https://doi.org/10.33778/kcsa.2020.20.5.003

P4 프로그래머블 네트워크를 통한 정책 기반 인-네트워크 보안 관리 방법

조 부 승*

요 약

최근 인터넷 그리고 네트워크는 사회를 구성하는 필수적인 인프라로 여겨짐과 동시에 이에 대한 보안 위협 상황이 지속적으로 증대되고 있다. 그러나 네트워크에서 실제 패킷을 전송하는 스위치 단에서는 기본적으로 고정적인 룰에 의한 방화벽 혹은 네트워크 접근 제어를 통해서만 보안 위협을 대응할 수 있어, 보안 위협에 대한 효과적인 대응은 네트워크 자체에서는 극히 제한적이며, 능동적으로 대처하지 못하고 있다. 본 논문에서는 네트워크 데이터 평면 프로그래밍 언어인 P4 (Programming Protocol-independent Packet Processor)를 통해 네트워크 내 모든 플로우를 P4 스위치 단에서 실시간으로 모니터링하고, 특정 보안 공격 패킷을 스위치 단에서 처리함으로써, 네트워크 단에서 분산 DDoS 공격, IP Spoofing 공격 등을 대응할 수 있는 인-네트워크 (In-Network) 보안 관리 방법을 제안한다. 또한 네트워크 사용자 혹은 보안 관리자의 운영 정책을 SDN (Software-Defined Networking) 제어기를 통해 P4 스위치에서 적용함으로써, 다양한 네트워크 응용 환경에서의 보안 요구 사항을 반영할 수 있다.

Policy-based In-Network Security Management using P4 Network DataPlane Programmability

Buseung Cho*

ABSTRACT

Recently, the Internet and networks are regarded as essential infrastructures that constitute society, and security threats have been constantly increased. However, the network switch that actually transmits packets in the network can cope with security threats only through firewall or network access control based on fixed rules, so the effective defense for the security threats is extremely limited in the network itself and not actively responding as well. In this paper, we propose an in-network security framework using the high-level data plane programming language, P4 (Programming Protocol-independent Packet Processor), to deal with DDoS attacks and IP spoofing attacks at the network level by monitoring all flows in the network in real time and processing specific security attack packets at the P4 switch. In addition, by allowing the P4 switch to apply the network user's or administrator's policy through the SDN (Software-Defined Network) controller, various security requirements in the network application environment can be reflected.

Key words : In-network security, Data Plane Programmability, Software-Defined Network, P4

접수일(2020년 10월 5일), 수정일(1차: 2020년 12월 15일), 게재확정일(2020년 12월 16일)

* 한국과학기술정보연구원/과학기술연구망센터
과학기술연합대학원대학교/데이터 및 HPC과학

1. 서 론

최근 인터넷 그리고 네트워크는 사회를 구성하는 필수적인 인프라로 여겨짐과 동시에 이에 대한 보안 위협 상황이 지속적으로 증대됨은 물론 사회적으로 기존보다 더 치명적인 위협으로 인식되고 있다. 이러한 네트워크 보안 위협으로부터 네트워크 방화벽, 웹 방화벽, 침입방지시스템, 침입차단시스템, 네트워크 접근 제어(Network Access Control) 등의 추가적인 네트워크 장비 혹은 기능을 통해 보안 공격을 탐지하여 네트워크를 방어하고 있다. 그러나 네트워크에서 실제 패킷을 전송하는 스위치 단에서는 기본적으로 고정적인 룰에 의한 방화벽 혹은 네트워크 접근 제어를 통해서만 보안 위협을 대응할 수 있어, 보안 위협에 대한 효과적인 대응은 네트워크 자체에서는 극히 제한적이며, 능동적으로 대처하지 못하고 있다.

최근에 각광을 받고 있는 소프트웨어 정의 네트워크(Software-Defined Networking, 이하 SDN) 기술을 통해 네트워크의 제어평면과 데이터평면으로 네트워크 기능을 분리하여 구현함으로써, 네트워크 구성 요소에 대한 중앙 집중적인 네트워크 제어를 가능하게 하고 있으며, 이를 네트워크 보안에 적용하려는 연구가 진행되고 있다. 그러나 기존의 SDN 기술 즉, SDN 제어기(Controller) 기반의 네트워크 보안은 보안 위협 패킷을 리다이렉션(Redirection)을 하는 방법에 대한 연구가 주로 진행되었지만, SDN 제어기 자체가 DDoS 등의 플러딩 기반 보안 공격에 노출될 수 있으며, 네트워크 내 SDN 스위치를 공격 패킷으로부터 즉각적으로 그리고 동적으로 제어하기 어렵다. 특히 기존의 SDN 스위치에서는 플로우 혹은 세션의 상태 모니터링이 불가하여, 동적으로 전개되는 사이버 공격에 대한 대응이 힘든 것 또한 사실이다[1][2]. 또한 원천적으로는 오픈플로우(OpenFlow) 기반의 SDN 스위치의 데이터평면으로 보안 위협 패킷이 유입될 경우, 해당 패킷의 처리를 위해 SDN 제어기에 처리 방법을 요청한 후 해당 결과를 다시 SDN 스위치에 해당 플로우 룰을 내려 보낸 후 해당 패킷을 처리하는 데에는 물리적으로 SDN 스위치와 SDN 제어기 사이의 통신에 드는 지연 시간 및 처리 시간이 소요됨으로 인해 즉각적인 대응을 못할 뿐 아니라, 물리적인 최대 속도(Line-rate)로 보안 공격 패킷을 처리할 수 없다.

이를 극복하고자 SDN 데이터 평면에서의 보안 공격에 대응을 고려해볼 수 있다. 그러나 전통적인 네트워크 스위치는 스위치의 데이터 평면은 기존의 고정된 TCP/IP 프로토콜 혹은 L2 프로토콜을 처리하기 위해 구현된 것으로, 네트워크의 플로우 혹은 세션을 지속적으로 모니터링하거나 스위치 단에서 특정 룰에 맞게 패킷을 차단(deny)/허용(allow)/리다이렉션(redirect) 등의 추가적인 네트워크 기능을 구현하는 것은 불가능하다. 보통의 경우 이러한 추가 기능에 대한 요구사항은 스위치 벤더에 전달되어 주문 제작 형태로 진행되는 경우도 있지만, 해당 기능을 주문한 후 실제 구현된 스위치를 인도하는데 상당한 기간이 필요하다. 또한 대부분의 스위치 벤더는 고정된 기능을 구현함으로써 대량 생산을 통해 스위치의 단가를 낮추어 판매하는 마케팅 전략을 사용하는데, 이러한 주문 형태의 제작은 스위치 벤처 측에서는 추가적인 스위치의 설계 및 구현에 드는 비용의 증가로 경제성이 낮아 대형 스위치 벤더의 대량 주문이 아니고서는 제작이 불가능한 것이 사실이다.

최근 데이터 평면에 대한 네트워크 특화된 고수준 언어인 P4 (Programming Protocol-independent Packet Processor)와 베어풋(Barefoot)사의 토피노(Tofino 2) 칩과 같은 P4 기반의 프로그래밍 가능한 테라급 고성능 스위치 칩[13]을 통해, 네트워크 스위치 단에서 공격 패킷을 직접 모니터링하고 차단할 수 있다. 본 논문에서는 데이터 펌면 프로그래밍 언어는 P4를 통해 네트워크 내 모든 플로우를 P4 스위치 단에서 실시간으로 모니터링하고, 특정 보안 공격 패킷을 스위치 단에서 처리함으로써, 네트워크 단에서 분산 DDoS 공격, IP Spoofing 공격 등을 대응할 수 있는 인-네트워크 보안 관리 방법을 제안한다. 또한 제안하는 보안 관리 방법은 네트워크 사용자 혹은 보안 관리자의 운영 정책을 기존의 SDN 제어평면을 제어하는 SDN 제어기를 통해 P4 스위치에서 적용할 수 있게 함으로써, 본 논문에서는 네트워크 응용 환경에서의 다양한 보안 요구 사항을 반영할 수 있는 메커니즘을 제안한다.

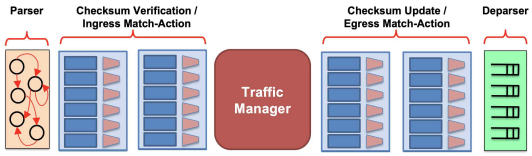
본 논문의 2장에서는 데이터 평면 SDN 기술인 P4와 SDN 및 P4 기반 기존 네트워크 보안 기술을 소개

하고, 3장에서는 몇가지 보안 공격에 대한 P4를 활용한 인-네트워크 보안 시나리오를 제안한다. 다음으로 4장에서는 정책 기반 인-네트워크(In-network) 보안 관리 방법을 제시한다. 그리고 5장에서는 인-네트워크 보안에 관한 SDN 자체에 대한 보안, 상태 기반 P4 자원 등에 대한 추가적인 이슈를 논의하며, 6장의 결론으로 마무리한다.

2. 관련 연구

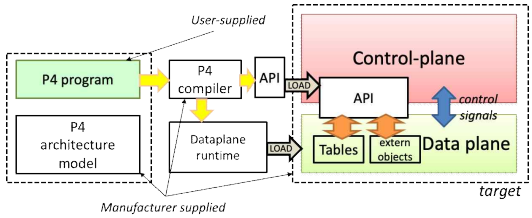
2.1 데이터 평면 SDN 기술, P4

SDN은 기존의 스위치 및 라우터 내에 구현되었던 네트워크 기능을 제어 평면과 데이터 평면으로 분리하는 구조로 각각의 평면은 프로그래밍 가능하다. 특히 기존에는 SDN 제어기와 SDN 스위치 간의 사우스바운드(Southbound) 인터페이스로써의 참조 표준인 오픈플로우 프로토콜 위주로 한 제어 평면의 연구가 진행되었다면, 최근에는 단순히 프로그래머블한 SDN 제어기보다 (그림1)과 같이 SDN 스위치 내 매치/액션(Match/Action) 기반 파이프라인 프로그래밍 가능한 데이터 평면 구조에 대한 연구가 활발히 진행되고 있다.



(그림 1) P4 Behavioral Model (bmv1)

특히 최근에 데이터 평면 프로그래밍 고수준 언어인 P4가 개발되었으며, P4에서는 파이프라인을 구성하는 각각의 매치/액션 스테이지는 ALU (Arithmetic Logic Unit)으로 구현하여, 하드웨어 속도로 헤더 필드에 대한 처리가 가능하다는 특징이 있다. P4는 네트워크 도메인에 특화된 프로그래밍 언어로써 네트워크의 포워딩 메커니즘을 파이프라인 기반 프로그래밍 할 수 있게 함으로써, 기존의 네트워크 프로토콜만 사용 가능한 제어 평면의 한계를 극복함으로써 제어 평면과 데이터 평면 모두를 프로그래밍 가능하도록 함으로써 진정한 SDN 환경을 가능하게 한다. 실제 P4를 통해 새로이 구현한 스위칭 패브릭에 대한 메커니즘을 (그림 2)와 같이 PISA (Protocol Independent Switch Architecture) 기반 네트워크 ASIC, FPGA, NIC 등을 동적으로 프로그래밍 할 수 있다.



(그림 2) P4 데이터평면 프로그래밍 구조

2.2 P4 기반 네트워크 보안 연구

기존의 SDN 기반의 엔터프라이즈 보안 솔루션으로 SANE, Ethane이 제안되었으며[3][4], SDN 제어기 자체에 대한 보안 위협 및 방어에 대한 연구가 진행되었다[7]. 또한 BYOD (Bring Your Own Device) 환경에서의 SDN 제어기 기반의 PBS (Programmable BYOD Security) 보안 솔루션과 BYOD에서의 SDN 데이터 평면 프로그래밍을 기반으로 한 컨텍스트 인지형 보안 기법으로 Poise (Programmable in-network security)가 제안되었다[5][6]. 특히 Poise의 경우, 기존의 정적인 보안 룰 기반의 네트워크 접근 제어, ACL (Access Control List) 등의 기법과 달리, SDN 데이터 평면 프로그래밍을 통하여 동적으로 컨텍스트 기반의 보안 정책(Context-aware security)을 적용할 수 있는 기법을 제안하였다. 추가적으로 P4-NetFPGA 기반 5G 멀티레이어 에지 단에서의 QoS 보장 및 보안을 위한 연구가 진행되었다[7].

본 논문에서는 기존의 BYOD 환경에서의 보안 위협에 대응하기 위한 사용자의 호스트 네트워크 단에 대하여 데이터 평면을 기술 적용을 넘어, 네트워크의 백본 및 엑세스 구간 모두에 적용 가능한 데이터 평면 프로그래밍을 통한 정책 기반 인-네트워크 보안 관리 방법을 제시한다는 점에서 기존 연구와 차별화된다. 또한 SDN 제어기와 연동하여, 동적으로 보안 정책을 적용할 수 있게 함으로써 특정 정책을 네트워크 보안 제어를 위해 적용할 수 있음은 물론 P4 기반의 스위치에서 지속적으로 상태가 변화는 보안 위협 플로우를 모니터

링하여, 사이버 공격 정보를 탐지하여, 이를 SDN 제어기를 통해 네트워크 내 다른 P4 기반의 스위치에 보안 정책을 직접 반영함으로써 네트워크 보안 운영 관점에서의 피드백 기반의 보안 운영 환경(Closed Operation Loop)을 구현할 수 있다.

3. P4 기반 인-네트워크 보안 관리 시나리오

3.1 분산 DDoS 공격 차단 시나리오

기존의 인터넷 혹은 OpenFlow 기반의 네트워크에서는 분산 DDoS (Distributed Denial-of-Service) 공격이 일어날 때 공격자의 IP가 공격대상자 IP에 대한 접근이 가능한 경우, 즉 공격자 IP가 공격대상자의 침입차단시스템 혹은 ACL에 화이트리스트(Whitelist) 혹은 블랙리스트(Blacklist)에 등록되어 있지 않은 경우, 분산 DDoS 공격을 제때에 방어하는 것은 불가능하다. 오픈플로우 기반 SDN 스위치의 경우 또한 해당 플로우에 대한 상태를 모니터링 하면서 플로우에 대한 허용/차단 정책을 동적으로 적용하여 패킷을 제어하는 것은 불가능하다. 즉, 기존 네트워크 환경에서는 해당 분산 DDoS 공격 시 이를 감지하고 탐지하기 위한 별도의 보안 장치가 추가적으로 필요하며, 이를 활용한 오픈플로우 기반 동적 플로우 제어가 가능하다. 이는 네트워크의 복잡도를 높일 뿐 아니라, 제때에 즉각적인 대응은 불가능한 구조이다. 현재 대부분의 분산 DDoS 공격이 이에 해당한다고 볼 수 있다.

P4 스위치에서는 P4 스위치를 지나가는 모든 네트워크 세션의 상태를 모니터링하고 추적할 수 있다. 이를 활용하여 기존 정상 상태의 네트워크 플로우에 대한 모니터링 후 분산 DDoS 공격이 벌어지고 있는 상황에서, P4 스위치 단에서 이를 즉각적으로 차단함으로써 분산 DDoS 공격을 차단할 수 있다. 특히, 이 경우 네트워크 플로우에 대한 차단을 위해 DPI (Deep Packet Inspection) 및 패킷의 시퀀싱 번호를 활용하여 바로 분산 DDoS 플로우에 대해 차단하는 것이 가능하다. 즉각적으로 차단하는 방법 이외에도 탐지된 공격 플로우를 P4 스위치의 원래 출력 포트에 전송하지 않고, 방화벽 혹은 침입차단장비와 연결된 P4 스위치의 출력 포트(예로 default 포트)로 리다이렉션 함으로써 차단하는 동작은 방화벽, 침입차단장비 등의 보안 장비에서 수행하게 하고 P4 스위치는 정상 플로우와 공격 플로우를 네트워크 플로우에 대한 지속적인 모니터링을 통해 해당 플로우를 분리시키는 역할만을 수행함으로써 즉각적인 패킷 차단 시 정상 플로우를 오인하여 차단함으로써 발생하는 이슈들을 해결할 수 있다.

또한 동적으로 오픈플로우를 통해 실시간으로 분산 DDoS 공격자 IP 혹은 공격 플로우에 대한 업데이트된 룰을 SDN 제어기로부터 P4 스위치가 수신하여, 동적인 플로우에 대한 제어 또한 가능하다. 추가적으로 P4 스위치에 연동되어 P4 스위치로부터 분산 DDoS 공격으로 의심되는 네트워크 플로우 정보를 수신하고 이를 차단하는 보안 장비와 해당 네트워크 전체를 제어하는 SDN 제어기를 연동함으로써, SDN 제어기에서 관리하는 분산 DDoS 공격자 정보를 보안 장비로부터 실시간으로 업데이트 받고 이를 다시 해당 네트워크의 다른 P4 스위치에 전파함으로써 보안을 위한 실시간 피드백 기반의 보안 운영 환경구축이 가능하다.

<표 1> 공격차단 대응방법 비교

	기존 방법	제안 방법
대응 방법	·방화벽, IPS, IDS 등 별도 보안장비 활용 (필요 시, SDN 제어기 기반 중앙제어)	·데이터평면에서의 P4 기반 보안 탐지 및 대응 ·제어평면에서의 SDN 제어기기반 보안 정책기반 중앙제어
장점	·기 개발된 전통적인 보안장비 활용 가능 ·기존 네트워크 구조 제한적 변경	·네트워크 단에서의 즉각적인 보안공격 탐지/대응 가능 ·10G/100G 이상 line-rate 수준 보안 처리 가능 *종단간(백본네트워크-캠퍼스네트워크-호스트) 적용 가능 ·다양한 정책기반 보안관리 ·스위치단 대응으로 보안공격에 따른 네트워크 부하 최소화
단점	·별도의 보안장비 필요 ·10G/100G 이상 line-rate 수준 보안 처리 불가능 *주로 캠퍼스 수준 네트워크 혹은 호스트 적용 ·제한적인 정책기반 보안 관리만 가능	·P4 등 데이터평면 프로그래머블 기술 확보 요구 ·고가의 P4 전용 ASIC 활용 ·Stateful 보안 정보 처리를 위한 메모리 확보 필요

조금 더 구체적으로 분산 DDoS 공격 차단 매커니즘을 살펴보면 P4 스위치에서 해당 네트워크 플로우의 패킷이 유효한 TCP SYN 정보를 가지고 있으면 해당 출력 포트로 포워딩하고 그렇지 않을 경우에는 분산 DDoS 공격 의심 플로우로 탐지한 후 해당 패킷의 TCP 포트 카운트 수를 증가시킨다. 증가된 TCP 포트 카운트가 특정 임계치를 넘어서면 이를 분산 DDoS 공격으로 최종적으로 판단하고 P4 스위치 자체에서 해당 패킷을 차단하거나 보안장비에 연동된 포트로 해당 패킷을 출력한다. 이를 위해 P4 스위치 내 SRAM의 출발지 IP 정보, 출발지 TCP 포트 정보, 목적지 IP 정보, 목적지 TCP 포트 정보를 하나의 엔트리로 표현되는 IP/포트 매치/액션 테이블 엔트리를 관리한다. 가장 최근 엔트리 정보와 신규로 들어오는 네트워크 플로우의 엔트리 정보를 비교한 후, TCP SYN Flood 공격 패턴이 특정 임계치를 초과할 경우, 분산 DDoS 공격으로 판단하고 해당 패킷을 차단하거나, 보안 장비에 연결된 특정 출력 포트로 보낸다.

3.2 스푸핑(Spoofing) 공격 차단 시나리오

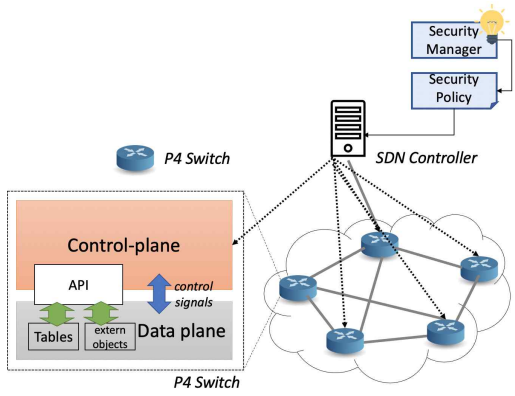
기존의 인터넷에서는 DHCP 스푸핑 공격, IP 스푸핑 공격, ARP 스푸핑 공격 등 다양한 형태의 공격이 존재한다. 대부분의 스푸핑 공격은 TCP/IP 인터넷 프로토콜에 정의된 MAC 주소와 IP 주소에 대한 조작 혹은 위장하는 기법으로 수행하기에 기존의 인터넷 프로토콜에 의해 동작하는 네트워크에서는 이를 차단하기 힘든 상황이다. 이에 P4 기반의 데이터 평면에서 해당 네트워크의 특정 DHCP 혹은 ARP 스푸핑 공격의 경우, 해당 DHCP 서버 혹은 네트워크에 정상 사용자의 IP와 MAC 정보에 대한 화이트리스트 기반 테이블을 유지 및 관리함으로써, IP 혹은 MAC 정보를 위장하는 공격자에 대하여 P4 기반의 프로그래머블한 스위치 단에서 즉각적으로 차단할 수 있다. 또한 화이트리스트에 속해 있지 않은 네트워크 내 노드의 경우, 네트워크 내 기존의 세션에 대한 하이잭킹을 통해 감청하거나 특정 노드에 대한 공격 시 P4 스위치 단에서 입력(ingress) 패킷 필터링을 통해 악의적인 패킷을 차단한다.

4. 정책 기반 인-네트워크 보안 관리 방법

4.1 정책 기반 인-네트워크 보안 관리 구조

본 논문에서 제시하는 SDN 데이터 평면 프로그래밍을 통한 정책 기반 인-네트워크 보안 관리 방법은 (그림 3)과 같이 네트워크의 플로우 정보에 대한 상태를 모니터링하고, 사용자 혹은 네트워크의 보안 정책에 기반하여 보안 의심 패킷 혹은 공격 패킷에 대하여 프로그래밍 가능한 P4 스위치 단에서 선제적으로 차단하는 것이다. 이때 P4 스위치로 구성된 네트워크에서 SDN 제어기는 보안 정책을 반영하는 역할만을 수행한다.

특정 분산 DDoS 공격 혹은 스푸핑 공격에 대한 정보를 RPC 기반 SDN 제어기로부터 P4 스위치에 전달하여, P4 스위치의 세션 매치/액션 테이블 엔트리 내 블랙리스트 혹은 화이트리스트를 업데이트하여, P4 스위치가 네트워크 내에서 특정 플로우에 대한 허용 및 차단을 가능하게 한다. 또한 P4 스위치 내 SRAM (Static random-access memory) 레지스터(Register)를 통해 네트워크 내 보안 위협 혹은 공격 플로우 정보에 대한 모니터링을 통해 최신의 보안 공격 정보를 바탕으로 신규 정책을 수립하거나 반영한다.



(그림 3) 정책 기반 인-네트워크 보안 관리 방법

P4 스위치 내 SRAM과 TCAM (Ternary Context Addressable Memory)을 통해 매치/액션 테이블을 구현하며, SRAM의 레지스터를 통해 모든 플로우 정보 모니터링을 수행한다. 레지스터는 패킷 당 라인속도로 동작하며, 최신의 플로우에 대한 정보를 가지고 있다. P4 스위치 내 매치/액션 테이블에서 모든 플로우에 대한 매치를 위한 키로 출발지 IP/Port, 목

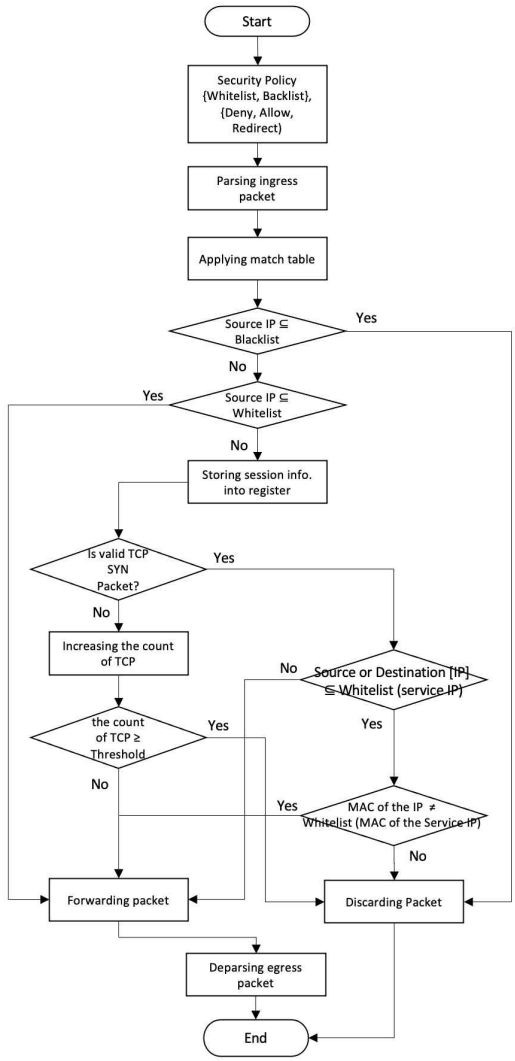
적지 IP/Port, 프로토콜 정보를 사용하며, 값으로는 차단(0)/허용(1)/리다이렉션(2)을 사용한다. 실제 매치 값에 해당하는 동작은 레지스터에 저장하여 유지한다. 정책 기반의 동적인 보안 위협 패킷의 차단을 위해 SDN 제어기를 통해 해당 보안 정책을 수신하여 해당 매치/액션 테이블 엔트리의 키와 값을 업데이트함으로써 스위치는 동적으로 보안 공격에 대응할 수 있도록 한다. 즉, SDN 제어기를 통해 블랙리스트 혹은 화이트리스트를 업데이트하여 네트워크 내 P4 스위치를 항상 최신의 보안 정책으로 운영할 수 있도록 한다.

4.2 인-네트워크 보안 관리 프로시저

본 논문에서 제안하는 P4 스위치에서 동작하는 인-네트워크 보안 관리 프로시저는 (그림 4)과 같이 입력 패킷 파싱(ingress packet Parsing), P4 매치/액션 테이블 적용, 블랙리스트 기반 차단, 화이트 리스트 기반 포워딩, 분산 DDoS 공격 대응, 스푸핑 공격 대응, 출력패킷 디파싱(egress packet deparsing) 등으로 진행되며, 이를 P4 언어를 통해 작성, 컴파일 그리고 P4 스위치에 로딩한다.

P4 스위치는 파싱과 매치/액션 적용 후 가장 먼저 블랙리스트를 기반으로 하여 선제적으로 보안 공격 패킷을 차단한다. 이는 이미 알려진 IP 혹은 이미 보안 정책으로 수립된 블랙리스트 IP를 기반으로 차단함으로써, 네트워크 내 이상 트래픽으로 인한 네트워크 혼잡을 최소화하고자 함이다. 다음으로 화이트리스트를 기반으로 하여, 신뢰 기반으로 이미 인증된 사용자에 대하여 선제적으로 허용하는 것이다. 이는 최근 데이터 집약형과학 등의 분야에서 대용량 플로우(elephant flow)에 기반한 빅데이터 전송이 증가하면서 신뢰 기반 협력을 위한 경우, 이미 인증된 사용자에 대해 선제적으로 해당 플로우 전달을 허용함으로써 더 이상 P4 스위치 내 해당 플로우 관련 패킷에 대한 처리에 드는 자원에 드는 비용(SRAM 내 레지스터 자원 등)을 최소화하기 위해서이다.

다음으로 분산 DDoS 공격 차단 프로시저를 살펴보면, 유효한 TCP SYN을 포함하지 않는 패킷의 경우, 해당 플로우에 대한 카운터를 증가시키며, 카운터 값이 특정 임계치를 초과하면 이를 보안 공격으로 간주하고 선제적으로 스위치에서 차단한다. 또한 스푸핑 공격의 경우, 네트워크 내 DHCP, DNS 등의 네트워크 서비스 혹은 해당 네트워크 내 인증된 사용자에 대한 IP 정보와 MAC 정보를 유지하면서, IP 정보 조작 혹은 MAC 정보에 대한 작위적인 조작임을 확인하면 이 또한 P4 스위치 단에서 즉각적인 대응을 통해서 차단한다.



(그림 4) 인-네트워크 보안 프로시저

추가적으로 모든 플로우 정보를 담고 있는 매치 테이블을 주기적으로 체크함으로써, 정상적이지 않은(inactive) 플로우 수를 점검함으로써 해당 세션에 대한 패킷을 리다이렉션 값을 태깅하여 우회시킬 수 있다.

5. 인-네트워크 보안 이슈

5.1 SDN 자체 보안 이슈

SDN에서는 제어 평면이 데이터 평면과 분리됨으로써 중앙 SDN 제어기를 통해 네트워크 전체의 중앙 집중적인 제어를 가능하게 하지만, 오히려 데이터 평면 즉 SDN 스위치가 공격 대상이 됨은 물론 중앙 SDN 제어기가 공격 대상이 되어, 분산 DDoS 공격, 패킷 조작 등의 사이버 공격으로 기존의 분산 네트워크 환경에서 보다 더 치명적인 네트워크 결함을 야기 시킬 수 있다[8][9]. SDN 제어기의 독립 및 복구 매커니즘 연구 등 이와 관련한 다양한 연구가 진행되고 있다.[10]

5.2 상태 기반 P4 프로그래밍 이슈

네트워크의 플로우 정보에 대한 모니터링을 기반으로 한 P4 스위치 단에서의 처리를 위해 해당 플로우의 상태를 저장할 수 있어야 한다. 수백만개 이상의 플로우 정보를 저장하기에는 P4 기반 토피노 칩의 경우, O(10MB) 수준의 SRAM이 장착되어 모든 플로우를 저장하는 것은 불가능하다. 즉 기존의 서버가 보통 O(10GB) 수준 이상의 DRAM (Dynamic random-access memory)을 활용하여 네트워크 기능을 수행하는 데 비해 아주 적은 용량이다. 이를 보완하기 위한 연구로써 NFV (Network functions virtualization) 클러스터 내의 값싼 DRAM을 활용하여 가상의 매치/액션 테이블을 구현하며, CPU의 개입 없이 외부 DRAM에 접근하여 최소한의 지연을 구현하고자 하는 TEA (Table Extension Architecture)가 제안되었다[11]. 추가적으로 기존의 서버 플랫폼과 같이 하나의 스위치 플랫폼에 토피노 등의 P4 칩, DRAM, FPGA 등을 동시에 장착한 후 FPGA를 통한 DRAM 제어기를 구현하고 PCIE 버스 등의 고속 버스로 연동하는 방법이 있다.

6. 결 론

본 논문에서는 데이터평면 프로그래밍 언어인 P4를 통해 분산 DDoS 공격, IP Spoofing 공격 등에 효과적으로 네트워크에서 처리할 수 있는 정책 기반 인-네트워크 보안 관리 방법을 제안하였다. 또한 SDN 제어기를 통해 사용자의 보안 정책을 네트워크 보안 정책에 반영할 수 있는 기법과 P4 기반의 인-네트워크 보안에 대한 SDN 자체 보안 및 P4 칩의 메모리 자원에 대한 이슈를 논의하였다.

향후 본 논문에서 제시한 정책 기반의 인-네트워크 보안 관리 방법을 P4 스위치에서 실제 구현함으로써 국가 과학기술연구망[12]의 100기가 이상의 하드웨어 속도에서의 보안 정책 기반 동적 보안 네트워크를 구현하고자 한다. 또한 분산 DDoS 공격, 스푸핑 공격 외의 다양한 보안 위협에 대처하기 위한 연구는 물론 피드백 기반의 자동 네트워크 보안 운영 환경 구축에 있어, AI 기술을 접목함으로써 정책 기반의 보안 자동 운영을 가능하게 하는 연구를 수행할 예정이다.

참고문헌

[1] S. Fichera, L. Galluccio, S. C. Grancagnolo, G. Morabito, and S. Palazzo, "OPERETTA: An OPEnflow-based REmedy to mitigate TCP SYNFLOOD Attacks against web servers," Computer Networks, Vol. 92, No. Part 1, pp. 89-100, 2015.

[2] W. J. A. Silva, "Avoiding inconsistency in OpenFlow stateful applications caused by multiple flow requests", International Conference on Computing, Networking and Communications (ICNC), pp. 548-553, 2018.

[3] M. Casado, T. Garfinkel, A. Akella, M. Freedman, D. Boneh, N. McKeown, and S. Shenker, “SANE: A protection architecture for enterprise networks”, 15th USENIX Security Symposium, 2006.

[4] M. Casado, M. J. Freedman, J. Pettit, J. Luo, N. McK- eown, and S. Shenker. “Ethane: Taking control of the enterprise”, ACM Special Interest Group on Data Communication (SIGCOMM), 2007.

[5] Qiao Kang, Lei Xue, Adam Morrison, Yuxin

Tang, Ang Chen, and Xiapu Luo, “Programmable In-Network Security for Context-aware BYOD Policies”, 29th USENIX Security Symposium, 2019.

[6] S. Hong, R. Baykov, L. Xu, S. Nadimpalli, and G. Gu. “Towards SDN-defined programmable BYOD (bring your own device) security”, Network and Distributed System Security Symposium (NDSS), 2016.

[7] F. Paolucci, F. Civerchia, A. Sgambelluri, A. Giorgetti, F. Cugini, and P. Castoldi, “P4 Edge Node Enabling Stateful Traffic Engineering and Cyber Security”, IEEE/OSA Journal of Optical Communications and Networking, Vol. 11, Issue 1, 2019.

[8] N. Narayanan, Ganesh C. Sankaran and Krishna M. Sivalingam, “Mitigation of security attacks in the SDN data plane using P4-enabled switches”, International Symposium on Advanced Networks and Telecommunication Systems (ANTS), 2019.

[9] R. Skowyra, L. Xu, G. Gu, T. Hobson, V. Dedhia, J. Landry, and H. Okhravi. “Effective topology tampering attacks and defenses in software-defined networks”, 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2018.

[10] T. Sasaki, A. Perrig, and D. E. Asoni, "Control-plane isolation and recovery for a secure SDN architecture," IEEE NetSoft Conference and Workshops (NetSoft), pp. 459-464, 2016,

[11] D. Kim, Z. Liu, Y. Zhu, C. Kim, J. Lee, V. Sekar, S. Seshan, “TEA: Enabling State-Intensive Network Functions on Programmable Switches, ACM Special Interest Group on Data Communication (SIGCOMM), 2020.

[12] 이명선, 조부승, 박형우, 김현철, “국가연구망의 발전방향 및 차세대 국가연구망 보안”, 제16권 제7호, pp.3-11, 2016.

[13] BAREFOOT NETWORKS, Tofino 2 Chip, https://www.barefootnetworks.com.

〔저자소개〕

조 부 승 (Buseung Cho)

2000년 2월 성균관대학교 전기전자 및 컴퓨터공학 학사
2002년 8월 성균관대학교 전기전자 및 컴퓨터공학 석사
2017년 2월 성균관대학교 컴퓨터공학 박사
2005년 6월 ~ 현재 한국과학기술정보연구원 책임연구원
2018년 3월 ~ 현재 과학기술연합대학원대학교 데이터 및 HPC과학 조교수
email : bscho@kisti.re.kr