스마트 홈 IoT 외부 침입 차단을 위한 지능 정의 네트워크 시스템 설계

최유준*, 황윤영*, 신용태**
*숭실대학교 컴퓨터학과
**숭실대학교 컴퓨터학부
pathfinder357@soongsil.ac.kr, doublewhy@soongsil.ac.kr, shin@soongsil.ac.kr

A system to block external intrusion Intelligent Definition Network System Design in Smart Home IOT environment

Yu-Jun Choi*, Yun-Young Hwang*, Yong-Tae Shin**
*Dept. of Computer, Soongsil Univ.
**Dept. of Computer Science Engineering, Soongsil Univ.

요 약

최근 사물 인터넷 관련 해킹 우려 신고 건수가 증가하는 추세를 보이고 있다. 하지만 급격하게 늘어나는 IoT 환경에 따라서 관리자가 새로운 침입 탐지 공격패턴을 인식하는 것에 대한 어려움이 있으며, 대량의 공격이나 새로운 공격 패턴이 등장할 경우 이에 맞는 특징을 재선정해야 할 경우도 발생한다. 본 논문에서는 운영 네트워크 상에 특정 이상동작 파악 및 근원지 진단을 위한 목적을 가진 전반적인 네트워크 상태 분석 및 사용자 이슈 식별이 가능한 프레임워크를 설계하였다.

1. 서론

한국 인터넷 진흥원과 과학기술정보통신부의 발표에 따르면 최근 사물 인터넷 관련 해킹 우려 신고 건수가 증가하는 추세를 보이고 있으며, 각 가구당 영상 디바이스를 통한 사생활 유출과 도어락의 원격 개폐기능을 악용한 가정내 무단 침입 등의 문제가 야기되고 있다. 해킹 범죄의 횟수가 급격히 늘고 있으며, 지능화되는 반면 이를 방지할 수 있는 인력은 반비례하고 있는 실정에 맞춰서 이를 해결 수 있는 인공지능 해결책이 필요하다.

이에 본 논문에서는 SDN 중앙집중식 제어와 머신러닝의 학습능력을 결합하여 네트워크를 자동적으로 제어하는 지능정의 네트워크 시스템을 제안한다.

2. 관련연구

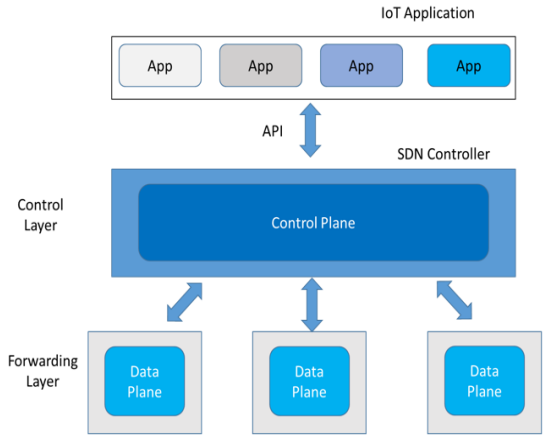
2.1. Software-Defined Networking

최근 클라우드 컴퓨팅 서비스 및 SNS 서비스등이 등장하였다. 이러한 서비스들은 기존의 IP 네트워크를 주로 사용하므로, 이로 인해 트래픽이 폭발적으로 증가하였다. 또한 기존 네트워크의 복잡한 구조와 다양한 트래픽 패턴은 여러 문제를 야기하는데, 이와 같은 복잡한 인프라의 해결을 위해 SDN 이 개발되었다.

일반적으로 SDN 아키텍처는 세 부분으로 구성되는데, 전반적인 리소스 요청 또는 네트워크 관련 정보를 통신하는 어플리케이션, 어플리케이션의 정보를 활용하여 데이터 패킷 라우팅 방식을 결정하는 컨트롤, 컨트롤러에서 데이터를 이동할 위치에 대한 정보를 수신하는 네트워킹 디바이스로 구성된다.

이러한 3 가지 요소는 서로 다른 물리적 위치에 구성이 가능하고 물리적 또는 가상 네트워킹 디바이스는 실제로 네트워크를 통해 데이터를 이동한다. 일부의 경우, 소프트웨어 또는 하드웨어에 내장된 가상 스위치는 물리적 스위치를 대신하여 지능적인 단일 스위치로 기능을 통합한다. 스위치는 데이터 패킷과 가상 머신 대상의 무결성을 확인하고 패킷을 이동한

다. 또한 SDN 의 중요한 특징 중 하나는 데이터 전송을 담당하는 Data Plane 과 Control Layer 을 분산시켜서 관리자가 프로그래밍을 통해 자체적으로 네트워크의 관리가 가능하다는 점이다.

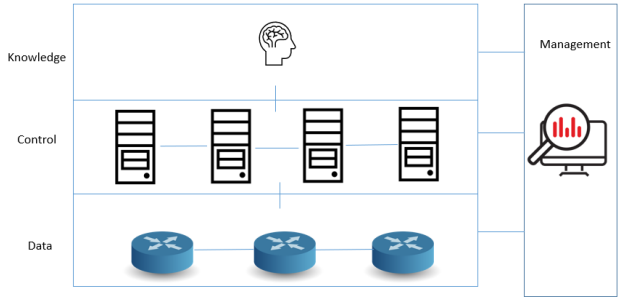


[그림 1] SDN 아키텍처 구조

3. 제안하는 시스템 설계

3.1. 시스템 구성요소

제안하는 시스템은 IoT 환경에서 IoT 디바이스와 연결된 허브와 통신 어플리케이션이 통신할 때 SDN 의 중앙집중식 제어와 머신러닝의 학습 능력을 결합하는 네트워크를 자동적으로 제어하는 방식으로 구성한다. 이를 위해 Data, Control, Management, Knowledge 4 개의 평면적 구조로 구성한다.

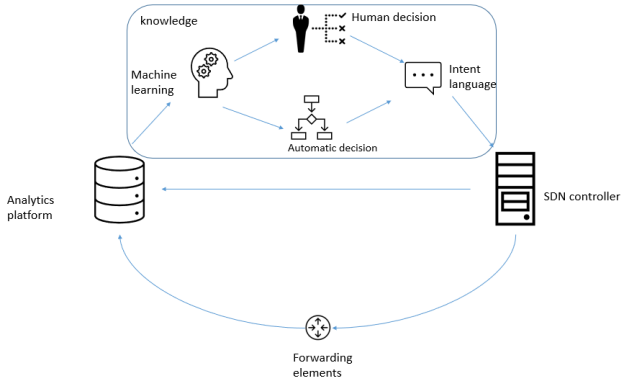


[그림 2] 제안하는 시스템 평면 구조[1]

Data 평면은 데이터의 패킷의 저장, 전송, 처리의 역할을 당담하고, Control 평면은 Data 평면의 운영을 위한 매핑 처리 및 처리 규칙을 생성하고 교환한다. Management 평면은 장기간에 걸쳐서 네트워크의 운영 및 성능 상태를 감시하고, 장비들의 설정을 핸들링하고, 연결구조, 즉 topology 를 정의한다.[2]
Knowledge 평면은 제안하고자 하는 시스템의 핵심 평면으로서 네트워크 행동 양식 모델을 통합하며, SDN 네트워크로의 의사결정을 위한 추론을 담당한다.

3.2 시스템 동작 절차

먼저 Analytics platform 은 네트워크 패킷을 전달하는 동안 데이터의 요소를 실시간으로 모니터링하여 네트워크를 분석할 수 있는 충분한 정보를 수집하는 것을 목표로 하고 네트워크의 구성정보, 작동상태와 같은 데이터를 얻기 위해 NETCONF(RFC 6241), NetFlow(RFC 3954), IPFIX(RFC7011)와 같은 프로토콜에 의존한다. Analytics platform 은 네트워크 분석을 통하여 머신 러닝에 필요한 알고리즘을 지식 평면에 제공하여, 지능평면에서 현재 및 레거시 네트워크 데이터 및 네트워크의 행동을 학습한다.
Knowledge 평면은 Analytics platform 에서 네트워크 구성정보, 작동상태와 같은 데이터를 받아 분석하여 이를 기반으로 Machine Learning 의 지도학습, 자율학습, 강화학습의 3 가지 학습을 수행한후 네트워크 정책을 생성하고, 이를 SDN Controller 에 전송하여 생성된 정책들이 네트워크 장비에게 전달되는 방식으로 작동한다.



[그림 3] 제안하는 시스템 운영루프

4. 결론

본 연구에서는 지능정의 네트워크를 기반으로 IoT 환경에서의 트래픽 분류 및 침입 탐지를 위한 시스템 설계를 제안했다. 본 연구에서 제안하는 시스템을 통해서 기존의 트래픽 패턴과 새로운 패턴 트래픽의 구분이 가능한 학습 네트워킹 기술로 통해 네트워크 보안의 강화를 기대할 수 있다. 향후 연구로는 시스템의 실제적인 구현과 실시간 침입 탐지에 적응력을 가지고 있는지에 대해 연구할 계획이다.

ACKNOWLEDGEMENT

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

참고문헌

[1] A. Mestres et al., "Knowledge-Defined Networking", arXiv 1606.06222v2, Jun, 2016

[2] 한연희."기계학습 기반 네트워크 지능화."전자파기술 28.5(2017):17-22.