SDN 환경에서 DDoS 공격에 대한 방어 기법

지승훈*, 박지수**, 손진곤*+
*한국방송통신대학교 대학원 정보과학과
**전주대학교 컴퓨터공학과
mayets@knou.ac.kr, jisupark@jj.ac.kr, jgshon@knou.ac.kr

Defense Techniques against DDoS Attack in SDN Environment

Seung Hun Jee*, Ji Su Park**, Jin Gon Shon*
*Dept. of Computer Science, Korean National Open University
**Dept. of Computer Science and Engineering, Jeonju University

요 약

소프트웨어 정의 네트워크(Software-Defined Networking; SDN) 기술은 기존 네트워크 기술의 폐쇄성과 복잡성의 한계를 극복하고, 중앙 집중적 관리 및 프로그래밍 기반의 네트워크 서비스를 제공할 수 있는 장점이 있다. 그러나 SDN 환경에서도 다른 네트워크 환경처럼 악의적인 DDoS 공격으로 인해 전체 네트워크 서비스가 마비될 수도 있는 문제가 있다. 이러한 문제를 해결하기 위한 기존의 연구들은 공격이 인입되는 스위치 포트를 차단하거나, 공격자의 출발지 주소 자체를 차단하는 기법 등이 있으나 공격 트래픽과 함께 정상 트래픽까지 차단하는 문제가 있다. 본 논문에서는 SDN 환경에서 DDoS 공격 발생 시 악의적인 트래픽만 방어하고, 정상적인 트래픽은 최대한 허용하는 서비스 Flow 기반의 방어 기법을 제안한다. 제안 기법은 SDN 환경에서 Flow 분석을 통해 DDoS 공격을 탐지한 후 이를 접근제어 리스트 방식을 통해 공격 트래픽만을 차단하는 것이 가능하다. 실험 결과를 통해 공격자의 악의적인 트래픽은 차단하고, 정상적인 트래픽은 허용하는 것이 확인되었다.

1. 서론

최근 네트워크 기술은 몇 가지 변화된 특징이 있다. 네트워크 장비는 하드웨어와 소프트웨어가 통합된 블랙박스 형태에서 하드웨어와 소프트웨어가 분리된 화이트박스 형태로 변화하고 있다. 네트워크 운영체제는 제조사 별로 상이하게 관리가 필요한 폐쇄적인 형태에서 범용 프로그래밍 언어로 관리가 가능한 개방적인 형태로 발전하고 있다.

이런 변화를 주도하고 있는 기술인 소프트웨어 정의 네트워크(Software-Defined Networking; SDN)는 네트워크 가상화의 핵심 기술로 활용되고 있다. 하지만 SDN의 구조는 분산 서비스 거부 공격(Distributed Denial of Service; DDoS) 발생 시 치명적인 서비스 단절 현상을 초래할 수 있는 단점이 있어 이를 방어하기 위한 기법이 필요하다.

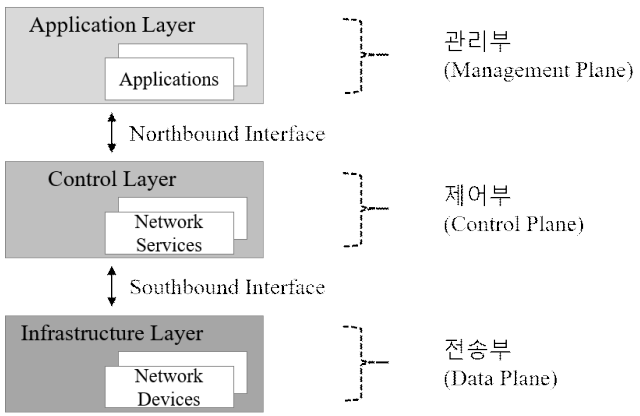
본 논문에서는 SDN 환경에서 DDoS 공격에 대한 방어 기법을 연구한다. 특히 TCP SYN Flooding 공격 유입 시 제안 기법은 해당 공격 Flow만 탐지 후 차단하고 나머지 정상 Flow는 모두 허용한다.

+ 교신저자

2. 관련 연구

2.1. SDN과 DDoS의 구조

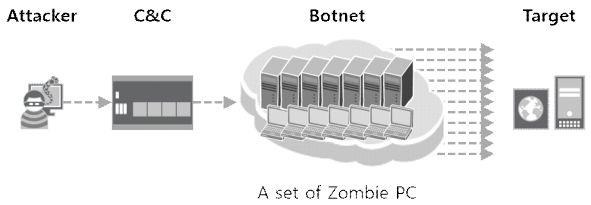
SDN이란 기존 네트워크 장비에서 하드웨어와 소프트웨어의 기능을 분리한 새로운 네트워크 기술을 의미한다[1]. SDN은 (그림 1)과 같이 관리 및 모니터링을 담당하는 관리부, 경로 설정 및 통제를 담당하는 제어부, 전송을 담당하는 전송부로 구성된다.



(그림 1) SDN의 구조

SDN을 통해 기존 네트워크 한계를 극복하기 위한 다양한 연구 성과에 비해 SDN 환경에서 보안을 강화하기 위한 연구는 상대적으로 부족하다. 이에 SDN 환경에서 악의적인 공격 발생 시 네트워크를 보호하기 위한 기법에 대한 연구가 필요하다[2].

한편 DDoS 공격이란 인터넷 상에 있는 악성 코드에 감염된 다수의 단말을 악용하여 공격 시스템에 대량의 트래픽을 전송하여 시스템의 정상적인 서비스를 마비시키는 공격을 말한다. DDoS 공격의 구조는 (그림 2)와 같이 공격자가 C&C 서버를 통해 다수의 좀비 PC로 이루어진 Botnet으로부터 대량의 트래픽 전송을 수행하게 하는 구조로 이루어진다[3].



(그림 2) DDoS 공격의 구조

2.2. 관련 논문 연구

SDN 환경에서 DDoS 공격에 대한 방어 기법에 대한 기존 연구는 탐지 기법에 대한 연구와 차단 기법에 대한 연구로 분류할 수 있다. 첫 번째로, SDN 환경에서 DDoS 공격 탐지 기법에 대한 연구를 3가지 기준으로 분류하였다.

정적 임계치 기반의 탐지는 설정된 임계값을 초과 시 초과 시 이를 탐지 시점을 판단하는 기법이다[4]-[5]. 이 경우 임계값 이하에서는 DDoS 공격 트래픽에 대한 탐지 자체를 할 수 없는 문제가 있다.

정책 기반의 탐지는 정형화된 DDoS 공격에 대해서는 효과적으로 탐지 가능하다[6]. 다만 비정형화된 새로운 DDoS 공격에 대해서는 탐지가 어렵다.

동적 학습 기반의 탐지는 인공 지능 기술을 활용하여 일정 기간 평시 사용량에 대한 학습 결과를 기반으로 이를 초과하는 트래픽 발생 시 탐지를 수행하는 기법으로 현재까지 연구에서 가장 지능적이고 효과적인 방안이다[7]-[8]. 다만 이 기법의 경우에도 평시와 다른 이벤트로 인한 대용량 트래픽과, DDoS 공격으로 인한 대용량 트래픽을 구별할 수 있는 기술적 방안에 대한 연구가 필요하다.

공격 탐지 기법을 정리하면 <표 1>과 같다.

<표 1> DDoS 공격 탐지 관련 연구

탐지 기준	탐지 대상	관련 논문
정적 임계치	네트워크 이용률	M. Nugraha[4]
	서버 큐 이용률	방기현[5]
정책	정의된 패턴 위반	조승신[6]
동적 학습	K-Means 기반	신동혁[7]
	SVM 기반	오대명[8]

두 번째로, SDN 환경에서 DDoS 공격 차단 기법에 대한 연구를 3가지 기준으로 분류하였다.

Port 기반의 차단은 공격 트래픽이 유입되는 스위치 Port 자체를 차단하는 기법으로[9], 해당 Port로부터 유입되는 정상 Flow를 포함한 모든 Flow를 차단하는 문제가 있다. Flow 기반의 차단은 공격자 주소 IP가 포함된 Flow 전체를 차단하는 기법으로[10], 해당 IP로부터 유입되는 정상 Flow까지 차단하는 문제가 있다. Host 기반의 차단은 공격자 단말 자체를 네트워크에서 격리 후 치료하는 기법으로[11], 공격 시도를 자체를 차단할 수 있으나 공격자는 대부분 외부 네트워크에 존재하고 있어 사실상 격리 및 치료가 어렵다. 공격 방어 기법을 정리하면 <표 2>과 같다.

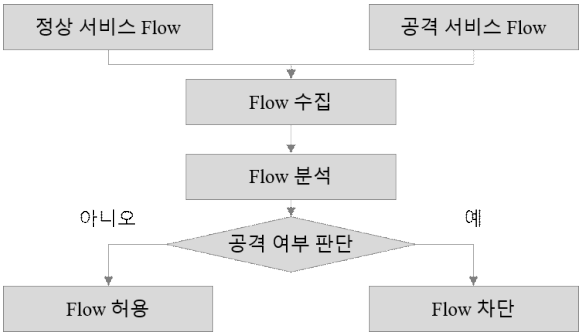
<표 2> DDoS 공격 방어 관련 연구

방어 기준	방어 대상	관련 논문
Port	공격 유입 Port 차단	박종환[9]
IP Flow	공격자 IP Flow 차단	김정훈[10]
Host	좀비 PC 격리/치료	배효빈[11]

기존 연구의 한계점을 극복하기 위해 전체 트래픽 Flow 중에서 비정상적인 Flow만 차단하고 나머지 정상적인 Flow는 허용하여, 오탐율을 최소화하고 공격 트래픽에 대해서만 최소한으로 방어하는 기법에 대한 연구가 필요하다.

3. 서비스 Flow 기반 DDoS 방어 기법

본 연구에서 제안된 서비스 Flow 기반 DDoS 방어 기법은 서비스 Flow 기반 DDoS 탐지 기법과 서비스 Flow 기반 DDoS 차단 기법으로 구성되어 있다. 첫 번째, 서비스 Flow 기반 DDoS 탐지 기법은 (그림 3)과 같이 서비스 SDN 스위치를 통해 수집된 Flow를 기반으로 SDN 애플리케이션에서 각각의 서비스 Flow 분석하여 DDoS 공격 여부를 탐지한다.



(그림 3) 제안 기법의 동작방식

제안 탐지 기법은 DDoS 공격 중 하나인 TCP SYN Flooding 공격 유입 시 <표 3>와 같이 의사 코드 형태로 표현된 알고리즘으로 동작한다.

<표 3> TCP SYN Flooding 공격 탐지 기법

```
D ← empty dictionary
max_syn ← 60 // can be modified
timer ← 60 sec // can be modified
while True :
  get TCP packet
  if protocol is "TCP" :
    get tcp_flag
    if tcp_flag is syn :
      if source_ip ∈ key(D) :
        D[source_ip] [0] ++
      else :
        start_time ← get current time
        D[source_ip] ← [0, start_time]
  if D[source_ip] [0] > max_syn :
    time_difference = current time -
    D[source_ip] [1]
    if time_difference < timer :
      print "TCP SYN Flooding attack"
```

두 번째, 제안된 서비스 Flow 기반 DDoS 차단 기법은 탐지된 공격 서비스 Flow는 SDN 컨트롤러를 통해 SDN 스위치에 접근 제어 리스트(Access Control List)를 추가하여 해당 Flow만 차단한다.

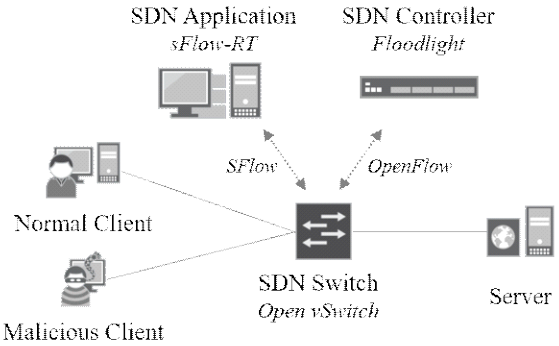
제안 기법은 Port 기반 또는 IP Flow 기반의 기존 연구와는 달리 공격자의 모든 Flow를 차단하는 것이 아니라, DDoS 공격 Flow만 차단한다. 공격자의 단말이 자신도 모르게 악성 코드에 감염되어 악의적인 공격에 참여할 경우 공격자 주소 자체가 네트워크 환경에서 차단되어, 향후 단말에 대한 방역이 끝난 이후에도 네트워크 통신이 불가능한 문제를 해결할 수 있다.

4. 실험 및 평가

제안 기법을 검증하기 위해 <표 4>와 같은 실험 환경과 (그림 4)와 같은 실험 구성을 기반으로 제안 기법에 대한 실험을 수행하였다.

<표 4> 실험 환경

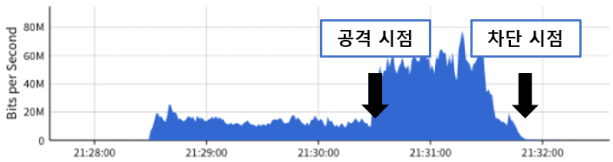
구분	실험 도구	버전
에뮬레이터	Mininet/Miniedit	2.3.0d6/2.2.0.1
컨트롤러	Floodlight	1.2
스위치	OvS	2.9.5
Flow 수집	sFlow-RT	3.0



(그림 4) 실험 구성

실험 환경에서 정상 사용자는 정상적인 ICMP 및 TCP 트래픽 전송하고, 공격자는 정상적인 ICMP 트래픽과 TCP SYN Flooding 공격 트래픽을 전송한다. 기존의 차단 기법과 제안된 차단 기법에서 각각 허용되는 트래픽과 차단되는 트래픽 검증을 위해 실험을 수행하였다.

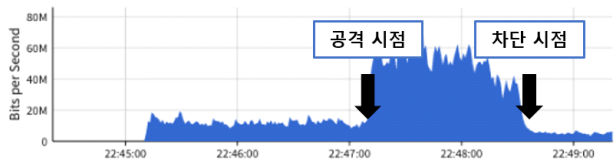
Port 기반 차단 기법을 적용한 결과 (그림 5)와 같이 공격 탐지 후 차단 시점에 다른 모든 정상 트래픽도 차단되어 차단 시점 이후 트래픽 유입이 전혀 없는 것을 알 수 있다.



(그림 5) Port 기반 차단 기법 적용 결과

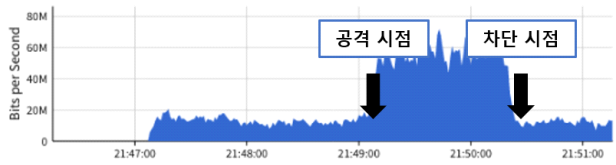
IP Flow 기반 차단 기법을 적용한 결과 (그림 6)과 같이 공격 탐지 후 차단 시점에 공격자의 정상

트래픽까지 차단되어 공격 시점 전과 차단 시점 이후 트래픽 유입량이 차이가 나는 것을 알 수 있다.



(그림 6) IP Flow 기반 차단 기법 적용 결과

이에 비해 제안된 서비스 Flow 기반 차단 기법은 (그림 7)과 같이 공격 탐지 후 차단 시점에 공격자의 공격 트래픽만을 차단하고 나머지 트래픽은 정상적으로 허용되어, 공격 시점 전과 차단 시점 이후 트래픽 유입량이 차이가 없는 것을 알 수 있다.



(그림 7) 서비스 Flow 기반 차단 기법 적용 결과

실험 결과는 아래 <표 5>과 같이 정리하였다.

<표 5> 차단 기법에 따른 실험 결과

차단 기법	정상 사용자		공격자	
	정상 ICMP	정상 TCP	정상 ICMP	공격 TCP
Port 기반	차단	차단	차단	차단
IP Flow 기반	허용	허용	차단	차단
서비스 Flow 기반	허용	허용	허용	차단

5. 결론

본 논문에서는 SDN 환경에서 DDoS 공격 발생 시 SDN 스위치에서 수집된 Flow 정보를 기반으로 SDN 애플리케이션에서 공격 Flow를 탐지하고, 해당 Flow에 대해서만 SDN 컨트롤러를 통해 차단하는 서비스 Flow 기반 DDoS 방어 기법을 제안하였다. 기존 연구 기법에 비해 제안 기법은 공격 Flow만을 탐지 후 차단함으로써 차단 범위를 최소화하고, 공격자 IP로부터의 정상적인 트래픽은 계속 허용하는 것을 확인하였다.

서비스 거부 공격에는 TCP 자원 고갈 공격 외에도 다양한 공격이 있다. 향후 연구에서는 SDN 환경에서 다양한 DDoS 공격 발생 시 이를 탐지하고 차단할 수 있는 방어 기법에 대해 연구한다.

참고문헌

[1] M. Casado et al., “Ethane: Taking Control of the Enterprise,” ACM SIGCOMM Computer Communication Review, Aug. 2007.

[2] Y. Liu et al., “A survey: typical security issues of software-defined networking,” China Communications, vol. 16, no. 7, pp. 13-31, Jul. 2019.

[3] J. Mirkovic et al., “A Taxonomy of DDoS Attack and DDoS Defense Mechanisms,” ACM SIGCOMM Computer Communiations Review, vol. 34, no. 2, Apr. 2004.

[4] M. Nugraha et al., “Utilizing OpenFlow and sFlow to Detect and Mitigate SYN Flooding Attack,” 멀티미디어학회논문지, vol. 17, no. 8, pp. 988-994, Aug. 2014.

[5] 방기현 외 2명, “SDN 환경에서의 목적지 주소별 패킷 샘플링을 이용한 SYN Flooding 공격 방어기법,” 멀티미디어학회논문지, vol. 18, no. 1, pp. 35-41, Jan. 2015.

[6] 조승신 외 1명, “Cookie 기반의 HTTP DDoS Attack 방어 시스템,” 한국통신학회 학술대회논문집, pp. 464-465. Jan. 2016.

[7] 신동혁, “Malicious traffic detection using K-means,” 성균관대학교 대학원 석사학위논문, 2016.

[8] 오대명, “SDN 환경의 플로우 테이블 특징 기반 DDoS 공격 완화 기법,” 서울과학기술대학교 대학원, 석사학위논문, 2016.

[9] 박종환 외 1명, “SDN 환경에서 소스의 입력 포트를 기반으로 한 DDoS 탐지 및 대응 방법,” 한국통신학회 학술대회논문집, Jan. 2019.

[10] 김정훈, “SDN 및 sFlow를 활용한 이동통신사 IP망 환경에서 DDoS 공격 대응 개선방안,” 연세대학교 공학대학원, 석사학위논문, 2016.

[11] HB. Bae et al., “Zombie PC Detection and Treatment Model on Software-Defined Network,” Computer Science and its Applications, pp. 837-843, Jan. 2015.