OT 네트워크에서 자산 식별을 위한 네트워크 트래픽 특성 분석

Analyzing Network Traffic Characteristics for Asset Identification in OT Network

박민수
단국대학교 인공지능융합학과
경기도 용인시
mspark@dankook.ac.kr

안석현
단국대학교 소프트웨어학과
경기도 용인시
seokhyun@dankook.ac.kr

조성제*
단국대학교 소프트웨어학과
경기도 용인시
sjcho@dankook.ac.kr

김홍근
동국대학교 국제정보보호대학원
정보보호학과
서울특별시 중구
hgkim4044@gmail.com

요 약

디지털 전환으로 인해 스마트 전력망, 스마트 빌딩, 스마트 팩토리 등의 '스마트 X' 기술로 인해 OT(Operational Technology) 네트워크가 인터넷과 연결되고 있다. 이로 인해 OT 네트워크에 대한 사이버 공격이 증가하고 있다. 사이버 공격을 방어하기 위한 시작점은 조직의 네트워크 내 자산을 식별하는 것이다. OT 시스템의 자원 부족과 실시간성의 요구로 인해, 전통적인 IT 시스템에서 사용되었던 자산 식별 방법을 OT 시스템에 적용하는 것은 한계가 있다. 본 논문에서는 OT 네트워크에서 자산을 식별하기 위한 네트워크 트래픽 특징 정보를 선정하고, 이를 활용하여 OT 장치를 식별할 수 있음을 보인다.

키워드 : 자산 식별, OT(Operational Technology), 네트워크 트래픽 특성, TTL(Time To Live)

1. 서론

OT는 하드웨어 및 소프트웨어를 기반으로 산업용 장비를 제어하는 기술로, 산업 사물 인터넷(Industrial Internet of Things) 및 산업제어시스템(Industrial Control System)과 같은 시스템에 사용되고 있다[1][2]. 최근 디지털 전환으로 인해 독립되어 있는 OT 영역이 IT 기술과 융합되면서 산업 전반에 편리함을 제공함에 따라, 스마트 전력망, 스마트 운송, 스마트 빌딩, 스마트 공장 등 산업 전반에 OT가 융합된 시스템이 증가하고 있다[3].

이러한 융합 기술이 편리성을 제공함과 동시에 보안에 대한 위협은 증가하고 있다[3]. 늘어나는 보안 위협을 효율적으로 방어하기 위해서는 중요 인프라에 있는 자산을 식별하고, 취약점 탐지 및 완화 조치를 수행해야 한다. 하지만, OT 장비들의 가용성 중요도와 자원의 한계로 인해 IT 시스템에서 자산을 식별하기 위해 사용하던 네트워크 스캐닝(Network Scanning) 기법이 적용하기 어렵다는 문제에 직면해 있다[2][4][5].

이를 해결하기 위해, 본 논문에서는 OT 네트워크에서 자산 식별을 위해 스마트 공장 네트워크에서 트래픽을 수집하고 OSI 7 Layer의 응용 계층, 전송 계층, 네트워크 계층 관점에서 특징 정보를 추출해 자산을 식별하는 연구를 수행하였다.

2. 관련연구

Caselli 등[6]은 장치 식별을 위해 사용되는 지문(Fingerprint) 채취 기술이 지원되지 않는 OT 및 ICS 환경에서 장치를 식별할 수 있는 장치 지문(Fingerprint)의 적용 가능성을 분석하고, 네트워크 지문을 만드는데 필요한 참조 모델 제시하였다.

Ghazo 등[7]은 20개의 네트워크 특징정보(프레임 길이, 공급업체 MAC ID, TCP Segment Length 등)를 활용하여, ICS 환경에서 장치의 통신 패턴과 장치 지문을 생성하여 제어 계층을 식별하고 제조 업체 및 모델을 식별하는 연구를 수행하였다.

Keliris 등[8]은 ICS 프로토콜인 Modbus를 활용해 산업용 장치 식별 기법을 제안하였다. 해당 연구는 Modbus 프로토콜이 제조사마다 구현이 다르다는 특성을 기반으로 연구가 진행되었다. 해당 연구는 인터넷에 연결된 308개의 장치에 대한 제조사 및 모델 정보를 정확하게 식별하여 Shodan의 장치 식별 기능을 28% 향상시켰다.

3. 실험 환경 및 설계

본 절에서는 OT 자산 및 장치가 있는 네트워크 실험 환경과 실험 내용을 설명한다. 그림 1은 네트워크 트래픽을 수집한 실험 환경을 보여준다.

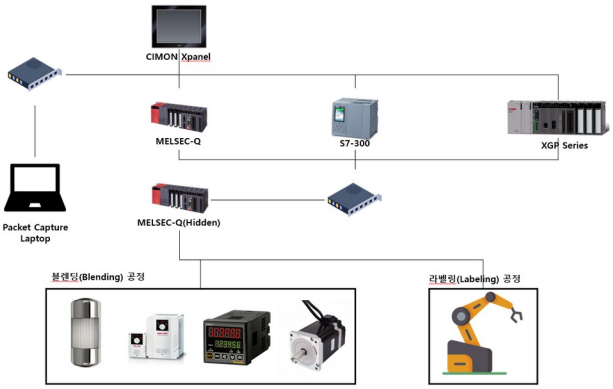

그림 1. 실험 환경 토폴로지

실험 환경은 총 4개의 PLC(Programable Logic Controller)와 1개의 HMI(Human-Machine Interface)로 구성된 네트워크에서 라벨링(Labeling) 공정과 블렌딩(Blending) 공정을 제어하는 OT 네트워크이다. 네트워크 트래픽 수집을 위해 HMI와 PLC를 연결해주는 네트워크 허브에서 포트 미러링(Port Mirroring) 설정한 후, 노트북에서 Wireshark 도구를 사용해 다음과 같이 2가지 경우에 대해 네트워크 트래픽을 수집하였다.

- 공정을 작동시키지 않는 경우(6시간 수집)
- 공정을 작동시키는 경우(6시간 수집)

표 1은 실험 환경의 OT 자산 목록을 보여준다. 이 중 Mitsubishi PLC는 총 2개로 구성되어 있으며, HMI와 상호작용하는 MELSEC-Q PLC와 직접적으로 공정을 제어하는 MELSEC-Q(Hidden) PLC로 나뉜다.

표 3. 장치 별 전송 계층 특징정보 비교

구분	모델명	TCP Window Size			TCP Segment Length			UDP Data Length		
		최소	최대	평균	최소	최대	평균	최소	최대	평균
공정 제어	XGT Series	16000	16000	16000	54	64	56.1	0	0	0
	MELSEC-Q	6132	6144	6138	30	83	32	0	0	0
	MELSEC-Q (hidden)	0	0	0	0	0	0	18	1472	484
	S7-300	2048	2048	2048	26	45	35.5	0	0	0
	Xpanel	62	68	65.1	33	61	60.4	40	40	40
공정 미제어	XGT Series	16000	16000	16000	54	64	56	0	0	0
	MELSEC-Q	6132	6144	6138	30	80	32.5	0	0	0
	MELSEC-Q (hidden)	0	0	0	0	0	0	18	1472	484
	S7-300	2048	2048	2048	26	45	35.5	0	0	0
	Xpanel	0	8192	65.1	33	61	60.4	40	40	40

표 1. 실험 환경 OT 자산 목록

장비	모델명
LS Electric PLC	XGT Series
Mitsubishi PLC	MELSEC-Q
Siemens PLC	S7-300
CIMON HMI	Xpanel

4. 실험결과

특징 정보 분석을 위해 OSI 7 계층의 응용 계층, 전송 계층, 네트워크 계층 관점에서 특징 정보를 추출하였다. 추출된 정보들은 [9][10][11][12]에서 IoT(Internet of Things) 장치 식별 정보로도 활용되었으며, 본 실험에서는 OT 장치를 식별하기 위해 특징 정보로 활용될 수 있음을 보인다.

4.1. 응용 계층에서 특징정보 분석

OT 장치는 자동 제어를 위해 제조사마다 독립적인 프로토콜을 사용한다. 표 2는 실험 환경에서 장치별로 사용하는 프로토콜을 분석한 내용을 보여준다.

표 2. OT 장치의 네트워크 프로토콜 사례

장비	프로토콜
XGT Series	XGP 전용 프로토콜
MELSEC-Q	Modbus
MELSEC-Q (Hidden)	MELSEC 전용 프로토콜
S7-300	S7 comm 프로토콜
Xpanel	Modbus

표 2는 공정을 제어하는 경우와 제어하지 않는 경우 모두 동일하다. MELSEC-Q와 Xpanel은 산업에서 자동 제어를 위해 만들어진 Modbus 프로토콜을 사용한다. 반면, XGT Series, MELSEC-Q(hidden), S7-300은 제조사 별로 개발한 전용 프로토콜을 사용한다. 즉, 장치 별로 사용하는 프로토콜을 확인하는 것은 장치를 식별하는데 유용한 정보가 될 수 있음을 알 수 있다.

4.2. 전송 계층에서 특징정보 분석

전송 계층에서는 TCP window size, TCP segment length, UDP data length의 최솟값, 최댓값, 평균값을 특징정보로 사용한다. 해당 특성은 장치 제어를 수행한 경우와 수행하지 않은 경우 발생하는 패킷에서 일부 차이가 발견되었다. 표 3은 특징 정보의 변화들을 보여주며, 모든 수치의 단위는 바이트(byte)이다.

제조사 전용 프로토콜을 사용하는 PLC 장치들(XGT Series, MELSEC-Q, S7-300)에서 각각 TCP window size의 최댓값, 최솟값, 평균이 모두 동일한 값을 갖고 있다는 것을 알 수 있다. TCP window size는 상대방에게 자신이 수용 가능한 window 크기를 알려주는 역할을 한다. 하지만, MELSEC-Q(Hidden) PLC는 TCP 프로토콜을 사용하지 않고 UDP 프로토콜로 통신하고 있었기 때문에 TCP window size와 TCP segment length 값을 파악할 수 없었다.

모든 PLC의 window size는 공정을 제어할 때와 제어하지 않을 때 모두 일치했다. HMI인 CIMON Xpanel만 공정을 제어하지 않을 때 최댓값과 최솟값이 변화가 있지만 평균의 값은 변화가 없는 것을 확인할 수 있다. 트래픽 분석 결과, 2개의 패킷만이 window size에서 변화를 보였다. 나머지 TCP segment length 값이 공정을 제어하는 경우와 제어하지 않은 경우에 XGT series와 MELSEC-Q에서 각각 0.1, 0.5 만큼 차이가 발생했다. UDP data length는 모두 동일한 것을 알 수 있다.

일부 특징 정보에서 차이가 발생했지만, 대부분의 특징 정보는 장치마다 값이 다르고 변화가 일정하기 때문에 장치를 식별하는 정보임을 알 수 있다.

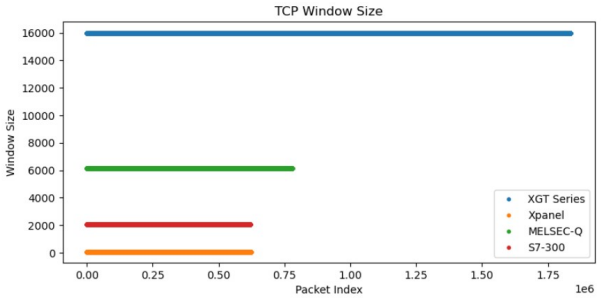

그림 2. 장치 별 TCP window size 변화

그림 2는 특징 정보가 변화하지 않는 것을 확인하기 위해 공정을 제어하고 있을 때, TCP

window size 값의 장치 별 변화를 점 그래프를 통해 보여준다. x 축은 패킷의 순서를 나타내는 패킷 인덱스(packet index)이며, y 축은 window size 값을 나타낸다. 장치를 제어하지 않는 경우와 장치를 제어하는 경우 window size 는 장치마다 값이 다르며, 모든 패킷에서 일정한 것을 알 수 있다.

4.3. 네트워크 계층에서 특징정보 분석

네트워크 계층에서 사용되는 특징 정보로 IP 헤더의 TTL(Time To Live) 값을 사용한다. IP 헤더의 TTL 값을 4.2 절과 마찬가지로 최솟값, 최댓값, 평균값을 확인하여 장치를 제어하는 경우와 장치를 제어하지 않는 경우 변화가 있는지 확인한다. TTL 값은 운영체제마다 기본 값이 다르게 설정되어 있어 운영체제를 식별하는 요소로도 사용되고 있다[13].

표 4 는 장치를 제어하는 경우와 제어하지 않는 경우 TTL 의 최솟값, 최댓값, 평균값을 분석한 내용을 보여준다. 공정을 제어하는 경우와 제어하지 않는 경우 장치마다 모두 동일한 값을 확인할 수 있다. 즉, 해당 특징정보는 장치마다 값이 다르고, 고유한 특징정보이기에 장치의 고유한 정보임을 알 수 있다.

표 4. 장치 별 TTL 값 비교

모델명	공정 제어 시 TTL 값			공정 미 제어 시 TTL 값		
	최소	최대	평균	최소	최대	평균
XGT Series	64	64	64	64	64	64
MELSEC-Q	250	250	250	250	250	250
MELSEC-Q (Hidden)	64	64	64	64	64	64
S7-300	60	60	60	60	60	60
Xpanel	128	128	128	128	128	128

마지막으로, 그림 3 은 4.2 절에서 확인한 window size 와 같이 TTL 의 패킷 별 변화를 점 그래프로 보여준다. 장치를 제어하는 경우와 제어하지 않는 경우 TTL 값은 모두 동일하였으며, 모든 패킷이 일정한 값의 TTL 갖는 것을 알 수 있다.

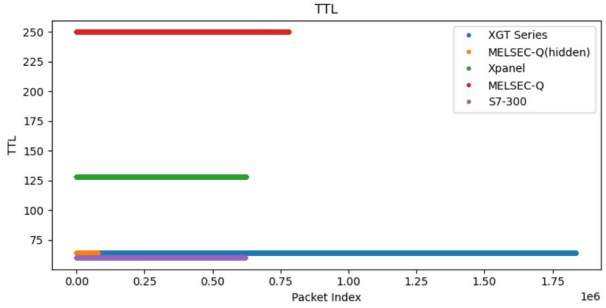

그림 3. 장치 별 TTL 변화

5. 결론

본 논문에서는 OT 네트워크에서 자산을 식별하기 위해 OSI 7 계층을 기준으로 응용 계층, 전송 계층, 네트워크 계층에서 활용할 수 있는 특징 정보를 사용하여 자산을 식별할 수 있음을 확인하였다. 실험 결과 각 계층별로 활용할 수 있는 특징정보들은 모두 실험에서 사용한 장치를 식별하는데 있어 고유한 정보인 것을 알 수 있었다. 하지만, 실험에 사용된 장치의 수가 적기 때문에 다른 OT 장치에 대한 추가적인 실험이 필요하다. 장치의 수가 많아지면, 지금까지 확인한 특징 정보로는 중복이 발생할 수 있어 추가적인 특징정보가 필요할 수 있다. 추가적인 특징 정보로 네트워크 흐름(network flow) 기반 특징 정보인 흐름 볼륨(flow volume), 패킷 간 도착 시간(inter arrival time)이 클록 스큐(clock skew) 등을 활용할 수 있다[14]. 향후 연구에서는 시장 점유율을 기반으로 분석 대상을 확대하여, 광범위한 OT 제품에 적용 가능한 자산 식별 기법을 개발할 계획이다.

Acknowledgement

이 논문은 산업통상자원부(MOTIE)와 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구 과제임 (No. 20212020800120).

참 고 문 헌

[1] Stouffer Keith, Joe Falco, and Karen Scarfone, "Guide to industrial control systems (ICS) security," NIST special publication 800.82, 16-16, 2011.

[2] Henri Pulkkinen, “SAFE SECURITY SCANNING OF A PRODUCTION STATE AUTOMATION SYSTEM,” Tampere University, 2022.

[3] Mark Bristow, "A SANS 2021 Survey: OT/ICS Cybersecurity," SANS Institution, 2021.

[4] Thomas Hanka, Matthias Niedermaier, Florian Fischer, Susanne Kießling, Peter Knauer and Dominik Merli, “Impact of Active Scanning Tools for Device Discovery in Industrial Networks,” Security, Privacy, and Anonymity in Computation, Communication, and Storage (SpaCCS), Proceedings 13, 557-572, 2020.

[5] J Helms, B Salazar, P Scheibel, M Engels, and C Regier, “Safe active scanning for energy delivery systems final report,” Lawrence Livermore National Lab (LLNL), No. LLNL-TR-740556, 2017.

[6] Marco Caselli, Dina Hadžiosmanović, Emmanuele Zambon, and Frank Kargl, “On the feasibility of device fingerprinting in industrial control systems,” Critical Information Infrastructures Security: 8th International Workshop (CRITIS), Sprintinger International Publishing 8, 155-166, 2013.

[7] Alaa T. Al Ghazo, and Ratnesh Kumar, "Ics/scada device recognition: A hybrid communication-patterns and passive-fingerprinting approach," IFIP/IEEE Symposium on Integrated Network and Service Management (IM), IEEE, 2019.

[8] Anastasis Keliris, and Michail Maniatakos, "Remote field device fingerprinting using device-specific modbus information," IEEE 59th international Midwest symposium on circuits and systems (MWSCAS), IEEE, 2016.
[9] Markus Miettinen, Samuel Marchal, Ibbad Hafeez, N. Asokan, Ahmad-Reza Sadeghi, and Sasu Tarkoma, "Iot sentinel: Automated device-type identification for security enforcement in iot," IEEE 37th International Conference on Distributed Computing Systems (ICDCS), 2017.
[10] Vian Adnan Ferman, and Mohammed Ali Tawfeeq, "Machine learning challenges for IoT device fingerprints identification," Journal of Physics: Conference Series. Vol. 1963. No. 1. IOP Publishing, 2021.
[11] Bruhadeshwar Bezawada, Maalvika Bachani, Jordan Peterson, Hossein Shirazi, Indrakshi Ray and Indrajit Ray, "Behavioral fingerprinting of iot devices," Proceedings of the 2018 workshop on attacks and solutions in hardware security. 2018.
[12] Arunan Sivanathan, Hassan Habibi Gharakheili, Franco Loi, Adam Radford, Chamith Wijenayake, Arun Vishwanath, and Vijay Sivaraman, "Classifying IoT devices in smart environments using network traffic characteristics," IEEE Transactions on Mobile Computing 18.8, 1745-1759, 2018.
[13] Lyon, Gordon Fyodor. Nmap network scanning: The official Nmap project guide to network discovery and security scanning. Insecure, 2009.
[14] Pedro Miguel Sánchez Sánchez, José María Jorquera Valero, Alberto Huertas Celdrán, Gérôme Bovet, Manuel Gil Pérez and Gregorio Martínez Pérez, "A survey on device behavior fingerprinting: Data sources, techniques, application scenarios, and datasets," IEEE Communications Surveys & Tutorials 23.2, 1048-1077, 2021.