한국컴퓨터정보학회 동계학술대회 논문집 제28권 제1호 (2020. 1)

SDN 네트워크 연구 및 고도화 제안

박재경[O], 이형수[*]
[O]한국폴리텍대학 정보보안과,
[*]한국폴리텍대학 정보보안과
e-mail:{jakypark, hslee01}@kopo.ac.kr[O*]

A Study and Advancement Proposal for Software Defined Network

Jae-Kyung Park[O], Hyung-Su Lee[*]
[O]Dept. of Information Security, Korea Polytechnics,
[*]Dept. of Information Security, Korea Polytechnics

● 요 약 ●

본 논문에서는 기존의 SDN(Software Defined Network)의 특징 및 활용 등에 대해 살펴보고 이를 활용한 네트워크의 고도화 및 보안 측면에서의 장단점 연구를 통해 향후 SDN이 보다 고도화 되어야 하는 방향을 제시한다. SDN은 소프트웨어 앱을 사용하여 네트워크를 지능화 하고 중앙에서 제어하거나 프로그래밍 할 수 있는 네트워크 아키텍처 접근법이다. 사업자는 기본 네트워크 기술에 상관없이 전체 네트워크를 일관적으로 전체적으로 관리할 수 있다. 물리적인 네트워크를 소프트웨어 기술을 이용하여 제어하는 네트워크 기술이다. SDN은 네트워크의 제어 플레인을 네트워크 트래픽을 전달하는 데이터 플레인과 분리한다는 개념이다. 이런 분리의 목적은 중앙에서 관리하고 프로그래밍이 가능한 네트워크를 만드는 것이다. 일부 SDN 구현 솔루션은 범용 네트워크 하드웨어를 통제하는 소프트웨어 기반 관리 플랫폼을 사용한다. 또 다른 접근법은 통합된 소프트웨어와 하드웨어를 사용하기도 한다. 하지만 이러한 SDN에도 많은 취약점이 존재하며 이를 보완할 수 있어야 하며 본 논문에서 이러한 방향을 제한하도록 한다.

키워드: SDN)Software Defined Network), NFV(Network Function Virtualization), OpenFlow

I. Introduction

소프트웨어 앱을 사용하여 네트워크를 지능화 하고 중앙에서 제어하거나 프로그래밍 할 수 있는 네트워크 아키텍처 접근법이다. 사업자는 기본 네트워크 기술에 상관없이 전체 네트워크를 일관적으로 전체적으로 관리할 수 있다. 물리적인 네트워크를 소프트웨어 기술을 이용하여 제어하는 네트워크 기술이다.

SDN은 네트워크의 제어 플레인을 네트워크 트래픽을 전달하는 데이터 플레인과 분리한다는 개념이다. 이런 분리의 목적은 중앙에서 관리하고 프로그래밍이 가능한 네트워크를 만드는 것이다. 일부 SDN 구현 솔루션은 범용 네트워크 하드웨어를 통제하는 소프트웨어 기반 관리 플랫폼을 사용한다. 또 다른 접근법은 통합된 소프트웨어와 하드웨어를 사용하기도 한다.

SDN은 주로 대기업 데이터센터에서 사용하는데, 전통적인 네트워킹 아키텍처와 비교해 비즈니스의 요구에 좀 더 쉽게 대응할 수 있는 네트워크를 필요로 하는 환경이다. SDN을 주목하는 이유는 네트워크 관리 측면에서의 효율성과 향상과 새로운 비즈니스 생태계 구축을 통해 현재 침체되어 있는 네트워크 시장을 활성화 시킬 수 있을 것이라는 기대감 때문이다.

하지만 SDN는 컨트롤러를 통해 네트워크의 흐름을 제어할 수 있고 이를 통해 네트워크를 단순화 할 수 있다. 하지만 컨트롤러로 인해 발생 가능한 보안 문제점도 있다.

첫 번째로 컨트롤러가 악성코드에 감염됐을 때로 컨트롤러가 악성코드에 감염된다면 공격자는 프로그램을 재설치 하여 네트워크 상에 있는 데이터 스니핑 또는 드랍핑 할 수 있다.

두 번째로 관리자가 악의적인 의도를 가졌을 때이다. 컨트롤러의 룰을 작성하는 관리자나 아키텍처가 악의적 의도로 컨트롤러의 룰을 변경하면 네트워크가 정지될 수 있고 정보유출까지 가능하다.

따라서 본 논문에서는 이러한 SDN의 문제점을 파악하고 이를 고도화할 수 있는 방안을 제안하도록 한다.

II. Preliminaries

1. Related works

1.1 SDN의 취약점

SDN는 컨트롤러를 통해 네트워크의 흐름을 제어할 수 있고 이를 통해 네트워크를 단순화 할 수 있다. 하지만 컨트롤러로 인해 발생 가능한 보안 문제점도 있다.

첫 번째로 컨트롤러가 악성코드에 감염됐을 때로 컨트롤러가 악성코드에 감염된다면 공격자는 프로그램을 재설치 하여 네트워크 상에 있는 데이터 스니핑 또는 드랍핑 할 수 있다.

두 번째로 관리자가 악의적인 의도를 가졌을 때이다. 컨트롤러의 룰을 작성하는 관리자나 아키텍처가 악의적 의도로 컨트롤러의 룰을 변경하면 네트워크가 정지될 수 있고 정보유출까지 가능하다.

마지막으로 컨트롤플레인과 데이터플레인 사이의 디도스 공격이다. 이 공격은 컨트롤러가 정상적으로 데이터 계층에 지시를 내리지 못하게 되어 정상 작동을 방해 받는다.

III. The Proposed Scheme

현재 네트워크와 차세대 네트워크를 연동한 제안 시스템을 통해 '대용량', '초고속', '고신뢰'를 제공 가능한 네트워크 및 보안 제공 가능할 수 있도록 다음의 그림과 같은 시스템을 제안하도록 한다.

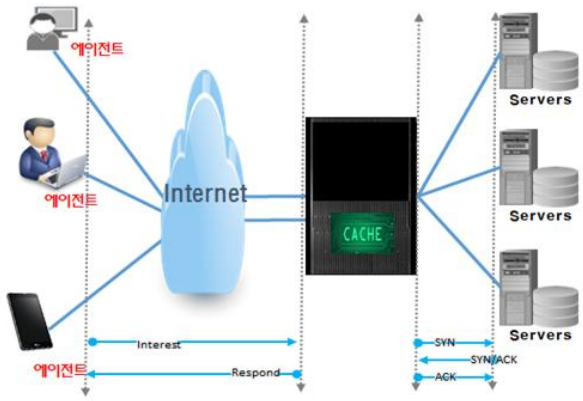

Fig. 1. Proposal System with Cache

IV. Conclusions

앞으로의 네트워크 서비스는 기존의 텍스트 및 이미지 중심에서 벗어나 비디오로 빠르게 변화하고 있고 향후 몇 년 안에 이러한 비디오 중심의 서비스는 전체 인터넷의 80~90% 이상을 차지할 것으로 전망하고 있다. 이러한 변화의 중심에 SDN 네트워크를 보다 고도화하기 위한 방안의 연구가 추가적으로 필요하다고 판단한다. 본 논문에서는 이러한 점을 부각하고자 기존 SDN에 캐쉬를 활용한 네트워크에 대해 제안하고 이를 시뮬레이션 하여 활용할 수 있는 방안을 제안하였다.

REFERENCES

[1] Jae-Kyung Park, Strengthening Authentication Through Content Centric Networking, KSCI, Mar 24 2018.

[2] Jae-Kyung Park, A Network Translate System Using Next Generation Content Centric Networking Technology, KSCI, Mar 24 2018.

[3] Jae-Kyung Park, A Design of client BBS systems for Secure HVA, KSCI, Sep 21 2018.

[4] IEEE "1903.1-2017 - IEEE Standard for Content Delivery Protocols of Next Generation Service Overlay Network", IEEE, 25 May 2018. DOI: https://dx.doi.org/10.1109/IEEESTD.2018.8365911

[4] Woo-Seok Yang, Jung-Ho Kim, Jae-oh Lee, "A Management for IMS Network Using SDN and SNMP", Journal of the Korea Academia-Industrial cooperation Society, 18(4) pp. 694-699. 2017. DOI: https://dx.doi.org/10.5762/KAIS.2017.18.4.694