SDN(Software-Defined Network) Network상에서 인공지능을 활용한 네트워크장비의 장애예측 및 대응시스템구현에 관한 연구

함대훈*

*(주)에스비정보기술

*dhhaam@sbit.co.kr

An Implementation of SDN Controller that has the AI algorithm can both detect network device faults and automatically handle them.

Haam Dae Hoon*

*SBIT

요 약

본 논문은 SDN 네트워크상에서 발생하는 다양한 형태의 요인으로 말미암아 서비스에 지장을 주는 것을 장애라 정의 하고 이에 대한 해결책으로 인공지능의 여러 알고리즘을 적용하여 자동화를 통하여 인간의 개입 없이 판단하고 조치를 취하는 시스템 구현에 대해 논하였다. 장애에 대한 판단은 네트워크 장비들이 제공하는 명확한 정보를 바탕으로 네트워크 장비의 통계를 바탕으로 하는 것과 Traffic 정보의 Pattern을 분석하여 이를 근거로 장애를 판단하는 것이 있다. 장애로 판명될 경우, 이에 대한 처리는 경험적 바탕에 근거를 둔 여러 정책을 적용하여 서비스의 지장이 없도록 하는 시스템을 목적으로 개발하였으며 장애 종류별 대응 알고리즘은 부분적으로 개발 시험 중이다. 명확한 장애에 대한 자동화는 기대한 것 이상의 결과를 보여주었으며, 시스템 장애 시 관련된 장비를 서비스에서 제외시키고 서비스 중인 Traffic을 우회시키고 새로운 Traffic 요청에 에 대해 새로운 경로를 결정하기 위한 강화학습기반의 알고리즘을 개발하여 시험 망에서 시험 중이다. 본 논문은 이라한 시스템을 구성하는 요소, 알고리즘의 구현 단계, 그리고 SDN을 기반으로 했을 때의 장점에 대해 논하였다..

Ⅰ. 서 론

데이터 통신은 지난세기 발전을 가져와 제3의 산업혁명을 이끌었으며, 5G 네트워크로 진화하면서 인공지능, 자율주행 자동자등의 초고속, 초저지연에 대한 네트워크의 요구사항을 만족하도록 발전하고 있다. 네트워크는 데이터 전달에 대한 경로 설정을 결정하는 제어 평면 부분과 실제 데이터 전송을 담당하는 데이터 평면으로 나뉜다. 기존 라우터와 스위치들은 제어평면과 데이터 평면을 동시에 제어하고 하나의 물리적 공간을 통해서 제어를 위한 정보와 실제 데이터 전송을 하고 있으며, 제어정보는 제조사 고유의 소프트웨어를 사용하여 제조사간 호환은 불가능하였다. 이러한 기존네트워크의 한계를 극복하고자 SDN이 제안되었으며 SDN은 제어평면과 데이터 평면을 분리하고 제어평면에 대한 표준화를 진행하여 제조사간 호환을 보장한다. 이러한 SDN에서도 다양한 장애가 발생하고 있으며, 그 장애에는 라우터, 스위치 같은 장치에서 발생하는 장애 , 데이터의 이상흐름 그리고 알 수 없는 전체 네트워크 차원의 성능저하가 포함된다. 이러한 다양한 장애에 대해 이를 처리하기 위해 인공지능 기반의 자동화 알고리즘 및 네트워크의 성능 저하를 가져오는 다양한 형태의 장애에 대한 처리 연구[1]를 바탕으로 시스템의 이상 징후를 인지하고 선제적으로 대응할 수 있는 인공지능 알고리즘 및 이를 바탕으로 대응 시스템개발에 대한 연구를 하고자 한다.

Ⅱ. 본론

본 논문에서는 SDN의 Data 평면에서의 장애처리를 인공지능 알고리즘을 활용하여 자동적으로 감지하고 그에 대한 대응을 할 수 있는 시스템 개발 및 구현에 관해 논하고자한다. 시스템 구성은 그림1. 과 같다. 그림1과 같은 구성에서 SDN Controller에서 수집되는 SNMP (Simple Network Monitoring System)정보와 Traffic정보 그리고 통계정보를 활용하여 네트워크의 이상 징후를 파악한다..

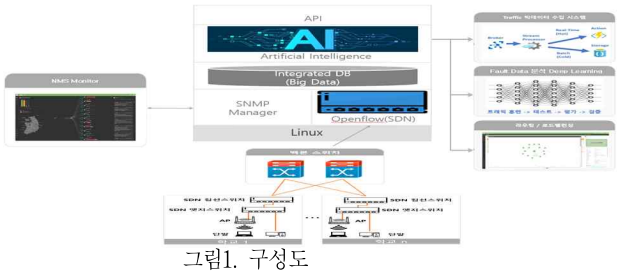

그림1. 구성도

네트워크 장비들이 전송하는 명확한 정보(Critical, Major, Minor 알람)과 장비의 통계정보를 조합하여 인공지능 알고리즘을 활용하여 Data 셑들과의 유사도 검사를 해서 유사도가 없다면 Single Failure로 간주하고 Traffic path를 다른 곳으로 Routing시킨 후 시나리오에 따라 장비를 복구 시도를 하고 그래도 복구가 안 될 때에는 Routing Path에서 제외시킨다.

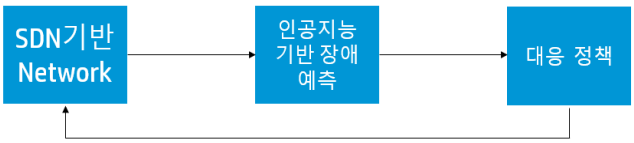

그림2. 장애 예측 및 정책 적용

Data Set	Value	Data Set	Value
CPU Load	30/50/70	Fan 상태	정상/이상
Memory	30/50/70	온도	50/60/70
Input Load	Bytes	Link Down	횟수
Output Load	Bytes	Rebooting	횟수

표 1. 장애에 대한 Data Set

한편, Traffic을 분석하여 이상 징후를 판단하는 것 중 대표적인 DDos(Distributed Denial of Service)공격에 대해서는 많은 연구가 되고 있으며[2] ,본 연구에서는 Clustering의 기법중 하나인 Random cut Forestfh 판별 한 후 STM알고리즘을 통한 DDoS를 판별한다. DDoS라 판별된 경우 경험에 의해 만들어진 정책을 통하여(Port 분리 /연결/ Port 분리)대응 한다.

장비의 장애. 또는 DDoS 공격을 받은 장비는 일시적으로 서비스에서 제외시키고 일정시간 후 서비스 복귀를 시키며, 서비스가 진행되던 또는 새로이 진행될 서비스는 다른 장비로 Routing할 수 있도록 강화학습 기반의 경로설정 알고리즘으로 최적의 경로를 선택하여 SDN스위치의 Flow Table을 제어한다.

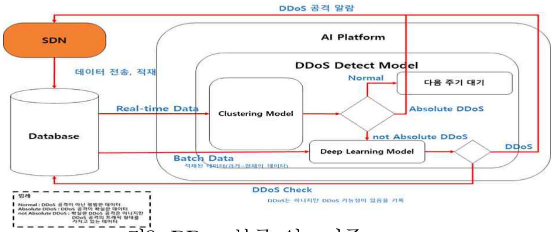

그림3. DDos 분류 알고리즘

$$Q(S_t, A_t) \leftarrow Q(S_t, A_t) + \alpha\,(R_{t+1} + \gamma \max_{a'} Q(S_{t+1}, a') - Q(S_t, A_t))$$

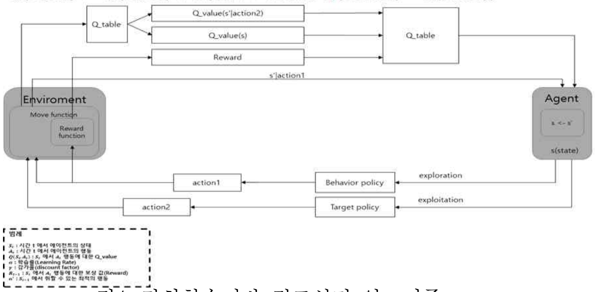

그림4. 강화학습기반 경로설정 알고리즘

Ⅲ. 결론

본 논문에서는 SDN상의 네트워크 환경 하에서 네트워크장비를 포함한 이상 징후 상태를 인공지능 알고리즘으로 종합적으로 파악 한 후 제어를 하기 위하여, 스위치 제조사가 다르더라도 SDN Openflow 규격을 준수하는 장비에 대해서 제어를 실시하여 전체 네트워크의 성능이 저하되지 않도록 하였으며 구체적인 및 시험은 아래그림과 같은 구성과 같이, SDN Controller와 빅 데이터 인공지능서버, L3 스위치3,대, 그리고 L2 스위치 3대로 망을 구성하여 시험 하였다.· ·

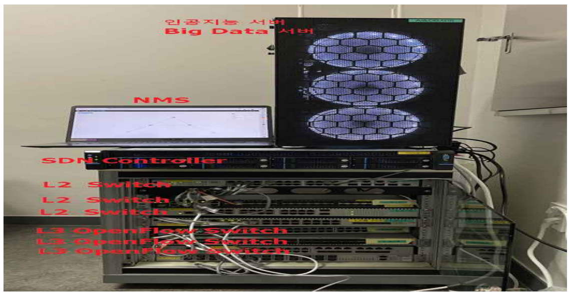

그림5. 실제 구현 장비

네트워크 장비가 제공하는 명확한 장애정보인 Critical 과 Major 알람에 대하여 자동화를 실시하여 절체 또는 Reboot을 실시하였으며, Link 장애에 대한 우회경로 확보를 포함한 장애처리는 좋은 결과를 보였으며, DDoS를 포함한 Traffic으로 이상유무를 판단하는 장애에 대한 처리는 시험 중이다..

ACKNOWLEDGMENT

참 고 문 헌

[1] Edjard Mota, “A Suvey on Fault Management in Software-Defined Netwokrs“ IEEE Communcations Survey & Rutorials, June, 2017

[2] Ali Chehab, “Flow-Based Intrusion Detection System for SDN“ , Proc IEEE Sympsium on Computer and Communications(ISCC) pp 787-793, Jul, 2017