가진다. 그러나 은밀한 takeover를 위해서는 공격대상의 위치에서 원래 신호와 실시간으로 추적하고 동기화하기 위한 전문 하드웨어가 필요하다. 두 번째 단계인 takeover는 한번 수행되고 나면 또 다시 수행해야 할 필요가 없고, 다음 단계에도 영향을 미치지 않는다.

본 시스템에서는 침입 드론을 이용한 공격이나 테러 등을 감안하여 빠르게 침입 드론을 내보내야 하므로 전자의 방법인 빠르고 강압적인 takeover 방식을 사용한다.



(그림 1) GPS-Spoofing 단계.

3. 제안하는 Anti-Drone 시스템

우리가 제안하는 Anti-Drone 시스템은 경찰드론과 GCS(Ground Control System)로 구성되어 있다. 경찰드론은 GPS-Spoofing 장치인 GPS-Spoofers를 직접 장착한 드론을 칭한다. 예를 들어, 허가받지 않은 드론이 특정지역을 침입할 경우 GCS는 침입한 드론의 현재 좌표데이터를 이용하여 침입한 드론을 어디로 내보낼 것인지에 대한 좌표를 계산한다. 계산된 좌표는 GPS-Spoofers에 등록되고 경찰드론이 출격하여 침입한 드론을 특정지역 밖으로 내보내게 된다. (그림 2)는 GCS와 경찰드론의 역할이다.



(그림 2) GCS와 경찰드론의 역할.

3-1. GPS-Spoofing 구성



(그림 3) GPS-Spoofing 구성.

우리는 주파수 송수신기인 Hack-RF One, Raspberry Pi 3B+, 안테나, 무선충전기를 이용하여 (그림3)의 GPS-Spoofing을 제작하였다. Raspberry Pi를 통하여 Hack-RF One을 제어함으로써 GPS 위치 정보를 입력할 수 있다.

3-2. GPS-Spoofing 지도를 통한 좌표 파악

우리는 GCS를 통한 Anti-Drone 시스템 컨트롤을 보다 쉽게 표현하기 위해 Java Eclipse와 Kakao API를 사용하여 GPS-Spoofing 지도를 구현하였다.

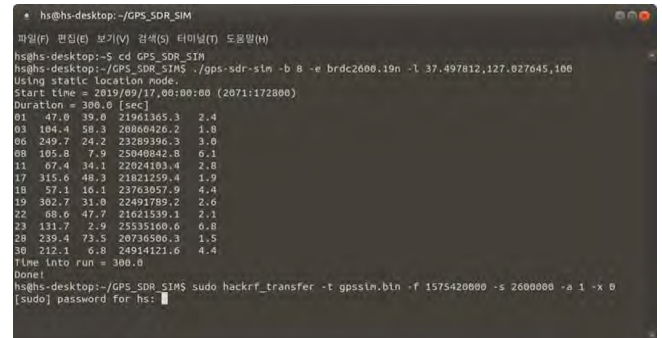
(그림4)의 파란색 사각형 부분은 본 시스템의 GCS가 관리하고 있는 영역이다. 만약 허가되지 않은 드론이 파란색 부분의 영역을 침입하게 되면 빨간색 마커로 침입 드론의 경로와 위도, 경도 좌표데이터가 표시된다. 표시된 위도, 경도 좌표데이터를 이용하여 GCS에서는 침입한 드론을 어디로 내보낼 것인지에 대한 Spoofing좌표를 계산한다.



(그림 4) GPS-Spoofing 지도.

3-3. 공격대상의 GPS 좌표 교란

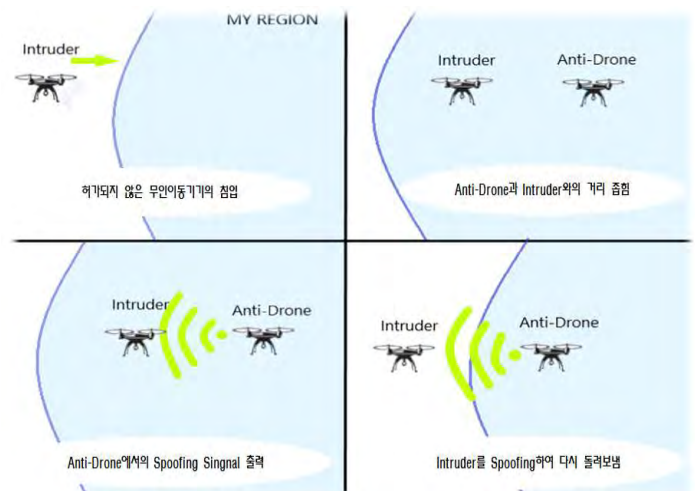
3-2 과정에서 계산된 Spoofing 좌표는 경찰드론이 장착한 GPS-Spoofing의 주파수 송수신기인 Hack-RF One에 등록된다. GPS-Spoofing을 장착한 경찰드론은 침입한 드론에게 다가가 거짓 GPS좌표 데이터 신호를 발사하여 침입한 드론을 특정지역 밖으로 내보낸다. (그림 5)는 Hack-RF One에서 거짓 신호가 발사되는 것을 라즈베리 파이를 통하여 받아보고 있는 것이다.



(그림 5) GPS-Spoofing 신호.

4. Anti-Drone 시스템 작동 시나리오

특정지역으로 허가받지 않은 드론이 침입하게 되면 GCS는 침입한 드론의 경도, 위도 좌표데이터를 수집하게 된다. 앞서 수집된 좌표데이터를 바탕으로 GCS는 침입한 드론을 어디로 내보낼 것인지에 대한 좌표를 계산하게 된다. 계산된 좌표데이터는 경찰드론이 장착한 GPS-Spoofing의 Hack-RF One에 등록이 된다. 출동한 경찰드론은 침입드론에게 다가가 거짓 좌표데이터 신호를 발사시켜 침입한 드론을 takeover 시킨다. takeover 된 침입드론은 특정지역을 벗어나 거짓 좌표데이터의 지역으로 이동하게 된다.



(그림 6) Anti-Drone 과정.

5. 결론 및 향후연구

본 논문에서는 최근 대두되고 있는 문제인 드론을 이용한 불법촬영(몰카)이나 테러공격 등 악의적으로 사용되는 드론을 사전에 차단하고 예방하고자 GPS신호를 교란시키는 기술인 GPS-Spoofing 기술을 이용하여 Anti-Drone 시스템 프로토타입을 제안하고 있다.

본 프로토타입은 크게 경찰드론과 GCS(Ground Control System)로 이루어져 있다. GCS가 관리하는 특정지역에 허가받지 않은 드론이 침입할 경우 GCS에게 침입한 드론의 현재 좌표데이터들이 전송되고, GCS는 이것을 바탕으로 침입한 드론을 어디로 내보낼 것인지에 대한 거짓 좌표를 계산한다. 계산된 거짓좌표를 경찰드론에게 전송된다. 경찰드론은 침입한 드론에게 거짓 GPS신호를 발사하여 침입한 드론을 특정지역 밖으로 내보낸다.

본 시스템은 비교적 쉽게 기본 하드웨어 장비들을 구입하여 구현해 볼 수 있다는 장점을 가지고 있다. 나아가 본 시스템을 실제 사람들이 사용하는 네비게이션이나 무인이동 자동차 등에도 적용해 볼 수 있을 것이라 예상된다.

"본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터지원사업의 연구결과로 수행되었음" (IITP-2020-2018-0-01417)

참고문헌

- [1] Zeng, K.1 et. al. "All Your GPS Are Belong To Us : Towards Stealthy Manipulation of Road Navigation Systems." Proceedings of the 27th USENIX Security Symposium, pp1527~pp1544, 2018
- [2] Eldosouky, AbdelRahman et. al. "Drones in Distress: A Game-Theoretic Countermeasure for Protecting UAVs Against GPS Spoofing" I E E E Internet of Things Journal, 7권, 4호, pp2840~pp2854, 2020
- [3] N Shijith, Prabakaran Poornachandran, V G Sujadevi, Meher Madhu Dharmana, "Spoofing technique to counterfeit the GPS receiver on a drone", 2017 International Conference on Technological Advancements in Power and Energy (TAP Energy), Kollam(India), 2017
- [4] 공현철 외 3명, 픽스호크 드론의 정석, 한국, 성안당, 2019년

Unity 엔진을 이용한 Aveva Marine 뷰어 구현

장원찬*, 양재균*, 김삼성**, 김병석**

*울산대학교

**에이스이엔티

jgyang@ulsan.ac.kr, sskim@aceent.co.kr, bsk0077@aceent.co.kr

Implementation of an Aveva Marine viewer using Unity engine

Jang Won Chan*, Yang Jae Gun*, Kim Sam Sung**, Kim Byung Suk**

*University of Ulsan

**ACEENT

요 약

3차원 CAD를 이용한 선박 설계는 완료 시점에서 부품간의 간섭여부를 판별할 수 있으나 작업순서에 따른 파트의 회전이나 이동 중의 간섭에 대한 판단은 어렵다. 현재는 생산 현장의 작업반장이나 숙련인력이 파트에 대한 회전, 이동시의 간섭 여부를 판단하여 작업순서를 조절한다. 이에 본 논문에서는 Unity 엔진을 이용하여 의장 작업을 실행하기 전에 대상 파트를 손으로 직접 회전, 이동시켜서 실제 작업이 가능한지 여부를 확인할 수 있는 AM 뷰어를 구현하고자 한다.

1. 서론

조선 해양플랜트 생산시물레이션을 디지털 가상시물레이션 기술들로 생산 공정 및 공법 검증, 설비 및 배치의 최적화 및 검증, 생산 관리의 최적화 등의 모사를 실행하는 시스템이다[1]. 3차원 CAD를 이용하여 설계함으로써 의장, 기장, 전장품이 장착완료 시점에서 상호간의 간섭여부를 판별할 수 있으나 작업순서에 따른 파트의 회전이나 이동 중의 간섭에 대한 판단은 설계 시점에서는 불가능하다. 현재는 생산 현장의 작업반장이나 숙련인력이 파트에 대한 회전, 이동시의 간섭여부를 판단하여 작업순서를 조절하거나 기존에 설치한 파트를 분리한 후 재작업을 해야 한다. 즉, 현재의 조선 해양플랜트 의장 작업은 숙련인력의 전문가 지식에 의존하고 있다.

조선소에서 추가적인 비용 및 시수가 발생하는 요소는 파손 3%, 작업미숙 3% 등 선박 건조현장에서 발생하는 것보다 블록의 간섭 50%, 설계정보 오류 30%, 정보누락 10% 등 정보의 오류로 인한 요인이 큰 비중을 차지하고 있다. 이는 설계 수정 과정에서 발생하는 원자재 비용 및 생산 공수, 유휴장비, 운송비, 경비 등 경쟁력 저하를 유발한다[2]. 이에 본 논문에서는 의장 작업을 실행하기 전에 대상 파트를 손으로 직접 회전, 이동시켜서 실제 작업이 가능한지 여부를 확인하는 뷰어를 구현하고자 한다.

2. AM 데이터 파일

AM Data 파일 구조

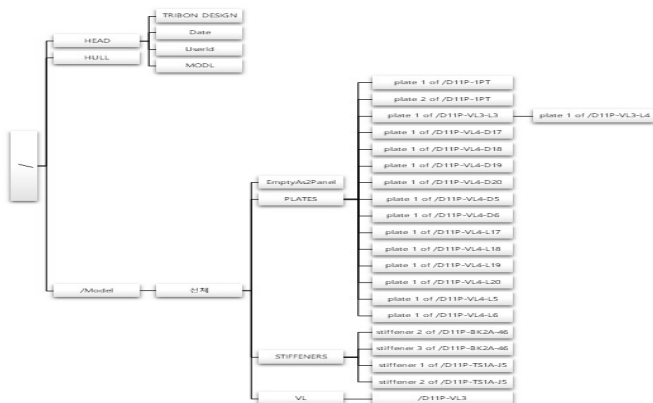
Aveva Marine은 팀 작업을 지원하기 위하여 3차원 형상 정보와 속성 정보를 DBMS를 이용하여 저장하고 관리한다. 한편, 특수한 목적을 위하여 설계 파일을 외부로 내보내기 할 수 있는데 이 경우에 별도로 추출된 파일을 리뷰 파일이라고 한다. 리뷰 파일에는 rvm, rvz, rev 등이 있다. 이 중에서 rvm과 rvz는 바이너리 형식이고 rev는 텍스트 형식이다.

선체	0.00000	0.00000	0.00000
0			
CNTB	1		
1	1		
EmptyAs2Panel	0.00000	0.00000	0.00000
0			
CNTB	1		
1	1		
PLATES	0.00000	0.00000	0.00000
0			
CNTB	1		
1	1		
plate 1 of /D11P-1PT	50150.00000	13450.00000	14706.00000
5			
PRIM	1		
1	1		
0.00100	0.00000	0.00000	0.00000
0.00000	0.00100	0.00000	0.00000
0.00000	0.00000	0.00100	0.00000
50050.00000	13200.00000	14700.00000	
50250.00000	13700.00000	14712.00000	
6			
1			
4			
50050.00000	13200.00000	14700.00000	
0.00000	0.00000	-1.00000	
50050.00000	13700.00000	14700.00000	
0.00000	0.00000	-1.00000	
50250.00000	13700.00000	14700.00000	
0.00000	0.00000	-1.00000	
50250.00000	13200.00000	14700.00000	
0.00000	0.00000	-1.00000	

(그림 1) 샘플 rev 파일 일부

AM 속성 Data 구조

Aveva Marine의 3D CAD 모델에 정의된 속성으로는 식별 속성, 스펙(spec) 카탈로그 속성, 기능 속성, 형상 관련 좌표 및 치수 속성, 객체 간의 연결 속성이 있다[3]. 객체 식별 속성으로는 객체의 고유 아이디(id)를 담고 있는 Name 속성, 객체의 고유 데이터베이스 아이디(id)를 담고 있는 REFNO 속성, 및 형상 파일 이름 정보를 담고 있는 SAT 속성이 있다. 스펙 카탈로그 속성으로는 배관의 카탈로그 정보를 담고 있는 PSPE 속성, 피팅에 대한 카탈로그 정보를 담고 있는 SPRE 속성, 절연 처리용 자재 (insulation) 정보를 담고 있는 ISPE 속성이 있다. 기능 속성으로는 설계 온도 및 설계 압력 정보를 담고 있는 TEMP 및 PRES 속성이 있다. 형상 속성으로는 객체의 좌표 정보를 담고 있는 HPOS, TPOS, POS, APOS, LPOS, 및 P3POS 속성, 객체의 직경 정보를 담고 있는 HBOR, TBOR, ABOR, LBOR, 및 P3BO 속성, 객체의 방향 정보를 담고 있는 HDIR, TDIR, 및 P3DIR 속성이 있다. 마지막으로 연결 속성으로는 객체간의 연결 정보를 담고 있는 HREF 및 TREF 속성이 있다.



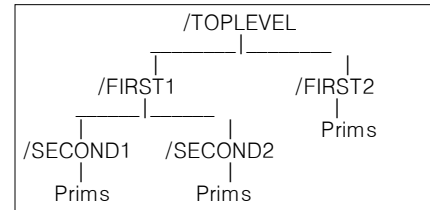
(그림 2) 속성 정보 구조도(일부)

3. AM 데이터 파일 파서

AM binary data file format

리뷰 파일은 여러 레코드 또는 청크로 구성되며 첫 번째는 헤더 청크이다. 청크는 4 개의 문자 식별자, 청크의 끝에 대한 포인터, 주 및 부 개정 번호 및 청크와 관련된 데이터를 포함하는 데이터 세트이다. 청크의 끝에 대한 포인터는 청크를 건너 뛰는데 사용될 수 있으며 개정 번호는 이전 버전과의 호환성을 제공한다. 리뷰 파일에는 다음과 같이 6 가지 유형의 청크가 있다. 헤더 청크(HEAD), 모델 파일 청크(MODL), 컨테이너 시작 청크(CNTB), 컨테이너 엔드 청크(CNTE), 프리미티브 청크(PRIM), 엔드(END):

모든 리뷰 파일의 처음 두 청크는 HEAD 및 MODL 청크이며 모델 파일에 대한 유용한 정보가 포함되어 있다. 작성된 날짜, 파일 노트, 프로젝트, MDB. 이 두 청크 다음에는 END : chunk로 표시된 파일 끝까지 CNTE, CNTB 및 PRIM 청크가 있다. CNTB 및 CNTE 청크는 '아래'에 해당하는 CNTB와 '위'에 해당하는 CNTE를 갖는 PDMS 데이터베이스 계층 구조를 설명한다. 아래 그림은 계층 구조를 재현하는 방법을 보여준다.



(그림 3) Hierachy

AM Data file parser

다음 과정으로 rvm 파일을 읽고 메모리로 로딩하는 프로그램을 작성하였다. 개발언어는 C#을 사용하였고 리뷰파일의 포맷에 따라서 각 청크에 해당하는 클래스를 선언하였다. 아래는 CNTB 청크에 대응하는 클래스의 일부이다.

```
class CNTB : Chunk
{
    private string ContainerName;
    private float[] Origin = new float[3];
    private int Colour;

    public CNTB()
    {
        ContainerName = "";
        Origin[0] = 0.0F;
        Origin[1] = 0.0F;
        Origin[2] = 0.0F;
        Colour = 0;
    }
}
```

(그림 4) CNTB 청크 클래스

아래의 그림은 청크의 데이터가 정수인 경우에 파일의 특정 위치에서 데이터를 읽어 오는 메소드이다.

```
public unsafe int getIntfromBuff(byte[] buff, ref int pos)
{
    int result = 0;
    fixed (byte* ps = &buff[pos])
    {
        result = *ps * 16777216 + *(ps + 1) * 65535 + *(ps + 2) * 256 + *(ps + 3);
    }
    pos += 4;
    return result;
}
```

(그림 5) 파일에서 정수를 반환하는 메소드

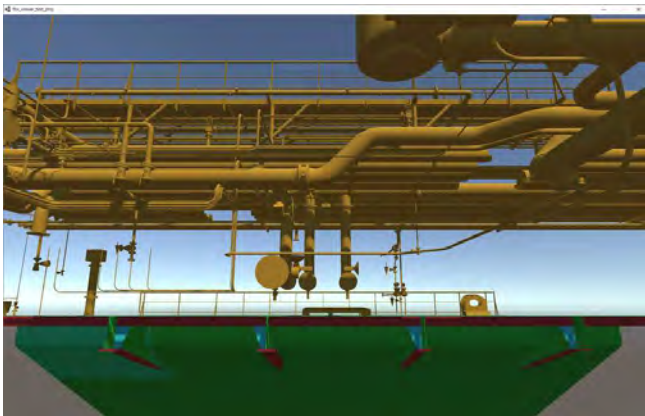
4. Unity 엔진의 동적 Asset 로딩

일반적인 Unity 엔진 사용 방법에서는 프로그램을 개발하는 과정에서 필요한 자원을 Asset으로 등록한 후 빌드하여 배포한다[4]. 3차원 도면 뷰어의 경우에는 다양한 도면을 필요시에 파일형태로 로딩해야 하기 때문에 사전에 Asset으로 등록 할 수 없다. 따라서 외부 도면 파일을 프로그램 실행 시점에서 Unity 엔진으로 로딩해야 한다[5]. 아래는 run-time에 외부 파일을 Unity로 로딩하는 메소드의 일부이다.

```
public GameObject LoadFromFileWithTextures(string
filename, AssetLoaderOptions options = null, GameObject
wrapperGameObject = null, string basePath = null,
AssimpInterop.ProgressCallback progressCallback = null)
{
    var fileData = FileUtils.LoadFileData(filename);
    var extension = FileUtils.GetFileExtension(filename);
    if (basePath == null)
    {
        basePath = FileUtils.GetFileDirectory(filename);
    }
    InternalLoadFromMemoryAndZip(fileData, extension,
basePath, options, wrapperGameObject != null, null, null,
progressCallback);
    var loadedGameObject = BuildGameObject(options,
extension, wrapperGameObject);
    ReleaseImport();
    return loadedGameObject;
}
```

(그림 6) run-time에 파일을 로딩하는 메소드

아래는 Unity엔진을 이용하여 AM 데이터 파일을 run-time에 읽어서 표현한 최종 결과이다.



(그림 7) 뷰어 최종 결과

참고문헌

- [1] 이필립,황인혁. "조선해양 공정 상호검증 시물레이션과 생산관리 플랫폼" 大韓造船學會誌 VOL.48 NO.4 (2011):10-13
- [2] 최영태(Yeong-Tae Choi),서흥원(Heung-Won Suh),이순섭(Soon-Sup Lee). "선체설계와 의장설계간의 정보인터페이스 기법 연구" 大韓造船學會 論文集 VOL.50 NO.6 (2013):458-465
- [3] 손명조(Myeong-Jo Son),강형우(Hyungwoo Kang),김태완(Tae-wan Kim). "조선 선체 블록 모델의 재사용을 위한 AVEVA Marine Scheme 기반 모델링" 한국CDE학회 논문집 VOL.19 NO.1 (2014):41-49
- [4] 최형욱 (Hyeoung Wook Choi), 강수명 (Soo Myung Kang), 김경준 (Kyung Jun Kim), 김동영 (Dong Young Kim), 정윤재 (Yun Jae Choung). "Unity 3D 엔진을 활용한 강우레이더 자료 시각화 프로토타입 개발" 한국지리정보학회지 VOL.18 NO.4 (2015):131-144
- [5] Unity Manual, <https://docs.unity3d.com/Manual/LoadingResourcesatRuntime.html>

ACKNOWLEDGMENT

이 성과는 2019년도 중소벤처기업부의 재원으로 한국산학 연합회 연구마을지원사업의 지원을 받아 수행된 연구임

스마트 기기를 활용한 노령인구의 헬스케어 플랫폼 개발

한보현*, 공인복**, 김다원***, 이혜민****, 정유담*****, 김상오*****

*상명대학교 휴먼지능정보공학과, **링크플러스 사업단 상명대학교, 상명대학교
컴퓨터과학과***, 상명대학교 글로벌경영학과, ****상명대학교 글로벌경영학과,
*****상명대학교 식품영양학과

hbh0604@naver.com, kib@smu.ac.kr, tmxk0460@gmail.com, 951001a@hanmail.net,
aadamk@naver.com, sangoh51@naver.com

Healthcare management platform for elderly population using smart devices

Bohyun Han*, In-bog kong**, Dawon Kim***, Hyemin-Lee****, Yoodam Jung*****,
Sangoh Kim*****

*Dept. of Human Intelligence Information Engineering, Sangmyung University, **Leaders
in INdustry-universty Cooperation, ***Sangmyung University, Dept. of Computer
Science, ****Sangmyung University, Dept. of Department of Global Management,
*****Sangmyung University, Dept. of Department of Global Management, *****Dept. of
Food and Nutrition, Sangmyung University

요 약

노년층의 건강관리를 위하여 몸상태를 확인할 수 있는 심박센서와 운동량을 확인할 수 있는 모션센서 및 간단한 센서를 활용하여 실시간으로 건강분석과 관리 및 처방을 할 수 있는 방안을 제시하고 플랫폼 개발에 도전함.

1. 서론

우리나라의 고령화 속도는 세계 최고 수준이다. 2017년 고령사회(총인구 비율의 14%이상)에 진입하였으며 2026년에는 초고령 사회에 진입할 것이라는 예측이 나오고 있다. 이에 따른 노년층의 의료 서비스의 수요가 증가하며 이에 따른 의료비용이 무시할 수 없는 수준이 되었다. 증가하는 의료비용의 부담을 낮출 해결방안으로 노년층을 주 타깃으로 한 'ICT 기반 스마트 헬스케어 시스템'을 제안하였다.



(그림 1) 스마트 헬스케어 시장 규모

웨어러블 기기가 시중에 보급되면서 그와 관계있는 스마트 헬스케어 산업 또한 발달하기 시작했다. 그림 1에서처럼, 스마트 헬스케어의 시장규모는

2020년 1,015억 달러 규모가 되었고 아직 성장하고 있는 분야이다.

스마트 웨어러블 기기를 활용하면 사용자의 생체 데이터를 지속적으로 측정하고 분석할 수 있다. 또한 분석한 데이터를 활용하여 사용자에게 건강한 일상생활(식생활, 운동 등)을 제안할 수 있다. 웨어러블 헬스케어 디바이스를 노령 인구의 건강 관리와 접목시킨다면 한국의 고령화로 인한 의료 비용 증가 문제를 해결할 수 있다고 가정하였다.

이를 위한 스마트 헬스케어 웨어러블 디바이스 제작을 위하여 실험을 진행하였다. 헬스 케어에서 노년층에게 필요한 요구사항을 분석하고, 개인 별 케이스에 대해서 가설을 설정하고 분석하는 과정에서 웨어러블 기기와 연계하여 헬스 케어에 적용할 수 있는 요소들을 정리하였다.

2. 웨어러블 기기 센서 실험

웨어러블 기기에 장착할 수 있는 센서를 사용하여 실험하였고 웨어러블 기기를 착용하였을 때 측정하고 수집할 수 있는 데이터들을 정리하였다.

센서는 (주)디엠비이치의 9축 모션센서를 활용하

였으며 이를 이용하여 동작 모니터링을 진행하였다. 결과적으로 웨어러블 기기의 센서를 활용하여 각속도와 가속도, 속도, 거리 등을 측정할 수 있고 이를 추적하여 사용자의 이동 경로 등을 측정할 수 있다는 것을 알게 되었다.



(그림 2) 9축 모션센서로 측정한 데이터

3. 실험



(사진 1) 스마트 웨어러블 디바이스 핏빗

웨어러블 디바이스로 얻은 생체 데이터를 기반으로 운동 처방을 내릴 수 있을 것이라 가정하였으며 이를 증명하기 위하여 간단한 실험을 통해 참가자들의 생체 데이터를 수집하였다.

이 실험에서 활용한 기기인 핏빗은 24시간 심박수 모니터링과 수영 방수, 피트니스와 수면 모니터링 등의 기능이 사용 가능하여 이 실험의 기기로 선정하였다.

실험 요소는 운동 강도와 수면 정도이다. 운동 강도에 따라서 운동을 많이 하는 사람 / 적당히 하는 사람 / 운동을 하지 않는 사람의 세 집단으로 나누어 진행하였다.

3-1. 가설

실험 과정에서 세운 가설은 이러하다. 심박수 센서를 통해 얻을 수 있는 정보들을 활용하여 가설을 정하였다.

-가설 1) 운동을 많이 한 사람은 수면의 질이 높을

것이다.¹⁾

-가설 2) 운동을 많이 한 사람은 심장 강화가 많이 되어 운동 시 심박수의 변화가 적을것이다.(스포츠 심장)²⁾

-가설 3) 수면이 부족할 경우 평균 심박수가 수면이 좋을 때보다 높을 것이다.³⁾

이 데이터들은 모두 웨어러블 디바이스를 활용하여 측정 가능한 데이터들이다. 이 가설의 기준은 인간의 생체 데이터를 수집할 때 가장 대표적인 센서인 심박 센서를 활용하여 측정할 수 있는 데이터를 활용하였다.

이 가설은 웨어러블 디바이스를 통해 얻을 수 있는 생체 데이터와 이를 활용한 운동 처방을 내리는 과정에서 생체데이터를 활용할 수 있는지를 실험하기 위한 단순한 수준의 가설이다. 이 가설을 증명하는 과정 동안 웨어러블 기기를 설계하는데 보완해야 할 점은 무엇인지, 어떤 데이터를 측정해야 하는지, 개인화된 운동 처방을 위해 어떤 데이터를 분석해야 하는지를 탐구하였다.

3-2. 실험과정



(사진 2) 운동하는 팀원

팀원들이 웨어러블 기기(핏빗)을 착용한 채 생체 데이터를 직접 수집하였다. 운동을 자주 하는 집단 / 운동을 적당히 하는 집단 / 운동을 전혀 하지 않는 집단으로 팀원들을 나누어 각자의 운동 강도를 정하였다. 운동을 자주 하는 집단과 운동을 적당히

하는 집단은 ‘7-Minute WorkOut’이라는 핏빗 내의 운동 프로그램을 진행하였고 공통된 운동에 대한 데이터를 수집하였다.

3-3. 결과

실험을 진행하여 얻은 결과는 이렇다.

수면 데이터 분석											
인원	1월 자	2월 자	3월 자	4월 자	5월 자	6월 자	7월 자	8월 자	9월 자	10월 자	평균 결과분석
C 수준	62	76	72	78	78	68	71	73	71	71	소폭상승
C 수준	70	70	76	76	52	65	60	75	67	47	소폭하락
B 수준	59	57	82	56	58	61	76	44	67	67	소폭상승
B 수준	67	79	78	61	78	80	60	78	71	70	소폭상승
B 수준	61	64	73	74	74	75	76	80	73	77	소폭상승
A 수준	75	71	71	70	73	72	77	73	67	67	소폭하락
A 수준	81	64	76	85	78	82	75	74	67	76	소폭하락

운동 시의 평균 심박수											
인원	1월 자	2월 자	3월 자	4월 자	5월 자	6월 자	7월 자	8월 자	9월 자	10월 자	평균 결과분석
C 수준											없음
C 수준											없음
B 수준	105	116	137	129	120	139	146	141	112	147	상승
B 수준	115	115	124	131	119	106	117	109	114	134	상승
B 수준	150	129	154	154	125	136	146	162	142	146	소폭하락
A 수준	128	125	128	128	129	146	137	140	139	140	상승
A 수준	117	130	128	148	125	128	126	116	110	145	상승

그 외 운동A 그룹 인원											
인원	1월 자	2월 자	3월 자	4월 자	5월 자	6월 자	7월 자	8월 자	9월 자	10월 자	평균 결과분석
A 수준	163	130	137	110	173	157	146	136	153	136	하락
A 수준	139	137	145	194	163	125	125	117	125	141	소폭하락

(표 1, 2) 실험 데이터 분석 표

-가설1)의 결과: 운동 강도가 낮을수록 수면 퀄리티 점수가 낮아지는 것을 볼 수 있었다.

-가설2)의 결과: 평소 운동의 강도와 운동 상황에서의 심박수의 변화에는 큰 차이가 없었다.

-가설3)의 결과: 수면이 부족할 경우 평균 심박수가 높았다.

각 가설을 증명하기 위해 웨어러블 기기로서 측정된 생체 데이터를 수집하고 분석하였다. 이 과정에서 생체 데이터 측정을 위해 필요한 센서가 무엇인지 분석하였고 웨어러블 기기를 통해 사용자의 신체 상태를 분석할 수 있으며 이에 따른 운동 처방이 가능하다는 것을 증명하였다.

첨부한 표 외에 운동시 최대 심박수와 심박 구간, 걸음 수 또한 분석하였다.

3-4. 운동처방 방안 구체화

웨어러블 기기를 활용하여 사용자의 운동 주기와 수면 양호도를 파악한다. 심박수 등 수집한 데이터를 기반으로 사용자의 건강 상태를 먼저 분석한 뒤에 운동 처방을 실시한다. 사용자의 요구에 따른 적절한 강도의 운동을 제시하며 운동을 했을 때 기기

의 모션 센서를 활용하여 자세를 분석하고, 그에 따른 정확도를 확인한다.

운동을 할 때마다 점수를 부여하며 평균 점수에 따라 운동의 강도를 점진적으로 강화한다.

운동 처방은 사용자가 운동을 잊지 않도록 주기적인 알람을 통해 처방되며 사용자의 운동 활동은 커뮤니티 기능을 활용해서 다른 사람들과 공유하고 성취를 나눌 수 있다.

운동의 결과는 측정된 생체 데이터를 한 달 단위로 분석하여 보고서로 전달한다.

4. 향후 과제

4-1. 현존 제품의 문제점 및 개선 방안

실험을 통해 분석한 웨어러블 기기 제품에는 몇 가지 문제점들이 존재했다. 실시간으로 데이터 전송이 불가능 했으며 서버와 데이터를 주고받지 않은 탓에 실시간으로 적절한 운동 처방을 내리지 못하였다. 개인에 맞춘 운동 처방을 내릴 수가 없었다.

또한 사용자가 웨어러블 기기를 착용하기 이전의 운동 주기를 분석하기 어려워 이 요소 또한 운동처방에 고려할 수 없었다.

4-2. 데이터 측면에서의 향후 활용 방안

노인 건강 관리 스마트 기기를 활용하여 얻을 정보는 크게 여섯가지로 나눌 수 있다. 자이로 센서를 활용한 회전 데이터, GPS 센서를 활용한 이동 위치 데이터, 공간 좌표에 따른 회전 데이터를 기록한 동작 데이터, 심박 센서를 활용한 심박 데이터, 사용자의 실시간 자세 데이터, 사용자 설정 운동 공간 데이터이다.

이 신체 모니터링 신호 기반의 데이터를 활용하여 사용자의 활동량을 파악하고 사용자의 운동 동작 자세를 검출할 수 있으며 올바른 동작을 권장해 줄 수 있다. 이 정보를 축적하여 빅데이터로 활용할 수 있다면 헬스, 의료 분야 등 다양한 분야에서 유용하게 활용될 수 있다.

4-3. 노인층을 주 사용자층으로 고려

노인층을 주 사용자층으로 고려한다. 그러므로 노

년층에게 흔한 위급 상황의 케이스에 대해 분석을 해야 한다.

사용자가 몸 상태에 문제가 생겼을 경우 가까운 응급시설에 연락하도록 하는 기능이 필요하다. 심박수 센서를 활용하여 사용자가 심장에 이상이 생겼을 경우 사용자에게 음성 기능을 활용하여 사용자의 의식을 확인해야 한다. 사용자의 체온을 주기적으로 파악하기 위하여 온도 감지 센서를 활용해야 한다.

그 외에도 사용자의 데이터를 정리하고 저장하기 위한 플랫폼이 필요하며 운동의 자세를 다각도로 평가하기 위한 센서가 필요하다.

결론적으로 웨어러블 기기를 이용한 노인층의 다양한 모니터링 방안을 제시하고 스마트 기기를 활용한 노령 인구의 헬스케어 플랫폼의 개발로 이어진다.

5. 구체적인 연구 성과

지식재산권(국내·외 특허, 실용신안, 프로그램 등록, 기타 등으로 종류 구분):

- 특허출원 :

. 출원번호/출원일 : 10-2019-0126462 / 2019. 10.

11

. 발명의 명칭 : 노령인구 건강관리 시스템

관인생략	
출원번호통지서	
출원일자	2019.10.11
특기사항	심사청구(유) 공개신청(무)
출원번호	10-2019-0126462 (접수번호 1-1-2019-1039847-39)
출원인명칭	상명대학교산학협력단(1-2013-011529-0)
대리인성명	특허법인 대한(9-2010-100001-4)
발명자성명	정유담 이해원 김다원 한보현 최정용 김상오 이해민 서정연 공인복
발명의명칭	노령인구 건강 관리 시스템.
특허청장	

(사진 2 : 출원번호통지서)

6. 연구 결과 최종 목표

몸 상태를 확인할 수 있는 심박센서와 운동량을

확인할 수 있는 모션 센서 등을 활용하여 실시간으로 모니터링과 건강 분석, 관리 및 처방을 할 수 있는 방안을 제시한다. 노령인구의 건강을 관리할 수 있는 플랫폼을 제시하며 이를 위한 새로운 웨어러블 기기를 고안했다.

웨어러블 기기와 중앙 서버 간의 네트워크를 구성하고 웨어러블 기기를 통해 측정된 데이터를 중앙 서버로 전송하는 시스템을 제시하였다. 중앙 서버에서 획득한 데이터를 사용하여 신체 상태를 분석하는 분석모델을 제시하고, 분석 결과를 피드백하여 이를 통해 운동요법과 식단요법을 함께 제안하는 평가모델을 제시한다.

7. 최종 결과

추후 노령 인구를 위한 스마트 밴드 개발 시, 실험을 통해 측정된 결과를 활용하여 수면 및 심박 상태를 기반으로 운동 처방 방안을 구체화한다. 이러한 생체 상태 측정을 기반으로 한 운동 솔루션 제공 방식은 향후 진행될 스마트 밴드 개발 과정에 유용한 기반으로 활용되고 몸 상태를 측정할 수 있는 여타 다른 요소를 연구할 수 있는 기회가 될 것이다.

- 1) <http://www.k-health.com/news/articleView.html?idxno=17403> : 피곤한 몸 자야할까?, 운동해야 할까? , 저자 : 고정아 디에이(D·A)성형외과·피부과 원장, 헬스경향/ 운동 강도가 수면의 질과 정서에 미치는 영향 논문, 저자 : 류호상
- 2) http://health.chosun.com/site/data/html_dir/2018/12/10/2018121001066.html : 선수들의 '스포츠 심장'... 일반 심장과 어떻게 다를까? 출처 : 헬스조선, 저자 : 이혜나 https://jhealthmedia.joins.com/article/article_view.asp?pno=19885 : [출처: 중앙일보] 운동 선수처럼 '스포츠 심장' 만들려다 독 된다, 저자 : 김선영 http://news.khan.co.kr/kh_news/khan_art_view.html?art_id=201812101032002 : [출처: 경향신문] 오늘날 박지성 있게 한 '스포츠심장', 저자 : 유대형
- 3) 심박변이도(HeartrateVariability)분석을 통한 불면과 자율신경계 기능의 상관관계 연구 논문, 저자 : <엄은진,정승환,박우람,이범준,나병조>강남경희한방병원 내과학교실 성인의 수면의 질에 따른 심박변이도, 피로, 우울 및 불안과의 관계 논문, 저자 : 김 주아 1 · 강승 완 2 서울대학교 간호대학 박사과정생 1, 서울대학교 간호대학 조교수2

디자인 씽킹 메카니즘과 소프트웨어공학 접목에 관한 연구

서채연*, 김장환*, 박보경*, 장우성*, 손현승*, 김영철*

*홍익대학교 소프트웨어공학연구실

{*chyun,janghwan,park,jang,sonh,bob}@selab.hongik.ac.kr

A Study on mapping Software engineering with Design thinking mechanism

ChaeYun Seo*, Janghwan Kim*, Bokyung Park*, Woo sung Jang*, Hyun Seung
Son*, R. Young Chul Kim*

*SE Lab, Dept of Software and Communications Engineering, Hongik
University

요 약

4차 산업혁명시대가 도래함으로써 수많은 영역에 다양한 소프트웨어(SW)가 필요할 것이며, 특히 비전공자 및 기초 전공자들의 창의적 사고 기반 SW에 대한 이해가 요구된다. 하지만 문제는 창의적 사고 기반의 SW에 대한 정의 및 아이디어가 부족하다. 우리는 교육 영역에서의 창의적 사고 방법 및 주요 쟁점들을 비전공자들에게 강의한 경험이 있지만 실질적으로 창의적 사고기법을 통해서 소프트웨어로 구현하는 것에 큰 어려움을 겪고 있다. 따라서 이러한 점을 개선하는 창의적 사고 기법과 소프트웨어 공학기법을 접목인 디자인 씽킹 메카니즘과 소프트웨어공학 접목을 제안한다.

1. 서론

4차 산업혁명시대가 도래하면서 SW가 지능형, 맞춤형으로 진화되고 있다. 지능 정보와 정보 통신 기술 융합 환경에서는 창의성, 사고력, 정보 수집, 처리, 활용 능력, 문제 해결력의 중요성이 필요하다. 창의적 인재양성은 문제 발견과 확장된 사고를 해야 하고, 논리적으로 분석하고 의미적으로 표현하기 위해 분석적 사고를 해야 한다. 창의적으로 무언가를 이루어내려면 다양한 분야의 지식과 경험을 통해 문제를 바라봐야한다. 또한 해결책을 찾기 위해 융복합하는 사고를 발휘해야 한다. 이처럼 생각이 한쪽으로 치우치지 않고 융합적으로 접근하는 사고가 디자인 씽킹이다[1].

비전공자/전공자들을 위한 창의적 문제 해결 방법으로 디자인 씽킹 및 컴퓨팅 씽킹을 통해 문제 해결 하려는 시도가 매우 많다. 문제는 비전공자에게 코딩은 너무 어려운 개념으로 받아들여져 코딩을 어려워한다는 것이다. 창조적 생각은 실현가능할지 모르나, 코딩까지의 연결 고리를 찾지 못하고 있다는 것이다. 이 문제를 해결하고자, SW공학적 디자인 씽킹 기반 코딩 개발 체계(방안)를 제안한다. 이 방법은 SW공학 기반 소프트웨어 개발과 디자인 씽킹

메카니즘을 접목한다. 디자인 씽킹 관점의 창의적 사고 기법을 통해 비전공자/기초 전공자들이 정확한 문제인식 및 해결 능력을 배양하고 창의 융합적 문제해결이 가능한 코딩 능력 향상을 목적으로 한다.

본 논문의 2장에서는 관련연구로서 디자인 씽킹과 소프트웨어 개발을 소개한다. 3장에서는 디자인 씽킹과 소프트웨어 개발을 접목을 제안하고 소개한다. 4장에서는 결론과 함께 향후 연구 방향에 대해 서술한다.

2. 관련연구

2.1 디자인 씽킹

최근 디자인 씽킹은 현장 중심의 디자인과 인간 중심의 창의적 문제 해결을 위한 사고 방법론으로 주목받고 있다. 창의적으로 문제를 해결하기 위해 확산적 사고와 수렴적 사고를 결합하여 다양한 사고능력을 키우는 것이 디자인 씽킹의 목표이다[1]. 디자인 씽킹은 다음의 절차를 따른다.



(그림 1) 디자인 씽킹 프로세스

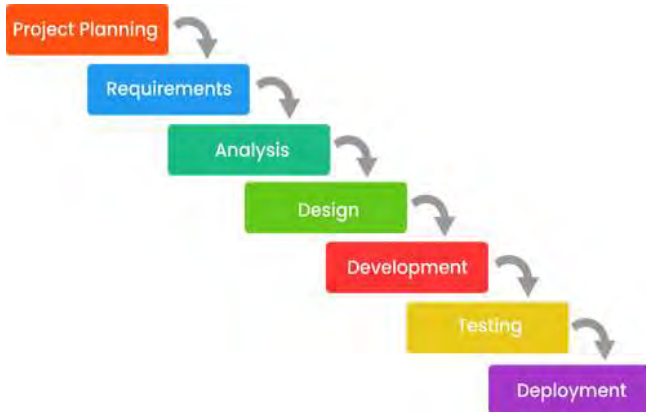
- 공감-인터뷰, 관찰
- 문제정의-문제해석, 문제정의
- 아이디어 찾기-확산적사고/수렴적 사고,

자유로운 아이디어 발상

- 프로토타입-제품구현
- 테스트-프로토타입 테스트, 피드백, 개선

(그림 1)은 디자인 씽킹 프로세스이다. 디자인 씽킹은 공감과 정의를 기반으로 문제를 발견하고 이해하는 단계를 거쳐 창의적 아이디어 발상, 창의적 아이디어 표현을 한다. 아이디어를 제품으로 구현하고, 시제품을 테스트 한 후, 피드백을 받고 개선시켜 나간다[1].

2.2. SW공학 개발 프로세스



(그림 2) 소프트웨어공학 개발 프로세스

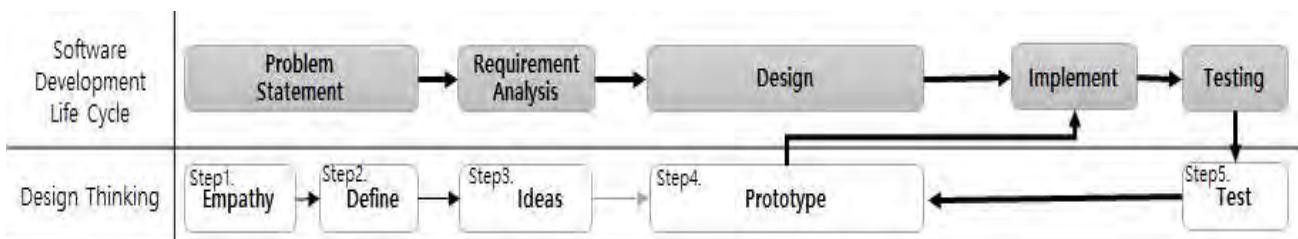
소프트웨어가 발전함에 따라 소프트웨어 개발의 규모가 점점 커지면서 보다 체계적이고 시스템적인 개발이 요구되어왔다. (그림 2)는 소프트웨어공학 개발 프로세스이다[4]. 계획단계에서는 비용, 기간 등 프로젝트 수행에 필요한 요소들을 계획하는 일을 한다. 또한 프로젝트 수행 시에 발생할 수 있는 위험을 파악한다. 요구분석 단계는 시스템 파악 및 문제점을 분석하고 사용자 인터뷰를 통해 새로운 요구사항들을 도출하여 수집한다. 설계 단계에서는 분석 단계에서 표현한 도구들을 바탕으로 시스템 및 구조를 설계하고 구현에 필요한 설계를 한다. 테스트 단계에서는 다양한 테스트 기법을 사용하여 작은 단위에서부터 큰 단위에 이르는 테스트들을 통해 소프트웨어의 품질을 높이고 오류들을 찾고 수정한다. 유지보수 단계에서는 개발이 완료된 시점으로부터 고

객이 사용하면서 생기는 문제점 등을 파악하고 수정, 보완, 보강 등의 작업을 통해서 소프트웨어가 지속적으로 잘 작동되도록 돕는다.

3. 디자인 씽킹과 소프트웨어공학 개발 접목

비전공자/기초 전공자의 코딩 수업은 컴퓨팅 사고력 기반의 창의적 문제 발견 및 해결 능력을 위해 디자인 씽킹을 이용한 새로운 어플리케이션 개발 과정을 교육하고 있다. 이런 다양한 이론들은 창의적 사고를 통해 문제점을 도출하고, 아이디어를 설정하는 측면에서는 매우 유용한 방법이다. 하지만 실질적인 코딩으로 넘어가는 단계가 명확하지 않아 학생들이 코딩으로 작성하기에 많은 어려움이 있다. 또한 비전공자/기초 전공자들은 디자인에서 코드를 유추하지 못한다. 프로그래밍을 만들거나 새로운 어플리케이션을 만들기 위해서는 소프트웨어공학 기반 코딩 개발 프로세스가 필수적이라고 생각한다. 따라서 디자인 씽킹과 소프트웨어 개발 프로세스(즉, 문제 정의부터 코딩까지의 공정 단계들)를 접목한 “**소프트웨어 공학적 디자인 씽킹 기반 코딩 개발**”이 필요하다.

제안하는 프로세스는 비전공자와 기초전공자를 위한 코딩 교육 프로세스이다. (그림 3)은 디자인 씽킹 기반 소프트웨어 공학적 개발 접목이다. 이 프로세스는 소프트웨어 개발 라이프 사이클에 있는 문제정의단계와 디자인 씽킹의 공감(Step 1)과 문제정의 단계(Step 2)를 접목시켜 체계적이고 정확한 문제인식을 통해 요구사항을 분석한다. 디자인 씽킹의 ‘공감’을 통해 고객과의 인터뷰를 하는 것이 문제를 보다 정확하게 인식하는데 도움이 된다. 인터뷰 등의 공감기법을 통해 문제를 인식하게 되면 자연어로 구성된 Problem Statement 고객이 원하는 문제를 보다 정확하게 정의 내릴 수 있다. 다양한 문제정의 방법에 의해 문제를 더 직관적으로 이해하고 이러한 방법들을 통해서 비전공자 및 기초전공자들은 문제를 보다 정확하게 인식 할 수 있다. 그렇게 정리된



(그림 3) 디자인씽킹 기반 소프트웨어 개발 접목

문제들을 정의하면 간결화된 문제들을 해결하는데 초점을 맞추고 문제의 범주가 좁아지기 때문에 설계에 더 용이하다. 문제가 정의 되면 문제를 해결하기 위한 다양한 아이디어(Step 3)를 제시할 수 있다. 이 단계는 소프트웨어공학의 요구사항 분석단계와 접목시켜 요구사항 분석단계에서 나올 수 있는 코딩에 필요한 입출력 정보와 기능/비기능을 도출할 수 있다. 아이디어 제시 방법으로는 브레인스토밍, 마인드맵 등의 방법들이 있다. 그 중 마인드맵 기법은 소프트웨어공학기법 중 유스케이스 모델로 표현이 가능하다. 유스케이스 모델로 맵핑이 되면 유스케이스 모델로부터 클래스 다이어그램과 시퀀스 다이어그램을 그려낼 수 있다. 시퀀스 다이어그램은 문제 해결을 위해 객체를 정의하고 객체간의 상호작용 메시지 시퀀스를 시간의 흐름에 따라 나타내는 다이어그램을 말한다. 이를 통해 문제로부터 소프트웨어에서 작동하는 메서드의 흐름을 알 수 있다. 또한 클래스 다이어그램은 UML 다이어그램의 한 종류로써 시간에 따라 변하지 않는 시스템의 정적인 면을 보여주는 대표적인 UML구조 다이어그램이다. 이 방법을 통해 소프트웨어를 구성하는 클래스들 사이의 관계를 알 수 있다. 이렇게 설계된 다이어그램들을 통해서 우리는 디자인 씽킹의 프로토타입(Step 4) 기법을 이용해 완성될 소프트웨어 모습을 추상화할 수 있다. 프로토타입이 완성되면 지속적인 고객과의 협력을 바탕으로 완성체에 가까운 프로토타입을 만들 수 있다. 프로토타입이 완성되면 코딩(개발)을 통해 소프트웨어를 구현한다. 구현된 소프트웨어는 테스트를 통해 고객의 요구사항 즉, 정의된 문제들과의 비교를 통해 구현된 소프트웨어의 품질 상태를 알 수 있다. 이때, 다시 디자인 씽킹 방법의 프로토타입 테스트(Step 5)을 통해 배포된 소프트웨어를 바로 수정하지 않고 프로토타입을 보완, 개선한다. 이렇게 개선된 프로토타입을 다시 구현함으로써 개선된 소프트웨어로 배포가 가능하다.

4. 결론

비전공자 및 기초 전공자들은 소프트웨어 공학적 디자인 씽킹 기반 코딩 개발프로세스를 통해서 창의적 문제 발견 및 해결 능력을 위한 코딩이 가능하다. 또한 창의적인 디자인과 논리적 사고 기반으로 훈련하고 체계적으로 시스템 내에서 코딩함으로써 표준화된 코딩 교육 및 코딩 개발자에게 좋은 습관 내재화가 가능하다. 코딩을 배우는 학생들에게 기초

프로그래밍의 코딩 절차 표준에 대한 성숙도를 향상시킬 수 있다. 또한 프로그래밍 교육을 체계적으로 공부하지 못했던 비전공자들에게 표준 코드 절차를 내재화시킴으로써, 코딩에 대한 두려움을 이겨낼 수 있다. 향후 연구는 소프트웨어 공학적 디자인 씽킹 기반 코딩 개발프로세스 기반의 코딩 교육 시스템을 개발할 것이다.

참고문헌

- [1] 송태란, 이정현, 문제해결력을 키우는 디자인 씽킹(대한민국), 한빛미디어, 2019
- [2] 소프트웨어 정책 연구소, 지능정보사회를 대비하는 SW교육 관련 정책
- [3] Chae Yun Seo, So Young Moon, R. Young Chul Kim, "Open Source of Integrated Service Tools for Venture Small Business Maintenance Solutions," The Journal of the Korea Information Processing Society (KIPS), Vol. 23, No. 6, pp. 22-32, November 2016.
- [4] 김치수, 쉽게 배우는 소프트웨어 공학, 한빛아카데미, 2020.
- [5] <https://www.interaction-design.org/literature/article/design-thinking-getting-started-with-empathy>

톡톡한 한경이: 학내 챗봇 서비스 설계 및 개발

박소희, 김미희*

한경대학교 컴퓨터응용수학부

sowe0127@gmail.com, mhkim@hknu.ac.kr*

TocTocHan HanKyongE: Design and Development of Chatbot Service in University

So-Hee Park, Mihui Kim*

School of Computer Engineering and Applied Mathematics, Hankyong National University

요 약

본 논문에서는 한경대학교 학생들에게 빠르고 정확하게 학내외 정보를 제공하기 위하여 개인의 스마트폰 보급과 흔히 사용되는 메신저 서비스에 맞춰 이에 기반한 챗봇 서비스를 설계하고 개발한다. 본 챗봇 서비스를 통해 학교 홈페이지, ARS, 어플리케이션 설치 등을 이용한 방법보다 더욱 빠르게 시공간의 제약 없이 원하는 학교 내 정보를 얻을 수 있다.

1. 서론

챗봇이란 자동화된 대화를 통해 목적을 이루도록 설계된 기술이자 서비스이다[1]. 인공지능 기술에 힘입어 챗봇 서비스는 점점 다양한 응용으로 개발되어 서비스되고 있고, 고객 상담, 예약, 주문을 위한 서비스 외에도 대학이나 기업 안내 서비스 등으로 확대되고 있다.

본 논문에서 설계 및 개발된 챗봇 시스템은 흔히 사용하는 카카오톡의 플러스 친구에서 '톡톡한 한경이'를 검색하여 친구를 맺으면 사용할 수 있는 챗봇 서비스이다. 사용자가 제일 처음 플러스 친구를 맺으면 웰컴 인사로 시작이 되고 그 이후에는 필요시에 챗봇을 호출하여 원하는 정보를 얻을 수 있다. 정보 검색으로는 두 가지 방법을 사용할 수가 있다. 첫 번째로는 주어진 선택지를 선택하여 답변을 얻는 방법, 두 번째로는 직접 입력하여 답변을 얻는 방법이다. 학교 관련 정보, 학과 관련 정보, 캠퍼스 내 시설에 대한 정보, 학점 계산에 대한 정보, 학교 주변에 관한 정보 등을 제공하고 있다.

2. 선행 연구 및 관련 작품

타 대학교에서 사용되고 있는 챗봇 서비스들을 직접 사용해봄으로써 어떤 장단점이 있는지 파악하였다. 또한, '카카오 I 오픈빌더[2]' 플랫폼이 카카오톡 챗봇 개발 환경에 대한 업데이트가 활발하여 많은 기능을 사용할 수 있고, 챗봇 서비스가 카카오톡

을 통해 많이 제공되는 만큼 가장 적절하다 생각되어 선택하였다. 타 대학교에서 개발 서비스 중인 챗봇 서비스로는 킹고봇[2], 특수리[3], 중앙대 챗봇 서비스[4]가 있다. 킹고봇은 성균관대 학내 정보 제공 서비스로서 학번으로 학생을 등록하여 개인화 정보 서비스가 가능하고, 학교에서 제공하는 정적 정보와 학교 DB 조회를 통해 도서관 좌석 및 빈 강의실 조회 등 동적 정보를 카카오톡 메시지로 조회 기능을 제공한다. 특수리는 연세인을 위해 학술정보 제공 서비스의 품질을 향상하기 위한 챗봇 서비스를 제공하고 있다. 중앙대 챗봇 서비스는 학식메뉴, 강의시간표, 교내연락망, 도서관이용에 관한 정보 등을 제공하고 있다. 본 논문에서 제안한 톡톡한 한경이는 한경대 교내외 정보를 제공하고, 인공지능 기술을 이용하여 부드러운 대화가 가능하다. 개인별 학점 계산과 캠퍼스맵과 지도를 제공하고 설정을 통해 원하는 정보 알림 받을 수 있다.

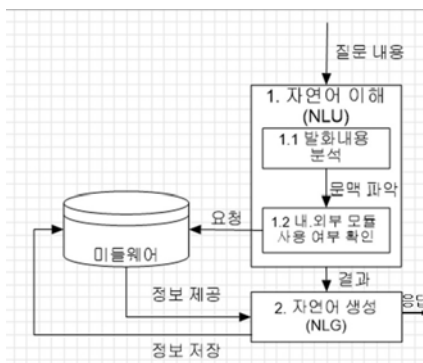
3. 제안하는 챗봇 서비스



(그림 1) 제안하는 시스템 개요도

(그림 1)은 제안하는 챗봇 서비스를 위한 시스템

개요도를 도시한 것이다. 사용자가 카카오톡 애플리케이션을 통해 질문을 입력하면 챗봇 서버에 질문을 전달하고, API를 통해 미들웨어의 기능을 제공하여 챗봇 서버를 통해 응답을 리턴하여 준다. (그림 2)는 챗봇 서버와 미들웨어를 통해 기능을 제공하는 구조도를 도시하였다. 사용자로부터 질문을 입력 받으면 1.자연어 이해와 2.자연어 생성 모듈을 통해 응답을 제공한다. 1.자연어를 이해하는 과정은 발화 내용을 분석하여 문맥을 파악하고 내·외부 모듈 사용 여부를 결정하여 미들웨어로 요청하거나 2.자연어 생성 모듈로 결과를 전달한다. 외부 모듈을 사용하는 경우 미들웨어에 정보를 제공하여 그 결과를 리턴 받아 자연어 생성 모듈로 입력된다. <표 1>은 본 논문에서 설계 및 개발한 ‘톡톡한 한경이’ 챗봇 서비스에서 제공하는 기능들이다.



(그림 2) 챗봇 내의 기능 구조도

<표 1> 한경대 톡톡이 챗봇 서비스에서 제공하는 기능

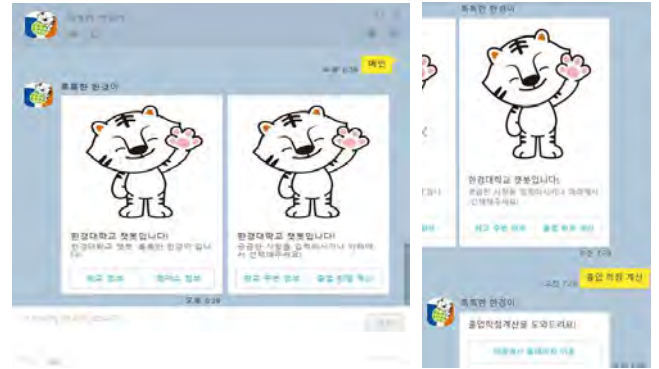
기능	설명
학교정보	학사일정, 학과, 장학금, 주요서비스의 정보를 제공
캠퍼스정보	캠퍼스 지도, 건물 내부의 정보를 제공
졸업학점계산	졸업학점과 수강해야할 잔여 교과목을 제공
학교주변정보	학교 주변 시설의 지도, 이벤트 정보를 제공
학점계산 홈페이지	졸업학점을 계산, 수강해야할 과목과 수강한 교과목을 조회할 수 있는 웹 페이지
데이터관리	학교정보, 캠퍼스정보, 학교주변정보의 데이터, 학점 계산에 필요한 교과목 데이터가 저장 되어 있음

4. 챗봇 서비스 개발

설계된 챗봇 서비스는 카카오 I 오픈빌더를 통해

개발하였다. 사용한 개발언어는 HTML, JAVA, Python, PHP이고, PostgreSQL DBMS를 사용하였다.

(그림 3)은 개발된 화면의 예시이다. 사용자를 처음 만났을 때 발송하는 웰컴 블록과 졸업학점 계산을 문의하였을 때 학점계산 홈페이지로 연결 버튼이 제공되는 화면이다.



(그림 3) 개발된 챗봇 서비스 화면 예시

5. 결론

본 논문에서는 유연한 대화를 통해 학내 정보 및 학교주변 정보를 제공하고 개인별 졸업학점을 계산하여 제공하는 챗봇 서비스를 설계하고 개발하였다. 향후, 학내 학사 및 행정 시스템과의 연동을 한다면 실시간 및 개인화된 챗봇 서비스를 제공할 수 있으며, 머신러닝 기술을 고도화하여 더욱 유연한 대화를 통해 정확한 정보를 제공할 수 있을 것이다.

논문사사

이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.2018R1A2B6009620). 이 논문은 캡스톤디자인(참여자:박소희,이영선,김다성)작품에 기반하여 작성됨. 교신저자 김미희.

참고문헌

- [1] 킨조 신이치로, “챗봇이 만드는 비즈니스 미래지도, 챗봇 혁명.” e비즈니스, 2020년 3월.
- [2] 카카오 I 오픈빌더, <https://i.kakao.com/>.
- [3] 박종혁, 이상원, “킹고봇 : 학내 정보 제공 챗봇,” 한국정보과학회 한국소프트웨어종합학술대회 논문집, pp. 324-324, 2017년 12월.
- [4] 연세대학교 챗봇 톡수리, <https://glc.yonsei.ac.kr/chatbot/index.do>.
- [5] 중앙대학교 챗봇, <https://chat.cau.ac.kr/>.

제53회
2020 온라인 춘계학술발표대회

소프트웨어공학



언어 학습 음원 분석 방법 및 언어 학습 음원을 재생하는 전자 디바이스 연구

송규빈*, 오정현**, 황채원**, 유동완***

*강남대학교 컴퓨터공학과

**가톨릭대학교 컴퓨터정보공학부

***성공회대학교 글로벌 IT 학과

E-mail : thd0427__@naver.com

LANGUAGE LEARNING SOURCE ANALYSIS METHOD AND ELECTRONIC DEVICE FOR PLAYING LANGUAGE LEARNING SOURCE RESEARCH

Gyu-Bin Song*, Jeong-Hyeon Oh**, Chae-won Hwang**, ***Dong-Wan Yu

*Dept. of Computer Science, GangNam University

**Dept. of Computer Science Information Engineering, Catholic University of Korea

***Dept. of Glocal IT, SungKongHoe University

요 약

언어 학습 음원 분석 방법 및 언어 학습 음원을 재생하는 전자 디바이스 연구로, 음원을 문장 단위로 분할하여 스크립트화하는 것을 주요 목표로 한다. 분석과정은 크게 세단계로 나눌 수 있다. 무음 구간 분석, 음원 분할 및 STT 구간, 스크립트 재구성이다. 이런 분석 과정을 통해 나온 결과물의 정확도는 90%로서 본 연구의 목표를 달성한다.

1. 서론

1) 연구의 필요성

본 연구는 언어 학습에 도움을 주는 음원 분석 방법 및 음원 재생 전자 디바이스에 대한 것으로, 보다 구체적으로 토익 리스닝 파트에 대한 학습을 도와주는 언어 학습 음원 분석 방법 및 언어 학습 음원을 재생하는 전자 디바이스에 관한 것이다.

본 연구에서는 공인 영어 능력 평가 시험 중 하나인 토익(TOEIC)에서 리스닝 파트를 연구 자료로 활용하였다. 토익은 현재 가장 많은 수험생들이 시험 본 영어 능력 평가 시험이다. 듣기와 읽기 능력에 대한 평가로 듣기는 part1에서 part4 까지, 읽기는 part5에서 part7 까지 구성되어 있다. 토익은 취업을 위한 필수 관문으로 여겨지며 매년 많은 학생 및 취업준비생들이 응시하는 시험이다. 이러한 토익 시험의 점수 향상을 위해서 오답 노트 작성과 같은 오류 점검 과정이 필수적으로 요구된다.

한편, 현재의 토익 리스닝 학습 시 틀린 문제나 다시 듣고 싶은 문제를 찾을 때, 음원 상태바를 움직여 수동적으로 원하는 부분을 찾아야 되기 때문에 원하는 부분을 찾지 못하는 문제점이 있다. 또한, 학습의 효율성을 위해 파트별 혹은 문제별 분할된 음원은 추가로 비용을 지불해야 획득할 수 있

기 때문에 사용자에게 부담이 될 수 있다.

이러한 불편함에 대응하는 언어 학습 음원 분석 방법 및 기술에 대한 필요성 검증을 위해 20 대 토익 학습 경험자 100 명을 대상으로 설문 조사를 진행하였다. 설문 참여자 중 ‘토익 학습 시, 어떤 애플리케이션을 사용했는가’ 문항에 대한 응답으로 90%가 ‘기본 미디어 플레이어를 사용했다.’를 선택하였다. 이는 대부분의 응답자들이 별도의 애플리케이션 도움 없이 갖고 있는 음원만 이용해 공부해 왔음을 보여준다. 이 중 ‘리스닝 파트 학습 시, 어떤 기능이 필요하다고 생각했는가’ 문항에 대한 응답으로 60%가 ‘원하는 부분으로 찾아가는 기능’을 선택했고 18%가 ‘속도 조절 기능’, 또 다른 18%는 ‘구간 반복 기능’을 선택하였다. 이는 기본 미디어 플레이어를 사용했던 토익 학습자들에게 학습 중 불가피하게 겪게 되는 불편함을 해소하고 학습의 효율성을 증대하는 다양한 기능에 대한 수요가 있다는 것을 보여준다.

이에, 토익을 준비하는 사용자들이 토익 리스닝 공부를 보다 쉽고 편리하게 할 수 있도록 돕는 학습 어플리케이션 및 이를 실행하는 전자 디바이스의 개발이 필요하다. 또한, 파트별 또는 문제별 분할 음원 재생을 제공할 수 있는 기술이 필요하다.

2) 연구의 해결과제

본 연구가 해결하고자 하는 과제는 사용자가 원하는 문제를 빠르게 다시 들을 수 있고 웨도잉(따라 말하기)을 더 편하게 하는 학습 분석 엔진과 이를 적용한 어플리케이션 및 디바이스를 제공하는 것이다. 또한, 본 발명이 해결하고자 하는 과제는 기존의 초 단위 음원 분석이 아닌 문장 단위 재생을 제공하는 것이다. 또한, 본 연구가 해결하고자 하는 과제는 추가 비용없이 파트별 또는 문제별 음원 재생 기능을 제공하는 것이다.

2. 본론

1) 분석과정

본 논문의 서론에서 설명된 서비스에 대한 분석엔진을 구현한 방법과 그 과정의 내용은 다음과 같다. 분석 엔진은 음원을 문장단위로 분할하여 스크립트화 하는 것을 주요 목표로 한다. 분석 과정은 크게 세단계로 나눌 수 있다. 무음 구간 분석(과정 1), 음원 분할 및 STT(Speech To Text)¹ 구간(과정 2), 스크립트 재구성(과정 3) 이다. 해당 과정은 Linux(Ubuntu 18.04)에서 구현되었다. 무음 구간 분석은 ffmpeg 와 sox 를 사용하였다. 또한 STT 는 Mozilla 재단의 오픈소스 DeepSpeech[1]를 활용하였다. 분석에 활용된 음원은 해커스에서 무료로 배포하고 있는 토익 LC 음원을 사용하였으며, 정답셋은 본 연구에서 정의한 토익 스크립트 구조로 재구성하여 만들었다.

A.과정 1. 무음 구간 분석

먼저 음원에서 특정 소리의 크기와 구간을 지정하여 무음 구간을 분석하고자 하였다. 예를 들어, -80dB 이하의 소리가 0.3 초 이상 지속될 경우, 해당 구간을 무음 구간이라고 정의하였다. 본 연구에서는 소리의 크기가 분석 결과에 큰 영향을 끼치는 요인으로 예상하였다. 이에 따라 다양한 설정값으로 시도하였으며, 이후 결과에서 정리하도록 한다.

B.과정 2. 음원 분할 및 STT

과정 1에서 분석된 무음 구간을 통해 과정 2에서는 실제로 음원을 분할하고 STT 하여 스크립트 결과를 얻었다. 해당 과정은 멀티프로세스 방식으로 구현되었다. 각 프로세스는 CPU bound 작업을 수행하며, 기존 단일 프로세스로 구현할 때보다 훨씬 좋은 성능을 보였다. 토익 음원 내 a, b, c, d 와 같은 선택지는 1 초 이하의 재생 시간을 가지므로 STT 결과가 제대로 출력되지 않아, 음원 양 끝에 1 초 정도의 패딩구간을 붙여서 사용하였다.

C.과정 3. 스크립트 재구성

해당 과정에서는 과정 2 의 STT 결과를 본 연구에서 정의한 토익 스크립트 구조로 매핑하는 작업을 하였다.

<예시 1. 매핑 전후 비교>

매핑 전	매핑 후
part one	PART 1
number twenty two	Number 22
a	(A)

해당 과정은 분기문으로 구현되었다.

2) 결과

분석엔진 결과의 정확도에 가장 주요한 영향을 끼친 요인으로 과정 1 의 소리의 크기를 예상하였다. 해당 요인에 대한 설정값과 정확도를 정리하면 다음과 같다.

<표 1. 소리의 크기에 따른 정확도 비교>

소리의 크기	정확도
-80dB	94.56%
-70dB	81.98%
-90dB	94.56%

위의 정확도는 저자가 정의한 토익 스크립트 구조로 정답셋을 만들고, 분석엔진의 결과와 단순비교를 통해 계산하였다.

표 1 에 나타나는 결과로 보아 특정 이상의 임계값을 넘으면 정확도는 더 이상 변하지 않는다.

-70dB 에서는 문장이 제대로 분할되지 않아 정확도가 떨어지는 문제가 발생했다.

현재 STT 기술은 다양한 언어(미국식 영어, 영국식 영어, 호주식 영어 등등)이 섞여 있을 경우 결과가 완벽하지 않고, 사람 이름이나 회사 이름 등의 고유명사를 정확하게 분석할 수 없으므로 100 에 가까운 정확도를 내는데 한계가 있다.

본 연구에서 사용한 음원에서의 최적 크기는 -80dB 이지만 해당 값은 음원 품질에 따라 달라질 수 있다. 값은 음원의 최고/최저 소리 크기에 따라 조절될 수 있다.

¹ STT(Speech To Text) : 음성을 텍스트로 변환하는 기술.

이외에도 결과의 성능에 영향을 끼친 주요한 요인은 과정 2의 구현방식이다. 단일 프로세스 방식과 멀티 프로세스 방식으로 구현했을 때의 차이를 다음 표에서 보여준다.

참고문헌

[1] <https://github.com/mozilla/DeepSpeech>

<표 2. 구현 방식에 따른 성능 비교>

구현방식	수행 시간
단일 프로세스	41 분
멀티 프로세스	5 분

해당 비교에 사용된 음원은 45 분의 완전한 토익 LC 음원이다.

멀티 프로세스로 구현한 엔진의 수행시간은 서버 환경에 따라 충분히 달라질 수 있다. 그러나 표 2 결과에 미루어 보아 단일 프로세스보다 멀티 프로세스로 구현하였을 때에 확연한 성능의 차이가 있다.

3. 결론

본 논문에서는 언어 학습, 구체적으로는 토익 리스닝 파트에 대한 학습을 도와주는 방법을 파악하였다. 리스닝 공부에는 반복 듣기와 따라 말하기가 중요하다. 일반 음원 플레이어에서는 듣고 싶은 부분을 음원 상태바를 움직여 수동으로 찾아야 했기에 원하는 부분을 한 번에 찾기 힘들다. 그렇기 때문에 듣고 싶은 부분을 한 번에 찾아서 들을 수 있는 방법에 관해 연구한 것이다.

연구 결과는 무음 구간 분석과 STT 기술을 활용하여 분석엔진을 통한 애플리케이션을 제안한 것이다. 자세한 결과는 다음과 같다.

무음 구간을 정의하여 음원을 분할하고 STT 하여 스크립트 결과를 얻었다. 멀티 프로세스 방식으로 구현하였다. 각 프로세스는 CPU bound 작업을 수행하였다. 정의한 무음 구간을 기준으로 음원을 한 문장 구간 단위로 분할하고 STT 요청을 보낸다. 그 후 스크립트를 추출하여 애플리케이션에 보여준다.

지금으로서는 토익 리스닝에 중점을 두었지만 차후 다른 언어시험에 대해 데이터를 쌓고 연구를 진행한다면 다양한 언어 듣기시험에 대한 더 좋은 결과를 얻을 수 있다.

블록체인을 기반으로 한 새로운 기부시스템 연구

강건욱*, 유혜진**

*경북대학교 경제통상학과

**경북대학교 경영학과

kkwteen@knu.ac.kr, wls00513@knu.ac.kr

A Study on the New Donation System Based on the Block Chain

Kun-Wook Kang*, Hye-Jin You**,

*the Department of Economics, Kyung-Book University

**the Department of Business Administration, Kyung-Book University

요 약

본 연구보고서는 기부사용내역 불투명성 등으로 인해 감소 추세에 있는 기부금의 감소문제를 분석하고 이를 해결하기 위한 방안을 모색함. 연구의 목적은 Block Chain을 활용하여 기존의 기부시스템 개선 및 새로운 기부시스템 도입에 있음.

기부문화 활성화를 위해서는 기부금 사용에 대한 신뢰성 확보가 필수적. 따라서 기부금 사용내역을 투명하게 관리하는 시스템이 필요함. 이를 위해 블록체인을 기반으로 한 새로운 기부시스템(New Donation System) 연구를 진행하였음. 새로운 기부시스템이 구축되기 위해서는 기부자, 기부단체, 정부가 서로 연계하여 블록체인을 기반으로 한 기부코인을 도입하고 이를 활용하는 금융 메커니즘의 적용이 필요함. 기부코인을 활용한 새로운 기부시스템이 도입된다면 우리나라의 기부시스템은 기존보다 진일보할 것이며 기부문화도 재활성화될 것으로 기대함.

1. 서론

[1] 통계청이 전국 3만 6000여명을 대상으로 표본조사를 실시한 결과 2013년도부터 만 13세 이상 인구 중 현금(후원금)이나 물품을 기부를 한 사람들의 비율이 감소하고 있다.



(그림 1) 기부율 도표

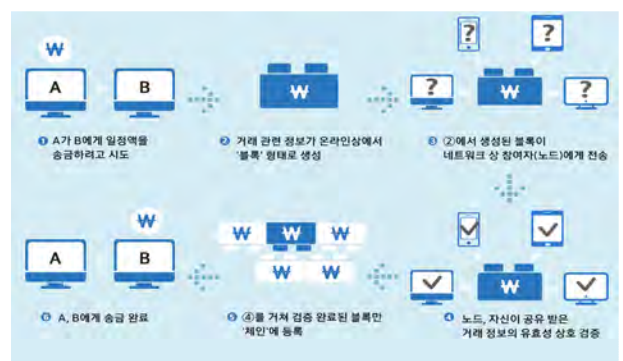
이처럼 기부가 매년 감소한 이유는 일부 기부기관 투명성 문제 등 때문인 것으로 분석됐다. 기부 문화의 회복을 위해서는 투명한 기부금 관리 및 기부자들이 이를 확인할 수 있는 시스템 도입이 필요하다.

규제 당국이 암호 화폐를 문제시하는 것은 암호화폐가 투기로 변질되는 것에 대한 거부감일 것이다. 따라서 매수한 사람이 전혀 이익이 없는 암호화폐

로 투기성 문제를 해결할 수 있다. 이와 더불어 블록체인의 스마트 컨트랙트 속성을 이용하여 기부에 파생상품 메커니즘을 연결한다면 기부의 투명성은 제고시킨 새로운 기부시스템으로서 기부의 패러다임을 바꿀 것이다.

2. 블록체인 기술과 스마트 컨트랙트

블록체인은 거래가 발생할 때마다 거래 내역을 서비스 참여자 모두에게 전송하고 전체 이용자가 보관하는 분산장부 형식을 가지며 가상화폐인 코인으로 거래할 때 발생할 수 있는 보안공격에 효과적인 대응이 가능한 기술이다.



(그림 2) [2] 블록체인 구조도

거래 내역은 블록 형태로 저장되며 블록은 데이터를 저장하는 단위로, 바디(body)와 헤더(header)로 구분된다. [3] 바디에는 거래 내용이, 헤더에는 머클해시(Merkle hash)와 넌스(Nounce) 등의 암호코드가 담겨 있다. 블록은 약 10분을 주기로 생성되며, 거래 기록을 끌어 모아 블록을 만들어 신뢰성을 검증하면서 이전 블록에 연결하여 블록체인 형태가 된다.

또한, 블록체인은 중앙 집중형 서버에 거래 기록을 보관, 관리하지 않고 거래에 참여하는 개개인의 서버들이 모여 네트워크를 유지 및 관리한다. 이 개개인의 서버, 즉 참여자를 노드라고 한다. 중앙 관리자가 없기 때문에 블록을 배포하는 노드의 역할이 중요하며, 참여하는 노드들 가운데 절반 이상의 동의가 있어야 새 블록이 생성된다. 노드들은 블록체인을 컴퓨터에 저장해 놓고 있는데, 일부 노드가 해킹을 당해 기존 내용이 틀어져도 다수의 노드에게 데이터가 남아 있어 계속적으로 데이터를 보존할 수 있다.

블록체인 내의 블록이 생성될 때마다 기존의 블록에 이어 연결되고, 새로 추가되는 블록에는 앞 블록의 내용이 포함되므로 이전에 연결된 블록의 경우 연결이후의 모든 블록을 수정해야 한다. 또한, 이후에 연결된 블록체인은 분산장부의 형식을 가지기 때문에 트랜잭션을 완벽하게 변경하기 위해 모든 서비스 사용자의 블록을 수정해야 한다.

따라서 블록체인을 수정하는 것은 사실상 불가능하기 때문에 결과적으로 블록체인은 거래 내역에 대한 무결성을 유지할 수 있다. 이와 같은 특성에 의해 블록체인은 보안성이 높은 기술로 인정받고 있다. 블록체인은 앞에서 설명한 암호화폐의 거래에 대한 검증을 기본으로 하며, 스마트 컨트랙트와 같은 기능적 요소를 가지고 있다. 스마트 컨트랙트(Smart Contract)는 블록체인에 기록하고 조건이 충족됐을 경우 자동으로 계약이 실행되게 하는 프로그램이다. 블록체인에 거래 내역 뿐 아니라 변수와 함수를 저장할 수 있도록 해 블록체인을 응용할 수 있는 다양한 가능성을 가지고 있다.

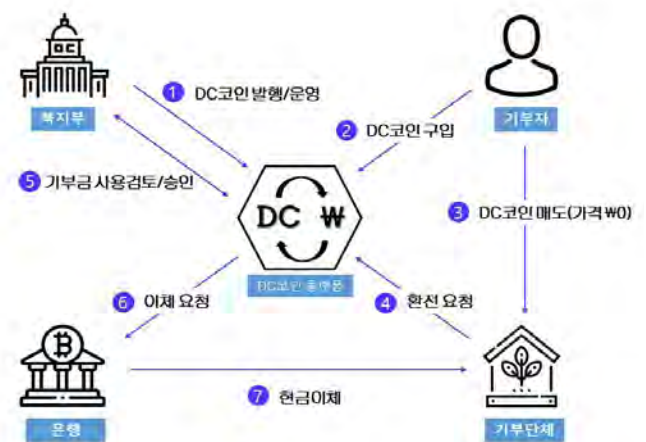
3. 새로운 기부시스템 구축에 응용

블록체인의 수정 불가능성과 내역확인가능성을 활용하기 위해 기부자들이 기부를 하고 기부금의 활용내역에 대해 모니터링은 가능하되 수정은 불가능

하도록 권한을 제한하는 블록체인을 적용한 기부시스템을 고안하였다. 이 시스템을 활용한다면 기부금의 사용시간, 금액, 내역 등과 같은 데이터를 기부자들이 원하는 시점에 확인할 수 있을 것이다.

예를 들어 정부가 기부관련 코인을 DC(Donation Coin)를 발행한다고 하자. DC를 누구나 매매를 할 수 있게 한다면 DC 하나의 가치는 계속해서 변동할 것이다. 많은 수의 DC를 구입하는 개인 혹은 단체가 있다면 DC의 가격은 수백만원 이상이 될 수 있다. 여기까지 보면 일반 코인 시장이나 다름없기에 기부코인이 투기처럼 될 것이라는 우려가 생길 수 있다.

따라서 기부시스템 고도화 및 투명성 확보를 위해 코인을 활용하기 위해서는 하나의 장치가 필요하다. 바로 매도가액을 0으로 설정하는 것이다. 기부 코인의 매수와 매도는 자유롭게 가능하지만 매수가액은 제한이 없되, 매도가액은 언제나 0원으로 고정되도록 설정한다면 이는 가치와 가격을 단절시키는 역할을 할 것이다. 가치와 가격의 단절은 DC의 투기화를 방지하고 DC 구입에 기부의 의미를 부여하게 된다.



(그림 3) 기부코인(DC) 구상도

위의 기부코인 구상도에 따라 운영되는 기부 메커니즘(Mechanism)은 다음과 같다. 기부를 원하는 기부자는 시장에서 기부를 희망하는 액수만큼의 DC를 구입한다. 해당 DC를 구입한 기부자는 원하는 자선단체 혹은 복지센터에 DC를 매도한다. DC의 매도가액은 0원이기에 자선단체 혹은 복지단체는 기부를 받는 것과 같은 의미가 된다. 시장에서 DC를 구입한 자선단체 혹은 복지단체는 DC를 통해 물품을 구입하거나 기획한 활동을 위해 필요한 자

금을 집행할 때 정부가 구축한 DC 환전시스템을 이용한다.

다음과 같은 복잡한 기부과정을 구축하는 이유는 기부 프로세스의 투명성을 위해 시장원리(Market principle)를 도입하기 위해서다. 시장원리가 적용된 DC코인은 그 운영에 있어서 시장균형이 유지될 것이며, 그 흐름이 모두 블록체인에 기록되기 때문에 기부금 전달 및 사용 과정을 투명하게 관리할 수 있다.

또한, 정부가 DC코인을 관리하는 플랫폼을 만들어 정부 DC환전시스템을 구축한다면 환전하게 되는 자선단체 혹은 복지단체는 해당 물품구입과 기획활동을 위한 기부금 사용시기와 규모, 내용을 공개하게 되고 이는 기부금 사용의 투명성을 확보할 수 있게 한다.

불투명한 기부금 운용은 불신을 키운다. 기부에 대한 거부감까지 불러일으킨다. 기부자의 알 권리를 강화해야 한다. 기부자가 기부 관련 정보를 들여다볼 수 있는 시스템을 구축하기 위해서는 필요한 절차이다. 현재 자선단체와 복지단체의 기부금을 운용 내용은 정보 보호문제로 확인하기 어렵다. 정보 접근성에 문제가 있다 보니 기부자들의 불신이 높아질 수 있다. 하지만 모든 기부금의 사용이 금융 거래처럼, 시장이라는 형태로 발생하면 정보가 집중되고 거래 내역이 오픈된다. 또한 자선단체와 복지단체들의 DC 환전내역을 확인하여 정부는 이들이 필요로 하는 부분에 더 많은 지원을 하거나 새로운 정책을 기획하는 등의 새로운 가치창출도 가능하다. 이 모든 것들이 기부시스템에 블록체인을 적용하여 금융 거래화하면 나타나는 이점이다.

4. 결론

최근 정부에서 블록체인 육성 관련 투자를 시작하고 있다. [4] 과기부에서는 2020년 블록체인과 관련하여 블록체인 육성 사업에 343억 원을 투입해 블록체인과 관련된 국가 경쟁력을 대폭 끌어올릴 예정이라고 선언했다. 국가적으로 블록체인 서비스와 사업을 키우려고 하는 시점에서 블록체인 기술을 활용하여 국가의 기부시스템을 개선하려는 시도는 필요하며 중점적으로 고려되어야 한다.

시스템 개선을 하고 실행함에 있어서 여러 가지 문제점들이 산재한 것은 사실이다. 기부시스템 고도화에 걸맞은 인프라 구축, 기부 코인 가치에 대한

밸런스 문제, 결식아동들의 기부코인 활용방안 및 채널확보 등의 시작을 위해서 이와 같은 문제들을 극복해 나가야 한다.

그럼에도 불구하고 블록체인을 통해 기부시스템을 개선한다면 블록체인 업계는 인식 전환으로 새로운 활로를 열수 있을 것이며, 기부 단체는 지속적인 팽배한 불신으로 인해 소외된 이웃을 도울 기부금 감소문제를 해결할 수 있을 것이다. 뿐만 아니라 이러한 시스템을 운영하는 기업과 기관들은 블록체인을 활용하는 데이터와 기술적인 측면에 노하우를 쌓을 수 있을 것이다.

블록체인과 기부시스템이라는 새로운 조합을 토대로 기존 기부 시스템이 가지는 한계점이 극복되고 이것이 국가발전에 이바지 할 수 있기를 기대한다.

**본 논문은 과학기술정보통신부
정보통신창의인재양성사업의 지원을 통해
수행한 ICT멘토링 프로젝트 결과물입니다.**

참고문헌

- [1] 엄승현, 기부 문화 시들 ‘차가워진 온정’, 전 북일보, 2020
- [2] ‘IEEE 스펙트럼’, 7월호, 2015
- [3] 남충현, ‘블록체인의 다변화: 채굴 없는 블록체인의 확산’, 정보통신정책연구원, 2018
- [4] 이영호, 과기정통부, 올해 블록체인 육성에 343억원 투입한다, 전자신문, 2020

자동화된 트위터 데이터 수집 시스템 설계 및 구현 : 환경 데이터를 중심으로

김도형*, 구자환**, 김응모***

*성균관대학교 소프트웨어대학

** 성균관대학교 사회과학대학

*** 성균관대학교 사회과학대학 소비자가족학과 / 소프트웨어대학
shape1248@skku.edu, jhkoo@skku.edu, ukim@skku.edu

Design and Implementation of Automated Twitter Data Collecting System : Focus on Environmental Data

Do-Hyung Kim* Jahwan Koo**, Ung-Mo Kim***

*College of Software, Sungkyunkwan University

** College of Social Sciences, Sungkyunkwan University

*** Dept. of Consumer and Family Sciences, College of Social Sciences / College of Software,
Sungkyunkwan University

요 약

소셜 네트워크 서비스의 사용자가 늘어나면서, 소셜 네트워크 서비스상에서 발생하는 빅데이터를 활용한 서비스가 늘어나고 있다. 소셜 네트워크 서비스 데이터는 실시간으로 생성되며, 따라서 데이터 수집 시스템 역시 자동화하여 준 실시간으로 데이터를 수집할 필요가 있다. 본 논문에서는 대표적인 소셜 네트워크 서비스인 트위터의 데이터를 지속적으로 수집하기 위한 자동 수집 시스템을 제안한다. 수집 시스템은 Twitter API 를 활용하는 Python 라이브러리를 통해 내용 및 메타데이터를 수집하며, 수집된 데이터를 재 검증한 뒤 저장한다. 또한 구현된 시스템에 환경 데이터를 주제로 하는 쿼리를 입력하여 실제 트위터 데이터를 수집하며 구현된 시스템을 검증해보았다.

1. 서론

최근 트위터, 페이스북과 같은 SNS(Social Network Service) 사용자가 늘어나면서, SNS 에서 발생하는 대량의 데이터를 정치, 경제, 문화 등 다양한 분야에 활용하려는 노력이 계속되고 있다. 이러한 SNS 에서 생성되는 데이터는 빅데이터의 정의에 정확히 부합한다. 즉, 정형화되지 않고, 대용량이며, 실시간으로 생성된다[1]. 따라서 이러한 SNS 빅데이터를 특성에 맞게 활용하기 위해서는 안정적이고 지속적으로 데이터를 수집할 수 있는 시스템이 요구된다.

많은 연구자들이 단기적인 데이터 분석을 위해 트위터 데이터 수집 시스템을 설계, 구현해왔다. 트위터는 트위터 데이터에 접근하기 위한 API 를 공개하고 있으며, 웹페이지를 통한 검색도 가능하다. 또한 트위터 데이터를 수집하는 다양한 Third party API 및 라이브러리도 만들어져 있다.

우리 연구에서는 정해진 쿼리에 따라 트위터 데이터를 수집하며, 불필요한 데이터와 중복 데이터를 제거한 후 날짜 별로 나누어 저장하는 과정을 지속적으

로 수행하는 시스템을 제안한다.

이를 통해 준 실시간으로, 지속적으로 트위터 데이터를 수집할 때 발생할 수 있는 데이터 중복 및 각종 예외 상황에 대한 관리를 사용자의 조작 없이도 시스템 자체적으로 지원할 수 있다.

본 논문의 구조는 다음과 같다. 2 장에서는 트위터 데이터를 수집 시스템을 설계 및 구현하였던 다양한 선행 연구를 소개하고, 트위터 데이터를 수집하는 다양한 방법을 서술한다. 3 장에서는 본 연구에서 제안하는 자동화된 트위터 데이터 수집 시스템의 요구조건과 구조를 제안한다. 이어 4 장에서 환경을 주제로 실제 트위터 데이터를 수집하여 결과를 확인한 후, 5 장에서 결론과 향후 계획에 대해 밝힌다.

2. 관련 연구

2.1. SNS 데이터 수집 선행연구

Byun, Kim, et al(2012)은 Twitter API 와 Java 를 이용하여 자동화된 트위터 데이터 수집 시스템을 제안하였다. 제안된 시스템은 트위터 계정간 팔로우 관계를

통해 데이터를 수집한 후, 수집된 데이터 내에서 키워드 검색을 통해 원하는 데이터를 데이터베이스에 저장한다.[2]

최민석(2015)은 Twitter API 를 이용하여 유저가 입력한 관심 키워드에 대한 트위터 데이터를 수집한 후, 분석 및 시각화하는 시스템을 제안하였다. 제안된 시스템은 트윗 데이터를 하루 분량만 MySQL DB 에 저장하며, 그 외에는 분석 완료된 데이터만 저장한다. 또한 관심 키워드에 대한 급격한 트윗 증가를 감지하여 유저가 이를 파악할 수 있도록 하였다.[3]

하승도 등(2016)은 트위터로부터 대화형 말뭉치 데이터를 수집하기 위하여 웹 크롤링 방식을 제안하였으며, 기존의 트위터 API 기반의 데이터 수집기와 비교하여 같은 시간동안 더 많고 완전한 말뭉치 데이터를 얻을 수 있었다.[4]

2.2. 트위터 데이터의 수집 방법

트위터는 Tweet 데이터에 접근하기 위한 API[5]를 공개하고있다. 트위터 계정을 통해 API key 를 지급받아 사용할 수 있으며, 무료 라이선스의 경우 최근 7 일 이내의 데이터에 대한 검색이 가능하다.

트위터 웹 페이지의 고급 검색 기능을 활용하여 웹 크롤링 방법으로 트위터 데이터를 수집할 수도 있다. https://twitter.com/search?q=<keyword>&src=typed_query&f=live 주소의 <keyword>에 검색 쿼리를 입력하여 URL 을 생성할 수 있으며, 한 번에 모든 정보를 표시하지 않기 때문에 같은 웹 페이지에 대해 스크롤 정보를 지속적으로 갱신하며 요청해야 완전한 정보를 얻을 수 있다.

Python3 라이브러리인 GetOldTweets3[6]은 트위터의 웹 API 를 사용하여 트위터 데이터를 수집한다. 트위터가 제공하는 프로그래밍 언어 수준의 API 가 가진 단점인 날짜 제한이 없고, 웹 크롤링 방식과 마찬가지로 쿼리를 작성하여 데이터를 수집할 수 있다. 따라서 본 연구에서는 해당 라이브러리를 통해 트위터의 데이터를 수집한다.

3. 트위터 크롤러 시스템 분석 및 구성

3.1. 요구조건

본 연구에서 설계한 Tweet 데이터 수집 시스템은 다음과 같은 요구조건을 충족시켜야 한다.

시스템을 구축한 후에는 추가적인 유저의 조작 없이 자동적이고 지속적으로 최신 데이터를 수집하여 기존 데이터에 추가해야 한다.

수집할 Tweet 데이터는 여러 종류이며, 각각 사전에 작성된 검색식과 제외식이 존재한다. Tweet 의 내용이 검색식에 포함되면서 제외식에는 포함되지 않는 데이터를 수집, 저장해야 한다.

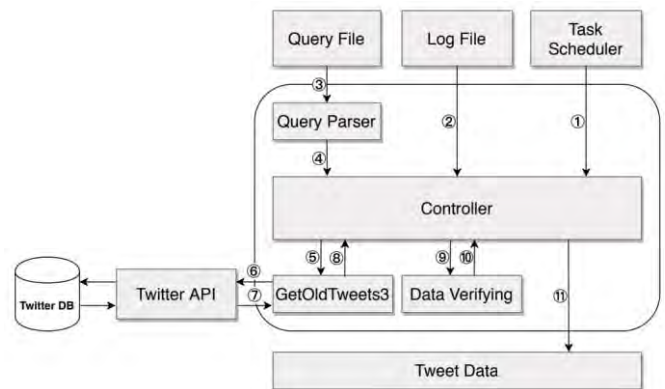
3.2. 시스템 아키텍처

GetOldTweets3 라이브러리는 Python 환경에서 사용 가능하다. GetOldTweets3.manager.TweetCriteria 함수를 사용하여 검색 쿼리 및 검색 기간 등을 설정한 후, GetOldTweets3.manager.TweetManager.getTweets 함수를 사용하면 Twitter API 를 활용하여 데이터를 수집한 후, 수집 결과를 되돌려준다.

Twitter API 는 검색 쿼리를 통해 데이터를 요청 시 쿼리의 검색어를 Tweet 의 내용뿐 아니라 작성자명까지 포함하여 검색하는 특징이 있다. Twitter API 를 사용하는 GetOldTweets3 라이브러리를 통해 수집한 데이터 역시 같은 특성을 가진다.

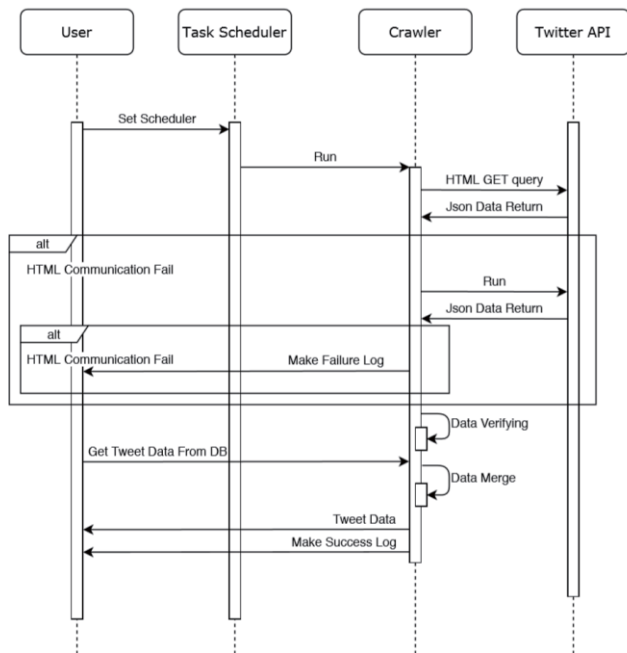
이렇게 수집된 데이터는 본 시스템이 원하는 데이터가 아니므로, 추가적인 데이터 검증 작업을 통해 내용에 검색어가 포함되지 않는 데이터를 제거하는 작업이 필요하다.

제외어 역시 Twitter API 에 포함하여 요청할 경우, 수집되어야 할 데이터가 제외식이 포함된 작성자명으로 인해 수집되지 않을 수 있다. 따라서 검색어만으로 이루어진 쿼리를 작성하여 데이터를 수집하고, 이후 제외어가 포함된 데이터를 제거하는 작업이 필요하다.



(그림 1) Tweet 수집 시스템의 activity diagram

1. Task Scheduler 가 크롤러 프로그램을 실행시킨다.
2. 이전에 작성된 로그 파일을 통해 검색 시작시점을 파악한다.
- 3,4. 쿼리 파일을 해석하여 검색어와 제외어 키워드 뭉치를 만든다.
5. GetOldTweets3 라이브러리에 검색어로 이루어진 쿼리와 검색 기간을 지정하여 데이터를 수집 요청한다.
- 6,7. GetOldTweets3 라이브러리는 Twitter API 에 해당 쿼리를 전송하여 데이터를 수집한다.
8. 수집된 데이터를 Controller 에 되돌려준다.
- 9,10. 데이터 검증 작업을 통해 내용에 검색어가 포함되지 않거나, 제외어가 포함된 데이터를 제거한다.
11. 최종적으로 얻은 데이터를 저장한다.



(그림 2) Tweet 수집 시스템의 sequence diagram

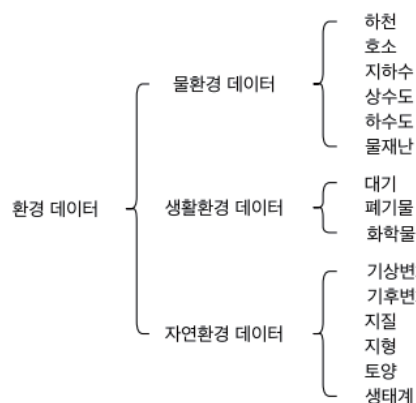
(그림 2)에 명시된 Crawler의 내부 구조는 (그림 1)의 activity diagram에서 표현된 내용과 같다.

유저가 OS의 Task Scheduler를 설정하면, Crawler는 오직 Task Scheduler에 의해서만 실행되며, 완성된 데이터는 User에게 파일로써 제공된다. 이 과정에서 Twitter API가 응답하지 않을 경우에 대해 최대 두 번까지 수집을 시도한다.

4. 구현 방법

우리는 본 시스템을 활용하여 Twitter에서 환경 관련 언급이 포함된 Tweet을 수집하였다.

수집할 환경 데이터는 (그림 3)과 같이 3 종류의 대분류로 나눌 수 있으며, 3종의 데이터는 다시 15종의 소분류로 나뉜다.



(그림 3) 환경데이터 분류

각 소분류 데이터 수집을 위한 검색어 및 제외어는 아래 <표 1>과 같다.

수집한 데이터는 대한민국 표준시에 따라 Tweet이 작성된 날짜 별로 나뉘어 csv 파일 형태로 저장된다.

4.1. 로그 파일

시스템 재부팅 및 프로그램 실행 실패 등의 상황에서 이 전 수집 시점에 이어서 수집할 수 있도록, 데이터 수집 성공 시 로그 파일에 데이터 수집 시점과 수집 데이터 종류, 수집 기간 정보를 남긴다. 크롤링 시스템은 프로그램 실행 시점마다 로그 파일을 통해 이전 수집 시점으로부터 이어서 데이터를 수집한다.

collecting tweeter data of 05-Jan-2020...						
keyword	Response data	09:00~23:59	00:00~09:00	invalid data	running time	
지하수	26 tweets	23	3	0	0:00:03	
하천	1286 tweets	979	304	3	0:02:03	
하천	3 tweets	1	2	0	0:02:05	
하천	7 tweets	6	1	0	0:02:07	
호소	843 tweets	565	271	7	0:03:23	
상수도	40 tweets	29	11	0	0:03:27	
하수도	21 tweets	16	5	0	0:03:30	
물재난	297 tweets	231	65	1	0:03:58	
대기	852 tweets	645	204	3	0:05:18	
폐기물	6 tweets	4	2	0	0:05:20	
폐기물	78 tweets	47	31	0	0:05:27	
화학물질	22 tweets	15	7	0	0:05:31	
기상변화	236 tweets	156	80	0	0:05:53	
기후변화	573 tweets	395	177	1	0:06:46	
지질	960 tweets	677	280	3	0:08:15	
지형	121 tweets	88	33	0	0:08:27	
토양	19 tweets	15	4	0	0:08:29	
생태계	17 tweets	11	4	2	0:08:32	
collecting tweeter data of 06-Jan-2020...						
keyword	Response data	09:00~23:59	00:00~09:00	invalid data	running time	
지하수	27 tweets	16	11	0	0:00:03	
하천	1161 tweets	810	350	1	0:01:50	
하천	5 tweets	3	2	0	0:01:52	
하천	9 tweets	7	2	0	0:01:54	
호소	849 tweets	579	263	7	0:03:11	

(그림 4) 데이터 수집중인 시스템의 UI

date	time	permalink/text
2020-01-06	8:44:44	https://twi[실시간 2위 소한] "소한맛아?" 겨울에 눈대신 비...때아닌 100mm 이상
2020-01-06	8:38:03	https://twi[마음속으로는 이미 홍수야] [마음속으로는 이미 홍수야]
2020-01-06	8:34:05	https://twi[그래도 폭우는아니니 다행이여^^]
2020-01-06	8:25:50	https://twi[충청: 인천대 종장 "4대강사업은 이 정부의 대표적인 지역정책. 홍수문
2020-01-06	8:18:58	https://twi[리안한테 오가게 될 것 같네요(버서살: 눈물바다 홍수)
2020-01-06	8:18:24	https://twi[베트남의 수도 Ha N?][하 노이]는 물(河) 안쪽(內)이라는 이름답게 홍
2020-01-06	8:12:18	https://twi[중드 특: A작품 끝났다고 먹칠끝나는거 아님. 그 작품 최대캐의 배우
2020-01-06	8:08:34	https://twi[청계천 정비해 했음에도 홍수로 인해서 청계천이 범람했다.범람을 막
2020-01-06	8:00:48	https://twi[떡밥 늘 홍수지만 연말연초엔 미친듯이 터지네... 컴백전까지는...다...
2020-01-06	7:52:09	https://twi[..... " 폭우, (적막을 깨더니 보이는 것은 자신의 두 손과 다리에 칼을
2020-01-06	7:27:24	https://twi[폭우]
2020-01-06	7:18:22	https://twi[SCP-3637 무효화 이 사랑은 많은 물이 꺼지지 못하겠고 홍수라도
2020-01-06	7:17:35	https://twi[폭우가 눈 앞을 가리는 어느 밤 그 어떤 불빛조차 없던 그날 라디오도
2020-01-06	7:15:49	https://twi[폭우를 대비해서 지하에 건설된 대규모 집수조 등을 둘러보는 도시 속
2020-01-06	7:14:47	https://twi[대덕구 여름철 집중호우대비 물막이벽 보급
2020-01-06	7:01:23	https://twi[또 비가 많이 내리는 홍수철엔 나무가 최대한 물을 흡수했다가 나무
2020-01-06	6:08:23	https://twi[한양성내 홍수가 찾아서 개천을 정비하기 위해서 개천도감을 만들었

(그림 5) 수집된 데이터(물재난)

5. 결론

본 논문에서는 가장 대표적인 소셜 네트워크 서비스인 트위터의 데이터를 자동화되어 지속적으로 수집하기 위한 시스템을 설계하였다. 그 후, 환경 데이터를 수집하는 Case study를 통해 트위터 데이터가 정상적으로 수집됨을 확인하였다.

추후에 데이터 수집 속도를 향상시키기 위한 병렬 수집 시스템과 같은 방법에 대한 연구와, 수집된 데이터를 Hadoop과 같은 대용량 데이터 분석 시스템에 저장하여 데이터 관리, 분석, 시각화에 쉽게 활용할 수 있도록 추가 연구가 수행된다면 시스템의 완성도가 높아질 것으로 기대된다.

<표 1> 15 중 환경 데이터 수집을 위한 검색어와 제외어

키워드	검색어	제외어
하천	하천수질 OR 수질오염 OR 유역오염 OR 물오염 OR 하천유량 OR 하천정비 OR 하천 OR 개천 OR 도랑 OR 개울 OR 한강 OR 영산강 OR 낙동강 OR 금강 OR4 대강 OR 이포보 OR 여주보 OR 강천보 OR 함안창녕보 OR 창녕합천보 OR 달성보 OR 강정고령보 OR 철곡보 OR 충주댐 OR 횡성댐 OR 안동댐 OR 임하댐 OR 합천댐 OR 남강댐 OR 밀양댐 OR 군위댐 OR 부항댐 OR 대청댐 OR 용담댐 OR 섬진강댐 OR 주암댐 OR 부안댐 OR 보령댐 OR 장흥댐 OR 영주댐 OR 청평댐 OR 화천댐 OR 괴산댐 OR 춘천댐 OR 의암댐 OR 팔당댐 OR 도암댐 OR 보성강댐 OR 송촌보 OR 소양강댐 OR 하천환경 OR 하천관리 OR 구미보 OR 낙단보 OR 상주보 OR 백제보 OR 공주보 OR 세종보 OR 죽산보	매매 OR 투어 OR 여행 OR 관광 OR 드라이브 OR 맛집 OR 펜션 OR 전원주택 OR 업체 OR 가볼만한곳
호소	호수 OR 늪 OR 저수지 OR 소택 OR 습원 OR 담수호 OR 민물호수 OR 담호	매매 OR 투어 OR 여행 OR 관광 OR 드라이브 OR 맛집 OR 펜션 OR 전원주택 OR 업체 OR 가볼만한곳
상수도	상수도 OR 수돗물 OR 상수관 OR 상하수도	제품 OR 필터 OR 미국 OR 매매 OR 투어 OR 여행 OR 관광 OR 드라이브 OR 맛집 OR 펜션
하수도	하수도 OR 하수처리 OR 하수관 OR 상하수도	매매 OR 투어 OR 여행 OR 관광 OR 드라이브 OR 맛집 OR 펜션 OR 전원주택 OR 업체 OR 고객
지하수	지하수 OR 암반수	생수 OR 천연 OR 매매 OR 투어 OR 여행 OR 관광 OR 드라이브 OR 맛집 OR 펜션
물재난	홍수 OR 폭우 OR 집중호우 OR 하천범람	매매 OR 투어 OR 여행 OR 관광 OR 드라이브 OR 맛집 OR 펜션 OR 전원주택 OR 업체 OR 가볼만한곳
대기	대기환경 OR 미세먼지 OR 미먼 OR 황사 OR 대기오염 OR 대기 배출 OR 도로 제비산 먼지 OR 자동차 배출가스 OR 실내공기질 OR 공기오염 OR 매연 OR 스모그 OR 오존 OR 부유먼지 OR 초미세먼지 OR 황산화물 OR 질소산화물	매매 OR 투어 OR 여행 OR 관광 OR 드라이브 OR 맛집 OR 펜션 OR 전원주택 OR 업체 OR 가볼만한곳
폐기물	폐기물 (음식물 OR 분뇨 OR 사업장 OR 생활 OR 건설 OR 자동차 OR 지정 OR 전기 OR 전자 OR 매립 OR 소각 OR 재활용 OR 해역배출 OR 가연성 OR 불연성 OR 비가연성 OR 플라스틱 OR 생활 OR 처리) OR 재활용쓰레기 OR 음식물쓰레기	매매 OR 투어 OR 여행 OR 관광 OR 드라이브 OR 맛집 OR 펜션 OR 전원주택 OR 업체 OR 가볼만한곳
화학물질	화학물질 OR 환경호르몬 OR 화학사고 OR 유해화학물질 OR 잔류성유기오염물질 OR 화학제품성분 OR 유독물질 OR 유해물질	매매 OR 투어 OR 여행 OR 관광 OR 드라이브 OR 맛집 OR 펜션 OR 전원주택 OR 업체 OR 가볼만한곳
기상변화	일사량 OR 일조량 OR 강우량 OR 습도 OR 운량 OR 기압 OR 풍향 OR 풍속 OR 기상변화 OR 강수량	매매 OR 투어 OR 여행 OR 관광 OR 드라이브 OR 맛집 OR 펜션 OR 전원주택 OR 업체 OR 가볼만한곳
기후변화	한파 OR 폭염 OR 가뭄 OR 집중호우 OR 지구온도 OR 해수면 OR 온난화 OR 대기온도 OR 오존층 OR 엘니뇨 OR 라니냐 OR 폭우 OR 기온변화 OR 강수량변화 OR 기후변화 OR 폭설 OR 온실가스 OR 온실효과	매매 OR 투어 OR 여행 OR 관광 OR 드라이브 OR 맛집 OR 펜션 OR 전원주택 OR 업체 OR 가볼만한곳
지질	지질 OR 지층 OR 지질재해 OR 지질학 OR 광물자원 OR 해저지질 OR 해저광물 OR 석유자원 OR 산사태 OR 지열 OR 지질자원 OR 지질도 OR 지진 OR 국토지질 OR 석유해저 OR 지반	매매 OR 투어 OR 여행 OR 관광 OR 드라이브 OR 맛집 OR 펜션 OR 전원주택 OR 업체 OR 가볼만한곳
지형	급경사지 OR 지표면 OR 지형곡곡 OR 지형경사도 OR 지형표고 OR 지형 OR 생크롤 OR 지형도	매매 OR 투어 OR 여행 OR 관광 OR 드라이브 OR 맛집 OR 펜션 OR 전원주택 OR 업체 OR 가볼만한곳
토양	토양 OR 토양오염 OR 토양환경 OR 성숙토	매매 OR 투어 OR 여행 OR 관광 OR 드라이브 OR 맛집 OR 펜션 OR 전원주택 OR 업체 OR 가볼만한곳
생태계	생태환경 OR 생태관광 OR 자연복원 OR 생태서비스 OR 생태계파괴 OR 국립습지 OR 환경영향평가 OR 생물계	매매 OR 투어 OR 여행 OR 관광 OR 드라이브 OR 맛집 OR 펜션 OR 전원주택 OR 업체 OR 가볼만한곳

참고문헌

- [1] A. Bhardwaj, R. Singh, V. Deep and P. Sharma, BDT3V — A Technique for Big Data Testing considering 3V's, 2018 Second International Conference on Green Computing and Internet of Things (ICGCIoT), Bangalore, India, 2018, pp. 222-225.
- [2] Byun, C., Kim, Y., Lee, H., & Kim, K. K. Automated Twitter data collecting tool and case study with rule-based analysis. In Proceedings of the 14th International Conference on Information Integration and Web-based Applications & Services, Bali Indonesia, December 2012, pp. 196-204.
- [3] 최민석. 효율적인 트윗 분석 시스템 설계 및 구현 방법. Journal of Digital Convergence, 13(2), pp. 43-50, 2015
- [4] 하승도, 선동성, 이해준, 이상구. 대화 말뭉치 구축을 위한 웹 크롤러 기반 대화 수집기. 한국정보과학회 학술발표논문집, pp. 334-336, 2016
- [5] Twitter, Inc. "Overview — Twitter Developers", 2020, <https://developer.twitter.com/en/docs/tweets/search/overview>
- [6] PyPI, "GetOldTweets3 · PyPI". 2020, <https://pypi.org/project/GetOldTweets3/>

의료영상 기반 간 질환 정량분석 통합소프트웨어 개발과 간 질환 환자 데이터 임상 적용

김지언*, 김승진*, 노시형*, 이충섭*, 김태훈*, 정창원**

*원광대학교 의료융합연구센터

e-mail:{kakasky112, koch369369, nosij123, cslee99, tae_hoonkim, mediblue}@wku.ac.kr

Development of an Integrated Software for Medical Image-Based Quantification and Its Clinical Application in Liver Disease

Ji-Eon Kim*, Seung-Jin Kim*, Si-Hyeong No*, Chung Sub Lee*,
Tae-Hoon Kim*, Chang-Won Jeong**

*Medical Convergence Research Center, Wonkwang University

**Smart Health IT Center, Wonkwang University Hospital

요 약

현재 의료영상 진단검사는 간 질환의 진단을 위해 실제 임상에서 사용하고 있는 중요한 검사 방법이며 의료영상을 기반으로 한 정량분석 소프트웨어 개발 연구가 활발히 진행되고 있다. 특히, 의료영상을 기반으로 간 질환을 정량화 하는 방법 가운데 간 결절 점수와 간세포 이질성 점수를 이용하여 간 질환에 대한 정량적 평가를 진행한 결과 간 결절 점수와 간세포 이질성 점수에 따른 간 질환 중증도의 상관관계가 증명되었으나 많은 문제점이 제기되었다. 의료영상에는 서로 상반되는 의료영상조건들을 가지고 있기 때문에 의료영상조건에 따른 영상처리 기술들이 필요하였으며 간 결절 점수와 간세포 이질성 점수는 수식에 의한 계산법을 기반으로 산출하기 때문에 수식 결과에 대한 검증 과정이 필요하였다. 따라서, 본 연구는 기존의 문제점을 해결하기 위해 의료영상에 따른 의료영상처리 기술을 자동화 할 수 있도록 개발하였으며 간염, 간질환, 간 경변 등 간 질환 중증도에 따른 정량적인 분석을 수행할 뿐만 아니라 분석 결과에 대한 리포트 결과까지 제공함으로써 간 질환을 진단하기 위한 정량적인 진단 지표가 될 수 있는 소프트웨어 기반의 간 질환 진단 기술을 제안하고자 한다.

1. 서론*

최근 의료영상을 기반으로 한 정량분석 소프트웨어 개발 연구가 활발히 진행되고 있다[1,2]. 의료영상 기반 형태학적 분석의 예로는 간세포 이질성(parenchymal heterogeneity), 결절(nodule)에 의한 간표면 형태 변화, 염증(inflammatory) 및 괴사(necrotic) 변화 등의 정량화가 있다. 정량화된 간 결절(nodularity)과 간세포 이질성 점수가 간 질환의 중증도 판정에 있어서 유용하다고 보고되었다. 간표면 결절(liver surface nodularity) 점수는 간섬유화(fibrosis)와 간경변을 감별 진단하는데 높은 민감도와 특이도(>0.9)를 나타냈다[1]. 간세포 이질성 점수는 B형 간염환자의 간 섬유화 진행단계에 따라 높은 감별력을 나타냈다(AUC>0.875)[4]. 또한 간세포 이질성 점수는 간질환 선별지표인 FIB-4 지수와 높은 상관성을 나타냈다. 이러한 선행연구 결과들에 종합해 보면, 간세포 이질성과 간표면 결절성을 정량 분석할 수 있는 통합 소프트웨어 기반의 기술은 간 질환의 중증도 감별 진단에 있어서 유용

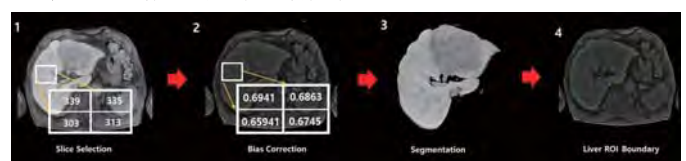
할 것으로 판단하였다.

따라서, 본 연구는 의료영상을 이용해서 정량분석을 위한 전처리 기능, 간세포 이질성 및 간 표면 결절성 정량 분석 알고리즘, 최종정량 분석결과 리포트를 제공하여 간 질환에 대한 중증도를 정량화 할 수 있는 통합 소프트웨어를 제안하고자 한다.

2. 전처리 알고리즘 및 간 질환 점수 산출

2.1 의료영상 전처리 알고리즘

본 논문에서는 의료영상 기반의 간 질환 정량 분석을 수행할 수 있도록 선행적으로 의료영상에 대한 균질성을 높이기 위해 Bias correction 알고리즘을 그림 1과 같이 자동화 할 수 있도록 개발하였다.



(그림 1) 의료영상 전처리 알고리즘 수행 과정

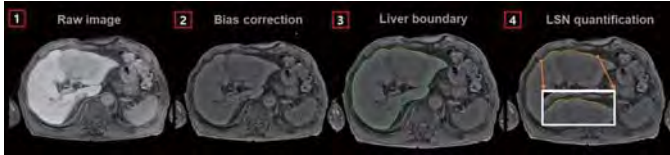
Bias correction 알고리즘이 자동화되어 적용되는 과정에서 간 표면 결절 점수를 산출하기 위해 필요한 간 표면

* This study was supported by the grants of the National Research Foundation of Korea (NRF) (2016M3A9A7918501) and the Korea Health Technology R&D Project through the Korea Health Industry Development Institute (KHIDI), funded by the Ministry of Health & Welfare (HI18C1216).

관심영역 (ROI) 정보들을 저장하며, 간세포 이질성 점수를 산출하기 위해 필요한 의료영상 픽셀 값을 정규화 하여 저장한다.

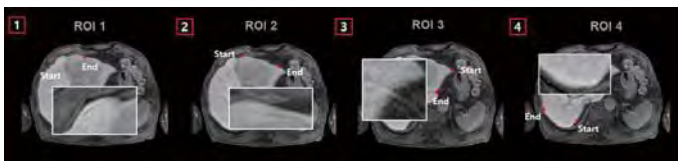
2.2 영상 전처리와 간 표면 결절 점수 산출

본 논문에서 제안하는 Bias correction 알고리즘이 의료영상에 적용될 경우 그림 2와 같이 간 표면 결절 점수를 산출하기 위해 필요한 간 표면 관심영역 정보들을 저장된 ROI 정보들을 기반으로 간 표면 결절 점수를 정량화한다.



(그림 2) 영상 전처리와 간표면 결절 점수 산출 과정

그림 3은 간표면 결절 점수 산출 예시이며 간표면 외곽선을 검출한 후 시작점(start)과 끝(end) 점을 입력하면 간표면 외곽선을 따라 피팅 커브(fitting curve)를 그려 결절성 점수를 산출한다. 개발된 통합소프트웨어는 다양한 간 세그먼트(segment) 위치에서 간표면 결절 점수를 정량화 할 수 있다.



(그림 3) 간표면 결절 점수 산출 예시

2.3 간세포 이질성 점수 산출

분석하고자 하는 영상을 전처리 알고리즘을 적용한 이후 간세포 이질성(heterogeneity) 점수를 정량화 할 수 있다. 간세포 이질성 점수는 픽셀별 변이계수(coefficient of variation, %)를 기준으로 한다. 간세포 이질성 분석을 위해서 먼저 정량화에 필요한 픽셀 값과 ROI정보를 저장한다. 간세포 이질성 점수는 의료영상에 저장된 픽셀 값을 기반으로 그림 4와 같이 간세포 이질성 점수를 정량화 할 수 있다.



(그림 4) 간 세포 이질성 점수 산출

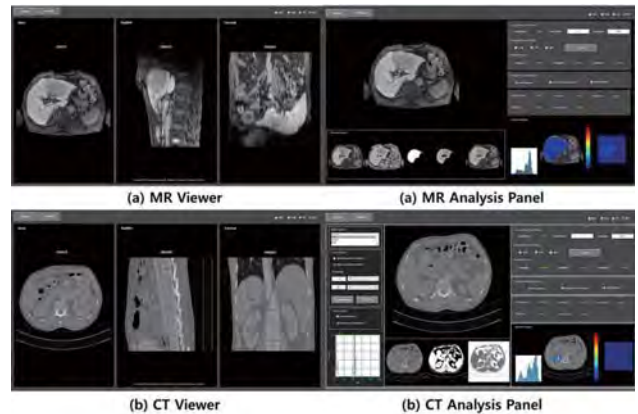
또한, 간세포 이질성 정량화를 위한 분석영역 (ROI) 형태는 사각형 (Rectangle), 원형 (Circle), 자유형 (Free-Hand), 간세분화 영역 (Liver Segmentation ROI)

등이 있으며 연구자의 분석 목적에 따라 다양하게 선택할 수 있다.

3. 결과

3.1 간 질환 분석 통합소프트웨어 GUI

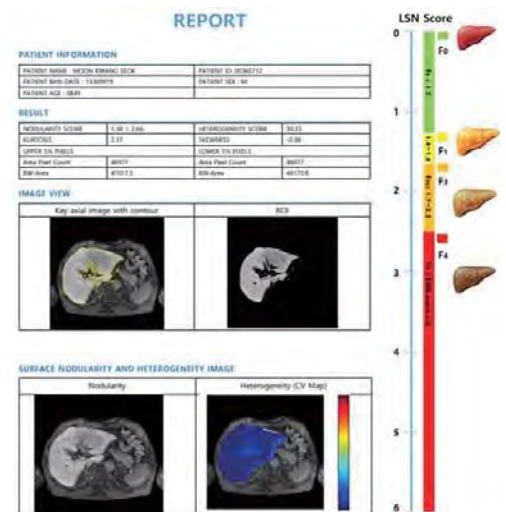
간표면 결절 점수와 간세포 이질성 점수를 정량화 할 수 있는 통합소프트웨어 GUI는 그림 5와 같이 구현하였다. 해부학적 의료영상 뷰어를 통해 간 질환에 대한 영상을 확인할 수 있으며 질환이 의심되는 절편 영상(slice image)에서 정량 분석을 수행할 수 있다. 정량분석을 위한 패널은 아래 우측에 보이는 화면상에서 보이는 것과 같이 MR영상, CT영상을 각각 분석할 수 있다.



(그림 5) 정량분석 통합소프트웨어 구현 결과

3.2 간 질환 분석 리포트

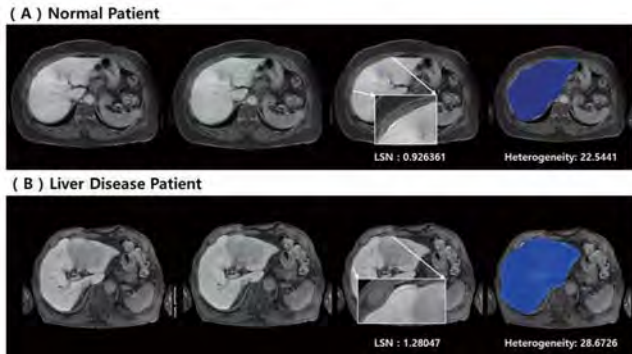
본 논문에서는 제안하는 통합소프트웨어를 통해 간 질환에 대해 정량화를 수행할 뿐만 아니라 간표면 결절 점수와 간세포 이질성 점수에 따른 정량화 분석 결과를 그림 6과 같이 간 질환 중증도에 대한 종합적인 결과를 문서화된 Report를 제공받을 수 있다. Report에 제공되는 결과는 환자 정보, 간표면 결절 점수, 간세포 이질성 점수이다. 또한, 간표면 결절 점수와 간 이질성 점수를 종합하여 간 질환이 진행된 섬유화 정도에 따라 F0-F4 단계로 어디에 속하는지 표현하여 명확하게 확인할 수 있다.



(그림 6) Liver Disease Quantitative Analysis Report

3.3 간 질환 분석 수행 결과

본 논문에서 제안한 소프트웨어를 통해 그림 7와 같이 간 질환 환자를 대상으로 정량화 분석을 수행하였다. 정상군 환자(n=10)의 경우 간표면 결절 점수와 간세포 이질성 점수는 0.99 ± 0.12 , $4.75 \pm 0.15\%$ 였으며, 간 질환 환자(n=18)의 경우 1.29 ± 0.42 , $6.54 \pm 0.24\%$ 였다. 따라서 개발한 통합소프트웨어를 통해 정상군 환자와 간질환 환자군에 따른 유의미한 차이를 확인할 수 있었다 ($p < 0.001$).



(그림 7) 정상군과 간 질환 환자군의 정량분석 결과

4. 결론

본 연구는 간 표면 결절성과 간세포 이질성을 정량 분석할 수 있는 통합소프트웨어를 개발하였다. 간 결절 점수와 간세포 이질성 점수를 정량화하기 위해 영상 균질성을 높일 뿐만 아니라 간 질환을 정량화하기 위해 필요한 간 결절 ROI, 의료영상 픽셀 정보들을 저장할 수 있는 자동화된 Bias Correction 알고리즘을 개발하여 의료영상에 적용하였다. Bias Correction 알고리즘을 통해 수집된 정보들을 기반으로 실제 정상군과 간 질환 환자군 영상데이터를 정량 분석한 결과, 간표면 결절과 간세포 이질성 점수들을 기반으로 간 질환 중증도를 평가할 수 있었으며 최종 분석 결과 리포트를 제공함으로써 간 질환을 감별진단 하는데 유용한 정량 지표로 활용할 수 있을 것으로 기대한다.

참고문헌

- [1]LO, Grace C., et al. Feasibility and reproducibility of liver surface nodularity quantification for the assessment of liver cirrhosis using CT and MRI. European journal of radiology open, 2017, 4: 95-100.
- [2]PICKHARDT, Perry J., et al. Accuracy of liver surface nodularity quantification on MDCT as a noninvasive biomarker for staging hepatic fibrosis. American Journal of Roentgenology, 2016, 207.6: 1194-1199.
- [3]Inchingolo, Riccardo, et al. "MR with Gd-EOB-DTPA in assessment of liver nodules in cirrhotic patients." World journal of hepatology 10.7 (2018): 462.
- [4] Lee GM, et al. Quantitative Measurement of Hepatic Fibrosis with Gadoteric Acid-Enhanced Magnetic Resonance Imaging in Patients with Chronic Hepatitis B Infection: A Comparative Study on Aspartate Aminotransferase to Platelet Ratio Index and Fibrosis-4

Index. Korean Journal of Radiology. 2017;18(3):444-451.

DEVS 기반 OHT 시뮬레이션 시스템 설계

이복주*, 강봉구**, 권용환***, 최영규*, 한경아****, 서경민*****

*한국기술교육대학교 컴퓨터공학과, **한국생산기술연구원,

*** (주)휴민텍, ****한국기술교육대학교 LINC+ 사업단,

*****한국기술교육대학교 융합학과

bokju618@koreatech.ac.kr, kbgmode@gmail.com, yhkwon@ihumin.co.kr,
ykchoi@koreatech.ac.kr, kyungahh@koreatech.ac.kr, kmseo@koreatech.ac.kr

DEVS Based OHT System Simulation Design

Bok-Ju Lee*, Bong-Gu Kang**, Young-Kyu Choi*, Yong-Hwan Kwon***,

Kyung-Ah Han****, Kyung-Min Seo*****

*Dept. of Computer Science, Korea University of Technology and Education,

Korea Institute of Industrial Technology, *HUMINTECH Co., Ltd.,

****LINC Foundation, Korea University of Technology and Education,

*****Dept. of Future Technology, Korea University of Technology and Education,

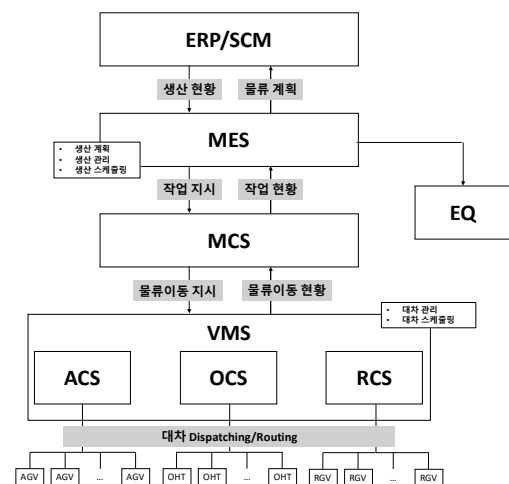
요약

반도체 제조시설의 효율성을 위해 대부분의 현장에서는 물류 자동화 시스템(AMHS, Automated Material Handling System)을 도입하여 운영하고 있다. OHT(Overhead Hoist Transfer)는 반도체 공정에서 주로 활용되는 Monorail 컨베이어 형태의 자동 반송 시스템의 일종으로 작업물을 들고 제조 라인 위에 설치된 레일을 따라 자율적으로 이동하는 방식으로 운영된다. 도체 물류 시스템의 계층적인 구조적 특징과 고가의 재료를 다루고, 외부유출이 어려운 실제 공정 현장, 실험 환경의 시간, 공간적 구축 등의 현실적 특징 때문에 반도체 제조 공정의 자동화 물류시스템에 대한 모델링 및 시뮬레이션 을 통한 연구의 필요성이 대두되고 있다. 본 논문에서는 OHT를 효율적으로 제어하기 위해 DEVS (Discrete Event System Specifications) 형식론을 기반으로 OHT 시스템 모델링 및 시뮬레이션 설계 방법을 제안한다. 이를 위해 반도체 제조 시스템의 전반적인 물류 과정에 대해 분석하고, DEVS 형식론에 대해 연구하며, 이를 바탕으로 반도체 물류 시스템을 위한 모델링 및 시뮬레이션을 설계하였으 면, 실험을 통해 제안된 모델리 반도체 물류 시스템 시뮬레이션을 수행할 수 있음을 보인다.

1. 서론

스마트 팩토리나 4차 산업혁명 등에서 추구하는 시스템 목표 중의 하나는 다품종 소량 생산이다. 다양한 제품들을 하나의 공장에서 생산 할 수 있는 유연한 생산 시스템에 대해서는 이미 80년대부터 여러 방면으로 논의되어왔지만, 이를 위해서는 개별 설비들의 유연성 확보뿐만 아니라 이를 지원할 안정적인 정보 시스템이 구성되어야 한다. 전체 공장 단위의 유연 생산이 실현되기 위해서는 어떤 제품이 어느 시점에 어떤 장비에서 작업이 진행되어야 하는지 등 자동화된 의사결정이 필요하고 이를 위해서는 데이터 수집, 공유, 처리 등을 지원할 인프라가 필요하다 [1]. 90년대 IT혁신 이후 공장 내 정보 시스템에도 혁신적인 변화가 일어났으며 이제는 공장 전체를 지휘하는 MES(manufacturing execution system)와 공장 내 물류를 제어하는 MCS(material control system)가 제품의 입고 및 전체 공급사슬망을 관장하는 SCM(supply chain management)시스템이나

ERP(Enterprise Resource Planning)시스템 과도 연동되어 진정한 유연 생산을 시도할 수 있는 정보 환경이 구축되고 있다. 스마트 팩토리나 4차 사업과 같은 제조 혁신이 주목받고 있는 이유이기도 하다.



(그림 1) MES, MCS, VMS의 구조

OHT나 AGV와 같은 반송차량을 관리하는 시스템을 대차 관리 시스템(Vehicle Management System, VMS)이라 하며, 산업에 따라 ACS(AGV Control System), OCS(OHT Control System)로 칭하기도 한다. 일반적으로 VMS는 제조 관리 시스템인 MCS로부터 물류 반송 지시를 받고 이를 수행하기 위한 데이터를 수집과 관리하고 운영에 필요한 자동화된 의사결정을 수행한다. 그림 1은 일반적인 제조 정보 시스템 내 MES/MCS/VMS의 구조를 설명하고 있다.

반도체 제조 공정의 지능형 물류시스템도 이와 같은 MES/MCS/VMS 구조를 지니고 있지만, 대부분의 핵심 기술을 미국, 일본 등에서 수입하고 있는 실정이다. 또한, 반도체 공정의 생산설비 및 방법을 관리하는 시스템을 수입하는 것은 국내 기술력을 외부로 노출할 수 있다는 위험성을 가지고 있기 때문에, 각 학계 및 업계의 연구 기관에서는 관련 시스템의 국산화 연구 개발이 활발히 진행되고 있다.

최근의 반도체 제조 공정은 웨이퍼의 크기가 점점 커짐으로 인해, 물류작업자에 의한 반도체 Foup 이동의 효율성이 하락하고 있다. 이를 위해, 자동화된 물류 시스템을 이용하여, 지능형 시스템을 추구하고자 하는 노력이 많아졌다. 또한, 반도체 물류 시스템의 계층적인 구조적 특징과 고가의 재료를 다루고, 외부유출이 어려운 실제 공정 현장, 실험 환경의 시간, 공간적 구축 등의 현실적 특징 때문에 반도체 제조 공정의 자동화 물류시스템에 대한 모델링 및 시뮬레이션을 통한 연구가 증가 하였다. 기존에는 공정위주로 시뮬레이션을 수행하여 공정 개선을 추구하였다면, 자동화 물류 시스템만을 모델링 및 시뮬레이션을 수행하여 개선하고자 하는 연구가 증가하고 있는 추세이다. [2-3]

본 연구에서는 반도체 물류 자동화 시스템의 모델링 및 시뮬레이션을 위해 시스템에 적합한 모델링 형식론에 대해 연구하고, 전반적인 반도체 제조 시스템의 물류 과정에 대해 분석하며, 이를 바탕으로 반도체 물류 시스템을 위한 모델링을 설계한다.

2. DEVS 형식론

이산사건 시스템 명세(이하 DEVS, Discrete Event System Specification)라는 형식론은 모델링 및 시뮬레이션의 대상이 되는 시스템이 이산시스템일 때 사용할 수 있는 대표적인 모델링 형식론이다[4]. 이산시스템은 아날로그적 신호가 일정한 주기 혹은 정해

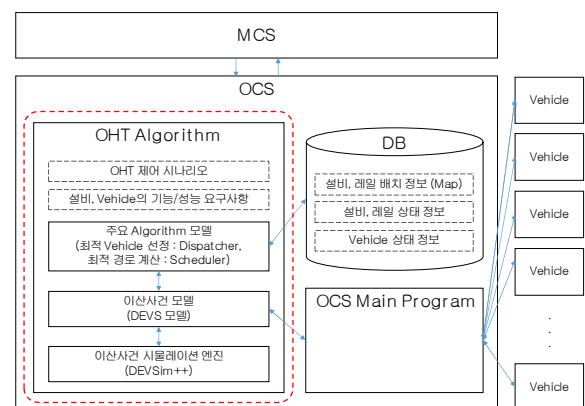
지지 않은 주기로 이산 신호(Discrete Signal)들에 의해 시스템의 상태가 특정 시점에 변하는 시스템을 말한다. 반도체 공정의 물류 자동화 시스템 또한 이산시스템으로 정의될 수 있다.

DEVS 형식론은 집합론에 근거한 형식론으로써 복잡한 시스템을 구성요소 별로 나누어 각각의 모델을 만든 후, 이를 합쳐서 전체 시스템을 표현할 수 있도록 되어있다. DEVS 형식론에는 3가지 집합과 4개의 함수로 시스템 구성요소를 나타내는 원자모델(Atomic Model)과 여러 모델을 합쳐서 새로운 모델을 구성하는 결합 모델(Coupled Model)이 있다. 이 두 가지 종류의 모델을 사용하여 시스템을 계층적이고 모듈러하게 표현할 수 있다.

3. DEVS를 이용한 OHT 스케줄링 시스템 모델링

3.1 제안하는 OHT 스케줄링 시스템 설계

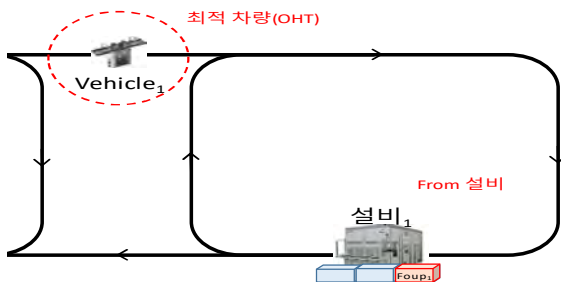
기존의 물류 시스템 관점에서 분류 해 봤을 때 OHT 시스템은 Monorail 컨베이어 시스템의 일종이다. OHT는 천장에 달린 Rail을 통해 단방향으로 이동하며, 작업물을 적재/하역 할 수 있는 로더(Loader, Robot arm, Crane)가 차량에 포함되어 있다. 또한, 배터리 없이 레일로 전력을 공급받는다. 이를 위해서, OHT 시스템 구축시 고려해야 할 사항에 시스템 레이아웃(Layout) 디자인, 반송차량의 수, 최적 차량 선택(Dispatching), 최적 경로 생성(Scheduling), 트래픽(Traffic), 충돌 방지, 교착 상태(Deadlock) 등의 해결을 포함해야 한다. 그리고 이 모든 기능들을 지원하기 위해서 차량의 상태, 작업물, 설비 정보가 모니터링(Monitoring) 되어야 한다. 그림 2는 본 논문의 설계 목표 범위를 나타낸다.



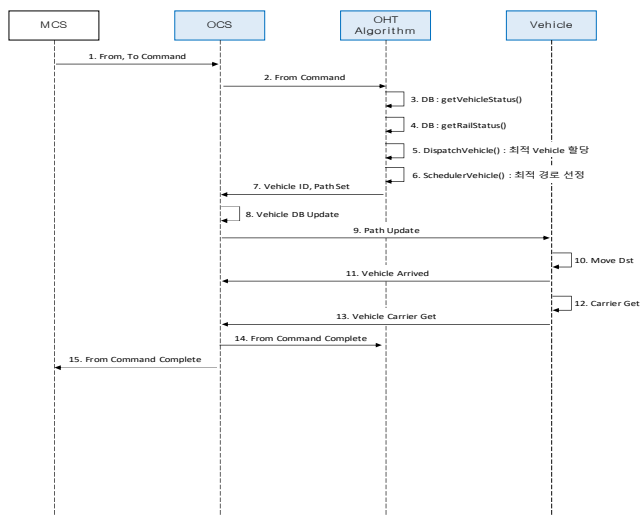
(그림 2) 제안하는 논문의 모델링 설계 목표 범위

3. 2 OHT 제어 시나리오 분석

OCS는 MCS에서 내려온 물류 이동 명령을 최적으로 수행하기 위한 시나리오를 가지고 있어야 한다. 반도체 제조 시스템은 무수히 많은 설비들의 공정을 거쳐서 하나의 제품을 완성하게 된다. 각 설비들의 공정 진행상황은 MCS가 파악하게 되고, 설비들의 공정 진행상황에 따라 OCS에게 반도체 Foup의 이송명령을 하달하면, OCS는 이송명령 수행을 위해서 최적 차량과 최적 경로를 계산하여 차량의 이동을 제어하여 전체 물류 시스템을 관리한다.



(그림 3) From 동작의 기본 시나리오



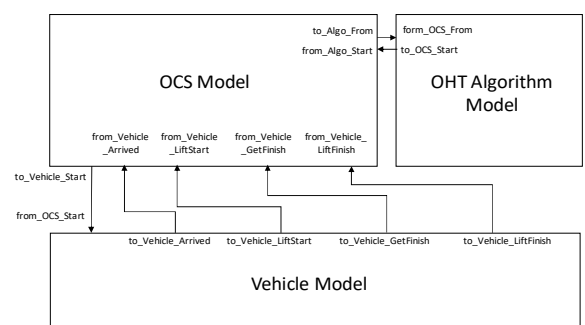
(그림 4) From 동작의 기본 Sequence Diagram

OHT가 반도체 물류 효율에 직접적으로 영향을 미치는 제어 시나리오를 분석하면, 예외상황을 포함하여 크게 4가지의 동작으로 분류할 수 있다. 첫 번째는 특정 설비 port에서 공정이 완료된 Foup을 가지러 가기 위한 From 동작이며, 두 번째는 From 동작을 통해 OHT에 적재한 Foup을 다음 공정을 수행하기 위해 다른 설비 port로 이송하기 위한 To 동작이 있으며, From과 To는 하나의 쌍으로 되어있다. 세 번째는 특정 설비의 공정 효율을 최대화 하기 위해, 2개의 From/To 쌍으로 구성 되어있는

Replace 명령, 네 번째는 위 세가지 From, To, Replace의 명령 수행간 방해되는 차량의 단순 이동을 위한 Go 동작이다. 그림 3은 From 명령 수행을 위해 레일 위에 있는 유휴 차량들 중 최적 차량이 선택되어 From 설비 위치로 이동하는 것을 표현한 그림이며, 그림 4는 이를 위한 시퀀스 다이어그램이다.

3. 3 DEVS 형식론 기반 시뮬레이션 모델

DEVS 형식론은 이산사건을 입력으로 받으며, 입력에 따라 이산상태를 변화하여, 이에 맞는 이산 사건 출력을 내보낸다. DEVS 형식론은 기본적으로 일정한 시간 간격동안 이산 사건이 발생하지 않을 때는 이상상태가 변화하지는 않는다. 내부 상태 천이 함수는 내부적으로 일정 시간 간격이 흐른 후에 이산 사건이 발생되면 내부 이산 상태가 변경되며, 이산 출력이 발생 된다. 본 논문에서는 그림 2의 모델링 설계 목표 범위를 포함하기 위해 그림 5와 같은 OHT 시스템의 개념모델을 제안한다. 전체 모델은 3개의 Atomic 모델로 이루어져 있다. 먼저, OCS라는 OCS Main Program과 두 번째는 최적 차량 선정 및 최적 경로 제어 계산을 담당하는 OHT Algorithm, 마지막으로 OCS Main Program과 통신을 주고받으면서 실제 반도체 Foup을 운반하는 차량인 Vehicle(=OHT)이 원자모델로 모델링 되었으며, 이 3개의 원자모델이 하나의 결합모델로 구성되는 전체모델을 구성하였다.

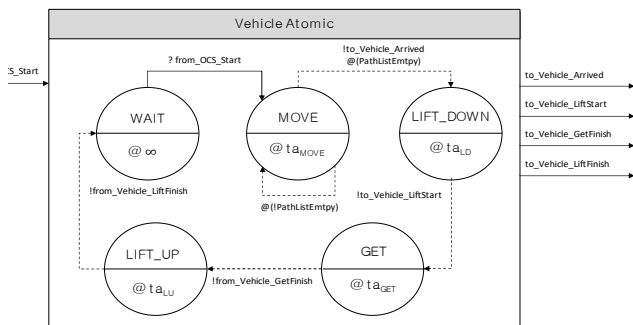


(그림 5) 제안하는 DEVS 개념모델

또한, 그림 4의 시퀀스 다이어그램을 표현하기 위해 각각의 원자모델을 구성하였는데, 식(1)은 그 중 Vehicle 원자모델의 구성요소이며, 그림 6은 식(1)을 바탕으로 Vehicle의 원자모델을 구성한 그림이다.

$$\text{Vehicle DEVS} = \langle X, Y, S, \delta_{\text{int}}, \delta_{\text{ext}}, \text{ta}, \lambda \rangle \quad \text{식(1)}$$

- $X = \{ \text{From_OCS_Start} \}$
- $Y = \{ \text{From_Vehicle_Arrived}, \text{From_Vehicle_LiftStart}, \text{From_Vehicle_GetFinish}, \text{From_Vehicle_LiftFinish} \}$
- $S = \{ \text{WAIT}, \text{MOVE}, \text{LIFT_DOWN}, \text{GET}, \text{LIFT_UP} \}$
- $\delta_{\text{ext}} = (\text{WAIT}, \text{From_OCS_Start}) = \text{MOVE}$
- $\delta_{\text{int}} = (\text{MOVE}) = \text{LIFT_DOWN} @ \text{PathListEmpty} == \text{True}$
- $\delta_{\text{int}} = (\text{MOVE}) = \text{MOVE} @ \text{PathListEmpty}! = \text{True}$
- $\delta_{\text{int}} = (\text{LIFT_DOWN}) = \text{GET}$
- $\delta_{\text{int}} = (\text{LIFT_DOWN}) = \text{LIFT_UP}$
- $\delta_{\text{int}} = (\text{LIFT_UP}) = \text{WAIT}$
- $\text{ta}(\text{WAIT}) = \infty$
- $\text{ta}(\text{MOVE}) = \text{ta}_{\text{move}} : \text{Vehicle Move Time To From Position}$
- $\text{ta}(\text{LIFT_DOWN}) = \text{ta}_{\text{LD}} : \text{Vehicle Lift Down Time}$
- $\text{ta}(\text{LIFT_UP}) = \text{ta}_{\text{LU}} : \text{Vehicle Lift Up Time}$
- $\lambda(\text{MOVE}) = \text{to_Vehicle_Arrived}$
- $\lambda(\text{LIFT_DOWN}) = \text{to_Vehicle_LiftStart}$
- $\lambda(\text{GET}) = \text{to_Vehicle_GetFinish}$
- $\lambda(\text{LIFT_UP}) = \text{to_Vehicle_LiftFinish}$



(그림 6) Vehicle Atomic Model

4. 시뮬레이션 구현 및 결과

시뮬레이션은 DEVS 형식론에 따른 모델구성 및 시뮬레이션 실행, 분석을 제공하는 C++로 개발된 DEVSim 어플리케이션을 활용하였다.



(그림 8) From 명령에 대한 시뮬레이션 결과

그림 8은 From 명령 수행을 위해서 DB로부터 Rail, 차량, 설비의 상태정보를 확인하여, OCS,

OHT Algorithm, Vehicle이 순차적으로 이벤트를 수행하고 있음을 보여준다. 입력으로 OCS로부터 임의의 명령이 발생하면, OCS가 OHT Algorithm으로 해당명령에 대한 최적 차량과 최적 경로 계산을 요청하고, 결과를 수신 받는다. 이 결과를 통해 차량을 이동하여 반도체 Foup을 이동 시킨다.

5. 결론 및 추후연구

본 논문에서는 반도체 물류 자동화 시스템을 위한 DEVS 형식론 기반 모델링 및 시뮬레이션 설계를 제안한다. 이를 위해 전반적인 반도체 제조 시스템의 물류 과정에 대해 분석하고, DEVS 형식론에 대해 연구하며, 이를 바탕으로 반도체 물류 시스템을 위한 모델링 및 시뮬레이션을 설계하였으며, 본 연구를 통해 제안된 형식론을 통해 반도체 물류 시스템의 시뮬레이션이 가능하다는 것을 확인하였다.

모델링 형식론을 이용하면, 시뮬레이션 모델에 대한 재사용성과 추후 유지 보수에 유용하다는 것은 당연하지만, 모델링 형식론 자체의 평가가 어렵다는 단점이 있다. 시뮬레이션 엔진, 프레임워크의 효용성 및 모델의 정합성은 실제 반도체 공정 데이터를 이용하여 실증적 실험을 통한 그 결과를 확인해 봐야 할 것이다.

따라서 추후 연구에서는 통해, 산학협력을 통해서 실제 반도체 공정 중 일부를 실체화하여 실증적 실험 결과를 도출할 예정이며, 최적 차량 선정 및 최적 경로의 계산을 위해 강화학습을 기반으로 하여 계산 효율성을 높이기 위한 연구도 함께 수행될 예정이다.

참고문헌

- [1] 황일희, et al. “데이터 기반 지능형 자동 반송 시스템 알고리즘 개발”. ie 매거진, 25.2: 26-30. 2018
- [2] F.K.Wang, J.T.Lin, “Performance evaluation of an automated material handling system for a wafer fab”Robotics and Computer-Integrated Manufacturing, Vol.20 , pp.91~100 (2016).
- [3] 안의국, 장대순, and 박상철. “Wafer FAB 의 납기 달성 향상을 위한 연구.” 한국 CDE 학회 학술발표회 논문집 (2015): 691-695.
- [4] Kim, Tag Gon, and Bernard P. Zeigler. “The DEVS formalism: hierarchical, modular systems specification in an object oriented framework”. Institute of Electrical and Electronics Engineers (IEEE), 1987.

Inception v3를 이용한 화장품 추천 시스템

장영훈¹, 사이드 무하마드 라자¹, 김문성², 추현승³

¹성균관대학교 전자전기컴퓨터공학

³성균관대학교 소프트웨어대학

²서울신학대학교 교양학부

^{1,2}{jang0h, s.moh.raza, choo}@skku.edu

²moonseong@stu.ac.kr

Recommended System for Cosmetics Using Inception v3 module

YoungHoon Jang¹, Syed Muhammad Raza¹, MoonSeong Kim², HyunSeung Choo³

¹Dept. of Electrical and Computer Engineering, Sungkyunkwan University

³College of Software, Sungkyunkwan University

²Dept. of Liberal Art, Seoul Theological University

요 약

최근 화장품이나 뷰티산업의 성장이 가속화되고 있다. 이에 따라 시장에 다양한 뷰티제품들이 출시되고 있지만 그로 인해 본인에게 적합한 제품이 무엇인지 알지 못하는 경우가 많다. 온라인을 통해 구매하는 경우 구매후기 및 광고에 의지해야 하며 전문가의 조언을 구하기 위해서는 오프라인 상점을 방문할 수밖에 없다. 그러나 오프라인 상점을 방문한 경우에도 자신에게 적합한 화장품을 추천받는 것 또한 다분하지 않다. 본 논문에서는 이러한 문제점을 해결하고자 온라인 환경에서 소비자에게 맞는 상품의 광고 및 정보를 받을 수 있는 화장품 추천 서비스를 제안한다. 또한 제안서비스는 AI기능을 적용하여 기존의 방식보다 소비자 친화적인 서비스를 제공하는 것을 목표로 한다.

1. 서론

현재 온라인 쇼핑 시장점유율은 가파르게 증가하고 있다. 정보통신정책연구원에 따르면 최근 5년간 평균 19%씩 성장하여 2022년에는 2017년의 2배가 넘는 규모인 189조 원대로 확대될 것이라는 분석이 있다. 이러한 변화에 있어 사용자 맞춤형 광고는 온라인 시장을 크게 성장시킨 주요 요인 중 하나이다.

광고 중에서도 오프라인 광고는 길에서 흔히 볼 수 있는 현수막, 게시판에 붙어있는 홍보 포스터 및 전봇대 등에 붙은 전단지 등이 있으며, 조금 더 발전된 방법으로 택시나 버스 등 이동수단을 이용한 광고 방법들이 대표적이다. 이러한 오프라인 광고는 온라인 광고에 비해 전달되는 거리가 제한적이며 가격 대비 낮은 효율을 갖기 그 실효성에 있어 부정적 평가를 받고 있다. 이러한 문제점으로 인해 온라인시장과 오프라인시장 규모의 격차가 더욱 커지고 있으며 이러한 격차는 더욱 가속화될 전망이다.

본 논문에서는 오프라인시장에서 온라인시장의

광고형태를 가져와 사용함으로써 앞서 제기한 문제들을 해결할 수 있음을 보이려 한다. 또한 오프라인시장에서 적용 가능한 온라인 광고 서비스에 AI기술을 접목시킨 시스템 구성도 및 모델을 제시하여 소비자 맞춤형 서비스를 구현한다.

2. 시스템 구축환경

2.1 TensorFlow[1]

텐서플로우는 다양한 작업에 대해 데이터 흐름 프로그래밍을 위한 오픈소스 소프트웨어 라이브러리이다. 심볼릭 수학 라이브러리이자, 뉴럴 네트워크와 같은 기계학습 응용프로그램에도 사용된다. 텐서플로우 라이브러리는 2015년에 공개되었으며 최근 머신러닝 및 딥러닝 시스템 개발 및 구현분야에 활발히 사용되고 있다. 본 논문에서 제안하는 서비스는 텐서플로우 라이브러리를 사용하여 구현되었다.

2.1 Inception v3[2]

Inception v3은 이미지 분석 및 객체 감지를 지원하기 위한 컨벌루션 신경망이며 Googlenet용

모듈로 시작되었다. TensorFlow에서의 공개 후 가장 많이 사용하는 컨벌루션 신경망 모델 중 하나이며, 이미지 추론에 많이 사용하는 모델이다.

딥러닝을 통한 이미지추론모델은 새로운 데이터셋에 최적화된 구조를 생성한다. 그러나 생성된 구조에 학습을 진행하는 것은 큰 시간적 비용이 발생한다. 이에 따라 최근에는 특정 분야 데이터 셋에 대해 검증된 모델의 구조와 파라미터들을 라이브러리 형태로 사용하는 것이 일반적이다. 이러한 동향을 통해 검증된 모델을 기반으로 새로운 데이터 셋에 대해 재학습(Retraining)을 진행하는 것이 보다 효율적이라는 것을 알 수 있다. 이러한 과정을 Transfer Learning이라고 하며, Inception v3 모듈은 재학습을 진행하기에 적합하고 저명한 모델이다.

3. 시스템 구성도

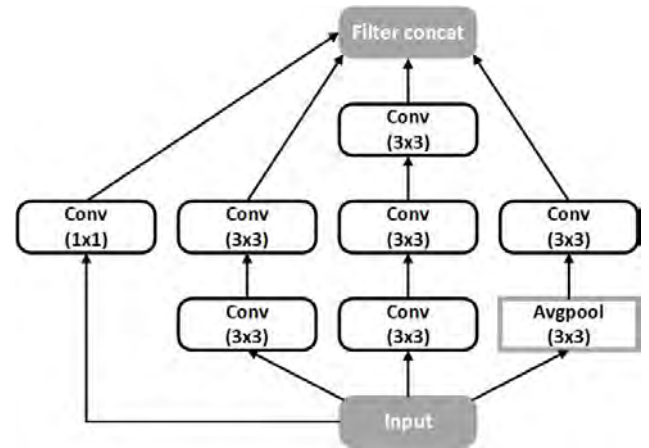
이 섹션에서는 본 논문에서 제안하는 시스템 구성, 성별 나이 예측모델, 여드름 예측모델과 얼굴크기 측정 메소드를 보여주며, 이를 시나리오에 적용하여 순서도와 함께 실제 동작과정을 설명한다.

3.1 성별 나이 예측 모델 Age_gender_model

성별과 나이 추측 값은 이를 추론하는 오픈소스 모델[3]을 사용하여 값을 도출 한다. 이를 통해 age_gender_model을 생성한다.

3.2 여드름 예측 모델 Pimple_model

학습모델을 구축하기 위해 여드름이 존재하는 사람의 얼굴 정면사진과 여드름이 존재하지 않는 정면사진을 각각 50장을 수집한다. 포괄적인 학습모델을 구축하기 위해 피부색의 특성이나 나이대를 폭 넓게 하여 사진을 수집하는 것이 핵심이다. 여드름의 유무를 추정할 수 있는 모델을 구축하는데 있어서, 위에서 언급한 Inception v3를 사용한다. 분류 클래스는 2가지로 pimple과 notpimple로 나뉜다. 학습을 진행하여 pimple_model을 생성한다.



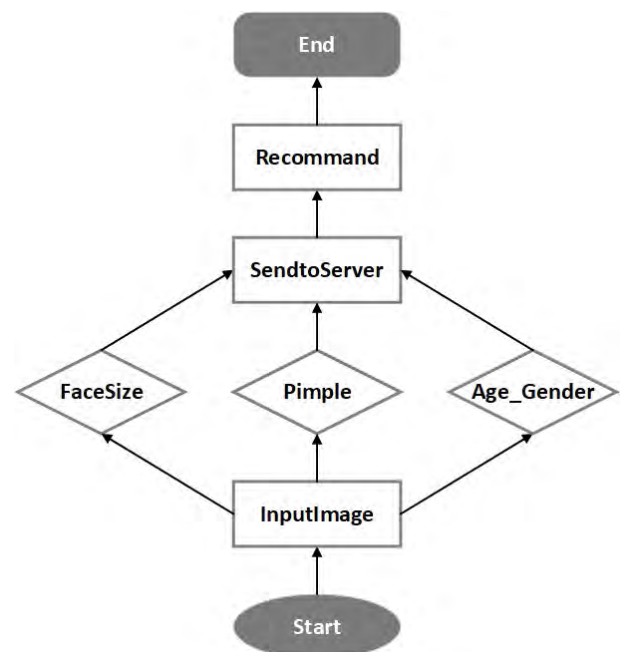
<표 1> Inception v3 Architecture

3.3 얼굴크기 측정

얼굴의 사이즈를 측정하는 방법은 먼저, 일정거리에서 얻은 사진으로부터 얼굴을 감지한다. 그 후, 감지한 얼굴의 얼굴길이를 pixel to cm로 변환하여, 얼굴의 상하길이 즉, 얼굴길이 값을 얻는다.

3.4 시나리오 순서도

1. 사용자 사진 요청
2. 사용자 얼굴 사진 전송
3. 학습된 age_gender_model, pimple_model 모델, 얼굴길이 측정메소드를 통해 사용자의 성별, 나이, 여드름 유무를 판단, 사용자의 얼굴크기 측정
4. 해당 상품정보 웹서버로 전송
5. 추천 상품정보를 사용자에게 전시



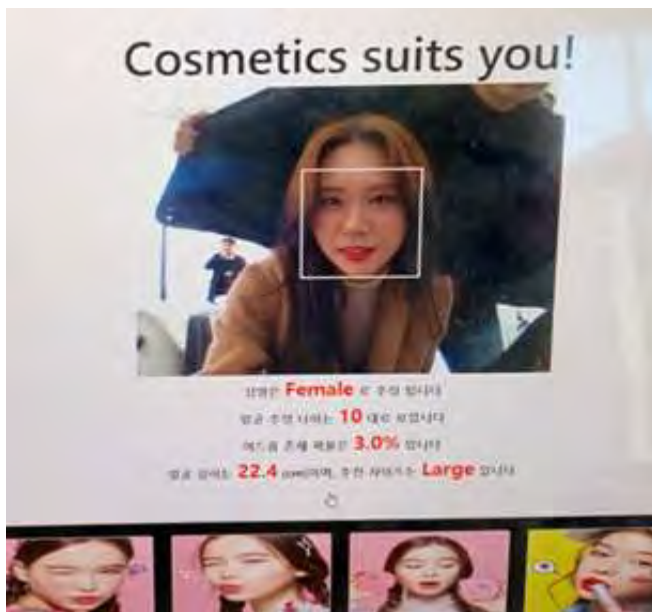
<표 2> 시나리오 순서도

3.5 구현 결과 및 설명



<그림 1 남자사용자>

이는 Pimple 값이 1%로 비 여드름자임을 알 수 있다. 성별은 Male, 연령대는 15~20세, 얼굴사이즈는 Small로 추정된다. 이를 통해 해당 남성 사용자에게 인기 있는 화장을 추천해주며, Small 사이즈의 마스크를 추천해준다.



<그림 2 여자사용자>

이는 Pimple 값이 3%로 비 여드름자임을 알 수 있다. 성별은 Female, 연령대는 15~20세, 얼굴사이즈는 Large로 추정된다. 이를 통해 해당 여성 사용자에게 인기 있는 화장을 추천해주며, Large사이즈의 마스크를 추천해준다.

4. 결과 및 향후 연구

구현 및 결과에 따르면 Inception v3는 적은양의 데이터 셋으로도 비교적 높은 정확도를 보여주고

있다. 하지만 Inception v3의 호환성은 높지 않아, 시스템의 성능이나 차별화된 학습모델을 구현하기 위해서 사용하기엔 좋지 못하다고 여겨진다. 본 논문에서 구현 및 평가를 위해 사용된 이미지 데이터 셋은 구글과 같은 빅데이터 플랫폼에서 얻어졌고, 학습에 이용된 이미지 데이터의 크기가 작아 구현된 모델이 실제 서비스로 사용되기 어렵다고 보인다. 상용되기 위해서는 보다 높은 정확도와 예측 안정성이 요구된다. 따라서 향후 연구에서는 보다 높은 정확도를 위해 예측 모델의 개량 및 학습데이터의 크기를 증진시키고자 한다.

ACKNOWLEDGEMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 Grand ICT연구센터지원사업(IITP-2020-2015-0-00742), 과학기술정보통신부 및 정보통신기획평가원의 글로벌핵심인재양성지원사업(IITP-2019-0-01579)과 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원(No.2019-0-00421, 인공지능대학원지원(성균관대학교))의 연구결과로 수행되었음.

참고문헌

- [1] Abadi, Martín, et al. "Tensorflow: Large-scale machine learning on heterogeneous distributed systems." arXiv preprint arXiv:1603.04467 2016.
- [2] Szegedy, Christian, et al. "Going deeper with convolutions." Proceedings of the IEEE conference on computer vision and pattern recognition. 2015.
- [3] Levi, Gil, and Tal Hassner. "Age and gender classification using convolutional neural networks." Proceedings of the IEEE conference on computer vision and pattern recognition workshops. 2015.

전력 소모 최소화를 통한 성능 개선의 코드 가시화 방법

안현식*, 박보경*, 김영철**

*홍익대학교 일반대학원 소프트웨어공학연구실

**홍익대학교 소프트웨어융합학과

{ahn*, park*}@selab.hongik.ac.kr, bob**@hongik.ac.kr

Code visualization approach for performance improvement via minimizing power dissipation

Hyun Sik An*, Bokyung Park*, R.Young Chul Kim**

*,**SELab. Hongik University

요약

높은 사양이 필요한 하드웨어 기반의 모바일 및 IoT 임베디드 시스템은 저전력과 성능에 중요한 이슈를 갖고 있다. 이는 전력 소비로 발열량 증가 및 기기의 수명 단축 문제가 발생된다. 이러한 환경에서 소프트웨어도 제한된 전력, 메모리 등에서 안정적인 동작을 수행해야 하므로 디바이스의 소비전력이 증가한다. 이를 해결하고자, 코드 관점에서 전력 소모 최소화를 통한 소프트웨어 성능 개선 가시화 방법을 제안한다. 이는 코드 가시화를 통해 복잡한 모듈을 식별하고, 저전력 코드 패턴을 적용하여 소프트웨어 성능을 개선한다. 이런 코드로 소비전력을 감소 및 성능을 개선함으로써 코드의 품질을 최적화 할 수 있다.

1. 서론

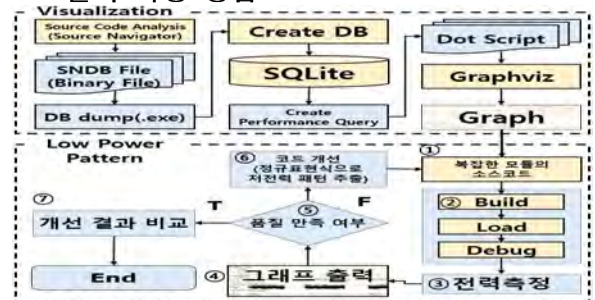
최근 자율주행, 드론, 스마트 폰 등 다양한 분야에서 임베디드 기기의 역할과 기능이 점차 확대되고 있다. 임베디드 시스템은 높은 사양을 가진 하드웨어로 구성된다. 고사양의 하드웨어에서 고성능의 소프트웨어가 작동함으로써 소비전력이 증가하고 있으며, 임베디드 시스템의 소비전력 증가는 기기의 수명단축으로 이어진다. 이러한 문제 해결을 위해 본 논문에서 소프트웨어 코드의 전력 측정을 통한 전력 소모 최소화 및 성능 개선 방법을 제안한다. 이 방법은 소프트웨어 가시화를 통해서 코드의 복잡도를 추출한다. 추출된 복잡도 중에서 소프트웨어의 성능을 저하시키는 모듈을 선정한다. 선택된 모듈은 본 연구에서 새롭게 정의한 저전력 패턴을 적용하여 소비 전력을 개선하고, 가시화를 통해 성능이 개선됐는지 확인한다. 본 논문의 구성은 다음과 같다. 2장은 관련 연구를 소개한다. 3장은 전력 측정 실험을 통해 새롭게 정의한 저전력 코드 패턴을 언급한다. 4장은 사례연구, 5장은 결론 및 향후 연구를 기술한다.

2. 관련 연구

Vetro가 제안한 Energy Code Smell은 소모 전력을 감소시킬 수 있는 가능성이 높은 패턴이다[1]. 하지만 에너지의 소모가 증가되는 경우도 있어 소비 전력을 절감하는데 적합하다고 볼 수 없다. 기존 연구에서는 Loop문에 대해서만 논하였다[2]. 이를 보완 및 확장하는 패턴은 3장에서 언급한다. 소프트웨어 가시화는 비가시적인 소프트웨어를 가시화하는 기법을 의미한다. (그림 1)의 Visualization 영역은 본 연구에서 사용한 성능 가시화 흐름도이다. 먼저 Source Navigator를 통해 소프트웨어 내부 정보를 SNDB 파일로 추출한다. 이 파일을 DBdump를 이용하여 텍스트로 변환한다. 그 후 변환된 데이터를 데

이터베이스 생성 후 각 테이블에 저장한다. 성능지표 추출을 위해 쿼리문을 생성한다. 결과물들을 Graphviz에 Dot Script로 입력하면 가시화 그래프에서 소프트웨어의 성능을 확인 할 수 있다[3].

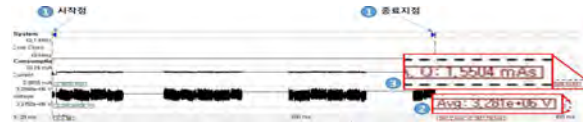
3. 소프트웨어 코드의 전력 소모 최소화를 위한 소스코드 전력 측정 방법



(그림 1) 성능가시화 및 전력소모 최소화 절차 흐름도

(그림 1)은 전력 소모 최소화를 통한 성능 개선의 코드 가시화 방법의 흐름도이다. 가시화한 그래프의 모듈 중에서 소프트웨어의 성능을 저하시키는 모듈을 선정한다. (그림 1)의 Low Power Pattern 영역은 성능가시화를 통해 선정된 복잡한 모듈의 전력 측정을 통한 전력소모 최소화 방안이다. 먼저 소스 코드 전력측정을 위한 환경을 구성한다. ①Keil uVision5 IDE에서 측정하고자 하는 소스 코드를 입력한다. ②소스코드를 실행한다. 프로젝트 실행은 3단계로 구성되어 있다. 입력한 소스코드를 Build하고 오류가 없으면 Load하여 보드에 Download한다. 그 후 Debug모드를 실행한다. ③디버깅 모드에 들어가면 입력된 소스 코드의 전력을 측정할 수 있다. 측정결과 ④와 같은 그래프로 나온다. ⑤측정된 전력값과 그래프를 참고하여 소스코드의 품질 만족 여부를 결정한다. ⑥만약 만족하지 못한다면

전력소모를 최소화 하기 위한 코드로 개선한다 만족한다면 소스 코드 전력 측정을 통한 전력소모 최소화 절차를 종료한다 (그림 2)는 측정 그래프다 ①번은 프로그램의 시작점과 종료지점을 나타낸다. 프로그램이 실행되는 동안의 전력을 측정하기 위해서는, 이 시작점과 종료지점까지 사용된 전류를 측정해야 한다 ②에서 전압은 3.3V가 일정하게 공급된다 실제로 그래프 상에서는 차이가 있지만 그 차이가 극소량이기 때문에 3.3V로 측정하였다 ③에서 나오는 데이터 중 Q는 시작점에서 종료지점까지의 누적 전류량을 나타낸다 이 누적 전류량을 전력을 구하는 공식인 $P = V \times I$ 에 대입하면 전력량을 측정할 수 있다



(그림 2) 전력 측정 결과 그래프

3.1 절차식 언어(C) 패러다임에 대한 저전력 패턴 정의

소프트웨어 코드의 전력을 측정하기 위해 절차식 언어 패러다임에 대한 코드 전력 패턴을 분석하였다. 본 연구에서는 3개의 절차식 코드 패턴을 정의하고 전력을 측정하였다. 장 수 때문에 2개의 패턴은 생략했다. 이 패턴들을 전체 소프트웨어에서 추출하기 위해 Cppcheck와 정규표현식을 사용했다. 또한 이를 개선하는 패턴을 정의한다.

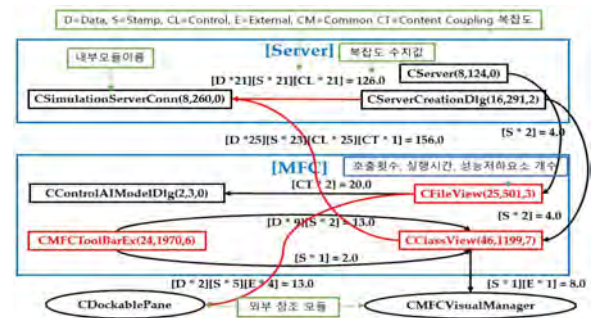
<표 1> Loop Up과 Loop Down 패턴 측정 결과

Item	Pattern Name	
	Loop Up	Loop Down
Code Pattern	<pre>int main(){ for (int i=0; i<100; i++){ printf("*"); } return 0; }</pre>	<pre>int main(){ for (int i=100; i>0; i--){ printf("*"); } return 0; }</pre>
평균 소비전력	5.2670697mW	5.2263594mW
정규 표현식	$[a-zA-Z]([a-zA-Z0-9])^* [&<] ([a-zA-Z0-9])^+ ;$ $[a-zA-Z]([a-zA-Z0-9])^* \backslash +$	

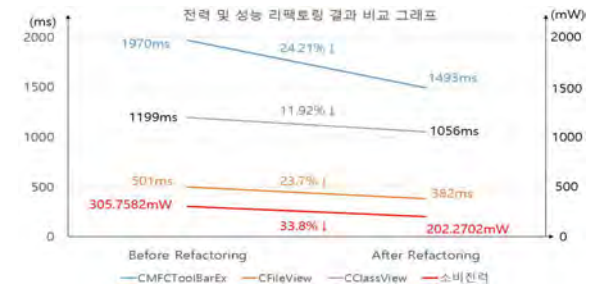
표1은 Loop Up과 Loop Down의 측정 결과이다. Loop Down 패턴의 전력 이 더 낮다 다음은 정규표현식에 대한 설명이다 for문 내부의 조건식에서 i는 변수이기 때문에 맨 처음에 숫자가 올 수 없으므로 '[a-zA-Z]'로 표현한다 그리고 그 뒤에 '([a-zA-Z0-9])^*'로 표현하여 변수의 값에 상관없이 겹칠 수 있다 '*'는 0개 이상 존재한다는 의미다 조건식 내부의 값을 비교하기 위해 '&<]'을 사용했고 조건을 비교하기 위해 변수 혹은 숫자가 올 수 있으므로 이를 '([a-zA-Z0-9])^+'로 표현했다 '+'는 1개 이상 존재한다는 의미다 증감식 'i++'은 변수를 표현하는 '[a-zA-Z]([a-zA-Z0-9])^*'뒤에 '\++'를 사용했다

4. 성능개선 코드 가시화

(그림 3)은 다관절 로봇 시뮬레이터 프로그램의 성능측정 결과 그래프이다[4]. 시각형 모듈은 모듈이름(호출횟수(번), 실행시간(ms), 성능저하요소(개))로 이루어져있고 성능저하요소가 3개 이상이면 빨간색으로 표시된다 동그라미 모듈은 헤더파일로 외부참조 모듈이다 각 모듈간의 호출 관계는 화살표로 표현하고 호출할 때 발생하는 결합도가 표시된다 성능가시화 결과 3가지 모듈이 심각한 성능저하요소를 가지고 있다 그림 4는 리팩토링 전 후를 비교하는 그래프이다 개선 전 전력량은



(그림 3) 성능 측정 결과 그래프



(그림 4) 전력 및 성능 리팩토링 결과 비교 그래프 305.7582mW이다. 이를 저전력 패턴을 적용한 후의 전력량은 202.2702mW이다. 총 33.8%의 전력감소효과를 얻을 수 있었다. 실행 시간도 1493ms, 1056ms, 382ms로 감소했다.

5. 결론 및 향후연구

IoT 기반 서비스 산업의 확장으로 IoT 디바이스들에 대한 수요가 증가하고 있다. 장기간 IoT 디바이스들을 운용하기 위한 저전력 사용 방법 및 성능 개선 등에 대한 연구가 필요하다. 본 연구에서 소프트웨어 코드의 전력 사용 효율화 및 성능 개선 방법을 제안했다. 이 방법은 전체 소스 코드의 복잡도를 가시화 하고 가장 복잡한 모듈들을 개선함으로써 소프트웨어의 소비전력 감소 및 성능 향상이 가능하다. 향후 연구로는 이번 연구에서 줄이지 못한 모듈간의 호출관계에서 발생하는 결합도를 개선하여 전력을 감소하고 성능을 개선하는 연구를 진행할 것이다.

ACKNOWLEDGE

본 논문은 2019년도 산업통상자원부의 '창의산업융합 특성화 인재양성사업'(과제번호 N000017)과 2017년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업(NRF-2017R1D1A3B0005421).

참고문헌

- [1] Antonio Vetro', Luca Ardito, Giuseppe Procaccianti, Maurizio Morisio, Definition, Implementation and Validation of Energy Code Smells: an Exploratory Study on an Embedded System, The Third International Conference on Smart Grids, 34-39, 2013
- [2] 안현식 이원영 김영철 고급 프로그래밍 코드 내 전력 소비 측정 통한 저전력 코드 패턴 매카니즘 식별 가이드, 2019년 ICT플랫폼 2019, 15-18
- [3] 강진희, 박보경, 장우성, 황준순, 권하은, 이한술, 이현준, 김영철, 소프트웨어 성능 가시화를 위한 툴 체인 개발, 18,1,395-398,2016
- [4] Bo Kyung Park, Byungkook jeon, R. Young Chul Kim, Improvement Practices in the Performance of a CPS Multiple-Joint Robotics Simulator, Applied Sciences, 10, 185-198, 2019

제53회
2020 온라인 춘계학술발표대회

데이터공학



여행 수요 파악 및 항공 노선 전략 연구 : 웹 크롤링 기반 분석 기법

조창현, 유현창
고려대학교 컴퓨터정보통신대학원 소프트웨어공학과
e-mail: {chogooood, yuhc}@korea.ac.kr

Study of Travel Demand and Air Route Strategy : Web Crawling-based Analysis Technology

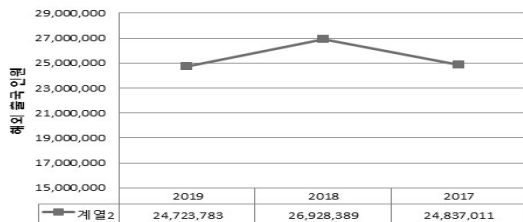
Chang-Hyeon Cho, Heonchang Yu
Dept of Software Engineering, Graduate School, Korea University

요 약

항공/여행 상품은 타 산업보다 불확실성에 취약하며 시간의 절대적인 종속성으로 인해 정확한 수요 파악 및 예측을 하지 못할 경우 가치가 0으로 수렴한다. 이에 본 논문은 웹 크롤링을 기반으로 잠재 여행 욕구를 파악하고, 향후 성장할 것으로 예상되는 항공 노선 및 취항지를 예측 및 분석하는 기법을 제안하고자 한다.

1. 서론

최근 여행 산업의 경우 (그림 1)의 통계 자료에서 보듯이, 2018년 여행자 수는 약 2,600만 명으로 여행업계는 유래 없는 기록을 갱신, 2019년은 조심스럽게 3,000만 명 출국 시대를 기대하는 분위기였다.



(그림 1) 최근 3년간 해외 출국자 수 (출처: 통계청)

하지만 2019년 홍콩 사태, 한/일 관계 악화, 2020년 중국의 코로나-19의 발생 및 확산 공포 등의 예상치 못한 돌발 변수로 인해 그 어느 때 보다 힘들고 혹독한 상황에 놓여 있다. 본 논문에서는 이런 어려움 속에서 여행 수요를 보다 효과적으로 파악할 수 있는 기법에 대해 제안하고자 한다[1].

2. 업계의 불확실성

현재 여행업계가 처한 어려운 상황은 여행업이 타 산업에 비해 불확실성에 취약하기 때문이다. 크게 여행업에서는 2가지의 불확실성이 존재한다. 첫째는 대외상황으로서, 국가 정치적, 질병, 테러, 전쟁 등의 제어하지 못하는 이슈

이고, 둘째는 수요와 수익 측면으로서, 고객 수요 파악이 어렵고 여행 상품을 기획하더라도 상품 정형화 및 품질 만족도 제고가 힘들다. 또한, 상품의 판매를 진행하더라도 상황 및 여건에 따라 매출 이익의 폭이 크기 때문에 안정적인 사업 확장이 어렵다. 따라서, 본 논문에서는 두 번째 불확실성에 대한 해결책으로 웹 크롤링을 통해 수요 파악의 불확실성을 최소화하고 정확한 상품 기획이 가능한 기법을 제시하고 검증한다.

3. 분석 및 실험 방법

3.1 수요 측정을 위한 니즈 파악 및 범위

여행 산업에서 고객 수요 파악 형태는 크게 2가지로 나누어 생각할 수 있다.

<표 1> 적극적 고객 정보 활용군 분석표

분류	적극적 고객 정보 활용군	
	(1) 검색형	(2) 대화형
내용	고객이 자신이 원하는 정보를 찾고, 직접 니즈를 입력하는 형태	질문을 통해 고객의 정보를 얻고, 답을 기반으로 직접적으로 니즈를 이끌어내는 형태
서비스 형태	여행 포털, Planner, 여행 오픈 마켓 등...	텍스트 기반 질문 챗봇, 심리테스트, 의사결정 트리 등...

<표 1>의 경우 고객의 정보를 최대한 많이 사용하여 수요를 파악하는 방법이다. <표 2>는 고객의 정보를 최소로 사용하여 수요를 파악하는 방법이다.

<표 2> 소극적 고객 정보 활용군 분석표

분류	소극적 고객 정보 활용군		
	(3) 테마 정의형	(4) 따라가기형	(5) 랜덤형
내용	3자가 여행 테마를 정하고 고객에게 최소한의 선택을 요구하여, 간접적으로 니즈를 파악하는 형태	기준에 만들어진 사례(여행 계획 등...)를 통해 고객이 직접 선택, 결정하게 만드는 형태	고객의 니즈 파악 없이 단순 랜덤 결과값을 제시하여, 최종 선택을 이끌어내는 형태
서비스 형태	테마 여행 상품, BRB 등...	여행 가이드 북, 셀럽 여행, 성지순례 등...	랜덤 박스, 랜덤 게임, 가차 게임 등...

(그림 2)는 고객 정보 활용군의 포지셔닝을 보여 준다.



(그림 2) 고객 정보 활용군 포지셔닝

본 논문에서는 적극적 고객 정보 활용군 중 잠재적 여행 고객이 가장 대중적으로 사용되는 (1) 검색형 고객 니즈에 대해 분석하고자 한다.

3.2 데이터 수집 범위 및 방법

고객의 수요를 파악하기 위해 먼저 고객의 취향을 반영하는 키워드(맛집, 가족, 살아보기 등...)를 선정하였다.

<표 3> 실험 언어 및 도구 정리

분류	실험 도구	수준
언어	Python	ver : 3.7.4
브라우저	Chrome	ver : 80.0.3987.122
환경	Visual Studio Code	ver : 1.43.0
통계	Excel	2016

<표 3>의 언어와 도구를 통해 실험을 진행하였고 총 3가지 방법을 통해 데이터를 수집하였다. (1) N사의 개발자 사이트 API를 활용하여 블로그, 카페, 뉴스의 키워드 빈도를 파악, (2) 여행 키워드와 높은 결합도를 보이는 단어들의 패턴 파악, (3) 인스타그램의 게시물 수준 및 해시태그(#) 빈도 파악 등 3가지 방법이다.

(1), (2)의 빈도 파악에 카페, 블로그, 뉴스를 중심으로 데이터 수집을 진행하였고 (그림 3), (그림 4)는 웹 크롤링을 진행한 Python의 소스 예시이다[2][3].

```

3 import os
4 import sys
5 import urllib.request
6 client_id = "U1YV7dF8Ym0LqG02X6n"
7 client_secret = "kSivLy0ybbq"
8 encText = urllib.parse.quote("차인하")
9 url = "https://openapi.naver.com/v1/search/blog?query=" + encText + "&json=false"
10 # url = "https://openapi.naver.com/v1/search/blog.xml?query=" + encText + "&xml=true"
11 request = urllib.request.Request(url)
12 request.add_header("X-Naver-Client-Id", client_id)
13 request.add_header("X-Naver-Client-Secret", client_secret)
14 response = urllib.request.urlopen(request)
15 rescode = response.getcode()
16
17 if(rescode==200):
18     response_body = response.read()
19     print(response_body.decode('utf-8'))
20 else:
21     print("Error Code:" + rescode)

```

(그림 3) API를 활용한 카페/블로그 웹 크롤링 예시

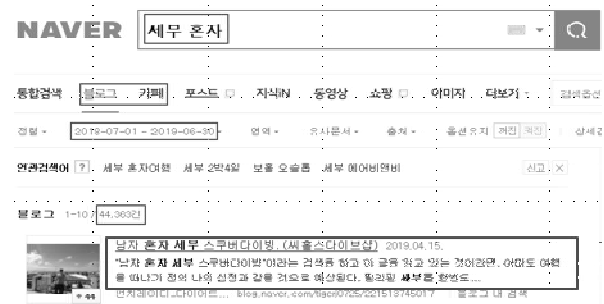
```

1 import requests
2 from bs4 import BeautifulSoup
3
4
5 for page in range(100):
6     raw = requests.get('https://search.naver.com/search.naver?where=blog&query=차인하&page=' + str(page))
7
8     html = BeautifulSoup(raw, 'html.parser')
9     articles = html.select('div.type01 > li')
10
11     for article in articles:
12         journal = article.select_one('span._sp_each_source').text
13         title = article.select_one('a._sp_each_title').text
14
15         print(journal, title)
16         print('페이지', page, '완료')
17
18 print('전체 완료')

```

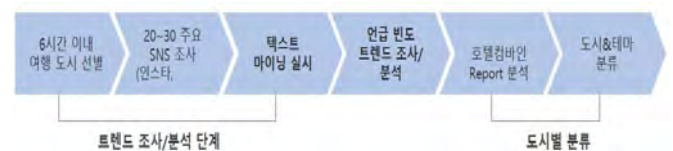
(그림 4) 뉴스 타이틀 및 본문 웹 크롤링 예시

(그림 5)의 경우 N사 중심의 키워드를 어디서 추출했는지를 화면에서 표시한 내용이다. 이 수집에서는 2010년부터 2019년까지의 총 87개 항공편 취항 도시 약 4,190만 건(약 블로그 2,350만개, 카페 1,480만개, 뉴스 360만개)의 여행자 수요 수집을 진행하였다.



(그림 5) N사 포털 실제 데이터 크롤링 영역

(3)의 방법인 (그림 6)의 경우 인스타그램 고객 수요 데이터 수집을 위한 프로세스이며, (1),(2)의 내용과 동일한 총 87개 도시에 대해 총 27,279,336건의 내용을 진행하였다.



(그림 6) 인스타그램에서 고객 수요 파악 프로세스

<표 4>는 87개 도시 중 누적 게시물 수 많은 곳을 보여 준다. 한국인에게 이미 알려진 휴양 명소, 쇼핑 명소 등이다. 추출 및 분석된 상위 10개의 도시의 경우 한국인에게 성숙된 관광지로 판단할 수 있다.

<표 4> 데이터 분석 기반 성숙 여행지 도시

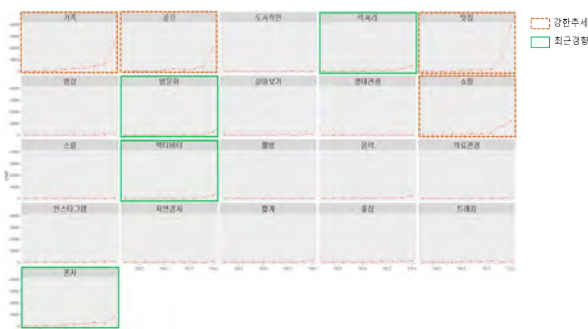
순위	도시	게시물 수	순위	도시	게시물 수
1	세부	5,175,810	6	방콕	1,972,262
2	도쿄	3,492,591	7	광	1,764,100
3	홍콩	3,476,560	8	다낭	1,318,809
4	오사카	2,438,283	9	후쿠오카	1,243,282
5	상해	2,240,256	10	베이징	977,491

<표 5>는 87개 도시 중 시간(Time)대비 최근 게시물 증가량이 높은 곳 상위 10개 도시를 추출한 결과이다.

<표 5> 데이터 분석 기반 성장 예상 도시

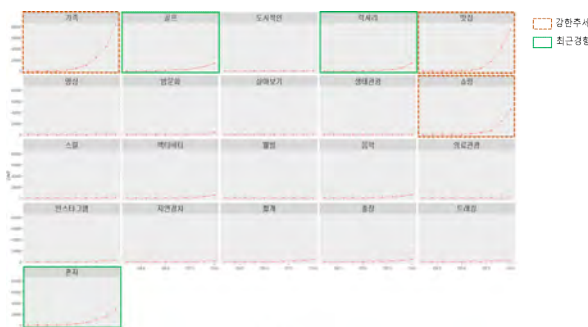
순위	도시	게시물 증가율	순위	도시	게시물 증가율
1	나트랑	111.60%	6	다카마쓰	47.90%
2	다낭	102.50%	7	하이퐁	45.10%
3	푸꾸옥	92.40%	8	코타키나발루	45.00%
4	가오슝	59.40%	9	타이중	43.90%
5	조호바루	56.50%	10	마쓰야마	42.00%

그리고 분석 당시 수요가 증가할 것으로 예측되는 여행 수요 도시는 나트랑, 다낭, 푸꾸옥 이다. 고객의 수요 내용의 구체화를 위해 각 도시의 자세한 여행 특성을 재분석 하였다.



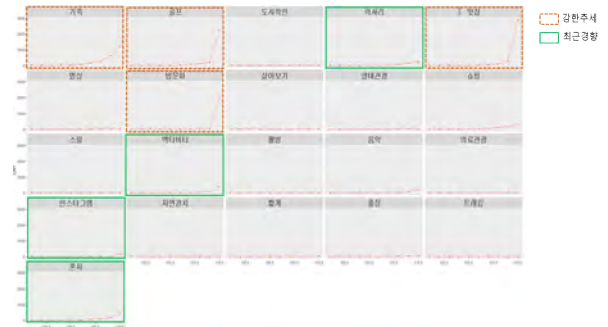
(그림 7) 나트랑 여행지 특성

(그림 7)과 같이 성장 예상 여행지 1위인 나트랑의 경우 기존에는 “럭셔리”, “밤문화”가 중심이었다면, 최근 강하게 보이는 추세는 “골프”, “가족”...등의 키워드이다.



(그림 8) 다낭 여행지 특성

(그림 8)은 2위인 다낭의 여행 특성이며 기존 여행의 테마 및 특성은 “골프”, “혼자”... 여행의 수요가 주를 이뤘고 최근 “가족”, “맛집”, “쇼핑”...에 대한 키워드가 있다.



(그림 9) 푸꾸옥 여행지 특성

(그림 9)과 같이 3위인 푸꾸옥의 경우 기존에 “액티비티”, “혼자” 여행이 주였다면, 최근 “가족”, “골프”, “맛집”의 키워드가 올라오면서 넓은 층의 여행 수요가 잠재해 있다는 것을 예상할 수 있다.

순위	도시	게시물 수	순위	도시	게시물 수
1	베트남	1,975,401	6	대만	1,972,262
2	태국	1,764,100	7	미국	1,764,100
3	인도네시아	1,318,809	8	일본	1,318,809
4	대만	977,491	9	한국	977,491
5	중국	5,175,810	10	홍콩	3,476,560

(그림 10) 인스타그램을 통한 고객 수요 파악

(그림 10)의 경우 인스타그램에서 여행자 수요를 게시물과 좋아요 등을 통해 파악된 연관 내용이며, 새로운 여행 수요는 나트랑, 다낭, 푸꾸옥이 추출되며, 연관 여행지 특성으로 “가족여행”, “맛집”, “골프”, “스냅사진” 등이 강한 성장을 보여주고 있다.

4. 분석 내용 검증

4.1 여행지 예상 수요 분석 검증

이번 데이터 수집 및 분석은 2019년도 9월에 진행하였다. 추후 성장 가능할 도시는 나트랑, 다낭, 푸꾸옥으로 예상되었고, 3곳 모두 베트남에 포함된 도시라는 특이점이 있다. <표 6>의 경우 한국인 인기 급상승 해외 여행지에 대한 관련 자료이다[4].

<표 6> 2020년 KLOOK 해외 인기 여행지 순위

순위	도시	성장률
1	베트남	603%
2	태국	412%
3	인도네시아	260%
4	미국	195%
5	대만	117%

(2019년 1월~12월 예약수 기준 YoY)

<표 7>의 경우 2020년 1월 28일에 만들어진 내용이며, 항공권 검색 및 예약 사이트로 잘 알려진 스카이스캐너(Skyscanner)와 중앙일보의 잠재 여행 고객 설문을 조합하여 발표된 자료이다[5].

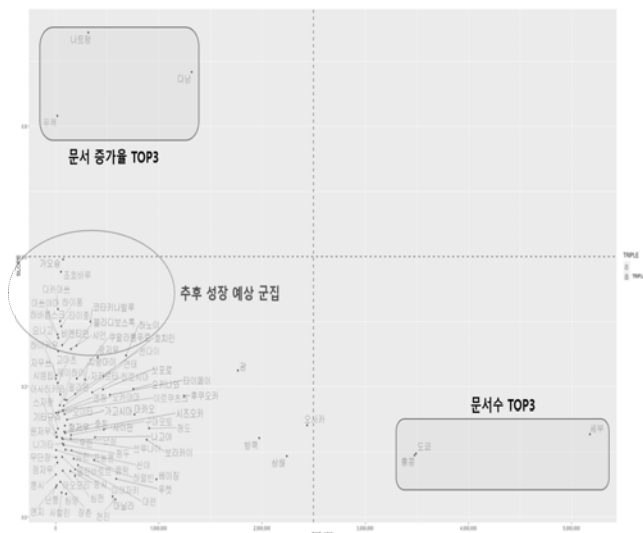
<표 7> 2020년 한국인 관심 여행지 Top 10

순위	도시	전년 대비 상승률
1	푸꾸옥	480%
2	나프랑	120%
3	보라카이	108%
4	치앙마이	57%
5	부다페스트	38%
6	베를린	25%
7	울란바토르	25%
8	블라디보스토크	24%
9	양곤	19%
10	하바나	18%

<표 6>과 <표 7>을 통해 웹 크롤링을 통한 여행 수요 파악이 가능하고 데이터 분석을 통해 향후 성장할 도시를 예측하는 것이 본 검증을 통해 확인되었다[4].

4.2 향후 성장 예상 도시

본 연구에서 도출한 성장이 예상되는 3개 도시의 경우 현재 이미 여행자에게 많이 알려졌고 2020년 상반기에 상품 개발을 적용 시킬 수 있는 여행지이다. 3개의 도시를 제외하고 추가적으로 앞으로 성장이 예상되는 지역에 대해 (그림 11)에서 87개 도시, “추후 성장이 예상되는 군집”을 표시하여 매트릭스에 추가해 보았다.



(그림 11) 신규 성장 예상 도시 매트릭스

지금까지의 가설 및 검증 내용을 적용시키면 동남아시아는 꾸준히 인기가 좋을 것으로 판단되며, 향후 한국인 여행수요가 증가할 것으로 예상되는 국가 및 도시는

“가오슝”, “조호바루”, “다카마쓰”, “하이퐁” 등이 될 것으로 예상 분석된다.

5. 결론 및 향후과제

본 논문에서는 웹 크롤링을 기반으로 잠재 여행 욕구를 파악하고, 향후 성장할 것으로 예상되는 항공 노선 및 취항지를 예측하여 기존의 여행 상품의 가치 불확실성을 줄일 수 있는 효과적인 예측 및 분석 기법을 제시하였다.

먼저 이번 수집에서 N사 개발자 API를 통해 2010년부터 2019년까지의 총 87개 항공편 취항 도시 약 4,190만 건 (약 블로그 2,350만개, 카페 1,480만개, 뉴스 360만개)의 여행자 수요 수집하였으며 인스타그램에서 총 27,279,336건의 게시물 및 해시태그(#) 데이터 수집을 진행하였다.

다음으로 이렇게 만들어진 수집 데이터를 기반으로 전체 게시물 수, 시간 대비 상승 수준, 여행 관련 키워드 빈도 등을 고려하여 분석을 진행하였다.

마지막으로 이렇게 만들어진 예측 결과를 실제 여행 상품 판매가 이뤄진 여행 액티비티(KLOOK) 사이트와 항공권 검색(Skyscanner)사이트에서 발표된 2가지 자료를 비교하여 제시한 기법에 대한 검증을 실시하였다.

다만, 2020년의 갑작스러운 코로나-19 이슈로 인해 현재 여행 시장은 물론 한국인의 해외 입국 자체가 불가능하다. 때문에 여행지 수요 예측의 내용을 모두 검증하는 것은 다소 어려우며 현업에 적용시키는 것이 시기적으로 불가능할 수 있다.

추후 시장이 안정화되고 다시 여행객이 증가되는 시기에 실질적으로 현업에 적용하여 제시된 기법을 보완 및 개선해 나갈 필요가 있다.

참고문헌

- [1] 조창현. (2019). “항공 예약/발권 시스템의 성능 및 편의성 개선 기법”, 석사학위논문, 고려대학교
- [2] 김경수. (2011). “웹 크롤링 수집주기의 동적 설계 및 구현”, 석사학위논문, 충북대학교
- [3] 웨스 맥키니, 파이썬 라이브러리를 활용한 데이터 분석 (2013). 한빛미디어, 한국
- [4] 파이낸셜뉴스. 베트남 6배 이상 성장... “KLOOK”자료 <https://www.fnnews.com/news/202001080919314871>
- [5] 중앙일보. 2020년 여기가 뜬다... <https://news.joins.com/article/236910021>

시차를 고려한 시계열 클러스터링 방법에 관한 연구

정재용*, 이주홍*, 송재원**
 *인하대학교 전기컴퓨터공학과
 ** (주)밸류파인더스

eoehd4108@gmail.com, juhong@inha.ac.kr, jwsong@valuefinders.co.kr

A Study on Time Shifted Time Series Data Clustering

Jae-Yong Jeong*, Ju-Hong Lee*, Jae-Won Song**
 *Dept. of Computer Engineering, Inha University
 **ValueFinders Co., Ltd

요 약

데이터 클러스터링은 데이터의 숨겨진 패턴을 찾아낸다. 시계열 데이터에서 시차가 존재하는 데이터를 클러스터링하는 것은 데이터의 미래 패턴을 찾아내기 위해서 사용한다. 데이터 클러스터링을 수행하기 위한 여러 가지 Metric이 존재하지만, 시계열 데이터의 노이즈로 인해서 클러스터링을 수행하는 Metric을 설정하는데 제약이 존재한다. 본 논문은 기존 시계열 데이터가 가지고 있는 노이즈를 PIP 기법을 사용하여 제거하고, 노이즈가 없는 시계열 데이터를 클러스터링하기 위한 효율적인 새로운 Metric을 제안한다.

1. 서론

시계열 데이터란 연속적인 시간에 걸쳐 측정된 순차적인 데이터 집합이다[1]. 시계열 데이터의 종류로는 금융 데이터, 음성 데이터 등이 있다. 시계열 데이터에서 시차란 두 시계열 데이터의 관측지점 사이의 거리를 의미한다. 시계열 분석을 위한 방법으로, 시계열 데이터의 패턴을 찾거나 데이터의 유사한 그룹을 찾아내는 시계열 클러스터링 방법이 있다[2,3]. 본 논문은 다른 시간의 시계열 데이터들의 관계를 분석하기 위해 시계열에 시차를 포함하여 클러스터링을 수행하여 데이터들의 패턴을 파악한다. 클러스터링에서는 데이터의 유사도를 비교하기 위한 기준이 필요하다. 일반적으로 사용되는 유사도 Metric으로 거리, 상관관계 등이 있다. 시계열 데이터 클러스터링에서는 데이터에 포함된 노이즈로 인해서 클러스터링에 사용할 수 있는 Metric이 제한된다. 따라서 시계열 데이터 클러스터링에서 적절한 유사도 Metric을 찾는 것은 중요하다. 시계열 데이터의 노이즈 문제를 극복하기 위하여서 PIP(Perceptually Important Points) 알고리즘으로 데이터의 중요한 지점을 찾아내고, 나머지 데이터를 제거함으로써 기존 시계열 데이터가 가지고 있는 노이즈를 제거한다. 노

이즈가 제거된 시계열 데이터에서 기존의 Metric이 찾지 못하는 패턴을 찾아내기 위하여 새로운 유사도 Metric을 제안한다.

2. THE PROPOSED METRIC

2.1 Problem Statement

시계열 데이터 클러스터링을 위한 시계열 데이터를 정의한다. 시계열 데이터 $Y_{t:d}^k$ 는 k 번째 시계열 데이터의 관측 시점 t 에서 d 까지 관측된 시계열 데이터를 나타낸다. 시계열 데이터를 다음과 같이 정의한다.

$$Y_{t:d}^k = \{y_t^k, y_{t+1}^k, \dots, y_d^k\}$$

데이터의 PIP를 찾는 보편적인 방법은 데이터의 양 끝 지점을 기준으로 만든 직선과 가장 멀리 떨어져 있는 데이터를 PIP로 정한다. 같은 과정을 반복하여서 다수의 PIP 찾아낼 수 있다. PIP를 찾는 방법은 데이터의 종류에 따라 다른 방법을 사용한다. 금융 데이터와 같이 데이터의 증감에 민감한 데이터의 경우는 PIP 변화의 증가와 감소가 반복되는 모양을 보

장하는 Zigzag-PIP 기법을 사용한다[4]. 본 논문에서는 데이터의 변동 비율이 임계치를 넘어가는 데이터를 PIP로 지정하였고, [5]에서 제공하는 ZigZag 패키지를 사용하여 구현하였다. 찾아낸 PIP를 제외한 나머지 데이터를 노이즈로 간주한다. 시계열 데이터 클러스터링을 수행하기 위해서는 모든 데이터가 동일 시점이어야 하는데, 시차가 존재하는 시계열 데이터의 시점은 서로 다르다. 이러한 이유로 시점이 다른 데이터들을 기준 시점으로 이동시킨다. 그래서 클러스터에 존재하는 모든 데이터는 모두 동일 시점 데이터로 표현되지만, 실제 각 데이터는 다른 시간 정보를 가진다.

2.1 클러스터링 Metric 제안

시계열 데이터 $Y_{t:d}^k$ 의 PIP 집합을 Z^k 이라고 정의한다. 두 개의 시계열 데이터 $Y_{t:d}^{k1}$, $Y_{t:d}^{k2}$ 의 유사도를 측정하는 Metric을 다음과 같이 유도한다. 먼저 두 데이터의 PIP를 공유하는 Z_{list} 를 만든다.

$$Z_{list} = Z^{k1} \cup Z^{k2}$$

PIP 구간으로 데이터의 기울기 d_i^k 을 다음과 같이 정의한다. (이때, $i \in Z_{list}$ 이다)

$$d_i^k = \frac{y_{z_i} - y_{z_{i-1}}}{z_i - z_{i-1}}$$

두 데이터 사이의 기울기의 유사도 함수 $SP(d_i^k, d_i^{k2})$ 를 다음과 같이 정의한다.

$$SP(d_i^k, d_i^{k2}) = e^{-(d_i^k - d_i^{k2})^2}$$

PIP와 실제 데이터 간의 오차를 기준으로 페널티 함수 $PN(y_i^k)$ 가 다음과 같이 정의한다.

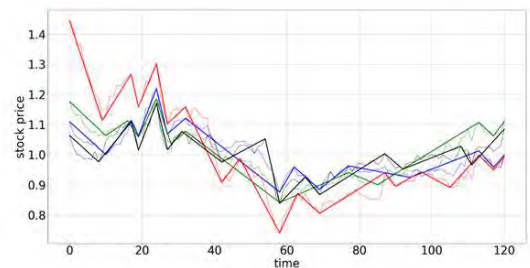
$$PN(y_i^k) = \sqrt{\frac{1}{(z_i - z_{i-1} - 2)} \sum_{i=z_{i-1}+1}^{z_i-1} (y_i^k - (\frac{y_{z_i}^k - y_{z_{i-1}}^k}{z_i - z_{i-1}} \times (i - Z_i) + y_{z_i}^k))^2}$$

페널티 함수와 기울기 유사도 함수를 조합하여 다음과 같이 유사도를 정의한다.

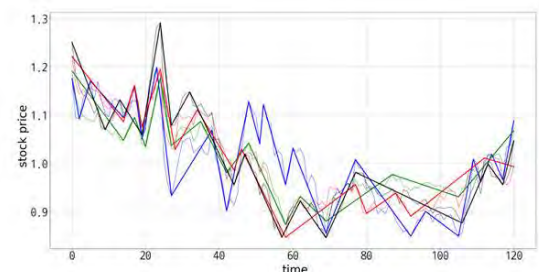
$$similarity(Y_{t:d}^{k1}, Y_{t:d}^{k2}) = \frac{\sum (\frac{SP(d_i^{k1}, d_i^{k2})}{(PN(Y_i^{k1}) + PN(Y_i^{k2}))} \times (Z_i - Z_{i-1}))}{\sum Z_i - Z_{i-1}}$$

3. 실험

제안한 Metric을 평가하기 위해 거리기반의 클러스터링 방법인 K-Means 모델[6]과 제안한 Metric을 사용한 클러스터링 모델의 결과를 비교한다. 클러스터링 데이터는 1185개의 종목, 720일 기간의 주가 데이터를 평균이 1이 되도록 정규화하여, 단위 기간인 120일로 자르고 PIP를 적용하여 노이즈를 제거한 데이터를 사용하였다. 클러스터링의 조건은 클러스터 36개, 반복횟수 5를 기준으로 한다. 실험결과는 아래의 그림들과 같다. 그래프의 선은 동일 클러스터에 존재하는 종목별 주식데이터를 의미한다. 그래프의 굵은 선은 PIP를 사용하여 노이즈를 제거한 주식데이터이고, 얇은 선은 실제 주식데이터이다. 그림 1에서 (a)는 데이터 사이의 거리가 크더라도 데이터의 증감하는 추세가 비슷하게 유지되지만, (b)에서는 데이터 사이에 거리가 가까워도 데이터의 추세가 잘 반영되지 않음을 볼 수 있다. 이를 통하여 제안한 Metric이 거리기반의 클러스터링 방법 보다 데이터의 추세를 잘 반영함을 볼 수 있다.



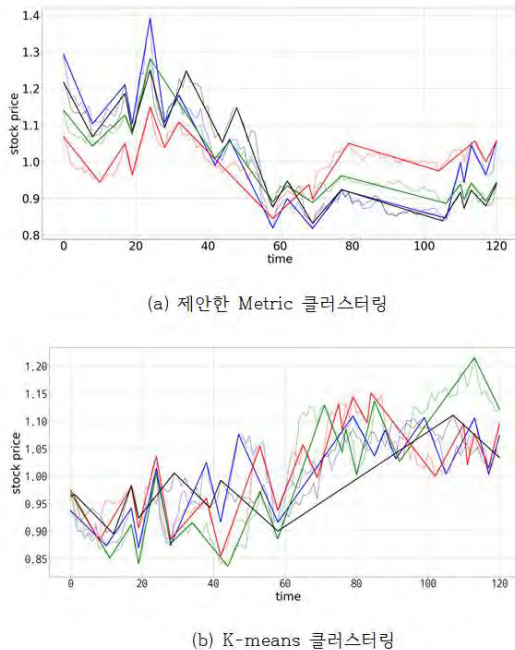
(a) 제안한 Metric 클러스터링



(b) K-means 클러스터링

(그림 1) 제안한 Metric과 K-means 클러스터링 비교

그림2에서 (a)와 (b) 모두 데이터의 추세를 반영하지만 (a)의 데이터 사이의 거리가 (b)에서의 데이터 사이의 거리보다 상대적으로 큰 것을 확인할 수 있다. 거리기반의 클러스터링 방법에서는 추세를 찾더라도 거리의 영향을 받지만, 제안한 Metric을 사용한 클러스터링은 거리의 제약을 받지 않고 데이터의 추세를 찾아낼 수 있음을 보여준다.



(그림 2) 제안한 Metric과 K-means 클러스터링 비교

4. 결론

클러스터링에서 유사도를 정의하기 위한 여러 Metric이 존재하지만, 시계열 데이터에 적용하기 적절하지 않은 경우가 존재한다. 따라서 시계열 데이터 클러스터링을 위한 유사도 Metric을 제안하였다. PIP의 기울기 차이를 사용하여 기울기 유사도 함수를 정의하고, PIP가 반영하지 못한 실제 데이터 정보를 페널티 함수를 정의하여 반영한다. 기울기 유사도 함수와 페널티 함수를 조합하여 유사도 Metric을 정의한다. Metric을 평가하기 위한 실험에서는 주식 데이터를 사용하고, 시차를 적용하여 다른 시점을 가진 시계열들의 패턴을 찾아낸다. 실험결과인 그림1과 그림2는 제안한 Metric을 사용한 클러스터링 모델과 K-Means 모델의 클러스터링 결과를 비교한 그림이다. 제안한 Metric을 사용한 클러스터링 모델이 K-Means 모델보다 데이터의 추세를 더 잘 반영함을 통하여 제안한 Metric의 성능을 검증하였다.

5. Acknowledgement

이 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 기초연구사업(과제번호: 2019R1F1A1062094)과 정보통신기획평가원의 지원(과제번호: 2019-0-01124)을 받아 수행된 연구임

참고문헌

- [1] Adhikari, Ratnadip, and Ramesh K. Agrawal. "An introductory study on time series modeling and forecasting." arXiv preprint arXiv:1302.6613 2013.
- [2] Roelofsen, Pjotr. "Time series clustering." Vrije Universiteit Amsterdam, Amsterdam, 2018.
- [3] Pena, Daniel. "A course in time series analysis." Wiley-Interscience, 2011.
- [4] Phetchanchai, Chawalsak, et al. "Index financial time series based on zigzag-perceptually important points." Journal of Computer Science. 2010.
- [5] "zigzag", <https://pypi.org/>, last modified Jul 18, 2017, accessed Mar 23, 2020, <https://pypi.org/project/ZigZag/>
- [6] Arthur, David, and Sergei Vassilvitskii. "k-means++: The advantages of careful seeding." Stanford, 2006.

빅데이터 분석과 머신러닝을 활용한 특정 정치인의 견해와 평판에 대한 프로파일링 기술

김민희, 강재은, 최주영, 황채연, 김명주
서울여자대학교 정보보호학과
xwoud@swu.ac.kr

Profile Generation on a Politician' Views and Reputations by using Big Data Analysis and Machine Learning

Min-Hee Kim, Jae-Eun Kang, Ju-Yeong Choi, Chae-Yeon Hwang, Myuhng-Joo Kim
Dept. of Information Security, Seoul Women's University

요 약

선거 기간 때마다 유권자들은 어떤 후보자에게 투표권을 행사해야 올바른 선택을 하게 될지 고민하게 되며, 후보자의 선거캠프에서는 후보자에 대한 유권자의 평판에 관심을 가지게 된다. 이러한 고민을 해결하기 위하여 본 논문에서는 TF-IDF 기법과 양방향 LSTM 기계학습모델을 활용해 특정 정치인의 분야별 행보와 여론에 대해 시계열 파악이 가능한 프로파일 보고서를 생성한다. 이를 통해 유권자는 후보자의 정치 철학과 경륜에 대한 이해가 쉬워져 올바른 투표권을 행사할 수 있으며 선거 캠프에서는 데이터 기반 평판에 대한 올바른 선거전략을 수립할 수 있게 된다.

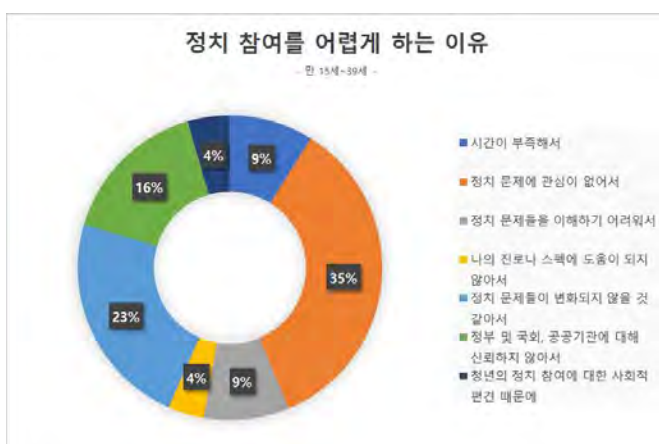
1. 연구 배경 및 목적

선거기간이 다가오면 많은 유권자들은 누구에게 투표해야 할지 모르겠고 어떤 후보가 무슨 공약을 세웠는지 관심을 갖지 않으면 알기 어렵다. 또한 이 공약을 제대로 수행할 수 있을지에 대한 신뢰성을 어떤 근거를 바탕으로 받아들여야 하는지 고뇌를 겪게 된다. 통계자료에 따르면 10~30대 연령층의 경우 정치 문제에 관심이 없어서, 정치 문제들을 이해하기 어려워하는 등 정치 참여를 어렵게 하는 다양한 의견을 표출하기도 하였다[1]. 이러한 문제는 정치적 무관심으로 이어질 수 있다.

반면에 4차 산업혁명 시대의 도래로 인해 언제 어디서든지 다양하고 흥미로운 정보를 얻을 수 있다. 이러한 점들을 바탕으로 정치 분야도 다소 변화를 겪게 되었다. 선거 연령이 낮아짐에 따라 스마트 기기나, SNS를 즐기는 층에서는 다소 흥미가 떨어지고 어려운 정치보다는 연예 기사와 같은 쉽고 재밌는 기사에 관심이 더 쏠리게 된다. 또한 SNS에 떠돌아다니는 불확실한 정치 관련 정보를 통해 편향된 정치 성향을 갖는 위험을 초래할 수 있다.

본 연구에서는 특정 정치인의 뉴스 기사와 댓글인 빅데이터를 수집하였다. 기사의 카테고리별 분류, 핵심문장 추출을 통해 시간 흐름에 따른 정치인의 견해 변화와 흐름을 쉽게 파악할 수 있게 타임라인을 작성하고 댓글 긍정, 부정 의견 분석을 진행하여 정치인의 평판을 한눈에 볼 수 있도록 하였다. 이를 통해 정치 이슈에 대한 접근성을 향상시켜 올바른 선거권을 행할 수 있게 설계하였다.

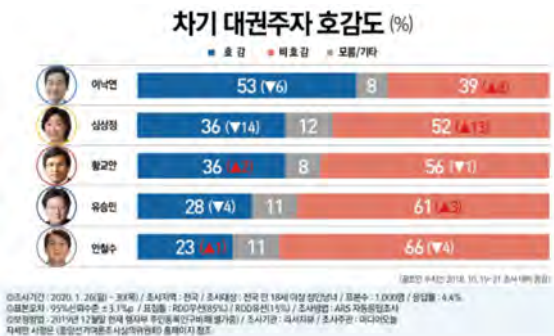
이를 위해 네이버 기사 2016년 1월부터 2020년 1월까지 약 4년 동안의 데이터를 수집했으며[2], 댓글의 경우 다른 성향의 매체로 네이버와 다음을 선정하여 2019년 9월부터 2020년 2월까지의 댓글을 수집하여 데이터를 분석하였다[3].



(그림 1) 정치 참여를 어렵게 하는 이유

2. 연구 구성

본 연구에서는 여론조사 전문기관 ‘리서치뷰’에서 시행한 호감도 조사 결과에 따라, 적용 샘플로 이낙연 정치인을 프로파일 대상으로 선정하였다.



(그림2) 차기 대권주자 호감도 여론조사

아래는 본 연구의 결과물로 대상의 간략 소개 및 기사 분석을 통해 파악할 수 있는 정치 행적을 대선, 통일, 외교, 노동이라는 4가지 주제의 타임라인 형태로 나타내고 있으며 댓글 분석을 통한 여론 평판을 보여주고 있다.



(그림3) 본 연구의 결과물

2.1 기사 수집과 데이터 전처리

이낙연 정치인의 행동/의견 타임라인을 제작하기 위해 기사를 수집하였다. 특정 언론사의 정치 성향에 영향을 받지 않기 위해 여러 언론사가 모여 있는 네이버 뉴스에서 기사 수집을 진행하였다. 기사 수집 기간은 2016년 01월부터 2020년 1월로, ‘이낙연’ 키워드가 들어있는 기사를 수집해 약 4만 5천 개의

기사를 타임라인 기사 후보로 두었다.

여기서 중요한 점은 올바른 데이터 분석 결과를 얻기 위해서는 올바른 데이터를 입력해야 한다는 것이다. 우수한 분석 알고리즘을 설계하는 것만큼이나 가다듬어진 데이터를 확보하는 것은 중요하다. 이를 확보하기 위해서 충분한 데이터 전처리 과정은 필수적이다. `konlpy` 라이브러리를 이용하여 한글 형태소 분석을 진행하였다. 그중 Okt(Open Korean Text) 분석기를 유사도 처리 및 댓글 글 부정에 사용하였다. 이때 불용어 리스트를 만들어 전치사, 관사, 너무 많이 등장하는 단어 등 문장이나 문서의 특징을 표현하는 데 있어서 불필요한 단어를 삭제하는 불용어 삭제 단계도 포함하여 진행하였다. 또한 `gensim` 라이브러리를 이용하여 Topic Modeling과 Word Embedding 기능을 통해 기사 학습 및 분류 그리고 핵심 문장 추출을 진행하였다. 이렇게 데이터 전처리 과정을 수행함으로써 데이터 마이닝이 정확성 면에서 높은 확률로 분석 결과가 도출되게 연구하였다.

2.2 기사별 유사도 처리

앞에서 수집한 타임라인 기사 후보들 중에서 같은 내용의 기사이거나 유사한 의미를 갖는 중복 기사를 걸러내기 위해 TF-IDF를 사용하였다[4]. TF-IDF는 텍스트 마이닝에서 문서에서 특정 단어의 빈도수를 이용해 중요도를 나타내주는 값이다. TF는 문서 안에서의 용어의 빈도, IDF는 한 용어가 문서 집합 전체에서 얼마나 공통적으로 나타나는지 나타내는 값으로 TF와 IDF를 곱한 수치를 문서 간 유사도를 파악하는데 사용하였다. TF-IDF를 이용해 80% 이상의 유사도를 갖는 기사들은 삭제하였다. 예를 들어, “이낙연 국무총리와 부인 김숙희 여사가 서울 서대문구 신촌세브란스 병원 장례식장을 찾아 조문하고 있다.”와 “이낙연 국무총리와 부인 김숙희 여사가 서대문구 신촌세브란스 병원 장례식장을 찾아 조문한 뒤 유족을 위로하고 있다”의 경우, 앞의 내용은 같지만, 뒤의 기사에서는 앞의 기사 내용에 “유족을 위로하고 있다”라는 내용만 추가되었기 때문에 문서 간 유사도가 높다고 판단되어 삭제된다. 이러한 과정을 통해 약 4만 5천 개의 기사에서 약 2만 5천 개의 기사로 후보를 축소하였다.

2.3 기사 카테고리 분류와 핵심기사 추출

본 논문에서는 기계학습 모델 중 ‘양방향 LSTM

순환 신경망'을 이용하여 기사를 대선, 통일, 노동, 외교 총 4가지의 카테고리로 분류하였다. 양방향 순환 신경망은 순방향과 역방향의 두 개의 분리된 순환 신경망을 통해 학습을 시키는 방법이다[5]. 역방향인 은닉층에서는 과거의 정보를 기억하여 학습시키므로 언어 간 의미를 파악하기 위한 본 실험에 적합한 모델이다. 기사를 분류하기 위한 트레이닝 셋을 만들기 위해 카테고리별 4천 개, 총 1만 6천 개의 기사를 수집하였다. Tensorflow v.3.7에서 Learning rate는 0.001로 설정하고 5번의 반복 학습을 수행하였다. 그 결과 87%의 정확도를 얻었다. Word2Vec를 이용하여 단어를 수치화하여 단어 간 유사도를 구하고 embedding 파일과 model을 생성하였다.

이후, 카테고리를 분류하는 방법은 분류하고자 하는 기사를 Word2Vec로 토큰 처리하여 생성된 embedding 파일과 Convert2Vec 하였다. 트레이닝 셋을 만들 때와 같은 환경으로 실험하여 96%의 정확도를 얻었다. 위의 과정을 통해 카테고리별로 타임라인 후보 기사들을 분류하였다. 해당 월중에 핵심 기사를 파악하기 위해 TextRank를 사용하였다. TextRank는 워드 그래프나 문장 그래프를 구축한 뒤, 그래프 랭킹 알고리즘인 PageRank를 이용하여 각각 키워드와 핵심 문장을 선택하는 방법이다[6]. 이러한 과정을 통해 각 카테고리별로 타임라인이 완성된다.



(그림4) 타임라인 작성 순서도

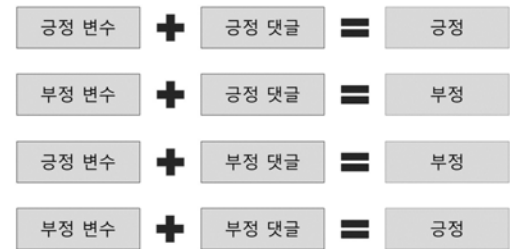
2.4. 댓글 학습과 분류를 통한 여론 분석

댓글 상에 나타난 '이낙연'에 대한 긍정과 부정의 여론을 보여주기 위해 2019년 9월부터 2020년 2월까지 6개월간의 '이낙연' 관련 기사의 댓글들을 네이버와 다음에서 각 포털별로 한 달에 5천 개씩을 수집하였다. 수집한 댓글들을 긍정과 부정으로 분류하기 위한 트레이닝 셋을 만들기 위해 정치 분야의 기사 댓글 약 3천 개를 추가로 수집하여 긍정과 부정, 중립으로 분류하였다. '이낙연'에 관한 여론만을 파악하기 위해 이낙연에 대한 긍정 변수 그룹과 부정 변수 그룹을 설정하고, 분류된 댓글 중 긍정 댓글과

부정 댓글의 주어 부분을 변수 '\$'로 바꾼 후 변수 그룹을 대입하여 트레이닝 셋을 만들었다.



(그림5) 긍정 변수 그룹과 부정 변수 그룹



(그림6) 긍·부정 파라미터 공식

이렇게 만든 트레이닝 셋을 바탕으로 앞서 기사의 분류에 사용했던 양방향 LSTM 기계학습모델을 통해 embedding 파일과 model을 생성한 후 각 월별 1만 개의 댓글을 분류하였다. 나온 결과에 대해서는 긍정과 부정 각각의 워드 클라우드를 생성하여 댓글에 많이 등장한 키워드를 보여주고, 긍정 대 부정의 비율로 계산하여 그래프로 보여준다.

3. 기대효과 및 향후 계획

본 연구의 결과물은 특정 정치인의 행보를 시간의 흐름에 따라 한눈에 보여주며, 댓글 상에 나타난 특정인에 대한 대중의 긍정, 부정의 의견을 보여준다. 이러한 결과물을 통해 기대할 수 있는 효과는 다음과 같다.

첫째, 유권자들이 올바른 선거권을 행사할 수 있도록 도와준다. 둘째, 정치 관련 이슈에 대한 접근성을 향상시킨다. 셋째, 정치인이 자기 자신의 평판을 점검하는 데에 사용할 수 있다.

향후 이 프로젝트에 대한 과정의 전반을 연결하고 자동화하는 것을 목표로 한다. 현재는 데이터의 수집과 유사도 기반 중복 제거, 분류 등 데이터를 처리하는 과정들이 분리되어있다. 이러한 과정들을 연결하고 자동화하여 데이터의 수집과 처리 사이의 격차를 좁히고, 최종적으로는 사용자들이 원하는 인물, 기간 등을 설정하여 만들어지는 사용자 기반의 프로파일링 프로그램을 구축하고자 한다.

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 SW중심대학지원사업의 연구결과로 수행되었음(2016-0-00022)

참고문헌

- [1] 한국청소년정책연구원, 「청년사회·경제실태조사」
- [2] <https://news.naver.com/>
- [3] <https://news.daum.net/>
- [4] 오유리, 민재욱, 김용일, 김대중, 박용균, 이봉건. (2017). 워드임베딩 기반 TF-IDF를 이용한 특허 문서의 유사 청구항 도출 기법 비교 분석. 한국정보과학회 학술발표논문집, 1002
- [5] 주일택, 최승호. (2018). 양방향 LSTM 순환신경망 기반 주가예측모델. 한국정보전자통신기술학회 논문지, 11(2), 204-208.
- [6] 배원식, 차정원. (2010). TextRank 알고리즘을 이용한 문서 범주화. 정보과학회논문지. 컴퓨팅의 실제 (한국정보과학회), 16(1), 110-114.

신뢰성있는 온라인 고객 리뷰 텍스트 마이닝 기반 식당 개별 음식 아이템 평가

무자밀 후세인 사이드*, 정선태**

*송실대학교 정보통신공학과, **송실대학교 스마트시스템소프트웨어학과

e-mail: engr.muzamilshah@gmail.com, cst@ssu.ac.kr

Rating Individual Food Items of Restaurant Menu based on Online Customer Reviews using Text Mining Technique

Muzamil Hussain Syed*, Sun-Tae Chung**

* Dept. of Information and Telecommunication, Graduate School, Soongsil University.

**Dept. of Smart System Software, Soongsil University

Abstraction

The growth in social media, blogs and restaurant listing directories have led to increasing customer reviews about restaurants, their quality of food items and services available on the internet. These user reviews offer a massive amount of valuable information that can be used for various decision-making purposes. Currently, most food recommendation sites provide recommendation scores about restaurants rather than food items of the restaurant and the provided recommendation scores may be biased since they are calculated only from user reviews listed only in their sites. Usually, people want a reliable recommendation about foods, not restaurant. In this paper, we present a reliable Korean food items rating method; we first extract food items by applying NER technique to restaurant reviews collected from many Korean restaurant recommendation web sites, blogs and web data. Then, we apply lexicon-based sentiment analysis on collected user reviews and predict people's opinions as sentiment polarity scores (+1 for positive; -1 for negative; 0 for neutral). Finally, by taking average of all calculated polarity scores about a food item, we obtain a rating to individual menu items of the restaurant. The proposed food item rating is more reliable since it does not depend on reviews of only one site.

1. Introduction

Sentiment Analysis or opinion mining from texts can be seen as a natural language processing (NLP) task that aims to analyze opinions, sentiments, and emotions expressed in unstructured data [1]. A common task in this research area is polarity classification, which consists in classifying the overall sentiment present in a document or sentence. Usually this task is simplified by classifying a text or a sentence in 3 classes: positive, negative or neutral. To build a sentiment classifiers, two main approaches have been investigated: lexicon-based methods [3], and machine learning algorithms [4,5].

Applying sentiment analysis to user reviews, to know their opinion about entities can give us some useful insights for marketing and decision-making purposes.

Analyzing and extracting meaningful information from the user reviews is useful from both client and restaurant owner perspectives. Today, people are highly interested in searching client's reviews on restaurants online to know one's perception of the food quality and services of a restaurant before the visit. The restaurant owner also gets to know about the clients' opinion over the quality of food items and services offered. This can help the restaurant owner to improve its marketing strategy and the quality of food and services. Most of current food recommendation sites in Korea provide recommendation scores about restaurants

rather than food items of the restaurant, furthermore the provided recommendation scores may not be reliable since they are calculated from user views listed only in their sites.

In this paper, we present a reliable food items rating method, which is based on text analysis on user reviews from different sources; food recommendation web sites, blogs, SNS(twitter, instagram, etc). Thus, it can provide a way to the local restaurant owner to identify people's opinions about the quality of their food and help other users to find the best food place for dining in. We use the Named Entity Recognition (NER) technique to identify food item names in restaurant reviews and apply lexicon-based sentiment analysis to extract people's opinions by sentiment polarity. In our work, we utilize a lexical resource approach such as a dictionary of opinionated terms. Korean Sentiment Analysis Corpus named KOSAC [7] is one such resource, which is the sentimental dictionary for Korean words and assigns three sentiment numerical scores to each word as positivity, negativity and neutral.

2. Proposed Method

The proposed method consist of three main steps.

2.1 Data Collection

The system initially targets for a small business area near Isu station in Seoul. We collect local restaurant data and reviews from multiple sources which are broadly categorized into two categories. i) Concrete data source: The data source contains complete information about the restaurant, menus, and reviews. These are GooglePlaces, KakaoPlace, MangoPlate, Naver Store, SiksinHot and DiningCode. ii) Partial data source: The data source which provides user opinion data by their posts, blogs or comments about the food items of the restaurant. These are Twitter, Instagram, Naver blogs.

The Collected data set includes 32 restaurants and 16656 reviews. The collected data is stored in the MongoDB database. We create a list of 20 famous selected Korean food items that contain only the real common food item names, that are used to identify the food name from the review and used as Named Entity Recognition. This is important as many of the restaurant menu names are customized based on the recipe, but users while writing a review, uses the common name of the food items. Figure1 shows the architecture of data collection and storage.

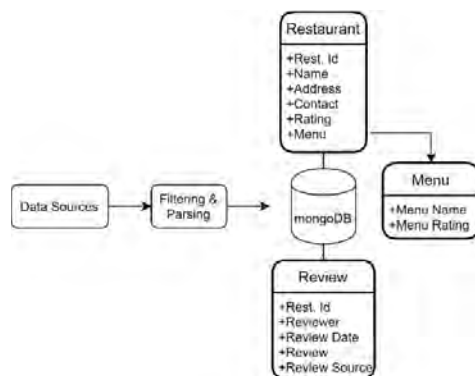


Figure 1: Data collection and storage architecture.

2.2 Rating Food Item

The initial rating of food items in the restaurant menu is applied based on the overall average rating score of the restaurant. The average rating of the restaurant is calculated from the rating scores obtained from the concrete data source. For example, if the rating scores for a restaurant R obtained from different data sources is 4.1, 2.6, 4.2, 4.3 and 3.6, then the overall average rating would be 3.8, which is assigned as the initial rating score for individual food items in the restaurant menu. This rating is then further updated based on the opinion of the user reviews. The process of rating food items in restaurant menu list consists of a pipeline of operations; see Figure 2.

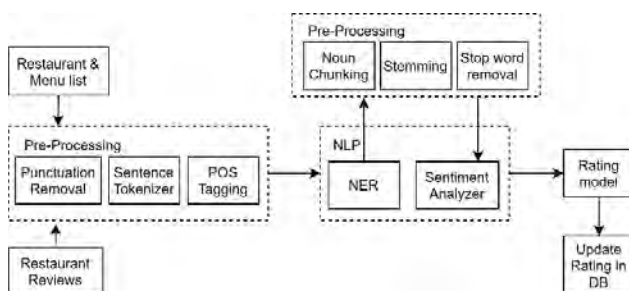


Figure 2: Process of rating food item.

The restaurant's menu list and reviews are fetched from the database.

A. Pre-processing of ReviewData

The aim of preprocessing is to remove unwanted and noisy data. To pre-process the review data, Korean NLP in Python KoNLPy has been used. KoNLPy is a Python package for natural language processing (NLP) of the Korean language. The pre-processing steps are performed at two stages. The need for processing data into two stages arises from the requirement of extracting the food names from the reviews. By processing the data in one stage may result in non-identified food names from the restaurant menu. The first stage comprises the following tasks:

- Punctuation Removal:** Punctuations in a text generally do not provide any useful information. This step, therefore, erases the punctuation characters from the word.
- Tokenization & POS tagging:** This process breaks a stream of text into a list of words. Each review is broken into sentences. The sentence detector in the KoNLPy toolkit is used to break reviews into sentences. Then, each of these sentences is tokenized and POS tagged using the toolkit.
- Noun Chunking:** The POS annotated tokens are then sent to the chunker, which combines the noun token and other possible noun category token identified by the toolkit. The noun chunker uses Regex to combine the noun token.

```
Regex = ""
NP: {<N.*>*<UN>?<N.*>?<Suffix>?}
""
```

The Regex considers all the noun tags (보통명사, 고유명사, 일반 의존 명사, 단위 의존 명사) and other tags that are estimated to be a noun (명사추정범주). This is because the food names in the reviews are not just the standard food names included in the food menu.

The second stage of data pre-processing is performed after NER extraction to perform sentiment analysis. The second stage comprises the following tasks:

- Stemming:** This step reduces words to its stem or root form as stemming simplifies the sentiment analysis process. The same word can be used in a different flavor for grammatical reasons such as consult, consulting, consultant.
- Stop Word Removal:** Stop words consist of prepositions, help verbs, articles, and so forth. They typically do not contribute to analyzing sentiments and are removed from the text.

B. Named Entity Recognition (NER)

Named Entity Recognition (NER) also known as entity chunking/extraction, is a popular technique used in information extraction to identify and segment the named entities, and classify or categorize them under various predefined classes. After pre-processing, an NER technique is utilized to extract food names from customer reviews. The noun chunks don't fit enough to find out food names from the reviews. To make use of NER to identify food names in restaurant reviews, a corpus annotated with food names is

required. Since such corpus was not available in Korean language for food names, we had to create one. Different approaches could be applied to make a custom food name annotated corpus[2] for Korean language. The possible approach could be, annotating all food names in collected reviews and train the model using spaCy to detect food domain name automatically. Instead of creating an annotated corpus, we use a list of selected food items that could be used as a NER. To identify a food name entity, we have used a two-way matching approach.

Firstly, in the selected list of food items only the common names are defined; i.e. ‘초밥’, ‘치킨’, ‘갈비’ etc. The selected food item list is used to detect the noun chunks that contain the food word from the review texts. In most of the cases the food names in restaurant menus are more verbose and customized based on the recipe but users, while writing a review, use the common name of the food items; i.e. ‘초밥’ that makes it harder to identify the food item from menu list; i.e. ‘스페셜 초밥’, ‘로로초밥’, ‘특 초밥’.

After a noun chunk matched with a food name from the selected list, the noun chunk is then compared with the food item names in the restaurant menu list using a fuzzy string matching algorithm to find the Levenshtein similarity ratio based on the Levenshtein distance. The similarity measure recognizes the menu items accurately and ignores the problem of spaces and wrong word tag collected by noun chunk.

Menu item	Noun Chunk	Similarity Ratio	Description
스페셜 초밥	과 스페셜 초밥	86 %	Extra noun token
특 초밥	특초밥	86 %	Space missing
로로초밥	로초밥	86%	Token missing
회덮밥	회덮밥	100%	Full matched

Table 1: Similarity measure of menu items collected from review.

The sentences containing the food item names are collected and further processed for sentiment analysis.

C. Sentiment Analysis

Sentiment Analysis is the computational methodology used in the study of sentiments or opinions of people towards various entities like individuals, subjects or events [1]. Suppose, we have a product review, it figures out if the review is of positive polarity or negative polarity.

Many different techniques have been presented for analysis of sentiments in product reviews. These approaches are basically categorized into machine learning based and lexicon-based approaches. Machine learning based approaches include some supervised and unsupervised classification algorithms. Lexicon based methodologies consist of dictionary-based and corpus-based approaches.

In our work we have applied a lexicon-based approach in order to avoid the need to prepare a labeled training set. The main disadvantage of machine learning approach is their reliance on labeled data. It is extremely difficult to ensure that sufficient and correctly labelled data can be obtained. In this work, we have used the subjectivity lexicon MPQA corpus named KOSAC [7]. A subjectivity lexicon is a list of positive or negative opinion words.

Korean Sentiment Analysis Corpus (KOSAC) consists of 332 news articles taken from the Sejong Syntactic Parsed Corpus [6]. The corpus includes 7,713 sentence subjectivity tags and 17,615 opinionated expression tags based on the annotation scheme called KSML which reflects the characteristics of the Korean language. Examples of sentiment scores associated with KOSAC entries are shown in Figure 3.

ngram	freq	COMP	NEG	NEUT	POS	max.value	max.prop
가/JKS	1	0	0	0	1	POS	1
가/JKS;	1	0	0	0	1	POS	1
있/VV							
가/JKS;	1	0	0	0	1	POS	1
있/VV;							
있/EP							
가/VV	3	0	0	0	1	POS	1
가/VV;	1	0	0	0	1	POS	1
나 다							
/EF							

Figure 3: KOSAC tagging.

In our approach, we apply sentence-level scoring. Therefore, it is important that a phrase must contain a single food item. If a sentence contains multiple food items names, we first split the sentence into separate sentences to have only a single food item.

The sentiment analyzing algorithm takes POS tagged sentence as input and provides a scoring value for the positive, negative and neutral polarity of the sentence. The overall sentiment of the sentence is calculated based on the higher value of polarity. For example, if a positive polarity score is greater, the overall sentiment of the sentence is 1, for negative and neutral polarity would be -1 and 0 respectively. The overall sentiment score is then applied to the respective food item in the sentence.

The overall rating of the food menu item from the reviews is then calculated based on the obtained sentiment score using the following formula.

$$\text{Rating from reviews} = \sum_{k=1}^n \frac{(\text{sentiment score} * 5)}{\text{food_item_count}}$$

The calculated food item rating from reviews then applied to initial rating of the restaurant menu item to get final rating of the food item.

$$\text{FinalRating}_{\text{food_item}} = \frac{(\text{initial_rating} + \text{review_rating})}{2}$$

3. Results

The results from a restaurant reviews are shown in Figure 4, and 5. The sentences are taken from the reviews which contain those food item names which we are interested to evaluate and rating those food items in the restaurant menu list.

The words polarity shown in Figure 4, depicts % in terms of positive, negative and neutral words. However, positive words holds high ratio than the others & neutral remains with the least.

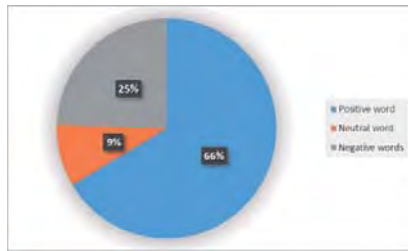


Figure 4: Words polarity.

The overall total rating is shown in Figure 5, the calculation of the total rating score is made on the basis of its initial rating and the calculated rating from the user reviews.

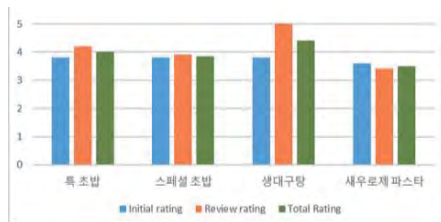


Figure 5: Initial, review and overall rating of food items.

The word cloud shown in Figure 6, visually shows the frequent words in review's sentences which contain a food item name.



Figure 6: Word cloud for frequent words in the sentences.

4. Conclusion and Future Work

Sentiment analysis is the process of identifying the feeling expressed in the text or document. We proposed a system for mining the restaurant and reviews data and to calculate score for the food items in the restaurant menu. It is evaluated the the proposed system has produced reasonable results in calculating the ratings for food items from user reviews. In future work, the NER technique would be applied on trained annotated corpus to identify all kinds of food items with more accuracy. A hybrid approach would be adopted by combining machine learning approach with existing approach to extract more features to handle implicit sentiment analysis and to identify deceptive reviews.

References

- [1] Lei Zhang and Bing Liu: "Sentiment Analysis and Opinion Mining" Encyclopedia of Machine Learning and Data Mining 2017.
- [2] Burusothman A., Paraneetharan S., Sanjith B., Thamayanthy S., Surangika R.: "Ruchi: Rating Individual Food Items in Restaurant Reviews" Intl. Conference on Natural Language Processing 2015.
- [3] Taboada, M., Brooke, J., Tofiloski, M., Voll, K., Stede, M.: "Lexicon-based methods for sentiment analysis." Computational linguistics 2011.
- [4] Pang B., Lee L., Vaithyanathan S.: "Thumbs up? Sentiment classification using machine learning techniques. Association for Computational Linguistics 2002.
- [5] Suchita V., Sachin N., Deshmukh: "Sentiment classification using machine learning techniques. International Journal of Science and Research 2013.
- [6] Hayeon J., Munhyong K., Hyopil S.: "KOSAC: A Full-Fledged Korean Sentiment Analysis Corpus" PACLIC 2013.
- [7] <http://word.snu.ac.kr/kosac/lexicon.php>

옷 추천 시스템 데이터 셋 구축을 위한 텍스트 데이터 마이닝

이주상*, 정선태**, 차준엽*
*송실대학교 대학원 정보통신공학과
**송실대학교 스마트시스템소프트웨어학과
ibmhbm2@naver.com, cst@ssu.ac.kr

Text Data Mining to build a Dataset for Clothing Recommendation System

Ju-Sang Lee*, Sun-Tae Chung**, Jun-Yup Cha
*Dept. of Information and Telecommunication Eng., Graduate School, Soongsil University
**Dept. of Smart Systems Software, Soongsil University

요 약

추천시스템은 대량의 정보를 이용하여 특정 사용자가 선호할만한 상품의 리스트를 추천하는 것이다. 현재 추천시스템으로 유명한 Netflix, Amazon, Youtube 등은 기업내의 상품 및 사용자 데이터를 토대로 이루어 졌으나 스타트업 및 소규모 기업이 추천 시스템을 구축하기 위해선 기반이 될 데이터셋 자체가 없으며 데이터 수집에도 한계가 있다. 본 논문에서는 옷 추천 시스템 구축을 위해 특정 기업만이 아닌 모든 의류매장들이 사용할 수 있는 데이터 셋 구축 방법에 대해 제안하며, 고객 데이터 셋 구축을 위한 텍스트 데이터 마이닝 처리 과정과 결과에 대해 기술한다.

1. 서론

추천 시스템은 여러 상품들중 특정 사용자가 가장 선호할만한 리스트만 찾아 추천하는 정보 필터링 시스템이다. 효과적인 추천 시스템 구축을 위해서는 추천 알고리즘의 성능과 충분한 양의 고객,상품 데이터가 필요하다. 알고리즘의 성능은 계산량이나 연산 속도뿐 아니라 빅데이터를 처리할 수 있는 환경인지를 고려해야한다. 예를 들어, 빅데이터 시스템이 구축되어 있다면 CF(Collaborative Filtering)나 DL(Deep Learning)을 사용할 수 있겠지만, 대량의 정보가 아니라면 오히려 성능이 떨어질수도 있기 때문이다[1]. 그리하여 전제조건이 되는 것이 고객 데이터와 상품 데이터이다. Netflix, Amazon, Youtube 등 추천 시스템을 적극 사용하고 있는 세계적인 대기업들은 그들만의 고객과 상품 데이터베이스를 기반으로 추천 알고리즘을 적용한다. 여기서 충분한 데이터가 없는 스타트업 및 중소기업은 추천 시스템 구축 이전에 콜드스타트 문제에 부딪치게 된다. 만약 추천 시스템을 위한 공공 데이터셋이 존재한다면 데이터가 없는 스타트업들

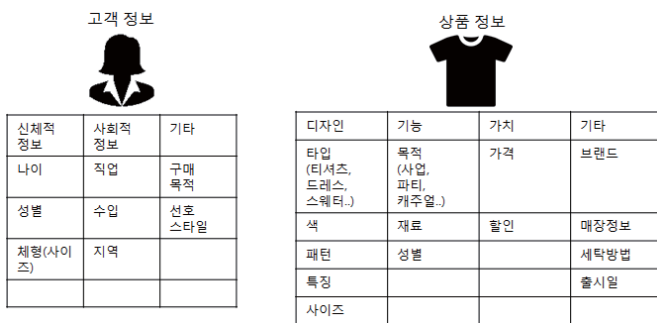
이 추천시스템 구축의 한계를 극복하는 것은 물론이며 이미 추천시스템을 적극 사용중인 기업이라도 연 구개발 목적으로 사용할 수 있을 것이다.

본 논문에서는 옷 추천 시스템을 위한 상품 및 고객 정보 데이터베이스 구축을 위해 Scrapy 기반의 웹 크롤러를 통해 Amazon, Yoox, Shopbop 등의 의류 페이지에서 상품 데이터와 리뷰 데이터를 수집하였고, 자연어 처리를 통한 리뷰 분석을 통해 리뷰 작성자의 정보와 상품에 대한 선호도를 알아내어 추천 시스템에 적합한 상품,고객 데이터셋을 구축하는 과정을 설명한다.

2. 제안 방법

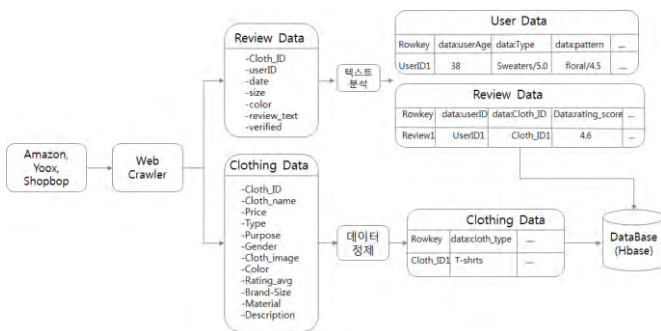
옷 추천 시스템을 위한 데이터 셋 구축을 위해 소비자 자신이 상품 구매를 결정하기까지 어떤 요인들이 영향을 끼치는지 고민하고 추천 시스템에서 필요로 하는 데이터의 성격을 파악해야 한다. 소비자들의 의류 제품 구매 결정 요인에 대한 관련 연구에서는 제품의 속성이 구매 결정에 유의미한 영향을 미치며 다른 요

인들은 제품의 표현적, 물리적 속성, 사진 효과, 연령 등의 순으로 영향력이 보인다고 말한다.[2] 추천 알고리즘은 특정 사용자가 특정 속성들에 대해 얼마의 평점(선호도)를 줬는지 계산하여 아직 구매하지 않은 상품을 그 사용자가 얼마나 선호할지 결정하는 것이 기본이며, 요즘은 더 나아가 상품의 특정 항목이 선호에 어떤 관계가 있는지를 알고리즘적으로 알아내는 잠재 모델 기반 추천 알고리즘이 많이 사용된다.[3] 추천 알고리즘에 적용할 것을 고려하여 추려낸 옷 추천 속성들은 <그림 1>의 표와 같다.



<그림 1> 추천에 영향을 미치는 속성

상품의 각 속성들에 대해 기존 사용자들의 구매내역이 있고, 그 사용자들의 프로필이 존재한다면 신규 고객이 원하는 상품도 기존 사용자들의 데이터를 기반으로 예측할 수 있을 것이다.



<그림 2> 옷 추천 시스템 데이터 셋 구축 프로세스

<그림 2>는 옷 추천 시스템 데이터 셋 구축 과정이다. 웹 크롤러는 Amazon, Yoox, Shopbop 등의 의류 페이지에서 앞서 정리한 추천 알고리즘을 위한 속성들을 상품 데이터로 수집해 상품 데이터 테이블을 구축하고 각 상품에 대한 리뷰 데이터를 분석해 사용자의 나이, 상품 선호도 등을 추출해 사용자가 상품의 각 속성에 매긴 평점과 사용자의 프로필을 가지고 있는 사용자 데이터 테이블과 리뷰 데이터 테이블을 만든다. 상품, 사용자, 리뷰 데이터 테이블의 관계는 사용자의 구매 기록, 상품에 대한 평점이 되면서 <표 1>과 같이 고객 D의 상품 1에 대한 선호도를 예측할 때 고객들의 상

품 구매내역과 평점을 기반으로 고객들간의 유사성을 계산하여 고객 D가 상품 1에 대해 얼마 만큼의 선호도를 가질지 예측할수 있는 CF 기반 추천 알고리즘을 위한 기본 데이터 셋이 구성된다.

	상품 1	상품 2	상품 3	상품 4
고객 A	5	3	2	
고객 B	4	4		5
고객 C	2		4	3
고객 D	?	4	3	3

<표 1> 추천시스템의 평점 테이블 예

2-1. 데이터 수집

초기 데이터는 Scrapy[4]를 기반으로 작성한 웹 크롤러를 사용하여 Amazon[5], Yoox[6], Shopbop[7]등에서 300,000 개 가량의 상품 데이터와 리뷰 데이터를 수집하였다. 상품 데이터는 별도의 분석과정을 거치지 않으나 <표 2>와 같이 서로 다른 웹 페이지인 만큼 같은 데이터도 다르게 표기가 되었으며 일부 상품 정보 업로드가 글 작성자의 주관적인 생각으로 작성되기 때문에 't shirt midi dress'와 같이 타입이 구체적으로 명시되지 않거나 같은 'blue'색상에 대해서도 'navy blue', 'cobalt blue' 등 유사 데이터도 많이 존재한다. 향후 추천 시스템에서 쉽게 분석하고 검색이 용이하게 유사 데이터는 통합하고 구체적이지 못한 데이터는 하나의 형태로 교정하는등 정제를 거친후 데이터베이스에 저장한다.

웹페이지 속성	Amazon	Yoox	Shopbop
사이즈	Small, Medium, Large	46, 48, 50	S, M, L
가격	\$ 90.00	\$90.00	US\$90.00
타입	T-Shirts	t-shirt	Tops
색상	Navy Blue	Blue	Cobalt blue
옷 이름	High waist T shirt midi dress with pockets	PRADA	SUNDRESSES

<표 2> 수집한 직후의 데이터 형태

2-2. 리뷰 데이터 분석

추천을 위해 고객의 데이터는 그동안의 구매내역과 구매한 상품에 대한 평점(선호도), 상품에 대한 평점은 더 나아가 상품의 어떤 속성이 선호에 영향을 미치는지도 고려하기 위해 상품의 각 속성에 대한 선호도까지 고려할 수 있다. 또한 앞서 추천 알고리즘에 들어갈 속성으로 정의했던 나이, 성별, 체형 등의 정보를 생각할 수 있다. 본 연구에서는 나이, 성별, 체형 세가지 속성들중 성별은 구매한 상품내역의 데이터에서 추출할수 있었고 체형은 고객이 직접 이미지를 업로드 하지 않으면 분석이 불가능했기에 제외하고 자연

어 처리를 기반으로 리뷰 작성자의 나이를 분석하고 상품에 대한 선호도를 분석하였다. 딥 러닝 기반 자연어 처리 분석 모델을 통해 리뷰 텍스트로부터 원하는 정보를 추출하며 <그림 3> 과 같은 과정을 거친다.



<그림 3> 고객 데이터 분석 자연어 처리 과정

본 연구에서는 23485 개의 의류 상품 리뷰, 평점, 카테고리, 작성자 나이 등의 정보가 있는 Women's E-Commerce review data[8]과 1,600,000 개의 트위터 글과 트윗에 대한 작성자의 감정 지표가 있는 Sentiment 140 dataset with 1.6million tweets[9]를 훈련 데이터 셋으로 사용하였다.

2-2-1 데이터 전처리

분석할 용도에 맞게 텍스트를 사전 처리하는 작업을 한다. 데이터 전처리를 위해 딥 러닝을 위한 Python 라이브러리 Keras 와 자연어처리를 돕는 여러 툴을 제공하는 NLTK 라이브러리를 사용하였다.

불용어처리: 'I', 'You', 'it'과 같이 문장내에 등장 빈도가 높으나 본 연구의 텍스트 분석 목적에 있어서 의미를 갖지 않는 단어들이 있다. NLTK 가 정의한 불용어를 사용하여 이러한 단어들을 제거한다.

정제/정규화: 분석에 영향을 주지 않는 특수문자, 구두점등을 제거하고 결측, 이상이 있는 데이터는 훈련에 잘못된 영향을 줄 수 있어 이러한 데이터들을 제거한다.

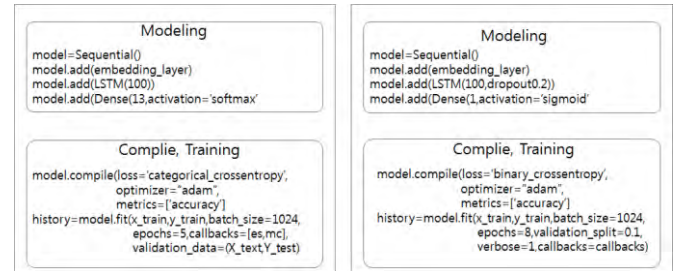
토큰화: 주어진 텍스트 데이터를 분석에 의미를 가지면서 가장 작은 단위로 나누는 것을 토큰화라고 한다. 여기서는 토큰의 기준을 단어로 정하였다.

워드임베딩: 자연어처리를 위해 필요한 과정으로 토큰화한 단어들에 실수를 부여하고 벡터화하는 것을 말한다.

2-2-2 자연어 처리 모델

컴퓨터가 분석할 수 있도록 하기 위해선 단어를 숫자화 시키는 워드임베딩 과정이 필요하다. Word2Vec 모델은 주어진 문장에서 모든 단어의 의미를 벡터화

하여 단어간 유사도를 반영한다.[10] 벡터화된 데이터는 분석 모델에 임베딩 층으로 들어간다.

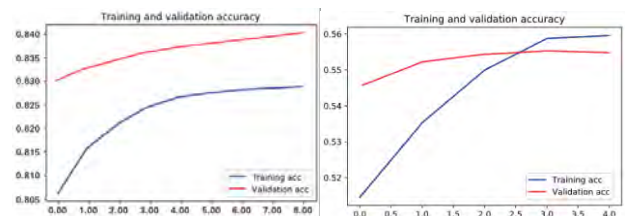


<그림 4> 나이분석, 선호도 분석 모델과 컴파일

텍스트 분석 모델은 <그림 4>와 같이 구성된다. embedding_layer 는 앞서 구성한 벡터화된 데이터로 인공 신경망의 층의 하나로서 추가된다. Dense()는 전결합층을 추가하는 것이다. 첫번째 인자는 출력 뉴런의 수, 두번째 인자는 출력층에 사용되는 함수를 의미한다. 나이 분석의 경우 더 간결하고 확실한 결과를 출력하기 위해 나이를 5 세 단위로 레이블을 나눴다. 따라서 레이블 만큼의 수가 들어간다. 선호도 분석의 모델의 경우 0 에서 1 사이의 실수 결과를 출력하며 1 에 가까울수록 선호도가 높음을 의미한다. 출력되는 결과는 한가지이기 때문에 1 이 입력된다. 그리고 각각 다중 클래스 분류와 이진 분류 문제에서 주로 사용되는 Softmax 함수와 sigmoid 함수를 적용하였다. model.compile()과 model.fit()은 각각 모델링한 신경망을 컴파일하고 훈련시키는 과정이다. 데이터의 크기를 고려하여 과적합 방지를 위해 훈련회수를 각각 5, 8 로 진행하였다.

3. 결과

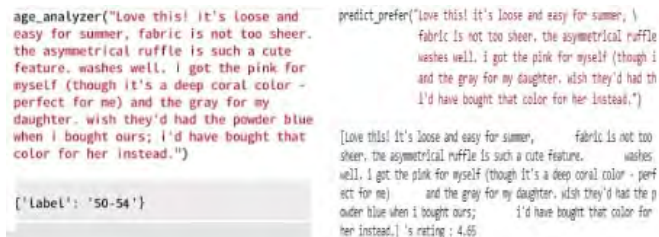
훈련용으로 사용한 데이터 셋을 8:2 비율로 나눠 8 은 훈련에 사용했으며 2 는 정확도 검증을 위한 테스트 데이터로 사용하였다. <그림 4>는 학습한 모델의 평가 결과를 나타낸다.



<그림 5> 선호도분석(좌) 나이분석(우)의 테스트 정확도

선호도 분석과 나이 분석의 평가 정확도는 각각 84%와 55%로 나타났다. 큰 차이의 정확도를 보인 원인은 데이터 셋의 규모 차이로 생각된다. 선호도 분석은 1,600,000 개의 충분한 양의 데이터 셋을 바탕으로

로 84%의 정확도를 보인것으로 여겨지며, 나이 분석의 경우 23,000 개 가량의 데이터는 텍스트로부터 단어가 내포하는 연령대별 특징 및 유사도를 계산할만한 충분한 크기의 데이터가 아니었던 것으로 생각된다. <그림 6>은 구현한 모델들을 사용하여 텍스트를 입력했을때 모델의 출력값을 보여준다.



```

age_analyzer("Love this! It's loose and easy for summer, fabric is not too sheer. the asymmetrical ruffle is such a cute feature. washes well. i got the pink for myself (though it's a deep coral color - perfect for me) and the gray for my daughter. wish they'd had the powder blue when i bought ours; i'd have bought that color for her instead.")
{'Label': '50-54'}

predict_prefer("Love this! It's loose and easy for summer, fabric is not too sheer. the asymmetrical ruffle washes well. i got the pink for myself (though i and the gray for my daughter. wish they'd had th i'd have bought that color for her instead.")
[Love this! It's loose and easy for summer, fabric is not too sheer. the asymmetrical ruffle is such a cute feature. washes well. i got the pink for myself (though it's a deep coral color - perfect for me) and the gray for my daughter. wish they'd had the powder blue when i bought ours; i'd have bought that color for her instead.] 's rating : 4.65
  
```

<그림 6> 나이 분석과 선호도 분석의 출력결과

4. 결론

본 논문에서는 옷 추천 시스템을 위해 데이터를 수집하여 상품 데이터 셋을 구축하고, 텍스트 분석을 통한 고객 프로필 데이터 셋 구축 방법을 추천 시스템을 위한 기반 데이터 셋 구축 방법을 제안했다. 텍스트를 통한 나이 분석 단계에서 충분한 정확도에 도달하지 못하여 고객 데이터를 온전히 구축하지 못하였다. 그러나 나이 분석 모델의 정확도가 적은 양의 데이터 셋으로 얻은 결과라는 점을 감안했을때, 향후 충분한 훈련 데이터 셋이 확보된다면 더 유의미한 결과를 도출해낼 수 있을 것으로 판단된다. 앞으로는 SNS에서 업로드한 이미지를 기반으로 이미지 데이터 분석을 진행하여 추천 시스템을 위한 질 높은 데이터 수집을 계속 할 계획이다. 연구가 계속 성과를 보인다면 콜드스타트 문제에 직면해있는 스타트업도 활용 가능한 추천시스템 공공 데이터 셋 구축이 가능해질 것이라 생각한다.

참고문헌

- [1] Sanjeevan Sivapalan, Alireza Sadeghian, Hossein Rahnama, Asad M. Madni, Recommender systems in e-commerce, 2014 World Automation Congress(WAC), p179-184,2014
- [2] 지혜경, 인터넷 쇼핑몰에서의 의류제품 구매결정 요인, 한국의상디자인학회지, 14(2) p185-189
- [3] 한국콘텐츠진흥원, <방송 트렌드 &인사이트> 2016년 4,5 월호(vol.05): 콘텐츠 추천 알고리즘의 진화
- [4] Scrapy, <https://docs.scrapy.org/en/latest/>
- [5] Amazon, Men's Fashion, Women's Fashion, https://www.amazon.com/ref=nav_logo
- [6] Yoox, <https://www.yoox.com/kr>
- [7] Shopbop, <https://www.shopbop.com/>
- [8] Women's E-commerce Clothing Reviews, <https://www.kaggle.com/nicapotato/womens-ecommerce-clothing-reviews>
- [9] Sentiment140 dataset with 1.6million tweets, <https://www.kaggle.com/kazanova/sentiment140>
- [10] Justin Garten, Kenji Sagae, Volkan Ustun, Morteza Dehghani, Combining Distributed Vector Representations for Words, Associations for Computational Linguistics, Proceedings of the 1st Workshop on Vector Space Modeling for Natural Language Processing, Pages 95-101, 2015

효과음 자막 생성을 위한 딥러닝 기반의 다중 사운드 분류

정현영*, 김규미*, 김현희*

*동덕여자대학교 정보통계학과

gusdud4573@gmail.com, kyume9@gmail.com, heekim@dongduk.ac.kr

A Multiclass Sound Classification Model based on Deep Learning for Subtitles Production of Sound Effect

Hyeonyoung Jung*, Gyumi Kim*, Hyon Hee Kim*

*Dept. of Statistics and Information Science, Dongduk Women's University

요 약

본 논문은 영화에 나오는 효과음을 자막으로 생성해주는 자동자막생성을 제안하며, 그의 첫 단계로써 다중 사운드 분류 모델을 제안하였다. 고양이, 강아지, 사람의 음성을 분류하기 위해 사운드 데이터의 특징벡터를 추출한 뒤, 4가지의 기계학습에 적용한 결과 최적으로 델로 딥러닝이 선정되었다. 전처리 과정 중 주성분 분석의 유무에 따라 정확도는 81.3%와 33.3%로 확연한 차이가 있었으며, 이는 복잡한 특징을 가지는 사운드를 분류하는데 있어 주성분 분석과 넓고 깊은 형태의 신경망이 보다 개선된 분류성능을 가져온 것으로 생각된다.

1. 서론

배리어프리영화(이하 배리어프리영화)란, 기존의 영화에 화면을 음성으로 설명해주는 해설과 자막 및 대사, 음악, 소리정보를 알려주는 자막을 넣어 모든 사람이 함께 즐길 수 있도록 만든 영화이다. 기존의 영화에서는 배우의 대사를 자막으로 생성하지만 효과음, 음악 소리, 동물 소리와 같은 대사 이외의 다양한 소리는 자막으로 제공되지 않는다. 따라서 배리어프리 영화가 일반화되면 청각 장애인도 보다 풍부한 소리를 자막으로 서비스 받을 수 있게 될 것이다.

현재의 자막 생성기술인 음성 인식(Speech To Text, STT) 기술은 대사만을 자막으로 생성해 낸다는 점에서, 대사 이외의 음향효과와 같은 소리 정보를 알리는 자막이 필요한 배리어프리영화에 적용하기엔 부족한 점이 있다. 따라서 본 논문은 화면에 나타나지 않은 소리정보도 자막으로 나타내는 사운드 기반의 자막 생성을 위한 다중 사운드 분류 모델을 제안하였다.

본 연구에선 강아지, 고양이, 사람의 사운드 데이터를 수집 후 고속 푸리에 변환(Fast Fourier Transform)을 적용하고 주성분 분석(PCA)을 통해

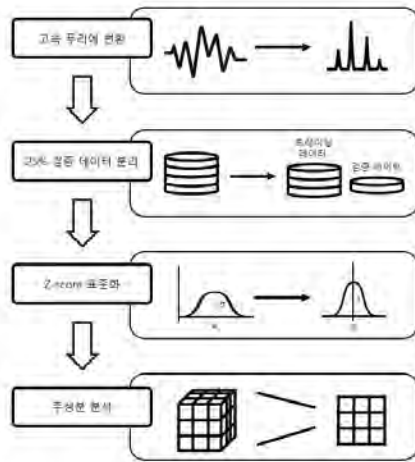
사운드의 특징을 추출하였다. 다음으로 다중 클래스 사운드 분류에 적절한 기계 학습 모델을 찾아내기 위해서, 가우시안 나이브 베이즈, 로지스틱 회귀, 랜덤 포레스트, 딥러닝까지 총 4가지 기계학습 모델을 적용하였다. 네 가지 모델의 분류 정확도를 비교한 결과, 주성분 분석을 적용한 딥러닝 모델이 81.3%의 정확도로 가장 높은 성능을 내는 것을 알 수 있었다.

제안한 모델을 활용하여 분류된 효과음을 자막으로 생성하면, 동물의 소리도 자막으로 볼 수 있어 청각 장애인들을 위한 자막 서비스가 보다 생동감있게 제공될 수 있을 것으로 기대된다.

2. 데이터 전처리

[그림 1]은 데이터 전처리 과정을 나타낸 것이다. 고양이 167개, 강아지 112개, 사람 100개의 사운드 데이터를 트레이닝 데이터로 수집했으며, 테스트 데이터로는 각 클래스별로 50개씩의 사운드 데이터를 「내 어깨 위 고양이, 밥」, 「화이트 갓」 등 다양한 영화로부터 추출하여 활용했다. 이때, 사람의 사운드 데이터는 여성 50%, 남성 50%로 동일하게 수집하였으며, 연령별 사운드의 차이를 고려하여 각

아이 15%, 성인 20%, 노인 15%로 연령대를 고르게 수집하였다.



[그림 1] 데이터 전처리 프로세스

다음으로 고속 푸리에 변환을 사용하여 데이터로부터 시간적 흐름의 소리 정보를 주파수의 흐름으로 변환하였다. 고속 푸리에 변환 기법[1]을 이용하면 임의의 신호를 수학적 변수로 변환할 수 있기 때문에 현재 음성분석, 지진파 분석 등 신호 분석에서 널리 사용되고 있다.

```
array([[ 15.30645979,  26.27110801,  30.61643619, ..., -54.33958484,
        -54.34032627, -54.33370308],
       [ 1.94797151,  29.3065174 ,  32.65448653, ..., -61.55720458,
        -61.59933568, -61.58510577],
       [ 8.62795442,  22.80452313,  22.9281394 , ..., -67.47438591,
        -67.46644165, -67.48636664],
       ...,
       [-1.01850621,  1.22566043, -5.30150667, ..., -43.20566552,
        -38.67296109, -42.82643031],
       [ 28.73957227,  35.47679534,  36.72878961, ..., -44.69949798,
        -44.70262766, -44.7064108 ],
       [-8.40316883, -21.84247719, -8.28662848, ..., -56.40225397,
        -56.3708293 , -56.36798461]])
```

[그림 2] 고속 푸리에 변환한 형태의 데이터프레임

[그림 2]는 고속 푸리에 변환을 통해 계산된 사운드 데이터이다. 고속 푸리에 변환을 통해 사운드 데이터를 샘플링 된 특징값으로 추출하여 기계학습에 적용하였다.

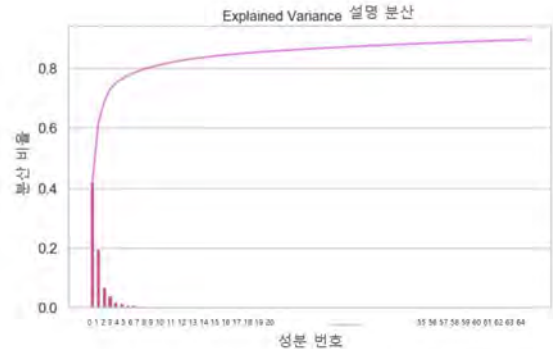
[표 1] 데이터 분리 표

	트레이닝	검증	테스트
고양이	125	41	50
강아지	83	29	50
사람	75	25	50

[표 1]은 고속 푸리에 변환된 트레이닝 데이터의 각 분류별 25%를 검증 데이터로 분리해 준 전체 데

이터의 개수이다. 테스트 데이터에 적용하기 전, 모델을 검증하기 위한 검증용 데이터와 트레이닝 데이터는 Z-score 표준화와 주성분 분석을 각각(따로) 진행하였다.

데이터를 효과적으로 분류하기 위하여 Z-score 표준화(Standard Scaler)한 후 주성분 분석(Principal Component Analysis)을 통해 차원을 축소하였다.



[그림 3] 트레이닝 데이터의 설명 분산

[그림 3]은 각각의 주성분 벡터가 이루는 축에 투영한 결과의 분산의 비율과 누적비율을 나타낸다. 이를 통해 방향벡터가 큰 6개의 성분(component)을 주성분으로 선택하여 입력 데이터로 사용하였다.

3. 성능비교 및 최적모델 선정

[표 2] 모델 별 정확도 비교

모델	검증 정확도	테스트 정확도
가우시안 나이브 베이즈	0.874	0.513
랜덤 포레스트	0.874	0.593
로지스틱 회귀	0.916	0.773
딥러닝	0.884	0.813

[표 2]는 가우시안 나이브 베이즈, 랜덤 포레스트, 로지스틱 회귀, 딥러닝 총 4가지 모델에 트레이닝 데이터와 테스트 데이터를 넣은 후 정확도를 보여준다. 로지스틱 회귀 모델에서 검증 정확도가 91%를 넘겨 가장 최적모델로 보이는 듯 했으나, 테스트 데이터에 적용하였을 때는 77%로 나타났다.

반면 검증 정확도에서 두 번째로 높은 성능을 보인 딥러닝 모델의 경우, 테스트 데이터에 적용하였을 때 81%의 정확도가 나타남으로써 이를 최적모델로 선정하였다.

4. 제안한 딥러닝 모델

[표 3] 제안한 딥러닝 모델의 분류별 인식률

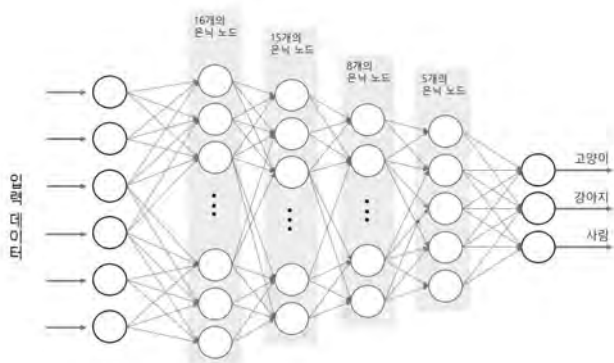
정확도 점수 : Accuracy Score: 0.813				
	정밀도 precision	재현율 recall	F1 점수 f1-score	support
고양이 cat	0.70	0.80	0.75	50
강아지 dog	0.87	0.78	0.82	50
사람 people	0.90	0.86	0.88	50
정확도 accuracy			0.81	150
macro avg	0.82	0.81	0.82	150
weighted avg	0.82	0.81	0.82	150

[표 3]는 테스트 데이터를 최적모델에 적용한 결과를 클래스별로 정밀도(precision), 재현율(recall), F1-score, 그리고 지지도(support)를 나타낸 표이다.

강아지와 사람은 각 82%와 88%로 높은 F1-score를 보였지만, 고양이는 75%로 비교적 낮은 F1-score를 보였다.

또한 추가적인 연구에 고양이와 강아지 소리가 동시에 나오는 테스트 데이터를 넣어 주었을 때, 강아지로 인식하는 것으로 보아, 강아지의 소리가 인식이 더 잘 되는 것을 알 수 있었다.

사람의 사운드 데이터의 경우, 트레이닝 데이터의 언어가 전부 영어로 이루어져 있으며, 테스트 데이터의 언어도 영어로 이루어져 있어 높은 F1-score를 보였다. 하지만 다른 언어가 테스트 데이터로 들어왔을 때는 낮은 F1-score를 보였다. 이로 인해 사람의 사운드와 다른 사운드를 분류할 때 다양한 언어로 학습하는 것이 중요한 요소임을 알 수 있었다.



[그림 4] 제안하는 딥러닝 모델의 구조

[그림 4]는 다중 사운드 분류를 위한 5층으로 구성된 완전연결구조의 딥러닝 모델의 학습과정을 나타낸다. 고속 푸리에 변환(FFT) 함수로 계산하여 주성분 분석을 적용한 데이터는 6개의 입력 노드를 거친다. 은닉층의 노드가 16, 15, 8, 5로 구성된 본

모델은 활성화 함수로 'relu'를 사용하고 있으며, 가중치 최적화를 위한 함수는 'adam'을 적용하였고, 고양이, 강아지, 사람을 분류하기 위해 3개의 출력 노드를 가지고 있다. 최대 학습 횟수는 200회로 설정하였으며, L2 규제를 위한 매개 변수인 알파(alpha)값은 0.015로 설정해주었다.

[표 4] 주성분 분석 적용에 따른 딥러닝 모델 성능비교

딥러닝 모델	검증 정확도	테스트 정확도
주성분 분석을 적용한 딥러닝 모델	0.884	0.813
주성분 분석을 적용하지 않은 딥러닝 모델	0.432	0.333

주성분 분석을 적용하지 않은 딥러닝 모델과 성능을 비교하였을 때, 전처리 단계에서 주성분 분석을 거친 모델과 확인한 성능차이가 있었다. 이는 고속 푸리에 변환된 수많은 값을 동일한 가중치로 넣어주는 것 보다 특징벡터를 분석한 후 입력 데이터로 넣어 주는 것이 더 효과적으로 보여 진다.

5. 다중 사운드 분류의 응용

본 연구에서 제안한 다중 사운드 분류 모델을 자막생성에 활용한다면 효과음도 자막으로 생성해 낼 수 있다. 또한 본 연구의 모델은 고양이, 강아지, 사람으로 이루어진 3개의 클래스로만 분류를 해냈지만, 향후 데이터의 확대를 통해 더 다양하고 세밀한 효과음까지 자막으로 표현할 수 있으리라 기대한다.



[그림 5] 다중 사운드 분류의 응용 예시

[그림 5]는 다중 사운드 분류모델을 영화에 적용하였을 때의 상황을 나타낸 것이다. 대사만을 자막

으로 나타내는 것이 아닌, 고양이나 강아지 소리도 자막으로 나타내면서 청각장애인의 영화 이해도를 높일 수 있으며, 풍성한 상황해설을 할 수 있다.

6. 결론 및 기대효과

본 논문은 대사 뿐 아니라 효과음도 자막으로 나타낼 수 있는 사운드 기반 자동 자막 생성을 제안하며, 이의 첫 단계로 다양한 사운드를 분류해 낼 수 있는 다중 사운드 분류 모델을 연구하였다.

사운드 데이터의 경우 복잡한 특징벡터를 가지고 있기 때문에 단순한 기계학습보다 딥러닝 모델에서 더 좋은 분류 결과를 보였으며, 주성분 분석 과정을 통하여 분류에 큰 영향을 미치는 성분을 추출하였다. 이를 딥러닝 모델에 적용했을 때, 주성분 분석을 적용하지 않은 모델에 비해 월등히 좋은 성능을 나타냈다는 점에서, 사운드 데이터를 분류하는데 특징벡터의 분석과정이 큰 의미가 있음을 알 수 있었다.

본 연구의 다중 사운드 분류 모델은 81% 정확도라는 결과를 냈으나, 영어가 아닌 언어의 데이터를 넣었을 때 성능이 크게 떨어졌다는 것을 고려하면 데이터셋의 확대가 이루어졌을 때 더 좋은 성능을 낼 수 있을 것이라 기대된다. 또한 향후 자동 자막 생성 기술과 접목된다면 대사 뿐 아니라 화면에 나타나지 않는 사운드까지 자막으로 나타낼 수 있다는 점에서 배리어프리영화에 적용하여 원활한 영화 공급 및 취약계층이 문화적 권리를 향유하는데 큰 도움이 될 것이라 기대된다.

참고문헌

- [1] 김형석, 김인태 “고속푸리에변환을 이용한 부식 강재의 응력집중계수 산출”, 대한토목학회 정기학술대회, 2018, pp.569-570
- [2] 최재승 “남녀성별 분류를 위한 화자종속 음성 인식 알고리즘”, 한국정보통신학회논문지, Vol.17, No.4, pp.775-780, 2013
- [3] 박대서, 방준일, 김화중, 고영준 “CNN을 이용한 음성 데이터 성별 및 연령 분류 기술 연구”, 한국정보기술학회논문지, Vol.16, No.11, pp.11-21, 2018
- [4] 김지은, 이인성 “MFCC를 이용한 GMM 기반의 음성/혼합 신호 분류”, 전자공학회논문지, Vol.50 No.2, pp.185-192, 2013
- [5] 금지수, 임성길, 이현수 “스펙트럼 분석과 신경망을 이용한 음성/음악 분류”, 한국음향학회지, Vol. 26, No.5, pp.207-213, 2007
- [6] 정명범, 고일주 “오디오의 파형과 FFT 분석을 이용한 대표 선율 검색”, 정보과학회논문지 : 소프트웨어 및 응용, Vol.34, No.12, pp.1037-1044, 2007

온라인 행동정보를 이용한 협업 필터링

곽지윤, 김가영, 홍다영, 김현희

동덕여자대학교 정보통계학과

jeeyoon3848@gmail.com, ga20171001@gmail.com, dayoung0308@daum.net,

heekim@dongduk.ac.kr

BICF : Collaborative Filtering Based on Online Behavior Information

Jee-yoon Kwak, Ga-veong Kim, Da-voung Hong, Hvon Hee Kim
Department of Statistics and Information Science,
Dongduk Women's University

요 약

현재 전자상거래에서 사용되는 협업 필터링은 고객이 입력한 평점 정보를 이용하여 추천 시스템을 구축한다. 하지만 기존의 평점 정보는 고객이 직접 입력해야 하므로 데이터 희소성의 문제가 있고 허위정보를 가려내지 못한다는 문제점 또한 존재한다. 본 논문에서는 기존 평점 정보 기반의 협업 필터링 추천 시스템의 문제점을 해결하기 위해, 온라인 고객 행동 정보를 활용한 협업 필터링 알고리즘을 제안하였다. 실험 결과 본 연구에서 제안한 Collaborative Filtering based on Online Behavior Information (BICF) 알고리즘이 기존의 평점 기반 협업 필터링 방식보다 우수한 성능을 보임을 보여주었다.

1. 서론

온라인 고객 행동 정보란 전자상거래에서 고객이 구매에 이르기까지 정보를 뜻하며, 제품 검색, 장바구니 추가 및 삭제, 구매 시도 등 다양한 온라인 상의 이벤트를 뜻한다. 이러한 온라인 고객 행동 정보는 암시적으로 나타나는 고객의 고유한 소비 패턴을 찾을 수 있다. 온라인 행동 정보를 활용하여 고객의 구매성향을 파악하는 것은 더욱 개인화된 서비스를 제공하고 더 세분화된 추천을 가능하게 한다. 또한 외부적으로 입력을 해야 하는 평점 정보와 달리 전자상거래를 사용하는 모든 사용자의 정보를 활용할 수 있으므로 데이터 희소성의 문제를 해결할 수 있다.

기존의 협업 필터링은 고객이 상품을 구매하고 그에 대한 평점을 매기면 이 평점 정보를 이용해서 상품을 추천한다. 평점 정보를 생성할 권한은 고객에게 있기 때문에 모든 아이템에 대한 평점을 얻을 수 없을 뿐만 아니라 평점 정보를 갖지 않는 신상품이나 인기있는 상품이 아닌 경우는 추천이 되지 않는 문제도 발생할 수 있다. 이런 제품의 경우 고객의 반응을 이끌어내기 위한 많은 노력이 필요하다. 또한 평점 정보는 고객의 주관적인 선호도와 만족도를

나타내고 간혹 거짓 정보를 포함하기 때문에 추천 시스템의 예측 성능을 저하시키는 요인이 된다.

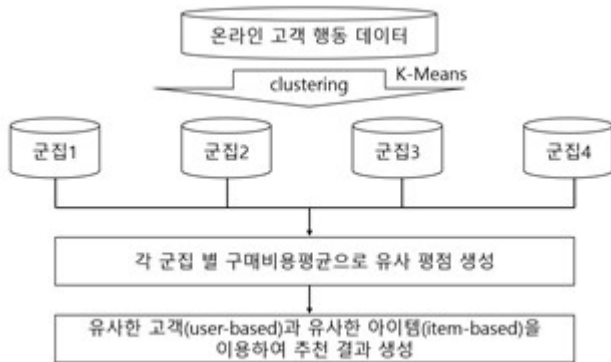
본 논문에서는 온라인 고객 행동 정보를 활용하여 기존의 평점 정보 시스템을 개선한 새로운 추천 시스템인 BICF알고리즘(Behavior Information based Collaborative Filtering)을 제안하였다. 먼저 고객의 온라인 행동을 기반으로 구매 패턴을 파악하고 세분화하기 위해 분석 단위를 세션별로 나누어 전처리를 진행하였다. 다음으로 다양한 온라인 행동 정보를 하나의 압축된 평점 정보로 나타내기 위해 k-means 클러스터링으로 데이터를 군집화하였다. 군집화된 네 가지 소비성향의 구매 금액 평균을 이용하여 유사평점 데이터를 생성하고, 이를 기반으로 협업 필터링을 진행하였다.

협업 필터링 과정에서는 BICF 알고리즘의 성능향상을 증명하기 위해 사용자 기반 협업 필터링과 아이템 기반 협업 필터링 모두 실험에 사용하였다. 마지막으로, 기존의 협업 필터링 시스템과 BICF 알고리즘을 비교하여 모델의 성능을 평가하였고, 그 결과 BICF 알고리즘이 기존의 방법보다 더 높은 정확도를 보임을 보여주었다.

제안하는 BICF 알고리즘은 고객의 온라인 행동 정보를 활용함으로써 기존의 추천 시스템에서 전형적

으로 나타나는 데이터 희소성의 문제와 평점 정보가 충분하지 않은 제품의 추천 문제를 해결할 수 있는 방안으로 활용될 수 있을 것으로 기대된다.

2. BICF 기반 추천 시스템 구조



<그림 1> BICF 기반 추천 시스템

<그림 1>은 제안하는 BICF 기반 추천 시스템의 구조를 보여준다. 먼저 L.point에서 제공하는 익명화된 3,196,362개의 온라인 행동 정보를 구매확정인 22,239개의 데이터로 분석 범위를 줄이고 고객을 세션 단위로 세분화하여 더 세밀하고 개인화된 분석이 가능하게 하였다.

고객 세분화를 위해 K-means 클러스터링을 실시하였는데, 클러스터링 과정으로 들어가기 전 유의미한 온라인 행동 정보 변수인 세션에 머문 시간, 유입 경로, 총 페이지 방문 횟수, 유입 기기, 구매 시간대를 뽑아 전처리를 진행하였다. 명목형 변수는 숫자를 부여하여 one-hot-encoding을 적용하였고, 수치형 변수는 MinMaxScaler를 이용하여 정규화하였다. 전처리된 명목형 변수와 수치형 변수를 하나의 입력으로 처리하기 위해 pipeline을 적용하였다.

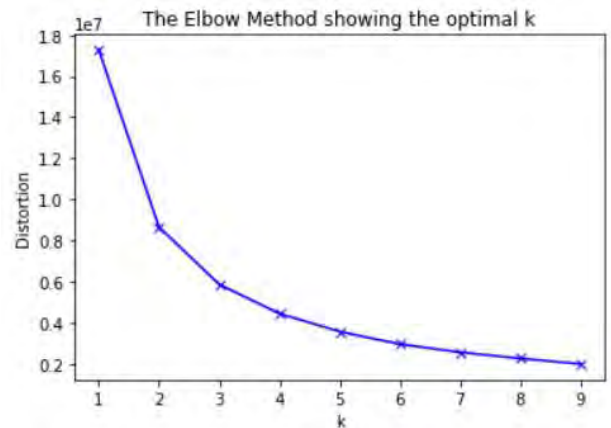
K-means 클러스터링을 이용하여 고객을 네 그룹의 세분화된 군집으로 나누고, 군집별 평균 구매비용을 각 제품에 대한 평점으로 생성하였다. 마지막으로 생성된 평점을 활용하여 사용자 기반 추천과 아이템 기반 추천에 적용하였으며, 이후 성능평가를 진행하였다.

3. BICF 알고리즘

3.1 온라인 행동 정보를 이용한 스코어 생성

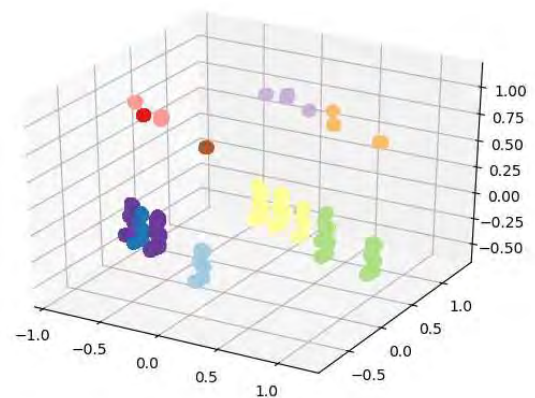
여러 개의 변수를 하나의 평점 데이터로 바꾸기 위

해 행동 정보를 kmeans로 군집화하여 비슷한 고객 그룹으로 나누었다. 클러스터의 개수를 지정하기 위해 엘보우 기법을 사용하여 최적의 군집 개수를 정하였다. 엘보우 기법이란 클러스터 개수에 따라 SSE(오차 제곱합) 값을 그려주는 함수로 다음과 같은 엘보우 그래프를 얻을 수 있었다. <그림 2>에서 볼 수 있는 바와 같이 군집의 개수 3과 4에서 좋은 군집을 찾을 수 있다.



<그림 2> 군집 개수를 정하기 위한 엘보우 그래프

최적의 군집 개수를 정하기 위해 군집의 결과를 시각화해 보았다. <그림 3>에서 볼 수 있는 바와 같이 3개의 군집일 경우보다 4개의 군집일 경우가 보다 명확하게 군집이 분리되므로 고객 그룹을 4개의 그룹으로 세분화하였다.



<그림 3> 고객 군집 결과

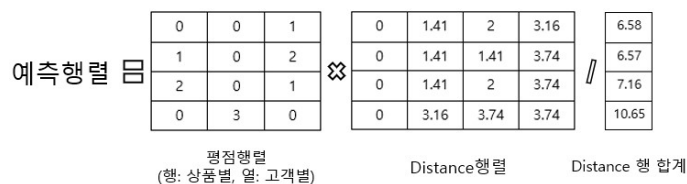
행동 정보로 생성한 클러스터를 협업 필터링에 적용하기 위해 명목형이었던 클러스터를 buy_am(총구매비용)의 평균값으로 오름차순으로 정렬하여 순서형 데이터인 평점 정보로 바꾸었다.

3.2 온라인 행동 정보 기반 협업 필터링 알고리즘

평점 정보를 기반으로 특정 고객과 유사한 성향을 지닌 다른 고객이 산 아이템을 추천하는 사용자 기반(User-based) 협업 필터링과 고객이 관심을 가진 아이템과 비슷한 아이템을 추천하는 아이템 기반(item-based) 협업 필터링을 구현하였다.

사용자 기반 협업 필터링의 구현은 다음과 같이 진행된다. 앞서 변형한 평점 정보 데이터를 활용하여 다중 차원 배열의 평가 행렬로 표현하였다. 사용자 기반 협업 필터링의 경우, 아이템에 대한 사용자 평가를 해당 아이템의 다른 모든 사용자 평가에 대한 가중치의 합으로 예측하였다. 알려지지 않은 사용자의 평가를 예측하기 위해서 사용자 기반 협업 필터링은 두 단계를 거친다. 먼저 고객 간의 유사도 행렬을 생성한다. 유사도는 sklearn에서 제공되는 코사인 유사도를 활용했다. 이렇게 형성된 고객 간의 유사도 행렬과 분할된 평점 행렬의 내적을 구하고 평가 수의 데이터를 정규화하여 알려지지 않은 평가를 예측하였다.

아이템 기반 협업 필터링은 앞서 설명한 사용자 기반 협업 필터링과 유사하지만 유사도 계산 부분에 약간의 변형을 주어 두 단계로 진행하였다. 먼저 K-NearestNeighbors 알고리즘을 활용하여 아이템 간의 코사인 유사도를 계산한 후 아이템 유사도 행렬을 생성하였다. 그 다음 평점이 없는 아이템을 예측하기 위해서 사용자 기반 협업 필터링과 같은 방법으로 아이템의 평점을 예측하였다.



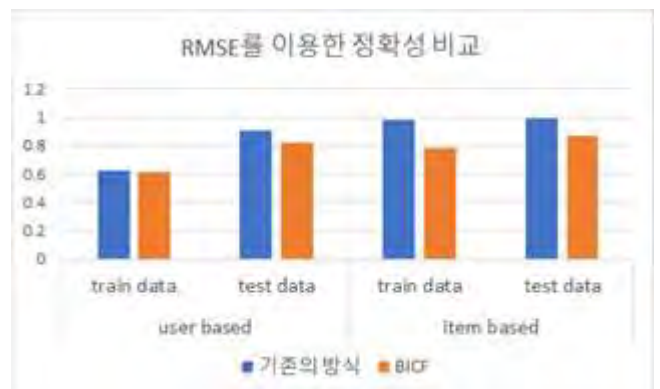
<그림 4> 예측 행렬 계산

4. 성능평가

본 연구의 모델의 정확성을 평가하기 위해 앞의 과정에서 생성된 평가 데이터를 BICF를 사용한 방식을 기존의 방식과 비교하였다. 우선 평가 데이터를 MinMaxScaler를 이용하여 정규화하였다. MinMaxScaler는 각각의 값에 최대값과 최소값의 차이를 나눠주는 방법이다. 이 방법을 사용하면 모든

feature들이 0과 1 사이에 재조정된다.

<그림 5>는 본 논문에서 제시한 방법이 타당한지 증명한 그래프이다. 모델성능 평가의 방법으로 RMSE(Root mean squared error)를 사용하였다. RMSE는 추천 시스템 모델을 평가하는 데에 가장 많이 사용하는 방법 중 하나로 숫자가 작을수록 좋은 모델임을 나타낸다. 그래프를 보면 user-based, item-based 두 가지 방식 모두 BICF의 RMSE가 더 작다. 그러므로 BICF 알고리즘이 기존의 알고리즘에 비해 더 향상된 알고리즘이라고 결론지을 수 있다.



<그림 5> 모델 정확성 평가를 위한 RMSE 비교

4. 결론 및 향후 연구

기존의 평점을 이용한 협업 필터링은 데이터 수집의 속도가 느리고 비용이 많이 든다는 점 등 많은 문제점이 존재한다. 본 연구에서는 이러한 문제를 해결하기 위해 온라인 고객 행동 정보를 활용하여 개선된 추천 시스템을 제안하였다.

본 연구에서 제안한 BICF 알고리즘은 기존보다 정교한 상품 추천을 위해 온라인 고객 행동 정보를 활용하여 군집화를 수행하였고, 군집화된 행동 정보를 활용하여 유사평점을 생성하였다. 그 다음 유사평점을 기반으로 고객과 아이템의 유사도를 계산하여 상품을 구매하지 않은 고객들의 평점을 예측하는 협업 필터링을 적용하였다.

온라인 고객 행동 정보 군집화를 통해 더 개인화된 추천을 가능하게 하였고, 기존의 평점 생성 방식 대신 온라인 행동 정보를 활용한 유사평점을 생성함으로써 평점이 있어야 가능했던 콘텐츠 추천을 더 다양한 분야와 데이터에 적용할 수 있게 되었다. 그 결과, 본 논문에서 제시한 BICF 알고리즘은 기존의 알고리즘에 비해 향상된 정확도를 보였다.

본 연구는 기존 상품 추천 시스템의 한계인 평점

정보의 희소성과 그로 인한 추천 시스템의 성능 하락의 문제를 보완하였다는 의의가 있으나 구매 관련 데이터 이외에 인구 통계 데이터나 검색 키워드 등 이용 가능한 변수를 모두 활용하지 못하였다는 한계점을 가진다. 향후 연구에서는 TF-IDF를 이용한 키워드 분석과 인구 통계 정보를 활용한 세대별 아이템 선호도 분석 등 고객 관련 정보를 충분히 활용한 연구가 필요하다.

참고문헌

- [1] Badrul Sarwar, George Karypis, Joseph Konstan, and John Riedl, "Item-Based Collaborative Filtering Recommendation Algorithms"
- [2] J. Ben Schafer, Dan Frankowski, Jon Herlocker, and Shilad Sen, "Collaborative Filtering Recommender Systems"
- [3] 김병희, 장병탁. 2015. 「온라인 공군집화를 이용한 추천 및 콜드스타트 문제 해법 연구」. 『한국지능시스템학회 학술발표 논문집』, 25(1), 41-42.
- [4] 김효석, 채선규, 유제성, 배석주. 2019. 「온라인 쇼핑몰 고객의 구매 유형 군집화 및 구매력 평가모형」. 『대한산업공학회 춘계공동학술대회 논문집』, 2597-2616.
- [5] Suresh K. Gorakala, 『Building Recommendation Engines』, 에이콘 출판. 2017
- [6] 김정재, 안현철, 「개선된 데이터 마이닝 기술에 의한 웹 기반 지능형 추천 시스템 구축」, 『Journal of Information Technology Applications & Management』, 41-56 (2005)

데이터 출처: 롯데멤버스, L.pay|L.POINT, 제6회 L.POINT Big Data Competition

머신러닝을 이용한 구축함 수리부속 예측 연구

정연오, 김재동
한국국방연구원

yono5083@gmail.com, soobahkin@gmail.com

A study on Destroyer Spare Parts Demand Forecasting using Machine Learning

Yeonoh Jeong, Jae-Dong Kim
Korea Institute for Defense Analyses

요 약

국방분야에서 전력 운영유지를 위한 군수분야 운영 효율화는 매우 중요한 이슈이다. 군수분야의 효율성을 위해 적정한 수리부속 확보는 장비의 가동률과 예산 절감 차원에서 중요성이 크다. 이에 군은 다양한 기법을 활용하여 수리부속 수요예측에 대한 노력을 계속해 왔으나, 여전히 예측 정확도 향상을 위한 지속적인 노력이 요구된다. 이에 본 연구에서는 지난 9개년의 수리부속 수요데이터를 분석하고 다양한 머신러닝을 활용하여 예측정확도를 비교·분석하고, 가장 적합한 수리부속 수요예측 모델을 제안한다.

1. 서론

국방분야에서 전력을 운영하는 측면에서의 효율화는 큰 이슈 중 하나이다. 전력의 운영유지를 위한 군수분야 운영 효율화는 무기체계 총수명주기 관점에서 매우 중요하다. 이러한 군수 측면의 효율화는 미래 첨단 무기체계의 전력화로 인한 장비의 다양화로 인해 그 필요성이 더욱 커지고 있다[1].

이러한 군수분야의 효율적인 운영을 위해 적정한 수리부속 확보는 장비의 가동률을 보장하고, 예산을 절감하는 차원에서 중요성이 크다. 이에 정확한 수리부속의 수요를 예측하기 위한 많은 연구들이 진행되어왔다[2]. 대표적인 방법은 기존에 많이 사용되어 오던 시계열과 머신러닝이 있다.

먼저 시계열은 일정기간 동안 변화하는 변수를 분류하여 움직임을 예측하는 기법으로, 시계열 자료의 변동형태를 파악하고 이를 통해 자기 상관성과 이동평균과정 요인의 차분 변수의 다양한 조합을 통해 시계열 속성을 분석하는 ARIMA(Auto Regressive Integrated Moving Average) 모델에 대한 연구가 진행되어 왔으며, 시계열을 이용하여 특정 분야의 수요를 예측하고, 예측정확도를 비교하는 형태의 연구가 활발히 진행되어왔다[3][4]. 하지만 수리부속의 비선형적 특징을 땀에 따라 기존에 많이 사용되어

오던 시계열은 정확한 수요를 예측하는데 제한적이다[5].

이를 보완하기 위해, 최근에는 머신러닝을 수요예측 분야에 적용하기 위한 연구가 활발하게 진행되고 있다[6]. 머신러닝은 대규모 데이터에서 유용한 정보의 관계를 탐색하고 분석 및 모델화하여 지식을 식별하는 일련의 과정으로 정의할 수 있다. 머신러닝은 기존의 시계열이 갖는 비선형 형태의 수요(Non-Linear Demand) 예측에 대한 제한사항을 극복하기 위해, 시계열 속성과 불규칙적 수요특성에 대한 패턴을 학습시켜, 일정한 패턴의 수요를 보다 정확하게 예측할 수 있도록 한다. 특히 인공 신경망을 기반으로 설계된 딥러닝은 하드웨어의 발전과 빅데이터, 다양한 알고리즘의 개발로 수요예측 분야에서도 최근 활발하게 연구되고 있다[7].

본 논문에서는 구축함정인 000 체계를 분석 대상으로 한다. 000 체계는 수리부속에 대한 많은 양의 데이터를 활용할 수 있어 분석의 정확도를 기대할 수 있다. 이에 수년간의 대규모 데이터를 기존에 많이 사용되었던 시계열과 최신의 다양한 머신러닝 및 딥러닝을 활용하여 각 기법별 예측정확도를 비교·분석하고, 이를 통해 최적의 수리부속 수요예측 모델을 제안하고자 한다.

2. 관련 연구

시계열은 전통적으로 수리부속의 불규칙한 수요를 예측하기 위해 사용되어 온 기법으로, 일정기간 동안 과거 수요의 평균과 추세, 계절 요인 등을 이용하여 수요를 예측한다. 대표적인 시계열로는 산술평균법과 이동평균법 등이 있다. 산술평균법은 수요예측의 가장 단순한 형태로 과거기간 중 발생한 수요를 모두 평균하여 수요를 예측하는 것으로, 과거 자료가 충분히 많고, 균등하게 형성될 경우 활용되는 방법이다[8]. 이동평균법은 일정기간의 시계열 자료를 대상으로 산술평균 또는 가중평균을 구하여 계절적 및 불규칙 요인을 제거하는 방법으로 기간을 이동하면서 예측값을 산출하는 방법이다[8].

머신러닝은 경험적 데이터를 기반으로 학습을 하고 예측을 수행하며, 스스로 성능을 향상시키는 기법을 의미한다. 대표적인 머신러닝으로는 의사결정나무 알고리즘, 서포트 벡터 머신(SVM) 등이 있다. 의사결정 나무 알고리즘은 의사결정 규칙을 나무 구조로 나타내어 전체 자료를 몇 개의 소집단으로 분류하거나 예측을 수행하는 분석방법으로, 분류를 위한 목표변수에 영향을 줄 수 있는 입력 변수들을 이용해 최적의 분류를 위한 의사결정 규칙을 트리 구조로 나타내어 준다[9]. 서포트 벡터 머신은 다차원 공간에 표시되는 점들 사이에 의사결정 초평면을 사용하여 유사한 클래스의 값들을 그룹으로 나누는 알고리즘이다[10].

딥러닝은 머신러닝의 한 종류로서 인공 신경망을 기반으로 발전된 것으로, 우수한 학습과 분류 성능을 보여준다. 대표적인 딥러닝으로는 순환신경망(RNN), LSTM(Long Short-Term Memory) 등이 있다. RNN은 각 은닉층에 저장된 특정 시점의 데이터 정보를 다음 시점으로 전달하도록 개발된 모델로써, 데이터 간의 비선형적 관계뿐 아니라, 시간 정보까지도 고려할 수 있다[11]. LSTM은 현재 가장 많이 사용되는 순환신경망 구조의 기법으로, 전통적인 순환신경망 구조에서 은닉 계층의 유닛들을 LSTM 블록(Block)으로 대체시킨 형태를 갖는다[12].

이러한 다양한 기법들이 다양한 분야의 수요예측 정확도를 향상시키기 위한 방법으로 활용되어왔다.

3. 수리부속 수요예측 모델 제안

본 연구의 분석 대상인 000 체계는 주력 구축함정으로서, 전시 해양우세 확보와 평시 해상침투 대응

등 핵심 임무를 수행하는 대표적인 구축함이다. 또한 해군의 가장 큰 비중을 차지하는 체계로써, 분석 대상으로 적합하다고 판단하였다.

실험과정은 [그림 1]과 같이 5단계 프로세스를 통해 진행하였다.



[그림 1] 실험 절차

먼저 대상 체계에 대한 데이터 수집은 군에서 2009년부터 운영 중인 장비정비정보체계(Defense Logistics Integrated Information System)를 이용하였다. 장비정비정보체계는 무기체계의 주 장비 중심으로 수리부속의 보급 및 정비 관련 사항을 최신 정보 기술을 이용하여 개발한 정보체계로써, 육·해·공군의 편성 부대로부터 국방부에 이르기까지 정비 관련 부서에서 사용하는 통합정보지원 시스템이다.

해군 장비정비정보체계에서 수집된 데이터에는 정비날짜, 정비당일 소모된 수리부속품목의 개수, 대당 구성수 등 00개 항목이 포함되어 있다. 이 데이터에서 수리부속별 수요예측을 위해 데이터를 품목별로 재정리하였으며, 수리부속 품목 수는 총

16,236개이다. 또한, 수리부속별로 2010년부터 2018년까지 9년간의 연도별 소모개수 데이터를 추출하여, 아래 <표 1>과 같이 총 9개의 변수를 사용하였다.

<표 1> 변수 설명

변 수	의 미
'10년 소모개수	'10~'18년 수리부속 품목별 연도별 소모 개수 합
'11년 소모개수	
'12년 소모개수	
'13년 소모개수	
'14년 소모개수	
'15년 소모개수	
'16년 소모개수	
'17년 소모개수	
'18년 소모개수	

실험방법은 2018년의 품목 발생 기준으로 16,236개 품목 중 8,118개의 발생 품목과 8,118개의 미발생 품목으로 분류하였으며, <표 2>와 같이 모델 성능측정은 분류결과표(Confusion Matrix)의 정확도로 측정하였다.

<표 2> 변수 설명

구분	예측 발생	예측 미발생
실제 발생	A	B
실제 미발생	C	D
Accuracy	$\frac{A + D}{A + B + C + D}$	

본 연구에서는 전통적인 시계열 중 산술평균법, 단순이동평균법, 가중이동평균법, 선형이동평균법, 최소자승법 등 5가지 모델을 사용하였다. 머신러닝은 DT(Decision Tree), NB(Naive Bayesian), SVM(Support Vector Machine), LR(Logistic Regression) 등 4가지 모델을, 딥러닝은 MLP(Multi Layer Perceptron), RNN(Recurrent Neural Network), GRU(Gated Recurrent Units), LSTM(Long Short Term Memory), Attention RNN, Attention GRU, Attention LSTM 등 7가지 모델을 사용하였다. 분석 도구는 Python을 사용하였다.

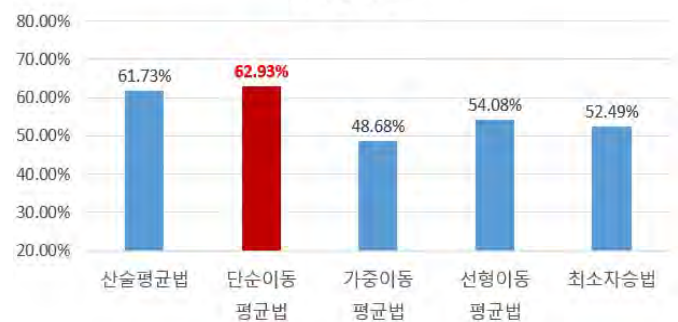
4. 실험 결과

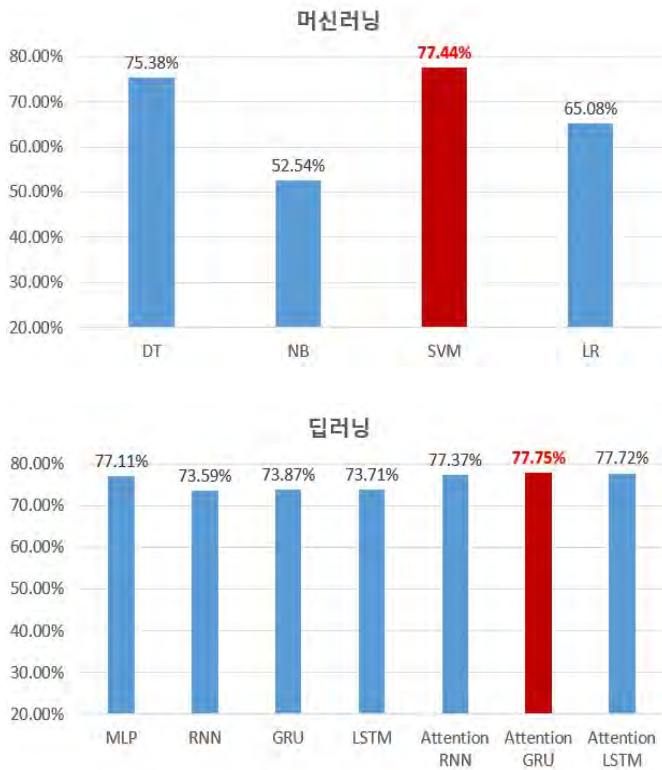
본 연구에서는 시계열과 머신러닝, 그리고 머신러닝의 한 분야인 딥러닝을 적용하여 각각의 예측정확도를 비교하였다. 실험방법은 훈련셋(training set)과 테스트셋(test set)을 7:3의 비율로 나누어 10겹 교차검증(10-fold cross validation) 방식을 사용하였다. 예측정확도를 기준으로 모델의 성능을 평가한 결과, <표 3>에서 보는 바와 같이, 시계열에서 가장 좋은 정확도를 보인 모델은 단순이동평균법으로 62.93%, 머신러닝에서 가장 좋은 정확도를 보인 모델은 SVM으로 77.44%, 딥러닝에는 Attention GRU 모델이 77.75%로 가장 좋은 정확도를 보였다. 본 실험을 토대로 기존의 시계열에 비해 머신러닝, 딥러닝이 보다 높은 예측 정확도를 보임을 확인하였다.

<표 3> 모델별 예측 정확도

방 법		정확도
시계열	산술평균법	61.73%
	단순이동평균법	62.93%
	가중이동평균법	48.68%
	선형이동평균법	54.08%
	최소자승법	52.49%
머신러닝	DT(Decision Tree)	75.38%
	NB(Naive Bayesian)	52.54%
	SVM(Support Vector Machine)	77.44%
	LR(Logistic Regression)	65.08%
딥러닝	MLP(Multi Layer Perceptron)	77.11%
	RNN(Recurrent Neural Network)	73.59%
	GRU(Gated Recurrent Units)	73.87%
	LSTM(Long Short-Term Memory)	73.71%
	Attention RNN	77.37%
	Attention GRU	77.75%
	Attention LSTM	77.72%

시계열 기법





5. 결론

본 논문에서는 해군의 대표적인 구축함정인 000 체계의 수리부속 수요예측 정확도 제고를 위하여 지난 9년간의 수리부속 수요데이터를 분석하고, 시계열, 머신러닝 및 딥러닝의 다양한 모델을 활용하여 수리부속 수요예측 결과를 비교 분석하고, 최적의 모델을 제안하였다. 제안한 머신러닝 및 딥러닝 모델이 기존의 수요예측 기법들에 비해 향상된 정확도를 나타냈다는 점에서 의미를 갖는다. 본 연구에서는 수리부속 소모이력의 정형 데이터만을 분석에 활용하였으나, 향후 장비의 운용 관련 변수 등을 추가하고, 텍스트 마이닝 기법을 활용한 비정형 데이터 분석 기법을 추가한다면, 보다 정확한 수요예측 결과를 얻을 수 있을 것으로 기대된다.

참고문헌

[1] Pinzariu, S., Minea, C.D., "The Military Units' Logistic Support Principles," Land Forces Academy Review Vol. XXIV, No 1(93), 2019.

[2] Regatterer, A., Gamberi, M., Gamberini, R., and Manzini, R., "Managing lumpy demand for aircraft spare parts," Journal of Air Transport Management, 11, 426-431., 2005.

[3] Shadra, R., and Patil, R., "Connectionist

approach to time series prediction: An empirical test," J. Intell. Manuf., 3, 317-323.

[4] Syntetos, A.A., and Boylan, J.E., "On the bias of intermittent demand estimates," Int. J. Production Economics, 71, 457-466., 2001.

[5] Hill, T., O'Conner, M., and Remus, W., "Artificial neural network models for times forecasts," Management Science, 42, 1082-1092., 1996.

[6] Gutierrez. R.S., Solis, A.O., and Mukhopadhyay, S., "Lumpy demand forecasting using neural networks," Int. J. Production Economics, 111, 409-420., 2008.

[7] Liao, S., Zhou, L., Di, X., Yuan, B., and Xiong J., "Large-scale short-term urban taxi demand forecasting using deep learning," In Proceedings of the 23rd Asia and South Pacific Design Automation Conference, Jeju, Korea, 22-25 January 2018; pp. 428-433.

[8] Laptev, Nikolay, et al. "Time-series extreme event forecasting with neural networks at uber." International Conference on Machine Learning. 2017.

[9] Tanizaki, T., Hoshino, T., Shimmura, T., and Takenaka, T., "Demand forecasting in restaurants using machine learning and statistical analysis," 12th CIRP Confernece on Intelligent Computation in Manufacturing Engineering, 679-682.

[10] Candelieri, A., Giordani, I., Archetti, F., Barkalov, K., Meyerov I., Polovinkin A., Sysoyev, A., Zolotykh N., "Tuning hyperparameters of a SVM-based water demand forecasting system through parallel global optimization," Computers & Operations Research, Volume 106, 202-209., 2019.

[11] Shi, H., Xu, M. Li, R., "Deep Learning for Household Load Forecasting-A Novel Pooling Deep RNN," IEEE Transactions on Smart Grid, 5271-5280., 2017.

[12] Kong, W., Dong, Z.Y., Jia, Y., David J.H., Xu, Y., Zhang, Y., "Short-Term Residential Load Forecasting Based on LSTM Recurrent Neural Network," IEEE Transactions on Smart Grid, 841-851., 2017.

빅데이터 도구 트렌드 및 긍·부정적 인식 결정 요소 조사

이명진, 구자환, 김응모
성균관대학교 소프트웨어대학
zj1081923@skku.edu, jhkoo@skku.edu, ukim@skku.edu

A Survey on Trend and Factor Determining Positive and Negative Recognition for Big Data Tools

Myungjin Lee, Jahwan Koo, Ung-Mo Kim
College of Software, Sungkyunkwan University

요 약

디지털 기술의 발전으로 데이터의 규모와 형태의 다양성이 기하급수적으로 증가하고 있다. 많은 업계에서 빅데이터를 비즈니스와 사용자의 서비스 제공에 사용하고 있으며, 데이터의 중요성 또한 커지고 있다. 본 연구에서는 빅데이터를 처리하기 위한 단계를 수집, 저장, 그리고 처리 및 분석 단계로 나눈 후, 단계별로 가장 높은 관심도를 가진 도구를 선정하고, 소프트웨어 리뷰 분석을 통해 긍부정 인식을 판단하며 인식 결정 요인을 조사한다. 이를 통해 다양한 빅데이터 생태계 속에서 사용자들이 관심을 많이 두고 있는 빅데이터 도구의 트렌드를 쉽게 파악하고 관련 빅데이터 도구를 선택하는 데에 도움을 줄 수 있다.

1. 서 론

4차 산업 혁명으로 인해 다양한 디지털 기기들이 일반 대중들에게 보급되고 있다. 데이터의 양과 그 종류는 PC, 스마트폰, SNS, IoT 기기, 센서 등 다양한 전자 기기의 대중화에 따라 기하급수적인 속도로 증가하고, 다양화되어가고 있다. 최근의 플랫폼과 서비스는 데이터의 축적을 통해 양질의 경험을 이용자에게 준다. 과거부터 현재까지 페이스북에 업로드된 사진은 약 400억 개이며 전체 데이터의 규모는 하루에만 500테라바이트에 달한다[1].

이와 같은 흐름 속에서 새로운 데이터의 출현과 함께 방대한 양의 데이터를 처리하고 분석할 수 있는 기술 또한 함께 등장했다. 비정형 데이터들을 저장하고 분류하는 다양한 수집·저장 소프트웨어, 저장된 데이터들을 분석할 수 있는 분석기법 등 여러 가지 기술과 플랫폼이 개발되고 있다. 빅데이터 관련 시장 규모가 연간 1,000억 달러를 넘어서며 해마다 10%씩 성장할 것으로 전망된다. 이 수치는 소프트웨어 산업 전체의 거의 2배에 가깝다.

빅데이터의 양은 굉장히 빠른 속도로 증가하며, 과거에는 없었던 다양한 형태의 데이터로 수집된다.

이 방대한 양의 데이터로부터 유의미한 정보를 제공해야 한다. 이 모든 과정은 다양한 빅데이터 도구들이 처리하고, 분석하고, 관리한다. 빅데이터를 가공하는 프로세스는 수집, 저장, 처리, 분석, 시각화의 단계를 거친다. 각각의 단계에서는 그 단계에 특화된 소프트웨어 도구가 존재한다. 예를 들어 데이터 수집 단계에는 Flume, Sqoop, Chukwa, Nutch 등, 데이터를 처리하는 데에는 Kafka, Storm, Spark 등이 있다.

다양한 도구들이 존재하는 만큼 각각이 가진 특성들도 다르고, 그로 인해 사용자들이 선호하는, 혹은 선호하지 않는 도구들도 있을 것이다. 각 단계에서 소프트웨어끼리의 비교에 대한 분석은 NoSQL 데이터베이스 성능 평가에 관한 연구[2]와 빅데이터 처리를 위한 도구를 비교한 연구[3]와 같이 이전에 관련된 연구가 존재한다. 첫 번째 연구에서는 Hbase, Cassandra, MongoDB, Redis 네 개의 NoSQL 데이터베이스의 성능을 비교했다. 두 번째 연구에서는 Computing tools인 Hadoop, Cloudera Impala RTQ, IBM Netezza, Apache Giraph를 다양한 항목에서 비교 분석했다. 또한, Storage tools인 Hbase,

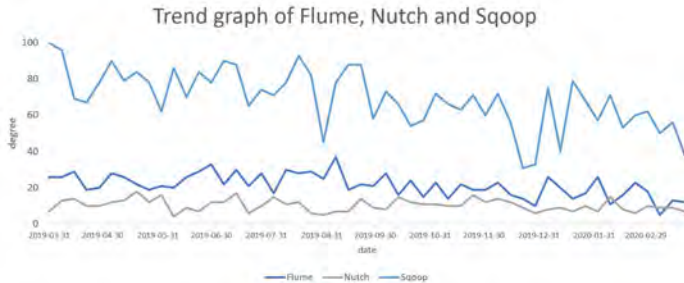
Apache Hive, Cassandra, Neo4j도 마찬가지로 다양한 항목에서 비교 및 분석했다.

그러나 소프트웨어 이용자들의 특정 소프트웨어 관심도와 트렌드에 대해서는 아직 구체적으로 연구된 바가 없다. 따라서 본 연구에서는 빅데이터 가공 단계를 수집, 저장, 처리 및 분석 이렇게 세 단계로 나누고, 각 단계에서의 트렌드를 분석하며 선정된 소프트웨어의 특징 및 장단점을 분석해보고자 한다.

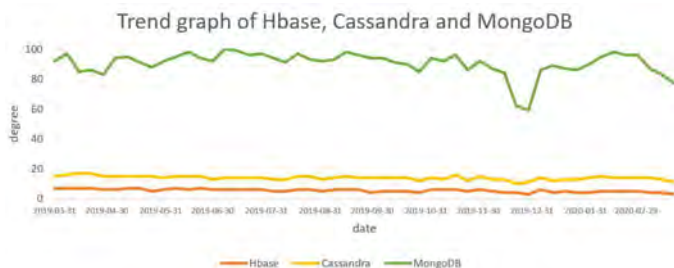
2. 사용자 관심도 분석

수집 단계에서는 Apache Flume, Nutch, Sqoop를, 저장 단계에서는 HBase, Cassandra, MongoDB를, 처리 및 분석 단계에서는 Apache Kafka, Spark, Hadoop 총 9개의 소프트웨어를 선정했다. 관심도는 구글 트렌드를 통해 확인했다. 기간은 모두 동일하게 2019년 3월 31일부터 2020년 3월 22일로 고정했다. 그래프의 y축 degree는 검색량이 가장 높은 지점의 검색 관심도를 100으로 해 나머지 값들을 계산한 결과이다.

그림 1의 그래프에서 볼 수 있듯이, 조사 기간 동안 Sqoop이 나머지 두 도구들보다 우위를 차지하고 있다.



(그림 1) Trend graph of Flume, Nutch and Sqoop

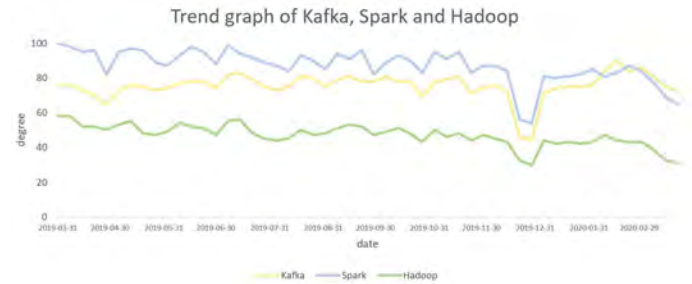


(그림 2) Trend graph of Hbase, Cassandra and MongoDB

그림 2의 그래프는 Hbase, Cassandra, MongoDB 중 MongoDB가 압도적인 관심도를 가지고 있는 것을 보여준다.

그림 3에서는 세 도구들 중 Spark의 관심도가 가장 높고 Kafka, Hadoop이 그 뒤를 잇고 있다.

이와 같은 결과로 말미암아 각 단계에서 Apache Sqoop, MongoDB, Apache Spark 세 도구를 정해 리뷰를 분석한다.



(그림 3) Trend graph of Kafka, Spark and Hadoop

3. 소프트웨어 리뷰 수집 및 분석

Apache Sqoop은 소프트웨어 리뷰 사이트인 'G2 Crowd', 'TrustRadius'에서, MongoDB는 'G2 Crowd', 'Capterra'에서, Apache Spark는 'G2 Crowd', 'Capterra', 'TrustRadius' 사이트에서 크롤링하여 데이터를 수집했다.

유효한 단어란 positive, negative, 혹은 neutral word로 분류될 수 있는 단어이다. 감성 분석을 통해 해당 소프트웨어에 대한 사용자의 반응이 긍정인지, 혹은 부정인지 판단했다. 분석을 위한 감성사전으로 SentiWordNet[4]을 이용했다.

<표 1> 리뷰 데이터에 대한 감성분석 결과

Apache Sqoop	총 단어 수	2368
	유효한 단어 수	904
	positive score	0.60
	negative score	0.40
MongoDB	총 단어 수	70458
	유효한 단어 수	26360
	positive score	0.61
	negative score	0.39
Apache Spark	총 단어 수	7369
	유효한 단어 수	2890
	positive score	0.57
	negative score	0.43

표 1의 positive score과 negative score은 감성 분석 결과 총 리뷰의 긍정정도, 부정정도를 점수화하여 백분율로 나타낸 값이다. 중립성을 띠는 단어는 제외했다.

표 1에서 Apache Sqoop은 긍·부정도가 각각 약 60%, 40%로 긍정적인 반응이 훨씬 크다는 것을 알 수 있다. 마찬가지로 MongoDB는 긍·부정이 각각 61%, 39%, 그리고 Apache Spark 역시 부정적인 반응보다 긍정적인 반응이 더 크다는 것을 알 수 있다.

이 결과를 통해 사용자들이 세 소프트웨어에 대해 만족감을 느끼고 있음을 알 수 있다. 그러나 긍·부정도가 극적인 차이를 보이지 않기 때문에 각 소프트웨어에 대한 특징과 강점뿐만 아니라 취약점 또한

조사했다.

3.1 Apache Sqoop 분석

Apache Sqoop은 Hadoop과 같은 관계형 데이터베이스처럼 구조화된 데이터 저장소 간에, 대량 데이터를 효율적으로 전송하도록 설계된 도구이다.[5] 맵리듀스를 기반으로 구현된 데이터 적재 프로그램이며, MySQL, Oracle 등의 관계형 데이터베이스와 Hadoop 파일 시스템 간 손쉬운 데이터 적재가 가능하기 때문에 널리 사용된다. 또한 데이터 전송을 병렬화해 빠른 성능을 보장한다. 그러나 Apache Sqoop은 command line 인터페이스로, GUI를 제공하지 않는다.[6-7]

RDBMS를 기반으로 하는 많은 어플리케이션 시스템을 운영하거나, 빠른 성능이 필요할 때 데이터 전송을 분할하고 병렬화할 수 있는 Sqoop은 좋은 솔루션이 될 수 있다. 그러나 event driven data를 다뤄야 하거나, 원천이 되는 데이터 저장소에 큰 부담이 가해져서는 안 되는 경우, 대량의 데이터 전송에 이용되는 Sqoop의 사용은 바람직하지 않다.[8]

3.2 MongoDB 분석

MongoDB는 높은 성능과 확장성을 가지고 있는 문서 기반 방식의 NoSQL DBMS이다. 가장 큰 특징으로는 RDBMS와는 다르게 고정된 스키마가 존재하지 않으며 JSON 형태의 문서로 저장하는데, 이를 BSON 형식이라고 부른다. key-value를 통해 복잡한 쿼리가 가능하고, 관계형 데이터베이스보다 응답속도가 빠르며, 인덱스 추가를 통해 처리 속도를 더 빠르게 할 수 있다. 그러나 복잡한 join이나 트랜잭션 처리에 제약이 있다는 단점이 있다. 또한 디스크에 쓰기가 비동기식으로 이루어져 데이터가 소실될 위험이 있다.

스키마가 존재하지 않기 때문에 데이터 모델의 변경, 추가, 확장이 비교적 쉽다. BSON 구조를 사용하므로 데이터를 직관적으로 파악할 수 있어 가독성이 높다. 그리고 native sharding을 지원하기 때문에 확장이 RDBMS보다 간단하다.[9]

IDC의 추정으로는, 데이터의 90%는 사전 정의된 데이터 모델이 없는 비정형 데이터이다. 이러한 종류의 데이터를 저장하기 위해서 사용자들은 다른 데이터베이스 저장 도구보다 MongoDB를 편리하게 선택한다. 방대한 양의 빠른 데이터 처리를 원하는 사용자라면 MongoDB를 사용하는 게 효율적이지만 높은 transactional application을 사용한다면, 혹은 은행과 같이 데이터 소실이 치명적인 결과를 초래하는 시스템에서 MongoDB는 좋은 선택이 아닐 수 있다.

3.3 Apache Spark 분석

Apache Spark는 대규모 데이터 처리를 위한 통합 분석 엔진이다. DAG 스케줄러, 쿼리 최적화 프로그램 및 물리적 실행 엔진을 사용해 배치-스트리밍 데이터 모두에 높은 성능을 보여준다. 예를 들어,

Logistic regression에서 Spark는 Hadoop보다 running time이 약 100배 빠르다. 또한 SQL, DataFrames, 머신 러닝을 위한 MLlib, Graph X, Spark Streaming 등을 포함한 라이브러리를 제공한다. Spark API는 개발자 친화적이며, 분산 처리 엔진의 복잡성을 간단한 메소드 호출로 가린다. 인메모리 컴퓨팅을 지원해 Hadoop과 같은 디스크 기반 엔진과 비교해 훨씬 빠르게 데이터를 쿼리할 수 있다. 그러나 Apache Spark는 현재의 모든 작업을 메모리 내에서 유지하는데, 이는 메모리 리소스의 부족을 야기한다.[10-11]

Spark는 Hadoop의 MapReduce 코드보다 훨씬 간결하고, 다양한 언어를 위한 API로 쉽게 작성할 수 있다. 또한 배치 프로그래밍과 인메모리 컴퓨팅에서 최소 10배, 최대 100배의 성능을 보이는 Spark는 사용자 입장에서 매우 매력적으로 보인다.

큰 빅데이터를 빠른 속도로 처리하려는 사용자는 Spark가 적절한 도구가 될 것이다. 그러나 비교적 작은 크기의 데이터를 처리하거나, 혹은 사용 가능한 메모리가 제한적이라면 Spark보다 Hadoop이 좋은 선택이 될 수 있다.

4. 결론

빅데이터 처리 과정을 수집, 저장, 처리 및 분석 세 단계로 나누어 각각의 단계에 특화된 소프트웨어를 선정했다. 각각의 단계에서 Apache Sqoop, MongoDB, Apache Spark가 사용자들에게 가장 높은 관심도를 가지고 있었다. 소프트웨어 리뷰 사이트에서 리뷰 데이터를 분석했고, 세 도구 모두 부정적인 반응보다 긍정적인 반응이 많았다. 따라서 Apache Sqoop, MongoDB, Apache Spark 모두 사용자들에게 편의성을 제공하고, 사용자에게 매력적인 소프트웨어라고 결론 내릴 수 있다. 그러나 긍정도와 부정도의 차이가 크지 않기 때문에 강점뿐만 아니라 취약점 또한 조사했다. 이를 통해 각 도구의 특징 및 장단점을 분석하고 소프트웨어 특성에 따른 적합한 사용자의 유형 또한 제안했다.

본 연구를 통해 언급된 빅데이터 도구들의 현재 트렌드가 어떠한지 살펴보고, 빅데이터 처리 각 단계에서의 도구 선택에 도움을 줄 수 있을 것이다.

참 고 문 헌

- [1] 이궁희 외 4인, “빅데이터의 이해”, 한국방송통신대학교 출판문화원, 2016.
- [2] 박홍진, “다양한 NoSQL 데이터베이스의 성능 평가 연구”, 한국정보전자통신기술학회논문지, Vol.9, No.3, pp.298-305, 2016.
- [3] Bakshi Rohit Prasad and Sonali Agarwal, “Comparative Study of Big Data Computing and Storage Tools: A Review”, International

- Journal of Database Theory and Application,
Vol.9, No.1, pp.45-66, 2016.
- [4] Text Learning Group, <http://sentiwordnet.istc.nr.it/>
- [5] Apache Sqoop, <https://sqoop.apache.org/>
- [6] 진고환, “하둡 분산 환경 기반의 데이터 수집 기
법 연구”, Journal of the Korea Convergence
Society, Vol.7, No.5, pp.1-6, 2016.
- [7] Varsha B.Bobade, “Survey Paper on Big Data
and Hadoop”, International Research Journal
of Engineering and Technology(IRJET), Vol.3,
No.1, pp.861-863, 2016.
- [8] Tomcy John, Pankaj Misra, “Data Lake for
Enterprises”, Packt, 2017.
- [9] MongoDB, <https://www.mongodb.com/>
- [10] Apache Spark, <https://spark.apache.org/>
- [11] Abdul Ghaffar Shoro, Tariq Rahim Soomro,
“Big Data Analysis: Ap Spark Perspective”,
Global Journal of Computer Science and
Technology (C), Vol.15, No.1, pp.7-14, 2015.

COVID-19 확산 예측 모형에 관한 연구

윤석용
명지대학교 ICT 융합대학 빅데이터융합교육
icanibe@mju.ac.kr

A Study on the Diffusion Prediction Model of COVID-19

Seok-Yong Yun
Big Data Convergence Education, Myongji University

요 약

COVID-19(Coronavirus Disease 2019)는 RNA 형 바이러스로써 점막감염(粘膜感染)과 비말전파(飛沫傳播)로 전염되는 급성 호흡기성 질병이다. 2019 년 12 월 중국 후베이 우한에서 처음 감염이 보고된 후 빠르게 글로벌로 확산되었고, 현재 여러 국가와 지역이 Lockdown 상태에 있다.

COVID-19 의 치사율은 국가별, 연령별 차이는 있으나 사스(SARS-CoV), 메르스(MERS-CoV) 등과 비교하여 높다고 할 수 없다. 그러나 COVID-19 는 신종 코로나바이러스로써 아직 백신(Vaccine)과 항바이러스제가 개발되지 않았고 다른 질병과 비교하여 빠른 감염 속도때문에 의료 공백, 사회적 혼란, 경제적 손실을 크게 일으키고 있다.

따라서 바이러스의 확산 양상을 데이터 분석을 통하여 예측할 수 있다면 사회·경제적인 폐해를 줄일 수 있어 Bass 모델과 R 패키지를 이용하여 COVID-19 확산 예측 모형을 계량적으로 제시하였다.

1. 서론

코로나바이러스는 Group IV 군 니도바이러스목 코로나바이러스과에 속하는 RNA 형 바이러스로써 광륜의 모양을 하고 있어 코로나로 불리는 급성 호흡기성 질병이다. 그러나 COVID-19(SARS-CoV2)는 코로나바이러스의 변종으로 2019 년 12 월 감염이 처음 보고된 이후 전 세계 모든 국가로 빠르게 전파되어 의료 공백 사태를 일으키고 있고 아직도 증가세는 멈추지 않고 있다.

COVID-19 의 이러한 현상으로 인하여 세계보건기구 WHO 는 전염병 경보 최종 6 단계인 팬데믹(Pandemic)을 3 월 11 일 선언하였다. 2009 년 214 개국에 감염되어 1 만 8 천여 명의 사망자를 가져온 신종 플루 이후 11 년 만에 선언된 세계 수준의 전염병이다.

지구온난화 등의 이유로 팬데믹 수준의 전염병은 앞으로도 발생 가능성이 높고 이를 예방하기 위한 백신과 치료제인 항바이러스제 개발은 늦을 수밖에 없다.

팬데믹이 발생하면 의료 공백과 국가 및 지역 단위의 Lockdown 으로 이어져 사회·경제적인 폐해는 예측할 수 없을 정도로 커진다. 따라서 이를 최소화하고 예측을 통한 사회적 혼란을 줄이기 위하여 데이터

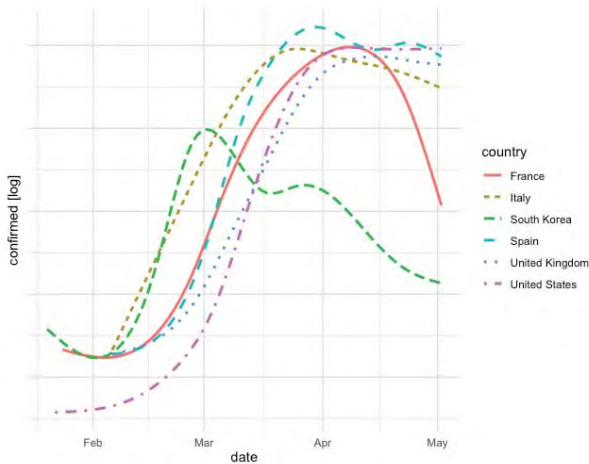
기반의 질병 확산 모형 개발이 무엇보다 중요하다.

본 연구는 COVID-19 의 국가별 일자별 코로나바이러스의 확진자 등의 데이터를 이용하여 다양한 기술 분석(Descriptive Analysis)과 중장기 예측에 많이 사용되는 Bass 모델을 이용하여 COVID-19 확산 예측 모형을 제시하고자 한다.

2. COVID-19 데이터 분석과 연구 모형

COVID-19 데이터는 확진자, 완치자, 사망자 그리고 감염경로 등으로 구성되어 있다. 데이터 분석은 COVID-19 데이터에 더하여 검사자 수와 국가별 인구수를 반영함으로써 비교 데이터의 객관성을 유지하였다.

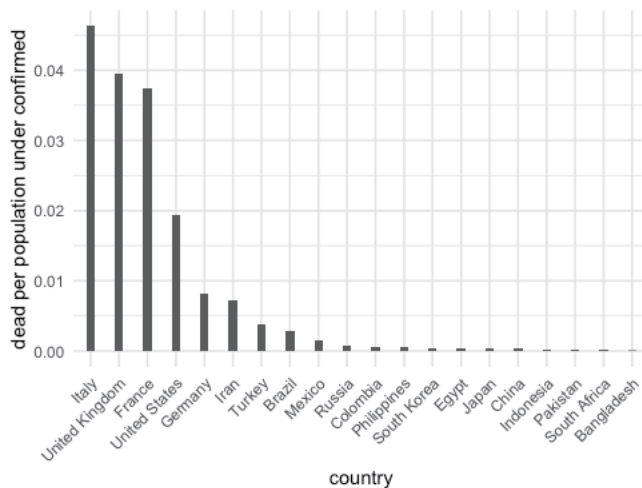
(그림 1)은 인구대비 일일 확진자 상위 5 개국과 한국을 로그 스케일(Log Scale)로 비교한 그래프로써 한국 등 몇몇 국가를 제외하고는 일일 확진자 수가 줄지 않고 있다.



(그림 1) 인구대비 확진률

코로나바이러스 사망률은 다른 전염병에 비하여 높지 않으나 빠른 감염¹으로 인한 입원 환자 수의 증가와 단기간 사망자 수의 급증으로 의료 공백이 발생하고 있다.

(그림 2)는 국가별 인구대비 감염자의 사망률로써 인구 5 천만 명 이상의 국가를 대상으로 데이터를 분석하면 이탈리아, 영국, 프랑스, 미국, 독일 순으로 사망률이 높아 현재 의료에 어려움이 발생하고 있음을 알 수 있다.



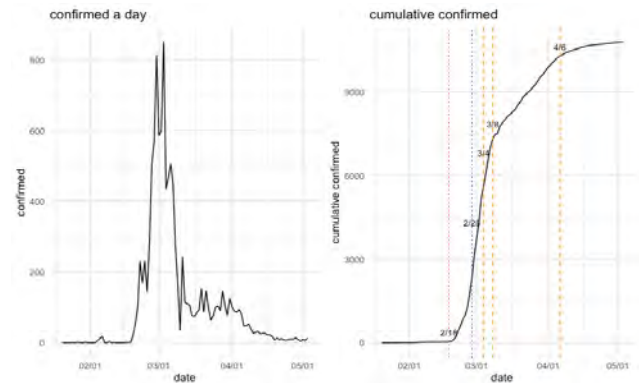
(그림 2) 인구대비 사망률

COVID-19 는 점막감염(粘膜感染)과 비말전파(飛沫傳播)로 전염되는 급성 호흡기성 질병으로 알려져 있기에 마스크 착용은 감염 속도를 낮추는 효과적인 수단이다.

(그림 3)은 2 월 18 일 31 번 확진자 발생으로 감염자가 급증하여 2 월 28 일 공적마스크를 공급함으로써

일일 확진자 발생 반감기가 약 1~2 주 단위로 나타나고 있음을 보여준다.

비교 데이터가 없어 반감기에 대한 통계적 유의성은 없으나 정책적 의사결정에는 참조가 가능할 수 있다.



(그림 3) 한국의 일자별 확진자

확산모형으로 마케팅을 포함한 여러 분야에서 활용되고 있는 것은 로지스틱과 Bass 모형 등을 들 수 있다.

로지스틱 모형은 1845 년 소개된 후 확산뿐만 아니라 S 형 성장모형에도[1] 널리 사용된다.

$$\hat{y} = \frac{m \cdot e^{(a+b \cdot t)}}{1 + e^{(a+b \cdot t)}}$$

$$t_{\max_rate} = \frac{\ln 2 - a}{b}$$

$$t_{\max_num} = -\frac{a}{b}$$

윗 식에서 a, b, m 은 OLS(Ordinary Least Squares)나 NLS(Nonlinear Least Squares)로 추정할 수 있는 모수이고 t_{\max_rate} 와 t_{\max_num} 은 증가율이 최대가 되는 시점과 예측값이 최대가 되는 시점이다.

Bass 모형도 Rogers[2]의 혁신이론에 기반한 확산 모형으로써 Bass[3]에 의해 수리적으로 증명된 후 주요 확산 예측에 많이 활용되고 있다.

$$\hat{y} = m \cdot f(t)$$

$$\frac{f(t)}{1 - F(t)} = p + q \cdot F(t)$$

¹ 사스의 기초감염재생산지수(R_0)는 2~5, 메르스는 0.4~0.9 로 COVID-19 는 사스 이상의 R_0 예상

$$\hat{y} = \frac{m \left[\frac{(p+q)^2}{p} \right] \cdot e^{-(p+q)t}}{\left[1 + \frac{q}{p} e^{-(p+q)t} \right]^2}$$

이 Bass 모형의 m, p, q 는 비선형 계획법을 이용하여 찾을 수 있다.

3. COVID-19 확산 예측 모형 결과

확산 예측 모형은 R 언어의 NLS 패키지를 이용하여 모수를 추정하였고, 데이터는 일일 확진자 수를 대상으로 데이터 최종 확진일 이후 120 일 동안을 일일 단위로 예측하였다. 그리고 예측 모형의 안정화를 위하여 일자별 확진자 수의 IQR 1.5 배 이상은 이상치(Outlier)로 처리하였다.

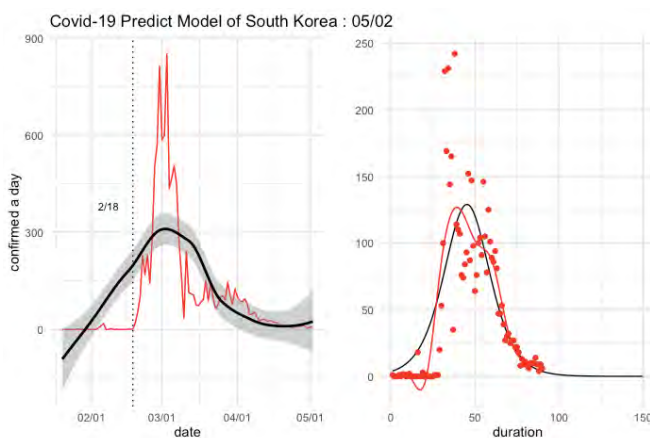
모형의 메트릭인 RMSE²는 Bass 354.76, 로지스틱 525.96 로 비교 우위가 있는 Bass 모형을 선택하였다.

<표 1>은 Bass 모형의 파라미터 계수와 통계량이다.

<표 1> Bass 모형 파라미터 통계량

	Estimate	Std. Error	t value	Pr(> t)
m	4678.81288	347.38501	13.4687	0.00000***
p	0.00077	0.00030	2.5455	0.01267**
q	0.10875	0.01062	10.2365	0.00000***

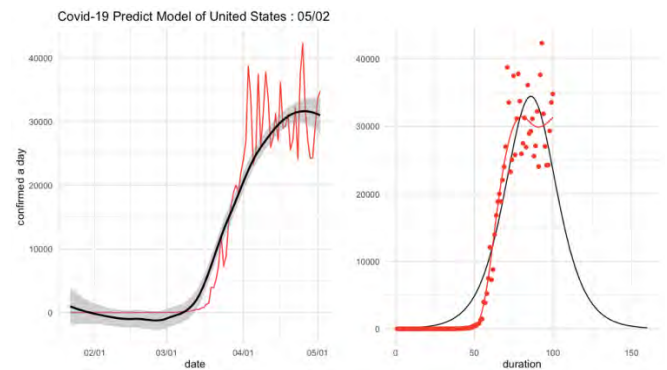
(그림 4)의 좌측 그래프는 한국의 일일 확진자 수와 흑색의 추세선을 보여주고 있고, 우측 그래프는 흑색의 COVID-19 확산 예측 모형과 일자별 확진자 수와 추세선이다.



(그림 4) COVID-19 예측 모형(한국)

예측 모형에서 한국은 5 월 초순에 확진자 영(Zero)

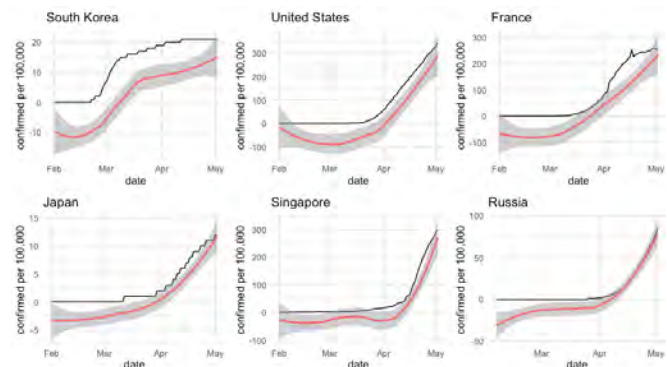
에 수렴하는 것으로 예측되었고 (그림 5)는 미국의 예측 모형으로 8 월하순에 확진자 발생이 영(Zero)에 수렴하는 것으로 예측하고 있다.



(그림 5) COVID-19 예측 모형(미국)

4. 연구결과 및 향후 연구과제

COVID-19 는 논문이 작성되고 있는 시점에서도 현재 진행형으로 (그림 6)은 10 만 명당 누적 확진자 수와 일일 확진자 수의 추세선으로 확산세가 아직 꺾이지 않고 있음을 보여주고 있다.



(그림 6) 인구 10 만 명당 확진자

팬데믹으로 한국을 포함한 많은 국가가 마이너스 성장을 예측하고 있어 Lockdown 조기 종료를 위한 바이러스 확산 예측 모형은 그 의미가 크다고 판단된다.

그러나 데이터에 기반한 예측 모형은 검진이나 확진 등과 관련한 데이터의 신뢰성이 무엇보다 중요하고 Bass 에 기반한 일반화된 단일 모형보다는 국가별 특성을 반영하여 세분화하고 로지스틱과 신경망 모델 등이 결합된 앙상블 모형으로의 추가적인 연구가 필요하다.

참고문헌

- [1] Kingsland, S., "The Refractory Model : The Logistic Curve and the History of Population Ecology," The

² Root Mean Square Error

- Quarterly Review of Biology, Vol.57, No.1(1982), pp.29-52.
- [2] Rogers, E.M., Diffusion of innovation, New York, 1962.
- [3] Bass, F.M., “A New Product Growth Model for Consumer Durables,” Management Science, Vol.15, No.5(1969), pp.215-227.
- [4] Bass, F.M., “Comments on a new product growth for model consumer durables the bass model,” Management Science, Vol.50 (2004), pp.1833-1840.
- [5] 홍정식, 김태구, 구훈영, “NLS 와 OLS 의 하이브리드 방법에 의한 Bass 확산모형의 모수추정”, 대한산업공학회지, 제 37 권 제 1 호(2011), pp.74-82.
- [6] 양진아, 민대기, 최형석, “Bass 확산모형을 활용한 국내 주택연금의 중장기 수요예측”, 한국경영과학회지, 제 42 권 제 1 회(2017), pp.29-41.
- [7] 이하늘, 김대회, 강지석, 이동환, 김윤배, “Bass 모형을 통한 WIPI 정책의 영향 분석:스마트 폰 시장을 중심으로”, 정보통신정책연구, 제 22 권 제 4 호 (2015), pp.1-18.
- [8] 홍정식, 김태구, 임달오, “확산 모형에 의한 고가 의료기기의 수요 확산의 특성분석 및 중장기 수요 예측에 관한 연구”, 보건행정학회지, 제 18 권 제 4 호(2008), pp.85-110.

마이데이터 서비스 활성화를 위한 분산 ID(Decentralized Identification, DID) 수용의도에 영향을 미치는 요인에 관한 연구

김지영*, 신용태**

*숭실대학교 IT정책경영학과

**숭실대학교 컴퓨터학부

jiygkim@naver.com, shin@ssu.ac.kr

A Study on Factors Affecting Intention to Accept Decentralized Identification(DID) for Activation of MyData Service

Ji-Young Kim

ITPM, Soongsil University

요 약

데이터 3법 시대에 접어들면서 기업들에는 가명화된 개인정보를 활용할 수 있는 길이 열렸다. 하지만 현 데이터 3법은 데이터를 생성하고 유통하며 활용할 기업들의 책임과 혜택에 내용이 맞춰져 있어 아쉬운 감이 있다. 개인의 기본권을 보장하면서도 마이데이터 유통 및 활용을 도울 방법은 없을까? 본 논문에서는 데이터의 주체인 개인이 데이터 주권을 행사하고 실질적인 혜택을 받는 마이데이터 서비스의 활성화를 위한 ID 관리 기술로 블록체인 기반 분산 ID(Decentralized Identification, DID)를 제안하고, DID 수용의도에 영향을 미치는 요인을 연구함으로써 마이데이터 서비스 개발 활성화를 위한 정책적, 실무적 시사점을 도출하고자 한다.

1. 서론

최근 데이터 3법 시대에 접어들면서 안전하게 가명화된 개인정보를 기업에서 활용할 수 있는 길이 열렸다. 이는 개인정보를 생성하고 유통하면서 활용할 기업으로서는 반가운 소식이다. 또한, 이는 AI 선진국으로 도약하기 위해 데이터 경제 활성화 방안 측면에서도 필요한 사항이기도 하다. 하지만 개인정보의 주체인 개인이 데이터 주권을 행사하고 실질적인 혜택을 받을 수 있는 마이데이터 서비스 내용이 빠져 있는 점은 아쉽다. 해서, 마이데이터 서비스의 활성화를 위한 ID 관리 기술로 블록체인 기반 분산 ID(Decentralized Identification, DID)를 제안하고, DID 수용의도에 영향을 미치는 요인을 연구함으로써 결과를 통해 마이데이터 서비스 개발 활성화를 위한 정책적, 실무적 시사점을 도출하고자 한다.

2. 분산 ID(Decentralized Identification, DID)

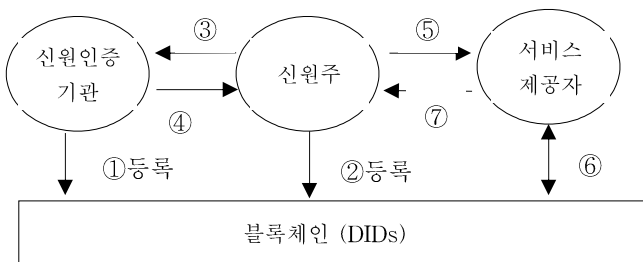
2.1 분산 ID(Decentralized Identification, DID) 개념

ID 관리(Identity Management) 기술은 적법한 개인이 적절한 시점에 올바른 자원(Resource)에 접근할 수 있게 하는 보안 분야 기술이다.[1] 최근 블록체인 기반 분산원장 기술을 이용한 새로운 ID 관리기술인 분산 ID(Decentralized Identification, DID)이 주목받고 있다. 이는 블록체인 기반으로 사용자가 자신의 ID 정보 및 디지털 자산을 완벽하게 제어하는 자기주권 신원 관리 기술을 제공하여 사용자 스스로 자신이 누구인지 증명할 수 있고, 데이터를 직접 제어할 수 있게 하는 디지털 신원 관리 체계이다.[2] 즉, 주민등록증, 운전면허증 등의 신분증처럼 온라인 환경에서 정보 주체가 자신의 신원정보를 관리, 통제하게 된다. 분산 ID 기술은 최근 개인정보의 자기주권 화와 더불어 금융권 비대면 거래가 확산하면서 디지털 금융의 핵심 기술로 떠오르고 있다.

2.2 마이데이터 서비스 활성화를 위한 분산 ID 도입의 필요성

전 세계적으로 개인의 프라이버시를 보호하고자 하는 움직임과 더불어 각 서비스 제공기관마다 인증 정보 및 개인정보를 관리함에 따른 위험성과 불편함을 인지하게 되었다. 더불어 사용자 처지에서도 개별 서비스마다 인증 정보를 다르게 설정하고 관리하기에는 한계가 있기 마련이다.

분산 ID는 블록체인을 활용해서 ③신원정보 발행자는 사용자의 신원을 검증 후 ④신원정보를 발행하게 되고, 이는 신뢰된 ID 저장소인 분산원장에 저장되게 된다. ⑤이후 사용자가 서비스 이용 시 신원정보를 서비스 제공자에게 제출하면 ⑥서비스 제공자는 신뢰된 ID 저장소를 이용해서 신원정보를 검증해 신원을 확인하게 되고 ⑦서비스 접근 허가를 해주게 된다.



(그림 1) 분산 ID 서비스 흐름

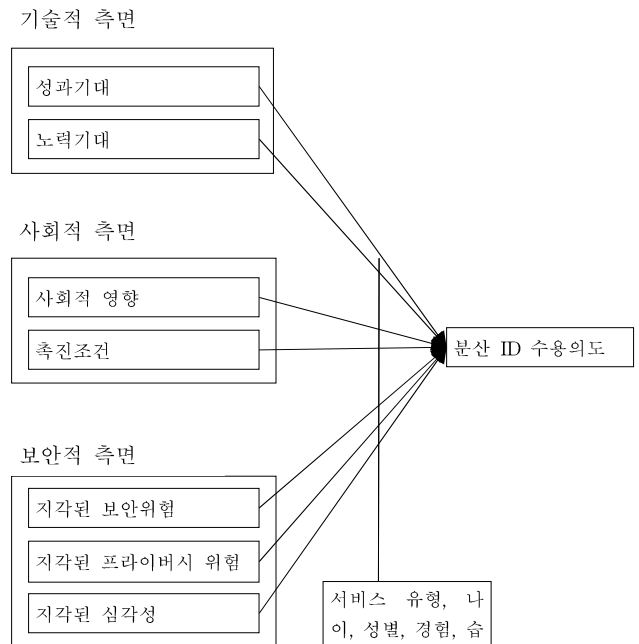
해당 서비스 흐름을 통해 영원성(Permanent), 판독성(Resolvable), 검증성(Verifiable), 분산성(Decentralized)을 보장받으면서 정보 주체인 개인이 본인에 관한 정보를 적극적으로 관리, 통제할 수 있게 된다. 이를 통해 신용관리, 자산관리 나아가 건강관리까지 개인 생애 관해 능동적인 마이데이터 서비스가 가능해진다.

3. 연구 모델 및 가설

3.1 연구 모델

선행연구와 문헌의 고찰을 통해 연구 모델을 설계하였다. 마이데이터 서비스 활성화를 위한 분산 ID 수용 의도에 영향을 미치는 요인으로, 독립변수로 기술적 측면에서 성과기대, 노력기대를 선정하였고,

사회적 측면에서 사회적 영향, 촉진조건을 선정하였으며, 보안적 측면에서 보안위험, 프라이버시 위협, 심각성을 선정하였다. 또한, 선행연구에서 정보보호 행동과 새로운 기술의 수용은 성별, 연령, 경험, 습관과 같은 인구통계학적 특성에 따라 상호작용하는 것을 확인함에 따라 이들을 조절변수로 설정하여 조절 효과를 살펴보았다. 이를 정리한 모델은 (그림 2)과 같다.



(그림 2) 연구 모델

3.2 연구 가설

기술수용이론(UTAUT)을 적용한 연구에서 성과기대, 노력기대, 사회적 영향, 촉진조건은 정보기술을 이용하고자 하는 의도에 영향을 미치는 요인으로 나타나고 있다. 또한 보호동기이론에 따르면 지각된 취약성과 지각된 심각성은 정보보호 동기와 행동에 영향을 미치므로 해당 내용을 세분화시킨 보안위험, 프라이버시 위협, 심각성 역시 분산 ID 수용의도에 영향을 미칠 것으로 판단되어 다음의 가설을 설정하였다.

H₁ : 성과기대는 분산 ID 수용의도에 정(+)의 영향을 미칠 것이다.

H₂ : 노력기대는 분산 ID 수용의도에 정(+)의 영향을 미칠 것이다.

H₃ : 사회적 영향은 분산 ID 수용의도에 정(+)의 영

향을 미칠 것이다.

H₄ : 축전조건은 분산 ID 수용의도에 정(+)의 영향을 미칠 것이다.

H₅ : 지각된 보안위험은 분산 ID 수용의도에 정(+)의 영향을 미칠 것이다.

H₆ : 지각된 프라이버스 위험은 분산 ID 수용의도에 정(+)의 영향을 미칠 것이다.

H₇ : 지각된 심각성은 분산 ID 수용의도에 정(+)의 영향을 미칠 것이다.

H₈ : 서비스 유형은 분산 ID 수용의도에 조절효과가 있을 것이다.

H₉ : 나이는 분산 ID 수용의도에 조절효과가 있을 것이다.

H₁₀ : 성별은 분산 ID 수용의도에 조절효과가 있을 것이다.

H₁₁ : 경험은 분산 ID 수용의도에 조절효과가 있을 것이다.

H₁₂ : 습관은 분산 ID 수용의도에 조절효과가 있을 것이다.

4. 결론

마이데이터 서비스 활성화를 위한 분산 ID (Decentralized Identification, DID) 수용의도에 영향을 미치는 요인을 실증 분석하기 위해 일반 소비자를 대상으로 설문 조사를 시행하여 통계 분석을 할 예정이다. 이를 통해 분산 ID 기반의 마이데이터 서비스를 개발하고 도입, 활성화하는 데 영향을 주는 요소를 파악하고, 궁극적으로는 기업이나 개인 모두에게 혜택이 돌아가는 균형적인 데이터 경제 발전에 이바지하고자 한다.

우리나라 인식 조사에 의하면, 우리나라 일반 시민이 개인정보 관리 서비스를 통해 본인 데이터를 직접 관리, 통제하는 데 관심이 높았으며 개인정보 활용에 대한 부정적인 태도보다 합리적인 수준에서의 긍정적인 태도가 엿보였다.[3] 현 데이터 3법에는 배제된 개인을 데이터 생태계의 주요 행위자로 끌어올리는 일에 분산 ID(Decentralized ID, DID)가 힘이 되었으면 한다.

참고문헌

- [1] Manohar, Arthi, Jo Briggs “Identity Management in the Age of Blockchain 3.0” HCI for Blockchain - CHI 2018 workshop, 22nd, April, 2018
- [2] 보안기술연구팀 “분산 ID(Decentralized Identity) 개념 및 해외 기술개발 동향” 금융보안원 제16호 pp. 15-39, 2019.03
- [3] 조성은, 정원준, 이시직, 이창범, 박규상 “개인주도 데이터 유통 활성화를 위한 제도 연구” 정보통신정책연구원, 기본연구 19-01, 2019
- [4] 백한중 “금융분야에서 마이데이터 서비스의 수용의도에 영향을 미치는 요인에 관한 연구” 숭실대학교, 2019
- [5] Drummond Reed, Manu sporny, Dave Longley, Christopher Allen, yan Grant, Markus Sabadello “Decentralized Identifiers (DIDs) v0.11.” W3C Community Group Report, March, 2019
- [6] Harer, Felix, Fill, Hans-Georg “Decentralized Attestation of Conceptual Models Using the Ethereum Blockchain” IEEE CBI Conference, 2019
- [7] 김석현, 조영섭, 김수형 “블록체인 기반의 ID 관리 기술 동향” 한국컴퓨터통신학회, 제2권 제1호 pp. 16-22, 2019.03

최근접 이웃 탐색 기반의 향상된 스카이라인 질의를 위한 전처리 기법[‡]

김지현*, 이상민*, 전형준**, 진창균**, 김지윤⁺, 권진영⁺⁺, 김종완[†], 오덕신[§]

*삼육대학교 인공지능·빅데이터 소프트웨어코드 연구소

삼육대학교 {**컴퓨터·메카트로닉스공학부, ⁺식품영양학과, [†]스미스학부대학, [§]경영정보학과}

⁺⁺건국대학교 정보통신경영학과

yeahegg@gmail.com, sangmin010203@gmail.com, chariot0720@gmail.com, jcg6074@naver.com,

wldbs3592@naver.com, oac0801@naver.com, kimj@syu.ac.kr, ohds@syu.ac.kr

Nearest Neighbor-based Pre-processing Scheme for Advanced Skyline Query

Ji-Hyun Kim*, SangMin Lee*, Hyeongjun Jeon**, ChangGyun Jin**, JiYun Kim⁺, Jin young Kwon⁺⁺, Jongwan Kim[†], Dukshin Oh[§]

^{*}AI-Big Data and Software Code Lab., Sahmyook University

요 약

스카이라인 질의는 객체의 속성을 기준으로 사용자의 선호에 적합한 대상을 탐색하는 기법이다. 기존 스카이라인 질의는 일괄처리 방식으로 탐색 결과를 반환하지만 대화형 앱이나 모바일 환경과 같이 잦은 위치이동 발생 시 일괄처리 방식으로 스카이라인 질의 결과를 신속하게 받기 어렵다. 최근접 이웃(Nearest Neighbor) 알고리즘은 사용자와 상호 작용이 필요한 대화형 앱에서 실시간으로 선호 객체를 탐색하여 사용자에게 전달함으로써 객체의 반환 속도를 향상시켰다. 그러나 최근접 이웃 알고리즘은 객체 탐색 과정에서 반복적인 비교 연산을 수행하여 불필요한 탐색 시간이 소요된다. 본 논문은 대화형 앱에서 신속한 스카이라인 결과를 산출하고자 연산 대상 객체의 범위를 축소함으로써 최근접 이웃 스카이라인 질의 알고리즘의 성능을 향상시킨 전처리 기법을 제안한다. 데이터 객체는 최대 40,000 개의 실험에서 제안 기법은 최근접 이웃 알고리즘보다 50% 빠른 성능을 나타내어 본 연구의 가용성이 증명되었다.

1. 서론

스마트 기기의 발전에 따라 대규모(Volume)의 멀티미디어 콘텐츠가 빠르게(Velocity) 생산되며, 각종 센서와 SNS로 인해 다양한(Variety) 데이터의 수집이 용이해졌다. 빅데이터가 발전하면서 데이터의 의미를 찾는 것이 중요해졌고 이로 인해 데이터 마이닝이 중요한 데이터 분석 기법으로 사용된다. 특히 데이터 객체의 속성이 다양한 경우에는 사용자의 선호도에 부합하는 데이터를 탐색할 수 있는 분석 기법이 필요하다.

Skyline Query [1]는 다차원 속성을 비교하여 사용자의 선호도에 맞는 객체를 추천하는 대표적인 기법으로 다른 속성에 의해 지배되지 않는 객체들을 탐색한다. 여기서 ‘지배된다’의 의미는 하나의 객체가 다른 객체에 대해 모든 속성에서 좋지 않은 값을 가지는

상태를 말한다. 예를 들어 중고차를 구매할 때 자동차 A, B가 속성으로 가격과 주행거리를 가지고 A는 (3, 5), B는 (6, 7)의 경우라고 하자. 사용자의 선호가 낮은 값일 때 B는 모든 속성에서 높은 값을 가지고 있으므로 A에 의해 지배된다. 즉, 점 A가 Skyline 후보군이 된다.

최근접 이웃 질의(Nearest Neighbor Query, NN) [2]는 Skyline Query의 정의에 부합하기 위해 빠른 결과를 제공한다. 먼저, D&C(Divide and Conquer) 알고리즘을 사용하여 데이터를 여러 부분의 파티션으로 나누고 각 부분에 대한 최근접 이웃 [3]을 구한다. NN의 성능은 탐색 영역에 포함된 데이터의 개수에 따라 달라지는데, 만약 탐색 영역에 데이터의 분포가 밀집되어 있다면 방문한 영역을 재 탐색하게 되므로 탐색 시간이 중복되어 전체적으로 성능 저하가 발생한다.

[‡] 이 논문은 2020년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (NRF-2018R1D1A1B07045642, NRF-2017R1D1A1B03035884).

§ 교신저자

본 논문에서는 NN 알고리즘을 사용할 때 전처리를 통해 성능 개선에 도움을 주는 Pre-NN 알고리즘을 제안한다. Pre-NN은 NN 질의에서 방문해야 할 데이터의 개수를 줄여 줌으로써 탐색 성능을 향상시킨다.

탐색할 데이터 객체가 많다면 NN은 최악의 성능을 가지게 되므로 객체들 사이의 지배관계를 평가하여 불필요한 데이터들은 제거하는 방법으로 NN의 성능 향상에 도움을 줄 수 있다.

논문의 구성은 다음과 같다. 2장은 기존의 스카이라인 질의에서 사용한 BNL, D&C 및 NN 알고리즘에 대해 설명한다. 3장에서는 논문에서 제안하는 Pre-NN 알고리즘을 소개하고 이를 기존 NN에 적용 시 갖게 되는 효과에 대해 기술한다. 4장에서 Pre-NN과 선행하는 NN 기법 간의 연산 속도를 비교함으로써 제안 기법의 성능을 증명한다. 마지막으로 5장은 결론을 서술한다.

2. 관련연구

본 절에서는 Skyline Query [1]에서 적용한 BNL(Block Nested Loop), D&C(Divide and Conquer)를 살펴보고 제안 기법이 개선하고자하는 NN 알고리즘 [2]에 대해 설명한다.

2.1 블록 중첩 루프 알고리즘

BNL은 Skyline을 구하기 위한 가장 직관적인 방법으로 Skyline 후보군 리스트를 만들고 리스트 내부의 객체와 새로 탐색되는 데이터 객체를 비교한다.

스카이라인 탐색을 시작하면 첫 번째 객체가 리스트에 들어가며 다음 탐색 객체와 리스트의 객체를 비교하여 만약 탐색 객체가 리스트의 객체를 지배한다면 리스트의 객체와 탐색 객체의 위치를 바꾼다.

리스트 내부 객체와 데이터의 객체를 비교할 때 세 가지 경우가 발생한다. 데이터 객체가 (1) 리스트 내부 객체에 의해 지배되는 경우 (2) 지배되지 않는 경우 (3) 위의 (1), (2)번이 모두 아닌 경우이다. 위 경우들 중 (1)을 제외하고는 모두 Skyline 후보군 리스트에 포함된다. 후보군 리스트를 사용하여 리스트 내부 객체들과 데이터 객체 전체를 비교하므로 BNL의 Skyline 후보군 리스트는 계산 과정이 길어질 수록 길어진다 [4].

2.2 분할 정복 알고리즘

D&C는 데이터를 여러 부분으로 나눈 뒤, 나눠진 부분들에 대해서 Skyline 객체를 구하고 부분 객체들을 합치면서 전체 Skyline 질의 결과를 구한다. 예를 들어 입력 받은 데이터의 중간 값을 계산한 뒤, 전체 데이터를 n 개의 파티션으로 나눈다. 파티션의 각 부분에서 Skyline을 구하고 해당 영역에서 다시 중간 값을 계산하여 파티션으로 나누는 일을 반복한다. D&C는 해당 과정을 파티션이 비어있거나 하나의 객체가 남을 때까지 반복한다. D&C 방식은 결국 전체 영역을 살펴보면서 반복적으로 파티션을 나누는 작업을 하기 때문에 전체 영역의 개수가 크면 클수록 성능이 나쁘다 [4].

BNL과 D&C는 Skyline 객체를 모두 구한 후에 한번에 결과를 반환하는 일괄처리 방식이다. 일괄처리 방식은 즉각적인 반응(interactive reaction)을 요구하는 대화형 애플리케이션에서 사용하기에는 부적절하다. 따라서 NN 알고리즘[2]에서는 이러한 점을 해결하기 위해 Divide and Conquer에 Nearest Neighbor 방식 [3]을 결합하여 스카이라인의 일부를 구함과 동시에 반환하는 알고리즘을 제안하였다.

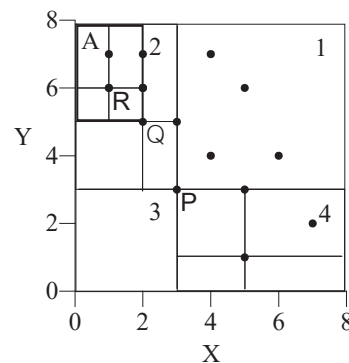
2.3 최근접 이웃 스카이라인 질의

NN 알고리즘은 D&C 방식을 토대로 최근접 객체를 찾는다. NN은 기존의 BNL과 D&C와 같은 일괄처리 방식이 즉각적인 반환을 할 수 없다는 단점을 해결하였다.

NN은 D&C 방식과 같이 영역을 분할하면서 해당 영역에서 스카이라인을 구하는 즉시 반환하기 때문에 대화형 애플리케이션에 적합하다. NN 알고리즘을 사용하기 위해서는 전체 데이터 중에서 영점 (0, 0)과 가까운 NN 객체를 찾고 해당 객체를 기준으로 2, 4 사분면을 대상으로 재연산한다. 이때, NN에 의해 지배되는 1 사분면의 객체들은 제거된다.

예를 들어, (그림 1)에서 첫 번째 NN 점은 전체 영역을 대상으로 구하게 되므로 유클리드 거리 [5]가 $3\sqrt{2}$ 인 P(3, 3) 객체가 된다. P를 대상으로 2, 4 사분면으로 영역을 나누고 2 사분면을 대상으로 NN 객체를 찾는다. 다음은 (0, 3)에서 (3, 8)까지의 영역에서 NN 객체를 찾게 되므로 유클리드 거리가 $\sqrt{29}$ 인 Q(2, 5)가 NN이 된다. 마지막으로 Q에 의해 2, 4 사분면으로 영역을 나누고 2 사분면을 살펴보면 된다. 유클리드 거리가 $\sqrt{37}$ 인 R(1, 6)이 NN에 해당한다.

여기서 영역 A의 객체들은 P, Q, R을 찾는 과정에서 반복적으로 재 탐색되어 3 번의 연산 과정에 참여하게 된다. A 영역의 객체 개수가 많을 수록 불필요한 연산에 노출되는 객체가 존재하며 이는 성능 저하를 발생시킨다. 위와 같은 NN의 단점은 객체들에 대한 지배관계 비교를 통한 탐색 대상 축소 방법으로 극복할 수 있다.



(그림 1) Nearest Neighbor Query

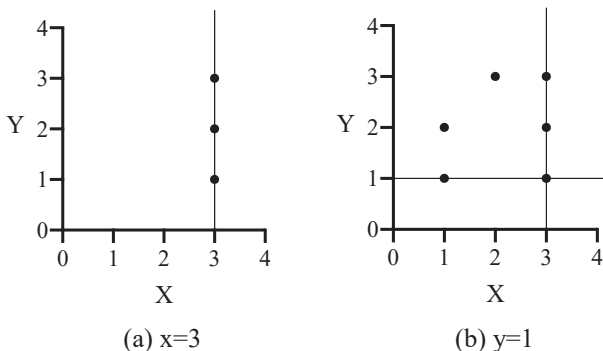
3. 스카이라인 질의 전처리 기법

스카이라인은 다량의 데이터 객체에서 사용자의 요구를 만족하는 속성을 중심으로 객체를 추천하기 위

해 사용된다. 기존의 스카이라인 질의에서 NN 알고리즘은 대화형 앱을 위해 실시간으로 스카이라인 객체를 출력하였으나 반복적인 객체 비교에 의해 탐색 성능이 저하되는 단점이 있었다.

본 논문에서 제안하는 스카이라인 질의 전처리 기법인 Pre-NN은 NN 알고리즘을 수행하기 전에 각 속성을 나타내는 축에서 탐색 범위를 제한 함으로써 처리 성능을 향상시킨다.

본 기법에서 속성 범위를 제한하는 방법은 다음과 같다. (그림 2(a))에서 x 축을 기준으로 x=3이라는 가상의 수직선을 긋는다면 (3, 1), (3, 2), (3, 3)의 객체가 존재한다. 해당 객체들은 모두 x 축은 3으로 고정되어 있고, y 축만 다르다. 즉 3으로 고정되어 있는 x 축 외에 y 축에 대해서만 여러 값을 갖는다. 선분에서 최솟값을 갖는 객체는 (3, 1)이 되므로 해당 정보만이 Skyline 후보군으로 저장한다. (그림 2(b))는 (그림 2(a)) 이후의 상황으로 y=1이라는 가상의 선에서 최솟값은 (1, 1)이 된다. 기존에 Skyline 후보군에 들어있었던 (3, 1)보다 (1, 1)이 x 속성에 대해 더 작은 값을 가지게 되므로 (3, 1)을 후보군에서 제거하고 (1, 1)을 후보군에 포함시킨다.



(그림 2) Pre-NN 예시

제안기법에서 각 축의 수직선으로 구별되는 최소 영역은 다음과 같이 정의된다.

Definition: 수직선의 최소범위(Minimum Range of Vertical Line).

ds를 탐색영역의 데이터 세트라 할 때 x, y는 데이터 객체의 속성이라 하자. 두 속성은 2차원 공간에서 각각 x 축과 y 축으로 표현된다. 이때, 각 축에서 데이터의 탐색 범위를 축소하기 위한 객체의 최소범위 (x, y)는 다음과 같다.

$$\{\forall x, \exists y, x \in ds \wedge y \in \min(y)\} \quad (1)$$

$$\{\exists x, \forall y, x \in \min(x) \wedge y \in ds\} \quad (2)$$

위의 정의는 x, y 축에 대한 범위 제한을 표현하고 있으며 수식 (1)은 x 축의 탐색 범위를 제한하는 것으로 x를 전체 데이터 세트(ds)로 놓고, y는 각 x의 수직선 상에 있는 좌표 중 최솟값을 의미한다. 이는 (그림 2(a))에 적용된다. 수식 (2)는 y 축의 수직선을

기준으로 y를 전체 데이터 세트(ds)로 놓고, x는 최솟값으로 탐색 범위를 제한한다.

Algorithm: pre_nn (ds)

Input: Dataset ds

M ← max value of integer

yMin ← dict-type which default value is m

xMin ← dict-type which default value is m

candidate ← empty dictionary

1: for x, y in data

2: if y < yMin[x]

3: yMin[x] = y

4: if xMin[yMin[x]] > x

5: if yMin[xMin[x]] is not m

and if yMin[xMin[x]] in candidate

delete candidate[xMin[yMin[x]]]

xMin[yMin[x]] = x

candidate[xMin[yMin[x]]] = yMin[x]

9: elseif xMin[yMin[x]] < x

if x in candidate

delete candidate[x]

12: return candidate

(그림 3) Pre-NN 알고리즘

Pre-NN 알고리즘은 크게 두 가지 단계로 진행된다. 첫 번째 단계로, 모든 데이터에 대하여 만약 x 값에 대해 최소값으로 저장된 y 값이(yMin[x]) 실제 y 속성보다 크다면 yMin[x]의 값을 y로 대체한다 (1~3). 두 번째 단계로, 만약 y 값에 대해 최솟값으로 저장된 x 값이 실제 x 속성보다 클 때(4 line) 만약 y의 최솟값으로 저장된 배열의 값이 초기값이 아니면서 후보군에 이미 들어 있다면 스카이라인 후보군에서 해당 객체를 지워줘야 한다 (5~6 line).

4번 줄에 이어서 xMin[yMin[x]]의 값을 x로 대체한다. 그 뒤 해당 객체를 스카이라인 후보군에 저장한다 (7~8 line). 4번 줄과 반대로 xMin[yMin[x]]의 값이 x보다 작고 또한 x가 후보군 안에 들어 있다면 candidate에서 x에 대한 정보를 삭제한다 (9~11 line). 마지막으로 저장된 후보군 Dict를 반환한다 (12 line).

Pre-NN 알고리즘은 같은 선상에 위치한 데이터들의 지배 관계를 비교하여 연산에 불필요한 객체들은 미리 제거해주는 알고리즘이다. 본 알고리즘의 장점은 데이터의 개수가 전체 영역의 최대 포함 가능 개수에 가까워질수록 밀집된 데이터가 많아지므로 불필요한 객체가 제거되어 탐색 성능이 향상된다는 것이다.

4. 실험

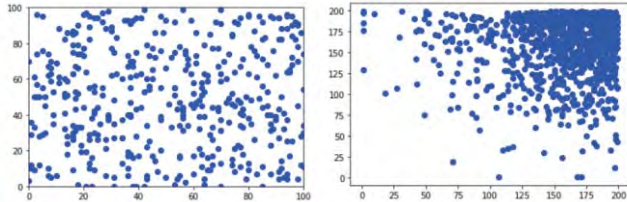
실험을 진행할 대상은 (그림 4(a))의 이산 균등 분포 데이터 세트와 (그림 4(b))의 이산 편향 분포 데이터 세트이다. NN 알고리즘과의 실험 환경을 같게 하기 위해 데이터의 중복은 없다고 가정한다.

실험 환경은 다음의 <표 1>과 같다.

<표 1> 실험 환경

구분	내용
시스템	Intel Xeon Silver 4114 CPU 2.20GHz * 2개, RAM 128GB

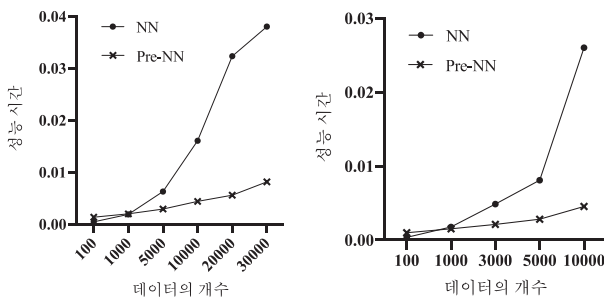
언어	Python
데이터 범위	200 개, 300 개
데이터 수	1,000 ~ 20,000 개
속성 수	2 개
실험 횟수	5,000 회



(a) 균등 분포 (b) 편향 분포
(그림 4) 이산 데이터 분포

x 축과 y 축의 범위는 편의를 위해 200 개로 지정하였고 중복이 없다는 가정에 따라 전체 영역으로 들어올 수 있는 데이터 세트의 개수는 $x \times y$ 로 40,000 개가 된다. 균등 분포의 경우 데이터 세트는 범위 사이의 값들을 랜덤하게 받아들여므로 데이터들은 (그림 4(a))와 같이 영역의 전반에 고르게 분포하게 된다.

실험은 극단적인 상황을 제외하기 위해 데이터의 개수를 최소 100 개, 최대 30,000 개로 지정한다. 편향 분포의 경우 (그림 4(b))와 같이 사각형의 특정 부분으로 치우친 데이터 세트가 형성되기 때문에 전체 영역으로 들어올 수 있는 데이터 개수의 1/4 크기에 해당하는 개수(사각형의 네 모서리 중 한 부분)만 실험한다. 즉 균등 분포의 경우 100 개, 1,000 개, 5,000 개, 10,000 개, 20,000 개, 30,000 개의 데이터로 실험을 진행하였고, 편향 분포의 경우 최대 데이터 개수의 1/4 개까지인 100 개, 1,000 개, 3,000 개, 5,000 개, 10,000 개 일 때의 pre-NN 과 NN 의 실행 시간을 비교하였다.



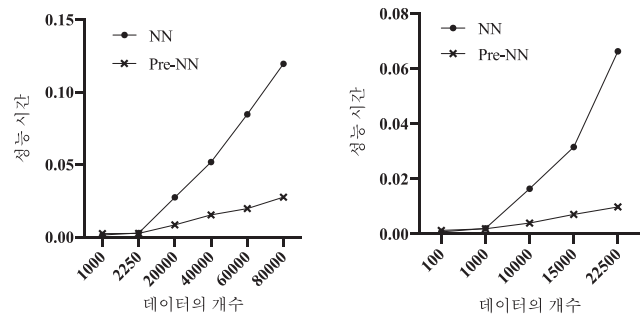
(a) 이산 균등 분포 (b) 이산 편향 분포
(그림 5) 200×200 평면에서의 성능 실험

데이터 공간이 x, y 축을 기준으로 확장하여도 동일한 성능 그래프를 나타내는지 확인하기 위해 두 번째 실험에서는 x 축과 y 축의 범위를 300 개로 지정하였다. 전체 영역으로 들어올 수 있는 데이터 세트 개수는 $x \times y$ 로 90,000 개가 된다. 균등 분포 데이터는 1,000 개, 2,250 개, 20,000 개, 40,000 개, 60,000 개, 80,000 개의 데이터로 진행한다. 편향 분포의 경우 최대 데이터 개수의 1/4 개까지인 100 개, 1,000 개, 10,000 개, 15,000 개, 22,500 개 일 때의 pre-NN 과 기존 NN 의 실행 시간을

비교하였다.

이산 균등 분포에서 Pre-NN 을 적용한 NN 은 기존 NN 에 비해 데이터의 밀집도가 커질 때마다 각각 약 1 배, 2 배, 4 배, 6 배의 순서로 빨라진다. 편향 분포에서 Pre-NN 을 적용한 NN 은 기존 NN 에 비해 약 1 배, 1.5 배, 3 배, 4.5 배의 순서로 빨라진다.

실험 결과 균등 분포의 경우 전체 영역으로 들어올 수 있는 최대 데이터 개수의 2.5%에 해당하는 개수 이상의 데이터가 분포되어 있으면 ((그림 5)에서는 데이터의 개수 1,000, (그림 6)에서는 데이터의 개수 2,250 에 해당) Pre-NN 의 성능이 좋아진다. 편향 분포의 경우 1,000 개를 기점으로 Pre-NN 을 사용했을 때 성능 향상을 보였다.



(a) 이산 균등 분포 (b) 이산 편향 분포
(그림 6) 300×300 평면에서의 성능 실험

5. 결과

본 논문에서 제안한 Pre-NN 알고리즘은 스카이라인 질의를 수행할 때 지배 관계를 미리 비교함으로써 NN 에서 처리할 데이터 객체의 수를 축소하였다. 이는 NN 에서 이웃하는 객체들에 대하여 비교해야 할 연산 횟수를 줄여줌으로써 전체 성능을 향상시키는 효과를 가져온다.

실험을 통해 제안 기법이 기존 NN 알고리즘 방식보다 빠른 속도로 스카이라인을 반환할 수 있음을 보였다.

참고문헌

- [1] S. Bořzsoňyi, D. Kossmann, and K. Stocker. "The skyline operator," In Proc. IEEE Conf. on Data Engineering, Heidelberg, Germany, pp. 421-430, 2001
- [2] D. Kossmann, F. Ramsak, and S. Rost, "Shooting Stars in the Sky: an Online Algorithm for Skyline Queries," VLDB, pp. 275-286, 2002
- [3] N. Roussopoulos, S. Kelley, and F. Vincent. "Nearest neighbor queries," In Proc. of the ACM SIGMOD Conference, San Jose, CA, May 1995
- [4] D. Papadias, Y. Tao, G. Fu, and B. Seeger: "An optimal and progressive algorithm for skyline queries," In: ACM SIGMOD International Conference on Management of Data, pp. 467-478, 2003
- [5] P. E. Danielsson, "Euclidean distance mapping," Computer Graphics and image processing, Vol. 14, No. 3, pp. 227-248, 1980.

시공간을 고려한 개인 맞춤형 경로 추천 알고리즘 제안

추민지*, 이혜진*, 박영호*,†

*숙명여자대학교 IT공학과

minchu96@sookmyung.ac.kr, adorablehye96@sookmyung.ac.kr, yhpark@sookmyung.ac.kr

†교신저자

Proposal of Personalized Path Recommendation Algorithm Considering Time and Space

Min-Ji Choo*, Hye-Jin Lee*, Young-Ho Park*,†

*Dept. of IT Engineering, Sookmyung Women's University

요 약

최근 스마트폰, 스마트 워치, 네비게이션 등과 같은 GPS가 내장된 기기가 늘어남에 따라 사용자의 위치 정보를 기반으로 하는 다양한 형태의 위치 기반 서비스와 다양한 목적에 따른 경로 추천 알고리즘이 제안되고 있다. 대부분의 연구들은 단순히 위치 및 거리 요소만 고려하기 때문에 시간의 측면에서 효율적이지 못하다는 단점이 있다, 이러한 문제를 효율적으로 해결하기 위해 시간과 공간을 모두 고려한 사용자 맞춤형 경로 추천 알고리즘을 제안한다.

1. 서론

최근 GPS가 내장된 기기가 기하급수적으로 증가함에 따라 사용자의 위치 정보를 기반으로 하는 다양한 형태의 위치 기반 서비스(LBS, Location-based Service)와 다양한 목적에 따른 경로 추천 알고리즘에 대해 활발한 연구가 진행 중이다[1, 2].

기존 연구들의 맞춤형 경로 추천 시스템은 대용량 빅데이터 처리 속도 개선을 위해 하둡 맵리듀스(Hadoop Mapreduce)[3], 스카이라인(Skyline), K-means 등의 다양한 알고리즘과 위치 기반 서비스를 융합하여 경로를 추천해 주는 알고리즘이 가장 많이 사용되고 있다.

이러한 위치 기반 맞춤형 경로 추천 알고리즘은 단순히 위치 및 목적지까지의 거리만 고려하기 때문에 시간의 측면에서 효율적이지 못한 경우를 추천해주는 경우가 생긴다. 효율적으로 경로를 추천하기 위해서는 위치 뿐 만 아니라 소요되는 시간 및 다양한 요소를 같이 고려해야 한다.

특히 각 요소들의 중요도는 사용자마다 다르기 때문에 적합한 경로를 추천해 줄 수 있는 맞춤형 경로 추천 알고리즘이 고안될 필요가 있다. 따라서 본 논문에서는 이를 효과적으로 해결하기 위해

시공간을 모두 고려한 개인 맞춤형 경로 추천 알고리즘을 제안한다.

2. 관련 연구

본 장에서는 제일 많이 사용되는 경로 추천 방법을 크게 2가지로 나누어 설명한다. 2.1절에서는 SNS데이터와 스카이라인을 활용한 경로 추천 방법, 2.2절에서는 Google Map을 활용한 목적 기반의 경로 추천 알고리즘에 대하여 설명한다.

2.1 SNS데이터와 스카이라인을 활용한 경로 추천

포인트 집합의 스카이라인은 다른 포인트가 지배하지 않는 포인트로 정의된다. 포인트는 모든 차원에 있어 우수하거나, 적어도 한 차원에서 우수하다면 다른 점을 지배한다[4]. 스카이라인 쿼리의 다차원을 포함할 수 있다는 특징 때문에 가격, 거리, 리뷰 등의 다양한 요소를 고려해야하는 경로 추천 알고리즘에서 연구가 활발히 진행되어 왔다.

Yu-Ting Wen이 제안한 KSTR(Keyword-Aware Skyline Travel Route Recommendation)[5]는 SNS의 이미지와 태그 데이터의 키워드를 추출하고 패턴을 분석하여 여행 경로를 추천한다.

위의 알고리즘은 실험결과를 통해 사용자에게 흥미가 높은 여행 경로를 추천해 줄 수 있음을 보여준다. 하지만 SNS데이터를 통해 키워드를 추출하기 때문에 잘못된 정보나 거짓된 데이터를 수집할 수 있다는 단점이 존재한다.

2.2 Google Map을 활용한 목적 기반의 경로 추천

대부분의 경로 추천 알고리즘들이 비용의 최소화를 목적으로 제안하지만 사용자들은 비용이 더 들더라도 우선시하는 목적이 있는 경우도 있다.

Yihong Zhan이 제안한 연구는 주변 풍경과 편의시설을 중요 요인으로 두고 경로를 추천하는 알고리즘[6]을 제안한다. 주변 풍경에 의한 경로는 구글 지도의 파노라마 이미지를 통해 색상과 감지되는 물체의 태그를 바탕으로 계산되었다. 또한 시설 기반의 경로는 가중 엔트로피를 사용하여 주어진 경로와 나란히 존재하는 시설 유형의 다양성을 측정하는 방법으로 경로를 계산하였다. 이를 통해 사용자는 같은 목적지를 향해 가더라도 다양한 경로를 추천 받을 수 있다.

위의 알고리즘은 데이터를 Google Map으로 한정하기 때문에 고려할 수 있는 요소가 극히 제한되어 있다는 한계점이 있다.

본 논문에서는 단순 위치만 고려하거나 제한적인 요소들로 경로를 추천하는 기존 연구들의 단점을 보완하기 위해 시공간 및 다양한 요소를 반영할 수 있는 사용자 맞춤 경로 추천 알고리즘을 제안한다.

3. 사용자 목적에 따른 경로 추천 알고리즘

본 장에서는 스카이라인 기반의 사용자 목적에 따른 경로 추천 알고리즘 단계에 대하여 설명한다. 단계는 총 3단계로 구성된다.

- Step 1(View 생성 단계)** : 기존 데이터베이스에서 목적지까지의 경로를 탐색하여 각 장소의 요소들을 View에 임시 저장한다.
- Step 2(가중치 계산 단계)** : 각 장소의 요소별로 점수를 매긴 후, 사용자의 조건과 목적에 적합한 가중치를 부여하여 장소의 랭킹을 계산한다. 장소의 랭킹을 구하는 식은 다음과 같다.

$$(\text{장소의 랭킹}) = \sum_{i=0}^n \text{factor}(i) * \text{weight}$$

* : 고려해야 할 요소들 중 i번째

- Step 3(시공간을 고려한 경로 생성 단계)** :

계산된 랭킹의 장소 카테고리 별로 내림차순 정렬하여 공간과 시간적 요소를 고려한 최적의 경로를 만든다.

위의 알고리즘을 통해 사용자는 원하는 목적에 따라 우선 순위가 반영된 맞춤형 경로를 추천 받을 수 있다. 실험에 사용된 데이터 셋 및 예상 결과는 4장 실험 및 예상 결과에서 확인할 수 있다.

4. 실험 기획 및 예상 결과

본 장에서는 3장에서 설명한 스카이라인 기반의 운전 목적 기반의 최적의 맞춤 경로 추천 알고리즘의 실험 및 예상 결과를 설명한다. 고려 요소는 평 점, 시간, 비용 총 3가지이며 탐색 장소 카테고리는 식당, 숙소, 관광지 총 3가지라고 가정한다. 또한 지정된 일 수 당 식당 2곳, 숙소 1곳, 관광지 2곳을 탐색하여 경로를 추천하며 마지막 날은 제외한다.

예제 1. 사용자 U1이 여행을 목적으로 서울에서 경주까지 1박의 평점을 위주로 한 경로를 추천 받고자 한다. 이때 장소 탐색 조건(O)은 평점 3점 이상, 출발지에서 장소까지의 거리는 시간 60분 이하, 비용은 관계 없다고 가정한다.

기존의 경로 탐색 알고리즘을 사용하여 서울에서 경주까지의 경로(Pi)를 모두 탐색한 뒤 경로 탐색 알고리즘을 통해 View에 저장한다. 표 1은 경로 탐색 알고리즘을 통해 View에 저장한 결과를 나타낸 것이다. 각 요소의 가중치는 평점=0.5, 시간=0.25, 비용=0.25로 두어 각각의 장소마다 평점, 거리, 시간을 구하여 랭킹을 계산한다. 이때 조건O에 부합하지 않는 장소가 있다면 계산에서 제외한다. 표2[7]는 계산 결과를 나타낸 것이며, 시공간적 요소를 고려하여 1박의 경로를 추천 받는다.

실험의 결과는 점수의 최소값으로 정렬한 A1, R2, R3, T2, T3가 최종적으로 경유할 장소이다. 이 장소들 내에서 다시 최소값으로 랭킹을 매기면 T2 ⇒ T3 ⇒ A2 ⇒ R2 ⇒ R3 순서의 경로가 나오게 된다. 다음은 본 예제를 질의로 표현한 것이다. "f(t) = (5-평점)*0.5+거리*0.25+시간*0.25"로 계산된다.

```
SELECT *
FROM Place P
WHERE P.starscore > 2 or P.time < 60
ORDERBY f(t)
```


표 1. 서울⇒경주 데이터베이스 예시

경로	장소	장소 카테 고리	평점 (최대 5점)	시간 (분)	비용 (1000원)
P1	A1	숙소	3	30	50
P1	R1	식당	2	30	30
P1	R2	식당	3	50	20
P1	T1	관광지	5	25	15
P2	A2	숙소	3	30	25
P2	R3	식당	5	50	40
P2	T2	관광지	4	10	5
P2	T3	관광지	3	25	10

표 2. 각 장소 별 가중치 반영 한 랭킹 계산 예시

장소	장소 카테 고리	평점 (최대 5점)	시간 (분)	비용 (1000 원)	점수
A1	숙소	1	7.5	12.5	21
A2	숙소	1	7.5	6.25	14.75
R1	식당	2	30	30	Non Score
R2	식당	1	12.5	6.25	19.75
R3	식당	0	12.5	10	22.5
T1	관광지	0.5	6.25	3.75	10.5
T2	관광지	0.5	2.5	1.25	4.25
T3	관광지	1	6.25	2.5	9.75

5. 결론 및 향후 연구

본 논문에서는 위치 및 시공간을 모두 고려한 사용자 맞춤 경로 추천 알고리즘을 제안하였다.

기존의 위치나 거리만 고려한 위치 기반 맞춤형 경로 추천 시스템은 시간의 측면에서 효율적이지 못하는 문제가 발생한다. 이를 효율적으로 해결하기 위해서는 위치뿐만 아니라 소요되는 시간 및 다양한 요소를 같이 고려해야 한다.

특히 각 요소들의 중요도는 사용자마다 다르기

때문에 이에 적합한 경로를 추천해 줄 수 있는 맞춤형 경로 추천 알고리즘을 제안하였다.

하지만, 본 논문에서 제안한 알고리즘은 경로에 같은 장소 카테고리 연속적으로 나올 때의 예외 상황을 고려하지 못한 문제점이 있으며 이를 향후 연구로 남겨둔다.

사사문구

이 논문은 2020년도 정부(미래창조과학부)의 재원으로
정보통신기술진흥센터의 지원을 받아 수행된 연구임.
(No.2016-0-00406. (기반 SW-창조씨앗 2단계)SIAT형
CCTV 클라우드 플랫폼 기술 개발)

참고문헌

- [1] 정주원; 박석. 도로 교통망에 대한 사용자의 선호도 변화를 반영한 경로 추천. *정보과학회논문지*, 2019, p. 77-85.
- [2] Dimitris, Papadimas; Yufe; Tao; Greg, Fu; Bernhard, Seeger, An optimal and progressive algorithm for skyline queries. In: *Proceedings of the 2003 ACM SIGMOD international conference on Management of data*. 2003. p. 467-478.
- [3] 이계형; 조영훈; 이태호; 박희민. 대용량 경로데이터 분류에 기반한 경험적 최선 경로 추천. *정보과학회 컴퓨팅의 실제 논문지*, 2015, p. 101-108.
- [4] KOSSMANN, Donald; RAMSAK, Frank; ROST, Steffen. Shooting stars in the sky: An online algorithm for skyline queries. In: *VLDB'02: Proceedings of the 28th International Conference on Very Large Databases*. Morgan Kaufmann, 2002. p. 275-286.
- [5] WEN, YuTing; Cho, KaeJer; Peng, WenChih; Yeo, Jinyoung; Hwang, Seungwon. KSTR: Keyword-aware skyline travel route recommendation. In: *2015 IEEE international conference on data mining*. IEEE, 2015. p 449-458.
- [6] ZHANG, Yihong; Panote, Siriaraya; Yuanyuan, Wang; Shoko, Wakamiya; Yukiko, Kawai; Adam, Jatowt. Walking down a different path: route recommendation based on visual and facility based diversity. In: *Companion Proceedings of the The Web Conference 2018*, 2018, p. 171-174.
- [7] 임선영; 박영호. Top-k 질의를 위한 격자 스카이라인 생성 및 처리 기법 연구. *한국정보과학회*, 2013, p. 85-93.

제53회
2020 온라인 춘계학술발표대회

인공지능



효과적인 이상 진단을 위한 클러스터링의 타당성 연구

이현용*, 김낙우*, 이준기*, 이병탁*

*한국전자통신연구원

{hyunyonglee, nwkim, jungi, bytelee}@etri.re.kr

A Feasibility Study on Clustering for Effective Anomaly Detection

HyunYong Lee*, Nac-Woo Kim*, Jun-Gi Lee*, and Byung-Tak Lee*

*Electronics and Telecommunications Research Institute (ETRI)

요 약

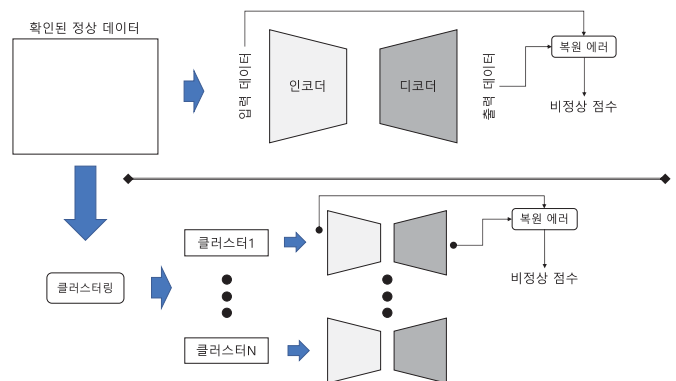
이상 진단은 주어진 데이터의 정상 유무를 진단하는 방법으로써 다양한 분야에 걸쳐 요구되는 기능이다. 이상 진단은 대상 환경에서 발생하는 데이터의 특성 등에 따라 다양한 방법으로 구현이 될 수 있는데, 본 연구에서는 정상 데이터가 다수의 클래스로 구분될 수 있는 상황에서의 이상 진단을 효과적으로 할 수 있는 방법에 대해서 다루고자 한다. 특히, 실험을 통해 정상 데이터를 유사한 데이터들끼리 구분하여 처리하는 경우와 그렇지 않은 경우의 비교를 통해서, 정상 데이터를 유사한 데이터들끼리 구분하여 이상 진단을 진행하는 방법의 타당성을 검증한다.

1. 서론

이상 진단은 기계학습 등과 같은 다양한 방법에 기반하여 주어진 데이터 (또는 상태)가 정상인지 비정상인지를 판단하는 것을 일컫는다 [1]. 이상 진단은 공장 설비 등의 이상 진단, 전력 소비의 이상 진단, 사람의 건강 상태의 이상 진단 등에 널리 요구되는 기술이다. 이상 진단은 진단 대상이 되는 환경의 데이터 특성 등에 따라서 다양한 방법으로 구현이 될 수 있는데, 주요한 연구 주제 중 하나는 효과적인 비정상 점수(abnormality score)를 찾는 것이다. 비정상 점수는 주어진 데이터의 비정상 유무 판단을 위해서 사용되며, 효과적인 비정상 점수는 정상 데이터와 비정상 데이터를 정확하게 구분할 수 있어야 한다.

본 논문에서는 보다 효과적인 비정상 점수 도출을 위한 방법을 제안하는데, 다음과 같은 상황을 고려한다. 정상 데이터는 다수의 클래스들로 구분될 수 있지만, 명시적으로 주어진 클래스 레이블은 없다. 본 논문에서 제안하는 방법의 핵심은, 정상 데이터를 구분없이 하나의 모델로 처리하는 것과 레이블은 없지만 클러스터링을 통해서 임의의 클래스로 분류한 뒤 클래스 별로 모델을 만들어 처리하는 것에는, 도출되는 비정상 점수 간의 유용성 측면에서 차이가 있을 것이라는 점이다. 본 논문에서는 본 연구의 시작점으로써 실험을 통해 위의 두 경우에서의 비정상 점수 간의 유용성을 비교한다.

2. 클러스터링 기반 이상 진단



(그림 1) 클러스터링 기반 이상 진단 구조.

본 연구에서 추구하는 이상 진단 구조는 그림 1에 표현되어있다. 확인된 정상 데이터가 주어졌다고 보고, 주어진 정상 데이터에 기반하여 이상 진단을 위한 모델을 어떻게 구성하느냐가 관건이다. 종래의 대부분의 방법은, 정상 데이터의 구분없이 전체 정상 데이터를 기반으로 하나의 모델을 학습하고, 이를 기반으로 이상 진단을 진행한다. 예를 들어, 주어진 정상 데이터에 기반하여 하나의 오토인코더 모델[2]을 만들 수 있고, 복원 에러를 비정상 점수로 사용하여 이상 진단을 진행할 수 있다. 이 때, 복원 에러가 지정된 기준 이상인 경우에, 비정상적으로 간주할 수 있다. 반면, 본 연구에서 추구하는 방법은, 주어진 정상

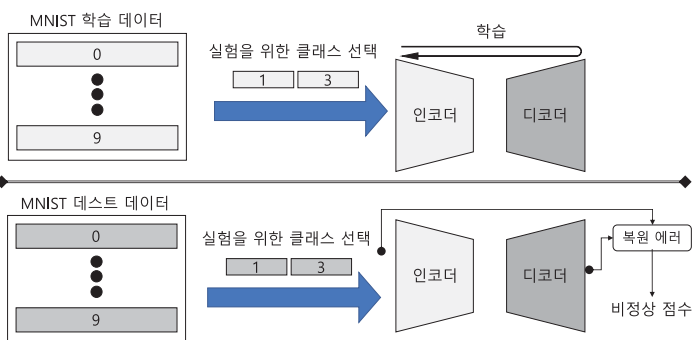
데이터 전체를 위한 하나의 모델을 만들기 보다, 정상 데이터를 유사한 특성을 지닌 클러스터로 분류한 뒤 클러스터 별로 모델을 만드는 것이다. 정상 데이터의 클러스터링을 위해서 K-means 클러스터링[3]과 같이 잘 알려진 방법을 사용할 수 있다. 단, 몇 개의 클러스터로 구분해야 하는지는 본 논문의 관심 사항이 아니다. 클러스터링 기법을 통해 주어진 정상 데이터가 다수의 클러스터로 구분된 후에, 클러스터 별로 하나의 모델을 만들 수 있다. 예를 들어, 클러스터 별로 하나의 오토인코더 모델을 생성할 수 있다. 이 경우, 주어진 테스트 데이터의 이상 진단을 위해서는, 클러스터링 기법을 통해 테스트 데이터가 어느 클러스터에 속하는지는 먼저 판별한 후에, 해당 클러스터의 오토인코더 모델을 적용하여 복원 에러를 추출하고 이를 기반으로 이상 진단을 진행할 수 있다.

전술한 방법과 같이 주어진 정상 데이터를 클러스터링을 통해 다수의 클러스터로 구분하는 것은, 클러스터 별 모델을 해당 클러스터의 데이터에 특화시킴으로써 비정상 데이터의 경우 비정상 점수가 더 극대화되도록 하기 위함이다. 다시 말하면, 상이한 특성을 보이는 정상 데이터를 하나의 모델을 통해 처리하는 것보다, 유사한 특성을 보이는 정상 데이터들끼리만 묶어서 하나의 모델을 통해 처리하는 방법의 경우에 해당 모델은 해당 클러스터의 데이터 특성을 더 잘 이해하고 표현하게 되어서, 비정상 데이터의 경우 복원 에러가 더 극대화되게 된다.

해당 클러스터의 학습 데이터에 기반하여 하나의 오토인코더 모델을 학습하고, 테스트 데이터를 적용하여 복원 에러를 점검한다. 비정상 점수로 사용되는 복원 에러는 오토인코더의 입력 데이터와 출력 데이터 간의 mean squared error 를 사용한다. 비정상 점수로 사용되는 복원 에러의 값이 작을수록 비정상 점수의 유용성이 더 크다고 볼 수 있다. 이는 해당 클러스터에 속한 데이터들을 더 잘 표현한다고 볼 수 있기 때문이다. 성능 검증 목적을 위해 별도의 클러스터링은 진행하지 않고, 공개된 클래스 정보를 클러스터 정보로 사용하였다. 다양한 클러스터 경우의 성능 비교를 위해서, 클러스터에 속하는 클래스 수를 상이하게 실험을 진행하였다. 실험은 Tensorflow 2.0 버전에 기반하여 진행하였다.

<표 1> 타당성 실험 결과

클러스터에 속한 클래스들	복원 에러 평균	복원 에러 표준편차
0	0.0141	0.005
1	0.004	0.0034
2	0.0172	0.0057
3	0.0152	0.0057
4	0.013	0.0049
5	0.0164	0.0055
6	0.0131	0.0054
7	0.0104	0.0054
8	0.0179	0.0064
9	0.0115	0.0056
1,3	0.01	0.0074
2,4	0.0166	0.0058
3,4	0.0156	0.0057
5,6	0.0157	0.0058
1,7,9	0.009	0.0058
0,3,4,7,8	0.0164	0.0063
1,2,5,6,9	0.0144	0.0075
0,1,2,3,4,5,6,7,8,9	0.016	0.0072



(그림 2) 타당성 검증 방법.

3. 실험 기반 타당성 검증

2 장에서 전술한 클러스터링 기반 이상 진단 기법의 타당성을 검증하기 위해서 기초 실험을 진행한다. 그림 2 는 이러한 과정을 보여준다. 실험의 목적은, 클러스터 별로 포함된 클래스의 수에 따른 그리고 클러스터에 포함된 클래스 간의 유사성 정도에 따른 비정상 점수 유용성 비교이다. 실험을 위해서 10 개의 클래스로 구성되는 MNIST 데이터[4]를 사용하였다. MNIST 는 0 부터 9 까지의 손글씨에 대한 데이터이다. 임의의 수의 클래스를 하나의 클러스터로 간주하고,

표 1 은 타당성 실험 결과를 보여준다. 가장 왼쪽의 열은 한 클러스터에 속한 클래스들을 보여준다. 가운데 열은 클러스터에 속한 모든 테스트 데이터에 대한 복원 에러의 평균을, 맨 오른쪽 열은 복원 에러의 표준 편차를 보여준다. 전술하였듯이, 복원 에러 평균이 낮을 수록 비정상 점수의 유용성이 높다고 판단할 수 있다. 0 부터 9 까지의 모든 클래스를 하나의 모델로 처리한 경우, 복원 에러의 평균은 0.016 이다. 반면, 하나의 클래스별로 모델을 구성한 경우에는 2,5,8 클래스의 경우를 제외하고는 더 낮은 복원 에러 평균

값을 보인다. 특히, 클래스 1 의 경우 복원 에러 평균은 0.004 이며 복원 에러 표준편차도 0.0034 로 매우 낮다. 추가로 점검해본 경우는, 2,4 와 같이 서로 상이한 숫자 모양을 보이는 클래스들을 하나의 클러스터로 묶은 경우와 1,7,9 처럼 비슷한 숫자 모양을 보이는 클래스들을 하나의 클러스터로 묶은 경우이다. 숫자 모양이 비슷한 경우는 비슷한 특성을 보이는 것으로 이해될 수 있다. 2,4 클래스를 묶은 경우, 모든 클래스를 하나의 클러스터로 묶은 경우와 유사한 복원 에러 평균을 보이는 반면, 1,7,9 를 묶은 경우 복원 에러 평균은 0.009 로 매우 낮아졌다. 표 1 에 보이는 나머지 경우에서도 관찰할 수 있는 것처럼, 이처럼 유사한 특성을 보이는 클래스끼리 클러스터로 묶는 것은 비정상 점수의 유용성을 향상시키는 것을 볼 수 있다. 반면, 관련이 없거나 특별한 구분없이 모든 데이터를 하나의 모델로 처리하는 경우에는 비정상 점수의 유용성이 낮아지는 것을 볼 수 있다.

4. 결론

효과적인 이상 진단을 위한 핵심 기술 중 하나는 정상 데이터와 비정상 데이터를 더 잘 구분하기 위한 비정상 점수를 도출하는 것이다. 본 논문에서는, 확보된 정상 데이터를 클러스터링 기법을 통해 다수의 클러스터로 구분하고 클러스터별로 모델을 구성함으로써 보다 효과적인 비정상 점수를 도출하는 방법의 타당성을 실험을 통하여 검증하였다. 본 연구의 연속을 위해서, ImageNet 과 같이 MNIST 보다 좀 더 복잡한 형태의 데이터에 기반하여 타당성 검증을 진행할 필요가 있다. 뿐만 아니라, 제안 방법의 핵심이 클러스터 별로 모델을 구성하는 것인데, 대상 테스트 데이터의 클러스터 뿐만 아니라 나머지 클러스터들의 모델들을 활용하여 비정상 점수를 도출하는 방법에 대한 연구도 의미가 있을 것으로 보인다.

감사의 글

이 연구는 정부의 ETRI R&D 프로그램(20ZK1140)의 재원을 받아 수행된 연구임.

참고문헌

- [1] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey" ACM Computing Surveys, vol. 41, no.3, July 2009.
- [2] P. Baldi, "Autoencoders, unsupervised learning and deep architectures" International Conference on Unsupervised and Transfer Learning Workshop, Washington, USA, 2011, pp.37-50.
- [3] T. Kanungo, et al., "An efficient k-means clustering algorithm: Analysis and implementation" IEEE Transactions on Pattern Analysis and Machine Intelligence, vol.24, no.7, pp.881-892, 2002.
- [4] The MNIST DATABASE of handwritten digits, <http://yann.lecun.com/exdb/mnist/>

N-grams를 사용한 CNN 기반의 악성코드탐지 기법 연구

허정원, 문봉교
동국대학교 컴퓨터공학과
hacel@dongguk.edu, bkmoon@dgu.edu

Malware Detection Based on CNN with N-grams

Jeong-Won Her, Bong-Kyo Moon
Dept. of Computer Science Engineering, Dongguk University

요 약

본 논문에서는 악성코드탐지 기법으로 n-grams를 사용한 특징 추출을 통해 이미지 인식 분야에서 널리 쓰이는 Convolutional Neural Network로 학습하는 프레임워크를 제안한다. 윈도우즈 실행 파일의 PE 포맷에서 특징을 추출하여 6-grams 확률을 구하고 grayscale 을 통해 이미지로 변환한다. 이것을 기존에 연구된 탐지방법과 비교하여 우수함을 보인다. 학습에 사용된 데이터는 총 55,000개로 5-folds 교차검증을 하였으며 예측 정확도는 98.87%였다.

1. 서론

오늘날에는 매 순간 새로운 악성코드들이 등장하고 있다. 하지만 현재 사용되는 탐지 알고리즘의 대부분은 악성코드의 해시값과 같은 시그니처를 기반으로 한다. 새롭게 변형된 악성코드는 기존 파일의 시그니처를 비교해 검출할 수 없다. 따라서 기존 방법의 단점을 해결하기 위해 딥러닝과 통계 기반의 탐지 기법이 주목받고 있다.

2. 관련 연구

악성코드의 딥러닝을 위한 특징 추출 기법으로 문자열 추출, import tables, byte n-gram, opcode, byte entropy 등을 살펴보는 방법들이 있다. Saxe et al.[1]은 byte entropy, import tables, 문자열 추출, PE metadata 네 가지 특징의 조합에 대한 Deep Neural Network (DNN) 탐지율을 비교한다. 다양한 특징 추출방법을 제시하지만, n-grams 방법에 대한 제시가 없으며 DNN만 사용하여 특징 인식에 더 뛰어난 성능을 보이는 CNN에 대한 논의가 부족하다.

특징 추출을 할 범위를 정하는 것도 중요하다. 실행 파일의 크기는 다양하다. 실행 파일의 모든 내용에 대한 특징 검사는 매우 느리고 불필요한 정보

를 검토하게 될 가능성이 크다. Stolfo et al.[2]은 파일의 시작과 끝만을 n-gramming 하여 정보를 추출한다. 본 연구도 유용한 부분만을 살펴보고, 특정 길이를 얻기 위해 PE 헤더만을 특징 추출에 사용한다.

N-grams가 악성코드 분류에 어떤 성능을 지니는지에 대해 Raff et al.[3]은 Elastic-Net과 LR를 사용해 조사한다. N-grams를 파일에 효과적으로 적용하는 방법을 제시하지만, Elastic-Net과 LR에 대한 성능만 제시되는 한계가 있다.

Raff et al.[4]에선 다양한 학습 기법의 악성코드 탐지 성능을 비교한다. Raff도 PE 포맷을 특징으로 추출해 악성코드를 탐지한다. 이것에 대해 Extra Random Trees(ET), Random Forests(RF), Logistic Regression(LR), Fully Connected Neural Network(FC), Long Short-Term Memory(LSTM) 다섯 가지 학습 기법을 적용하고 탐지 성능을 비교한다. 다양한 탐지 기법에 소개가 있지만 역시 CNN에 대한 논의가 부족하다.

본 연구에서는 n-grams 특징 추출과 CNN 학습 기법을 동시에 사용해 기존 연구 결과와 탐지 정확도를 비교한다. 결과로 얻은 탐지 정확도는 98.87%로 기존 연구 결과보다 우수한 악성코드탐지에 기법을 보인다.

3. 제안 모델

제안하는 탐지 프레임워크는 (그림 1)과 같이 학습한다. 첫째로 파일 특징 추출로 PE 포맷 추출과 n-grams 제작 단계로 나뉜다. 둘째로 데이터의 이미지화 단계이다. 이 단계에서 PE 포맷의 byte는 문맥에서 등장할 확률에 따라 grayscale 하여 이미지로 변환된다. 셋째로 CNN의 학습이다. CNN은 filter를 사용하여 데이터의 특징을 추출한다. 따라서 사소한 내용의 차이(회전, 왜곡, 변형)가 있어도 특징을 검출하기 때문에 악성코드 변종에 대한 감지가 수월할 것으로 생각된다. 다음 단락에서 각각의 단계를 설명한다.

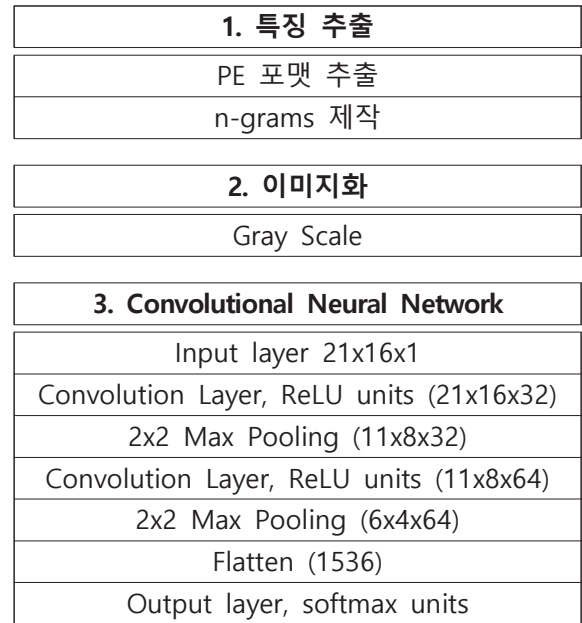
가. 특징 추출

PE 포맷은 윈도우 OS에 실행 파일 포맷으로 실행에 필요한 정보, 메모리 로드 위치, 사용하는 라이브러리, 실행시간에 결정되는 정보를 담은 구조체이다. PE 포맷은 (그림 2)와 같이 크게 DOS header, Common Object File Format(COFF), optional header, import tables로 나뉜다. 본 연구는 PE 포맷에서 DOS header, COFF, Optional header 부분을 추출해 총 328 bytes 배열을 얻게 된다. 이것은 실행 파일의 핵심적인 특징이며, 적은 분량이고, 일정한 크기를 가진다. 이 특징들은 이후 신경망에 적용하기 쉽게 해준다.

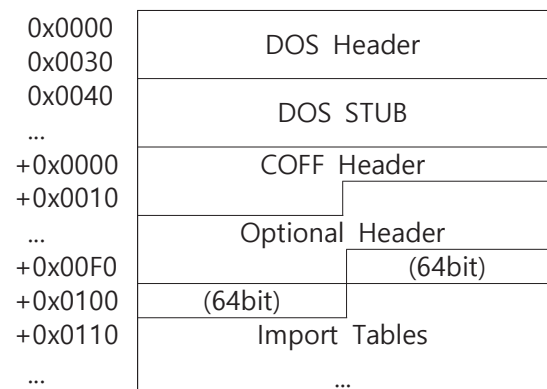
n-grams는 통계에 기반해 나타날 단어를 추론한다. n-grams는 앞서 등장한 n-1개 단어 h에 대해 n번째 단어 w가 나타날 확률을 (식 1)과 같이 계산한다.

$$P(w|h) = \frac{C(h+w)}{C(h)} \quad (\text{식 1})$$

n-grams로 byte의 문맥을 학습시킬 수 있다. 이 방법은 대상에 대한 사전 지식이 필요 없이 특징의 자동적인 추출이 가능하다는 장점이 있다. 본 연구에서는 6-grams로 13500개의 정상코드의 문맥을 학습시켜 byte의 등장 확률을 구한다.



(그림 1) 악성코드탐지 프레임워크



(그림 2) PE 포맷의 구조

나. 이미지화

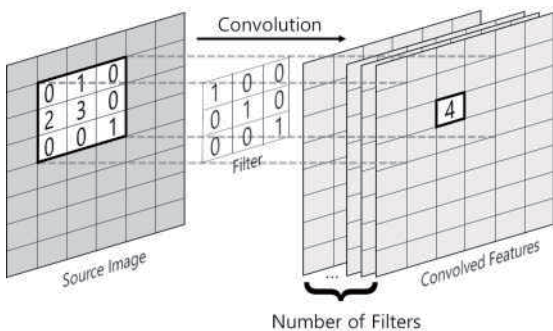
앞선 방법으로 얻은 byte 등장 확률을 각각의 이미지 픽셀로 변환하게 된다. 정상코드의 문맥에 가까울수록 높은 확률값을 가지고 처음 등장하는 문맥, 즉 악성코드이면 낮은 확률값을 가진다. 0을 검은색 1을 흰색으로 하여 0~1 범위의 확률값을 grayscale 하여 이미지로 바꿔주게 된다. 따라서 문맥에 어긋나는 부분일수록 검은색으로 나타나게 된다. 328 bytes 배열은 위치를 알기 쉽게 16개의 행을 가지도록 한다. $328/16 = 20.5$ 이므로 8개의 0 값 padding을 더해 (그림 3)과 같은 $16 \times 21 (=336)$ 크기의 이미지를 얻는다.



(그림 3) 16x21 Grayscale 예시

다. Convolutional Neural Network

Convolution은 (그림 4)와 같이 특정한 필터값으로 입력 데이터에 대한 합성곱 연산을 수행함을 말한다. 따라서 필터에 따라 이미지 일부분이 강조되고 이는 특징을 추출하는 기능을 한다. 본 연구에서는 2개의 convolution layer를 사용하며 각각 32, 64개의 3x3 필터 합성곱 연산을 한다.



(그림 4) Convolution

4. 실험 및 분석

사용된 데이터는 KISA에서 수집한 윈도우즈 실행 파일 정상코드 13,500개 악성코드 41,500개 총 55,000개의 데이터를 사용하였다. 이 데이터를 사용할 때 5-fold cross validation 기법을 적용하여 검증하였다. 실험 환경은 윈도우즈 10(64bit) 운영체제에서 Tensorflow backend Keras로 실험하였다. 상세 실험 환경은 <표 1>에 기술하였다.

제안하는 모델과 비교하는 모델은 Raff et al.[4]의 방법들이다. Raff는 악성코드탐지를 위해 PE 포

맷에서 328byte를 추출해 FC, LSTM, ET, RT, LR 3-grams를 사용한다. <표 2>는 Raff가 industry partner에게 받은 데이터(Group B)를 사용해 얻은 모델 정확도와 제안하는 모델의 정확도를 비교한다.

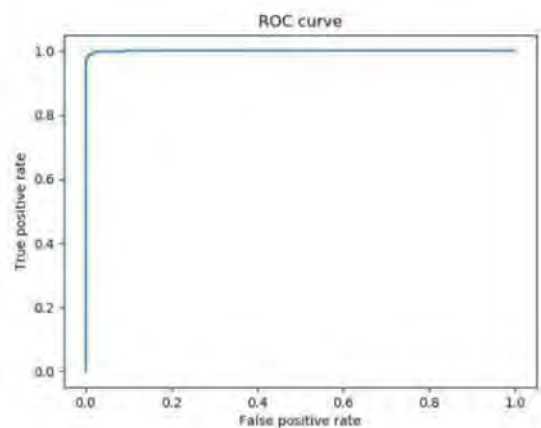
앞서 얻은 모델의 정확도(Accuracy)는 98.87%이다. 하지만 모델성능을 정확도로만 판별하는 것은 위험하다. 이 맹점을 해결하기 위해 Receiver Operating Characteristic(ROC)을 사용한다. (그림 5)는 6-grams로 전처리를 한 ROC 그래프이고 (그림 6)은 Raff의 모델에 대한 ROC 그래프이다. 이것을 수치로 정확히 판별하기 위해 Area Under the Curve(AUC) 값을 구한다. 이 값은 100%의 정확도를 가지는 완벽한 모델에서 1 값을 가진다. <표 2>에서 제안 모델과 Raff의 모델에 대한 AUC 값을 비교하였다. 6-grams로 전처리를 한 제안 모델에 대해 AUC는 0.999의 값을 가져 단순히 신경망을 적용한 것보다 더 좋은 모델을 생성했음을 알 수 있다.

이름	내용
OS	Windows 10.0.18362
CPU	i5-8250U 3.40GHz
RAM	8GB
Tensorflow	2.0.0
Keras	2.3.1

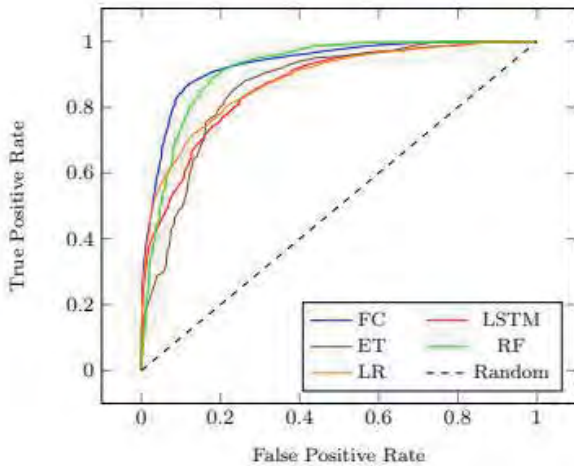
<표 1> 실험 환경

	Accuracy(%)	AUC(%)
FC	83.7	91.4
LSTM	77.5	86.7
ET	80.7	86.1
RT	82.3	91.2
LR 3-grams	77.8	87.3
CNN 6-grams	98.9	99.9

<표 2> 결과 비교



(그림 5) 6-grams 전처리 CNN의 ROC 그래프



(그림 6) ROC plot for all models on Group B test data[4].

4. 결론

본 연구는 배경 지식 없이 적절한 특징 추출 기법과 빅데이터만으로도 효과적인 학습을 수행할 수 있음을 보여준다. 그러나 PE 포맷의 특징 추출 기법은 windows 운영체제에서만 적용할 수 있다. 이점은 다른 운영체제의 실행 파일에 적용할 수 없다는 명확한 한계점을 지닌다. 이를 개선하기 위해 악성 코드 분류와 통합 플랫폼을 만들 수 있을 것이다. Islam et al.[5]은 문자열을 추출해 효과적으로 악성 코드 분류법을 제안한다. 이 논문에서 보이는 분류 정확도는 98.8%로 상당한 정확도로 분류 가능함을 보인다. 이러한 방법을 응용해 효과적으로 파일의 실행 가능한 운영체제나 포맷, 유형에 따라 분류하고, 각각에 적절한 특징 추출 기법을 연구한다면 변형 악성코드에도 빠르게 대처할 수 있을 것이다.

본 연구는 한국인터넷진흥원(KISA)에서 운영하는 정보보호 R&D 데이터셋 [대용량 정상/악성파일 I, 대용량 정상/악성파일 II, 대용량 정상/악성파일 III]을 활용하여 작성되었음

참고문헌

[1] Saxe, Joshua, and Konstantin Berlin. "Deep neural network based malware detection using two dimensional binary program features." 2015 10th International Conference on Malicious and Unwanted Software (MALWARE). IEEE, 2015.

[2] Stolfo, Salvatore J., Ke Wang, and Wei-Jen Li. "Towards stealthy malware detection." Malware Detection. Springer, Boston, MA, 2007. 231-249.

[3] Raff, Edward, et al. "An investigation of byte n-gram features for malware classification." Journal of Computer Virology and Hacking Techniques 14.1 (2018): 1-20.

[4] Raff, Edward, Jared Sylvester, and Charles Nicholas. "Learning the pe header, malware detection with minimal domain knowledge." Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security. ACM, 2017.

[5] Islam, Rafiqul, et al. "Classification of malware based on string and function feature selection." 2010 Second Cybercrime and Trustworthy Computing Workshop. IEEE, 2010.

대규모 외생 변수와 Deep Neural Network를 사용한 금융 시장 예측의 성능 향상에 관한 연구

천성길*, 이주홍*, 최범기*, 송재원**

*인하대학교 전기컴퓨터공학과

** (주)밸류파인더스

chkrdp@gmail.com, juhong@inha.ac.kr, bgchoi666@gmail.com,

jwsong@valuefinders.co.kr

A Study on Improving the Performance of Financial Market Forecasting Using Large Exogenous Variables and Deep Neural Network

Sung-gil Cheon*, Ju-Hong Lee*, Bumghi Choi*, Jae-Won Song*

*Dept. of Computer Engineering, Inha University

**ValueFinders Co., Ltd

요 약

시장예측 문제를 해결하기 위하여 과거부터 꾸준한 연구가 진행되어왔다. 하지만 금융 시계열 데이터에는 분산이 일정하지 않으며 Non-stationarity 등 예측을 하는 것에 있어서 여러 가지 방해 요인이 존재한다. 또한 광범위한 데이터 변수는 기존에 사람이 직접 경험적으로 선택하는 것에 한계가 있기 때문에, 모델이 변수를 자동으로 추출할 수 있어야 한다. 본 논문에서는 여러 가지 금융 시계열 데이터의 문제를 고려하여 타임 스텝 정규화를 제안하며 자동 변수 추출을 위해 LSTM 형태의 오토인코더 모델을 학습하였으며 LSTM 네트워크를 이용하여 시장 예측하는 모델을 제안한다. 해당 시스템은 실제 주식 거래나 시장 거래를 위하여 온라인 학습이 가능하며 긴 기간을 테스트 구간으로 실험한 결과 미래의 수익률을 예측하는 것에 있어서 우수한 성능을 보였다.

1. 서론

최근 딥러닝의 발달로 머신러닝 분야는 크게 주목받고 있으며 각종 의료, 헬스, 금융, 인터넷 분야에서 좋은 성능을 보이며 많은 분야에서 딥러닝이 활용되고 있다[1].

금융 시장을 분석하기 위한 시도는 아주 오래전부터 진행되어왔다. 시장예측을 한다는 것은 단순히 예측된 값을 보고 거래를 목적으로 하는 것이 아닌 투자자에게 투자의 방향성을 제시할 수 있는 중요한 자료가 되기 때문이다. 과거 전통적인 방법으로 통계 기반의 시계열 분석 방법이 많이 사용되었으며 최근 딥러닝의 발달로 ANN, CNN, LSTM등 다양한 방법으로도 시도되고 있다. 또한 기술 지표를 사용하는 방법뿐만 아니라 뉴스 크롤링과 시장 감정분석 등 여러 가지 방법을 이용하여 복합적으로 시도되고 있다[2].

하지만 많은 시도에도 불구하고 시장예측은 사람이 만족할 만큼의 결과를 주지 못하였다. 금융과 관련된 변수는 매우 다양하기 때문에 사람이 직접 수

집하는 것조차 쉬운 일이 아니며 전문적인 지식을 바탕으로 분석하는 것도 한계가 있다. 또한 금융 시계열 데이터에는 몇 가지 특징이 존재하는데, 분산이 일정하지 않은 Volatility, 기대치가 특정한 방향으로 증가 또는 감소하는 형태이거나 패턴이 명확하지 않은 Non-stationarity, 혹은 시차 간 상관관계가 존재하지 않은 Non-linearity, 과거의 정보가 미래의 정보에 영향을 미치는 장기 의존성 등의 특징들은 우리가 데이터의 trend와 noise를 다루는 것을 어렵게 만들며, 시장예측의 큰 방해 요인이 된다.

본 논문에서는 이러한 방해 요인들을 해결하기 위한 전처리 시스템, 모델이 자동으로 변수를 추출하는 시스템, 예측 모델 및 학습 시스템을 제안한다. Volatility 및 Non-stationarity를 해결하기 위해 타임 스텝 별로 정규화하고 target을 미래의 수익률로 정의한다. 정규화된 데이터는 오토인코더 모델을 학습시켜 자동 변수 추출 시스템을 구성하며 미래의 수익률을 예측하는 LSTM기반의 모델을 학습하고, 이 과정을 online 학습할 수 있는 시스템으로 구축한다.

2. 관련 연구

ARIMA모델은 시장예측 모델로서 많은 연구의 대상이 되었다[3]. 이 모델은 실제 다양한 응용에 대한 효과를 보였지만 비선형 관계를 제대로 모델링할 수 없었으며 외생 변수를 입력으로 사용하기가 어려웠다. 이러한 문제점을 보완하기 위해 Nonlinear Autoregressive exogenous(NARX)와 관련된 모델들이 개발되었다[4]. 이 모델은 예측 시계열의 과거 데이터와 외생 변수 시계열 데이터를 사용하여 시계열을 예측할 수 있는 비선형 회귀 모델로 ARIMA모델의 단점을 어느 정도 보완을 해주었다. 하지만 장기 의존성 문제를 제대로 처리할 수 없었으며 외생 변수의 개수가 많아지게 되면 생기는 문제 또한 가지고 있었다.

한편 인공신경망을 사용하여 시장예측을 하는 연구로써, [5]는 MLP모델을 사용하여 도쿄 주식 시장의 지수를 예측하는 연구이고, [6]는 ANN과 SVM의 시장 예측 성능을 비교하여 ANN이 SVM보다 예측 능력이 더 뛰어난을 입증하였다. [7]는 DNN이 얇은 ANN보다 더 우수함을 보였다.

RNN과 LSTM은 과거의 특징을 추출하고 이를 기반으로 예측할 수 있는 모델이다. [8]은 LSTM을 사용하여 시장 수익률을 예측하였으며, [9]는 LSTM을 사용하여 시장 주식이 15분 뒤 상승할지 하락할지를 예측하여, LSTM이 MLP보다 성능이 더 좋음을 보였다.

3. LSTM 오토인코더 시장예측 시스템

3.1 전처리 시스템

예측 모델이나 분류 모델을 만들 때 학습의 효율을 높이기 위해 정규화된 데이터를 사용되며, z-변환이 자주 사용된다. z-변환은 다음 수식과 같다.

$$Z_t = \frac{X_t - \mu_X}{\sigma_X} \quad (1)$$

금융 시계열 데이터의 학습데이터와 테스트 데이터를 같이 정규화하면, 금융 데이터의 Non-stationarity 때문에 테스트 구간의 데이터 값이 제대로 정규화되어 있지 않은 문제가 발생한다. 즉 평균이 0이고 표준편차가 1이 되지 않으며 매우 큰 값이 존재하거나 매우 작은 값이 존재하므로, 테스트 데이터의 예측 실패율이 증가한다. 본 논문에서는 금융 시계열 데이터의 정규화 문제를 해결하고자 타임 스텝 정규화를 제안한다. 학습데이터 전체의 분포로 정규화를 하는 것이 아닌 LSTM 모델의

입력으로 들어가는 개별 과거 데이터의 분포로 해당 데이터를 정규화를 한다. 이렇게 하면, 모든 데이터에서 평균 0이고 표준편차가 1인 데이터가 생성된다.

3.2 오토인코더 차원축소 모델

본 논문에서는 가능한 많은 변수를 활용하여 차원 축소화 함께 피처를 잘 추출할 수 있는 오토인코더 모델을 제안한다. 이 오토인코더 모델은 many to many LSTM의 형태로 설계되었는데 이는 시장예측 모델이 LSTM기반이므로 입력 데이터의 형태를 고려하고 타임스텝간의 관계를 함께 모델링 할 수 있도록 하였다. 입력 데이터는 정규화된 과거 원가 데이터, 기술 지표, 경제 및 시장 등 다양한 변수를 갖는 데이터이며 일일 데이터를 사용한다. 이 시계열 데이터는 time×feature의 형태에서 batch×timestep×feature의 3D array로 변환한다. 여기서 timestep LSTM모델에 입력으로 들어갈 과거 history이다. 모델은 입력 데이터의 분포를 학습하여 생성하는 것이 목적으로 그 출력값 또한 입력 데이터가 되며 목적 함수는 MSE(Mean squared error)를 사용한다.

3.3 시장예측 모델

본 논문에서 사용한 LSTM기반의 예측 모델은 Many to many LSTM의 형태로 구성하였으며 학습한 오토인코더의 인코더 출력을 입력 데이터로 batch×timestep×feature의 형태인 데이터를 사용하는데 feature의 수는 차원 축소된 데이터의 차원 수와 같다. 모델의 출력은 각 time별로 q일 후의 수익률로 수익률 변환 방법은 trend ratio를 사용하였다.

$$trendratio = \frac{price_{t+q} - price_t}{price_t} \times 100 \quad (2)$$

4. 실험 및 결과

4.1 실험 데이터

FnGuide에서 제공하는 각종 기술 지표와 경제, 시장, 환율 등 2331개의 변수를 갖는 데이터를 사용하였으며 예측하고자 하는 시장에 따라 해당하는 변수를 추가로 사용한다. 기업의 경우 주가 및 재무와 관련된 1659개의 변수가 추가되며 지수의 경우 323개의 주식지수 변수가 추가된다. 예측 시장은 삼성전자, POSCO, S-Oil, 나스닥 종합, 대한민국 KOSPI로 실험하였으며 데이터의 기간은 1997년부터 2019년까지의 데이터를 사용하였다.

4.2 축소 변수 크기별 실험

본 논문에서 실험은 추출된 변수의 개수에 따른 영향과 전반적인 시장예측 성능을 평가하게 된다. 평가 지표로는 MSE(Mean squared error), RMSE(Root Mean Square Error), MAPE(Mean absolute percentage error), 주가의 방향성에 대한 Accuracy를 기준으로 한다. MAPE는 예측 수익률에서 변환된 가격으로, 나머지는 예측된 수익률 값으로 계산하며 y 는 실제 값(MAPE의 경우 실제 가격) \hat{y} 은 예측 값(MAPE의 경우 예측 값으로 변환된 가격)이 된다.

$$MAE = \frac{1}{n} \sum |y - \hat{y}| \quad (3)$$

$$RMSE = \sqrt{\frac{1}{n} \sum (y - \hat{y})^2} \quad (4)$$

$$MAPE = \frac{1}{n} \sum \left| \frac{y - \hat{y}}{y} \right| \times 100 \quad (5)$$

$$hit = \begin{cases} 1 & \text{if } y \cdot \hat{y} > 0 \\ 0 & \text{otherwise} \end{cases} \quad (6)$$

$$Accuracy = \frac{\sum hit}{n} \quad (7)$$

<표 1> 실험 파라미터.

파라미터	값
Lookback days	240
Time interval	2
Prediction day	60
Coding size	{128,256,512}

표<1>은 해당 실험에 필요한 파라미터이다. Lookback days는 t 시점으로부터 과거 t-240까지의 데이터를 사용하며 Time interval은 Lookback days의 시간 간격을 나타낸다. Prediction day는 t 시점으로부터 60일 뒤의 수익률 예측을 의미하고 Coding size는 비교실험을 위한 축소된 변수의 크기이다.

<표 2> 축소 변수 크기 별 실험 Accuracy.

	삼성전자	POSCO	S-Oil	나스닥 종합	대한민국 KOSPI	평균
128	0.779	0.743	0.81	0.835	0.724	0.7782
256	0.817	0.761	0.821	0.856	0.722	0.7954
512*	0.809	0.782	0.818	0.842	0.746	0.7994

평균	0.8016	0.762	0.8163	0.8443	0.7306	0.791
----	--------	-------	--------	--------	--------	-------

<표 3> 축소 변수 크기 별 실험 RMSE.

	삼성전자	POSCO	S-Oil	나스닥 종합	대한민국 KOSPI	평균
128	8.3956	8.7927	10.2672	5.1561	3.997	7.32172
256	7.6907	8.152	10.1084	4.9795	3.8547	6.95706
512*	7.6286	8.6154	10.1392	4.985	3.9067	7.05498
평균	7.904967	8.520033	10.1716	5.0402	3.919467	7.111253

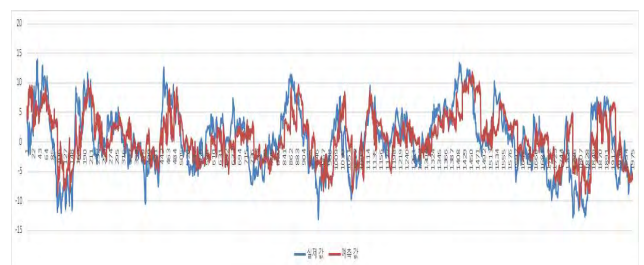
<표 4> 축소 변수 크기 별 실험 MAE.

	삼성전자	POSCO	S-Oil	나스닥 종합	대한민국 KOSPI	평균
128	6.5677	6.8005	7.7102	3.8607	3.1942	5.6266
256	6.0151	6.3724	7.4256	3.681	3.0861	5.3160
512*	5.9852	5.7976	7.3871	3.6407	3.0641	5.1749
평균	6.1893	6.3235	7.5076	3.7274	3.1148	5.3725

<표 5> 축소 변수 크기 별 실험 MAPE.

	삼성전자	POSCO	S-Oil	나스닥 종합	대한민국 KOSPI	평균
128	6.4208	6.8575	7.4835	3.7391	3.1699	5.5341
256	5.8455	6.4598	7.216	3.5808	3.0684	5.2341
512*	5.8149	5.8807	7.2436	3.5568	3.041	5.1074
평균	6.0270	6.3993	7.3143	3.6255	3.0931	5.2918

표(2)(3)(4)(5)에서 각 시장의 변수 크기별 결과가 조금씩 다르지만 대체로 512개의 변수로 줄였을 때가 가장 좋은 성능이 나왔다. 예측 테스트 기간 2012.01.02. ~ 2019.7.26에서의 Accuracy를 기준으로 평균 79%의 정확도를 보였다. 그림(1)(2)는 코스피의 예측 그래프를 보여준다. 파란 선은 실제 값을 나타내며 빨간 선은 예측 값을 나타낸다.



(그림 1) 코스피 예측 수익률 그래프.



(그림 2) 코스피 예측 가격 그래프.

5. 결론 및 향후 계획

타임 스텝 정규화를 하여 테스트 구간은 철저하게 가려진 채 모든 구간에서 정규화가 잘 이루어졌으며 또한 모델의 출력을 가격이 아닌 변환된 수익률로 함으로써 금융 시계열 데이터의 문제인 Non-stationarity를 전반적으로 잘 극복할 수 있었다.

본 논문에서는 금융과 관련된 많은 데이터를 수집하여 오토인코더 모델을 학습시켰고 이를 자동 변수 추출 모델로 데이터를 압축해서 표현하였다. LSTM 예측 모델은 긴 타임 스텝의 입력을 잘 처리하였으며, 장기 의존성 문제를 극복하고 추출된 변수의 패턴을 찾아 좋은 예측 결과를 보여주었다. 향후 자동 변수 추출 모델을 더욱더 고도화시키고 시장예측 모델에서 noise 학습을 통한 trend 예측 연구를 진행할 예정이다.

6. Acknowledgement

본 연구는 2019년도 중소벤처기업부의 기술개발사업 지원에 의한 연구임 [S2796242]

참고문헌

- [1] Yann LeCun, Yoshua Bengio, "Deep learning", Nature, 521, 436 - 444, 2015.
- [2] Kartik Goyal, "Stock Price Movement Prediction using Attention-Based Neural Network Framework", ISSN, 2319-7064, 2017.
- [3] Adebisi A. Ariyo, "Stock Price Prediction Using the ARIMA Model", 2014 UKSim-AMSS 16th International Conference on Computer Modelling and Simulation, Cambridge, UK, 2014.
- [4] S. Chen, "Narx-based nonlinear system identification using orthogonal least squares basis

hunting", IEEE Transactions on Control Systems Technology, 16, 1, 78 - 84, 2008.

- [5] T.Kimoto & K.Asakawa, "Stock Market Prediction System with Modular Neural Networks", 1990 IJCNN International Joint Conference on Neural Networks, San Diego, CA, USA, USA, 1990.

- [6] Yakup Kara, "Predicting direction of stock price index movement using artificial neural networks and support vector machines: The sample of the Istanbul Stock Exchange", Expert Systems with Applications, 38, 5, 5311-5319, 2011.
- [7] AH Moghaddam, "Stock market index prediction using artificial neural network". Journal of Economics, Finance and Administrative Science 21, 41, 89-93, 2016.
- [8] Kai Chen, "A LSTM-based method for stock returns prediction: A case study of China stock market", 2015 IEEE International Conference on Big Data (Big Data), Santa Clara, CA, USA, 2015.
- [9] David M. Q. Nelson, "Stock market's price movement prediction with LSTM neural networks", 2017 International Joint Conference on Neural Networks (IJCNN), Anchorage, AK, USA, 2017.

Actor-Critic 모델을 이용한 포트폴리오 자산 배분에 관한 연구

칼리나 바야르체체^{*1}, 이주홍^{*2}, 송재원^{**3}^{*}인하대학교 전기컴퓨터공학과^{**}(주)밸류파인더스¹kb0422.bk@gmail.com, ²juhong@inha.ac.kr, ³jwsong@valuefinders.co.kr

A Study on Portfolio Asset Allocation Using Actor-Critic Model

Bayartsetseg Kalina*, Ju-Hong Lee*, Jae-Won Song**

^{*}Dept. of Computer Engineering, Inha University^{**}ValueFinders Co., Ltd

요 약

기존의 균등배분, 마코위츠, Recurrent Reinforcement Learning 방법들은 수익률을 최대화하거나 위험을 최소화하고, Risk Budgeting 방법은 각 자산에 목표 리스크를 배분하여 최적의 포트폴리오를 찾는다. 그러나 이 방법들은 미래의 최적화된 포트폴리오를 잘 찾아주지 못하는 문제점들이 있다. 본 논문은 자산 배분을 위한 Deterministic Policy Gradient 기반의 Actor Critic 모델을 개발하였고, 기존의 방법들보다 성능이 우수함을 검증한다.

1. 서론

포트폴리오 자산 배분이란 개인의 목표를 달성하기 위한 위험과 수익률의 적절한 균형을 맞추어서 자산을 배분하는 투자전략을 말한다. 자산의 예로는 주식, 채권, 상품 및 현금 등이 있다. 포트폴리오 이론은 마코위츠(Markowitz)에 의해서 체계화되었다. 마코위츠 모델[3]은 공분산 행렬형태의 위험을 최소화하면서 포트폴리오의 기대 수익률을 최대화하는 평균-분산 최적화 방법이다. Risk budgeting[6]은 자본이 아닌 포트폴리오의 위험에 따라 자산을 할당하는 방법이다. 이 방법은 포트폴리오 매니저가 일련의 위험 예산(Risk Budget)을 정의한 다음 포트폴리오의 가중치를 계산한다. 균등배분(Equally weighted)은 포트폴리오 각 자산에 동일한 가중치를 부여하는 가중치 방법이다. 일반적으로 포트폴리오를 할당한다는 것은 투자 매니저의 의사결정 프로세스를 의미한다. 강화학습은 순차적인 의사결정 작업을 학습하는 일반적인 프레임워크다. Temporal difference 방법[8]으로 매개변수를 조정하여 시스템의 action에 따른 기대보상(expected reward)을 최대화한다. 자산 배분에서 포트폴리오 가중치는 강화학습으로 정의된다. RRL(Recurrent Reinforcement Learning) 알고리즘[4]은 샤프지수(Sharpe ratio)를

최소화하여 네트워크를 학습한다. RRL[4]이 포함된 자산 배분 시스템은 행동(action)의 value를 학습한 후, 측정된 행동들의 value를 기반으로 행동을 선택한다. 이러한 방법은 기대 수익률이나 샤프지수 같은 value 함수에 따라 달라진다. 이 문제점을 해결하기 위하여 DPG(Deterministic Policy Gradient)[7]를 사용하는 actor critic 모델을 제안한다.

2. 제안 방법

2.1 Problem Statement

먼저 포트폴리오 자산 배분을 위한 금융 시계열을 정의한다. 자산 가격 행렬은 m 개의 자산의 t 날 자산의 가격을 열 단위로 나타내었다.

$$P_{1:t} = [p^1 p^2 \dots p^m] = \begin{bmatrix} p_1^1 & p_1^2 & \dots & p_1^m \\ p_2^1 & p_2^2 & \dots & p_2^m \\ \dots & \dots & \dots & \dots \\ p_t^1 & p_t^2 & \dots & p_t^m \end{bmatrix} \quad (1)$$

다른 방법과 마찬가지로 강화학습 시스템의 상태(state) 입력으로 과거 d 일 동안의 자산 수익률 데이터를 사용한다.

$$s_t = \{z_{t-d:t}^1, \dots, z_{t-d:t}^m\} = Z_{t-d:t}$$

시간 t 에서 i 번째 자산의 수익률은 $z_t^i = \frac{p_t^i}{p_{t-1}^i} - 1$ 로 정의된다. 그래서 자산 수익률 행렬을 $Z_{2:t}$ 로 정의할 수 있다.

$$Z_{2:t} = [z_{2:t}^1 z_{2:t}^2 \dots z_{2:t}^m] = \begin{bmatrix} z_2^1 & z_2^2 & \dots & z_2^m \\ z_3^1 & z_3^2 & \dots & z_3^m \\ \dots & \dots & \dots & \dots \\ z_t^1 & z_t^2 & \dots & z_t^m \end{bmatrix} \quad (2)$$

강화학습 에이전트의 행동은 포트폴리오 가중치 $w \in \{w^1, w^2, \dots, w^m\}$ 에 의해 정의되고, trader는 매 수($w^i \geq 0$)만 사용한다. 본 논문에서는 샤프지수를 즉각적인 보상(immediate reward)으로 사용한다.

2.2 포트폴리오 자산 배분의 Actor Critic 모델

Actor 네트워크는 상태를 특정 행동에 결정적으로 대응하는 CNN[2]을 가진 LSTM[1]을 사용하고, 훈련 알고리즘은 DPG 방법을 사용한다.

$$\theta \leftarrow \theta + \alpha_\theta \frac{\partial u_\theta(s)}{\partial \theta} \frac{\partial Q_w(s, w)}{\partial w} \Big|_{w = u_\theta(s)} \quad (3)$$

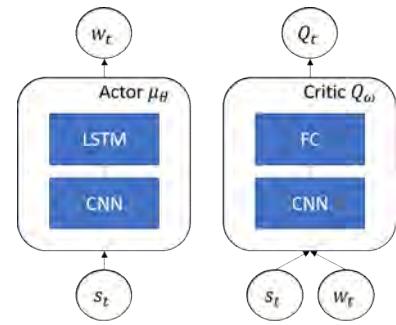
$Q_w(s, w)$ 는 critic 네트워크의 출력이고 α_θ 는 학습률이다. Actor 네트워크가 $\sum_{i=1}^m w^i = 1$ 과 $w^i \geq 0$ 조건을 만족하기 위해 softmax 함수 식(4)을 사용한다.

$$w^i = \exp(y^i) / \sum_{j=1}^m \exp(y^j) \quad (4)$$

$y \in \{y^1, \dots, y^m\}$ LSTM의 출력이고, CNN은 과거 수익률을 입력으로 사용하고, 중요한 특징(feature)을 찾아내서 출력한다. 출력값은 LSTM의 입력으로 사용된다. Q_w 를 타겟 critic 네트워크로 사용하고, 매개변수 w' 와 experience replay로 critic 네트워크를 학습한다. Critic 네트워크의 에이전트는 상태(s_t)와 행동(w_t)를 입력으로 사용하여, $\hat{q} = Q_w(s_t, w_t)$ 로 정의된 q-value를 추정한다. 타겟 q-value는 시간 t 에서 다음과 같이 정의된다.

$$q_t = r(s_t, w_t) + \gamma Q_{w'}(s_{t+1}, w_{t+1}) \quad (5)$$

여기서 $r(s_t, w_t)$ 는 즉각적인 보상(샤프지수), $Q_{w'}(s_{t+1}, w_{t+1})$ 는 타겟 critic 네트워크의 출력이다. 평균 제곱 오차(Mean Square Error)를 최소화하여 critic 네트워크를 학습한다.



<그림 1> Actor Critic 모델

$$L(w) = E_{s_t \sim p^u, w_t \sim u} [(q - Q_w(s_t, w_t))^2] \quad (6)$$

Gradient를 사용하여 critic 네트워크의 매개변수를 업데이트할 수 있다.

$$w \leftarrow w + \alpha_w \frac{\partial L(w)}{\partial \theta} \quad (7)$$

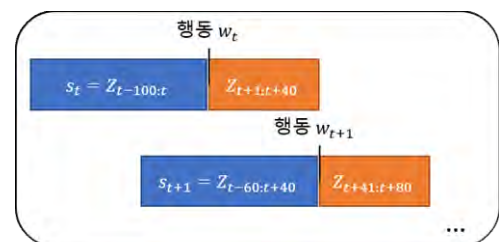
α_w 는 학습률이다. Q 네트워크의 구조는 FC(fully connected) layer와 CNN을 사용하였다. Actor Critic 모델의 일반적인 프레임워크는 그림1과 같다.

	포트폴리오 -A	포트폴리오 -B	포트폴리오 -C
Markowitz	0.0630	0.2448	0.8613
EquallyWeighted	-0.4643	-0.3111	0.4386
Risk Budgeting	0.2051	0.2084	1.0246
RRL	1.6197	1.4177	1.7444
Actor Critic	1.7803	1.4736	1.7925

<표 1> 실험결과 (샤프지수)

3. 실험

Actor Critic 포트폴리오 자산 배분 시스템은 일 단위 데이터로 학습하며, 제안된 모델의 특성을 평가하기 위해 3개의 포트폴리오(포트폴리오-A, 포트폴리오-B, 포트폴리오-C)를 사용한다. 각 포트폴리오는 총 10개의 자산으로 구성되어 있다. 2012년 1월부터 2019년 7월까지 총 8년의 일일 데이터(1970 trading days)를 사용한다. 2012년 1월부터 2019년 1월 사이의 데이터(1850 trading days)를 훈련 세트로 사용하고 다른 데이터(120 trading days)는 테스트 세트로 사용한다.



<그림 2> 자산배분 모델의 입력 및 포트폴리오 재조정

Benchmark 모델과 Actor Critic 모델의 상태 입력 값으로 과거 5개월(100 trading days) 동안의 자산 수익률 데이터를 사용한다.

$$s_t = \{z_{t-100:t}^1, \dots, z_{t-100:t}^{10}\}$$

두 달(40 trading days)에 한 번 모든 포트폴리오를 재조정한다. 그림2는 자산배분 모델들의 입력(과거 수익률 데이터)과 포트폴리오를 재조정한 기간을 보여준다. 본 논문에서는 모델의 학습을 위하여 0.001의 학습률을 가진 Adam Optimizer[5]을 사용한다. 포트폴리오-A는 니케이 225, 나스닥 종합, 코스피 200, 독일 DAX, S&P500 5개의 주가지수와 S-Oil, SK텔레콤, POSCO, 삼성전자, 한국전력 5개의 주식으로 구성된다. 포트폴리오-B는 니케이 225, 영국 FTSE 100, 코스피 200, 독일 DAX, S&P500 5개의 주가지수와 SK텔레콤, POSCO, 삼성전자, 한국전력, 현대차 5개의 주식으로 구성된다. 포트폴리오-C는 니케이 225, 나스닥 종합, 영국 FTSE 100, 독일 DAX, S&P500 5개의 주가지수와 SK텔레콤, POSCO, 삼성전자, S-Oil, 현대차 5개의 주식으로 구성되어 있다. 각 포트폴리오의 실험결과로 나온 샤프지수는 표1과 같다. 실험결과를 통해 Actor Critic 강화학습 모델이 가장 우수한 성능을 나타낼 수 있다.

4. 결론

자산 배분을 위한 Actor Critic 강화학습 모델을 제시하였다. 강화학습을 적용한 모델들의 결과가 기존 방법들에 비해 매우 우수한 성능을 보인 점을 통해 강화학습이 자산 배분 문제에 적합함을 알 수 있었다. 시계열 데이터의 temporal dependency를 반영하기 위해 강화학습 모델에 LSTM을 적용함으로써 모델의 성능을 개선할 수 있었다. 그러나 샤프지수를 최대화하는 RRL 모델은 샤프지수의 영향을 많이 받는다는 단점이 발생하였다. 이를 해결하기 위하여 q-value 함수를 근사화하는 Actor Critic 모델을 제안하였다. Actor Critic 모델은 타겟 네트워크와 experience replay를 통하여서 훈련 모델을 효과적으로 학습한다.

감사의 글

이 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 기초연구사업(과제번호: 2019R1F1A1062094)과 정보통신기획평가원의 지원(과제번호: 2019-0-01124)을 받아 수행된 연구임

참고문헌

- [1] Hochreiter, S. and Schmidhuber, J. Long short-term memory. *Neural Computation*, 9(8): 1735-1780, 1997.
- [2] Krizhevsky, A., Sutskever, I., and Hinton, G. E. Imagenet classification with deep convolutional neural networks. In *NIPS*, pp. 1106-1114, 2012.
- [3] Markowitz, H. Portfolio selection. *The Journal of Finance*, 7(1): 77-91, 1952.
- [4] Moody, J., Wu, L., Liao, Y., and Saffel, M. Performance functions and reinforcement learning for trading systems and portfolios. *Journal of Forecasting*, 17: 441-470, 1998.
- [5] P.Kingma, D. and Ba, J. Adam: A method for stochastic optimization, 2014.
- [6] Roncalli, T. Introduction to risk parity and budgeting, 2014.
- [7] Silver, D., Lever, G., Heess, N., Degris, T., Wierstra, D., and Riedmiller, M. Deterministic policy gradient algorithms. In *Proceedings of the 31st International Conference on Machine Learning (ICML 2014)*, pp. 387-395
- [8] Sutton, R. S. Learning to predict by the methods of temporal differences. *Machine Learning*, 3: 9-44, 1988.

인공지능을 활용한 스트리밍 서비스/SNS 내에서의 폭력 감지 시스템

김선민, 이석원, 임승수, 최상일
강릉원주대학교 컴퓨터공학과

ksmabcd135@gwnu.ac.kr actto1014@gwnu.ac.kr eungsu@gwnu.ac.kr schoi@gwnu.ac.kr

Violence Detection System in Streaming Service and SNS Using Artificial Intelligence Technologies

Seon-Min Kim, Seok-Won Lee, Seung-Su Lim, and Sangil Choi
Department of Computer Science & Engineering, Gangneung-Wonju National University

요 약

인터넷 및 IT 기술의 발전과 더불어 미디어산업에도 큰 변화가 일어나고 있다. TV 를 대신하여 스트리밍 서비스를 이용하는 사람들이 늘고 있으며 SNS 를 활용하여 서로의 경험을 간접적으로 공유하는 형태의 새로운 문화 콘텐츠가 자리잡아가고 있다. 하지만 이러한 콘텐츠를 소비하는 주요 계층 중에는 초중고 학생들도 포함되어 있다. 인터넷 혹은 SNS 에서 소비되는 콘텐츠들을 관리 감독하는 컨트롤 타워가 부족하거나 전무하기 때문에 폭력, 음주, 흡연 등 사회적으로 악영향을 줄 수 있는 영상 또는 사진이 무분별하게 생산되어 청소년들에 의해 소비되고 있으며 더 나아가 이것이 사회적 문제로까지 대두되고 있다. 이러한 문제를 해결하기 위해 인공지능 기술을 활용한 여러 다양한 감시 시스템 개발을 위한 연구가 한창이다. 본 연구에서는 SNS 및 스트리밍 서비스에서 제공되는 영상 및 사진을 Pose Estimation 및 표정 인식 기술을 활용하여 폭력을 자동적으로 감지할 수 있는 폭력 감지 시스템을 개발하는데 그 목적이 있다.

1. 서론

최근 인터넷의 발전과 4 차산업혁명의 도래로 미디어 시장 또한 큰 변화가 일어나고 있다. 대표적으로 스포츠, 음식 등 다양한 콘텐츠를 기반으로 실시간으로 소통하거나 영상을 편집하여 특정 플랫폼에 업로드 하는 1 인 미디어의 수요가 급증하고 있으며 자신 및 타인의 근황을 공유하는 SNS 서비스가 인기를 끌고 있다. 이와 같은 공유 콘텐츠가 확산되면서 검증되지 않거나 걸리지 않는 정보들이 무분별하게 소비되고 있는 것이 현실이다. 이러한 정보의 유통은 예기치 않은 문제들을 양산할 가능성이 매우 높다.



[그림 1] 방송 편성 과정¹

[그림 1]은 공영방송 편성 과정을 보여준다. 공영방송의 경우 한정된 콘텐츠를 방송심의위원회의 검증과

정을 거친 후 송출하기 때문에 사전에 위험 요소들을 차단할 수 있지만 스트리밍 서비스 및 SNS 의 경우 이러한 사전 작업없이 무분별하게 정보를 공유하는 경우가 대부분이기 때문에 인터넷 방송이나 SNS 에서 음주, 흡연, 폭력 등 자극적이며 사회적 문제를 발생시킬 수 있는 장면들이 아무 제재없이 송출되는 상황이 발생한다.

국내 스트리밍 서비스 시장에서 높은 점유율을 자랑하고 있는 아프리카 TV 의 경우 시스템 관리자가 직접 콘텐츠 내에서의 폭력성 여부를 판별하고 있다. 하루 동안 제작되는 대량의 콘텐츠를 관리자가 일일이 감시하여 폭력성 여부를 판단하는 것은 불가능에 가깝다.

[표 1] 플랫폼 별 분당 이용량²

	플랫폼		
	YouTube	Instagram	FaceBook
분당 이용량	277 만 영상 시청	8611 사진 업로드	300 시간 영상 업로드

전세계적으로 수 많은 사용자들이 이용하고 있는 SNS 및 영상 제공 플랫폼인 YouTube, Instagram, Face

¹ 방송편성의 이론과 실제, 한국방송통신대학교, 2015 년 발행

² IDC(International Data Corporation)분석 자료

Book 의 경우 부적절한 사진 및 영상을 부분적으로나마 인공지능 기술을 이용하여 판별하고 있으나 많은 사용자들이 그 정확성에 의문을 제기하고 있다. [표 1]에서와 같이 엄청난 양의 데이터가 매일 업로드 되고 있기 때문에 이러한 방대한 양의 콘텐츠를 관리자가 직접 관리하고 확인하는 것은 불가능에 가깝다.

본 연구는 이러한 문제점을 해결하기 위하여 사람의 골격 정보를 파악할 수 있는 Pose Estimation 기술과 얼굴의 특징을 읽어 감정을 예측하는 Emotion Detection 기술을 접목하여 폭력적인 장면을 검출하는 새로운 방향을 제시하고자 한다.

2. 관련 연구

국내에서 상용화를 위해 시험을 마친 폭력 감지 시스템의 경우 승강기의 내의 폭력 감지 시스템, 교내 폭력 상황 감지 및 알림 시스템이 있다. 더불어 폭력 감지에 대한 연구 또한 많이 이루어지고 있다. 그렇지만 ‘제한된 공간에서 객체가 적게 출현해야한다’와 같이 특정 조건을 만족 시켜야 정확성이 보장되는 문제를 안고 있다.

승강기 CCTV 에서의 폭력 감지 연구[1]에서는 폭력 행위가 발생할 시에는 객체의 형태가 심하게 변한다는 점을 이용하여 화면상의 객체의 크기 및 변화 횟수가 급격히 증가하면 이를 폭력행위로 간주한다. 객체의 움직임이 한정되고 밀폐된 공간이라는 조건을 충족시키는 승강기에선 신뢰성이 높은 결과를 얻을 수 있다. 하지만 객체의 움직임이 많은 개방되어 있는 공간에서는 정확도가 떨어질 가능성을 내포한다.

두 번째 연구는 드론을 활용하여 시위 중에 발생하는 폭력을 인식하는 시스템에 관한 것이다[2]. 이 연구에서는 드론으로 시위 영상을 촬영한 뒤 서버로 데이터를 전송하여 Yolo(You Only Look once)를 사용하여 위험한 객체(총, 파이프 등)를 검출하고 폭력과 관련된 움직임을 학습시켜 폭력적인 상황을 검출한다. 이 연구에서는 위험한 객체를 검출하는 것에는 높은 정확도를 얻었지만 폭력성을 내포하는 움직임을 검출하는 데는 정확도가 떨어졌다. 정확도가 떨어진 이유는 3.1 절의에서 자세히 설명한다.

관련 연구에서 보는 바와 같이 특정 조건을 만족해야만 정확도가 높아지거나 특정 위험 객체를 검출하는 것에만 높은 정확도를 나타내는 시스템은 이와 같은 특수 상황이나 조건을 만족시킬 수 없는 스트리밍 서비스 및 SNS 에서의 폭력 감지에는 적용하기 어렵다. 따라서 스트리밍 서비스 및 SNS 를 위한 새로운 폭력 감지 시스템이 요구된다.

3. Pose Estimation

3.1 Pose Estimation 의 사용 이유

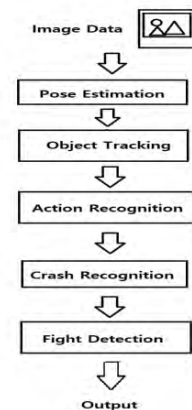
[그림 2]는 Object Detection 의 결과를 보여준다. 폭력 장면이 담긴 영상에서 물리적 충돌 상황을 폭력으로 정상적으로 인식하지만(왼쪽 사진) 동시에 악수와 같은 단순 신체 접촉(오른쪽 사진)도 폭력으로 잘못 탐지하는 경우가 발생하므로 객체의 관절 좌표를 이

용하는 Pose Estimation 기술을 활용하여 이 문제를 해결하였다.



[그림 2] Object Detection 기반 폭력 탐지 결과

3.2 폭력 탐지의 과정



[그림 3] 전체적인 Fight Detection 과정

[그림 3]은 이미지 데이터에서 폭력을 감지하기 위한 전체 과정을 나타낸다. 첫째, 이미지에 있는 사람의 관절 좌표를 구하기 위해 OpenPose 를 이용하여 Pose Estimation 을 실행한다. 둘째, 이미지에 있는 사람을 실시간으로 추적하기 위하여 SORT(Simple, Online, Realtime, Tracking Algorithm) 를 이용한 Object Tracking 을 실행한다. 셋째, 실시간으로 추적되고 있는 사람의 이미지가 어떤 행위를 하고 있는지 Action Recognition 을 실행하여 4 가지 동작(서있기, 걷기, 발차기, 주먹 지르기)으로 구분한다. 넷째, Crash Recognition 을 실행 하여 이전 단계인 Action Recognition 에서 발차기 또는 주먹 지르기가 감지 된다면 Object Tracking 을 이용하여 얻은 Object 간 접촉이 있었는지 감지한다. 마지막으로 Fight Detection 단계에서 객체(사람)가 발차기 또는 주먹을 지르면서 다른 객체와도 접촉해 있다면 폭력 상황으로 판단한다. Pose Estimation, Object Tracking, Crash Recognition 단계는 OpenPose 와 SORT 라이브러리를 사용하였다. 따라서 Fight Detection 을 위한 상세 과정에 대한 내용은 Action Recognition 만을 다룬다.

3.3 Action Recognition 을 위한 Dataset 수집

Action Recognition 을 위해 사람의 행동을 발차기, 주먹 지르기, 서있기, 걷기 총 4 가지로 구분했다. 주먹 지르기 데이터는 MHAD(Berkeley Multimodal Human Action Database) dataset 을 이용하였다. 이 비디오 데이

터는 4 개의 각도에서 촬영된 5 개의 반복에 대해 주먹 지르기 동작을 하는 12 명을 대상으로 구성된다. 나머지 3 개의 동작은 CMU Panoptic Dataset 을 이용했다. 이 비디오 데이터는 31 가지 각도에서 촬영된 3 가지 동작을 수행하는 13 명을 대상으로 구성된다.

3.4 관절 좌표를 이용한 학습 데이터 변환



[그림 4] OpenPose 를 이용한 관절 좌표 정보

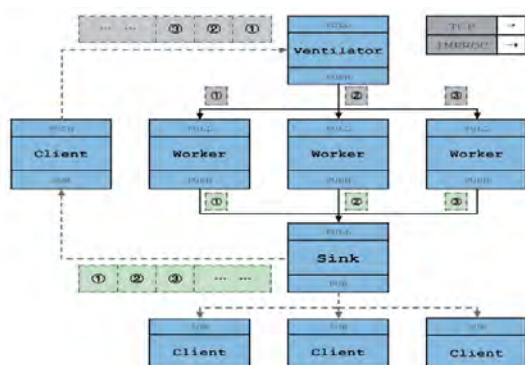
[표 2] 특징 벡터

Index	0	1	2	3	4	5	6	7
Angle	2-3	3-4	5-6	6-7	8-9	9-10	11-12	12-13
ΔAngle	2-3	3-4	5-6	6-7	8-9	9-10	11-12	12-13
ΔPoint	3	4	6	7	9	10	12	13

[그림 4]는 OpenPose 를 이용한 총 18 개의 관절 좌표를 나타낸다. 이 중에서 2~13 번의 관절 좌표만을 학습 데이터로 사용했다. [표 2]는 특징 벡터를 나타낸다. 각 관절 좌표를 이용하여 관절의 각도, 관절 좌표의 변화, 관절 각도의 크기 변화, 현재 프레임에서의 관절 각도 등 총 3 가지 특징을 벡터로 변환한다. 이전 프레임의 데이터와 비교하여 각 변화의 크기를 알 수 있다.

3.5 딥러닝 서버

실시간에 가까운 딥러닝 연산 처리를 수행하기 위해 GCP(Google Cloud Platform)의 GPU(Nvidia V100)를 대여하여 서버를 구축하였다. 서버와 클라이언트 간에는 ZMP 메시지 라이브러리를 사용하여 TCP 통신을 하도록 구현하였다(모든 메시지는 JSON 형식). 서버 내부에서는 GPU 자원을 최대한 활용하기 위해 [그림 5]와 같은 병렬 파이프 라인 구조를 적용하였다. 각 프로세스 간 통신 또한 ZMQ 메시지 라이브러리를 사용하여 구현하였으며 각 프로세스별 세부적인 기능은 [표 3]과 같다.



[그림 5] 이미지 처리 서버 구조

[표 3] 이미지 서버 구조

Client	처리할 이미지를 Server 측 Ventilator 에게 전송
Ventilator	Client 가 전송한 이미지를 수신하여 Worker 에게 순차적으로 분배
Worker	Ventilator 로부터 수신한 이미지 처리 작업을 수행 후 Sink 에게 전달 ※Object Detection 기반 폭력 탐지 : YOLO 모델의 CNN 연산을 수행 ※Pose Estimation 기반 폭력 탐지 : OpenPose 모델의 CNN 연산을 수행
Sink	Worker 로부터 수신한 이미지 처리 작업 결과에 추가 처리 작업을 수행하고 순차적으로 Client 에게 전달 ※Object Detection 기반 폭력 탐지 : YOLO 탐지 결과를 바탕으로 이미지에 Bounding Box 를 그림 ※Pose Estimation 기반 폭력 탐지 : OpenPose 탐지 결과를 바탕으로 SORT Object, Tracking, RNN Action Recognition, 충돌 탐지 작업을 수행 ※CNN 연산은 Darknet, RNN 연산은 Tensorflow 를 사용

4. Emotion Detection

4.1 표정 인식 방법

표정을 분석한 후 사람의 감정을 인식하여 분류하는 방법은 크게 Convolutional Neural Networks (CNN)을 이용한 방법과 얼굴의 특징점을 이용하는 방법이다. 본 논문에서는 위의 두가지 방법을 모두 사용하여 결과를 도출하였다.

4.2 CNN 을 이용한 감정 분류



[그림 6] CNN 을 이용한 표정 분류 결과

[그림 6]은 CNN 을 이용한 감정 분류[3] 결과를 보여준다. 감정 분류의 과정은 다음과 같다. 첫째, Haar Cascade 를 이용하여 이미지에서 얼굴의 위치를 찾는다. 둘째, 확인된 얼굴을 48×48 사이즈로 변환하여 CNN 에 입력한다. 셋째, CNN 실행 결과를 7 가지 감정(Angry, Disgusted, Happy, Neutral, sad, surprised, fearful)에 대한 Softmax 점수를 출력한다. 마지막으로 가장 높은 점수를 받은 감정을 화면으로 출력한다. 그러나 CNN 을 이용한 감정 분류는 첫번째와 세번째 단계에서 제한적인 학습 데이터로 인해 카메라를 정면으로 보고 찍은 사진만 분류가 된다는 한계가 있다. 포착된 얼굴이 조금이라도 틀어진 모습이 있으면 이미지 상에서 얼굴을 찾지 못하고 결과적으로 표정을 감정별로 분류할 수 없다.

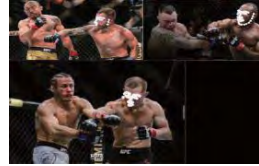
4.3 얼굴의 특징점을 이용한 감정 인식

OpenPose 의 Face Tracking 은 얼굴의 특징점을 찾는

프로그램이다. [그림 7]은 Face Tracking의 예시이며 정면의 얼굴뿐만 아니라 카메라를 기준으로 각도가 틀어져 있는 얼굴에 대해서도 얼굴의 특징을 포착하는 것을 볼 수 있다. 또한 얼굴의 특징점 좌표와 KNN(K-Nearest Neighbors Algorithm)을 이용하여 사용자 감정 인식을 성공적으로 수행한 사례도 있다[4].



[그림 7] OpenPose의 Face Tracking 예시



[그림 8] 싸움 이미지 판독 결과

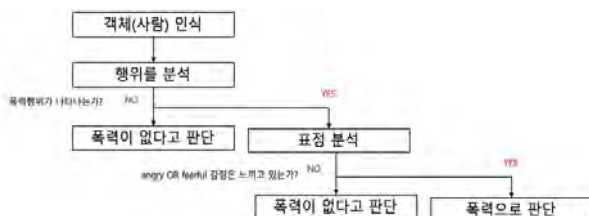


[그림 10] 감정과 행위 감지를 함께 실행한 예시

특징점이란 얼굴의 윤곽, 눈, 눈썹, 코, 입을 인식하여 점으로 나타낸 것을 말하며 이 특징점들이 모두 연결되어 [그림 7]과 같이 윤곽선이 잡힐 경우 얼굴이 정확하게 인식되었다고 한다. [그림 7]과 [그림 8]은 영상을 OpenPose의 Face Tracking을 이용하여 실행한 결과이다. [그림 7]의 경우 감정 인식을 위해 사용되는 특징점들이 정확하게 인식된 반면, [그림 8]의 경우 폭력을 행하는 사람은 얼굴 윤곽선, 코, 입, 눈에 대한 특징점 중 윤곽선 및 눈썹에 대한 특징점이 누락되었고 폭력을 당하는 사람의 특징점은 하나도 검출되지 못하였는데 이것은 [그림 8]의 영상이 [그림 7]의 영상에 비해 상대적으로 빠른 움직임과 데이터 학습 부족으로 인해 특징점을 검출하지 못하여 생긴 현상이며 이러한 특징점 누락으로 인해 감정 인식에 실패하여 결과적으로 폭력 상황을 검출하지 못했다. 스트리밍 서비스 특성상 [그림 8]과 같이 움직임이 많은 상황이 대부분이기 때문에 Face Tracking만을 이용하여 폭력성을 인지하는 것은 불가능하다고 판단된다.

5. 해결방안

[그림 9]는 해결방안으로 제시한 폭력을 검출하는 알고리즘을 나타낸 것이다. 먼저 행위를 분석하여 폭력적인 모습이 나타나는지를 확인한 후 폭력적인 장면이 인식되면 그 다음 단계에서 표정을 인식하여 사람의 감정을 판독한다. 판독 결과에서 Fearful 또는 Angry라는 감정을 인식하면 결론적으로 폭력적인 상황이 발생했다고 결론을 내린다.



[그림 9] 폭력을 검출하는 알고리즘

[그림 10]은 [그림 9]에 나타나있는 감정과 행위를 동시에 감지하는 알고리즘을 통해 감지해낸 결과이다. 행위 분석 또는 표정을 통한 감정 분석 중 한 가지의

기술을 이용하여 폭력을 검출했을 경우 단순한 접촉을 폭력으로 판단하거나 얼굴의 각도가 빠르게 변화하여 감정 검출에 실패하여 폭력을 검출하지 못했던 영상, 사진에 대하여 Fearful, Surprise Fearful이란 감정을 추출함으로써 폭력적인 상황이 발생하고 있다고 판단한 모습을 보여준다.

6. 결론

폭력적인 상황의 특성상 폭력을 행하고 있는 사람과 폭력을 당하고 있는 사람 모두 화면에 얼굴을 정면으로 향하게 하는 것은 쉽지 않다. 발차기와 주먹치르기 행위를 감지하는 동시에 사람의 감정을 감지하여 폭력을 판단하려면 사람의 정면 얼굴은 물론이고 부분 얼굴 표정을 통한 감정을 파악하는 과정이 필수적이다. 이를 위해 지금까지 2 가지 방법을 사용했다. 그러나 학습데이터의 한계, 불안정한 얼굴 특징점 파악이라는 두가지 문제가 있다. CNN을 활용하여 개선하는 방법으로 정면 얼굴의 감정 인식은 기존 시스템을 이용하되 부분 얼굴(profile face)은 LBP Cascade Classifier를 이용하여 이미지에서 부분얼굴인식을 거친 후 감정 분류를 진행할 수 있다. 그러나 감정 분류를 위해 CNN을 학습시키려면 각 감정에 대한 부분 얼굴 DataSet을 충분히 확보해야한다. 하지만 이러한 문제점이 있음에도 불구하고 하나의 기술만을 사용하였을 경우에는 실제로 폭력적인 상황이 발생했지만 폭력이라고 인식하지 못했던 문제점이 2 가지 이상의 기술을 접목한 후 정상적으로 폭력으로 인식하는 것을 확인 할 수 있었다. 이러한 기술을 SNS 및 스트리밍 서비스와 접목시킨다면 폭력적인 장면이 송출되거나 사진이 업로드 되는 상황을 빠르게 막을 수 있을 뿐만 아니라 거대한 용량의 데이터를 인간이 처리하는 것보다 빠르고 정확하게 처리할 수 있을 것으로 예상된다.

참고문헌

- [1] 심영빈, 박화진, "CCTV에서 폭력 행위 감지 시스템 연구", 디지털 콘텐츠 학회, 제 16 권, 제 1 호, pp 26-30, 2015.
- [2] Yeon-Su Lee, Hyun-Chul Kim, "Deep Learning-based Violent Protest Detection System", 한국컴퓨터 정보학회 논문지, 제 2 권, 제 3 호, pp 87-93, 2019.
- [3] Enrique Correa, Arnoud Jonker, Michael Ozo, Rob Stolk, "Emotion Recognition using Deep Convolutional Neural Networks", Tech Report IN4015, TU Delft, 2016.
- [4] 이용환, 김홍준, "얼굴 특징점 추적을 통한 사용자 감정 인식", 반도체디스플레이기술학회지 제 18 권, 제 1 호, pp 98-100, 2019.

단일 단계 검출 방법을 위한 이미지 합성기반 학습 데이터 증강에 관한 연구

이선경^{*,**}, 정치윤^{*}, 문경덕^{*}, 김채규^{**}

^{*}한국전자통신연구원 인공지능연구소 휴먼증강연구실

^{**}부경대학교 IT융합응용공학부

ssunkyung00@gmail.com, iamready@etri.re.kr, kdmooon@etri.re.kr, kyu0707@pknu.ac.kr

A Study on Synthesizing Training Data for One-stage Object Detector

Seon-Gyeong Lee^{*,**}, Chi Yoon Jeong^{*}, KyeongDeok Moon^{*}, Chae-Kyu Kim^{**}

^{*}Human Enhancement & Assistive Technology Research Section,
Artificial Intelligence Research Lab, ETRI

^{**}Dept. of IT Convergence & Application Engineering, Bukyoung University

요 약

딥러닝 기반의 영상 분석 방법들은 많은 양의 학습 데이터가 필요하며, 학습 데이터 구축에는 많은 시간과 노력이 소요된다. 특히 객체 검출 분야의 경우 영상 내 객체의 위치, 크기, 범주 등의 정보가 모두 필요하여 학습 데이터 구축에 더 많은 어려움이 있으며, 이를 해결하기 위해 최근 이미지 합성기반 데이터 증강에 관한 연구가 활발히 진행되고 있다. 이미지 합성기반 데이터 증강 방법은 배경 영상에 객체를 합성할 때 객체와 배경 영상이 접한 영역에서 아티팩트(Artifact)가 발생하며, 이는 객체 검출 모델이 아티팩트를 객체의 특징으로 모델링하여 검출 성능이 저하되는 원인이 된다. 이러한 문제를 해결하기 위하여 본 논문에서는 양방향 필터 기반의 이미지 합성 방법을 제안하고, 단일 단계 검출의 대표적인 방법인 RetinaNet을 이용하여 이미지 합성기반 데이터 증강 방법의 성능을 분석하였다. 공개 데이터셋에 대한 실험 결과 본 논문에서 사용한 단일 검출 방법 및 데이터 증강 기법을 사용하면 더 적은 양의 증강 데이터로 기존 방법과 동일한 성능을 보여주는 것을 확인하였다.

1. 서론¹⁾

디지털 기기들의 발전으로 각양각색의 개인 데이터들이 대량으로 증가하고 있으며, 이를 분석하기 위하여 딥러닝 기반 영상 분석에 관한 연구가 활발히 진행되고 있다. 딥러닝 기반의 영상 분석 방법들은 많은 양의 학습 데이터가 필요하며, 학습 데이터 구축에는 많은 시간과 노력이 소요된다. 특히 영상에 존재하는 객체를 검출하는 객체 검출 분야의 경우 영상 내 객체의 위치, 크기, 범주 등의 정보가 모두 필요하여 학습 데이터 구축에 더 많은 시간과 노력이 필요하다.

이러한 어려움을 해결하기 위해 객체 검출 분야에서 이미지 합성기반의 데이터 증강에 관한 연구가 진행되고 있다[1-3]. 이미지 합성기반의 데이터 증강 기법은 배경 영상에 원하는 객체를 특정한 위치에 배치하고 합성하여 학습 데이터를 증강시켜 객체 검출 방법의 성능을 향상시키는 기법이다. 기존 연구

에서는 배경 영상의 레이아웃을 분석하여 실제와 유사한 영상이 생성되도록 객체를 배치하는 방법이 제안되었다[2]. 이렇게 생성된 합성 영상을 학습데이터로 활용하면 SSD(Single shot multibox detector)와 Faster R-CNN 등의 객체 검출 방법의 성능이 향상된다는 것을 보여주었다. 그러나 배경 영상의 레이아웃을 분석하는 방법은 새로운 형태의 배경 영상에 적용하기 어렵고, 배경 영상에 객체를 합성할 때 객체와 배경 영상이 접한 영역에서 아티팩트(Artifact)가 발생하는 문제가 있다. 또한, 객체 검출 알고리즘이 아티팩트를 객체의 특징으로 모델링할 수 있기 때문에 객체 검출 성능이 저하될 수 있다. 이러한 문제를 개선하려는 노력으로, 동일한 객체를 배경 영상의 같은 위치에 가우시안 필터(Gaussian filter), 포아송 블렌딩(Poisson blending) 등의 다양한 블렌딩 방법을 적용하여 합성하고 이렇게 생성된 다양한 영상을 학습 데이터로 활용하는 방법이 제안되었다[3]. 이러한 방법은 배경과 객체가 합성된 영역에 다양한 블렌딩 방법이 적용된 학습 데이터를 사용함으로써 아티팩트 효과를 줄이고 객체 검출 방법의 성

* 본 연구는 한국전자통신연구원(ETRI) 연구운영비지원 사업의 일환으로 수행되었음[20ZS1200, 인간의 감각·지각 능력을 증강하는 다중 감각 융합 기술 개발 사업]

능 향상시킬 수 있다. 하지만, 이 방법의 경우 블렌딩 방법마다 학습 데이터가 생성되므로 전체 학습 데이터의 양이 증가하여 객체 검출 모델의 학습에 많은 시간이 소요되는 문제점이 있다.

본 논문에서는 아티팩트 효과를 줄이면서도 학습에 필요한 데이터의 양을 줄일 수 있는 이미지 합성기반 데이터 증강 방법을 제안하였다. 먼저, 본 논문에서는 배경 영상에 객체 영상을 합성할 때 발생하는 아티팩트 효과를 줄이기 위하여 양방향 필터(Bilateral filter) 기반의 이미지 합성 데이터 생성 방법을 제안하였다. 또한, 단일 단계 검출의 대표적 방법인 RetinaNet[4]을 사용하여 이미지 합성기반 데이터 증강 방법의 성능을 분석하였다. 본 논문에서 제안한 방법을 공개 데이터셋을 사용하여 실험한 결과 기존 방법보다 더 적은 양의 증강 데이터를 사용하여 기존 방법과 동일한 성능을 가지는 것을 확인하였다.

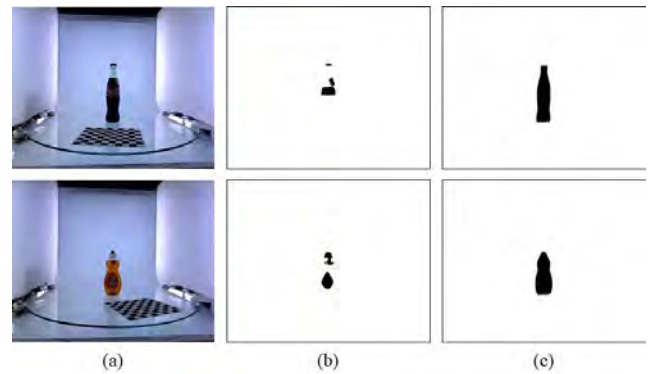
본 논문은 2장에서 이미지 합성기반 객체 검출 성능 향상 방법을 제안하여 검증하고 3장에서는 실험 결과를 종합하였으며 4장에서 결론을 서술하였다.

2. 이미지 합성기반 객체 검출 성능 향상 방법

본 논문에서 제안하는 이미지 합성기반 객체 검출 성능 향상 방법은 그림 1과 같이 3단계로 구성된다. 첫 번째 단계에서는 배경 영상에 합성할 객체 영상을 생성하는 단계로써, 객체가 포함된 영상에서 해당 객체의 영역으로만 구성된 마스크 영상을 생성한다. 두 번째 단계에서는 배경 영상에 랜덤하게 객체의 위치를 설정한 후 해당 위치에 객체 영상을 합성함으로써 객체의 범주 및 위치에 대한 학습용 데이터

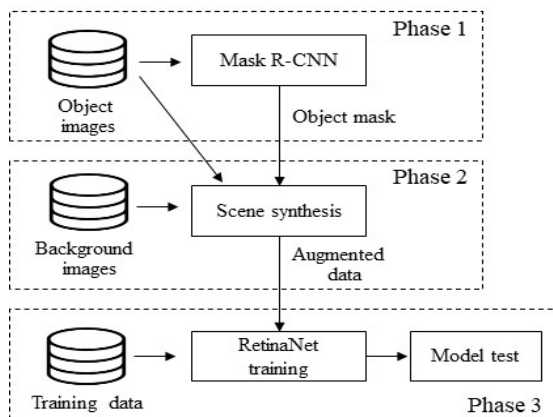
를 생성한다. 마지막 단계에서는 실제 데이터 및 합성 데이터를 사용하여 객체 검출 방법 및 이미지 합성 방법의 성능을 분석한다.

첫 번째 단계인 객체 영역 추출 단계에서는 Big Berkeley Instance Recognition Dataset (BigBIRD) 데이터셋을 사용하였다. BigBIRD 데이터셋은 125개의 객체를 카메라의 각도 및 위치를 달리하여 촬영한 영상으로 구성되어 있으며, 본 논문에서는 GMU-Kitchen 데이터셋[6]에 존재하는 11개의 객체 데이터를 사용하였다. BigBIRD 데이터셋은 객체 영상마다 객체 마스크 영상이 존재하지만, 투명한 재질로 이뤄진 객체의 경우 마스크 영상이 부정확하게 검출되는 문제점이 존재한다. 따라서 객체 마스크를 정확하게 추출하기 위하여 Mask R-CNN[7] 알고리즘을 사용하였다. Mask R-CNN은 Faster R-CNN이 검출한 객체 영역에서 각 픽셀이 객체에 해당되는지를 판단하는 Fully Convolutional Network을 결합한 알고리즘이다. 그림 2는 Mask R-CNN을 사용하여 객체 영역을 검출한 결과를 나타낸다. 유리병과 같이 투명한 재질의 물체는 그림 2의 (b)와 같이 원본 마스크 영상이 부정확하게 나타나지만, Mask R-CNN을 활용하면 그림 2의 (c)와 같이 객체 영역을 정확하게 검출함을 확인할 수 있다.



(그림 2) 객체 영역 추출 결과 (a) 입력 영상 (b) 원본 마스크 영상 (c) Mask R-CNN 결과 영상

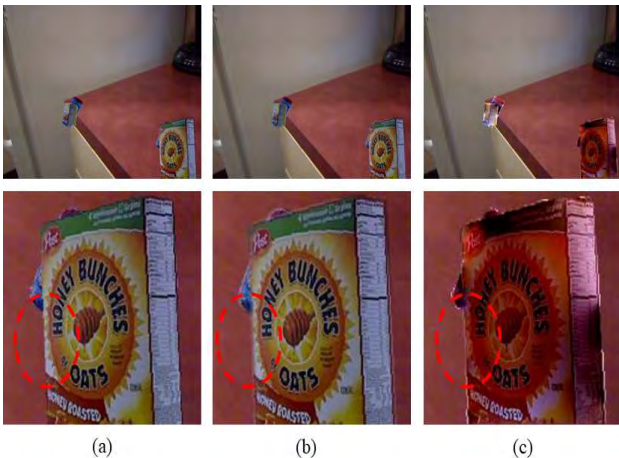
영상 합성 단계에서는 배경 영상과 객체 영상을 합성하여 객체 검출 모델의 학습 데이터를 생성한다. 영상 합성을 위한 배경 영상은 UW Scenes 데이터셋[8]을 사용하였다. 배경 영상에 객체 영상을 합성하게 되면 객체 영상의 경계에 아티팩트가 생성되며, 이는 객체 검출 방법의 성능을 저하하는 원인이 된다. 따라서 기존 연구[3]에서는 아티팩트로 인한 성능저하를 해결하기 위하여 배경 영상의 같은 위치에 동일 객체를 배치하고 다양한 블렌딩 방법을 적용한 다수의 영상을 생성하여 객체 검출 알고리즘



(그림 1) 이미지 합성기반 객체 검출 성능 향상 방법 흐름도

을 학습시키는 방법을 사용하였다. 다양한 블렌딩 방법을 적용하면 배경 영상과 객체 영역이 만나는 영역의 정보가 비일관성을 갖게 되어 객체 검출 알고리즘 학습 과정에서 아티팩트로 인한 성능저하를 해결할 수 있지만, 학습 데이터의 양이 증가하게 되어 네트워크 모델 학습에 많은 시간이 소요되는 단점이 있다.

본 논문에서는 다양한 블렌딩 방법을 적용하지 않고 양방향 필터 기반의 영상 합성 방법을 제안한다. 기존 연구에서 사용한 가우시안 필터의 경우 경계의 모든 영역을 평활화(Smoothing)하여 객체의 윤곽선도 평활화되는 문제점이 존재하였다. 객체 검출 알고리즘에서 윤곽선 정보는 중요한 특징 중 하나이므로 윤곽선이 평활화되는 경우 객체 검출 알고리즘의 성능이 저하될 수 있다. 양방향 필터[9]는 에지 성분을 보존하면서 다른 영역을 평활화 할 수 있기 때문에 객체 검출 알고리즘의 성능을 향상시킬 수 있을 것으로 기대된다.



(그림 3) 객체와 배경 영상 합성 결과 (a) 양방향 필터 (b) 가우시안 필터 (c) 포아송 블렌딩

그림 3은 다양한 필터를 사용하여 객체를 배경 영상에 합성한 결과를 나타내며, 상단은 합성한 영상의 전체 영역을 나타내고 하단은 객체와 배경의 경계 영역을 나타낸다. 그림 3 하단의 객체 영역을 확대한 영상에서 알 수 있듯이 가우시안 필터를 사용하면 객체의 경계선 영역이 평활화되는 반면, 양방향 필터의 경우 경계선을 유지함을 확인할 수 있다. 그림 3의 (c)는 포아송 블렌딩을 사용한 경우를 나타내며, 경계와 주변 영역이 부드럽게 연결되지 않고 색상의 변화가 발생하는 단점이 있다. 기존 연구[3]에서도 포아송 블렌딩을 사용하는 경우 색상 변화가 발생하는 단점이 있다고 지적하였다.

객체 검출 단계에서 기존 연구들은 Faster R-CNN 과 같은 두 단계 검출 방법을 주로 사용하였다. 두 단계로 수행되는 검출 방법의 경우, 높은 정확도를 가지지만 검출 속도가 느리기 때문에 실제 활용에는 어려움이 있다. SSD로 대표되는 단일 단계 검출 방법은 두 단계 검출 방법과 비교하면 정확도가 낮지만 검출 속도가 빠른 장점이 있다. 단일 단계 검출 방법의 낮은 검출 정확도는 학습 과정에서 클래스 간 불균형으로 인하여 발생하며, 최근 클래스의 불균형 문제를 해결하면서 단일 검출 방법의 성능을 향상시킨 RetinaNet이 발표되었다. RetinaNet은 Focal loss를 사용하여 학습 과정에서 분류하기 쉬운 예제들의 학습 기여도를 낮춤으로써 클래스의 불균형 문제를 해결하였으며, 두 단계 검출 방법보다 높은 검출 성능과 처리 속도를 보여주었다[4]. 따라서, 본 논문에서는 RetinaNet을 사용하여 이미지 합성기반 데이터 증강 방법의 성능을 분석하였다.

3. 실험 결과

이미지 합성기반 데이터 증강 방법의 성능 분석에는 GMU-Kitchen 데이터셋을 사용하였다. GMU-Kitchen 데이터셋은 9개의 영상으로 구성되어 있으며, 각 영상은 11개의 객체 정보를 포함한다. GMU-Kitchen 데이터셋은 3-겹 교차 검증으로 구분되어 있으며, 본 실험에서도 데이터셋에서 정의한 3-겹 교차 검증을 수행하여 성능을 측정하였다.

데이터 증강을 위한 객체 데이터는 BigBIRD 데이터셋 중 GMU-Kitchen 데이터와 중복되는 11개 객체 데이터를 사용하였다. BigBIRD 데이터셋에서 한 객체는 5개의 카메라 위치와 120 개의 다른 각도 촬영된 총 600장의 영상으로 구성되어 있으며, 본 논문에서는 객체별로 2개의 카메라 위치에서 촬영된 240장 영상을 랜덤하게 선택하여 합성에 사용하였다.

영상 합성 단계에서는 1.358장의 배경 영상이 사용되었으며, 성능 비교를 위한 영상 합성 방법은 기존 연구[3]에서 사용한 가우시안 필터, 포아송 블렌딩, 박스 필터와 본 논문에서 제안한 양방향 필터를 사용하였다. 영상 합성을 위해 사용된 방법의 파라미터는 기존 연구에서 사용한 값을 사용하였으며, 본 논문에서 제안한 양방향 필터의 경우 거리는 5, 색상과 공간에 대한 표준편차 값은 25를 사용하였다. 배경 영상에 최소 1개에서 최대 4개의 객체가 랜덤하게 선택되어 배치되며, 동일 영상에 대해서 각기 다른 필터를 적용한 합성 영상이 생성된다.

<표 1> 이미지 합성기반 객체 검출 성능 평가 결과

	coca cola	coffee mate	honey bunches	hunt's sauce	mahatma rice	nature v1	nature v2	palmolive orange	pop secret	pringles bbq	red bull	mAP
No augmentation	82.9	93.7	90.5	85.8	90.5	97.2	86.5	88.9	89.7	89.4	71.6	87.9
No blending	84.7	94.3	91.7	87.5	88.9	96.7	86.6	88.1	90.8	90.1	61.2	88.1
Box blurring	84.5	95.5	92.1	87.5	89.1	96.8	87.3	87.5	88.3	90.6	69.3	88.0
Gaussian blurring	83.9	93.8	82.2	88.0	91.0	96.8	87.7	88.8	90.3	89.9	69.7	88.5
Poisson	84.1	95.0	91.2	87.6	86.5	97.1	87.1	88.5	91.3	89.7	71.0	88.1
Ours	83.9	95.1	91.6	88.7	88.6	97.3	88.6	88.7	91.8	91.2	70.8	88.7
Georgios's [2]	82.6	92.9	91.4	85.5	81.9	95.5	88.6	78.5	93.6	90.2	54.1	85.0
Dwibedi's [3]	88.5	95.5	94.1	88.1	90.3	97.2	91.8	80.1	94.0	92.2	65.4	88.8

객체 검출을 위한 RetinaNet 모델은 백본 네트워크로 ResNet-50을 사용하였으며, 에포크(epochs)는 30으로 설정하고, 반복(iteration) 횟수는 객체 데이터의 수로 설정하였다. 학습 비율은 0.00001을 설정하였으며 네트워크 모델은 Keras 라이브러리를 사용하여 구현하였다. 객체 검출 방법의 성능 측정은 IoU (Intersection over Union) 가 0.5일 때의 mAP (mean Average Precision)을 사용하였다.

표 1은 이미지 합성기반 객체 검출 성능평가 결과를 나타낸다. 실험 결과를 살펴보면 이미지 합성기반 증강 데이터를 사용하여 RetinaNet을 학습하면 증강 데이터를 사용하지 않은 경우에 비하여 성능이 증가하게 되며, 이미지 합성 방법 중 본 논문에서 제안한 양방향 필터를 사용한 합성 방법의 성능 향상이 가장 크게 나타났다. 제안 방법은 배경 영상의 레이어아웃을 분석하여 데이터를 증강하는 기존 방법 [2]보다 높은 성능을 나타내며, 다양한 블렌딩 방법을 적용한 기존 연구[3]와 동일한 성능을 보여주었다. 기존 연구[3]는 블렌딩을 사용하지 않은 합성 영상과 가우시안 필터 및 포아송 블렌딩을 적용한 합성 영상을 모두 학습 데이터로 사용하므로 본 논문에서 제안된 방법보다 3배나 많은 증강 데이터를 사용하게 된다. 따라서 본 논문에서 제안한 방법은 기존 방법보다 더 적은 양의 증강 데이터로 동일하거나 더 높은 성능을 보여주는 것을 표1의 결과에서 확인할 수 있다.

4. 결론

본 논문에서는 양방향 필터 기반의 이미지 합성 데이터 생성 방법을 제안하고, 단일 단계 검출의 대표적인 방법인 RetinaNet에서의 이미지 합성기반 데이터 증강 방법의 성능을 분석하였다. 제안 방법에서는 Mask R-CNN을 사용하여 객체 영역의 마스크

를 추출한 후, 객체와 배경 영상을 합성하는 과정에서 객체의 경계선을 보존하면서도 주변 영역을 평활화하여 영상 합성의 품질을 높일 수 있는 양방향 필터를 적용하였다. 실제 데이터 및 합성 데이터를 사용하여 RetinaNet의 객체 검출 성능을 분석하였다. 공개 데이터셋을 사용한 실험 결과를 통해 본 논문에서 제안한 양방향 필터 기반의 합성 방법이 다른 블렌딩 방법보다 객체 검출 방법의 성능을 더 향상시키는 것을 확인하였다. 또한, 본 논문에서 사용한 단일 검출 방법 및 이미지 데이터 증강 기법을 사용하면 기존 방법보다 더 적은 양의 증강 데이터로 동일한 성능을 보여주는 것을 실험 결과로 확인하였다.

참고문헌

- [1] A. Gupta, A. Vedaldi, and A. Zisserman, "Synthetic data for text localisation in natural images," *Proc. CVPR*, 2016.
- [2] G. Georgakis, A. Mousavian, A. C. Berg, and J. Kosecka, "Synthesizing training data for object detection in indoor scenes," *arXiv preprint arXiv:1702.07836*, 2017.
- [3] D. Dwibedi, I. Misra, and M. Hebert, "Cut, paste and learn: Surprisingly easy synthesis for instance detection," *Proc. ICCV*, 2017.
- [4] T.-Y. Lin, P. Goyal, R. Girshick, K. He, and P. Dollar, "Focal loss for dense object detection," *Proc. ICCV*, 2017.
- [5] A. Singh, J. Sha, K. Narayan, T. Achim, and P. Abbeel, "BigBIRD: A large-scale 3D database of object instances," *Proc. ICRA*, 2014.
- [6] G. Georgakis, Md. Reza, A. Mousavian, P. Le, and J. Kosecka, "Multiview. RGB-D Dataset for Object Instance Detection," *arXiv preprint arXiv*

:1609.07826, 2016.

[7] K. He, G. Gkioxari, P. Dollar, and R. Girshick, “Mask R-CNN,” *Proc. ICCV*, 2018.

[8] K. Lai, L. Bo, X. Ren, and D. Fox, “A large-scale hierarchical multi-view rgb-d object dataset,” *Proc. ICRA*, 2011.

[9] C. Tomasi and R. Maduchi, “Bilateral filtering for gray and color images,” *Proc. ICCV*, 1998.

형태소 임베딩과 SVM을 이용한 뉴스 기사 정치적 편향성의 자동 분류

조단비*, 이현영*, 박지훈**, 강승식*

*국민대학교 컴퓨터공학과

**다ahami 커뮤니케이션즈

daanv319@kookmin.ac.kr, hyunyoung2@kookmin.ac.kr,

hoonzinope@dahami.com, sskang@kookmin.ac.kr

Automatic Bias Classification of Political News Articles by using Morpheme Embedding and SVM

Dan-Bi Cho*, Hyun-Young Lee*, Ji-Hoon Park**, Seung-Shik Kang*

*Dept. of Computer Science, Kookmin University

**Dahami Communications Co.

요 약

딥러닝 기술을 이용한 정치적 성향의 편향성 분류를 위하여 신문 뉴스 기사를 수집하고, 머신러닝을 위한 학습 데이터를 구축하였다. 학습 데이터의 구축은 보수 성향과 진보 성향을 대표하는 6개 언론사의 뉴스에서 정치적 성향을 이진 분류 데이터로 구축하였다. 뉴스 기사의 수집 방법으로 최근 이슈들 중에서 정치적 성향과 밀접하게 관련이 있는 키워드 15개를 선정하고 이에 관한 뉴스 기사들을 수집하였다. 그 결과로 11,584개의 학습 및 실험용 데이터를 구축하였으며, 정치적 편향성 분류를 위한 머신러닝 모델을 설계하였다. 머신러닝 기법으로 학습 및 실험을 위해 형태소 단위의 임베딩을 이용하여 문장 및 문서 임베딩으로 확장하였으며, SVM(Support Vector Machine)을 이용하여 정치적 편향성 분류 실험을 수행한 결과로 75%의 정확도를 달성하였다.

1. 서론

입력 문장을 분석 또는 생성하기 위해 문장들을 토큰 단위로 표현하여 벡터로 구성하는 기법을 사용한다. 영어에서는 문장의 의미를 표현하는 최소 단위로 단어를 하나의 토큰으로 임베딩한다.[1,2] 특히, 머신러닝 모델에서는 토큰을 연속적인 벡터 공간에 표현함으로써 모델의 입력값으로 사용한다.[3,4]

단어 임베딩 방법은 TF-IDF와 같이 단어 쌍이 함께 출현하는 빈도수를 기반으로 임베딩하는 방법과 주변 단어들로부터 단어를 예측하여 벡터를 구성하도록 하는 예측 기반의 임베딩 방법으로 나누어진다.[6] 예측 기반의 임베딩 기법으로는 Mikolov(2013)가 제안한 CBOW(Continuous Bag Of Words)와 skip-gram의 word2vec과 GloVe, FastText 등이 있다.[3,4,7] 대부분의 연구에서 이와 같은 예측 기반 임베딩이 보다 높은 성능을 나타낸 것으로 알려져 있으며[8], Kim(2014)과 Santos(2014)는 어절 단위 토큰의 단어 임베딩으로 skip-gram을 사용하여 실험을 진행하였다.[1,2]

굴절어인 영어와 달리, 교착어인 한국어의 어절은 형태소들의 조합으로 이루어진다. 이러한 점에서

한국어는 어절보다 형태소 단위 토큰이 다양한 언어적 의미를 표현할 수 있다.[5] 본 논문에서는 정치적 성향의 편향성을 분류 실험에서 형태소 단위 토큰화를 이용한 한국어 임베딩 방법론을 제안한다.

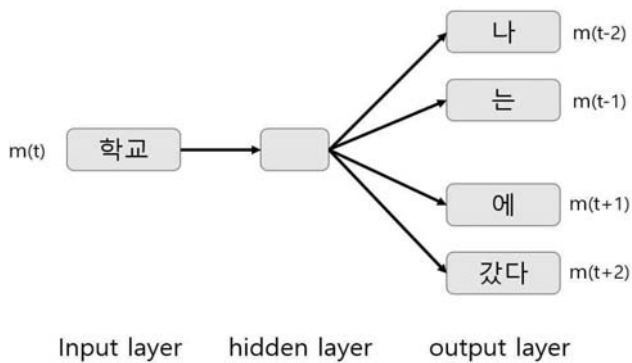
2. 정치적 편향성의 분류 모델

skip-gram¹⁾은 어절 단위 토큰을 사용하여 중심 단어 벡터로부터 주변 단어를 예측하는 방식으로, 연속적인 벡터 공간에 각각의 독립적인 단어들을 벡터로 표현한다.[3] 이처럼 단어들마다 독립적인 벡터를 할당하기 때문에 어절 내부의 형태학적 정보를 포함하지 못하므로 어절을 구성하는 형태소 단위 토큰을 입력 벡터로 구성하는 형태소 임베딩을 제안한다.

형태소 임베딩은 skip-gram을 확장한 모델로 각각의 단어가 어절이 아닌 형태소 단위의 토큰으로 입력된다. “나는 학교에 갔다”를 형태소 분석기²⁾

1) gensim을 이용하여 window size 5, min-count 1, negative sampling 5, ns_exponent 0.75의 skip-gram으로 파라미터를 조정하여 벡터를 구성하였다.
(<https://radimrehurek.com/gensim/>)

Okt로 분석하면 ['나', '는', '학교', '에', '갔다']의 형태소 토큰이 생성되며, 이러한 형태소 임베딩의 예시는 그림 1과 같다.



(그림 1) skip-gram을 이용한 형태소 임베딩

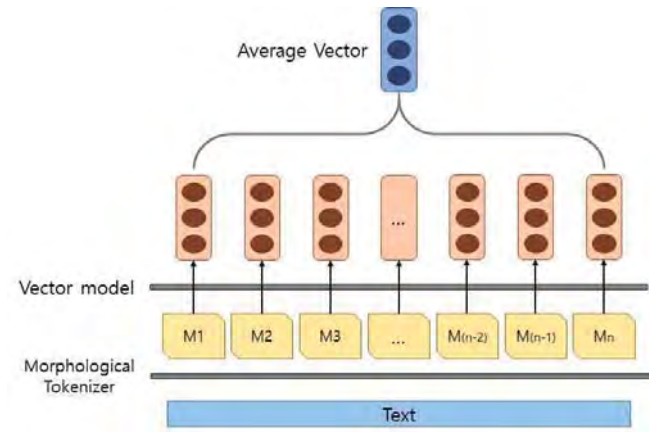
학습 데이터 M 를 구성하는 토큰 $\{m_1, m_2, m_3, \dots, m_T\}$ 에 대하여 중심 단어 c 의 벡터를 V_c , 윈도우 크기에 속하는 주변 단어 s 의 벡터를 V_s 라고 할 때, 중심 단어 토큰 m_c 와 주변 단어 토큰 m_s 의 등장 확률 값은 softmax 함수로 계산되며 (1)과 같이 정의된다. 이는 목적 함수 (2)를 계산할 때 학습 데이터의 크기만큼 연산 비용이 소요된다는 단점이 존재하며, 효율적인 연산을 위해 확률을 근사적으로 계산하는 negative sampling 기법의 목적함수를 사용하였다.[9]

$$P(m_s|m_c) = \frac{\exp(v_s^T v_c)}{\sum_{m=1}^M \exp(v_m^T v_c)} \quad (1)$$

$$\mathcal{J}(\theta) = \frac{1}{T} \sum_{t=1-s \leq j \leq s, j \neq 0}^T \log P(m_{t+j}|m_t) \quad (2)$$

정치적 편향성을 분류하기 위해서는 문서 벡터를 구성하여야 한다. 형태소 임베딩을 통해 생성된 문서 내 형태소 토큰들의 벡터를 (v_1, v_2, \dots, v_n)라고 할 때, 문서 벡터 V 는 $\text{average}(v_1, v_2, \dots, v_n)$ 와 같이 토큰 벡터들의 평균으로 표현된다. 이처럼 형태소 임베딩을 통해 문서 벡터를 구성하는 모델은 그림 2와 같이 설계하였다.

SVM³⁾은 대표적인 분류 모델이다. 이는 분류 모델의 입력 데이터를 기저 벡터라고 할 때, 각 정치적 성향의 기저 벡터들과 분류 경계면 간의 거리,



(그림 2) 정치적 성향의 편향성을 위한 분류 모델

즉 마진을 최대화하고자 한다.[10] 분류 경계면의 직선 판별함수는 $f(x) = w^T x - w_0$ 과 같다. 이 판별함수를 통해 계산되는 값을 score라고 할 때, 보수 성향에 속하는 기저 벡터의 score는 0보다 큰 값이고, 진보 성향에 속하는 기저 벡터의 score는 0보다 작은 값이 된다. SVM의 분류 모델을 최적화하기 위한 손실함수는 hinge loss를 사용하였으며, (3)과 같이 계산된다. SVM은 이러한 손실 값을 최소화하도록 모델을 학습한다.

$$L_i = \sum_{j \neq y_i} \begin{cases} 0 & \text{if } s_{y_i} \geq s_j + 1 \\ s_j - s_{y_i} + 1 & \text{otherwise} \end{cases} \quad (3)$$

$$= \sum_{j \neq y_i} \max(0, s_j - s_{y_i} + 1)$$

3. 실험 및 평가

3.1 데이터 구축

정치적 성향의 편향성을 분류하기 위해 정치적 성향을 나타내는 키워드를 기반으로 뉴스 기사를 크롤링하여 데이터를 수집하였다. 보수 성향과 진보 성향을 대표하는 6개 언론사의 뉴스에서 정치적 성향과 밀접한 관련이 있는 키워드를 선정하고, 각 키워드를 통해 검색되는 기사를 추출하여 구축하였다. 키워드는 인물, 사건, 주요 단어를 기준으로 추출하였으며, 총 15개의 키워드를 기준으로 하여 11,584개의 기사를 수집하였다. 정치적 편향성 관련된 키워드는 나무 위키⁴⁾에서 선정하였으며, 선정한 키워드 15개는 다음과 같다.

2) <https://konlpy-ko.readthedocs.io/ko/v0.4.3/>

3) SVM은 Cornell 대학에서 구현한 SVM-Light 모델을 사용하였다. (<http://svmlight.joachims.org/>)

4) <https://namu.wiki/w/분류:2019년%20사건>

<표 1> 정치적 편향성 기사의 문장과 어절 수

	보수	진보
기사 수	5,792	5,792
문장 수	122,544	163,264
어절 수	2,082,330	2,748,160

<표 2> 토큰나이저 별 중복 제거한 토큰 수

	Train(9,267)	Test(2,317)
Hannanum	201,139	79,450
Komoran	62,181	35,325
Okt	114,594	57,998

<표 3> SVM을 이용한 정치적 편향성 분류 정확도(%)

	Hannanum			Komoran			Okt		
	100	200	300	100	200	300	100	200	300
100	69.23	69.57	71.21	72.59	72.42	72.64	71.69	72.42	72.81
200	70.18	69.36	69.83	73.93	74.28	74.71	73.72	72.77	73.41
300	65.69	71.86	68.80	73.24	74.06	74.75	74.54	75.27	74.58
400	70.69	71.56	67.33	75.18	75.31	75.44	73.50	75.70	72.90
500	73.72	66.98	74.02	75.49	75.49	74.41	74.94	75.57	75.31

- 인물: 홍익표, 이명박, 손혜원, 트럼프, 조국
- 사건: 지소미아, 패스트트랙, 파업, 하명수사, 검찰 개혁
- 주요어: 교과서, 판문점, 탈북인, 여경, 부동산

수집한 데이터에서 특수 기호, 기자 이름, 날짜 등의 텍스트를 제거하고 구두점으로 끝나는 문장들 로만 뉴스 기사의 본문을 구성하도록 정제하여 데이터를 구축하였다. 구축한 데이터의 보수 및 진보 성향 기사의 문장 수와 어절 수는 표 1과 같다. 보수 성향과 진보 성향의 데이터 크기는 이진 분류를 위해 동일한 크기로 사용하여 데이터의 균형을 맞추었다. 형태소 분석기를 이용한 토큰나이저 별 중복을 제거한 토큰의 수는 표 2와 같으며, 학습 데이터와 훈련 데이터는 8:2의 비율로 분할하여 모델을 학습하고 자동 분류 정확도를 평가하였다.

3.2 평가 및 결과

뉴스 기사의 본문 내용을 형태소 분석기를 통해 형태소 단위로 토큰화하고, 벡터 크기를 각각 100, 200, 300, 400, 500으로 생성한 후에 100, 200, 300의 반복 횟수로 학습하여 토큰 벡터를 구성하였다. 문서를 구성하고 있는 토큰들의 벡터를 평균값으로 문서 벡터를 구성하고 이를 SVM 분류 모델을 통해 실험하였으며 정확도는 표 3과 같다.

SVM을 사용한 자동 분류 결과, 표 4와 같이 벡터 크기 400, 반복 횟수 200으로 Okt 형태소 분석기를 사용하였을 때 정확도 75.7%로 가장 높은 성능을 보였다. 또한, 정치적 편향성의 자동 분류 실험 결과로 전반적으로 Okt와 Komoran은 비슷한 성능

을 보였으며, Hannanum의 성능이 가장 낮게 나타났다.

4. 결론

한국어의 교착어 특성을 고려하여 어절을 형태소 단위의 토큰열로 분할하여 각 형태소 분석기 별 성능 비교 실험을 진행하였다. 정치적 성향의 편향성을 분류하기 위해 정치 키워드를 기반으로 검색된 뉴스 기사를 수집하여 데이터를 구축하였으며, 구축한 데이터를 활용하여 형태소 단위 토큰화를 진행하였다. 형태소 토큰을 사용한 머신러닝 기법으로 SVM 모델을 사용하였으며, 형태소 분석기 별 정확도에 따른 성능을 비교하였다. SVM 모델을 사용한 정치적 편향성의 자동 분류 실험에서 Okt의 형태소 분석기를 사용했을 때 가장 높은 성능을 나타냈다.

Acknowledgements

이 논문은 2019년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임(NRF-2019S1A5A2A03046571).

참고문헌

- [1] Santos. C. D. & Gatti. M. "Deep convolutional neural networks for sentiment analysis of short texts," Proceedings of COLING 2014, the 25th International Conference on Computational Linguistics: Technical Papers, pp.69-78, 2014.
- [2] Kim. Y. "Convolutional neural networks for sentence classification." Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing(EMNLP), pp.1746-1751,

- 2014.
- [3] Mikolov. T., Chen. K., Corrado. G., & Dean. J. "Efficient estimation of word representations in vector space." arXiv preprint arXiv:1301.3781, 2013.
 - [4] Mikolov. T., Sutskever. I., Chen. K., Corrado. G. S., & Dean. J. "Distributed representations of words and phrases and their compositionality." Advances in Neural Information Processing Systems, pp.3111-3119, 2013.
 - [5] 이홍식, "형태소와 문법 기술," 어문학 109호, pp.1-35, 2010.
 - [6] 이동준, 임유빈, 권태경, "형태소 기반 효율적인 한국어 단어 임베딩," 정보과학회논문지, 45권 5호, pp.444-450, 2018.
 - [7] Pennington. J., Socher. R., & Manning. C. D, "Glove: Global vectors for word representation," Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing(EMNLP), pp.1532-1543, 2014.
 - [8] Baroni. M., Dinu. G. & Kruszewski. G., "Don't count, predict! a systematic comparison of context-counting vs. context-predicting semantic vectors," Proceedings of the 52nd Annual Meeting of the Association for Computational Linguistics, Vol.1: Long Papers, pp.238-247, 2014.
 - [9] Y. Goldberg and O. Levy, "word2vec Explained: deriving Mikolov et al.'s negative-sampling word-embedding method," arXiv preprint arXiv:1402.3722, 2014.
 - [10] Joachims. T. *Learning to classify text using support vector machines*, Springer Science & Business Media, 2002.

신경망 모델의 편향성을 줄이기 위한 데이터 증강 연구

손재범

한양대학교 컴퓨터공학과

e-mail : netoou@hanyang.ac.kr

A Study of Mixed Augmentation for Reducing Model Bias

Jaebeom Son

Dept. of Computer Engineering, Hanyang University

Abstract

Recent studies demonstrate that deep learning model is easily biased by trained with unbalanced datasets. For example, the deep network can be trained to make a prediction by background feature instead the real target's feature. For those problem, a measurement called leakage was introduced to digitize this tendency. In this paper, we propose augmentation strategy which are used generally in computer vision problem to remedy this bias problem and we showed a simple augmentation methods have a effect to this task with experiments.

1. Introduction

Upon development of peripheral environment of computational learning such as accumulation of big data and the advanced technology of parallel computing, deep neural networks have renown for its learning capability and ability to solve various range of tasks (e.g. image recognition [2], machine translation [3], generative model [4]). At this moment of artificial intelligence being integrated to real world services, non-technical issues (e.g. ethical, social) are emerged. For instance, the existence of accuracy disparities in neural network model which trained to solve face recognition task was reported on Buolamwini et. al. to warn for commercial gender classification applications and the authors demanded urgent attention to this problem (gender shades MIT media-lab). To outline this, the model made worst accuracy score when they predict darker-skinned female. On the other hand, lighter-skin male showed the best error rate. This was supposed to occur with respect to class biased training dataset. The other problem also reported that trained deep network doesn't use the main feature of target class to decide its prediction, instead it looks other background information [10]. For example, to predict woman the model use features like 'long hair' or 'white dress' rather than utilize the physical characteristics of female. Other method [6] proposed the measurement of gender bias of image feature space using reverse engineering strategy and proposed adversarial approach this gender bias problem on MS-COCO dataset [1].

In this paper, we propose simple and applicable data augmentation strategy to many neural network pipeline especially image recognition task. Named *mixup* [7] and *cutmix* [8], these methods are mixing two or more data onto one which has containing many soften features and relaxed class label information. We was able to show that the gender bias problem was mitigated by augmentation approach on subset of MS-COCO dataset which male is major class whereas female is minor. We will introduce about the two augmentation method and

leakage measurement to measure gender bias. Then, we will show the specific experiment method and results at following sections.

2. Leakage measurement

In image recognition problem, such relationships between classes can occur class correlation on dataset. For instance, class 'long hair', 'lipstick' are more likely to be appeared with 'woman' class. Models trained with this type of datasets are prone to predict images which has 'long hair' or 'lipstick' as 'woman' class. Numerically express how trained model likely to be affected by internal classes relation of dataset, we use *leakage* [6]. *Leakage* is measured by train and evaluate base model called *attacker* [6] with internal class label and its original label. *Attacker* is expected to behave as reverse engineering about internal classes in the input images original label. we simply point out formal definition of *leakage* and other notations. Suppose an annotated dataset D is given which contain three attributes (x, y, c) that mean image, class label, internal class label each. And we refer attacker as f . The *dataset leakage* ℓ_D is:

$$\ell_D = \frac{1}{|D|} \sum_{(y_i, c_i) \in D} 1\{f(y_i) == c_i\}$$

Where $1\{\cdot\}$ is the indicator function and (y_i, c_i) is data sampled from dataset D . The $|D|$ indicates the number of sampled in dataset D . The term *dataset leakage* ℓ_D is identical to performance of attacker f w.r.t training dataset, in other words, 'accuracy'. For measure the degree of model bias we introduce similar measurement to *dataset leakage* which named *model leakage* ℓ_H :

$$\ell_H = \frac{1}{|D|} \sum_{(y_i, c_i) \in D} 1\{f(y_i) == c_i\}$$

Where $\hat{y}_i = H(x_i)$, prediction of model H about input data x_i . H is pretrained with data x and its original targets y . The magnitude of model bias defined to distance of two leakage scores called *bias amplification*, $\Delta = \ell_H - \ell_D$. Our goal is to curtail Δ to introduce simple approach.

3. Data augmentation

‘Mixing’ strategies are able to show effect to mitigate the proposed problems by internal class bias [5, 6]. The following two methods are simple and easy to apply to current training pipeline.

3.1 Mixup

One of our augmentation strategy to relax biased training with internal class representation is *mixup* [7]. *Mixup* linearly mixes two different data sampled from same dataset with mixing proportion parameter λ . The proportion of two different data λ is determined at random and drawn from the beta distribution $\lambda \sim \text{Beta}(\alpha, \alpha)$, $\alpha \in (0, \infty)$. Then, we can define mixed data $(x_{\text{mixed}}, y_{\text{mixed}})$ which is sampled from the following vicinal distribution [9] called *mixup*:

$$\mu(x_{\text{mixup}}, y_{\text{mixup}} | x_i, y_i) = \frac{1}{n} \sum_j E_\lambda \left[\delta \left(x_{\text{mixup}} = \lambda \cdot x_i + (1-\lambda) \cdot x_j, y_{\text{mixup}} = \lambda \cdot y_i + (1-\lambda) \cdot y_j \right) \right]$$

Also we can write sampled data from this distribution as:

$$\begin{aligned} x_{\text{mixup}} &= \lambda \cdot x_i + (1-\lambda) \cdot x_j \\ y_{\text{mixup}} &= \lambda \cdot y_i + (1-\lambda) \cdot y_j \end{aligned}$$

Where the (x_i, y_i) and (x_j, y_j) are two data sampled at random from dataset.

In this paper, the key property of *mixup* that blends two data while they keep their characteristics after mixed will help to achieve our goal ‘reduce internal bias’. Features of each data are weakened by multiplied with λ or $1-\lambda$ but the mixed data x_{mixed} contains broader range of features. The target y_{mixed} has two different softened labels with regarding to data x_{mixed} . In learning procedure, this mixed information which contain two different internal classes feature will guide model to learn less biased representation.

3.2 Cutmix

Possessing the key property of *mixup*, blending information of two data, *cutmix* [8] showed effect on relaxing biased learning. However, in detail of mixing algorithm *mixup* and *cutmix* are distinct. Suppose we manage image datasets. To generate mixed sample $(x_{\text{cutmix}}, y_{\text{cutmix}})$ from (x_i, y_i) and (x_j, y_j) , proportion of two different data λ drawn from uniform distribution which is a special case of beta distribution $\text{Beta}(1,1)$. The masking area M is generated from λ . Then the mask region of sample image x_i will be replaced to cropped patch of x_j by the mask M . Following show this

$$\begin{aligned} x_{\text{cutmix}} &= M \odot x_j + (1 - M) \odot x_i \\ y_{\text{cutmix}} &= \lambda \cdot y_j + (1 - \lambda) \cdot y_i \end{aligned}$$

Gender balance	Split	Man #	Woman #
False	no balance	16,225	6,601
	$\gamma = 1$	3,078	3,078
	$\gamma = 2$	8,885	6,588
	$\gamma = 3$	10,876	6,598
	Val	3,813	1,554
	Test	3,894	1,579
True	Train	3,000	3,000
	Val	1,500	1,500
	Test	1,500	1,500

Table 1. Dataset with several split conditions, used to train, validation, test Resnet model and measure *leakage*. Gender balance and γ is hyperparameter which influence to gender quantity of data.

Learning rate	Model mAP		
	mixup	cutmix	normal
1e-5	42.593	39.555	45.765
1e-4	51.274	50.062	52.858
1e-3	52.882	49.595	52.901

Table 2. This table shows the resnet model suffered underfitting problem. Instead to extend training epoch we increase learning rate to observe convergence. Lr with 1e-3 shows best mAP scores.

Where \odot is element-wise multiplication. W, H are width and height of image. Mask region $M \in \{\text{binary}\}^{W \times H}$ is initialized to zero first then filled with 1 accordingly box coordinates (r_x, r_y, r_w, r_h) . r_x and r_y are the center coordinates of masking region which are drawn from uniform distribution $r_w \sim U(0, W), r_h \sim U(0, H)$. r_w and r_h are determined by λ , $r_w = W\sqrt{1-\lambda}, r_h = H\sqrt{1-\lambda}$.

Similar to *mixup*, x_{cutmix} and y_{cutmix} also has two different softened features and labels. However, ‘erase out and fill with another one’ strategy is able to lead a risk to lost some information of original in image space. But this strategy can assist to relax down the internal class bias problem by cutting off correlation between features and internal classes.

4. Experiments

In this paper, we show the effect of two mixing augmentation methods on the relaxing internal class bias problem. Experiment setting and training method are introduced at section 4.1 and the results are shown at table 2 of section 4.2.

4.1 Experiment Environment

We have taken experiments based on the similar setting of Wang et. al. which discussed about gender bias problem. Gender dataset of extracted subset of MS-COCO was used with several setting in regard of gender class balance. This gender class balance was determined by hyper-parameter γ . Transfer learning is effective strategy to handle classification task. We used ResNet-50 [11] pretrained on Imagenet as base model to train and evaluate internal gender bias. We set training epoch to 50 for fine-tuning pretrained Resnet model. We followed the same architecture of *attacker* to measure *leakage* and bias. We did not use F1 score measurement to derive bias amplification.

Attacker gender balance	Augment gender balance	Splits	Dataset leakage	Model leakage			Minimum bias amplification
				mixup	cutmix	normal	
False	False	no balance	73.85 \pm 0.19	77.38 \pm 0.39	77.61 \pm 0.17	78.49 \pm 0.29	3.98
		$\gamma = 3$	73.28 \pm 0.37	74.82 \pm 0.36	74.84 \pm 0.62	75.97 \pm 0.14	1.54
		$\gamma = 2$	68.42 \pm 2.19	74.26 \pm 0.36	73.04 \pm 0.43	76.21 \pm 0.42	4.62
		$\gamma = 1$	52.34 \pm 1.14	64.78 \pm 1.60	64.66 \pm 1.71	67.79 \pm 1.55	12.32
	True	$\gamma = 3$	73.28 \pm 0.37	75.07 \pm 0.56	76.63 \pm 0.50	75.97 \pm 0.14	1.79
		$\gamma = 2$	68.42 \pm 2.19	73.85 \pm 0.54	73.09 \pm 0.57	76.21 \pm 0.42	4.67
		$\gamma = 1$	52.34 \pm 1.14	64.30 \pm 0.82	64.94 \pm 0.79	67.79 \pm 1.55	11.96
True	False	$\gamma = 3$	67.06 \pm 0.56	70.78 \pm 0.46	69.20 \pm 0.87	71.33 \pm 0.12	2.14
		$\gamma = 2$		69.43 \pm 0.80	67.75 \pm 0.61	70.86 \pm 1.21	0.69
		$\gamma = 1$		68.69 \pm 0.37	68.58 \pm 0.87	69.86 \pm 0.53	1.52
	True	$\gamma = 3$		68.12 \pm 1.06	68.92 \pm 0.54	71.33 \pm 0.12	1.06
		$\gamma = 2$		69.65 \pm 1.24	67.53 \pm 0.62	70.86 \pm 1.21	0.47
		$\gamma = 1$		64.30 \pm 0.82	64.94 \pm 0.79	69.86 \pm 0.53	-2.12

Table 3. Comparisons of two different training data augmentation and normal(without any other augmentation) conditions. Highlighted to light gray color indicates that best condition of each experiment environment. The model was trained with learning rate 1e-3. We also highlight best bias amplification score to gray color, the model trained with dataset split ratio 2 and *cutmix* with balancing sampled gender class method shows best amplification score when the attacker trained with gender balanced status. In every experiment setting on this table, *mixup* or *cutmix* shows better model leakage.

ation instead we use accuracy measure. Performance of trained model is measured with mAP score. We compared experiments of three different settings, ‘with mixup’, ‘with cutmix’, ‘without mixing augment’.

In detail of learning process, every model was trained with splits of dataset (Table 1). We wrapped Pytorch dataset to *mixup* dataset with fixed parameter of beta distribution α to one. *Cutmix* implemented similar way to *mixup*. We mixing only two images and we divided mixing sampling into two cases, one was sampling two data at random and the other was sampling data at balanced gender ratio. Later case means that mixed image should contain both gender features and the label should contain two gender classes. Wang did experiments with fixed learning rate but we used learning rate of 1e-5, 1e-4, 1e-3. The attacker was trained with different splits of datasets contrasting with Wang et. al. which used only gender balanced dataset.

4.2 Results

To summarize the results of our experiments, in most cases, *mixup* and *cutmix* have shown that they reduced bias amplification between model and dataset leakage (Table 3). However, the performances of Resnet model which trained with selected MS-COCO dataset are dropped slightly measured with mAP score whereas performance improvement was reported on *mixup* and *cutmix* with Imagenet dataset. We conducted experiments to observe the influence of internal class balance on the *leakage* and *bias amplification*. We was able to observe that leakage was decreased when the class ratio goes to equal but the bias amplification was largely increased. Control learning rate of transfer learning also have shown effect to model performance (Table 2). We conducted other experiments with learning rate 1e-3 which showed the best model performances. In default setting of Wang et. al., we could discover the underfitting issue it was arisen owing to insufficient learning rate which makes model parameters to stopped before it trained enough.

5. Conclusion

In this paper, we investigated to simple augmentation method to relax internal bias problem called mixing augment which is effective to this type of task. However it still remains hard work to remedy bias problem and improve model performance both.

References

- [1] Lin, Tsung-Yi, et al. "Microsoft coco: Common objects in context." *European conference on computer vision*. Springer, Cham, 2014
- [2] Russakovsky, Olga, et al. "Imagenet large scale visual recognition challenge." *International journal of computer vision* 115.3 (2015): 211-252.
- [3] Sutskever, I., O. Vinyals, and Q. V. Le. "Sequence to sequence learning with neural networks." *Advances in NIPS* (2014).
- [4] Goodfellow, Ian, et al. "Generative adversarial nets." *Advances in neural information processing systems*. 2014.
- [5] Buolamwini, Joy, and Timnit Gebru. "Gender shades: Intersectional accuracy disparities in commercial gender classification." *Conference on fairness, accountability and transparency*. 2018.
- [6] Wang, Tianlu, et al. "Balanced datasets are not enough: Estimating and mitigating gender bias in deep image representations." *Proceedings of the IEEE International Conference on Computer Vision*. 2019.
- [7] Zhang, Hongyi, et al. "mixup: Beyond empirical risk minimization." *arXiv preprint arXiv:1710.09412* (2017).
- [8] Yun, Sangdoo, et al. "Cutmix: Regularization strategy to train strong classifiers with localizable features." *arXiv preprint arXiv:1905.04899* (2019).
- [9] Chapelle, Olivier, et al. "Vicinal risk minimization." *Advances in neural information processing systems*. 2001.
- [10] Ribeiro, Marco Tulio, Sameer Singh, and Carlos Guestrin. "Why should i trust you?: Explaining the predictions of any classifier." *Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining*. ACM, 2016.
- [11] He, Kaiming, et al. "Deep residual learning for image recognition." *Proceedings of the IEEE conference on computer vision and pattern recognition*. 2016.

전력 데이터의 특징 추출 및 XGBoost 를 이용한 숙박 업소 재실 여부 판단

김에덴*, 고석갑*, 손승철*, 이형옥*, 이병탁*
*한국전자통신연구원

{kimed93, softgear, sson, oklee, bytelee}@etri.re.kr

Determination presence of people in accommodation using feature extraction and XGBoost method of energy data

Eden Kim*, Seok-Gap Ko*, Seung-Chul Son*, Hyung-Ok Lee*, Byung-Tak Lee*
*Electronics and Tele-communications Research Institute (ETRI)

요 약

스마트미터의 기술 발달과 보급으로 인해 전력데이터의 수집이 보다 수월 해짐에 따라 각 시스템에 효율적인 맞춤 서비스 제공을 위한 전력 데이터 분석 기술에 관한 다양한 연구가 활발하게 진행되고 있다. 관련하여 본 논문에서는 숙박업소의 각 방마다 전력소비량을 측정 및 수집하여 전력소비패턴을 분석하고 특징 추출 및 XGBoost 를 이용한 머신러닝 분석방법으로 각 방의 사람 재실 여부를 판별하는 방법을 소개한다. 이와 같은 연구를 통해 추후 숙박업소 혹은 숙박업소를 이용하는 소비자들의 맞춤 서비스 제공에 응용 및 적용 할 수 있다.

1. 서론

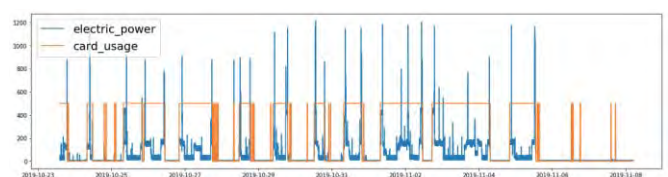
최근 에너지 분야에서 전력의 효율적인 사용과 관리를 위해 스마트 그리드 기술이 활성화 되면서 스마트미터의 보급이 늘어나고 있고, 이와 함께 지능형 시스템을 위한 기술 개발이 다양하게 이루어지고 있다 [1]. 특히, 보급된 스마트미터를 이용하여 에너지 전력 사용량을 실시간으로 측정하고 정보를 주고받는 기술들이 발달하면서 학교, 회사, 관공서 등 각 사용처에 맞춤 서비스 제공을 위해 전력 데이터 분석을 비롯한 많은 연구들이 진행되고 있다 [2]. 이에 일환으로, 본 논문에서는 전력 데이터를 이용한 숙박업소에서 사람의 재실 여부 분석 기술을 소개한다.

본 연구에서는 숙박업소의 각 방에 해당하는 전력 소비 데이터와 카드키 on/off 정보를 수집한다. 카드키 정보는 사람의 재실 여부를 파악하는 정보로 활용되며 기존 과거 전력 데이터와 카드키 정보를 통하여 머신러닝 모델 학습을 하고, 추후 전력 데이터만을 이용하여 재실 유무를 높은 정확도로 판별 가능함에 관한 실험을 진행하였다. 가장 간단하게는 전력 신호와 카드키 정보를 매칭하여 임계 값 설정을 통한 판별 방법 혹은 원시데이터를 이용한 머신러닝 분류

방법 등을 고안해 볼 수 있다. 하지만 보다 높은 정확도를 보이는 분석 알고리즘을 만들기 위해서 본 연구에서는, 전력 데이터는 시계열 특징을 가지는 것을 고려하여 시계열 데이터가 가질 수 있는 특징들을 생성 및 추출하였고, 원시데이터를 바로 사용하는 것이 아닌 새로 추출한 특징 벡터와 카드키 정보의 관계 매칭을 통해 XGBoost 방법을 적용함으로써 기존 단순한 판별 기술보다 더 우수한 결과를 나타내는 분석 알고리즘을 개발 하였다.

2. 데이터 수집 및 전처리

본 연구를 진행하기 위해 센서를 통하여 1 초단위의 전력 데이터와 카드키 정보를 실시간으로 수집하여 데이터베이스에 저장하였다. 수집한 전력 데이터와 카드키 정보의 관계는 다음 그림 1 과 같이 서로 연관성이 있음을 보여준다.

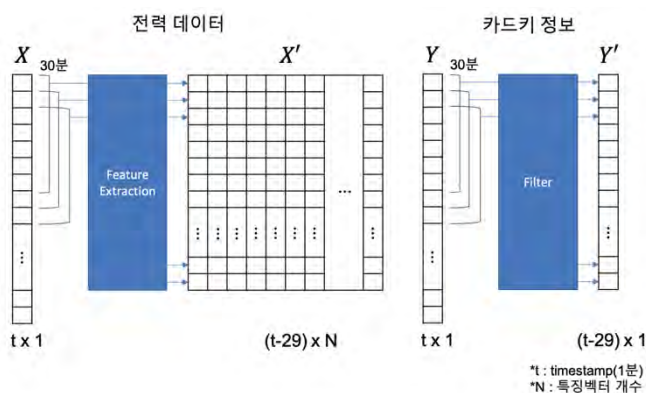


(그림 1) 전력데이터와 카드키 정보의 관계

각 데이터는 초단위로 수집되었지만, 재실 유무를 초 단위까지 고려하여 판별할 필요는 없기 때문에, 모든 데이터를 1분 단위로 평균을 통한 다운샘플링을 진행하였다. 전력 데이터는 방마다 기저 전력이 다르고 피크 전력량이 다르기 때문에 min-max 정규화를 통하여 모든 방의 전력들의 스케일을 조정하였다. 또한, 카드키 정보 중에는 1분 단위 기준으로 30분 이내 시간 동안 카드키가 on이 되었다 다시 off가 되는 경우가 간혹 존재하는데, 이의 경우는 실제로 손님이 대실 혹은 숙박의 목적으로 머무르고 있는 상황이 아니라 방 청소 혹은 잠시 물건만 놔두고 다시 외출하는 등 숙박업소에 재실 하는 경우와 다른 상황일 확률이 높아 30분 이내 기준으로 on되어있는 값들은 모두 off로 간주하도록 전처리를 진행하였다.

3. 특징 추출 및 XGBoost를 이용한 분석

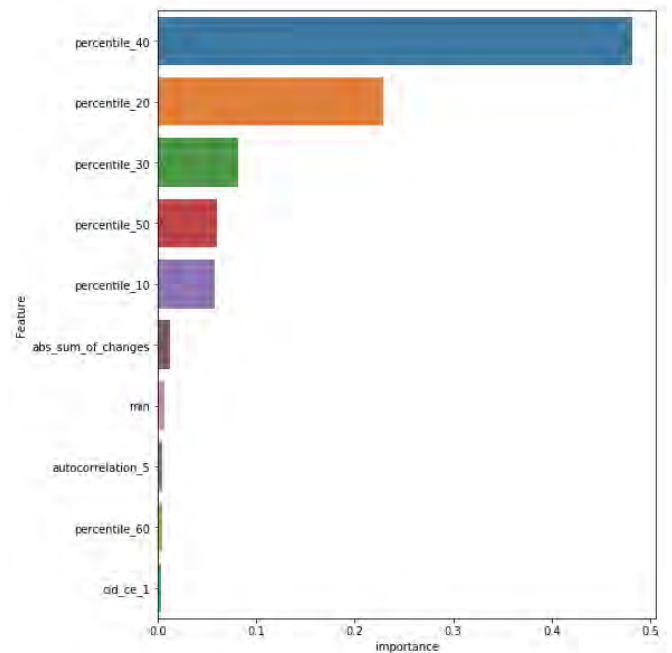
본 3 장에서는 전처리 된 전력 데이터와 카드키 정보를 통하여 시계열 특성을 반영한 특징 벡터들을 먼저 추출한다. 시계열 데이터의 특징 추출 방법에 관하여 다양한 연구들이 진행 되었는데, 그 중에 파이썬 패키지 중 하나인 tsfresh를 통한 특징 추출의 방법들에 대하여 참고하였다 [3]. 2장에서 30분을 기준으로 전처리를 진행하였던 바와 같이 본 연구에서 사용하는 데이터는 30분을 기준으로 데이터의 의미를 부여하여 30분동안의 시계열 전력 데이터 세트를 통하여 평균, 최댓값, 최솟값 등을 포함한 58가지의 시계열 특징 벡터들을 추출하였다. 카드키 정보의 경우는 30분을 기준으로 필터링 하여 30분동안 on인 경우가 off인 경우보다 많으면 on, off인 경우가 on인 경우보다 많으면 off로 카드키 정보를 재구성 하였다. 그림 2는 전력데이터의 특징 추출하는 과정과 카드키 정보를 필터링 하는 과정을 보여준다.



(그림 2) 데이터 셋의 특징 추출 및 필터링 과정

다음 진행으로는 특징 추출된 X'와 필터링 된 Y' 데이터 셋을 가지고 XGBoost 모델을 사용하여 학습

하였다. XGBoost는 캐글 커뮤니티에서 각광 받았던 트리 기반 부스팅 방법으로 빠르고 유연하게 사용 가능하고 보다 직관적이다 [4].



(그림 3) 모델의 상위 10 가지 Feature Importance

위 그림 3은 X'와 Y'를 XGBoost로 학습한 모델의 특징 중요도를 나타낸다. 선택한 58가지 시계열 특징들 중 가장 중요한 상위 10가지 특징들을 살펴보면 대부분 Percentile 특징들이 재실 여부를 판별하는데 중요한 정보를 가지고 있음을 알 수 있다.

4. 실험 결과 및 타당성 검증

3장에 기술한 특징 추출 및 XGBoost를 통한 분석 결과 검증을 위해 아래의 표 1과 같이 실험 데이터를 구성하였다.

<표 1> 실험 데이터 셋 구성

호	날짜	
	2019.10.23 ~2019.11.15	2020.01.23 ~2020.02.12
101	A1	A2
102	B1	B2
103	C1	C2

실험에 사용된 데이터는 한 숙박업소의 101호, 102호, 103호 방 세 곳의 전력 및 카드키 정보를 수집한 것이고, 각각은 19년 10월 23일부터 11월 15일까지의 데이터와 20년 1월 23일부터 20년 2월 12일까지의 데이터로 나누어 각각 A1, A2, B1, B2, C1, C2로 표기하였다.

다음과 같은 데이터 셋을 이용하여, 첫번째로는 같

은 방의 데이터를 사용한 트레이닝 및 테스트를 하는 방식, 두번째로는 두 방의 데이터를 트레이닝, 두 방 이외의 나머지 다른 방을 테스트 하는 방식으로 진행하여 기존 전력 원시데이터를 이용한 XGBoost 분석과 제안된 특징 추출을 통한 XGBoost 분석을 비교 실험하였다. 아래의 표 2 는 실험 데이터 셋에 따른 분석 결과 비교를 나타낸다.

<표 2> 실험 데이터 셋에 따른 판별 결과 비교

	실험 데이터 셋	판별 정확도	
		기본 방법	제안 방법
1	A1 트레이닝 A2 테스트	97.28%	99.78%
	B1 트레이닝 B2 테스트	94.04%	98.22%
	C1 트레이닝 C2 테스트	81.45%	98.21%
2	A1, B1 트레이닝 C2 테스트	82.27%	98.22%
	B1, C1 트레이닝 A2 테스트	83.31%	99.88%
	C1, A1 트레이닝 B2 테스트	73.62%	93.86%

전반적으로 같은 방의 데이터를 트레이닝 하고 테스트 하는 경우는 정확도가 대부분 90% 이상으로 높게 나왔으나, 트레이닝과 테스트 하는 방의 데이터가 다른 경우는 비교적 낮은 정확도를 보였다. 그 중에서도 원시데이터를 이용한 기본 분석 방법을 취했을 때는 70~80%의 낮은 정확도를 보였으나, 제안된 방법은 더 높은 정확도를 보여 이 논문에서 제안한 방법이 더 우수한 성능을 보이는 것을 확인하였고 두번째와 같은 실험을 통하여 트레이닝 셋에 포함되지 않은 다른 방을 테스트 하는 경우에도 여전히 90% 이상의 높은 정확도를 보여 실제 학습에 사용되지 않은 방의 경우도 전력데이터만 보유하고 있으면 꽤 높은 정확도로 사람의 재실 여부를 판별 할 수 있다.

5. 결론

스마트미터로부터 측정되는 전력데이터를 통하여 분석함으로써 여러 서비스들을 위한 정보를 제공 할 수 있다. 본문에서는, 특히 숙박 업소에 측정되는 에너지 전력 데이터를 통하여 사람 재실 여부를 판별하는 분석 방법에 대하여 소개하였다. 기본적인 방법으로 원시데이터를 머신러닝 적용하여 판별하는 것보다 본 논문에서 제시된 시계열 특징을 지닌 전력데이터의 특징 벡터를 뽑아 판별 분석하였을 때 더 뛰어난 정확도를 보임을 실험을 통하여 검증하였다. 본 연구에

나아가서는 본 논문에서 선택했던 58가지의 특징벡터들을 최적화 하는 방법, 결과의 후처리 등을 통하여 정확성을 더 높일 수 있을 것으로 보이며, 이와 같은 재실 판별의 정확도가 높아지면 숙박업소와 숙박업소를 이용하는 사람들을 위한 서비스 응용에 적용 가능할 것으로 보인다.

감사의 글

본 연구는 산업통상자원부(MOTIE)와 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구 과제입니다. (No. 20181210301570)

참고문헌

- [1] 이일우, et al. “스마트 그리드 기술 동향.” *한국통신학회지 (정보와통신)*, vol. 26, no.9, pp.24-33, 2009.
- [2] Alahakoon, Daminda, and Xinghuo Yu. “Smart electricity meter data intelligence for future energy systems: A survey.” *IEEE Transactions on Industrial Informatics*, vol.12, no.1, pp.425-436, 2015
- [3] Christ, Maximilian, et al. “Time series feature extraction on basis of scalable hypothesis tests (tsfresh-a python package).” *Neurocomputing*, vol.307, pp.72-77, 2018.
- [4] Chen, Tianqi, and Carlos Guestrin. “Xgboost: A scalable tree boosting system.” *Proceedings of the 22nd acm sigkdd international conference on knowledge discovery and data mining*, San Francisco, USA, 2016, pp.785-794.

시니어 사용자를 위한 언어 모델 기반 질환 증상 인식 방법

박민경*, 최진우*, 황보택근**†
*가천대학교 인공지능 헬스케어 연구센터
**가천대학교 컴퓨터공학과
parkminkyung32@gmail.com, {jwchoi, tkwhagbo}@gachon.ac.kr

A Symptom Recognition Method of Diseases for Senior User Based on Language Model

Min-Kyung Park*, Jin-Woo Choi*, Taeg-Keun Whangbo**†
*A.I. Healthcare Research Center, Gachon University
**Dept. of Computer Engineering, Gachon University

요 약

2025년 초고령 사회로 진입할 것으로 예상됨에 따라 고령화 시대에 발생하는 문제점들을 IT기술을 응용하여 지능적으로 해결할 수 있는 인공지능 헬스케어 솔루션이 주목받고 있다. BIS리서치의 보고서에 따르면 헬스케어 산업의 챗봇 시장 규모가 2029년 약 4억 9,800만 달러로 성장할 것으로 예상된다. 따라서 시니어 사용자를 위한 기술 연구가 적극적으로 필요한 시점이다. 본 논문에서는 사전학습한 언어모델과 BiLSTM기반 신경망 모델을 이용하여 시니어 사용자에게 특화된 질환 증상 인식 모델 구현에 관한 범위 및 방법에 대해 기술한다. 이는 시니어 대상 건강관리 챗봇 솔루션에 도입하여 시니어 사용자에게 자주 발생하는 질환들을 조기에 발견할 수 있도록 지원하여 위험의 발생 예방에 도움을 주는 서비스가 될 것으로 전망한다.

1. 서론

통계청의 2019 고령자 통계에 따르면, 우리나라 65세 이상 고령 인구는 급속히 증가하여, 2019년에는 고령사회가 되었으며, 2025년은 초고령 사회로 진입할 것으로 전망되고 있다. 이에 따라 인공지능 헬스케어 솔루션이 인구 고령화와 만성질환 환자 급증에 따른 삶의 질 저하에 대한 선제적, 예방적 대응의 핵심기술로 주목받고 있다. 특히 인공지능 기술과 자연어처리 기술을 접목한 ‘챗봇’ 기술은 사용자와 대화를 나누며 다양한 의학적 요구를 해결할 수 있는 창구의 기능을 할 것으로 기대되고 있다. 하지만 아직 챗봇은 사용자의 요청과 의도의 뉘앙스를 완벽히 이해하지는 못하며 응답에 관한 자유도가 낮다는 한계가 있다. 일반 사용자가 사용하기에도 한계가 있는 챗봇을 시니어 사용자에게 적용하려고 한다면 다른 접근 방식을 이용해야 한다고 판단하였다. 따라서 본 연구에서는 기존의 대화식 명령을 이용하는 챗봇이 아닌 시니어 사용자의

발화를 통해 증상을 예측하고 나아가 관련된 질병에 대한 정보를 받을 수 있는 ‘시니어 건강 관리’ 분야에 집중한 딥러닝과 자연어처리 기반의 ‘시니어 대상 건강관리 챗봇 솔루션’ 개발 내용 중 ‘시니어 사용자 질환 증상 인식’ 신경망 모델을 개발하였고 이를 기술한다.

2. 모델 구현 범위 및 방법

2.1 언어 모델 학습 데이터

대용량의 코퍼스를 사전 학습시켜 단어 임베딩을 생성하는 언어모델을 구축하기 위해, ‘네이버 지식인’의 건강 카테고리 질문 글을 덤프 데이터로 사용하였다. 헬스케어 분야는 챗봇이 응답을 자연스럽게 하려면 방대한 지식과 학습이 요구되는데, 실제 의료데이터는 접근에 한계가 있다. 개방형 데이터나 서비스 또는 크롤링 기술을 통해 활용 가능한 콘텐츠 확보를 위해 ‘네이버 지식인’의 건강 카테고리 질문 글 중 ‘의사 답변’이 등록된 게시글을

크롤링하여 챗봇에 활용할 수 있는 형태로 구축하였다. 보통 자연어처리를 위한 코퍼스 구축에는 Wikipedia같은 문어체로 이루어진 덤프 데이터를 많이 사용하지만, 대화체로 작성된 ‘네이버 지식인’ 데이터가 챗봇 발화 및 응답 시스템을 구축하기에 적절할 것으로 판단하였다. 한 문장씩 데이터 셋을 구성하면 문장당 토큰의 수가 작으므로 모델이 문맥을 파악하기 힘들어 학습이 잘 진행되지 않는다. 따라서 한 게시 글 당 하나의 데이터로 구성하였으며 Word2Vec 모델 훈련 데이터로 사용한 게시글은 총 175,884개이다.

2.2 질환 증상 학습 데이터

가천대 길병원 의료진들을 대상으로 설문조사 및 진료협력센터 자료를 통해 확보한 ‘질환DB 데이터’는 시니어 다빈도 질환에 관련된 증상명 36가지의 ‘증상명’, ‘정의’, ‘동의어’가 수록되어 있다. 이 중 ‘증상명’과 ‘동의어’를 키워드로 사용해 지식인 데이터(2009-2020)를 추출하였다. Supervised Learning을 진행하기 위해 추출한 게시 글 중 Question 컬럼은 입력데이터로 Keyword 컬럼은 Label로 사용하였다.

<표1> 훈련 데이터 예시

구분	내용
Index	4
Question	며칠 전부터 심장이 마치 긴장되거나 떨리듯 한 느낌과 가슴이 터질 것 같은 통증과 함께 식은땀도 나고 10 분 가까이 숨이 조여 오는 듯 했습니다.
Keyword	심계항진

KoNLPy의 ‘Kkma’ 형태소 분석기를 사용해 데이터를 정제하였고, 한 문장 내 토큰 수는 대부분 500안팎이며 주로 0-200 사이인 것을 고려해 길이를 512로 제한하여 Outlier를 무시하였다. 이렇게 총 115,711개의 훈련데이터를 생성하였다.

2.3 언어 모델

언어모델 생성을 위해 텍스트 분류 문제에 많이 사용하는 인공 신경망 기반의 텍스트 임베딩 방법론 중 하나인 Word2vec을 이용하였다. Word2vec은 유사한 의미가 있는 어휘는 유사한 문맥에서 등장한다는 Distributional Hypothesis에 기반하여 인공 신경망을 이용해 단어(토큰)를 연속적인 벡터 공간으로 임베딩하는 방법이다.

$$p(o|c) = \frac{\exp(u_o^T v_c)}{\sum_{w=1}^W \exp(u_w^T v_c)}$$

(식1) Distributional Hypothesis

Word2vec은 중심단어(c)가 주어졌을 때, 주변단어(o)가 등장할 조건부 확률인 (식1)을 최대화하는 쪽으로 학습이 진행된다. 총 175,884개의 데이터를 KoNLPy의 ‘Kkma’ 형태소 분석기를 사용해 추출한 토큰의 수는 총 30,830개 였으며 Word2vec 모델의 Hyper parameters는 다음 <표2>와 같다.

<표2> Word2Vec Model Hyper Parameters

Iter	Size	Window	Workers	Min_count	Sg
300	256	10	4	10	1

Size는 임베딩 벡터의 차원을 뜻하는데, 차원이 높을수록 Embedding word의 품질이 향상되고 주로 128, 256차원으로 지정한다.[1] 실험에서는 200차원에서 300차원 사이로 지정할 때 좋은 성능을 보였다. min_count는 단어 등장 최소 빈도수를 의미하며 3에서 5, 10으로 늘려가며 실험을 진행하였으며 min_count의 수가 높아질수록 Task Model의 val_loss 값이 개선되었다. Sg는 0이면 CBOW, 1이면 Skip-grams 방식을 사용한다. 여러 논문에서 성능 비교를 진행하였을 때, 전반적으로 Skip-grams 성능이 좋다고 알려져 있다[1]. 또, Window는 10으로 설정하였고 이는 Skip-grams를 사용할 경우 권장 값이다[2]. 다른 파라미터는 Task Model의 성능에 눈에 띄는 영향이 없었다.

2.4 신경망 학습 모델

RNN의 Gradient vanishing/exploding 문제에서의 취약점을 개선한 ‘Bidirectional LSTM’모델을 분류 모델로 사용하였다. BiLSTM(양방향 장단기 기억)계층은 시계열, 시퀀스 데이터의 스텝 간의 양방향 장기 종속성을 학습하고 모델이 전체 시퀀스로부터 학습하도록 할 때에 유용하므로 모델로 선정하게 되었다[3]. 긴 문장에서 포함한 단어의 주변 정보를 균형 있게 담기 위한 BiLSTM 레이어와 각 Feature Map의 상의 노드의 평균값을 뽑아 차원을 줄이는 GlobalMaxPool1D레이어로 모델을 구성하였다. 모델 출력층의 활성화(activation), 손실(loss) 함수는 Multi-class Classification 문제에 사용하는 ‘Softmax’, ‘Categorical Cross-entropy’로 Keras API를 사용하였고 batch크기는 64로 학습하였다. 과적합을 방지하기 위해 Keras API EarlyStopping을 loss기준으로 적용하였고 epoch 40에서 훈련을 멈추어 복잡도를 낮게 파라미터를 조정하였고 처음 지정한 epoch 300 모두 수행한 후 훈련을 마쳤다.

3. 결과 및 분석

3.1 학습, 검증 및 시험 데이터 결과

<표3> Model Performance Evaluation

Accuracy	Loss	Val_acc	Val_loss	Test_acc
0.9442	0.1914	0.9381	0.8704	0.8349

<표4> Classification Report

	Precision	Recall	F1-score
Macro avg	0.92	0.90	0.91
Weighted avg	0.93	0.93	0.93

모든 클래스의 평균 Precision, Recall, F1-score는 <표4>와 같으며 각 클래스의 수를 고려하지 않는 Macro 평균 보다, 클래스 수별 가중치를 둔 Weighted 평균의 값이 더 컸다. 각 클래스의 f1-score, recall, precision을 고려하여 최종 모델을 선정하였다. 본 문제는 다중 클래스 문제를 다루고 있어 Accuracy 성능보다는 Precision, Recall의 가중조화평균(Weight harmonic Average)인 F-score를 지표로 활용해야 한다. Scikit-learn의 metrics 패키지를 통해 각 클래스별 precision, recall, f1-score를 포괄적으로 살펴보았고 훈련데이터는 각 class의 개수가 다른 Imbalanced 데이터므로 f1-score에 중점을 두어 최종 모델을 선정하였다.

3.2 결과 분석

실험 결과는 토큰의 수가 많은 문장으로 학습하여도 적은 토큰의 수의 발화 데이터도 잘 인식한다는 것을 확인하였다는 것에 의의가 있다. 훈련데이터는 평균 70개의 토큰으로 우리가 챗봇에 사용하는 데이터와는 다소 차이가 있다. 챗봇 발화에 사용되는 문장은 3~20개 정도의 토큰을 가진 길이의 문장일 것이다. 선정한 모델로 예측 모듈을 만들고, ‘요즘에 잤은 기침이 있어.’, ‘어제는 잇몸에서 피가 났어.’ 등 실제 챗봇에 사용하듯 문장을 입력으로 넣고 테스트를 진행해 보았을 때, 긴 문장으로 테스트했을 때와 큰 차이 없이 잘 진행되었다.

또한 36개의 클래스 중 24개의 클래스의 f1-score가 0.9이상으로 측정되었다. 하지만, 데이터를 수집하는 과정에서 클래스 불균형이 생기고 실제로 테스트를 진행해 보았을 때도 수가 적은 클래스의 예측은 성능이 다른 클래스에 비해 떨어진다는 연구[4]처럼 실제 테스트에서도 이를 확인하였다. 따라서 향후 연구로 재샘플링 기법을 이용하여 이를 보완하거나 데이터 구축이 가능하다면, 문제 자체를 Multi-Label Classification 문제로 바꾸어 연구를 진행하려고 한다.

4. 결론

본 연구에서는 ‘시니어 대상 건강관리 챗봇 솔루션’을 위해 시니어 사용자의 발화 데이터를 얻고, 발화 속의 증상을 분류하는 신경망 모델 연구에 관해 기술하였다. 연구를 통해 최종적으로 선정된 Word2vec 언어 모델과 BiLSTM 신경망 모델의 조합으로 구성된 증상 분류 모델의 활용방안은 다음과 같다.

건강보험공단 자료를 바탕으로 시니어 다빈도 질환 상위 100개 중 질환명이 특정되는 질환들 41가지를 선정하고 질환 별 ‘정의’, ‘원인’, ‘진료과’, ‘진단’, ‘증상’, ‘증상 설명’, ‘치료’, ‘동의어’, ‘관련 질환’ 컬럼으로 구성된 활용데이터를 이용하여, 시니어 사용자의 발화에서 분류된 증상들의 조합으로 시니어 사용자들에게 의심되는 질환을 알려주고 질환의 정보에 관해 알려주어 건강관리를 도와주는 헬스케어 챗봇을 구현할 예정이다. 이는 AI기술과 사회적 이슈가 융합된 신성장 동력 서비스로써 좋은 예가 될 것이며 시니어 사용자들의 다양한 의학적 요구를 해소하며 나아가서는 의료비 감소, 모니터링 시스템 대체로 인건비 등에 대해 비용 절감이 가능한 기술이 될 것으로 기대된다.

Acknowledgement

본 연구는 경기도의 경기도 지역협력연구센터 사업의 일환으로 수행하였음.

[GRRC-가천2017(B04), 인공지능기반 의료상담 챗봇 최적화 솔루션 개발]

참고문헌

- [1] Mikolov, Tomas; et al, ICLR 2013 conference submission, "Efficient Estimation of Word Representations in Vector Space". arxiv.org/abs/1301.3781, 2013
- [2] "Google Code Archive - Long-term storage for Google Code Project Hosting", <https://code.google.com/archive/p/word2vec/>
- [3] Tao Chen; et al. "Improving sentiment analysis via sentence type classification using BiLSTM-CRF and CNN", Elsevier, 2017
- [4] 서민지 외, 클래스 불균형 문제가 있는 다중클래스 텍스트 분류에서의 특징 선택 방법. 대한산업공학회지, 45(2), 93-100, 2019

EEG, MRI 와 조현병의 상관관계를 이용한 진단 시스템 연구

성지현*, 김도연*, 김지은*
*이화여자대학교 컴퓨터공학과
e-mail: {szh1109, ririiiing, taurusx}@naver.com

Study on a Diagnosis System using Correlation between Schizophrenia and EEG, MRI data

Ji-Hyeon Seong, Do-Yeon Kim, Ji-Eun Kim
Dept. of Computer Science and Engineering, Ewha Womans University

요 약

조현병(정신분열증)은 사고, 감정, 지각, 행동 등 인격의 여러 측면에 걸쳐 광범위한 임상적 이상 증상을 일으키는 정신 질환이다. 심각한 정신 질환임에도 불구하고 여전히 과학적 진단 체계가 갖춰져 있지 않아 진단의 많은 부분을 환자의 진술에 의존하고 있으며, 이로 인해 조현병이라는 진단을 받고 치료방법을 찾는 데 까지 오랜 시간이 걸린다. 이에 본 연구는 EEG, MRI 데이터와 조현병의 상관관계를 이용한 조현병 진단 시스템을 제안하고자 한다. 본 시스템은 MRI 데이터와 머신러닝 알고리즘을 통한 조현병의 확률적 진단과 함께, EEG 데이터의 시각화 기능을 제공하는 소프트웨어를 개발함으로써 조현병 진단의 과학적 근거를 의사에게 제공하여 정확한 병의 진단을 목표로 한다. 진단 후에는 환자 데이터의 체계적 관리를 통해 머신러닝 알고리즘의 학습 데이터 확보 및 환자의 상태를 지속적으로 관리·관찰 할 수 있도록 하여 의료 소프트웨어로서 조현병의 체계적 진단 및 관리 시스템을 구축한다.

1. 서론

현재 전 세계 인구의 약 0.7%가 조현병(정신분열증)을 앓고 있으며, 그 수는 매년 꾸준히 증가하고 있다. 조현병은 완치가 힘들지만 조기 치료를 할 경우 그 증세가 호전될 수 있어, 빠르고 정확한 진단과 그 후의 지속적 경과 관찰을 통해 호전된 상태를 유지하는 것이 중요하다. 하지만 육체적 질환과 달리 정신 질환의 특성 상 조현병은 여전히 체계적 진단 시스템이 없어, 진단 시 환자의 진술과 행동 특성 관찰에 대부분을 의존하고 있다. 이 때문에 오진 확률이 매우 높으며 환자는 수년에 걸쳐 자신에게 맞는 치료법을 찾게 된다. 특히 조현병 발병의 과학적 원인을 찾지 못해 발생한 사회적 편견은 환자들이 자신의 병을 숨기고 치료를 기피함으로써 병을 더욱 악화시켜 범죄로 이어지기도 하는 등의 사회적 문제를 야기한다.

최근 4 차 산업혁명의 빅데이터 및 인공지능(AI) 기술을 기반으로 의료 산업은 변화하고 있다. 정신의학계에서도 정신 질환과 여러 의료 데이터의 연관성을 밝히는 연구가 활발히 진행되고 있다. 특히 머신러닝 알고리즘과 MRI, EEG(뇌파) 데이터를 이용하여 조현병 환자와 건강인을 높은 정확도로 분류할 수 있음을 입증한 연구의 등장으로 조현병에 대한 과학적 진단의 가능성이 제시되었다. MRI 를 이용한 신경 영상 연구는 조현병 발병 후 뇌의 구조적·기능적 변화의 연관성을 발견하였고, EEG 는 밀리세컨드

(ms) 간격의 측정으로 뇌의 미세한 변화를 감지하여 인간의 인식 과정에 대한 신경 역학 분석 도구를 제공하였다.[1, 2] 그러나 이와 같은 연구들은 조현병 진단 및 치료를 위해 활용되지 못하고 단순히 연구에만 그치는 한계점이 있다.

이에 본 연구는 조현병과 유의미한 상관 관계가 있는 MRI, EEG 데이터를 활용하여 조현병을 자동으로 진단하는 시스템을 제안하고자 한다. 본 시스템은 소프트웨어로 MRI 데이터와 가우시안 프로세스를 이용한 조현병의 확률적 진단과 함께, EEG 데이터 시각화 기능을 통한 표준 건강인과 환자의 비교 뇌파 그래프를 제공함으로써 환자의 뇌 상태를 관찰할 수 있도록 한다. 정신의학과 전문의에게 조현병 진단을 위한 여러 객관적 지표를 제공함으로써 오진의 가능성을 줄이고, 환자는 정확한 진단으로 빠른 시일 내에 적절한 치료를 받을 수 있다.

2. 이론적 배경

2.1 MRI 와 조현병의 상관관계

최근 몇 년간 이론신경과학(계산신경과학, computational neuroscience)에 대한 과학계의 관심은 지속적으로 증가했다. 특히 이에 활용되는 수학적 이론(computational method)은 전처리

후의 MRI(자기공명영상) 데이터 분석에 많이 적용되고 있다. MRI 데이터를 분석하는 것은 인간의 뇌 특징을 특정하고 설명하기 위한 혁신적인 생물정보학적 방법이다. 수년간의 신경영상(neuroimaging) 연구는 정신 질환 장애와 뇌의 구조적·기능적 변화의 존재 사이에 설득력 있는 연관성을 확립하여 조현병 진단의 새로운 대안을 제시하였다.[3]



(그림 1) MRI 스캔에서 파생되는 수치 데이터

특히, fmri와 smri를 이용한 환자의 뇌 상태 분석을 통해 조현병이 뇌에 미치는 영향에 대한 연구들이 진행됨에 따라, 신경영상연구와 MRI 데이터 처리 기술을 기반으로 그림 1과 같은 데이터 처리가 가능해 졌다.[4] 변환된 MRI 수치 데이터를 이용한 머신러닝 알고리즘의 조현병 환자와 건강인의 분류에 대한 연구는 상당히 고무적이다. 이는 MRI 데이터가 조현병과 유의미한 상관관계가 있다는 것을 입증함으로써 조현병의 확률적 진단을 가능하도록 한다.

2.2 EEG와 조현병의 상관관계

밀리세컨드(ms) 수준의 해상도인 EEG 데이터는 인지에 대한 신경 역학을 분석하는 민감한 도구이다. 정신생리학적 연구에 사용되는 EEG 활동의 주요 척도는 ERP(사건관련전위)로, 특정 시간에 발생하는 이벤트(자극)에 대한 전압 변화의 표준 패턴으로 정의되며 평균 파형에서 측정된 피크 진폭에 의해 정량화 된다.

ERP	시계열	극 값(피크)
N100	이벤트 후, 100ms 전후	음의 피크
P200	이벤트 후, 200ms 전후	양의 피크
P300	이벤트 후, 300ms 전후	양의 피크

(그림 2) ERP 데이터의 종류

조현병 환자는 ERP 데이터의 N100, P200 등의 특정 시계열에서 건강인에 비해 억제된 파형 그래프, 즉 피크 값이 건강인에 비해 떨어지는 뇌파 파형이 나타난다. 또한 환자는 이벤트에 건강인보다 느리게 반응하는 특징을 가져, 그림 2의 시계열에서 그래프의 파형으로 EEG 데이터를 시각화하면 전압 차이 및 이벤트 반응 속도에 대한 건강인과 조현병 환자의 차이를 확인할 수 있다. 이는 조현병 환자의 뇌 상태에 대해 MRI와는 다른 지표를 제공한다.[5]

2.3 데이터 검증

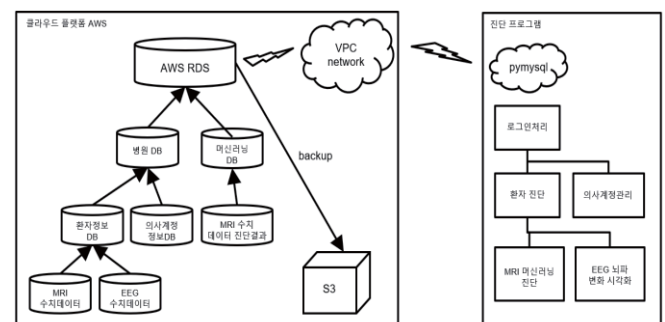
연구에서 사용된 데이터는 Kaggle에서 가져왔으며, 시스템에 활용하기 위해 머신러닝 정확도를 검증해 보았다. 먼저 검증에 사용한 MRI 데이터는 그림 1과 같이 fmri에서 파생된 FNC와 smri에서 파생된 SBM 수치 데이터(SZ-40, HC-47)로, 머신러닝 모델인 가우시안 프로세스에 학습 시 조현병 환자와 건강인을 평균 92%의 정확도로 분류할 수 있다.[6]

ERP 데이터(SZ-49, HC-32)는 EEG의 64개의 전극 채널과 그 외의 얼굴 부위 6개의 전극 채널로 측정된 데이터로 그림 2와 같은 시계열의 피크 값을 추출하는 데이터 가공 과정을 거쳤다.[7] 하지만 검증 결과, 머신러닝 모델 및 퍼셉트론(심층 신경망) 학습 시, 훈련 정확도는 평균 97%로 우수하지만 검증 정확도는 평균 59%로 낮았다. EEG 데이터의 특성 상 노이즈로 인해 머신러닝 모델 학습 중에는 정확도가 증가하지만 검증 정확도는 떨어지는 과적합이 높은 확률로 발생했으며, 뇌파 측정 환경이나 조건(이벤트)에 영향을 많이 받기 때문에 데이터에 따른 머신러닝 정확도 차이가 크게 나타났다. 이에 머신러닝을 활용한 진단 데이터로서는 부적합하다는 결론에 도달하였다. 하지만 데이터를 파형 그래프로 나타냈을 경우, 이벤트에 따른 환자의 구체적 인식 과정을 확인할 수 있기 때문에 MRI의 확률적 진단과는 다른 지표를 제공하는데 분명한 의의가 있다.

3. 시스템 개요

3.1 제안 시스템 구조

최근 머신러닝 기반의 의료 진단 보조 소프트웨어가 많이 개발되고 있는 추세이나, 정신질환에 있어서는 미비한 실정이다. 이에 MRI, EEG와 머신러닝 알고리즘을 이용한 조현병 진단 시스템을 제안하고자 한다.[8] 환자의 진술에 의존하여 진단을 하는 기존의 방식과는 달리, 환자의 뇌를 검사한 객관적인 MRI 데이터를 이용해 조현병 진단을 하도록 한다. 또한, 분석하기 어려운 EEG 수치 데이터의 시각화를 통해 환자의 인식 과정에 따른 뇌의 상태를 관찰하고, 진단 결과 데이터의 축적을 통해 병의 경과를 추적한다. 이를 통해 조현병의 진단 및 환자 관리 시스템의 체계를 구축하여 의사와 환자 모두에게 편리성을 제공한다.

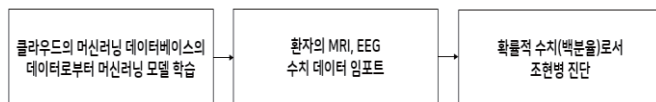


(그림 3) 시스템 구조도

그림 3 은 시스템의 구조를 나타낸 것으로 다음과 같은 컴포넌트들로 구성된다.[9]

- 환자 진단 머신러닝 알고리즘: MRI 데이터로 사전 학습된 가우시안 프로세스 알고리즘으로 병에 대한 확률적 진단을 내리는 기능을 수행한다.
- 데이터 시각화: EEG 데이터를 특정 시계열(N100, P200)에서 뇌파 파형으로 시각화하여 제공하며, 환자의 과거 진단 결과를 꺾은선 그래프로 나타내어 데이터 분석을 용이하도록 한다.
- 클라우드 데이터베이스: 병원 데이터베이스와 머신러닝 데이터베이스로 나뉘어 데이터를 관리한다.

3.2 조현병 진단

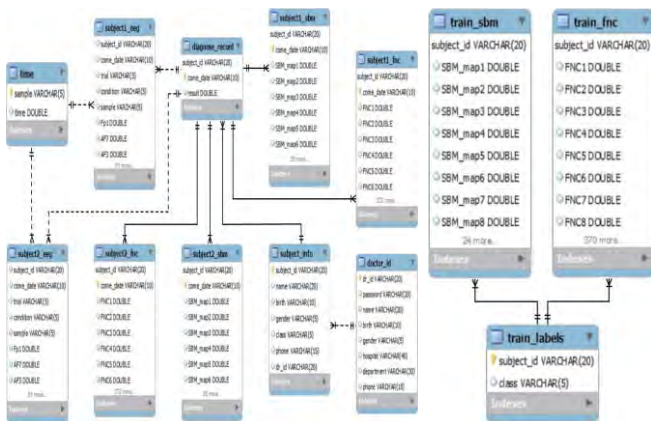


(그림 4) 조현병 진단 로직

그림 4 는 환자의 조현병 여부를 진단하기위한 로직이다. 머신러닝 모델은 GPtoolbox 의 가우시안 프로세스(GP) 분류기를 사용하였으며, 관측치는 베르누이(0,1) 분포로 도출된다. 여기서 가우시안 프로세스란, 랜덤 변수의 집합으로 각각 가우시안 분포(정규 분포)를 가지며 제한적 최적화 및 이미지 처리에 유용하다. 예측 확률은 단위 간격으로 변환하는 시그모이드 함수(0,1)를 기반으로 한다.

모델은 환자를 진단하기 전에 데이터에 대한 학습이 완료되어 있어야 한다. 환자의 검사 결과는 수치로서 전처리 되어 시스템에 사용되며, 진단 결과는 백분율(%)로 제공된다.

3.3 클라우드 데이터베이스



(그림 5) 좌. 병원 데이터베이스 우. 머신러닝 데이터베이스 스키마

최근 병원은 자율 데이터베이스 관리와 전자차트, 보안 강화 등의 서비스가 제공되는 클라우드 기술에 주목하고 있다. 특히 환자 데이터의 저장 및 분석, 진단과 진료 정보 교류 등에서 클라우드의 수요가 높아지고 있으며, 실제 클라우드 시스템을 도입하는 병원도 늘어나고 있는 추세이다.[10] 본 시스템은 이런 변화를 반영해 클라우드 데이터베이스를 구축하여 시스템과의 연결을 통해 데이터를 관리한다. 그림 5 와 같이 병원 데이터베이스는 의사, 환자 정보 관리 및 환자의 MRI, EEG 데이터를 저장하고 머신러닝 데이터베이스는 오직 MRI 데이터와 0(건강인), 1(환자)로 구분된 환자의 결과만 저장하여 머신러닝 모델 학습에만 사용된다. 병원 데이터베이스와 머신러닝 학습 전용 데이터베이스의 분리를 통해 환자의 개인 정보를 안전하게 보호함과 동시에 머신러닝을 위한 데이터는 공유 가능하도록 하여, 인공지능 기술을 위한 의료 데이터베이스로서 기능한다.

4. 시스템 구현 결과

4.1 시스템 사용자 인터페이스

본 시스템의 실제 소프트웨어 구현 결과는 그림 6, 7 과 같다. 사용자는 정신건강의학과 전문의로 가정한다. 사용자는 프로그램 실행 후 본인의 ID 와 PW(password)로 시스템에 로그인 할 수 있다. 전문의 계정 정보, 환자의 개인 정보 및 검사 데이터는 클라우드 데이터베이스 플랫폼인 AWS RDS 에서 저장·관리된다. 로그인 후 의사는 그림 6 의 환자 등록 및 데이터 등록 화면 외 환자 진단, 의사 계정 관리 메뉴에 접근할 수 있다.

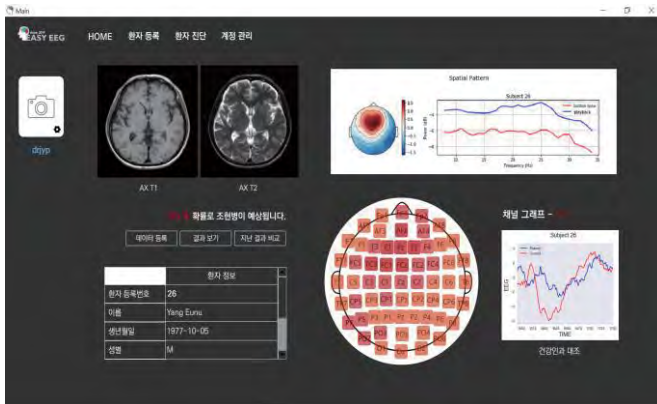
The image shows two screenshots of the system's user interface.

- Left Screenshot (Patient Registration):** A form titled '환자 등록' (Patient Registration) with fields for '환자 등록번호' (Patient Registration Number), '이름' (Name), '생년월일' (Date of Birth), '성별' (Gender) with radio buttons for MALE and FEMALE, '조현병 여부' (Schizophrenia Status) with radio buttons for HC, SZ, and Pending, '연락처' (Contact), and '등록 의사 ID' (Registration Doctor ID). There are '등록' (Register) and '취소' (Cancel) buttons at the bottom.
- Right Screenshot (Exam Data Registration):** A form titled '검사 데이터 등록' (Exam Data Registration) with a dropdown for '등록 일자' (Registration Date) showing '2020-01-01'. It has input fields for 'FNC Data', 'SBM Data', and 'EEG Data', each with a '파일 업로드' (File Upload) button. There are 'OK' and 'Cancel' buttons at the bottom.

(그림 6) 좌. 환자 등록 우. 검사 데이터 등록

<환자 등록> 메뉴 선택 시, 환자의 기존 등록 여부에 따라 다른 절차를 따른다. 새로운 환자 등록 시 환자의 이름, 생년월일, 성별, 조현병 유무, 전화번호 등의 개인 정보를 입력 후 환자 등록 번호(subject_id)를 부여한다. 주치의는 현재 로그인 중인 의사로 자동 배정된다. 기존 환자 등록 시에는 <환자 조회> 란에 환자 등록 번호를 검색하여 해당 환자를 찾는다. 환자 설정 후, 전처리가 완료된 EEG, MRI-FNC, MRI-SBM 데이터를 업로드 한다. 환자 정보와 EEG 데이터는 병원 DB 에 업로드되며, MRI 데이터는 환자 검사 정보로서 병원 DB 에, 머신러닝 모델 학습 데

이터로서 진단 후 머신러닝 DB에 각각 업로드 된다. 이 때, 의사가 조현병 환자로 진단 할 경우 label 1을 부여 받으며, 머신러닝 데이터베이스에 저장 시 진단 확률이 아닌 오직 0, 1로만 저장된다. 머신러닝 학습은 새 데이터가 입력되었을 때 진단 후 재학습하도록 설정되어 있다.



(그림 7) 환자 진단 화면

<환자 진단> 메뉴 선택 시, 해당 환자의 데이터 분석 결과를 이용해 의사가 종합적으로 판단한다. 진단 결과 화면의 좌측에는 MRI-FNC, SBM의 절단면 이미지와 머신러닝을 이용한 확률적 진단 결과가 백분율(%)로 출력되며, 화면의 우측에는 EEG 데이터의 파형 그래프를 볼 수 있다. 먼저, 우측 아래의 위치 별 전극을 선택하면, N100-P200 구간의 해당 환자 뇌파 그래프(파란색 선)와 건강인의 평균 뇌파 그래프(빨간색 선)를 함께 비교-확인할 수 있다. 그 상단에는 1. 버튼을 누른 후, 생성되는 톤을 듣는 이벤트에 대한 뇌파가 붉은색으로 표시되고 2. 지속적으로 일정한 톤을 듣는 이벤트의 뇌파가 파란색으로 표시되어 이벤트에 따른 환자 상태를 알 수 있다. 마지막으로 '지난 결과 보기'를 통해 환자의 과거 진단 기록을 꺾은선 그래프로 출력하여 시간이 지남에 따른 경과 관찰이 가능하다.

4.2 조현병 진단 시나리오

본 시나리오에서 의사의 계정 정보 데이터는 정신건강의학과 전문의를 가정하고 임의로 생성한 데이터이며, 조현병 환자의 EEG, MRI 데이터는 학습 데이터와 같은 출처의 Kaggle 데이터를 사용하였으나, 학습 데이터와는 철저히 분리하여 진행하였다.

환자 진단 결과는 그림 7과 같다. 먼저, 92%의 확률로 조현병 환자와 건강인을 구분하는 머신러닝 모델을 사용하여 확률적 수치 결과를 도출한다. 진단 결과는 90%로 조현병 환자라는 잠정적 진단을 내릴 수 있다. 또한 우측의 뇌파 그래프에서, 파란 파형의 환자가 빨간 파형의 건강인과 비교하여 N100의 시점에서 더 느리고 억제된 피크를 나타내는 것이 확연히 드러나며, 이는 조현병 환자의 뇌파 특성과 일치한다. 의사는 이 두 가지 과학적 근거와 기존의 환자 진술 및 행동관찰의 소견을 종합하여 해당 환자가 조현병이라는 결론에 도달할 수 있다. 이는 기존의 진단 방법보다 더욱 향상된 확률로 조현병 진단을 가능하게 한다.

4.3 적용 결과

정성적 진단만을 이용했던 기존 진단 방법과 달리, 진단 결과가 수치와 그래프로 표현됨으로써 정량적 진단이라는 객관성을 획득할 수 있다. 또한 그래프 및 시각화를 통해 문자나 수치로만 데이터를 표현했을 때보다 직관적인 판단이 가능하다.

하지만 뇌파 데이터 전체를 관계형 데이터베이스의 테이블(table) 형태로 저장 후 프로그램에서 불러올 시, 다시 데이터 프레임(data frame)화 하기 때문에 뇌파 그래프 출력에 대한 응답 시간이 다소 길게(약 1분) 측정되는 한계가 있다. 또한, 임상실험을 통해 보다 많은 환자의 데이터를 확보를 통한 머신러닝 모델의 신뢰성 향상이 필요하다.

5. 결론

본 논문에서는 MRI 데이터의 머신러닝 모델 학습 결과를 바탕으로 조현병 여부를 확률적으로 진단하고, 환자의 이벤트에 따른 뇌파 변화 양상을 활용하여 적절한 조기 치료가 중요한 조현병 환자를 진단하는 시스템을 제안한다. 육체적 질병과 같이 객관적 검사를 통한 정신 질환의 진단이라는 의의를 가진다. 향후 의료 전문가 혹은 병원과의 협업을 통해 전문적 의료 지식과 충분한 데이터를 토대로 연구를 진행한다면 보다 신뢰도 있는 시스템을 제공할 수 있을 것이라 기대된다.

참고문헌

- [1] Elisa Veronese, Umberto Castellani, Denis Peruzzo, Marcella Bellani, and Paolo Brambilla, Machine Learning Approaches: From Theory to Application in Schizophrenia, Mathematical Methods and Applications in Medical Imaging, Article ID 867924, p12, 2013
- [2] Jason K. Johannesen, Jinbo Bi, Ruhua Jiang, Joshua G. Kenney & Chi-Ming A. Chen, Machine learning identification of EEG features predicting working memory performance in schizophrenia and healthy adults, Neuropsychiatric Electrophysiology, Article number: 3, 2016.2.11
- [3] Sarina J. Iwabuchi¹, Peter F. Liddle¹ and Lena Palaniyappan, Clinical utility of machine-learning approaches in schizophrenia: improving diagnostic confidence for translational neuroimaging, Front. Psychiatry, 29 August 2013
- [4] MLSP 2014 Schizophrenia Classification Challenge, <https://www.kaggle.com/c/mlsp-2014-mri>
- [5] Judith M. Ford, Vanessa A. Palzes, Brian J. Roach, and Daniel H. Mathalon, Did I Do That? Abnormal Predictive Processes in Schizophrenia When Button Pressing to Deliver a Tone, Schizophr Bull. 2014 Jul; 40(4): 804-812. 2013 Jul 10
- [6] asolin, MLSP2014-kaggle-challenge, <https://github.com/asolin/MLSP2014-kaggle-challenge>
- [7] EEG data from basic sensory task in Schizophrenia, <https://www.kaggle.com/broach/button-tone-sz>
- [8] 장현웅 외, 캡슐네트워크의 위치추적을 위한 CNN 기반 위장관 랜덤마크 분류기 설계, 한국정보처리학회, 제주대학교 아라캠퍼스, 2019
- [9] 장소은 외, 빅 데이터 기반의 식품관 분석 및 관련 상품 추천 온라인 물 API, 한국정보처리학회, 제주대학교 아라캠퍼스, 2019
- [10] Business Watch, 네이버, '의료·병원' 클라우드에 꽃힌 이유 <http://news.bizwatch.co.kr/article/mobile/2018/05/31/0022>

ESRGAN과 Semantic Soft Segmentation을 이용한 객체 분할의 성능 개선

윤동식, 곽노윤
백석대학교 ICT학부

kevinds1106@naver.com, nykwak@bu.ac.kr

Performance Improvement of Object Segmentation Using ESRGAN and Semantic Soft Segmentation

DongSik Yoon, Noyoon Kwak
Division of ICT, Baekseok University

요 약

본 논문은 ESRGAN(Enhanced Super Resolution GAN)과 Semantic Soft Segmentation을 이용한 객체 분할의 성능 개선에 관한 것이다. 본 논문의 연구진이 이미 제안한 Mask R-CNN과 Semantic Soft Segmentation을 이용한 객체 분할 방법은 전반적으로 객체 분할 성능이 양호한 반면, 객체의 크기가 상대적으로 작으면 분할 성능이 저조해지는 문제점이 있었다. 본 논문은 이러한 문제점을 해결하기 위한 것으로, Mask R-CNN을 통해 검출된 객체의 크기가 일정 기준치 이하인 경우, ESRGAN을 통해 초해상화를 수행한 후, Semantic Soft Segmentation을 수행함으로써 소형 객체의 분할 성능을 개선함에 그 목적이 있다. 제안된 방법에 따르면, 기존의 방법에 비해 크기가 작은 객체의 분할 특성을 좀 더 효과적으로 개선할 수 있음을 확인할 수 있었다.

1. 서론

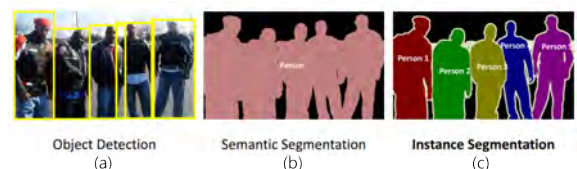
널리 알려진 Mask R-CNN[1]은 객체 검출(Object Detection)과 인스턴스 분할(Instance Segmentation) 두 측면에서 유용한 모델인데, 객체를 검출하는 성능은 우수한 편이지만 객체를 분할하는 성능은 기대에 미치지 못하는 경우가 많다. 이러한 점을 보완하기 위해 본 논문의 연구진은 Mask R-CNN과 Semantic Soft Segmentation[2]을 사용한 객체 분할 방법[3]을 기 제안한 바 있다. 하지만 이 방법에 따르면 Mask R-CNN을 통해 검출된 객체의 크기가 일정 이하인 경우에는 Semantic Soft Segmentation의 성능이 미진해 오히려 분할결과가 이전보다 나빠지는 문제점이 있다. 본 논문은 이러한 문제를 해결하기 위해 Mask R-CNN을 통해 검출한 객체의 크기가 일정 이하인 경우 ESRGAN(Enhanced Super Resolution GAN)[4]을 사용하여 초해상화를 수행한 후 Semantic Soft Segmentation을 수행함으로써 그 성능을 개선함에 목적이 있다.

2. 관련 연구

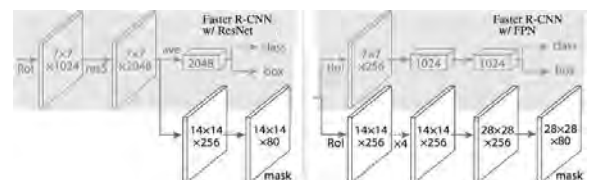
2.1 Mask R-CNN을 이용한 객체 검출 및 분할

본 논문에서 객체 검출(Object Detection) 및 Instance Segmentation을 위해 채택한 Mask R-CNN[1]은 Faster R-CNN[5]에서 가능한 경계박스 단위의 분할과 FCN(Fully Convolutional Network)[6]에서 가능한 Semantic Segmentation을 결합한 것으로, 경계박스 단위로 전경 객체를 별도로 구별해 분할하는 알고리즘이다. Faster R-CNN이 객체 검출만을 위한 모델이라면, Mask R-CNN은 이를 확장하여 검출된 경계박스 내 마스크를 학습시키는 모델이다. 이 모델은 객체를 분할하기 위해 물체를 분류하는 브랜치와 경계박스를 회귀

(regression)하는 브랜치에 객체 마스크를 예측하는 브랜치를 추가한 것이다. 즉 Mask R-CNN은 Faster R-CNN에 각 픽셀이 객체에 해당하는지 아닌지를 예측하는 추가적인 마스크 브랜치를 삽입해 경계박스 내 각각의 픽셀이 그 객체의 일부인지를 판별하는 이진 마스크를 구한다.



(그림 1) (a) Faster R-CNN에서의 객체 검출, (b) FCN에서의 Semantic Segmentation, (c) Mask R-CNN에서의 Instance Segmentation[5][6][1]



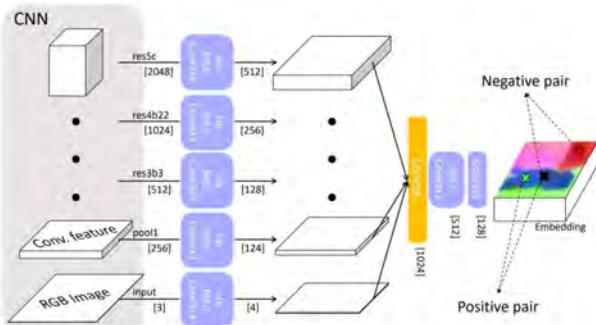
(그림 2) Faster R-CNN(ResNet/FPN)에 마스크 브랜치를 추가한 구조

통상, Mask R-CNN에서는 정확한 픽셀 위치가 필요하기 때문에 양선형 보간(bilinear interpolation)을 사용하는 RoIAlign을 추가적으로 채택함으로써 오정합 현상을 방지하고 각 특징맵과 원본 이미지의 해당 영역이 더 잘 정합되도록 한다.

2.2 Semantic Soft Segmentation

2.2.1 특징벡터 추출

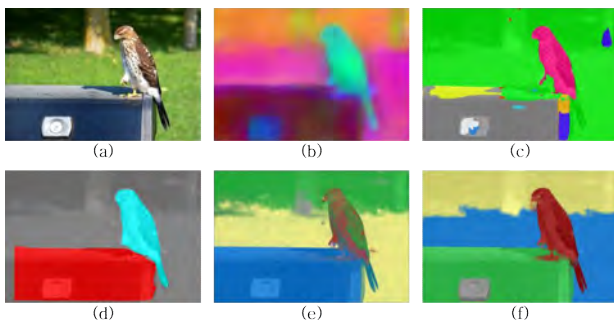
본 논문에서 의미론적 분할을 위해 사용한 Semantic Soft Segmentation[2]은 DeepLab ResNet-101 기반[7]의 네트워크를 사용하여 128차원의 벡터를 추출한다. 그림 3에서와 같이 ResNet-101의 'input', 'pool1', 'res3b3', 'res4b22', 'res5c'층을 추출해 나온 특징들을 3×3 합성곱을 취한 후 양선형 보간법을 사용하여 원본 이미지의 해상도로 업샘플링하고 이를 모두 결합하여 ReLU에 통과시킨다. 이때 중간 특징의 차원은 {3, 256, 512, 1024, 2048}인데 이를 {4, 124, 128, 256, 512}로 각각 압축하여 총 1024의 차원이 되게 한다. 그 후 두 번의 1×1 합성곱층을 통해 1024의 특징 차원을 512차원, 128차원으로 단계적으로 감소시킨다. 이 네트워크의 훈련에는 COCO Stuff dataset이 사용되었다.



(그림 3) Semantic Soft Segmentation의 특징 벡터 추출 네트워크의 구조

2.2.2 변형된 Spectral Matting을 이용한 의미론적 분할

그래프 이론 기반의 라플라시안 행렬(Laplacian matrix)을 사용하는 Spectral Matting[8]은 작은 패치들을 저수준 통계 특성(low-level statistics)만으로 다루기 때문에 객체를 판별하는 능력이 제한되는 단점이 있다. 이러한 단점을 보완하기 위해 Semantic Soft Segmentation은 라플라시안 행렬에 의미론적 특징을 혼합하고 장면 객체(scene objects)와 같은 고수준 개념(high-level concepts)을 포착해 이미지를 폭넓은 시점에서 판별하게 한다.



(그림 4) (a) 원본 이미지, (b) PCA기법을 사용해 128차원에서 추출한 특징벡터, (c) PSPNet을 이용한 분할 결과, (d) Mask R-CNN을 이용한 분할 결과, (e) Spectral Matting을 이용한 분할 결과, (f) Semantic Soft Segmentation을 이용한 분할 결과[9][11][8][2]

Semantic Soft Segmentation은 색상 기반의 원거리 상호작용을 하는 저수준의 유사도항을 비국부 색상 유사도(nonlocal color affinity)로 정의하였다. Semantic Soft Segmentation은 과분할된 이미지 기반의 가이드 샘플링(guided sampling)을 진행하는데, 이미지 크기의 20% 이내

에 해당하는 반지름을 가진 2,500개의 슈퍼픽셀[10]을 생성하고 각 슈퍼픽셀들 간의 유사도를 측정한다. 이 방법은 특징을 대표하기 충분한 각 슈퍼픽셀들을 하나의 샘플로 사용하며, 큰 반경을 사용하기 때문에 연결되지 않은 영역끼리의 연결도 가능하게 하는 장점이 있다. 추가적인 정보 없이 비국부 색상 유사도로 확장된 공간상에서 상호작용을 통한 이미지 분할을 진행할 시, 색상이 유사한 다른 객체들을 하나로 합치는 문제가 발생할 수 있다. Semantic Soft Segmentation은 의미론적으로 유사한 영역들이 하나의 덩어리로 분할되도록 세분화하기 위해 의미론적 유사도항을 추가하였다. 이는 같은 장면 객체들의 픽셀들은 서로 같이 분류되도록 도와주면서 서로 다른 객체끼리는 분리되도록 도와준다.

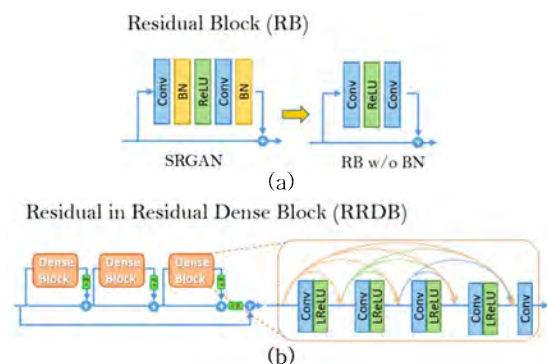
Semantic Soft Segmentation은 DeepLab ResNet-101 기반의 네트워크를 사용하여 나온 128차원의 벡터를 PCA기법을 통해 3차원으로 줄이고 기존의 Spectral Matting 연산 시 사용하는 라플라시안 행렬에 새로 만든 비국부 색상 유사도와 의미론적 유사도를 추가해 의미론적 분할을 진행하여 더 부드러운 영상 분할을 수행한다.

2.3 ESRGAN(Enhanced Super Resolution GAN)

기존의 SRGAN(Super Resolution GAN)은 한 장의 이미지만으로 초해상화를 수행하면서 현실적인 질감의 결과를 생성한다. 하지만 부분적으로 시각적 거부감이 초래되는 바, ESRGAN[4]은 세 가지 핵심 요소를 추가해 화질을 개선한다.

2.3.1 Residual-in-Residual Dense Block(RRDB)

본 논문에서 이미지 초해상화를 위해 사용된 ESRGAN은 기존의 SRGAN에서 화질을 향상시키기 위해 생성자의 구조에서 다음과 같은 두 가지의 보완 사항을 추가하였다. 그 하나는 모든 BN(Batch Normalization)층을 삭제한 것이고, 또 다른 하나는 그림 5(b)와 같이 제안된 Residual-in-Residual Dense Block(RRDB)을 사용하는 것이다.



(그림 5) (a) SRGAN의 Residual Block에서 BN층을 제거한 구조 (b) 제안된 Dense Block을 사용한 RRDB의 구조

BN층은 배치의 평균과 분산을 사용해서 특징들을 정규화하여 훈련하고 테스트 시에는 전체 데이터셋의 평균과 분산을 사용한다. 이 때문에 훈련과 테스트 데이터셋의 통계가 많이 다른 경우 BN층은 시각적 거부감을 생성하고 일반화하는 성능을 제한하는 경향이 있다. ESRGAN은 BN층을 제거함으로써 훈련을 안정화시키면서 일반화 성능을 높이고 계산 복잡도를 줄였다.

ESRGAN의 고차원 네트워크 구조는 SRGAN을 유지하면서 그림 5(b)와 같이 RRDB라는 새로운 기본 블록을 사용하였다. 더 많은 층과 연결이 있는 경우 성능이

더 잘 나온다는 Residual Networks[11]의 실험을 기반으로 제안된 RRDB는 SRGAN의 Residual Block보다 더 깊고 복잡한 구조를 가진다. 추가로 ESRGAN은 향상된 구조를 통해 매우 깊은 네트워크를 학습시킬 수 있는 두 가지 기술을 추가로 활용한다. Residual Scaling은 학습의 불안정을 방지하기 위해 연산된 블록을 주경로(main path)와 결합하기 전에 0에서 1사이의 상수를 곱해서 블록을 축소한다. 또 Residual 네트워크 구조가 시작 파라미터의 분산이 작은 경우에 학습이 더 잘되는 것을 이용해 작은 초기값을 사용한다.

2.3.2 상대 판별자(Relativistic Discriminator)

ESRGAN은 생성자의 구조를 향상시키는 것뿐만 아니라 Relativistic GAN[12]을 기반으로 판별자도 강화한다. 기존의 SRGAN의 표준 판별자는 입력 이미지 x 가 얼마나 진짜 같은지에 대한 가능성을 판별하는 것이었다면 ESRGAN의 판별자는 진짜 이미지 x_r 이 생성한 가짜 이미지 x_f 보다 얼마나 더 진짜 같은지를 예측하는 상대 평균 판별자(Relativistic average Discriminator)를 사용한다.

SRGAN의 표준 판별자는 $D(x) = \sigma(C(x))$ 의 식으로 나타낼 수 있다. 이때 σ 는 시그모이드 함수이고 $C(x)$ 는 아직 변환되지 않은 판별자의 출력을 의미한다. ESRGAN에서 사용한 상대 평균 판별자의 식은 $D_{Ra}(x_r, x_f) = \sigma(C(x_r) - \mathbb{E}_{x_f}[C(x_f)])$ 로 나타낼 수 있다. 여기서 $\mathbb{E}_{x_f}[C(x_f)]$ 는 미니 배치에 있는 모든 가짜 데이터의 평균을 의미한다. 이를 사용한 판별자의 손실 함수는 식 (1)과 같으며 생성자의 손실 함수는 식 (2)와 같이 판별자의 손실 함수와 대칭적인 형태를 보인다.

$$L_D^{Ra} = -\mathbb{E}_{x_r}[\log(D_{Ra}(x_r, x_f))] - \mathbb{E}_{x_f}[\log(1 - D_{Ra}(x_f, x_r))] \quad (1)$$

$$L_G^{Ra} = -\mathbb{E}_{x_r}[\log(1 - D_{Ra}(x_r, x_f))] - \mathbb{E}_{x_f}[\log(D_{Ra}(x_f, x_r))] \quad (2)$$

식 (1) 및 (2)에서 $x_f = G(x_i)$ 이며 x_i 는 입력 LR(Low Resolution) 이미지를 의미한다. 식 (2)에서와 같이 생성자의 손실 함수는 x_r 과 x_f 모두를 포함하기 때문에 SRGAN과 달리 생성된 이미지와 원본 이미지 모두 경쟁 학습에 영향을 미치는 것을 볼 수 있다.

2.3.3 시각 손실(Perceptual Loss)

ESRGAN은 좀 더 효과적인 시각 손실(perceptual loss)을 이용한다. 보통의 시각 손실은 사전 학습된 네트워크의 활성화 층을 통과한 특징을 최소화하는 것으로 정의한다. 이와 달리 ESRGAN에서는 활성화 층을 통과하기 전의 특징을 사용하는 것으로 두 가지 문제를 개선한다. 네트워크가 매우 깊은 경우 활성화되는 특징들이 매우 드물게 나타나기 때문에 좋지 못한 결과를 초래하는 문제와 활성화 층을 통과한 특징을 사용하는 경우 원본 이미지와 비교하여 재구성된 밝기가 일관되지 않은 문제이다.

결론적으로 ESRGAN의 생성자 손실 함수는 식(3)과 같이 정의할 수 있다.

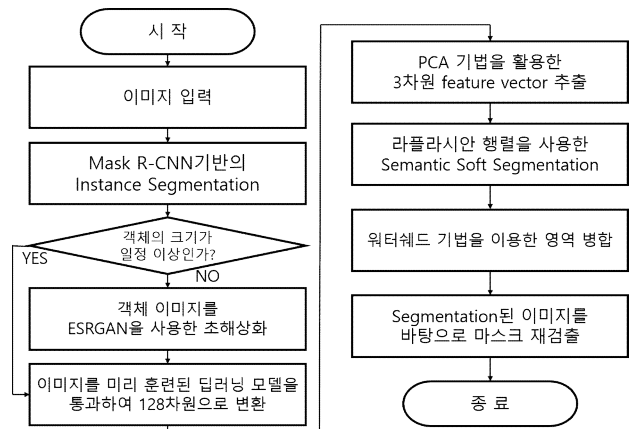
$$L_G = L_{percep} + \lambda L_G^{Ra} + \eta L_1 \quad (3)$$

식 (3)에서 $L_1 = \mathbb{E}_{x_i} \|G(x_i) - y\|_1$ 은 콘텐츠 손실로, 생성

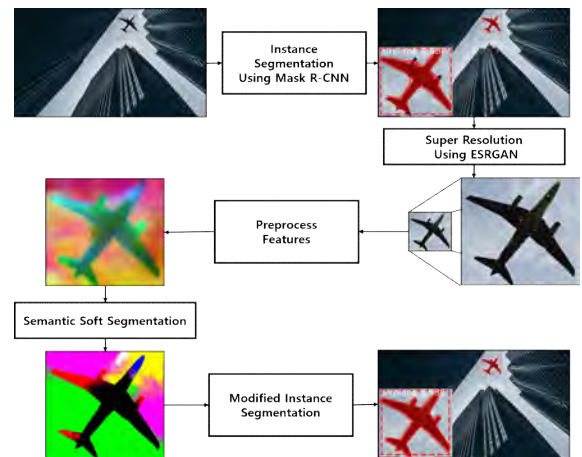
된 이미지 $G(x_i)$ 와 원본 이미지 y 의 차이를 구한 것이다. λ 와 η 는 다른 손실과의 균형을 맞추기 위한 계수이다.

3. 제안된 객체 분할 방법

본 논문은 Mask R-CNN으로 객체를 검출하고 Semantic Soft Segmentation을 통해 의미론적 분할을 수행한다. 이후 상기 검출 객체와 상기 분할 결과를 대응시켜 최종적으로 객체를 분할한다. 이때 Mask R-CNN의 검출 객체의 크기가 일정 기준치 이하라면 ESRGAN을 활용해 해상도를 높인 이미지를 생성하여 Semantic Soft Segmentation을 수행한다. 결과적으로 Mask R-CNN의 검출 객체의 크기가 작은 경우에 Semantic Soft Segmentation의 분할 성능을 개선하는 효과가 있다. 그림 6은 제안된 방법의 순서도를 나타낸 것이고, 그림 7은 제안된 객체 분할 블록도를 나타낸 것이다.



(그림 6) 제안된 방법의 순서도



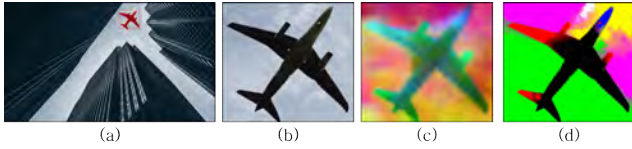
(그림 7) 제안된 방법의 블록도

3.1 객체 검출 및 초해상화

- 객체 검출 및 분할: Mask R-CNN 모델을 활용하여 입력 이미지에서 객체를 검출하고 분할한다. Mask R-CNN 모델은 그림 8(a)와 같이 각 객체의 경계박스 정보와 객체 분할된 마스크 정보, 객체 종류(class_ids), 정확도를 반환한다.
- 초해상화: Mask R-CNN을 활용하여 검출된 객체 중에서 크기가 일정 기준치 이하인 경우, ESRGAN을 사용해 그림 8(b)와 같이 소형 객체 이미지를 대상으로 4배 초해상화를 수행한다.

3.2 Semantic Soft Segmentation의 영상 분할

- 특징 벡터 추출: ResNet-101 기반의 사전 훈련된 네트워크를 사용하여 128차원의 벡터를 추출한다. 그 후 PCA 기법을 사용해 그림 8(c)와 같이 3차원의 특징 벡터를 추출한다.
- Semantic Soft Segmentation 수행: PCA 기법을 활용해 3차원으로 만든 특징 벡터와 원본 이미지를 사용해 그림 8(d)와 같이 Semantic Soft Segmentation을 수행한다.



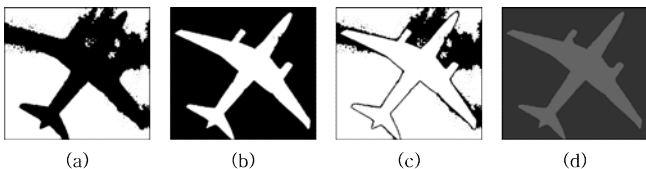
(그림 8) (a) 객체 검출을 완료한 이미지, (b) ESRGAN을 활용해 객체를 초해상화한 이미지, (c) PCA기법을 통해 특징 벡터를 추출한 이미지, (d) Semantic Soft Segmentation을 수행한 이미지

3.3 워터셰드 기법을 활용한 영역 분할

- 워터셰드 마커 설정: 워터셰드 기법을 통해 의미론적 분할 결과의 보정 및 영역 병합을 수행하기 위해 확실한 배경인 그림 9(a)와 확실한 전경인 그림 9(b)를 각각의 마커들로 설정한다.
- 워터셰드 분할 수행: 특징 벡터인 그림 8(c)와 마커로 설정한 그림 9(c)를 참조하여 그림 9(d)와 같은 워터셰드 분할을 수행한다.

3.4 객체 분할

- 객체 마커 탐색: 워터셰드 기법으로 분할된 여러 마커들 중 의미론적 분할 결과를 기반으로 검출된 객체에 해당하는 마커들을 찾는다.
- 객체 분할: 객체에 해당하는 마커들을 Mask R-CNN의 마스크와 교차하여 객체 분할을 완료한다.



(그림 9) 의미론적 분할 결과 확실한 전·배경에 마커를 설정한 이미지(c), 그림 8(c)와 그림 9(c)를 참조하여 워터셰드를 수행한 이미지 (d)

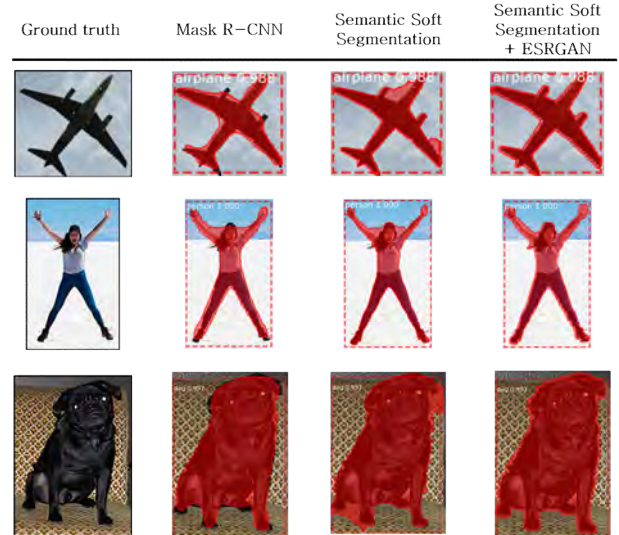
4. 시뮬레이션 결과 및 고찰

본 논문에서는 Jupyter Notebook과 NVIDIA GTX 1070Ti GPU 환경에서 사전훈련된 Mask R-CNN과 Semantic Soft Segmentation 및 ESRGAN 모델을 사용하여 컴퓨터 시뮬레이션을 수행하였다. 그림 10은 기존의 방법과 제안된 방법의 결과를 비교한 것으로 전경과 배경 구분이 뚜렷함에도 불구하고 객체 분할 결과가 만족스럽지 못하다. 반면에 제안된 방법은 상대적으로 우수한 객체 분할 성능을 제공함을 시작적으로 확인할 수 있었다.

5. 결론

제안된 방법은 Mask R-CNN과 Semantic Soft Segmentation을 이용한 객체 분할 시 검출된 객체의 크기가 작은 경우, ESRGAN을 이용한 초해상화를 통해 Semantic Soft Segmentation의 의미론적 분할 성능을 개선한 것이다. 제안된 방법은 검출된 객체의 크기가 작더라도 우수한 분할 성능을 제공함을 확인할 수 있었다.

이를 감안할 때 추가적인 성능 개선이 이뤄진다면 고품질의 영상 편집, 객체 인식 및 트래킹 영상 이해 등이 가능할 것으로 기대된다. 또 제안된 방법을 통해 기존의 COCO 데이터셋과 같이 객체 분류 모델을 학습시키기 위해 사람의 손으로 일일이 생성해주던 데이터셋을 수작업을 거치지 않고 자동으로 생성해 비용과 시간을 절감하고 좀 더 세밀한 데이터셋 기반의 학습으로 모델의 성능 향상을 기대할 수 있을 것이다.



(그림 10) 기존의 객체 분할 방법과 제안된 객체 분할 방법

참고문헌

- [1] K. He, G. Gkioxari, P. Dollar, and R. Girshick, "Mask R-CNN," *Proc. IEEE International Conference on Computer Vision*, pp. 2980-2988, 2017.
- [2] Y. Aksoy, T.-H. Oh, S. Paris, M. Pollefeys, and W. Matusik, "Semantic Soft Segmentation," *ACM Trans. Graph.*, 2018.
- [3] 윤동식, 박노운, "MaskR-CNN과 Semantic Soft Segmentation을 이용한 객체 분할", 2020년도 한국통신학회 동계종합학술발표회 논문집, pp. 872-873, 2020. 2.
- [4] X. Wang, K. Yu, S. Wu, J. Gu, Y. Liu, C. Dong, C.-C. Loy, Y. Qiao and X. Tang, "ESRGAN: Enhanced Super-Resolution Generative Adversarial Networks," *Proc. ECCV*, 2018.
- [5] S. Ren, K. He, R. Girshick, and J. Sun, "Faster R-CNN: Towards Real-time Object Detection with Region Proposal Networks," in *Neural Information Processing Systems*, 2015.
- [6] J. Long, E. Shelhamer, and T. Darrell, "Fully Convolutional Networks for Semantic Segmentation," *Proc. IEEE Conference on Computer Vision and Pattern Recognition*, 2015.
- [7] L.-C. Chen, G. Papandreou, I. Kokkinos, K. Murphy, and A. L. Yuille, "DeepLab: Semantic Image Segmentation with Deep Convolutional Nets, Atrous Convolution, and Fully Connected CRFs," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 40, 2017.
- [8] A. Levin, A. Rav-Acha, and D. Lischinski, "Spectral Matting," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 30, no. 10, pp. 1699-1712, Oct. 2008.
- [9] H. Zhao, J. Shi, X. Qi, X. Wang, and J. Jia, "Pyramid Scene Parsing Network," *Proc. CVPR*, 2017.
- [10] R. Achanta, A. Shaji, K. Smith, A. Lucchi, P. Fua, and S. Süsstrunk, "SLIC Superpixels Compared to State-of-the-Art Superpixel Methods," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 34, no. 11, pp. 2274-2281, Nov. 2012.
- [11] Lim B, Son S, Kim H, Nah S, Lee KM, "Enhanced deep residual networks for single image super-resolution," *Proc. CVPR*, 2017.
- [12] Jolicoeur-Martineau, "The relativistic discriminator: a key element missing from standard gan," *arXiv preprint arXiv:1807.00734*, 2018.

희소 클래스 분류 문제 해결을 위한 전처리 연구

류경준*, 신동규**, 신동일*

*세종대학교 컴퓨터공학과

**세종대학교 컴퓨터공학과

rkj6663@sju.ac.kr, shindk@sejong.ac.kr, dshin@sejong.ac.kr

A Study on Pre-processing for the Classification of Rare Classes

Kyungjoon Ryu*, Dongkyoo Shin**, Dongil Shin*

*Dept. of Computer Engineering, Sejong University

**Dept. of Computer Engineering, Sejong University

요 약

실생활의 사례를 바탕으로 생성된 여러 분야의 데이터셋을 기계학습(Machine Learning) 문제에 적용하고 있다. 정보보안 분야에서도 사이버 공간에서의 공격 트래픽 데이터를 기계학습으로 분석하는 많은 연구들이 진행 되어 왔다. 본 논문에서는 공격 데이터를 유형별로 정확히 분류할 때, 실생활 데이터에서 흔하게 발생하는 데이터 불균형 문제로 인한 분류 성능 저하에 대한 해결방안을 연구했다. 희소 클래스 관점에서 데이터를 재구성하고 기계학습에 악영향을 끼치는 특징들을 제거하고 DNN(Deep Neural Network) 모델을 사용해 분류 성능을 평가했다.

Machine-Learning, Deep-Learning, Rare Class, Feature Selection, Data Reconstruction

1. 서론

최근 실생활에서 나타나는 사례로 생성된 데이터를 기계학습(Machine Learning)으로 해결하기 위한 연구들이 등장하고 있다. 현재 IT산업에서는 4차 산업혁명 시대의 중요 자산으로써 데이터의 의미는 가중되고 있으며, 사회에 각 기관들과 세계의 여러 국가들은 정보보호, 정보수집과 정보 활용에 대한 연구를 진행하고 있다. 실생활 데이터를 이용한 기계학습에 있어서 가장 큰 문제점은 데이터 불균형(Data Imbalance)이다.

데이터 불균형 문제는 한 데이터 세트 내에서 유형별 샘플 수가 균형 잡혀있지 않는 것을 말한다. 이런 데이터 내에서 샘플의 수가 적은 유형을 가리켜 희소 클래스라고 한다. 이러한 문제가 생기는 이유는 실생활에서 정상적인 상황보다 비정상적인 상황이 훨씬 적게 발생하기 때문이다. 이를 해결하기 위해 인공적으로 데이터를 생성할 수도 있지만, 그 역시도 물리적인 한계에 부딪히는 경우가 많다[1, 2].

본 논문에서는 네트워크 정상 트래픽과 비정상 트래픽으로 구성된 데이터셋의 희소 클래스(Rare Class)에 해당하는 공격 트래픽 데이터의 분류 성능을 높이기 위한 연구에 초점을 두고, 실험을 진행했다.

2. 관련 연구

M.H.ABDULAHEEM[2]의 연구에서는 신경망 알고리즘을 통해 분류하기 전에 데이터셋에서 학습의 효율이나 성능을 저해하는 특징을 중요도(Importance)와 상관관계(Correlation)를 통해 분석하고 데이터의 분류 성능을 크게 개선했다. 학습에 있어서 가장 중요한 작업은 정규화(Normalization)이다. 정규화는 학습에 유의미한 결과를 가져다주는 효과도 있지만, 분류기 성능에도 영향을 미친다[3]. 정규화 방법에는 여러 방법이 있다. 대표적인 방법으로 ‘Min-Max Scaler’, ‘Standard Scaler’와 ‘Quantile Transform’이다. M.H.ABDULAHEEM[2]은 대표적인 3가지 정규화 방법에 대해서 실험을 진행했다. 3가지 정규화 방법 중 분류기 성능이 가장 우수하게 나타나는 방법은 ‘Quantile Transform’이라고 실험을 통해 증명했다.

3. 본론

3.1 데이터셋 재구성

CSE-CIC-IDS 2018 데이터셋의 유형별 구성은 가장 많은 정상 데이터(BENIGN)가 전체 데이터셋의 80%이고, 가장 적은 공격 데이터(Heartbleed)는 0.0004%로 데이터의 불균형이 문제를 가진 데이터

셋이다[4]. 이처럼 데이터의 불균형이 심각한 경우, 샘플이 적은 클래스의 데이터들이 샘플 수가 많은 클래스의 데이터에 역눌려서 데이터가 제대로 학습하지 못하는 경우가 발생한다. 본 논문에서는 1,500개 미만의 샘플을 가진 클래스의 데이터가 희소 클래스(Rare Class)라고 정의하고[2], 10,000개 미만의 샘플을 준희소 클래스(Semi-Rare Class)로 구분하고 해당 클래스에 대한 분류 성능을 개선하기 위해 <표 1>과 같이 각각의 희소 클래스에 초점을 맞추고 유사 공격데이터 합치는 방식으로 재구성하였다.

<표 1> 재구성한 데이터셋의 클래스와 샘플 개수

구분	클래스 이름	개수
원본 데이터 (Set A) 15 Class	BENIGN	2687419
	PortScan	317860
	DDoS	256054
	DoS Hulk	231073
	DoS GoldenEye	10293
	FTP-Patator	7938
	SSH-Patator	5897
	DoS slowloris	5796
	DoS Slowhttptest	5499
	Bot	3932
	Web Attack Brute Force	1507
	Web Attack XSS	652
	Infiltration	36
	Web Attack Sql Injection	21
	Heartbleed	11
병합 데이터 (Set B) 10 Class	BENIGN	2687419
	PortScan	317860
	DDoS	256054
	DoS [Hulk+GoldenEye+slowloris+Slowhttptest]	252661
	FTP-Patator	7938
	SSH-Patator	5897
삭제 데이터 (Set C) 12 Class	Bot	3932
	Web Attack [BruteForce+XSS+Sql Injection]	2180
	Infiltration	36
	Heartbleed	11
	BENIGN	2687419
병합&삭제 데이터 (Set D) 8 Class	PortScan	317860
	DDoS	256054
	DoS	252661
	FTP-Patator	7938
	SSH-Patator	5897
	Bot	3932
	Web Attack	2180
	BENIGN	2687419
	PortScan	317860
	DDoS	256054
	DoS	252661
	FTP-Patator	7938

정상 데이터(BENIGN)를 제외한 공격 데이터에 대해서 희소 클래스를 기준으로 그룹화와 제거를 통해 4개의 데이터셋을 구성하였다. 병합 데이터(Set B)는 ‘DoS’계열과 ‘Web Attack’계열로 그룹화하고 ‘FTP-Patator’와 ‘SSH-Patator’ 클래스는 희소 클래스로 정의하지 않아 그대로 두어서 총 10개의 클레

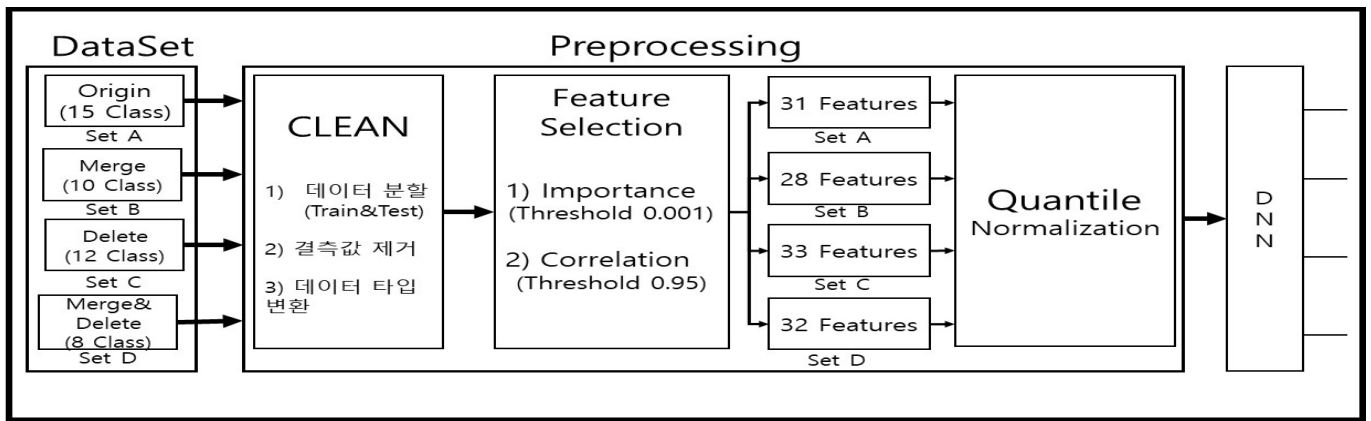
스로 구성되었다. 삭제 데이터(Set C)는 원본 샘플의 개수가 작아 오히려 희소 클래스로 분류되지 않는 데이터에 잡음으로 들어가 잘못된 정확도가 될 것이라고 판단한 3개의 희소 클래스(Infiltration, Heartbleed, Web Attack Sql Injection)를 제거해서 준희소 클래스(Semi-Rare Class) 총 12개의 클래스로 구성되었고, 병합&삭제 데이터(Set D)는 앞에서 말한 2가지 방법을 결합하여 먼저 ‘DoS’계열과 ‘Web Attack’ 계열을 그룹화하고 나머지 희소 클래스인 ‘Infiltration’과 ‘Heartbleed’를 제거해서 총 8개의 클래스로 구성했다.

3.2 데이터 전처리

본 논문에서 사용한 CSE-CIC-IDS 2018 데이터셋[5]은 ‘금요일 오전, 오후’, ‘월요일 오전, 오후’, ‘목요일’, ‘수요일’로 구성되어있고 동일한 특성과 각기 다른 공격 유형에 대한 정보를 가지고 있다. Q.Zhou[4]의 연구에서는 데이터셋을 기계학습을 위한 전처리 단계에서 데이터 분할(Train set&Test set), 결측값 제거, 데이터형 변환, 특징선택(Feature Selection), 데이터 정규화(Normalization)를 수행한다. 데이터 분할은 Train set과 Test set을 7:3의 비율로 나눈다. 학습에 영향을 끼친 데이터를 테스트에 사용하면 정확도 성능은 오르지만, 제대로된 평가가 되지 않는 과적합(Overfitting) 문제로 이어질 수 있다. 결측값 제거에서는 Null 값을 포함한 레코드는 삭제하고 inf 값은 최대값으로 채워주며, 데이터형은 모두 float type으로 변환한다. 그 후에 특징선택은 Importance와 Correlation을 0-1사이의 값으로 표현하고, Importance는 0.001이하의 값을 가지는 Feature와 상관관계가 0.95이상인 Feature를 제거한다. Importance는 앙상블 방법인 RandomForest 알고리즘으로 분석한 후, 0.001이하의 값을 갖는 특징은 학습 성능(정확도)을 저하시키고 효율(시간)을 감소시킨다고 판단하여 제거하였고, Correlation은 두 개의 특징의 상관관계가 0.95이상일 경우, 한 특징만 있어도 학습 성능에 있어서 무방하다고 판단하고 학습 효율 향상을 위해 하나의 특징은 제거하였다. 마지막으로 Quantile Normalization을 적용하면 학습 모델에 들어가기까지의 전처리 과정이 끝난다.

4. 실험

희소 클래스에 대한 분류 성능을 개선하기 위해 데이터셋을 재구성하고 (그림 1)의 구조를 제안하였



(그림 1) 제안된 구조

다. 원본 데이터(Set A)과 재구성 데이터셋(Set B, Set C, Set D)은 각각 전처리 과정을 수행한다. 먼저 데이터 CLEAN 과정에서 데이터 분할과 결측값 제거, 그리고 데이터 타입변환을 수행하고 Feature Selection과정을 수행한다. 먼저, 10개의 추정기를 가진 RandomForest알고리즘으로 Threshold Value가 0.001이하인 특징은 제거하고, 특징 간에 상관관계를 따졌을 때, Threshold Value가 0.95이상인 경우에 제거하는 방식으로 각각 Feature Selection을 수행하며, 그 결과 Set A는 31 Features, Set B는 28 Features, Set C는 33 Features, Set D는 32 Feature를 얻는다. 새로운 Feature 구성으로 재구성된 데이터는 마지막 전처리 과정인 Quantile Normalization을 수행한 후에, <표 2>와 같이 구성된 DNN(Deep Neural Network) Classifier를 통해 각각 분류된다.

<표 2> DNN Classifier의 Hyper Parameter

	Hyper Parameter
DNN	epoch 100
	batch size 100
	validation_split 0.2
	Hidden Layer [1000, 500, 100]

<표 3>은 Set A와 Set B의 성능을 Web Attack 계열과 DoS계열의 혼동행렬에서의 TP(True Positive) 증감율로 비교하였다. DoS 계열의 TP의 전체 합은 75,540개에서 75,522로 약 0.0002% 감소했지만, Web Attack계열은 410개에서 624개로 약 0.52% 증가했다. 재구성 데이터 Set B는 희소 클래스에 대해 좋은 성능을 보였다.

<표 3> 원본 데이터(Set A)와 병합 데이터(Set B)의 그룹화 클래스 TP 성능 비교

Set A(Class)	TP	Set B(Class)	TP
DoS GoldenEye	3067	DoS	75522
DoS Hulk	69261		
DoS Shttptest	1532		
DoS slowloris	1680		
Total	75540		
Web Attack Brute Force	409	Web Attack	624
Web Attack Sql	1		
Web Attack XSS	0		
Total	410		

<표 4>는 Set A와 Set C의 성능을 비교한 내용이다. Set C는 Set A에서 잡음이라고 판단할 수 있을만큼 적은 데이터 샘플을 가진 희소 클래스인 Heart bleed, Infiltration, Web Attack Sql Injection를 삭제해서 구성한 데이터셋으로 잡음을 제거했을 때, 준희소 클래스라고 정의한 클래스들의 성능을 TP 증감율로 비교하였다. Bot은 591개에서 836개로 약 0.41% 증가, DoS Slowhttptest는 1532개에서 1610개로 약 0.05% 증가, DoS slowloris는 1680개에서 1713개로 약 0.01% 증가, FTP-Patator는 1532개에서 2342개로 약 0.52% 증가, SSH-Patator는 1775개에서 1789개로 약 0.007%증가, Web Attack Brute Force는 409개에서 439개로 약 0.07%증가했고, Web Attack XSS는 0개에서 3개로 증가했다.

<표 4> 원본 데이터(Set A)와 삭제 데이터(Set C)의
준(Semi) 희소 클래스 TP 성능 비교

Set A(Class)	TP	Set C(Class)	TP
Bot	591	Bot	836
DoS Shttptest	1532	DoS Shttp	1601
DoS slowloris	1680	DoS slow	1713
FTP-Patator	1532	FTP-Patator	2342
SSH-Patator	1775	SSH-Patator	1789
Web Attack Brute Force	409	Web Attack Brute Force	439
Web Attack XSS	0	Web Attack XSS	3

<표 5>는 Set A와 Set D의 성능을 비교한 내용이다. Set D는 단순히 Set B와 Set C의 아이디어를 결합해서 DoS계열과 Web Attack계열로 그룹화하고, 잡음으로 판단되는 클래스는 삭제한 데이터셋이다. Bot은 591개에서 431개로 약 0.27%감소, DoS는 75540개에서 75268개로 약 0.003% 감소, FTP-Patator는 1532개에서 2355개로 약 0.53%로 증가, SSH-Patator는 0.02%감소, Web Attack만 410개에서 630개로 약 0.53% 증가했다.

<표 5> 원본 데이터(Set A)와 병합&삭제 데이터(Set D)의
희소 클래스 TP 성능 비교

Set A(Class)	TP	Set D(Class)	TP
Bot	591	Bot	431
DoS GoldenEye	3067	DoS	75268
DoS Hulk	69261		
DoS Shttptest	1532		
DoS slowloris	1680		
Total	75540		
FTP-Patator	1532	FTP-Patator	2355
SSH-Patator	1775	SSH-Patator	1732
Web Attack Brute Force	409	Web Attack	630
Web Attack Sql	1		
Web Attack XSS	0		

5. 결론

많은 정보를 포함하고 있는 네트워크 트래픽으로부터 불필요한 정보를 제거하고 유의미한 정보만을 가지고 학습하여 희소 클래스에 대한 분류 성능을 개선했다. 본 논문에서 제안했듯이, 특성 중요도와 특성 상관관계를 고려하여, 특징을 선택하고 희소 클래스에 대한 분류에 있어서 일반적인 기계학습 모델인 DNN Classifier로 원본 데이터셋과 분류 결과를 비교하였다.

향후, 우리가 살아가는 실생활 속 데이터의 불균형이 심한 경우에 본 논문의 연구를 인용하여 여러 도메인 환경에서 발생하는 데이터만으로도 더 좋은 성능을 끌어낼 수 있을 것이다.

Acknowledgement

본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다 (UD190016ED).

참고문헌

- [1] 서재현. (2018). 딥러닝 기반 불균형 침입탐지 데이터 분류에 관한 비교 연구. 한국지능시스템학회 논문지, 28(2), 152-159.
- [2] ABDULRAHEEM, MOHAMMED HAMID; IBRAHEEM, NAJLA BADIE. A DETAILED ANALYSIS OF NEW INTRUSION DETECTION DATASET. Journal of Theoretical and Applied Information Technology, 2019, 97.17.
- [3] SINGH, Bikesh Kumar; VERMA, Kesari; THOKE, A. S. Investigations on impact of feature normalization techniques on classifier's performance in breast tumor classification. International Journal of Computer Applications, 2015, 116.19.
- [4] ZHOU, Qianru; PEZAROS, Dimitrios. Evaluation of Machine Learning Classifiers for Zero-Day Intrusion Detection--An Analysis on CIC-AWS-2018 dataset. arXiv preprint arXiv:1905.03685, 2019.
- [5] SHARAFALDIN, Iman; LASHKARI, Arash Habibi; GHORBANI, Ali A. Toward generating a new intrusion detection dataset and intrusion traffic characterization. In: ICISSP. 2018. p. 108-116.

AI 음악 큐레이션과 AR 운동방법을 이용한 전기자극 장치 개발

김홍윤*, 진세한**, 강지영***

*주식회사 제우기술

**주식회사 캐스트유

***호서대학교 컴퓨터정보공학부

kimhongyoon@naver.com, jinsehan@naver.com, wldud68512@gmail.com

Development of electric muscle stimulation device using AI music curation and AR exercise method

Hong-youn Kim*, Se-han Jin**, Ji-young Kang***

*R&D Lab, Zeus tech co.,ltd

**CAST U INC.

***Dept. of Computer Engineering, Hoseo University

요 약

본 논문은 전기 자극 장치에 관한 것으로서, 운동상황에 맞게 인공지능 기능이 음악을 선별해 주고 음악의 BPM(beats per minute)에 맞게 전기 자극 장치에서의 PWM(pulse width modulation)신호가 동기화 되어 재활 기능과 더불어 헬스 케어와 관련된 추가적인 기능 및 효과를 제공할 수 있는 개선된 전기 자극 장치에 관한 것이다. 언제 어디서나 간편하게 셀프 운동케어와 할 수 있도록 AR기술을 이용한 카메라가 있는 디지털 디바이스를 활용하며, 해당 신체의 운동부위를 지정하게 되면 이에 맞는 운동방법을 AI기술을 이용하여 적용할 수 있다. 수행자가 잘못 운동을 하는 것을 올바르게 개선시키기 위하여 실시간 AI 음성기능과 텍스트 코칭을 통해서 올바르게 운동할 수 있게 제한하며, 이에 대한 과정과 결과를 시각적으로 보여주면, 결과에 대해서는 리포팅을 하여 사용자가 올바르게 운동을 하고 효과적으로 운동을 했는지에 대해서 정량적인 수치의 운동횟수와 운동량에 대해서 표현해준다.

1. 서론

최근 건강에 대한 관심이 날로 증대되고 있으며, 그에 따라 건강 증진을 위한 각종 기기들이 다양하게 개발되어 보급되고 있다.

일례로 전기 자극 장치의 일종인 저주파 치료기는 저주파 발생장치에서 발생한 저주파 전류를 이용하여 인체 근육 부위를 자극하는 것으로, 비만이나 통증 등의 치료에 효과적인 것으로 알려져 있다.

일반적으로 피부를 통해 인체에 미약한 저주파 전기를 통하게 할 경우 근육을 운동시켜 기초대사량을 높일 수 있고, 지방 세포를 직접 자극하여 세포 수를 감소시키는 동시에 크기를 줄일 수 있다.

또한, 혈액 순환을 촉진하고 체내 온도를 상승시켜 에너지 소모량을 늘릴 수 있고, 피부를 자극하여 피부와 대장을 직접 운동시키고 장 운동을 활발하게 해주는 등 숙변 제거와 변비 치료에 효과적이다.

그 밖에 저주파는 인체에 흐르는 전류와 유사하여

인체를 쉽게 투과할 수 있으므로 신경과 근육을 자극하기에 적합하고, 근육을 자극하여 활동량과 혈액의 움직임을 증가시켜 근육 마비, 통증, 피로 등의 증상을 완화시킨다.

2. EMS 장치의 운동법 및 구조

전기 자극 장치 중에 전기적 근육 자극(EMS:Electrical Muscle Stimulation)을 통해 근육을 운동시키는 EMS기기(Electrical Muscle Stimulator)가 시판되고 있고, 이를 이용한 EMS 운동법이 각광받고 있다.

EMS 운동법은 저주파 또는 중주파 전기를 이용하여 근육을 자극함으로써 운동 효과를 극대화하는 마이크로 트레이닝으로도 불리는 운동법으로, 체내에서 가해지는 전기 자극으로 근육이 수축하는 현상을 응용하여 운동 시 신체 곳곳에 약한 전기 자극을 가함으로써 운동 효과를 높이는 운동법이다.

이러한 EMS 운동법에서는 저주파가 발생하는 단

말을 사용자 신체에 직접 붙이거나, 단말이 설치된 의복 또는 밴드 등을 착용하여 단말을 신체에 간접적으로 밀착시킴으로써 단말을 통해 신체에 저주파 또는 중주파 전류를 인가한다.

일반적인 EMS장치는 PWM신호를 개발초기 임의로 영역을 지정하여 구성한다. 이에 따라서 사용자마다 각기 근육량이 다르기 때문에 전기쇼크나 놀라는 경우가 많이 발생한다.[1,2] 이러한 문제점을 고찰하여 초기 EMS부착시 근육량을 전기적인 저항값으로 인식하고 이에 대해서 안정적으로 사람마다 초기값을 정해주는 Dual stochastic 알고리즘을 적용하였다. 이러한 알고리즘을 통해 사람마다의 근육 및 피부의 저항값을 인지하여 안정된 범위의 PWM 신호가 출력되도록 장치에 적용하였다.[3,4]



(그림 1) 개발한 EMS모듈사진

전기자극장치는 전극 패드를 포함하며, 전극 패드는 근섬유 조직을 직접 자극할 수 있도록 저주파나 중주파 전기를 사용자 신체 부분에 잘 인가할 수 있는 구조로 제작하였다.

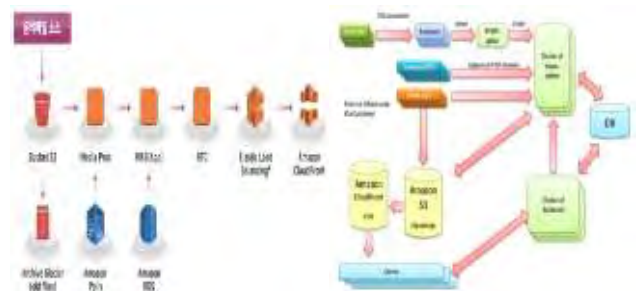
이를 위해 전극 패드는 신체 굴곡에도 불구하고 신체와의 밀착도를 높일 수 있는 재질로 제작되는데, 일반적인 형태로는 실리콘 고무나 합성수지 시트로 제작된 패드형 몸체에 탄소 소재 등의 도전성 물질을 코팅하는 방식으로 전극을 형성한 형태가 알려져 있으며, EMS 장비를 이용한 운동 방식 중 하나로 복수 개의 전극 패드를 부착하여 특수 제작한 일렉트릭 슈트를 착용하도록 개발하였다.

이와 같이 다양한 형태의 EMS 기기나 장비들이 개발되어 사용되고 있으며, 대부분의 EMS 기기나 장비들이 형태나 사용 방식은 달리고 있지만 주요 구성에 있어서는 저주파나 중주파 전류를 신체에 인가하여 근육에 전기 자극을 줄 수 있도록 하였으며, EMS 기기나 장비들이 전기적 근육 자극의 단순 기능만 하는 것이 아니라 음악의 BPM을 80이하, 80이상 120이하, 120이상으로 구분하여 음악의 비트에 맞게 전기자극장치의 PWM신호를 동기화 하여 음

악을 틀면 그 비트에 맞게 전기자극이 되도록 구성하였다. 이러한 하드웨어 및 연동 솔루션은 주식회사 제우기술에서 개발하였다. 추가로, 헬스 케어와 관련하여 새롭고 보다 다양한 기능 및 효과를 제공할 수 있는 전기 자극 장치를 요구되고 있으며 이에 부흥하는 제품을 개발할 수 있었다.

3. AI기반의 음악 스트리밍

EMS와 연동하기 위해서 AI클라우드, WEB RTC, 스트리밍 기술이 융합되어 모바일 앱(App) 과, WEB (POS,Window) 형태로 사용자에게 제공되는 음성 방송 서비스를 주식회사 캐스트유에서 개발하였다. 빅데이터 음악과 ,오픈 API 빅데이터가 크롤링 되며 아마존 AWS 라이브러리와 구글클라우드 환경에서 딥러닝 학습 과정을 거쳐 최종적으로 사용자의 성향에 맞춘 마이닝을 통해 최종 큐레이션 되어 사용자에게 제공되어진다. 온디맨드(사용자 맞춤형 개발 앱 방향) 서비스 환경으로 네이티브 웹 시스템보다 보다 빠르고 합리적인 가격으로 사용자에게 제공 되는 서비스 형태를 가지고 있다. 이러한 솔루션을 통해서 빅데이터와 AI 기반의 다양한 기법들을 활용하여 방송시스템의 자동화와 음악 데이터의 매핑을 통해 공간을 관리 , 지배, 통계정보를 활용하여 사용자의 가치를 상승시키는 프로그램이다.



(그림 2) AI 클라우드 / streaming 설계도

구체적으로는 음악 빅데이터 가공 솔루션 (Mapreduce 방식의 알고리즘 데이터 매핑방식)을 적용하고 구글 머신러닝 적용 (파이프라인 TENSORFLOW 적용) 하여 DATA FLOW 형태의 모델로 손쉽게 딥러닝 적용 가능하도록 프로그램을 설계하였다. 추가로 web-to-web 방식으로 일반적인 Pass 방식과 SK텔레콤의 AudioCodes WebRTC Sonus WebRTC Gateway Mobile SDK 을 활용하여 시스템에 적용하여 WRTC 기반의 다자통화 서비스 설계를 하였다. 데이터로부터 정보를 추출하기 위해 기법을 적용하기 위해 웹 마이닝을 적용하였으

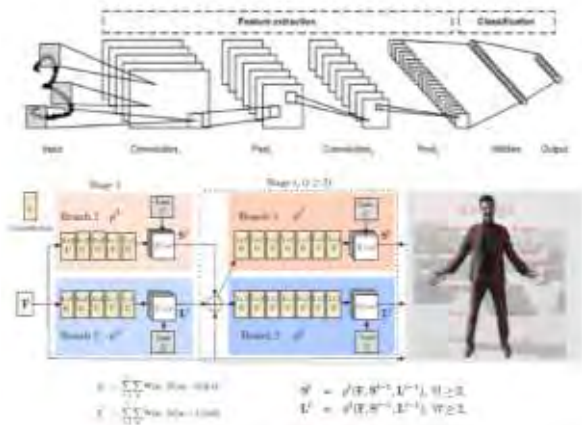
며 신경망(Neural Networks) 분석기법[5]과 동시발생 매트릭스(Co-Occurrence Matrix)을 선택하여 시스템에 적용하여 사용자 분석 마이닝 (웹 사용기반 알고리즘)[6]을 할 수 있다.



(그림 3) 개발한 모바일 앱 및 윈도우 플레이어

4. AR 기반의 운동방법 제안

CNN(Convolutional Neural Networks)기반의 특징점 추출 및 유사도 기반(Part affinity Fields)의 연속 Tracking 시스템을 통해 실시간으로 2D영상의 각 skeleton information추출 및 분석하는 기계학습 솔루션을 개발하였다. 이는 실시간 행동 분석과 머신러닝기반 영상분석 처리를 통해서 행동 분석의 경량화 및 고도화를 할 수 있도록 기계학습(Machine Learning) 기반의 실시간 동작분석 시스템 개발을 하였다.



(그림4) CNN기반의 데이터 추출 및 학습 모식도

각 트레이너로부터 입력되는 다양한 운동 처방 경우의 수를 학습하고 진단 결과와 처방 간의 상관관계를 도출하여 자동화된 맞춤 운동 프로그램을 큐레이팅을 통해 사용자 맞춤형 운동관리 프로그램 큐레이션 DB 및 알고리즘을 개발하였다.

텍스트와 음성가이드를 통해서 프로토콜 데이터 베이스 기반의 오류동작 분석 및 피드백 가이드 시스템을 통해서 올바른 운동을 할 수 있도록 제안하였

으며 엘리스헬스케어에서 개발하였다.



(그림5) 프로토콜 데이터베이스 기반 오류동작 분석

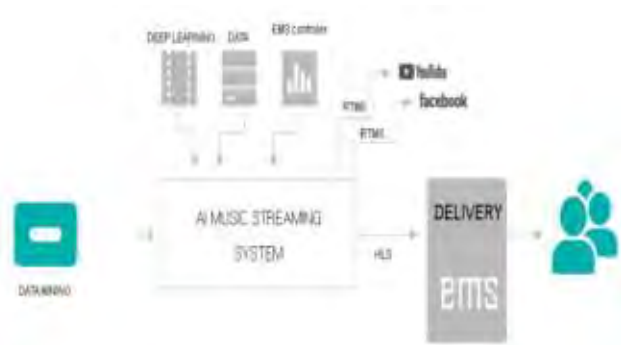
사용자 단말 기반 솔루션을 통해 클라이언트에서 축적된 데이터 크롤링 및 서비스 최신화 자동배포등을 위한 관리자-클라이언트-서버 간의 시스템 구축 (HIPPA 규정준수)하였다.

5. ICT 융복합 콘텐츠 솔루션 (AI, AR, IoT하드웨어 솔루션) 구축

가정에서나 장소에 구애받지 않고 카메라가 있는 모듈(핸드폰, 노트북, 웹캠이 장착된 컴퓨터)을 이용하여 사용이 용이하며, 개인 맞춤화 및 최적화된 다양한 운동 프로그램 추천 알고리즘, DB구축하였으며 올바른 운동을 할 수 있도록 음성 및 텍스트 기반으로 제안하며, 정상인 뿐만 아니라 장애인도 음성이나 화면을 통해서 쉽게 따라할 수 있도록 프로그램을 구성하였다. 이에 대해서는 녹음된 것이 아니라 실시간으로 자동 코칭 및 피드백 알고리즘을 통해 기존 저장된 DB를 이용하여 학습할 수 있다.

기존에 헬스나 재활프로그램에서 사용되는 음악은 저작권법에 문제가 되는바 이에 대해서 저작권을 확보하고 사용자의 성향에 맞춘 음악큐레이션 솔루션을 통해서 사용자가 휘트니스, 요가, 재활병원등의 어떤장소에 가더라도 이에 맞는 음악을 큐레이션하여 송출 될 수 있도록 AI기반의 음악큐레이션 솔루션을 개발하여 적용하였다. 또한 이렇게 송출되는 음악의 BPM에 맞도록 EMS 모듈에 블루투스로 정보를 전달하여 전기자극장치가 저주파상에서 PWM로 근육부위에 전달될 수있게 전기근육자극을 이용한 근육 재활 및 운동효과 극대화 할 수 있었다.

이러한 솔루션을 바탕으로 ICT 융복합 콘텐츠 솔루션 (AI, AR, IoT하드웨어 솔루션)을 구축할 수 있었다.



(그림 6) 데이터 마이닝과 EMS 연결 구성도

6. 결론

EMS를 이용한 훈련은 물리치료 분야에서 환자들의 고정된 근육의 비활동 근위축 감소 및 예방을 위해 등척성 운동을 중심으로 다양한 방법으로 활용하고 있음을 확인할 수 있으며, 정상인을 대상으로 EMS 처치와 등장성 운동에 대한 연구는 매우 미흡한 실정이다. 신경계의 적응을 크게 유발시킬 수 있는 EMS를 등장성 운동 시 적용하여 근력 및 균형 능력에 미치는 효과를 적용함으로써 다양한 방법으로 근육 운동을 돕는 EMS기기를 개발[3,7]하였으며 보통 음악을 들으면서 헬스장이나 물리치료를 받게 되며 이러한 음악적인 효과 또한 재활이나 운동에 심리적으로 많은 도움을 주고 있다.



(그림 7) ICT 융복합 콘텐츠 솔루션

치료를 받거나 헬스장에 가게 되면 원하는 음악이 아닌 전체적으로 듣는 음악으로 개인의 영향보다는 분위기 전체에 따른 음악을 듣고 운동을 하게 된다. 이러한 음악에 대해서 그날의 추천 운동, 날씨, 기분 등에 대해서 앱을 통해서 노래를 추천해주거나 원하는 음악을 듣게 해주어 환자나 운동하는 사람들이 효과적으로 운동할 수 있도록 음악을 AI 마이닝 솔루션을 적용하여 제공할 수 있다.

음악의 BPM(Beats per minute)신호를 앱으로 보내주고 펄스폭변조(Pulse width modulation ; PWM)를 통해서 신호를 EMS기기로 보내주어 근육 자극을 시키게 되면 환자나 운동하는 사람들도 이에 대한 귀로 듣는 심리적인 효과와 더불어 근육량의 증가를 위한 재활 및 운동에도 많은 도움이 될 것이다.

다. 추가적으로 빅데이터를 확보하고 데이터에 맞는 운동방법도 추가적으로 개발한다면 가정에서도 카메라가 있는 디바이스 만으로 운동 방법제안 및 재활을 위한 솔루션 적용이 가능할 것이다.

참고문헌

- [1] Hoon Heo, Yun Hyun Cho, Dae Jung Kim, "Stochastic control of Flexible beam in Random flutter. Journal of Sound and Vibration" Vol. 267, No. 2, pp335 ~ 354, 2003.
- [2] Sung-Man Park , Dong-Hee Lee, Jin-Hwan Kim, Jong-Bok Lee, Hoon Heo, "Experimental system identification in stochastic domain using cantilever beam", Control Automation and Systems, ICCAS '07, International Conference paper pp.1700 - 1703.
- [3] Yul-Kyu Son, Yong-Min You, Byung-Il Kwon, "Optimal Design to Increase Thrust Force in Electro Magnetic Linear Actuator for Fatigue and Durability Test Machine" IEEE Transactions on Magnetics - IEEE TRANS MAGN , vol. 47, no. 10, pp. 4294-4297, 2011.
- [4] 김홍윤, "복합시스템의 모델링 및 제어", 고려대학교, 2016.
- [5] K. Ogata, Modern Control Systems, Prentice Hall, 2010.
- [6] N. S. Nise, Control Systems Engineering, Wiley, 2010.
- [7] Sung-man Park, O-shin Kwon, Jin-sung Kim, Jong-bok Lee, Hoon Heo, "Identification of Non-Gaussian Stochastic System", Journal of Dynamic Systems, Measurement, and Control. Vol. 136, 041006(1~5), 2014.

합성곱 신경망을 이용한 동결절편의 암세포 전이 여부 자동진단에 관한 예비연구

정대일*, 강재구*, 전혜린*, 오세종*, 김성철**, 김영곤**, 공경엽**,
송인혜***, 박소연****, 안수민****, 이현나**, 양동현**, 유원상*****

*단국대학교 컴퓨터학과, **서울아산병원,

서울성모병원, *분당서울대학교병원, *****선문대학교 정보통신공학과
wjdeodlf0123@gmail.com, jkkang3250@gmail.com, wjsur1028@gmail.com, sejongoh@dankook.ac.kr,
sungchul7039@gmail.com, younggon2.kim@gmail.com, gygong@amc.seoul.kr, shade03@naver.com,
sypmd@snu.ac.kr, suminy317@gmail.com, hyunnalee@gmail.com, donghyun.yang@gmail.com,
wyoun@sunmoon.ac.kr

A Pilot Study on Automatic Diagnosis of Cancer Cells Metastasis in Frozen Section Using Convolutional Neural Network

Dae-Il Jung*, Jae-Ku Kang*, Hye-Lynn Jeon*, Se-Jong Oh*, Sungchul Kim**, Young-Gon Kim**,
Gyungyub Gong**, In Hye Song***, So Yeon Park****, Soomin Ahn****, Hyunna Lee**,
Dong Hyun Yang**, Wonsang You*****

*Dept. of Computer Science, Dankook University,

**Asan Medical Center,

***Seoul St. Mary's Hospital,

****Seoul National University Budang Hospital,

*****Dept. of Information and Communications Engineering, Sun Moon University

요 약

동결절편검사는 수술과 연계하여 암 전이 여부를 판단하기 위한 응급한 병리검사가 필요할 때 이용된다. 합성곱 신경망은 이미지 분류에 뛰어난 성능을 보이는 딥러닝 기법으로 본 논문에서는 이를 이용하여 유방암 전이 여부를 자동적으로 진단하는 방법을 제안한다. 실험과정은 전처리, 학습, 후처리의 과정으로 구성되어 있으며, 합성곱 신경망으로는 Resnet-18 모델을 사용하였다. 실험 결과 예측 정확도 및 종양의 최대 길이 정합 여부를 점수로 환산하여 약 0.514의 결과를 보였다.

1. 서론

동결절편검사는 유기용제와 가열 등의 처리 없이 세포내의 단백질, 지질, 가용성 항원물질 등의 유출이나 생존 능력 상실 없이 신속하게 진단이 가능하며 전자현미경 수준의 위치확인도 가능한 진단 방법이다. 특히, 수술과 연계하여 암 전이 여부를 판단하기 위해 응급한 병리검사가 필요할 때 이용된다.

수술 중 시행되는 동결절편 병리검사는 적절한 수술 범위를 결정하는데 매우 중요한 역할을 하게 되는데, 동결절편 병리검사 시간이 길어질 경우 수술 및 마취 시간이 길어져 환자에게 해를 끼칠 수 있으며, 판독이 잘못될 경우 암을 완전히 제거하지 못하거나, 불필요한 절제로 인한 합병증이 생길 우려가 있다.

특히, 유방암 환자에서 수술 중 감시림프절 동결절편검사는 주요 암 덩어리 수술 시 액와림프절 절제술 시행 유무를 결정하기 위하여 다양한 기관에서 시행되고 있다. 이는 전이가 있다고 판단된 환자들에게만 액와림프절 절제술을 시행하여 합병증을 방지하는 것으로 환자의 삶의 질을 높이기 위함이다[1].

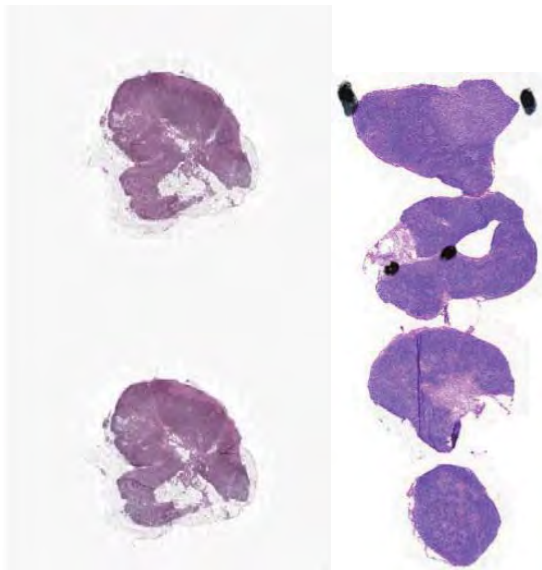
동결절편검사는 빠른 시간 내에 정확한 판독이 필수적인 반면, 육안으로 암 전이영역을 판단하기 어렵다. 이러한 문제를 해결하기 위하여, 본 연구에서는 2019년 12월 서울아산병원이 주최한 의료인공지능 개발 콘테스트(HeLP Challenge 2019)에서 제공된 데이터에 기반하여 딥러닝 알고리즘 가운데 하나인 합성곱 신경망을 이용하여 동결절편검사 시 유방암 전이 여부를 자동적으로 진단하는 방법에 관한 예비 연구를 수행하였다.

2. 관련연구

합성곱 신경망(Convolutional Neural Network, 이하 CNN)은 모델이 직접 이미지, 비디오, 텍스트 또는 사운드를 분류하는 알고리즘이다. CNN은 이미지에서 객체, 얼굴, 장면을 인식하기 위해 패턴을 찾는 데 특히 많이 사용된다. CNN은 데이터에서 직접 학습하며, 패턴을 사용하여 이미지를 분류하고 특징을 수동으로 추출할 필요가 없는 것이 특징이다.

H&E(Hematoxylin and Eosin) 염색조직 이미지 이용한 조직표본을 대상으로 유방암 전이 여부를 진단하는 과정에서 CNN을 이용한 연구 결과가 있다[2]-[4]. 해당 연구에서는 카파 계수(Cohen's Kappa)로 점수를 기록하였는데, 최고 0.8993의 높은 점수를 기록하였다. 해당 연구에서는 CNN을 이용하여 조직표본을 분석하는 것으로 좋은 결과를 보일 수 있음을 보였다.

그림 1의 왼쪽은 H&E 염색조직의 이미지이며 오른쪽은 동결절편의 이미지이다. 본 연구에서는 두 조직병리의 유사성을 이용함과 동시에 알고리즘의 발전을 통해 동결절편의 암세포 전이 여부를 자동으로 진단하는 방법을 모색하고자 하였다.



(그림 1) H&E 염색조직과 동결절편 이미지

3. 실험대상

동결절편 데이터는 서울아산병원 환자 297명, 분당 서울대학교 병원 환자 46명로부터 취득되었다. 종양 슬라이드 141개와, 정상 슬라이드 95개로 학습 데이터를 구성하였으며, 테스트는 62개의 종양 슬라이드와 45개의 정상 슬라이드로 진행하였다. 총 종양 슬라이드의 수는 203개이며, 정상 슬라이드의 수는 140개였다. 학습, 검증 및 테스트를 위해 각각 188, 48, 107개의 샘플이 사용되었다.

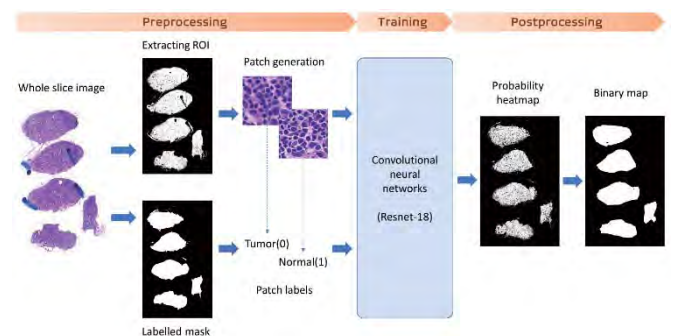
실험에 사용한 동결절편 이미지의 특성은 표 1에 요약되어 있다. 마스크 이미지의 경우 원본 이미지의 1/16 크기로 축소된 이미지에서 종양 부위가 임상 의에 의하여 정의되어 이진화 된 파일의 형태로 제공되었다.

<표 1> Dataset의 이미지 특성

Format	“.mrxs”
Resolution	93,952 x 132,352 pixels
Scanner	Panoramic 250 Flash, 3DHISTECH (Hungary)
MPP (micros per pixel)	0.221
Apparent magnification	20X
Image bit depth	8 bits
Color channel	RGBA

4. 실험방법

실험 진행방법은 그림 2으로 요약하여 설명한다. 크게 전처리(Preprocessing), 학습(Training), 후처리(Postprocessing), 총 세 단계로 구분할 수 있다.



(그림 2) 실험 진행방법 요약

먼저 이미지 전처리 단계에서는 세포와 배경을 구분하기 위하여 관심 구역(ROI)을 이진화하였다. 이들 가운데 세포 영역으로부터 1000개의 픽셀을 샘플링한 후, 각 픽셀을 중심으로 하는 256 x 256 크기의 패치(patch) 이미지를 추출하였다. 이후 종양 여부의 실측 정보(ground truth)를 담고 있는 마스크 이미지와 대조하여 각 패치의 종양 여부를 라벨링하였다.

학습 단계에서는 합성곱 신경망을 이용하여 학습을 진행하였다. 데이터 학습 모델로서 18개의 레이어로 구성된 resnet-18을 적용하였다. 랜덤하게 초기화된 가중치로부터 시작하여, 확률적 경사 하강법(SGD)에 따라 0.0001의 학습율로 가중치를 최적화하였다. 활성화 함수로서 ReLU, 손실 함수로서 로지스틱 이진 교차 엔트로피(Binary cross entropy with logits)가 사용되었다. 12의 Batch size와 함께, 30번의 epoch가 적용되었다. 학습은 카카오 클라우드의 고성능 GPU 컴퓨팅 시스템에서 수행되었다.

후처리 단계에서는 모든 세포에 대하여 추론을 진행하여 확률 지도(Probability heatmap)를 생성하였

다. 임계처리(thresholding), 홀 채움(hole filling), 경계선 검출 및 스무딩(contour extraction and smoothing) 기법 등을 적용하여 확률지도 이미지로부터 가장 큰 암 전이 영역을 추출하였다. 이로부터 해당 이미지의 종양 여부와 최대 암 전이 영역의 최장 길이를 계산하였다.

종양 예측의 정확도는 다음 두 가지 방법으로 측정하였다. 첫 번째는 종양 여부(Metastasis)를 ROC 커브의 AUC(Area Under the Curve)를 사용하여 평가하였다. 두 번째는 종양의 최장 길이(Major axis)를 정답의 오차범위($\pm 5\%$) 내 정합 여부에 따른 정확도로 평가하였다. 각각을 50%씩 반영하여, 정확도 점수는 다음 수식과 같이 정의되었다.

$$\text{Score} = 0.5 \times \text{AUC of Metastasis} + 0.5 \times \text{Acc of Major axis}$$

5. 실험결과

여러 차례의 실험 결과 가장 높은 정확도 점수는 0.514였다. 종양 여부의 정확도는 확률지도로부터 최대 암 전이 영역을 추출하는 후처리 과정의 세부 설정에 따라 크게 달라지는 양상을 보였다. 특히, 학습 데이터 가운데 가장 작은 종양의 최장 길이는 30.6이었는데, 후처리 과정에서 종양의 최장 길이의 임계점을 낮게 설정할 경우 종양 판별의 정확도가 현저히 저하되는 결과를 보였다.

6. 결론

본 논문에서는 동결절편검사에서 암세포 전이 여부를 자동으로 진단하기 위한 딥러닝 알고리즘으로서 합성곱 신경망인 resnet-18의 성능을 평가하였다.

콘테스트 참가의 형식으로 제한된 시간에 실험이 이루어져 만족할 만한 수준의 결과를 얻지는 못하였지만, 사전학습 모델의 적용, 전이학습(transfer learning), 하이퍼파라미터 최적화, 추가적 데이터 변조(data augmentation) 기법의 적용 등을 포함한 후속 연구를 통하여 암 전이 예측의 정확도를 향상시킬 수 있을 것으로 기대된다.

이번 실험의 결과는 인공지능 기술을 사용한 유방암 자동진단 기술의 잠재적 효용성과 발전 가능성을 보여준다.

Acknowledgement

본 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (2018-0-00242. 빅데이터 기반 인공지능 안과 진단기술 및 스마트 진료 플랫폼 개발)

참고문헌

- [1] Langer I, Guller U, Berclaz G, Koechli OR, Schaer G, Fehr MK, et al. Morbidity of sentinel lymph node biopsy (SLN) alone versus SLN and completion axillary lymph node dissection after breast cancer surgery: a prospective Swiss multicenter study on 659 patients. *Ann Surg* 2007;245:452-61.
- [2] Bándi, P., Geessink, O., Manson, Q., Dijk, M., Balkenhol, M., Hermesen, M., Bejnordi, B., Lee, B., Paeng, K., Zhong, A., Li, Q., Zanjani, F., Zinger, S., Fukuta, K., Komura, D., Ovtcharov, V., Cheng, S., Zeng, S., Thagaard, J., Dahl, A., Lin, H., Chen, H., Jacobsson, L., Hedlund, M., Çetin, M., Halıcı, E., Jackson, H., Chen, R., Both, F., Franke, J., Küsters-Vandeveld, H., Vreuls, W., Bult, P., Ginneken, B., Laak, J., Litjens, G. (2019). From Detection of Individual Metastases to Classification of Lymph Node Status at the Patient Level: The CAMELYON17 Challenge *IEEE Transactions on Medical Imaging* 38(2), 550-560.
- [3] Litjens, G., Bándi, P., Bejnordi, B., Geessink, O., Balkenhol, M., Bult, P., Halilovic, A., Hermesen, M., Loo, R., Vogels, R., Manson, Q., Stathonikos, N., Baidoshvili, A., Diest, P., Wauters, C., Dijk, M., Laak, J. (2018). 1399 H&E-stained sentinel lymph node sections of breast cancer patients: the CAMELYON dataset. *GigaScience* 7(6), giy065.
- [4] Bejnordi, B., Veta, M., Diest, P., Ginneken, B., Karssemeijer, N., Litjens, G., Laak, J., Consortium, a., Hermesen, M., Manson, Q., Balkenhol, M., Geessink, O., Stathonikos, N., Dijk, M., Bult, P., Beca, F., Beck, A., Wang, D., Khosla, A., Gargeya, R., Irshad, H., Zhong, A., Dou, Q., Li, Q., Chen, H., Lin, H., Heng, P., Haß, C., Bruni, E., Wong, Q., Halici, U., Öner, M., Cetin-Atalay, R., Berseth, M., Khvatkov, V., Vylegzhanin, A., Kraus, O., Shaban, M., Rajpoot, N., Awan, R., Sirinukunwattana, K., Qaiser, T., Tsang, Y., Tellez, D., Annuscheit, J., Hufnagl, P., Valkonen, M., Kartasalo, K., Latonen, L., Ruusuuvuori, P., Liimatainen, K., Albarqouni, S., Mungal, B., George, A., Demirci, S., Navab, N., Watanabe, S., Seno, S., Takenaka, Y., Matsuda, H., Phoulady, H., Kovalev, V., Kalinovsky, A., Liauchuk, V., Bueno, G., Fernandez-Carrobles, M., Serrano, I., Deniz, O., Racocceanu, D., Venâncio, R. (2017). Diagnostic Assessment of Deep Learning Algorithms for Detection of Lymph Node Metastases in Women With Breast Cancer *JAMA* 318(22), 2199.

임베디드 시스템을 위한 멀티태스킹 딥러닝 학습 기반 경량화 성별/연령별 추정

Huy-Tran Quoc Bao*, 정선태**

*Dept. of Information and Telecommunication, Graduate School, Soongsil University

**Dept. of Smart System Software, Soongsil University

*Huy.tsusak@gmail.com, **cst@ssu.ac.kr

A light-weight Gender/Age Estimation model based on Multi-taking Deep Learning for an Embedded System

Huy-Tran Quoc Bao*, Chung Sun-Tae**

*Dept. of Information and Telecommunication, Soongsil University

**Dept. of Smart System Software, Soongsil University

ABSTRACT

Age estimation and gender classification for human is a classic problem in computer vision. Almost research focus just only one task and the models are too heavy to run on low-cost system. In our research, we aim to apply multi-tasking learning to perform both task on a lightweight model which can achieve good precision on embedded system in the real time.

1. Introduction

The studying of age estimation and gender classification issue has many useful applications in products recommendation or human-computer interaction. Estimating physical ages for facial images are such a challenge not only for computer but also for humans because more often than not, physical ages can be very different from apparent ages. Gender classification seems to be a lighter task compared to age estimation because the classes to be classified are just two (male or female) while estimation of the age can range from 0 up to 100.

Multi-task learning [1] is a technology to learn several tasks at the same time. In deep neural network, Multi-task learning model can do several predictions simultaneously from the input data. Multi-task learning was inspired from human's learning process. For example, a person who studied playing piano can also use that knowledge about music notes and chords to for studying how to play the guitar. Thus, when a multi-task neural networks learn to perform multi tasks, tasks should have some relations among them. Since the feature extraction layer of multi-task networks can learn much more information, they could perform better than single task ones.

In a simultaneous age estimation and gender classification, features extracted from facial image can support each other to perform the task better. In research of B.Yoo[2], they create a

CNN which can apply gender information to utilize age prediction. They also show that the gender information significantly improves robust age estimation accuracy.

Inspired by that result and Multi-task learning. we create a light-weight model which do both tasks of age estimation and gender classification. Through experiments, our model can run in real-time on an embedded system such as Nvidia Jetson Nano board[3] with high accuracy compared to. previous models for gender/age estimation

2. Related work

Many approaches are proposed to solve age estimation problem. The age estimation task is more complicated than gender classification because the number of age value is much more than gender.

There are proposed many models showing great results on age estimation. DEX[4], MV[5], ARN[6] do the task by using VGG-16[7] architecture and applying multi-class classification. DEX also ensembles the outputs of many network to produce a robust result. AgeNet[8] approaches aging labeling as a regression problem using deep neural net based on GoogleNet[9]. For making it run on embedded systems or low-cost devices, many lightweight neural network architectures have been designed so as to reduce the model size such as

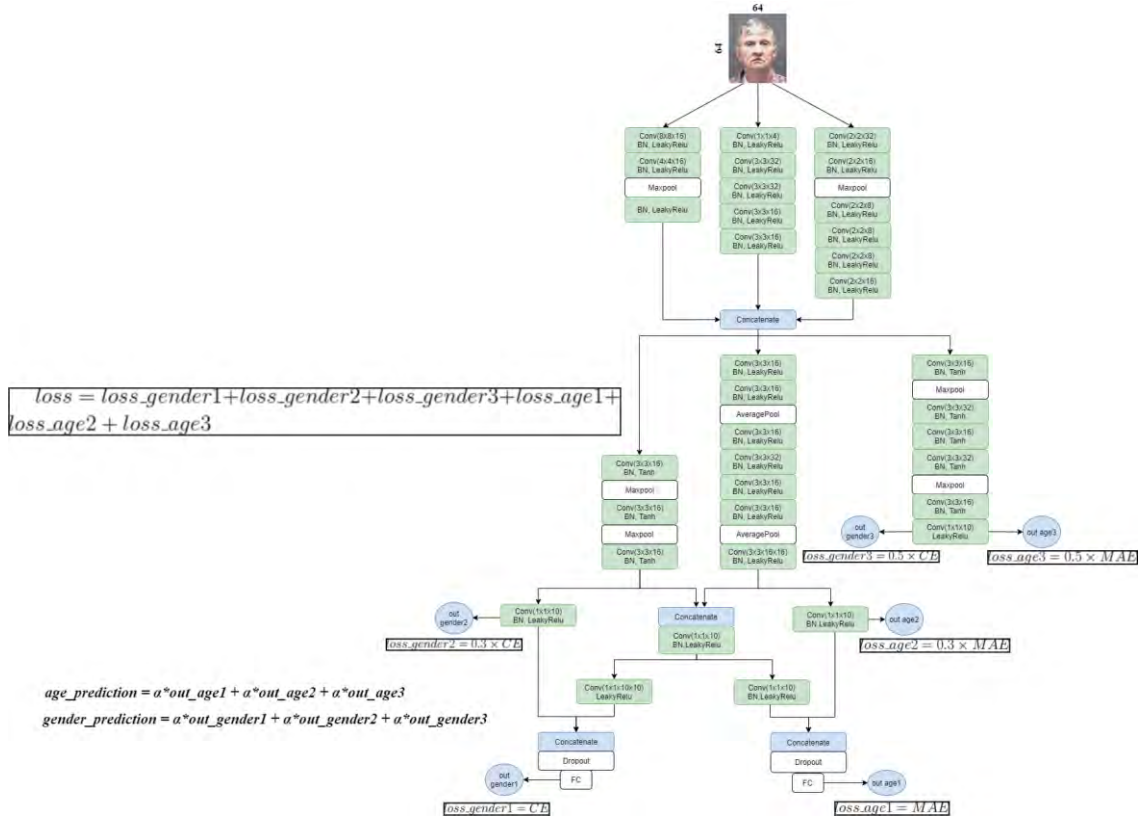


Figure 1: Proposed Network architecture

MobileNet[10], DenseNet[11]. SSR-Net[12] proposed by Tsun-Yi Yang using Soft-Stagewise regression network is a very compact model but also achieves competitive results.

[2] proposed a model which predicts both age and gender label using conditional Multi-task learning. The model performs age estimation job with combined gender information so as to improve accuracy. The research shows that gender feature really useful for age estimation task.

We propose a light-weight CNN neural network with multi-task learning to predict age and gender simultaneously from facial image.

3. Proposed CNN network with multi-tasking

The overall proposed network architecture is showed in Figure 1. At the beginning of the network, we use 3 branches of convolution layers followed by Batch Normalization and Leaky-Relu activation function to extract some general features. Each branch describes information of images differently to get useful information for both age and gender estimation.

After getting some general features, we instruct our network to extract gender and age feature separately. To do that, we construct the network with two branches added; the first branch aims to detect gender features and the second branch aims to detect age features. Since age estimation is harder task, the second branch contain more convolution layers. In order to force the second branch to learns about ages features, we add a

virtual output with a loss function at the end of this branch. The loss function here is aimed to instruct this branch to learn about age features. We only make the age prediction at this output. Similarly, for the gender task is easier, we also add a virtual output at the end of this branch to force this branch to learn useful features for gender classification. At the top of our network, we combine both age and gender features with a few simpler convolution layers, dropout layers and fully connected layers to output proper age and gender. Beside the age and gender branch, we also design another branch to predict both age and gender. This branch uses low level features to make prediction which use only 6 convolution layers followed by fully connected layers. These low-level outputs are used to ensemble with virtual outputs and the final outputs to make prediction. The input images are used with small size (64x64) to reduce the number of computation.

Ensemble is a well-known and efficient technique to improve accuracy by aggregating prediction of many machine learning models. Inspired by this idea, we design our network to have 3 pairs outputs of gender and age. After getting 3 outputs we ensemble them to get the final prediction. By doing this way, we can utilize the advantage of ensemble technique without sacrificing processing speed too much and make our model run successfully on our embedded board – Jetson Nano[3].

4. Training process

4.1 Dataset

MORPH-II[13] is a large dataset for real age estimation, which contains 55,134 color images of 13,617 subjects with age and gender information. The ages in MORPH-II ranges from 16 to 77 years old.

FGNET[14] data set contain 1002 image of 82 people; each image is labeled with physical age. The ages range from 0 to 69. This is a small dataset; the method usually adopted to evaluate is ‘leave one-person-out (LOPO)’[15].

We aim to detect age and gender for Asian people, however the face dataset which consist of both age and gender information for Asian people is limited. To the best of our knowledge, MegaAge-Asian dataset [16] is the largest face dataset for Asian people which includes about 44k face images. However, this dataset only provides age information. Therefore, we need to annotate gender information for this dataset. To do that, we train 4 well-known image recognition models on another Asian dataset - AAF[17] dataset and annotate mega-Asian dataset semi-automatically using the trained models. Recognition. If the 4 networks produce the same results, we keep that result as ground-truth, if not we manually annotate them. The four networks we use for this purpose are Inceptionv3[18], Xception[19], Resnet50[20] and Densenet201[21].

4.2 Loss function

We define 6 losses for 6 outputs. For gender recognition, we use binary cross entropy loss function which is defined as in (1). For age estimation, we use mean absolute error which is defined as formula (2). We use a small weight loss for 2 virtual outputs, slightly larger weights for low-level output since our final output is more important.

$$H_p(q) = -\frac{1}{N} \sum_{i=1}^N y_i \cdot \log(p(y_i)) + (1 - y_i) \cdot \log(1 - p(y_i)) \quad (1)$$

where y is the label (1 for man and 0 for woman) and $p(y_i)$ is the predicted probability of i class for all N images.

$$MAE = \frac{1}{N} \sum_{i=1}^N |y_i - \hat{y}_i| \quad (2)$$

Where y_i is the ground truth age and \hat{y}_i the predicted age, N is the total images used for calculating loss.

The final loss is the weighted loss of 4 losses as in formula (3).

$$\begin{aligned} total \ loss &= loss_{Gender1} + loss_{Age1} \\ &+ (loss_{Gender2} + loss_{Age2}) \times 0.3 \\ &+ (loss_{Gender3} + loss_{Age3}) \times 0.5 \end{aligned} \quad (3)$$

5. Experiment

We evaluate our model on Morph-II, MegaAge-Asian, and FGNET dataset and compare the evaluations with results of some state-of-art age-gender recognition methods.

Table1. result on Morph II dataset Age+Gender task

Network	Params	MAE	Acc (Gender)	Protocol
CMT	5M	2.91	99.2	5-fold
Compact CNN	56.9M	3.23	98.8	2-fold
Ours	99.2k	2.88	99.34	5-fold

Protocol: k-fold means splitting the dataset equally into k parts, and chosen $(k-1)$ parts are used for training and the remaining 1 part is used for evaluating. Then, take average of evaluation of all choices.

From Table 1, CMT model has over 5-million parameters which is 50 times more than ours. Furthermore, they use higher resolution images (128x128) for their application. Even though our model has less parameters and uses smaller input images, it produces better result (2.88/99.34) than CMT (2.91/99.2) respectively for age estimation and gender classification. Ours method also outperforms the performance of Compact CNN.

Table 2. Results on FG-NET dataset

Network	Params	MAE	Protocol
CMT	5M	3.43	LOPO
Ours	99.2K	3.41	LOPO

Our model also performs better than CMT among FGNET dataset with the same evaluation method – leave-one-person-out (LOPO).

In addition to comparison with Multi-task model, we also compare with some models which focus in just only single task – age estimation.

Table3: compare with single task network on Morph-II:

Network	Parameter	MAE
Ranking CNN	500M	2.96
DEX	138M	3.25
ARN	138M	3.00
MV	138M	2.41
Dense-Net	242K	5.05
MobileNet-V1	226.3K	6.50
SSR	40.9K	3.16
Ours	99.2K	2.88

Table 4: compare with single task network on FGNET:

Network	MAE
DEX	4.63
MV	4.10
Ours	3.41

Compared with the MV network, our network predicts with a lower accuracy in Morph-II dataset. However, the result in the Table 4 shows that we achieve better result in the FGNET dataset. Ours network is also much more lightweight than the MV network.

Cumulative accuracy (CA) measurement is calculated when evaluate on MegaAge-Asian dataset

$$CA(n) = \frac{K_n}{K} \quad (4)$$

K is total number of test images, K_n is number of test images whose absolute error is less than n .

Table 5. Results on MegaAge-Asian dataset

Network	Parameters	CA(3)	CA(5)
MobileNet-V1	226.3K	0.440	0.606
DenseNet	242K	0.517	0.694
SSR	40.9K	0.549	0.741
Ours	99.2K	0.585	0.788

Even though our network has a larger volume of parameters, it is still a light-weight model and has more functionality and produce much better result compared to SSR net.

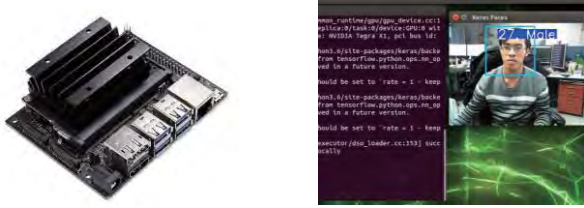


Figure 2: Jetson Nano board and executing age/gender estimation

6. Conclusion

In this paper, we proposed a network model which can perform age estimation and gender classification at the same time and achieve good precision. In addition, this model is light-weight enough to be deployed on embedded system-Jetson Nano. In the future work, we are going to continue to apply Multi-tasking learning for learning more tasks and improve the results.

References

[1] Ruder, Sebastian. "An overview of multi-task learning in deep neural networks.", arXiv preprint arXiv:1706.05098 (2017).
 [2] Yoo, ByungIn, et al. "Deep facial age estimation using conditional Multi-task learning with weak label expansion.", IEEE Signal Processing Letters 25.6 (2018): 808-812.

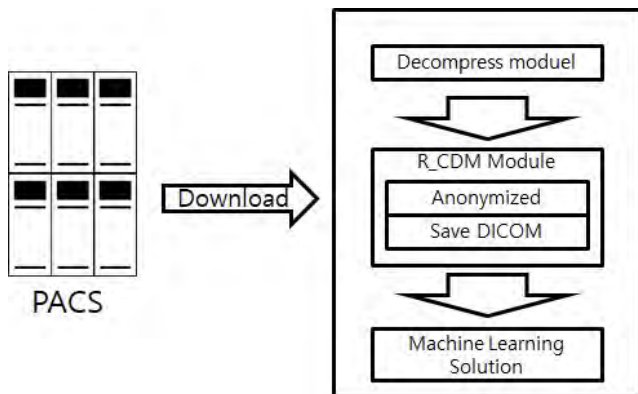
[3] https://elinux.org/Jetson_Nano
 [4] Rothe, Rasmus, Radu Timofte, and Luc Van Gool, "Dex: Deep expectation of apparent age from a single image." Proceedings of the IEEE international conference on computer vision workshops. 2015.
 [5] H. Pan, H. Han, S. Shan, and X. Chen, "Mean-variance loss for deep age estimation from a face.", CVPR, 2018.
 [6] E. Agustsson, R. Timofte, and L. Van Gool. "Anchored regression networks applied to age estimation and super resolution.", ICCV, 2017
 [7] K. Simonyan and A. Zisserman. "Very deep convolutional networks for large-scale image recognition." CoRR, abs/1409.1556, 2014.
 [8] G. Levi and T. Hassner. "Age and gender classification using convolutional neural networks.", CVPRW, 2015.
 [9] C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. Reed, D. Anguelov, D. Erhan, V. Vanhoucke, and A. Rabinovich. "Going deeper with convolutions.", CVPR, 2015.
 [10] A. G. Howard, M. Zhu, B. Chen, D. Kalenichenko, W. Wang, T. Weyand, M. Andreetto, and H. Adam. "Mobilenets: Efficient convolutional neural networks for mobile vision applications.", arXiv preprint arXiv:1704.04861, 2017.
 [11] G. Huang, Z. Liu, L. Van Der Maaten, and K. Q. Weinberger. "Densely connected convolutional networks.", CVPR, 2017.
 [12] Yang, Tsun-Yi, et al. "SSR-Net: A Compact Soft Stagewise Regression Network for Age Estimation.", IJCAI. Vol. 5. No. 6. 2018.
 [13] K. Ricanek and T. Tesafaye. "Morph: A longitudinal image database of normal adult age-progression.", FGR, 2006.
 [14] The FG-NET Aging Database, https://yanweifu.github.io/FG_NET_data/, 2014.
 [15] J. Chen, A. Kumar, R. Ranjan, V. M. Patel, A. Alavi and R. Chellappa, "A cascaded convolutional neural network for age estimation of unconstrained faces," 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS), Niagara Falls, NY, 2016, pp. 1-8.
 [16] Y. Zhang, L. Liu, C. Li, et al., "Quantifying facial age by posterior of age comparisons", Proceedings of the British Machine Vision Conference, London, UK, 2017.
 [17] Cheng, Jingchun, et al. "Exploiting effective facial patches for robust gender recognition.", Tsinghua Science and Technology 24.3 (2019): 333-345.
 [18] Xia, Xiaoling, Cui Xu, and Bing Nan. "Inception-v3 for flower classification." 2017 2nd International Conference on Image, Vision and Computing (ICIVC). IEEE, 2017.
 [19] Chollet, François. "Xception: Deep learning with depthwise separable convolutions." Proceedings of the IEEE conference on computer vision and pattern recognition. 2017.
 [20] K. He, X. Zhang, S. Ren, and J. Sun. "Deep residual learning for image recognition.", CVPR, pages 770–778, 2016.
 [21] Huang, Gao, et al. "Densely connected convolutional networks.", Proceedings of the IEEE conference on computer vision and pattern recognition. 2017.

인공지능 학습용 플랫폼은 R_CDM을 기반으로 인공지능 플랫폼을 통해 학습의 결과를 도출한다. Web based R_CDM을 통해 의료영상에서 환자의 민감 정보를 익명화하고, 인공지능 연구에 필요한 데이터 셋을 다양한 형태로 제공함으로써 수요자에게 필요한 인공지능 알고리즘을 개발하거나 개발된 인공지능 알고리즘의 검증과 테스트를 할 수 있는 환경을 제공한다.

그 후 Deep Learning을 수행하기 위한 인공지능 플랫폼을 통하여 자신이 원하는 조건에 맞춘 학습을 수행할 수 있게 되는데, 이 때 이 환경은 웹 기반으로 하고 있어 일반 사용자에게 인공지능 알고리즘의 학습과 검증 그리고 테스트 할 수 있는 환경을 제공한다.

2.1 전체 시스템 환경

그림 2는 영상기반 인공지능 학습 플랫폼을 위한 전체 시스템 환경을 나타낸다.



(그림 2) 전체 시스템 환경

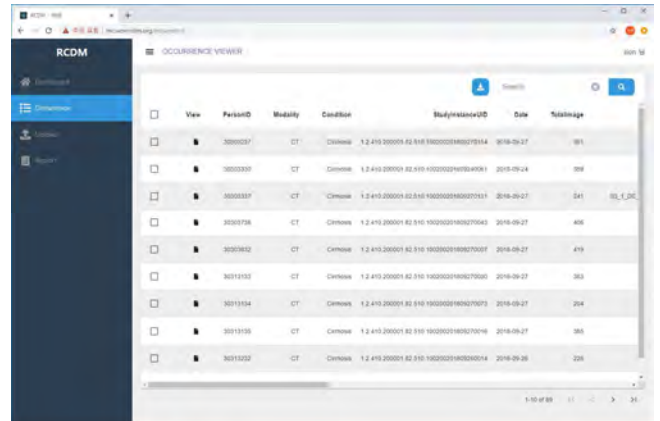
먼저 의료영상 표준(DICOM)을 기반으로 하는 PACS 시스템으로부터 데이터를 다운을 받는다. 다운로드 이 후 압축이 된 영상이 있을 수 있기 때문에 의료영상을 Decompress해준 후 Web based R_CDM에 업로드 하게 된다. 이 과정에서 DICOM Tag정보에 저장되어있는 환자의 민감정보에 대한 익명화가 진행되는데, Patient ID와 Name, Age, Gender가 Blank처리된다. 마지막으로 R_CDM에 의해 익명화된 의료영상을 원하는 형태(png, dcm, excel, csv 등)의 데이터셋을 구성하여 다운로드 받을 수 있다. 그 후 인공지능 플랫폼을 통해 Deep Learning을 수행하여 만들어진 데이터 셋을 학습하고, Accuracy, Loss등의 결과를 확인할 수 있다.

2.2 Web based R_CDM

그림 3은 Web환경을 통해 구축된 R_CDM으로 변환된 결과 리스트를 보이고 있다. Web based R_CDM GUI의 주요기능은 Dashboard와 Occurrence, Upload 그리고 Report로 이루어져 있다.

Dashboard에서는 R_CDM으로 변환된 데이터의 수를 Modality, Condition등으로 분류하여 현황을 보여준다. 이를 통해 원하는 데이터가 있는지를 파악하고 이용할 수

있다. Occurrence에서는 실제로 데이터를 확인할 수 있으며, 검색 기능을 제공하여 필터링된 데이터를 확인할 수 있다. 또한 조건에 맞는 데이터를 다운로드를 할 수 있는데 DICOM으로 받을지, Image, Excel로 받을지를 선택할 수 있으며, Axial과 Coronal, Sagittal을 각각 구분하여 다운로드 받을 수 있으며, Plane, Phase에 따라 다운로드 받을 수 있다.



(그림 3) Web based R_CDM의 Occurrence 화면

Upload는 PACS와 직접적으로 업로드 하거나, 연구목적으로 수집한 데이터를 Condition을 지정하여 업로드하며, 업로드 할 때 환자정보를 익명화하여 업로드 한다. 그리고 업로드 할 때 표준화된 규칙에 의해 환자의 민감정보를 제거하여 데이터베이스에 저장된다. Report는 임상연구를 위해 업로드 된 영상에 대한 판독 소견을 신속하게 저장할 수 있는 기능을 제공한다.

2.3 Web based medical AI Platform

그림 4는 인공지능을 이용하기 위한 웹 기반 플랫폼의 사용자 화면이다. Web based R_CDM으로부터 다운받은 데이터 셋을 학습용 데이터 셋으로 등록하고 image processing 모듈을 선택하여 기본적으로 제공되는 알고리즘을 사용하거나 CNN, RNN등의 인공지능 알고리즘을 직접 구현하여 Deep Learning이 가능하도록 구성되어 있다.



(그림 4) Deep Learning Web 화면

Image processing에서는 2D영상과 3D영상을 지원하는

데, 각각 Classification과 Segmentation을 기본적으로 지원한다. 세부적으로 Resample과 Clahe, Normalization, Standardization, Resize를 할 수 있는 기능이 있다. 또한 각 기능들을 내부에 Python을 기반으로 하는 코드로 수정하여 원하는 조건으로 간단히 수정할 수 있도록 구성되어 있다.

Deep Learning역시 image processing과 마찬가지로 구성되어 있는데, 크게 2D Classification과 Segmentation, 3D Classification과 Segmentation으로 구성되어 있다. Image Processing과 마찬가지로 내부의 코드를 수정하여 Model, Learning Rate, Epoch, Batch size등 학습에 필요한 옵션을 자유롭게 설정할 수 있으며, Depth나 Block Count 등의 model을 구성하는 옵션역시 손쉽게 수정할 수 있도록 구성되어 원하는 Neural Network를 구성하여 학습을 진행할 수 있다. 지원하는 인공지능 알고리즘을 선택할 수 있을 뿐만 아니라 옵션을 선택하여 학습시키거나 검증 또는 테스트하여 알고리즘을 개발할 수 있다. 학습을 진행하면 단계별로 상세정보가 출력되는데, Accuracy와 Loss, Sensitivity, Specificity의 결과가 그래프로 출력된다.

3. 결론 및 향후 연구

본 논문에서는 의료영상기반의 인공지능 연구를 수행할 수 있는 윈스톱 플랫폼을 제안한다. 기존의 인공지능연구를 위한 데이터 셋 구성과 확보에 대한 문제점 해결과 제안하는 플랫폼은 user-friendly한 개발 환경을 제공한다.

향후 계획으로는 다양한 임상연구에 적용하여 개발된 플랫폼의 유용성을 평가하고, 다기관 공동연구를 진행하면서 기능개선 및 보완할 계획이다.

참고문헌

- [1] EliGibson, WenqiLi, CaroleSudre, LucasFidon, Dzhoshkun I.Shakir, GuotaiWang, Zach Eaton-Rosen, RobertGray, TomDoel, YipengHu, TomWhyntie, ParashkevNachev, MarcModat, Dean C.Barratt, SébastienOurselin, M. JorgeCardoso, TomVercauteren “NiftyNet: a deep-learning platform for medical imaging”, Computer Methods and Programs in Biomedicine, Volume 158, May 2018, Pages 113-122
- [2] J.S Kim , T.S Chung, “Deep Learning Applications in Medical Image Analysis”, IEEE Access , vol 6, 29 December 2017, 10.1109/ACCESS.2017.2788044, Pages 9375 - 9389
- [3] E. Y. KWON, C.-W. Jeong, D. M. Kang, Y. R. Kim, Y. H. Lee, K.-H. Yoon, “Development of common data module extension for radiology data (R-CDM): A pilot study to predict outcome of liver cirrhosis with using portal phase abdominal computed tomography data”, ECR 2019, 10.26044/ecr2019/C-1876
- [4]G Hripcsak, JD Duke, “Observational Health Data Sciences and Informatics (OHDSI): Opportunities for Observational Researchers,” in Stud Health Technology Information. 2015;216:574-8.

호스트 기반 침입 탐지 데이터 분석 비교

박대경, 신동규, 신동일
세종대학교 컴퓨터공학과

dkpark@sju.ac.kr, shindk@sejong.ac.kr, dshin@sejong.ac.kr

A Host-based Intrusion Detection Data Analysis Comparison

DaeKyeong Park, Dongkyoo Shin, Dongil Shin
Dept. of Computer Engineering, Sejong University

요 약

오늘날 정보통신 기술이 급격하게 발달하면서 IT 인프라에서 보안의 중요성이 높아졌고 동시에 APT(Advanced Persistent threat)처럼 고도화되고 다양한 형태의 공격이 증가하고 있다. 점점 더 고도화되는 공격을 조기에 방어하거나 예측하는 것은 매우 중요한 문제이며, NIDS(Network-based Intrusion Detection System) 관련 데이터 분석만으로는 빠르게 변형하는 공격을 방어하지 못하는 경우가 많이 보고되고 있다. 따라서 HIDS(Host-based Intrusion Detection System) 데이터 분석을 통해서 위와 같은 공격을 방어하는데 현재는 침입탐지 시스템에서 생성된 데이터가 주로 사용된다. 하지만 데이터가 많이 부족하여 과거에 생성된 DARPA(Defense Advanced Research Projects Agency) 침입 탐지 평가 데이터 세트인 KDD(Knowledge Discovery and Data Mining) 같은 데이터로 연구를 하고 있어 현대 컴퓨터 시스템 특징을 반영한 데이터의 비정상행위 탐지에 대한 연구가 많이 부족하다. 본 논문에서는 기존에 사용되었던 데이터 세트에서 결여된 스레드 정보, 메타 데이터 및 버퍼 데이터를 포함하고 있으면서 최근에 생성된 LID-DS(Leipzig Intrusion Detection-Data Set) 데이터를 이용한 분석 비교 연구를 통해 앞으로 호스트 기반 침입 탐지 데이터 시스템의 나아갈 새로운 연구 방향을 제시한다.

1. 서론

오늘날 정보통신 기술이 급격하게 발달하면서 IT 인프라에서 보안의 중요성이 높아졌고 동시에 사이버상의 공격은 지능형 지속 공격(APT)처럼 고도화 되고 지능적으로 다양해지고 있다. 점점 더 고도화되는 공격을 방어하는 것은 매우 중요한 문제인데, IDS(Intrusion Detection System) 발달 속도가 빠르게 변형되는 공격을 완벽하게 막지는 못한다. HIDS 데이터 분석을 통해서 위와 같은 공격을 방어하는데 현재는 침입탐지 시스템에서 생성된 데이터가 주로 사용된다.[1] 침입탐지 시스템은 네트워크 기반인 NIDS, 호스트 기반인 HIDS 두 가지 방식으로 나눌 수 있다. 네트워크기반 침입탐지 시스템과 달리 호스트 기반 침입탐지 시스템은 시스템 내부와 외부로 전체적으로 모니터링 해야 하는 어려움 때문에 연구가 많이 부족하고 침입탐지 시스템은 새로운 공격 및 내부 공격에 의해 방어 대책이 미흡하고 오경보가 증가하는 문제점이 있다. 호스트 기반 침입

탐지 시스템 방식은 오용 탐지와 이상 탐지 2가지 방법으로 나눌 수 있다.[2] 오용 탐지 방법은 시그니처 기반으로 공격을 탐지하기 때문에 기존의 공격을 탐지하는 것은 효과적이지만 반면에 새로운 공격에 대한 탐지는 부적합하다. 이상 탐지 방법은 오용 탐지 방법과 반대로 정상적인 동작 및 행위로 정의된 상태가 아닌 것에 대한 모든 상황을 이상 행위로 판단하여 탐지하게 된다. 즉 오용 탐지 기법과 달리 제로 데이 공격에 대한 탐지에는 적합하지만 정상 동작 및 이상 행위를 판단할 수 있는 많은 데이터가 요구되거나 데이터가 너무 부족하여 기계 학습에 적용하기에는 어려움이 있다.[3]

본 연구에서는 LID-DS(Leipzig Intrusion Detection-Data Set) 데이터 세트와 이전에 공개되었던 UNM (University of New Mexico)과 ADFA(Australian Defence Force Academy) 호스트 침입탐지 시스템 데이터 세트들을 비교 분석하고 LID-DS 데이터 세트와 기계 학습을 이용한 호스트 기반 침입탐지 시스템의 새로운 연구를 제시한다.

2. 관련 연구

KDD 및 UNM 데이터 세트는 공개적으로 사용이 가능한 데이터이며 침입탐지 시스템의 검증의 기초가 되고 성능 테스트의 기준이 되어 많은 연구들이 진행되고 있다. 하지만 일부 네트워크 정보 중에서 시스템 호출을 통해 프로세스와 커널 간에 전달되는 데이터 형식으로 호스트에서 수집된 추적을 제공하는데 기존의 데이터들은 더 이상 현대적인 특징을 가지고 있지 않기 때문에 최신 컴퓨터 시스템의 다양한 특징들과 공격 특징들이 반영되지 않아 새로운 데이터가 필요하다.[4,5,6]

프로세스 활동이 여러 프로세스에 분산되어있는 유형의 공격은 프로세스의 활동을 특정 프로그램에 따라 분류되지 않고 여러 프로그램에서 무차별적으로 수집해야 하는데 ADFA 데이터 세트에서는 정상과 비정상의 분리성이 약하다. 짧은 시퀀스 모델을 기반으로 SVM(Support Vector Machine)알고리즘을 적용하여 중복된 엔트리는 짧은 시퀀스에 제거되고 정상과 비정상 사이의 기준이 명확해 지기 때문에 기준점이 더 선명해진다. 또한 시스템 콜 기반으로 구성되어 있는 호스트 기반 침입탐지 시스템 방식을 평가하기 위해 시스템 특징들을 반영하고 있으며 리눅스와 윈도우에 따른 많은 공격 패턴들을 포함하고 있어 많은 연구가 진행되고 있다.[4,5,7,8]

3. 본론

3.1 LID-DS Dataset

본 논문에서 사용한 LID-DS 데이터 세트는 1990년대 후반, 호스트 기반 침입 탐지 시스템을 연구하기 위해 처음 만들어진 KDD 데이터는 현재까지도 많은 연구자들이 이용하고 있지만 KDD 데이터는 너무 오래된 컴퓨터 시스템의 특징과 공격 패턴으로 이루어져 있어 현재 사용하기에는 적합하지 않다. 2018년 Leipzig University에서 호스트 기반 침입탐지 시스템의 이상 탐지 연구를 위한 LID-DS 데이터 세트를 공개하였다. LID-DS 데이터 세트는 기존 공개되었던 데이터들과 다르게 현재 공개된 데이터 세트들 보다 최신 컴퓨터 시스템의 다양한 특징들과 공격 방법 및 시나리오로 구성되어 있다. LID-DS 데이터를 통해 기존에 데이터 세트들의 데이터가 부족하여 기계학습에 적용하기 어려웠던 부분을 해결하고 기계학습 방법을 이용하여 새로운 이상 행동들을 더 정확하게 탐지하여 차단할 수 있다. 이를 통해 침입탐지 시스템의 문제점인 오경보율을

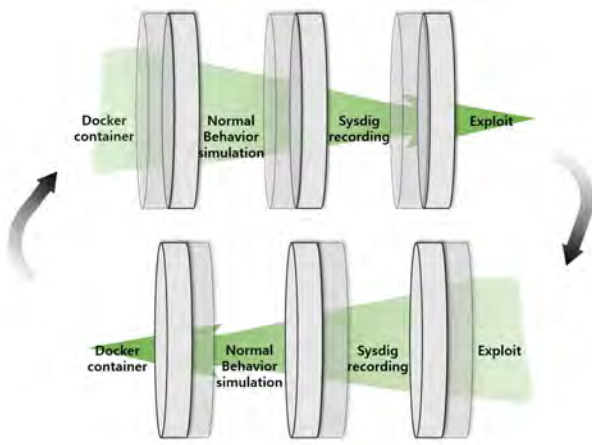
줄일 수 있다.[4,7,8,9]

LID-DS 데이터 세트는 시스템 호출과 관련된 다양한 데이터가 포함되어 있으며 소프트웨어와 다양한 공격이 기록된다. LID-DS 데이터 세트는 표 1과 같이 공격 방법과 여러 시나리오로 구성되며 시나리오를 통해 정상적인 데이터, 비정상적인 데이터를 생성하고 기록하는 프로세스를 구성할 수 있다.

<표 1> LID-DS 데이터에 저장된 공격방법

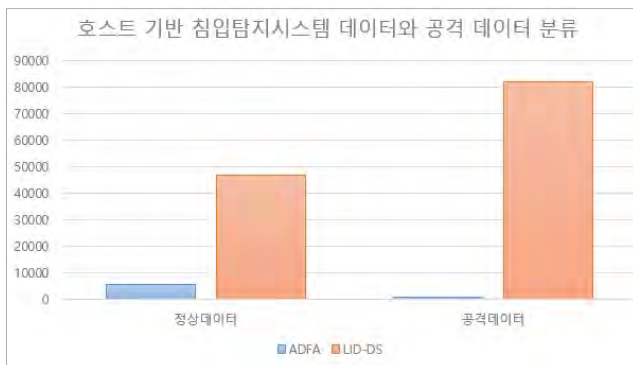
데이터 종류	설 명
CVE-2012-2122	동일한 잘못된 암호로 반복적으로 인증하여 공격자가 인증을 우회할 수 있다.
CVE-2014-0160	서버에 메모리 내용 즉 비밀 키, 데이터에 액세스 가능
Heartbleed	
CWE-307	무차별 대입 사용자 이름 및 암호 추측 시도
무분별한 인증 시도	
CWE-89	공격 데이터를 SQL 명령 변수에 삽입
SQL Injection	
CWE-434	PHP 스크립트와 같은 위험한 유형의 파일을 업로드 할 수 있다.
무분별한 파일 업로드 (PHP)	
CVE-2014-3120	공격자가 임의의 Java 코드를 실행할 수 있도록 한다.
임의 코드 실행	
CVE-2015-1427	공격자가 임의의 셸 명령을 실행할 수 있도록 한다.
임의 코드 실행	
CVE-2017-7529	검사되지 않은 프로그램 코드가 평가된 후 실행될 수 있도록 한다.
CVE-2018-3760	응용 프로그램의 루트 디렉터리 외부에 있는 파일 시스템에 액세스할 수 있다.
CVE-2019-5418	조작된 수락 헤더로 인해 공격 대상 시스템의 파일 시스템에 있는 임의의 파일 내용을 취득할 수 있다.
Zip slip	공격자가 광범위하게 임의의 파일을 덮어 쓰기를 할 수 있다.
CWE-434	서비스가 다른 이미지 형식의 이미지를 svg 파일 형식으로 변환 후 eps를 사용하여 이미지에 악성 코드를 포함 시킨다.
무분별한 파일 업로드 (EPS)	

그림 1은 공격 시나리오를 기록하기 위한 과정이다. LID-DS 데이터 세트의 결과 시스템 호출 추적을 기록하기 위해 공격 대상은 초기 상태를 정의하고 각 공격 후 초기 상태로 되돌리기 위해 Docker10 컨테이너 가상화 소프트웨어 내에서 실행된다. 기록을 위해 LID-DS 프레임 워크를 이용하여 먼저 공격 대상을 호스팅 하는 Docker 컨테이너를 시작하고 그 다음 시나리오에 따라 초기화 작업이 실행되며 정상 동작의 시뮬레이션이 시작된다. 그 후 Sysdig이 활성화되기 전에 짧은 시간동안 기다린다. 이 시간은 Sysdig이 공격 대상 소프트웨어의 시작 효과를 기록하지 못하게 해야 한다. 공격 동작을 기록하는 경우 임의의 시간이 지나면 공격이 시작 되는데 원하는 시간 동안 녹화가 실행 된 후 제어 스크립트에 의해 녹화가 중지 된다. 또한 정상적인 동작 및 사용 된 Docker 컨테이너의 시뮬레이션을 중지하고 제거한다.



(그림 1) LID-DS 데이터 세트의 공격 시뮬레이션 절차

그림 2는 그림 1의 방법으로 생성된 LID-DS의 정상 데이터와 공격 데이터, ADFA의 정상 데이터와 공격 데이터양을 비교하였다.



(그림 2) HIDS 데이터와 공격 데이터 분류

기존에 사용하는 데이터 세트들의 데이터양이 부족하여 기계 학습에 적용하지 못하였다. 반면에 LID-DS 데이터는 시나리오를 통하여 직접 데이터를 생성하기 때문에 방대한 양의 데이터를 수집할 수 있게 된다. 그림 1을 이용하여 생성된 데이터는 표 2의 형식대로 저장된다.

<표 2> LID-DS 데이터의 속성

속 성	설 명
event_number	이벤트 발생 넘버
event_time	고정밀 타임스탬프
cpu	사용된 CPU
user_uid	사용자 UID
process_name	프로세스 이름
thread_id	스레드 ID
event_direction	Enter(>)/Exit(<)
event_type	이벤트 유형
event_arguments	인수 및 반환 값

ADFA 데이터 세트는 일련의 시스템 호출 ID만 포함하고 현대의 공격 패턴을 포함하지 않기 때문에 ADFA 데이터 세트를 이용하여 이상 탐지 테스트를 하기에는 적절하지 않다.[10]

LID-DS의 데이터 파일 자체의 형식은 표 3과 같다. ADFA와 다르게 LID-DS 데이터에는 시스템 호출의 인수, 반환 값, 고정밀 타임스탬프, 해당 프로세스 이름 및 데이터 버퍼의 내용이 포함되어 있다.[11]

<표 3> LID-DS 저장된 데이터

8	13:16:35.219910910	1	33	apache2	21486	< epoll_wait res=1
9	13:16:35.219919842	1	33	apache2	21486	> accept flags=0

3.2 제안점

LID-DS의 타임스탬프의 값은 기존에 존재하는 데이터들의 타임스탬프 보다 초 단위 까지 측정하는 고정밀 값을 측정하기 때문에 시계열 분석을 통해 기계 학습 하여 이상 탐지를 할 수 있다. 시계열 분석은 과거와 현재의 분석에 대해서는 매우 정확하고 사람의 개입이 필요한 이상 징후 탐지 과정을 거치지 않는다. 결과적으로 데이터 또는 문제에 알맞은 특징을 이상 탐지 하는 효과를 나타내게 되고, 이는 학습에 사용했던 데이터 세트의 범위에 따라 이상 탐지 정확성을 높일 수 있을 것 이다.[12]

LID-DS는 기존의 데이터 세트와 다르게 데이터 버퍼를 저장한다. 저장된 데이터 버퍼를 이용하여 공격자가 특정 공격을 수행하기 전에 나타나는 패턴들을 기계 학습 하여 공격 직전에 미리 탐지하여 이상 탐지 정확성을 높일 수 있을 것 이다.

4. 결론 및 추후 연구

본 논문에서 소개하는 LID-DS 데이터 세트는 관련 연구에서 언급 한 이전 데이터 세트의 문제점이었던 시스템의 최신 보안 취약점을 최신 상태로 유지했으며 기본 스레드 정보가 사라지지 않고 새로운 유형의 HIDS를 평가하는 데 사용할 수 있는 방식으로 데이터를 기록한다. 표 4는 앞서 언급 한 데이터 세트들의 속성에 대한 비교이다.

<표 4> 데이터 세트 속성 비교

속 성	LID-DS	ADFA-LD	UNM	KDD99
Arguments	o	x	x	o
Returnvalues	o	x	x	o
Timestamps	o	x	x	o
Process ID	o	x	o	o
Not outdated	o	o	x	x
Data buffers	o	x	x	x
Amount of data	o	x	x	o

추후에는 LID-DS 데이터 세트로 기록된 정상적인 데이터와 비정상적인 데이터를 이용하여 초 단위까지 기록하는 타임스탬프 속성을 가지고 시계열 분석을 통하여 기계 학습을 진행한 후 이상 탐지 하는 연구를 진행할 계획이다. 또한 특정 공격이 시작되기 전에 데이터 버퍼에서 반복되는 현상들을 기계 학습을 통해 이상 탐지 하는 방법과 앞서 제시한 두 가지 방법으로 새로운 공격이나 내부 공격자에 대한 탐지 정확도를 올리기 위한 연구 계획하고 있다.

Acknowledgement

본 연구는 방위사업청과 국방과학연구소의 지원으로 수행 되었습니다 (UD190016ED).

참고문헌

[1] Su, Yunfei, et al. "A framework of apt detection based on dynamic analysis." 2015 4th National Conference on Electrical, Electronics and Computer Engineering. Atlantis Press, 2015.

[2] 최윤정, and 박승수. "이상탐지 (Anomaly Detection) 및 오용탐지 (Misuse Detection) 분석의 정확도 향상을 위한 개선된 데이터마이닝 방법 연구." 한국정보과학회 학술발표논문집 (2006): 238-240.

[3] 최승오, and 김우년. "제어시스템 침입탐지 시스템 기술 연구 동향." 정보보호학회지 24.5 (2014): 7-14.

[4] Mouttaqi, Tarik, Tajjeeddine Rachidi, and Nasser Assem. "Re-evaluation of combined Markov-Bayes models for host intrusion detection on the ADFA dataset." 2017 Intelligent Systems Conference (IntelliSys). IEEE, 2017.

[5] O. Yavanoglu and M. Aydos, "A review on cyber security datasets for machine learning algorithms," 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, 2017, pp. 2186-2193.

[6] Pendleton, Marcus, and Shouhuai Xu. "A dataset generator for next generation system call host intrusion detection systems." MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM). IEEE, 2017.

[7] Creech, Gideon, and Jiankun Hu. "A semantic approach to host-based intrusion detection systems using contiguous and discontinuous system call patterns." IEEE Transactions on Computers 63.4 (2013): 807-819.

[8] Xie, Miao, and Jiankun Hu. "Evaluating host-based anomaly detection systems: A preliminary analysis of adfa-ld." Image and Signal Processing (CISP), 2013 6th International Congress on. Vol. 3. IEEE, 2013.

[9] Röhling, Martin Max, et al. "Standardized container virtualization approach for collecting host intrusion detection data." 2019 Federated Conference on Computer Science and Information Systems (FedCSIS). IEEE, 2019.

[10] Khraisat, Ansam, et al. "Survey of intrusion detection systems: techniques, datasets and challenges." Cybersecurity 2.1 (2019): 20.

[11] Grimmer, Martin, et al. "A modern and sophisticated host based intrusion detection data set." IT-Sicherheit als Voraussetzung für eine erfolgreiche Digitalisierung (2019): 135-145.

[12] 문성은, et al. "기계학습 및 딥러닝 기술동향." 한국통신학회지 (정보와통신) 33.10 (2016): 49-56.

랜덤 탐색과 유전 알고리즘 탐색을 이용한 효율적 기계학습 방법 연구

이경태, 권영근
울산대학교 컴퓨터공학과
lmuffin@naver.com, kwonyk@ulsan.ac.kr

A Study on Efficient Machine Learning Method Using Random Search and Genetic Algorithm Search

Kyung-Tae Lee, Young-Keun Kwon
Dept. of Computer Engineering, Ulsan University

요 약

기계학습 모델을 이용한 분류 및 회귀 문제해결에는 다양한 전처리 알고리즘 및 기계학습 모델이 활용된다. 하지만 합리적인 성능을 위해서는 주어진 데이터에 따라 적절한 알고리즘 조합에 대한 탐색 및 최적화 과정이 필수적이다. 본 논문에서는 최적의 알고리즘 조합을 탐색하는 방법 중 랜덤 탐색과 유전 알고리즘 탐색 방법을 구현하고 8가지 데이터에 대한 성능 비교를 통해 여러 기계학습 모델을 고려하는 탐색 방법의 필요성을 보인다.

1. 서론

기계학습 모델을 이용한 분류 및 회귀 문제해결에는 다양한 전처리 알고리즘 및 기계학습 모델이 활용된다. 하지만 합리적인 성능을 위해서는 주어진 데이터에 따라 적절한 알고리즘 조합에 대한 탐색 및 최적화 과정이 필수적이다. 일반적으로 문제 해결을 위한 데이터의 처리과정은 Data Scaler(DS), Feature Construction(FC), Feature Selection(FS), Machine Learning(ML) 등으로 구성되며, Classification 문제의 경우 타겟 클래스의 비율을 조정하는 Data Rebalancing(DR) 과정이 추가로 고려될 수 있다.

최적의 알고리즘 조합을 찾기 위해서는 일반적으로 Grid Search, Random Search(RS)[1], Genetic Algorithm(GA)[2] 등의 방법을 고려할 수 있다. 여기서 Grid Search는 탐색 가능한 모든 영역을 탐색하는 방법으로, 최적의 성능을 보장하지만 시간적 비용이 크다. 반면에 RS는 임의의 영역을 탐색하는 방법으로, 최적의 성능을 보장하진 않지만 시간적 비용을 제한할 수 있기 때문에 상대적으로 시간적 비용에서 이점이 있다. 마지막으로 GA를 통한 탐색 방법은 RS와 마찬가지로 모든 영역을 탐색하지 않

는 방법으로, 최적의 성능을 보장하진 않지만 마찬가지로 시간적 비용을 제한할 수 있기 때문에 시간적 비용에서 이점이 있다. 또한, RS와는 달리 GA은 탐색 방식을 어떻게 구성하느냐에 따라 특정 영역으로의 탐색을 집중하도록 할 수 있으며, 이에 따라 수렴 속도를 높이거나 최적의 성능으로 유도할 수 있게 된다.

본 논문에서는 최적의 알고리즘 조합을 찾기 위한 두 가지 방법 GA와 RS를 각각 구현하여 문제특성에 대한 사전 정보가 없는 상황에서 단일 기계학습 모델을 이용한 탐색 대비 GA와 RS 기반 탐색 방법의 성능을 비교하는 실험을 진행하였으며, 데이터의 종류에 따라 최적의 기계학습 모델의 종류가 다를 수 있음을 확인하였다. 또한 이를 위해 여러 종류의 기계학습 모델을 고려하여 알고리즘 조합을 탐색하는 방법의 필요성을 제시한다.

2. 문제 정의

<표 1>은 본 논문에서 고려한 각 데이터 처리과정의 알고리즘 종류를 나타낸다.

Rebalancing 과정은 Classification 문제에 대해서만 고려되며, 가장 적은 종류의 데이터와 가장 많은 종류의 데이터의 비율이 최소 75%를 만족하도

<표 1> 데이터 처리 과정 별 알고리즘 종류

Processing	Algorithm	Remarks
DR	Adaptive Synthetic	다수 클래스 대비 소수 클래스 비율 0.75-1.00 조정
	SVM SMOTE	
	Random	
	KMeans SMOTE	
	Borderline SMOTE	
	Condensed Nearest Neighbour	
	Edited Nearest Neighbour	
	NearMiss	
DS	StandardScaler	
	MinMaxScaler	
	Normalizer	
FC	PCA	기존 입력 데이터 크기의 10% 혹은 2-3개 생성
	Truncated SVD	
	Feature Agglomeration	
	Gaussian Random Projection	
	Sparse Random Projection	
FS	Variance Threshold	
ML	MLP	
	KNN	
	SVM	
	DT	
	RF	

록 파라미터를 조정하였다. ML 과정은 Multi Layer Perceptron(MLP), K-Nearest Neighbor(KNN), Support Vector Machine(SVM), Decision Tree(DT), Random Forest(RF) 모델을 사용하였다.

3. 탐색 방법

3.1. RS

각 기계학습 모델(MLP, KNN, SVM, DT, RF)별로 탐색시도만큼 DR, DS, FC, FS 각 단계에 적용할 알고리즘을 임의로 선택한 조합을 생성한다.

3.2. GA

<그림 1>은 구현한 GA의 의사 코드를 나타낸다. 본 논문에서는 기존의 일반적인 GA와 다르게 유력한 기계학습 모델의 집중적인 탐색을 유도하기 위해 하위 성능의 두 그룹사이의 T-Test 결과를 바탕으로 최하위 ML 그룹을 진화 대상에서 제외하는 방법을 적용하였다.

초기화 과정에서는 RS로 임의의 알고리즘 조합을 생성하며, 진화과정 중 자손을 생성하기 전에 각 ML 그룹의 평균 mean squared error(mse)를 기준으로 값이 큰 두 그룹에 대해 T-Test를 진행하며, 이때 p-value 값이 0.05 이하의 값을 만족하면 가장 값이 큰 ML 그룹은 진화 대상에서 제외하게 된다. 자손을 생성하는 과정에서는 두 개의 부모 해를 선택하며, 이때 두 해 중에서 mse 값이 더 작은 해를 s1, 다른 하나를 s2로 사용한다.

4. 실험 결과

```

Generate p initial chromosomes;
for i ← 1 to g
  Remove low performance model group by t-test result;
  Select two chromosomes s1, s2;
  offspring ← Crossover(s1, s2);
  offspring ← Mutation(offspring);
  if worst.mse < offspring.mse
    continue;
  else if s2.mse < offspring.mse
    worst ← offspring;
  else
    s2 ← offspring;
return best chromosome in population;

```

<그림 1> 구현하는 GA 의사코드

4.1. 실험 데이터

실험에서 사용된 데이터는 모두 UCI Machine Learning Repository에서 제공하는 데이터를 활용하였다. <표 2>은 실험에 사용된 각 Dataset의 이름, Input의 개수, Output의 개수, 문제유형을 보인다. 각 데이터는 전체 샘플을 3:1:1의 비율로 Train Set, Validation Set, Test Set을 구성하였다.

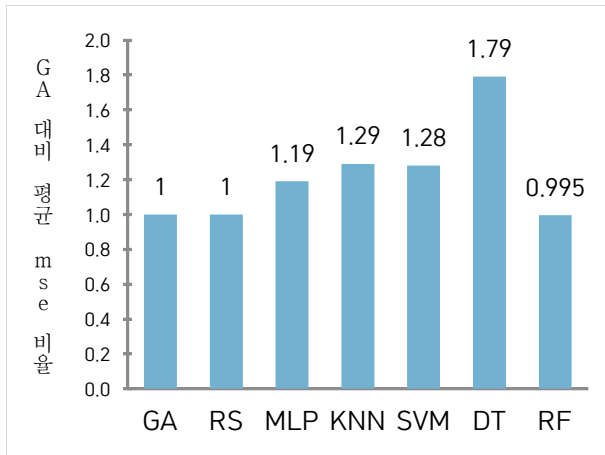
4.2. 분석 결과

실험에 사용된 GA는 초기화 과정에서 <표 1>에 제시된 5가지의 ML방법에 대해 50개의 초기 해를 생성하며, 950세대 진화를 한다. RS는 5가지의 알고리즘에 대해 1000개의 알고리즘 조합을 생성한다. 마지막으로 앞의 두 방법과의 성능 비교를 위해 제시된 5가지의 각 알고리즘별로 RS를 진행하여 각각 1000개의 조합을 생성한다. 평가지표는 mse를 사용하였다. 앞의 과정은 각 데이터에 대해 21회씩 진행하였다.

GA 대비 각 방법의 성능 비교를 위해 Test Set 결과(mse)에서 GA의 결과를 나눈 값을 성능 비율로 사용하였다. <그림 2>는 각 방법의 전체 데이터에 대한 평균 mse 비율을 나타낸 것이며, <표 3>은 각 데이터에 대한 결과의 Top 3를 나타낸 것이다.

<표 2> 데이터의 이름, Input의 개수, Output의 개수 및 문제 구분

Data	Input	Output	Type
Cardiotocography(FHR Pattern) (CTGP)[3]	21	10	Classification
Cardiotocography(Fatal State) (CTGS)[3]	21	3	Classification
Wireless Indoor Localization (WIL)[3]	7	4	Classification
Steel Plates Faults (SPF)[3]	27	7	Classification
Combined Cycle Power Plant (CCPP)[3]	4	1	Regression
Airfoil Self Noise (ASN)[3]	5	1	Regression
QSAR Aquatic Toxicity (QAT)[3]	8	1	Regression
QSAR Fish Toxicity (QFT)[3]	6	1	Regression



<그림 2> 각 방법의 GA 대비 평균 mse 비율

평균 mse 비율에서 가장 낮은 값을 나타내는 RF는 WIL, ASN, QFT 데이터를 제외한 모든 경우에서 가장 mse 값이 나타났고, QFT 데이터에서만 TOP 3 내에 포함되지 못하였다. 최적의 조합을 찾기 위해 다양한 종류의 ML을 고려했던 RS와 GA는 평균 mse 비율에서 두 번째로 낮은 mse를 보였으며, 마찬가지로 전체 데이터에서 TOP 3 내에 6번씩 포함되었고, 특히 QFT 데이터에서는 GA가 가장 낮은 mse를 보였다. 평균 mse 비율에서 상대적으로 좋지 못한 결과가 나왔던 SVM(GA대비 평균 28% 높은 mse)과 MLP(GA대비 평균 19% 높은 mse)는 WIL과 ASN에 대해서는 각각 TOP 1의 결과가 나타났다.

<표 4>는 GA의 진행 과정 중, 각 기계학습 모델이 선택된 횟수를 나타낸다. CTGP, CTGS, SPF, CCPP, QFT 데이터의 경우 GA가 적응적으로 탐색 빈도를 조절하여 가장 적합했던 기계학습 모델과 탐색 횟수가 가장 많았던 모델이 일치했다. 반면에 이외의 데이터에서는 가장 적합한 기계학습 모델일지라도 초기 그룹의 성능이 낮아, 일찍 탐색 고려대상에서 제외되어 결국 탐색 횟수가 저조하게 나타났다.

<표 3> 데이터에 따른 성능 TOP 3

	TOP 1	TOP 2	TOP 3
CTGP	RF	GA	RS
CTGS	RF	RS	GA
WIL	SVM	KNN	RF
SPF	RF	RS	GA
CCPP	RF	GA	RS
ASN	MLP	RF	RS
QAT	RF	SVM	GA
QFT	GA	RS	SVM

<표 4> GA 과정 중 각 기계학습 모델 선택 횟수

	MLP	KNN	SVM	DT	RF
CTGP	34	69	54	52	791
CTGS	41	68	59	42	790
WIL	27	382	171	26	394
SPF	98	107	131	31	633
CCPP	36	29	40	37	858
AFN	53	36	55	64	792
QAT	137	275	294	27	267
QFT	47	42	813	40	58

5. 결론

본 논문은 문제특성에 대한 사전정보가 없는 상황에서 단일 기계학습 모델 대비 GA와 RS 기반 탐색 방법의 성능을 비교하는 실험을 진행하였다. RF는 대부분의 데이터에 대해서 안정적인 성능을 보였지만 QFT 데이터에 대한 결과와 같이 성능이 좋지 못한 경우도 있기 때문에, 최적의 알고리즘 조합을 찾기 위해서는 여러 알고리즘을 고려해야한다. 또한, ASN 및 WIL 데이터와 같이 문제에 적합한 기계학습 모델에 대한 탐색을 강화하도록 유도하는 GA에 대한 개선이 필요하다.

참고문헌

- [1] James Bergstra, Yoshua Bengio, "Random Search for Hyper-Parameter Optimization", Journal of Machine Learning Research, 13, 281-305, 2012
- [2] Chih-Hung Wu, Gwo-Hshiung Tzeng, Yeong-Jia Goo, Wen-Chang Fang, "A real-valued genetic algorithm to optimize the parameters of support vector machine for predicting bankruptcy", Expert Systems with Applications, 32, 397-408, 2007
- [3] Machine Learning Repository, <https://archive.ics.uci.edu/ml/index.php>

OBDII 데이터 기반의 회귀 분석을 통한 실시간 연료 소비량 예측

양희은*, 김도현**

*단국대학교 EduAI센터

**성균관대학교 데이터사이언스융합학과
yanghe@skku.edu, kimtj@me.com

Realtime Fuel Consumption Prediction using In-Vehicle Data from OBDII and Regression Methods

Hee-Eun Yang*, Do-Hyun Kim**

*EduAI Center, Dan-Kook University

**Dept. of Applied Data-science, Sungkyunkwan University

요 약

자율주행 차량이 많아지고 차량의 ECU가 고도화되면서 정확한 차량의 데이터를 획득하고 분석하여 활용하는 것이 중요해지고 있다. 현재에는 내연 기관 차량의 ECU 데이터를 얻기 위해서 OBDII 포트(규격)에 기반한 CAN통신을 주로 이용하고 있다. 하지만 OBDII 규격을 통해서 연비와 같은 중요한 차량 정보를 얻는 경우, 변환식(MAF 센서(흡입 공기량 센서)와 공기/연료 비율을 이용)의 오차 범위가 커서 데이터의 정확도가 낮다. 본 연구에서는 머신 러닝 기법 중에 하나인 회귀 기법을 통해서 기존의 계산보다 더 정확한 연비를 구할 수 있는 모델을 개발하였다. 이러한 모델 개발을 통하여 차량의 RAW 데이터를 기반으로 필요한 차량 데이터를 정확하게 구할 수 있게 되었으며 20회가 넘는 실 도로주행을 통해서 본 모델의 정확도를 검증하였다.

1. 서론

자율주행 차량이 점점 증가하면서 차량에서 정확한 데이터를 획득하고 이를 알맞게 분석하는 중요성이 대두되고 있다.[1] 현재는 자동차 제조사를 제외하고 내연기관 차량의 데이터를 얻기 위해서는 OBDII 규격을 활용하고 있다. 이러한 OBDII의 규격에는 표준 항목과 비표준 항목이 있는데 표준 항목은 법으로 명시되어 있어 비교적 획득하기 간단한 반면에 비표준 항목은 완성차 제조업체와 ECU 제조사에 따라서 일관된 통일성이 없어서 다양한 차량의 데이터를 상대적으로 얻기 힘든 실정이다.

이러한 비표준 항목 중에는 연비, 즉, 연료 소모량(순간 연료 분사량)변수도 속해 있다. 현재에는 연료 소모량을 예측하기 위해서 주로 MAF(Mass Air Flow)센서의 데이터를 이용하여 연비를 계산하는 방식[2]을 주로 사용하고 있다. 하지만 이러한 접근으로 연비를 계산하기 위해서는 공기/연료 비율(air/fuel ratio)을 계산해야 하며[3], 해당 비율은 각 엔진/제조사의 ECU 세팅에 따라서 차이가 있을 수 있어 정확한 계산이 어렵다. (일반적으로 가솔린 14.7, 디젤 14.6, 하이브리드 34 등과 같은 비율로 계산)

본 연구에서는 MAF를 포함한 OBDII의 표준항목 데이터를 이용하여 기존보다 정확하게 차량의 연료소모량을 예측하고자 한다. 이를 위해서 차량의 데이터를 추출 할 수 있는 OBDII 센더와 단말기, 그리고 펌웨어를 제작하였다. 이를 바

탕으로 데이터를 획득하고 가공한 데이터를 기반으로 순간 연료 분사량 변수를 통해 정확하게 연비를 예측하는 모델을 제시[4]하고자 한다.

2. 연구 방법

2.1 차량의 데이터 획득

차량의 RAW 데이터를 얻기 위하여 자체적으로 OBDII 하드웨어 및 펌웨어를 제작하였다. OBDII 하드웨어는 ARM기반의 32비트 CPU와 데이터 저장을 위한 4GB의 롬 메모리가 있으며, 실시간 데이터를 확인할 수 있도록 3G/LTE 모듈과 블루투스칩을 탑재하였다.

다양한 OBDII 프로토콜 중에서 SAEJ1850과 ISO 15765를 지원하며 현재에도 다양한 차량의 규격과 요구에 맞도록 지원 프로토콜 및 차종을 늘려나가고 있다.



(그림 1) OBDII Device(Left) / OBDII Gender PCB(Right)

2.2 획득한 데이터 파악 (리버스엔지니어링)

OBDII 단말기를 통하여 데이터를 얻는다고 해서 바로 모델링에 적용할 수 있는 것은 아니다. RAW 바이너리 데이터를 분석하여 각 데이터가 의미하는 수치를 파악해야 한다. 제작한 하드웨어에서 데이터를 기록하면 (그림 2)와 같이 각 데이터 인덱스의 바이너리 값을 얻을 수 있다.

	ID	A	B	C	D	E	F	G	H	a	b	c	d	e	f	g	h
	112	FF	20	10	00	FF	00	00	98	255	32	16	0	255	0	0	152
	113	FF	20	10	00	FF	00	00	5C	255	32	16	0	255	0	0	92
	113	FF	20	10	00	FF	00	00	10	255	32	16	0	255	0	0	16
	113	FF	20	10	00	FF	00	00	D4	255	32	16	0	255	0	0	212
	113	FF	20	10	00	FF	00	00	98	255	32	16	0	255	0	0	152
	113	FF	20	10	00	FF	00	00	5C	255	32	16	0	255	0	0	92
	113	FF	20	10	00	FF	00	00	10	255	32	16	0	255	0	0	16
	113	FF	20	10	00	FF	00	00	D4	255	32	16	0	255	0	0	212
	113	FF	20	10	00	FF	00	00	98	255	32	16	0	255	0	0	152
	113	FF	20	10	00	FF	00	00	5C	255	32	16	0	255	0	0	92
	113	FF	20	10	00	FF	00	00	10	255	32	16	0	255	0	0	16
	113	FF	20	10	00	FF	00	00	D4	255	32	16	0	255	0	0	212
	113	FF	20	10	00	FF	00	00	98	255	32	16	0	255	0	0	152
	113	FF	20	10	00	FF	00	00	5C	255	32	16	0	255	0	0	92
	113	FF	20	10	00	FF	00	00	10	255	32	16	0	255	0	0	16
	113	FF	20	10	00	FF	00	00	D4	255	32	16	0	255	0	0	212

(그림 2) Binary Data from CAN Communication

OBDII에서 얻은 바이너리 데이터를 리버스 엔지니어링하여 각 항목들이 의미하는 변수를 역으로 알아내는 과정이 필요하다. 각 인덱스가 의미하는 데이터를 차량 직접 주행 및 기능 동작을 통해 찾아내었다. 그림 3은 바이너리 데이터를 변수에 맞춰 변환한 값이다.

[illegible]

(그림 3) Reverse Engineered Feature Data

또한 GPS 수신기를 탑재하여 위/경도를 포함하였고, 자이로센서를 포함하여 X,Y,Z 축의 기울기 정보도 포함하였다.

3. 데이터 가공 및 실험방법

3.1 데이터 범위

본 논문에서는 제작한 소프트웨어를 이용하여 2019년 1월부터 2019년 2월의 주행 데이터를 수집하였다. 전체 데이터 53,580건(초당 Data Set)에서 80%에 해당하는 데이터를 학습데이터(Training data), 20%에 해당하는 데이터를 테스트 데이터(Validation/Test Data)로 사용하였다.

	Start date	End date	Count
Training data	2019.01.09	2019.01.29	42,864
Validation/Test data	2019.01.30	2019.02.12	10,716

<H 1> Data Classification for Model

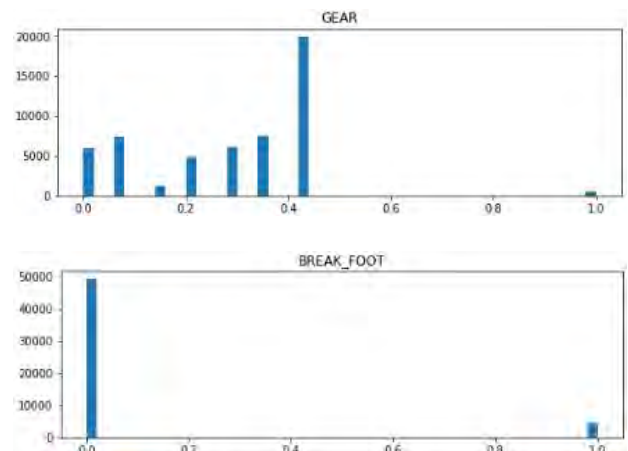
OBDII에서 추출한 데이터는 다음과 같이 구성되어 있다.

칼럼	설명	타입	칼럼	설명	타입
TIMS (iso8601)	측정 시각	연속형	Break_foot (0, 1)	페달 브레이크	논리형
RPM (rpm)	엔진회전수	연속형	Break_side (0, 1)	사이드 브레이크	논리형
Vss (km/h)	차량속도	연속형	Slop_x (°)	x축 기울기	연속형
Lever (P,R,N,D)	레버 위치	범주형	Slop_y (°)	y축 기울기	연속형
TPS (%)	가속페달량	연속형	Slop_z (°)	z축 기울기	연속형
FCO (uL)	순간 연료소모량	연속형	ACON (0, 1)	에어컨	논리형
Mil (0, 1)	엔진경고등	논리형	Torque (N.m)	순간 토크	연속형
Latitude (°)	GPS위도	연속형	Handle (°)	핸들 조향각	연속형
Longitude (°)	GPS경도	연속형	Belt (0, 1)	안전벨트 착용	논리형
Gear (1,2,3,4,5,6,14)	기어 단	범주형	Light (L,R,FR)	방향지시등	범주형

<Ⅹ 2> Data Feature List

3.2 데이터 가공

학습에 사용할 feature들을 살펴보기 위해 모든 수치형 feature들의 분포를 시각화하여 확인해 본 결과 일부 항목들은 매우 불균형 분포를 가진다는 것을 알 수 있었다. 또한, feature 간의 단위가 달랐는데 예를 들어 ‘Gear(기어 단)’ 데이터는 값이 1~14인 반면, ‘Break’ 데이터는 0~1 사이의 값을 포함하고 있다. 이러한 feature값들의 편차를 줄이기 위해 Scaling 과정을 통하여 데이터를 가공하였으며, Scaling 방법 중 MinMax Scaler를 이용하여 값이 0 ~ 1 사이가 되도록 데이터를 재조정하였다[5].



(그림 4) Data Histogram (Gear/Footbreak)

3.3 실험방법

실험은 회귀분석을 기반으로, Linear regression, Ridge, Gradient Boosting, XGBoost, Adaboost 모델 5가지를 구성하여 성능을 측정하였다. 실험은 모델의 학습(Training), 평가(Evaluation), 예측(Prediction) 세 부분으로 나누어 진행하였다. 성능 측정 지표는 평균절대오차, MAE(Mean Absolute Percentage Error)와 평균제곱근 오차인 RMSE(Root Mean Square Error)를 이용하였다. 두 개의 지표는 회귀문제의 성능 지표이며 오차가 커질수록 RMSE값은 커지며, MAE 또한 이상치로 보이는 값이 많을 경우 사용하는 지표로써 값이 클수록 예측에 오차가 많은 것을 나타낸다. 모델 별로 파라미터 값은 가장 최적의 성능을 보이는 값으로 설정하였다.

4. 실험 결과 분석

Statsmodel 라이브러리의 OLS클래스를 이용하여 계수에 대한 분석내용을 <표 3>와 같이 살펴보았다. 결정계수(R-square)는 0.408로 회귀분석으로 추정된 모델이 주어진 데이터를 얼마나 잘 설명하는지에 대한 점수로 값이 1에 가까울수록 데이터를 잘 설명하는 모델이다. 다음으로 F-통계량에 대한 수치를 확인하였을 때, Prob(F-statistic)을 살펴 보았다. 각 입력 변수의 p-value값을 확인한 결과 [GEAR] p-value값이 0.619로 유의미하지 않았다.(p-value>0.05) [GEAR] 칼럼을 제외한 나머지 변수는 0.05 미만으로 회귀 분석에서 유의미한 것으로 나타났다.

Dep. Variable	MPG	R-squared	0.408
Model	OLS	Adj. R-squared	0.408
Method	Least Squares	F-statistic	1556.
Date	Thu, 09 Apr 2020	Prob (F-statistic)	0.00
Time	15:01:07	Log-Likelihood	10522.
No. Observations	42864	AIC	-2.100e+04
Df Residuals	42844	BIC	-2.083e+04
Df Model	19	Covariance Type	nonrobust

<표 3> OLS Regression results

표 5는 3장에서 설명한 실험 모델에 대한 성능을 나타내고 있다. 회귀분석 모델을 적용한 결과, MAE 값이 0.009, RMSE 값이 0.178 으로 AdaBoost 모델의 성능이 제일 좋은 것으로 나타났다.

	Linear regression	Ridge	Gradient Boosting	XGBoost	AdaBoost
MAE	0.14	0.143	0.035	0.049	0.009
RMSE	0.192	0.192	0.062	0.077	0.178

<표 4> Prediction Results

5. 결 론

최근 연료 값의 폭등과 환경적인 문제에 있어서 자동차 연비가 차량 구매에 있어 결정적인 요소 중 하나가 되고 있다. 본 연구는 MAF를 포함한 OBDII의 표준항목을 이용하여 추출한 데이터를 통하여 가장 효과적인 연비 예측 모델을 개발하고자 scaler 및 기계학습 알고리즘 등을 이용하여 변수와 연비와의 관계를 예측하는 연구를 진행하였다. 기계학습을 이용하여 최대 0.009의 MAE값을 갖는 연비 예측 모델을 만들 수 있었다.

더 나아가 신경망 모델을 적용하여 예측 모형의 성능을 고도화[7]하는 연구를 진행할 것이며, 다양한 차종의 데이터를 OBDII 단말기로부터 획득하여 모델에 적용한다면 범용적인 모델을 활용한 실제 응용에 활용될 수 있을 것으로 기대된다.

References

- [1] Dimitrios Rimpas & Andreas Papadakis & Maria Samarakou(2020). OBD-II sensor diagnostics for monitoring vehicle operation and consumption. Energy Reports, Vol 6, Iss , Pp 55-63 (2020)
- [2] <https://www.windmill.co.uk/fuel.html>
- [3] https://www.researchgate.net/figure/Scheme-of-the-different-possibilities-of-MAF-calculation_fig4_285614280
- [4] Aliyu, Abdullateef & Adeshina, Steve & Siraj, Fadzilah. (2014). Classifying Auto-MPG Data set using Neural Network. Proceedings of the 11th International Conference on Electronics, Computer and Computation, ICECCO 2014. 10.1109/ICECCO.2014.6997582.
- [5] Shaheen, H. Agarwal, S. Ranjan, P. Minmax scaler binary pso for feature selection(2020). In: 1st International Conference on Sustainable Technologies for Computational Intelligence- Proceedings of ICTSCI 2019. (Advances in Intelligent Systems and Computing, 2020, 1045:705-716)
- [6] Jamala, Mohammed & Abu-Naser, Samy. (2018). Predicting MPG for Automobile Using Artificial Neural Network Analysis. Information Systems Research. 2. 5-21.
- [7] Han, Chang-Wook. (2017). Auto MPG Prediction using Tree Architectures of Fuzzy Neural Networks. 39-43. 10.14257/astl.2017.145.08.

딥러닝 기반 특허의 종속 청구항 인식 개선

박주연*, 신예지*, 김민수*, 김동호**, 김지희**

*동국대학교 컴퓨터공학과

**동국대학교 융합교육원

pjuyeon25@gmail.com, gjsld1@naver.com, duqrlpig@gmail.com

dongho.kim@dgu.edu, jihie.kim@dgu.edu

Improving Recognition of Patent's Claims with Deep Neural Networks

Ju-yeon Park*, Yeji Shin*, Minsu Kim*, Dongho Kim**, Jihie Kim**

*Dept. of Computer Science and Engineering, Dongguk University

** Dongguk Institute of Convergence Education

Abstract

특허를 통해 기술의 권리를 정의하고 보호하는 일이 매우 중요해짐에 따라 특허 문서를 분석하는 연구 또한 중요해지고 있다. 특히 특허의 청구항을 종속항과 독립항을 구분하고, 관련된 인용을 찾아내는 일은 관련 특허들을 분석하는데 매우 중요하다. 본 연구는 최근 텍스트 분석 분야에 획기적 성능 개선을 이끈 BERT(Bidirectional Encoder Representations From Transformers) 언어 모델을 사용하고 Neural Network의 파인 튜닝 과정을 통해 청구항의 독립과 종속을 구분하였고, 인용하는 항의 번호와 인용 문구로 이루어진 인용 패턴을 통해 종속항의 인용 항을 찾아내었다. 이 방법을 2003년 이후의 xml 형식의 미국 특허 데이터에 사용한 결과, 정확도 99%의 성능을 확보하였다.

1. Introduction

4차 산업혁명 시대를 맞이하여 기술은 점점 빠르게 변화하고 발전하고 있다. 이러한 시대의 중심에서 기술의 권리를 정의하고 보호하는 일은 매우 중요하다. 최근 글로벌 기업들 간의 대규모 특허 침해 소송이 증가함에 따라 특허문서분석을 활용한 체계적인 연구도 요구되고 있다. 특허 권리 범위의 정확한 해석을 위해서는 권리범위에 대한 상위/하위 포함 관계의 명확한 구분이 필요하다. 청구 범위는 독립항과 종속항들로 구성되는데, 이러한 독립항과 종속항들의 명확한 구분을 통해 특허문서분석에 도움을 줄 수 있다.

최근의 특허는 XML/SGML 형태로 제공되어, 인용된 종속항이 태그로 표현된다. 미국의 특허 데이터 관련, 과거의 2003년 이전의 특허는 텍스트 정보로, 인용하는 항의 태그가 되어있지 않기 때문에 직접 판별해야 한다. 또한, 종속 관계는 다양한 표현으로 이루어져있고, 오기가 있을 수 있기 때문에 주의해야 한다.

따라서 본 연구는 2003년 이후의 태그 청구범위가 구분된 5만여개의 데이터를 통해 2003년 이전 특허 데이터의 청구항 인용 관계를 명확하게 하는 것을 목표로 한다. 특허의 청구항의 상하 포함 관계 파악은

총 2단계로 이루어지며, 약 8 : 1의 종속항과 독립항 간의 학습데이터의 양과 질의 균형을 향상시키기 위해 최근 텍스트 분석 분야에 획기적 성능 개선을 이끈 BERT(Bidirectional Encoder Representations From Transformers)[1] 모델을 사용하고, 특허 분류 데이터를 이용하여 파인 튜닝 한다. 문맥의 구조뿐만 아니라 문맥의 이해를 포함시킨 BERT 모델을 통해 특허 청구항의 종속 관계를 명확하게 구분하고, 데이터 불균형 문제도 완화시킨다. 마지막으로 인용하는 항의 번호와 인용 문구로 이루어진 인용 패턴을 이용하여 종속항의 인용 항의 번호를 찾는다. 이 방법을 2003년 이후의 xml 형식의 미국 특허 데이터에 사용한 결과, 정확도 99%의 성능을 확보하였다

2. Related Work

특허를 분석하는 다양한 연구들이 진행되고 있는 가운데, 이 연구에서는 특허의 청구항들을 분석하여 독립항과 종속항을 구분하고자 한다.

이미 학습된 BERT 모델의 파인 튜닝을 이용하여 특허의 분류를 진행하는 연구도 있다.[2] 이 연구에서는 특허의 다른 부분이 아닌 청구항만을 분석하여 특허의 분류를 진행한다. 같은 BERT 모델의 파인 튜

닝을 이용하여 청구항을 분석하지만 최종 분류하는 결과물이 특허 전체의 분류라는 점에서 차이가 있다.

청구항의 분류 알고리즘을 통해 특허 청구항의 구조분석을 하는 연구도 존재한다.[3] 이 연구에서는 청구항의 형식적 특징과 청구대상(subject-matter)을 이용한 독립항과 종속항을 분류하는 알고리즘을 제안한다. 하지만, 이 연구에서는 국내 특허 문서에 한정되며, 청구항의 “n 항(청구항 n)에 있어서/에서”의 문구의 여부를 통해 단순히 종속항과 독립항을 구분하게 된다. 우리의 연구에서는 BERT 모델을 도입해 보다 종속항을 구분 한다는 점에서 좀 더 높은 완전성을 보여줄 수 있다.

딥 러닝 을 활용한 특허를 분류하는 연구[4]에서는 특허 문서의 IPC(International Patent Classification) 와 IPC sub 분류를 진행한다. 특허 문서 분석을 위해 특징 벡터들을 추출한 후, 인코더 층과 네트워크 층을 활용하여 특징 학습을 진행한 후에 Softmax 회귀를 통해 분류를 하게 된다. 이 연구에서는 특허 문서 분석에 쓰이는 Softmax 회귀 이외에도 특허 문서의 특징을 찾는 학습 과정이 필요하게 되므로 특허 문서 분석 이전의 전처리 과정이 복잡하게 된다.

문장의 형태소 단위의 분석을 통해 특허 항간의 구조 분석을 진행한 연구도 있다.[5] 일본어 특허를 기반으로 문장의 단어에 따라 총 6 개의 문장 구조로 구분하고, 이런 구조를 바탕으로 청구항을 트리 형태로 시각화하여 특허의 가독성을 높인다. 따라서, 특허 청구항에 대한 더 정확한 이해를 할 수 있지만, 이 연구에서는 단순히 청구항의 구조만을 나타낼 뿐 어떠한 인용 관계도 알 수 없기 때문에 청구항의 전체적인 맥락을 이해하는 데에는 어려움이 있다.

이 논문에서는 특허의 청구항을 분석하여 인용 문구와 인용하는 항의 번호로 이루어진 인용 패턴을 이용하여 BERT 학습 모델에 적용시킨 후, 이 학습 모델을 이용하여 간단하게 청구항의 인용 관계를 파악하여 특허 청구항의 내용을 보다 정확하게 파악하는데 도움이 되고자 한다.

3. Approach

현재 미국의 특허는 청구항에서 인용하는 항의 정보를 태그 형식으로 (그림 1)과 같이 제시하고 있다.

```
<PATN> US06844315B1
<RN> US6844315
<CLMS> <CLAIMS><CLAIM ORDER='1' id='CLM-00001'> <claim-text>1. A method of treating sepsis in a subject comprising: <claim-text>administering, in a pharmaceutically acceptable manner, a pharmaceutically effective amount of two or more immunoregulators, immunoregulators peptides, functional fragments or functional analogues thereof to the subject, wherein said immunoregulators comprise peptide and recombinant hCG. </claim-text></claim-text> </CLAIM>
<CLAIM ORDER='2' id='CLM-00002'> <claim-text>2. The method of <claim-ref idref="CLM-00001">claim 1</claim-ref> wherein the peptide is selected from the group consisting of SEQ ID NO: 1, SEQ ID NO: 2, SEQ ID NO: 3 and a functional fragment thereof.</claim-text> </CLAIM> <CLAIM ORDER='3' id='CLM-00003'>
```

(그림 1) 미국 특허 문서 예시

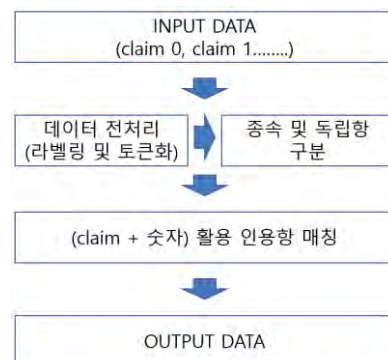
항의 인용 관계 정보를 나타낼 수 있는 태그는, 항의 정보를 가지고 있는 <CLAIM ORDER>와 인용 관계를 제시하는 <claim-ref>태그로, 이 인용 태그들을 중심으로 분석하였다.

인용 태그와 인용 태그의 앞, 뒤 문장들을 (그림 2)와 같이 파싱 하였다. 데이터를 분석한 결과, 각 data 종속항 중 인용 태그이지만 [claim + 숫자] 문구가 없는 경우는 총 1,618,116 개의 데이터 중 7696 개로 약 0.005%에 불과하였다. 따라서, 독립항과 종속항만 잘 구분해낸다면, 산술적으로 99.5% 이상의 확률로 정확한 인용 태그 지칭 가능할 것이라고 예상하였다.

PDATA1	Attribute:CLREF	PDATA2
3. Indenyl compound according to	CLM-00001	, wherein R contains at least one aryl group.
4. Indenyl compound according to	CLM-00001	wherein R contains at least one phenylene group.
5. Indenyl compound according to	CLM-00001	wherein R contains a bisaryl group.
6. Indenyl compound according to	CLM-00001	wherein R is a 2,2'-biphenylene.
7. Indenyl compound according to	CLM-00001	wherein M is Ti, Zr or Hf.
8. Indenyl compound according to	CLM-00001	wherein Q is Cl or a methyl group.

(그림 2) 데이터 파싱 예시

이와 같은 [claim + 숫자] 특징을 활용하여 (그림 3)과 같이 청구항 분류의 전반적인 프로세스를 구축하였다.



(그림 3) 전반적인 프로세스

각 종속항과 독립항을 구분하기 위해서 딥러닝 모델을 활용하고자 하였으며 우선 CNN 모델을 활용하였다. 각 청구항의 네번째 이상의 어절을 더미 데이터로 보고 잘라내어 종속 여부를 라벨링 한 뒤 Lookup 테이블 (벡터화 된 입력 데이터)을 구축해 전

처리과정을 마쳤다. 하지만 CNN 모델의 트레이닝 결과는 예상보다 낮은 70% 수준으로 나타났으며, 이에 대한 원인으로 문장 구조 기반의 알고리즘과 데이터의 편향성(true: 90%, false: 10%)을 지목하였다.

첫번째 문제점인 문장 구조기반의 알고리즘을 개선하기 위해 CNN 모델에서 문맥이해 기반의 알고리즘인 NLP 기반 딥러닝 모델로 변경하였다. 또한 데이터 편향성을 개선하기 위하여 사전 학습된 모델을 튜닝하는 파인 튜닝 방식을 활용하였다. 이때 활용한 모델은 BERT 모델이며 BERT는 구글이 공개한 사전 훈련된 자연어 처리의 딥러닝 모델이며 일부 성능 평가에서 인간보다 높은 정확도를 보인다. 이러한 사전 훈련된 모델을 튜닝하여 활용한다면 데이터의 부족, 비용 및 시간적인 문제들을 다수 해결할 수 있다.

BERT 모델을 튜닝하기 위해선 해당 모델이 이해할 수 있는 형태로 데이터를 전처리 하는 과정이 필요하다. 우선 모델 학습을 위해 활용될 학습 데이터 셋(약 100,000 여개)을 .tsv 형태의 확장자로 준비하였다. 다음으로 해당 데이터는 (그림 3)과 같이 column 0에 각 행의 ID, column 1에 각 행의 라벨(종속성 여부), column 2에 alpha 데이터, column 3에 각 행의 문자열의 형태로 구성하였다.

	id	label	alpha	text
0	0	0	a	Unfortunately, the frustration of being Dr. Go...
1	1	1	a	Been going to Dr. Goldberg for over 10 years. ...
2	2	0	a	I don't know what Dr. Goldberg was like before...
3	3	0	a	I'm writing this review to give you a heads up...
4	4	1	a	All the food is great here. But the best thing...

(그림 3) 전처리 데이터 구성

현재까지의 전처리 된 데이터를 인간이 이해할 수 있는 문자표현의 형태라고 한다면, 다음으로 BERT 모델이 이해할 수 있는 특징표현의 형태로 추가 전처리 과정을 진행하였다. 각 행은 라벨과 텍스트의 토큰화가 진행되며 각각의 토큰 쌍은 앞선 column 0의 id에 따라 구분된다.

```
{
  "attention_probs_dropout_prob": 0.1,
  "hidden_act": "gelu",
  "hidden_dropout_prob": 0.1,
  "hidden_size": 768,
  "initializer_range": 0.02,
  "intermediate_size": 3072,
  "max_position_embeddings": 512,
  "num_attention_heads": 12,
  "num_hidden_layers": 12,
  "type_vocab_size": 2,
  "vocab_size": 28996
}
```

(그림 4) Training parameter

앞서 만들어진 전처리 데이터를 사전 학습된 BERT 모델에 적용하여 retraining 과정을 거쳐 종속항과 독립항을 구분하는 모델을 만들어내었다. 해당 모델의 테스트 과정을 위해 약 23,000 여개의 테스트 데이터 셋을 준비하였고 앞선 전처리 과정을 거친 후에 evaluate 하였다.

```
# Load pre-trained model (weights)
model = BertForSequenceClassification.from_pretrained(BERT_MODEL, cache_dir=CACHE_DIR, num_labels=num_labels)
# model = BertForSequenceClassification.from_pretrained(CACHE_DIR + 'cached_base_bert_pytorch.tar.gz', cache_dir=CACHE_DIR, num_labels=num_labels)

1%|
| 3306496/404400730 [00:19<08:08, 820603.15B/s]
```

(그림 5) BERT 모델의 retraining

4. Result

NLP BERT 모델의 튜닝 결과는 다음과 같다. 10 만개의 데이터를 학습시킨 후, 2 만개의 데이터를 통해 테스트를 진행한 결과는 <표 1>, <표 2>와 같다.

항목	값
MCC (Matthews correlation coefficient)	99.97%
Evaluate loss	0.07%

<표 1> BERT 모델 성능

		실제 결과 (종속항 19242 개, 독립항 4351 개)	
		true	false
분류 결과	true	19240 개	0 개
	false	2 개	4351 개

<표 2> BERT 모델 테스트 결과

<표 1> 높은 매튜 상관관계수(MCC) 값으로 테스트 데이터가 분류되었다. <표 2> 분류 결과에서는 총 19242 개의 종속항 중 실제로 종속으로 구분한 개수는 19240 개, loss 는 2 개가 나왔다. 또한, 총 4351 개의 독립항 중 실제로 독립으로 구분한 개수는 4351 개, loss 는 0 개가 나왔다. 결론적으로 0.07%의 낮은 손실률(Evaluate loss)로 테스트 데이터가 올바르게 분류되었다는 것을 알 수 있다.

5. Discussion

특허의 청구항들을 독립항과 종속항으로 구분하고, 종속항의 경우 인용하고 있는 항을 찾는 BERT 학습 모델의 정확도가 99% 이상으로 높게 나왔다. 특허의 종속항들이 대부분 인용 문구와 인용하는 항의 번호 형식으로 인용 패턴이 정형화되어 있기 때문에 단순한 BERT 학습 모델을 통해서도 높은 정확도를 얻을 수 있었다. 그렇지만 인용하는 항의 번호가 명시되어 있지 않거나, 인용하는 번호가 여러 개(e.g. 1,2,3 or 1-3)인 예외적인 경우가 존재하는데, 지금의 BERT 학습 모델로는 이런 예외 케이스들을 정확하게 찾을 수 없다. 따라서 정형화되어 있지 않은 소수의 예외 케이스들을 처리할 수 있도록 하기 위해 단순한 패턴을 통해 인용 항을 찾는 것이 아니라 문맥의 이해를 포함한 자연어 처리를 활용한 청구항 인용 방식을 학습하여, 이를 찾아낸다면 하나 이상의 청구항들을 모두 찾아낼 수 있게 되어 더 높은 정확도를 얻을 수 있을 것이다.

* 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 SW 중심대학지원사업의 연구결과로 수행되었음" (2016-0-00017)

참고문헌

- [1] Jacob Devlin, Ming-Wei Chang, Kenton Lee, Kristina Toutanova, "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding", 24 May, 2019, Google AI Language, 10 Apr, 2020, <<https://arxiv.org/abs/1810.04805>>
- [2] Jieh-Sheng Lee, Jieh Hsiang, "Patent BERT: Patent Classification with Fine-Tuning a pre-trained BERT Model", 1 Jul, 2019, National Taiwan University, 10 Apr, 2020, <<https://arxiv.org/abs/1906.02124>>
- [3] 송민호, 임소라, 권용진 "특허 청구항의 구조분석을 위한 청구항 분류 알고리즘", 한국통신대회, 2018, 102-103(2 pages)
- [4] Bing Xia, Baoan LI, Xueqiang LV "Research on Patent Classification Based on Deep Learning", Advances in Intelligent Systems Research, 2016
- [5] Akihiro S., Manabu O., Yuzo M., Makoto I. "Patent Claim Processing for Readability", "03: Proceedings of the ACL-2003 workshop on Patent corpus processing", 2003, 56-65(10 pages)

초해상화 모델의 활성화함수 변경에 따른 성능 분석

유영준, 김대희, 이재구*
국민대학교 컴퓨터공학과
*jaekoo@kookmin.ac.kr

Performance Analysis of Various Activation Functions in Super Resolution Model

YoungJun Yoo, DaeHee Kim, JaeKoo Lee*
Dept. of Computer Science, Kookmin University

요 약

ReLU(Rectified Linear Unit) 함수는 제안된 이후로 대부분의 깊은 인공신경망 모델들에서 표준 활성화함수로써 지배적으로 사용되었다. 이후에 ReLU를 대체하기 위해 Leaky ReLU, Swish, Mish 활성화 함수가 제시되었는데, 이들은 영상 분류 과업에서 기존 ReLU 함수 보다 향상된 성능을 보였다. 따라서 초해상화(Super Resolution) 과업에서도 ReLU를 다른 활성화함수들로 대체하여 성능 향상을 얻을 수 있는지 실험해볼 필요성을 느꼈다. 본 연구에서는 초해상화 과업에서 안정적인 성능을 보이는 EDSR(Enhanced Deep Super-Resolution Network) 모델의 활성화함수들을 변경하면서 성능을 비교하였다. 결과적으로 EDSR의 활성화함수를 변경하면서 진행한 실험에서 해상도를 2 배로 변환하는 경우, 기존 활성화함수인 ReLU가 실험에 사용된 다른 활성화함수들 보다 비슷하거나 높은 성능을 보였다. 하지만 해상도를 4 배로 변환하는 경우에는 Leaky ReLU와 Swish 함수가 기존 ReLU 함수 대비 다소 향상된 성능을 보임을 확인하였다. 구체적으로 Leaky ReLU를 사용했을 때 기존 ReLU보다 영상의 품질을 정량적으로 평가할 수 있는 PSNR과 SSIM 평가지표가 평균 0.06%, 0.05%, Swish를 사용했을 때는 평균 0.06%, 0.03%의 성능 향상을 확인할 수 있었다. 4 배의 해상도를 높이는 초해상화의 경우, Leaky ReLU와 Swish가 ReLU 대비 향상된 성능을 보였기 때문에 향후 연구에서는 다른 초해상화 모델에서도 성능 향상을 위해 활성화함수를 Leaky ReLU나 Swish로 대체하는 비교실험을 수행하는 것도 필요하다고 판단된다.

1. 서론

초해상화(Super Resolution)는 저해상도의 영상을 고해상도 영상으로 변환하는 과업이다. 기존 영상의 품질을 향상할 수 있는 특성 때문에 초상해도는 CCTV 영상 데이터에서의 얼굴 인식, 특정 장면에서의 객체 탐지, 천문 영상, 의학 촬영 영상 등의 다양한 분야에서 사용된다.[1] 또한 초해상화는 크게 하나의 영상을 이용하는지, 여러 영상을 이용하는지에 따라 SISR(Single Image Super Resolution)과 MISR(Multi Image Super Resolution)로 나뉜다. MISR이 SISR에 기초를 두고 있기 때문에 주로 SISR에 대한 연구가 주를 이루고 있다.

EDSR(Enhanced Deep Super-Resolution Network) [2]은 NTIRE2017 Super-Resolution Challenge[3]에서 우승한 초해상화 모델인데 제안된 당시 SOTA(State-Of-The-Art)를 달성하였다. EDSR 이전에 제시되었던 SRResNet[4]은 영상 분류 과업과 같은 고수준의 과업을 해결하기 위해 고안된 ResNet[5]이라는 인공신경망 구조를 사용하였다. 하지만 SISR과 같은 저수준

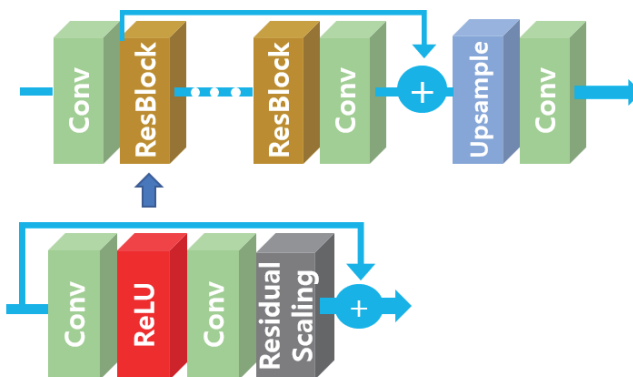
과업을 풀기 위해서 ResNet 구조를 동일하게 사용하는 것은 문제가 있었다. EDSR는 SRResNet보다 성능이 향상되었는데, SRResNet과 같은 이전 인공신경망 구조들에서 불필요한 모듈들을 제거하여 최적화를 했고 훈련 과정을 안정화하였다. 최적화를 통해 확보한 메모리 공간을 사용해 모델의 크기를 늘려서 구조를 보다 적합하게 수정할 수 있었다. 활성화함수로는 ReLU[6]를 사용하였다.

최근 깊은 인공신경망 연구에서 ReLU 함수는 다른 활성화함수들과 비교해서 간단한 구현과 일관된 성능 때문에 대부분의 모델들에서 표준 활성화함수로써 지배적으로 사용되었다. 특히 영상 분류 과업에서 좋은 성능을 보였다. 최근 ReLU의 단점들을 보완한 다양한 활성화함수들이 제안되었으며 대표적으로 Leaky ReLU[7], Swish[8], Mish[9]가 있다. 이 활성화함수들은 특히 영상 분류 과업에서 기존의 ReLU 함수보다 좋은 성능을 보였다. 따라서 초해상화 과업에서도 활성화함수를 대체하여 이러한 성능 향상을 얻을 수 있는지 검증할 필요성이 대두되었다.

본 논문에서는 초해상화 모델의 활성화함수를 기존의 ReLU에서 Leaky ReLU, Swish, Mish로 대체했을 때 모델의 성능을 높일 수 있는지 확인하였다. 초해상화 모델로는 초해상화 평가지표인 PSNR(Peak Signal-to-Noise Ratio)과 SSIM(Structural Similarity)에서 안정적인 성능을 보이는 EDSR 을 사용하였다. 기존 ReLU와 더불어 Leaky ReLU, Swish, Mish 활성화함수를 EDSR에 변경하면서 활성화함수에 따른 성능을 비교 및 분석하였다.

실험에서는 초해상화 과업에서 주로 사용되는 5개의 데이터집합을 사용하였고, 해상도를 2배로 변환하는 경우와 해상도를 4배로 변환하는 경우로 나누어, 각 모델에서 활성화함수에 따른 성능 비교를 진행하였다.

2. EDSR (Enhanced Deep Super-Resolution Network)

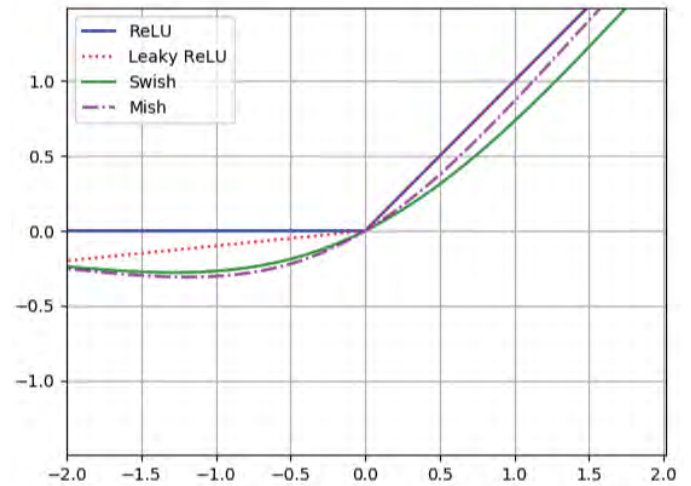


(그림 1) EDSR 구조

EDSR은 SRResNet이 잔차 블록(Residual Block)에서 사용했던 배치 정규화(Batch Normalization)층을 모두 제거하였다. 인공신경망의 특징들을 정규화시켜 인공신경망의 유연성을 저해하는 배치 정규화 층 제거를 통해 성능을 향상할 수 있었다. 또한 배치 정규화 층을 제거함으로써 GPU 메모리 사용량을 줄였는데, 이렇게 확보한 메모리를 사용해 더 큰 모델을 구성하여 제한된 계산 자원하에서 SRResNet보다 더 좋은 성능을 얻을 수 있었다. 활성화함수로는 ReLU 함수를 사용하였는데, (그림 1)에서 보면 잔차 블록에서 ReLU를 사용하는 것을 볼 수 있다.

3. 활성화함수 (Activation Function)

(그림 2)에서는 본 논문에서 사용된 ReLU, Leaky ReLU, Swish, Mish 활성화함수를 표현하였다. 식 (1)은 ReLU 함수의 수식을 표현하였으며, ReLU를 사용하면 깊은 인공신경망에서 Sigmoid 또는 Tanh 함수를 사용한 것보다 더 쉽게 최적화가 된다. Sigmoid와 Tanh 같은 활성화함수들은 입력이 커지면 미분 값이 포화가 되어 오류를 전달 못 하는 문제가 있었는데, ReLU는 양수 영역에서 값이 선형적으로 출력되어 경사소멸(Vanishing Gradient)을 피할 수 있다. 그리고 구현이 매우 간단하고 연산 비용이 많이 들지 않는다.



(그림 2) 활성화함수 비교 그래프

$$f(x) = \begin{cases} (x < 0) & f(x) = 0 \\ (x \geq 0) & f(x) = x \end{cases} \quad (1)$$

또한 입력으로 들어오는 값이 음수면 출력을 모두 0으로 처리하여 규제 효과를 얻을 수 있다. 하지만 이러한 특성 때문에 해당 노드가 학습이 안 되는 단점이 있다.

$$f(x) = \begin{cases} (x < 0) & f(x) = ax \\ (x \geq 0) & f(x) = x \end{cases} \quad (2)$$

이러한 단점을 극복하고자 Leaky ReLU라는 활성화함수가 제안되었다. 식 (2)는 Leaky ReLU 함수의 수식을 표현하였다. Leaky ReLU는 음수 영역을 모두 0으로 처리하는 ReLU의 단점을 보완하여 만들어진 활성화함수이다. Leaky ReLU는 ReLU와 거의 유사하지만, ReLU와 달리 음수 영역에서, 0에서 1의 범위를 갖는 사용자 매개변수 a 값에 따라 조정되는 작은 기울기를 부여한다.

$$f(x) = x \cdot \sigma(x) \quad (3)$$

ReLU의 단점을 해결하기 위해 또 다른 활성화함수인 Swish가 제안되었다. 식 (3)은 Swish 함수의 수식을 표현하였으며, Swish는 ReLU와 달리 부드럽고 비 단조함수(Non-monotonic Function)이다. Swish는 큰 음수값이 입력되면 출력이 0이 되어 미분 값이 포화되지만, 작은 음수값이 입력되면 들어온 값을 어느 정도 보존한다. 이런 특성을 바탕으로 기존 ReLU의 문제를 어느 정도 해결하여 최적점에 더욱 잘 도달하게 해준다. 또한 Swish의 부드러운 오차 손실 경사(Loss Landscape)는 학습률과 초깃값에 대한 민감성을 줄일 수 있다. 이후에 Swish와 유사한 Mish라는 활성화함수도 제안되었다.

<표 1> 각 활성화함수에 따른 EDSR 성능 비교 결과

Scale	DataSet	ReLU(기준)		Leaky ReLU		Swish		Mish	
		PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
x2	DIV2K[3]	36.56	0.9407	33.71	0.9140	36.47	0.9401	36.48	0.9401
	Set5[10]	38.19	0.9445	35.32	0.9237	38.19	0.9447	38.19	0.9447
	Set14[11]	33.95	0.8969	31.60	0.8723	33.88	0.8966	33.83	0.8965
	B100[12]	32.35	0.8928	30.65	0.8683	32.31	0.8922	32.33	0.8922
	Urban100[13]	32.97	0.9268	28.02	0.8583	32.77	0.9252	32.79	0.9251
	Average	34.80	0.9203	31.86	0.8873	34.73	0.9198	34.72	0.9197
x4	DIV2K	30.73	0.8269	30.74	0.8271	30.74	0.8270	30.69	0.8258
	Set5	32.48	0.8686	32.55	0.8692	32.51	0.8690	32.48	0.8679
	Set14	28.82	0.7511	28.82	0.7514	28.83	0.7513	28.79	0.7501
	B100	27.72	0.7189	27.73	0.7191	27.73	0.7190	27.70	0.7176
	Urban100	26.65	0.7836	26.67	0.7844	26.67	0.7841	26.55	0.7809
	Average	29.28	0.7898	29.30	0.7902	29.30	0.7900	29.24	0.7885

$$f(x) = x * \tanh(\zeta(x)) \quad (4)$$

식(4)는 Mish 함수의 수식을 표현하였으며, Mish도 Swish와 유사하게 부드럽고 비 단조함수이다. 양수 영역에서 값이 선형적으로 증가하는 ReLU와 달리 Mish는 부드럽게 증가하기 때문에 지속해서 미분이 가능하다. 이는 효과적인 최적화와 일반화를 하는 데 도움이 된다. 그러나 ReLU, Swish와 비교하여 계산비용이 더 많이 필요해서 학습 시 세대(Epoch) 당 더 많은 시간이 소요된다.

4. 실험

실험에서 학습은 초해상화에서 보편적으로 사용되는 DIV2K[2] 데이터집합을 공통으로 사용하여, EDSR 모델의 활성화함수를 ReLU, Leaky ReLU, Swish, Mish로 변경하면서 각각 학습시켰다. 이때 EDSR 모델은 해상도를 2배로 변환하는 경우와 4배로 변환하는 경우를 각각 학습시켰다. 학습을 시킬 때 활성화함수 이외의 다른 매개 변수들은 기존의 EDSR 모델과 동일하게 학습을 진행하였다. Leaky ReLU의 α 값은 0.01로 설정하여 학습을 진행하였다.

테스트는 EDSR 모델을 초해상화 모델에서 보편적으로 사용되는 총 5가지 데이터집합(DIV2K[3], SET5[10], SET14[11], B100[12], Urban100[13])을 사용해 진행하였다. 성능 지표로 영상 또는 동영상 손실 압축에서 화질 손실 정보를 평가할 때 사용되는 PSNR과 영상 품질을 측정하기 위한 구조적 유사도 지수를 구할 때 사용되는 SSIM을 사용하였다.

<표 1>은 5가지의 데이터집합 별로 해상도를 2배로 변환하는 경우와 해상도를 4배로 변환하는 경우의 활성화함수에 따른 성능을 비교한 결과이다. EDSR에서 기존에 활성화함수로 사용하던 ReLU를 기준으로 하

였다.

결과를 보면 해상도를 2배로 변환하는 경우, 기존 EDSR 모델의 활성화함수로 사용되던 ReLU가 실험에 사용된 다른 활성화함수들 보다 비슷하거나 높은 성능을 보인다. ReLU를 기준으로 PSNR과 SSIM이 평균적으로, Leaky ReLU는 8.50%, 3.58% 낮았고, Swish는 0.23%, 0.06% 낮았으며, Mish는 0.23%, 0.07% 낮았다. 종합적으로는 ReLU가 비교에 사용된 다른 활성화함수들보다 PSNR과 SSIM에서 평균적으로 약 2.99%, 1.24% 정도 성능이 높은 것을 알 수 있었다.

해상도를 4배로 변환하는 경우에는 Leaky ReLU와 Swish가 기존에 사용되던 ReLU보다 약간 더 높은 성능을 보인다. ReLU를 기준으로 PSNR과 SSIM이 평균적으로, Leaky ReLU는 0.06%, 0.05% 높았고, Swish는 0.06%, 0.03% 높았으며, Mish는 0.14%, 0.17% 낮았다.

결과적으로 해상도를 2배로 변환하는 경우, ReLU가 가장 성능이 좋았던 결과를 보였으며, ReLU의 음수 영역을 0으로 만드는 특성이 다른 초해상화 모델보다 상대적으로 층수가 깊고 채널이 많은 EDSR 모델에 규제효과로 작용하여 가장 좋은 성능을 보인 것으로 해석된다. 이에 비해 해상도를 4배로 변환하는 경우는 해상도가 4배로 커지는 만큼 저해상도 영상과 변환된 고해상도 영상 간의 사상(Mapping) 관계가 복잡하다. 따라서 Leaky ReLU와 Swish가 ReLU보다 약간 향상된 성능을 보인 결과는 해상도를 4배로 변환하는 경우에 사상 관계의 복잡성에 대응하는 모델의 용량이 상대적으로 적절해져 음수 영역을 0으로 만드는 ReLU의 규제효과가 큰 의미를 가지지 못한 것으로 판단된다. 이러한 이유로 Leaky ReLU와 Swish가 ReLU보다 성능이 다소 향상된 것으로 해석된다. <표 1>에서 볼 수 있듯이 음수 영역을 0으로

만들지 않고 값을 어느 정도 유지하는 특성을 가진 Leaky ReLU 가 해상도를 2 배로 변환하는 경우, ReLU 에 대비해 성능이 크게 하락하였지만, 해상도를 4 배로 변환하는 경우에는 오히려 ReLU 보다 성능이 다소 향상된 결과가 이러한 해석을 뒷받침한다.

5. 결론

본 논문에서는 초해상화 과업에서 좋은 성능을 보인 EDSR 모델과 ReLU 를 대체하기 위해 제안된 활성화함수인 Leaky ReLU, Swish, Mish 를 비교분석 하였다. 실제 5 가지 데이터집합을 사용하여 각 활성화 함수에 따른 EDSR 모델의 성능을 정량화 하였다. 해상도를 2 배로 변환하는 경우, 기존에 사용하던 ReLU 가 가장 성능이 좋았지만, 해상도를 4 배로 변환하는 경우에는 Leaky ReLU 와 Swish 가 ReLU 보다 다소 향상된 성능을 보임을 확인하였다.

본 연구에서 해상도를 4 배로 변환하는 EDSR 모델에서 Leaky ReLU 와 Swish 가 ReLU 에 대비해 다소 향상된 성능을 보였기 때문에, 향후 연구에서는 ReLU 를 활성화함수로 사용하는 다른 초해상화 모델에 활성화 함수를 Leaky ReLU 나 Swish 로 대체하는 비교실험을 수행하는 것도 필요하다고 판단된다.

사사

이 성과는 2020 년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원과 과학기술정보통신부 및 정보통신기획 평가원의 SW 중심대학지원사업으로 수행된 연구임 (No. NRF2018R1C1B5086441)

참고문헌

- [1] Saeed Anwar, Salman Khan, and Nick Barnes, "A Deep Journey into Super-resolution: A Survey", arXiv:1904.07523, 1, 2019.
- [2] B. Lim, S. Son, H. Kim, S. Nah, and K.M. Lee, "Enhanced Deep Residual Networks for Single Image Super-Resolution", In CVPR Workshops, 2017, 1.
- [3] R. Timofte, E. Agustsson, L. Van Gool, M.-H. Yang, L.Zhang, et al, "Ntire 2017 challenge on single image super-resolution: Methods and results", In CVPR Workshops, 2017, 1,2,4,6,7,8.
- [4] C. Ledig, L. Thesis, F. Huszar, J. Caballero, A. Cunningham, A. Acosta, A. Aitken, A. Tejani, J. Totz, Z. Wang, et al, "Photo-realistic single image super-resolution using a generative adversarial network", arXiv:1609.040802, 1,2,3,4,5,6,7, 2017.
- [5] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition", In CVPR, 2016, 3.
- [6] Nair, Vinod and Hinton, Geoffrey E, "Rectified linear units improve restricted Boltzmann machines", In ICML, 2010, pp. 807-814.
- [7] Bing Xu, Naiyan Wang, Tianqi Chen, Mu Li, "Empirical Evaluation of Rectified Activations in Convolutional Network", arXiv:1505.00853, 1, 2015.
- [8] Prajit Ramachandran, Barret Zoph, and Quoc V. Le, "Swish: a self-gated activation function", arXiv:1710.05941 7, 1, 2017.
- [9] Diganta Misra, "Mish: A Self Regularized Non-Monotonic Neural Activation Function", arXiv:1908.08681, 1, 2019.
- [10] M. Bevilacqua, A. Roumy, C. Guillemot, and M. L. Alberti-Morel, "Low-complexity single-image super-resolution based on nonnegative neighbor embedding", In BMVC, 2012, 2,4.
- [11] R. Zeyde, M. Elad, and M. Protter, "On single image scale-up using sparse-representations", In Proceedings of the International Conference on Curves and Surfaces, 2010, 2,4.
- [12] D. Martin, C. Fowlkes, D. Tal, and J. Malik, "A database of human segmented natural images and its application to evaluating segmentation algorithms and measuring ecological statistics.", In ICCV, 2001, 4.
- [13] J.-B. Huang, A. Singh, and N. Ahuja, "Single image super-resolution from transformed self-exemplars.", In CVPR, 2015, 2,4,6.

기상 인자와 대기오염 인자를 활용한 LSTM 기반의 미세먼지 농도 예측

유지훈*, 신동일*, 신동규*

*세종대학교 컴퓨터공학과

yoojihoon@sju.ac.kr, dshin@sejong.ac.kr, shindk@sejong.ac.kr

LSTM-based Fine Dust Concentration Prediction using Meteorological factors and Air Pollution factors

Jihoon Yoo*, Dongil Shin*, Dongkyoo Shin*

*Dept. of Computer Engineering, Sejong University

요 약

미세먼지(PM10, PM2.5)는 배출가스 증가와 함께 빠르게 악화되어 왔으며, 다양한 화학성분 뿐만 아니라 금속 성분이 포함되어 있어 인체에 큰 유해성을 발생한다. 이에 정부는 미세먼지 저감 정책 및 법률을 통해 개선하고자 했지만, 2013년부터 그 효력을 잃기 시작하였다. 이에 본 연구에서는 미세먼지 저감 정책 및 법률을 수립하는데 있어 가장 중요한 요소인 미세먼지 농도를 예측하는 연구를 진행한다. 이전 연구들에서 미세먼지 영향 요소들이 시계열 기반의 데이터(기상인자와 대기오염 인자)인 것을 확인하였기에, 시계열 데이터에 좋은 성능을 보이는 LSTM 알고리즘을 사용하여 학습 후, 서울시 '구별' '시간단위' 미세먼지 농도 예측에 대한 예측 오차(RMSE, MAE)성능을 비교하였다. 실험 결과 PM10의 경우 (7.2, 4.78), PM2.5의 경우 (4.7, 3.2)의 예측 오차를 보였으며, 금천구의 경우 PM10이 (5.3, 3.71), PM2.5에서 (3.5, 2.5)로 가장 좋은 성능을 보였다.

1. 서론

대기오염 문제는 자동차 매연, 화석 연료 등과 같은 배출 가스 증가와 함께 빠르게 악화되기 시작했으며, 이중 입자의 직경이 $10\mu\text{m}$ 이하의 일반 미세먼지(PM10)와 $2.5\mu\text{m}$ 이하의 초미세먼지(PM2.5)는 1급 발암물질로 지정될 만큼 심각한 문제로 야기되었다.[1] 이러한 미세먼지는 다양한 화학성분 뿐만 아니라, 금속 성분이 포함되어 있기 때문에 인체의 호흡기나 심장 질환에 큰 유해성을 발생시킨다.[2, 3] 이에 정부는 미세먼지 저감 정책 및 법률과 같은 다양한 방법을 통해 미세먼지 오염도를 개선하였으나, 2013년부터 개선 추세가 정체되었고, 2016년에는 고농도 미세먼지가 자주 발생하여 현재까지 부정적인 영향을 끼치고 있다. 미세먼지가 다시금 사회적 관심과 문제를 야기하기 시작하면서 정부에서도 미세먼지 오염도 개선을 위한 정책 및 법률을 재수립하기 위해 준비하고 있다.[4] 이전과 같이 미세먼지 오염도의 개선 추세가 정체되는 것을 방지하기 위해 미세먼지 발생에 연관된 영향 인자와 농도에 대한 예측이 매우 중요해 지고 있다.

이에 본 연구에서는 국립환경과학원과 아테네 지역의 연구를 바탕으로 미세먼지 발생에 기상 인자와 대기오염 인자가 연관된 인자라는 것을 확인할 수 있었다.[5, 6] 두 가지 인자들은 시간에 따른 패턴을 가지는 시계열 기반의 데이터로 구성되기에, 시계열 기반의 데이터에 좋은 성능을 보이는 LSTM(Long Short Term Memory) 알고리즘을 통해서 미세먼지 예측을 모델링한다. 최종적으로 서울시 '구별' '시간단위'의 기상 및 대기오염 인자 데이터를 모델링된 LSTM을 통해 미세먼지 농도 예측에 대한 실험을 진행한다.

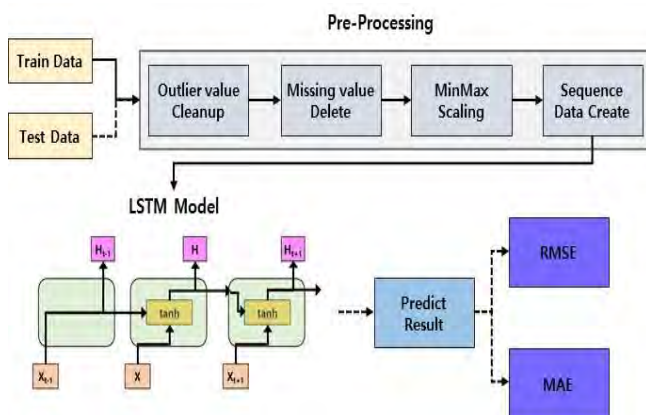
2. 최근 연구 동향

미세먼지 농도를 정확하게 예측하는 것이 중요해진 만큼 다양한 연구 방법을 통해 미세먼지를 예측하는 연구가 진행되어왔다. 이전에는 연구에서는 McKendry와 Zhao의 경우 다층신경망(Multi Layer Perceptron) 및 단일 회귀(Regression) 알고리즘들을 사용하여 단일 회귀 알고리즘이 더 좋은 성능을 보인다고 발표하였지만, 좋은 예측 성능을 보이지 못

하였다.[7, 8] 차진욱의 연구에서는 기상 인자와 대기 오염 데이터를 사용하여 ANN(Artificial Neural Network)과 KNN(K-Nearest Neighbor) 알고리즘을 응용하여 PM10에 대한 예측을 시도 하였으며, Yadav는 PCA(Principal Component Analysis)를 활용하여 최상의 예측 결과를 제공하는 입력 변수 조합을 ANN 알고리즘 학습에 사용하여 예측을 진행했다.[9, 10] 하지만 위의 모든 연구들은 시계열 데이터의 특성을 고려하지 않고 학습을 진행하여 좋은 예측 성능이 나오지 않았다. 이에 반해 데이터의 시계열 특성을 고려하는 LSTM 및 RNN과 같은 알고리즘을 통해 학습을 진행한 이홍석과 Di Antonio 연구에서는 미세먼지 예측에 대한 좋은 성능을 보인 것을 확인할 수 있었다.[11, 12]

3. LSTM 알고리즘 기반의 미세먼지 예측 모델

그림 1은 연구에서 제안하는 LSTM 모델의 학습 및 테스트에 대한 흐름을 보여준다.



(그림 1) LSTM 기반의 미세먼지 예측 모델

LSTM은 순환신경망(Recurrent Neural Network)의 한 종류로, 기존 순환신경망과 달리 신경망 내부에 input, forget output gate cell을 포함하고 있는 모델이다. 신경망 내부 메모리를 대체하는 cell을 통해, 긴 시퀀스 학습에 발생하는 타임스태프를 학습하지 못하는 기울기 소실 문제(Vanishing Gradient Problem) 또는 처음 입력된 데이터 학습이 제대로 반영되지 않는 장기 의존성 문제(Long-Term Dependencies)를 해결할 수 있는 시계열 데이터에 강한 모델이다.

3.1 데이터 세트

데이터는 ‘2015년 ~ 2019년 11월’까지의 서울시

‘구별’ ‘시간 단위’의 기상인자와 대기오염 인자로 구성된다. 기상 인자는 온도, 풍향과 같은 기상의 원인이 되는 5개의 속성을 사용하며, 빠른 시간 변화를 나타내는 요소에 대해 측정 순간의 값 혹은 측정 시간 평균값을 사용한다. 기상 인자 데이터는 “기상자료개발포털(<https://data.kma.go.kr/cmmn/main.do>)”에서 제공된다.

(표 1) 기상 인자 예시

날짜	기온	풍향	풍속	강수량	습도
15-01-01-01	-4.3	289.9	3.4	0.0	0.0
15-01-01-02	-10.1	341.8	5.3	0.0	48.2
...
19-11-30-24	3.8	78.4	0.7	0.0	71.0

대기오염 인자는 대기 오염 현상에 영향을 주는 물질들로, 발생원에 의해서 1차 오염물질과 상호 반응을 통해 생성되는 2차 대기오염 물질로 분류된다. 대기오염 인자 데이터는 6개의 속성으로 구성되며, 이중 PM10과 PM2.5는 예측 값으로 사용된다. 해당 데이터는 “에어코리아(www.airkorea.or.kr)”에서 제공된다.

(표 2) 대기오염 인자 예시

날짜	SO2	NO2	O3	CO	PM 10	PM 2.5
15-01-01-01	0.005	0.7	0.025	0.015	31	8
15-01-01-02	0.005	0.2	0.019	0.008	70	3
...
19-11-30-24	0.005	0.4	0.02	0.027	29	24

3.2 전처리 과정 (Pre-Processing)

전처리 과정은 그림 1의 Pre-Processing에서 제시되어 있으며, 모델 예측 성능에 부정적인 영향을 주는 요소를 제거 해주는 과정이다.

1. Outlier Cleanup : 2015, 2016년 몇몇 지역의 PM10 및 PM2.5의 수치가 900, 1000과 같이 특이값을 해당 지역의 정상적인 가장 큰 PM10, PM2.5의 수치로 변경한다.
2. Missing Value Deletes : 데이터 구조에서 각각의 속성에 대한 Null Value를 제거하는 단계이다. 2019년 데이터 세트의 ‘습도’ 속성은 대다수의 지역에서 데이터가 Null Value로 되어 있어 속성 자체를 제거하였다. 또한 PM10 및 PM2.5의 Null Value의 경우 예측 값(Target Value) 이므로, Null Value를 다른 값으로 채우기 보다는 row를

제거하는 방법을 사용하였다.

3. MinMax Scaling : 데이터들의 간의 분포 차이가 큰 경우 학습에 부하가 가는 것을 방지하기 위해서 예측 값(다음 시간 PM10, PM2.5)을 제외한 모든 데이터에 대해 MinMax Scaler를 사용해 0~1 사이 값으로 데이터의 범위를 일치시킨다.
4. Sequence Data Create : LSTM 알고리즘은 시퀀스 데이터를 모델의 입력으로 사용하기 때문에, 사용되는 데이터 세트를 LSTM 입력에 가능한 포맷으로 재구성해야한다. 본 연구에서는 Pandas Library의 Shift() 함수를 사용하여, 미세먼지 농도가 예측 되는 시점(t+1)을 기준으로 모델의 시퀀스 길이만큼 이전 시간(t-i)과 현재 시간(t)의 미세먼지 농도, 대기오염 인자 및 기상 인자가 시퀀스로 연속되는 형태로 구성된다.

$$X_{Seq} = \{(X_{1(t-i)}, Y_{1(t-i)}, X_{1(t_i)}, Y_{1(t_i)}), \\ \dots (X_{i(t-1)}, Y_{i(t-1)}, X_{i(t)}, Y_{i(t)})\}$$

$$Y_{pm10} = \{Y_{1(t+1)}, Y_{2(t+1)}, \dots Y_{i(t+1)}\}$$

$$Y_{pm2.5} = \{Y_{1(t+1)}, Y_{2(t+1)}, \dots Y_{i(t+1)}\}$$

$X = \{\text{기상 인자, 대기오염 인자}\}$, $t = \text{현재 시간}$
 $i = \text{시퀀스 길이 } t-i : \text{시퀀스 길이 만큼 이전 시간}$
 $Y = \{pm10 \text{ or } pm2.5\}$

(그림 2) 시퀀스 데이터 구성

4. 실험 및 평가

제안된 모델의 실험 환경은 표 4와 같으며, 전체 데이터 중에서 2015년 1월 1일 1시부터 2018년 12월 31일 24시까지 데이터는 학습을 위한 데이터로 2019년 1월 1일 1시부터 2019년 11월 30일 24시까지 데이터는 모델의 예측 성능을 테스트하기 위한 데이터로 사용한다. 모델 학습에 사용되는 파라미터는 표 5에 제시되어있으며, 모델의 성능 평가는 다음 시간(t+1)에 대한 두 개의 미세먼지 농도(PM10, PM2.5)에 대한 예측 오차를 통해 확인한다.

(표 4) 실험 환경

구분	이름
Language	Python
	Tensorflow 2.1.0
Library	Keras 2.2.4-tf
	Scikitlearn 0.22.1
GPU	Nvidia Geforce RTX 2070 Super
Memory	64GB

(표 5) 예측 모델 Hyperparameter

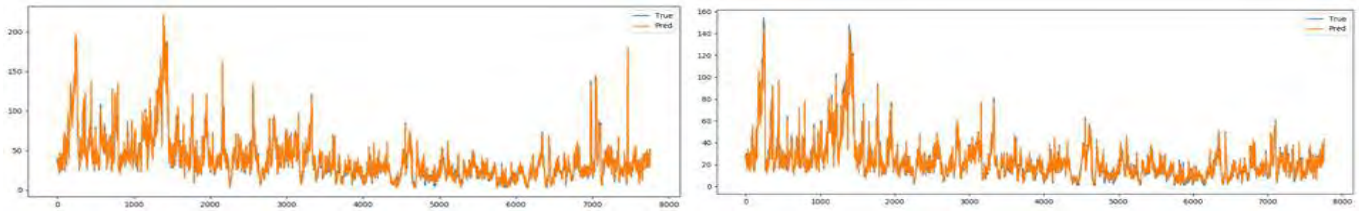
Parameter	Value
epoch	50
batch_size	32
Hidden Layer	256
Optimizer	Adam
learning rate	0.001
Sequence Length	1

예측 오차를 구하기 위해서, RMSE(Root Mean Square Error) 및 MAE(Mean Absoul Error)를 통해 실제 값과 예측 값의 차이를 계산한다. 실험 결과는 표 6에 제시되어 있으며, 대부분의 지역에서 낮은 수치의 예측 오차(RMSE, MAE)가 계산된 것을 확인할 수 있었다. 하지만 지역별 예측 오차의 값의 차이가 생각보다 높은 것을 볼 수 있는데, 전처리의 Missing Value Delete 단계에서 지역별로 삭제된 데이터양이 다른 것이 원인이라 생각된다.

(표 6) 구별 RMSE, MAE 성능 지표

서울시 구	RMSE		MAE	
	PM10	PM2.5	PM10	PM2.5
중구	5.7	3.75	3.7	2.5
용산구	5.9	4.4	3.9	2.9
광진구	7.9	5.4	5.2	3.7
성동구	8.5	5.5	5.9	3.8
중랑구	6.4	4.3	4.3	2.9
동대문구	6.5	4.4	4.2	2.8
성북구	8.0	5.2	5.4	3.7
도봉구	7.3	4.9	5.0	3.3
은평구	7.9	4.7	5.2	3.2
서대문구	7.7	5.07	5.0	3.3
마포구	8.3	5.59	5.4	3.7
강서구	7.4	4.51	4.9	3.08
구로구	8.2	5.63	5.3	3.7
영등포구	8.07	6.04	5.3	4.08
동작구	6.4	4.25	4.0	2.8
관악구	8.6	6.04	5.8	4.2
강남구	6.4	4.63	4.2	3.1
서초구	8.8	5.26	5.6	3.4
송파구	7.4	4.93	5.2	3.4
강동구	6.6	4.12	4.2	2.8
금천구	5.3	3.71	3.5	2.5
강북구	7.6	4.3	4.9	2.9
양천구	6.9	4.1	4.4	2.8
노원구	5.7	4.2	3.7	2.9
평균	7.2	4.78	4.7	3.2

가장 예측 성능이 좋은 곳은 금천구로 PM10(5.3, 3.71) 및 PM2.5(3.5, 2.5) 속성 모두 가장 낮은 예측 오차를 보였으며, 이에 대한 예측 그래프 그림 3을 통해 실제 미세먼지 농도와 예측 값이 매우 근사한



(그림 3) 금천구 미세먼지 예측 그래프 PM10(좌), PM2.5(우)

것을 확인할 수 있다. 하지만 PM10의 경우 미세먼지 농도가 200 μm 이상인 경우, 과대 예측되는 성향을 보인다.

5. 결론

본 연구에서는 미세먼지 농도를 예측을 위해 시계열 데이터에 좋은 성능을 보이는 LSTM 알고리즘을 사용하여 미세먼지 농도 예측을 평가 했다. 데이터는 이전 연구를 분석을 통해 기상 인자와 대기오염 인자를 활용하였으며, 4단계의 전처리 과정을 통해 학습과 테스트에 사용할 데이터를 정리하였다. 학습된 모델에 RMSE 및 MAE를 사용하여 미세먼지 농도의 예측 오차를 계산한 결과 평균적으로 PM10의 경우 '7.2, 4.78', PM2.5의 경우 '4.7, 3.2'의 예측 오차를 보였으며, 금천구의 경우 PM10이 '5.3, 3.71' PM2.5이 '3.5, 2.5'로 가장 좋은 성능을 보였다. 하지만 PM10의 경우 200이상일 경우 과대 예측하는 현상을 보였으며, '시간 단위'로 구성된 데이터의 Null Value가 많아 지역별로 예측 오차 값의 차이가 발생되었다. 추후 시간별 데이터와 일치하는 일별 평균값으로 Null Value를 대체하여 실험해보는 방법과 통계 모델인 ARIMA, VAR과 같은 방법의 예측 성능을 비교해보는 연구를 계획하고 있다.

Acknowledgement

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (2018R1D1A1B07050633)

참고문헌

- [1] 우정현. "수도권 미세먼지 환경 개선을 위한 미국의 대기환경정책 사례 조사 연구." 한국대기환경학회지 (국문) 25.6 (2009): 579-593.
- [2] 최종규, et al. "미세먼지의 질병에 미치는 유해성." 생명과학회지 30.2 (2020): 191-201.
- [3] Jaafari, Jalil, et al. "Characterization, risk

assessment and potential source identification of PM10 in Tehran." Microchemical Journal 154 (2020): 104533.

[4] 김봉균, et al. "미세먼지 저감을 위한 정책 선정 연구." 한국전자거래학회지 25.1 (2020): 109-121.

[5] 공부주, 한진석, 이민도, 이정영, 박진수, "기상인자가 미세먼지 농도에 미치는 영향 연구", 국립환경과학원, pp. 1-137, 2006.

[6] Abatzoglou, G., Chaloulakou, A., Assimacopoulos, D., Lekkas, T, "Prediction of air pollution episodes: Extreme value theory applied in Athens," Environmental technology, vol.17, NO.4, pp349-359, 1996.

[7] Pires, J. C. M., Martins, F. G., Sousa, S. I. V., Ferraz, M. C. M. A., & Pereira, M. C., "Prediction of the daily mean PM10 concentrations using linear models," American Journal of Environmental Sciences, vol.4, no.5, pp.445-453, 2008.

[8] Zhao, Yin, "Machine learning algorithms for predicting roadside fine particulate matter concentration level in Hong Kong Central,"

[9] 차진욱, and 김장영. "미세먼지 수치 예측 모델 구현을 위한 데이터마이닝 알고리즘 개발." 한국정보통신학회논문지 22.4 (2018): 595-601.

[10] Yadav, V., and S. Nath. "Novel hybrid model for daily prediction of PM 10 using principal component analysis and artificial neural network." International Journal of Environmental Science and Technology 16.6 (2019): 2839-2848.

[11] 이홍석, et al. "도심지 교통흐름 및 미세먼지 예측을 위한 딥러닝 LSTM 프레임워크." 정보과학회논문지 47.3 (2020): 292-297.

[12] Di Antonio, Ludovico, et al. "Multivariate Prediction of PM 10 Concentration by LSTM Neural Networks." 2019 Photonics & Electromagnetics Research Symposium-Fall (PIERS-Fall). IEEE, 2019.

사전 지식에 의한 강화학습 에이전트의 학습 속도와 경향성 변화

김지수*, 이은현*, 김현철*

*고려대학교 컴퓨터학과

gameboyjisoo@korea.ac.kr, booksky@korea.ac.kr, harrykim@korea.ac.kr

How the Learning Speed and Tendency of Reinforcement Learning Agents Change with Prior Knowledge

Jisoo Kim*, Eun Hun Lee*, Hyeoncheol Kim*

*Dept. of Computer Science and Engineering, Korea University

요 약

학습 속도가 느린 강화학습을 범용적으로 활용할 수 있도록 연구가 활발하게 이루어지고 있다. 사전 지식을 제공해서 학습 속도를 높일 수 있지만, 잘못된 사전 지식을 제공했을 위험이 존재한다. 본 연구는 불확실하거나 잘못된 사전 지식이 학습에 어떤 영향을 미치는지 살펴본다. OpenAI Gym 라이브러리를 이용해서 만든 Gamble 환경, Cliff 환경, 그리고 Maze 환경에서 실험을 진행했다. 그 결과 사전 지식을 통해 에이전트의 행동에 경향성을 부여할 수 있다는 것을 확인했다. 또한, 경로 탐색에 있어서 잘못된 사전 지식이 얼마나 학습을 방해하는지 알아보았다.

키워드: 기계학습, 강화학습, 사전 지식, Q-learning, 강화 학습 에이전트

1. 서론

기계학습의 분야 중 하나인 강화학습은 trial-and-error 방식으로 주어진 환경(environment)에서 보상에 도달하는 정책(policy)을 배우는 알고리즘이다. 강화학습에서는 행동의 주체가 되는 에이전트(agent)가 가능한 행동(action) 중 한 개를 계속 선택해서 최종적으로 목표에 도달하는 것을 목표로 삼는다[1]. 단계적으로 문제를 푸는 이 방식은 현존하는 방식 중 사람의 문제풀이 방식과 가장 유사하다는 특징이 있다[2].

그러나 강화학습은 복잡한 환경에서 많은 학습시간이 필요하다는 단점을 가지고 있다[3]. 이를 해결하는 방법 중 하나가 에이전트에게 사전 지식(prior knowledge)을 알려주는 것이다[4]. Q-learning[5]을 쓰는 로봇에게 사전 지식을 알려주었을 때가 백지상태(tabula rasa)에서 학습하는 것보다 더 빠르게 학습하고 좋은 성과를 나타낸 사례가 있다[6][7]. 또한, 사람이 보여주는 선례를 모방하여 학습하는 에이전트도 좋은 결과를 보여준 적이 있다[8]. 그러나 이런 방법이 성공할 수 있었던 이유는 해당 문제에 대해 정답에 해당하는 지식을 제공할 수 있었기 때문이다[9]. 정답이 명확하지 않은 문제에 대해서는 인공지능에게 잘못된 지식을 전달할 수 있으며, 그것이 잘못된 행동으로

이어질 수도 있다[10][11]. 그렇기 때문에 이런 잠재적 위험이 어떤 경우에 발생할 수 있는지 살펴볼 필요가 있다.

이에 본 연구는 Q-learning 을 쓰는 3 가지 환경에서 이런 사전 지식의 영향력을 확인한다. 2 개의 경로 탐색 환경에서는 탐색을 방해하는 사전 지식과 차선책을 지향하는 사전 지식이 최종 경로 결정에 어떤 영향을 미치는지 본다. 도박 환경에서는 안정성 혹은 도박성을 추구하는 사전 지식의 강도에 따라서 어떻게 행동이 바뀌는지 확인한다.

본 연구의 2 장에는 관련 연구에 대해서 서술했다. 3 장에는 구축한 환경에 대한 세부 정보를 기술했으며, 4 장에는 각 환경에서 진행한 실험에 대해 설명하고 실험 결과를 분석했다. 결론에는 본 연구를 통해 얻은 결과 및 연구의 한계에 대해서 서술했다.

2. 관련 연구와 비교

Q-learning 에 사전 지식은 실험 시작 전부터 알고 있는 지식이며, 이런 사전 지식을 적용해서 학습 속도와 성능을 높인 연구가 있다. 그 중 Dixon[6]은 부분적인 사전 지식이 학습을 얼마나 돕는지 확인했다. 벽을 끼고 이동하는 로봇이 가장 혼한 12 개의 상태에 대한 정답을 알면 얼마나 더 빠르게 학습하는지

봤다. 그 결과 일부 상황에만 적용한 사전 지식이 학습 속도를 7.5 배까지 높일 수 있다는 것을 확인했다.

Moreno[7]는 복잡한 환경을 단계별로 나눠서, 술래잡기 환경에서 플레이어가 술래를 피해서 목표 지점에 도달하도록 학습시켰다. 처음에는 목표 지점만 존재하는 환경에서 학습시켰으며, 환경에 익숙해지면 술래와 플레이어 한 명을 차례대로 추가해서 학습시켰다. 그 결과 사전 지식을 쓴 플레이어의 승률이 약 2 배 높였으며, 학습 시간 또한 절반 이하로 줄었다.

두 연구를 통해서 사전 지식으로 정답을 찾을 때 학습 시간을 줄이고 성능을 높일 수 있다는 것을 확인했다. Dixon 은 사람이 제공하는 사전 지식의 효과를 확인했으며, 같은 문제를 다른 환경에서 풀 때도 범용적인 사전 지식이 쓰일 수 있다는 것을 알게 되었다. Moreno 는 일부 상황에 대한 정답을 배우면, 그것을 기반으로 더 복잡한 상황을 빠르게 학습할 수 있다는 것을 확인했다. 강화학습 에이전트도 단계별로 문제를 나눠서 풀 수 있다는 것을 검증했다.

그러나 Dixon, Moreno 모두 사전 지식으로 정답을 주는 경우에 대해서만 확인했다. 때로는 사람이 알고 있는 사전 지식이 잘못됐을 수도 있으며, 학습에 도움이 안되는 문제의 일부를 먼저 학습시킬 수 있다. 또한, 정답이 없는 문제에 대해서 확인하지 않았다. 그렇기에 본 연구는 잘못되거나 경향성을 주는 사전 지식이 어떻게 학습에 영향을 주는지 확인한다.

3. 환경 소개

오픈소스 라이브러리인 OpenAI Gym[12]의 Kelly Coinflip, Cliff, Frozen Lake 환경을 참고해서 최종적으로 Gamble, Cliff, Maze 환경을 만들었다. 모든 환경에서 처음에는 탐험을 우선시할 수 있도록 무작위성을 어느 정도 부여하고, 학습이 진행되면서 무작위 행동을 취할 확률을 점차 감소시켰다. 또한 모든 환경에서 할인계수(discount rate)는 0.97, 학습률(learning rate)은 0.01 로 고정했다.

경로 탐색 환경에서는 목표 지점까지 가는 최적 경로를 찾을 수 있도록 이동에 대한 부정적인 보상을 적용했다. 한 번 행동을 취할 때 보상을 -1 로 지정함으로써 에이전트가 효율적으로 이동하도록 유도했다.

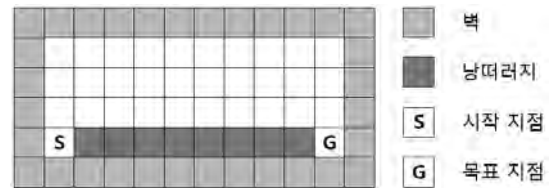
3.1 Gamble 환경

Gamble 환경에서는 동전 뒤집기로 도박하면서 최대 돈을 모아야 한다. 보유한 자산의 일정 비율을 베팅하고, 앞면이 나오면 베팅 금액만큼 얻고 뒷면이 나오면 베팅 금액만큼 잃는다. 한 학습 회차는 총 10 라운드 동안 진행되며, 그 전에 돈을 다 잃거나 최대 금액까지 벌면 회차가 종료된다. 초기 자금은 20 원, 동전 앞면 확률은 0.62, 최대 금액은 150 원으로 책정했다. 그 이유는 해당 초기값으로 했을 때, 에이전트의 성향이 조금씩 다르게 나왔으며, 사전 지식으로 행동이 어떻게 변하는지 알아볼 수 있었기 때문이다.

현재 보유 금액을 5 로 나눈 것(나머지는 버린다)이 에이전트의 상태가 되고, 보유 금액에 따라서 총 30 개의 상태가 존재한다. 가능한 행동은 보유 자산의

10%, 20%, 40%, 60%를 도박하는 것으로 총 4 가지가 있다. 처음에 무작위 행동을 취할 확률을 100%로 설정했으며, decay rate 를 0.999 로 설정했다.

3.2 Cliff 환경

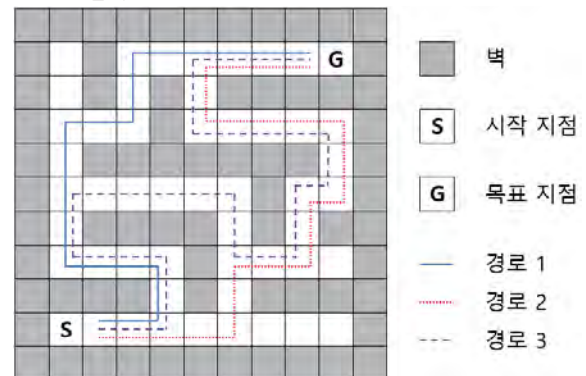


(그림 1) Cliff 환경

낭떠러지를 피해서 목표 지점으로 가는 경로 탐색 환경이다(그림 1). 목표 지점에 도달하면 +30 보상을 얻고, 낭떠러지에서 떨어지면 -30 보상을 얻으면서 학습 회차가 종료된다. 제자리걸음을 방지하기 위해서 벽에 부딪히면 -10 의 보상을 얻게 했다.

에이전트의 위치가 현재의 상태이며, 총 72 개의 상태가 존재한다. 그 중 28 개는 벽이며 실제로 사용하는 상태는 44 개다. 가능한 행동은 상하좌우 이동 네 가지다. 처음에 무작위 행동을 취할 확률을 60%로 설정했으며, decay rate 를 0.99 로 설정했다.

3.3 Maze 환경



(그림 2) Maze 환경

Cliff 환경과 같이 경로 탐색 환경이다 (그림 2). 목표 지점에 도달하면 +30 보상을 얻고, 제자리걸음을 방지하기 위해서 벽에 부딪히면 -20 의 보상을 얻는다.

경로 1 은 최적 경로로 22 번의 행동 후에 목표 지점에 도달하며, 경로 2, 3 은 각각 24 번, 34 번 만에 목표 지점에 도달한다.

에이전트의 위치가 현재의 상태이며, 총 121 개의 상태가 존재한다. 그 중 70 개는 벽이며 실제로 사용하는 상태는 51 개다. 가능한 행동은 상하좌우 이동 네 가지다. 처음에 무작위 행동을 취할 확률을 10%로 설정했으며, decay rate 를 0.99 로 설정했다.

4. 실험 및 실험 결과

사전 지식이 에이전트에 미치는 영향을 보기 위해서 최적화를 돕는 사전 지식, 최적화를 방해하는 사전 지식, 차선책으로 유도하는 사전 지식, 그리고 경향성을 부여하는 사전 지식을 점차 적용해봤다.

<표 1> Gamble 환경에서의 각 베팅 비율에 대한 사전 지식 적용 결과

	사전 지식 無		10% 베팅 유도		20% 베팅 유도		40% 베팅 유도		60% 베팅 유도	
사전 지식	평균	표준 편차	평균	표준 편차	평균	표준 편차	평균	표준 편차	평균	표준 편차
0.2	389.7	121.27	327.65	113.35	400.65	149.68	374	129.54	355.3	105.70
0.4			306.75	98.12	355.15	133.68	372.45	152.95	434.75	149.05
0.6			286.55	97.50	342.25	128.98	423.75	141.79	457.9	148.20
0.8			277.45	107.23	351.85	100.52	358.5	123.64	440.25	211.78
1.0			265.95	66.13	320.55	91.16	426.35	139.19	455.75	172.02

원래 모든 값이 0 으로 시작하는 Q-table 의 일정 구간에 양수값, 음수값을 적용하는 방식으로 실험에서 사전 지식을 부여했다.

4.1 Gamble 환경

총 300 번 학습시킨 후 생성된 Q-table 을 기반으로 게임을 플레이하도록 했다. 모든 테스트는 플레이 20 회로 진행됐으며, 평균과 표준편차를 비교했다.

사전 지식이 없을 때, Q 값이 약 0.2~5 사이에 머물렀다. 또한 평균 389.7 원을 모은 상태로 게임이 종료되었으며, 게임 간의 표준편차는 약 121.27 이었다.

사전 지식의 정도에 따라서 에이전트의 행동이 어떻게 바뀌는지 살펴보았다. 돌아가면서 한 행동에 대해 0.2, 0.4, 0.6, 0.8, 1.0 의 Q 값을 적용했다. 경향성의 변화를 나타낸 결과는 표 1 과 그림 3 에 나타냈으며, 소수점 아래 2 자리까지 반올림했다.

사전 지식 無					10% 베팅 사전 지식 1.0					60% 베팅 사전 지식 1.0				
10% 베팅	20% 베팅	40% 베팅	60% 베팅	10% 베팅	20% 베팅	40% 베팅	60% 베팅	10% 베팅	20% 베팅	40% 베팅	60% 베팅	10% 베팅	20% 베팅	40% 베팅
0.23	0.24	0.26	0.28	0.39	0.19	0.21	0.21	0.19	0.18	0.20	0.43	0.19	0.18	0.20
0.20	0.26	0.26	0.28	0.35	0.20	0.22	0.23	0.17	0.20	0.22	0.41	0.17	0.20	0.22
0.23	0.24	0.25	0.28	0.43	0.18	0.21	0.17	0.18	0.19	0.22	0.41	0.18	0.19	0.22
0.23	0.20	0.26	0.31	0.36	0.20	0.20	0.23	0.19	0.17	0.16	0.49	0.19	0.17	0.16
0.23	0.24	0.28	0.25	0.32	0.21	0.21	0.25	0.22	0.21	0.23	0.35	0.22	0.21	0.23
0.25	0.22	0.28	0.25	0.39	0.15	0.22	0.24	0.13	0.18	0.24	0.45	0.13	0.18	0.24
0.23	0.29	0.24	0.24	0.41	0.16	0.26	0.18	0.19	0.17	0.20	0.44	0.19	0.17	0.20
0.24	0.22	0.24	0.30	0.47	0.18	0.22	0.13	0.15	0.21	0.16	0.48	0.15	0.21	0.16
0.25	0.19	0.32	0.25	0.52	0.18	0.17	0.13	0.17	0.22	0.21	0.40	0.17	0.22	0.21
0.24	0.24	0.28	0.23	0.51	0.14	0.20	0.16	0.20	0.19	0.16	0.44	0.20	0.19	0.16
0.28	0.29	0.19	0.25	0.39	0.18	0.16	0.27	0.20	0.11	0.18	0.52	0.20	0.11	0.18
0.31	0.24	0.21	0.25	0.50	0.17	0.16	0.17	0.19	0.18	0.22	0.41	0.19	0.18	0.22
0.28	0.16	0.23	0.34	0.46	0.16	0.21	0.17	0.11	0.17	0.21	0.51	0.11	0.17	0.21
0.37	0.21	0.17	0.25	0.42	0.22	0.18	0.19	0.15	0.18	0.21	0.46	0.15	0.18	0.21
0.19	0.19	0.34	0.28	0.46	0.12	0.26	0.15	0.15	0.19	0.22	0.44	0.15	0.19	0.22
0.26	0.29	0.27	0.18	0.46	0.12	0.15	0.28	0.13	0.13	0.14	0.60	0.13	0.13	0.14
0.22	0.19	0.30	0.28	0.47	0.18	0.16	0.19	0.24	0.15	0.21	0.40	0.24	0.15	0.21
0.25	0.26	0.31	0.18	0.45	0.17	0.10	0.28	0.19	0.11	0.21	0.48	0.19	0.11	0.21
0.31	0.21	0.17	0.32	0.45	0.18	0.19	0.18	0.10	0.13	0.19	0.58	0.10	0.13	0.19
0.07	0.10	0.10	0.73	0.21	0.10	0.09	0.60	0.05	0.02	0.08	0.85	0.05	0.02	0.08
0.13	0.14	0.18	0.55	0.32	0.12	0.07	0.49	0.13	0.13	0.08	0.66	0.13	0.13	0.08
0.16	0.11	0.32	0.42	0.27	0.13	0.18	0.42	0.07	0.14	0.23	0.55	0.07	0.14	0.23
0.11	0.14	0.27	0.48	0.33	0.07	0.29	0.31	0.09	0.05	0.32	0.54	0.09	0.05	0.32
0.14	0.11	0.44	0.31	0.24	0.09	0.40	0.28	0.04	0.13	0.27	0.56	0.04	0.13	0.27
0.16	0.10	0.49	0.25	0.24	0.09	0.27	0.40	0.14	0.10	0.29	0.47	0.14	0.10	0.29
0.18	0.28	0.26	0.29	0.18	0.19	0.29	0.34	0.08	0.28	0.24	0.40	0.08	0.28	0.24
0.10	0.32	0.31	0.26	0.30	0.16	0.24	0.30	0.09	0.32	0.12	0.47	0.09	0.32	0.12
0.28	0.24	0.24	0.23	0.41	0.24	0.22	0.14	0.16	0.20	0.20	0.44	0.16	0.20	0.20
0.40	0.23	0.12	0.25	0.54	0.09	0.19	0.17	0.18	0.19	0.09	0.54	0.18	0.19	0.09
0.40	0.15	0.17	0.28	0.43	0.17	0.20	0.20	0.15	0.25	0.16	0.45	0.15	0.25	0.16
0.25	0.25	0.25	0.25	0.47	0.17	0.17	0.17	0.17	0.17	0.17	0.47	0.17	0.17	0.17

(그림 3) Gamble 환경에서 사전 지식으로 행동 선택에 변화를 대표적으로 나타낸 사례들의 히트맵

사전 지식을 강하게 부여하면 에이전트의 행동에 경향성을 부여할 수 있다는 것이 확인되었다. 특히 안전성을 추구하는 10% 베팅과 도박성을 추구하는 60% 베팅에 대한 사전 지식은 확실한 변화를 보여준다. 사전 지식을 강하게 적용했을 때는 거의 항상 해당 행동을 선택하는 것이 확인되었다.

안전성을 추구하는 사전 지식이 강하면 평균 총수익이 약 30%까지 줄지만, 표준편차는 절반까지 감소한다. 도박성을 추구하는 사전 지식이 강할수록 평균

총수익이 약 17% 늘지만, 표준편차도 2 배까지 는다.

4.2 Cliff 환경

처음으로 최적 경로를 찾는 학습 회차를 확인하는 실험을 진행했다. 모든 테스트는 플레이 20 회로 진행됐으며, 평균과 표준편차를 비교했다.

사전 지식이 없을 때, Q 값이 약 -9 에서 20 사이에 머물렀다. 목표 지점에 가까울수록 양수 값이 컸으며, 낭떠러지 직전에서 낭떠러지로 이동하는 행동에 대한 Q 값이 가장 낮았다. 평균적으로 300 번째 회차에 학습이 됐으며, 표준편차는 약 92.53 이었다.

긍정적, 부정적 사전 지식의 정도에 따라서 학습 속도가 얼마나 바뀌는지 살펴보았다. 낭떠러지로 떨어질 수 있는 8 개의 상태에 최적 경로를 가르치는 사전 지식(우측으로 이동)과 낭떠러지로 유도하는 사전 지식(아래로 이동)을 적용했다. 또한, 이 두 가지 중 한 가지에 양수의 Q 값을 적용하면, 다른 경우에 대해서 같은 Q 값을 음수로 적용했다.

여러 테스트를 해본 결과, 0.1~0.6 사이의 Q 값들이 가장 유의미한 결과를 나타냈기 때문에 해당 값으로 최종 실험을 진행했다. 최대 1000 번까지 학습을 할 수 있도록 설정했으며, 그때까지 학습이 안 되면 실패했다고 간주했다. 결과는 표 2 에 나타냈으며, 소수점 아래 2 자리까지 반올림했다.

<표 2> 최적 경로와 낭떠러지로 떨어지는 경로에 대한 사전 지식을 적용했을 때 학습 결과

사전 지식	최적 경로		낭떠러지		
	평균	표준 편차	평균	표준 편차	실패 횟수
0.1	148	155.18	339.1	92.92	0
0.2	46.25	115.57	339.15	78.83	0
0.3	21.7	54.14	364.2	83.78	0
0.4	9.85	6.51	358.05	77.15	0
0.5	9.8	4.88	406.38	84.06	7
0.6	8.05	4.70	439.44	111.86	11

최적 경로를 찾는데 도움이 되는 사전 지식의 경우, 적은 양을 부여하더라도 학습 속도를 크게 높일 수 있었다. 낭떠러지로 유도하는 사전 지식의 경우에도 적은 양으로도 학습 속도를 10%~20% 늦출 수 있었다. 또한, 잘못된 사전 지식이 너무 커지면 절반 이상의 경우에 학습 자체를 실패한다. 이를 통해 간단한 경로 탐색 환경에서 작은 양의 사전 지식도 큰 영향을 끼칠 수 있다는 것을 확인했다.

4.3 Maze 환경

3 개의 경로 중 한 경로로 학습을 유도하는 사전 지식을 부여했을 때 어떤 경로를 선택하는지 확인하는 실험을 진행했다. 학습과 테스트를 병행했으며, 총 3000 번 학습을 시키면서 한 경로만 계속 선택하게 되는 시점을 기록했다. 경로를 찾을 때 100 번 이상 행동을 취해도 목표 지점을 찾지 못하면, 다음 학습 회차로 넘어가도록 했다.

사전 지식 없이 5 회 테스트했을 때, 약 1780 회 학습을 진행하면 최적 경로를 확정적으로 찾기 시작했다. 이때 Q 값이 약 -10 에서 20 사이에 머물렀다. 양수 값은 목표 지점 근처라는 것을 고려하면, 중간 경로의 Q 값은 -10 까지 간다고 판단했다.

Q-learning 특성상 한 방향으로 이동하게 하기 위해서 나머지 세 방향에 음수인 Q 값을 적용했다. 그렇지 않으면, 사전 지식으로 부여한 양수의 Q 값이 나머지 3 방향과 같아질 때까지 반복적으로 사전 지식이 부여된 상태 내에서만 이동했기 때문이다.

경로 1, 2, 3 으로 유도하는 사전 지식을 적용하고 그 결과를 살펴보았다. 여러 테스트를 해본 결과, 1~30 사이의 Q 값들이 가장 유의미한 결과를 나타냈기 때문에 해당 값으로 최종 실험을 진행했다. 이때, 환경의 복잡도를 반영하여 부분적으로만 사전 지식을 적용했다. 경로 전체에 대해 사전 지식을 적용하지 않고 시작 지점부터 전체 경로의 약 3 분의 1 에 대해 사전 지식을 부여했다. 결과는 표 3 에 나타났다.

<표 3> 경로별로 사전 지식을 적용했을 때 학습을 마치는 학습 회차

사전 지식 無	사전 지식 有	경로 1	경로 2	경로 3
1783	1	1987	1818*	1846*
1791	5	2181	1605*	1733*
1777	10	1973	1985*	1532*
1780	20	1405	1593	2387
1799	30	1414	1570	2401

* 해당 경우에는 경로 1 로 학습이 마무리되었다.

극단적이지 않은 사전 지식도 학습에 도움을 준다는 보장이 없었다. 최적 경로인 경로 1 에 대해서 -10 이상의 사전 지식을 부여했을 때만 학습 속도가 빨라지는 것이 확인되었으며, 그보다 적은 사전 지식은 학습 속도를 높이지 못했다. 나머지 경로의 경우에도 Q-table 에 일반적으로 나타나는 값 이상으로 부여했을 때만 에이전트가 선택하는 최종 경로를 바꿀 수 있었다. 또한, 경로 3 의 경우에는 극단적인 사전 지식을 적용하더라도 더 많은 학습 회차가 필요했다.

이런 결과를 통해서 Q-learning 에서 사전 지식의 한계를 살펴볼 수 있었다. 경로가 길어질수록 목표 지점의 보상이 경로 전체에 적용될 때까지 많은 학습 회차가 필요하다. 또한, 사전 지식을 부여하는 방식 때문에 적은 사전 지식이 오히려 학습을 방해하는 효과를 가져왔다.

5. 결론

본 연구는 3 개의 환경에서 진행한 Q-learning 실험을 통해서 최적화되지 않은 사전 지식의 영향에 대해 살펴보았다. 그 결과 정답이 없는 환경에서 에이전트의 행동 경향을 성공적으로 바꿨다. 또한, 부여하는 사전 지식의 정도에 따라서 행동 경향을 더 많이 바꿀 수 있다는 것도 확인했다. 경로 탐색 환경의 경우, 사전 지식이 최적 경로 탐색을 방해하면, 학습이 느려지거나 실패할 수 있다는 것을 확인했다. 그리고 환경이 복잡해지면 극단적인 사전 지식을 부여해야지만 학습에 영향을 끼칠 수 있다는 것을 확인했다.

향후에는 Q-learning 외 다른 강화학습 기법에서 정답이 아닌 여러 종류의 사전 지식이 어떤 영향을 끼치는지 살펴볼 필요가 있다. 또한, 기존 연구에 쓰였던 주변 사물을 인식하는 관계적 상태 공간에서도 다른 종류의 사전 지식의 영향을 확인할 필요가 있다.

참고문헌

- [1] Kaelbling, L. P., Littman, M. L., & Moore, A. W. Reinforcement learning: A survey. Journal of artificial intelligence research, 4, 237-285. 1996.
- [2] Sutton, R. S. and Barto, A. G. Reinforcement Learning: An Introduction. MIT Press. 1998.
- [3] Driessens, K., & Džeroski, S. Integrating guidance into relational reinforcement learning. Machine Learning, 57(3), 271-304. 2004.
- [4] Smart, W. D., & Kaelbling, L. P. Practical reinforcement learning in continuous spaces. ICML. 2000. 903-910.
- [5] Watkins, C. J., & Dayan, P. Q-learning. Machine learning, 8(3-4), 279-292. 1992.
- [6] Dixon, K., Malak, R. J., & Khosla, P. K. Incorporating prior knowledge and previously learned information into reinforcement learning agents. Carnegie Mellon University, Institute for Complex Engineered Systems. 2000.
- [7] Moreno, D. L., Regueiro, C. V., Iglesias, R., & Barro, S. Using prior knowledge to improve reinforcement learning in mobile robotics. Proc. Towards Autonomous Robotics Systems. Univ. of Essex, UK. 2004.
- [8] Abbeel, Pieter, and Andrew Y. Ng. Exploration and apprenticeship learning in reinforcement learning. Proceedings of the 22nd international conference on Machine learning. 2005.
- [9] Argall, B. D., Chernova, S., Veloso, M., & Browning, B. A survey of robot learning from demonstration. Robotics and autonomous systems, 57(5), 469-483. 2009.
- [10] Amodei, D., Olah, C., Steinhardt, J., Christiano, P., Schulman, J., & Mané, D. Concrete problems in AI safety. arXiv preprint arXiv:1606.06565. 2016.
- [11] Everitt, T., Krakovna, V., Orseau, L., Hutter, M., & Legg, S. Reinforcement learning with a corrupted reward channel. arXiv preprint arXiv:1705.08417. 2017.
- [12] <https://gym.openai.com/>

딥러닝 기반 한국 표준 산업분류 자동분류 모델 비교

우찬균*, 임희석**

*고려대학교 컴퓨터정보통신대학원 빅데이터융합학과

**고려대학교 컴퓨터학과 교수

ckwoo@korea.ac.kr, limhseok@korea.ac.kr

Comparison of Korean Standard Industrial Classification Automatic Classification Model on Deep Learning

Chan Kyun Woo*, Heui Seok Lim**

*Dept. of Big Data Convergence, Korea University Graduate School of Computer and Information Technology

**Dept. of Computer Science and Engineering, Korea University

요 약

통계청에서는 지역별고용조사, 인구총조사 등 다양한 조사를 실시하고 있다. 이러한 조사에서는 응답자의 사업체명, 사업체가 주로 하는 일, 응답자가 한 일, 부서 및 직책 정보 등을 조사해서 조사되어진 자료를 토대로 한국 표준 산업분류 형태로 코드를 부여해 주고 있다. 각 조사에서는 자연어 형태로 입력을 받아서 자료처리 기간에 코딩작업을 하는 조사가 있고, 조사원이 입력을 하면서 자동코딩시스템을 이용해서 산업분류 코드를 입력하는 방식도 있다. 본 연구에서는 전자의 방법을 자동화하는 것에 초점을 두었다. 딥러닝 알고리즘을 이용해서 기존에 코드부여가 완료된 자료를 가지고 실험을 해본 결과 조사된 모든 항목을 사용했을 때에는 CNN이 81.36%로 가장 좋은 성능을 보였고, 항목을 2가지로 (사업체가 주로 하는 일/응답자가 한 일) 줄였을 경우 전체적으로 더 좋은 성능을 보였다. 그 중에 CNN-LSTM이 85.91%로 가장 좋은 성능을 보였다.

keywords : KSIC, Autocode, Deep Learning, CNN, LSTM, CNN-LSTM

1. 서론

통계청에서는 지역별고용조사, 인구총조사 등 다양한 조사를 실시하고 있다. 이러한 조사에서 응답자의 사업체명, 사업체가 주로 하는 일, 응답자가 한 일, 근무부서와 직책 정보를 받아서 산업이나 직업을 분류한다. 한국 표준 산업분류는 총 5개의 단계로 분류가 되어있는데 대분류 21개, 중분류 77개, 소분류 232개, 세분류 495개, 세세분류 1,196개로 매우 다양하게 분류가 되어 있다. 분류가 매우 다양하기 때문에 조사원이나 응답자가 관련된 분류에 정확한 지식을 가지고 있지 않다면 잘못된 분류정보를 선택할 수 있고, 너무 복잡한 내용으로 조사표를 구성할 경우 무응답 비율이 많아질 수 있다.

각 조사에서는 이러한 정보를 자연어로 입력을 받아서 자료처리 기간에 코드를 부여해 주는 방법으로 코드를 부여해 주는 조사가 있는 반면, 자동코딩시스템의 도움을 받아서 응답자의 정보를 자동코딩시스템 정보를 토대로 코드를 부여해 주는 조사도 있다. 두 방법 모두 1차적으로 사례사전 및 색인DB를

이용해서 자동으로 코드를 분류한다. 이렇게 분류했을 때 모든 조사자료가 자동으로 분류되지는 않고 일부 데이터만 분류가 되고 또는 순위를 매겨서 해당 조사자료는 어떠한 코드에 가장 적합한지 추천을 해 준다. 말 그대로 현재의 자동코딩시스템은 코드 부여 작업을 도와주는 시스템이다.

세계의 통계청은 이러한 조사자료의 자동분류에 대한 고민을 함께하고 있다. 특히 최근에는 UNECE 통계현대화 그룹에서 머신러닝을 공식 통계생산[1]에 이용하기 위해서 머신러닝 그룹을 운영하고 있다. 각 나라의 현재 머신러닝을 이용하는 현황을 공유하기도 하고 여러 머신러닝 테스트나 논문을 공유하면서 공식통계에 머신러닝을 이용하기 위해서 노력 하고 있다. 특히 캐나다나 미국의 같은 경우 딥러닝을 이용한 실험에서 아주 좋은 성능을 보이고 있고 실제 조사에서도 머신러닝이나 딥러닝을 이용하고 있다. 본 연구에서는 한국 통계청 조사자료를 딥러닝 알고리즘을 이용해서 한국 표준 산업분류를 자동으로 분류하는 실험을 해보았다.

2. 자동코딩 방법

통계청에서는 산업·직업분류를 정확하고 빠르게 분류하는 것을 도와주기 위해서 자동코딩시스템을 운영하고 있다. 자동코딩시스템은 크게 2가지로 나뉜다. 첫번째로 사례사전관리시스템이다. 이 시스템은 지역별고용조사, 전국사업체조사 등 실제 코드 부여가 완료된 조사 자료를 가지고 사람이 규칙을 만들어서 관리하는 시스템이다. 매년 상·하반기를 나누어서 자료를 업데이트 하고 있다. 정확도가 매우 높고 코딩 결과는 1:1로 결과가 나온다. 두번째로는 색인DB가 있다. 색인DB는 사례사전관리시스템과 동일하게 동일한 조사에서 학습데이터를 가져 오지만 코드를 부여하는 방식은 다르다. 색인DB는 조사자료에서 색인어를 추출해서 해당 DB에 저장해 놓고 코드를 부여해야 하는 자료가 들어오면 DB의 정보를 통해서 코드를 부여해 주는 방식이다. 코드는 사용자가 정하는 범위에 따라 1순위부터 10순위에 이까지 설정이 가능하다. 1순위는 입력한 자료와 가장 가까운 코드를 보여주는 방식이다.

일반적으로 사례사전관리시스템에서는 전체데이터가 모두 코드부여가 되지 않기 때문에 사례사전관리시스템과 색인DB를 같이 사용하게 된다. 사례사전에서 나온 코드와 색인DB에서 나온코드를 비교해서 내검원이나 조사원이 최종 코드를 부여해 주는 방식으로 산업·직업코드를 부여해 주고 있다.

3. 모델 및 평가

3-1. 학습데이터

학습데이터는 통계청 조사에서 산업 분류코드가 대분류로 부여된 자료를 사용했다. 총 14,831건의 자료를 사용했다. 학습데이터로 10,000건, 평가로 1,864건, 테스트로 2,967건을 사용했다.

학습데이터는 KoNLPy 라이브러리 okt 객체를 사용해서 어간 단위의 형태소 토큰나이징을 했다. 각 데이터의 길이가 다르기 때문에 길이를 8단어로 통일했다. 8단어보다 긴 데이터는 뒷부분을 자르고 짧은 경우는 0 값으로 패딩처리 했다. 그리고 의미 없는 단어 O, o, (주) 등의 단어를 불용어 처리 했다.

3-2. 모델구성 및 평가 방법

모델은 학습데이터가 각 딥러닝 알고리즘에 어떻게 동작하는지 실험하기 위해서 CNN (Convolution Neural Network), LSTM (Long Short-Term Memory units), CNN-LSTM 3가지의 모델을 가지고 비교를 했다.

합성곱 신경망(CNN)은 1개의 합성곱 신경망 + 맥스풀링 층을 사용하였다. 배치크기는 256, 필터크기는 3, optimization은 adam을 사용했고 overfitting을 막기 위해서 dropout 은 0.2 로 설정했다. 평가는 accuracy를 비교했다.

순환 신경망 모델(LSTM)은 128 메모리 셀을 가진 LSTM 레이어 1개, Dense 레이어 1개로 구성했다. 합성곱 신경망(CNN)과 동일하게 optimization은 adam을 사용했고 평가는 accuracy를 비교했다.

마지막으로 순환 컨볼루션 신경망 모델 (CNN-LSTM)은 컨볼루션 레이어에서 나온 feature vector들을 MaxPooling을 통해서 1/4로 줄인 다음에 순환 신경망 모델(LSTM) 입력으로 사용하도록 구성했다. 위와 동일하게 optimization은 adam을 사용했고 평가는 accuracy를 비교했다.

3-3. Feature 구성

첫 번째 실험 (Case 1)은 사업체명, 사업체가 주로 하는 일, 응답자가 한일, 근무부서와 직책 정보 모든 데이터를 feature 해서 각 모델을 돌려 보았다.

두 번째로는 (Case 2) 각 항목을 구분해 주고 학습시키는 것이 성능이 좋은 선행연구[2]를 활용해서 각 항목 앞에 구분자 A,B,C,D를 넣어서 학습을 시켰다.

마지막으로는 (Case 3) 지금까지 한국 표준 산업 분류 코딩작업을 해 본 경험으로 코드 분류에 주로 영향을 주는 요소는 대부분 사업체가 주로 하는 일, 응답자가 한 일 두 항목이 영향을 주고 있다는 판단에 의해서 딥러닝 모델도 두 항목만을 가지고 학습을 시켜 보았다.

3-4. 하이퍼파라미터

각 모델을 구성하고 가장 좋은 성능의 모델을 비교해 보기위해서 파라미터값을 조절 하는데 epochs 20, batch size 128 일 때 가장 좋은 성능을 보였다.

4. 실험결과

3가지 Case를 비교해 본 결과 Case 3이 전체적으로 가장 좋은 성능을 보였다. 그 중에 CNN-LSTM 모델이 85.91%로 가장 좋은 성능을 보였다. 3가지 모델을 비교 했을 때에는 모두 비슷한 성능을 보였지만 대체적으로 CNN이 좀 더 좋은 성능을 보였다.

Case	CNN	LSTM	CNN-LSTM
Case 1	81.36%	79.23%	79.51%
Case 2	81.05%	78.66%	80.24%
Case 3	85.40%	83.48%	85.91%

표 1 실험 결과

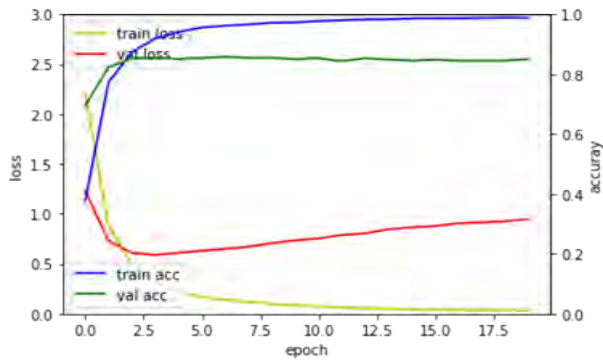


그림 1 CNN

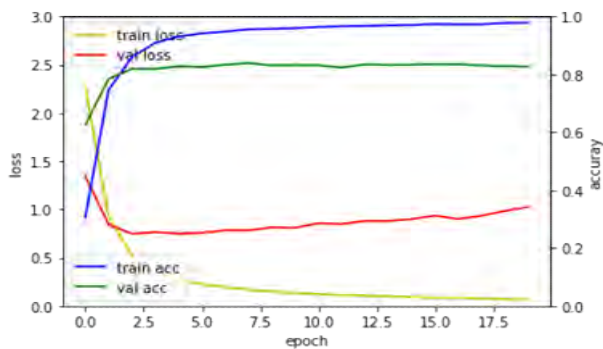


그림 2 LSTM

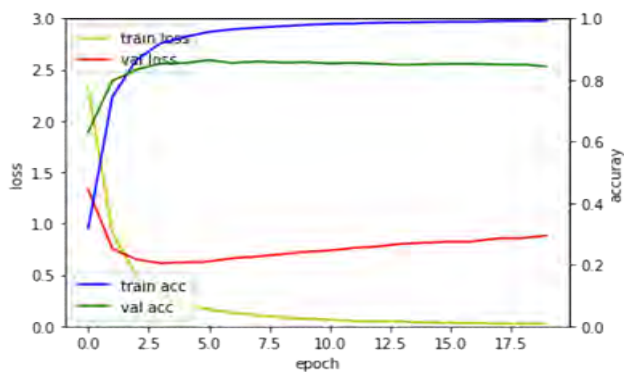


그림 3 CNN-LSTM

5. 결론 및 향후 연구

실험 결과 조사 되어진 모든 자료를 사용하는 것 보다는 분류를 잘할 수 있는 항목을 선택해서 학습 하는 것이 성능이 더 좋은 것을 확인했다. 그리고 Feature가 많을 때에는 CNN이 좋은 성능을 보였고 Feature가 적을 때에는 CNN-LSTM이 좋은 성능을 보였다.

향후 연구에서는 이번 연구를 토대로 조사된 항목 중 어떠한 항목을 선택하는 것이 산업분류 자동분류 성능을 높일 수 있는지 비교해 보고, 한국어 단어의 임베딩 방법을 달리해서 성능을 비교해 볼 예정이다.

참고문헌

- [1] UNECE Machine Learning Team "The use of machine learning in official statistics' November 2018
- [2] 김병수, CNN을 활용한 화계 계정코드 분류, 2019 한국정보기술학회·한국디지털콘텐츠학회 하계 공동학술대회 논문집, 2019, 583p

인공지능 기반의 언어 생성 모델 분석

이승철, 장용훈, 박창현, 서영석*

영남대학교 컴퓨터공학과

fatalist316@gmail.com, killerwise@ynu.ac.kr, park@yu.ac.kr, ysseo@yu.ac.kr[‡]

AI-based language generation model analysis

Seung Cheol Lee, Yonghun Jang, Chang-Hyeon Park, Yeong-Seok Seo[‡]

Dept. of Computer Engineering, Yeung-nam University

요 약

1989년에 WWW(World Wide Web)이 도입 되면서 세계적으로 인터넷의 보급이 시작되었다. 정보화 시대라고 알려진 3차 산업혁명 이 후로 대량의 정보들이 소셜 미디어를 통하여 생산되었다. 소셜 미디어는 2007년에 인터넷 사용자들 중 56%의 이용률을 보였지만 2008년 2분기에는 75%의 이용률로 증가함에 따라 대부분의 사용자들이 많이 사용하며 의존하게 되었다. 또한 소셜 미디어를 통해 발생 되는 데이터들을 이용하여 기업들은 이윤 창출을 할 수 있다. 하지만 이러한 소셜 미디어는 악의적인 목적을 통해 주가 조작, 정치적 선동 등을 할 수 있는 가짜 뉴스와 허위 정보들을 생성할 수 있으며 이에 따라 대책이 시급하다. 또한 가짜 뉴스는 사람이 글을 작성할 수도 있지만 최근 인공지능 기술의 발달에 따라 프로그램을 통해 자동적으로 생성 될 수도 있다. 본 논문에서는 이와 같은 실제 뉴스와 인공지능을 기반으로 한 뉴스를 분석한다. Kaggle에서 실제 뉴스 데이터를 수집하여 헤드라인을 OpenAI의 GPT-2 언어 모델을 통해 뉴럴 가짜 뉴스를 생성하였다. 파이썬의 NLTK 모듈을 이용하여 전처리를 진행하였고 t-검정과 박스 플롯을 활용하여 분석을 진행하였다. 분석된 주요 속성들을 의사결정트리를 통해 모델 검증을 하였고 k-fold 교차검증을 통해 분류 모델을 평가하였다. 결과로 전체 분류 정확도 평균 89%의 성능을 보여주었다.

1. 서론

정보화 시대라고 알려진 3차 산업 혁명 이래로 대량의 데이터들이 발생하였으며 현 시대에 이르러 국가, 기업, 개인의 커뮤니티 활성을 위한 소셜 미디어의 발전이 중요시 되었다[1]. 인터넷을 이용하는 사용자 중 소셜 미디어를 이용하는 사용자는 2007년에 56%가 사용 하였으며 바로 다음 해인 2008년 2분기에는 75%를 달성하였다[2].

현재 소셜 미디어는 개인 또는 특정 단체의 채널로 운영되며 주로 다양한 사용자들과 정보를 공유하기 위해 사용된다. 공유되는 정보에는 사실 뉴스의 정보도 포함된다. 하지만 전달되는 정보는 진실과 거짓이 존재한다. 거짓 된 정보를 뉴스처럼 전달하는 것을 가짜 뉴스라 하며 Parkinson은 가짜뉴스가 미국의 2016년 대선에 많은 영향을 미쳤다고 언급하

였다[3]. 따라서 소셜 미디어에 확산되고 있는 가짜 뉴스의 진위 여부를 판단하는 연구뿐만 아니라 자동화 된 가짜 뉴스의 사실 확인에 대한 연구의 관심도 함께 높아졌다[4]. 과거에 가짜뉴스는 사람에 의해서 작성되었지만 현재에는 인공지능 기술을 기반으로 한 언어 모델을 통해서도 작성이 가능하다. 비영리 인공지능 연구기관인 OpenAI의 GPT-2가 대표적이다. GPT-2는 일부 텍스트의 이전 단어 혹은 문장을 키워드로 제시하면 다음 단어 및 문장들을 예측 할 수 있도록 설계된 언어 모델이다[5]. 인공지능 기반의 언어 모델로부터 작성된 기사를 뉴럴 가짜 뉴스(Neural fake news)라 부르고 있으며 뉴럴 가짜 뉴스는 인간이 작성한 뉴스와 거의 유사하다[6-7].

본 논문에서는 실제 인간이 작성한 뉴스와 인공지능을 기반으로 한 언어 생성 모델이 작성한 뉴스의 분류를 위한 분석을 진행한다.

2장은 OpenAI의 GPT-2에 대한 설명과 관련 연구를 서술하며 3장에서는 분석에 필요한 데이터의 수집 및 전처리 과정을 서술한다. 4장에서는 모델

* 교신저자 : 서영석(Yeong-Seok Seo), 컴퓨터공학과(Dept. of Computer Engineering), 영남대학교(Yeung-nam University), Email : ysseo@yu.ac.kr

검증 및 분석 결과를 서술하며 5장은 결론으로 진행한다.

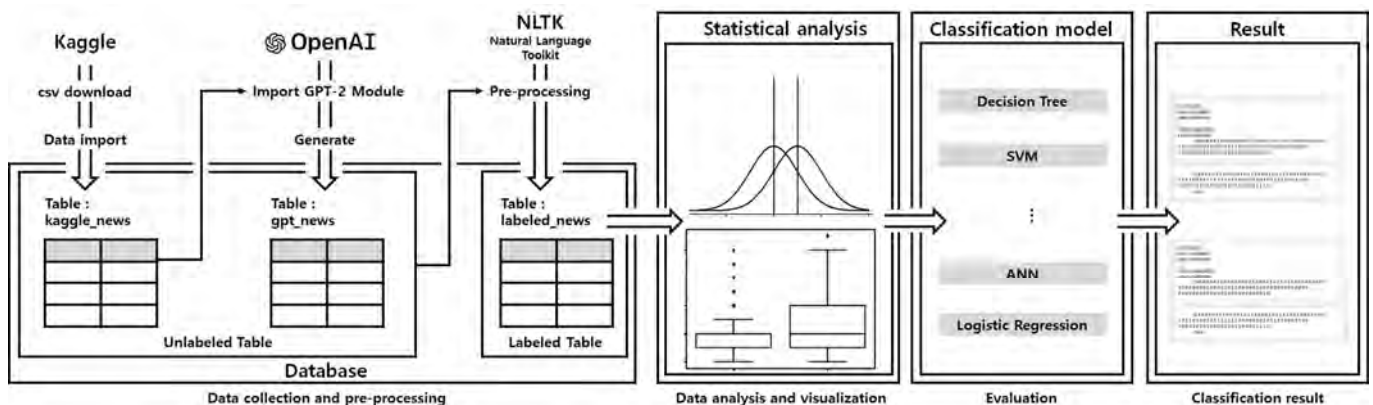
2. 관련 연구

비영리 인공지능 연구기관인 OpenAI는 2019년 2월에 GPT-2를 발표하였다. GPT-2는 텍스트 생성 기능을 가진 인공지능 모델로서 학습에 사용된 데이터는 약 800만 건의 웹페이지 데이터와 약 1,000만 건의 텍스트를 사용하였다. 단어나 문장을 키워드로 제시를 하면 약 40GB의 데이터를 기반으로 한 텍스트를 생성해준다. 또한 생성텍스트의 길이, top-k 등의 매개변수를 설정할 수 있다. 방대한 데이터를 학습한 결과로 GPT-2는 기존에 인간들이 작성하던 뉴스 기사, 블로그 게시물, 소셜 등의 글을 작성할 수 있다. 하지만 GPT-2는 특정 목적으로 악용될 소지가 있다. GPT-2는 1시간에 수백에서 수천 개의 뉴스 기사를 생성할 수 있다. 결과적으로 진실과 거짓을 구분 할 수 없는 글들이 소셜 미디어를 통해 전파되어 가짜 뉴스, 주식에 관련한 거짓 정보, 정치적 선동이 가능한 글들로 인하여 소셜 미디어의 사용자들에게 혼란을 야기할 수 있다.

인공지능을 기반으로 한 언어 생성 모델에 관련한 연구는 다음과 같다. Rowan은 텍스트 생성 모델인 Grover와 생성된 텍스트에 대한 탐지 모델을 제안하였다[7]. Joseph는 UN총회에서 발표된 연설 데이터에 대해 사전 훈련된 AWD-LSTM모델을 미세 조정하여 정치적 스타일의 텍스트를 생성하는 모델을 제안하였으며 이를 통해 자동화된 텍스트에 대한 위험성과 이를 방지하기 위한 정책의 필요성을 제안하였다[8].

<표 1>실제뉴스와 뉴럴 가짜 뉴스의 유니온을 진행 후 전처리가 진행된 테이블 정의

Table : labeled news		
Column name	Type	Describe
class	int	0 : human, 1 : bot
text	longtext	news text
num_cnt	int	Number of numbers used
word_cnt	int	Number of words used
sentence_cnt	int	Number of sentence used
strong_pos_word_cnt	int	Number of strong positive words
strong_neg_word_cnt	int	Number of strong negative words
weak_pos_word_cnt	int	Number of weak positive words
weak_neg_word_cnt	int	Number of weak negative words
sentimental_score2	double	Positive score 2 = NLTK positive score + NLTK negative score
pos_sentence_cnt	int	Number of positive sentences
neg_sentence_cnt	int	Number of negative sentences
sentimental_score1	double	Emotion score = strong positive - strong negative + (weak positive - weak negative) * 0.5
sentence_score1	double	Sentence score of sentence = positive - negative
sentence_score2	double	Sentence positive score 2 = nltk sentence positive score + nltk sentence negative score
link_cnt	int	Number of links
schar_cnt	int	Number of special characters
noun_cnt	int	Number of nouns
pronoun_cnt	int	Number of pronouns
verb_cnt	int	Number of verbs
modal_cnt	int	Number of auxiliary verbs
adject_cnt	int	Number of adjectives
adverb_cnt	int	Number of adverbs
interject_cnt	int	Number of admirers
interrogat_cnt	int	Number of interrogators
conjunct_cnt	int	Number of conjunctions
unkwon_cnt	int	Number of non-attributes



(그림 1) 데이터 수집과 전처리 및 시각화 과정.

<표 2> 각 속성의 T-검정 결과

col_name	p-value
num_cnt	*0.516443
word_cnt	*0.473975
sentence_cnt	*0.25634
strong_pos_word_cnt	*0.646823
strong_neg_word_cnt	**0.035263
weak_pos_word_cnt	*0.804468
weak_neg_word_cnt	*0.723293
sentimental_score2	*0.081138
pos_sentence_cnt	*0.581243
neg_sentence_cnt	**0.001746
sentimental_score1	*0.081138
sentence_score1	*0.127788
sentence_score2	*0.134157
link_cnt	*0.169426
schar_cnt	**1.23E-51
noun_cnt	*0.278986
pronoun_cnt	*0.877456
verb_cnt	**0.018639
modal_cnt	**0.142529
adject_cnt	**0.000252
adverb_cnt	**7.20E-05
interject_cnt	*0.843937
interrogat_cnt	*0.167491
conjunct_cnt	**0.003081
unkwon_cnt	**0.001539

* : p-value >= 0.05

** : p-value < 0.05

3. 언어 생성 모델을 통한 데이터 수집 및 전처리

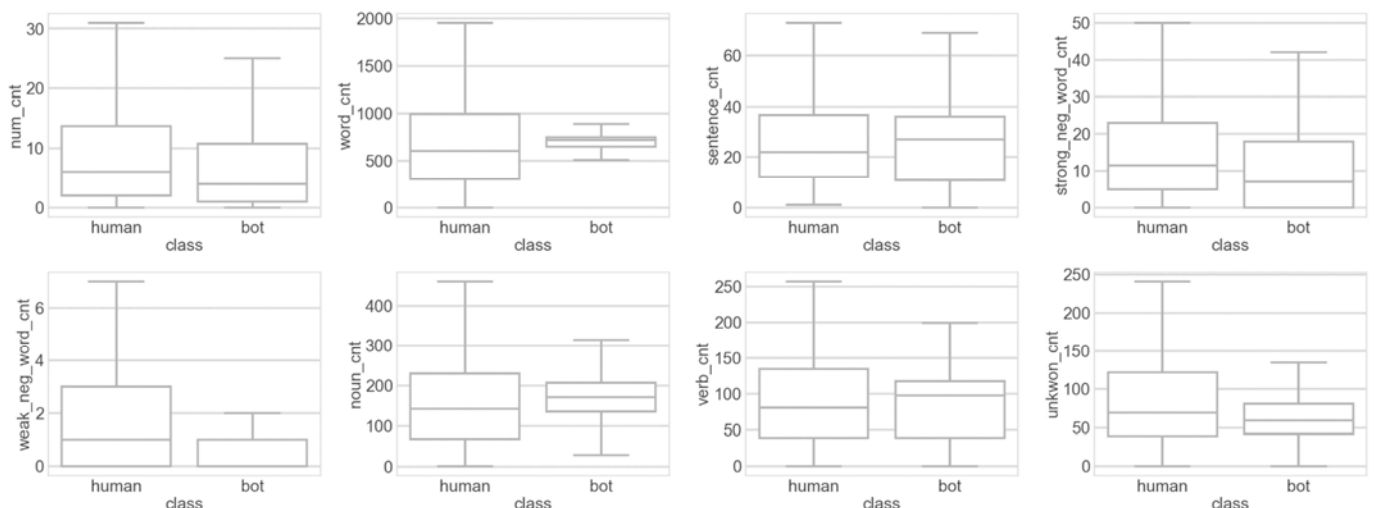
본 장에서는 인간이 작성하는 뉴스 기사와 GPT-2를 이용하여 작성된 뉴럴 가짜 뉴스 기사를 분석하기 위한 데이터 수집 및 전처리 과정을 설명한다. 인간이 작성하는 뉴스 기사를 수집하기 위해 Kaggle의 데이터셋을 다운로드 한다. 다운로드한 csv파일을 데이터베이스에 저장하기 위해 데이터 테이블을

정의한다. 그림 1과 같이 GPT-2를 이용하여 실제뉴스의 헤드라인을 키워드로 제시하여 뉴럴 가짜 뉴스를 생성한다. 마찬가지로 GPT-2로 생성한 뉴스의 테이블을 정의하였으며 헤드라인은 뉴럴 가짜 뉴스를 생성하기 위해 제시했었던 키워드로 설정하였다. 실제뉴스 테이블과 뉴럴 가짜 뉴스 테이블을 유니온한 후 파이썬의 자연언어처리지원모듈인 NLTK를 통하여 뉴스의 내용을 표 1과 같이 25개의 속성으로 전처리 작업을 진행하여 데이터베이스에 저장한다. 최종 레이블 된 테이블을 t-검정과 파이썬의 seaborn 모듈을 이용하여 분석결과를 시각화 하며 분류 모델을 통한 검증을 진행한다.

4. 모델 검증 및 분석 결과

실제 인간이 작성한 뉴스를 실제 뉴스라 통일하며 뉴럴 가짜 뉴스와의 차이를 확인하기 위해 실제 뉴스 300건과 뉴럴 가짜 뉴스 300건을 활용하였다. 표 2는 각 속성에 대해 t-검정을 수행한 결과이며, 그림 2는 각 속성들에 대한 데이터 분포를 박스플롯을 이용하여 유의미한 차이가 있는 속성을 나타낸 것이다. 그림 2의 박스플롯에서 x축은 뉴럴 가짜 뉴스 여부를 의미하고 y축은 각 속성 값의 범위를 나타낸다.

실제 뉴스와 뉴럴 가짜 뉴스간의 유의한 차이를 보이는 속성들은 숫자 사용수(num_cnt), 단어의 수(word_cnt), 문장의 수(sentence_cnt), 강한 부정 단어 사용의 수(strong_pos_word_cnt), 약한 부정 단어 사용의 수(weak_neg_word_cnt), 명사 사용 수(noun_cnt), 미 분류 속성의 수(unkwon_cnt) 등이다. 실제 뉴스와는 달리 뉴럴 가짜 뉴스를 생성하는 GP



(그림 2) 각 속성들의 데이터 분포

<표 3>실제 뉴스와 뉴럴 가짜 뉴스 간
K-Fold 교차 검증 결과

5-fold	accuracy (%)		
	total	bot	human
case 1	91%	98%	85%
case 2	87%	96%	79%
case 3	91%	94%	87%
case 4	92%	98%	88%
case 5	65%	97%	78%
avg	89%	96%	83%

T-2 모듈은 대체적으로 단어의 수가 현저히 적은 것으로 보이기 때문에 사용하는 명사의 수도 적은 것으로 예상된다. 또한 문장의 수가 적은 것으로 보아 인간과는 달리 긴 문장을 구성하는 것이 아닌 여러 짧은 문장으로 구성하는 특성이 있어 보인다. 강한 부정 단어 사용의 수와 미 분류 속성의 수를 제외한 속성들은 t-검정에서 p-value가 0.05보다 큰 값이 계산되었다. 이는 두 속성을 제외한 속성들이 실제 뉴스와 뉴럴 가짜 뉴스간의 차이가 통계적으로 유의함을 의미한다.

실제 뉴스와 뉴럴 가짜 뉴스의 분류를 위해 의사결정트리를 사용하였다. 학습 데이터와 검증 데이터의 균형을 위해 k-fold 교차 검증을 진행 하였으며 결과는 표 3에 나타내었다. 분류 모델의 성능은 k-fold step 4에서 92%의 정확도를 나타내었고 분류 정확도의 평균 89%의 성능을 달성하였다.

5. 결론

미디어의 발전과 함께 소셜 미디어의 확산은 급격하게 증가하며 조직 및 개인의 사설 뉴스가 확산되었다. 사설 뉴스의 진실 및 거짓 여부 판단이 어렵고 인공지능에 기반한 언어 모델을 통하여 뉴스를 작성하게 되면 더더욱 어려워 지게 된다. 본 연구에서는 인간이 작성한 실제 뉴스와 OpenAI에서 개발한 GPT-2 언어 모델을 통해 작성된 뉴럴 가짜 뉴스의 분석 및 모델 검증을 하였다. 실제 뉴스 수집을 위해 Kaggle을 통하여 데이터를 다운로드 하였으며 다운로드 된 데이터의 헤드라인을 GPT-2 언어 모델을 통하여 뉴럴 가짜 뉴스를 생성하였다. 수집한 실제 뉴스와 생성된 뉴럴 가짜 뉴스의 텍스트를 파이썬의 NLTK 모듈을 통해 전처리 작업을 진행 하였으며 이를 분석하기 위해 t-검정과 박스 플롯을 활용하였다. 숫자 사용수, 단어의 수, 문장의 수, 강한 부정 단어 사용의 수, 약한 부정 단어 사용의 수, 명사 사용 수, 미 분류 속성의 수중에서 강한

부정 단어 사용의 수와 미 분류 속성의 수를 제외한 나머지 속성에서 p-value가 0.05보다 큰 것을 통해 통계학적으로 유의미한 것을 확인하였다. 또한 의사결정트리를 통해 분류 모델 검증을 하였으며 k-fold 교차 검증을 통해 데이터의 범위별 분류 정확도의 평균 89%의 성능을 달성하였다.

Acknowledgement

이 성과는 2019년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2017R1C1B5018295). 이 연구는 2019년도 영남대학교 학술연구조성비에 의한 것임

참고문헌

- [1] Kyle Hensel, Michael H. Deis, "Using social media to increase advertising and improve marketing.", The Entrepreneurial Executive. Vol. 15, pp. 87, 2010.
- [2] Andreas M. Kaplan, Michael Haenlein, "Users of the world, unite! The challenges and opportunities of Social Media.", Business horizons, Vol. 53, No. 1, pp. 59-68, 2010.
- [3] Hannah Jane Parkinson, "Click and elect: how fake news helped Donald Trump win a real election.", The Guardian, Vol. 14, 2016.
- [4] Jan Christian Blaise Cruz, Julianne Agatha Tan, Charibeth Cheng, "Localization of Fake News Detection via Multitask Transfer Learning.", arXiv preprint arXiv:1910.09295, 2019.
- [5] Alec Radford, Jeffrey Wu, Rewon Child, David Luan, Dario Amodei, Ilya Sutskever, "Language models are unsupervised multitask learners.", OpenAI Blog, Vol. 1, No. 8, pp. 9, 2019.
- [6] Anne K. Cybenko, George Cybenko, "AI and fake news.", IEEE Intelligent Systems, Vol. 33, No. 5, pp. 1-5, 2018.
- [7] Rowan Zellers, Ari Holtzman, Hannah Rashkin, Yonatan Bisk, "Defending against neural fake news.", Advances in Neural Information Processing Systems. pp. 9051-9062, 2019.
- [8] Joseph Bullock, Miguel Luengo-Oroz, "Automated Speech Generation from UN General Assembly Statements: Mapping Risks in AI Generated Texts.", arXiv preprint arXiv:1906.01946, 2019.

Transformer-based DKN for News Recommendation

Hanwei Xia*, Inwhae Joe**

*Dept. of Computer Science, Hanyang University

**Dept. of Computer Science, Hanyang University

ABSTRACT

In recent years, deep learning has been widely used in news recommendation systems. In the previous personalized news recommendation, a large number of CF-based methods, content-based or hybrid methods have been proposed. But most of the works are only modeling the user's interaction history, ignoring the hidden meaning of the user's continuous behaviors. In this paper, we propose to adopt the powerful Transformer model in order to understand the hidden meaning of the user's continuous behaviors in news recommendations. The experimental results prove the superiority of the transformer, and the AUC has been significantly improved as compared to the original model.

1. INTRODUCTION

In many real-world applications, the current interests of users are intrinsically dynamic and evolving, and are affected by their historical behaviors. For example, after reading the news of large-scale dissemination of covid-19, the user will want to know the symptoms and preventive measures of covid-19, but he/she will not read such news under normal circumstances.

In the era of deep learning, Google's WDL [1] embeds a large number of raw features as vectors into low-dimensional spaces and then fed into fully connected layers that are multi layer perceptron (MLP) to predict whether a user will click on an item. But they just concatenate all features without learning the hidden information between the user's continuous behaviors. Alibaba's DIN [2] is improved based on WDL, and they proposed to use attention mechanism to compare the similarities between the target item and the previously clicked items of a user. Deep Knowledge-Aware Network (DKN) [3] also uses DNN as an attention network to distinguish the impact of different news in the user's click history on target news. None of them takes into account the hidden meaning of the user's continuous behaviors.

To solve the above problem, we try to incorporate continuous information of the user's behavior sequence into the DKN. Inspired by the great success of the Transformer in natural language processing (NLP) [4], we treat news in a user's behavior sequence as words in a sentence, and then use the self-attention mechanism to learn a better representation for each news in a user's behavior sequence, and then feed them into MLPs to predict the probability that the user will click on target news. The advantage of the Transformer is that it can use the self-attention mechanism to better capture the relevance among words in sentences. In other words, the Transformer can extract the "relevance" among news in a user's behavior sequences. We used the real data set attached

to the DKN for experiments. The results show that the Transformer has made significant progress in deep learning-based recommendation methods, and AUC has improved significantly.

2. RELATED WORK

Personalized News Recommendation. In personalized news recommendation, CF-based methods [5] often have the cold-start problem because news items are frequently replaced. Therefore, many content-based or hybrid methods have been proposed [6, 7]. Recently, researchers have also tried to combine topic models [8] and recurrent neural networks [9] into news recommendations. The major difference between prior work and ours is that we use the Transformer to extract the "dependency" among news in a user's behavior sequences, in order to better understand the hidden meaning of user behavior sequences.

Attention Mechanism. The Transformer lets people see the power of attention mechanism in machine translation [4] and text classification. Recently, researchers try to employ the attention mechanism to improve recommendation performances and interpretability [3, 10]. For example, DKN [3] uses DNN as an attention network to distinguish the impact of different news in the user's click history on target news. DKN treats attention mechanism as an additional component to the original models. In contrast, the Transformer is built solely on multi-head self-attention and achieves great success in text sequence modeling. So Transformer can better extract the "relevance" among news in a user's behavior sequences.

Sequential Recommendation. Recently, RNN, Gated Recurrent Unit (GRU) [11] and Long Short-Term Memory (LSTM) [12] are widely used in modeling user behavior sequences [14]. These methods usually encode the user's previous records into vectors with various recurrent architectures and loss functions. Other than RNN, deep

learning models are also introduced for sequential recommendation. For example, BST [13] also uses the Transformer model. The major difference between BST and ours is that We have different architectures in the feature embedding layer.

3. METHODOLOGY

Fig 1 is the overview architecture of this paper. We improved on the basis of DKN [3], using KCNN to convert news headlines into news embedding, and embed positional features as low-dimensional vectors. After concatenating news embedding and positional embedding, use the Transformer layer to learn the deeper representation of each news in the sequence. We connect the embedding of Other Features with the output of the Transformer layer, then use three fully connected layers to learn the interactions of the mixed features, and then use the sigmoid function to generate the final output.

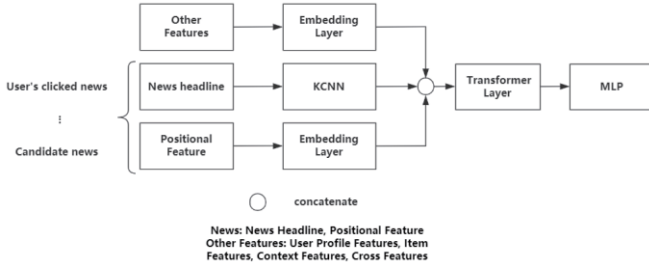


Fig.1: overview architecture

3.1 Knowledge Distillation and Knowledge-aware CNN

First, DKN [3] split the news headline into a set of words, and then link the words in the headline with the entities of the knowledge base. If the entity corresponding to the word can be found, then all adjacent entities within one hop from the linked entity are found, and these adjacent entities are called context entities. The word2vec model can be used to obtain the word embedding, and the knowledge graph embedding model can be used to obtain the knowledge entity embedding. Context embedding is to average multiple entity embeddings.

KCNN. DKN maps entity embedding and context embedding to the same vector space through a non-linear transformation. Then use word embedding, entity embedding, and context embedding as the multi-channel CNN input, and obtain news embedding of the news headline through the convolution operation.

3.2 Embedding layer

The role of the embedding layer is to embed all the input features into a fixed-size low-dimensional vector. We concatenate user profile features, item features, context features, and the combination of different features and embed them into low-dimensional vectors. Then we concatenate the matrix embedding of these features with the matrix embedding output by Transformer as the input of the MLP layer.

Positional embedding. Position feature is equivalent to the positional encoding in [4], which is the position information of the news in the users' behavior sequence. The purpose is to

introduce timing information to the users' behavior sequence. We use $pos(v_i) = t(v_t) - t(v_i)$ to calculate the position value of news v_i , and then project it into a low-dimensional vector after discretization. Where $t(v_t)$ represents the recommending time and $t(v_i)$ the timestamp when user click news v_i . Then we concatenate news embedding and positional embedding as the input of the Transformer.

3.3 Transformer layer

Fig 2 is the architecture of the Transformer Encoder layer.

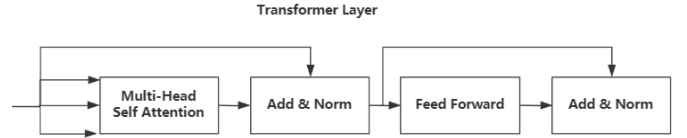


Fig.2: Transformer Encoder Layer

Self-attention layer. Below is the scaled dot-product attention [4]:

$$\text{Attention}(\mathbf{Q}, \mathbf{K}, \mathbf{V}) = \text{softmax}\left(\frac{\mathbf{Q}\mathbf{K}^T}{\sqrt{d}}\right)\mathbf{V}, \quad (1)$$

where \mathbf{Q} is the queries, \mathbf{K} is the keys, and \mathbf{V} is the values. The self-attention operation takes the embedding of items as input, transforms them into three matrices by linear projection, and enters them into an attention layer. Following [4], we use the multi-head attention:

$$\mathbf{S} = \text{MH}(\mathbf{E}) = \text{Concat}(\text{head}_1, \text{head}_2, \dots, \text{head}_h)\mathbf{W}^H, \quad (2)$$

$$\text{head}_i = \text{Attention}(\mathbf{E}\mathbf{W}^Q, \mathbf{E}\mathbf{W}^K, \mathbf{E}\mathbf{W}^V), \quad (3)$$

where the projection matrices $\mathbf{W}^Q, \mathbf{W}^K, \mathbf{W}^V \in \mathbb{R}^{d \times d}$, and \mathbf{E} is the embedding matrices of all news, and h is the number of heads.

Point-wise Feed-Forward Networks. Following [4], We define point-wise Feed-Forward Networks (FFN) as follows:

$$\mathbf{F} = \text{FFN}(\mathbf{S}). \quad (4)$$

We use dropout and LeakyReLU in self-attention and FFN to avoid overfitting and learn hidden features hierarchically. Below is the output of the self-attention and FFN layers:

$$\mathbf{S}' = \text{LayerNorm}(\mathbf{S} + \text{Dropout}(\text{MH}(\mathbf{S}))), \quad (5)$$

$$\mathbf{F} = \text{LayerNorm}(\mathbf{S}' + \text{Dropout}(\text{LeakyReLU}(\mathbf{S}'\mathbf{W}^{(1)} + b^{(1)})\mathbf{W}^{(2)} + b^{(2)})), \quad (6)$$

Where $\mathbf{W}^{(1)}, \mathbf{W}^{(2)}, b^{(1)}, b^{(2)}$ are the learnable parameters, and LayerNorm is the standard normalization layer.

Stacking the FNN blocks. It aggregates all the embeddings of previous news to learn the complex relationship hidden in the news sequences after the first self-attention block. Below is the definition of the self-building blocks and the b -th block:

$$\mathbf{S}^b = \text{SA}(\mathbf{F}^{(b-1)}), \quad (7)$$

$$\mathbf{F}^b = \text{FFN}(\mathbf{S}^b), \forall i \in 1, 2, \dots, n. \quad (8)$$

The output of the Transformer layer is the matrix \mathbf{F} , which represents the news embedding in the users' behavior sequence, and the candidate news that contains the characteristics of the users' behavior sequence.

3.4 MLP layer

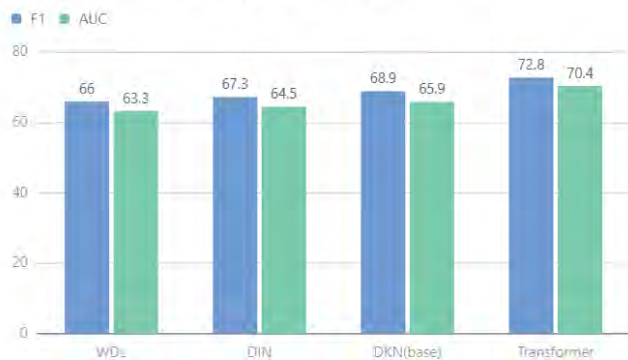
Due to the good performance of WDL [1] and DIN [2], we connect the embedding of Other Features with the output of

the Transformer layer, then use three fully connected layers to learn the mutual effects among the hybrid features. Finally, we use the sigmoid function to output the probability that the user clicks on the target news because whether users will click on the candidate news is a dichotomy classification problem.

4. PERFORMANCE EVALUATION

The results are shown in Fig 3, from which we can see the superiority of the Transformer model over other models. In specific, the F1 score is improved from 66.0(WDL), 67.3(DIN), and 68.9(DKN) to 72.8(Transformer). The AUC is improved from 63.3(WDL), 64.5(DIN) and 65.9(DKN) to 70.4(Transformer). In contrast, the Average RT of Transformer has not increased a lot, which guarantees the feasibility of using the Transformer model in real news recommendations.

F1 score and AUC score of different models



Methods	F1	AUC	Average RT(ms)
WDL	66.0 ± 1.2 (-2.9%)	63.3 ± 1.5 (-2.6%)	14
DIN	67.3 ± 1.3 (-1.6%)	64.5 ± 1.1 (-1.4%)	16
DKN(base)	68.9 ± 1.5	65.9 ± 1.2	19
Transformer	72.8 ± 1.5(+3.9%)	70.4 ± 1.4(+4.5%)	21

Fig.3: F1 scores and AUCs of different methods

5. CONCLUSION

In this paper, we introduced the use of transformer as an attention mechanism to dynamically calculate the total historical performance of users on the basis of DKN [3]. Experimental data show the superiority of this model in modeling user behavior sequences. If there is a better model of the attention mechanism, you can try to replace it.

REFERENCES

- [1] Heng-Tze Cheng, Levent Koc, Jeremiah Harmsen, Tal Shaked, Tushar Chandra, Hrishikesh Aradhya, Glen Anderson, Greg Corrado, Wei Chai, Mustafa Ispir, et al. Wide & deep learning for recommender systems. 2016.
- [2] Guorui Zhou, Xiaoqiang Zhu, Chenru Song, Ying Fan, Han Zhu, Xiao Ma, Yanghui Yan, Junqi Jin, Han Li, and Kun Gai. Deep interest network for click-through rate prediction. 2018. In KDD. 1059–1068.
- [3] Hongwei Wang, Fuzheng Zhang, Xing Xie, and Minyi Guo. DKN: Deep Knowledge Aware Network for News Recommendation. 2018. In Proceedings of The 2018 Web Conference (WWW 2018). ACM, New York, NY, USA, 10 pages. <https://doi.org/10.1145/3178876.3186175>
- [4] Ashish Vaswani, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N Gomez, Łukasz Kaiser, and Illia Polosukhin. Attention is all you need. 2017. In NIPS. 5998–6008.
- [5] Chong Wang and David M Blei. Collaborative topic modeling for recommending scientific articles. 2011. In Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining. ACM, 448–456.
- [6] Michal Kompan and Mária Bielíková. Content-Based News Recommendation. 2010. In EC-Web, Vol. 61. Springer, 61–72.
- [7] Owen Phelan, Kevin McCarthy, and Barry Smyth. Using twitter to recommend real-time topical news. 2009. In Proceedings of the third ACM conference on Recommender systems. ACM, 385–388.
- [8] Tapio Luostarinen and Oskar Kohonen. Using topic models in contentbased news recommender systems. 2013. In Proceedings of the 19th Nordic Conference of Computational Linguistics. Linköping University Electronic Press, 239–251.
- [9] Shumpei Okura, Yukihiro Tagami, Shingo Ono, and Akira Tajima. Embedding-based News Recommendation for Millions of Users. 2017. In KDD. ACM, 1933–1942.
- [10] Jing Li, Pengjie Ren, Zhumin Chen, Zhaochun Ren, Tao Lian, and Jun Ma. Neural Attentive Session-based Recommendation. 2017. In Proceedings of CIKM. ACM, New York, NY, USA, 1419–1428.
- [11] Kyunghyun Cho, Bart van Merriënboer, Caglar Gulcehre, Dzmitry Bahdanau, Fethi Bougares, Holger Schwenk, and Yoshua Bengio. Learning Phrase Representations using RNN Encoder–Decoder for Statistical Machine Translation. 2014. In Proceedings of EMNLP. Association for Computational Linguistics, 1724–1734.
- [12] Sepp Hochreiter and Jürgen Schmidhuber. Long Short-Term Memory. 1997. Neural Computation 9, 8 (Nov. 1997), 1735–1780.
- [13] Qiwei Chen, Huan Zhao, Wei Li, Pipei Huang, Wenwu Ou. Behavior Sequence Transformer for E-commerce Recommendation in Alibaba. 2019. arXiv: 1905.06874v1 [cs.LG]
- [14] Balázs Hidasi, Alexandros Karatzoglou, Linas Baltrunas, and Domonkos Tikk. Session-based Recommendations with Recurrent Neural Networks. 2016. In Proceedings of ICLR.

Hybrid Feature Selection과 Data Balancing을 통한 네트워크 침입 탐지 모델

민병준, 신동규*, 신동일*

세종대학교 컴퓨터 공학과

okminkr@gmail.com, shindk@sejong.ac.kr, dshin@sejong.ac.kr

Network intrusion detection Model through Hybrid Feature Selection and Data Balancing

Byeongjun Min, Dongkyoo Shin*, Dongil Shin*

Dept. of Computer Engineering, Sejong University

요 약

최근 네트워크 환경에 대한 공격이 급속도로 고도화 및 지능화 되고 있기에, 기존의 시그니처 기반 침입탐지 시스템은 한계점이 명확해지고 있다. 이러한 문제를 해결하기 위해서 기계학습 기반의 침입 탐지 시스템에 대한 연구가 활발히 진행되고 있지만 기계학습을 침입 탐지에 이용하기 위해서는 두 가지 문제에 직면한다. 첫 번째는 실시간 탐지를 위한 학습과 연관된 중요 특징들을 선별하는 문제이며 두 번째는 학습에 사용되는 데이터의 불균형 문제로, 기계학습 알고리즘들은 데이터에 의존적이기에 이러한 문제는 치명적이다. 본 논문에서는 위 제시된 문제들을 해결하기 위해서 Hybrid Feature Selection과 Data Balancing을 통한 심층 신경망 기반의 네트워크 침입 탐지 모델을 제안한다. NSL-KDD 데이터 셋을 통해 학습을 진행하였으며, 평가를 위해 Accuracy, Precision, Recall, F1 Score 지표를 사용하였다. 본 논문에서 제안된 모델은 Random Forest 및 기본 심층 신경망 모델과 비교해 F1 Score를 기준으로 7~9%의 성능 향상을 이루었다.

1. 서론

네트워크 침입 탐지 시스템(NIDS)은 네트워크 트래픽을 감시하여 공격 여부를 판단하는 시스템으로, 기존의 NIDS는 시그니처 기반의 탐지 기법이 주를 이루었다. 이는 전문가를 통해 미리 정립된 공격 패턴과의 패턴 매칭을 통해 공격을 탐지한다. 하지만 APT(Advance Persistent Threat) 공격과 같이 위협이 고도화 및 지능화됨에 따라서 트래픽 및 로그에 대한 분석 과정에서의 시간과 비용적 문제가 발생하고 있다. 최근 이러한 문제를 해결하기 위해 기계학습 기반의 탐지 시스템의 연구가 활발하다[1-3].

현실 세계에서 수집되는 많은 데이터들은 클래스 간 균형이 완벽하지 않은 환경이 대부분으로, 특히 침입 탐지 문제에서는 전체 데이터 중 침입 데이터의 비율이 약 1%로 알려져 있다[4]. 이러한 소량의 침입 데이터로 정상학습을 하는 것은 매우 어려우며, 실시간 탐지 위해 사용 가능한 많은 속성 중에서 학습과 관련 있는 특징들을 선별하는 것도 중요하게 다뤄지고 있다.

본 논문에서는 최근 다양한 도메인에서 좋은 결과를 보이고 있는 심층 신경망 모델을 통한 네트워크 침입 탐지 모델을 제안한다. 또한 학습에 중요한 특징들을 선별하기 위하여 Hybrid Feature Selection 기법을 제안하며, SMOTE(Synthetic Minority Over sampling Technique)기법과 RUS(Random Under Sampling) 기법을 통해 데이터 셋의 불균형 문제를 해소하여[5], 소수 클래스들의 탐지율을 개선하였다.

2. 관련 연구

2.1 기계학습 기반 네트워크 침입 탐지 시스템

강승호 외[2]는 NSL-KDD 데이터로부터 Pearson 상관계수 기반의 특징 선택 알고리즘을 제안하였다. 주어진 임계치 이상의 상관계수를 갖는 특징 집합을 그래프 자료구조로 표현한 뒤, 최소 지배 집합(Minimum dominating set)문제로 정의하였다. 최희수 외[3]는 NSL-KDD 데이터로부터 특징들의 빈도수와 평균값을 통한 새로운 특징 선택 기법 AR(Attribute Ratio)을 제안하였다. Nutan 외[4]는

Hybrid Feature Selection 방법을 제안하였다. 서로 다른 특징 선택 알고리즘으로부터 중복제거 합집합으로 표현하여 학습에 사용하였다.

2.2 NSL-KDD 데이터 셋

KDD CUP 99 데이터 셋[6]은 1999년 DARPA 침입탐지 평가 프로그램을 통해 만들어진 데이터 셋으로, 미 공군의 네트워크를 모델링하여 38가지의 네트워크 침입 탐지 공격 시뮬레이션을 통해 만들어졌다. M. Tavallaei 외[6]은 KDD CUP 99 데이터 세트의 규모가 지나치게 크며, 많은 중복 레코드 등을 포함하는 문제점을 지적하며 NSL-KDD 데이터 셋을 제안하였다. NSL-KDD 데이터 세트는 41개의 컬럼으로 구성되며, 표1과 같이 4가지 공격 유형을 포함하고 있다.

<표 1> NSL-KDD 데이터 셋의 공격 유형

공격 유형	설명
DoS	서비스 거부 공격
Probe	침입 전 취약점 분석을 위한 사전 작업
U2R	루트 권한 탈취를 위한 비인가 접근
R2L	원격으로부터의 비인가 접속 시도

3. 본론

3.1 데이터 전처리

NSL-KDD 데이터 셋 컬럼들의 데이터 형식은 nominal, binary, numeric 3가지로 구분할 수 있다. nominal 데이터들은 모두 정수형으로 인코딩 한 뒤 원핫(onehot) 벡터로 변환하였으며, numeric 데이터들에 대해서는 최소 최대 정규화(Min-max Normalization)를 진행하며, binary 데이터들의 경우 모두 0과 1로 구성되기 때문에 별다른 전처리 과정을 수행하지 않는다. 이를 통해 최종적으로 41개의 입력차원이 122개의 입력차원으로 변환되어 학습에 사용된다.

3.2 Hybrid Feature Selection

본 논문에서는 Pearson 기반 특징 선택과 AR 기반 특징선택 및 Feature Importance 기반 특징 선택을 활용한 HFS(Hybrid Feature Selection)을 제안한다. HFS 기법은 그림 1에 명시된 3가지 특징 선택 기법들의 교집합 특징 집합을 사용한다. HFS는 중첩 특징 제거 및 학습에 무관한 특징 제거 2가지 목적에 따라 특징 선택 기법들을 나뉘어 구성하였

다. 실제로 Pearson 상관계수가 높은 특징들끼리는 Feature Importance를 뽑을 경우 같이 높은 값을 가지게 된다. 따라서 Feature Importance 만을 통해 특징 선택을 할 경우 이러한 중첩 특징들을 고려할 수 없다. 본 논문에서 제시하는 HFS는 이러한 두 가지 관점의 특징들을 모두 걸러낼 수 있다. 또한 ‘num_outbound_cmds’ 특징은 표준편차가 0으로 관찰되어 사전에 제거하였다.

<표 2> 0.9 이상의 Pearson 상관계수 관계 속성들

완전 그래프 노드	
1	dst_host_srv_count, dst_host_same_srv_rate
2	error_rate, srv_error_rate, dst_host_error_rate, dst_host_srv_error_rate
3	error_rate, srv_error_rate, dst_host_error_rate, dst_host_srv_error_rate
4	num_compromised, num_root

Pearson 상관계수를 통한 특징선택 기법에서는 NSL-KDD 데이터 셋의 numeric 속성들(31개)의 특징들에 대해서만 진행하였다. 0.9 이상의 상관계수를 가진 특징들 간의 관계를 무방향 그래프 자료구조로 표현한 결과 4쌍의 완전 그래프로 표현되며, 표 2는 4쌍의 그래프들의 노드들을 보여준다. 각 그래프들 사이에서 특징 집합을 대표할 수 있는 최소수의 특징들을 선택하면 특징 벡터의 크기를 최소화 할 수 있다[1]. 하지만 표 2의 결과 그래프는 완전 연결 그래프로 어떠한 것을 임의 삭제하여도 무방하다. 이를 통해 113개의 부분 특징 집합이 선택되었다.

<표 3> HFS를 통해 선택된 특징 집합

특징 집합 (39)
count, diff_srv_rate, dst_bytes, dst_host_count, dst_host_diff_srv_rate, dst_host_same_src_port_rate, dst_host_srv_count, dst_host_srv_diff_host_rate, duration, flag_REJ, flag_RST, flag_S0, flag_SF, hot, is_guest_login, logged_in, num_compromised, num_failed_logins, num_file_creations, protocol_type_icmp, protocol_type_tcp, protocol_type_udp, error_rate, root_shell, same_srv_rate, serror_rate, service_domain_u, service_eco_i, service_ftp, service_ftp_data, service_http, service_other, service_private, service_smtp, service_telnet, src_bytes, srv_count, srv_diff_host_rate, wrong_fragment

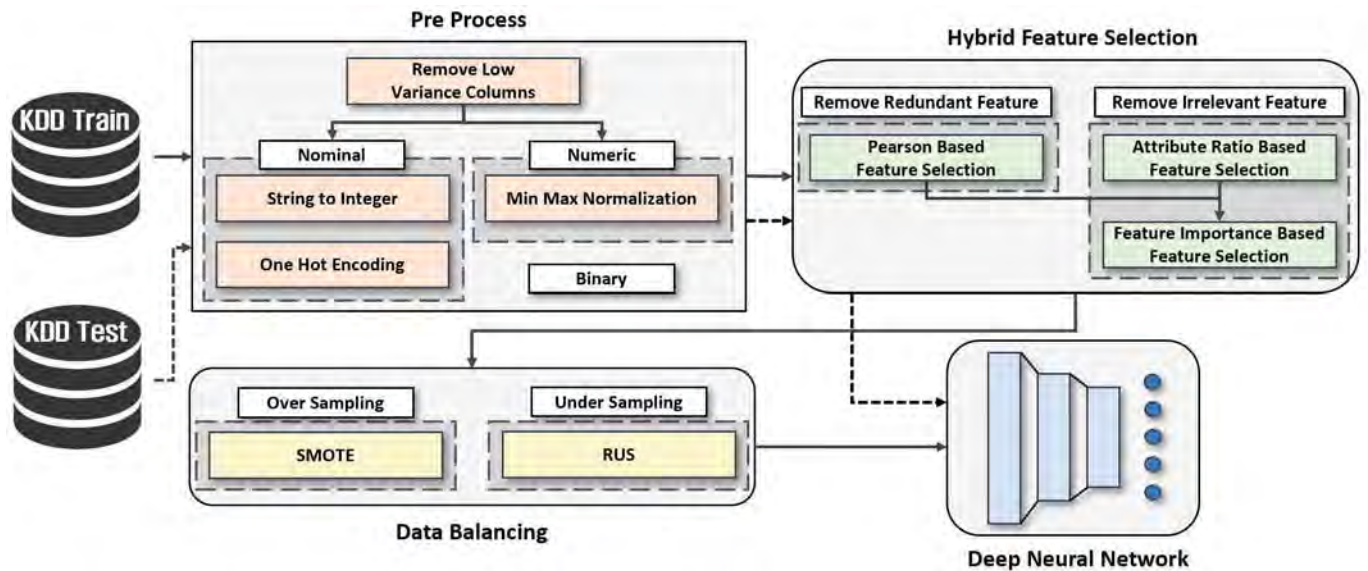


그림 1. 제안하는 네트워크 침입 탐지 모델

AR 기반 특징 선택 기법에서는 0.1 임계값을 이용해 특징들을 선택한 결과 50개의 특징 집합이 선택되었으며, Feature Importance는 Random Forest 모델을 학습시켜 추출하여 상위 55개의 특징 집합을 선출하였다. 해당 특징 선택 기법들의 교집합을 통해 제안되는 HFS 기법의 최종 특징 집합은 표 3과 같이 39개 특징 집합으로, 32% 규모로 축소되었다.

3.3 Data Balancing

불균형 데이터를 통하여 심층 신경망 모델을 학습할 경우는 다수 클래스들에 편향된 학습을 진행하기에 소수 클래스들의 분류 성능은 크게 떨어진다. 본 논문에서는 심각한 불균형 데이터로 분류되는 NSL-KDD 데이터 셋의 불균형 문제를 해소하기 위해서 그림 1에 표기된 SMOTE 기법과 RUS 기법을 활용한다. 표 4를 통해 데이터 불균형을 해소한 데이터 셋의 샘플 수와 비율을 확인할 수 있으며, 다수 클래스는 언더 샘플링을, 소수 클래스는 오버샘플링을 진행하였다.

<표 4> NSL-KDD Dataset 클래스별 샘플

	KDD Train+		Balanced KDD Train+	
Normal	67343	(53%)	45000	(25%)
DoS	45927	(37%)	45927	(25.2%)
Probe	11656	(9.11%)	30000	(16.6%)
U2R	52	(0.04%)	30000	(16.6%)
R2L	995	(0.85%)	30000	(16.6%)
Total	125973		180927	

4. 실험

<표 5> 실험에 사용된 심층 신경망 구조

DNN Parameters	
Architecture	[39-256-512-512-5]
Activation / Initializer	Relu, Softmax / He Uniform
Regularizer / Strength	L2 / 0.0001
Optimizer / Learning rate	Adam / 0.0005
Loss	Cross Entropy

실험에 사용한 심층 신경망의 구조는 표 5와 같으며, 전체 학습 데이터의 20%는 validation set으로 활용하였다. 학습 중 validation loss가 10 epoch 이상 증가할 경우 조기 멈춤을 실행하였으며, 이후 가장 validation loss가 낮은 모델을 선택하여 실험에 사용하였다.

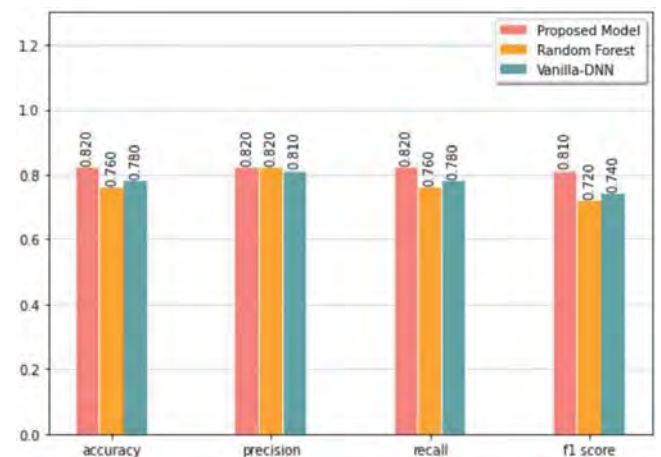


그림 2 제안된 모델의 성능 비교

불균형 데이터에 대해서 Accuracy만을 가지고 평가하는 것은 부적합하다. 따라서 본 논문에서는 학습된 모델의 성능 평가로 Accuracy, Precision, Recall, F1 Score를 평가 지표로 사용하였다. 그림 2를 참조하면 제안된 모델의 4가지 성능지표가 비교 모델들에 비해 더 좋은 것으로 확인된다.

<표 6> 제안된 모델의 클래스별 성능 평가

Proposed Models				
	precision	recall	f1	support
DoS	0.96	0.85	0.90	7458
Probe	0.84	0.66	0.74	2421
R2L	0.64	0.42	0.51	2754
U2R	0.26	0.14	0.18	200
Normal	0.77	0.96	0.86	9711
Total	0.82	0.82	0.81	22544

<표 7> 비교 모델들의 소수 클래스 분류 결과

Random Forest				
	precision	recall	f1	support
R2L	0.99	0.08	0.15	2754
U2R	0.5	0.01	0.02	200
Vanilla DNN				
R2L	0.95	0.08	0.14	2754
U2R	0.	0.	0.	200

표 6은 본 논문에서 제안된 모델의 각 클래스별 성능 지표로, 표 7과 비교하면 소수 클래스들의 성능 지표들을 비교할 수 있다. 특징 선택과 데이터 균형을 맞추지 않은 데이터를 학습한 두 모델은 소수 클래스들에 대해서 제대로 분류를 하지 못하고 있는 것을 확인할 수 있다. 단순 심층 신경망의 모델의 경우 네트워크 구조는 동일하지만 모든 U2R 클래스의 분류에 실패한 것을 확인하였다. 그에 반해 본 논문에서 제안된 모델은 R2L 클래스의 탐지 성능의 경우 눈에 띄게 상승한 것이 보이며, U2R 클래스 탐지 성능 또한 개선이 된 것을 확인할 수 있다. 그럼에도 불구하고 U2R의 분류 성능이 낮은 것을 확인할 수 있는데, 이는 Train 셋에서 제공되는 데이터양이 52개인 반면에 Test 셋에서 제공되는 양은 200개로 더 적은 것을 알 수 있다. 따라서 테스트 데이터들의 분포가 더 넓게 분포되어 있을 것으로 분석된다.

5. 결론

본 논문에서는 네트워크 침입 탐지의 성능 개선을 위해 Hybrid Feature Selection 기법을 제안하였다. 또한 학습에 사용된 NSL-KDD 데이터 셋의 불균형 문제를 해소하여 성능이 개선된 네트워크 침입 탐지 모델을 제안하였다. 특징 추출을 통해 32% 규모로 입력 차원을 축소할 수 있었으며, 오버 샘플링 기법을 통해 소수 클래스들의 성능 개선을 실험을 통해 확인할 수 있었다. 이를 통해 본 논문에서 제안한 모델의 F1 Score 가 두 모델에 비해서 7~9% 높은 것으로 확인할 수 있었다. 향후 연구로는 VAE, GAN과 같은 생성모델들을 통해 데이터 증감(Data Augmentation)기법을 연구하여, SMOTE를 대체할 수 있으며, 또한 다른 침입 탐지 데이터 셋을 통한 연구 또한 진행할 수 있다.

Acknowledgement

본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다(UD190016ED).

참고문헌

- [1] 강승호, 정인선, and 임형석. "실시간 공격 탐지를 위한 Pearson 상관계수 기반 특징 집합 선택 방법." 융합보안논문지 18.5 (2018): 59-66.
- [2] Chae, Hee-su, et al. "Feature selection for intrusion detection using NSL-KDD." Recent advances in computer science (2013): 184-187.
- [3] Haq, Nutan Farah, Abdur Rahman Onik, and Faisal Muhammad Shah. "An ensemble framework of anomaly detection using hybridized feature selection approach (HFSA)." 2015 SAI Intelligent Systems Conference (IntelliSys). IEEE, 2015.
- [4] Song, Jungsuk, et al. "Correlation analysis between honeypot data and IDS alerts using one-class SVM." Intrusion Detection Systems (2011): 173-192.
- [5] Yang, Xin-Li, et al. "High-impact bug report identification with imbalanced learning strategies." Journal of Computer Science and Technology 32.1 (2017): 181-198.
- [6] Tavallae, Mahbod, et al. "A detailed analysis of the KDD CUP 99 data set." 2009 IEEE symposium on computational intelligence for security and defense applications. IEEE, 2009.

가사의 감정 분석을 이용한 GAN 기반 댄스 공연 배경 생성 방법

윤혜원, 곽정훈, 성연식*
동국대학교 멀티미디어공학과

hyewon@dongguk.edu, jeonghoon@dongguk.edu, sung@dongguk.edu

GAN-based Dance Performance Visual Background Generation Method using Emotion Analysis on Lyrics

Hyewon Yoon, Jeonghoon Kwak, Yunsick Sung*
Dept. of Multimedia Engineering, Dongguk University-Seoul

요 약

최근 인공지능을 활용하여 예술 작품에 몰입할 수 있도록 무대 효과를 디자인하는 연구가 진행되고 있다. 무대 효과 중에서 무대 배경은 공연의 분위기를 형성한다. 춤의 장르별로 무대 배경에 사용되는 이미지를 생성하기 위해 소셜 미디어 기반 무대 배경 생성 시스템이 있다. 하지만 같은 장르 춤은 동일한 무대 배경 이미지가 제공되는 문제가 있다. 같은 장르의 춤이지만 노래의 분위기를 반영하여 차별된 무대 배경 이미지를 제공하는 것이 필요하다. 본 논문은 노래 가사의 감정을 활용하여 Generative Adversarial Network(GAN)을 통해 각 노래의 분위기를 고려한 무대 배경 이미지를 생성하는 방법을 제안한다. GAN은 노래에 포함된 단락별 감정 단어를 추출하여 스타일을 생성하도록 학습된다. 학습된 GAN은 노래 가사에 포함된 감정 단어를 활용하여 곡의 분위기를 반영한 무대 배경 이미지를 생성한다. 노래 가사를 고려하여 무대 배경 이미지를 생성함으로써 곡의 분위기가 고려된 무대 배경 이미지 생성이 가능하다.

1. 서론

춤은 감정을 표현하기 위해 신체 언어를 사용하는 예술로 춤 공연은 보통 춤 예술과 음악, 조명, 연기 및 무대 배경과 같은 다양한 종류의 무대 효과가 결합된다[1]. 무대 효과 중에서 무대 배경은 분위기를 제공하므로 가장 중요한 기능 중 하나이다. 무대 배경을 제작하기 위하여 곡의 내용, 곡의 분위기 등과 같이 복합적인 요소 고려가 필요하다.

소셜 미디어를 기반으로 춤의 장르(발레, 벨리 댄스, 스트리트 댄스, 모던 댄스, 탱고, 왈츠)에 따라 무대 배경 이미지를 하는 추천하는 시스템이 있다 [1]. 무대 배경 추천 시스템은 춤의 장르별 댄서의 게시물 공유나 클릭 액션 등과 같은 장르별 댄서의 관심사를 활용하여 무대 배경 이미지가 추천된다.

* 교신저자: 성연식 (sung@dongguk.edu)

"본 연구는 과학기술정보통신부 및 정보통신기획평가원의 글로벌핵심인재양성지원사업의 연구결과로 수행되었음"(2019-0-01585)

추천된 무대 배경 이미지는 공연에서 사용되는 무대 배경 이미지로 사용 가능하다. 하지만 춤의 장르에 따라 무대 배경을 만드는 것은 각 노래 고유의 분위기를 반영하지 않아 같은 장르의 춤은 동일한 무대 배경 이미지가 제공된다. 동일한 춤의 장르일지라도 노래 고유의 분위기를 반영하여 차별화된 무대 배경 이미지를 생성하는 것이 필요하다.

노래의 고유 분위기를 파악하기 위하여 노래 가사에 포함된 감정 단어를 사용하여 각 노래의 분위기를 파악한다[2]. 노래의 가사에 포함된 감정단어로 노래의 분위기를 분석 가능하다. 하지만 노래 가사에 포함된 감정단어를 활용하여 무대 배경 이미지를 생성하는 방법이 요구된다.

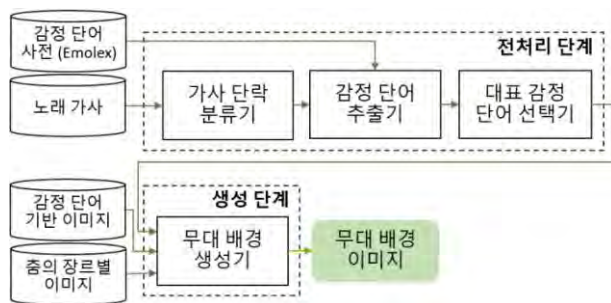
문장을 기반으로 이미지를 생성하기 위하여 Generative Adversarial Network(GAN)을 활용한다 [3]. GAN을 통하여 문장에 맞는 이미지를 생성한다. 하지만 문장에 포함된 분위기를 반영한 이미지를 제공하지 못하는 단점이 있다. GAN을 활용하여 노래 가사의 분위기를 전체 이미지에 적용하는 방법이 필

요하다.

본 논문은 GAN을 기반으로 노래 가사에 포함된 감정 단어를 이용하여 무대 배경 이미지를 생성하는 방법을 제안한다. 노래 가사에 포함되는 감정 단어 (Emotion Word)를 추출한다. GAN은 추출된 감정 단어가 나타내는 색상 특징 및 Stroke 특징을 반영한 무대 배경 이미지가 생성된다. 곡의 분위기에 맞는 새로운 무대 배경 이미지를 생성한다.

2. GAN을 활용한 노래 가사의 감정 단어 기반 무대 배경 생성 방법

노래 가사에 포함된 감정 단어를 활용하여 그림 1과 같이 무대 배경 이미지를 생성하는 방법을 제안한다. 노래 가사를 가사 단락 분류기를 통해 단락별로 구분한다. 일반적인 노래의 가사는 Verse, Chorus, Bridge로 구성된다[4]. Verse, Chorus, Bridge를 나눈 단위를 단락이라고 정의한다. Bridge는 단락이 너무 짧아 의미를 담기 어렵기 때문에 본 논문에서는 가사 단락 분류기를 통해 추출된 Chorus와 Verse에서 추출된 감정 단어를 활용한다.



(그림 1) 무대 배경 생성 과정

감정 단어 추출기는 단락에 포함된 다수의 감정 단어를 추출한다. 하나의 단락에는 하나 이상의 감정 단어가 포함된다. 단락에 포함된 감정 단어들을 추출하기 위해 감정 단어 사전(Emolex)을 이용한다[2]. Emolex는 심리학자 Plutchik이 제시한 인간의 여덟 가지 기본 감정(anger, anticipation, disgust, fear, joy, sadness, surprise, trust)에 긍정과 부정을 더하여 10차원 수준의 감정 단어 사전을 제공한다. Emolex는 14,177개의 단어가 들어있다. 감정 단어 추출기를 통해 Emolex와 노래 가사에 포함된 단락별 감정 단어가 일치하는 감정 단어를 추출한다.

대표 감정 단어 선택기는 단락별로 대표가 되는 감정 단어를 선택한다. 단락별 추출된 다수의 감정 단어를 기반으로 TF-IDF[5]를 통해 단락별 대표하는 감정 단어를 선택한다.

무대 배경 생성기는 GAN을 활용하여 감정 단어를 기반으로 무대 배경 이미지를 생성한다. 춤의 장르별 이미지는 춤의 장르를 표현하는 이미지이다. GAN의 생성기에서는 춤의 장르별 이미지에 감정 단어 기반 이미지 스타일을 합성하여 무대 배경 이미지를 생성한다. 감정 단어 기반 이미지는 추출된 단락별 대표 감정 단어가 그림 제목 또는 설명에 포함되어있는 이미지이다. GAN의 판별기에서는 GAN의 생성기에서 무대 배경 이미지와 감정 단어 기반 이미지가 판별 가능한지 확인한다. GAN의 생성기를 통하여 춤의 장르별 이미지에 감정 단어 기반 이미지의 색상 특징 및 Stroke 특징이 반영되어 무대 배경 이미지가 생성된다.

본 논문에서는 노래 가사의 단락별 대표 감정 단어로부터 학습된 스타일을 춤의 장르별 이미지에 적용하여 단락별 무대 배경 이미지 생성이 가능하다.

사사표기

“본 연구는 과학기술정보통신부 및 정보통신기획평가원의 글로벌핵심인재양성지원사업의 연구결과로 수행되었음”(2019-0-01585)

참고문헌

- [1] Wen, J., She, J., Li, X., Mao, H., “Visual Background Recommendation for Dance Performances Using Deep Matrix Factorization,” ACM Transactions on Multimedia Computing Communications and Applications, Vol. 14, No. 1, pp. 1-19, 2018.
- [2] 이재환, 임혜원, 김형주, “가사의 감정 분석과 구조 분석을 이용한 노래간 유사도 측정”, 정보과학회 컴퓨팅의 실제 논문지, Vol. 22, No. 10, pp. 479-487, 2016.
- [3] Zhang, H., Xu, T., Li, H., Zhang, S., Wang, X., Huang, X., Metaxas, D.N., “Stackgan++: Realistic Image Synthesis with Stacked Generative Adversarial Networks,” IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 41, No.8, pp. 1947-1962, 2019.
- [4] “Ten Minute Master No 18: Song Structure,” MUSIC TECH magazine, pp. 62-63, 2003.
- [5] Chowdhury, G.G., “Introduction to Modern Information Retrieval,” Facet publishing, 2010.

단일 LiDAR를 활용한 End-to-End 기반 3D 모델 생성 방법

곽정훈, 성연식*
동국대학교 멀티미디어공학과
{jeonghoon, sung}@dongguk.edu

End-to-End based 3D Model Generation Method using a Single LiDAR

Jeonghoon Kwak, Yunsick Sung*
Dept. of Multimedia Engineering, Dongguk University-Seoul

요 약

원격 및 가상환경에서 사용자의 동작에 따른 3D 모델을 제공하기 위해 light detection and range (LiDAR)로 측정된 3D point cloud로 사용자의 3D 모델이 생성되어 원격 및 가상환경에 사용자의 모습이 제공된다. 하지만 3D 모델을 생성하기 위해서는 사용자의 신체 전부가 측정된 3D point cloud가 필요하다. 사용자의 신체 전체를 측정하기 위해서는 적어도 두 개 이상의 LiDAR가 필요하다. 두 개 이상의 LiDAR를 사용할 경우에는 LiDAR를 사용할 공간과 LiDAR를 구비하기 위한 비용이 발생한다. 단일 LiDAR로 3D 모델을 생성하는 방법이 요구된다. 본 논문에서는 단일 LiDAR에서 측정된 3D point cloud를 이용하여 3D 모델을 생성하는 방법이 제안된다. End-to-End 기반 Convolutional Neural Network (CNN) 모델로 측정된 3D point cloud를 분석하여 사용자의 체형과 자세를 예측하도록 학습한다. 기본자세를 취하는 동안 수집된 3D point cloud로 기본이 되는 사용자의 3D 모델을 생성한다. 학습된 CNN 모델을 통하여 측정된 3D point cloud로 사용자의 자세를 예측하여 기본이 되는 3D 모델을 수정하여 3D 모델을 제공한다.

1. 서론

사용자의 모습을 가상 및 원격환경에서 활용하기 위하여 사용자의 모습을 제공하기 위한 3D 모델이 생성된다. 3D 모델을 생성하기 위하여 가상 및 원격 환경에서 사용할 사용자의 3D 모델을 Light Detection And Range (LiDAR) 또는 깊이 카메라로 측정된 3D point cloud로 사용자의 3D 모델이 생성되어 제공된다[1]. 측정된 3D point cloud로 3D 모델의 외형이 결정된다. 3D point cloud로 3D 모델을 구성하기 위해서는 최소 2개 이상의 센서로 3D point cloud의 측정이 필요하며, 사용자의 신체의 360도를 측정하기 위한 공간도 요구된다. 다중 센서를 사용하여 3D 모델을 생성하는 과정에서 따라 발생하는 비용 또는 공간적인 문제를 해결하기 위하여

단일 센서로 실시간으로 사용자에게 동작에 따른 3D 모델을 생성하는 방법이 필요하다.

단일 센서로 측정된 3D point cloud과 사전에 사용자 동작에 따라 3D 모델을 제공하는 템플릿을 사용하여 3D 모델을 생성한다[2]. 측정된 3D point cloud가 템플릿에 포함되는 3D 모델 중에서 가장 유사한 3D 모델을 찾아 3D 모델을 제공한다. 그러나 3D 모델을 생성하는 과정에서 다양한 사용자의 신체 또는 사용자의 다양한 동작에 사전에 정의하기에는 한계가 발생한다. 사용자의 다양한 동작에 3D 모델 템플릿을 사전에 구축하지 않고 3D 모델을 제공하는 방법이 필요하다.

단일 카메라로부터 촬영된 단일 이미지와 3D 모델 템플릿을 활용하여 사용자의 동작에 맞게 3D 모델이 제공된다[3]. 단일 이미지로부터 사용자의 자세와 체형을 예측하고 예측된 자세 및 체형에 따라 3D 모델이 보정된다. 하지만 단일 이미지로부터 사용자의 자세를 추정하기 위한 방법이 필요하다. 사용자의 자세를 사전에 지정하지 않고 사용자에게 자세

* 교신저자: 성연식 (sung@dongguk.edu)

"본 연구는 과학기술정보통신부 및 정보통신기획평가원의 글로벌핵심인재양성지원사업의 연구결과로 수행되었음"(2019-0-01585)

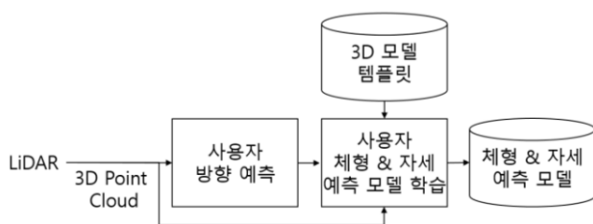
에 맞게 3D 모델을 제공하는 방법이 요구된다.

본 논문은 3D 모델 템플릿을 활용하여 단일 3D point cloud를 기반으로 3D 모델을 생성하는 방법을 제안한다. 3D point cloud가 End-to-End 기반 Convolutional Neural Network (CNN) 모델에 입력되어 3D 모델의 체형과 자세를 예측할 수 있도록 학습한다. CNN 모델은 3D 모델이 3D point cloud와 일치할 수 있게 학습된다. 실행 시에는 사용자의 외형과 유사한 기본 3D 모델을 생성한다. 학습된 CNN 모델을 측정된 3D point cloud를 활용하여 사용자의 자세를 예측한다. 예측된 자세를 기반으로 기본 3D 모델을 보정함으로써 사용자의 3D 모델이 제공된다.

2. 3D Point Cloud 기반 3D 모델 생성 방법

사용자로부터 측정된 3D point cloud를 이용하여 사용자의 체형과 자세에 맞는 3D 모델을 생성하기 위해 CNN 모델을 학습하는 과정은 그림 1과 같다. 사용자 방향 예측에서는 사용자의 신체가 전방이 되는 방향을 예측한다. 3D 모델은 전체를 제공되지만 3D point cloud는 사용자의 신체 일부가 측정되기 때문에 사용자 신체에 맞게 회전이 필요하다. 예측된 사용자 방향을 활용하여 사용자 신체의 전방과 같이 3D 모델 템플릿의 3D 모델의 방향이 동일하게 3D 모델의 방향을 변경한다.

사용자 체형 & 자세 예측 모델 학습에서는 3D 모델 템플릿을 활용하여 CNN 모델을 학습한다. 3D 모델 템플릿은 SMPL 모델[4]과 같이 다양한 남성 및 여성의 체형이 3D 모델을 제공되며 스켈레톤을 기반으로 체형과 자세를 변형할 수 있다. CNN 모델은 입력된 사용자의 3D point cloud를 이용하여 3D 모델의 체형과 자세를 예측할 수 있게 학습된다. 3D point cloud에 포함된 위치들과 3D 모델간의 유클리디안 거리로 차이가 계산된다. 계산된 차이를 이용하여 CNN 모델이 수정된다.

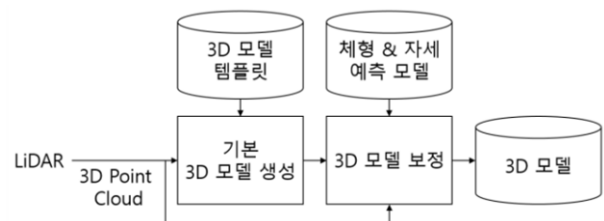


(그림 1) 체형과 자세를 예측하기 위한 학습과정

사용자로부터 측정된 3D point cloud를 이용하여 사용자의 체형과 자세에 따른 3D 모델을 생성하는

과정은 그림 2과 같다. 기본 3D 모델 생성에서는 사용자의 기본 3D 모델을 생성한다. 기본자세를 수행하는 과정동안 전체 신체의 3D point cloud를 수집한다. 수집된 3D point cloud와 유사한 3D 모델 템플릿을 찾고 사용자의 신체 특성에 맞게 보정된다.

3D 모델 보정에서는 학습된 CNN 모델을 활용하여 3D point cloud를 이용하여 사용자의 자세가 예측된다. CNN 모델에 3D point cloud의 체형과 자세가 예측된다. 하지만 체형 정보는 이미 사용자의 신체에 맞게 추론하였기 때문에 사용하지 않고 자세의 값만 활용한다. 기본 3D 모델을 현재 사용자의 자세에 맞게 수정하여 사용자의 모습을 제공하는 3D 모델이 제공된다.



(그림 2) 체형과 자세를 제공하는 3D 모델 생성과정

사사표기

"본 연구는 과학기술정보통신부 및 정보통신기획평가원의 글로벌핵심인재양성지원사업의 연구결과로 수행되었음"(2019-0-01585)

참고문헌

- [1] Kim, Y., Baek, S., Bae, B., "Motion Capture of the Human Body Using Multiple Depth Sensors," ETRI Journal. Vol. 39, No. 2, pp. 181-190, 2017.
- [2] Zhao, T., Li, S., Ngan, K.N., Wu, F., "3-D Reconstruction of Human Body Shape from a Single Commodity Depth Camera," IEEE Transactions on Multimedia, Vol. 21, No. 1, pp. 114-123, 2019.
- [3] Kanazawa, A., Black, M.J., Jacobs, D.W., Malik, J., "End-to-end Recovery of Human Shape and Pose," IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Salt Lake City, USA, 2018, pp. 7122-7131.
- [4] Loper, M., Mahmood, N., Romero, J., Pons-Moll, G., Black, M.J., "SMPL: A Skinned Multi-person Linear Mode," ACM Transactions on Graphics, Vol. 34, No. 6, pp.1-16, 2015.

경량 딥러닝과 지식베이스를 활용한 모바일 질환별 식품 추천 시스템

현범수*, 김도현**, 이상근***

*고려대학교 컴퓨터학과

**고려대학교 컴퓨터·전파통신공학과

***고려대학교 인공지능학과

bshyeon@korea.ac.kr, dhkim1028@korea.ac.kr, yalphy@korea.ac.kr

Mobile Food Recommendation System for Patients Using Light-weight Deep Learning and Knowledge Bases

Bumsu Hyeon*, Dohyun Kim**, SangKeun Lee***

*Dept. of Computer Science and Engineering, Korea University

**Dept. of Computer and Radio Communications Engineering, Korea University

***Dept. of Artificial Intelligence, Korea University

요 약

본 논문에서는 딥러닝과 지식베이스를 융합하여 활용한 질환 인식 및 식품 추천 시스템을 제안한다. 제안하는 시스템은 온전히 모바일 디바이스 내에서 작동하는 시스템이다. 본 시스템은 압축된 딥러닝 모델을 이용해 사용자 대화 텍스트를 분석하여 사용자의 질환을 예측한다. 그 후, 지식베이스를 기반으로 해당 질환 관리에 도움이 되는 식품을 매칭하고 사용자에게 추천한다. 이는 사용자 친화적 헬스케어 애플리케이션으로써 체크리스트 작성 등 번거로운 작업 없이도 사용자에게 유용한 건강 정보를 제공할 수 있다.

1. 서론

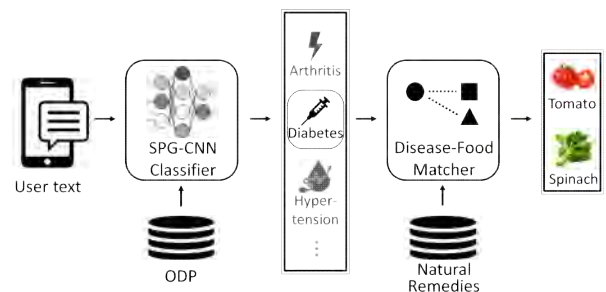
고령화와 만성 질환의 만연으로 스마트 헬스케어의 수요가 증가하고 있다. 이에 따라 딥러닝을 활용한 다양한 헬스케어 응용 시스템이 제안되었고, 괄목할 만한 성능 및 효용성을 보이고 있다[1]. 또한 관련 분야에서 딥러닝과 지식베이스를 융합한 시스템에 관한 연구 역시 활발하게 이루어지고 있다.

하지만 헬스케어 애플리케이션을 구축하기 위해 서버-클라이언트 구조를 사용하면 민감정보로 분류되는 건강정보를 취급하는 데 있어 네트워크 전송, 저장 등에 엄격한 규제가 적용된다. 반면, 시스템 전체를 사용자의 디바이스에서 구동할 경우, 이러한 문제를 피할 수 있으나 컴퓨팅 자원이 현저히 제한된다.

본 논문에서는 위와 같은 문제를 해결하기 위해 사용자 디바이스 내에서 구동되는 경량 헬스케어 시스템을 제안한다. 본 시스템은 모바일 환경에서 구동되며, 사용자에게 개인화된 질환별 식품 추천 서비스를 제공한다. 본 시스템에서는 경량 딥러닝 모델인 SPG-CNN[2]을 채택하고, 딥러닝 모델 압축

기법을 적용하여 매우 적은 리소스를 사용하는 텍스트 분류 모델을 구축한다. 텍스트 분류 모델을 이용해 사용자 텍스트로부터 질환을 예측한 후 지식베이스 Natural Remedies를 활용해 예측된 질환과 추천 후보 식품을 매칭하여 사용자에게 제공한다.

제안하는 시스템은 질환 예측 정확도 66.7%로 상당한 예측률을 나타내어 만성 질환자 및 위험군 사용자들에게 건강 관리를 위한 유용한 정보를 제공할 수 있을 것으로 기대된다.



(그림 1) 시스템 구조.

2. 제안하는 시스템

그림 1은 전체 시스템 구조를 보여준다. 본 시스템은 모바일 디바이스의 메신저 대화 텍스트를 추출

한 후 텍스트 분류기를 통해 대화 정보로부터 사용자가 가질 수 있는 질환을 예측한다. 예측된 질환은 질환-식품 매칭을 통해 식품과 매칭된다.

2.1 질환 예측

질환 예측에는 딥러닝 모델 SPG-CNN[2] 및 지식베이스 ODP¹⁾를 사용한다. SPG-CNN은 경량 합성곱 신경망(convolutional neural network)으로, 멀티태스킹 학습(multi-task learning) 기법을 활용한 텍스트 분류 모델이다. 본 시스템에서는 SPG-CNN을 8비트 양자화(8-bit quantization)를 통해 압축하여 사용한다. 또한 SPG-CNN의 파라미터 중 상당수를 차지하는 워드 임베딩(word embedding)에는 압축률을 높이기 위해 별도로 Compositional Code Learning 압축 기법[3]을 사용한다. 표 1에서 위 압축 기법 사용 시 모델 정확도에 거의 손실을 주지 않고 9배 이상의 압축률을 달성함을 확인할 수 있다. SPG-CNN의 학습 데이터에는 ODP를 사용한다. ODP는 온라인 참여자들이 400만여 개의 웹페이지를 주제에 따라 80만여 개의 카테고리로 분류한 지식베이스이다. 본 시스템에서는 [4]에서 제안한 방법으로 ODP를 정제한 후 질환명에 해당하는 카테고리라 그 카테고리에 속하는 웹 페이지를 학습 데이터로 사용한다.

	크기	정확도
압축 전	233 MB	67.2%
압축 후	25 MB	66.7%

(표 1) 압축 전·후 모델 크기 및 정확도

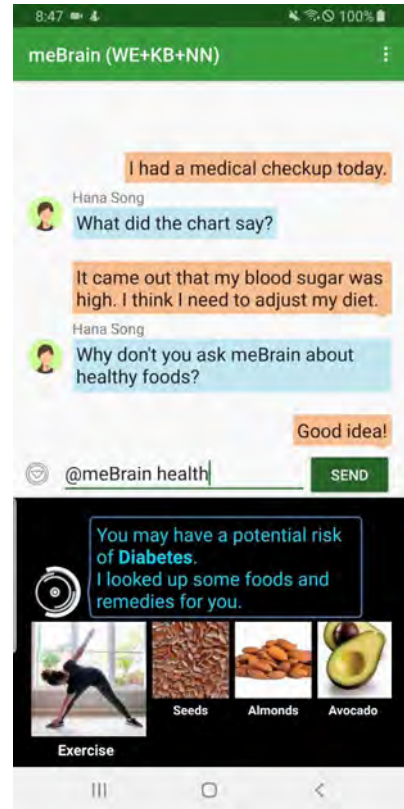
2.2 질환-식품 매칭

질환과 식품을 매칭하는 과정에는 지식베이스 Natural Remedies²⁾를 룩업하는 방식을 사용한다. Natural Remedies는 질환별 추천 식품을 추천도 순으로 정리한 지식베이스로, 121개의 질환에 대응되는 485개의 식품이 존재한다. 여기에는 식품 외에도 운동 등 생활습관 관련 내용도 일부 포함되어 있다. 본 시스템에서는 추천도가 높은 4개의 항목을 사용자에게 제시한다. 그림 2는 안드로이드 스마트폰에서 실행 중인 본 시스템을 보여준다.

3. 결론

본 논문에서는 압축된 딥러닝 모델과 지식베이스

를 활용하여 모바일 환경에서 사용자의 대화 텍스트로부터 질환을 예측하고, 해당 질환의 관리에 도움이 되는 식품을 추천하는 시스템을 제안하였다. 향후 본 시스템은 예측된 질환 정보를 활용하여 의료 정보 등 더 다양한 서비스를 제공하는 플랫폼으로 확장될 수 있을 것으로 기대된다.



(그림 2) 질환 예측 및 식품 추천 화면.

참고문헌

- [1] R. Miotto, F. Wang, S. Wang, X. Jiang, and J. T. Dudley, "Deep Learning for Healthcare: Review, Opportunities and Challenges," Briefings in Bioinformatics, 2017, pp. 1 - 11.
- [2] K. Kim, Y. Kim, J. Lee, J. Lee, and S. Lee, "From Small-scale to Large-scale Text Classification," The World Wide Web Conference (WWW), San Francisco, 2019, pp. 853-86.
- [3] R. Shu and H. Nakayama, "Compressing Word Embeddings via Deep Compositional Code Learning," International Conference on Learning Representations (ICLR), Vancouver, 2019.
- [4] J. Lee, J. Ha, J. Jung, and S. Lee, "Semantic Contextual Advertising Based on the Open Directory Project," ACM Trans. Web (TWB), vol. 7, no. 4, 2013, article 24.

1) <http://odp.org/>

2) <http://classic.personalremedies.com/Remedy.asp>

비디오 감시 카메라 내 사물 추적을 통한 골목길 교차로 사고 예방 시스템

김형진*, 김준영*, 박주홍*, 심재욱*, 고석주*, 김정석**

*경북대학교 컴퓨터학부

**SK 텔레콤

gudwls15978@gmail.com, juneyoung5919@gmail.com, kr.xerus.inauris@gmail.com, wodnr96@gmail.com,
sjkoh@knu.ac.kr, jeongseok.kim@sk.com

Traffic-Accident-in-Alley Prevention System by Object Tracking in Video Surveillance Camera Streaming Video

Hyungjin Kim*, Juneyoung Kim*, Juhong Park*, Jaek Shim*, Seokju Ko*, Jeongseok Kim**

*Dept. of Computer Science Engineering, Kyungpook National University

**SK Telecom

요 약

길이 좁고 차도와 인도의 구분이 없는 골목길의 특성상 사각지대가 많고 보행자의 동선을 예측하기 힘들어 교통사고가 많이 발생하고 있다. 따라서 본 논문에서는 AI를 활용, 영상 내 사물을 추적하여 골목길에서의 사고를 예방하는 시스템을 제안한다. 해당 시스템은 Object - Detection & Tracking을 사용하여 보행자 및 차량을 식별·추적하여 두 개 이상의 사물이 동시에 교차로에 접근 시 사고 예방 알람을 발생시킨다. 이 시스템을 전국에 설치되어 있는 CCTV에 활용하면 추가적인 비용과 설치 시간에 제한받지 않고 전국적으로 응용할 수 있을 것으로 기대된다.

1. 서론

1769년 최초의 자동차가 발명된 후, 자동차 산업이 눈부시게 발전함에 따라 교통사고 역시 항상 함께 발생해왔다. 한국에서도 1978년에 자동차의 급격한 증가와 함께 센터시스템을 갖춘 온라인 신호시스템이 등장한 후 차량신호등, 보행신호등이 설치 기준에 따라 도로 곳곳에 설치되어서 교통사고 방지에 일조해왔다. 신호등과 같은 교통안전장치 마련과 정부의 교통안전사업 추진, 그리고 운전자 및 시민의 의식이 수준이 향상됨에 따라 2000년대에 접어들어 교통사고 발생수는 점점 줄어드는 추세이지만 상대적으로 무방비한 교차로에서 발생하는 사고 수는 오히려 늘어나는 추세이다. 그 중에서도 교통사고 사망자 중 보행자 비중은 한국이 OECD 가입 국가 중에서도 가장 높은 축에 속한다 [1].

2019년 4분기, 한국 교통안전공단에서 교통안전 실현을 위한 아이디어 공모전[2]을 개최함에 이어 2020년에는 경찰청, 국토부, 행안부는 국민생명 지키기 3대 프로젝트 중 ‘교통사고 절반 줄이기’

의 일환으로 보행자에 대한 교통안전 종합대책[3]을 추진한 만큼 해당 문제는 정부 차원에서도 해결해야 할 주된 과제 중 하나이다.

한편 CCTV에 관해서는 한국은 CCTV 공화국이라고 불릴 만큼 세계 최대 규모이다. 인구밀도와 국토면적 대비 CCTV 설치율은 압도적 1위이고 이는 앞서 말한 도로 및 교차로에도 해당된다[4]. 이 CCTV들을 활용한다면 안전 사각지대에서 발생하는 교통사고를 줄이는 것에 큰 도움이 될 것이다.

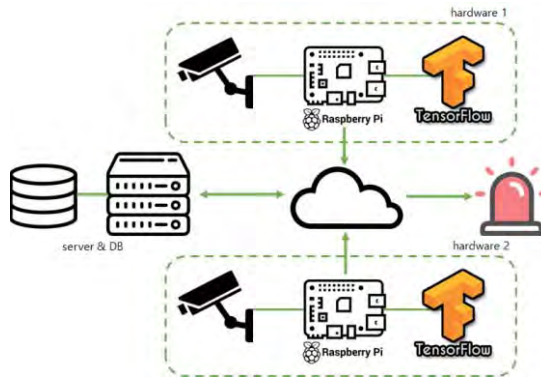
따라서 본 논문에서는 비디오 감시 카메라, 임베디드 보드와 알람 시스템을 결합하여 간이 신호등 및 경보기 역할을 하는 하드웨어를 구성한 후 머신 러닝 기반의 사물 추적을 이용하는 골목길 교차로 사고 예방 시스템을 제안하고자 한다.

2. 본론

2.1. 시스템의 전체 구조

사각지대 위험인식 시스템은 크게 위험 상황을 감지하는 서버와 각 카메라와 구역의 정보를

저장하고 관리하는 데이터베이스, 카메라 영상을 처리하고 서버와 통신하는 임베디드 보드, LED 알람으로 구성되어 있다. 시스템 전체 구조는 (그림 1) 과 같이 나타낼 수 있다.



(그림 1) 사각지대 위험인식 시스템 전체 구조.

2.2. 프로그램 동작 과정

각각의 임베디드 보드는 내장된 카메라를 사용하여 실시간으로 영상을 촬영하고, 기존에 학습된 모델을 사용하여 영상 내의 사람과 자동차를 인식한다. 이때 인식된 사람과 자동차의 움직임을 감지한다.

그 후 각각의 임베디드 보드는 움직이는 물체에 대한 정보를 서버로 전송한다. 서버는 데이터베이스를 활용하여 전송받은 정보들의 연관성을 확인한다. 연관성 있는 정보들을 비교하여 사고 발생 가능성을 예측한다.

서버는 사고가 발생할 것으로 예측되는 경우, LED 가 내장된 임베디드 보드로 발광 신호를 전송하여 해당 LED 주변의 보행자 또는 운전자에게 경고한다.

2.3. 클라이언트

클라이언트는 카메라 영상 인식 후 Object Detection 을 적용, 영상 분석을 통해 원하는 데이터를 추출하고 소켓을 이용한 네트워크로 서버와 통신한다.

클라이언트에서 대부분의 연산 작업을 함으로서 서버와 네트워크의 부담을 줄여 클라이언트의 확장을 용이하게 하며 동시에 서버에서는 다수의 클라이언트에서 오는 데이터들을 적은 부담으로 처리할 수 있게 함을 목표로 한다.

2.3.1. openCV 와 Tensorflow

카메라로 촬영된 영상의 처리를 위해 openCV 와

Tensorflow 를 사용한다. openCV 를 활용하여 스트리밍 데이터를 프레임 단위로 처리한다. Tensorflow 의 Object Detection 기술은 본 프로젝트의 핵심 기술로, 프레임 내에서 인식되는 객체 중 사람과 차량만을 추출하고 이를 서버 내의 사고 위험 조건을 판단하는 알고리즘에 적용한다.

2.3.2. 기준선과 객체 추적

객체 추적을 위해서 각 객체들의 경로를 파악하는 방식이 있지만 해당 방식은 많은 연산량을 요구하기 때문에 기준선을 설정해서 해당 기준선에서 객체가 멀어지는지 여부를 파악하는 방식을 활용한다. 이 때 상대적으로 연산량이 적은 이차원 평면에서의 유클리디안 거리를 계산한다.

기준선을 설정하기 위해서 두 점 (x_1, y_1) 과 (x_2, y_2) 을 선택하는 작업이 필요하다. 다음과 같은 수식을 통해 두 점을 지나는 직선의 방정식을 구할 수 있다.

$$(y_2 - y_1) * x + (x_1 - x_2) * y + (x_2 * y_1 - x_1 * y_2) = 0$$

(수식 1) 두 점을 지나는 직선의 방정식

(수식 1)를 통해 두 점 사이의 기준선을 설정할 수 있으며, 해당 기준선을 직선의 방정식 형태로 표현할 수 있다.

Tensorflow 의 Object Detection 기능을 통해 인식된 객체는 박스 형태로 좌표를 반환한다. 이 때 박스의 모서리 좌표들의 X 축 좌표들의 합의 평균값을 A, Y 축 좌표들의 합의 평균값을 B 라고 하자.

점 (A, B) 와 직선의 방정식 사이의 거리를 다음과 같은 수식을 활용하여 구할 수 있다.

$$d = \frac{|(y_2 - y_1) * A + (x_1 - x_2) * B + (x_2 * y_1 - x_1 * y_2)|}{\sqrt{(y_2 - y_1)^2 + (x_1 - x_2)^2}}$$

(수식 2) 점과 직선 사이의 거리 방정식

(수식 2)를 통해 인식되는 객체가 기준선에 가까이 접근하는지 여부를 확인할 수 있다.

2.3.3. 데이터 통신 프로토콜

클라이언트는 아래의 (표 1) 과 같이 영상 프레임 내의 기준선 안에서 어떠한 객체도 검출하지 못했을 때 -1, 기준선 안에서 보행자의 접근을 검출하였을 때 0, 기준선 안에서 차량의 접근을 검출하였을 때 1 을 Value 값으로 설정한다.

<표 1> 감지 신호.

미검출	보행자 접근	차량 접근
-1	0	1

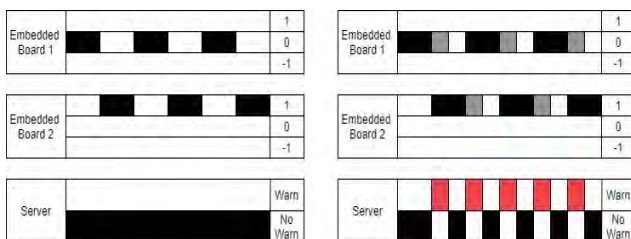
이 때 카메라 고유의 ID 값과 함께 Value 값을 바탕으로 JSON 형식으로 데이터를 구성하여 전송한다. 아래는 전송되는 데이터 값의 예시이다.

```
{ "camera_data" : [{
    "Camera_ID" : "1",
    "Value" : "1"
}]}
```

네트워크 통신 시 비동기 입출력을 사용하는 데 이는 입출력 과정에서 발생할 수 있는 리소스의 유휴 시간을 없애고 영상 처리 성능과 반응 속도를 높이기 위함이다.

2.3.4. 신호 지속 알고리즘

Tensorflow 의 Object Detection 기능은 모델의 성능에 따라서 인식률의 차이가 존재하기 때문에 객체를 항상 인식하는 데에는 한계점이 존재한다. 극단적인 예로, 임베디드 보드 1에서는 기준선을 넘어 접근하는 보행자가 인식되고, 임베디드 보드 2에서는 기준선을 넘어 접근하는 차량이 인식되지만 동시에 인식되지 않으면 서버에서 사고 발생을 감지하지 못한다. 따라서 신호가 감지되면 일정 시간 동안 해당 감지 신호를 유지시키는 방법이 필요하다. 이 때 상위신호 또는 동일신호가 발생하면 감지 신호를 갱신하고 다시금 일정 시간 동안 해당 신호를 유지시킨다.



(그림 2) 예시

위의 예를 이어, 임베디드 보드 1에서 기준선을 넘어 접근하는 보행자가 인식되면 감지 신호(0)을 일정 시간 동안 유지시켜 서버로 일정 시간 동안 value 값이 0인 데이터를 전송하고, 임베디드 보드 2에서 기준선을 넘어 접근하는 일정 시간 내에 자동차가 인식되면 감지 신호(1)을 일정 시간 동안 유지시켜 서버로 일정 시간 동안 value 값이 1인

데이터를 전송한다. 따라서 서버에는 일정 시간동안 임베디드 보드 1에서 value 값이 0인 데이터, 임베디드 보드 2에서 value 값이 1인 데이터를 전송받을 수 있게 된다.

2.4. 서버

서버는 데이터베이스의 제어, 결과값 도출 및 클라이언트와의 통신을 담당한다. 각 클라이언트로부터 카메라별 인식 결과를 실시간으로 전달받고 접근 검출 시 해당 위치에 위험 알람을 전송한다.

서버는 (표 1)의 정보를 카메라 고유 ID와 함께 전달받으며 검출 데이터가 발생했을 시 이를 데이터베이스에서 대조하여 같은 구역인지 판단한다. 같은 구역에서의 데이터를 2개 이상 수신하고 검출 데이터의 합이 1을 넘기게 되면 (표 2)와 같이 위험 상황으로 판단, 해당 구역 알람에 신호를 전송한다.

<표 2> 위험 상황 감지 방식.

Data 1	Data 2	합
0	0	0
0	1	1 (Danger)
1	0	1 (Danger)
1	1	2 (Danger)

2.4.1. 데이터베이스 및 클러스터링

각 카메라별 고유 ID와 구역별 ID, 알람 LED ID를 관리한다. Camera 테이블에서 각 카메라 ID와 구역 ID를 이용하여 카메라의 구역을 판단하고, Alarm 테이블에서 해당 구역의 알람 LED 정보를 받아 위험 알람을 전달한다.

Camera

Camera_ID	Section_ID
카메라 ID	구역 ID

Alarm

Section_ID	LED_ID
구역 ID	알람 LED ID

(그림 3) 데이터베이스 내부 테이블 및 속성

3. 결론

본 논문에서는 기존 골목길의 문제점인 사각지대에서 일어날 수 있는 차량 사고를 예방하기 위한 시스템을 구성하여 문제를 해결할 수 있는 가능성을 보여주기 위해 교육용 장비인 라즈베리파이와 서버 PC 를 활용한 프로토타입 모델을 구현하였다. 이 시스템을 통해 기대되는 효과는 다음과 같다.

- 1) 보다 안전한 골목길을 형성을 통해 인명사고를 예방한다.
사각지대라는 보이지 않는 영역에서 발생할 수 있는 사고를 예방하는 시스템을 구축함으로써 사각지대의 한계를 극복하여, 예상치 못한 골목길 교통사고를 줄일 수 있다.
- 2) 불필요한 알람을 최소화하여 골목길의 생활 여건을 보장한다.
골목길에서 차량이나 사람이 단독으로 접근하는 경우에는 알람 신호를 주지 않도록 설정하여 불필요한 에너지낭비, 소음을 만들어내지 않음으로써 보다 쾌적한 골목길 생활 환경을 만들어낼 수 있다.
- 3) 저비용으로 총괄적인 시스템 구축을 실증한다.
전체 카메라 설치 및 시스템 구축 비용이 높다는 현 시장의 문제점을 보완하여 기존에 설치된 CCTV 를 활용하여 합리적인 방법으로 골목길의 영상을 확보하고, 구현된 시스템으로 영상 정보를 처리할 수 있는 통합적인 환경을 제시함으로써 시장환경에 보다 효율적인 시스템서비스가 제공될 여지를 줄 수 있다.
- 4) 저비용 통합 시스템을 통한 즉각적인 사고 예방 효과를 얻을 수 있다.
기술은 빠른 속도로 발전하지만, 실제적인 기술의 적용 및 활용까지의 시간은 상대적으로 긴 편이다. 가장 큰 원인이 비싼 비용과 진행에 필요한 인력과 시간, 투자 비용에 따른 효과의 의문성이다. 저비용의 통합적인 서비스를 제공하는 본 시스템을 통해 실제 활용 시까지 소모 시간을 낮추어 시스템을 이용함으로써 빠른 시일 내에 직접적인 결과를 확인할 수 있고 골목길

사고율을 감소시킬 수 있다.

본 논문에서는 기존에 설치된 CCTV 를 활용, 해당 시스템 구현을 통해 단기간 내에 골목길 안전 시스템 체계 구축을 가능하게 함으로써 전체적인 교통사고율 감소를 달성할 수 있음을 기대한다.

사사문구

“본 연구는 과학기술정보통신부 및 정보통신기획평가원의 SW 중심대학사업의 연구결과로 수행되었음” (2015-0-00912)

참고 문헌

- [1] TAAS 교통사고분석시스템
<http://taas.koroad.or.kr/>
- [2] 한국교통안전공단
<http://www.kotsa.or.kr/>
- [3] 경찰청
<https://www.police.go.kr/>
- [4] ”그날 거기 있었지?” 한국 CCTV 세계 최대
<https://news.mt.co.kr/mtview.php?no=2014010715584080504>

일반 필기데이터와 CNN 을 이용한 온라인 서명인식

박민주*, 윤희용**

*성균관대학교 소프트웨어대학 컴퓨터공학과

**성균관대학교 정보통신대학 전자전기컴퓨터공학과

wyuinche.mido@gmail.com, youn7147@skku.edu

Online Signature Verification using General Handwriting Data and CNN

MINJU PARK*, HEE YONG YOUN**

*Dept. of Computer Science and Engineering, Sungkyunkwan University

**Dept. of Electrical and Computer Engineering, Sungkyunkwan University

요 약

본 논문에서는 대표적인 이미지 분류 모델인 CNN(Convolutional Neural Network)과 시간에 따른 이미지의 변화를 학습할 수 있는 LSTM(Long Short-Term Memory) 기반의 온라인 서명인식 모델을 제안한다. 실제로는 위조서명을 미리 구하기 어렵다는 사실을 고려해 서명검증 대상자가 아닌 타인의 진서명과 대상자의 일반 필기 데이터를 음의 데이터로서 학습에 사용하였다. 실험 결과, 전체 이미지 중 서명 부분의 비율에 따라 좋은 성능을 보이는 검증 모델이 다르며 Accuracy 성능지표를 통해 이 비율이 높거나 낮을 경우 CNN-LSTM 이, 중간일 경우 CNN 이 적합하다는 것을 확인하였다.

1. 서론

최근 온라인 상의 금융거래, 핀테크가 활성화되고 있다.[1] 그에 따라 생체인식 등을 통한 본인인증에 대한 수요 또한 높아지고 있다. 서명인식의 경우 단순히 정적 데이터만을 사용하는 오프라인 방식은 위조가 쉽기 때문에 최근에는 개인의 동적 데이터를 포함한 온라인 방식에 대한 연구가 활발히 이루어지고 있다. 특히 서명검증에는 딥러닝과 SVM 을 이용한 사례가 많아지고 있는데 그 중 CNN 에 시간에 따른 이미지의 변화를 학습할 수 있는 LSTM 모델을 도입한 연구도 증가하고 있다. [2][3][4][5][6]

서명에 포함된 동적 데이터로는 특정 순간의 서명 완성도, 펜의 위치나 압력, 작성 속도 등이 있다. 서명을 그대로 따라 그리는 방법으로 원본에 가깝게 위조할 수는 있으나 실제 사용자의 서명 속도 등 개인적인 특징까지 따라하기는 어렵다. 또한 실제 서명을 작성하는 과정을 그대로 지켜보지 않는 한 서명의 동적 정보를 얻기는 힘들기 때문에 온라인 방식이 오프라인 방식에 비해 보안상 더 안전하다고 할 수 있다.

본문에서는 서명검증에 많이 쓰이는 CNN 모델과 그에 동적 데이터를 학습할 수 있는 LSTM 을 결합한 새로운 CNN-LSTM 모델을 함께 제안하여 서명 분류 성능을 관찰하고 각 모델의 성능을 비교한다. CNN 의 경우 하나의 이미지에 동적 데이터를 포함할 수 있도

록 최승호, 정성훈의 논문에서 사용한 방법을 참고하였다.[2][4] 서명 습득 과정과 가공 방법은 본문에 자세히 서술한다.

서명은 스타일러스 펜을 사용하여 필기압력을 적용한 펜으로 작성한 서명과 그렇지 않은 서명을 구분해 얻었으며 이를 CNN, CNN-LSTM 에 기반한 모델에 학습한 결과를 비교하였다. CNN 모델은 중간 정도의 밀도를 가진 서명에 강한 검증 성능을 보였으며 CNN-LSTM 의 경우 과소적합을 일으키기 쉬우나 Dropout Layer 를 더 추가한 모델의 경우 밀도가 낮거나 높은 서명 검증에서 좋은 결과를 보일 것이라고 기대되었다. 여기서 밀도는 전체 서명 이미지에서 서명 부분이 차지하는 비율을 의미한다.

2. 관련 연구

서명 검증에는 오프라인 방식과 온라인 방식이 있다.[7] 오프라인은 서명이 완전히 완료된 시점의 이미지를 이용하는 방법이며 온라인은 시간에 따른 펜의 압력, 획의 수 등 동적 데이터를 함께 이용하는 방법이다. 특히 복잡한 이미지의 분류를 다루기 위해 많은 연구에서 Krizhevsky 가 제안한 AlexNet 이 적용되었다. 처음 제안된 AlexNet 에는 두개의 LRN(Local Response Normalization) Layer 가 포함되어 있으나 이후 몇몇 연구에서는 Batch Normalization 이 대신 사용되

나 아예 삭제되기도 하였다.[8][9] AlexNet 에 Dropout Layer 을 더 추가한 필기 인식 성능 향상 모델을 제안한 R.Almodfer 의 연구에서는 ReLU 와 tanH 활성화 함수를 사용한 두 경우 모두 92% 이상의 분류 정확도를 달성하여 적절히 변형된 AlexNet 도 필기인식에서 좋은 성과를 낼 수 있다는 것을 보여주었다.[10]

최승호, 정성훈에 의해 제안된 연구에서는 CNN 모델에 시간에 따른 서명 이미지의 변화를 학습하기 위해 서명을 동영상의 형태로 얻어 등간격의 10 프레임으로 나눈 뒤 이를 하나로 합성하여 사용하였다.[2][4] 그러나 이 방식은 합성된 이미지가 지나치게 커지거나 특정 프레임의 영향이 작아지는 단점이 있다. 또한 해당 연구에서는 모델 학습 시 진서명과 위조서명의 수를 같은 비율로 설정하였으나 실제로는 위조서명을 사전에 충분히 얻기 힘들다는 문제가 있다.

부족한 위조서명의 수를 보충하기 위해 대상 서명 외의 필기데이터를 이용한 연구들이 있다. CY. Park 외 2 인이 연구한 서명검증 모델에서는 일반적인 위조서명과 함께 서명검증 대상자 본인이 스스로 위조한 듯 작성한 서명을 필기데이터로서 이용하였다.[9] SVM 기반의 온라인 서명검증 기법을 연구한 최훈, 허경용의 논문에서는 타인의 진서명을 음의 데이터로 사용한 실험에서 더 높은 분류 성능을 보였다.[5]

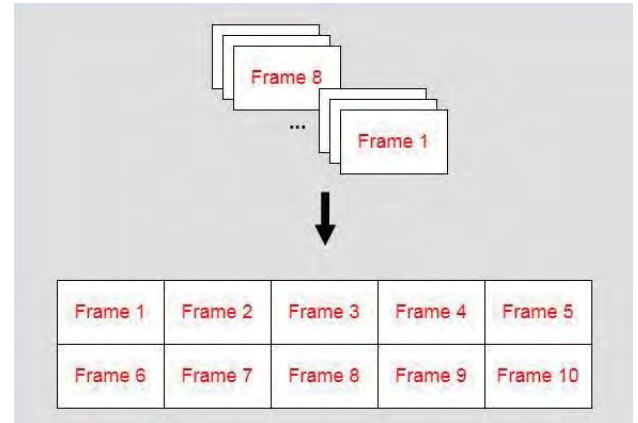
3. 서명 데이터

<표 1> 서명집합의 구성

	Original	Forgery	Others	Written Data
Normal	50 EA	30 EA	4 EA	1 EA
Pen	50 EA	30 EA	4 EA	1 EA

서명집합은 최승호, 정성훈의 연구와 동일한 방식으로 수집하였다.[2][4] 스타일러스 펜을 사용할 수 있는 안드로이드 스마트폰으로 서명 영상을 얻어 서명의 시작과 끝을 기준으로 10 프레임으로 나눈 것을 하나의 서명집합으로 상정하였다. 표 1 은 사용자 1 명에 대한 서명집합의 구성을 표현한 것이다. 표 1 의 서명들을 행을 기준으로 하나의 서명 집합으로 묶어 모델 학습 및 판별 테스트를 진행한다. 위조서명(Forgery)은 특정 5 명 중 서명 판별의 대상자를 제외한 4 명이 대상자의 진서명을 약 20 회 정도 연습한 후 각각 7~10 개씩 작성한 것을 사용하였으며 해당 4 명의 진서명(Others)은 학습 시 음의 데이터로 사용된다. 또한 검증 대상자가 자신의 서명을 위조한 듯이 작성한 필기 데이터(Written Data)도 음의 데이터로 분류된다. 최종적으로는 같은 사용자에 대해 필기압력이 적용된 경우의 서명과 그렇지 않은 경우 두 가지의 서명집합

(Normal, Pen)을 각각 수집하였다. 연구는 총 2 명의 사용자, CASE1, CASE2 에 대해 각 2 개씩 총 4 개의 서명집합을 가지고 진행하였다. 이 4 개의 서명집합을 CASE1-normal, CASE1-pen, CASE2-normal, CASE2-pen 으로 표기하겠다.



(그림 1) 서명 이미지 합성 방법

그림 1 은 CNN 모델에 사용하는 서명 이미지의 합성 방법을 나타낸 것이다. CNN-LSTM 에 기반한 모델은 서명 프레임을 합성하지 않고 각 프레임을 230X160 픽셀로 조정한 것을 사용하였으며 CNN 에 기반한 모델에는 한 서명의 10 프레임을 시간 순서에 따라 왼쪽 위에서 오른쪽 아래 방향으로 합성 후 1225X340 픽셀로 조정한 것을 사용하였다.

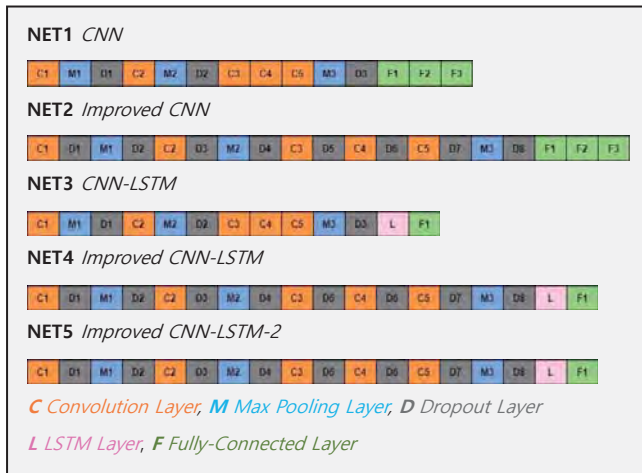
각 서명 이미지는 서명의 펜 선보다 배경의 면적이 훨씬 넓기 때문에 데이터를 배열의 형태로 변환한 경우 최대 휘도인 255(흰색)의 원소가 많아진다. 그러나 배경부분의 값은 실제 서명 학습에 필요한 정보가 아니므로 각 원소의 휘도값 I 에서 255 를 뺀 뒤 결정되는 회소행렬을 사용하는 것이 더 효율적이다. 그 다음 각각을 0~1. 사이의 값으로 표준화하기 위해 -255 로 나누었는데 이를 식으로 나타내면 (1)과 같다.

$$I'(x,y) = (I(x,y) - 255) \times (-\frac{1}{255}) \quad (1)$$

서명 이미지는 배경 부분을 투명하게 만든 뒤 사용하였으며 모델 학습에서는 RGBA 형식으로 이미지를 처리하였기 때문에 실제로 배경원소가 255 의 값을 가지는 것을 확인할 수 있었다.

4. 제안 방법

본 논문에서는 온라인 서명 검증을 위해 5 가지 DL(Deep Learning) 모델을 제안한다. 각 모델은 이미지 분류의 대표적인 모델 중 하나인 AlexNet 을 기반으로 하였으나 Krizhevsky 가 제안한 모델에서 LRN Layer 를 삭제한 것을 사용하였다.[8]



(그림 2) 제안모델의 구조

그림 2 는 제안모델의 구조를 간략히 나타낸 것이다. 모든 모델에서 활성화함수는 ReLU 함수가 쓰였으며 Max Pooling 의 Size 는 (3, 3), Stride 는 (2, 2)로 고정되었다. Convolution Layer 의 경우 첫번째 층은 Stride 가 (4, 4), 그 외에는 전부 (1, 1)로 설정하였다. 마지막 Fully-Connected Layer 의 활성화 함수로는 Softmax 를 사용하였다. NET1-NET2 의 Fully-Connected Layer 는 각각 1024, 1024, 2 개의 뉴런을 가지고 있으며 NET3-NET5 의 경우 128 개의 뉴런을 가지는 LSTM Layer 와 2 개의 뉴런을 가진 Fully-Connected Layer 로 구성되어 있다.

NET1, NET3 와 달리 NET2, NET4, NET5 에서는 과대적합을 줄이기 위한 Dropout Layer 가 각 Convolution Layer 뒤에 하나씩 더 추가가 됐다는 점에서 차이가 있다. Dropout Layer 마다 설정된 Probability 값은 표 2 에 나타났다.

<표 2> Dropout Layer 의 Probability

	D1	D2	D3	D4	D5	D6	D7	D8
NET1	0.1	0.3	0.5	-	-	-	-	-
NET2	0.0	0.1	0.1	0.3	0.2	0.3	0.4	0.5
NET3	0.1	0.3	0.5	-	-	-	-	-
NET4	0.0	0.1	0.1	0.3	0.2	0.3	0.4	0.5
NET5	0.0	0.1	0.0	0.2	0.1	0.2	0.2	0.3

모델 학습은 epoch 100, batch size 10 로 진행하였으며 진서명 30 개와 타인의 진서명 4 개, 위조서명 10 개, 검증 대상자의 일반 필기데이터 1 개를 사용한다. 실제로는 위조서명을 얻기 힘들다는 점을 고려해 위조서명은 진서명 30 개에 비해 적은 10 개가 사용되었는데 부족한 위조서명 데이터를 보충하기 위해 타인의 진서명과 대상자의 일반 필기데이터를 사용하였다. 진서명 30 개만을 양의 데이터인 1 로 설정하였으며 나머지는 모두 음의 데이터인 0 으로 취급하였다. 위

조서명은 NET1-NET5 에서 모두 고정된 객체를 사용하였으나 진서명은 학습마다 랜덤으로 선택하였다. 이는 위조서명은 습득하기 어려운 반면 진서명은 일반적으로 학습에 사용가능한 데이터가 충분한 상황을 반영한 것이다.

5. 실험 결과

표 3 은 4 개의 서명집합에 대한 NET1-NET5 의 테스트 결과를 나타낸 것이다. 테스트 시에는 서명집합의 진서명 50 개와 위조서명 30 개에 대해 검증하였으며 성능평가는 ACC(Accuracy)를 사용하였다.

<표 3> 제안모델(NET1-NET5)의 테스트 결과

ACC Value (Range: 0~1)					
CASE1	NET1	NET2	NET3	NET4	NET5
Normal	0.3750	0.3750	0.6250	0.6250*	0.3750
Pen	0.6250	0.6250	0.6250	0.6250	0.6250
CASE2	NET1	NET2	NET3	NET4	NET5
Normal	0.9625	0.3750	0.6250	0.6750	0.6250
Pen	0.3750	0.3750	0.6250	0.5500	0.5625

대부분의 모델이 0.3750 혹은 0.6250 의 ACC 값을 가지고 있다. 각 서명에 대한 예측 결과를 분석하니 0.6250 은 모든 서명을 진서명으로, 0.3750 은 반대로 모두 위조서명으로 판단한 경우로 확인되었다. 즉, ACC 가 0.6250 인 것은 과소적합으로, 0.3750 인 것은 과대적합으로 학습된 상황을 의미한다. 예외적으로 CASE1-Normal 로 학습한 NET4 의 경우 서명의 예측 결과가 일관적인 것은 아니나 단지 우연히 제대로 검증된 서명의 수가 전체 80 개 중 50 개인 것으로 확인되었다. 표 3 의 결과만 보았을 때에는 CASE2-Normal 서명집합의 NET1 을 제외하고는 전부 제대로 검증을 수행하지 못한 것으로 보인다.

이 결과를 더 면밀히 분석하기 위해 각 서명집합의 서명 밀도를 측정하였다. 이때 밀도는 50 개의 진서명을 grayscale 의 230X160 크기로 추출해 배경을 제외한 서명 부분의 픽셀 수를 모두 더한 뒤 전체 픽셀수인 230X160X50 으로 나눈 결과를 말한다. CASE1-normal 이 0.09 로 밀도가 가장 낮았으며 CASE1-pen 과 CASE2-normal 은 각각 0.44 와 0.47 로 중간 정도, CASE2-pen 은 0.69 로 밀도가 가장 높았다.

서명 밀도가 낮은 집합인 CASE1-normal 의 경우 CNN 과 CNN-LSTM 모델 종류에 상관없이 전반적으로 과대적합 되는 경향이 높은 것으로 나타났다. 이는 전체 서명 이미지 중 서명 획이 차지하는 비율이 작아 학습에 필요한 정보의 양이 부족하기 때문인 것으로 보인다. 하지만 NET4 에서는 ACC 값이 아주 높지는 않으나 과소적합이나 과대적합이 발생하는 경향

은 상대적으로 작은 것을 알 수 있다. 이 경우 본 논문에서 제안한 100 보다 높은 epoch 를 설정하여 학습하면 정확도가 향상될 것으로 보인다.

중 수준 밀도의 서명인 CASE1-pen 과 CASE2-normal 에서는 전체 모델 중 ACC 값이 0.6250 인 과소적합이 발생할 확률이 0.8 로 매우 높았다. 다만 CNN 을 사용한 NET2 에서는 반대로 과대적합이 발생하였으며 CASE2-normal 의 NET1 에서는 ACC 가 0.9625 로 거의 대부분의 서명을 정확하게 검증하였다. 이는 CASE2-normal 과 비슷한 밀도를 가진 서명의 경우 NET3-NET5, 즉 CNN-LSTM 을 이용한 모델에서는 과소적합이 발생할 경향이 크며 오히려 일반적인 CNN 모델에서 좋은 검증 성능을 보인다는 것을 의미한다.

마지막으로 CASE2-pen 에 대한 모델 검증 결과에 미루어 볼 때 서명 밀도가 높은 경우 CNN 을 이용한 모델(NET1-NET2)에서는 과대적합이 발생할 확률이 높으며 3 개의 Dropout Layer 만을 포함한 일반적인 수준의 CNN-LSTM(NET3)에서는 과소적합이 발생할 수 있다는 사실을 알려준다. 반면 6-8 개의 Dropout Layer 가 포함된 CNN-LSTM(NET4-NET5)에서는 CASE1-normal 을 사용한 NET4 의 경우와 마찬가지로 과대/과소적합이 발생하는 경향이 낮은 것을 보아 epoch 를 높인 학습에서 좋은 분류 성능이 기대된다.

6. 결론

밀도가 다른 각 서명 집합을 일반적인 CNN, CNN-LSTM 모델과 Dropout Layer 를 더 추가한 모델에 학습, 검증한 결과 서명의 밀도에 따라 검증에 적합한 모델이 달라지는 것을 알 수 있었다. 서명의 밀도가 낮거나 반대로 높은 경우 6 개 이상의 Dropout Layer 를 포함한 CNN-LSTM 모델에 학습할 때 과대/과소적합이 발생하는 경향이 낮았으며 이때 정확도가 낮은 것은 충분히 높은 epoch 를 설정하면 해결할 수 있을 것으로 기대된다. 서명의 밀도가 중간정도 수준일 때는 반대로 적은 수의 Dropout Layer 를 포함한 CNN 모델에서 거의 정확한 수준의 검증 성능을 보였다. 다만 실생활에서 서명 학습을 위한 데이터를 얻기가 매우 제한적이며 같은 사람이라도 서명을 할 때마다 결과가 조금씩 달라진다는 사실을 고려해볼 때 적은 수의 서명으로도 정확도를 충분히 높일 수 있는 서명 검증 연구가 필요할 것이다.

참고문헌

- [1] Kim, Hyun-Woo and Seung-In Kim. "A study on User experience of Fintech Application Service-Focused on Toss and Kakaobank." *Journal of Digital Convergence* 18.1: 287-293. (2020)
- [2] Choi, Seoung-Ho and Sung Hoon Jung. "Fake Discrimination using Time Information in CNN-based Signature Recognition." *Proceedings of the Korean Society of Computer Information Conference*. Korean Society of Computer Information, 2017. p. 293-294.
- [3] Zeng, Zihan and Jing Tian. "Deep Learning Methods for Signature Verification." *arXiv preprint arXiv:1912.05435*. (2019)
- [4] Choi, Seoung-Ho and Sung Hoon Jung. "Performance improvement of fake discrimination using time information in CNN-based signature recognition." *Journal of Digital Contents Society* 19.1: 205-212. (2018)
- [5] Choi, Hun and Gyeongyong Heo. "Online Signature Verification Method using General Handwriting Data and 1-class SVM." *Journal of the Korea Institute of Information and Communication Engineering* 22.11: 1435-1441. (2018)
- [6] Agarap, Abien Fred. "An architecture combining convolutional neural network (CNN) and support vector machine (SVM) for image classification." *arXiv preprint arXiv:1712.03541*. (2017)
- [7] Hafemann, Luiz G., Robert Sabourin, and Luiz S. Oliveira. "Learning features for offline handwritten signature verification using deep convolutional neural networks." *Pattern Recognition*, 70: 163-176. (2017)
- [8] Krizhevsky, Alex, Ilya Sutskever, and Geoffrey E. Hinton. "Imagenet classification with deep convolutional neural networks." *Advances in neural information processing systems*, 2012. p. 1097-1105.
- [9] Park, Chan-Yong, Han-Gyu Kim, and Ho-Jin Choi. "Robust Online Signature Verification Using Long-term Recurrent Convolutional Network." *2019 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2019. p. 1-6.
- [10] Almodfer, Rolla, et al. "Enhancing AlexNet for Arabic Handwritten words Recognition Using Incremental Dropout." *2017 IEEE 29th International Conference on Tools with Artificial Intelligence (ICTAI)*. IEEE, 2017. p. 663-669.

GAN 기반 고해상도 의료 영상 생성을 위한 연구

고재영*, 조백환**, 정명진**

*성균관대학교 삼성융합의과학원 디지털헬스학과

**삼성서울병원 스마트헬스케어연구소 AI 연구센터

kojae8311@g.skku.edu, baekhwan.cho@samsung.com, mjl.chung@samsung.com

GAN-based research for high-resolution medical image generation

Jae-Yeong Ko*, Baek-Hwan Cho**, Myung-Jin Chung**

*Dept. of Digital Health, SAIHST, Sungkyunkwan University

**Medical AI Research Center, Smart Healthcare Research Institute, Samsung Medical Center

요 약

의료 데이터를 이용하여 인공지능 기계학습 연구를 수행할 때 자주 마주하는 문제는 데이터 불균형, 데이터 부족 등이며 특히 정제된 충분한 데이터를 구하기 힘들다는 것이 큰 문제이다. 본 연구에서는 이를 해결하기 위해 GAN(Generative Adversarial Network) 기반 고해상도 의료 영상을 생성하는 프레임워크를 개발하고자 한다. 각 해상도마다 Scale의 Gradient를 동시에 학습하여 빠르게 고해상도 이미지를 생성해낼 수 있도록 했다. 고해상도 이미지를 생성하는 Neural Network를 고안하였으며, PGGAN, Style-GAN과의 성능 비교를 통해 제안된 모델이 양질의 고해상도 의료영상 이미지를 더 빠르게 생성할 수 있음을 확인하였다. 이를 통해 인공지능 기계학습 연구에 있어서 의료 영상의 데이터 부족, 데이터 불균형 문제를 해결할 수 있는 Data augmentation이나, Anomaly detection 등의 연구에 적용할 수 있다.

1. 서론

인공지능 기계학습 연구에서는 품질 좋은 데이터량에 따라 연구의 성과가 달라질 수 있기 때문에 데이터량은 중요하다. 특히 의료 분야는 privacy issue, annotation에 필요한 노동력 등 다양한 문제로 인해 정제된 양질의 데이터를 대량으로 획득하기가 어렵다.

흉부 방사선 영상(Chest X-ray) 촬영은 병원에서 가장 대중적으로 이루어지고 있는 검사 중 하나로 의료 영상 데이터중에는 상대적으로 데이터의 개수가 많지만 각종 질환이나 병변 위치의 annotation을 위해서는 여전히 많은 자원을 필요로 한다. 뿐만 아니라 건강 검진 등을 위해서 Chest X-ray 촬영을 많이 하기 때문에 정상(normal) 데이터가 비정상(abnormal) 데이터에 비해 데이터량이 많아 데이터 불균형 현상이 발생한다. 이러한 문제들을 해결하고자 생성 모델(Generative model)들을 이용한 연구들이 진행되고있다.

Generative Model 중 GAN을 이용한 연구가 많은 분야에서 활발하게 이루어지고 있다. 그 중에서 Convolutional layer를 처음 GAN에 적용시킨 DCGAN[5]은 가장 기본이 되는 GAN 모델이다. DCGAN은 저해상도 영상을 빠르게 생성해주는 장점이 있지만 고해상도 영상의 경우 네트워크 구조에서

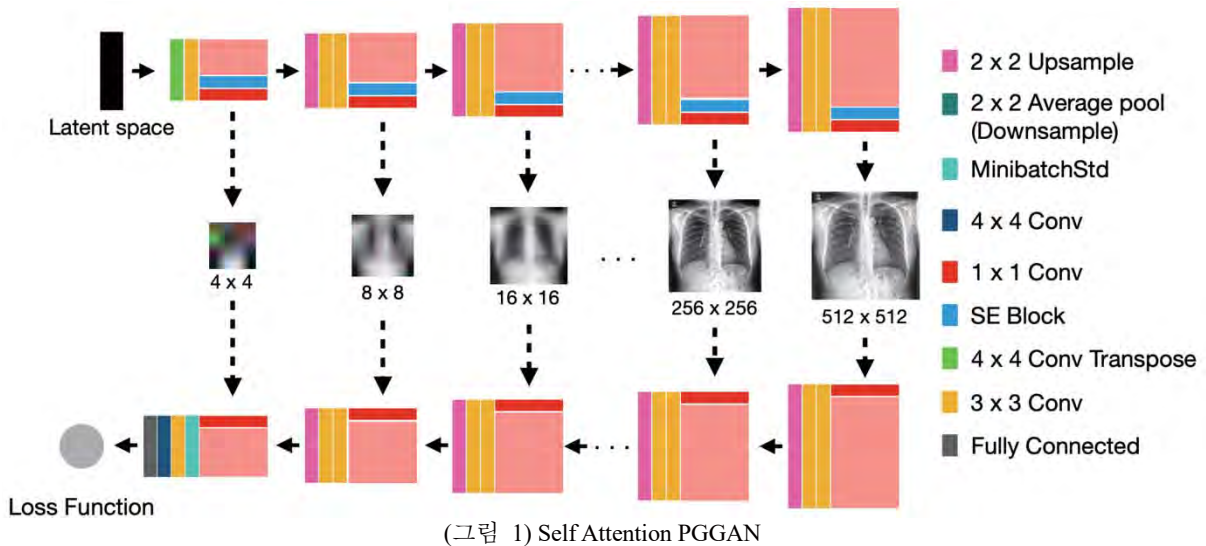
기인하는 GPU 메모리의 한계로 인해 batch 크기에 대한 제약이 있어 학습 성능이 좋지 않다.

고해상도 영상을 생성하는 대표적인 모델인 PGGAN[4]은 Discriminator와 Generator를 점진적으로 layer를 쌓아 영상의 해상도를 증가시키면서 학습을 진행하는 특징을 갖고 있다. 하지만 이와 같은 방법으로 학습을 진행하는 것은 학습에 매우 많은 시간이 걸린다는 단점이 있으며, 충분한 학습 데이터량이 필요하다. 그러나 의료 데이터 특성상 다른 분야의 데이터에 비해 데이터량이 상대적으로 부족하므로 데이터량이 적은 상태로 학습을 진행할 시 학습이 불안정하게 진행될 우려가 크다. 따라서 우리는 본 연구에서 의료 영상 데이터의 근본적 문제인 데이터 불균형 문제와 데이터량 부족 문제를 해결하기 위해 GAN 기반 고해상도 의료 영상 이미지를 생성하는 연구를 진행했다.

2. 방법

2-1. 데이터

삼성서울병원에서 촬영한 흉부 방사선 영상은 40,301명의 환자에서 80,675개의 데이터로 구성된 DICOM 형식의 익명화된 흉부 방사선 데이터 셋이다. 사용된 데이터는 측면 방사선 이미지(Lateral Chest radiograph)



와 전면 방사선 영상(Posteroanterior Chest radiograph)으로 구성되어 있다. 본 연구에서는 전면 방사선 사진만 필요하므로 전면 방사선 사진인 PA Chest radiograph 로만 연구를 진행했다. 최종적으로 본 연구에서는 40,940 개의 데이터로 연구를 진행했다.

2-2. 전처리

방사선 전문가들은 촬영된 방사선 영상을 판독할 때 Histogram 을 조절해서 판독하기 적절한 상태로 변경하여 판독을 진행한다. 본 연구에 사용된 영상도 동일한 효과를 적용하기 위해 Contrast Limited Adaptive Histogram Equalization 을 이용하여 방사선 영상의 전처리를 진행했다. 또한 원본 방사선 영상 크기의 5% 만큼 Random Crop 을 적용한 후 512x512 크기로 resize 를 해주었다.. 또한 PGGAN 의 구조를 그대로 사용하기 때문에 Feature vector 를 RGB Color 로 만들어 주는 layer 를 적용하기 위해 Gray Scale 영상을 duplication 을 통해 3 채널 영상인 RGB 로 변경하였으며, 메모리를 효율적으로 사용하기 위해 DICOM 이미지를 Pickle 형태로 변환하였다..

2-3. 네트워크

본 연구에서는 SAGAN[9]에서 Self Attention 을 적용한 것과 마찬가지로, PGGAN 모델 구조를 응용해서 각 해상도를 담당하는 중간 계층에 SE Block[2]을 적용시켰다. 그 후 1x1 convolution layer 를 통해 각 해상도 이미지의 Feature 를 추출해서 최종적으로 (그림 1)와 같이 추출된 Feature 들이 Discriminator 의 입력으로 들어가는 구조로 학습을 진행했다.

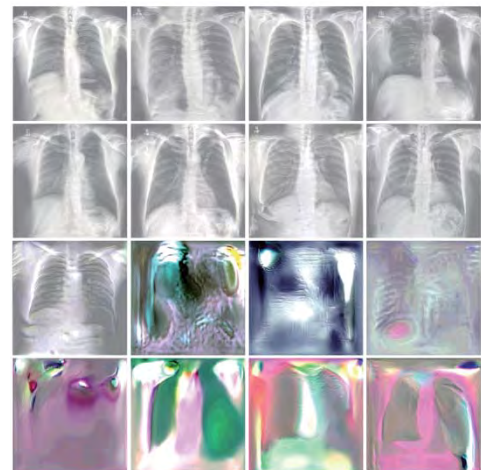
본 연구에서는 4 가지 손실 함수(Minmax Loss, WGAN-GP Loss[1], Hinge Loss, RA-Hinge Loss)를 적용하였고, 전면 흉부 방사선 영상(PA Chest radiograph) 데이터셋에는 RA-Hinge Loss[3] 가 더 빠르고 안정적으로 학습이 진행되는 것을 확인하였다.



(그림 2) PGGAN, Style-GAN 의 CelebA-HQ 학습 결과

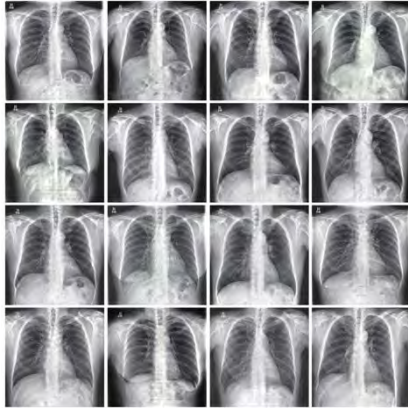
3. 연구 결과

PGGAN[4]과 Style-GAN 모델을 사용해서 CelebA-HQ 데이터로 학습을 진행한 결과는 (그림 2)와 같이 보다 안정적으로 학습이 진행되었지만 본 연구에서 사용한 PA Chest radiograph 으로 학습을 진한 결과는 (그림 3)와 같이 학습이 불안정하게 학습이 진행되어 학습 영상과 전혀 다른 형태의 영상을 생성하였다.



(그림 3) PGGAN 모델에 Chest x-ray 학습 결과 불안정하게 학습된 GAN의 512x512 생성 이미지.

본 연구에는 제안한 모델을 사용한 결과는 (그림 4)와 같이 안정적으로 학습이 진행된 것을 확인할 수 있었다. GAN 모델의 성능을 정량적으로 확인하기 위해 <표 1>과 같이 Epoch 마다 FID(Fréchet Inception distance)[8] Score 를 측정하였다. 기존 GAN Model 들에 비해 제안한 Self Attention PGGAN 이 FID Score 가 가장 낮았으며 특히 상대적으로 다른 모델들에 비해 Epoch 이 낮아도 안정적이고 빠르게 데이터 생성을 하고 있다는 것을 확인할 수 있었다.



(그림 4) Self Attention PGGAN 과 Relativistic Hinge GAN Loss 를 이용한 Chest X-ray 생성 결과.

<표 1> Chest x-ray 를 이용한 GAN Model 의 Epoch 에 따른 Fréchet Inception distance (FID)

Methods	FID			
Epoch	10	50	100	150
DCGAN[5]	9045.36	8045.15	8195.39	7853.76
PGGAN[4]	305.43	105.94	208.36	207.46
Style-GAN[7]	206.53	90.63	109.34	305.28
Self Attention PGGAN	35.36	28.57	20.34	18.09

4. 결론

본 논문에서는 PA Chest radiograph 데이터를 이용하여 고해상도 이미지를 만들도록 연구를 진행했다. 제안한 모델은 PGGAN 구조에 Self Attention Module 을 적용하여, 기존의 모델에 비해 안정적으로 (그림 5)와 같이 고해상도 의료 영상을 생성하는 것을 확인하였다.



(그림 5) 생성된 512 x 512 흉부 방사선 사진.

본 연구에서 사용된 모델은 Data Augmentation, Anomaly Detection 등 의료 영상을 이용한 다양한 인공지능 기계학습 연구에 적용 가능하다.

"본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학 ICT 연구센터지원사업의 연구결과로 수행되었음" (IITP-2020-2018-0-01798)

참고문헌

- [1] Gulrajani, I., et al. Improved training of wasserstein gans. Advances in neural information processing systems. (2017).
- [2] Hu, J., et al. Squeeze-and-excitation networks. Proceedings of the IEEE conference on computer vision and pattern recognition. (2018).
- [3] Jolicoeur-Martineau, A. "The relativistic discriminator: a key element missing from standard GAN." (2018).
- [4] Karras, T., et al. "Progressive growing of gans for improved quality, stability, and variation." (2017).
- [5] Radford, A., et al. "Unsupervised representation learning with deep convolutional generative adversarial networks." (2015).
- [6] Zhang, H., et al. "Self-attention generative adversarial networks." (2018).
- [7] Karras, T., et al. A style-based generator architecture for generative adversarial networks. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. (2019).
- [8] Heusel, M., et al. Gans trained by a two time-scale update rule converge to a local nash equilibrium. Advances in neural information processing systems. (2017).

기계학습 기반의 낙상 검출

김인경, 김대희, 허성실, 이재구*
국민대학교 컴퓨터공학과
*jaekoo@kookmin.ac.kr

Machine Learning based Fall Detection

InKyung Kim, DaeHee Kim, Seongsil Heo, JaeKoo Lee*
Dept. of Computer Science, Kookmin University

요 약

노인인구의 급증에 따라 노인 건강에 대한 관심이 증가하였고 노인 낙상을 발견하는 방법에 대한 관심도 함께 대두되기 시작하였다. 낙상 사고의 경우 낙상을 일으킨 원인보다 낙상이 제때 감지되지 않아 발생하는 이후의 상황이 더욱 심각한 결과를 초래한다. 따라서 낙상이 발생했을 때, 바로 낙상을 감지할 수 있는 시스템 구축이 필요하다. 다양한 낙상 검출을 위한 방법이 존재하지만 그 중 착용이 쉽고 원격지에서 관찰 및 관리가 가능한 웨어러블(Wearable) 기기의 센서 데이터를 사용한 낙상 검출을 진행하였다. 본 논문에서는 머신 러닝 모델들을 사용해서 낙상 검출 성능 비교 및 적절한 모델을 제안한다. 기계 학습 기반의 모델인 결정 트리(Decision Tree), 랜덤 포레스트(Random Forest), SVM(Support Vector Machine)을 사용하여 실제 측정된 데이터에 낙상 검출 학습 능력을 정량화하였다. 또한, 모델의 입력 값에 적용한 데이터 분할, 전처리 및 특징 추출 방법을 통해서 효율적인 낙상 검출을 위한 기계학습 관점에서의 타당성을 판단하고자 한다.

1. 서론

일반적으로 낙상(Fall)은 높은 곳에서 낮은 곳으로 신체의 중심을 잃고 빠르게 움직이는 것을 의미한다. 반면 ADL(Activity of Daily Living)은 사람들이 일상 생활에서 수행하는 자기 관리를 포함한 모든 활동을 의미하며, 걷기, 식사 하기 등이 이에 해당한다. 현재까지 많은 낙상 검출 연구들은 낙상과 ADL 을 구별하는 방식으로 진행되고 있다[1].

노인인구가 증가함에 따라 낙상에 대한 관심도 함께 증가하는 추세이다. 2018 년 통계청 자료에 따르면, 2018 년 65 세 이상 인구는 738 만 1 천명으로 전체 인구의 14.3%를 차지한다. 2018 년 노년부양비는 19.6 명에서 저출산과 고령화의 영향으로 2060 년에는 82.6 명으로 증가할 전망이다[2]. 2017 년 보건복지부에서 진행한 노인실태조사에 따르면 노인의 15.9%는 낙상 경험이 있으며, 지난 1 년간 낙상 횟수는 평균 2.1 회이다[3]. 낙상으로 인한 주요 손상 부위는 남녀 모두 고관절골절이 가장 많은 것으로 나타난다. 고관절골절은 골절 자체의 문제보다 동반되는 합병증으로 인해 생명까지 위협받을 수 있다.

이렇듯 낙상은 노인들의 건강에 매우 큰 영향을 미칠 수 있기 때문에 낙상이 일어난 순간에 조기 발견이 매우 중요하다. 이를 위해서는 노인들의 행동과

신체적 균형을 지속적으로 관찰해야 한다. 이러한 방법 중 하나가 웨어러블 기기 안에 포함된 가속도계나 자이로스코프 센서를 사용하여 낙상을 검출하는 것이다. 센서를 통해서 기기 사용자가 움직이는 x, y, z 축에 대한 가속도 신호와 방위각을 계산하여 사용자의 움직임을 파악한다.

본 논문에서는 웨어러블 기기의 센서를 통해 수집한 데이터를 대표적인 기계 학습 모델인 결정 트리, 랜덤 포레스트, SVM 을 통해 낙상 검출 성능을 측정하였다. 또한 기계학습 모델에 적용하기 위한 낙상 검출에 특화된 데이터 분할, 전처리 및 특징 추출 방법에 대해서도 함께 논한다.

2. 관련 연구

국내에서 진행된 연구들 중 기계 학습이나 심층 학습(Deep Learning)을 사용한 관련 연구의 다수는 웨어러블 기기와 같은 센서를 통해 추출한 센서 데이터 기반이 아닌 카메라를 통해 얻은 영상을 분석해서 낙상을 검출하고 예측하였다[4][5][6][7]. 이 외에도 낙상 이후 발생하는 실내 바닥의 진동을 측정, 분석하여 낙상의 유무를 판단한 연구도 존재한다[8]. 센서 데이터만 이용한 연구도 존재하지만 기계 학습이나 심층 학습을 사용한 경우가 아닌 단순 임계점을 기준으로

낙상과 ADL 을 구분한 연구가 대다수였다[9]. 기존 카메라를 통해 영상을 분석한 연구와 바닥의 진동을 이용한 연구는 낙상 검출 공간이 실내로 제한되며 검출 기기를 모두 실내에 설치해야 한다는 제한점을 갖는다. 임계점을 통해 낙상을 검출하는 연구의 경우, 사람이 경험적으로 임계점 값을 설정하고 이를 기준으로 낙상을 검출하는 것이기 때문에 신호 자체에 대한 규칙 분석이나 특징 추출이 부재하다. 이는 낙상의 규칙을 통한 검출이 아니기 때문에 일반화된 검출을 유도할 수 없다. 따라서 영상이나 진동을 이용한 방법보다는 웨어러블 기기를 통해 추출한 센서데이터를 사용하는 방법이 좀더 대중적으로 낙상을 검출하는데 도움이 될 수 있으며, 본 연구는 기계 학습 기반의 낙상 검출에 대한 포괄적인 이해를 전달하고자 한다.

3. 실험 환경

3.1 데이터 설명

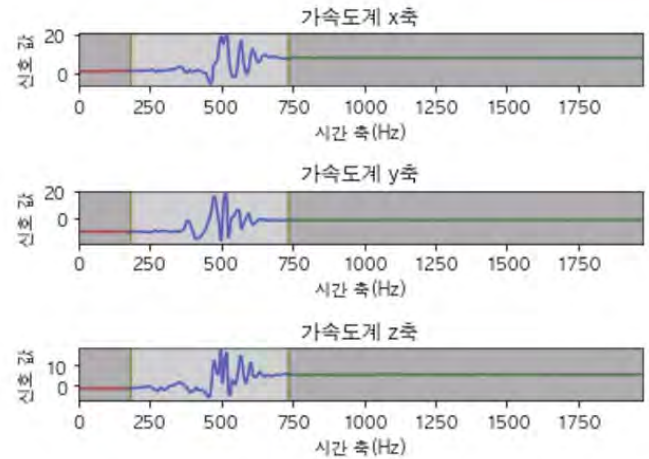
본 실험에서는 공개 데이터인 MobiFall Dataset 을 사용하였다[10]. MobiFall 데이터는 삼성 갤럭시 S3 스마트 폰을 이용하여 수집되었고 낙상과 ADL 의 가속도계 신호와 자이로스코프 신호를 포함한다. 가속도계의 평균 샘플링 주파수는 87Hz 이고 자이로스코프의 평균 샘플링 주파수는 200Hz 이다. ADL 의 경우 19 명의 참가자들은 11 가지의 ADL 을 시행하였고, 59 명의 참가자는 9 가지의 ADL 을 실행하였다. FALL 의 경우 66 명의 참가자들이 4 가지의 낙상을 실행하였다. 수집된 데이터는 상황에 대한 라벨 값을 모두 포함하고 있다. 아래의 <표 1>은 ADL, 낙상 대한 데이터 라벨 종류를 나타낸 것이다.

	라벨	활동 명	횟수	실행시간(s)
ADL	STD	서있기	1	300
	WAL	걷기	1	300
	SIT	의자에 앉아있기	1	60
	JOG	조깅하기	3	30
	JUM	점프하기	3	30
	STU	계단 오르기	6	10
	STN	계단 내려가기	6	10
	SCH	서있다가 앉기	6	6
	CHU	앉아있다가 서기	6	6
	CSI	차에 타기	6	6
	CSO	차에서 내리기	6	6
FALL	FOL	앞으로 넘어지기	3	10
	FKL	무릎 닿고 넘어지기	3	10
	BSC	뒤로 의자에 앉으면서 넘어지기	3	10
	SDL	옆으로 넘어지기	3	10

<표 1> ADL 과 FALL 데이터 종류

실험에는 MobiFall 데이터에 포함된 가속도계 센서 신호만을 이용하였다. 낙상이 발생하는 상황에서의

가속도계 신호 데이터를 시각화한 결과는 아래 (그림 1)과 같다. (그림 1)의 분할된 영역은 각각 순서대로 ‘STD(서있기)’, ‘FALL(낙상)’, ‘LYI(누워있기)’를 의미한다. 각각의 값에는 각각의 값들이 어떠한 상황인지를 알려주는 꼬리표가 포함되어 있다.



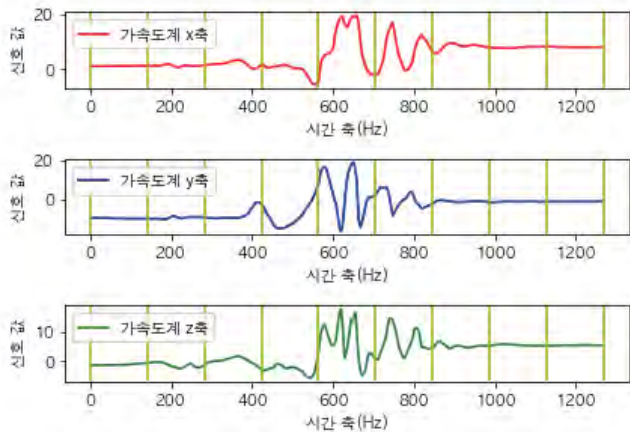
(그림 1) 낙상 가속도계 데이터 예시

낙상의 특징을 추출하기 위해서는 낙상이 일어나기 전 상황과 낙상이 발생한 후의 상황을 모두 포함해서 전처리를 진행해야 한다. 이를 위해서 ‘FALL’로 레이블 되어있던 부분을 기준으로 앞 뒤로 1 초 간격의 STD 와 LYI 가 포함되도록 수정하였다. 그 다음으로 a 모든 데이터 샘플의 길이를 최대 길이에 맞추어서 재 샘플링(Resampling)하였다. 이후 평균 이동 필터 (Average Filter)를 사용하여 신호의 잡음을 제거하였다. 사용한 평균 이동 필터는 M=2 인 다음의 식을 이용하였다.

$$Y[i] = \frac{1}{M} \sum_{j=-\frac{M-1}{2}}^{\frac{M-1}{2}} X[i+j] \quad (1)$$

3.2 데이터 분할

이전 연구들[11][12]은 낙상이 일어나는 시점부터 낙상이 발생한 후까지의 시간을 모두 포함하는 적절한 시간 간격이 약 2 초라고 판단하였다. 실험에서는 데이터를 분할하는 한 윈도우가 141 개의 값을 포함하도록 설정하였다. 즉, 한 윈도우 당 약 2 초를 포함할 수 있도록 하였다.



(그림 2) 데이터 분할 표시

3.3 특징 추출

특징 추출에 사용된 입력 값 벡터는 다음과 같다.

- 1) (a_x, a_y, a_z) 는 각각 가속도계 신호 데이터의 x, y, z 축 데이터를 의미한다. 즉, 3 개의 축에 대해 각각 141 개의 샘플을 포함하는 $Y(1, \dots, 3, 1, \dots, 141)$ 로 표현할 수 있다.
- 2) A 는 x, y, z 축에 대한 삼차원 가속도를 의미한다. 각 축 벡터의 크기를 사용해서 계산하며 계산식은 아래와 같다.

$$A(1 \dots 141) = \sqrt{Y(1, 1, \dots, 141)^2 + Y(2, 1, \dots, 141)^2 + Y(3, 1, \dots, 141)^2} \quad (2)$$

- 3) AV 는 벡터 A 의 각도 변화를 의미한다. AV 를 통해서 몸이 변화하는 각도를 계산할 수 있기 때문에 자이로스코프와 같은 다른 센서 데이터를 추가적으로 사용하지 않았다. AV 의 경우 141 차원의 벡터로 표현이 되어 모든 축(a_x, a_y, a_z)에 대해서 계산한다. n 은 1 부터 141 까지이며 이 값들을 통해 변화하는 a_x, a_y, a_z 에 대한 각도를 구할 수 있다.

$$AV = \left[\cos^{-1} \left(\frac{y^n \cdot y^{n+1}}{\|y^n\| \cdot \|y^{n+1}\|} \right) \right] \frac{180}{\pi} \quad (3)$$

결과적으로 (a_x, a_y, a_z, A, AV) 는 특징을 추출하기 위해 사용한 벡터이다. 해당 5 가지 벡터를 x 라고 칭할 때, 추출된 통계적 혹은 신호적 특징들은 다음과 같다.

- 1) 평균(Average): 다섯 개의 벡터를 모두 사용하여 시간 윈도우 내의 각각의 평균 값을 계산하였다.
- 2) 최대값(Maximum): 다섯 개의 벡터를 모두 사용하여 시간 윈도우 내의 각각의 최대 값 계산하였다.
- 3) 최소값(Minimum): 다섯 개의 벡터를 모두 사용하여 시간 윈도우 내의 각각의 최소 값 계산하였다.
- 4) 에너지(Energy): 이산 신호의 에너지는 다음의 방법으로 계산하였다.

$$E = \sum_{i=1}^n |x[n]|^2 \quad (4)$$

- 5) 스펙트럴 에너지(Spectral Energy): 이산 신호의 푸리에 변환을 사용하여 스펙트럴 에너지 값을 계산하였다.

$$E = \sum_{i=1}^n |FFT(x)|^2 \quad (5)$$

- 6) 표준편차(Standard Deviation): 다섯 개의 벡터를 모두 사용하여 시간 윈도우 내의 표준 편차를 계산하였다.
- 7) 상관도(Correlation): 가속도계 벡터 사이의 상관도를 계산하였다. 즉 $(a_x, a_y), (a_x, a_z), (a_y, a_z)$ 사이의 상관도를 측정하였다. 이를 위한 수식은 다음과 같다.

$$\text{corr}(x, y) = \frac{E((X - \mu_x)(Y - \mu_y))}{\sigma_x \sigma_y} \quad (6)$$

제시된 방법들을 통해서 총 33 개의 특징을 추출하였고 이를 데이터에 적용하였다.

4. 실험

기계 학습 모델로는 결정 트리, 랜덤 포레스트, SVM 을 사용하였다. MobiFall 데이터의 FALL 데이터 비율은 ADL 데이터 비율보다 훨씬 작다. 그리하여 각각의 모델에 큰 데이터 수에 맞춰 임의의 복원 추출한 훈련 데이터와 작은 데이터 수에 맞춰 임의의 복원 추출한 훈련 데이터를 사용하여 학습을 진행하였다. 실험 데이터의 경우 작은 데이터 수에 맞춰 임의의 복원 추출하였다. 아래의 <표 2>는 진행한 실험의 결과이다.

	F1 점수	정밀도	재현율	정확도
결정 트리				
작은 데이터에 맞춰 임의의 복원 추출	0.77	0.76	0.78	0.77
큰 데이터에 맞춰 임의의 복원 추출	0.77	0.79	0.76	0.78
랜덤 포레스트				
작은 데이터에 맞춰 임의의 복원 추출	0.83	0.79	0.88	0.82
큰 데이터에 맞춰 임의의 복원 추출	0.85	0.86	0.83	0.85
SVM				
작은 데이터에 맞춰 임의의 복원 추출	0.85	0.80	0.90	0.84
큰 데이터에 맞춰 임의의 복원 추출	0.86	0.82	0.90	0.85

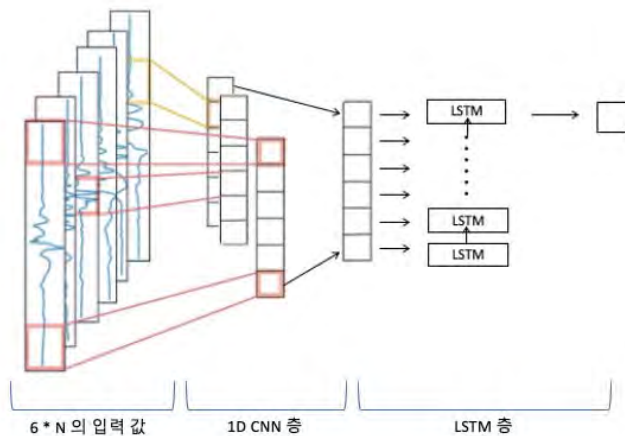
<표 2> 기계학습 모델 별 결과

<표 2>에서 볼 수 있듯이 SVM 이 가장 좋은 성능을 보이는 것을 확인할 수 있다. 정밀도(Precision)와 재현율(Recall)의 경우 상충 관계(Trade-Off)에 있기 때문에 하나의 점수가 높으면 상대적으로 다른 점수가

낮은 경향을 함께 보여주고 있다. 또한 전반적으로 작은 데이터에 맞춰 임의 복원 추출한 결과보다 큰 데이터 수에 맞춰 임의 복원 추출한 실험의 성능이 더 좋은 경향을 보인다.

낙상 검출에서는 정확도(Accuracy) 점수만큼 정밀도와 재현율의 점수가 적절하게 함께 높아야 한다. 정밀도 점수는 잘못된 알람(False Alarm)의 여부를 알려주기 때문에 중요하다. 다른 연구들에서도 정밀도와 재현율을 함께 참고할 수 있는 F1 점수를 함께 사용한다. 실험에서는 SVM 의 F1 점수가 0.86 으로 가장 높았다.

본 연구를 통해 전통적인 기계 학습 기반의 낙상 검출의 타당성을 확인하였으며 향후 연구로 깊은 인공 신경망 모델인 CNN(Convolutional Neural Network)과 RNN(Recurrent Neural Network)을 이용하여 낙상 검출을 진행할 예정이며 예상되는 모델은 아래의 (그림 3)과 같다.



(그림 3) 1D CNN 예시

5. 결론

본 논문에서는 다양한 낙상 검출 방법들 중 초기 설치 비용이 상대적으로 저렴하고 실내외에서도 낙상을 바로 검출할 수 있는 웨어러블 기기를 사용하여 기계 학습 기반의 낙상 검출을 실험하였다. 이를 위해 데이터 분할 및 전처리를 진행하였고 모델 학습에 이용하는 전반적인 낙상 검출에 대해서 정량적으로 검증하였다. 대표적인 기계 학습 모델인 결정 트리, 랜덤 포레스트, SVM 등을 적용하였으며 SVM 의 낙상 검출 성능이 다른 모델에 비해 가장 높음을 확인할 수 있었다. 본 연구 결과를 기반으로 최신 깊은 인공 신경망을 적용하여 낙상 검출 성능을 향상시킬 계획이다.

사사

이 성과는 2020 년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원과 과학기술정보통신부 및 정보통신기획 평가원의 SW 중심대학지원사업으로 수행된 연구임 (No. NRF2018R1C1B5086441)

참고문헌

- [1] YACCHIREMA, Diana, et al, 'Fall detection system for elderly people using IoT and big data', Procedia computer science, 130: 603-610, 2018.
- [2] 통계청. '2018 고령자 통계'. https://kostat.go.kr/portal/korea/kor_nw/3/index.board?bmode=read&aSeq=370781&pageNo=&rowNum=10&amSeq=&sTarget=&sTxt=
- [3] 보건복지부, '2017 노인실태 조사', 2017
- [4] 황세현, 반성범, '오픈소스 하드웨어와 RGB 카메라를 이용한 낙상 검출 시스템', 한국정보기술학회 논문지, 14.4: 19-24, 2016
- [5] Serdaroglu Werkan, 박장식, '딥러닝을 이용한 영상기반 사람 쓰러짐 검출', 제어로봇시스템학회, Vol.2018 No.5, 273-274, 2018
- [6] 김대연, 전봉규, '열화상 카메라를 이용한 3D 컨볼루션 신경망 기반 낙상 인식', 로봇학회 논문지, 13(1), pp. 45-54, 2018
- [7] 김선기, 안종수, '영상처리 기반 낙상 알고리즘의 구현', 한국위성정보통신학회논문지, Vol 12 Issue2, p. 56-60, 2017
- [8] 김동완, 유종현, 백승화, '바닥 진동을 통한 노인 낙상 검출', 전기전자학회논문지, 18.1: 134-139, 2014
- [9] 안순재, 김종만, '공개데이터셋을 이용한 충격 전 낙상 검출 알고리즘 평가 및 비교', 한국재활복지 공학회, 192-193, 2018
- [10] VAVOULAS, George, et al, 'The mobifall dataset: Fall detection and classification with a smartphone, In: Artificial intelligence: Concepts, methodologies, tools, and applications, IGI Global, p. 1218-1231, 2017
- [11] GIBSON, Ryan M., et al, 'Multiple comparator classifier framework for accelerometer-based fall detection and diagnostic', Applied Soft Computing, 39: 94-103, 2016.
- [12] Banos, O., Galvez, J. M., Damas, M., Pomares, H., & Rojas, I. 'Window size impact in human activity recognition', Sensors, 14(4), 6474-6499, 2014

오프로드형 자율주행 로봇 구동 메커니즘에 관한 연구

정혜원*, 김상훈*

*한경대학교 전기전자제어공학과

e-mail: kimsh@hknu.ac.kr

A Study on the off-road self-driving robot drive mechanism

Hye-Won Jeong*, Sang-Hoon Kim*

*Dept of Electrical, Electronic and Control, Hankyong National University

요 약

본 논문은 주행 로봇의 h/w에 관련된 연구로서, 기존의 험난한 지형을 극복하기 위해 1-자유도 반의 4-bar linkage 구조인 deformation wheel로 로봇 자체 지능을 통해 바퀴 변형을 수행한다. 바퀴 변형을 통해 평지뿐만 아니라 비평지 지형도 극복하는 로봇을 제시한다. 또한, 로봇 몸체 중간에 관절로 다이내믹셀을 삽입해 deformation wheel로 극복하지 못하는 장애물을 관절이 로봇 body를 들어 올려줘서 장애물의 크기에 대한 관절의 각도 조절 방법에 대해 제시한다.

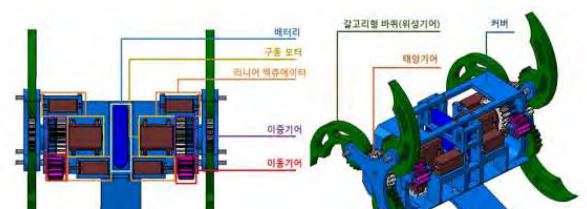
1. 서론

21세기에 접어들며 로봇의 종류와 성능은 다방면으로 두각을 드러냈다. 로봇 부문별 사업 중 로봇 부품 및 부분품이 45.7%를 차지하고 제조업용 로봇, 전문 서비스용 로봇, 개인 서비스용 로봇으로 순차적으로 32.5%, 14.8%, 7.4%를 차지한다.[4] 이렇게 활성화된 로봇 시장에서 재난 현장에서의 실종자 탐색 및 수색을 하는 로봇은 드물다. 탐사 로봇 가운데, 바퀴변형 로봇도 많이 나온 추세이다. 2-자유도 기반의 적응형 변형 바퀴 로봇[5].과 기어와 스포크를 사용한 변형 바퀴 로봇[6] 등이 존재한다. 재난 로봇이 구조 현장에서 필요한 이유는 인간이 들어가기 어렵거나 위험한 사고 현장에 사람 대신 로봇을 투입하기 위함으로 작은 로봇의 활약이 클 것으로 예상된다.[8] 본 논문은 평지와 비평지 지형을 모두 극복하는 '바퀴변형 기반의 오프로드형 로봇'의 H/W를 목표로 두었다. 로봇 몸체 중간 부분에 Joint를 추가해 장애물 크기에 맞는 몸체 각도 조절을 통해 극복할 수 있는 장애물 높이의 범위를 넓히는 모습을 볼 수 있다.

2. 관련 연구

(1) 장애물 극복을 위한 바퀴변형 이동로봇의 개발

기본적으로 바퀴 형태의 변형을 통해 장애물을 극복하는 로봇으로 다양한 환경에서 이동이 가능한 로봇이다. 바퀴변형에 필요한 주요 부품은 이동 기어, 이중기어, 리니어 액추에이터, 구동 모터 등이 있다.[1] 이 로봇은 전반적으로 많은 기어를 사용해 바퀴변형을 수행한다.



(그림 1. 장애물 극복을 위한 바퀴변형 이동로봇 외형)

(2) 서울대학교 스누맥스

스누맥스는 소프트 로봇으로 아르마딜로의 몸체 변형을 모방하여 바퀴가 접혔다 펴지는 종이 접기식 바퀴를 고안했다. 이 로봇은 전반적으로 바퀴의 크기를 변형해 바퀴 변형을 수행한다. 이 로봇 역시 모래밭 건너기, 계단 오르기 등을 수행할 수 있다.[2]



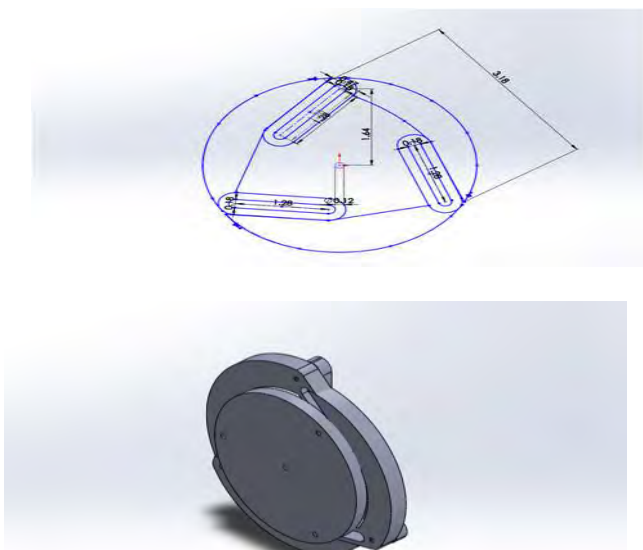
(그림 2. 스누맥스 외형)

위와 같은 로봇은 지형 중심의 바퀴변형 메커니즘을 갖는다. 본 논문은 지형뿐만 아니라 로봇의 몸체 중심에 부착된 관절을 통해 기존의 바퀴로 수행할 수 없는 장애물의 극복을 향상하는 연구를 제시한다.

3. 본론

3.1 구동 메커니즘

붕괴지역이나 사람이 투입되기 위험한 상황에서 로봇의 활용이 중요하다. 이런 험난한 지형에서 로봇이 무리 없이 이동하기 위해서는 로봇의 주행부가 중요하다. 따라서 로봇의 바퀴와 다리를 모두 사용할 수 있는 바퀴변형 기반의 로봇을 선정했다. 평지에서는 원형 wheel로 주행을 수행하고 비평지 주행에서는 3축 다리로 변형해 주행을 수행하는 방식을 생각했다. 그리하여 1-자유도 기반의 4-bar linkage 구조로 원형 wheel과 3축 다리가 모두 공존하는 가변형 wheel의 설계를 진행했다. 한 개의 wheel에는 wheel_circle, base, leg가 존재한다. circle 또는 base의 회전 시, 3축 leg가 펼쳐지는 메커니즘이다. wheel의 설계 툴은 Solidwork 2017을 사용했다.



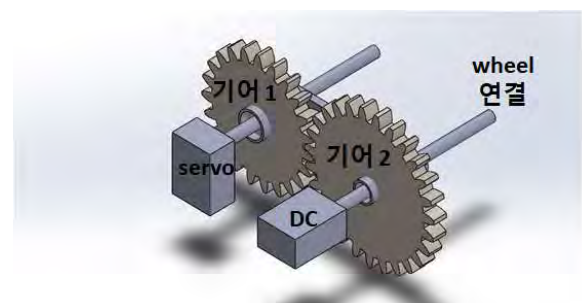
(그림 3. Solidworks simulation)

circle은 9.5cm, base는 10.5cm, leg는 10cm로 설계했다. wheel의 전체 반경의 크기는 12.5cm이고 leg식 wheel로 변형했을 때의 전체 크기는 21.5cm이다. 이때, 이 크기의 wheel이 극복 가능한 장애물의 높이는 전체 wheel 반지름에 2.6배를 곱한 값이 된다. 따라서 $6.5 \times 2.6 = 16.25\text{cm}$ 로 최대 극복 가능한 장애물의 높이는 16.25cm가 나왔고 이 높이는 평균 실내 계단의 높이를 극복할 수 있다. 이렇게 설계한 wheel을 3D Printer로 출력했고 필라멘트는 PLA를 사용했다.



(그림 4. Wheel 3D Printer 출력)

본 논문에서 제시한 wheel은 변형바퀴로 원형 wheel과 leg식 wheel이 자유자재로 변형되어야 한다. 변형을 위한 메커니즘으로 기어 방식을 선택했다. 기어는 이중기어 기반의 타이밍 풀리를 사용했다. 그리고 구동을 위한 액추에이터로 서보모터와 DC 모터를 사용하며 각 기어에 거쳐서 모터의 동력을 전달해줄 구동축을 사용했다.



(그림 5. 이중기어 방식 메커니즘)

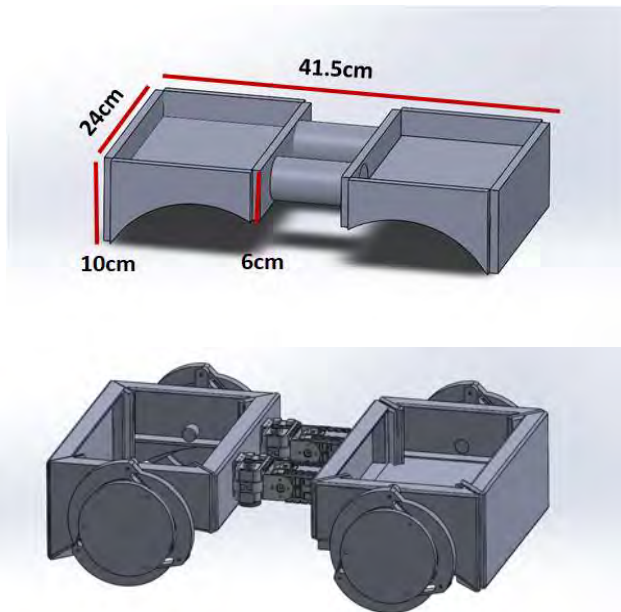
DC모터의 동력전달 방법은 DC모터를 시작으로 축을 통해 wheel이 구동된다. 서보모터의 동력전달 방법은 서

보모터를 시작으로 기어1, 기어2를 거쳐 축을 통해 wheel이 변형된다.



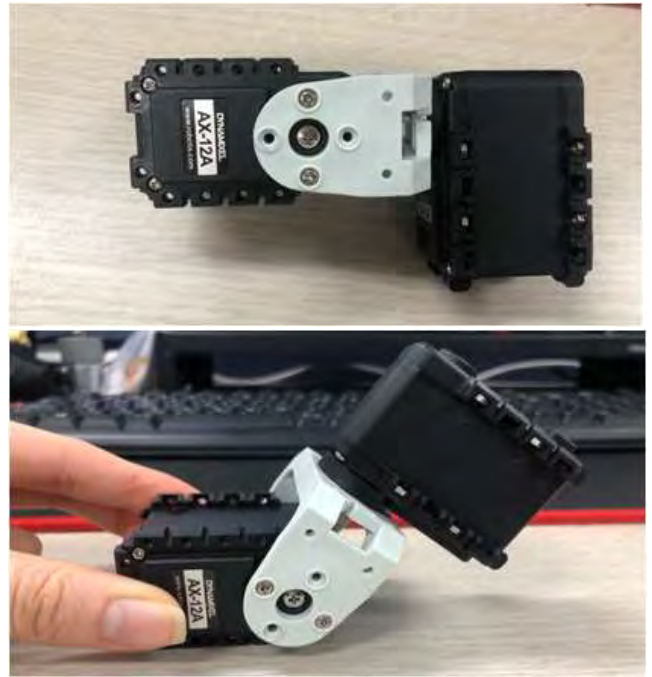
3.2 Body 구조 설계

협소한 공간에서 로봇 body는 주행부 만큼 중요하다. 사람이 들어갈 수 없는 공간을 오로지 로봇이 수행하기 때문에 로봇 크기가 작으면 작을수록 수월하다. 로봇 body는 전체 45cm 이하로 설계를 진행했다. 그리고 극복 가능한 장애물의 높이를 극대화하기 위해 body 중간에 관절을 추가했다. 모양은 전체 직육면체 모양의 중간 홈이 파여있는 형상으로 설계를 진행했다.



(그림 7. body design)

각 body 사이에 존재하는 관절은 Dynamicxel AX 시리즈를 사용했다. 관절 1개당 Dynamicxel을 총 두 개를 사용했다.



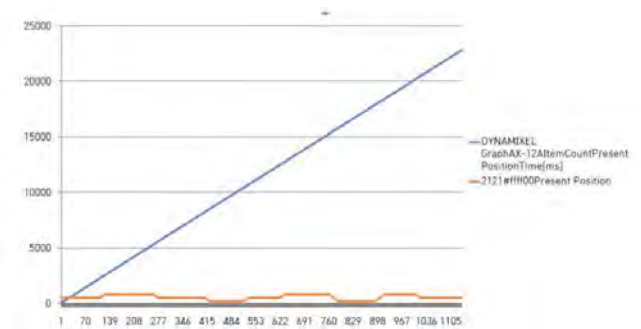
(그림 8. 로봇 관절을 위한 Dynamicxel 조립)

4. 실험 및 검토

Dynamicxel을 구동하기 위해 ROBOTIS에서 보급하는 software인 Dynamicxel Wizard 2.0과 RoboPlus[7]를 사용했다. 관절이 로봇 앞부분을 들어 올리기 위한 최대 각도는 90도로 설정했고 로봇이 전복되었을 때를 고려해 -90도도 포함했다.



(그림 9. Dynamicxel 각도 조절마다 데이터 형성)



(그림 10. Dynamicxel 각도 조절마다 excel 데이터 형성)

5. 결론 및 향후계획

기존 탐사 및 재난 로봇은 다양한 H/W 프레임이 존재한다. 다른 탐사 로봇과 차별화된 점은 원형 wheel에서 3축 다리 wheel로 변형하는 deformation wheel이라는 점이다. 그리고 로봇의 몸체에 존재하는 관절을 통해 극복할 수 있는 장애물 높이의 범위를 넓힐 수 있다는 점이다.

협소하고 험난한 지형을 수행하는 로봇의 메커니즘을 설계하며 보완해야 할 점들이 있다. 우선 wheel의 변형에 있어 기어 방식에서 힘을 전달하는 구동축의 내구력이 약해 회전에 필요한 힘을 견디지 못하는 상황이 발생할 수 있다. 그래서 바퀴변형 방식을 기어 방식이 아닌 다른 방식을 더 고려해볼 계획이다. 그리고 body를 출력할 때, body의 밑면을 내구력이 강한 소재를 이용해 제작할 계획이다. 그래서 밑면은 아크릴이나 카본을 사용할 예정이고 body의 옆면들은 PLA 필라멘트를 이용해 3D Printer로 출력할 계획이다. 그리고 body 관절 부품으로 사용할 Dynamicxel에 IMU센서가 내장된 시리즈를 사용해 장애물의 높이에 맞게 알맞은 각도를 보상해주는 실습도 진행할 예정이다.

참고문헌

- [1] M. Kim, S. Heo, J. Ahn, B. Chu, Transformable Wheeled Mobile Robot for Overcoming Obstacles, 한국기계항공학회 234-234, 2018.4
- [2] <http://www.irobotnews.com/news/articleView.html?idxno=7559>
- [3] Yoo Seok Kim, Haan Kim, Gwang Pil Jung, Seong Han Kim, Kyu-Jin Cho, Chong Nam Chu, A New Wheel Design for Miniaturized Terrain Adaptive Robot, 한국정밀공학회지, 30(1), 32-38, 2013.1
- [4] 산업통상자원부 '2017년 로봇산업 실태 조사 결과 보고서'
- [5] Ki joong Kim, Optimal trajectory planning for 2-DOF adaptive transformable wheel robot based on kinematics, 서울대학교 대학원 기계항공공학부 학위논문, 1-28
- [6] M. N. Kwag, H. S. Yang, Study on a stair climbing robot with hybrid wheel, 한국정밀공학회 373-374, 2010.5
- [7] <http://emanual.robotis.com/docs/kr/>
- [8] <http://www.hani.co.kr/arti/science/technology/824488.html>

그래프 신경망과 멀티 모달 맥락 정보를 이용한 장면 그래프 생성

정가영, 김인철

경기대학교 컴퓨터과학과

email: jgyy4775@kyonggi.ac.kr, kic@kyonggi.ac.kr

Scene Graph Generation with Graph Neural Network and Multimodal Context

Ga-Young Jung, In-cheol Kim

Department of Computer Science, Kyonggi University

요 약

본 논문에서는 입력 영상에 담긴 다양한 물체들과 그들 간의 관계를 효과적으로 탐지하여, 하나의 장면 그래프로 표현해내는 새로운 심층 신경망 모델을 제안한다. 제안 모델에서는 물체와 관계의 효과적인 탐지를 위해, 합성곱 신경망 기반의 시각 맥락 특징들뿐만 아니라 언어 맥락 특징들을 포함하는 다양한 멀티 모달 맥락 정보들을 활용한다. 또한, 제안 모델에서는 관계를 맺는 두 물체 간의 상호 의존성이 그래프 노드 특징값들에 충분히 반영되도록, 그래프 신경망을 이용해 맥락 정보를 임베딩한다. 본 논문에서는 Visual Genome 벤치마크 데이터 집합을 이용한 비교 실험들을 통해, 제안 모델의 효과와 성능을 입증한다.

1. 서론

심층 영상 이해(Deep Image Understanding)를 요구하는 대표적인 인공지능 및 컴퓨터 비전 문제 중 하나로, 장면 그래프 생성(Scene Graph Generation) 문제가 있다. 장면 그래프는 한 영상에 담긴 장면을 그래프 형태로 표현한 것으로서, 그래프를 구성하는 각 노드(node)는 영상 속의 물체(object)를, 각 간선(edge)은 물체들 간의 관계(relationship)를 각각 나타낸다. 따라서 하나의 장면 그래프는 해당 영상의 장면을 설명하는 <주어 물체(subject)-관계 서술자(relationship predicate)-목적어 물체(object)> 형태의 사실 집합(fact set)으로 볼 수 있다. 즉 장면 그래프 생성 문제는 입력 영상에 관한 심층 이해의 결과로 해당 영상의 장면을 표현하는 하나의 지식 그래프(knowledge graph)를 생성하는 문제이다.

(그림 1)은 일반적인 장면 그래프 생성 과정을 보여주고 있다. 장면 그래프 생성을 위해서는 영상 속 물체 탐지(object detection)뿐만 아니라, 물체들 간의 관계 탐지(relationship detection)도 필수적으로 요구된다. 물체 탐지는 종래의 컴퓨터 비전 분야에서 많이 연구된 문제이나, 관계 탐지는 최근에 와서야 관심을 모으고 있는 문제로서 아직은 연구의 초기 단계에 머물고 있다. 영상 속의 두 물체들 간에 가질 수 있는 관계들은 매우 다양하다. 일반적으로 장면 그래프 생성 연구에서 많이 다루어지는 물체들 간의 관계에는 공간 관계(spatial relationship)와 의미적 관계(semantic relationship)가 있다. 공간 관계는 'on', 'next to', 'in front of'와 같이 영상 안에 놓인 물체들 간의 상대적 위치 관계를 나타내며, 반면에, 의미적 관계는 'wearing', 'eating', 'holding'과 같이 한 물체가 다른 물체에 행하는 행위와 연관된 관계이다.

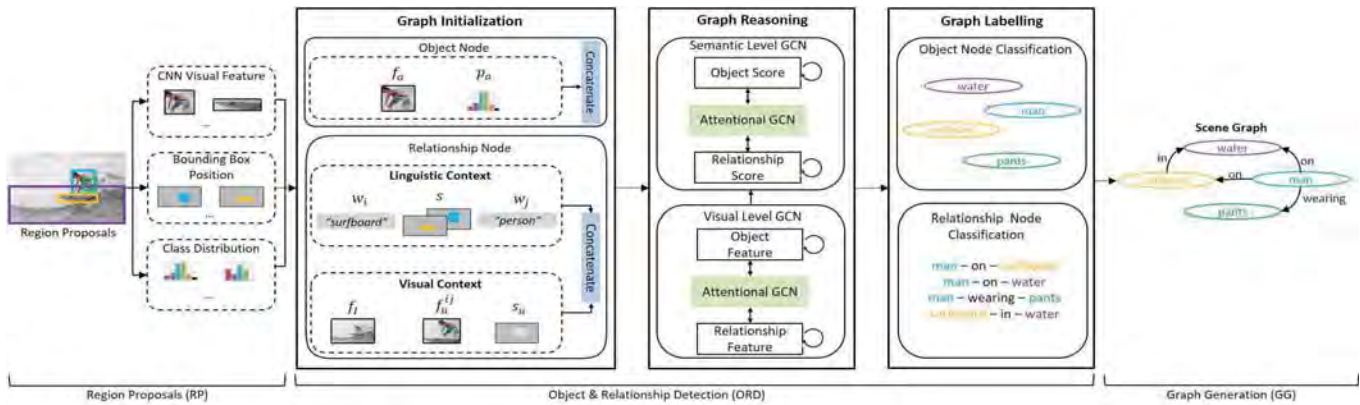
합성곱 신경망(Convolutional Neural Network, CNN)을 이용한 물체 탐지 기술은 현재 높은 수준에 도달해 있으나, 아직은 물체 식별과 영역 탐지에 오류가 있을 수 있다. 이는 곧 관계 탐지에 기초가 되는 두 물체의 식별에 불확실성과 오류가 있을 수 있다는 것을 의미한다. 비록 관계를 맺는 두 물체의 식별이 매우 분명하다고 하더라도, 두 물체 간에 가능한 관계의 수 또한 많기 때문에 물체 간의 관계를 정확히 판별하는 일은 결코 쉬운 일이 아니다. 더욱이 일반적으로 특정 관계와 그 관계를 맺을 수 있는 두 물체의 유형에는 다양한 의미적 제약이 존재한다. 예컨대, (그림 1)의 예에서, <man-wearing-shoes>의 관계는 가능하지만, <man-wearing-racket>이나 <shoes-wearing-man>과 같은 관계는 불가능하다는 것을 인간은 상식적으로 잘 알고 있다. 이러한 문제의 특성을 잘 고려하여, 영상으로부터 정확한 장면 그래프를 효과적으로 생성할 수 있는 모델의 개발이 필요하다.



(그림 1) 장면 그래프 생성 예시

장면 그래프 생성에 관한 많은 기존의 연구들[1, 2]에서는 장면 그래프 생성에 필요한 물체 탐지와 관계 탐지를 위해 합성곱 신경망(CNN)을 통해 영상에서 추출한 시각 특징만을 활용하였다. 대신 [2]의 연구에서는 그래프 신경망(Graph Neural Network)의 하나인 aGCN(attentional Graph Convolutional Network)을 통해, 장면 그래프를 구성하는 이웃 노드들의 맥락 정보를 각 노드의 특징값에 반영될 수 있도록 모델을 설계하였다. 한편, 시각적 관계

* 본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2017-0-01642)



(그림 2) 제안 모델의 구조

탐지(Visual Relationship Detection)에 관한 [3]의 연구에서는 두 물체 간의 효과적인 관계 탐지를 위해 영상에서 추출한 합성곱 신경망 시각 특징이 아닌 영상 캡션(image caption)이나 물체 범주명(object category)과 같은 텍스트에서 추출한 언어 특징도 함께 활용하였다. 하지만, 이 연구는 물체 탐지와 관계 탐지 간의 상호 작용을 고려해 이 두 문제를 동시에 해결해야 하는 장면 그래프 생성과는 달리, 이미 탐지된 물체들을 토대로 단지 그들 간의 관계만을 판별해내는데 연구에 초점이 맞추어져 있다. 따라서 이웃한 물체 노드와 관계 노드들의 맥락 정보를 각 그래프 노드에 반영하기 위한 별도의 그래프 신경망 기반의 특징값 임베딩 과정은 적용되지 않았다.

이러한 기존 모델들의 한계성을 고려하여, 본 논문에서는 장면 그래프 생성을 위한 새로운 심층 신경망 모델을 제안한다. 제안 모델에서는 물체와 관계의 효과적인 탐지를 위해, 합성곱 신경망 기반의 시각 맥락 특징들뿐만 아니라 언어 맥락 특징들을 포함하는 다양한 멀티 모달 맥락 정보들을 활용한다. 특히 <주어 물체-관계 서술자-목적어 물체> 형태의 관계 표현에 내포된 각 물체의 순서와 역할을 고려해 양방향 순환신경망(bidirectional Recurrent Neural Network, biRNN)을 이용해 언어 맥락 특징 벡터를 생성한다. 또한, 제안 모델에서는 관계를 맺는 두 물체 간의 상호 의존성이 그래프 노드 특징값들에 충분히 반영되도록, 그래프 신경망을 이용해 맥락 정보를 임베딩한다. 본 논문에서는 제안 모델의 효과와 성능을 분석하기 위해, Visual Genome[4] 벤치마크 데이터 집합을 이용한 다양한 비교 실험들을 수행하고 결과를 소개한다.

2. 장면 그래프 생성 모델

2.1 모델 개요

본 논문에서 제안하는 장면 그래프 생성을 위한 신경망 구조는 (그림 2)와 같다. 제안 모델은 물체 영역 탐지(region proposals, RP), 물체 및 관계 탐지(object & relationship detection, ORD), 그리고 그래프 생성(graph generation, GG)의 3단계로 이루어진다. 물체 영역 탐지(RP) 단계에서는 대표적인 물체 탐지 모듈인 Faster R-CNN을 이용하며, 입력 영상의 각 물체 후보 영역별 ResNet101 시각 특징 벡터, 바운딩 박스(bounding box)의 위치와 크기, 물체 범주별 확률 분포(object class distribution) 등을 구해낸다.

물체 및 관계 탐지(ORD) 단계는 다시 그래프 초기화(graph initialization), 그래프 추론(graph reasoning), 그래프 레이블링(graph labelling)의 세부 단계들로 구성된다. 그래프 초기화 단계에서는 물체 영역 탐지(RP) 과정을 통해 얻어진 입력 영상 내 각 물체 영역들을 기초로 장면 그래프를 구성할 물체 노드 및 관계 노드들을 생성하고, 이들 노드에 초기 특징값을 부여한다. 그래프 추론 단계에

서는 그래프 합성곱 신경망(Graph Convolution Neural Network, GCN)을 이용하여, 그래프 내 이웃한 물체 노드 및 관계 노드들 사이에 서로 맥락 정보를 교환하며 각 노드의 특징값을 갱신한다. 그래프 레이블링 단계에서는 각 노드의 최종 특징값을 바탕으로 물체(object) 및 관계(relationship)를 분류(node classification)해낸다. 마지막 그래프 생성 단계에서는 분류된 각 노드들을 토대로 하나의 장면 그래프를 완성한다.

2.2 물체 노드 특징

제안 모델의 그래프 초기화(Graph Initialization) 단계에서는 영상에서 탐지된 각 물체 영역별로 그래프 내에 하나의 물체 노드(object node)를 생성하고, 해당 노드에 초기 특징값을 부여한다. 제안 모델에서는 대표적인 물체 탐지 모듈인 Faster R-CNN을 입력 영상에 적용하여, 각 물체 후보 영역별로 추출한 시각 특징 벡터와 물체 클래스 확률 분포를 각 물체 노드의 초기 특징값으로 할당한다. 이 초기 특징값은 추후 그래프 신경망을 통해 이웃 노드들의 풍부한 맥락 정보가 결합된 후, 물체 노드의 분류에 사용된다. 따라서 제안 모델에서 최종 판별하는 각 노드의 물체 범주는 Faster R-CNN이 추측한 초기 물체 범주와는 달라질 수도 있다.

- **물체 시각 특징(object visual feature)**
 - f_o : 해당 물체 영역의 합성곱(CNN) 시각 특징
- **클래스 확률 분포(class probability distribution)**
 - p_o : 해당 물체 영역의 물체 클래스 확률 분포

따라서 각 물체 노드의 초기 특징 벡터 O 는 (식 1)과 같다.

$$O = [f_o, p_o] \quad (\text{식 1})$$

(식 1)의 $[,]$ 은 연결 연산(concatenate)을 나타낸다.

2.3 관계 노드 특징

그래프 초기화 단계에서는 앞서 설명한 물체 노드의 초기화 이외에, 관계 노드의 초기화도 수행한다. 즉 영상에서 탐지된 물체 영역들의 각 쌍(pair)에 대해 그래프 내에 하나의 관계 노드를 생성하고, 해당 노드에 초기 특징값을 부여한다. 기존 모델들과는 달리, 제안 모델에서는 효과적인 관계 탐지를 위해 영상 기반의 시각 맥락 특징(visual context feature)들 외에 텍스트 기반의 언어 맥락 특징(linguistic context feature)들도 포함하는 풍부한 멀티 모달 맥락 정보를 관계 노드의 초기 특징값으로 할당한다. 관계 노드를 위한 시각 맥락 특징 집합과 언어 맥락 특징 집합의 구성은 다음과 같다.

- **시각 맥락 특징 집합(visual context feature set)**
 - f_I : 입력 영상 전체의 합성곱 시각 특징
 - f_u^{ij} : 하나의 관계(relationship)를 맺을 수 있는 주어

물체(subject) 영역과 목적어 물체(object) 영역을 둘러싸는 영상 영역(union box)의 합성 곱 시각 특징

- s_u : 주어 물체와 목적어 물체를 둘러싸는 영역(union box)의 위치 정보

$$s_u = \left(\frac{x_{tl}}{W}, \frac{y_{tl}}{H}, \frac{x_{br}}{W}, \frac{y_{br}}{H}, \frac{(x_{br} - x_{tl})(y_{br} - y_{tl})}{WH} \right) \quad (\text{식 } 2)$$

(식 2)의 x, y, w, h 는 각각 물체 영역의 중심 좌표와 너비, 높이를 의미하며, W, H 는 union box의 너비와 높이를 각각 나타낸다. 한편, (식 3)의 x_{tl}, y_{tl} 은 union box의 왼쪽 상단 모서리 좌표를, x_{br}, y_{br} 은 오른쪽 하단 모서리 좌표를 각각 나타낸다.

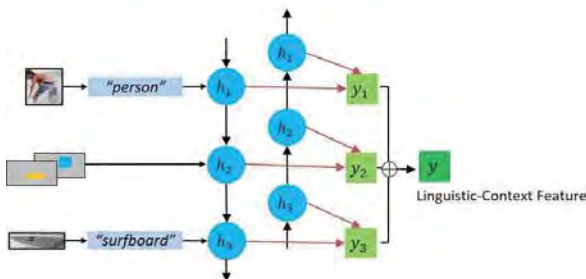
• 언어 맥락 특징 집합(linguistic context feature set)

- w_i : 주어 물체의 예상 범주명(object category)을 다층 퍼셉트론(MLP)으로 임베딩한 특징
- s : 주어 물체 영역과 목적어 물체 영역의 영상 내 위치 정보

$$s = [x_i, y_i, w_i, h_i, \frac{x_i - x_j}{W}, \frac{y_i - y_j}{H}, \log \frac{w_i}{w_j}, \log \frac{h_i}{h_j}, x_j, y_j, w_j, h_j] \quad (\text{식 } 3)$$

- w_j : 목적어 물체의 예상 범주명을 다층 퍼셉트론으로 임베딩한 특징

한편, 하나의 관계를 표현하기 위한 언어 맥락 특징 벡터 y 는 앞서 소개한 w_i, s, w_j 등 3 가지 구성 요소들을 단순 연결(concatenate), 단방향 순환신경망(RNN), 양방향 순환신경망(biRNN) 등 다양한 결합 방식으로 구할 수 있다. 일반적으로 두 물체 간의 관계는 <주어-관계 서술자-목적어>와 같이 3가지 언어 구성 요소 각각의 위치와 순서, 그리고 역할을 고려하여 하나의 시퀀스(sequence)로 표현하는 것이 바람직하다. 이 점에 착안하여, 본 제안 모델에서는 3가지 언어 구성 요소들(w_i, s, w_j)을 양방향 순환신경망(bidirectional Recurrent Neural Network, biRNN)을 이용해 순차적으로 결합함으로써, 언어 맥락 특징 벡터 y 를 생성해낸다. 특히, 언어의 개념적 관계에 기초하여 해당 관계를 맺을 수 있는 가능한 주어 물체 유형과 목적어 물체 유형 간의 쌍방향 제약(bidirectional constraint)을 특징 벡터 y 에 효과적으로 담아내기 위해 제안 모델에서는 양방향 순환신경망(biRNN)으로 언어 맥락 시퀀스 $\langle w_i, s, w_j \rangle$ 를 임베딩한다. (그림 3)은 biRNN 기반의 언어 맥락 특징값 임베딩 과정을 그림으로, (식 4)는 해당 과정을 수식으로 각각 나타내고 있다.



(그림 3) biRNN 기반의 언어 맥락 특징 임베딩

$$y = (W_{h_{y_1}}^{\rightarrow} h_1 + W_{h_{y_1}}^{\leftarrow} h_1) + (W_{h_{y_2}}^{\rightarrow} h_2 + W_{h_{y_2}}^{\leftarrow} h_2) + (W_{h_{y_3}}^{\rightarrow} h_3 + W_{h_{y_3}}^{\leftarrow} h_3) \quad (\text{식 } 4)$$

W 는 학습 파라미터, h 는 순방향에서의 은닉상태(hidden

state), h 는 역방향에서의 은닉상태를 의미한다. 제안 모델에서 각 관계 노드의 초기 특징값은 시각 맥락 특징 벡터와 biRNN으로 임베딩된 언어 맥락 특징 벡터를 결합하여, (식 5)와 같이 주어진다.

$$R = [f_I, f_u^{ij}, s_u, y] \quad (\text{식 } 5)$$

2.4 그래프 추론 및 레이블링

제안 모델의 그래프 추론(Graph Reasoning) 과정은 각각 시각적 추론 단계(visual level)와 의미적 추론 단계(semantic level)를 나타내는 그래프 합성 곱 신경망(Graph Convolutional Network)의 2개 계층으로 구성된다. 각 계층에서는 그래프 초기화 단계에서 부여된 각 노드의 초기 특징값들을 토대로 그래프의 이웃한 노드들 사이에 맥락 정보를 서로 교환함으로써, 각 노드의 특징값을 새롭게 갱신한다. 특히 제안 모델에서는 주의 집중 그래프 합성 곱 신경망(attentional GCN)을 사용함으로써, 이웃 노드들 중 집중해야 할 노드와 그렇지 않은 노드를 구별하여 각 노드의 특징값 갱신에 이웃 노드의 정보를 차등적으로 반영한다. 각 노드의 주의 집중 값 a_i 는 (식 6) 및 (식 7)과 같이, 두 노드의 특징값 z_i 와 z_j 를 토대로 예측한다.

$$m_{ij} = w\sigma(W_a[z_i^{(l)}, z_j^{(l)}]) \quad (\text{식 } 6)$$

$$a_i = \text{softmax}(m_i) \quad (\text{식 } 7)$$

(식 6)과 (식 7)에서 σ 는 2개 계층 퍼셉트론(MLP)을, w 와 W 는 학습용 파라미터를 각각 나타낸다.

주의 집중 그래프 신경망을 이용하여 물체 노드의 특징값을 갱신할 때는 주어물체 노드<->목적어 물체 노드, 주어물체 노드<->관계 노드, 목적어 물체 노드<->관계 노드 간에 맥락 정보 교환이 이루어진다. 반면에 관계 노드의 특징값을 갱신할 때는 관계 노드<->주어물체 노드, 관계 노드<->목적어 물체 노드 간에 맥락 정보 교환이 일어난다. 따라서 그래프 내 각 물체 노드의 특징값 갱신은 (식 8)과 같고, 반면에 관계 노드의 특징값 갱신은 (식 9)와 같다.

$$z_i^o = \sigma(W_{so}Z^o a_{so} + W_{sr}Z^r a_{sr} + W_{or}Z^r a_{or}) \quad (\text{식 } 8)$$

$$z_i^r = \sigma(z_i^r + W_{rs}Z^o a_{rs} + W_{ro}Z^o a_{ro}) \quad (\text{식 } 9)$$

(식 8)과 (식 9)에서 s, r, o 는 주어 물체(subject) 노드, 관계(relationship) 노드, 목적어 물체(object) 노드를 각각 나타낸다. 시각적 추론 단계와 의미적 추론 단계로 구성되는 2개의 주의 집중 그래프 신경망 계층에서는 이와 같은 노드 특징값 갱신 과정이 각각 수행된다. 대신 시각적 추론 단계의 결과인 각 노드의 물체 및 관계 클래스 확률 분포가 의미적 추론 단계의 초기 노드 입력으로 제공된다.

끝으로, 그래프 레이블링(Graph Labelling) 단계에서는 의미적 추론 단계에서 얻어진 각 노드의 최종 특징값을 바탕으로, 물체 및 관계를 분류해낸다. 물체 노드는 물체 클래스 확률 분포에서 가장 큰 값으로 레이블링한다. 관계 노드 또한 같은 과정을 거쳐 레이블링 된다. 이를 통해 <주어-서술자-목적어>형태의 정형화된 결과물을 얻는다.

3. 구현 및 실험

3.1 데이터 집합과 모델 학습

본 논문에서는 Visual Genome[4] 벤치마크 데이터 집합을 이용하여, 제안하는 모델의 성능을 평가하였다. Visual Genome 데이터 집합에서 등장 빈도수가 높은 물체 종류 150개와 관계 종류 50개를 선별하여 평가에 사용하였다. 또한, 데이터 집합 영상들 중에서 56,224장은 학습 데이터로, 26,446장은 평가 데이터로 사용하였다.

제안 모델은 Ubuntu 16.04 LTS 환경에서 Python 딥러

닝 라이브러리인 PyTorch를 이용하여 구현하였다. 모델의 학습과 평가는 GeForce GTX 1080Ti GPU카드가 설치된 하드웨어 환경에서 수행하였다. 모델 학습을 위해 일괄 처리량(batch size)은 8, 반복 횟수(epoch)는 6으로 각각 설정하였다. 또한 학습율(learning rate)은 0.005, 최적화 함수(optimizer)는 확률적 경사 하강법(stochastic gradient descent)을 사용하였다.

3.2 실험

본 논문에서의 제안하는 장면 그래프 생성 모델의 성능을 평가하기 위해 SGGen, PhrCls, PredCls 총 3가지의 평가 지표를 사용하였다. 위 지표들은 어느 정도의 정답을 사용하는지에 차이를 둔다. SGGen은 물체의 영역, 종류, 관계를 모두 예측하고 PhrCls는 물체의 영역만 정답을 사용하여 나머지를 예측한다. PredCls는 물체의 영역과 종류를 정답을 사용하여 관계만을 예측한다. 모두 장면 그래프를 나타내는 트리플들의 재현율을 측정하며 트리플을 구성하는 주어 물체와 목적어 물체 그리고 그 둘의 관계가 모두 정답과 같아야 정답으로 인정한다. SGGen은 추가적으로 두 물체의 영역이 정답 물체의 영역과 0.5이상의 IoU값을 가질 때 해당 트리플을 정답으로 인정한다. 총 3가지의 비교 실험을 진행하였으며 성능 평가를 위해 상위 50개(r@50)와 100개(r@100)에 대한 성능을 측정하였다.

첫 번째 실험은 제안 모델의 관계 노드를 위한 언어 맥락 특징 임베딩 방법인 biRNN의 효과를 입증하기 위한 실험이다. 이 실험에서는 언어 맥락 특징을 단순 연결(concat)하였을 경우, RNN으로 임베딩 하였을 경우, biRNN으로 임베딩 하였을 경우를 서로 비교하였다.

<표 1> 언어 맥락 특징의 임베딩 방법 간의 성능 비교

method	SGGen		PhrCls		PredCls	
	r@50	r@100	r@50	r@100	r@50	r@100
concat	24.35	27.07	41.96	52.50	65.20	69.32
RNN	24.82	27.20	43.33	53.81	65.98	69.75
biRNN	24.91	27.61	43.69	54.16	66.87	71.15

<표 1>은 실험 결과를 나타낸다. 실험 결과에서 biRNN을 적용하였을 때 3가지 평가 지표 모두 가장 높은 성능을 보여주었다. 단순 연결(concat)하였을 때는 <주어-서술자-목적어>의 시퀀스를 전혀 반영하지 못해 가장 성능이 낮았다. RNN의 경우 시퀀스 특징을 반영하였기에 단순 연결보다는 나았으나, 양방향성까지 고려한 biRNN보다는 낮은 성능을 보였다.

두 번째 실험은 본 논문에서 제안하는 언어 맥락 특징 집합(LC)과 시각 맥락 특징 집합(VC)을 포함하는 멀티모달 관계 노드 특징값의 효과를 분석하기 위한 실험이다. 이 실험에서는 시각 맥락 특징 집합(VC)만 사용하였을 경우, 언어 맥락 특징 집합(LC)만 사용하였을 경우, 두 가지 모두 사용하였을 경우를 각각 비교한다. 물체 노드 특징값은 모두 동일하게 사용하였고, 언어 맥락 특징 집합을 사용한 경우에는 biRNN을 통한 임베딩 과정을 거친다.

<표 2> 특징 집합들 간의 성능 비교

Feature Set		SGGen		PhrCls		PredCls	
VC	LC	r@50	r@100	r@50	r@100	r@50	r@100
✓		23.93	26.92	40.50	51.30	63.94	68.35
	✓	24.49	27.35	42.76	53.29	66.92	71.03
✓	✓	24.91	27.61	43.69	54.16	66.87	71.15

<표 2>는 실험 결과를 나타낸다. 이 실험 결과는 본 제안 모델과 같이 관계 노드 특징값으로 언어 맥락 특징 집합(LC)과 시각 맥락 특징 집합(VC)을 모두 활용하였을 때, 가장 높은 성능을 보여주었다. 또한, 시각 맥락 특징 집합(VC)만을 사용하였을 때에 비해, 언어 맥락 특징 집합(LC)만을 사용하였을 때가 상대적으로 더 높은 성능을 보였다. 이 결과를 통해, 언어 맥락 특징 집합(LC)이 시각 맥락 특징 집합(VC)에 비해 성능 개선에 더 큰 도움을 주는 것으로 판단한다.

세 번째 실험은 본 논문에서 제안한 장면 그래프 생성 모델을 최신 기존 모델들(state-of-the-art models)과 성능을 비교하는 실험이다. 앞서 설명한 바와 같이 [1]과 [2]의 모델은 시각 특징만을 이용하는데, 반해 [3]의 모델은 영상 캡션(caption)에 기초한 언어 특징을 활용한다. 또한, [1]과 [3]의 모델들과는 달리, [2]의 모델은 그래프 신경망 기반의 노드 특징값 임베딩 과정을 별도로 포함하고 있다.

<표 3> 장면 그래프 생성 모델 간의 성능 비교

model	SGGen		PhrCls		PredCls	
	r@50	r@100	r@50	r@100	r@50	r@100
[1]	10.72	14.22	24.34	26.5	67.03	71.01
[2]	11.4	13.7	29.6	31.6	54.2	59.1
[3]	22.17	23.62	28.58	31.69	85.02	91.77
ours	24.91	27.61	43.69	54.16	66.87	71.15

<표 3>에서 알 수 있듯이, 제안 모델이 SGGen과 PhrCls에서 기존 모델들보다 더 우수한 성능을 보였다. 다만, PredCls 평가 지표에서만 [3]의 모델보다 낮은 성능을 보였다. [3]의 모델은 본 제안 모델과는 달리, 입력 영상에 관한 캡션 텍스트 데이터를 추가적으로 활용하였기에 이러한 성능 차이를 보인 것으로 판단한다. 하지만 일반적인 장면 그래프 생성 작업에서는 영상이외에 별도로 이와 같은 설명글을 제공하는 경우는 매우 드물다. 따라서 본 실험을 통해, 장면 그래프 생성을 위한 제안 모델의 높은 성능을 확인할 수 있었다.

4. 결론

본 논문에서는 영상으로부터 장면 그래프를 효과적으로 생성할 수 있는 심층 신경망 모델을 제안하였다. 제안 모델은 시각 맥락 특징, 언어 맥락 특징 등 다양한 멀티모달 맥락 정보를 활용하며, 특히 언어 맥락 특징의 효과를 극대화하기 위해 별도의 biRNN 네트워크를 사용한다. 또한, 제안 모델에서는 관계를 맺는 두 물체 간의 상호 의존성이 그래프 노드 특징값들에 충분히 반영되도록, 그래프 신경망을 이용해 맥락 정보를 임베딩한다. Visual Genome 벤치마크 데이터 집합을 이용한 비교 실험들을 통해서, 기존 모델들에 비해 우수한 제안 모델의 성능을 확인할 수 있었다.

참고문헌

- [1] Y. Li, W. Ouyang, and B. Zhou, et. al., "Scene Graph Generation from Objects, Phrases and Region Captions," *Proc. of ICCV-17*, 2017.
- [2] J. Yang, J. Lu, and S. Lee, et al., "Graph R-CNN for Scene Graph Generation," *Proc. of ECCV*, 2018.
- [3] W. Liao, B. Rosenhahn, and L. Shuai, et al., "Natural Language Guided Visual Relationship Detection," *Proc. of IEEE*, 2019.
- [4] R. Krishna, Y. Zhu, and O. Groth, et al., "Visual Genome: Connecting Language and Vision Using Crowdsourced Dense Image Annotations," *Proc. of the IJCV*, 2017.

시각-언어 이동 에이전트를 위한 모방 학습과 강화 학습의 결합

오선택, 김인철
경기대학교 컴퓨터과학과
email:choice37@kyonggi.ac.kr, kic@kyonggi.ac.kr

Combining Imitation Learning and Reinforcement Learning for Visual-Language Navigation Agents

Suntaek Oh, Incheol Kim
Department of Computer Science, Kyonggi University

요 약

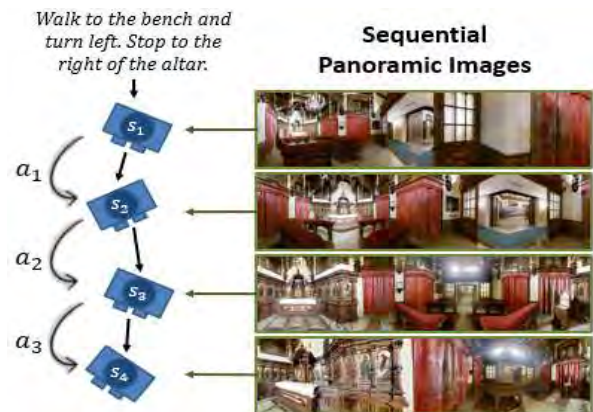
시각-언어 이동 문제는 시각 이해와 언어 이해 능력을 함께 요구하는 복합 지능 문제이다. 본 논문에서는 시각-언어 이동 에이전트를 위한 새로운 학습 모델을 제안한다. 이 모델은 데모 데이터에 기초한 모방 학습과 행동 보상에 기초한 강화 학습을 함께 결합한 복합 학습을 채택하고 있다. 따라서 이 모델은 데모 데이터에 편향될 수 있는 모방 학습의 문제와 상대적으로 낮은 데이터 효율성을 갖는 강화 학습의 문제를 상호 보완적으로 해소할 수 있다. 또한, 제안 모델은 서로 다른 두 학습 간에 발생 가능한 학습 불균형도 고려하여 손실 정규화를 포함하고 있다. 또, 제안 모델에서는 기존 연구들에서 사용되어온 목적지 기반 보상 함수의 문제점을 발견하고, 이를 해결하기 위해 설계된 새로운 최적 경로 기반 보상 함수를 이용한다. 본 논문에서는 Matterport3D 시뮬레이션 환경과 R2R 벤치마크 데이터 집합을 이용한 다양한 실험들을 통해, 제안 모델의 높은 성능을 입증하였다.

1. 서론

최근 에이전트의 복합 지능에 관한 관심이 높아지면서 VLN(Vision-and-Language Navigation) 문제[1]가 주목받고 있다. VLN이란 3차원 실내 공간에 놓인 한 에이전트가 실시간 입력 영상(input image)과 자연어 지시(natural language instruction)에 따라 스스로 이동 행동(navigational action)을 결정함으로써 미지의 목적지까지 도달해야 하는 작업이다. (그림 1)은 VLN 작업의 한 예를 보여준다. (그림 1)의 왼쪽은 에이전트에 주어진 자연어 지시와 이 지시에 따른 에이전트의 행동 시퀀스를 보여주며, 그림의 오른쪽은 에이전트의 위치에 따라 입력되는 순차적인 파노라마 영상(panoramic image)을 보여준다.

VLN 작업에서 중요한 문제 중 하나는 한정된 학습 데이터(seen data)를 이용하여 ‘비-학습 작업(unsseen task)’에서 얼마나 좋은 성능을 갖는 에이전트로 학습시키느냐 하는 학습의 일반화(generalization) 및 지식 전이(knowledge transfer) 문제이다. 이러한 VLN 에이전트의 일반화 능력을 향상시키고자 노력한 대표적인 연구들로는 [1-5]가 있다. [1]의 연구에서는 VLN 에이전트를 위한 모방 학습 방법을 제시하였으나, [2-3] 연구에서는 모방 학습과 강화 학습을 결합하는 방법을 제시하였다. 모방 학습은 에이전트의 학습을 가속화할 수 있지만 한정된 데모 데이터로 인해 편향(bias)이 발생한다. 이들은 강화 학습의 경험 데이터로부터 모방 학습의 편향을 줄이고 에이전트의 일반화 능력을 높이고자 하였다. 하지만 두 학습 방법으로부터 얻어낸 손실(loss)들은 규모가 다르므로 학습의 불균형 문제가 발생할 수 있다. [2-3]에서 제시한 모델들은 학습의 불균형 문제를 고려하지 않고 있다.

한편, [3-5]의 연구들에서는 VLN 에이전트의 일반화 능력 향상을 위해 학습 데이터 증강(data argumentation) 기법을 제시하였다. [3]의 연구에서는 영상에서 특정 물체들에 대한 마스크(mask)를 찾고 이 마스크만큼의 영역을 영상에서 소실(drop out)시킴으로써 새로운 영상정보를 만들었다. 또한, [3]의 연구에서는 새로운 영상정보를 토대로 정답 경로를 만들고 이에 대한 지시를 자동으로 생성하는

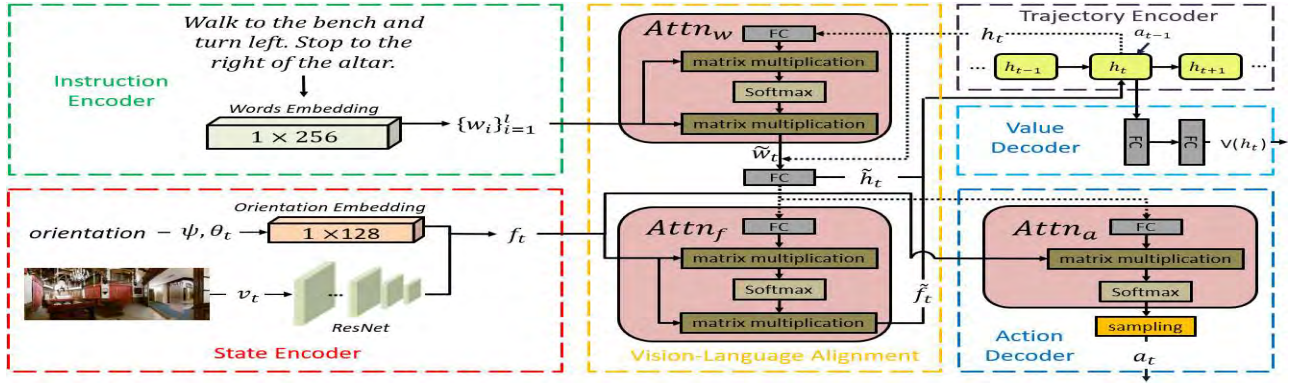


(그림 1) 시각-언어 이동(VLN) 문제의 한 예
발화자(speaker) 모델[4]을 채용하였다. [5]의 연구에서는 정답 경로들 중 시작 위치와 목적 위치가 일치하는 정답 경로들을 연결하여 기존의 학습 데이터 집합 R2R보다 길이가 더 긴 학습 데이터 집합 R4R을 만들었다. 이 연구들은 학습 데이터에서 지시와 영상정보를 증강하고자 하였다. 하지만 이 연구들은 하나의 지시에 대해 여러 정답 경로가 존재할 수 있음에도 불구하고 하나의 정답 경로만 제시한다는 문제점이 있다.

한편, [2-3] 연구에서 강화 학습을 위해 사용한 밀집 보상 함수(dense reward function)는 정답 경로와는 상관없이 현재 상태가 이전 상태보다 목적지에 가까우면 무조건 보상을 받기 때문에, 에이전트가 목표에 도달했어도 이동한 경로가 지시를 잘 따랐는지 판별할 수 없다는 결함이 있다.

이러한 문제점들을 해결하기 위해 본 논문에서는 VLN 에이전트를 위한 새로운 학습 모델을 제시한다. 이 모델은 모방 학습과 강화 학습을 결합한 새로운 학습 방법인 CIR(Combining Imitation learning and Reinforcement learning)과 새로운 보상 함수인 RBA(Region Based Alignment)를 이용한다. CIR은 낮은 데이터 효율성을 갖는 강화 학습의 문제와 데모 데이터에 편향될 수 있는 모

* 이 연구는 2020년도 산업통상자원부 및 산업기술평가관리원(KEIT) 연구비 지원에 의한 연구임('10077538')



(그림 2) VLN 에이전트를 위한 제안 모델의 구조

방 학습의 문제를 상호 보완적으로 해소할 수 있다. 또한, CIR은 두 학습 방법의 손실 규모 차이로 인해 발생하는 학습 불균형 문제를 고려하여 손실 정규화를 포함한다. 한편, 목적지 기반 보상 함수의 문제점을 해결하기 위해 새로 설계된 RBA 보상 함수는 일정한 범위 내에서 에이전트가 최적 경로를 유지하고 있는지를 판별하는 경로 기반 보상 함수이다. 이 보상 함수는 VLN 에이전트의 작업 성공률뿐만 아니라, 목적지까지 이동 경로의 품질을 향상시키는 데도 큰 도움을 줄 수 있다. 본 논문에서는 Matterport3D 시뮬레이션 환경과 R2R 벤치마크 데이터 집합을 이용한 다양한 실험들을 통해, 제안 모델의 성능을 분석한다.

2 시각과 언어기반의 이동

2.1 문제 정의

VLN 문제는 3차원 실내 공간에서 실시간 영상을 입력 받는 에이전트가 자연어 지시(instruction)를 따라 목적지로 이동하는 작업이다. 지시 $I = \{u_0, u_1, \dots, u_l\}$ 는 l 개의 단어 u_i 들로 이뤄진 문장들로 구성된다. 에이전트는 지시를 따라 n 개의 상태 시퀀스로 이뤄진 정답 경로 $R = \langle s_1, s_2, \dots, s_{n-1}, s_n \rangle$ 를 찾아야 한다.

본 논문에서는 마르코프 결정 프로세스(Markov Decision Process, MDP)를 기초로 VLN 문제를 강화 학습 문제로 정의한다. 먼저, 상태 $s \in S$ 는 (v, ψ, θ) 로 구성된다. 여기서 v 는 에이전트의 위치에서 포착 가능한 360° 파노라마 영상이다. 파노라마 영상은 가로로 30°씩 12개, 위아래 30°씩 3개로 총 36개의 부분 영상으로 이루어져 있다. ψ 와 θ 는 각각 수평(elevation), 수직(heading)으로 이루어진 방향(orientation) 정보를 의미한다. 다음으로 행동 $a \in A$ 는 (m, s) 로 구성된다. 여기서 m 은 이동, s 는 정지를 의미한다. 이동은 최대 36개의 방향으로 이동할 수 있고 위치마다 이동 가능한 방향(navigable directions)이 한정되어 있다. 에이전트는 지시를 잘 따르면서 목적지에 빠르게 도착할수록 높은 보상을 받는다.

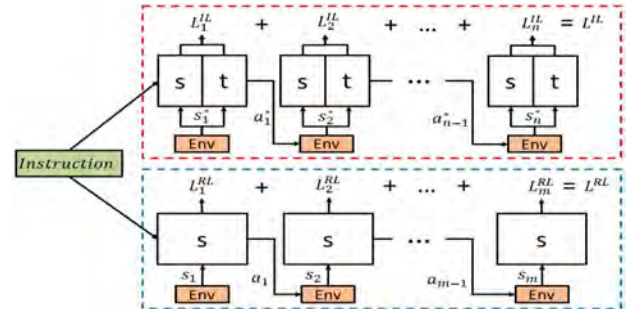
2.2 VLN 에이전트 모델

본 논문에서는 기초 모델(baseline)[3]에서 제안한 인코더-디코더(encoder-decoder) 기반의 VLN 에이전트 모델을 채용한다. 이 VLN 에이전트 모델의 구조도는 (그림 2)와 같다. VLN 에이전트는 환경으로부터 현재 위치에서 관측된 파노라마 영상 v_t 와 이동 가능한 방향 정보 ψ_t, θ_t 를 입력받고, 환경 외적으로는 지시(instruction)를 입력받는다. 파노라마 영상과 이동 가능한 방향 정보는 상태 인코더(state encoder)에 의해 하나의 연결된(concatenated) 특징 벡터 f_t 로 변환된다. 특징 벡터 f_t 의 계산 식은 아래와 같다.

$$f_t = [ResNet(v_t), (\cos\theta_t, \sin\theta_t, \cos\psi_t, \sin\psi_t)] \quad (식 1)$$

지시는 지시 인코딩(instruction encoding)에 의해 단어 임베딩(word embedding) 벡터 $\{w_i\}_{i=1}^l$ 로 변환된다. 여기

서 l 은 단어의 수를 의미한다. f_t 와 $\{w_i\}_{i=1}^l$ 는 시각-언어 정렬(vision-language alignment, VLA)에 의해 주의 집중 벡터 \tilde{f}_t 와 \tilde{h}_t 로 계산된다. \tilde{h}_t 는 주의 집중 벡터 \tilde{w}_t 와 h_t 를 연결(concatenation)한 값이다. h_t 는 에이전트가 매 시간 단계(time step)마다 지시의 어느 부분을 따르고 있는지를 표현하는 벡터이다. h_t 는 LSTM(Long Short-Term Memory) 기반의 경로 인코딩(trajecory encoding)을 통해 생성된다. 가치 디코딩(value decoding)은 h_t 로부터 상태 가치 $V(h_t)$ 를 계산한다. 행위 디코딩(action decoding)은 f_t 와 \tilde{h}_t 로부터 행동 a_t 를 계산한다.



(그림 3) 모방 학습과 강화 학습 에피소드

본 논문에서는 (그림 3)과 같이 한 번의 학습 반복을 위해 모방 학습 손실을 계산하는 에피소드와 강화 학습 손실을 계산하는 에피소드를 동시에 진행한다. 모방 학습에서는 전문가 에이전트(teacher, t)의 정책에 따라 에피소드를 진행하고 강화 학습에서는 학습자 에이전트(student, s)의 정책에 따라 에피소드를 진행한다. 에피소드가 진행된 후에는 두 에피소드를 통해 얻어낸 손실로부터 학습자 에이전트를 갱신한다. 이에 대한 자세한 내용은 2.3절에서 소개한다.

2.3 학습 방법

본 논문에서는 낮은 데이터 효율성을 갖는 강화 학습의 문제와 데모 데이터에 편향될 수 있는 모방 학습의 문제를 상호 보완하기 위해 두 학습 방법을 결합한 학습 모델 CIR(Combining Imitation learning and Reinforcement learning)을 제안한다. 제안 방법 CIR의 학습 과정을 나타내는 의사 코드(pseudo code)는 <표 1>과 같다. <표 1>에서 1번 줄은 정책 매개변수 θ_p 를 무작위로 초기화한다. 다음으로 2-8번 줄은 모방 학습과 강화 학습을 동시에 진행하는 학습 반복(iterations) 과정을 나타낸다. 3-5번 줄은 모방 학습 손실 L^M 을 계산한다. L^M 은 (식 2)와 같이 매 시간 단계마다 교차 엔트로피 손실(cross entropy loss)을 계산하고 이를 합하여 얻어낸다. L^M 은 정책 네트워크 π_{θ_p} 가 최적 행동 a_t^* 를 결정할 확률을 높이도록 학습을 유도한다.

<표 1> CIR 학습 알고리즘

Algorithm 1 Learning with CIR

```

1 initialize  $\theta_p$  randomly
2 for i in range(MAX_ITER):
3   for t in range(n): #teacher_forcing
4      $L^L \leftarrow \log \pi_{\theta_p}(h_t, a_t^*)$ 
5      $s_{t+1} = \text{perform}(s_t, a_t^*)$ 
6   for t in range(m): #student_forcing
7      $L^{RL} \leftarrow (G_t - V(h_t)) \log \pi_{\theta_p}(h_t, a_t) + \eta H(\pi_{\theta_p}(h_t, a_t))$ 
8      $s_{t+1} = \text{perform}(s_t, a_t)$ 
9    $L^{MX} = \lambda_L L^L + L^{RL}$ 
10   $\theta_p = \theta_p + \gamma \nabla L^{MX}$ 

```

$$L^L = -\sum_{t=1}^N \log \pi_{\theta_p}(h_t, a_t^*) \quad (\text{식 } 2)$$

6-8번 줄은 강화 학습 손실 L^{RL} 을 계산한다. L^{RL} 은 (식 3)과 같이 A2C(advantage actor-critic) 알고리즘을 기반으로 강화 학습 손실 L^{RL} 을 계산한다. (식 3)에서 $G_t - V(h_t)$ 는 우세 함수(advantage function)이다. $\eta H(\pi_{\theta_p}(h_t, a_t))$ 는 다양한 행동을 결정할 수 있도록 장려하는 엔트로피 함수이다.

$$L^{RL} = -\sum_{t=1}^M ((G_t - V(h_t)) \log \pi_{\theta_p}(h_t, a_t) + \eta H(\pi_{\theta_p}(h_t, a_t))) \quad (\text{식 } 3)$$

9번 줄은 L^L 과 L^{RL} 을 더하여 혼합 손실 L^{MX} 를 계산한다. 한편, L^{RL} 보다 L^L 의 값이 훨씬 크기 때문에 학습의 불균형이 발생한다. 이를 위해 CIR은 λ_L 를 통해서 L^L 을 정규화를 한다. 마지막 10번 줄은 L^{MX} 를 토대로 θ_p 를 갱신한다.

제안 방법 CIR은 낮은 데이터 효율성을 갖는 강화 학습과 데모 데이터에 편향될 수 있는 모방 학습의 문제를 상호 보완할 수 있다. 또한, CIR은 L^L 정규화를 통해 두 학습 방법의 불균형 문제를 해결하였다.

2.4 보상 함수

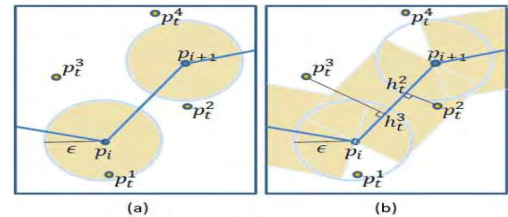
기존 연구들[2-3]에서는 매시간 단계마다 이동한 에이전트의 위치가 목적 위치에 가까워지면 양의 보상(+1)을 받고 그렇지 않으면 음의 보상(-1)을 받는다. 그리고 에이전트가 생성한 경로의 마지막 위치에서 목적 위치와의 거리가 3m 이내이면 목적 위치에 도달했다는 의미로 양의 보상(+2)을 받고 그렇지 않으면 음의 보상(-2)을 받도록 하였다. 이 보상 함수는 매시간 에이전트의 위치와 목적 위치와의 거리만을 고려하기 때문에 에이전트가 목적 위치에 도달하도록 학습을 유도할 수 있지만, 지시를 잘 따라 최적 경로를 지나도록 유도할 수 없는 문제가 있다. 이러한 문제를 해결하고자 본 논문에서는 새로운 보상 함수 RBA(Region Based Alignment)를 제안한다. 제안 보상 함수 RBA는 정답 경로를 기준으로 특정 거리 ϵm 내에서 목적 위치에 가까워지면 양의 보상(+1)을 받고 그렇지 않으면 음의 보상(-1)을 부여한다. 이를 수식으로 표현하면 아래와 같다.

$$r(p_t) = \begin{cases} 2 & \text{if } p_{t-1} \equiv p_t \text{ and } D(p_t) \leq 3 \\ -2 & \text{if } p_{t-1} \equiv p_t \text{ and } D(p_t) > 3 \\ 1 & \text{if } f(p_t) \text{ and } g(p_t) \\ -1 & \text{otherwise} \end{cases} \quad (\text{식 } 4)$$

(식 4)에서 첫 번째 조건식과 두 번째 조건식은 에이전트가 정지 행동을 수행하여 위치 변화가 없을 때 다익스트라 알고리즘(Dijkstra algorithm)을 이용하여 목적 위치와의 거리가 3m 이내인지 판단하는 식이다. 세 번째 조건식에서 $f(p_t)$ 는 현재 위치 p_t 가 정답 경로에서 특정 거리 ϵm 이내에 있으면 참(true)을, 그렇지 않으면 거짓(false)을 반환하는 함수로서 아래 (식 5)와 같다.

$$f(p_t) = \begin{cases} \text{true} & \text{if } \exists p_i \in P \Rightarrow \overline{p_i p_t} \leq \epsilon \text{ or } \\ & \exists h_i \in \overline{p_i p_{i+1}} \Rightarrow \overline{p_i p_{i+1}} \perp \overline{h_i p_t}, \overline{h_i p_t} \leq \epsilon \\ \text{false} & \text{otherwise} \end{cases} \quad (\text{식 } 5)$$

(식 5)에서 P 는 정답 경로상의 모든 노드의 집합, p_i 는 정답 경로상의 i 번째 노드, p_t 는 에이전트의 위치, h_i 는 p_t 에서 선분 $\overline{p_i p_{i+1}}$ 에 내린 수선의 발을 의미한다. 따라서, $f(p_t)$ 는 p_t 와의 거리가 ϵm 이내인 p_i 또는 h_i 가 존재하면 참을 반환한다. 예를 들어 (그림 4)의 (a)에서 p_t^1 는 p_i 와의 거리가 ϵm 이내이기 때문에 참이다. 나머지 p_t^2, p_t^3, p_t^4 는 정답 경로의 모든 노드와의 거리가 ϵm 이내가 아니다. 하지만 (그림 4)의 (b)에서와 같이 p_t^2 에서 정답 경로상에 내린 수선의 발 h_t^2 가 존재하고 $\overline{p_t^2 h_t^2}$ 의 길이가 ϵm 이내이기 때문에 참이다. 한편, p_t^3 는 정답 경로상에 내린 수선 발 h_t^3 이 존재하지만 $\overline{p_t^3 h_t^3}$ 의 길이가 ϵm 보다 크기 때문에 결국 거짓이고 p_t^4 는 정답 경로상에 내릴 수 있는 수선의 발이 존재하지 않기 때문에 결국 거짓이다.

(그림 4) 함수 $f(p_t)$ 의 조건 만족 영역

(식 4)에서 $g(p_t)$ 는 기존 연구[2-3]에서 사용하는 보상 함수이다. $g(p_t)$ 는 아래 (식 6)과 같이 에이전트의 이동 위치가 이전 위치보다 목적지에 더 가까워지면 참, 그렇지 않으면 거짓을 반환한다.

$$g(p_t) = \begin{cases} \text{true} & \text{if } D(p_{t-1}) - D(p_t) > 0 \\ \text{false} & \text{otherwise} \end{cases} \quad (\text{식 } 6)$$

이러한 제안 보상 함수 RBA는 에이전트가 목적지와 가까워지도록 이동할 뿐만 아니라, 정답 경로를 벗어나지 않게 이동할 수 있도록 하는 장점이 있다. 또한, RBA는 하나의 지시에 하나의 정답 경로만 제시하는 기존 연구들[1-5]과는 달리, 하나의 지시에 여러 정답 경로를 제시해주는 정답 영역을 사용한다. 따라서 정답 경로를 증강시켜 에이전트의 일반화 성능을 높여주는 부수 효과가 있다. 이 효과는 [3-5]의 데이터 증강(data argumentation) 기법의 원리와 유사하다.

3. 구현 및 실험

3.1 데이터 집합과 모델 학습

본 논문에서는 R2R 데이터 집합을 이용하여 제안 모델의 성능을 분석하기 위한 실험을 수행한다. 이를 위해 제안 모델은 Python 3.7, Pytorch 1.2.0 라이브러리를 이용하여 구현하였다. 한편, 모델 학습과 실험에 사용된 R2R 데이터 집합은 Matterport3D[1] 가상 환경의 시작 위치에서 목적 위치로 가는 최단 경로와 이를 설명하는 세 가지의 자연어 지시들의 집합으로 구성되어 있다. R2R 데이터 집합에서 학습 데이터(seen training data)는 14,025개, 학습 검증 데이터(seen validation data)는 1,020개, 비-학습 검증 데이터(unseen validation data)는 2,349개, 비-학습 테스트 데이터(unseen test data)는 2,349개의 지시로 각각 구성된다. 입력 영상으로부터 시작 특징 추출을 위해서는 미리 학습된 ResNet-152 모델을 이용하였다. 모델 학습을 위해 엔트로피 함수의 반영 비율 η 는 0.01로, 모방 학습과 강화 학습의 손실을 정규화하기 위한 λ_L 는 0.05로, 학습률(learning rate) γ 는 0.0001로 각각 설정하였다.

3.2 성능 분석 실험

본 논문에서는 제안 모델에서 채택한 CIR 학습 방법과 RBA 보상 함수의 효과를 분석하고, 기존 모델들과의 비교를 통해 제안 모델의 우수성을 입증하기 위한 실험을 수행하였다. 실험에 사용된 성능 평가 척도는 SC(Success rate)와 SPL(Success rate weighted by Path Length)이

다. SC는 VLN 에이전트의 작업 성공률을 나타낸다. VLN 작업은 에이전트의 마지막 위치가 목적지와의 거리가 3m 이내일 때 성공으로 간주한다. 반면, SPL은 정답 경로 길이를 에이전트가 실제 이동한 경로 길이로 나눈 값이다. 따라서 VLN 에이전트가 실제 이동한 경로가 짧을수록 높은 SPL 점수를 받을 수 있다.

첫 번째 실험은 제안 모델에서 채택한 보상 함수의 효과를 분석하기 위한 비교 실험이다. 이 실험에서는 목적지까지의 거리 변화만을 고려한 보상 함수 DBA(Destination Based Alignment)[3], 에이전트가 진행해온 경로와 정답 경로와의 유사도 변화를 DTW(Dynamic Time Warping) 알고리즘으로 계산하는 보상 함수 SBA(Similarity Based Alignment)[6], 그리고 본 논문에서 제안한 보상 함수 RBA 등 3가지 보상 함수에 따른 VLN 작업 성능을 서로 비교하였다. RBA의 임계 거리 ϵ 는 1m로 설정하였다. 이 실험을 위해 매시간 단계마다 에이전트에게 즉각적인 보상이 부여되는 밀집 보상(dense reward) 방식과 순수 강화 학습만을 이용해 학습하였고 학습 반복 횟수는 8만 번으로 설정하였다.

<표 1> 보상 함수에 따른 성능 비교

Reward Function	Seen		Unseen	
	SC	SPL	SC	SPL
DBA[3]	0.273	0.041	0.225	0.031
SBA[6]	0.409	0.381	0.405	0.382
RBA	0.436	0.414	0.399	0.375

이 실험의 결과는 <표 1>과 같다. 본 논문에서 제안하는 RBA와 SBA가 각각 학습 데이터(seen)와 비-학습 데이터(unseen)에서 높은 성능을 보였고, DBA는 좋지 못한 성능을 보였다. DBA는 에이전트의 위치와 목적 위치와의 차이만을 고려하였기 때문에, 지시를 따르지 않는 잘못된 경로를 학습하게 되는 문제점이 있다. SBA와 RBA는 보상 함수의 설계는 다르지만, 정답 경로와 유사한 경로를 학습하려는 같은 목적을 갖는 보상 함수이다. 따라서 하이퍼 파라미터(hyper parameter)에 따른 약간의 차이가 있지만, 대부분 비슷한 성능을 내는 것을 확인할 수 있었다. 하지만, SBA는 에이전트가 지나온 이전 경로의 길이가 길수록 계산량이 커지는 문제가 존재한다. 반면, RBA는 비교적 적은 계산량으로도 에이전트가 최적 경로를 따라 목적지에 가까워지는 방향으로 이동할 수 있도록 한다는 장점이 있다.

두 번째 실험은 제안 모델에서 채택한 모방 학습과 강화 학습을 결합한 복합 학습(CIR)의 효과를 분석하기 위한 실험이다. 이 실험을 위해 순수 강화 학습(only RL), 순수 모방 학습(only IL), 복합 학습 방법(CIR)을 각각 채용했을 때의 VLN 작업 성능을 서로 비교하였다. 이 실험에서 보상 함수는 RBA를 이용하였으며, 하이퍼 파라미터 ϵ 는 1.5m로, 학습 반복 횟수는 20만 번으로 각각 설정하였다.

<표 2> 학습 방법에 따른 성능 비교

Learning Strategy	Seen		Unseen	
	SC	SPL	SC	SPL
only RL	0.420	0.388	0.385	0.338
only IL	0.549	0.527	0.433	0.406
CIR ($\lambda = 0.05$)	0.653	0.622	0.488	0.447

이 실험의 결과는 <표 2>와 같다. 본 논문에서 제안한 복합 학습(CIR)의 성능이 가장 높았으며, 다음은 순수 모방 학습(IL), 순수 강화 학습(RL) 순으로 높은 성능을 나타내었다. 순수 모방 학습은 양질의 데모 데이터를 활용함으로써, 데이터 효율성이 상대적으로 낮은 강화 학습에 비해 높은 성능을 보였다. 하지만 한정된 데모 데이터에 편향되어, 복합 학습 방법보다는 낮은 성능을 보인 것으로 추정된다. 반면, 본 논문에서 제안한 복합 학습 방법(CIR)은 강화 학습(RL)의 데이터 비효율성 문제와 모방 학습(IL)의 데모 데이터에 대한 편향성 문제를 어느 정도 해소함으로써, 이 실험에서 상대적으로 가장 높은 성능을 보인

것으로 판단한다.

마지막 실험은 기존의 VLN 모델들에 비해 본 논문에서 제안한 모델의 우수성을 입증하기 위한 실험이다. 이 실험에서는 발화자 모델을 이용해 새로운 지시를 생성한 Speaker-Follower[4], 발화자 모델을 이용해 에이전트가 경로를 잘 따랐는지 판별한 RCM[2], 학습 데이터 증강을 위한 환경 드롭아웃(dropout) 기능과 혼합 손실 함수(mixed loss function)를 채용한 Env-Dropout[3], 새로운 보상 함수와 학습 방법을 도입한 제안 모델(CIR)의 VLN 작업 성능을 서로 비교하였다.

<표 3> 기존 모델들과의 성능 비교

Model	Seen		Unseen	
	SC	SPL	SC	SPL
Speaker-Follower[4]	0.52	0.43	0.36	0.29
RCM(no SIL)[2]	0.55	0.48	0.41	0.33
Env-Dropout(base)[3]	0.61	0.57	0.47	0.43
CIR ($\lambda = 0.05$)	0.65	0.62	0.49	0.45

이 실험의 결과는 <표 3>과 같다. 비교 모델들 중에서 본 논문의 제안 모델 CIR이 모든 척도에서 가장 높은 성능을 보였다. 특히 제안 모델 CIR은 미-경험 환경(unseen env)에 비해 이미 경험한 환경(seen env)에서 작업 성능의 향상이 더욱 뚜렷했다. 이것은 기존의 VLN 모델들에 비해 제안 모델의 우수성을 확인시켜주는 실험 결과로 볼 수 있다.

4. 결 론

본 논문에서는 시각-언어 이동 에이전트를 위한 새로운 학습 모델을 제안하였다. 이 모델은 모방 학습과 강화 학습을 함께 결합한 복합 학습 CIR을 채택하고 있다. 또한, 제안 모델은 기존의 목적지 기반 보상 함수의 결함을 개선하기 위한 새로운 경로 기반 보상 함수 RBA를 포함하고 있다. 본 논문에서는 R2R 데이터 집합과 Matterport3D 시뮬레이션 환경을 이용한 다양한 실험을 통해, 제안 모델의 우수한 성능을 확인할 수 있었다. 향후에는 기존의 Matterport3D 환경과 R2R 데이터를 이용하여 새로운 경로와 자연어 지시를 자동 생성하는 데이터 증강 기법을 연구할 계획이다.

참고 문헌

- [1] P. Anderson, Q. Wu, and D. Teney, et al, "Vision-and-Language Navigation: Interpreting Visually-Grounded Navigation Instructions in Real Environments," *Proc. of CVPR-2018*, pp. 3674-3683, 2018.
- [2] X. Wang, Q. Huang, A. Celikyilmaz, "Reinforced Cross-Modal Matching and Self-Supervised Imitation Learning for Vision-Language Navigation," *Proc. of CVPR-2019*, pp. 6629-6638, 2019.
- [3] H. Tan, L. Yu, and M. Bansal, "Learning to Navigate Unseen Environments: Back Translation with Environmental Dropout," *Proc. of NAACL-2019*, pp. 2610-2621, 2019.
- [4] D. Fried, V. Cirik, and A. Rohrbach, et al, "Speaker-Follower Models for Vision-and-Language Navigation," *Proc. of NeurIPS-2018*, pp. 3314-3325, 2018.
- [5] V. Jain, G. Magalhaes, A. Ku, "Stay on the Path: Instruction Fidelity in Vision-and-Language Navigation," *Proc. of ACL-2019*, pp. 1862-1872, 2019.
- [6] G. Ilharco, V. Jain, and A. Ku, et al, "General Evaluation for Instruction Conditioned Navigation using Dynamic Time Warping," *Proc. of NeurIPS-2019*, 2019.

쌍 선형 그래프 신경망을 이용한 지식 그래프 기반 질문 응답

이상의, 김인철

경기대학교 컴퓨터과학과

rmrlrmrl124@kyonggi.ac.kr, kic@kyonggi.ac.kr

Question Answering over Knowledge Graphs Using Bilinear Graph Neural Network

Sangui Lee, Incheol Kim

Department of Computer Science, Kyonggi University

요 약

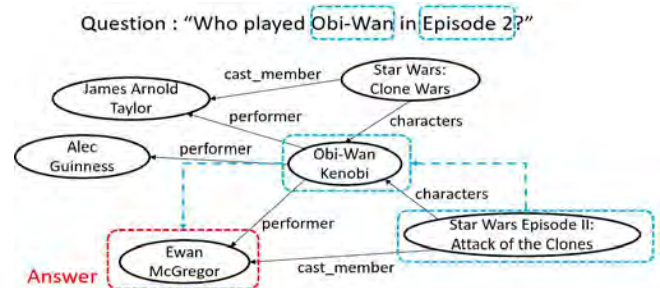
지식 그래프 기반의 질문 응답 문제는 자연어 질문에 대한 이해뿐만 아니라, 기반이 되는 지식 그래프상에서 올바른 답변을 찾기 위한 효과적인 추론 능력을 요구한다. 본 논문에서는 다중 홉 추론을 요구하는 복잡한 자연어 질문에 대해 연관 지식 그래프 위에서 답변 추론을 효과적으로 수행할 수 있는 심층 신경망 모델을 제안한다. 제안 모델에서는 지식 그래프상의 추론 과정에서 추론 경로를 명확히 하기 위한 노드의 양방향 특징 전파와 이웃 노드들 간의 맥락 정보까지 각 노드의 특징값에 반영할 수 있는, 표현력이 풍부한 쌍 선형 그래프 신경망(BGNN)을 이용한다. 본 논문에서는 오픈 도메인의 지식 베이스 Freebase와 자연어 질문 응답 데이터 집합 WebQuestionsSP를 이용한 실험들을 통해, 제안 모델의 효과와 우수성을 확인하였다.

1. 서론

대규모 지식 베이스를 토대로 인간을 대신해 자연어 질문에 스스로 답할 수 있는 지능형 에이전트는 실세계 다양한 분야에서 폭넓게 활용될 수 있다. 특히 최근 들어 심층 신경망(deep neural network)을 이용한 자연어 처리 기술들이 획기적으로 발전함에 따라, 지식 베이스 기반 질문 응답(Knowledge Base Question Answering, KBQA) 문제와 이를 해결하기 위한 다양한 모델들에 관한 관심도 함께 증가하고 있다. 일반적으로 비정형 문서 집합(corpus)에 비해, 지식 베이스(knowledge base)는 대부분 트리플(triplet)과 같은 구조화된 형태로 지식을 저장하고 있으므로 질문 응답(QA)에 활용하기가 상대적으로 용이하다. 하나의 지식 트리플은 주어 개체(subject entity), 관계 서술자(relational predicate), 목적어 개체(object entity)로 구성되는데, 이것은 두 개체 간의 관계를 나타내는 하나의 사실(fact)로 간주할 수 있다. 따라서 다수의 트리플들로 이루어진 지식 베이스는 개체 노드(node)들과 그들 간의 관계를 표현하는 간선(edge)들로 구성되는 하나의 큰 지식 그래프(knowledge graph)로 볼 수 있다. 이러한 지식 그래프를 토대로 자연어 질문에 대한 답변을 찾기 위해서는 지식 그래프 위에서 전개되는 효율적인 추론(reasoning) 혹은 탐색(search) 과정이 요구된다.

한편, 지식 그래프 기반 질문 응답 문제는 추론의 복잡도에 따라 단순 질문(simple question)과 복잡 질문(complex question)으로 나뉜다. 일반적으로 질문에 대한 답변을 위해 지식 그래프 위에서 단일 홉(single hop) 추론이 필요하나 아니면 다중 홉(multi-hop) 추론이 필요하나에 따라 단순 질문과 복잡 질문을 구분한다. 본 논문에서는 특히 다중 홉 추론을 요구하는 지식 그래프 기반 질문 응답 모델을 제안한다.

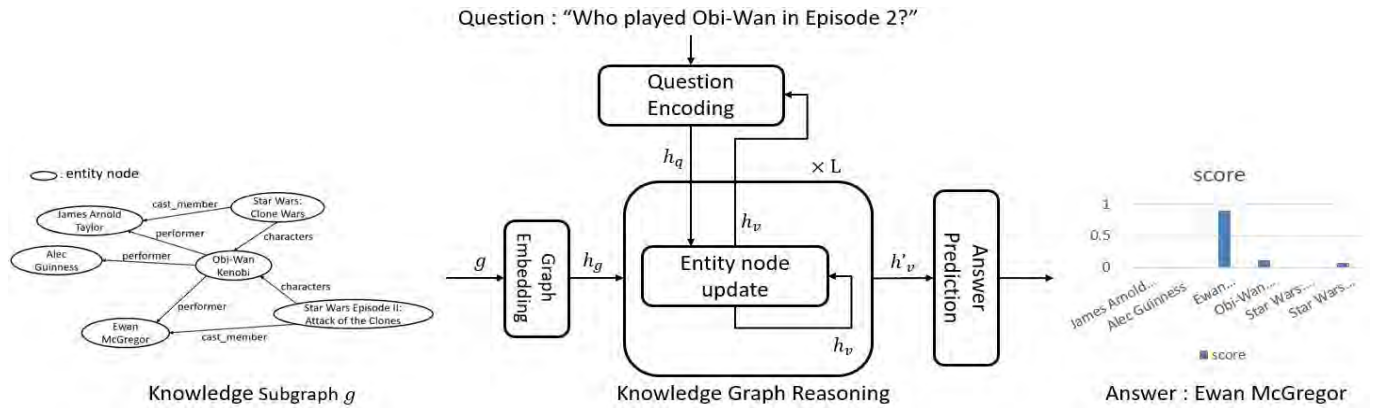
(그림 1)은 지식 그래프를 이용한 다중 홉 추론의 한 예를 보여준다. (그림 1)에서 개체는 타원형으로, 개체 사이의



(그림 1) 지식 그래프를 이용한 다중 홉 추론의 예

관계는 간선으로 표현되어 있다. (그림 1)의 상단에서처럼 자연어 질문이 주어지면 지식 베이스로부터 질문과 연관된 지식 그래프를 추출해야 한다. 지식 그래프를 추출할 때 질문에 언급된 개체를 중심으로 추출하며, 추출한 지식 그래프로부터 답을 추론할 수 있어야 한다. 다중 홉 추론을 요구하는 복잡 질문인 “Who played Obi-Wan in Episode 2?”에 대해 답변인 Ewan McGregor를 찾으려면 먼저 질문과 연관 있는 트리플 <Star Wars Episode II: Attack of the Clones, characters, Obi-Wan Kenobi>을 찾아야 한다. 이 트리플로부터 질문의 답변인, Obi-Wan Kenobi를 연기한 Ewan McGregor를 포함하는 트리플 <Obi-Wan Kenobi, performer, Ewan McGregor>을 찾을 수 있어야 한다.

지식 그래프를 이용한 다중 홉 추론에 관해 기존 연구 [1]에서는 (키(key), 값(value)) 쌍의 메모리 슬롯에 트리플들을 저장하고, 자연어 질문과 키(key)의 연관성에 따른 값(value)들의 가중치 합(weighted sum)을 이용해 메모리 슬롯을 반복적으로 참조하여 답변 개체를 예측하는 KVMN 모델을 제안하였다. 이때 키(key)는 트리플의 주어 개체와 관계 서술자로 이루어진 튜플(tuple)에 해당하고 값(value)은 목적어 개체에 해당한다. 한편, 기존 연구



(그림 2) 제안 모델의 전체 구조

[2]에서는 그래프 합성곱 신경망(Graph Convolutional Network, GCN)[3]과 페이지랭크(PageRank) 점수를 이용한 지식 그래프 추론을 수행하는 GraftNet 모델을 제안하였다. 그러나 이러한 기존 연구들은 KVMN 모델과 같이 지식 그래프 추론 과정에 그래프 이웃 노드들과의 맥락 정보(structural context)를 반영하려는 별도의 노력이 없거나, 그래프 합성곱 신경망(GCN)에 기초한 GraftNet 모델처럼 이웃 노드들의 특징 정보를 단순 선형 응집(Linear Aggregation, LA)해서 얻은 맥락 정보만을 활용하였다. 하지만 대규모 지식 그래프 위에서 다중 홉 추론을 요구하는 다양한 복잡 질문(complex question)들에 대한 올바른 답변을 찾아내려면, 각 노드와 이웃 노드 간의 맥락 정보뿐만 아니라 이웃 노드와 이웃 노드 간의 맥락 정보도 효과적으로 활용할 수 있는 그래프 신경망(Graph Neural Network) 기반의 지식 그래프 추론 모델이 요구된다.

이러한 기존 연구들의 한계점을 고려하여, 본 논문에서는 새로운 그래프 신경망 기반의 질문 응답 모델을 제안한다. 제안 모델에서는 질문에 대한 효과적인 지식 그래프 추론을 위해 그래프 노드들 간의 양방향 특징 정보 전파(bidirectional propagation) 기능을 포함하고 있을 뿐만 아니라, 두 이웃 노드들 간의 맥락 정보도 활용할 수 있는 쌍 선형 응집(Bilinear Aggregation, BA) 연산이 추가된 쌍 선형 그래프 신경망(Bilinear Graph Neural Network, BGNN)을 새롭게 채용하고 있다. 본 논문에서는 제안 모델의 성능 평가를 위해 WebQuestionsSP[4] 벤치마크 데이터 집합을 이용한 다양한 실험들을 수행하고, 그 결과를 소개한다.

2 다중 홉 오픈 도메인 질문 응답

2.1 문제 정의

본 논문에서는 지식 베이스로부터 추출된, 질문과 연관된 지식 그래프상에서 자연어 질문에 대한 답을 추론하는 문제를 다루고 있다.

지식 베이스는 $K = (V, E, R)$ 로 정의할 수 있다. 여기서 K 는 지식 베이스, V 는 개체들의 집합, E 는 트리플 $t = (s, r, o)$ ($s, o \in V, r \in R$)들의 집합, R 은 개체들 사이의 관계 서술자들의 집합이다. Q 는 자연어 질문들의 집합, 질문은 단어들의 집합으로 정의할 수 있다. $q \in Q$ 에 대해, K 에서의 q 와 연관된 지식 그래프 g 를 $g = (q, K)$ 로 정의할 수 있다.

질문 응답(QA) 작업은 g 에서 q 에 대한 답 $v \in V$ 찾기 로 정의할 수 있다. 다중 홉 추론은 v 를 찾기 위해 g 에서 q 에 언급된 개체 s 로부터 v 까지의 경로 $d = (t_1, t_2, \dots, t_{|d|})$ 찾기로 정의할 수 있다. d 를 구성하는 t_{n-1} 의 o 는 t_n 의 s

와 같은 개체이다.

2.2 제안 모델

(그림 2)는 본 논문에서 제안하는 모델의 전체 구조도를 나타낸다. 입력으로 질문과 지식 그래프를 갖고, 출력으로 질문에 대한 답변인 개체를 갖는다. 여기서 지식 그래프는 [2]의 전처리(preprocessing)를 이용하여 지식 베이스인 FreeBase로부터 추출한, 질문과 연관된 지식 그래프를 이용한다. 제안하는 모델은 질문 인코딩(Question Encoding), 지식 그래프 추론(Knowledge Graph Reasoning), 답변 예측(Answer Prediction)으로 이루어져 있다.

질문 인코딩은 순환 신경망(Recurrent Neural Network)의 한 종류인 LSTM(Long Short-Term Memory)으로 자연어 질문을 인코딩하여 특징을 추출한다. 추출된 특징은 지식 그래프 추론에서 초기에 사용된 후 매 레이어(layer)마다 질문에 언급된 개체들의 노드 특징들 간의 맥락 정보로 다시 인코딩된다.

지식 그래프 추론은 지식 그래프상에서 질문에 대한 답변을 찾는 다중 홉 추론을 수행한다. 지식 그래프가 입력으로 들어오면, 각 노드에 대해 쌍 선형 그래프 신경망을 이용하여 이웃 노드들 간의 맥락 정보를 얻는다. 이렇게 얻은 맥락 정보와 질문 인코딩에서 얻은 질문의 특징을 활용하여 노드의 특징을 갱신하는 개체 노드 갱신(Entity node update)을 수행한다.

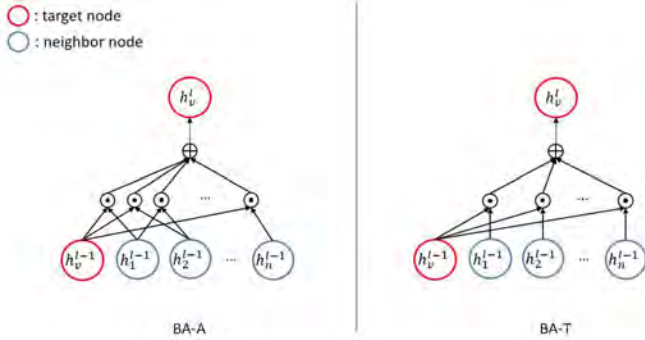
마지막으로 답변 예측은 지식 그래프 추론을 거쳐 나온 개체 노드들에 대해 시그모이드(sigmoid) 함수를 적용한다. 그 결과로 가장 높은 점수를 받은 개체 노드가 질문에 대한 답변으로 선택된다.

2.3 지식 그래프 추론

지식 그래프 추론에 앞서 신경망을 학습하기 위해 질문, 개체와 관계 서술자를 임베딩한다. 질문과 관계 서술자는 GloVe 임베딩 값을 이용한다. 개체 노드의 초기 특징값은 GloVe 임베딩 값과 지식 그래프를 미리 학습한 임베딩 값을 이용한다.

지식 그래프 추론 과정에서 다중 홉 추론을 수행하기 위해 쌍 선형 그래프 신경망의 구조를 채용한다. 즉, 기존에 선형 응집만 수행하던 연구들과 다르게 본 논문에서는 쌍 선형 응집(BA)을 추가하여 같이 사용한다. 갱신되는 노드를 목표 노드(target node)라고 할 때, 쌍 선형 응집을 사용하면 목표 노드와 이웃 노드 간의 맥락 정보뿐만 아니라 목표 노드의 이웃 노드들 간의 맥락 정보도 활용할 수 있다. 쌍 선형 응집으로 얻은 맥락 정보는 노드들

간의 요소별 곱(element-wise product)으로 인해 서로 유사한 특징 정보가 강조된 정보를 갖는다. 선형 응집과 쌍 선형 응집을 같이 사용함으로써 노드에 대한 다양한 맥락 정보를 토대로 효과적인 다중 홉 추론을 기대할 수 있다.



(그림 3) BA-A와 BA-T의 구조

쌍 선형 응집은 계산 방식에 따라 BA-A와 BA-T로 나눌 수 있고, 그에 따라 쌍 선형 그래프 신경망의 형태가 BA-A를 사용한 BGNN-A와 BA-T를 사용한 BGNN-T로 나눌 수 있다. (그림 3)은 BA-A와 BA-T를 나타낸 그림이다.

BA-A는 목표 노드와 이웃 노드, 이웃 노드와 이웃 노드끼리 요소별 곱을 수행하여 맥락 정보를 구하는 방식으로 (식 1)과 같다.

$$BA-A^l(v) = FFN\left(\frac{1}{2} \sum_{v'} \sum_{v''} (h_v^{(l-1)} \odot h_{v'}^{(l-1)}) + \sum_{v'} (h_v^{(l-1)} \odot h_{v''}^{(l-1)})\right) \quad (v', v'' \in N(v), v' \neq v'') \quad (식 1)$$

$N(v)$ 은 목표 노드의 이웃 노드들의 집합을 뜻한다. (식 1)에서 이웃 노드끼리 요소별 곱을 수행하면 같은 계산을 2번 하게 되므로 2로 나눈다.

BA-T는 목표 노드와 이웃 노드만 요소별 곱을 수행하여 맥락 정보를 구하는 방식으로 (식 2)와 같다.

$$BA-T^l(v) = FFN\left(\sum_{v'} (h_v^{(l-1)} \odot h_{v'}^{(l-1)})\right) \quad (v' \in N(v)) \quad (식 2)$$

본 논문에서는 목표 노드와 이웃 노드 간의 맥락 정보를 활용하는 BA-T를 이용한다. 3.2절 성능 평가 실험에서 BA-A를 사용한 모델과 BA-T를 사용한 모델의 다중 홉 추론 능력을 비교한다.

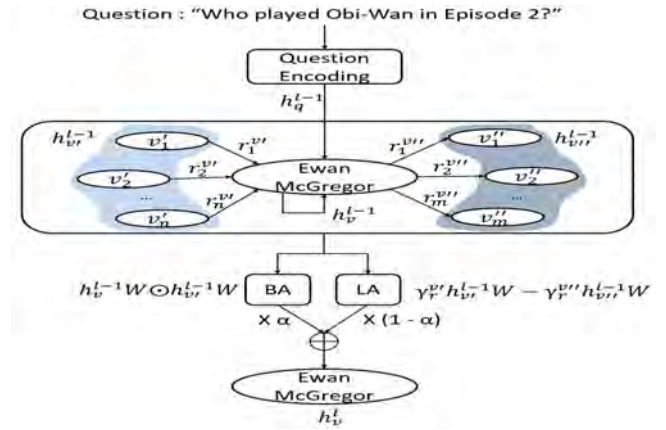
개체 노드 갱신은 (그림 4)와 같은 구조를 갖는다. 이는 (식 3)과 같이 나타낼 수 있다.

$$h_v^l = (1 - \alpha) * LA^l(v) + \alpha * BA^l(v) \quad (식 3)$$

(식 3)에서 α 는 하이퍼파라미터에 해당한다. α 의 값에 따라 선형 응집(LA)과 쌍 선형 응집(BA)의 적용 비율이 달라진다. LA에 대한 계산은 (식 4)에서처럼 차례대로 목표 노드의 특징 $h_v^{(l-1)}$, 자연어 질문의 특징 $h_q^{(l-1)}$, 선형 응집에 의한 이웃 노드들의 맥락 정보 $h_N^{(l-1)}$ 을 이용한다. (식 4)의 \parallel 기호는 연결(concatenation)을 뜻한다.

$$LA^l(v) = FFN([h_v^{(l-1)} \parallel h_q^{(l-1)} \parallel h_N^{(l-1)}]) \quad (식 4)$$

선형 응집에 의한 이웃 노드들의 맥락 정보 $h_N^{(l-1)}$ 을 계산할 때는 목표 노드에 연결된 간선의 방향을 고려한다. 다중 홉 추론에서 목표 노드로 들어오는 간선과 연결된 이웃 노드들의 특징들은 목표 노드에 대한 추론 경로에 해당하는 정보로 볼 수 있다. 반대로, 목표 노드로부터 나가는 간선과 연결된 이웃 노드들의 특징들은 목표 노드에 대한 추론 경로에 해당하지 않는 정보로 볼 수 있다. 따라



(그림 4) 개체 노드의 갱신

서, (식 5)와 같이 선형 응집에 의한 이웃 노드들의 맥락 정보 $h_N^{(l-1)}$ 을 계산할 때 목표 노드로 들어오는 간선과 연결된 이웃 노드들의 특징들은 더하고 목표 노드로부터 나가는 간선과 연결된 이웃 노드들의 특징들은 빼도록 계산한다. 또한, 목표 노드가 이웃 노드들과 맺는 관계와 질문의 연관성에 따라 다른 주의집중(attention)을 주면서 가중치 합을 계산한다. 이렇게 함으로써 질문과 연관성이 높은 관계를 맺는 이웃 노드의 특징에 더 큰 가중치를 줄 수 있다.

$$h_N^{(l-1)} = FFN\left(\sum_r \sum_{v' \in N_r(v)} \gamma_r^{v'} FFN(x_r, h_{v'}^{(l-1)})\right) - FFN\left(\sum_r \sum_{v'' \in N_r(v)} \gamma_r^{v''} FFN(x_r, h_{v''}^{(l-1)})\right) \quad (식 5)$$

(식 5)에서 $r \in INR$ 에 대해, N_r 는 노드로 들어오는 간선과 연결된 이웃 노드들의 집합, N_r' 는 노드로부터 나가는 간선과 연결된 이웃 노드들의 집합을 뜻한다.

질문 응답을 수행하기 위해서 신경망을 학습할 때 질문의 정보를 이용해야 한다. 따라서, (그림 4)처럼 개체 노드의 특징 $h_v^{(l-1)}$ 을 갱신할 때 자연어 질문의 특징 $h_q^{(l-1)}$ 을 이용한다. 또한, 선형 응집에 의한 이웃 노드들의 맥락 정보 $h_N^{(l-1)}$ 을 계산할 때도 질문을 이용한 주의집중 γ_r^v 을 준다. 자연어 질문의 특징 $h_q^{(l-1)}$ 은 초기값으로 (식 6)처럼 LSTM의 직전 은닉 상태(hidden state)를 이용한다. 이후 그래프 신경망에서 각 레이어를 거칠 때마다 자연어 질문에 언급된 개체들의 노드들의 맥락 정보로 갱신한다. 자연어 질문과 지식 그래프상의 개체 노드는 서로 다른 멀티모달(multimodal)이므로 처음에만 자연어 질문의 특징을 LSTM으로 인코딩하고 이후에는 질문에 언급된 개체들의 노드 특징들을 이용한 것이다.

$$h_q^l = \begin{cases} LSTM(q) & l = 0 \\ FFN(\sum_{v \in V_q} h_v^l) & l > 0 \end{cases} \quad (식 6)$$

(식 6)의 $v \in V_q$ 는 질문에 언급된 개체의 노드를 뜻한다.

(식 5)에서 자연어 질문과 연관성이 높은 관계에 대해 더 큰 주의집중을 주기 위해 (식 7)과 같이 주의집중 γ_r^v 을 계산한다.

$$\gamma_r^v = softmax(x_r^T h_q^{(l-1)}) \quad (식 7)$$

x_r 은 관계 서술자의 임베딩 벡터다. v 가 이웃 노드들과 맺는 관계에 대해 소프트맥스(softmax) 정규화가 행해진다.

BA에 대한 계산은 (식 8)에서처럼 쌍 선형 응집 BA-T로 구한, 목표 노드와 이웃 노드 간의 맥락 정보를 이용한다. 실험상 모든 이웃 노드에 대해 쌍 선형 응집을 하는 것보다 목표 노드로 들어오는 간선과 연결된 이웃 노드들에 대해서만 하는 것이 더 좋은 성능을 보였다. 따라서, 본

논문에서는 목표 노드로 들어오는 간선과 연결된 이웃 노드들에 대해서만 쌍 선형 응집을 수행한다.

$$BA^l(v) = FFN([h_v^{(l-1)} \| h_q^{(l-1)} \| FFN(\sum_{v'} (h_v^{(l-1)} \odot h_{v'}^{(l-1)}))] (v' \in \mathcal{N}_r(v)) \quad (\text{식 8})$$

답변을 추론할 때 모든 노드에 대해 답인지 아닌지 분류하는 이진 분류를 수행한다. 손실 함수로 바이너리 크로스 엔트로피 손실(binary cross entropy loss)을 사용한다.

3. 구현 및 실험

3.1 데이터 집합과 모델 학습

본 논문의 제안 모델은 Ubuntu 16.04 LTS에서 Python 딥러닝 라이브러리인 PyTorch를 이용하여 구현하였다. 모델의 학습 및 평가를 위한 질문-응답 데이터 집합으로는 WebQuestionsSP[4]를 사용하였다. WebQuestionsSP는 지식 베이스인 FreeBase를 토대로 생성한 오픈 도메인 질문-응답 데이터 집합이다. 이 데이터 집합은 총 4737개의 자연어 질문과 답변들 중 3098개는 훈련용(training set), 1639개는 검증용(validation set)으로 구성되어 있다. 특히 전체 질문의 약 70%는 단일 홉 추론을 요구하는 단순 질문들(single-hop simple questions), 약 30%는 2-홉 질문들(double-hop complex questions)이다.

모델 학습을 위해 쌍 선형 그래프 신경망(BGNN)의 레이어 수(number of layers)는 3, 반복 학습주기(epoch)는 100, 배치 크기(batch size)는 10, 학습률(learning rate)은 0.001로 설정하였다. 실험은 64GB의 메인 메모리와 Geforce RTX 2080 SUPER 1개를 포함한 컴퓨터 환경에서 수행되었다.

3.2 성능 평가 실험

본 논문에서는 제안하는 모델의 성능 평가 척도로 Hits@K와 F1 score을 채택하였다. Hits@K는 답변이라고 예측한 것들 중 가장 점수가 높은 K개를 선택했을 때 실제 답변이 포함되어 맞춘 비율을 나타낸 것이다.

첫 번째 실험은 제안하는 모델의 지식 그래프 추론에서 쌍 선형 응집의 효과를 보이는 실험이다. 선형 응집만 썼을 때(LA), 쌍 선형 응집만 썼을 때(BA-A와 BA-T) 그리고 둘 다 사용했을 때(BGNN-A와 BGNN-T) 나타난 성능을 비교하였다. <표 1>은 첫 번째 실험을 수행하여 측정한 표이다. 이 실험에서는 BGNN의 α 값을 BGNN-A에서는 0.1, BGNN-T에서는 0.3으로 설정하였다.

<표 1> 지식 그래프 추론 방식에 따른 성능 비교

method	Hits @1	Hits @5	Hits @10	Hits @20	F1 score
LA	66.9	79.7	83.3	86.0	58.2
BA-A	19.6	19.9	29.4	39.6	0.6
BA-T	44.7	68.9	76.5	82.2	35.4
BGNN-A	67.2	80.5	83.3	86.1	59.1
BGNN-T	68.4	80.9	83.9	86.0	61.0

<표 1>에서 보듯이 선형 응집(LA)과 쌍 선형 응집(BA)을 모두 사용하는 BGNN-T가 모든 척도에서 가장 우수한 성능을 보였다. 또한, 선형 응집(LA)과 쌍 선형 응집(BA)만 비교했을 때는, 선형 응집(LA)의 성능이 쌍 선형 응집(BA)보다 우수한 성능을 나타내었다. 또한, Hits@1을 기준으로 보면, 선형 응집과 쌍 선형 응집을 모

두 사용하는 BGNN-T와 BGNN-A가 선형 응집(LA)만 사용했을 때보다 각각 약 1.5%와 약 0.3% 더 높은 성능을 보여주었다. 또, BGNN-T를 사용했을 때가 BGNN-A를 사용했을 때보다 약 1.2% 더 높은 성능을 보였다. 이러한 실험 결과로 볼 때, WebQuestionsSP 질문-응답에서는 선형 응집(LA)이 쌍 선형 응집(BA)에 비해 상대적으로 성능 향상에 좀 더 도움을 주었으나, 제안 모델과 같이 선형 응집(LA)과 쌍 선형 응집(BA)을 함께 채용한 쌍 선형 그래프 신경망(BGNN)이 가장 높은 성능 개선 효과를 보인 것을 확인할 수 있었다.

두 번째 실험은 제안하는 모델과 기존 선형 연구들의 모델들의 성능을 비교하는 실험으로, <표 2>는 그에 대한 성능 비교표이다.

<표 2> 기존 모델들과의 성능 비교

model	Hits@1	F1 score
KVMN[1]	46.7	38.6
GraftNet[2]	66.7	62.4
Ours	68.4	61.0

<표 2>에서 보듯이 제안하는 모델의 성능이 Hits@1에서 68.4%로 GraftNet[2]보다 약 1.7% 더 높고, F1 score에서는 GraftNet[2]보다 약 1.4% 더 낮다. 비록 F1 score에서 GraftNet[2]보다 더 낮은 성능을 보였지만 Hits@1에서 더 높은 성능을 보여, 질문-응답에서 중요한 답변 추론 능력은 더 뛰어난 것을 확인할 수 있었다. 지식 그래프를 (키(key), 값(value)) 쌍의 메모리 슬롯으로 다루는 KVMN[1]은 Hits@1에서 약 46.7%, F1 score에서 약 38.6%를 기록하여 가장 낮은 성능을 보였다.

4. 결론

본 논문에서는 지식 그래프 위에서 다중 홉 추론을 요구하는 복잡한 자연어 질문에 효과적으로 답변을 추론할 수 있는 심층 신경망 모델을 제안하였다. 제안 모델에서는 지식 그래프 노드들 간의 양방향 특징 정보 전파 기능을 포함하고 있을 뿐만 아니라, 두 이웃 노드들 간의 맥락 정보도 활용할 수 있는 쌍 선형 그래프 신경망(BGNN)을 새롭게 채용하고 있다. WebQuestionsSP 벤치마크 데이터 집합을 이용한 다양한 실험들을 통해, 제안 모델의 효과와 우수성을 확인할 수 있었다.

감사의 글

“본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음” (IITP-2017-0-01642)

참고 문헌

- [1] A. Miller, A. Fisch, and J. Dodge, et al., “Key-Value Memory Networks for Directly Reading Documents,” *Proc. of EMNLP-16*, 2016.
- [2] H. Sun, B. Dhingra, and M. Zaheer, et al., “Open Domain Question Answering Using Early Fusion of Knowledge Bases and Text,” *Proc. of EMNLP-18*, 2018.
- [3] T. N. Kipf, and M. Welling, “Semi-Supervised Classification With Graph Convolutional Networks,” *Proc. of ICLR-17*, 2017.
- [4] W. Yih, M. Richardson, and C. Meek, et al., “The Value of Semantic Parse Labeling for Knowledge Base Question Answering,” *Proc. of ACL-16*, 2016.

신경망 기반 음원 분리 시스템의 학습 속도 향상을 위한 음역대 강조 기법

김민석*, 최우성*, 정순영*

*고려대학교 컴퓨터학과

rlaalstjr47@korea.ac.kr, ws_choi@korea.ac.kr, jsy@korea.ac.kr

Frequency Range Enhancement for Faster Convergence of Neural Music Source Separation Systems

Min-Seok Kim*, Woo-Sung Choi*, Soon-Young Jung*

*Dept. of Computer Science, Korea University

요 약

여러 악기가 섞여 있는 음원으로부터 원하는 악기 소리를 추출하는 음원 분리 기법 중 최근 신경망 기반 시스템이 활발히 연구되고 있다. 악기마다 고유의 음역대를 가진다는 사실에 감안하여, 연구진은 기존 음원 분리 신경망에 적은 수의 학습 파라미터를 추가하여 학습 속도를 대폭 향상시킬 수 있는 음역대 강조 기법을 제안한다.

1. 서론

음원 분리(Musical Source Separation)란, 여러 악기 소리로 이루어진 혼합 음원으로부터 원하는 악기 소리만으로 이루어진 단일 악기 음원을 추출하는 작업이다. 대중음악으로부터 목소리를 분리해내거나 반주만 남기는 작업이 대표적이다.

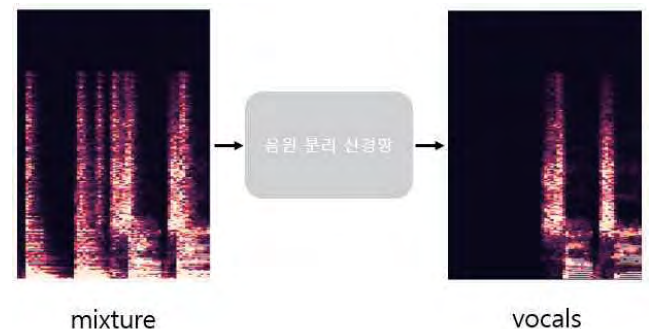
최근에 들어 딥러닝을 통한 음원 분리가 활발히 연구되고 있다 [1,2,3,4]. 이들은 대부분 시간에 따른 각 주파수 세기의 변화를 표현해주는 spectrogram을 학습 데이터로 사용한다. 이러한 기존 음원 분리 신경망의 더욱 효율적인 학습을 위해, spectrogram에 포함된 불필요한 주파수를 제거하고 음원 분리에 중요한 역할을 하는 주파수일수록 세기를 증가시켜주는 “음역대 강조” 기법을 본 논문에서 제안한다.

2. 제안 기법

2.1 기존 연구 및 기초 지식

신경망 기반 음원 분리 시스템은 supervised 방식이 대다수이며, 학습 데이터 instance는 혼합 음원과 그로부터 추출하고자 하는 단일 악기 음원의 쌍으로 이루어진다. 신경망은 임의의 혼합 음원을 받았을 때 그에 대응되는 단일 악기 음원을 예측하여 생성하도록 학습된다.

여기서 음원을 표현하는 방식에 따라 음원 분리



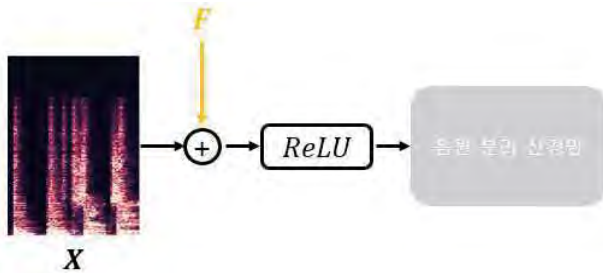
(그림 1) Spectrogram 방식의 신경망 기반 음원 분리.

시스템을 크게 두 부류로 나눌 수 있다. 1차원 배열의 형태를 가지는 음악 신호(waveform)를 그대로 학습에 사용하는 방법([3,4]), 그리고 푸리에 변환의 일종인 Short Time Fourier Transform(STFT)을 전처리 방식으로 이용하여 주파수 차원과 시간 차원으로 이루어진 2차원 배열(spectrogram)로 학습을 하는 방법([1,2])이 있다. 특히 spectrogram은 이미지와 유사한 특성을 가지기 때문에 이미지 처리 분야에서 개발된 CNN을 그대로 활용하여 준수한 성능을 얻을 수 있었다. 그림 1은 혼합 음원으로부터 목소리를 추출하는 spectrogram 방식의 신경망 기반 음원 분리의 예시이다.

2.2 음역대 강조 기법

제안 기법은 spectrogram 방식으로 개발된 기존 신경망의 학습을 개선시키는 방법이다. 혼합 음원의 spectrogram이 음원 분리 망을 통과하기 전에, 음원 분리에 필요한 주파수만 남기도록 하는 것이다. 어떤 주파수를 강조하고 어떤 주파수를 거를지는 추가 파라미터를 통해 학습되며, 이 학습은 기존 음원 분리 신경망의 학습과 동시에 end-to-end 방식으로 진행된다.

물론, 이러한 주파수 필터링은 사람의 수작업으로도 충분히 가능하다(downsampling, equalizer 활용 등). 하지만 음원 분리 신경망이 대상 악기의 음역대 안의 정보만 활용한다는 보장이 없기 때문에, 단순히 악기의 음역대가 아닌 음원 분리에 필요한 음역대를 학습할 수 있는 제안 기법이 이러한 전처리 방식과 차별화될 수 있다.

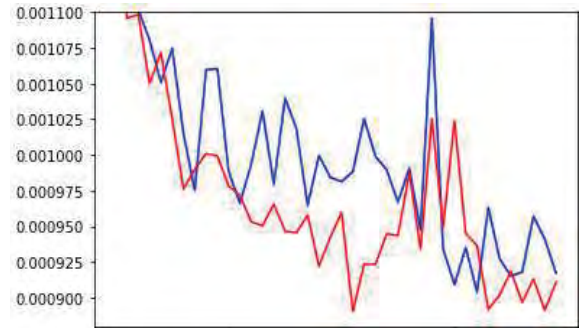


(그림 2) 음역대 강조 기법.

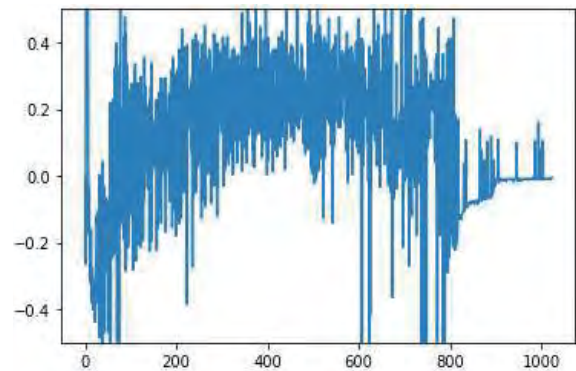
제안 기법은 그림 2처럼 표현될 수 있다. 신경망 input으로 들어온 mixture spectrogram $X \in R^{d_t \times d_f}$ 에 음역대 강조를 위한 추가 파라미터셋 $F \in R^{1 \times d_f}$ 을 broadcast하여 더해준 후, ReLU activation을 통과시켜 음수를 0으로 만들어준다. 단위 시간마다 같은 1차원 벡터 F 를 더해줌으로써 시간 축과는 무관한 주파수 축만의 특징을 학습하도록 하였다. 결국 F 는 절댓값이 큰 음수들을 활용하여 불필요한 주파수들을 제거하고, 중요한 주파수일수록 큰 양수를 더하여 강조하도록 학습된다(실험 평가 그림 4).

3. 실험 평가

목소리 음원 분리 실험을 진행하였으며, 이를 위해 MUSDB[5] 데이터셋을 사용하였다. 수렴 속도 비교 실험에 사용된 기존 음원 분리 기법은 MDenseNet[1]이며 frame 수(d_t)를 제외한 모든 STFT 파라미터는 [1]에 기재된 것과 동일하다($d_t = 64$, $d_f = 1025$). 학습 loss function 및 validation metric은 모두 MSE를 사용하였다.



(그림 3) Validation loss의 수렴 속도 비교.



(그림 4) F 벡터 가시화.

그림 3은 음역대 강조로 인한 수렴 속도 향상을 보여준다. 청색 그래프는 MDenseNet, 적색 그래프는 이에 음역대 강조 단계를 추가한 망의 validation loss를 나타낸다. 각각 대략 7 epoch 동안 학습이 진행됐으며, 제안 기법의 경우 기존 기법과 비교했을 때 약 2 epoch 일찍 수렴한 것을 알 수 있다. 최종 수렴 loss는 심지어 더 낮은 경우도 많았으나, 분리된 목소리 샘플을 비교하여 감상했을 때 유의미한 차이가 느껴질 만큼은 아니었다.

마지막으로, 그림 4의 뒤집어진 포물선 형태를 통해 F 의 파라미터셋이 지나치게 낮거나 높은 주파수를 걸러내는 방향으로 학습됐음을 알 수 있었다.

4. 결론

본 연구는 기존 음원 분리 신경망에 소수의 파라미터를 추가하는 것으로 학습 속도를 향상시킬 수 있음을 보여주었다. 또, 그림 4와 같은 가시화만으로도 사람이 학습 결과를 어느 정도 파악할 수 있다는 장점을 가진다. 더욱 일반화될 수 있는 기법인지를 확인하기 위해, 향후 다른 악기 혹은 다른 망을 대상으로도 실험을 진행할 예정이다.

5. 사사

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2019R1F1A1062719).

참고문헌

- [1] Naoya Takahashi, et al. "Multi-scale multi-band DenseNets for audio source separation", WAS-PAA, New York, 2017, pp. 261-265.
- [2] Woosung Choi, et al. "Investigating Deep Neural Transformations for Spectrogram-based Musical Source Separation." arXiv preprint arXiv:1912.02591, 2019.
- [3] Daniel Stoller, et al. "Wave-U-Net: A Multi-Scale Neural Network for End-to-End Audio Source Separation", ISMIR, Paris, 2018, pp. 334-340.
- [4] Alexandre Défossez, et al. "Music Source Separation in the Waveform Domain." arXiv preprint arXiv:1911.13254, 2019.
- [5] Zafar Rafii, et al. "MUSDB18 - a corpus for music separation", 2017.

다중 구면 영상으로부터 물체의 3D 위치 추정

홍철기, 박종승
인천대학교 컴퓨터공학과
mico9901@inu.ac.kr, jong@inu.ac.kr

Estimation of Object Position from Multiple Spherical Images

Cheol-gi Hong, Jong-Seung Park
Dept. of Computer Science and Engineering,
Incheon National University

요 약

핀홀 카메라는 그 특성상 전체 공간 중에서 일부분만을 촬영할 수 있으므로 전체 공간을 염두에 두는 3D 재구성에서는 구면 영상에 비해 많은 데이터를 확보해야 한다. 본 논문에서는 다수의 구면 영상에 촬영된 물체의 실제 3차원 위치를 추정하는 방법을 제안한다. 두 카메라의 배치 간격이 가까운 스테레오 비전과는 달리 제안하는 방법에서는 여러 대의 카메라를 넓은 간격으로 배치하여 장애물에 대한 폐색을 극복하도록 한다. 구면 카메라의 화각은 공간 전체를 담을 수 있기 때문에 촬영 간격과 카메라의 회전각이 크더라도 전 영역에 대한 일치 관계를 계산할 수 있다. 실험 결과 구면 영상에 나타난 물체의 실제 위치에 근접한 결과를 얻을 수 있었다.

1. 서론

전체 공간에 대해 부분적인 정보만을 가지는 일반 평면 영상과는 달리, 구면 파노라마 영상은 촬영 지점으로부터 모든 방향에 대한 정보를 갖는 특성을 가지기 때문에 적은 숫자의 카메라 배치나 영상의 개수만으로도 전체 공간 정보를 파악할 수 있다. 최소 2개의 구면 영상과 각 영상을 촬영한 카메라의 자세를 알고 있다면 트인 공간에서 특징점이나 물체의 위치를 알아낼 수 있고, 촬영 지점을 추가하면 더 복잡한 구조를 가진 공간에서도 물체의 위치를 계산할 수 있다.

촬영한 물체의 정확한 3차원 위치를 파악하기 위해서 주로 스테레오 비전을 사용한다. 마찬가지로 구면 영상에서도 두 개의 영상의 시차를 이용하여 물체의 위치를 파악할 수 있다. 이에 대해 Li[1][2]는 구면 스테레오 영상에서의 실시간 특징점 매칭을 제시했고, Tong 등[3]은 구면 스테레오 영상에서 특정 물체의 위치를 추정하는 방법을 제시했다. Igbinedion[4]는 여러 장의 구면 영상을 사용하여 장면을 재구성하는 방법을 제안하였다.

본 논문에서는 넓은 간격으로 배치한 여러 대의

구면 카메라로 촬영한 구면 영상들로부터 물체의 위치를 추정하는 방법을 제안한다. 2장에서 다수의 구면 영상에 동시에 나타나는 물체의 위치를 찾는 방법을 설명하고 3장에서 실험을 통해 제시한 방법의 활용성을 보인다. 마지막으로 4장에서 결론을 맺는다.

2. 알고리즘 개요

본 논문에서 제안하는 방법을 위해 설치된 여러 대의 구면 카메라의 위치를 알고, 카메라의 회전각은 일정하다고 가정한다. 먼저 각 영상들에서 나타나는 동일한 물체의 좌표를 얻고, 카메라의 회전 각도와 위치를 고려하여 삼각측량법으로 해당 물체의 실제 위치를 추정한다. 이 과정에서 구면 영상의 해상도에 따라 계산된 물체의 위치에 오차가 날 수 있으므로 여러 영상에서 나타난 결과에 평균을 취한다. (그림 1)은 본 논문에서 제안하는 방법의 전체 흐름을 나타낸 의사코드이다.

Input: O_m, O_n, I_m, I_n

Output: L

Begin

$p_m^k \leftarrow \text{GetImagePosition}(I_m)$

$p_n^k \leftarrow \text{GetImagePosition}(I_n)$

$\theta_1, \theta_2, \theta_3, \phi_1, \phi_2 \leftarrow \text{DefineAngles}(p_m^k, p_n^k)$

$l \leftarrow \text{GetBaseLineLength}(O_m, O_n)$

$S_1, S_2 \leftarrow \text{HorizontalProcess}(l, \theta_1, \theta_2, \theta_3)$

$V_1, V_2 \leftarrow \text{VerticalProcess}(S_1, S_2, \phi_1, \phi_2)$

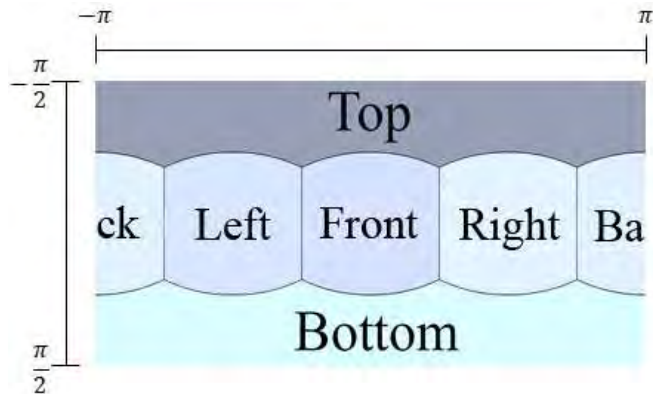
$L \leftarrow \text{EstimateObjPostion}(S_1, \theta_1, \phi_1)$

End

(그림 1) 제안 방법의 의사 코드

2.1. 영상 내에서의 물체 좌표

구면 영상의 좌표는 구 표면과 일대일 대응시켜 구면 좌표 $(1, \theta, \phi)$ 로 나타낼 수 있으며, 가로 범위 θ 와 세로 범위 ϕ 의 범위는 (그림 2)와 같이 나타난다. k 개의 물체 P_1, P_2, \dots, P_k 가 각 영상들 I_1, I_2, \dots, I_n 에서 나타나는 좌표를 구면 좌표로 변환하고, 이를 $p_n^1, p_n^2, \dots, p_n^k$ 이라고 한다. 이 과정은 의사 코드에서 $\text{GetImagePosition}()$ 함수에 해당한다.



(그림 2) 구면 파노라마의 각도 좌표

2.2. 카메라의 높이 관계 고려

물체 P 의 실제 위치를 계산하기 위해 앞서 두 카메라의 높이가 얼마나 어긋나 있는가를 고려한다. 현재 선택된 두 카메라 $O_m, O_n (m < n)$ 를 이은 선분을 d 라고 했을 때 d 를 기준 수평면에 사영한 선분을 l 이라 한다. l 은 식 (1)에 의해 정의된다.

$$l = d \cos \psi^v \quad (1)$$

의사 코드의 $\text{GetBaseLineLength}()$ 함수에서는 두 카메라 위치의 차이로 ψ^h 와 d 를 구하고 위 식을 사용해 삼각 측량을 위한 밑변의 길이를 구한다.

2.3. 물체 위치 계산

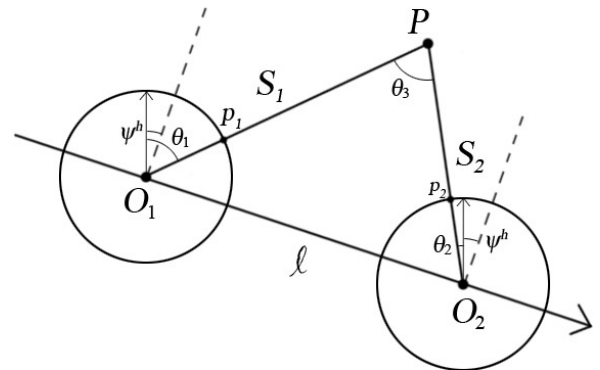
다음으로 삼각 $\text{DefineAngles}()$ 함수를 통해 측량을 위한 각도를 찾는다. 각 카메라들의 위치를 O_1, O_2, \dots, O_n 로 하고 이 지점을 기준으로 Front-Back 방향을 x 축, Left-Right 방향을 y 축, Top-Bottom 방향을 z 축으로 하는 n 개의 로컬 좌표계를 생성한다. l 은 현재 선택된 두 카메라 $O_m, O_n (m < n)$ 사이의 거리를 l , p_m^k 과 p_n^k 의 값을 θ_1 와 θ_2 , ϕ_1 와 ϕ_2 로 한다. 물체의 3차원 좌표는 수평 방향에 대해 먼저 계산한 후 수직 방향에 대해 계산한다. $\text{HorizontalProcess}()$, $\text{VerticalProcess}()$ 두 함수는 각각 식 (2)과 식 (3)에 해당하며 (그림 3)과 (그림 4)에 시각화하여 나타났다.

$$S_1 = \frac{l \cos(\theta_2 - \psi^h)}{\sin \theta_3} \quad (2)$$

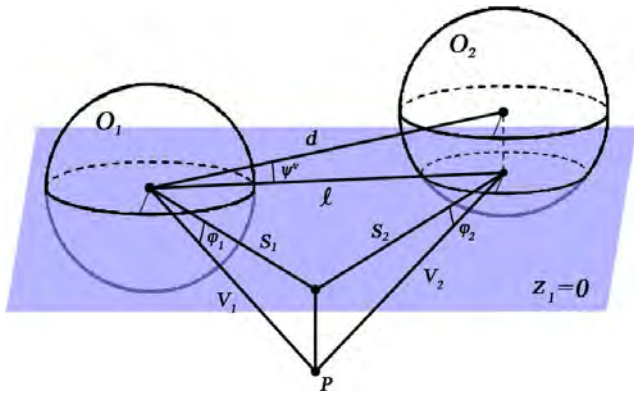
$$S_2 = \frac{l \cos(\theta_1 - \psi^h)}{\sin \theta_3}$$

$$V_1 = S_1 \sec \phi_1 \quad (3)$$

$$V_2 = S_2 \sec \phi_2$$



(그림 3) HorizontalProcess 함수 시각화



(그림 4) VerticalProcess 함수 시각화

식 (1)-(3)을 통해서 일차적인 물체의 위치를 추정할 수 있으며, 이는 식 (4)로 나타난다.

$$L = S_1 (\cos \theta_1, \sin \theta_1, \tan \phi_1) \quad (4)$$

영상의 해상도가 낮거나 선택된 물체의 영상 내 좌표에 오차가 있을 경우 오차를 최소화하기 위해 *EstimateObjPostion()* 함수를 실행한다. 이 함수에서는 P_k 가 나타난 모든 영상의 매칭 쌍에서 이 과정을 반복하고 평균을 내는 방식으로 물체의 위치 L 을 추정한다.

3. 실험

본 논문에서 제안하는 방법의 추정 결과 오차는 다음과 같은 절차로 확인한다. 먼저, 공간에 배치된 물체들의 위치 P_n 와 카메라들의 위치 O_n 를 측정한다. 각 카메라에서 촬영한 n 장의 구면 영상에서 물체의 위치를 직접 찾고 해당 물체들이 실제로 어디에 위치하는지 추정한다.

본 논문의 실험은 Intel Core i7 CPU, NVIDIA Geforce GTX 970, 16GB RAM, Windows 7 64bit OS의 시스템에서 수행되었고, C++ 언어와 OpenCV 라이브러리를 사용한 코드로 구현되었다. 실험에 사용된 영상은 Ricoh Theta S 카메라를 사용하여 촬영했고 2000×1000의 해상도에서 실험을 진행했다. 월드에 4개의 서로 다른 색의 물체를 배치하고 중앙 지점에 장애물을 배치한 후 4곳에서 구면 영상을 촬영했다(그림 5). 카메라의 위치와 배치된 물체의 중심 좌표는 <표 1>과 <표 2>에 나타난다. 물체의 추정 좌표는 <표 3>에 나타난다.

제시하는 방법의 정확도는 직육면체의 꼭짓점들의 실제 위치와 추정된 위치를 비교하여 나타냈다. 추정한 직육면체의 꼭짓점 좌표의 오차는 (그림 6)에 나타난다. 그래프의 청색, 녹색, 적색 막대는 각

각 x, y, z 축에 대한 추정 오차를 나타낸다. 추정 좌표는 대부분 1cm 이하의 오차를 보였으며, 오차가 가장 크게 나타나는 경우에도 2cm 보다 작은 오차 범위를 보였다.



(그림 5) 실험에 사용된 구면 영상

4. 결론

본 논문에서는 여러 장의 구면 영상을 통해 물체의 위치를 추정하는 방법을 제시했다. 기존 구면 스테레오 비전에서 물체의 위치를 찾는 방법을 응용하여 큰 장애물이 있어도 모든 물체의 위치를 찾는 방법을 제안했다. 실험 결과 제안한 방법은 찾고자 하

는 모든 물체에 대해 수 센티미터 이내의 오차만을 가지는 정확도를 보임을 확인하였다.

현재의 알고리즘은 의도적으로 찾고자 하는 물체만을 찾을 수 있지만, 구면 영상에서의 특징점 매칭과 영상 매칭 등의 기법을 추가적으로 접목하여 효율성을 향상시킴으로써 공간 전체에 대한 알고리즘으로 발전할 수 있다. 제안한 다중 구면 영상으로 물체나 특징점의 실제 위치를 추정하는 방법은 향후 하나의 실내 공간 전체를 AR을 위한 공간으로 사용하기 위한 방법으로 발전시킬 수 있을 것으로 기대된다.

<표 1> 카메라 좌표 (단위: cm)

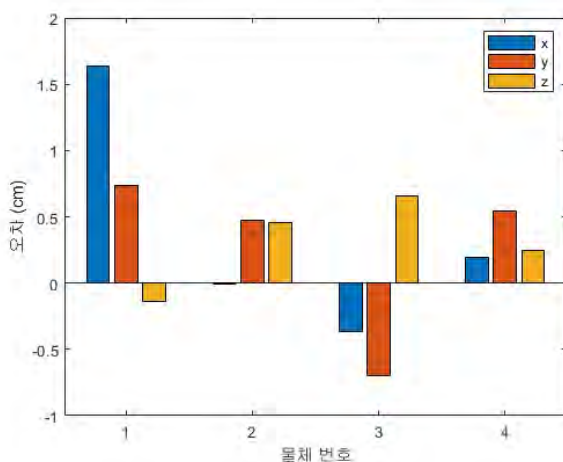
	좌표(x, y, z)
카메라 1	-20, -20, 10.9
카메라 2	20, -20, 10.9
카메라 3	20, 20, 10.9
카메라 4	-20, 20, 10.9

<표 2> 배치된 물체의 좌표 (단위: cm)

	좌표(x, y, z)
물체 1	-50, -30, 7.8
물체 2	50, 20, 7.8
물체 3	-20, 40, 7.8
물체 4	30, -30, 7.8

<표 3> 물체의 추정 좌표 (단위: cm)

	좌표(x, y, z)
물체 1	-48.36, -29.26, 7.66
물체 2	49.99, 20.47, 8.25
물체 3	-20.36, 39.30, 8.46
물체 4	30.19, -29.45, 8.05



(그림 6) 추정된 위치 좌표의 오차

Acknowledgments

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. NRF-2019R1F1A1060828).

참고문헌

- [1] Shigang Li, "Real-Time Spherical Stereo", 18th International Conference on Pattern Recognition (ICPR'06), pp. 1046-1049, 2006.
- [2] Shigang Li, "Binocular Spherical Stereo", IEEE Transactions on Intelligent Transportation Systems, Vol. 9, No. 4, pp. 589-600, 2008.
- [3] Guofeng Tong, JiuHong Gu, "Locating Objects in Spherical Panoramic Images", Proceedings of the 2011 IEEE International Conference on Robotics and Biomimetics, pp. 818-823, 2011.
- [4] Ifueko Igbinedion, Harvey Han, "3D Stereo Reconstruction Using Multiple Spherical Views", Accessed 20 April 2020.

TensorRT 엔진과 SSD를 이용한 Face detection

유혜빈*, 김상훈*

*한경대학교 전기전자제어공학과

e-mail: kimsh@hknu.ac.kr

Objedet detection using TensorRT engine and SSD

Hye-Bin Yoo*, Sang-Hoon Kim*

*Dept of Electrical, Electronic and Control, Hankyong National University

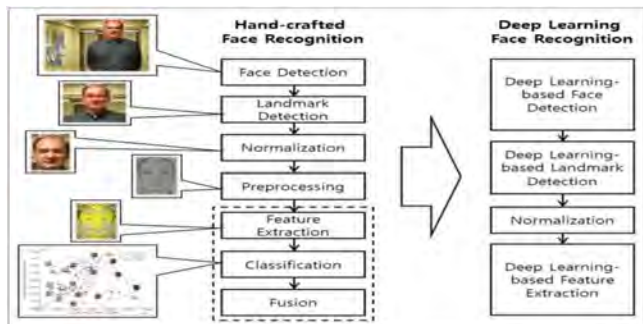
요 약

최근에는 딥러닝 기술의 발달로 물체 인식 및 검출에 관한 기술들 또한 발달하고 있다. 검출에 관한 여러 기법(Faster R-CNN, R-CNN, YOLO, SSD 등) 중 SSD는 다른 기법들과는 다르게 높은 정확도와 빠른 속도가 특징이다. 동시에 여러 detection network들도 쉽게 이용이 가능하다.

본 논문에서는 detection network중 Mobilenet V2 network를 이용하여 SSD와 결합해 모델을 훈련하고, TensorRT engine을 이용하여 더 빠른 속도로 검출할 수 있는 방법에 대해 논의한다. 이 방법을 통해 face detector를 만들어 여러 상황에서 쓰일 수 있도록 한다.

1. 서론

딥러닝 기술의 발달 [1]로 인해 Computer vision 방식들에도 많은 변화가 생기고 있다. 특히 얼굴 인식 분야에서 기존의 방식인 Hand-crafted Feature인 HOG, LBP, GABOR등의 특징들이 모두 딥러닝 기반의 특징으로 바뀌었고 얼굴 검출에서도 Viola-jones의 Haar-like Feature를 Boosting하는 방식에서 딥러닝 기반의 방식으로 바뀌며 계속해서 성능을 개선하고 있다.



(그림 1) 얼굴 인식 기술의 변화

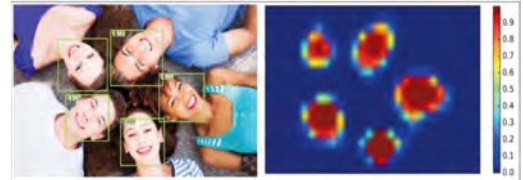
2.본론

2.1. 현재 기술의 한계

얼굴 검출 관련 딥러닝 기술은 ICMR에서 2015년도에 기본적인 AlexNet [4]을 기반으로 한 얼굴 검출기가 발표되었다. 이 당시에는 AlexNet을 얼굴 영상으로 Fine-tuning하여 [그림 2]와 같은 결과를 산출하였지만, 이때까지는 검출 성능이 높지 않아 최종 단계 SVM을 이용하여 얼굴 유무를 최종 판단하였다.

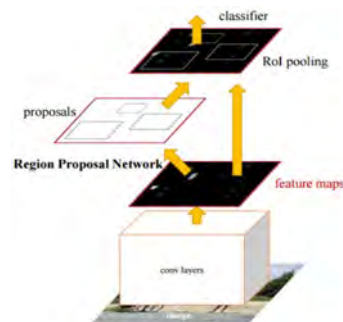
AlexNet을 이용한 얼굴 검출 방식을 제외하고도 고속

물체 검출기인 YOLO를 fine-tuning한 얼굴 검출기 및 Faster R-CNN을 fine-tuning한 얼굴 검출 알고리즘들이 속속 소개되고 있다.



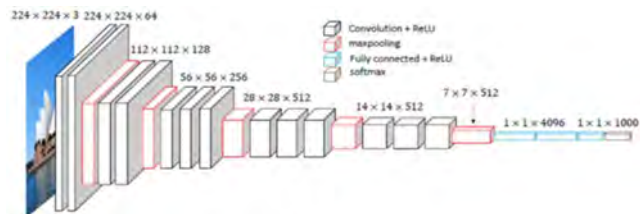
(그림 2) AlexNet

이 중에서도 가장 많이 사용되었던 대표적인 detector는 Faster R-CNN이다. 이 Faster R-CNN은 Detecting을 위해 들어온 image의 후보 영역을 뽑아 뽑은 부분의 특징이나 픽셀을 resampling하고 높은 성능의 classifier를 이용한다.[그림 3] 하지만 Faster R-CNN은 전작인 R-CNN을 열심히 개선했음에도 불구하고, 속도가 느려(7 FPS with mAP 73.2%) 실시간 영상 분석에 사용할 수는 없었다. Faster R-CNN에 비해 YOLO의 속도는 빠른 편이었지만, 그만큼 성능이 낮았다.(45FPS with mAP 63.4%)



(그림 3) Faster R-CNN

보편적으로 사용되고 있는 다른 Deep-learning Detector들은 처음 훈련 시킨 크기만을 입력으로 받을 수 있다. 대표적으로 VGG-16, AlexNet에서 줄 224x224 크기의 이미지를 입력으로 받는다.[그림 4] 즉 원하는 사진에서 객체가 있는지 없는지 확인하기 위해서는 그림을 224x224로 자르거나 변형해야 한다.



(그림 4) VGG-16 architecture

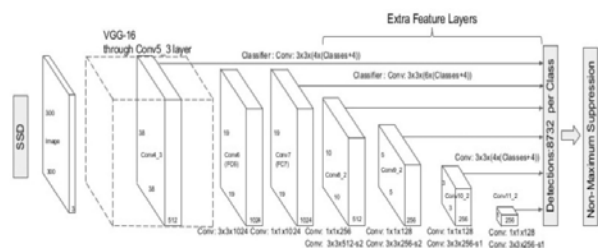
이러한 과정을 위해 Image Pyramid & Sliding Window라던가 Region Proposal Network(Faster R-CNN)등으로 입력 이미지를 변형시켜 네트워크에 집어 넣게 된다. 문제는 위의 처리과정을 통해 얻은 여러가지 sample들을 하나씩 network에 넣어 하나씩 검출해야 한다는 것이다. 여러 장의 정보를 처리해야 하기 때문에 그만큼 네트워크를 많이 돌게 되고, 횟수 차이에 의한 속도 저하가 일어나게 된다.

2.2. 관련연구

Single shot multibox detector(SSD) [2]는 Single-shot detector라는 말 그대로 사진의 변형 없이 그 한 장으로 훈련 및 검출을 하는 detector를 의미한다. SSD는 후보 영역 추출 과정과 resampling 과정을 제거한 방식을 이용하여 높은 정확성과 빠른 속도를 모두 얻어냈다. (59FPS with mAP 74.3%) (위의 모든 성능 측정은 VOC2007 test 기반)

SSD는 전부 새로 만든 구조가 아니다. 원래 잘 만들어졌던 feed-forward convolutional network에서 feature map을 뽑아내는 과정까지를 하나의 기본 구조로 가지고, 여러 보조적인 몇 가지 구조만을 추가한 것이다.

하지만 single-shot learning을 위해서는 한 가지 큰 문제를 해결해야 한다. 단 한 장의 사진만을 가지고 여러 가지 크기의 물체를 검출해야 한다는 것이다. SSD는 이러한 문제를 기본 구조 뒤에 보조 구조를 붙여 얻은 Multi-scale feature maps를 이용하여 해결하였다. [그림 5]가 SSD의 architecture이다. 기본 구조나 보조 구조에서 얻은 feature map들은 각각 다른 convolutuional filter에 의해 결과값을 얻게 된다.

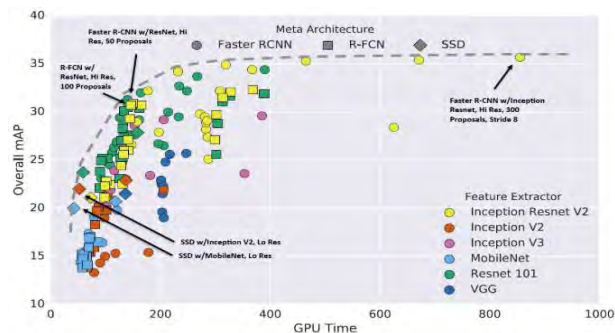


(그림 5) SSD architecture

속도를 제외한 SSD의 가장 큰 장점은 다른 어떠한 detection network이던 single-shot learning에 이용할 수 있다는 것이기에 real-time detector 연구에 용이하다고 볼 수 있다.

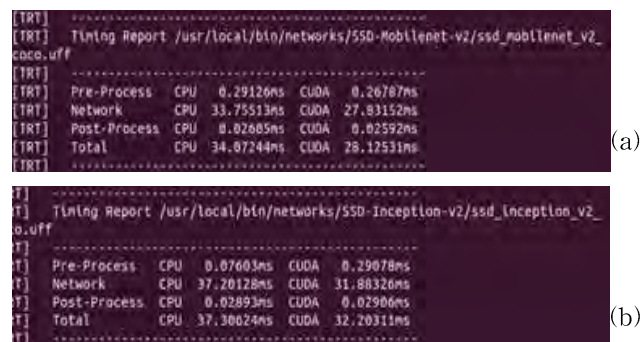
3. SSD Mobilenet V2

single-shot learning은 detection network 종류에 상관 없이 이용이 가능하다고 앞에서 언급하였다. SSD의 장점은 높은 속도와 정확도인데 이를 활용하기 위해 detection network 또한 높은 속도와 정확도를 가지고 있다면 그 효율은 뛰어날 것이다. 이와 같은 이유로 detection network는 Mobilenet v2를 선정하였다.



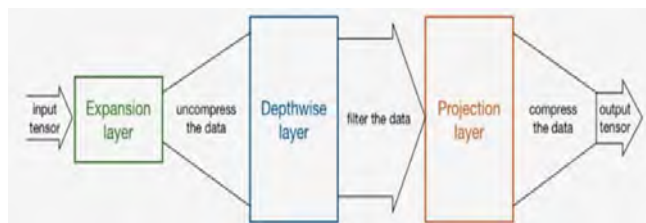
(그림 6) Accuracy vs Time

[그림 6]에서 볼 수 있듯이 SSD를 이용한 모델 중 가장 속도가 빠른 것은 Mobilent network임을 확인할 수 있다.



(그림 7) ssd의 mobilenet v2(a)와 inception v2(b) 속도

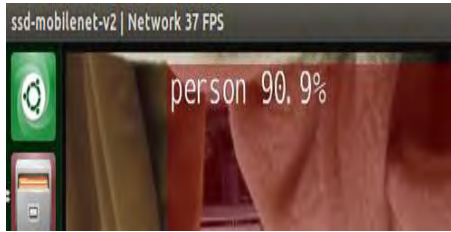
MobileNet v2 [3]는 MobileNet V1의 속도 저하 원인이었던 PW의 부담을 인식하고 DW 연산 비중을 올리는 테크닉을 사용한다. Expansion Layer, Projection Layer가 추가되었고, 그 중간에 DW가 존재한다. 즉, Expansion Layer PW에서 Channel을 늘려준 상태에서 DW를 한다. Projection Layer에서는 원래의 Channel 개수로 줄여주는 역할을 해가 된다. 즉, Channel을 기준으로 Expansion하고 Projection한다는 것이다.



(그림 8) Mobilenet V2 기술

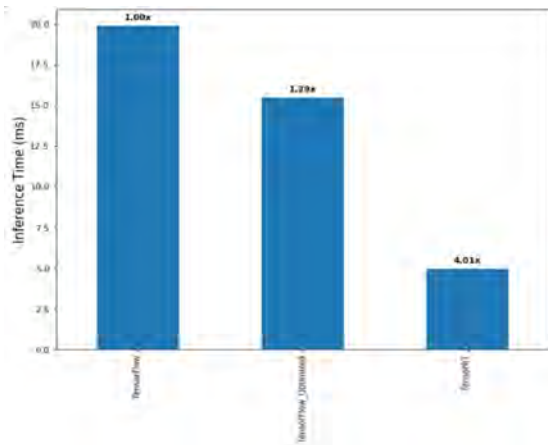
4. 실험 및 고찰

coco dataset으로 훈련된 ssd_mobilenet_v2를 Jetson TX2 임베디드 보드에서 실시간 영상으로 실험해본 결과 [그림 9]와 같이 높은 정확도와 빠른 속도를 보여주었다.



(그림 8)

실시간 검출 속도가 평균 35~37 FPS정도인데, 이는 TensorRT 최적화 과정을 거친 것으로 이 과정을 거치지 않으면 10FPS 안팎의 속도를 보이게 된다. [그림 9]를 보면 알 수 있듯이 ssd_mobilenet_v2를 tensorflow로만 이용하는 것을 기준으로 보았을 때 TensorRT 엔진을 사용하게 되면 최대 4배에 가까운 성능을 내는 것을 알 수 있다.



(그림 9) TensorRT 최적화 결과

5. 결론 및 향후 연구계획

본 논문은 더 효과적인 detection을 하기 위한 연구이다. 기존 Tensorflow만을 이용한 detection은 속도가 느려 제한된 상황에서만 쓰일 수 있었다. TensorRT engine을 이용하여 detection을 하게 된다면 제한된 상황에서도 보다 뛰어난 성능으로 detection이 가능해지게 된다.

향후 연구는 SSD를 이용하여 mobilenet v2 네트워크를 TensorRT 엔진을 사용하여 사람의 얼굴에 관한 detection을 진행할 예정이다. 현재 사람에 관한 것은 'person'이라는 class만 기존 훈련된 네트워크에 있고, 이를 얼굴에 관한 detection으로 더 구체화하여 성별, 인종, 연령대 등으로 검출할 수 있게 하는 것이 최종 목표이다.

참고문헌

- [1] 황원준 - 딥러닝 기반 얼굴 검출, 랜드마크 검출 및 얼굴 인식 기술 연구 동향
- [2] Wei Liu, Dragomir Anguelov, Dumitru Erhan, Christian Szegedy, Scott Reed, Cheng-Yang Fu, Alexander C. Berg1/UNC Chapel Hill Zoox Inc. Google Inc. University of Michigan, Ann-Arbor - SSD: Single Shot MultiBox Detector
- [3] Mark Sandler, Andrew Howard Menglong Zhu, Andrey Zhmoginov, Liang-Chieh Chen/Google Inc. - MobileNetV2 : Inverted Residuals and Linear Bottlenecks
- [4] Alex Krizhevsky, Ilya Sutskever, Geoffrey E. Hinton - ImageNet Classification with Deep Convolutional Neural Networks

DNN 과 LSTM 기반의 대기질 예측 모델 성능 비교 연구

조성재*, 김준석**, 김성희**, 윤주상**

*동의대학교 응용소프트웨어공학과

**동의대학교 산업ICT기술공학과

xc11161@gmail.com, junsuk.kim@deu.ac.kr, sh.kim@deu.ac.kr, jsyoun@deu.ac.kr

A Comparative Study on the Performance of Air Quality Prediction Model Based on DNN and LSTM

Sung-Jae Jo*, Junsuk Kim**, Sung-Hee Kim**, Joosang Youn**

*Dept. of Application Software Engineering, Dong-eui University

**Dept. of Industrial ICT Engineering, Dong-Eui University

요 약

최근 인공지능을 활용한 대기질 예측 모델 개발 연구가 활발히 진행 중이다. 특히 시계열 데이터 기반 예측 시스템 개발에 장점을 가진 DNN, LSTM 알고리즘을 활용한 다양한 예측 시스템이 제안되고 있다. 본 논문에서는 LSTM을 활용한 모델과 Fully-Connected 기반의 DNN 모델을 활용한 대기질 예측 시스템을 개발하고 두 모델의 예측 정확도를 비교한다. 성능 평가 결과를 보면 LSTM 모델이 DNN 모델보다 모든 면에서 좋은 결과를 보여줬다. 그리고 이산화황(SO₂), 이산화질소(NO₂), 초미세먼지(PM_{2.5})에 대해서는 그 차이가 두드러지게 나타났다.

1. 서론

최근 인공지능 기술을 활용한 대기질 예측 연구가 활발히 진행 중이다. 특히, DNN(Deep Neural Network)을 활용한 연구와 LSTM(Long Short-Term Memory)을 활용한 연구가 제안되었다[1, 2]. 이 외에도 많은 연구에서 다양한 알고리즘을 적용한 대기질 예측 모델이 제안되고 있지만 사용된 알고리즘에 따른 예측 정확도를 비교하는 연구 결과는 아직 제안되어 있지 않다. 본 논문은 기존 시계열 데이터 학습을 위해 사용되는 대표적 알고리즘인 DNN과 LSTM 알고리즘을 활용한 대기질 예측 모델을 개발하고 두 예측 모델의 대기질 예측 정확도를 비교 분석할 것이다.

이어지는 2장에서는 관련 연구를 기술하고, 3장에서는 [1]에서 제안된 DNN 모델과 LSTM 기반 대기질 예측 시스템을 제시할 것이다. 4장에서 각 모델의 성능을 비교 분석할 것이고, 마지막으로 5장에서 논문의 결론을 내린다.

2. 관련 연구

[1]에서는 완전연결신경망을 기반으로 하는 대기

질 예측 모델을 제안했다. 학습을 위한 데이터는 대기오염물질의 시간대별 농도자료 6종(SO₂, CO, O₃, NO₂, PM₁₀, PM_{2.5})과 이와 상응하는 시간대의 기상정보(온도, 습도, 풍향, 풍속) 4종을 활용한 10종이 활용됐으며, 총 3년간의 연속 시간별 데이터가 학습에 사용되었다. 그 결과 각각의 대기오염물질 농도에 대한 예측 정확도는 75% ~ 88%를 보였다.

3. 대기질 예측 모델

3.1 학습 데이터

대기질 예측 모델에 사용된 학습데이터는 한국환경공단 에어코리아에서 제공하는 대기오염물질의 시간대별 농도자료 6종(SO₂, CO, O₃, NO₂, PM₁₀, PM_{2.5}) 및 기상청 기상자료개방포털에서 제공하는 기상자료 4종(온도, 습도, 풍향, 풍속)으로 서울 중구 지역의 3년간(2016.01.01. ~ 2018.12.31.)의 데이터를 사용했다.

3.2 DNN 기반 대기질 예측 모델

DNN모델은 [1]논문에서 사용된 구현 방법을 기반으로 했으며, 일부 수정을 거쳤다. 모델은 입력층

과 3개의 은닉층 그리고 출력층으로 설계되고, Keras의 Sequential Model과 Dense Layer로 구현했다. 각 은닉층에 할당되는 노드의 개수는 각각의 대기오염물질에 따라 100 ~ 400 개가 할당된다. 모델의 입력으로는 대기오염물질 6종의 농도자료와 기상자료 4종이 사용되고 예측 결과는 입력 시간으로부터 한 시간 후의 대기오염물질 농도를 나타내도록 했다.

3.3 LSTM 기반 대기질 예측 모델

LSTM 모델은 기본적으로 입력층, 은닉층, 출력층 3계층 구조를 갖지만, 미세먼지(PM₁₀)와 초미세먼지(PM_{2.5})에 대해서는 예측 정확도를 높이고자 은닉층을 한 층 늘린 4계층으로 설계했다. 그리고 3계층 모델의 은닉층에는 4개의 LSTM 유닛을 할당했고, 4계층 모델의 은닉층에는 각각 256, 128개의 LSTM 유닛을 할당했다. 모델의 구현은 Keras의 Sequential Model과 LSTM layer를 활용해 구현했다. 모델의 입력으로는 각각의 물질에 대해 직전 100시간 동안의 시간대별 연속 관측 자료가 적용되고 예측 결과는 입력 데이터로부터 한 시간 후의 대기오염물질 농도를 나타내도록 했다.

4. 모델 성능 평가

4.1 모델 성능 평가 방법

모델의 예측 결과를 실제 관측값과 비교하기 위해 각각의 대기오염물질에 대해 IOA(index of agreement), ME(bias) NRMSE (Normalized RMSE) 값을 산출하여 표로 정리하여 나타냈다. 비교에 사용된 수식은 논문[1]의 모델 검증 과정에서 사용된 수식이다.

$$IOA = 1 - \frac{\sum_{i=1}^n (|O_i - M_i|)^2}{\sum_{i=1}^n (|M_i - \bar{M}| + |O_i - \bar{O}|)^2}$$

$$ME(bias) = \frac{1}{n} \sum_{i=1}^n (O_i - M_i)$$

$$NRMSE = \frac{100}{\bar{O}} \times \sqrt{\frac{1}{n} \sum_{i=1}^n (O_i - M_i)^2}$$

여기서 O_i 는 관측 값, M_i 는 모델의 예측 값을

나타낸다. \bar{O} 와 \bar{M} 는 각각 관측 값과 모델 예측 값의 평균이다. n 은 검증에 사용된 데이터의 개수다.

4.2 모델 성능 평가 결과

모델의 성능을 평가하기 위해 사용된 검증데이터는 학습 과정에서 사용되지 않은 데이터로 서울 중구 지역의 3개월간(2019.01.01. ~ 2019.03.31.) 데이터다. 생성된 모델이 일정한 성능을 보이는지 확인하기 위해 입력데이터에 대해 총 10회의 예측을 진행했고, 그 결과 산출된 IOA, ME(bias), NRMSE 값의 평균을 <표 1>에 제시했다.

대기오염물질	IOA		ME(bias)		NRMSE	
	LSTM	DNN	LSTM	DNN	LSTM	DNN
SO ₂	0.915	0.669	-0.277	0.461	14.653	29.145
CO	0.967	0.953	-14.719	29.422	13.373	15.312
O ₃	0.969	0.944	0.530	0.857	24.859	32.048
NO ₂	0.966	0.898	-0.594	4.961	16.454	25.312
PM ₁₀	0.987	0.977	-0.264	5.121	12.417	16.106
PM _{2.5}	0.987	0.960	-0.296	5.738	16.354	25.739

<표 1> 검증 결과

IOA는 관측값과 예측값의 시계열 유사성을 나타내는 척도로 0 ~ 1 사이의 값을 가진다. IOA 값이 1에 근접할수록 관측값과 모델의 예측값이 시계열에 대해 일치함을 뜻한다. 모든 경우에서 LSTM의 IOA 값이 DNN에 비해 높게 나타났고, 특히 이산화황(SO₂)에서 그 차이가 두드러지게 나타났다.

ME(bias)는 관측값과 모델의 예측값 간의 평균 편향을 나타내는 지표로 0에 근접할수록 편향이 적음을 의미한다. 단위는 각 대기오염물질의 농도와 동일하다. 두 모델에서 ME(bias)의 값은 매우 낮은 수치를 보였다. 하지만 일산화탄소(CO), 이산화질소(NO₂), 미세먼지(PM₁₀), 초미세먼지(PM_{2.5})에서 LSTM이 비교적 적은 편향을 나타냈다.

NRMSE는 RMSE 값을 관측 평균으로 나누어 백분율로 나타낸 것이다. 모든 경우에서 LSTM이 DNN에 비해 낮았고 이산화황(SO₂), 오존(O₃), 이산화질소(NO₂), 초미세먼지(PM_{2.5}) 큰 차이를 보였다.

5. 결론

모델의 성능 평가 결과 모든 지표에서 LSTM 기반 모델이 DNN 기반 모델 보다 좋은 예측 결과를 보였다. 특히 이산화황(SO₂), 이산화질소(NO₂), 초미

세먼지(PM_{2.5})에 대해서는 유의미한 차이를 보였다.

본 결과는 대기질 데이터가 시계열에 의존적임과 동시에 LSTM 모델이 시계열 데이터 기반 예측 시스템에 강점을 가지고 있기 때문이다[3]. 하지만 학습하는 과정에서 에포크(epoch)횟수, 배치(batch)사이즈 그리고 입력 데이터의 형태 등 모든 조건이 동일하게 적용되지 않아 절대적인 비교는 불가능했다는 한계점이 있다.

ACKNOWLEDGMENT

본 연구는 ICT R&D 혁신 바우처 지원 사업의 지원을 받아 수행된 결과임. (20190019150 012002_104)

참고문헌

- [1] 조경학, 이병영, 권명흠, 김석철. (2019). 심층 신경망을 이용한 대기질 예측. 한국대기환경학회지, 35(2), 214-225.
- [2] İ. Kök, M. U. Şimşek and S. Özdemir, "A deep learning model for air quality prediction in smart cities," 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, 2017, pp. 1983-1990.
- [3] 백창룡. (2013). 한국의 미세먼지 시계열 분석: 장기종속 시계열 혹은 비정상 평균변화모형. 응용통계연구, 26(6), 987-998.

DenseNet 을 통한 얼굴 스푸핑 탐지 기술

김소의¹, 유수경¹, 이의철^{1,*}

¹상명대학교 휴먼지능정보공학전공
soeui291@gmail.com, tnrud7495@gmail.com

*Corresponding author: eclee@smu.ac.kr

Face spoofing detection using DenseNet

So-Eui Kim, Su-Gyeong Yu, Eui Chul Lee

Dept. of Human Centered Artificial Intelligence, Sangmyung University

요 약

얼굴을 이용한 신원인식 방법은 높은 사용 편의성과 보편성 때문에 다양한 분야에서 활용되고 있다. 그러나 타인의 얼굴 사진이나 테블릿 PC 를 통한 얼굴 동영상 재생과 같은 손쉬운 방법을 통한 얼굴 스푸핑 공격 사례가 다수 보고되고 있다. 하지만 기존의 영상의 텍스처 특징을 활용한 방법은 영상의 초점 상태에 취약하고 기계학습에 사용된 데이터에 의존적이다. 따라서 보다 강력한 스푸핑 탐지 기술이 필요하다. 본 연구에서는 다양한 각도와 거리 편차 요소를 포함하는 자체 구축 DB 와 DenseNet 을 활용한 딥러닝 기반의 위조 얼굴 검출 기술을 연구했다.

1. 서론

오늘날 생체 인식은 보다 안정적이게 발전했다. 여러 생체 인식 방법 중 얼굴 인식 시스템은 편리하며 거부감이 낮은 방법 중 하나이다. 하지만 지난 몇 년 간 스푸핑 공격과 같은 생체 인식 시스템의 잠재적 취약점이 다수 보고됐다 [1]. 따라서 얼굴 인식의 안전성을 보장하기 위해 보다 정확한 얼굴 인식 시스템 개발이 요구되고 있다.

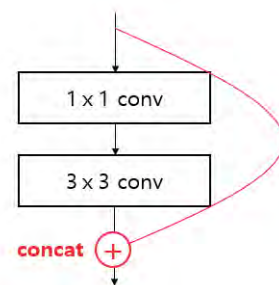
기존의 연구에서는 LBP, DCT, SVM 을 이용해 얼굴 스푸핑 공격을 탐지했다 [2]. 이러한 방식들은 고수준 특징인 질감을 기반으로 한다 [3]. 그러나 질감 정보는 영상의 초점, 해상도에 따라 유의미한 동작을 하지 못할 수 있다. 또 기존의 연구에서 사용된 대부분의 공개 DB 들은 거리, 각도 편차에 대한 정보가 담겨있지 않다.

본 논문에서는 이러한 문제점을 해결하고자 CNN 기반의 신경망 모델인 DenseNet-121 을 통한 얼굴 스푸핑 공격 탐지 기술을 연구했다. 연구에 사용한 DB 는 거리, 각도와 같은 차별화된 특성을 가지는 PR-FASD 이다 [4].

2. 본론

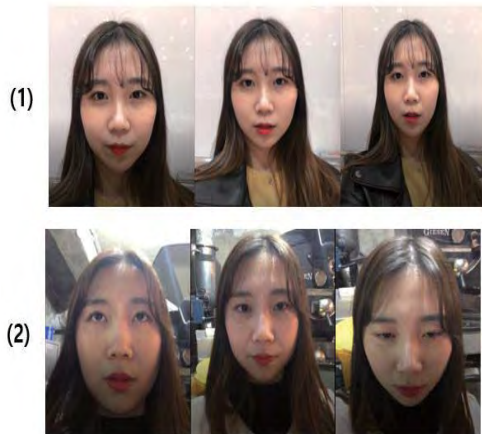
기존에 사용되던 기계학습 모델에서는 사람이 구현한 프로그램에 의해 추출된 특징을 이용하여 학습하였다. 반면 DenseNet-121 은 신경망 모델 중 하나로 입력 데이터의 특징을 스스로 추출하고 학습한다. 이때, Densely connection 을 기반으로 하여 layer 의 feature

map 을 계속해서 다음 layer 의 입력과 Concatenation 한다. 즉, concatenation 연산을 이용해 이전 layer 의 정보가 다음 layer 의 출력에 연결됨으로써 최초의 정보가 마지막까지 반영되는 것이다. 이를 통해 기존의 신경망모델에서 나타났던 degradation 문제와 Vanishing-gradient 문제를 개선했다[5]. (그림 1)은 Densnet-121 모델의 구조를 나타낸다.



(그림 1) DenseNet-121 신경망 모델 방식.

연구에 사용한 DB 는 고정되지 않은 배경과 조명, 3 가지의 거리(near, halfway, distant), 그리고 3 가지의 각도(bottom, middle, top)라는 차별화된 특성을 가지는 PR-FASD 이다. 이 DB 에는 30 명(남성: 19 여성: 11)의 실제 얼굴 영상과 스푸핑 공격 방지를 위한 인쇄된 사진과 재생 비디오를 촬영한 가짜 얼굴 영상이 있다. PR-FASD 의 예시는 (그림 2)에서 볼 수 있다.



(그림 2) PR-FASD 얼굴 이미지 예시 (1): 3 가지 거리,
(2): 3 가지 각도.

3. 실험 및 결과

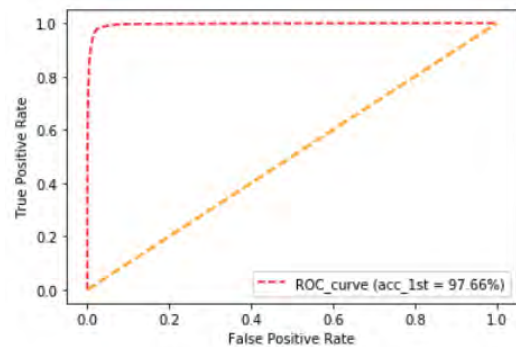
본 논문에서는 PR-FASD 데이터베이스를 학습, 검증, 테스트 데이터로 이용하였다. 신경망 모델인 Densenet-121의 입력으로 들어온 얼굴 이미지는 7×7 크기의 convolution filter 64 개를 사용하여 학습되었으며, 이 과정에서 1×1 및 3×3 convolution filter로 이루어진 Dense Block은 총 4 개로 구성되어졌다. 각각의 feature map의 depth는 128, 256, 512, 1024으로 2 배씩 증가하였으며, 이때 stride=2, epoch=100으로 지정하였다. 학습과정에서 Binary cross entropy를 손실함수로, 확률적 경사 하강법을 최적화함수로 사용하였으며 learning rate은 0.001 이었다. 또한, 과적합 등의 문제를 방지하기 위해 학습과정에서 검증데이터를 추가적으로 이용하였다.

얼굴 스푸핑 공격 검출 성능 결과 확인 지표로 Half Total Error Rate(HTER)과 정확도를 사용하였다. HTER은 값이 작을수록 성능이 좋은 것으로 오분류의 비율만을 이용한 값이다. Equal error rate(EER)은 False Rejection Rate(FRR)과 False Acceptance Rate(FAR)값의 동일한 비율을 말하며 값이 낮을수록 좋은 성능을 나타낸다. 최종 학습된 모델을 사용하여 테스트 얼굴데이터를 분류한 결과로 HTER, EER은 각각 2.34, 2.85로 아래 <표 1>과 같다. 얻어진 결과는 Receiver Operating Characteristic(ROC) 곡선을 이용하여 시각화되었다. ROC 곡선은 False Positive Rate(FPR)과 True Positive Rate(TPR)을 각각 x, y 축으로 놓은 그래프로 ROC 곡선의 밀면적인 Area Under the Curve(AUC)의 넓이가 넓을수록 분류 모델의 성능이 좋음을 나타낸다. 분류성능에 대한 ROC 곡선은 (그림 3)에서 볼 수 있다. 결과적으로 PR-FASD를 이용한 위조 얼굴 검출에 대한 Densenet-121의 분류 정확도는 97.66%로 매우 뛰어났다. 비교를 위해 추가적으로 수행한 SVM 모델의 정확도는 92.26%로 비교적 저조한 성능을 보

였다. Densenet-121 모델은 concatenation을 통해 이미지의 저수준 특징을 깊은 layer까지 보존 가능한 구조를 가지고 있다. 이는 고수준 특징만 사용되고 나머지는 버려졌던 기존 모델들과는 다르게, 저수준 특징까지도 분류 과정에 사용한다. 따라서 기존 방식보다 위조 얼굴 검출에 있어서 유효성을 가진다고 할 수 있다.

<표 1> DenseNet-121 분류 성능 결과

구분	HTER	EER
PR-FASD	2.34	2.85



(그림 3) DenseNet-121 모델의 ROC 곡선.

추후, Densenet-121과 더불어 이진 분류를 위해 유용하게 이용되는 신경망 모델인 Resnet-18을 이용한 위조 얼굴 분류 검출을 할 예정이다. 또한 두 모델의 결과 비교를 통해 이미지의 저수준 특징 반영이 위조 얼굴 검출 성능에 유효한 영향을 미치는가에 대한 연구를 진행할 계획이다.

참고문헌

- [1] Biggio, B., Akhtar, Z., Fumera, G., Marcialis, G. L., & Roli, F. Security evaluation of biometric authentication systems under real spoofing attacks. IET biometrics, 1(1), 11-24, 2012.
- [2] TIAN, Ye; XIANG, Shijun. Detection of video-based face spoofing using LBP and multiscale DCT. In: International Workshop on Digital Watermarking. Springer, Cham, 16-28, 2016.
- [3] MÄÄTTÄ, Jukka; HADID, Abdenour; PIETIKÄINEN, Matti. Face spoofing detection from single images using micro-texture analysis. In: 2011 international joint conference on Biometrics (IJCB). IEEE, p. 1-7, 2011.
- [4] BOK, Jin Yeong; SUH, Kun Ha; LEE, Eui Chul. Verifying the Effectiveness of New Face Spoofing DB with Capture Angle and Distance. Electronics, 9.4: 661, 2020.
- [5] HUANG, Gao, et al. Densely connected convolutional networks. In: Proceedings of the IEEE conference on computer vision and pattern recognition, 4700-4708, 2017.

기호 실행에서의 인공 지능 적용에 대한 연구: 퍼징과 취약점 탐지에서의 활용

하회리*, 안선우*, 김현준*, 백윤홍*

*서울대학교 전기,정보공학부, 반도체공동연구소

wrha@sor.snu.ac.kr, swahn@sor.snu.ac.kr, hjkim@sor.snu.ac.kr, ypaek@snu.ac.kr

A Study on the Application of Artificial Intelligence in Symbolic Execution: Usage in fuzzing and vulnerability detection

Whoi Ree Ha*, Sunwoo Ahn*, Hyunjun Kim*, Yunheung Paek*

*Dept. of Electrical and Computer Engineering and Inter-University Semiconductor Research Center
(ISRC),
Seoul National University

요 약

기호 실행 (symbolic execution)은 프로그램을 특정 상태로 구동하는 입력 값을 찾는 코드 분석 기법이다. 이를 사용하면 자동화 소프트웨어 테스트 기법인 퍼징 (fuzzing)을 훨씬 효율적으로 사용하여 더 많은 보안 취약점을 찾을 수 있지만, 기호 실행의 한계점으로 인하여 쉽게 적용할 수 없었다. 이를 해결하기 위해 인공 지능을 활용한 방법을 소개하겠다.

1. 서론

기호 실행(symbolic execution)은 프로그램을 특정 상태로 구동하는 입력 값에 대한 이유를 나타내는 코드 분석 기법이다 [1]. 프로그램의 경로를 따라 연산을 수행하고 분석하여 특정 경로에 대한 제약 조건(symbolic path constraints)을 수집한다. 특정 경로에 대한 제약 조건을 취득하면, 역으로 그 조건들을 풀어, 해당 경로를 위한 입력 값 생성도 가능하기 때문에 소프트웨어 테스트 툴로 각광 받고 있다.

기호 실행으로 생성된 입력 값을 seed로 삼으면 특정 경로를 꾸준히 반복 실행하여 분석할 수 있다. 또한 제약 조건들을 분석하여 다양한 경로 및 상태에 대한 도달 가능성을 확인할 수 있으며, 실행 공간을 효율적으로 검색할 수 있다. 이런 특성들 때문에 자동화 소프트웨어 테스트 기법인 퍼징에 자주 사용되어 왔다 [2].

2. 퍼징 (Fuzzing)

퍼징은 소프트웨어 버그를 찾기 위해 자주 사용되는 기술이다. 퍼징에서는 무작위 테스트 입력을 생성하고 이 입력 값을 사용하여 프로그램을 실행한다. 이를 통해 해당 프로그램의 잠재적인 보안 취약점을 찾는다 [3].

이론적으로 퍼징은 주어진 시간 내에 발견된 취약점의 수를 최대화하는 프로그램 입력을 찾는 최적화 문제이다. 하지만 보안 취약점은 불연속적으로 분포되어 있기 때문에, 퍼징으로 최대한 많은 양의 코드를 실행하여 코드 커버리지(code coverage)를 최대화하는 것을 목적으로 한다. 따라서, 다양한 경로에 도달할 수 있는 제약 조건과 입력 값을 찾을 수 있는 기호 실행을 사용하면 퍼징을 훨씬 효율적으로 활용할 수 있다.[4]

3. 기호 실행의 문제점

기호 실행은 강력한 기술이지만 실제 적용 가능성에는 많은 제약이 있다. 첫번째로, 화이트 박스 형식을 취하기에 코드에 대한 액세스가 필요하다. 코드를 완전히 분석하기 위해서 해당 코드의 언어도 이해해야 함으로 특정 언어만 인식할 수 있다. 따라서 다른 언어로 제작된 프로그램이나 코드가 주어지지 않은 경우에 적용할 수 없다.

두번째로, 기호 제약 조건(symbolic path constraints)을 효율적으로 풀 수 없는 경우가 빈번하다. 기호 실행 프로그램은 기호 제약 조건을 풀 때, SAT/SMT solver를 사용하는데, 이들은 명확한 한계점을 가지고 있다. 예를 들어, 비선형 조건에 대해서 기존 solver를 적용하면 굉장히 느리고 문제점이 많다 [5]. 또한 string에

대해서도 정확한 처리를 하지 못한다 [6].

세번째로, 기호 변수(symbolic variable)에 대한 가능 경로가 너무 많아지는 path explosion의 경우, 정확한 기호 제약 조건을 추론하지 못한다. Path explosion은 기호 실행할 때, 실행 공간이 기하급수적으로 커지는 경우를 말한다 [7].

아래 <그림 1>의 코드와 같은 경우, input의 각 byte가 'B'가 맞는지 아닌지에 대해서 경로가 존재하기 때문에 총 2^{100} 가능한 실행 경로가 생성된다. 따라서 이 모든 경로에 대한 제약 조건을 생성하는데 메모리가 부족하거나 너무 오랜 시간이 걸린다.

<그림 1> path explosion의 예제 코드[8]

```
1 int counter = 0, values = 0;
2 for ( i = 0 ; i < 100 ; i ++ ) {
3     if (input[i] == 'B') {
4         counter ++;
5         values += 2;
6     } }
7 if (counter == 75) bug ();
```

4. 인공 지능의 적용 및 성능 지표

위와 같은 기호 실행의 문제점들을 해결하기 위해 인공 지능을 활용할 수 있다. 인공 지능은 기호 실행으로 추론하기 어려운 기호 제약 조건의 관계를 학습하여 상호 보완적인 기능을 할 수 있다 [9].

I. Preprocessing

기호 실행을 하기에 앞서 정적 분석을 통해 프로그램 코드에서 보안 취약점 (candidate vulnerability points, CVP)이 될 수 있는 지점들을 확인한다. 이 경우는 divide-by-zero나 buffer overflow를 일으킬 수 있는 모든 코드에 해당한다.

<그림 2> CVP 예제 [9]

```
max = psf_calc_signal_max (infile);
while (readcount > 0) {
    readcount = sf_readf_double(infile, data, frames);
    for (k = 0; k < readcount; k++)
        data[k] /= max; // potential divide-by-zero
```

II. Design

CVP를 찾은 후, 기호 실행을 사용하다 위에서 언급된 문제점으로 인해 효율적이지 않은 상황이 오면 그 시점부터 인공 지능을 활용하여 제약 조건을 찾고 푸는 방식이다. 기호 실행이 효율적이지 않은 상황은 총 4가지로 나눌 수 있다. (1) 같은 루프에서 빠져나가지 못 할때; (2) path explosion이 일어나 메모리가 부족할 때; (3) 기존 solver로 제약 조건을 풀지 못 할때; (4) 코드가 주어지지 않은 외부 함수를 사용할 때. 이

4가지 상황에서는 기호 실행이 효율적이지 못하기에 인공 지능을 활용한다.

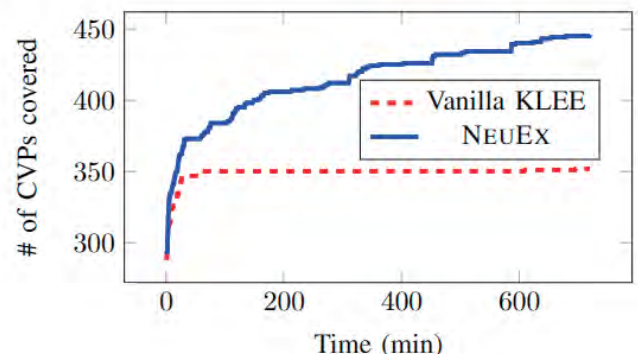
인공 지능을 사용할 때는, deep learning을 사용하여 나머지 코드 부분을 추론한다. 기호 실행이 효율적이지 못한 코드 지점까지 생성된 기호 제약 조건을 풀어 해당 지점까지의 입력을 생성한다. 이 입력 값을 randomly mutate하여 프로그램을 실행하고, CVP로 도달하는 입력 값과 CVP 지점에서의 결과 값을 모아 training data로 삼는다. 결과 값은 CVP에서 버그를 발생시킬 수 있는 변수의 값이다. <그림 2>에서는 max의 값이 결과 값이 된다. 이 training data를 사용하여 나머지 코드 부분을 추론하는 neural network를 생성한다.

이 Neural network를 사용하면 해당 CVP에서 보안 취약점이 존재하는지 확인할 수 있다. 먼저 랜덤 input을 neural network에 넣어 expected 결과 값을 확인한다. 이 결과 값과, CVP에서 bug를 trigger하는 값을 비교하여 gradient-based algorithm을 사용해 bug trigger하는 값과 가장 가까운 값을 찾는다. 예를 들면 <그림 2>에서 max 값이 0일 때, 보안 취약점이 발생한다. 따라서 neural network에서 추론하는 max 값이 0에 가장 가까운 input을 찾는 방식이다. Local minima가 존재할 수 있기 때문에 random input을 여러번 바꿔가면서 해당 neural network가 0에 도달할 수 있는지 확인한다.

III. Performance

코드 분석에 사용된 프로그램은 cURL, SQLite, libTIFF, libsndfile, BIND, Sendmail, WuFTP이다.

<그림 3> KLEE vs NeuEx [9]



<그림 3>은 기존 기호 실행 툴인 KLEE와 인공 지능을 사용한 기호 실행 툴인 NeuEx를 비교한 그래프이다. 전처리 과정에서 확인한 CVP를 NeuEx가 더 많이 확인한 것을 알 수 있다. 이는 특정 CVP 지점을 기존 기호 실행 툴로는 확인할 수 없는 반면에 NeuEx를 사용하면 기존에 확인할 수 없는 code 부분도 확인할 수 있기 때문이다.

또한 아래 <표 1>을 보면 NeuEx 를 사용하여 더 많은 보안 취약점을 찾은 것을 확인할 수 있다. 이는 NeuEx 가 더 넓은 코드 커버리지를 보장하기 때문에 더 많은 취약점을 확인한 것으로 보인다.

<표 1> KLEE vs NeuEx

	KLEE	NeuEx
발견된 보안 취약점	18	34

5. 결론

본 논문에서는 인공 지능을 적용한 기호 실행과 이를 퍼징에 활용하여 더 많은 보안 취약점을 찾아낸 방법을 소개하였다. 기호 실행은 이론적으로 굉장히 강력한 코드 분석 기법이다. 프로그램 실행 경로에 따라 제약 조건을 확인하고, 제약 조건을 solver로 풀어 해당 경로를 위한 입력 값을 생성할 수 있다. 따라서 자동화 소프트웨어 테스트 기법인 퍼징과 연계하면 더 효율적으로 잠재적 보안 취약점을 확인할 수 있다. 하지만 화이트 박스 기법인 점, 기존 solver의 한계점, 그리고 실행 공간이 너무 커지면 비효율적인 점들이 문제가 되어 실제 코드를 분석하는데 빈번히 실패한다. 또한 퍼징과 같이 사용하기도 좋지 않다. 이를 해결하는 방법으로 인공 지능을 활용한 연구는 기존 기호 실행을 진행하다 한계점에 도달하면 나머지 코드 부분을 neural network로 추론한다. 이 neural network를 사용하여 잠재적 보안 취약점이 있는지 확인할 수 있다. 이 방법은 기존 기호 실행에서 분석 실패하던 코드 부분을 분석 가능하게 하여, 더 넓은 범위의 코드에서 보안 취약점을 찾을 수 있게 하였다.

6. ACKNOWLEDGEMENT

본 연구는 2020년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행되었으며(NRF-2017R1A2A1A17069478), 2020년도 두뇌한국 21 플러스사업, 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임. (No.2018-0-00230, (IoT 총괄/1세부) IoT 디바이스 자율 신뢰보장 기술 및 글로벌 표준기반 IoT 통합보안 오픈 플랫폼 기술개발 [TrusThingz 프로젝트])

참고문헌

- [1] J. C. King, "Symbolic Execution and Program Testing," Communications of the ACM, 1976.
- [2] P. Godefroid, M. Y. Levin, D. A. Molnar et al., "Automated WhiteboxFuzz Testing," in NDSS'08.
- [3] B. Miller, L. Fredriksen, and B. So. "An empirical study of the reliability of unix utilities". Communications of the ACM, 33(12):32-44, 1990.
- [4] N. Stephens, J. Grosen, C. Salls et al., "Driller: Augmenting Fuzzing Through Selective Symbolic Execution". NDSS'16
- [5] S. Gao, S. Kong, and E. M. Clarke, "dReal: An SMT Solver for Nonlinear Theories over the Reals," in CADE'13.
- [6] Y. Zheng, X. Zhang, and V. Ganesh, "Z3-str: A Z3-Based String Solver for Web Application Analysis," in FSE'13.
- [7] C. Cadar and K. Sen, "Symbolic Execution for Software Testing: Three Decades Later," Comm of ACM'13.
- [8] T. Avgerinos, A. Rebert, S. K. Cha, and D. Brumley. "Enhancing Symbolic Execution with Veritesting," ICSE'14
- [9] S. Shiqi, S. Shinde, S. Ramesh et al. "Neuro-Symbolic Execution: Augmenting Symbolic Execution with Neural Constraints." NDSS'19

소포물 분류를 위한 그리드 타입 시스템의 강화 학습 기반 행동 제어

최호빈*, 김주봉*, 황규영*, 한연희*[†]

*한국기술교육대학교 컴퓨터공학과

{chb3350, rlawnqhd, to6289, yghan}@koreatech.ac.kr

Reinforcement learning-based behavior control of a grid-type system for sorting parcels

Ho-Bin Choi*, Ju-Bong Kim*, Gyu-Young Hwang*, Youn-Hee Han*[†]

*Dept. of Computer Science Engineering, KoreaTech University

요 약

공정 데이터를 실시간으로 수집할 수 있는 스마트 팩토리의 장점을 활용하여, 일반적인 기계 학습 대신 강화 학습을 사용한다면 미리 요구되는 훈련 데이터 없이 행동 제어를 할 수 있다. 하지만, 현실 세계에서는 물리적 마모, 시간적 문제 등으로 인해 수천만 번 이상의 반복 학습이 불가능하다. 따라서, 본 논문에서는 시뮬레이터를 활용해 스마트 팩토리 분야에서 복잡한 환경 중 하나인 이송 설비에 초점을 둔 그리드 분류 시스템을 개발하고 협력적 다중 에이전트 기반의 강화 학습을 설계하여 효율적인 행동 제어가 가능함을 입증한다.

1. 서론

물류 관리 분야에서, 분류는 제품(상품, 수하물, 우편물 등)을 식별하여 특정 목적지로 전환하는 프로세스이다. 전통적인 분류기는 컨베이어를 기반으로 하여 많은 시스템에 응용되어왔다. 컨베이어 기반의 분류 시스템은 장비의 성능이나 장비끼리의 호환성 등을 중요시하였다면, 최근에는 컨베이어를 활용하여 시스템 전체의 성능을 최적화하는 다양한 분류 시스템이 연구되고 있다. 그러한 연구들은 장비들의 배치 구성이나 작업 처리 알고리즘과 관련되어 있다. 특히, 그리드 구조의 분류 시스템 연구가 활발하며 실제 상업 제품으로 사용되고 있어 실용성이 입증되었다. 그리드 구조의 분류 시스템은 전통적인 분류 시스템에 비해 더 높은 처리량을 보여주며 더 적은 공간으로 시스템을 구성할 수 있다.

본 논문에서는 Real Games사에서 제공하는 3D Simulation Software 중 스마트 팩토리 분야에 해당하는 Factory I/O를 사용하여 스마트 팩토리 분야에서 복잡한 환경 중 하나인 이송 설비에 초점을 둔 그리드 분류 시스템을 개발한다[1]. 개발한 그리드 분류 시스템의 소형 버전에 협력적 다중 에이전트 기반 강화 학습 환경을 설계하고 적용하여 복잡한

규칙 기반의 알고리즘 없이 효율적인 행동 제어가 가능함을 입증한다.

2. 개발한 시스템

그림 1은 본 연구에서 개발한 3×3개의 Chain Transfer가 그리드 구조로 중앙에 구성된 3-Grid Sortation System이다. 본 시스템은 N×N개의 Chain Transfer로 구성되는 N-Grid Sortation System의 간단한 버전이며 쉽게 확장 가능하다. 시스템의 상단과 하단에는 2N 개의 Emitter가 존재하며 좌측과 우측에는 2N 개의 Remover가 존재한다.

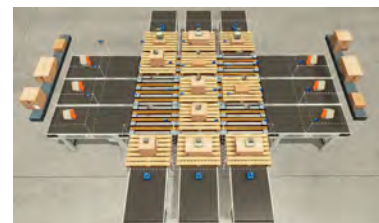


그림 1. 3-Grid Sortation System

3. 강화 학습 설계

그림 2는 본 연구에서 사용한 협력적 다중 에이전트 강화 학습 구성이다. 각 셀의 윗줄은 Factory I/O의 Parts를 나타내며 각 셀의 아랫줄은 강화 학습에서의 역할을 의미한다. D는 분류 목적지를 나타

내며, 각 Chain Transfer는 독립적인 Sorting 에이전트가 제어하고 6개의 Emitter는 하나의 Emitting 에이전트가 제어한다. 모든 에이전트는 서로 다른 CNN을 가지며, Sorting 에이전트들은 DQN 알고리즘을 사용하였고 Emitting 에이전트는 PPO 알고리즘을 사용하였다[2, 3].



그림 2. RL Configuration

3.1 Environment

본 연구에서 설정한 강화 학습의 에피소드 시나리오는 다수의 Emitter에서 분류 대기 중인 무작위 타입 500개의 상자를 타입에 맞게 올바른 목적지로 신속하게 이동 분류하는 것이다. 분류할 상자의 타입은 Small, Medium, Large로 총 세 가지가 있으며 각각의 목적지는 순서대로 D_1 , D_2 , D_3 가 된다. 최종 학습 목표는 높은 분류 정확도를 유지하며 최대한 빠르게 모든 상자를 분류하는 것이다.

3.2 State, Action, Reward

1) Sorting Agents

state로 전체 상자들의 위치와 자신의 위치를 사용한다. action은 타임 스텝마다 정지할 것인지 상자를 인접한 Chain Transfer 또는 Remover로 보낼 것인지 선택한다. reward는 분류 정확성과 충돌 여부를 고려하여 결정된다.

2) Emitting Agent

state로 전체 상자들의 위치와 Sorting Agent들의 액션 정보를 사용한다. action은 타임 스텝마다 6개의 Emitter 각각에 대해서 정지할 것인지 상자를 인접한 Sorting 에이전트에게 보낼 것인지 선택한다. reward는 emission 양, 분류량 및 충돌 여부를 고려하여 결정된다.

4. 실험

수식 1은 본 연구에서 설계한 강화 학습의 성능 평가를 위한 지표 PI (Performance Index)이며 에피소드마다 측정이 된다.

$$PI = \alpha \frac{R_{right} - R_{wrong}}{N_{destination}} + (1 - \alpha) \frac{R_{emission}}{N_{emitter}} \quad (1)$$

PI는 두 항의 합으로 이루어져 있으며 α 를 통해

두 항의 가중치를 조절한다. 첫 번째 항에 포함된 R_{right} 는 해당 에피소드에서 타임 스텝당 올바르게 분류한 상자의 수이고, R_{wrong} 은 해당 에피소드에서 타임 스텝당 올바르게 분류하지 않게 분류한 상자의 수이다. $N_{destination}$ 은 분류 목적지의 수로 정규화의 역할을 한다. 따라서, 첫 번째 항은 상자가 올바르게 분류될수록 1에 가깝고 올바르게 분류될수록 -1에 가까운 값이 계산된다. 두 번째 항에 포함된 $R_{emission}$ 은 해당 에피소드에서 타임 스텝당 6개의 Emitter가 한 Emission 횟수이다. $N_{emitter}$ 는 Emitter의 수이며 정규화의 역할을 한다. 따라서, 두 번째 항은 Emission 되는 횟수가 많을수록 1에 가깝고 적을수록 0에 가까운 값이 계산된다.

그림 3은 에피소드에 따른 PI 값의 변화 그래프를 나타내며 PI 값이 일정 기간 오르지 않으면 학습을 종료시켰다. 학습은 약 550 에피소드에서 종료되었으며 학습이 진행될수록 PI 값이 증가하는 것을 확인할 수 있다. 본 실험은 3-Grid Sortation System으로 수행한 것이기 때문에 상자들이 이동할 수 있는 버퍼가 매우 부족해 많은 제약사항이 존재한다. 따라서, Grid의 수를 늘릴수록 PI 값이 커질 것으로 사료된다.

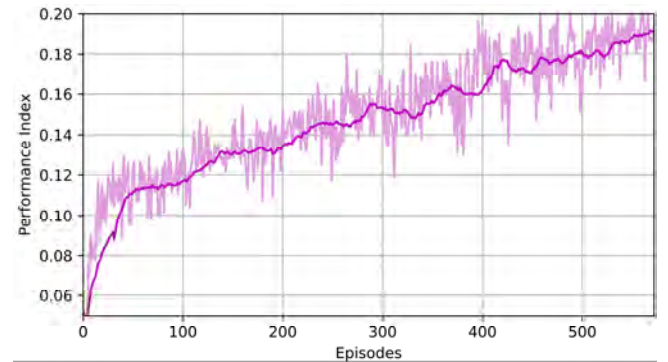


그림 3. Performance Index

ACKNOWLEDGMENT

†: 교신저자 한연희

이 논문은 2018년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. 2018R1A6A1A03025526).

참고문헌

- [1] <https://factoryio.com>.
- [2] V. Mnih, K. Kavukcuoglu, D. Silver, A. Rusu, J. Veness, M. Bellemare, A. Graves, M. Riedmiller, A. Fidjeland, G. Ostrovski, S. Petersen, C. Beattie, A. Sadik, I. Antonoglou, H. King, D. Kumaran, D. Wierstra, S. Legg, and D. Hassabis, "Human-level control through deep reinforcement learning," *Nature*, vol. 518, pp. 529–533, Feb. 2015.
- [3] John Schulman, Filip Wolski, Prafulla Dhariwal, Alec Radford, Oleg Klimov, "Proximal Policy Optimization Algorithms," *arXiv:1707.06347*, Jul. 2017.

Contextual LSTM 기반 변분 오토인코더를 이용한 이동 경로 예측

조광호*, 차재혁*

한양대학교 컴퓨터소프트웨어학과*

whrhkdghkd@hanyang.ac.kr, chajh@hanyang.ac.kr

Trajectory Prediction by Using Contextual LSTM based Variational AutoEncoder

KwangHo Cho*, JaeHyuk Cha*

Dept. of Computer Software, HanYang University*

요 약

스마트폰, GPS 장비, 위치 기반 소셜네트워크의 발달로 방대한 이동 경로 데이터 수집이 가능하게 됐다. 이를 통해 다양한 분야에서 GPS 데이터를 가지고 사람의 이동성을 분석하고 POI를 예측하는 기회가 많아졌다. 실생활에서 사람의 이동성은 다양한 상황에 영향을 받지만, 실제 GPS 데이터는 위치, 시간 정보의 수준이다. 따라서 다양한 상황을 내재하는 정보가 사람의 이동성 분석과 POI 예측에 필요하다. 본 논문에서는 POI의 순위, 사용자의 POI 활동, 카테고리 선호도 같은 맥락적 특징을 이용하여 이에 관련된 상황에 맞는 POI 시퀀스를 예측하는 Contextual LSTM 기반 딥 러닝 기법을 제안한다. Contextual LSTM은 사람의 이동성에 영향을 주는 시퀀스의 맥락적 특징을 모델에 통합하기 위해 LSTM을 확장한다. 제안된 기법은 HITS 알고리즘과 여러 제약조건 기반으로 추출한 맥락적 특징별로 딥 러닝 모델에 통합하여 각각 POI 시퀀스를 검출했으며, 다양한 맥락적 특징에 대해서 공공 데이터와 수집한 데이터로 평가하였다.

1. 서론

스마트폰, GPS 장비, 위치기반 소셜네트워크(Location Based Social Network, LBSN)의 발달로 인해 수집되는 이동 경로(trajecory) 데이터의 양이 급증하고 있다. 방대한 데이터로 인해 사용자의 이동성을 발견하고 이동 경로를 예측하는 기회가 많아졌다. 사람의 이동성 예측은 목적에 따라 사용자에게 여행 경로 추천, 지능형 교통수단, 도시 계획, 이동성 관리 등 다양한 분야에서 활용된다[1].

최근 몇 년 동안 딥 러닝 분야에서 다양하고 많은 이동 경로 예측 기법이 연구되었지만 대부분 명시적인 과거의 시간, 위치 데이터를 활용하여 사용자의 단일적인 위치 또는 맥락상 의미가 없는 임의의 이동 경로를 예측하는 경우가 많다. 따라서 다양한 상황에 큰 영향을 받는 현실 세계의 이동성과는 많이 다른 결과를 보여준다. 대부분 사용자는 지역적으로 가치가 있는 핫스팟(Hot spot)이나 사용자의 선호에 따라 상황에 맞는 예측된 이동 경로가 필요하다.

본 논문에서는 위치, 시간 정보뿐만 아니라 전체이동 경로에 적용되는 사람의 이동성에 영향을 미치는 새로운 특징 (1) 지역 POI(Point of Interest) 순위점수, (2) 활동 관련 사용자 POI 선호도, 그리고 (3) 카테고리 관련 사용자 POI 선호도를 추출하고, 이와 같은 맥락적 특징들을 통합하여 POI 시퀀스를 예측하는 Contextual LSTM 기반 딥 러닝 모델을 제안한다. 제안된 모델은 사용자의 이동 경로 데이터로부터 더욱 풍부한 정보를 인코딩하고 이를 통해 사용자의 다음 이동 경로를 예측한다. 실제로, 새로운 특징을 통합한 모델은 기존의 모델보다 우수한 예측 성능을 나타낸다. 이후 본 논문의 구성은 다음과 같다.

제2장에서는 Contextual LSTM 기반 딥 러닝 모델에 관한 용어 및 문제 정의와 선행 연구에 대해 다루고, 제3장에서는 새로운 특징들과 모델의 구성도와 각 과정에 대해 설명한다. 제4장에서는 모델에 대한 성능을 비교한다. 마지막 장에서는 결론 및 향후 연구 방향에 대해 기술한다.

2. 용어 및 문제 정의 & 관련 연구

이 장에서는 Contextual LSTM 기반 딥 러닝 모델에 관한 용어 및 문제를 정의하고, 선행 연구에 대해 소개한다.

2.1 용어 및 문제 정의

정의 1. 이동 경로(Trajectory): 각 POI를 l_i 라고 하면, POI 집합들은 $\{l_1, l_2, \dots, l_n\}$ 가 되고, 이를 이동 경로 T_i 라고 한다. 이동 경로 안의 POI들은 시간순의 연속적인 집합이다.

정의 2. 맥락 (Context): 맥락이란 현재 POI에서 다음에 올 POI에 직접적인 또는 간접적인 영향을 미치는 현재 및 이전의 시나리오(senario)를 나타낸다. 예를 들어, 이전 및 현재 장소의 시간/거리 차이, 인기도, 카테고리 등으로 고차원 벡터로 표현될 수 있다.

정의 3. 이동 경로 예측 문제(Trajectory Prediction Problem): $T_i = \{l_i^1, l_i^2, \dots, l_i^N\}$ 이라는 N개의 POI로 이루어진 이동 경로 T_i 가 주어졌을 때, 다음 이동 경로인 $T_{i+1} = \{l_{i+1}^1, l_{i+1}^2, \dots, l_{i+1}^M\}$ 를 예측한다.

2.2 관련 연구

이동 경로 예측에 대한 선행 연구로는 Wang이 제안한 [2]이 있다. [2]에서는 이동 경로 데이터의 전반적인 정보를 인코딩하기 위해 자연어 처리학술(Natural Language Processing, NLP)에 뛰어난 효과를 보여준 Long Term Short Term Memory(LSTM)[3] 순환 신경망과 Seq2Seq(Seq2Seq)[4]구조를 적용했으며, 특히 Seq2Seq를 사용하여 다중 사용자들의 전반적인 이동 경로를 예측하였지만 길이가 긴 이동 경로 입력에는 장기 의존성 문제에 대한 한계가 있었다. 이 문제를 해결하기 위해 어텐션 메커니즘[5]을 적용한 모델[6]도 제안되었다.

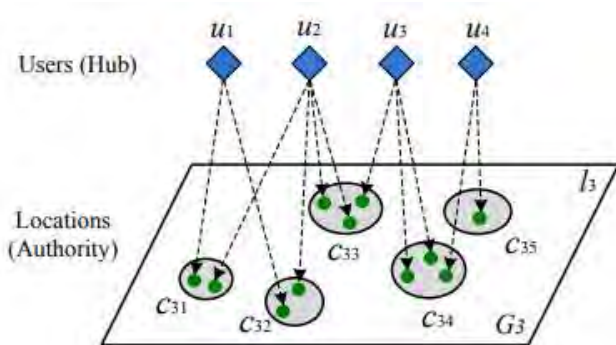
이 외에도 이동 경로 안의 각 데이터끼리의 시간 차이, 거리 차이를 나타내는 위치적 맥락 정보를 변분 오토인코더(Variational Auto Encoder, VAE)[7]를 사용하여 통합하여 인코딩하고 학습한 연구[8][9]가 있다. [8][9]에서 제안한 맥락 학습은 특정 주제에 대해 어떻게 모델링하는 것에 따라 영향력 있는 결과를 나타낼 수 있다고 했다.

3. 제안 기법

3.1 특징점(Features)

이동 경로 데이터로부터 사람의 이동성에 영향을 미치는 3가지 특징을 추출했고, 추출한 특징별로 모델에 통합하여 학습하였다.

3.1.1 지역 POI 순위 점수(Authority of POI): 실제로 위치 예측은 특정 지역의 크기 단위로 행해지는 경우가 대부분이다. 특정 지역이라는 공간에 관해 사람들마다 지식의 정도가 다르며, 또한 POI들의 인기도 또한 다르다. 게다가 그 지역의 경험이 많은 사람이 특정 POI에 가는 것이 더 큰 영향을 미칠 수 있다. 즉, 사람들의 특정 지역에 대한 지식과 그 지역의 POI들의 흥미도는 상호증강 관계를 가진다. 그래서 우리는 그래프 기반 랭킹 알고리즘인 HITS 알고리즘[10]을 사용하여 Authority 점수를 구한다. 단순히 모든 사용자들의 특정 지역의 POI에 대한 방문 횟수와 빈도수로 POI의 인기를 결정하는 게 아니라 특정 지역의 여행 경험이 많은 사람의 방문 횟수와 빈도수에 더욱 영향을 받은 POI들의 순위 점수를 구한다. 그림1은 특정 지역에 대한 POI들(Authorities)과 사용자들(Hubs)의 관계를 나타낸다.



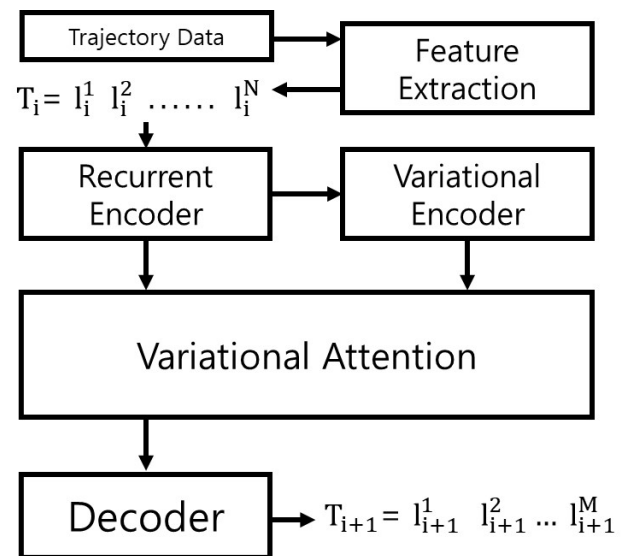
(그림 1) Authority와 Hub의 관계.

3.1.2 개인별 POI 카테고리 선호도 점수(Preference score of POI Category): [11]에서 제안한 특징으로, 각 POI의 평균 체류 시간과 횟수, 해당 POI와 같은 카테고리의 POI들의 평균 체류 시간과 횟수, 그리고 제약조건(거리, 시간)을 이용하여 사용자의 POI에 대한 개인적인 카테고리 선호도 점수를 구한다.

3.1.3 개인별 POI 활동 선호도 점수(Activity score of POI Activity): 개인별 POI 카테고리 선호도 점수와 마찬가지로 사용자가 각 POI에서 한 활동에 대해서 평균 체류 시간과 횟수와 제약조건을 이용하여 사용자의 POI에 대한 활동 선호도 점수를 구한다.

3.2 시스템 설계

아래 그림 2는 현재 순간까지의 이동 경로 데이터로부터 다음 이동 경로를 예측하기 위한 모델의 구성도이다. 최근 자연어 처리 학습에 큰 효과를 보여준 인코더-디코더 구조의 변분 오토인코더(VAE) 모델을 사용했으며, 긴 입력 시퀀스에 대한 장기 의존성 문제를 해결하기 위해 어텐션 메커니즘을 적용했다. 각 인코더, 디코더는 LSTM 순환 신경망으로 이루어져 있다.



(그림 2) 제안 모델 구조.

구체적으로 설명하면, 사용자들의 이동 경로 데이터로부터 위치 정보뿐만 아니라 사람의 이동성에 영향을 미치는 새로운 특징점을 파악하기 위한 특징 추출(Feature Extraction)이 요구된다. 추출된 특징은 지역의 POI 순위 점수, POI 활동 선호도 점수, POI 카테고리 선호도 점수이며, 이 특징들은 모델의 입력이 될 이동 경로 데이터에 매핑(Mapping)된다. 순환 인코더(Recurrent Encoder)는 입력 시퀀스로부터 각 순간의 은닉 상태(hidden state)를 추출하고, 이동 경로 데이터의 맥락적인 정보를 통합하여 전반적인 정보를 나타내는 컨텍스트 벡터(context vector)를 인코딩한다. 다음으로, 변분 인코더(Variational Encoder)는 앞에서 구한 컨텍스트 벡터를 확률 분포인 잠재변수(latent variable)로 변환한다. 동시에, 순환 인코더의 각 순간의 은닉 상태에서 어텐션 벡터(attention vector)를 추출하고 마찬가지로 확률 분포인 잠재변수로 변환한다. 마지막으로, 디코더(Decoder)는 두 개의 잠재변수를 사용하여 다음에 올 가장 확률이 높은 이동 경로를 생성한다.

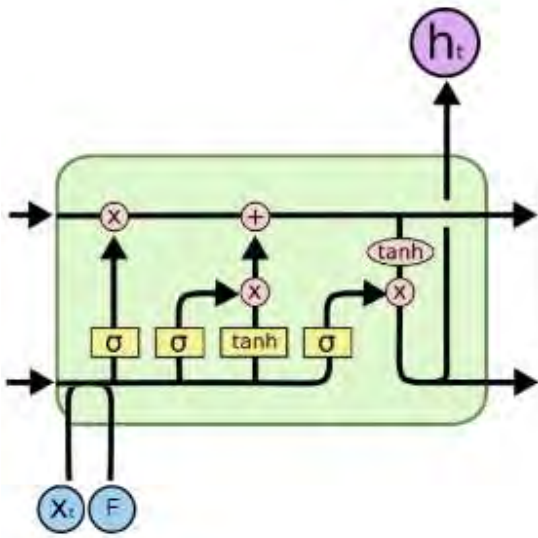
3.3 이동 경로 맥락 인코딩(Trajectory Context Encoding)

3.2.2 Recurrent Trajectory Encoder

순환 인코더는 양방향 LSTM[12] 순환 신경망으로 구성되어 있다. 양방향 은닉층의 결합에 의해 POI의 은닉 상태를 얻을 수 있다. 이동 경로의 맥락적인 정보들을 은닉

상태에 통합하는 것이 사용자의 이동성을 표현하는데 훨씬 도움이 된다. 그러나, 기본적인 LSTM(Vanilla LSTM)은 POI와 관련된 맥락적인 정보를 처리하는데 적합하지 않기 때문에 확장된 LSTM을 제안한다. 그림3은 새롭게 확장된 LSTM 구조이다. LSTM의 메모리 셀 내/외부부의 정보 흐름을 조절하는 기존의 입력/출력/망각 게이트 안에 추출한 특징 벡터를 추가하여 Contextual LSTM으로 확장한다. 식1은 확장된 LSTM 게이트의 동작 식이다.

확장된 LSTM은 순간마다 이전 순간의 POI와 다음 순간의 POI의 정보를 포함하고 있는 은닉 상태를 추출하고, 마지막 순간의 은닉 상태를 이동 경로 데이터의 맥락적인 정보를 통합하여 전반적인 정보를 나타내는 고정된 크기의 하나의 컨텍스트 벡터(context vector) c 로 인코딩한다.



(그림 3) 확장된 LSTM 구조.

$$\begin{aligned} i_t &= \sigma(W_i x_t + U_i h_{t-1} + V_i F + b_i) \\ f_t &= \sigma(W_f x_t + U_f h_{t-1} + V_f F + b_f) \\ o_t &= \sigma(W_o x_t + U_o h_{t-1} + V_o F + b_o) \\ c_t &= f_t \odot c_{t-1} + i_t \odot \sigma(W_c x_t + U_c h_{t-1} + V_c F + b_c) \\ h_t &= o_t \odot \tanh(c_t) \end{aligned}$$

(식 1) 확장된 LSTM의 게이트 동작 식.

3.2.3 Variational Trajectory Encoder

변분 인코더를 앞에서 구한 고정된 컨텍스트 벡터를 확률 분포인 잠재변수 z 로 인코딩하는 데 사용한다. 생성된 잠재변수는 랜덤 샘플(Random Sample)을 사용하여 디코더에서 다양한 데이터를 재구성할 수 있다[7].

3.2.4 Variational Attention

일반적인 어텐션 메커니즘은 입력 시퀀스와 정답 시퀀스에 대한 정렬 관계를 자동으로 학습한다. 구체적으로, 입력 시퀀스의 모든 순간마다 해당 순간의 정답과 어느 정도 관련이 있는지 확률 값을 계산하고, 계산된 확률 값을 각 입력 시퀀스의 은닉 상태에 가중치 합해주어 어텐션 벡터를 구한다[5]. 어텐션 벡터 또한 컨텍스트 잠재 변수와 마찬가지로 확률 분포인 잠재변수로 인코딩한 후 디코더로 전달된다.

3.2.5 Trajectory Decoders

위에서 언급하였듯이, 디코더는 현재 이동 경로가 주어졌을 때, 어텐션 잠재변수 c 와 컨텍스트 잠재변수 z 를 이용하여 다음에 올 이동 경로를 예측한다. 두 잠재변수와 이전 순간 디코더 은닉 상태를 사용하여 다음에 오는 POI를 예측하고 식2의 조건부 확률 식이 최대화되도록 학습한다.

$$p(\{l_{i+1}^1, l_{i+1}^2, \dots, l_{i+1}^M\}) = \prod_{t=1}^M p(l_{i+1}^t | l_{i+1}^{<t}, c, z)$$

(식 2) 디코더의 조건부 확률 식.

4. 평가

이 섹션에서는 이동 경로 예측 문제에 대한 데이터셋, BaseLine, 평가 메트릭, 실험결과에 대해 설명한다.

4.1 데이터 셋

본 논문에서 구하려는 이동 경로의 새로운 맥락적 특징 추출과 관련 있는 속성을 가지고 있고 잘 정리된 특정 지역의 이동 경로 데이터를 사용하여 평가했다: Weeplaces 공공 데이터, 서울시 성동구 데이터

Weeplaces[13] 데이터는 위치 기반 소셜네트워크 Weeplaces에서 제공한 오픈 데이터로서, 15,799명의 사용자가 등록한 위치 정보가 수집되었으며, 7,658,368개의 체크인 위치가 포함되어 있다. 각 장소의 카테고리가 10개로 분류되었으며, 장소에서 한 활동을 96개로 분류했다.

서울시 성동구 데이터는 위치수집 앱인 트래카(Traccar)[14]를 사용해서 2주 기간의 성동구 주변 사람들의 위치를 수집한 데이터이다. 각 장소의 카테고리를 9개로 분류했다.

모든 데이터 셋에 대해서, 훈련을 위해 90%를 무작위 선택하여 훈련데이터로 사용하고, 나머지 10%는 테스트 데이터로 사용하였다.

4.2 BaseLines

본 논문에서는 예측한 이동 경로의 정확성과 방문순서의 타당성을 측정하기 위해 두 가지 메트릭(Metrics)을 사용하여 평가하고, 각 특징별로 통합한 제안된 모델과 기존의 이동 경로 예측 모델들과 비교 한다.

VAE(Variational AutoEncoder): 인코더-디코더로부터 생성되는 데이터의 확률 분포를 잠재변수로 생성하고 학습하는 모델

VAE with Attention: VAE 모델에 어텐션 메커니즘을 적용한 모델

CATHI[9]: VAE를 사용하여 POI의 시간/거리 차이만 맥락적 특징으로 통합하여 학습하는 예측 모델.

위의 2개의 모델은 기존의 LSTM을 그대로 사용한 모델들이고, **CATHI**는 LSTM을 확장하여 맥락적 특징을 통합한 모델이다.

4.3 Metrics.

우리는 F1 점수(F1 score)와 pairs-F1 점수(pairs-F1 score)[15]를 사용하여 이동 경로 예측을 평가했습니다. F1 점수는 예측된 이동 경로의 POI들이 실제 이동 경로의 POI들과 적합한지에 대한 점수를 나타내고, pairs-F1 점수는 이동 경로의 POI 순서가 적합한지를 확인한다. pairs-F1 점수는 순서대로 POI들의 쌍의 F1 점수를 사용해서 계산한다. 다음 식3은 pairs-F1을 구하는 식으로, P_{pairs} 와 R_{pairs} 는 순서대로 POI 쌍들의 정밀도(Precision)

와 재현율(Recall)을 나타낸다.

$$pairs - F_1 = \frac{2P_{pair}R_{pair}}{P_{pair} + R_{pair}}$$

(식 3) pairs-F1 식

4.4 실험 결과

전반적인 성능

< 표1 > Baseline과 제안 모델 실험 결과

		Trajectory Prediction	
Methods		F1	Pairs-F1
We replace	VAE	0.599±0.174	0.347±0.209
	VAE+Att	0.624±0.159	0.365±0.166
	CATHI	0.749±0.123	0.473±0.150
	Our Model (Feature1)	0.790±0.108	0.485±0.138
	Our Model (Feature2)	0.862±0.087	0.615±0.105
	Our Model (Feature3)	0.829±0.098	0.560±0.117
성동구 위치 데이터	VAE	0.409±0.143	0.223±0.342
	VAE+Att	0.420±0.122	0.248±0.304
	CATHI	0.557±0.102	0.358±0.209
	Our Model (Feature1)	0.621±0.094	0.365±0.166
	Our Model (Feature2)	0.653±0.087	0.473±0.130

다음 표 1은 각 데이터에 대한 예측 결과의 F1 점수와 pairs-F1 점수입니다. 논문에서 제안된 모델들은 확장한 Contextual LSTM 기반 VAE모델에 각각 특징1(POI 순위), 특징2(POI 선호도(카테고리)), 특징3(POI 선호도(활동))을 통합한 것이다. F1, pairs-F1 점수 측면에서 전반적으로 모든 Baseline보다 맥락적 특징을 통합한 모델이 그렇지 않은 모델에 비해 성능이 크게 개선된 것을 볼 수 있다. 기존 VAE보다 어텐션 메커니즘을 적용한 VAE가 좀 더 우수한 성능을 보이고, 시간/거리 차이만 맥락적 특징으로 통합하여 학습시킨 CATHI는 더욱 향상이 되었다. 즉, 제안된 모델의 맥락적인 정보 인코딩이 이동 경로의 정보를 잘 내재하며, 예측에 큰 영향을 미친다는 뜻이며, 우리가 추가로 넣은 새로운 맥락적 정보 중 사용자 POI 선호도(카테고리) 특징2가 사용자의 이동성에 가장 큰 영향을 미친다는 것을 알 수 있다. 이유는 특징1(Authority 점수)은 사람들의 특정 지역 POI의 방문 수를 기반으로 구한 것으로, 개인화 측면보다는 전반적인 관계를 나타내고 특징2(사용자 POI 선호도(카테고리)), 특징3(사용자 POI 선호도(활동))은 개인에 관한 POI의 선호도를 구한 것으로 이동 경로를 예측하는 각 사용자 별 이동성을 효율적으로 모델링한다.

이 평가 결과는 어텐션 메커니즘이 인코더-디코더 구조 모델을 향상시키는데 기여를 하며, LSTM의 확장에 대한 주장을 뒷받침하며 맥락적 특징을 통합한 LSTM의 변형이 사람의 이동성 모델링에 효율적이고, 개인별 이동성을 내재하는 맥락적 특징들이 이동 경로 예측에 큰 영향을 미친다는 것을 알 수 있다.

또한, 제안한 모델이 다른 방법에 비해 표준편차의 값이 낮은 것을 보았을 때, 더 안정적이라는 걸 알 수 있다.

5. 결론 및 미래 연구

본 논문에서는 맥락적 정보에 의존하고, 추출한 새로운 특징을 확장된 Contextual LSTM 기반 딥러닝 모델에 통합했다. 두 개의 데이터 셋으로 제안된 모델을 평가하고 맥락적인 정보를 통합하는 것이 사람의 이동성을 표현하는 데 도움이 될 것을 보여준다. 제안된 모델은 더 큰 데이터 셋에서 약간 더 나은 성능을 보였다. 그리고 HITS 알고리즘, POI 선호도 식을 사용해서 얻은 새로운 특징들은 이동 경로 데이터를 나타내는 데 좋은 지침이라는 것을 보여주며, 새롭게 확장한 LSTM으로 더 유의미한 정보를 내재한 컨텍스트 벡터를 제공한다는 걸 보여준다. 이동 경로 데이터로부터 추출할 수 있는 흥미로운 맥락적 특징은 많이 있다. 앞으로 사용자의 선호도 및 장소의 인기도를 정의하기 위해 텍스트 정보(예: 태그, 팁 및 리뷰)와 시각적 정보(예: 장소 사진) 또한 통합해보려고 한다.

사사

이 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.2018R1A5A7059549).

참고문헌

- [1] Z. Kai, S. Tarkoma, S. Liu, and H. Vo, "Urban human mobility data mining: An overview," in Proc. IEEE Int. Conf. Big Data, Dec. 2017, pp. 1911 - 1920.
- [2] W. Chujie, M. Lin, and H. Zhang, "Exploring Trajectory Prediction Through Machine Learning Methods" in IEEE Access, July. 2019, pp.101441 - 101452.
- [3] Sepp Hochreiter, Jürgen Schmidhuber, "Long short-term memory". Neural Computation. 9 (8), 1997, 1735 - 1780.
- [4] Kyunghyun Cho, Bart van Merriënboer, Dzmitry Bahdanau and Yoshua Bengio, "Learning Phrase Representations using RNN Encoder-Decoder for Statistical Machine Translation" in EMNLP, Jun 2014.
- [5] Dzmitry Bahdanau, Kyunghyun Cho and Yoshua Bengio, "Neural Machine Translation by Jointly Learning to Align and Translate" in ICLR, 2015.
- [6] Jie Feng, Yong Li, Chao Zhang, Funing Sun, Fanchao Meng, Ang Guo, and Depeng Jin, "DeepMove: Predicting Human Mobility with Attentional Recurrent Networks". In WWW, 2018.
- [7] Diederik P. Kingma and Max Welling, "Auto-Encoding Variational Bayes", in cs.LG, May 2014.
- [8] Jarana Manotumruksa, Craig Macdonald, and Iadh Ounis, "A Contextual Attention Recurrent Architecture for Context-Aware Venue Recommendation", In SIGIR. 2018.
- [9] Fan Zhou, Xiaoli Yue and Goce Trajcevski, "Context-aware Variational Trajectory Encoding and Human Mobility Inference", in WWW, May 2019.
- [10] Christopher D. Manning, Prabhakar Raghavan & Hinrich Schütze, "Introduction to Information Retrieval". Cambridge University Press. Retrieved, 2008.
- [11] Ramesh Baral, Tao Li, XiaoLong Zhu, "CAPS: Context Aware Personalized POI Sequence Recommender System", in Information Retrieval (cs.IR), Mar 2018.
- [12] Schuster, Mike, and Kuldeep K. Paliwal. "Bidirectional recurrent neural networks." Signal Processing, IEEE Transactions, 1997, 2673-2681.
- [13] X. Liu, Y. Liu, K. Aberer, C. Miao, "Personalized point-of-interest recommendation by mining users' preference transition", in CIKM, 2013, pp.733 - 738.
- [14] <https://www.traccar.org/documentation/Traccar>, Traccar Documentation.
- [15] Dawei Chen, Cheng Soon Ong, Lexing Xie, "Learning Points and Routes to Recommend Trajectories", in CIKM '16, 2016.

분류 복잡도를 활용한 오버 샘플링 비율 산출 알고리즘 개발

이도현*, 김경옥**

*서울과학기술대학교 데이터사이언스학과

**서울과학기술대학교 산업공학과

e-mail: skypo1000@ds.seoultech.ac.kr,

kyoungok.kim@seoultech.ac.kr

A Study on Calculating Over-sampling Ratio using Classification Complexity

Do-Hyeon Lee*, Kyoungok Kim**

*Dept. of Data Science, Seoul National University of Science and Technology

**Dept. of Industrial and Information Systems Engineering, Seoul National University of Science and Technology

요 약

불균형 데이터는 범주에 따른 데이터의 분포가 불균형한 데이터를 의미한다. 이런 데이터를 활용해 기존 분류 알고리즘으로 분류기를 학습하면 성능이 저하되는 문제가 발생한다. 오버 샘플링은 이를 해결하기 위한 기법 중 하나로 수가 적은 범주[이하 소수 범주]에 속한 데이터 수를 임의로 증가시킨다. 기존 연구들에서는 수가 많은 범주[이하 다수 범주]에 속한 데이터 수와 동일한 크기만큼 증가시키는 경우가 많다. 이는 증가시키는 샘플의 수를 결정할 때 범주 간 데이터 수 비율만 고려한 것이다. 그런데 데이터가 동일한 수준의 불균형 정도를 갖더라도 범주별 데이터 분포에 따라서 분류 복잡도가 다르며, 경우에 따라 데이터 분포에서 존재하는 불균형 정도를 완전히 해소하지 않아도 된다. 이에 본 논문은 분류 복잡도를 활용해 데이터 셋 별 적정 오버 샘플링 비율을 산출하는 알고리즘을 제안한다.

1. 서론

불균형 데이터는 범주에 따른 데이터의 분포가 불균형한 데이터를 뜻한다. 대부분의 분류 알고리즘은 범주 간 데이터의 수가 균형을 이룰 때 좋은 성능을 낼 수 있기 때문에 범주가 불균형한 분포를 가지는 데이터로 분류 알고리즘을 학습한 경우 해당 분류기의 성능이 저하된다. 그렇지만, 사기 감지, 질병 진단 등을 위한 많은 데이터들이 실제로 데이터의 수가 적은 소수 범주와 데이터 수가 많은 다수 범주로 이뤄진 사례가 많다. 이에 불균형 데이터에서도 높은 성능의 분류기를 학습할 수 있는 많은 연구가 진행되었다.

대표적으로 오버 샘플링은 수가 적은 범주에 속한 데이터 수를 임의로 증가시키며, 앙상블은 여러 개의 분류 모델을 학습시켜 이들을 종합적으로 활용하는 방식으로 불균형 정도를 해소한다. 최근에는 이들을 결합하는 연구들이 진행되었다. 대표적으로 Boosting에 오버 샘플링을 적용한 알고리즘을 예로 들 수 있다[1],[2],[3]. 매 약한 학습기 학습 시 이들의 입력 데이터에서 소수 범주에 속한 샘플 수를 증

가시켜 매 학습에서 성능 개선이 가능하다.

그런데 오버 샘플링 시 사용자는 소수 범주에 속한 데이터 수를 얼마나 늘릴지를 결정해야 한다. 기존의 연구들은 주로 다수 범주에 속하는 데이터 수와 동일하도록 그 수를 조절 한다[1],[2],[3],[6]. 즉, 이것은 다수 범주와 소수 범주 사이의 비율을 이용해서 오버 샘플링 비율을 결정하는 것이다.

그러나 동일한 데이터 수 불균형 정도를 갖는 데이터라도 서로 다른 분류 복잡도를 가지게 되고, 최종 분류기의 성능 또한 달라질 수 있다. 특히 Boosting에 오버 샘플링을 적용한 알고리즘의 경우 학습 시간에도 영향을 끼칠 수 있다.

앙상블 계열 기법에서는 이미 두 범주 간 데이터 분포가 꼭 완전 균형을 이루지 않아도 됨을 증명 한 바 있다[4].

이를 반영하여 본 논문에서는 불균형 정도와 분류 복잡도를 고려해, 완전 균형 상태보다 좋은 성능을 내지만 낮은 수준의 오버 샘플링 비율을 산출하는 알고리즘을 제시한다. 추가적으로 분류 복잡도를 구성하는 요인 간 비교 실험을 통해 더 나은 요인을

탐색한다.

2. 관련연구

2.1 불균형 데이터 문제 해결을 위한 연구

불균형 데이터 문제 해결을 위해 제안된 방법론들은 전체적으로 전처리, 알고리즘 및 앙상블 기법으로 구분할 수 있다[6]. 전처리 기법은 임의로 각 범주에 속하는 데이터 수를 조정한다. 알고리즘 기법은 수가 극단적으로 적은 범주의 데이터를 올바르게 분류하도록 cost를 의도적으로 부여한다. 앙상블 기법에서는 여러 개의 분류 모델을 학습시켜 이들의 결과를 종합적으로 활용한다.

오버 샘플링은 전처리 기법 중 하나로, 소수 범주에 속한 데이터 수를 임의로 증가시켜 데이터 불균형 정도를 해소한다. 최근에는 이를 알고리즘 및 앙상블 단계에서 제안된 기법들과 결합하여 사용하는 연구가 진행되었다. 대표적으로 Boosting에 이를 적용한 알고리즘을 예로 들 수 있다.

앙상블 알고리즘 중 하나인 Boosting 알고리즘은 순차적으로 약한 학습자를 학습시키고, 이들의 결과를 결합하여 강한 학습자를 얻는다. 이 과정에서 오버 샘플링을 적용시키면 매 약한 학습자를 학습시킬 때마다 입력 데이터의 불균형을 해소하여 분류기의 성능 개선이 종합적으로 발생할 수 있다.

2.2 분류복잡도

분류 복잡도는 범주별 데이터들의 변수 분포에 따라 분류 경계가 명확한 정도를 의미한다[5]. 일반적으로 분류 모형은 학습을 통해 서로 다른 범주를 구분할 기준이 되는 분류 경계선을 생성한다. 이는 범주별 일종의 구역 할당을 의미하며, 분명하고 명확할수록, 기대 성능은 높아질 수 있다.

이들은 주로 근접 이웃을 통해 설정한 지역 내에서의 동일 범주 간 데이터 분포 밀도 정보 및 개별 변수 특성을 활용하여 표현할 수 있다.

근접 이웃을 사용한 지표는 대표적으로 *cohesion* (응집도)[7]와 *noise* (이상도)[8]가 있다. *cohesion*은 k 개의 근접 이웃 중 같은 범주에 속한 경우의 확률적 표현이다. 이는 동일 범주 데이터의 분포 밀도를 의미한다. 따라서 최종 산출 분류 복잡도와 역비례 관계를 가진다. 이는 T_1 으로 표기하며 수식 (1)로 정의된다. 추가적으로 다수 범주는 N , 다수범주 데이터 수는 n , 소수 범주는 P , 소수범주 데이터 수는 p , 각 데이터별로 활용할 근접 이웃의 수는 k 로 표

기한다.

$$T_1 = 1 - \frac{1}{n, k} \sum_{x \in P} \sum_{r=1}^k I_r(x, S = P \cup N) \quad (1)$$

$$I_r(x, S) = \begin{cases} 1, & \text{if } x \in P \text{ and } NN_r(x, S) \in P \\ 0 & \text{otherwise} \end{cases} \quad (2)$$

범주별 개별 변수 특성을 이용하는 지표는 변수별 정보를 활용하여 범주별 데이터 분포를 측정한다. 개별 변수 별로 측정 후, 대표 값을 선정한다. 대표적으로 Fisher's Discriminant Ratio(이하 $f1$)와 Feature Efficiency가 있다[5].

$f1$ 은 범주 별 구별 가능성을 측정한다. 이는 수식 (4)로 정의 되며, 범주별 분산 합의 제곱 대비 범주별 평균의 차이의 제곱의 비율을 의미한다[5]. 범주별 평균의 차이는 범주 간 구별 가능성, 분산 합은 데이터 산포도 정도를 의미한다. $f1$ 에 기반을 둔 분류 복잡도 T_2 는 수식 (3)으로 정의된다. 변수 수는 Z , 개별 변수의 $f1$ 은 $f1_z$, 개별 범주에서의 소수 범주 및 다수 범주 평균과 표준 편차는 각각 μ_{P_i} , μ_{N_i} , σ_{P_i} , σ_{N_i} 로 표기한다.

$$T_2 = \frac{1}{1 + \max(f1_z)} \quad (3)$$

$$f1_z = \frac{(\mu_{P_i} - \mu_{N_i})^2}{(\sigma_{P_i})^2 + (\sigma_{N_i})^2} \quad (4)$$

$f2$ 는 개별 변수에서의 범주별 최솟값 중 최댓값과 최댓값 중 최솟값 사이에 모든 범주 데이터 셋의 개수를 측정한다[5]. 이는 데이터의 중첩의 정도를 나타낸다. 높은 중첩의 정도는 범주별 뚜렷한 구분 없이 데이터가 분포됨을 의미한다. 대표 $f2$ 은 개별 변수들의 $f2$ 평균값으로 선정한다.

3. 제안 알고리즘

3.1 용어정의

불균형 정도란 소수범주 대비 다수범주 데이터 수의 비율을 의미한다. 오버샘플링 비율(O_r)이란 오버샘플링을 통해 달성하고자 하는 다수범주 대비 소수범주 데이터 수의 비율을 의미한다. O_r 이 1일 때, 데이터의 분포가 균형 함을 의미한다.

3.2 분류복잡도 요인 선정

데이터 밀도 정보 및 개별 변수 별 특성을 반영하는 요인을 하나씩 선정한다. 전자는 데이터 간 분포 밀도를 반영하므로, 전체 변수 정보를 모두 고려하는 반면. 후자는 특정 변수에서의 데이터 분포를 고려한다. 이를 통해 다른 성격의 분류 복잡도 요인

간 비교가 용이해진다. 이들은 모두 아래 수식에서 T 로 표기한다.

3.2 알고리즘 설계

기본적으로 알고리즘을 통해 산출되는 오버 샘플링 비율(O_r)은 앞서 구한 분류 복잡도와 비례 관계를 가지므로 T 로 나타낸다. 단 산출된 오버 샘플링 비율을 적용했을 때, 소수 범주의 최종 크기가 기존 보다 작으면 이를 기존 소수 범주 크기가 되도록 조정했다. 이는 수식 (5)으로 정의된다.

$$O_r = \begin{cases} T, & \text{if } T > \frac{p}{n} \\ \frac{p}{n} & \text{otherwise} \end{cases} \quad (5)$$

4. 실험

4.1 실험 데이터

본 실험에서는 “UCI Machine Learning Repository”에서 공개된 불균형 데이터 셋들을 사용하였다. 이들의 특성은 표 1.에 정리되어 있다. 특히 다중 분류 데이터는 기존 연구들과 동일하게 소수 범주 선정 후, 데이터 명의 괄호 안에 표기하였다. 오버샘플링 및 분류학습 시 범주형 독립변수는 제외하였다.

4.2 실험설계

<표 1> 데이터 셋 특성 요약

데이터명 (소수범주명)	다수범주 데이터수	소수범주 데이터수	변수 수	불균형 정도
Abalone(7)	3786	391	7	9.68
Cm	449	48	22	9.35
Ecoli(imU)	301	35	8	8.60
Glass(table)	205	9	9	22.78
Ionosphere	225	126	34	1.79
Isolet(A,B)	7197	600	617	12.00
Kc	1783	326	21	5.47
Letter Img(Z)	19266	734	16	26.25
Mammography	10923	260	6	42.01
Oil	896	41	47	21.85
Optical Digits (8)	5066	554	64	9.14
Pc	4817	113	6	42.63
Satimage(4)	5809	626	36	9.28
Segment	1980	330	20	6.00
Spectrometer (44이상)	486	45	93	10.80
Us Crime (0.65초과)	1844	150	100	12.29
Wine Quality (4이하)	4715	183	11	25.77
Yeast Me2 (ME2)	1433	51	8	28.10

본 논문에서 제안한 알고리즘과 완전 균형 상태 (O_r 이 1인 상태) 간 분류 성능 평가를 위해 4.1에서 제시한 18개의 데이터 셋을 사용하였다. 산출된 오버 샘플링 비율은 소수점 한 자리로 올림 후 사용하였다. 분류 학습자로 Boosting에 오버 샘플링을 적용한 알고리즘(SMOTEBoost [1], RAMOBoost [2], WOTBoost [3])을 사용했다. 또한 강건성이 높은 AUC(Area under the ROC Curve)를 주요 성능지표로 사용하였다. 일반적으로 확률 기반 분류 학습자는 최종 분류에 앞서, 각 범주에 속할 확률을 출력하는데, AUC는 모든 cutoff(기준선)에서의 결과를 반영하기 때문이다.

성능검증 방법으로는 층화 추출을 통한 5-겹 교차를 20번 반복하였다. 오버 샘플링 및 분류 복잡도 산출에 필요한 근접 이웃 수(k)는 5로 설정하였다.

4.3 실험 결과

요인 별 산출 오버 샘플링 비율과 최종 분류 성능 결과는 표 2.에 정리되어 있다. 특히 최종 분류 성능 비교에서 분류 학습자 별로 가장 성능이 좋은 경우는 굵은 글씨로 표시했다. 또한 표 2.의 Win Count 항목에서 요인 간 분류 성능 비교 결과를 나타냈다.

먼저 Glass, Oil, Yest Me2를 제외한 모든 실험 데이터 셋에서 하나 이상의 분류 학습자를 대상으로 완전 균형일 때 보다 높은 성능을 보였다. 성능이 낮은 경우에서도 아주 근소한 차이를 보였다. Cm, Segment의 경우에서 낮은 비율로도 높은 성능을 기대할 수 있음을 알 수 있다. 추가적으로 진행한 요인 간 비교 실험에서 산출 비율에서의 차이는 대체로 0.5 이하로 나타났다. *cohesion*의 경우 산출 비율이 높아질수록 공통적으로 낮은 수준의 분류 성능을 기대할 수 있음을 알 수 있다. 각 요인 별 Win Count 및 분류 복잡도 설명력을 종합했을 때, *cohesion*이 더 나은 요인임을 알 수 있다.

5. 결론

Boosting에 오버 샘플링을 적용한 알고리즘에 관한 기존 연구에서는 일반적으로 오버 샘플링 비율을 데이터 불균형 정도만을 고려하여 완전 균형(O_r 이 1인 상태)로 설정하였다. 본 논문에서는 분류 복잡도를 고려해 오버 샘플링 비율을 산출하는 알고리즘을 제안하였다. 완전 균형과의 분류 성능 실험 비교 결과 Glass, Oil, Yest Me2를 제외한 모든 데이터 셋에서 완전 균형 이상의 분류 성능을 보였다. 특히

<표 2> 요인 별 산출 오버샘플링 비율 및 분류성능(AUC) 비교

비교 항목 데이터명	산출 비율		분류 성능								
	cohesion	f1	Smote			Ramo			Wot		
			cohesion	f1	균형	cohesion	f1	균형	cohesion	f1	균형
Abalone	0.7	0.5	0.8532	0.8507	0.8529	0.8474	0.8473	0.8457	0.8483	0.8486	0.8472
Cm	0.2	0.3	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
Ecoli	0.3	0.4	0.9961	0.9960	0.9968	0.9961	0.9959	0.9960	0.9960	0.9967	0.9959
Glass	0.5	0.5	0.9863	0.9863	0.9878	0.9865	0.9865	0.9871	0.9862	0.9862	0.9873
Ionosphere	0.6	0.6	0.9551	0.9551	0.9544	0.9515	0.9515	0.9490	0.9507	0.9507	0.9473
Isolet	0.3	0.6	0.9731	0.9727	0.9715	0.9730	0.9715	0.9691	0.9728	0.9715	0.9691
Kc	0.7	0.6	0.7889	0.7876	0.7909	0.7825	0.7863	0.7791	0.7853	0.7868	0.7798
Letter Img	0.1	0.4	0.9948	0.9922	0.9828	0.9950	0.9945	0.9932	0.9950	0.9948	0.9930
Mammography	0.4	0.5	0.9247	0.9222	0.9188	0.9326	0.9318	0.9341	0.9314	0.9323	0.9333
Oil	0.6	0.4	0.8613	0.8527	0.8656	0.8637	0.8475	0.8824	0.8578	0.8561	0.8944
Optical Digits	0.2	0.6	0.9797	0.9795	0.9775	0.9792	0.9792	0.9775	0.9796	0.9794	0.9779
Pc	1.0	0.9	0.7051	0.7100	0.7051	0.7069	0.7070	0.7069	0.7041	0.7106	0.7041
Satimage	0.3	0.7	0.9268	0.9283	0.9258	0.9249	0.9233	0.9215	0.9257	0.9244	0.9230
Segment	0.2	0.2	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
Spectrometer	0.3	0.5	0.9578	0.9560	0.9583	0.9559	0.9548	0.9565	0.9550	0.9585	0.9557
Us Crime	0.7	0.3	0.8978	0.8975	0.9026	0.8837	0.8884	0.8832	0.8817	0.8905	0.8724
Wine Quality	0.8	0.8	0.8202	0.8202	0.8191	0.8077	0.8077	0.8061	0.8071	0.8071	0.8063
Yeast Me2	0.8	0.4	0.8503	0.8265	0.8672	0.8431	0.8188	0.8537	0.8425	0.8164	0.8596
Win Count	분류	학습자별 측정	9	2	7	9	4	5	8	6	4

본 실험에서 사용한 Boosting에 오버 샘플링을 적용한 알고리즘의 경우 학습 시간이 약한 학습자 수와 곱에 비례하는 특성을 고려했을 때, 해당 논문의 알고리즘은 학습 시간 단축 면에서도 활용 가능하다. 추가적으로 진행한 요인 간 비교 실험을 통해 요인 간 산출 비율에서의 차이는 대체로 0.5 이하로 나타났다. cohesion의 경우 산출 비율이 높아질수록 공통적으로 낮은 수준의 분류 성능을 기대할 수 있음을 알 수 있다. 요인 별 산출 오버 샘플링 경향과 분류 성능을 종합했을 때, cohesion이 더 나은 요인이라고 결론지을 수 있다.

추후 연구에서는 요인 별 상반된 비율에 대한 원인 분석을 수행하고자 한다. 또한 Boosting에 적용할 오버 샘플링 기법의 다양성 측면에서도 연구를 수행하고자 한다. 본 논문에서 사용한 분류 학습자는 초기 기법(Smote)을 기반으로 설계되었기 때문이다. 마지막으로 분류 복잡도 산출에 필요한 근접 이웃 수(k)에 대한 파라미터 분석(Parameter Analysis)을 수행하고자 한다.

참고문헌

[1] Chawla, Nitesh V., et al, "SMOTEBoost: Improving prediction of the minority class in boosting.", European conference on principles of data mining and knowledge discovery. Springer, Berlin, Heidelberg, 2003, pp. 107-119.
 [2] Chen, Sheng, Haibo He, and Eduardo A. Garcia, "RAMOBoost: ranked minority oversampling in boosting.", IEEE Transactions on

Neural Networks 21.10, 2010, pp. 1624-1642.

[3] Zhang, Wenhao, Ramin Ramezani, and Arash Naeim, "WOTBoost: Weighted Oversampling Technique in Boosting for imbalanced learning.", arXiv preprint, 2019, arXiv:1910.07892 .
 [4] Hido, Shohei, Hisashi Kashima, and Yutaka Takahashi. "Roughly balanced bagging for imbalanced data." Statistical Analysis and Data Mining: The ASA Data Science Journal 2.5 6, 2009, pp. 412-426.
 [5] Lorena, Ana C., et al, "How Complex is your classification problem? A survey on measuring classification complexity.", ACM Computing Surveys (CSUR) 52.5, 2019, pp. 1-34.
 [6] Shakeel, Fatima, A. Sai Sabhitha, and Seema Sharma, "Exploratory review on class imbalance problem: An overview.", 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE, 2017.
 [7] Alkhalid, Abdulaziz, Mohammad Alshayeb, and Sabri Mahmoud, "Software refactoring at the function level using new Adaptive K-Nearest Neighbor algorithm.", Advances in Engineering Software 41.10-11, 2010, pp. 1160-1178.
 [8] Han, Hui, Wen-Yuan Wang, and Bing-Huan Mao., "Borderline-SMOTE: a new over-sampling method in imbalanced data sets learning.", International conference on intelligent computing. Springer, Berlin, Heidelberg, 2005.

IoU 의 최적화에 관한 연구

서신*

*한양대학교 컴퓨터소프트웨어학과
xiner6899@gmail.com

A Study on the Optimization of IoU

Xu Xin*

*Dept. of Computer Software, Hanyang University

요 약

IoU (Intersection over Union) is the most commonly used index in target detection. The core requirement of target detection is what is in the image and where. Based on these two problems, classification training and positional regression training are needed. However, in the process of position regression, the most commonly used method is to obtain the IoU of the predicted bounding box and ground-truth bounding box. Calculating bounding box regression losses should take into account three important geometric measures, namely the overlap area, the distance, and the aspect ratio. Although GIoU (Generalized Intersection over Union) improves the calculation function of image overlap degree, it still can't represent the distance and aspect ratio of the graph well. As a result of technological progress, Bounding-Box is no longer represented by coordinates x,y,w and h of four positions. Therefore, the IoU can be further optimized with the center point and aspect ratio of Bounding-Box.

1. 서론

IoU (Intersection over Union) is a common evaluation standard in target detection. It mainly measures the degree of overlap between the bounding box and ground-truth bounding box generated by the model, and is often used to evaluate the advantages and disadvantages of the bounding box. It is often used in target detection or semantic segmentation tasks in the field of deep learning.

In the target detection task, we often make the model generate a large number of candidate bounds at one time, and then sort the frames according to the confidence of each frame, and then calculate the IoU between the frames in turn. The method of NMS (Non-maximum suppression) is used to judge which one is the object we are really looking for and which ones should be deleted. After we get the final output, we can also take the IoU between the output box and the ground-truth bounding box and use 1-IoU as the Loss (interval [0,1] to find the minimum value),

and In this way, iterative optimization of the model is achieved.

Advantage :

- [1] It can reflect the detection effect of prediction detection box and real detection box.
- [2] It also has a good feature of being scale invariant. In the regression task, the most direct indicator of the distance between the predict box and the ground-truth bounding box is IoU.

Disadvantage:

- [1] If the two boxes do not intersect, by definition, $IoU=0$, it cannot reflect the distance between them (coincidence degree). At the same time, because $Loss=0$, there is no gradient return, so the learning training cannot be carried out.
- [2] For two objects with the same IoU, their alignment IoU is not sensitive.

GIoU (Generalized Intersection over Union) has one more "Generalized" than the IoU. This also means that it can calculate IoU on a more general level, which can solve the problem of "when tw

o images do not intersect, the distance between two images cannot be compared".

Features of GIoU:

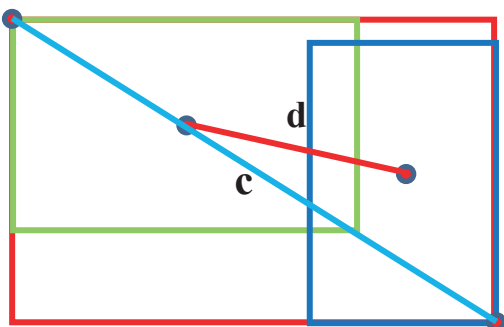
- [1] Similar to the IoU, GIoU is also a distance measure. As a loss function, it can meet the basic requirements of the loss function.
- [2] GIoU is still insensitive to scale.
- [3] GIoU is the lower bound of IoU. If the two boxes coincide, IoU=GIoU.
- [4] The value of IoU is [0,1], but GIoU has a symmetric interval, the value range is [-1,1]. The maximum value is 1 when they coincide, and the minimum value is -1 when they have no intersection and are infinitely far apart. So GIoU is a very good measure of distance.
- [5] Unlike an IoU, which only focuses on overlap. GIoU focuses not only on overlapping regions, but also on other non-overlapping regions. Therefore, it can better reflect the degree of coincidence between the two.

Although GIoU has improved the calculation function of image overlap, it still cannot express the distance and similarity of the image well.

2. IoU의 최적화의 요구사항

The calculation of the IoU can be considered as comparing whether two boxes or two image regions are in the same position. Therefore, the Euclidean distance can be used to calculate the normalized distance between the center points of the two bounding boxes. On the basis of distance, we can increase the idea of fitting the ratio of width to height of prediction box and the ratio of width to height of target box.

$$IoU - \frac{\rho^2_{(o,o^{Ground-truth})}}{C^2} - X$$



(그림 1) 공식 사진.

$o, o^{Ground-truth}$: represents the center point of the two boxes.

ρ : represents the Euclidean distance between the two center points.

C : represents the diagonal of the smallest enclosing rectangle.

X is the penalty term for the shape difference calculated from the aspect ratio. Used to reflect the difference between the two boxes.

$$X = \frac{4}{\pi^2} \left(\arctan \frac{w^{Ground-truth}}{h^{Ground-truth}} - \arctan \frac{w}{h} \right)^2$$

The range of \arctan is $[0, \pi/2)$.

Finally, gradient descent is needed to optimize the loss function.

The gradient of w and h needs to be specified.

$$\frac{\partial X}{\partial w} = 2 * \frac{4}{\pi^2} * \left(\arctan \frac{w^{Ground-truth}}{h^{Ground-truth}} - \arctan \frac{w}{h} \right) * (-1) * \frac{1}{1 + \left(\frac{w}{h} \right)^2} * h^{-1}$$

$$= \frac{8}{\pi^2} * \left(\arctan \frac{w^{Ground-truth}}{h^{Ground-truth}} - \arctan \frac{w}{h} \right) * (-1) * \frac{h^2}{w^2 + h^2} * h^{-1}$$

$$= -\frac{8}{\pi^2} * \left(\arctan \frac{w^{Ground-truth}}{h^{Ground-truth}} - \arctan \frac{w}{h} \right) * \frac{h}{w^2 + h^2}$$

$$\frac{\partial X}{\partial h} = 2 * \frac{4}{\pi^2} * \left(\arctan \frac{w^{Ground-truth}}{h^{Ground-truth}} - \arctan \frac{w}{h} \right) * (-1) * \frac{1}{1 + \left(\frac{w}{h} \right)^2} * w * (-1) * h^{-2}$$

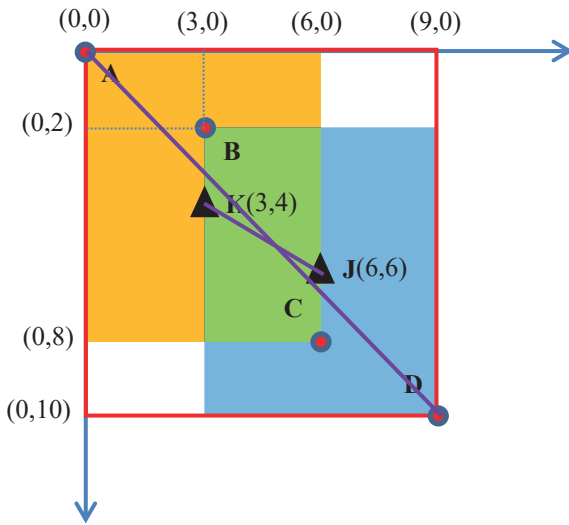
$$= \frac{8}{\pi^2} * \left(\arctan \frac{w^{Ground-truth}}{h^{Ground-truth}} - \arctan \frac{w}{h} \right) * \frac{h^2}{w^2 + h^2} * w * h^{-2}$$

$$= \frac{8}{\pi^2} * \left(\arctan \frac{w^{Ground-truth}}{h^{Ground-truth}} - \arctan \frac{w}{h} \right) * \frac{w}{w^2 + h^2}$$

Overlap region factor has higher priority in regression, especially in non-overlap case. Therefore, a weight can be added, and the overlapping area can control the weight.

$$\frac{X}{Loss_{IoU} * X}$$

As shown in figure:



(그림 2) 실제의 예 사진.

By calculation, the coordinates of center point **K** in the yellow box and center point **J** in the blue box :

K: (3,4) **J**: (6,6)

$$IoU = \frac{|A \cap B|}{|A \cup B|}$$

$$\begin{aligned} &= (Cx-Bx) * (Cy-By) / (Cx-Ax) * (Cy-Ay) + (Dx-Bx) \\ &* (Dy-By) - (Cx-Bx) * (Cy-By) \\ &= (6-3)*(8-2) / ((6-0)*(8-0)+(9-3)*(10-2)-(6-3)*(8-2)) \\ &= (3*6) / ((6*8)+(6*8)-(3*6)) \\ &= 18/78 \\ &= 0.23 \end{aligned}$$

$$IoU - \frac{\rho_{(o,o^{Ground-truth})}^2}{C^2} - \frac{X}{Loss_{IoU} * X} * X$$

$$= 0.23 - \frac{\sqrt{3^2 + 2^2}}{\sqrt{9^2 + 10^2}} - \frac{X}{Loss_{IoU} * X} * \frac{4}{\pi^2} \left(\arctan \frac{6^{Ground-truth}}{8^{Ground-truth}} - \arctan \frac{6}{8} \right)^2$$

$$= 0.158 - 0$$

$$= 0.158$$

In the example, the first two matrices have the same shape. So the penalty term for the calculated shape difference X is 0.

Initially, IoU was only used as a simple evaluation standard, mainly used to measure the degree of overlap between the bounding box generated by the model and the ground-truth box that is the correct result of the label. In target detection, in order to make the positioning more accurate. Make region-proposal closer to ground-truth. You need to fine-tune region-proposal with bounding-box regression. Therefore, IoU can be optimized by making full use of the characteristics of IoU in the original technology. Not only are you limited to measuring the overlap between the two boxes, you can also measure the distance and shape differences between the two boxes. More flexible than before, can be further rapid convergence and performance improvement.

참고문헌

- [1] Ross Girshick, "Fast R-CNN", The IEEE International Conference on Computer Vision (ICCV), Santiago Chile, 2015, pp.1440-1448
- [2] Joseph Redmon, Santosh Divvala, Ross Girshick, Ali Farhadi, "You Only Look Once: Unified, Real-Time Object Detection", The IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Las Vegas America, 2016, pp.779-788
- [3] Kaiming He, Georgia Gkioxari, Piotr Dollar, Ross Girshick, "Mask R-CNN", The IEEE International Conference on Computer Vision (ICCV), Venice Italy, 2017, pp.2961-2969
- [4] Navaneeth Bodla, Bharat Singh, Rama Chellappa, Larry S. Davis, "Soft-NMS -- Improving Object Detection With One Line of Code", The IEEE International Conference on Computer Vision (ICCV), Venice Italy, 2017, pp.5561-5569
- [5] Tsung-Yi Lin, Priya Goyal, Ross Girshick, Kaiming He, Piotr Dollar, "Focal Loss for Dense Object Detection", The IEEE International Conference on Computer Vision (ICCV), Venice Italy, 2017, pp.2980-2988
- [6] Zhaowei Cai, Nuno Vasconcelos, "Cascade R-CNN: Delving Into High Quality Object Detection", The IEEE Conference on Computer Vision and Pattern Recognition

tion (CVPR), Salt Lake City America, 2018, pp.6154-6162

[7] H e i L a w , J i a D e n g ,
“CornerNet: Detecting Objects as Paired Keypoints”, The European Conference on Computer Vision (ECCV), Munich Germany, 2018, pp.734-750

[8] Chenchen Zhu, Yihui He, Marios Savvides,
“ Feature Selective Anchor-Free Module for Single-Shot Object Detection”, The IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Long Beach California America, 2019, pp.840-849

[9] Yihui He, Chenchen Zhu, Jianren Wang, Marios Savvides, X i a n g y u Z h a n g ,
“Bounding Box Regression With Uncertainty for Accurate Object Detection”, The IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Long Beach California America, 2019, pp.2888-2897

[10] Hamid Rezatofighi, Nathan Tsoi, JunYoung Gwak, Amir Sadeghian, Ian Reid, Silvio Savarese,
“Generalized Intersection Over Union: A Metric and a Loss for Bounding Box Regression”, The IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Long Beach California America, 2019, pp.658-666

제53회
2020 온라인 춘계학술발표대회

멀티미디어처리



다시점 360도 영상을 사용한 자유시점 영상 생성 방법

조영광*, 안희준*

*서울과학기술대학교 전기정보공학과
choyg@seoultech.ac.kr, heejune@seoultech.ac.kr

Free view video synthesis using multi-view 360-degree videos

Young-Gwang Cho*, Heejune Ahn*

*Dept. of Electrical and Information Engineering,
Seoul National University of Science and Technology

요 약

360 영상은 시청자가 시야방향을 결정하는 3DoF(3 Degree of Freedom)를 지원한다. 본 연구에서는 다수의 360 영상에서 깊이 정보를 획득하고, 이를 DIBR (Depth-based Image Rendering) 기법을 사용하여 임의의 시점 시청기능을 제공하는 6DoF(6 Degree of Freedom) 영상제작 기법을 제안한다. 이를 위하여 기존의 평면 다시점 영상기법을 확장하여 360 ERP 투영 영상으로부터 카메라의 파라미터 예측을 하는 방법과 깊이영상 추출 방법을 설계 및 구현하고 그 성능을 조사하였으며, OpenGL 그래픽스기반의 RVS(Reference View Synthesizer) 라이브러리를 사용하여 DIBR을 적용하였다.

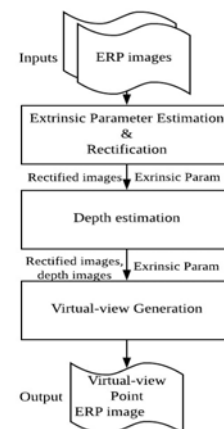
1. 서론

최근 HMD(Head Mounted Display)와 같은 장치와 360도 카메라가 보급되면서 가상현실을 위한 콘텐츠 개발이 활발히 진행되고 있다[1]. 그러나 렌더링을 통해 시점변화가 용이한 애니메이션기반 방식과 달리 실사영상을 바탕으로 한 가상시점 6DoF(6 Degree of Freedom) 제공은 어려움이 있다.

기존의 연구와 표준화 과정을 보았을 때 임의시점 영상을 생성하기 위해서는 깊이정보를 사용하는 것이 필수적일 것으로 보인다. 최근 표준화에서도 3DoF+(3 Degree of Freedom +), 6DoF 영상표준화에서 깊이정보를 사용하는 방향을 연구 중이다[1]. 본 논문은 기존의 다시점 평면영상의 다시점 영상 생성기법을 사용하였지만, 그 실현 과정에서 평면투영과 구형투영 영상 사이의 차이점으로 인하여 세부적인 알고리즘을 확장하였다. 두개이상의 ERP(Equi-Rectangular Projection)의 360도 영상을 입력으로 하여 카메라간의 외부 파라미터를 추정하여 위치관계를 파악한다. 이를 바탕으로 카메라를 정합(Rectification)하고 영상의 깊이를 추정한다. 추정된 깊이를 활용하여 각 픽셀들의 3차원 위치를 계산하여 가상시점에서의 영상을 생성한다.

2. 제안하는 ERP 가상시점 영상 생성 시스템

가상시점 생성을 위한 순서는 크게 3단계로 진행된다. 첫 번째로 사용자로부터 ERP 영상을 입력받아 각 영상의 카메라 간의 외부 파라미터를 추정하고 정합한다. 두 번째로 정합된 영상들을 이용하여 SAD(Sum of Absolute Difference) 방법을 통해 깊이 영상을 생성한다. 세 번째로 정합된 두 영상과 생성된 깊이 영상을 바탕으로 각 픽셀들의 가상 3차원 위치를 계산하여 구하고자하는 가상시점에서의 영상을 생성한다.



(그림 1) 가상시점 생성 절차

가. 카메라 파라미터 추정 및 정합

ERP 영상의 포맷은 위도 θ 와 경도 ϕ 및 반지름이 r (본 논문에서는 1로 고정)인 구좌표계를 따른다. 다수의 ERP 영상의 카메라 상대 파라미터를 추정하기 위해 화소위치를 구면 좌표계에서 직교좌표계(Cartesian coordinate)로 변환한다. 좌표계는 그림 2와 같이 MPEG의 OMAF(Omnidirectional Media Format)[2]의 좌표계를 따른다. 단위 구면에 투영된 구면 좌표와 직교좌표계로 변환하는 식은 다음과 같다.

$$x = -\sin\theta\cos\phi \quad (1)$$

$$y = \sin\theta\sin\phi$$

$$z = \cos\theta$$

$$\theta = \arccos(z) \quad (2)$$

$$\phi = \arctan\left(-\frac{y}{x}\right)$$

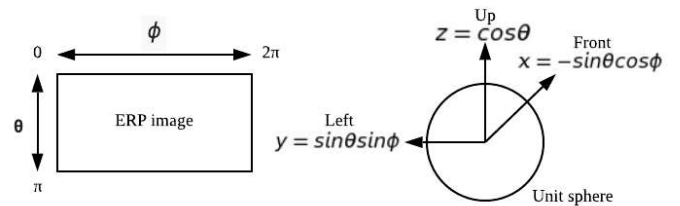
본 논문에서는 ERP 영상에서 SURF를 이용하여 특징점 추출하고 대응점으로부터 8-Point 카메라 파라미터 추정 알고리즘[3]을 사용한다. 평면 투영 이미지와 달리 ERP 투영에서는 래디컬 외곡이 발생하며(특히, 상단 및 하단), 기존의 SURF를 적용하기 위해서 Hajime Taira[4]가 제안한 회전을 통해 외곡이 적은 좌표영역으로 회전을 하는 방법을 사용하였다. 또한 신뢰성을 높이기 위하여 RANSAC(Random sample consensus)에 기반을 둔 알고리즘을 적용한다.

1. N개의 대응점에서 N/4개의 대응점을 무작위로 선택한다.
2. 8-Point 방법을 이용하여 $R|t$ 를 구한다.
3. 구해진 R 행렬을 XYZ-Eular 회전 벡터 R_vec 으로 변환한다.
4. 변환된 R_vec 을 배열 R_vec_arr 에 저장한다. 이후 정확하게 측정된 회전 벡터 R_vec 를 얻기 위해 다음과 같은 과정을 임의의 M회 수행한다.
 1. R_vec_arr 중 m번째 R_vec 과 다른 R_vec 간 유클리드 놈(Euclidean norm)을 구한다.
 2. 구해진 놈들을 배열 $norm_arr$ 에 저장 후, 정렬한다.
 3. 정렬된 놈 중 하위 20% 및 상위 20%를 제외한 $norm_arr$ 의 평균을 구한다.
 4. 구해진 $norm$ 의 평균을 m번째 R_vec 의 오차로 한다.

위와 같은 과정을 통해 구해진 XYZ-Eular 회전 벡터 R_vec 중 오차가 가장 적은 R_vec 과 그와 대응되는 이동 벡터 t 를 최종 외부 파라미터로 한다.

다음으로, 8-Point 외부 파라미터 추정 실험을 위해 두 개의 실사 ERP 영상을 이용하였다.

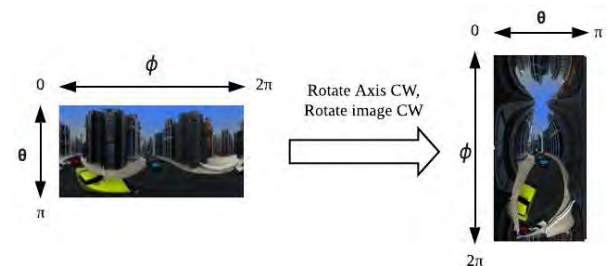
1. 좌우에 위치한 두 카메라 간 최초 회전 행렬 및 이동 벡터 $R_0|t_0$ 를 측정한다.
2. 우측 ERP 영상에 임의의 회전 행렬 R_i 을 적용한다.
3. 두 카메라 간 Essential 행렬을 구한 뒤 $R_e|t_e$ 를 추출한다.
4. 임의로 적용시킨 $R_i = R_e R_0^{-1}$ 이어야 할 것이다.
5. 이동 벡터는 $t_0 = t_e$ 이어야 할 것이다.



(그림 2) ERP 영상의 Spherical coordinate(왼쪽) 및 Cartesian coordinate와 Unit sphere(오른쪽)

나. 깊이추정

기존 원근 투영(Perspective projection)영상 기반의 디스패리티(disparity)계산 및 깊이 영상 생성 방법에 대한 많은 연구가 있다[5]. 본 논문에서는 실시간 처리에 중점을 두고 OpenCV 라이브러리에서 가속화지원이 되는 StereoBM[6]을 이용하여, 기존의 잘 정리되어있는 스테레오 매치(Stereo match) 방식을 ERP 영상에 변형하여 사용하였다. ERP 영상은 투영 방식 특성상 기존의 등극선 기하(Epipolar Geometry)를 그대로 적용할 수 없기 때문에 그림 3과 같이 영상의 좌표축을 시계 방향으로 90도 회전하는 H. Kim 등[7]의 방식을 사용하였다.



(그림 3) 원본 ERP 영상(왼쪽)과 StereoBM 적용을 위해 좌표축 회전 후 다시 영상을 회전한 입력 영상(오른쪽) 디스패리티(시차) 맵을 획득한 후 이를 이용해 각 픽셀들에 해당하는 거리를 계산한다. 그림 4와 같이 B 는 카메라 간 거리이며 h 는 회전된 영상의 가로길 이로 정의했을 때, 구면 좌표계의 각의 차이 d_θ 는

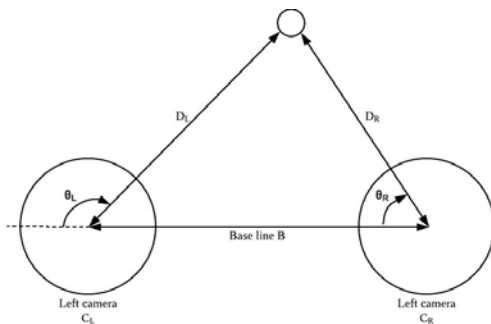
화소 디스패리티 d 로부터 식 3으로 얻어진다. 이로부터 구의 중심에서 투영된 물체까지의 거리 D_L 과 D_R 은 회전된 입력 영상의 구면 좌표계에서의 위도 θ_L, θ_R 에서부터 식 (4)으로 구해진다.

$$d = \theta_L - \theta_R \quad (3)$$

$$d_\theta = d \times \frac{\pi}{h}$$

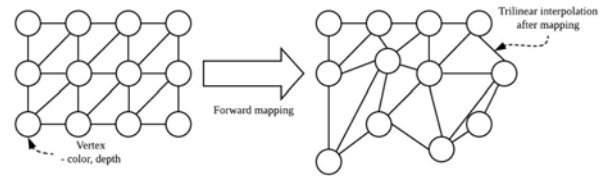
$$D_L = B / \left(\frac{\sin \theta_L}{\tan(\theta_L - d_\theta)} - \cos \theta_L \right) \quad (4)$$

$$D_R = B / \left(\cos \theta_R - \frac{\sin \theta_R}{\tan(\theta_R + d_\theta)} \right)$$

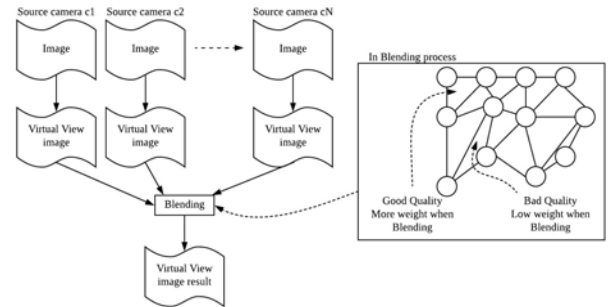


(그림 4) 정합된 두 단위 구 형태의 입력에서의 거리정보다. 가상 시점 생성

DIBR (depth-based image Rendering) 기법은 다시점 영상 생성을 위하여 꾸준히 연구 되어 왔다. 통상의 DIBR 기법은 가상시점의 모든 화소에서의 깊이정보를 필요로 하여 깊이 값을 추정하기 위한, 특히 깊이정보가 없는 occlusion영역을 제거하는 휴리스틱에 대한 연구가 주를 이루었다[8]. 본 연구에서는 OpenGL의 그래픽스 처리기법을 사용한 RVS(Reference View Synthesizer)[9]를 사용한다. RVS는 그림5와 같이 필터링이 필요한 역방향 사상 과정을 거치지 않고 각각의 픽셀을 메쉬 노드(vertex)로 정의하여 인접한 메쉬 삼각형들을 구성한다. 이를 순방향 사상을 진행하여 삼선형 보간법을 이용하여 빈 공간을 제거한다. 그리고 그림6과 같이 복수의 원본 영상으로부터 얻어진 가상 시점 영상들을 혼합함으로써 위치에 의해 발생하는 빈 영역을 제거하고 높은 품질의 결과물을 만들어내도록 한다. 이를 위해 순방향 사상 과정에서 발생하는 각 삼각형들의 변형 정도를 품질척도로 이용하여 삼각형의 변형이 적은 픽셀의 가중치를 크게 주어 최종 결과물의 품질을 향상시킬 수 있다.



(그림 5) RVS의 forward mapping과 삼선형 보간법을 이용한 가상시점 생성



(그림 6) RVS의 Blending 과정

3. 실험

8-Point 외부 파라미터 추정은 다음순서로 두 개의 실사 ERP 영상을 이용하였다. 실사 영상은 외부에서 카메라 간의 간격을 약 1m 로 하여 촬영한 것이다. 추정된 회전 행렬들은 XYZ-Euler 회전 벡터로 변환한 후 유클리드 놈을 구하여 오차를 측정하였다. 또한 추정된 외부 파라미터를 바탕으로 영상 정합을 진행하였다. 그 후 정합된 영상을 바탕으로 생성된 거리 영상은 그림8과 같다.

<표 1> 회전 행렬 추정 결과 및 오차, degree 표현

XYZ-Euler vector (x, y, z) of R_i	XYZ-Euler vector (x, y, z) of $R_e R_0^{-1}$	Error
(15, 0, 0)	(14.984, -0.016, 0.247)	0.248
(0, 15, 0)	(0.069, 14.938, -0.166)	0.190
(0, 0, 15)	(-0.304, 0.046, 14.961)	0.309
(15, 15, 0)	(14.884, 14.963, 0.184)	0.220
(15, 0, 15)	(14.782, 0.022, 15.255)	0.336
(0, 15, 15)	(-0.324, 15.029, 15.004)	0.325
(15, 15, 15)	(14.621, 15.189, 15.309)	0.524

<표 2> 이동 벡터 추정 결과 및 오차, 단위 벡터

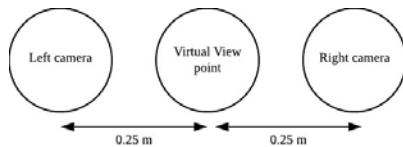
t_0	t_e	Error
(-0.001, -0.999, -0.011)	(0.06, -0.998, -0.002)	0.062
	(0.063, -0.997, -0.004)	0.064
	(0.046, -0.998, -0.019)	0.048
	(0.092, -0.995, 0.001)	0.094
	(0.073, -0.994, 0.069)	0.109
	(0.147, -0.989, 0.003)	0.149
	(-0.045, -0.998, -0.024)	0.046

가상시점 생성 실험을 위해 컴퓨터 그래픽스 도구인 Blender[10]로 만들어진 영상 및 거리 영상을 사용하였다. 이를 RVS 프로그램의 입력으로 하여 가상시점을 생성해보았다. 두 영상의 카메라 위치 및 가상시점의 위치는 그림9와 같으며 그림10과 그림11

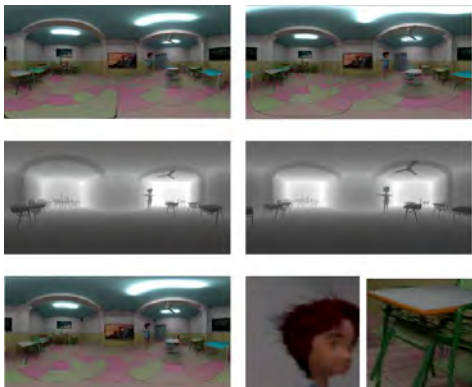
은 생성된 결과를 보여준다.



(그림 8) 정합 전 좌측 영상 및 우측영상(상단), 정합 후 좌측 영상 및 우측 영상(중간), 정합된 영상으로부터 구해진 좌측 및 우측 거리 영상(하단)



(그림 9) 입력 영상과 가상시점의 카메라 위치

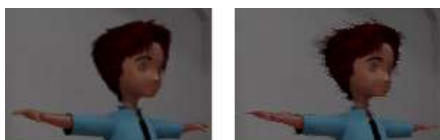


(그림 10) 입력 영상(상단), 입력 거리 영상(중간), 생성된 가상시점(왼쪽 하단), 가상시점의 부분 확대(오른쪽 하단) 생성된 가상시점과 같은 위치에서의 Ground Truth 영상과 PSNR을 구하였다. PSNR 계산은 MPEG의 WS-PSNR[11] 프로그램을 이용하였다.

본 연구에서 다중 360 ERP 영상으로부터 자유시점 영상생성을 위하여 필요한 절차들을 확장하고 실험하였다. 앞으로 효과적인 카메라 추정기법과 깊이 영상 생성에 대한 연구 추가적으로 요구된다.

<표 3> Ground Truth 영상과 생성된 가상시점 영상의 WS-PSNR 결과

YUV채널	Y	U	V
WS-PSNR	36.747	49.324	45.193



(그림 11) 가상 시점 위치에서의 Ground Truth 영상(왼쪽) 과 RVS로 생성된 영상(오른쪽)의 부분 확대

감사의 글

본 연구는 과학기술정보통신부, 정보통신기술진흥센터, 방송통신산업기술개발사업의 지원을 받았음. (시청자 이동형 자유시점 360VR 실감미디어 제공을 위한 시스템 설계 및 기반기술 연구(2016-0-00144)).

참고문헌

- [1] 호요성, "MPEG-I 표준과 360도 비디오 콘텐츠 생성", 전자공학회지, vol. 8, pp. 52 - 57, 2017.
- [2] Miska M. Hannuksela, "An Overview of the OMAF Standard for 360° Video", Data Compression Conference, Snowbird, UT, USA, 2019, pp. 580-593.
- [3] H.C. Longuet-Higgins, "A Computer Algorithm for Reconstructing a Scene From Two Projections," Nature, vol. 293, pp. 133 - 135, 1981.
- [4] Hajime Taira, "Robust feature matching for distorted projection by spherical cameras", IPSJ Transactions on Computer Vision and Applications, Japan, 2015, pp. 84-88.
- [5] Heiko Hirschmuller, "Stereo Matching in the Presence of Sub-Pixel Calibration Errors", IEEE Conference on Computer Vision and Pattern Recognition, Miami, FL, USA, 2009, pp. 437-444
- [6] Bradski G, "The OpenCV Library", Dr. Dobb's Journal of Software Tools, 2000.
- [7] H. Kim, "3D Scene Reconstruction from Multiple Spherical Stereo Pairs", International Journal of Computer Vision, vol. 104, pp. 94-116, 2013.
- [8] S. Zinger, "Free-viewpoint depth image based rendering", Journal of Visual Communication and Image Representation, vol. 21, pp. 533-541, 2010.
- [9] MPEG, "Reference View Synthesizer (RVS) manual", The 124th MPEG meeting, Macau, China, 2018.
- [10] Community BO, Blender - a 3D modelling and rendering package, Stichting Blender Foundation, Amsterdam, 2018.
- [11] MPEG, "WS-PSNR Software Manual", The 124th MPEG meeting, Macau, China, 2018.

Unity 엔진을 이용한 노년층을 위한 VR 멀티 시뮬레이션 게임 개발

차주영*, 윤혜원*

*이화여자대학교 엘텍공과대학 컴퓨터공학과

ryuha.kuma@ewhain.net, hyeppy@naver.com

Development of VR Multi Simulation Game for Old People using Unity Engine.

Jooyoung Cha*, Hyewon Youn*

*Dept. of Computer Science, Ewha Womans University

요 약

본 논문은 노인의 외로움 해소를 위해 Unity를 이용한 VR 멀티 시뮬레이션 게임 프로그램의 설계 및 개발 내용을 다루고 있다. 본 시뮬레이션은 주 타겟층인 노년층을 고려하여 최소한의 간단한 조작법을 지향하고 있으며 따라서 3D 1인칭 어드벤처 시점, 바라보는 방향으로 이동하는 연속 이동 방식을 채택하였다. 서버를 이용하여 2인 이상의 멀티 시뮬레이션 환경을 지원하며 텍스트 채팅이 아닌 음성 채팅을 통하여 시뮬레이션 유저들 간의 소통을 지원해준다. 다른 유저들과 함께 GameObject의 상호작용을 보며 대화를 이어가거나, 낚시, 채집 활동을 할 수 있다. 이로 하여금 노년층의 외로움 해소를 도울 수 있도록 개발하였다.

Key words : Unity, VR, Simulation game, Voice chatting, Multi-play

1. 서론

우리 사회의 고령화에 잇따라 노인 인구의 외로움 문제가 심각하게 대두되고 있다. 정부 통계에 의하면 2010년과 비교해 2018년 정신건강 질환의 연령별 증가율을 살펴보면, 우울증의 경우 10~19세 68.5%, 20~29세 106.3%, 70~79세 59.4%, 80세 이상 176.5% 등으로 나타났다. 2018년 전체 우울증 환자(68만 4천 690명) 중에서 60세 이상은 40.2%(27만 5천 684명)였다.[1] 또한 통계청의 사망 원인 통계를 보면 60대 이상의 노년층의 자살률이 청소년층이나 청년층과 비교도 되지 않을 정도로 큰 차이를 보인다는 것이다. 노년층의 외로움은 자살 등의 극단적 선택 등을 야기시키는데 이는 심각한 사회문제로 떠올랐다. 고독사로 인한 사망자는 2012년 1021에서 2018년 2,447명으로 2배 이상으로 늘었다.[2] 본 연구에서는 위와 같은 노인의 외로움 문제를 해소하는 데 도움을 줄 VR 멀티 시뮬레이션의 개발을 진행하였다. 시뮬레이션 게임 개발 엔진으로는 Unity를 채택하였으며 플랫폼은 모바일, Google VR을 채택하였다. 컨트롤러로 VR Shinecon 컨트롤러를

사용한다. 혼자서 즐기는 것이 아닌 여럿이 즐길 수 있는 멀티 시뮬레이션을 지원한다는 데에 다른 시뮬레이션과의 차별점을 두었다.

2. 시뮬레이션 게임 UI 기능

본 시뮬레이션의 주 타겟층은 60세 이상의 노년층이기 때문에 더 쉽고 직관적인 UI가 요구된다. UI를 제작하기 위해서 Unity의 canvas에 직접 제작한 이미지 리소스들을 사용하여 버튼과 메뉴 등을 만들었다. 타겟층의 평균적인 시력에 적합하도록 UI 크기를 크게 조정하며 어떤 기능인지 확실히 알 수 있도록 메타포와 함께 텍스트 설명을 덧붙였다.

본 개발에서는 기본적인 UI 디자인 외에도 유저에게 더 편리성을 제공하기 위한 기능을 조금 더 추가하였다. 이에 대한 기능을 개발하기 위해서 C# 스크립트를 작성하였다.

첫 번째 UI 기능으로는 Raycast를 이용한 응시 로직 구현이다.[3][4] 이를 위해 레티클을 직접 구현하였다. 레티클은 유저의 헤드 트래킹에 따라 시점이 변화할 때 화면 중앙에 항상 생겨 있는

응시점을 말한다. 단순한 응시점인 렉티클에 C# 스크립트를 추가하여 상호작용이 있는 GameObject 를 응시하면 이벤트가 발생하게 한다. 이벤트가 발생하는 모든 GameObject 들에는 Collider 컴포넌트가 추가되어있으며 EventTrigger 컴포넌트 또한 포함해야 한다. C# 스크립트를 통해 Raycast 가 발생했는지 아닌지를 감지하고, 만약 발생하였으면 True, 아닌 경우에는 False 를 반환한다. 이를 통해 유저는 해당 GameObject 가 상호작용이 있는지 없는지를 바라보는 것만으로 알 수 있다.



(그림 1) Raycast 를 이용한 응시 로직 렉티클 UI

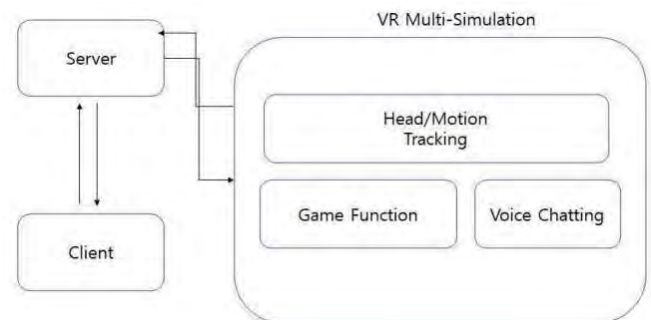
두 번째는 빌보드(Billboard) 기능이다. 빌보드란 3D 공간상에서 GameObject 의 Polygon 의 방향이 항상 유저의 시야 방향으로만 보이게 하는 기법이다. 이를 이용하여 글자가 적힌 표지판 등을 항상 정렬된 순서로 보는 것이 가능해진다. 본 시뮬레이션에서는 빌보드 기능이 적용된 UI 는 화면에 정렬되는 화면 정렬 방식을 채택했다. 본 프로젝트에서는 해당 기능을 메인 카메라의 Transform 컴포넌트를 캐시 처리한 후, 빌보드 기능이 추가된 게임 오브젝트를 메인 카메라를 응시하도록 .LookAt() 기능을 사용하여 구현했다.



(그림 2) Billboard 기능을 적용한 GameObject(Welcome)과 적용하지 않은 GameObject

3. 게임 기능 구현

본 게임에서는 노인이라는 유저층에 맞게 다양한 편의 사항들과 외로움 해소를 위한 멀티플레이 기능을 추가하였다.

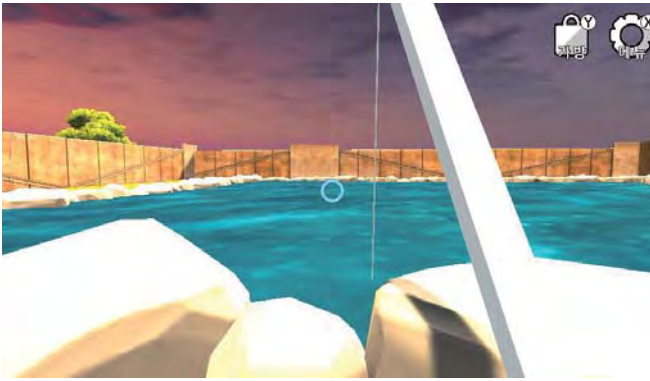


(그림 3) 시뮬레이션 전체 구조도

위 그림은 시뮬레이션의 전체 구조도다. 전체적으로 서버와 클라이언트가 통신을 하며 게임 내에서는 후술할 기능들이 각각의 역할을 수행한다.

3-1. 오브젝트와의 상호작용 기능

사용자의 리얼리티를 반영하기 위하여 다양한 오브젝트와의 상호작용 기능을 설계하였다. LookItem 스크립트 내의 함수와 게임 오브젝트의 EventTrigger 과의 작용으로 구현을 하였다. 시뮬레이션 내의 NPC 와 마주치게 되면 오브젝트임을 인식하여 이동을 멈추고 커서의 모양이 바뀐다.



(그림 4) 시뮬레이션 내의 낚시 상호작용 구현 화면

낚시터에서 멈추게 되면 태그 비교 기능으로 낚시터임을 인식하고 낚싯대가 나오게 되며 낚시를 할 수 있게 된다. 그리고 모든 오브젝트에는 Collider를 추가하여 실제로 부딪히면 충돌하는 상호작용도 구현했다.

3-2. 서버-클라이언트 기능 지원

서버는 BaaS(Mobile Backend As A Service)중 하나인 Photon Unity Networking2를 사용하여 클라이언트들이 게임에 접속하면 자동으로 방을 생성하여 입장을 할 수 있도록 하였다. 서로의 움직임은 observe 컴포넌트를 설정한 PhotonView를 할당하여 실시간으로 반영한다. 추가로, A 단말과 B 단말의 캐릭터가 다르기 때문에 자신의 캐릭터는 흰색, 다른 사용자들의 캐릭터는 다른 색으로 보이도록 하였다.

3-3. 헤드 트래킹 기능

거동이 불편한 유저층을 고려해 VR 기기를 착용하고 머리를 움직이면 사용자의 머리를 추적하여 시뮬레이션 내의 시야도 변하는 헤드 트래킹 기능을 추가하였다. MoveCtrl 스크립트로 보는 방향으로(LookAt) 이동이 가능하게 구현하였다. 메인 카메라가 헤드 트래킹 기능으로 인하여 사용자의 응시 방향에 따라 달라지므로 특별한 컨트롤러 없이도 사용자가 보는 방향으로 이동할 수 있다.

3-4. 음성채팅 지원

키보드가 익숙하지 않은 노년층을 위하여 키보드 채팅 대신 음성채팅을 지원하였다. Photon Voice2를 게임에 적용하여 음성채팅을 원활하게 구현하였다. 이

애플리케이션 내의 Photon Voice Network 컴포넌트는 자동으로 싱크를 맞춰주어 유저와 서버와의 동기화를 하고 Recorder 컴포넌트는 마이크로 녹음된 오디오 스트림을 다른 클라이언트들에게 전송한다.

4. 결론

본 논문은 Unity를 이용하여 노년층을 주 타겟층으로 한 힐링용 멀티 시뮬레이션의 구현을 하였다. 기존의 다른 시뮬레이션과는 달리 서버를 이용하여 멀티플레이를 지원하는 방법을 다뤄보았으며 이는 향후 유사 시뮬레이션 개발에 도움이 되리라 생각한다. 타인을 만나기 힘든 상황에 처한 노년층에게 다른 사람과 소통을 할 수 있는 기회를 제공할 수 있을 것이다. 더욱 나아가서는 시뮬레이션을 이용하는 노년층의 우울증 해소 효과를 기대할 수 있을 것이다. 향후, 더욱 다양한 상호작용을 추가하고 효율적인 시스템을 구축하여 시뮬레이션을 개선할 계획이다.

참고문헌

- [1] 서한기, “노년층 정신건강 심각...우울증 환자 10명중 4명은 60세 이상”, 연합뉴스, 2019년 10월 2일, 1쪽.
<https://www.yna.co.kr/view/AKR20191001156300017>
- [2] 홍준기, “독거노인 늘고 노후빈곤 겹쳐... 고독사, 6년새 2배로”, 조선일보, 2019년 9월 27일, 1쪽.
http://news.chosun.com/site/data/html_dir/2019/09/27/2019092700309.html
- [3] 이재현, 『절대강좌! 유니티 VR/AR : 유니티로 배우는 가상현실/증강현실 콘텐츠 제작 기법』, 파주, 출판사 위키북스, 2019.
- [4] 조나단 리노위즈, 『유니티 5 가상현실 VR 프로젝트 : 실용적인 프로젝트와 상세한 설명을 통한 가상현실 개발』, 서울, 출판사 에이콘, 2016.

구면 PTAM의 구현을 위한 카메라 모델 설계

김기식, 박종승
인천대학교 컴퓨터공학과
wis1906@naver.com, jong@inu.ac.kr

Design of Camera Model for Implementation of Spherical PTAM

Ki-Sik Kim, Jong-Seung Park
Dept. of Computer Science & Engineering, Incheon National University

요 약

시각적 환경 인식을 위하여 PTAM 연구가 활발히 이루어지고 있다. 최근 모든 방향의 시야각을 제공하는 구면 비디오를 위한 연구로 확장되고 있다. 기존의 구면 SLAM 방법은 Unified Sphere Model을 사용하며 앞면 시야각만 제공할 수 있는 한계가 있다. 본 논문에서는 구면 비디오를 위한 PTAM의 구현을 위한 카메라 모델을 제시한다. 제안된 카메라 모델은 핀홀 투영 카메라에 기반한 듀얼 영상 평면을 사용한다. 제안 방법은 앞면 시야각에 제약되지 않으며 전체 시야각을 지원한다. 또한 구면 비디오의 PTAM 적용 과정에서 평면 연산식을 직접 적용할 수 있는 장점이 있다.

1. 서론

구면 파노라마 이미지는 전 방향에 대한 정보를 한 장의 이미지로 표현한다. 이 이미지는 가로세로 2대 1의 비율을 가지는 이미지 평면에 구면 좌표계를 기반으로 이미지를 표현하기 때문에 이미지의 적도 라인에서 멀어질수록 급격하게 왜곡이 늘어난다. 구면 파노라마 이미지는 왜곡량이 많을 뿐더러 균일하지 않기 때문에 일반적으로 다른 형태의 카메라 모델을 설계하여 재투영하는 과정을 거친다.

SLAM(Simultaneous Localization and Mapping)은 미지의 영역에 대한 이미지의 특징점을 활용하여 지속적으로 맵을 그려나가 실시간으로 지형을 파악하고 카메라의 위치를 추정하는 기술이다. 구면 파노라마 이미지는 한 장의 이미지로도 주변의 거의 모든 정보를 분석할 수 있는 장점 때문에 과거부터 구면 파노라마 이미지를 입력으로 하는 SLAM에 대한 연구가 활발히 이어졌다.

David Caruso등[1]은 Fisheye Camera를 이용하여 Unified Omnidirectional Model에 대한 직접적인 공식화를 통해 Large-Scale Direct SLAM을 구현하였다. David Valiente등[2]은 이동형 로봇에 Fisheye Camera를 부착하여 로봇의 시스템 정보 매트릭스를 활용하여 불안정한 실측 정보를 보완

SLAM을 구현하였다. Alejandro Rituerto등[3]은 EKF(Extended Kalman Filter)를 활용하여 전 방향 카메라를 이용한 SLAM을 구현하였다. Jianfeng Li 등[4]은 구면 좌표계를 사용하는 구면 투영 모델을 설계하여 실내 환경에 적합한 SLAM 기능을 구현하였다.

PTAM[5]은 SLAM에서 파생된 기술로, Tracking과 Mapping을 병렬적으로 수행한다. PTAM은 상대적으로 수행 시간이 짧은 Tracking은 매 프레임마다 수행하여 정확한 카메라 위치 추정 데이터를 제공하고, 수행 시간이 긴 Mapping은 특정한 조건을 만족시키는 좋은 Frame에 한하여 수행한다. PTAM은 이와 같은 방법으로 수행 시간을 대폭 감소시켜 AR Workspace에 적합한 SLAM 기술이다.

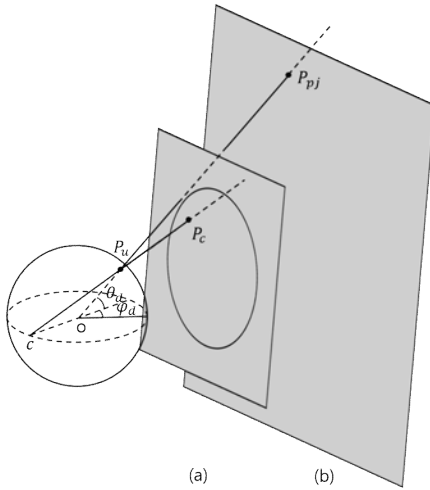
기존의 구면 SLAM의 구현을 위한 방법은 Unified Sphere Model을 사용하며 앞면 시야각만 제공할 수 있는 한계가 있다. 본 논문은 Spherical Panorama Video를 입력 이미지로 하는 PTAM의 구현을 위해 전 방향을 모두 활용할 수 있는 카메라 모델의 설계 방법을 제안한다. 본 논문에서 제안하는 카메라 모델은 구형의 이미지의 전면과 후면 반구를 각각 투영시킨 듀얼 영상 평면을 사용한다. 이는 전방과 후방 모두 시야각에 제약이 없기 때문에

전체 시야각을 지원한다. 또한 기존의 PTAM과 동일한 핀홀 모델을 기반으로 설계함으로써 PTAM에 적용하는 과정에서 평면 연산식을 직접 사용할 수 있는 장점이 있다.

2. 구면 PTAM을 위한 카메라 모델

핀홀 모델은 가장 잘 알려졌으며, 가장 많은 연구가 이루어지고 있는 카메라 모델이다. 따라서 핀홀 모델에 기반한 투영 모델은 다양한 기존의 시스템과 호환을 이룰 수 있다. 본 장에서는 구면 파노라마 이미지를 핀홀 모델에 투영하고, 최대한의 영역을 투영할 수 있는 내부 파라미터를 설계하는 방법을 제안한다.

2.1 카메라 모델 설계



(그림 1) 카메라 투영 모델: (a) Unified Sphere Model, (b) Pinhole Model

실제 세계의 한 점 $P_w = [x_w, y_w, z_w]^T$ 을 깊이 z_{pj} 인 핀홀 투영 평면상의 한 점 $P_{pj} = [x_{pj}, y_{pj}, z_{pj}]^T$ 로 투영하기 위한 공식은 식 (1)과 같다.

$$P_{pj} = AC \begin{bmatrix} P_w \\ 1 \end{bmatrix} = \begin{bmatrix} f_x & scf_x & c_x \\ 0 & f_y & c_y \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} r_{11} & r_{12} & r_{13} & t_1 \\ r_{21} & r_{22} & r_{23} & t_2 \\ r_{31} & r_{32} & r_{33} & t_3 \end{bmatrix} \begin{bmatrix} x_w \\ y_w \\ z_w \\ 1 \end{bmatrix} \quad (1)$$

여기서 A 는 카메라의 내부 파라미터이며, f_x 와 f_y 는 초점거리, c_x 와 c_y 는 주점, scf_x 는 비대칭계수이다. C 은 카메라의 외부 파라미터로 회전벡터 행렬과 평행이동 변환 행렬의 조합이다. 이는 실제 세

계의 한 점과의 변환 공식이므로, 이미 얻어진 구면 파노라마 이미지에서의 한 점 $P_s = [x_s, y_s]^T$ 을 핀홀 투영 평면상의 한 점 P_{pj} 로 변환하는 방법을 알아야 한다. 이 변환을 위해서는 데카르트 좌표계에서 벗어나 극 좌표계에서의 계산이 필요하다. 우선, 구면 파노라마 이미지의 정 중앙 지점을 경도(ϕ)와 위도(θ)가 0인 지점이라 하고 이미지의 크기를 S 라 할 때 P_s 을 극 좌표계에서의 점 $P_l = [\phi_l, \theta_l]^T$ 로 변환해야 한다.

$$P_l = \begin{bmatrix} x_s 2\pi / S_x - \pi \\ y_s \pi / S_y - \pi/2 \end{bmatrix}, \quad (2)$$

그 후 P_l 은 유클리드 공간에서 3차원 좌표를 갖는 한 점 $P_u = [x_u, y_u, z_u]^T$ 로 변환이 가능하다.

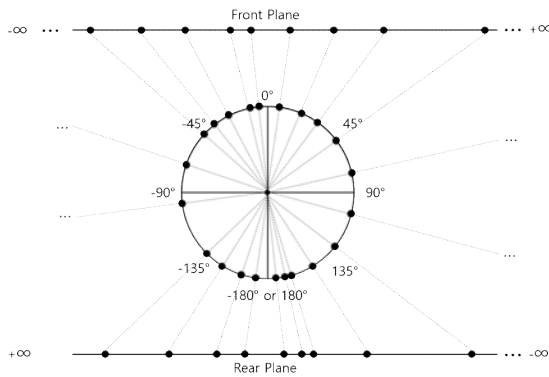
$$P_u = \begin{bmatrix} \cos \theta_d \cos \phi_d \\ \cos \theta_d \sin \phi_d \\ \sin \theta_d \end{bmatrix}, \quad (3)$$

P_u 은 반지름이 1인 3차원 구에서의 좌표이다. 구면 파노라마 이미지상의 모든 점을 위의 과정으로 투영하여 원하는 각도로 선형 회전 변환을 하고 한 축을 제거한 후 적절한 배율을 곱해준다면 Fisheye Image가 된다. 따라서 Fisheye Image의 경우 여기서부터 투영 과정을 수행하면 된다. 핀홀 모델에서는 구면 파노라마 이미지의 모든 영역을 투영할 수 없으므로 투영하고자 하는 부분의 경도와 위도를 정해 부분적인 투영을 해야 한다. 투영하고자 하는 부분의 경도와 위도를 각각 ϕ_r , θ_r 라 할 때 식 (4), (5)와 같은 방법으로 핀홀 투영 이미지상의 점 $P_{pj} = [x_{pj}, y_{pj}, z_{pj}]^T$ 을 구할 수 있다.

$$P_{ru} = \begin{bmatrix} \cos \theta_r & 0 & \sin \theta_r \\ 0 & 1 & 0 \\ -\sin \theta_r & 0 & \cos \theta_r \end{bmatrix} \begin{bmatrix} \cos \phi_r - \sin \phi_r & 0 \\ \sin \phi_r & \cos \phi_r & 0 \\ 0 & 0 & 1 \end{bmatrix} P_u, \quad (4)$$

$$P_{pj} = s \left[\frac{y_{ru}}{x_{ru}}, \frac{z_{ru}}{x_{ru}}, 1 \right]^T. \quad (5)$$

이렇게 구해진 P_{pj} 은 적절한 Z축 깊이 s 를 지정함으로써 육안으로 확인할 수 있는 이미지로 사용이 가능하다.

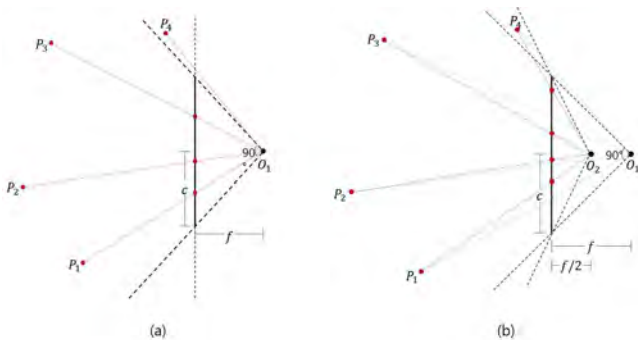


(그림 2) 듀얼 영상 평면 투영

본 논문에서 제안하는 시스템은 구의 전면 반구와 후면 반구를 투영시킨 두 장의 핀홀 투영 이미지를 획득할 것이므로 식 (4)에서 (ϕ_r, θ_r) 에 각각 $(0, 0)$, $(\pi, 0)$ 을 대입한 투영 이미지를 두 장 획득한다.

2.2 내부 파라미터 설계

일반적인 핀홀 투영 모델에서의 투영 구조는 식 (1)과 같다. 이 중 내부 파라미터 A 은 캘리브레이션을 통해 구하게 된다. 우선 2.1과 같은 방법으로 구면 파노라마 이미지를 화각이 90° 인 핀홀 카메라에 투영하여 얻어낸 평면 영상이 있다고 가정하자. 해당 영상의 캘리브레이션을 통해 내부 파라미터를 얻는다면 (그림 3)과 같은 투영 법칙이 성립할 것이다.



(그림 3) 초점거리에 따른 투영 법칙의 변화 : (a) 90° 화각 투영, (b) 초점거리가 변했을 때의 투영

(그림 3)의 (a)에서 점 P_1, P_2, P_3 은 이미지 평면에 도달해 픽셀로 자리 잡지만, P_4 의 경우는 90° 의 각에 들어오지 않아 이미지 평면에 자리 잡지 못한다. 하지만, 만약 모든 내부 파라미터가 같은 채 초점거리 f 가 짧아진다면 다른 결과를 가져온다. (그림 3)의 (b)는 다른 내부 파라미터는 그대로 둔 채 초점거리를 두 배 줄였을 때의 모습이다. 점 $P_1,$

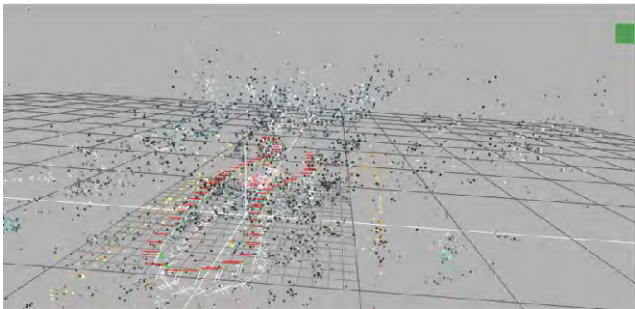
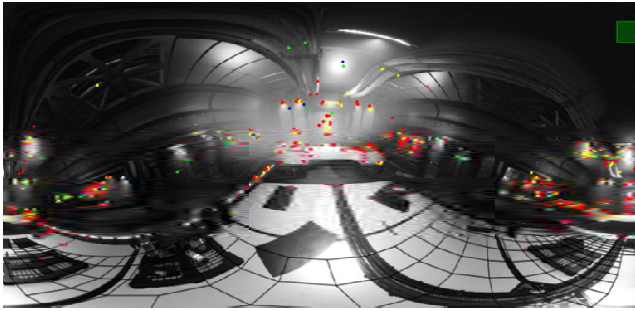
P_2, P_3 의 투영 지점은 중심에 가까워졌으며, 초점거리를 f 로 설정하였을 때 이미지 평면 안에 들어오지 않았던 P_4 역시 이미지 평면에 들어온 것을 볼 수 있다. 이는 화각이 더욱 넓어진 것을 뜻한다. 이때, 카메라 화각을 θ 라 할 때, $\cos(\theta/2) = f/c$ 이므로, θ 와 초점거리 f 사이에 다음과 같은 식이 성립한다.

$$\theta = 2\arccos\left(\frac{f}{c}\right). \quad (6)$$

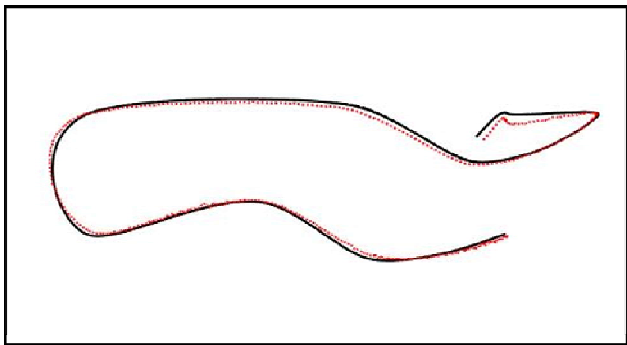
따라서, f 가 짧아지면 카메라 화각은 늘어나게 되고, f 가 0에 수렴하면 카메라 화각은 180° 가 된다. 만약 $f = n$ 일 때 화각이 90° 라면, $f = n/10$ 일 때 화각은 약 172° 가 나오고, $f = n/20$ 일 때 화각은 약 176° 가 나온다.

3. 실험 결과

카메라 투영 모델이 올바르게 적용되는지 확인하기 위해 PTAM에 적용시켜 Tracking 상태를 점검하였다. 만약 좋은 Tracking 결과가 나온다면 해당 투영 모델은 올바르게 적용되어 동작하는 것이다. 실험은 3.40GHz Intel(R) Core i7-6700 CPU와 32.0GB RAM의 사양을 가지는 Desktop PC를 통해 진행했으며, Windows 운영체제 환경에서 진행하였다. PTAM은 매 프레임 프레임마다 영상 정보를 포함한 다양한 정보를 함축한 Keyframe 구조체를 생성하고 이것을 기반으로 동작하는데, 이 때 한 개의 Keyframe은 한 장의 프레임 이미지만을 사용한다. 본 논문에서 제안하는 카메라 투영 모델은 한 프레임 당 전면과 후면 두 장의 이미지를 가지기 때문에 이에 맞게 한 프레임 당 전면과 후면에 관한 두 번의 처리를 할 수 있도록 PTAM의 내부 코드를 일부 변형하였다. 또한, PTAM 내부에 들어가는 많은 연산은 본 논문에서 제안하는 투영을 진행한 후 하였지만, 초광각의 핀홀 평면을 이미지로 표현하는 것은 가시성이 떨어지며 그 사이즈가 매우 크기 때문에 최종적인 출력 이미지와 그 위에 표시되는 특징점 등은 다시 구면 파노라마 형태로 투영하여 보여주도록 설계하였다. 실험은 정확한 Ground Truth를 획득하기 위해 언리얼 엔진 상에서 제작한 3D 가상 환경에서 진행하였다.



(그림 4) 가상 세계의 프레임과 3D 맵



(그림 5) Ground Truth(검은 선)와 추정 경로(빨간 선)

(그림 4)는 3D 가상 환경에서 촬영한 비디오를 통해 실측 경로와 구면 PTAM이 추정한 경로를 비교한 것이다. 실험을 위한 시스템은 62개의 키프레임과 5802개의 Map Point를 가졌다. 실측 경로는 언리얼 엔진에서의 길이 단위를 기준으로 측정하였다. 실측 경로와의 RMSE는 0.0770m이다. 오차는 1.38cm/m로 좋은 위치 추정 상태를 보였다. 이는 카메라 투영 모델이 올바르게 설계되어 동작함을 보여주는 결과이다.

4. 결론

본 논문에서는 AR 시스템에 적합한 구면 PTAM 구현을 위한 카메라 모델 설계 방법을 제안하였다. 이 과정에서 높은 수행 속도를 유지하였으며, 정확한 동작을 통해 PTAM의 위치 추정 정확도를 유지

하였다. 본 논문의 아이디어는 기존의 PTAM과 같은 투영 모델로 변환함으로써 호환성이 우수하고 정확한 법칙에 의해 동작하는 모델을 설계했다는 점에서 독창성이 있다.

Acknowledgments

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. NRF-2019R1F1A1060828).

참고문헌

- [1] David Caruso, Jakob Engel, Daniel Cremers “Large-Scale Direct SLAM for Omnidirectional Cameras” In Proceedings of IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), pp.141-148, 28 September-2 October 2015.
- [2] David Valiente, Arturo Gil, Luis Paya, Jose M. Sebastian, Oscar Reinoso “Robust Visual Localization with Dynamic Uncertainty Management in Omnidirectional SLAM” Applied Science, 1294, 2017.
- [3] Alejandro Rituerto, Luis Puig, J. J. Guerrero “Comparison of omnidirectional and conventional monocular systems for visual SLAM” 10th OMNIVIS with RSS, 2010.
- [4] Jianfeng Li, Xiaowei Wang, Shigang Li “Spherical-Model-Based SLAM on Full-View Images for Indoor Environments” Applied Science, 2268, 2018.
- [5] Georg Klein, David Murray “Parallel Tracking and Mapping for Small AR Workspaces” In Proceedings of the 6th IEEE and ACM ISMAR, Vol. 17, No. 4, pp.225-234, 13-16 November 2007.

바퀴변형과 센서를 이용한 안정적 계단이동 로봇의 설계

박성현*, 김상훈*

*한경대학교 전기전자제어공학과
psh_mail@naver.com , kimsh@hknu.ac.kr

Design of a stable stair-moving robot using wheel deformation and sensors

Sung-Hyun Park*, Sang-Hoon Kim*

*Dept. of Electrical, Electronic and Control Engineering, HanKyong Nation
University

요 약

본 논문은 안정적으로 계단을 주행하는 로봇에 관한 연구로 바퀴변형 시스템의 설계 방법을 제시하고, 기존의 계단극복 로봇의 문제점 중 하나인 계단 주행 시 발생하는 추락을 IMU센서와 서보모터를 이용한 방지법과 아날로그 IR센서를 통한 간단하고 빠르게 계단을 감지하는 방법을 제시한다.

1. 서론

과거 이동로봇은 일부 제한된 곳에서만 활용이 되었으나 현재 이동로봇의 응용 분야는 재난현장과 같이 위험한 환경에서 인간을 대체하여 작업하거나, 인간 생활에서의 특정 서비스 수행 등 이동로봇의 응용범위가 점점 넓어지고 있다. [1] 이처럼 다양한 환경에서 로봇이 성공적으로 작업을 수행하기 위해서는 빠른 기동성과 계단을 주행할 수 있는 능력이 필요하다.



(그림 1) 소프트뱅크社의 pepper와 Transcend Robotics 社의 ARTI3

하지만 기존 로봇의 경우 Fig 1과 같이 계단 주행 자체가 되지 않거나[2] 설령 계단을 주행할 수 있더라도 기동성이 느리거나 불안정한 주행을 하는 문제점을 가지고 있는 것을 볼 수 있다.[3] 물론, 위와 같은 문제점을 해결하기 위한 다양한 연구들 또한 진행 되었다. 그 중 대표적인 계단로봇인 Turboquad[4]의 경우 Fig 2와 같이 바퀴가 절반으로 나뉘어 Leg로 변하는 휠을 이용하여 빠른 바퀴변형과 기동성을 가지는 장점을 볼 수 있다. 하지만 로봇이 극복 가능한 계단의 높이가 매우 낮아 계단 주行的 한계가 발생하고, 계단 주행 시 로봇의 안정성 또한 떨어진다.



(그림 2) Turboquad 휠 변형 과정

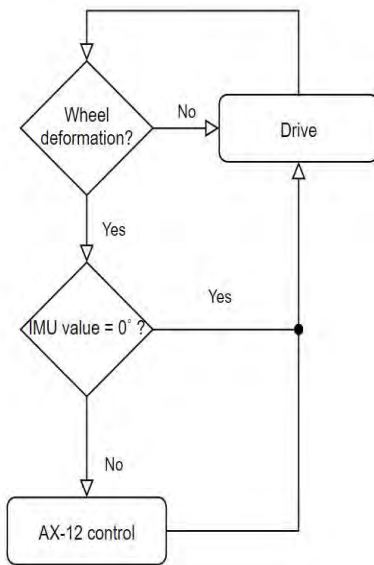
따라서 본 논문에서는 로봇이 계단을 주행할 때 기존 로봇의 문제점을 센서를 통해 보완하여 더욱 안정적인 주행과 바퀴변형 메커니즘을 이용하여 빠른 기동성을 구축하고, 아날로그 센서를 통해 비교적 간단한 방법으로 장애물 중 계단을 빠르게 감지하는 방법을 통해 기존의 로봇보다 더욱 실용적인

로봇 설계를 제시한다.

2. 본론

2.1 로봇 구조 및 메커니즘

개발하고자 하는 로봇의 메커니즘은 다음과 같다. 계단이 감지될 경우 MCU에서 서보모터로 정해진 명령을 주고, 이에 따라 바퀴가 변형된다. 그 후 로봇의 가운데에 있는 서보모터를 IMU센서를 통해 실시간으로 제어하고 계단 주행 시 무게중심을 계속해서 변경하여 안정적인 계단 주행을 한다.



(그림 2) 로봇 주요 기능 알고리즘

2.2 바퀴의 기구적 설계

계단을 극복할 수 있으면서 빠른 기동성을 가진 로봇을 설계하기 위해 Fig 3과 같이 일반적인 Wheel에서 Legged-wheel로 변형이 가능한 바퀴변형 시스템을 채택하였다. [5]

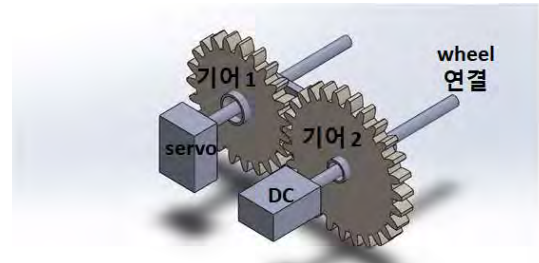


(그림 3) 일반적 Wheel(위)과 변형한 형태인 Legged-wheel(아래)

Wheel의 전체 반경의 크기는 12.5cm이고 Leg-wheel로 변형했을 때의 전체 크기는 21.5cm이다. 이때, Legged-Wheel이 극복 가능한 계단의 높이는 전체 Wheel 반지름에 2.6배를 곱한 값이 된다. 따라서 $6.5 \times 2.6 = 16.25\text{cm}$ 로 최대 극복 가능한 계단의 높이는 16.25cm로 계산되고, 이는 건축물의 피난·방화구조 등의 기준에 관한 규칙(약칭: 건축물 방화구조규칙)[6]에 명시되어 있는 실내 건축물 계단의 높이를 극복 가능한 수치이다.[7]

2.3 바퀴변형 제어시스템

본 논문에서 제시한 바퀴변형을 시행하기 위해서는 Fig 4와 같은 이중 기어 방식의 메커니즘을 선택하였다. [8]



(그림4) 이중 기어 방식의 메커니즘

DC 모터 축의 경우 바퀴가 회전하여 주행하는 역할을 하고, 서보모터 축의 경우 MCU를 통해 특정 신호를 받으면 정해진 명령을 통해 작동하며 바퀴가 Legged-wheel로 변형한다.

이러한 방법으로 바퀴변형을 하기 위해서는 서보모터가 로봇의 무게를 들어 올릴 수 있을 정도의 충분한 토크가 필요하다. 무게의 경우 Fig 5와 같이 최소(m_{\min}) 1630g 이고 최대(m_{\max}) 1890g 이다. 바퀴변형 시 로봇이 들어 올려지는 높이(h)는 최소(h_{\min}) 0.06m이고 최대(h_{\max}) 0.08m, 바퀴가 회전하는 각도(θ)는 50° 로 0.872rad로 측정이 된다.[9]



(그림5) 로봇의 부품과 무게

따라서 식 (1)과 식 (2)와 같이 계산하여 바퀴변형을 위해 필요한 토크는 최소 $11.22\text{kgf}\cdot\text{cm}$ 이상의 토크로 고려 되고, $17.34\text{kgf}\cdot\text{cm}$ 이상의 토크를 사용하는 것이 권장된다. [10]

$$W_{\min} = 9.8 \times m_{\min} \times h_{\min} \approx 0.96\text{J}$$

$$T_{\min} = \frac{J}{\theta} = \frac{0.96\text{J}}{0.872\text{rad}} \approx 1.1\text{N}\cdot\text{m}$$

$$\therefore T_{\min} = 1.1\text{N}\cdot\text{m} \times 10.2\text{kgf}\cdot\text{cm} = 11.22\text{kgf}\cdot\text{cm}$$

(식 1) 최소 토크 T_{\min} 값

$$W_{\max} = 9.8 \times m_{\max} \times h_{\max} \approx 1.48\text{J}$$

$$T_{\max} = \frac{J}{\theta} = \frac{1.48\text{J}}{0.872\text{rad}} \approx 1.70\text{N}\cdot\text{m}$$

$$\therefore T_{\max} = 1.70\text{N}\cdot\text{m} \times 10.2\text{kgf}\cdot\text{cm} = 17.34\text{kgf}\cdot\text{cm}$$

(식 2) 최대 토크 T_{\max} 값

Fig 6은 바퀴변형 시 필요한 초기값 설정과 명령 코드를 나타낸다. 초기설정의 경우 서보모터를 작동하기 위해 적절한 프리스케일과 주기를 적용하였고, 바퀴변형 인터럽트가 발생하면 MCU와 서보모터가 연결된 핀의 PWM 값을 250~1250 만큼 변화시킴으로써 바퀴변형을 진행하도록 코드를 설계한다.

```

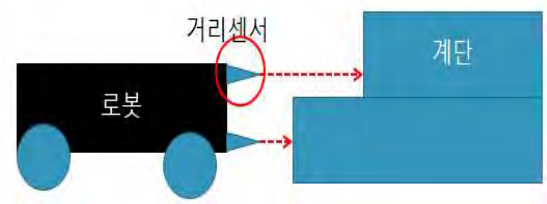
29 /* TIM2 init function */
30 void MX_TIM2_Init(void)
31 {
32     TIM_ClockConfigTypeDef sClockSourceConfig = {0};
33     TIM_MasterConfigTypeDef sMasterConfig = {0};
34     TIM_OC_InitTypeDef sConfigOC = {0};
35
36     htim2.Instance = TIM2;
37     htim2.Init.Prescaler = 168-1;
38     htim2.Init.CounterMode = TIM_COUNTERMODE_UP;
39     htim2.Init.Period = 20000-1;
40     htim2.Init.ClockDivision = TIM_CLOCKDIVISION_DIV1;
41     htim2.Init.AutoReloadPreload = TIM_AUTORELOAD_PRELOAD_DISABLE;
42     if (HAL_TIM_Base_Init(&htim2) != HAL_OK)
43     {
44         Error_Handler();
45     }
46
47     while (1)
48     {
49         HAL_TIM_PWM_Start(&htim2, TIM_CHANNEL_1); //servo pwm start
50         for (int i = 250; i<1250; i++) {
51             __HAL_TIM_SET_COMPARE(&htim2, TIM_CHANNEL_1, i);
52             HAL_Delay(10);
53         }
54     }

```

(그림 6) 서보모터 초기설정 및 제어코드

2.3 계단 감지

본 논문에서는 아날로그적 방식의 감지를 이용하여 다양한 장애물 중 빠르고 비교적 단순하게 계단을 감지하는 방법을 제시한다. Fig 7과 같이 로봇의 전면의 상단과 하단에 아날로그 센서를 설치하고 두 개의 아날로그 센서 데이터의 차를 구한값이 건축물 방화구조규칙에서 제시한 계단의 단 너비인 26cm 이상의 값이 나오면 계단으로 감지하고 바퀴변형을 진행 후 주행을 진행한다.



(그림 7) 계단 감지 메커니즘

2.4 자세제어 시스템

바퀴변형을 통해 계단을 주행하는 로봇이나, 캐터필러를 기반으로 하는 로봇 등 기존의 계단을 극복하는 로봇들에서 볼 수 있는 문제점은 어느 정도 경사가 있는 계단을 주행하는 경우 낙하를 하는 모습을 볼 수 있다. 이러한 문제점은 주행 시 무게중심이 한쪽으로 집중되어 생기는 문제점으로 본 논문에서는 Fig 8과 같이 로봇 가운데에 서보모터로 구성된 관절을 설치하고, IMU센서를 통해 기울어짐을 인식하면 실시간으로 로봇의 서보모터를 조절하여 무게중심을 이동시키는 방법을 제시한다.



(그림 8) 자세제어 메커니즘

Fig 9는 IMU센서의 헥사 출력값을 MCU로 받아 실시간으로 서보모터를 제어하는 코드이다. 본 로봇에서는 Roll 값을 통해서 서보모터의 듀티비(Duty Ratio)를 조절하였다.

```

185 void HAL_UART_RxCpltCallback(UART_HandleTypeDef *huart)
186 {
187     if(huart-> Instance == USART1)
188     {
189         HAL_UART_Receive_IT(&huart1, &rx_data, 10);
190         EulerRoll = (rx_data[2]<<8)|rx_data[3];
191         EulerPitch = (rx_data[4]<<8)|rx_data[5];
192         EulerYaw = (rx_data[6]<<8)|rx_data[7];
193
194         Roll = EulerRoll/100.0;
195         Pitch = EulerPitch/100.0;
196         Yaw = EulerYaw/100.0;
197
198         rr = Roll;
199         duty = 604+4/9+(rr-1)*(40/9);
200
201         //led off
202         HAL_GPIO_WritePin(GPIOB, GPIO_PIN_4, GPIO_PIN_SET);
203
204         // servo controll code
205         HAL_TIM_SET_COMPARE(&htim2, TIM_CHANNEL_1, duty);
206     }
207 }
208
209
210
211 }

```

(그림 9) 자세제어 코드

3. 실험 및 분석

앞서 설명한 방법으로 설계를 진행하면, 로봇의 일반 주행시 초당 2.5cm를 주행하는 모습을 볼 수 있다. 계단 주행의 경우 낮은 계단은 칸당 1~2초의 시간이 걸리고, 높은 계단의 경우 칸당 2~3초의 시간이 걸리는 모습을 볼 수 있다. 또한, 로봇이 오르내리는 경우 로봇이 계단을 올라가는 주행을 진행할 때에는 실시간 로봇 관절제어에는 무리가 없지만 내려가는 주행을 진행할 때 발생하는 급격하고 빠른 높이 감소와 같은 갑작스러운 환경변화에 로봇의 제어속도가 따라가지 못하는 상황이 발생한다.

4. 결론 및 향후 연구 방향

본 논문에서는 바퀴변형에 필요한 바퀴 설계와 제어시스템을 제시하고, 아날로그 거리 센서를 통한 계단 감지 메커니즘을 통해 안정적인 계단 주행과 감지하는 방법을 고안 하였다. 이러한 방법을 사용해도 로봇의 안정성과 계단을 주행하기 위해 설계한 로봇의 크기 문제, 아날로그 센서의 단순한 감지에 따라오는 계단 감지의 한계, 로봇제어의 속도와 같은 또 다른 문제점을 새로 일으킨다. 향후 연구에서는 역 푸아송 비 구조(Negative Poisson's Ratio)[11]를 바탕으로 로봇의 크기를 제어하는 연구와 아날로그 센서의 값을 정확한 디지털 거리의 값으로 변환

하여 로봇과 장애물과의 거리를 더 정확하고 빠르게 감지해, 그 결과를 통해 로봇의 행동을 제어하는 방법, 로봇이 계단을 이동할 때 생기는 변화값에 대해 데이터를 먼저 얻을 수 있는 방법에 관한 연구가 진행되어야 한다.

참고문헌

- [1] 이재웅, 현웅근, 서희현, 서동진, 류영곤 “센서 융합에 의한 이동로봇 위치 인식 및 제어”, 2017년 대한전자공학회 춘계학술대회
- [2] Available at :https://www.softbankrobotics.com/emea/en/papper?utm_source=robots.ieee.org
- [3] Available at :<https://www.solvelight.com/product/arti3-mobile-robot-platform/>
- [4] Wei-Hsi Chen, Hung-Sheng Lin, Pei-Chun Lin, “TurboQuad: A Novel Leg - Wheel Transformable Robot With Smooth and Fast Behavioral Transitions”, IEEE Transactions on Robotics, 2017년
- [5] 김유석, 김한, 정광필, 김성한, 조규진, 주종남 “협지 주행용 소형 로봇을 위한 바퀴의 설계”, 한국정밀공학회지, 제 30권, 1호, p32-38, 2013년
- [6] 건축물의 피난·방화구조 등의 기준에 관한 규칙(약칭: 건축물 방화구조규칙), Available at :<https://glaw.scourt.go.kr>
- [7] 김유석, 김한, 하경호, 주종남, “동적 모델링 분석을 통한 변신바퀴 로봇의 최적설계”, 한국정밀공학회지, p1489-1490, 2013년
- [8] Long Bai, Jian Guan, Xiaohong Chen, Junzhan Hou, Wenbo Duan, “An optional passiveactive transformable wheel-legged mobility concept for search and rescue robots”, Robotics and Autonomous System, p145-155, 2018년
- [9] AHMAD FAIZ BIN FADZIL, “STAIR CLIMBING MOBILE ROBOT (SCMOR)”, 2010년
- [10] Available at : <http://study.zum.com/book/12025>
- [11] 송원호, 김진원, 사공지혁, 정현경, 주백석 “역푸아송비를 사용한 크기조절 로봇”, 한국기계가공학회 춘계학술대회 논문집, 275-275, 2019년

코로나 19에 대해 일일 브리핑을 하는 정부 관계자의 목소리 특징 분석

조일영*, 이선경**, 조동욱***

*중원대학교 생체의공학과

**한국교통대학교 의료IT공학과

***충북도립대학교 생체신호분석연구실

whdlfdud0104@gmail.com, dltjsrud1@naver.com, ducho@cpu.ac.kr

Analyzing the Characteristics of Voices of Government Officials Giving a Daily Briefing on covid-19

Il-Yeong Cho*, Sun-Kyung Lee**, Dong-Uk Cho***

*Dept. of Biomedical Engineering, Jung-Won University

**Dept. of Medical IT Engineering, Korea National University of
Transportation

***Lab. of Bio-Signal Analysis, Chung-Buk Provincial University

요 약

최근 중국으로 인해 코로나19 바이러스가 전 세계로 퍼지면서 각 나라에 큰 위협이 되고 있다. 이에 대한민국의 국민들은 매일 코로나 바이러스 확진자와 사망자, 그리고 대처방안에 대한 브리핑을 정부 관계자로부터 듣고 이를 시행하고 있다. 본 논문에서는 코로나바이러스에 대해 브리핑을 하는 정부 관계자의 음성이 어떤 특징이 있는가를 규명해 보고자 한다.

1. 서론

작년 말 중국이 퍼트린 코로나 변형 바이러스[1]인 코로나 19 바이러스가 각 나라에 퍼지면서 국민들을 위협하고 있다. 우리나라 공항에서 잠복된 바이러스를 가지고 국내에 들어오는 것을 시작으로 바이러스가 전국으로 확산이 되었다. 이에 따라 정부에서는 국민들에게 마스크 착용은 권유했고 사회적 거리두기[2]라는 활동을 시행하였다. 현재 안정권에 들어 가 있는 상황에서 이 같은 상황은 코로나 바이러스의 현 상황과 대처방안을 매일 브리핑 한 사람들에게 대한 신뢰도를 믿고 이를 실천한 것이 크게 한 역할을 한 것으로 추정된다. 본 논문에서는 국가재난안전대책본부의 김강립 1 총괄조정관에 대한 음성 특징을 분석하여 이들의 음성이 우리에게 어떤 영향을 주었는지에 대해 규명하고자 한다.

2. 실험에 사용한 음성 분석 요소

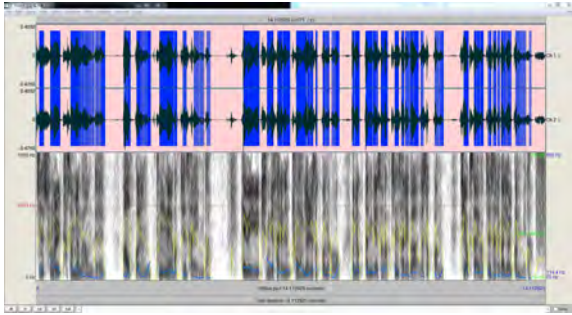
목소리 분석에 사용한 음성 분석 요소로는 음높이 관련 항목과 화자의 신뢰도에 대한 항목인 진폭변동률 주파수 변화율, NHR[3]을 실험에 적용하였

다. 또한 말을 할 시 음성에 실리는 에너지[4]와 발화속도 분석을 통해 실험대상자의 음성 특징을 규명해 보고자 한다. 음성 분석기로는 프라트를 사용하였다[5].

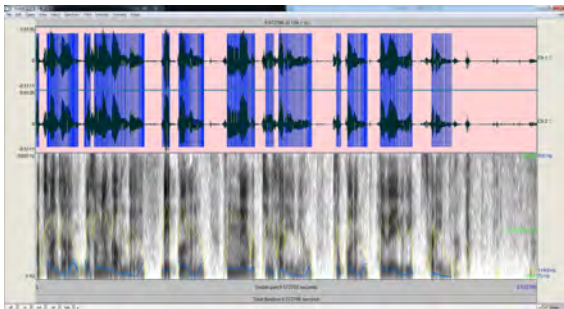
3. 실험 및 고찰

우선 국가재난안전대책본부 김강립조정관의 음성 특징을 규명하기 위한 실험 결과를 샘플링한 날자별로 [그림 1] - [그림 5]에 보인다. 아래 그림에서 알 수 있듯이 김강립조정관의 음성 특징은 음높이의 변화폭을 작게 가져간다는 것이다. 낮은 음높이와 음높이 변화폭을 적게 하여 차분함을 유지하여 청자로 하여금 안정감을 느끼게 한다. 아울러 높은 DoVB, 천천히 말하는 발화속도, 신뢰감이 들게 하는 주파수변동률과 진폭변동률, NHR의 수치를 보이고 있다. 또한 음성 에너지의 크기를 작게 함으로서 부드러움을 느끼게 하고 있다. 결론적으로 김강립조정관의 브리핑은 청자로 하여금 안정감, 신뢰감, 진중함과 부드러움을 느끼게 하여 국민들이 브리핑 내용대로 따라 하면 문제가 없을 것이라는 느낌을 갖게 하는 음성 구사력을 보이고 있다. 실험 결과를

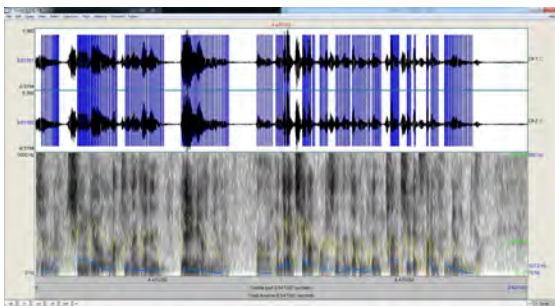
다음 <표 1>에 나타내었다.



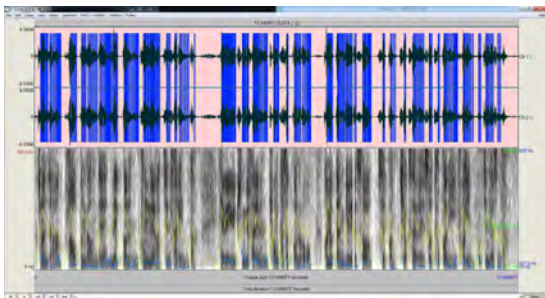
[그림 1] 4월 13일 브리핑에 실험결과



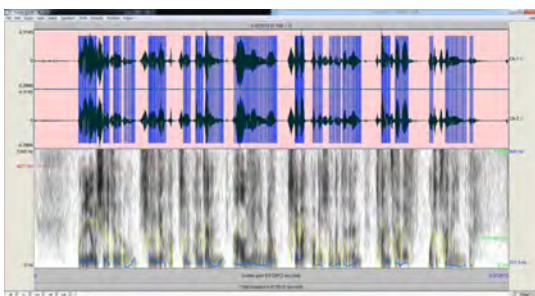
[그림 2] 4월 24일 브리핑에 대한 실험결과



[그림 3] 4월 27일 브리핑에 대한 실험결과



[그림 4] 4월 29일 브리핑에 대한 결과



[그림 5] 5월 1일 브리핑에 대한 결과

<표 1> 실험 결과 표

	Pitch mean [Hz]	Pitch min [Hz]	Pitch max [Hz]	Bandwidth [Hz]	Jitter [%]	Shimmer [dB]	Intensity [dB]	NHR [%]	DoV [%]	Speech speed
4월 13일	116.651	76.456	200.053	123.597	2.3	1.005	68.09	0.230	43.166	140
4월 24일	119.822	82.385	184.324	178.7939	2.32	0.897	69.18	0.180	29.576	203
4월 27일	117.755	75.817	187.532	111.715	2.384	1.177	62.16	0.222	29.442	205
4월 29일	107.568	75.789	190.655	114.866	2.329	1.063	69.79	0.221	40.365	150
5월 1일	101.482	75.305	160.623	85.318	2.506	1.095	62.38	0.187	34.029	180
평균값	112.6556	77.1504	184.6374	122.857	2.367	1.047	66.32	0.285	35.315	175

4. 결론

본 논문에서는 코로나19 바이러스에 대한 정부 관계자의 일일 브리핑에 대해 대표적 정부관계자인 김강립조정관에 대한 음성 특징을 규명하였다. 낮은 음높이와 그 변화폭 그리고 부드러움을 느끼게 하는 음성 에너지로 지시사항이 아닌 함께 할 협조사항이라는 느낌을 주었으며, 신뢰도 관련 수치, 발화속도를 통해 청자로 하여금 안정감, 진중함을 느끼게 하는 음성임을 규명해 낼 수 있었다.

참고문헌

- [1] http://ncov.mohw.go.kr/baroView.do?brdId=4&brdGubun=41&dataGubun=&ncvContSeq=&contSeq=&board_id=&gubun=
- [2] <https://terms.naver.com/entry.nhn?docId=5928099&cid=43667&categoryId=43667>
- [3] D. U. Cho, "The communicability observations of broadcasting programs MC by extracting voice feature," *J. KBS*, vol. 59, no. 6, pp. 36-73, Dec. 2009.
- [4] D. U. Cho, et al., "Study of the effect of voice transmission change on announcer speech repetition learning," *J. KICS*, vol. 43, no. 03, March, 2018.
- [5] B. G. Yang, *Theory and Practice of speech Analysis Using Praat*, Masu Publishing Co., 2003.

차량번호판 영역 추출 방법론 비교 분석

이은지*, 박영호**

*숙명여자대학교 IT공학전공

**숙명여자대학교 빅데이터 연구센터

lej9031@sm.ac.kr, yhpark@sm.ac.kr

Comparison of methodologies for license plate recognition

Eun-Ji Lee*, Young-Ho Park**

*Dept. of IT Engineering, Sookmyung Women's University

**Bigdata Using Research Center, Sookmyung Women's University

요 약

최근, 국내 자동차 보유율은 매년 증가하고 있으며, 자동차 증가율에 따라 자동차로 인한 사건, 사고 발생률 또한 증가하고 있다. 국가에서도 지능형교통시스템(ITS) 중 차량 번호판을 인식하는 연구가 활발히 진행되고 있다. 차량 번호판 인식은 사건·사고 발생 차량을 추적하거나 주차 무인시스템 등의 분야에 적용된다. 본 논문에서는 차량 번호판 영역을 추출하기 위한 여러 가지 방법들을 비교 분석하여 각 상황에 맞는 알고리즘을 적용하고자 한다.

하이브리드 차량 번호판 인식 알고리즘을 제시한다. 마지막으로 6장에서는 결론을 맺는다.

1. 서론

국내 자동차 등록 현황은 매년 증가하고 있으며, 국토교통부 보도에 따르면 우리나라 인구 2.19명 당 자동차를 1대 보유하고 있음을 밝혔다. 차량 수가 증가함에 따라 교통사고, 차량 도난, 주차장 부족 등 자동차에 관련된 사건, 사고가 증가하고 있다. 이러한 문제의 대안 중 하나로 CCTV가 있으며 도로 위 CCTV를 통해 과속을 방지하거나 돌발 상황을 감지할 수 있다. 하지만 CCTV만으로 도로 위 상황을 통제하기에는 부족하며, 4차 산업이 발달하면서 교통 분야 또한 지능형교통시스템(ITS)을 위한 연구가 활발히 진행되고 있다. 차량 번호판 인식은 지능형 교통시스템에서 기본이 되는 기술 중 하나이며, 주차·속도 단속 등 도로 위에서 발생하는 각종 사건, 사고에 응용된다. 본 논문은 기존의 차량 번호판을 인식하기 위한 기술들을 설명하고 비교함으로써 다양한 상황에 적합한 알고리즘을 실행할 수 있는 하이브리드 차량 번호판 인식 알고리즘을 제안한다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 차량 번호판 인식을 위한 프로세스를 설명하고 3장에서는 차량 번호판 영역 추출을 위해 사용하는 방법을 설명한다. 4장에서는 차량 번호판 영역 추출을 위한 방법론을 비교 분석을 하고 5장에서는 새로운

2. 차량번호판 인식을 위한 프로세스

본 장에서는 차량 번호판 인식을 위한 프로세스를 설명한다. 차량 번호판 인식 프로세스는 크게 차량 번호판 영역 추출과 문자 영역추출 및 문자 인식 과정으로 나뉘며[1], 세부적인 프로세스는 5단계로 설명한다. 첫째, 차량 번호판 이미지를 획득한다. 둘째, 이미지에서 차량 번호판 영역을 추출한다. 셋째, 추출된 번호판 영역 전처리 과정을 거친다. 넷째, 번호판에서 문자 부분 영역을 추출한다. 다섯째, 문자를 인식하며 마무리한다. 본 논문에서는 차량 번호판 인식 과정 중 번호판 영역을 추출하는 단계의 방법론을 비교하고 분석하여 인식률을 높일 수 있는 방안을 도출하고자 한다.

3. 차량 번호판 영역 추출

차량 번호판 영역 추출을 위한 방법은 컬러 모형을 이용하여 번호판을 추출하는 방법[2], 명암도 변화 값을 이용하여 추출하는 방법[3], 번호판의 수평·수직 에지를 이용하여 번호판 검출하는 방법[4] 등이 있다. 본 장의 3.1 ~ 3.3장에서는 차량 번호판 영

역 추출을 위해 주로 사용되는 방법론 3가지의 추출 과정을 설명한다.

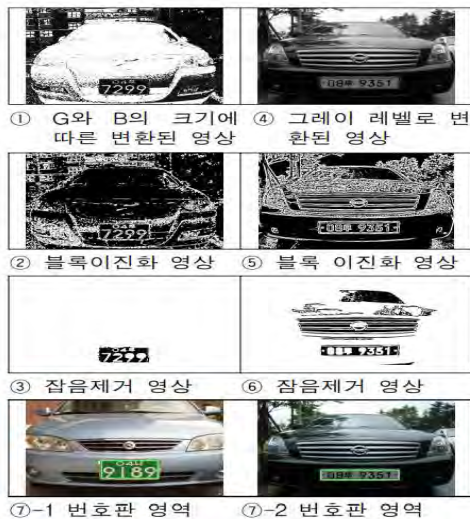
3.1 컬러 모형을 이용한 번호판 추출

차량 번호판은 일정한 색을 가지고 있기 때문에 이러한 특징을 활용하여 차량 번호판 영역을 추출할 수 있다. 이는 차량 번호판이 초록색일 경우 RGB컬러 공간 중 식 1과 같이 G, B의 크기를 이용하여 영상에서 녹색번호판 후보 영역을 추출한 후 블록이진화를 적용하여 번호판 영역을 추출한다[2]. 만일 번호판이 하얀색일 경우 번호판 영역이 추출되지 않을 수 있다. 이때 입력 영상을 그레이 레벨로 변환한 후에 블록 이진화를 적용하고 잡음을 제거한 후에 번호판 영역을 추출한다. 초록색 번호판과 흰색 번호판의 형태학적 특성이 다르기 때문에 위와 같은 작업이 필요하다.

$$\text{IF } G > B \text{ THEN } (G+B)/2$$

$$\text{ELSE } 255$$

(식 1) RGB컬러 공간에서 G와 B를 이용한 변환.

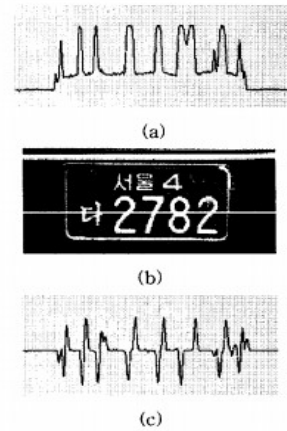


(그림 1) 컬러 모형을 이용한 번호판 영역 추출.

3.2 명암도 변화를 이용한 번호판 추출

차량 번호판은 흑백 영상에서 어두운 바탕에 밝은 글자 혹은 밝은 바탕에 어두운 글자로 서로 대조적인 명암 값을 갖는다[4]. 이는 영상을 수평방향으로 읽을 때 명암 값이 그림2와 같이 음에서 양으로 또는 양에서 음으로 연속적인 벡터를 가지는 것을 의

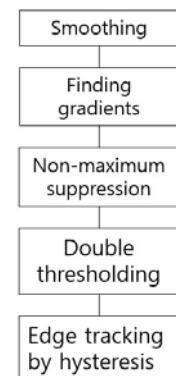
미한다. 이러한 특성을 이용하여 번호판 차량 영상에서 명암벡터가 대칭적인 곳에 번호판이 있음을 추정하여 번호판 영역을 검출한다.



(그림 2) 번호판 명암 값과 기술기.

3.3 수평·수직 에지를 이용한 번호판 추출

케니 에지 추출 (Canny Edge Detection) 방법을 이용하여 이미지에서 수직, 수평 성분을 분리하고 연결된 에지의 좌표 정보를 이용하여 번호판 영역을 추출한다[6]. 케니 에지 추출 방법은 다음과 같은 순서로 진행된다. 1단계에서는 가우시안 블러를 이용하여 블러링을 통해 노이즈를 감소시킨다. 2단계는 Sobel Operator를 통해 매그니튜드(Magnitude)를 갖는 에지를 검출한다. 3단계는 Sobel Operation을 통해 얻은 에지에서 매그니튜드가 maximum인 경우만 에지로 사용하고 불필요한 에지를 제거한다. 4단계 Double thresholding는 검출된 에지를 low와 high로 구분하여 잡음에 의해 검출된 에지를 구별해낸다. 마지막으로 5단계에서는 에지라고 판단된 선들 중 연관성이 없는 에지는 제거하고 실제 에지를 찾아내어 연결한다.



(그림 3) 케니 에지 추출 프로세스.

4. 비교 분석

본 장에서는 3장에서 살펴본 차량번호판 추출 방법을 비교한다.

컬러 영상을 입력받아 색상 정보를 분석하여 배경 색상 영역을 추출하여 인식하는 컬러 정보를 이용한 방법은 번호판의 기울어짐이나 모양이 훼손되어도 인식이 가능하지만, 이러한 방법은 어두운 밤이나 빛과 같은 외부요인으로 인해 색이 왜곡될 경우에는 번호판 인식의 어려움이 있다.

명암도 영상을 입력받아 영상의 밝기를 분석하여 번호판 영역을 추출하는 방법은 영상에서 전체 영역이 아닌 일정 라인에서의 명암 값 변화를 통해 번호판 영역을 추출하므로 처리시간을 줄일 수 있지만 영상 잡음에 민감하다는 단점이 있다[7].

수평·수직 에지를 이용한 번호판 추출 방법은 조명이나 색상 등에 방해받지 않지만 메모리량의 소모가 크고 처리 시간이 오래 걸린다는 단점이 있다 [6].

<표 1> 차량번호판 영역 추출 방법론 비교

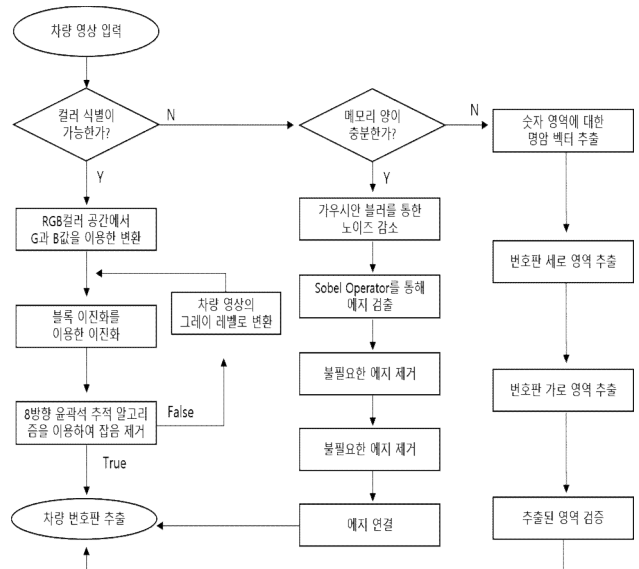
구분	장점	단점
컬러 모형을 이용한 번호판 추출	번호판의 기울어짐, 모양이 훼손에 강인함	야간이나 조명 여부의 영향을 받음
명암도 변화를 이용한 번호판 추출	처리 시간이 짧음	영상 잡음에 민감함
수평·수직 에지를 이용한 번호판 추출	조명이나 색상 영향에 강인함	메모리량 소모가 크고 처리 시간이 오래 걸림

위의 표에서는 차량번호판 추출방법을 비교, 분석하였다. 각 방법론은 차량 영상의 외부적인 요인이나 번호판의 상태 등에 따라서 인식이 잘 되는 경우도 있지만 잘 되지 않는 경우도 존재하기 때문에 본 논문의 5장에서는 각 상황 별로 적합한 알고리즘을 실행시키는 하이브리드 알고리즘을 제안한다.

5. 하이브리드 차량 번호판 인식 알고리즘

4장에서 비교한 3가지 방법론은 영상의 외부 요인 및 차량 번호판 상태에 따라서 인식률에 영향을 받는다. 본 논문에서는 컬러 모형, 명암도 변화 값, 에지를 이용한 알고리즘을 융합하여 각 상황에 맞게 적합한 알고리즘을 실행시킬 수 있는 하이브리드 차량 번호판 인식 알고리즘을 제시한다. 만일 차량 번호판 영상에서 컬러 식별에 문제가 없다면 컬러모형 알고리즘을 통해 차량 번호판을 인식한다. 반면에 영상이 야간이거나 조명 등의 영향을 받을 시에는

메모리량의 여부를 판단하여 메모리량이 충분할 경우에는 수평·수직 알고리즘을 통해 번호판을 추출하고 메모리량이 충분하지 않을 땐 명암도 변화를 이용하여 번호판 영역을 추출한다. 본 논문에서 제시하는 하이브리드 차량 번호판 인식 알고리즘은 영상의 외부환경에 맞는 적합한 알고리즘을 실행시킬 수 있다.



(그림 4) 차량 번호판 인식 하이브리드 알고리즘.

5. 결론

본 논문은 차량 번호판 인식 방법론을 비교 및 분석하였다. 기존 번호판 인식은 연구는 촬영 장소, 밝기와 색상, 번호판 상태 등 외부적 요인에 영향을 받아 잡음이 많이 생긴다. 본 연구에서는 영상에서의 외부 환경 요인에 따라 적합한 알고리즘을 실행시킬 수 있는 하이브리드 차량 번호판 인식 알고리즘을 제안하였다. 향후 연구로는 제안한 알고리즘을 직접 구현하여 다양한 상황에서도 차량 번호판을 인식률을 높일 수 있는 연구가 필요하다.

사사문구

이 논문은 2020년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임. (No.2016-0-00406. (기반 SW-창조씨앗 2단계)SIAT형 CCTV 클라우드 플랫폼 기술 개발)

참고문헌

- [1] 김도형, 이선화, 김미숙, 차의영 “자동차번호판 영역의 문자추출과 인식에 관한 연구,” 한국정보과학회, 2000, pp.338-340.
- [2] 조재현, 양황규 “컬러 정보 및 형태학적 특징과

신경망을 이용한 차량 번호판 인식,” 한국전자통신 학회, 2010, pp.304-308.

[3] 이용주, 석영수 “명암도 변화값과 기하학적 패턴 벡터를 이용한 차량번호판 인식,” 한국정보처리학회, 2002, pp.195-200.

[4] 김숙, 조형기, 민준영, 최종욱 “명암벡터를 이용한 차량번호판 추출 알고리즘,” 한국정보과학회, 1998, pp.676-684.

[5] M. Sarfraz, M.J. Ahmed, S.A. Ghazi. “Saudi Arabian license plate recognition system,” International Conference on Geometric Modeling and Graphics, 2003.

[6] 박승현, 김준영, 조성원, 정선태, 이기성. “캐니 에지 추출 및 CLNF 알고리즘을 이용한 차량 번호판 인식 알고리즘,” 한국지능시스템학회, 2011, pp.37-41.

[7] 강용석, “영상분할 기법을 이용한 자동차 번호판 인식 시스템의 성능개선,” 관동대학교 박사학위논문, 2014.

제53회
2020 온라인 춘계학술발표대회

웹사이언스



오픈 API에서의 새로운 파라미터 요청 방식 제안

박재훈*, 서화정*†

*한성대학교 IT융합공학부 (대학원생)

*† 한성대학교 IT융합공학부 (교수)

p9595jh@gmail.com, hwajeong84@gmail.com

Suggestion of New Parameter Request Method for Open API

Jae-Hoon Park*, Hwa-Jeong Seo*†

*Division of IT convergence engineering, Hansung University (Graduate student)

*† Division of IT Convergence Engineering, Hansung University (Professor)

요 약

오픈 API에서는 사용자로부터 조회할 데이터를 요청을 통해 조건에 해당하는 데이터들을 선별하여 리턴하게 되는데, 현재 통용되는 방식은 다양한 조건을 설정하는 것에 있어 상당한 불편함이 따른다. 이에 따라 오픈 API에서 다양한 조건을 검색할 수 있는 방식을 제안한다. POST 메소드를 통해 숫자의 경우 원하는 검색 범위에 대한 설정을, 문자열의 경우 조건에 따라서 포함 혹은 일치하는 데이터를 검색한다. 이렇게 파라미터의 종류가 다양해짐에 따라 SQL 인젝션과 같은 보안에 대한 위험성도 커지며, 그것을 원천적으로 차단하기 위해 쿼리에 사용자로부터 받은 변수를 넣는 것이 아닌, 데이터베이스에서 얻은 데이터로부터 특정 알고리즘을 통해 사용자의 원하는 조건에 해당하는 데이터를 추출해내는 방법 또한 제안한다. 이를 통해 생산성 극대화를 기대한다.

송 방식에 대한 문제 제기 및 그에 대한 해결책을 제안한다.

1. 서론

오늘날 여러 개인 및 기관들에서 개발자들에게 필요한 정보를 제공해주기 위해 웹 서버를 이용하여 오픈 API를 제공하고 있다.[1] 개발자들은 이렇게 제공되는 정보들을 이용하여 새로운 서비스를 개발할 때에 이용할 수 있다. 오픈 API는 대부분 XML 혹은 JSON 형태의 데이터로 제공되며 보통 해당 API가 제공되는 서버에 GET 메소드를 통해 요청을 보내서 원하는 데이터를 제공받는 방식이다. 이 요청은 GET 메소드를 통하기 때문에 URI에 쿼리 형태로 파라미터를 담아서 보내는 형식이다.

기관에서 제공되는 오픈 API는 대부분 데이터를 제공할 때 인증키를 이용한다. 아무나 서버 자원에 접근하여 부하를 증가시키는 것을 막는 이유에서이다. 개발자는 서비스를 상용화하기에 앞서 오픈 API를 이용할 수 있도록 해당 기관으로부터 인증키를 얻어야 하며, 이렇게 얻은 인증키를 파라미터에 담아서 요청하는 것이다.

2. 파라미터 전송 방식

본 논문에서는 현재 사용되고 있는 파라미터 전

2-1. 문제

오픈 API는 조회를 위해 활용되는 경우가 대부분이며, API를 제공하는 측에서 URI를 통해 요청하는 방식을 지정한다. 개발자는 이렇게 지정된 요청 방식을 통해서 URI 내에 쿼리 파라미터를 합친 뒤 해당 API에 요청하여 조건에 맞는 정보를 얻게 된다.

하지만 데이터의 형식과 종류가 다양함에 비해 URI를 통해 요청하는 방식은 표현이 다양하지 못하게 된다. GET 메소드를 통해 URI로 파라미터를 보낼 경우 'name1=value1&name2=value2&...' 형태로 요청을 보내게 되는데, 이럴 경우 일치하는 값밖에 얻지 못하여 요청의 자유도가 떨어지며 API를 제공하는 측에서도 다양한 요청을 받아들이려면 또다른 방식을 제공해야 한다. 가령 어떤 오픈 API로부터 2020년 2월 29일에 해당하는 정보를 얻고 싶을 경우, 쿼리 파라미터(query parameter)의 경우에는 'uri.com?year=2020&month=2&day=29' 형태로, 필수 파라미터(required parameter)의 경우에는

'uri.com/2020/2/29'와 같은 형태로 요청을 하게 된다. 필수 파라미터의 경우에는 답을 수 있는 파라미터가 매우 제한적이므로, 보통 오픈 API에서는 쿼리 파라미터가 주로 사용된다. 하지만 이렇게 할 경우 원하는 형태의 조건 검색이 어렵다. 가령 '2월'이 아닌 '2월부터 5월까지'를 검색하고 싶을 경우 2, 3, 4, 5월 각각에 대해서 총 4개의 요청을 전송해야 한다. 서버측에서 따로 요구조건을 만들어놓지 않았을 경우 이렇게 요청이 낭비되는 문제가 발생한다.

이런 불편한 점들에 대해 좀 더 자유롭게 데이터를 얻을 수 있는 요청 방식을 제안한다.

2-2. 제안

파라미터를 헤더에 담아서 전송하는 GET 메소드보다 바디에 담아서 전송하는 POST 메소드를 이용할 것을 제안한다. 그리고 요청의 바디 내부에 JSON 형태의 데이터를 담는다. JSON 데이터에는 컬럼의 타입에 맞춰서 문자열, 숫자, 불리언 등에 대한 각각의 형식에 따라서 데이터를 전송한다.

표 1. 숫자 검색에 대한 형식

변수명	타입	상세
over	number	초과
above	number	이상
below	number	이하
under	number	미만
same	number	동일

표 2. 문자열 검색에 대한 형식

변수명	타입	상세
allCaseAllow	boolean	대소문자 구분여부
str	string	검색할 문자열

```
{
  "birth_year": {
    "above": 1995,
    "under": 2001
  },
  "email": {
    "allCaseAllow": false,
    "str": "%example%"
  }
}
```

Fig 1. 요청 JSON 데이터 예시

문자열 검색에서 str은 SQL의 LIKE 구문과 같

이 '%'를 통해 포함 여부를 결정한다. 가령 str을 'hello'라고 설정하면 'hello'에 해당하는 데이터만 리턴되지만, '%hello%'라고 설정하면 'hello world' 등의 'hello'가 포함된 문자열이 리턴되게 된다. 원하는 위치에서 검색하기 위해 '%'를 앞 혹은 뒤에만 설정할 수도 있다. 이를 통해 좀 더 다양한 검색이 가능하게 한다.

Fig 1에서의 JSON 데이터 예시는 태어난 연도가 1995 이상, 2001 미만이며 이메일에 'example'이 포함된 사람들 검색하는 예시이다. allCaseAllow 옵션이 false로 설정되어 있기에 'eXample' 등의 대소문자가 다른 경우는 검색 결과에서 배제된다.

숫자 검색 조건에서 'above'와 'over'을 동시에 사용할 경우 두 조건의 교집합이 되는 'above'에 해당하는 결과가 검색된다.

3. 보안

오픈 API에서는 파라미터를 통해 받은 문자열을 충분한 검증을 거치지 않고 데이터베이스에 대입할 경우 보안에 관련한 문제를 야기할 수 있다. 이에 대한 문제점 및 해결책을 제안한다.

3-1. 문제

관계형 데이터베이스를 이용할 경우 대부분 쿼리문을 조합하여 데이터베이스에 실행시킨 뒤 결과값을 받아서 이용하는 방식을 가진다. 이는 올바르게 않은 문자가 포함될 경우 SQL 인젝션이 생길 가능성을 가지게 된다.

가령, 회원 로그인을 위해 사용자가 아이디와 비밀번호를 form을 통해 전송할 경우 서버에서는 그것을 검증하기 위해 SELECT * FROM users WHERE ID = '전송된 ID' AND PASSWORD = '전송된 비밀번호' 쿼리를 실행시켜서 결과가 있을 경우 얻어진 결과값을 이용하여 로그인을 진행시키고, 결과가 없을 경우에는 아이디 혹은 비밀번호가 틀렸다는 경고를 띄워주게 된다. 하지만 만약 사용자가 아이디를 ADMIN, 비밀번호를 1234' AND '1'=1 이라고 전송할 경우 쿼리의 형태는 SELECT * FROM users WHERE ID = 'ADMIN' AND PASSWORD = '1234' AND '1'=1'이 되어, '1'=1'에 의해 무조건 TRUE가 되면서 ADMIN 계정으로 로그인 할 수 있게 된다. 이러한 SQL 인젝션에 대해서 프로그래머가 확실한 대비책을 구현해야 한다. 싱글 쿼테이션(')이 포함되어 있을 경우 실행시키지

않는 방법도 있지만, 어디까지나 그러한 처리를 직접 해줘야 하는 것이고, 이는 프로그래머의 실수로 처리가 되어 있지 않을 경우 문제가 생길 수 있다.

ORM(Object Relational Mapping)을 이용할 경우에도 인젝션을 야기할 수 있다. ORM은 데이터베이스 테이블을 객체 형태로 다루게 되어서 통상적인 사용의 경우에는 인젝션이 일어날 일이 없게 되지만, ORM을 구현하는 여러 라이브러리들은 복잡한 쿼리 작업은 객체 형태가 아닌 직접적인 SQL을 이용하여 구현할 수 있도록 방안을 마련해놓고 있다. 대표적으로 Hibernate의 HQL이 그러한 것인데, 이것을 이용할 때에 인젝션이 일어날 수 있다.

SQL을 아예 이용하지 않는 NoSQL에서도 인젝션 문제를 원천적으로 피할 수는 없게 된다. 대표적인 NoSQL인 MongoDB의 경우 검색을 할 때에 문자열을 넣어서 하는 방식을 이용하는데, 이때 사용자로부터 받은 문자열을 직접 넣을 경우 인젝션이 일어날 수 있다. 가령 아이디를 보냈을 경우 {id: '사용자로부터 받은 id값'} 형태의 쿼리를 수행한다고 가정했을 때, 해커가 MongoDB의 명령어인 \$ne나 \$exists와 같은 구문을 문자열에 추가시킬 경우 원하는 정보를 빼갈 수 있게 된다.

이렇듯 다양한 데이터베이스에서 해커는 인젝션을 일으켜 서버에서 강제로 정보를 빼갈 수가 있는데, 이러한 인젝션의 예방이 충분하지 않게 되면 뚫릴 수밖에 없게 된다. 특히나 오픈 API와 같이 여러 변수를 사용자로부터 직접 입력받는 서비스의 경우 더욱 보안에 취약해지게 된다. 그렇기에 이러한 공격으로부터 원천적으로 방어할 수 있는 수단이 필요하다.

3-2. 제안

쿼리문에 사용자로부터 받은 변수를 직접 넣지 않는 방법을 제안한다. 데이터베이스에서 쿼리문을 실행시키려 할 때 사용자로부터 받은 변수를 직접 담은 쿼리문을 이용할 경우 전부 인젝션 방어를 처리를 해주지 않는 경우 결국 인젝션 문제가 일어날 수밖에 없게 된다. 이러한 문제를 원천적으로 차단하기 위해서 데이터베이스로부터 데이터를 받을 때부터 조건을 거는 것이 아닌, 별다른 조건을 걸지 않은 채로 데이터를 받은 뒤 그것을 조건에 따라 걸러내어 사용자에게 리턴시키는 방식을 사용한다.

예를 들어 로그인 할 때에 사용자로부터 아이디와 비밀번호를 전송받을 경우, 쿼리문 내부에 ID =

‘입력받은 ID’ AND PASSWORD = ‘입력받은 비밀번호’와 같은 조건을 거는 것이 아닌, SELECT * FROM USERS와 같이 조건이 걸려있지 않는 쿼리문을 실행시킨 뒤 받은 사용자 데이터로부터 반복문과 조건문을 이용하여 사용자를 확인하고 로그인을 수행하는 것이다.

이러한 방식을 상기한 오픈 API에서의 파라미터를 구체화하는 방식에 적용시킴으로써 오픈 API에서 생길 수 있는 인젝션 문제를 예방할 수 있다. 서버에서 받을 수 있는 형식은 정해져 있으므로 코드를 통해 데이터를 분류하는 작업도 마찬가지로 정형화 될 수 있다.

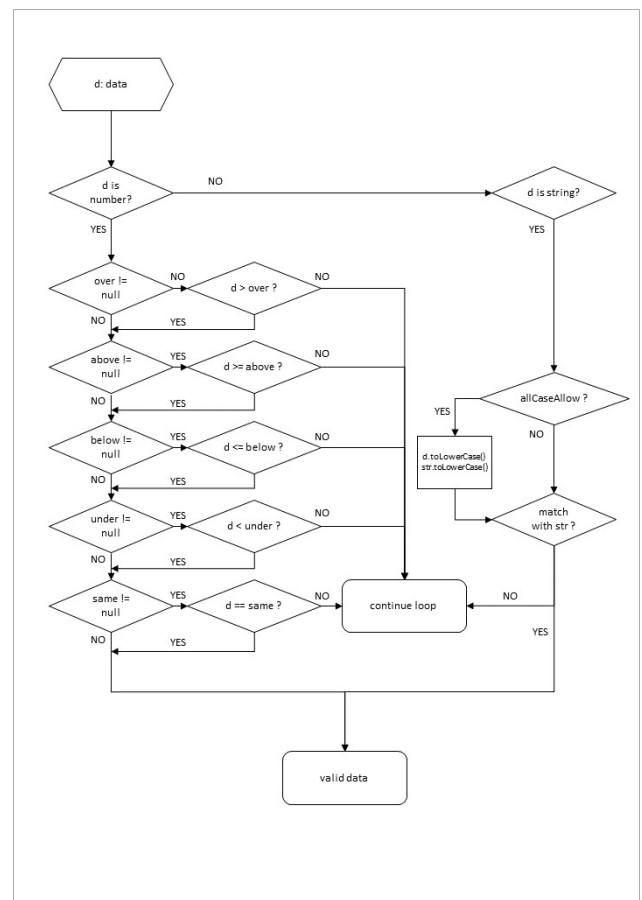


Fig 2. 조건 확인 알고리즘 순서도

데이터베이스를 거쳐서 나온 결과 배열값으로부터 루프를 돌면서 Fig 2의 알고리즘을 거쳐서 조건에 맞는 데이터들만을 골라내어 사용자에게 리턴시켜준다. 이렇게 될 경우 인젝션 공격으로부터 원천 차단할 수 있게 된다. 다만 해당 데이터의 타입이 무엇인지에 대한 확실한 명시가 필요하다.

다량의 데이터를 처리하는 것에 따라 서버의 CPU 사용량이 증가하는 것이 우려된다면, 검색 조

건에 페이징을 추가하여 각 요청에 대해 처리하는 데이터의 개수를 제한하는 방식을 이용할 수 있다. 가령 한 페이지에 30개의 데이터를 갖고 있다고 가정한다면, 페이징 파라미터에 따라 몇 번째 페이지 인지를 알아내고 그에 해당하는 데이터들을 데이터 베이스에서 얻어낸 뒤 30개의 데이터에서 조건 확인 알고리즘을 거친 뒤 사용자에게 결과를 리턴해주면 된다.

4. 결론

데이터를 다루는 서비스가 증가함에 따라 다양한 오픈 API의 사용도 증가하고, 그에 따라 복잡한 조건 검색 및 향상된 보안을 요구하게 되었다. 본 논문에서는 오픈 API에서의 타입에 따른 다양한 검색 조건 설정과, 그러한 방식을 적용하면서 SQL 인젝션 공격에 더 취약해질 수 있음에 따라 인젝션 공격으로부터 방어할 수 있는 방식을 제안하였다.

최근 RESTful API[2] 사용이 증가함에 따라 RESTful API의 조회에서도 이러한 방식을 이용하는 것을 기대한다. 조회 화면이 많은 어플리케이션의 경우 이러한 방식을 통해 생산성을 극대화 할 수 있을 것이다.

참고문헌

- [1] 공공 데이터 이용 가이드 [Internet], <https://www.data.go.kr/guide/guide/guide.do>.
- [2] R. T. Fielding, "Architectural styles and the design of network-based software architectures," Ph.D. dissertation, Information and Computer Science, Univ. of California, IRVINE, 2000.

사용자 정보를 이용한 Indexed DB 암호화 인증

황우섭*, 박지수**¹⁾, 손진곤*

*한국방송통신대학교 대학원 정보과학과

**전주대학교 컴퓨터공학과

wooseob@knou.ac.kr, zetsaver@gmail.com

Indexed DB Encryption Authentication using User Information

Woo Seob Hwang*, Ji Su Park**, Jin Gon Shon*

*Dept. of Computer Science, Graduate School, Korea National Open University

**Dept. of Computer Science and Engineering, Jeonju University

요 약

인터넷의 발전으로 웹 서비스를 사용하는 사용자가 기하급수적으로 늘어났고 사용자에게 다양한 서비스를 제공하기 위해 많은 기술이 등장하고 있다. 서비스를 받는 사용자의 웹브라우저에서도 서버의 많은 기술을 구현할 수 있는 공간을 제공하고 있는데 바로 Web Storage와 Indexed DB이다. Web Storage는 용도에 따라 수 MB 정도를 사용하지만 많은 양의 데이터를 구조화하여 사용한다면 Indexed DB가 적합하다. 하지만 Web Storage뿐만 아니라 Indexed DB 역시 영속적이고 평문의 데이터를 저장하고 있다. 이러한 데이터는 웹 보안에 취약하여 XSS 등의 공격에 사용자의 데이터가 노출되어 탈취되거나 편집되어 악용될 우려가 매우 크다. 본 논문에서는 이와 같은 취약점을 보완하기 위해 운영체제와 디바이스 정보를 이용하여 사용자를 인증하고 암호화하는 기법을 구현하여 성능 평가를 하였다.

Keyword : 사용자, 디바이스 정보, 인증, 암호화, HTML5, Indexed DB, Encryption, Authentication

1. 서론

HTML5는 웹 문서를 기술하기 위한 웹 표준 규약이다. 이 HTML5에는 다양한 기술을 활용하기 위해 여러 종류의 저장 공간을 제공한다[1]. 대표적으로 웹 스토리지에 속하는 로컬 스토리지와 세션 스토리지가 있다[2]. 그러나 저장할 수 있는 용량에 제한점이 있어 많은 양의 데이터를 구조화하는 Index DB를 사용한다[3]. Indexed DB는 평문의 데이터가 영속적으로 저장되어 사용자의 개인 정보 등이 노출될 위험이 있다. 이는 공격자가 XSS 등의 다양한 방법으로 정보를 탈취하거나 편집되어 악용될 수 있다[4]. 이러한 문제를 해결하기 위해 최근 많은 연구가 이루어지고 있는데, 패스워드 기반 암호화 기법이나 핀(비밀번호)을 이용하면서 서버를 통해 인증하는 기법, 혹은 브라우저 확장 기능을 이용하여 프레임워크를 연구하는 기법 등 다양하다[5-10].

최근 연구들에서는 보안 취약점 해결을 위한 암호화를 사용한다. 그러나 이 연구들 또한 사용자 인증을 위해 서버를 이용하거나, 사용자에게 비밀번호를

요청한다. 그러나 보안 강화를 위해 인증 서버를 별도로 구축할 경우 비용적인 문제가 발생하고, 비밀번호를 이용한 인증 절차는 편리성이 떨어지며 key-logger 등의 공격을 고려해야 한다. 따라서 본 논문에서는 이러한 문제들을 해결하기 위해 운영체제와 디바이스 정보를 암호화에 활용하였다.

2. 관련 연구

2.1 Indexed DB

HTML5에서 Indexed DB는 클라이언트에 영속적으로 구조화된 데이터를 저장하며 키와 값으로 관리한다. 또한 데이터는 B-Tree 구조로 되어 있으며 온라인뿐만 아니라 오프라인에서도 사용한다[3]. 이러한 Indexed DB는 다른 Web Storage처럼 평문 형태로 데이터를 저장하여 XSS 등의 공격에 취약하여 데이터가 탈취되거나 변조되어 악용될 우려가 높으므로 보안에 취약한 문제가 있다[4]. 최근 연구에서는 인증 서버를 추가함으로써 발생하는 비용의 문제점이나 비밀번호를 이용하는 인증 절차의 편리성 저하와 함께 key-logger 등의 다른 공격에도 고려해야

1) 교신저자

한다[5-10].

2.2 암호화 및 인증

기존 연구에서 사용자 정보를 로컬 스토리지에 이용하여 암호화를 인증한다[11]. 본 논문에서 제안하는 기법은 Indexed DB에서 사용자 정보를 이용하여 기밀성과 편리성을 높인다. 사용자 정보는 운영체제의 현재 사용자와 디바이스 정보를 이용하며, 암호화 인증에 활용할 사용자 정보는 다음과 같다.

- 메인보드(MB)의 일련번호(SN: Serial Number).
- 메인보드(MB)에 존재하는 BIOS(Basic Input Output System)의 일련번호(SN: Serial Number).
- 메인보드(MB) 시스템의 고유식별자 (UUID: Universally Unique Identifier)
- 운영체제의 현재 로그인된 User ID 정보

위의 사용자 정보 중 사용자가 많이 이용하는 윈도우 운영체제를 기준으로 registry의 현재 User ID와 디바이스 정보를 사용하여 암호화하고 사용자를 인증한다[12].

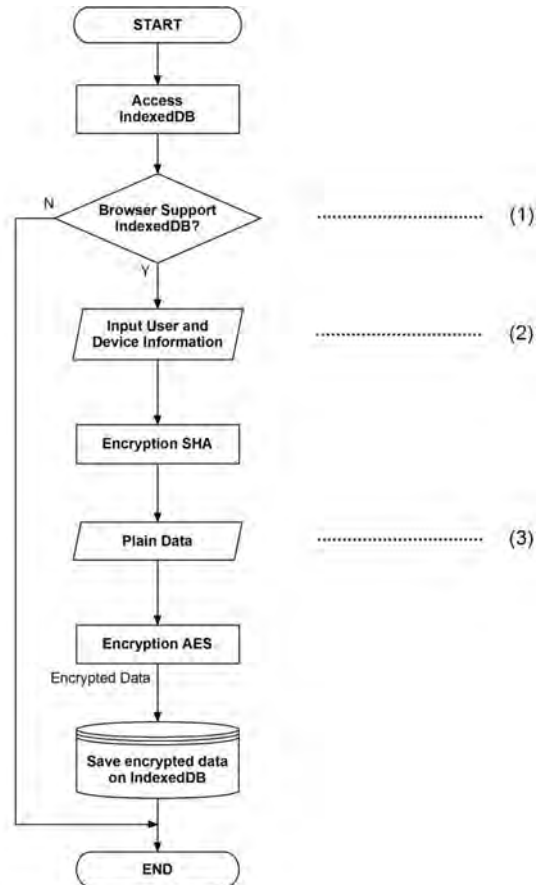
3. Indexed DB 암호화 인증 설계

본 논문에서는 Indexed DB에 저장될 데이터를 암호화할 때 별도의 비밀번호 입력이나 인증할 서버 없이 사용자 정보를 이용하여 암호화하는 기법을 제안한다. 사용자 정보는 운영체제에서 로그인한 현재 사용자 값과 하드웨어의 고유값이며 이 정보를 이용하여 SHA 암호화를 진행한다. SHA로 암호화된 사용자 정보와 평문 데이터를 같이 한 번 더 AES로 암호화한다. 이와 같은 암호화 인증 방식은 데이터가 다른 디바이스로 탈취되거나 변형되어도 안전성이 보장된다. 제안하는 기법의 알고리즘 중 암호화를 설명하면 (그림 1)과 같이 처리되며 설명은 아래와 같다.

- (1) 브라우저 응용 애플리케이션이 Indexed DB를 지원하는지 확인한다.
- (2) 운영체제의 현재 로그인된 사용자 값을 Registry의 HKey_CURRENT_USER\Identities\User ID에서 가져오고 디바이스 값은 메인보드 내에서 BIOS SN, MB SN, UUID 값을 가져온다. 이 값들은 SHA 256으로 암호화한다.

데이터를 저장할 때 인증할 수 있는 값으로 사용한다.

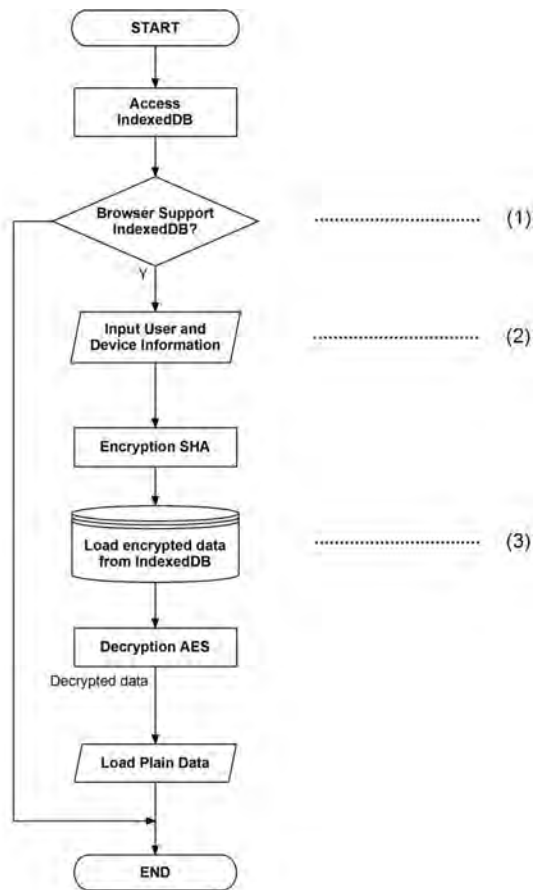
- (3) 데이터를 저장하면 SHA로 암호화된 사용자 값과 평문 데이터 값을 AES 암호화한다.



(그림 1) 제안 기법 암호화 흐름도

제안하는 기법의 알고리즘 중 복호화를 설명하면 (그림 2)와 같이 처리되며 설명은 아래와 같다.

- (1) 브라우저 응용 애플리케이션이 Indexed DB를 지원하는지 확인한다.
- (2) 운영체제의 현재 로그인된 사용자 값을 Registry의 HKey_CURRENT_USER\Identities\User ID에서 가져오고 디바이스 값은 메인보드 내에서 BIOS SN, MB SN, UUID 값을 가져온다. 이 값들은 SHA 256으로 암호화한다. 데이터를 불러올 때 인증할 수 있는 값으로 사용한다.
- (3) 데이터를 불러올 경우 Indexed DB에서 암호화된 데이터 값을 얻어오고 SHA로 암호화된 사용자 값으로 AES 복호화 한다.



(그림 2) 제안 기법 복호화 흐름도

4. 성능 평가

본 논문의 제안 기법을 구현하여 테스트한다. 일반적으로 사용자가 많이 접하고 있는 윈도우 운영체제와 IE(Internet Explorer)로 구현한다. 암호화는 SJCL(Stanford Javascript Crypto Library)를 사용한다[13].

성능 평가는 비밀번호를 기반으로 한 연구와 제안하는 기법과 비교하였다. 그 결과는 <표 1>과 같으며 암호·복호화에 걸리는 수행 시간에는 큰 차이를 보이지 않았다. 하지만 사용자의 암호 입력을 기다리는 동안의 시간과 제안 기법의 사용자 정보를 암호화하는 시간에서 암호 입력을 기다리는 시간의 차이만큼 차이를 보여 제안하는 방식이 더 빨랐다.

앞서 언급한 것처럼 윈도우의 IE 환경에서 검증한 것인 만큼 다른 브라우저에서 구현할 때에는 구현 코드가 달라질 수 있다. Chromium 기반의 Chrome 브라우저에서는 Native Message(메시지교환) 방식이나 NaCl(Native Client)의 PPAPI(Pepper API)를 사용하여 구현해야 한다[14-16].

<표 1> 암호 입력과 제안 기법 비교(단위:ms)

* t : 암호 입력 시간

비교 대상 인증 방식	저장 시간 비교			불러오는 시간 비교		
	사용자 인증	암호화	총시간	사용자 인증	암호화	총시간
제안 기법	86.22	5.92	92.14	71.52	5.30	76.82
암호 입력	t	5.17	t+5.17	t	4.69	t+4.69

5. 결론

HTML5의 Indexed DB는 많은 양의 구조화된 데이터들을 활용도 높게 사용할 수 있다. 하지만 평문 형태 데이터를 영속적으로 저장하며 이는 XSS 등의 공격으로부터 목표가 되고 있어 데이터가 탈취되거나 편집되어 악용될 수 있다.

본 논문은 Indexed DB의 기능을 그대로 사용하면서 추가 절차 없이 편리하게 사용하면서 정보를 암호화하여 기밀성을 높였다. 성능 평가도 사용자에게 암호를 요구하여 입력될 때까지 대기시간의 차이만큼 논문에서 제안하는 방법이 빠른 성능을 보였다.

향후 연구에서 최근 많이 발전하고 있는 Web-Assembly를 이용하게 된다면 개발 코드의 큰 변화가 없이 처리 속도까지 향상할 수 있을 것이다 [17].

참고문헌

- [1] W3C Recommendation, "HTML 5.2", Available : <https://www.w3.org/TR/html52/>, Access : april 2020.
- [2] W3C Recommendation, "Web Storage (Second Edition)", Available : <https://www.w3.org/TR/webstorage/>, Access : April 2020.
- [3] W3C Recommendation, "Indexed Database API 2.0", Available : <https://www.w3.org/TR/IndexedDB/>, Access : April 2020.
- [4] OWASP, "Cross Site Scripting (XSS) | OWASP", Available : <https://owasp.org/www-community/attacks/xss/>, Access : April 2020.
- [5] J Park, D Shin, D Shin, J Lee, H Lee, "Design and Implementation of Web Browser Secure Storage for Web Standard Authentication

- Based on FIDO”, Symposium on Information and Communication Technology(SoICT), ACM, Dec 2019.
- [6] Amirhossein Akbari, “A NOVEL APPROACH FOR SECURING HTML5 CLIENT-SIDE DATABASE, INDEXEDDB”, Tallinn University of Technology, Master thesis, May 2018.
- [7] Stefan Kimak, Jeremy Ellman, “The role of HTML5 IndexedDB, the past, present and future”, International Conference for Internet Technology and Secured Transactions(ICITST), IEEE, Dec 2015.
- [8] Mayssa Jemel, Ahmed Serhrouchni, “Security enhancement of HTML5 Local Data Storage”, International Conference and Workshop on the Network of the Future (NOF), IEEE, Dec 2014.
- [9] Stefan Kimak, Jeremy Ellman, Christopher Laing, “Some Potential Issues with the Security of HTML5 IndexedDB”, International Conference on System Safety and Cyber Security(IET), Oct 2014.
- [10] Stefan Kimak, Dr. Jeremy Ellman, Dr. Christopher Laing, “An investigation into possible attacks on HTML5 IndexedDB and their prevention”, international Conference on Software, Knowledge, Information Management & Applications(SKIMA), Sep 2012.
- [11] 황우섭, 박지수, 손진곤, “사용자 정보를 이용한 인증 절차 자동화”, 한국정보처리학회 춘계학술대회, 26권 2호, 1125p~1128p, Nov 2019.
- [12] Microsoft, “Microsoft Developer Network”, Available : <https://msdn.microsoft.com/>, Search : Registry API, Access : April 2020.
- [13] Stanford University Cryptography Group, “Stanford Javascript Crypto Library”, Available : <https://crypto.stanford.edu/sjcl/>, Access : April 2020.
- [14] Google Chrome, “Native Messaging”, Available : <https://developer.chrome.com/extensions/native-messaging/>, Access : April 2020.
- [15] Google Chrome, “Welcome to Native Client”, Available : <https://developer.chrome.com/native-client/>, Access : April 2020.
- [16] Google Chrome, “Pepper API Reference (Stable)”, Available : https://developer.chrome.com/native-client/pepper_stable/, Access : April 2020.
- [17] WebAssembly, “WebAssembly”, Available : <https://webassembly.org/>, Access : April 2020.

제53회
2020 온라인 춘계학술발표대회

인간과 컴퓨터 상호작용



고객만족 및 서비스 품질에 관한 연구 - KOSEN 사례를 중심으로

김상국*, 최선희*

*한국과학기술정보연구원

e-mail : skkim@kisti.re.kr, sunny.choi@kisti.re.kr

A Study on Customer Satisfaction and Service Quality - A Case Study KOSEN

Sang-kuk Kim*, Seon-heui Choi*

*Korea Institute of Science and Technology Information

요 약

본 논문에서는 고객추천지수(NPS : Net Promoter Score)를 이용하여 2019년도 이용 고객의 서비스 만족 및 품질에 대하여 모니터링하고 기관의 고객만족 개선 활동에 대한 고객의 의견을 분석하기 위함이다. 한국과학기술정보연구원의 한민족과학기술자네트워크(KOSEN : The Global Network of Korean Scientists & Engineers)는 전 세계 한인 과학기술자들을 하나로 연결하는 네트워크 서비스로 2019년 현재 70여개국 14만여 회원들로 이루어진 거대한 네트워크로 성장하였습니다. 1999년 이래 과학기술부, 교육과학기술부, 미래창조과학부, 과학기술정보통신부 지원 사업으로 한국과학기술정보연구원에서 운영해오고 있습니다. 네트워크를 통한 한인 과학기술자들의 지식 공유가 주목적이며, 연구자들을 위한 다양한 서비스를 무상으로 제공하고 있습니다. 이를 위해 서비스를 경험한 262여 명의 의사결정자를 대상으로 한민족과학기술자네트워크에 대한 고객충성도를 분석하였다. 이와 같은 연구결과는 인터넷 등 정보의 발달로 고객의 긍정적 또는 부정적인 구전이 급속도로 노출되는 환경에서 고객의 만족도를 관리함으로써 핵심고객을 확보하는데 사전 예측자료로 활용될 수 있다.

1. 서론

다양한 온라인정보서비스가 등장하고 이에 대한 이용이 증대됨에 따라 온라인정보서비스에 대한 품질관리의 중요성도 높아지고 있다. 이에 순추천고객지수(NPS : Net Promoter Score) 조사는 각 조사 시점에서의 모집단을 대표하는 결과를 얻을 수 있고, 주기적으로 조사를 실시한다면 고객군이 어떻게 변화해 가는지 시계열 분석이 가능하다. 이러한 특징을 보완하여 조사 시점의 모집단을 대표하는 결과를 얻을 수는 없으나 동일 고객의 요구 변화 등을 확인할 수 있고, 서비스를 계속해 온 집단에 대한 결과의 대표성을 확보할 수 있을 뿐 만 아니라 미이용 고객이 있더라도 조사대상으로 포함할 수 있어 서비스를 이용하지 않게 된 사유들을 확인할 수 있는 NPS 추적조사 방식을 적용하였다.

본 설문 조사는 사업의 성장을 위한 고객 로열티를 매우 심층하게 측정할 수 있다는 장점이 있다. 또한 VOC Probing 과정과 함께 진행하여 실제 고객의 핵심 Needs에 보다 집중할 수 있다는 장점이 있다.[1]

2. NPS 추적조사 분석

한민족과학기술자네트워크는 2018년 NPS 참여 고객 467명 중 2019년 개인 정보 활용을 동의한 고객 262명을

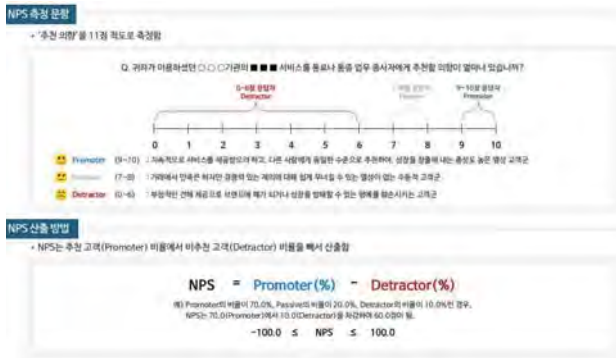
조사 대상으로 하였다. 조사방법은 구조화된 설문지에 의한 전화조사로 하고 전수 조사를 실시하였다. 실사 진행은 1주 정도 걸렸으며 VOC 세 분류를 위한 분석을 서비스 담당자와 컨설턴트가 2주 정도 참여하여 정리하였다.



(그림 1) NPS 추적조사 진행 프로세스

최근 1년 이내에 KOSEN 서비스에 참여한 고객을 대상으로 현재 서비스 추천 의향, 추천/중립/비추천 사유, 추천도 사유를 조사함. 순추천고객지수(NPS)는 11점 척도로 측정된 추천 의향을 Promoter, Passive, Detractor로 구분하여 Promoter의 비율에서 Detractor의 비율을 차감하여 산출한다. 산출되는 순추천고객지수

의 범위는 -100.0점부터 +100.0점까지로 구성된다. Promoter(9-10점)는 지속적으로 서비스를 제공받으려 하고, 다른 사람에게 동일한 수준으로 추천하여, 성장을 창출해 내는 충성도 높은 열성 고객군을 말한다. Passive(7-8점)는 이용시 만족은 하지만 경쟁력 있는 제의에 대해 쉽게 무너질 수 있는 열성이 없는 수동적 고객군을 말한다. Detractor(0-6점)은 부정적인 견해 제공으로 브랜드에 해가 되거나 성장을 방해할 수 있는 명예를 훼손시키는 고객군을 말한다.[2]



(그림 2) NPS 산출 방법

3. 분석 결과

KOSEN는 2019년 NPS조사 참여가능 고객 467명 중 262명을 대상으로 서비스 만족 조사를 완료되었다. NPS는 30.3점으로 양호한 수준이었다. Promoter가 67명(44.1%), Passive가 64명(42.1%), Detractor가 21명(13.8%)으로 나타났으며, 2018년도 대비 KOSEN 서비스 이용률이 증가한 고객이 11명(7.2%), 이용률이 감소한 고객이 54명(35.5%)로 나타났다. 미이용 고객의 2018년도 조사 당시 NPS는 18.2점이었다. 미이용 사유로는 최근 관련 업무 부재(22건, 20.0%), 바빔(19건, 17.3%), 원하는 정보 및 서비스 부재(16건, 14.5%), 퇴직이나 휴직(16건, 14.5%) 등으로 나타났다.



(그림 3) NPS 고객군 및 추천도 분포 현황

본 조사에서는 연령대별 NPS 분석 결과 50대 고객이 50.6점으로 가장 높았으며, 2018년(33.4점) 대비 18.2점이 상승하였다. 40대 고객은 27.1점으로 2018년(53.2점) 대비 큰 폭(26.1점)으로 하락하였다. 소속 기관별은 중소기업 소속 고객이 45.5점으로 가장 높고, 연구기관 소속 고객이 17.7점으로 가장 낮았다. 직업별 분포는 기업 대표의 NPS가 50.0점으로 가장 높고, 학생의 점수가 9.1점으로 가장

낮았다. 주 이용서비스별 NPS 분석 결과, 가장 많은 비율을 차지하는 전문 자료 검색을 주로 이용하는 고객군이 31.4점으로 나타났다. 161건의 VOC(Voice of Customer)는 “정보의 양”이 가장 많이 수집되었다. VOC 분류 방식을 시계열로 분석한 결과 “정보-양”과 관련한 내용을 언급한 고객군의 NPS가 45.4점으로 나타났으며, 2018년 대비 3.5점 하락하였다. “정보-수준”과 관련한 내용을 언급한 고객군의 NPS가 83.9점으로 나타났으며, 2018년 대비 4.8점 상승하였다. “정보-최신성”과 관련한 내용을 언급한 고객군의 NPS가 33.3점으로 나타났으며, 2018년 대비 33.4점 하락하였다.



(그림 4) VOC 분류 기준별 시계열 분석

4. 제언

전문 정보를 제공하는 채널은 다양해지고 있으며 이에 따라 다수의 경쟁 상대가 있을 것으로 보이지만, 그럼에도 고객들은 KOSEN만의 차별점이 있다는 점에 동의하였으며, 고객들은 KOSEN의 차별점으로 수많은 정보 중에서 전문가들이 선별한 질 높은 자료를 얻을 수 있다는 점을 언급하였다. 새로운 분야에 입문하기 위한 정보 탐색 시, KOSEN이 가장 적합하다는 의견도 나타났다. 고객들은 전문가가 선별한 자료를 제공한다는 점을 KOSEN REPORT의 특징이라고 느끼고 있다. 이것은 고객이 생각하는 KOSEN 서비스의 차별점과 동일하다. 선별된 자료를 제공한다는 점은 효율적인 정보 탐색을 가능하게 한다는 긍정적 평가가 나타남. 반면, 자료를 작성하는 사람의 역량 관리가 제대로 이뤄지지 않을 경우, 자료의 품질에 부정적 영향을 미칠 수 있다는 우려도 함께 나타났다.

감사의 글

본 연구는 한국과학기술정보연구원(KISTI)의 「과학기술정책 연구(K-19-L07-C01-S01)」 사업으로부터 지원을 받아 수행된 연구임.

참고문헌

- [1] Sang-kuk Kim, “A Study on the Customer Satisfaction Strategies of information Service Using VOC”, The Ninth International Conference on Emerging Networks and Systems Intelligence EMERGING 2017
- [2] Sang-kuk Kim, “A Study on a Plan for Enhancing Customer Satisfaction on government-funded Research Institutes - A Case study in KISTI”, The 4th International Conference on digital Policy & Management 2017, vol. 4No1, January 2017

무대 공연을 위한 제스처 인식 기반 동적 프로젝션 맵핑 프레임워크 구현

고유진*, 김태원*, 최유주*[†]

*서울미디어대학원대학교 미디어공학과, [†]교신저자
ssummerr8.8@gmail.com, wingtgnw@naver.com, yjchoi@smit.ac.kr

Implementation of Dynamic Projection Mapping Framework based on Gesture Recognition for Stage Performance

You-Jin Koh*, Tae-Won Kim*, Yoo-Joo Choi*

*Dept. of Newmedia, Seoul Media Institute of Technology

요 약

본 논문에서는 미디어영상을 기반한 무대 공연의 다양한 미디어 효과를 분석하고, 무대 공연을 위한 제스처 기반 동적 프로젝션 맵핑 프레임워크를 설계 구현한다. 이를 위하여, 동적 프로젝션 맵핑 기반 기존 공연에서 공연자의 제스처와 이에 따른 미디어 효과를 분석하고, 동적 프로젝션 맵핑 기술을 효율적으로 구현하기 위하여 모션 히스토리 이미지를 이용한 CNN(Convolutional Neural Network) 기반의 제스처 인식 기술을 구현한다. 또한, 구현된 제스처인식 기술을 기반으로 공연자의 서로 다른 제스처와 미디어 효과를 매칭시킬 수 있는 프레임 워크 구현 내용을 소개한다.

1. 서론

기존의 프로젝션 맵핑 공연은 이미 만들어진 비디오와 공연 안무의 싱크를 맞추어 실제 공연 때는 마치 맵핑 비디오가 사람의 동작에 실시간 반응을 하는 것처럼 보이게 했다. 최근 제스처 인식 기술이 발전하면서 최근에는 공연자의 제스처에 따라 실시간 인터랙션 퍼포먼스가 가능한 동적 프로젝션 맵핑 연출이 관심을 모으고 있다. 대다수의 미디어 아트 퍼포먼스가 라이브 공연인 만큼 공연자의 동작에 따른 효율적인 미디어 이펙트에 대한 처리와 이를 보다 용이하게 조작할 수 있는 프레임워크가 요구되고 있다.

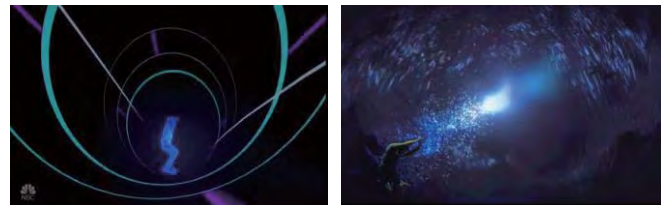
본 논문에서는 대표적인 동적 프로젝션 맵핑 공연 연출과 제스처 인식 연구 현황에 대해 간단히 알아보고 보다 효율적인 제스처 인식 구현을 위해 모션 히스토리 이미지를 이용한 CNN(Convolutional Neural Network)기반의 제스처 인식 실험을 진행하고, 제스처 인식을 기반한 무대 공연에 적합한 동적 프로젝션 맵핑 프레임워크를 설계 구현한다.

2. 프로젝션 맵핑 기반 미디어 아트 퍼포먼스와 제스처 인식기술 현황

2.1 미디어 아트 퍼포먼스와 동적 프로젝션 맵핑

프로젝션 맵핑은 투사하는 대상물의 평면에 가상의 무대 공간을 창조할 수 있기 때문에 빠른 무대 장면 전환을 통한 이야기 전개가 가능하다. (그림 1)은 공연자를 기준으로 가상의 3D 배경을 입혀 공연자가 마치 실제와 같은 효과를 준다. 여기에 제스처 인식 기술이 더해진 동적 프로젝션 맵핑은 공연자가 무대 위에서 자신의 몸짓만으로 메시지 전달을 할 수 있게 한다. (그림 2) 같이 제스처 인식과 인터랙션이 가미된 프로젝션 맵핑 기술은 예술가와 관객이

같은 공연 안에서 함께 즐길 수 있도록 만든다.



(그림 1,2) 프로젝션 맵핑 퍼포먼스 예시 1,2[2-3],

2.2 딥러닝 기반의 제스처 인식

최근 딥러닝을 기반한 제스처 인식 방법이 높은 성능을 보이고 있다. 제스처 및 동작 인식을 위한 딥러닝 접근법은 (그림 4)와 같이 크게 세 가지로 나뉜다. 하나는 학습에 사용하는 신경망의 고도화와 입력데이터의 전처리 그리고 RNN(Recurrent Neural Network)과 같이 연속 데이터(Sequence Data)를 이용한 시간적 방법들(temporal methods) 들이 있다[3].

본 논문에서는 데이터의 사용량을 줄여 성능을 높이는 모션기반 입력 특징값을 활용하는 방법을 택하여 모션 히스토리 이미지를 학습 데이터로 사용하는 CNN 기반의 제스처 인식 방법을 구현하고 이를 사용하였다.

3. 구현 및 실험

3.1 구현 제스처

<표 1>은 직관적 제스처 ‘기모이기’, ‘장풍 쏘기’, ‘발차기’로, 본 논문에서는 해당 제스처들을 인식하고 각 제스처에 해당하는

인터랙션을 구현한다.

<표 1> 구현 제스처 종류



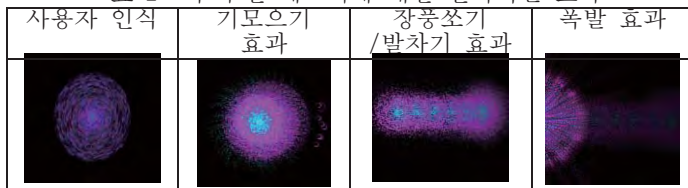
3.2 모션 히스토리 이미지 기반 제스처 인식

본 논문에서는 제스처 인식 실험에 대한 입력데이터로 Motion History Image(MHI)를 사용한다. MHI는 동작이나 제스처의 진행 경로를 이해할 수 있는 정적 이미지 템플릿으로, 여러 프레임으로 나누는 하나의 동작 데이터를 적은 메모리로 활용할 수 있다[4].

3.3 제스처 별 타겟 영상 효과

<표 2>는 제스처와 매칭되는 인터랙션 효과를 나타내고 있다. <표 6>의 ‘만세’ 제스처의 경우, 사용자를 인식하여 프로그램 시작을 판단하는 척도로 사용된다. ‘기모으기’ 제스처는 주변에 발산하던 빛들이 사용자의 중심으로 모여 뭉쳐지는 효과를 준다. ‘장풍 쏘기’는 공연자의 두 손 중심에서 손을 뻗는 방향으로 파티클 덩어리가 발사된다. ‘발차기’는 장풍쏘기와 같은 효과로 연결되고, 장풍쏘기/발차기의 마지막 시점에 불꽃 형태의 파티클이 주변으로 발산하여 폭발효과를 표현한다.

<표 2> 각 구현 제스처에 대한 인터랙션 효과



3.4 제스처와 미디어 효과의 매칭 정의

제스처와 매칭되는 미디어 효과는 텍스트로 구성되는 프로젝션 맵핑 구성 파일에 정의한다. <표 3>은 구성파일에서 제스처와 매칭 효과를 정의하는 규칙과 이에 따라 정의한 형식을 보여준다.

<표 3> 제스처와 미디어 효과 매칭을 위한 구성 파일 규칙

제스처/미디어 효과 정의 규칙	의미
Num_Gesture: 3	타겟 제스처 수
GestureDir: "gesture dir 명"	학습완료 배포데이터디렉토리명
Num_Effect:4	미디어 효과 수
Effect1: "ParticleEffect1"	파티클 효과번호
Effect2: "ParticleEffect2"	파티클 효과번호
Effect3: "ParticleEffect3"	파티클 효과번호
Effect4: "ParticleEffect4"	파티클 효과번호
Performer check 1: 1	Performer가 있다고 판단되는 1의 경우, 1번이펙트 매칭
Gesture2: 2	Gesture2과 2번이펙트 매칭
Gesture3: 3	Gesture3과 3번이펙트 매칭
Gesture3: 4	Gesture4과 4번이펙트 매칭

3.5 실험 방법

총 5명의 참가자가 한 동작마다 10회씩 반복한 후 각 영상을 프레임별로 쪼개어 이미지 데이터를 생성하였다. 4명의 데이터를 학습데이터로 사용하고 1명의 데이터는 테스트 데이터로 사용하였다. 최종

생성된 데이터셋에 대해 CNN을 활용하여 흑백 영상인 모션 히스토리 이미지 기반의 제스처 인식 실험을 진행하였다. <표 4>는 <표 1>의 제스처에 관한 MHI이다.

<표 4> 각 타겟 제스처에 대한 모션 히스토리 이미지



3.6 실험 결과

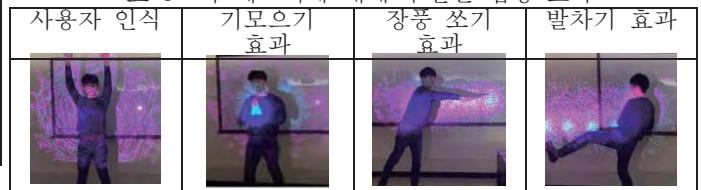
<표 5>는 각 제스처에 대한 인식 실험을 진행한 결과이다.

<표 5> 모션 히스토리 이미지 입력에 따른 제스처 인식률 및 하나의 제스처 인식에 걸리는 시간

Number of filters in Convolution Layer1	Number of filters in Convolution Layer2	Number of nodes in FC layer	Accuracy
32	32	32	0.90
16	16	16	0.95
8	8	8	0.91

<표 6>은 최종적으로 구현된 동적 프로젝션 맵핑 애플리케이션을 사용하여 실제로 제스처를 취했을 때 보여지는 인터랙션 맵핑 효과이다. 결과이다.

<표 6> 각 제스처에 대해 구현된 맵핑 효과



4. 결론

우리는 기존의 동적 프로젝션 맵핑 공연 기술의 유연한 공연 연출을 위해 MHI 기반의 제스처 인식 방법을 통한 동적 프로젝션 맵핑 프레임워크 구현을 시도하였다. 해당 논문에서 제안된 방법은 MHI라는 보다 가벼운 메모리를 통해 제스처를 인식하고 아웃풋을 재현한다. 본 논문에서 구현한 동적 프로젝션 맵핑 프레임워크는 동적 프로젝션에 대해 사용자의 경험을 보다 쉽게 유도할 수 있고 연출하고자 하는 맵핑 연출의 빠른 테스트가 가능할 것으로 예상된다.

사사의 글

이 연구는 “한국연구재단
이공학개인기초연구지원사업
(NRF-2017R1D1A1B03035718)”의 지원을 받아서 수행되었다.

참고문헌

- [1] The Most Amazing Multimedia Act Gets A Simo Cowell Standing Ovation!-America's Got Talent 2018, <https://youtu.be/B3ZlW4-BI4>
- [2] Multimedia Show / video mapping 360 / dome projection / Danel Stryjecki, <https://youtu.be/zrF52zwk284>
- [3] Mayam Asadi-Aghbolaghi, Albert Clapes, Marco Bellantonio. A survey on deep learning based approaches for action and gesture recognition in image sequences. Washington, D.C., USA IEEE 2017
- [4] Motion History Images from Wikipedia, https://en.wikipedia.org/wiki/Motion_History_Images

Unity 기반 물리 실험 교육 시뮬레이터 개발

김연정*, 윤세희**, 신병석*

*인하대학교 컴퓨터공학과

**인하대학교 인간중심컴퓨팅연구소

leeyh0109@nate.com, heehee2738@naver.com, bsshin@inha.ac.kr

Development of Unity-based Physics Experiment Education Simulator

Yeon Jeong Kim*, Sei Hee Yun**, Byung-Seok Shin*

*Department of Computer Science and Engineering, Inha University

**Human Centered Computing Research Center, Inha University

요 약

공학기술의 발전에 따라 인간은 Smart Learning을 넘어서 증강/가상현실 기술을 현실에 접목하여 교육의 매체로 사용을 하고자 여러 방면으로 시도를 하고 있다. 이에 과학교육 방면에서도 가상현실 환경 구축 기술을 이용하여 공간 및 상황 등의 여러 제한에서 벗어나 보다 다양하고 활동적인 실험을 할 수 있는 물리 실험 시뮬레이션을 필요로 하고 있다. 본 연구에서는 Unity Editor를 이용하여 코드 스크립트를 적용하여 가상 세계를 구축하고 물리 현상 중 하나인 포물선 운동 공식을 활용한 실험 프로그램을 만들어 VR 구현기기인 Vive를 이용하여 실제 물리실험에 적용한 사례를 소개한다.

1. 서론

4차산업 혁명으로 인해 우리 사회는 스마트폰, 스마트TV, 스마트 웨어러블 등에 친숙해지고 자연스레 일상생활에서 스마트 디바이스를 활용하고 있다. 교육 분야에서도 스마트 디바이스를 이용하여 PC를 이용해 수업을 듣던 이러닝을 접근성과 이동성, 개인성을 앞세운 스마트 러닝(Smart Learning)으로 변화시키고 있다[1].

특히 컴퓨팅 및 그래픽 기술의 발달과 함께 새로운 기술이 적용된 다양한 스마트 매체들이 개발되고 있는데 그 중 증강현실 기술은 증강현실 전용 매체를 이용하여 가상 현실 공간 체험을 통해 현실감 있는 학습을 제공하고, 학습자의 직접적인 조작 및 활동을 통하여 새로운 학습경험을 제공할 수 있는 교육 매체로 높은 관심을 받고 있다[2]. 증강현실을 이용한 가상현실 기술의 교육적 활용이 관심을 받고 있는 이유 중 하나는 기존의 교육 매체들과 비교했을 때 학습자가 가상에서 구현된 세계의 모습을 볼 수 있고 디지털화된 정보를 얻을 수 있다는 독보적인 학습정보 제시방법 때문이다.

이러한 교육적 관심을 바탕으로 가상현실 학습이 물리교육에서의 학습효과를 향상시켜줄 수 있는 가능성이 있는지, 또는 가상현실의 어떤 특징적인 요

인들이 물리 학습 활동과 관련되어 교육면에서 활용할 수 있는지에 대한 연구를 진행해보았다. 이와 같은 배경에서 본 연구에서는 물리의 성질 중 ‘파찰력’과 관련하여 가상현실 실험을 구성하여 체험해보고자 하였고 이를 발판으로 다른 물리의 성질을 이해할 수 있는 실험을 설계할 수 있는지 여부를 확인하여 물리실험 시뮬레이션 VR프로그램의 개발 가능성 및 다른 공학 매체를 이용하여 물리 및 과학 과목의 교육법의 발전 및 향상 가능성을 알아보고자 한다.

2. 관련연구

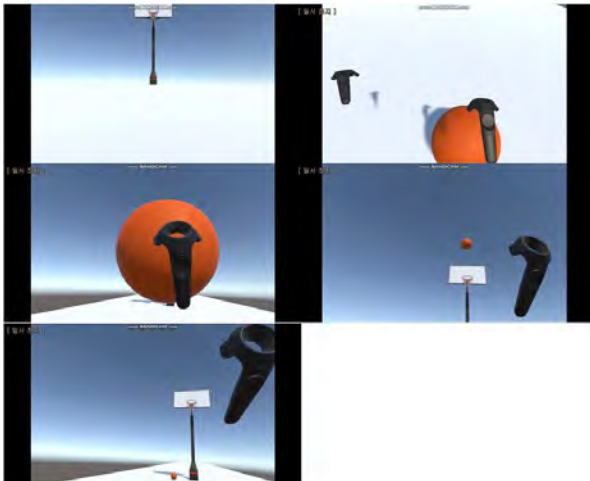
STEAM은 미국에서 시작한 STEM(Science, Technology, Engineering, Mathematics)에 예술(Arts)을 추가한 것이다[3]. STEM은 미국의 기술교육 전문가들에 의하여 시작되었고, OSU와 NCSU에서 시작한 MST(수학, 과학, 기술)에 Virginia Tech에서 E(공학)를 접목하여 시작된 개념이다[4]. STEM의 두 가지 흐름은 과학교육을 통한 STEM과 기술교육을 통한 STEM으로 구분할 수 있다[6].

융합인재교육(STEAM)은 과학과 수학의 기초 이론과 개념을 토대로 기술적 방법과 시스템을 통해 실생활과 연계된 공학적 실행을 적용하고 여기에 예술적 감성을 입혀 과학기술에 대한 학생들의 흥미와 이해를 높이고, 과학기술기반 융합적 소양(STEAM

LITERACY)과 문제해결력을 배양하는 교육으로 정의할 수 있다.

3. 물리 시뮬레이션 설계 및 구현

실험은 포물선 운동에 관련한 포물체의 무게 및 속도에 따른 포물선 운동을 기반으로 설계하였다. 실험 시뮬레이션은 농구 게임 형태로 구현이 되었으며, 공의 무게 및 속도, 각도, 골대와의 거리를 사용자가 스스로 조절하면서 공을 골대에 넣을 수 있도록 하는 내용이다. 공이 골대를 통과했을 때만 Goal을 인정하였고, 골대 아래에서 공이 통과했을 때, 골대 테두리에 공이 맞았을 때 등은 Goal을 인정하지 않도록 설계하였다. 공을 던지는 위치 및 각도는 사용자가 직접 움직이면서 조절을 할 수 있도록 하였고, 공을 던지는 세기, 속도 등은 코딩 및 Unity 엔진을 활용하여 사용자가 직접 세팅을 할 수 있도록 하였다. 해당 시뮬레이션을 직접 체험하기 위하여 VR 실험 기기인 Vive를 이용하였다.



(그림 1) 가상현실에서의 게임 장면

실험에서는 실험체인 공이 포물선 운동을 할 수 있도록 코드를 만들어 설정하였고, 공이 농구 골대를 통과했을 때만 득점 인정이 되도록 하였다. 만약 골대 아래에서 공이 통과된 후 수직으로 떨어지며 다시 골대를 통과할 때에는 득점 인정이 되지 않도록 하였으며, 공이 바닥에 한번 닿은 후에 정상적으로 공이 골대를 통과하였을 때 득점이 될 수 있도록 예외 처리를 하였다. 또한 공이 농구 골대의 다른 부분과 충돌했을 때는 공이 튕겨져 나오도록 충돌 처리를 하였다.

Vive Controller를 이용하여 사용자 스스로 공을 들고서 움직이며 골대에 공을 넣을 수 있도록 하였다. 게임이 시작되면 공이 사용자의 앞에 떨어지고,

그 공을 주워서 골대에 넣는 방식으로 게임을 진행할 수 있도록 하였다. 이 때, 사용자가 가상현실에서 중력을 이겨낼 수 있도록 Y방향으로 10, Z방향으로 10의 힘을 추가시켜주었다. X방향으로 힘을 주게 될 경우, 물체를 앞으로 던질 때 우측 방향으로 휘어서 들어가기 때문에 힘을 설정하지 않았다.

코드스크립트를 적용 후 농구 게임을 진행하면 [그림 1]과 같은 플레이 상황을 확인할 수 있다. 공이 골대를 제대로 통과를 했을 때만 득점이 인정되며 공이 골대 아래에서 위로 골대를 통과한 후 다시 위에서 아래로 골대를 통과했을 경우, 골은 인정되지 않았다.

가상현실을 이용하여 실험 시뮬레이션 구현 및 진행을 함으로써 물리 엔진과 VR 구현 장비를 통해 물리 공식을 체험할 수 있었다. 이는 학교의 재정적인 면에서 비용 대비 가성비가 좋고 실험을 손쉽게 여러 번 반복하여 진행할 수 있으며 오차의 범위가 좁기 때문에 정확한 물리 개념을 전달할 수 있다는 장점이 있다. 또한 학교뿐만 아니라 물리 엔진과 VR 구현 기기가 있는 곳에서는 직접 실험을 설계하고 진행할 수 있다는 장점이 있다.

컴퓨터 언어를 사용할 수 있는 학생이라면 물리 엔진을 통해 실험을 직접 구현을 해서 실험 진행을 할 수 있기 때문에 물리와 컴퓨터공학 분야의 융합된 학습을 진행할 수 있으므로 현재 우리나라의 교육과정에서 지향하고 있는 STEAM 교육법에 적합하다고 할 수 있다.

4. 결론

본 연구에서 가상 세계에서 구현한 실험은 물리 현상 중 포물선 운동에 관련한 실험으로, 농구 게임을 통하여 포물체에 적용하는 힘, 각도 등의 변인에 따라 포물체의 진행 방향이 달라질 수 있다는 것을 체험할 수 있는 시뮬레이션을 만들어 실행해보는 실험이었다.

가상현실에서 물리 실험을 구현하여 진행하는 것의 가장 큰 장점은 우리가 실제 세계에서 통제할 수 없는 변인들을 통제할 수 있어 실험의 오차를 줄일 수 있다는 것이다. 이에 따라 학생들은 실험을 진행하면서 수업시간에 배운 이론을 직접 경험해 볼 수 있으며, 이로 인하여 학생들이 가질 수 있는 물리적 오개념을 바른 개념으로 심어줄 수 있다. 아울러 본 연구에서는 포물선 운동에 대해서만 실험을 구현하였으나 학문적 범위를 확장하여 마찰력, 뉴턴의 운

동 법칙, 역학적 에너지의 보존 법칙, 물체의 운동 변화 등의 일반 역학을 넘어 전반적인 물리 실험에 대해서 구현 가능성을 확인할 수 있었다. 또한 물리 분야를 넘어서 이공학 분야의 실험을 구현 및 진행할 수 있다는 가능성을 확인할 수 있었다.

참고문헌

- [1] 이인숙, “스마트러닝에서 모바일 증강현실의 효과적인 활용 방향성 제안”, 한국디자인포럼, 제 40호, 195-208(14 pages), 2013
- [2] 장상현, “증강현실(Augmented Reality) 콘텐츠의 교육적 적용”, 한국콘텐츠학회지, 제 5권, 제 2호, 79-85(7 pages), 2007
- [3] 맹준희, “스마트교육기반 STEAM프로그램 적용에 관한 연구”, 한국기술교육학회지, 제 14권, 제 2호, 258-287(30 pages), 2014
- [4] 이철현, “융합인재교육(STEAM)의 스마트러닝 전략”, 한국실과교육학회지, 제 25권, 제 4호, 123-147(25 pages), 2012
- [5] 심재호, “STEM, STEAM 교육과 우리나라 융합인재교육의 이해와 해결 과제”, Journal of the Korean Association for Science Education, 제 35권, 제 4호, 709-723(16 pages), 2015
- [6] 김진수, “기술교육의 새로운 통합교육 방법인 STEM 교육의 탐색”, 한국기술교육학회지, 제 7권, 제 3호, 1-29(29 pages), 2007

2020 온라인 춘계학술발표대회 논문집 제27권 제1호

발 행 일 : 서기 2020년 5월 29일 발행

발 행 인 : 이 상 현

발 행 처 :  **사단법인 한국정보처리학회**
KIPS Korea Information Processing Society

04376 서울시 용산구 한강대로 109, 1002호(한강로 2가 용성비즈텔)

TEL : (02) 2077-1414(代)

FAX : (02) 2077-1472

<http://www.kips.or.kr>

E-mail : kips@kips.or.kr

인 쇄 처 : (주)이환디앤비

((02) 2254-4301(代), E-mail : ewhan@ewhan.com)
