한국정보전자통신기술학회논문지(jkiiect)'20-2, Vol.13 No.1
논문 20-13-01-81 http://dx.doi.org/10.17661/jkiiect.2020.13.1.81

소프트웨어-정의 네트워크에서 분산형 서비스 거부(DDoS) 공격에 대한 탐지 기술 연구

김순곤*

A Study on the Detection Technique of DDoS Attacks on the Software-Defined Networks

SoonGohn Kim*

요 약 최근 네트워크 구성은 SDN/NFV 기반으로 쉽고 자유로운 네트워크 서비스 구성이 가능하도록 빠르게 전환중이다. SDN의 많은 장점과 적용에도 불구하고 분산형 서비스 거부(Distributed Denial of Service: DDoS) 공격과 같은 많은 보안 문제가 연구 이슈로 지속적으로 제기되고 있다. 특히, DDoS 공격의 효과는 훨씬 더 신속하게 나타나며 기존의 네트워크에 비하여 SDN에서는 더욱더 치명적인 피해를 발생시키고 있다. 본 논문에서는 SDN에서 DDoS 공격을 감지하고 완화하기 위해 엔트로피 기반 기법을 제안하고 실험을 통해 입증하였다. 본 논문에서 제안하는 기법은 단일 시스템에 대한 DDoS 공격을 탐지하고 시간 특성 기법을 활용하여 이러한 공격을 완화하도록 설계하였으며, 제안한 기법을 적용했을때 3.21%의 네트워크 혼잡도를 발생시키지만, 20(19.86)%의 패킷 분실률을 줄이는 효과를 실험을 통해 확인하였다..

Abstract Recently, the network configuration is being rapidly changed to enable easy and free network service configuration based on SDN/NFV. Despite the many advantages and applications of SDN, many security issues such as Distributed Denial of Service (DDoS) attacks are being constantly raised as research issues. In particular, the effectiveness of DDoS attacks is much faster, SDN is causing more and more fatal damage. In this paper, we propose an entropy-based technique to detect and mitigate DDoS attacks in SDN, and prove it through experiments. The proposed scheme is designed to mitigate these attacks by detecting DDoS attacks on single and multiple victim systems and using time - specific techniques. We confirmed the effectiveness of the proposed scheme to reduce packet loss rate by 20(19.86)% while generating 3.21% network congestion.

Key Words : Software-Defined Networks, Network Security, DDoS, Entropy, Computer Network

1. 서론

기존 네트워크는 클라우드, 5G, IoT 등으로 인해 네트워크 규모가 커지고 복잡성이 증가되고 있으며 네트워크를 관리하는 기능 역시 특정 장비에 종속되어 있어 불필요한 장비의 구입 비용이 지속적으로 증가되고 있다. 또한 네트워크 정책 변경 및 확장에 대한 어려움으로 인해 구조적 한계성을 가지고 있으므로 이러한 환경 변화와 다양한 요구에 따라 최근 네트워크 구성은 SDN/NFV 기반으로 쉽고 자유로운 네트워크 서비스 구성이 가능하도록 빠르게 급속하게 전환중이다. SDN(Software Defined Network)은 트래픽 경로를 지정하는 컨트롤 플레인과 트래픽 전송을 수행하는 데이터 플레인으로 분리하고 OpenFlow 프로토콜과 같은 개방형 API를 통해 네트워크의 트래픽 전달 동작을

This Paper was supported by research and development Fund of Joongbu University in 2019.
*School of Software Engineering, Joongbu University(sgkim@joongbu.ac.kr)
Received January 30, 2020 Revised February 24, 2020 Accepted February 25, 2020

소프트웨어 기반 컨트롤러에서 제어하는 접근 방식으로서 스위치, 라우터와 같은 네트워크 장비 내에 해당 단말의 동작을 제어하는 기능과 데이터를 전송하는 기능을 모두 포함하는 기존 방식과 차별성을 가지고 있다[1]. 하지만, SDN의 많은 장점과 적용에도 불구하고 분산형 서비스 거부(Distributed Denial of Service; DDoS) 공격과 같은 많은 보안 문제가 연구 이슈로 제기되고 있다. 특히, DDoS 공격의 피해 효과는 훨씬 더 신속하게 나타나며 기존의 네트워크에 비하여 SDN에서는 더욱더 치명적인 피해를 발생시키고 있다. 이러한 이유는 SDN이 네트워크 운용 통제에 있어서 단일 지점(컨트롤러)에 의존하기 때문이며 이 지점에 대한 어떠한 잠재적 공격이나 오작동도 전체 네트워크 붕괴로 이어질 수 있는 심각한 문제를 가지고 있다.

일반적으로 SDN에서 발생되는 공격은 첫째,호스트에 새로운 패킷이 도착하고 이 패킷이 스위치의 플로우 테이블에서 매칭되지 않는 경우, 둘째, 컨트롤러로 전송되어 플로우 테이블에 플로우 입력 규칙을 생성하게 되고 스위치 디바이스 테이블이 업데이트 된다. 이런 방식으로 최종 사용자에게 높은 트래픽을 전송하고 다시 이 트래픽을 스위치 디바이스를 통해 컨트롤러로 전송함으로써, 호스트를 통해 컨트롤러와 스위칭 디바이스를 다운시킬 수 있다. 공격자들은 이를 악용하여 새로운 패킷들로 구성된 높은 트래픽을 보내 SDN 컨트롤러에까지 이르도록 하는 것이다. SDN의 어떠한 부분에 대해 DDoS 공격을 해도 이러한 동작은 SDN 컨트롤러 자체를 공격하는 것이 된다. 따라서, SDN 컨트롤러를 보호함으로써 모든 네트워크 요소를 안정적으로 보호할 수 있다. 이러한 이유로 SDN 컨트롤러에 적절한 조기 공격 탐지 메커니즘을 통해 DDoS와 같은 치명적인 공격을 감지하고 방어할 수 있는 효과적이고 신뢰성이 높은 방법이 필요하다[2,3].

이러한 연구 이슈를 해결하기 위해 최근까지 여러 연구자들이 다양한 기법들을 제안해 왔다. 그중 하나는 엔트로피(entropy) 기반 기법으로서 수신되는 패킷의 무작위성(확률)을 이용하여 공격을 탐지하는 것이다[4]. 최대 엔트로피는 각 수신 패킷이 서로 다른 호스트로 향할 때(공격이 없는 경우) 발생하며, 최소 엔트로피는 모든 패킷이 동일한 목적지로 향할 때(공격이 있는 경우) 발생한다. 엔트로피 기반 기법에서는 해당 네트워크 내 모든 호스트가 비교적 동일한 트래픽 비율을 가진다고 가정하며, 하나의 호스트에 트래픽이 증가할 때만 공격을 감지할 수 있다. 그러나 사실상, 악의적인 공격자들은 쉽게 상이한 IP를 향해 다수의 트래픽 플로우를 발생시켜 여러 호스트들이 컨트롤러를 과부하 시킬 수 있다. 모든 네트워크에서 완화 프로세스가 중요한 이유는 DDoS 공격이 네트워크 리소스와 대역폭을 소비하지 못하도록 하여 서비스 중단을 막는 것이다.

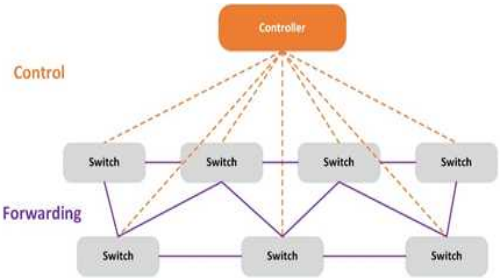

그림 1. SDN 컨트롤 플레인과 데이터 플레인
Fig. 1. SDN Control plane and Data plane

또한, 엔트로피 기반 기법은 DDoS 공격을 물리칠 수 있는 완화(mitigation) 메커니즘이 부족하다는 문제점을 내포하고 있다. 이러한 이유는 엔트로피 기반 기법이 공격의 시간적인 특성을 고려하지 않아 공격 초기에 공격을 완화하지 못하기 때문이다. 따라서 본 논문에서는 SDN에서 DDoS 공격을 감지하고 완화하기 위해 엔트로피 기반 기법을 제안하고 실험을 통해 입증하는 것이다. 본 논문에서 제안하는 기법은 단일 및 다수 피해 시스템에 대한 DDoS 공격을 탐지하고 시간 특성 기법을 활용하여 이러한 공격을 완화하도록 설계되어 있다.

본 논문의 구성은 다음과 같다. 2장은 배경 연구로 엔트로피 개념을 기반으로 SDN에 대한 공격에 대응하는 관련 연구를 소개한다. 제 3장에서는 SDN 환경에서 여러 가지 공격중 DDoS 공격을 탐지하고 완화할 수 있는 연구 내용과 실험 결과를 제시한다. 마지막으로 4장에서는 본 연구가 갖는 한계점 및 향후 연구에 대하여 기술한다.

2. 관련 연구

엔트로피 기반으로 공격 탐지 스키마를 이용한 연구가 [4]에서 제시되었다. 이 연구에서 스키마는 소스 포트, 착신 포트, 소스 IP, 착신 IP 주소와 같은 4개 요소에 근거하고 있다. 먼저, 작동 중인 로컬 IP 주소가 모니터링 인터벌에 해당되는 특정 시간에 계산된다. 이렇게 작동 중인 호스트로 흘러가는 패킷의 숫자가 트래픽이 지나가는 엣지 스위치(edge switch)를 통해 계산된다. 그리고 나면, 각 IP 빈도가 계산된 후 이 빈도수를 이용하여 로컬 IP 주소의 확률 분포가 도출된다. 이때, 작동 중인 로컬 IP 주소의 확률 분포에 대한 엔트로피가 도출된다. 이상 결정 함수를 이용하여 도출된 엔트로피가 공격을 의미하는지 여부를 결정한다. 이 함수는 동적이며 네트워크의 모든 변화에 반응하므로 그 값이 고정되어 있지 않다. 여기에는 도출된 엔트로피 값과 비교하는데 사용되는 기준 값도 포함된다. 도출된 값이 기준 값보다 낮은 경우는, 공격으로 의심된다. 그렇지 않은 경우는 네트워크에서 어떠한 악의적 활동으로 의심되지 않는다.

DDoS 공격 탐지를 위한 엔트로피 기반 기법은 [5]에서 진행되었다. 이 방법은 무작위성을 활용하여 특정 호스트로 가는 수신 패킷의 수를 계산한 후, 이를 기준 값과 비교한다. 이 비교 결과에 따라서 공격여부를 결정하고 감지한다. 이 연구에서는 수신되는 패킷을 측정하는 무작위성을 활용하였으며, 무작위성을 측정하는 좋은 방법으로 엔트로피를 활용하였다. 엔트로피는 총 이벤트 수에 대하여 하나의 이벤트가 발생할 확률을 도출하며 무작위성이 감소하면 엔트로피가 감소한다는 것을 의미하고 있다. [6]과 [7]과 같은 연구에서는 DDoS 공격을 탐지하기 위해 다른 기술을 사용했습니다. 시간-기반 기술에서는 시간 특성 값이 다른 연구에서 고려되지 않았던 DDoS 공격을 탐지하는데 중요하게 활용하는 요소 중 하나이다. 특히, [6] 기법에서는 패킷의 특성과 흐름 시간을 기반으로 통계적 방법을 제안했다. 이 방법은 sFlow[8]를 사용하여 흐름 정보를 수집하고 특정 임계 값을 적용하여 DDoS 패킷을 인식할 수 있도록 제안했다.

3. SDN 기반 DDoS 탐지 및 완화시스템

3.1 데이터 수집 단계

본 논문에서 제안한 SDN 환경에서 엔트로피 기반의 DDoS 공격에 대한 감지 및 완화 기법은 데이터 수집, 감지, 완화 단계로 구성되어 있다.

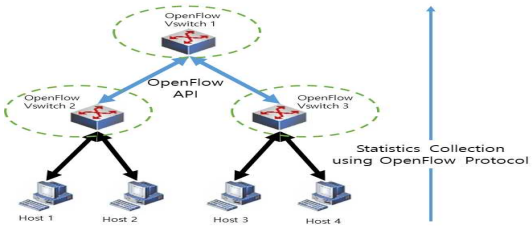

그림 2. 오픈플로우 프로토콜을 이용한 데이터 수집 과정 및 단계
Fig. 2. Data Collection Prodedure and Stage using OpenFlow Protocol

데이터 수집은 그림 2와 같은 환경에서 우선적으로 작동 중이지 않은 플로우를 감지하고, 도착 IP 주소 빈도수와 플로우 개시율에 대한 엔트로피 도출 관련 정보를 제공하기 위해 활용된다. 감지 메커니즘의 첫 단계에서는 컨트롤러가 그림 2와 같이 OpenFlow 프로토콜을 사용하여 해당 네트워크 내 모든 OpenFlow 스위치로부터 플로우 정보(통계)를 수집한다. 이 정보는 보안 커뮤니케이션을 위한 보안 전송 계층 프로토콜을 통해 수집된다. 실제 실험과정에서 수집되는 통계 자료들은 100 패킷의 고정된 윈도우 사이즈를 사용하여 컨트롤러에 수집되도록 하였다. 100 패킷으로 설정한 근본적인 이유는 컨트롤러의 연산 오버헤드를 줄일 수 있으며 보다 큰 윈도우 사이즈보다 더 정확한 결과를 제공하기 때문이다. 또한 이러한 메커니즘은 공격 감지 단계에서 추가적인 프로세싱에 대한 파라미터들을 정의한다. 이 파라미터에는 100 패킷을 수집하는데 필요한 기간을 도출하기 위해 시간 파라미터가 포함되며 수신 IP 주소 빈도수를 저장하기 위한 다른 파라미터도 포함된다.

3.2. 감지 단계

데이터가 수집된 후, 컨트롤러 플레인에서는 DDoS 공격 감지 메커니즘이 작동된다. 공격자들이 대량의 위

조 IP 주소 출처로부터 네트워크를 공격할 수 있으므로 플로우 정보를 분석하는 감지 메커니즘이 견고하게 유지되는 것이 필수적이다. 본 논문에서는 감지 동작을 위해 3개의 카운터를 이용한다. 첫 번째 카운터는 목적지 IP 주소를 계산하기 위해 사용한다. 두 번째 카운터는 네트워크에 위치해 있는 소스 IP 주소의 빈도수를 계산하기 위해 사용한다. 실제로 가상의 IP는 xxx.x.x.1번부터 8까지 지정하여 실험하였으며 탄력적으로 조정할 수 있도록 하였다. 마지막으로 세 번째 카운터는 윈도우 크기를 계산하는데 사용하며 실제 실험 과정에서는 윈도우 크기를 100 패킷 크기로 고정하여 엔트로피를 계산하였으며 감지 동작은 5개의 연속적인 윈도우 다음에 동작하도록 지정하였다. 따라서 최종적으로 500개 이상의 패킷을 통해 감지하는 동작을 실험하였다. 실제적인 감지 동작은 그림 3과 같이 패킷이 컨트롤러에 도착했을 때, 타이머가 동작되며 타이머는 감지 동작과 100개의 패킷을 모으는데 필요한 시간을 계산하는데 필요하다.

```
def NewPacketInEvent():
    if Counter() == 0:
        StartTimer(); DestinationIP();
    else: DestinationIP()
    if DestiantionIP() == True:
       DestinationIPTrue();
    else: DestinationIPFalse()
    if SourceIP() == True: SourceIPTrue()
    else: SourceIPFalse();
    if DestinationCounter100() == 100:
        DestinationCounter()
    else: NewPacketInEvent()
    if LowerThanThreshold() == True:
        WindowCounterPlus()
    else:
        CalculateFlowRate()
        if HigherThanThreshold() == True:
            WindowCounterPlus()
        else: ClearCounter(); NewPacketInEvent()
    if WindowCounter() == 5:
        AttackDetected(); StartMitigationProcess()
        break
    else: NewPacketInEvent()
while True:       NewPacketInEvent()
```

그림 3. 감지 동작 알고리즘
Fig. 3. Detection Algorithm

3.3 완화 단계

공격이 감지된 후에는 DDoS 공격이 해당 네트워크를 방해하지 못하도록 완화 또는 방어 동작을 수행해야 한다. DDoS 공격에 대한 완화 과정은 컨트롤러에서 시작하여 그림 4와 같이 최종 호스트로 하향식으로 진행된다. 네트워크 보안을 위해 사용되는 일반적인 방법 중의 하나는 손상된 경로에서 오는 패킷을 거부하거나 의심스러운 공격자로부터 오는 수신 포트를 막는 것과 같이 새로운 규칙을 통해 새로운 플로우를 설치하는 것이다. 이러한 방법은 네트워크에 대한 악의적 공격을 방지할 수 있다. 그러나 정당한 트래픽에도 속도 등에 막대한 영향을 미칠 수 있는 한계점을 가지고 있다.

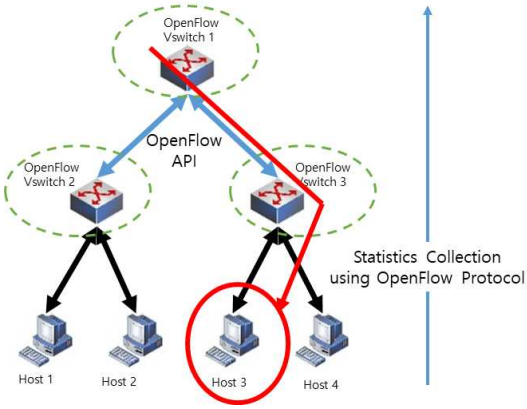

그림 4. 하향식 완화 과정
Fig. 4. Top-down Mitigation Process

```
if ( Attack_Detected )
 then Time Value = Mitigated Value
      if( Participating in Attack )
       then Block Host //Attack
       else Clear Counter //
 else Time Value = Mitigated Value
//...
```

그림 5. 완화 단계 알고리즘
Fig. 5. Mitigation Process Algorithm

스위치는 일반적으로 제한된 리소스를 이용하여 설계되고 플로우 테이블이 네트워크의 정상적인 동작을 방해할 수 있는 정보로 채워지기 때문에 DDoS 공격 등에 대해 강력하지 대처하지 못하고 있다. 완화 단계에서, 타이머는 그림 5와 같이 각 플로우의 타임아웃(만료) 값을 체크하기 위해 기본(Default)과 완화

(Mitigated) 타이머 값을 이용한다. 이 두 개의 타이머 값은 임계값으로 사용되는 타이머의 상태를 변경하는 데 사용된다. 완화 타이머 값은 기본 타이머 값보다 작으므로 짧은 악의적인 흐름에 대해 만료된다. 또한 악의적인 플로우는 정상적인 플로우보다 시간 제한 값이 작다. 이 타이머가 특정 흐름에 대해 만료되면 스위치의 플로우 테이블에서 플로우가 제거된다. 완화 메커니즘은 연결 시간이 길고 패킷 수가 많기 때문에 정상적인 플로에 영향을 미치지 않는다.

3.4. 실험 및 검증

본 논문에서 제안한 기법은 Mininet[9] 가상 네트워크 환경을 활용하여 구현하였으며 Mininet은 가상 머신 관련된 어플리케이션, 커널, 스위치를 제공하는 현실적인 가상 네트워크를 지원한다. 추가적으로 POX가 네트워크 컨트롤러로 이용되는 이유는 파이썬 기반 SDN 컨트롤 어플리케이션에 대한 오픈 소스 개발 플랫폼이기 때문이다. POX는 신속한 개발 및 프로토타이핑을 가능하게 하며 다른 타입의 컨트롤러보다 더 보편적으로 사용되었다. 본 논문에서는 OpenFlow[10] 버전 1.1.0을 사용하였으며, 이러한 이유는 POX 컨트롤러와 가장 호환성이 높은 버전이기 때문이다. 또한 오픈 가상 스위치(OVS)를 네트워크 스위치로 사용하였다. 침입 테스트 툴인 Scapy[11]가 악성 및 정당한 두 가지 유형의 트래픽에 대한 UDP 패킷 생성을 위해 사용된다. 7개 스위치와 8개 호스트를 포함하고 있는 트리 타입 토폴로지가 적용되었으며, 본 실험 환경의 네트워크 구조상 루트 노드가 필요하므로 이 노드는 POX 컨트롤러로 대변되었다. 실험을 위해 1부터 8까지의 호스트에는 각각 xx.x.x.1부터 xx.x.x.8까지 나열된 디폴트 IP 주소를 부여하였다.

실험에서 공격자는 도용 IP 주소 UDP 플러딩 공격을 네트워크 내 여러 호스트를 대상으로 생성한다. 각 IP 주소가 xx.x.x.2, xx.x.x.5, xx.x.x.8인 호스트 2, 호스트 5, 호스트 8이다. 이 시뮬레이션은 세 가지 조건으로 나누어지며 각 조건은 60초에 해당된다. 이 과정을 별도로 두 번 이상 진행하였으며 첫 번째는 본 연구에서 제안된 기법을 적용하였다. 첫 번째 조건에서는 네트워크에 공격 트래픽 없이 운영하였으며, 본 논문에서 제안된 기법이 네트워크에 영향을 미치는지 여부를 확인하게 된다. 두 번째 조건에서는 정상 및 공격 트래픽이 동시에 생성되는데 공격 트래픽은 총 트래픽의 25% 정도에서 생성하여 본 논문에서 제안된 기법이 이 비율을 식별해 낼 수 있는지 확인하는 실험을 진행하였다. 두 번째 조건에서, 공격 트래픽은 0.033의 속도(초당 30패킷)로 생성된다. 정상 트래픽은 9개 터미널로부터 0.099초 간격으로 생성되어 25% 공격률이 달성되었다. 세 번째 조건에서는 정상 및 공격 트래픽이 다시 생성하지만 공격 트래픽은 50% 속도로 생성되었다. 공격 트래픽은 0.015초 간격(초당 67 패킷)으로 생성되나, 정상 트래픽은 4개 터미널(초당 67 패킷)로부터 0.06초 간격으로 생성된다. 동일한 방식으로, 정당한 트래픽에는 30 바이트의 데이터(payload)가 포함되나, 공격 트래픽에는 어떠한 데이터도 포함되지 않는다. 본 제안된 기법 사용 시, 총 패킷 손실은 9.72%이다. 반면, 제안된 기법이 적용되지 않았을 때 총 패킷 손실은 29.58%이다. 그러므로, 제안 기법 실행 시 총 패킷 손실은 디폴트 기법보다 20(19.86)% 낮다. 본 논문에서 제안된 기술에 적용된 POX 컨트롤러와 디폴트 POX 컨트롤로에 대한 평균적인 링크 성능은 그림 6과 같다.

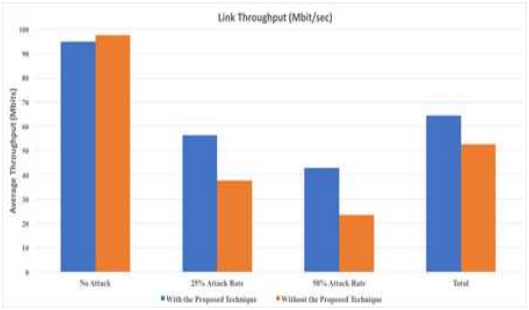

그림 6. 링크 성능
Fig. 6. Link Throughput

첫 번째 조건에서는 어떠한 악의적인 트래픽이 없이 UDP 패킷이 소스로부터 목적지에 전송하였다. 평균적인 성능 비교는 본 연구에서 제안된 방법을 적용한 경우의 성능이 94.73 Mbits/sec 반면, 제안된 기술이 적용되지 않은 경우 97.57 Mbits/sec 임을 확인하였다.

실제로 본 논문에서 제안된 기법이 구현된 경우, 데이터 수집 단계에서 일정 부분 오버헤드를 가지고 있으며 실제 네트워크상에서 네트워크의 혼잡을 발생시키는 요인임을 확인하였다. 따라서, 본 논문에서 제안된 기술을 적용한 경우 기술을 적용하지 않은 경우에 비해 평균적으로 3.21%의 네트워크 혼잡 오버헤드가 발생하는 것을 확인하였다. 이러한 이유는 DDos의 공격을 감지하고 완화 동작을 위해 일정한 오버헤드가 발생되지만, 이로 인해 예상 공격을 탐지하고 완화시키는 효과가 기대되므로 소비되는 trade-off로 간주하고 있다.

SDN의 핵심인 컨트롤러가 공격을 받아 심각한 상황을 유발하는 손실에 비해 충분히 감수할 수 있는 성능 감소로 판단된다.

발생되는 오버헤드 값(3.21%)과 94.73 Mbits/sec 성능 값의 검증은 본 연구 방법을 적용했을 경우와 적용하지 않았을 경우를 2회 이상 적용한 후의 평균값이다. 특히, 발생되는 오버헤드 값의 실질적인 근거는 스위치 노드에서 공격 감지에 소요되는 시간 비용과 감지된 경우 완화 기술을 적용하기 위해 콘트롤 플레인에서 지연되는 값으로 실험과정에서 확인하였다.

4. 결론 및 향후 과제

보안 취약점은 SDN의 주요한 연구 이슈로서 특히, DDoS 공격에 대해 취약성과 피해 파급효과가 막대하다. 공격자는 SDN 네트워크의 취약성을 쉽게 악용하여 다양한 유형의 공격을 시작할 수 있으며 이를 완화하고 방어하기 위한 많은 기법들이 제안되었지만 공격 속도가 매우 낮을 때 공격을 완화 할 수 있는 방안이 미흡한 상태이다. 본 논문에서는 SDN 컨트롤러에 대한 DDoS 공격을 탐지하고 완화하기 위해 시간 특성 기법을 적용한 엔트로피 기반 기술을 제안하고 실험을 통해 검증하였다. 본 논문에서 제안한 기법은 다양한 공격 시나리오에서 SDN 네트워크의 단일 시스템에 대한 DDoS 공격을 탐지할 수 있으며 제안된 기술을 적용하여 정상적인 트래픽과 공격적인 트래픽을 효율적으로 구분할 수 있다. 특히, 완화 단계에서는 정상적인 트래픽에 미치는 요소를 제거하였고 공격 특성을 식별하기 위해 지속 시간 매개 변수를 추출하여 시간 특성 기술을 사용하여 구현하였으며, 트래픽이 악성 트래픽으로 탐지 된 경우 트래픽을 삭제하도록 네트워크 스위치에 요청하는 모듈을 추가하였다. 향후 지속적인 연구 진행을 위해 실제적이고 확장 가능한 네트워크에서 본 연구에서 제안한 기술을 적용하여 UDP 플러딩 DDoS 공격으로부터 네트워크를 처리하고 보호하기 위해 동적 네트워크에 적용하는 연구를 진행하고자 한다.

REFERENCES

[1] Akhunzada A., Ahmed E., Gani A., Khan M. K., Imran M., and Guizani, S., “Securing software defined networks: taxonomy, requirements, and open issues”, IEEE Communications Magazine, Vol. 53, No. 4, pp. 36-44, 2015.

[2] Scott-Hayward S., Natarajan S., and Sezer S., “A survey of security in software defined networks”, IEEE Communications Surveys & Tutorials, Vol. 18, No. 1, pp. 623-654, 2016.

[3] Scott-Hayward S., O’Callaghan G., and Sezer, S, “SDN security: A survey. In Future Networks and Services (SDN4FNS)”, 2013 IEEE SDN, pp. 1-7, 2013.

[4] Wang R., Jia Z., and Ju, L., “An Entropy-Based Distributed DDoS Detection Mechanism in SDN”, In Trustcom/BigDataSE/ISPA, 2015 IEEE, Vol. 1, pp. 310-317, 2015.

[5] Mousavi S.M. and St-Hilaire M., “Early detection of DDoS attacks against SDN controllers”, In Computing Networking and Communications (ICNC) International Conference, pp. 77-81, 2015.

[6] Muhammad Nugraha, Isyana Paramita, Ardiansyah Musa, Deokjai Choi, Buseung Cho, “Utilizing OpenFlow and sFlow to Detect and Mitigate SYN Flooding Attack,” Journal of Korea Multimedia Society, Vol. 17, No. 8, pp.988-994, Aug. 2014.

[7] Dharma N. G., Muthohar M. F., Prayuda J. A., Priagung K., Choi, D., “Time-based DDoS detection and mitigation for SDN controller, ”. In Network Operations and Management Symposium (APNOMS 2015), pp. 550-553,

Aug. 2015.
[8] sFlow Version 5. [Online]. http://sflow.org/sflow version 5.txt, May 2017.
[9] Mininet, http://mininet.org/, 2018, May.
[10] Openflow, https://openflow.stanford.edu/display/Beacon/Home, 2018. May
[11] Scapy. http://www.secdev.org/projects/scapy/, 2018, May.

저자약력

김 순 곤 (SoonGohn Kim) **[종신회원]**

- 1999년 : 전북대학교 전자계산기공학과(공학박사)
- 1987년 : 동국대학교 전산교육학과(교육학석사)
- 1987년~1995년 : 한국원자력연구소 선임연구원
- 1995년~현 재 : 중부대학교 소프트웨어공학부 교수

〈관심분야〉 데이터베이스, 정보보호, 유비쿼터스컴퓨팅, 모바일컴퓨팅, 정보시스템감리, SDN 등