SDN환경에서 보안성 향상을 위한 IP주소 은닉화 기법

홍석찬, 진태용, 송관호, 신용태
숭실대학교
{schong, tyjin}@icn.ssu.ac.kr, {khsong, shin}@ssu.ac.kr

IP Address hiding method for Security purposes in SDN environments

Seok-Chan Hong, Tae-Yong Jin, Kwan-Ho Song, Yong-Tae Shin
Soongsil University

요 약

최근 무선 인터넷의 발달 및 스마트 디바이스의 등장 등의 이유로 다양한 분야의 네트워크 기반 서비스가 등장하고 있다. 폭발적으로 증가하는 네트워크 서비스를 신뢰적이며 효율적으로 운영하기 위한 기술로 미래 네트워크 기술의 하나인 SDN이 주목받고 있다. 하지만 SDN은 기존 네트워크의 보안 취약성인 IP주소를 타깃으로 하는 공격에 대한 취약점을 보완하지 못하고 있다. 이에 본 논문은 SDN망에서 기존 Control Layer외에 Security Layer를 추가함으로서 네트워크 위협사항에 능동적으로 대처가 가능하고 해당 구조의 기반 위에 검색가능 암호화 기법을 사용하여 IP주소를 은닉화하는 기법을 제안하고자 한다.

1. 서론

최근 모바일 인터넷, IOT(Internet of Things), VOD(Video on Demand), 클라우드 등 다양한 분야의 네트워크 기반 서비스를 신뢰적이고 안정적이며 효율적으로 운영할 수 있는 미래 네트워크 기술에 대한 요구가 증가하고 있다. 기존 네트워크 기술로는 점점 증가하는 네트워크 인프라 이용 서비스의 다양성과 이에 따라 폭발적으로 증가하고 있는 데이터 수요를 감당하기에는 신뢰성 및 효율성 측면에서 그 한계를 드러내고 있다.

이에 기존 네트워크 장비에 종속적이던 소프트웨어 기능을 Controller로 분리시킴으로서 즉, 네트워크의 제어 기능을 네트워크 디바이스들로부터 추상화시킴으로서 네트워크 서비스에 대한 효율성을 향상시킨 SDN(Software Defined Network)기술이 주목받고 있다.

하지만 SDN은 기존 네트워크의 보안 취약성 중 하나인 IP주소를 타깃으로 하는 IP 스니핑, IP 스푸핑, DOS 공격 등에 대한 취약점을 기술적으로 보완하지 못하고 있다. NAT, VPN등은 타깃의 보호를 위한 IP주소 은닉화 기능을 제공하고 있지만 해당 기술들은 NAT, VPN등으로 보호되는 내부 즉 내부망으로 부터의 공격에는 무력하며 NAT, VPN장비 등이 공격의 타깃이 될 수 있다는 한계점을 가지고 있다.

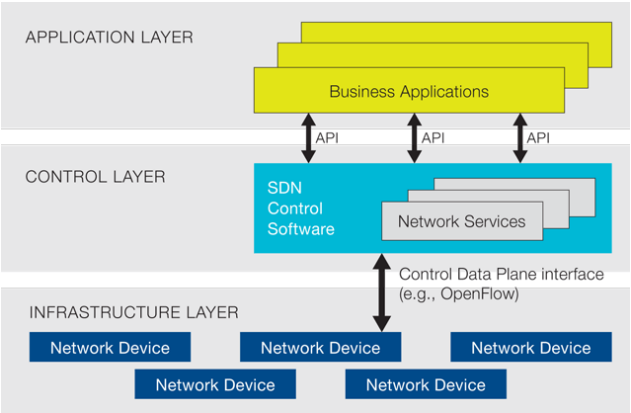
이에 본 논문은 기존 SDN의 SDN Controller 및 네트워크 디바이스들에 종속적이던 보안기능을 분리·응집함으로서 네트워크 위협사항에 능동적으로 대처가 가능하게 하는 기법을 제안한다. 또한 해당 구조의 기반위에 검색가능 암호화 기법을 사용하여 IP주소를 은닉화 함으로서 SDN의 보안 기능을 향상시키는 기법을 제안하고자 한다.

2. 관련연구

2.1 SDN

SDN은 전달 기능과 제어 기능이 밀결합 되어있던 기존의 전송 장치에서 제어 기능을 분리하여 중앙집중화 시키고, OpenFlow와 같은 개방형 API를 통해 네트워크 트래픽 전달 동작을 소프트웨어 기반 컨트롤러에서 제어·관리하는 기술이라 정의할 수 있다.[1]

SDN의 논리적 구조는 (그림 1)과 같은 3계층의 Layer로 구성되어 있다.



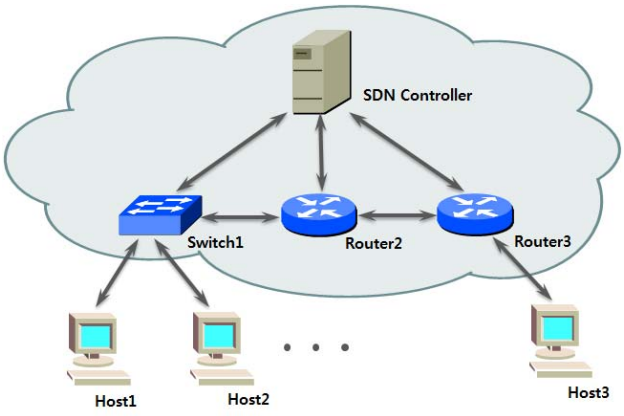
(그림 1) SDN 논리적 구조

Infrastructure Layer는 데이터를 전송 및 포워딩 하는

"이 논문은 2013년도 정부(미래창조과학부)의재원으로 한국연구재단-차세대정보컴퓨팅기술개발사업의 지원을 받아 수행된 연구임(No.2012-0029926)"

역할을 담당하며 Control Layer는 Infrastructure Layer의 제어·관리를 담당한다. Application Layer는 실제 SDN 인프라를 사용하는 네트워크 서비스 이용 애플리케이션들을 의미한다.

각각의 Layer는 상위 또는 하위 계층과의 인터페이스를 제공한다. 네트워크 디바이스에 대한 Control Layer의 제어는 개방형 사우스바운드 API(Southbound API)에 의해 이루어지고 애플리케이션들에 필요한 다양한 네트워크 서비스의 개발을 지원하기 위해 Application Layer와 Control Layer간에 노스바운드 API(Northbound API)를 제공한다.



(그림 2) SDN 물리적 구조

SDN의 물리적 구조는 (그림 2)와 같다. Host1에서 Host3으로 패킷을 전송할 때 Switch1의 Flow Table내에 전송 패킷에 대한 Flow Rule이 존재하지 않는다면 Switch1은 SDN Controller로 해당 Flow Rule을 요청하고 SDN Controller는 해당 Flow Rule을 만들어 Switch1으로 응답한다. 전송 패킷이 Router2와 Router3을 지날 때 Router2와 Router3은 해당 과정을 반복하며 패킷을 Host3로 전달한다.

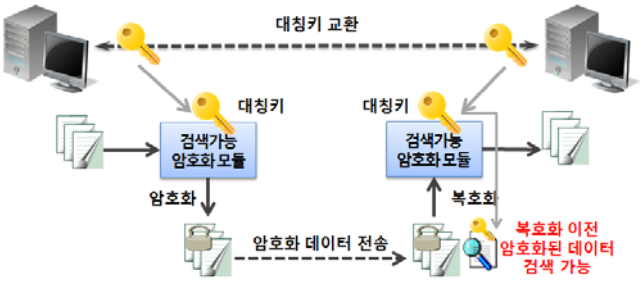
2.2 대칭키 기반 검색가능 암호화 시스템

검색가능 암호화 시스템은 암호화된 암호문을 복호화하지 않은 상태에서도 원하는 자료를 검색 할 수 있도록 하는 암호화 기법이다.[2]

이는 데이터베이스의 데이터들을 암호화하여 저장하였을 때 암호화 된 자료의 자료검색 시 복호화 하는 과정에서 검색 속도를 현저히 저하시키는 문제를 해결하기 위한 방안으로 주목받고 있는 기술이다.

검색가능 암호화는 크게 대칭키 기반의 암호화 기법과 공개키 기반 암호화 기법으로 나누어지며 키 생성 과정(key generation), 암호화 과정(build index), 트랩도어 생성 과정(trapdoor generation), 검색을 위한 테스트 과정(test for search)의 4가지 단계로 이루어진다.[2]

(그림 3)은 대칭키 기반의 검색가능 암호화 시스템을 도식화한 것이다. (그림 3)에서 수신측은 대칭키를 이용해 검색 키워드의 트랩도어를 생성하며 암호문은 복호화 하지 않은 상태에서도 생성된 트랩도어와 XOR등의 비교적 단순한 연산을 이용하여 키워드의 검색이 가능하다.



(그림 3) 대칭키 기반 검색가능 암호화

이는 키워드 검색 시 평문이 드러나지 않는다는 점과 복호화로 인한 속도 손실을 최소화 할 수 있다는 점에서 그 의의가 있다.

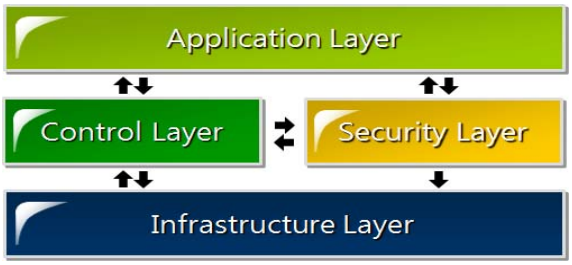
본 논문에서는 IP주소 은닉화 시 대칭키 기반 검색가능 암호화 기법 중 가장 단순한 구조를 가진 Single Keyword Search를 사용한다.

3. 제안모델

본 논문에서는 SDN의 보안성 향상을 위해 SDN의 보안기능을 추상화 하여 Control Layer와는 별도로 Security Layer를 추가하고 또한 추가된 Security Layer와 검색 가능 암호화 기법을 이용하여 SDN을 이용하는 네트워크 서비스에 IP주소가 은닉화된 보안채널을 제공하는 기법을 제안하고자 한다.

3.1 SDN Security Layer

제안하는 SDN모델의 논리적 구조는 (그림 4)와 같다.

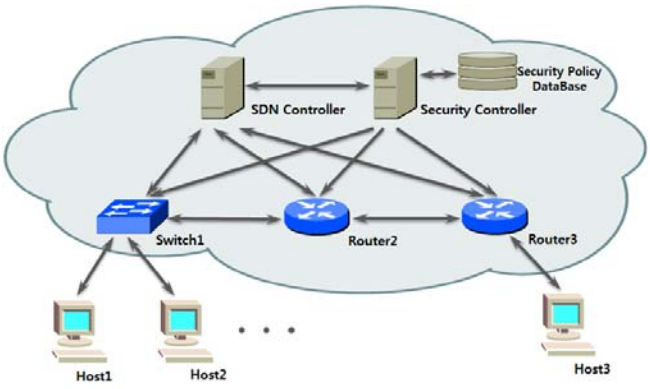


(그림 4) 제안하는 SDN모델의 논리적 구조

(그림 4)에서 Application Layer의 서비스 및 애플리케이션들은 Security Layer에서 제공되는 API를 통해 제안하는 SDN모델의 보안기능을 제공받는다.

제안 SDN모델의 Security Layer는 Control Layer를 통해 Infrastructure Layer를 구성하는 네트워크 디바이스들의 이상 트래픽 및 DoS공격 등을 감지하고 대처하는 기능을 하며 Infrastructure Layer에서 Security Layer로의 직접적인 접근은 불가능 하다. 또한 제안 SDN모델은 보안기능이 Infrastructure Layer 및 Control Layer로부터 분리·응집화된 구조로 인해 보안기능의 추가 및 확장이 용이하다.

제안하는 SDN모델의 물리적 구조는 (그림 5)와 같다.

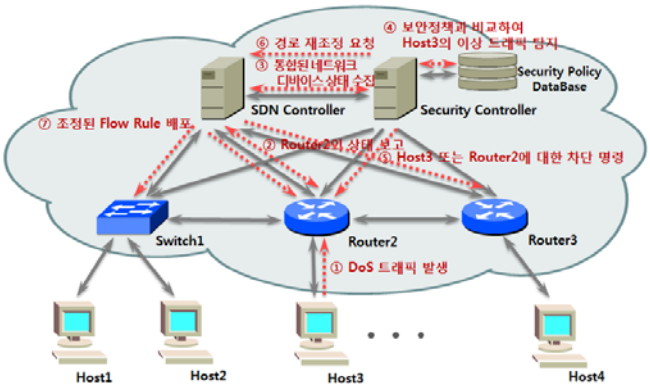


(그림 5) 제안하는 SDN모델의 물리적 구조

(그림 5)는 기존 SDN의 구조와 달리 SDN Controller와 별도의 Security Controller가 존재한다. SDN Controller는 포워딩 제어를 담당하며 Security Controller는 SDN의 전반적인 보안 기능을 제어한다. Security Controller는 SDN Controller를 통해 네트워크 디바이스들을 감시하고 Security Policy DataBase(이하 SPD)의 보안정책을 이행한다.

SPD는 SDN의 보안정책 및 보안채널 이용 애플리케이션 리스트등 보안정책 이행에 필요한 정보들을 저장한다.

제안하는 SDN구조에서 DoS등 이상 트래픽 발생 시 대응 전략은 (그림 6)과 같다.



(그림 6) DoS 대응 절차

① Host3은 DoS 트래픽 등 이상 트래픽을 발생시킨다.

② SDN Controller는 네트워크 디바이스들의 정기적이 상태 보고를 통해 네트워크 디바이스들의 상태를 수집 및 통합한다.

③ Security Controller는 SDN Controller의 통합된 네트워크 디바이스 상태정보를 정기적으로 수집한다.

④ 수집된 통합 상태정보를 SPD의 보안정책과 비교하여 Host3의 이상트래픽 여부를 판단한다.

⑤ Security Controller는 Host3 또는 Router2에 대한 차단 명령을 내린다.

⑥ Security Controller는 SDN Controller에게 Router2또는 Host3를 제외한 Switch및 Router의 포워딩 경로 재조정을 요청한다.

⑦ 조정된 Flow Rule들을 배포한다.

만약 일반적인 DoS공격이 아닌 SDN Controller에 대한 DoS공격이 발생한다면 Security Controller는 SDN Controller의 상태체크를 통해 부하를 감지하고 DoS의 원인이 되는 Host 또는 Router에 대한 차단 명령을 내린다.

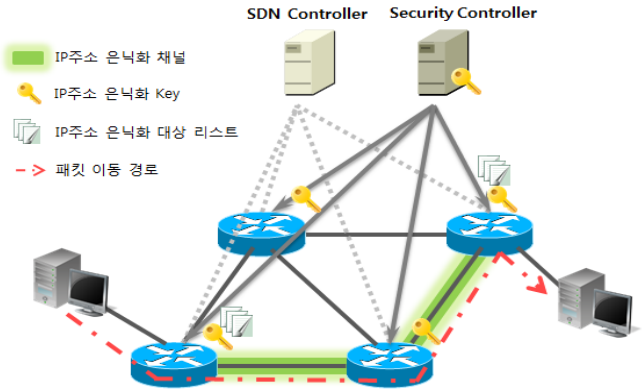
Security Controller와 네트워크 디바이스간의 단방향 통신을 제공하는 이유는 Security Controller에 대한 접적인 DoS공격을 방지하기 위함이다.

3.2 IP주소 은닉화

먼저 제안하는 IP주소 은닉화 기법의 가정사항은 다음과 같다. 첫째 제안하는 기법에서 Edge Router와 Host 사이에 구성된 망은 안전하다고 가정한다. 둘째 제안하는 기법은 기존 네트워크 및 타 망과의 연계를 고려하지 않는다.

제안하는 IP주소 은닉화 기법은 다음과 같다. 먼저 SDN의 모든 코어 네트워크 디바이스에 대칭키 기반 검색 가능 암호화 기법인 Single Keyword Search(이하 SKS) 모듈이 설치되어야 한다. 망 내부에 신규 Router를 설치할 경우 신규 Router는 Security Controller로 부터 SKS모듈을 다운받은 후 설치한다.

또한 망 운영 시 Security Controller는 SPD의 IP은닉화 대상 애플리케이션 리스트에 변경사항이 발생할 경우 이를 감지하여 SDN의 Edge Switch 및 Edge Router로 변경된 정보를 전달하여야 한다.



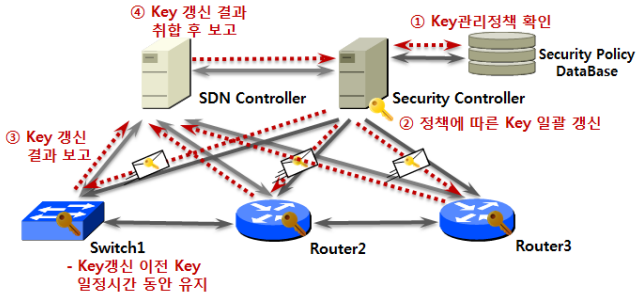
(그림 7) 제안하는 IP주소 은닉화 구조

제안하는 SDN모델 에서 IP주소 은닉화 패킷 전송 시 출발지에서 가장 가까운 Edge Router는 해당 패킷이 IP주소 은닉화 대상 애플리케이션 패킷인 것을 확인한 후 IP 은닉화 대상 패킷이라면 SKS모듈을 이용하여 출발지 IP주소 및 목적지 IP주소를 암호화 한다.

IP주소가 암호화된 해당 패킷이 코어의 Router를 지날 때 목적지 IP주소를 복호화 하지 않더라도 Router내부 Flow Table의 Flow Rule과 비교가 가능하기 때문에 포워딩 시의 시간적 손실을 최소화 할 수 있다. 해당 패킷이 목적지의 Edge Router를 지날 때 목적지의 Edge Router는 목적지 IP주소 및 출발지 IP주소를 복호화 한다.

제안하는 IP주소 은닉화 기법의 IP주소 암호화 Key는 Key의 유출 및 유추에 대응하기 위해 시간축을 두어 망

에 무리가 가지 않는 선에서 주기적으로 갱신하다. 제안하는 Key관리 절차는 다음과 같다.



(그림 8) 제안하는 Key관리 절차

Key갱신 시 Security Controller는 Key갱신 주기의 최소시간과 최대시간을 두어 최소시간과 최대시간 사이의 시간을 Random하게 선택하여 Key를 일괄 갱신한다.

코어 네트워크 디바이스들은 망 내부에 남아있는 Key 갱신 이전에 생성된 패킷들을 처리하기 위해 갱신 이전 Key를 Key갱신 이후에도 일정시간 동안 유지한다.

패킷이 Key의 변경 전 패킷인지 변경 후의 패킷인지 구분하기 위해 패킷 내부에 Time Stamp값을 이용한다.

4. 결 론

본 논문에서는 기존 SDN의 구조에 Security Layer를 추가하여 보안기능을 Infrastructure Layer와 Control Layer로 부터 분리·집중한 후 해당 구조 기반 위에 검색 가능 암호화 기법을 사용하여 보안채널을 제공하는 기법을 제안하였다.

하지만 제안하는 기법은 SDN 내부에 한정하여 보안기능을 제공하며 Edge Router와 Host 사이에는 보안채널을 제공하지 않는다는 점에서 그 한계점을 가지고 있다.

따라서 Edge Router와 Host 사이에 IP주소 은닉화 채널을 제공하는 방안과 제안기법의 효용성 및 비용에 관한 성능평가는 향후 연구과제이다.

참고문헌

[1] 강세훈, 김영화, 양선희, “SDN 핵심 기술 및 진화 전망 분석” 한국통신학회지 (정보와통신) 제30권 제3호, pp.3-8, 2013.2

[2] 김선영, 서재우, 이필중, “검색 가능 암호 기술의 연구 동향” 정보보호학회지 제19권 제2호, pp.63-73, 2009.4

[3] 김선영 외, “SDN 표준 참조구조 기반의 개방형 인터페이스, 추상화 기술 및 컨트롤러 언어 분석” 한국통신학회지 (정보와통신) 제30권 제2호, pp.36-42, 2013.1

[4] Phillip Porras “A Security Enforcement Kernel for OpenFlow Networks” Association for Computing Machinery, Aug 2012

[5] 강동훈 외, “오픈플로우 네트워크를 위한 QoS 서비스 모듈 개발” 정보과학회논문(정보통신) 제40권 제1호, pp.1-11, 2013.2

[6] 임재근 외, “혼합트래픽 환경에서 Open Flow 네트워크 성능 평가” 한국콘텐츠학회논문지 제12권 제12호, pp.46-53, 2012.12