SDN 기반 네트워크 공격 탐지 기법에 대한 동향 연구

홍지훈*, 정준권*, 정태명**
*성균관대학교 전자전기컴퓨터공학과
**성균관대학교 정보통신대학
e-mail:*{jhhong88, jkjung}@imtl.skku.ac.kr, **tmchung@ece.skku.edu

A Survey on Network Attack Detection Techniques Based Software-Defined Network

Ji-Hoon Hong*, Jun-Kwon Jung*, Tai-Myoung Chung**
*Dept. of Electrical and Computer Engineering, SungKyunKwan University
**College of Information and Communication Engineering, Sungkyunkwan University

요 약

최근 클라우드 서비스의 발전으로 인해 네트워크 트래픽이 폭발적으로 증가함에 따라 네트워크를 보다 효율적으로 관리하는 방법들에 대한 필요성이 제기되었고 해결책으로 소프트웨어 정의 네트워크(Software-Defined Network: SDN)가 제안되었다. 네트워크 구조가 기존보다 효율적인 SDN으로 변화함에 따라 보안 기술들도 함께 변화하고 있는데 본 논문에서는 보안 기술들 중 SDN을 이용한 네트워크 공격 탐지 기법들을 패킷 분석 기반과 임계값 기반으로 분류하고 보안성과 자원 사용에 대한 효율성 측면에서 분석하였다. 본 논문의 분석 결과를 통해 앞으로의 SDN 기반 네트워크 공격 탐지 기법들의 연구 방향을 제시하고 향후 새로운 SDN 기반 네트워크 공격 탐지 기법 연구와 탐지 시스템 구현에 기틀을 마련한다.

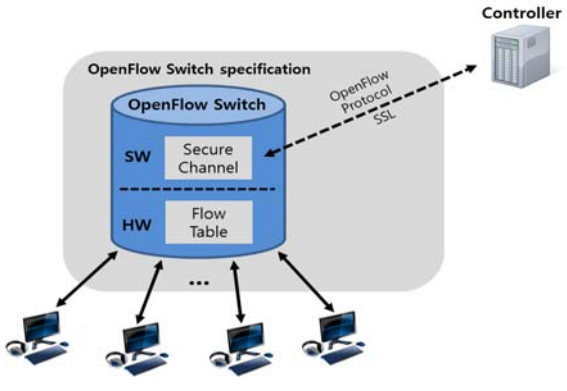
1. 서론

최근 클라우드 서비스의 발전으로 인해 네트워크 트래픽이 폭발적으로 증가함에 따라 네트워크를 보다 효율적으로 관리할 수 있는 방법들에 대한 연구가 활발히 진행되고 있다. 연구의 일환으로 기존 네트워크가 가지는 관리의 비효율성을 해결함과 동시에 추가적으로 네트워크 구조의 복잡성 네트워크 장비를 생산하는 벤더에 대한 의존성을 중앙 통제 방식으로 해결 할 수 있는 소프트웨어 정의 네트워크(Software-Defined Network: SDN)가 제안되었고 현재 많은 주목을 받고 있다. 또한, 국제 표준화 기구인 ITU-T, IETF, ONF(Open Networking Foundation) 등에서 SDN과 관련하여 표준화 작업 및 표준 제정을 추진함에 따라 그 관심도는 더욱 높아지고 있는 추세이다[1]. 한편, ONF에서는 SDN 표준화 과정 중 고려해야하는 보안 사항들을 Network Security Challenges-Security Solutions에서 정리하며 SDN으로 네트워크 구조가 변화하면서 동시에 보안기술들 또한 변화되어야 함을 강조하였다[2]. 기존 네트워크에서는 개인정보보호를 위해 네트워크 공격을 탐지하기 위한 솔루션으로 IDS(Intrusion Detection System)를 사용하고 있다. 본 논문에서는 SDN 환경에서 네트워크에 대한 공격을 탐지하는 기법들을 분류하여 보안성 측면과 SDN 자원 사용의 효율성 측면으로 분석한다. 분석 결과를 통해 향후 SDN 기반 네트워크 공격 탐지 기법 연구와 탐지 시스템 구현에 기여한다.

본 논문의 구성은 다음과 같다. 2장에서는 SDN의 기본적인 개념을 설명하고 3장에서는 SDN을 기반으로 한 네트워크 공격 탐지 기법들을 패킷 분석과 임계값 기반으로 분류한 후 해당되는 기법들을 분석한다. 4장에서는 3장의 분석을 통해 얻은 결과를 정리하고 마지막으로 5장에서는 분석 결과에 기반해 향후 연구 과제로 새로운 SDN기반 네트워크 공격 탐지 방법을 제시하여 앞으로의 SDN기반 네트워크 공격 탐지 시스템을 연구하고 개발하는 기틀을 마련한다.

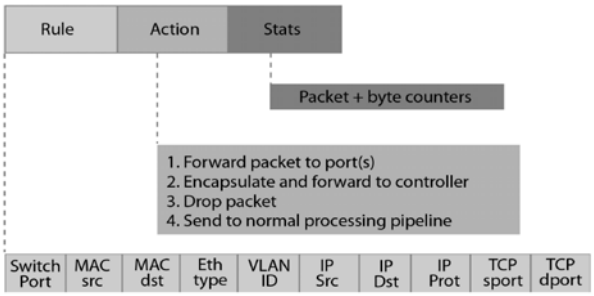
2. SDN의 개념

SDN은 기존 네트워크 포워딩 장치의 기능을 패킷 포워딩기능과 제어 기능으로 분리한 기술이다[3]. (그림 1)과 같이 SDN은 제어기능을 담당하는 컨트롤러, 통신에 사용되는 OpenFlow프로토콜과 포워딩 기능을 담당하는 OpenFlow스위치로 구성되어있다[4].



(그림 1) SDN의 구성[4]

SDN 환경에서 네트워크 관리자는 패킷의 유출입 흐름을 지정해주는 컨트롤러의 소프트웨어를 직접 프로그래밍 할 수 있으며 포워딩 장치마다 존재하는 FlowTable을 이용해 패킷의 흐름을 제어하고 흐름에 대한 통계분석도 가능하다. FlowTable은 (그림 2)와 같이 패킷의 헤더정보 중 어떤 정보를 수집할지에 대한 Rule, 수집한 패킷을 어떻게 처리할지에 대한 Action, 흐름 통계 Statistics 로 구성되어 있다.



(그림 2) FlowTable의 구성[4]

3. SDN기반 네트워크 공격 탐지 기법 분석

본 장에서는 SDN기반 네트워크 공격 탐지 기법들을 탐지 방법에 따라 패킷 분석 기반과 임계값 기반의 두 가지 분류로 나누어 분석한다. SDN을 기반으로 한 네트워크 공격 탐지 기법들은 기존의 네트워크에서 사용되던 침입 탐지 알고리즘들을 SDN의 자원을 이용해 재구현한 기법들이다. 여기서 SDN의 자원이란 SDN의 구성을 이루는 컨트롤러, OpenFlow스위치, FlowTable과 같은 하드웨어 장치나 소프트웨어 등 이다.

3.1 패킷 분석 기반 탐지 기법

패킷 분석 기반 탐지 기법은 유입되는 패킷에 대한 페이로드정보나 헤더정보의 분석을 통해 네트워크 공격 유무를 판단하는 기법을 말한다. 이 기법에는 알려진 공격 패턴 정보와 유입되는 패킷을 비교 분석하는 기법과 필터링을 이용해 유해패킷을 분석하고 분류해내는 기법이 있다.

3.1.1 OpenFlow스위치 모듈을 이용한 탐지 기법

Kumar외 1명은 OpenFlow스위치에 하드웨어 모듈을 추가하여 네트워크 공격을 탐지하는 기법을 제안했다[5]. 추가된 하드웨어 모듈은 두 가지의 정보를 포함한다. 이 정보는 의심스러운 IP들(IDS IP InfoTable)과 알려진 공격의 패턴 정보(IDS 데이터베이스)이다.

패킷이 스위치로 유입 되면 의심스러운 IP정보를 가진 테이블을 블랙리스트 기반으로 비교한다. 이 후 패킷이 공격 인지 판단하기 위해 패턴 매칭 알고리즘을 이용하여 IDS 데이터베이스와 비교, 분석한다. 만약 해당 패킷이 공격으로 판단 될 경우 패킷의 헤더에 포함되어있는 출발지 IP주소를 IDS IP InfoTable에 추가하고 패킷을 폐기한다.

이 기법은 컨트롤러의 제어 없이 스위치에 추가된 하드웨어 모듈을 사용하기 때문에 빠른 분석이 가능하다는 장점이 있다. 하지만 알려진 공격 패턴 데이터베이스를 사용하기 때문에 알려진 공격만 탐지가 가능하다는 단점도 있다.

3.1.2 필터링을 이용한 탐지 기법

Mehdi외 3명은 Mahoney외 1명이 제안한 유해 패킷 필터링 기법을 SDN환경에서 구현하고 평가했다[6,7]. 이 기법은 먼저 스위치로 들어오는 패킷을 컨트롤러로 전송하고 컨트롤러 내에서 IP, TCP, Telnet, FTP, SMTP, HTTP 프로토콜 패킷들로 분류한다. 이 후 분류한 패킷의 페이로드에 유해 패킷 필터링 기법을 적용해 필터링되는 패킷을 공격 패킷으로 판단한다.

이 기법은 유입된 패킷의 페이로드를 공격 패턴 데이터베이스와 비교 분석하는 기법보다 분석을 위한 단계가 적다는 장점이 있다. 하지만 OpenFlow스위치 모듈을 이용한 탐지 기법과 마찬가지로 알려진 공격만 탐지가 가능하다는 단점도 있다.

3.2 임계값 기반 탐지 기법

임계값 기반 탐지 기법은 미리 임계값을 지정해놓고 그 값의 초과여부를 통해 네트워크 공격의 유무를 판단하는 기법이다. 임계값은 사전의 실험을 통해 얻거나 관리자가 네트워크의 보안강도에 따라 지정하여 사용한다. 이 기법에는 IP 주소, 포트번호 등의 정보들을 각각 카운트하여 임계값과 비교하는 기법과 관리자가 큐의 최대 길이와 주기를 지정하고 주기마다 큐의 길이를 측정하여 임계값과 비교하는 기법이 있다.

3.2.1 TRW-CB 알고리즘을 이용한 탐지 기법

Mehdi외 3명은 TRW-CB(Threshold Random Walk with Credit Based Rate Limiting) 알고리즘을 이용하여 네트워크 공격의 전 단계인 악성 웜의 전파를 탐지하고 전파하려는 호스트를 차단하는 기법을 제안했다[6]. 여기서 TRW-CB는 단계별로 입력된 값과 임계값을 비교해주는 알고리즘이다[8].

TRW-CB 알고리즘을 이용한 탐지 기법은 스위치에 플로우가 생성되어있지 않은 내부호스트가 외부호스트로 보내는 TCP-SYN 패킷들을 모두 컨트롤러로 전송한다. 컨트롤러에서는 내부호스트가 수신해야하는 ACK 패킷을 대신 받는다. 이 후 연결 설정 단계를 진행하며 TRW-CB 알고리즘을 이용해 연결 과정 동안에 관리자가 지정한 지연시간 임계값 초과 여부를 분석한다. 임계값을 초과할 경우 악성 행위 가능성이 있는 호스트와의 연결이라고 판단하고 해당 호스트를 차단한다.

이 기법은 연결 설정 과정에서 미리 공격 여부를 판단하고 해당 호스트를 차단한다는 장점이 있으나 새로운 연결에 대한 처리와 공격 탐지 등에 대한 모든 동작을 컨트

롤러에서 담당하기 때문에 부하가 발생할 수 있다.

지정해놓은 길이를 넘어서는 경우 공격으로 판단한다.

<표 1> SDN기반 네트워크 공격 탐지 기법 비교

기법	탐지하는 공격의 범위	탐지에 사용되는 SDN자원	탐지 방법	기반
OpenFlow Switch 모듈	알려진 공격	OpenFlow스위치	사전에 알고있는 공격 패턴과 패킷 페이로드를 비교 분석	패킷 분석
필터링	알려진 공격	FlowTable, 컨트롤러	분류를 거친 패킷의 페이로드에 유해 패킷 필터링을 적용하여 비교 분석	
TRW-CB 알고리즘	웜의 전파	FlowTable, 컨트롤러	두 호스트의 연결설정 동안의 지연시간과 연결설정 성공 가능성 측정 및 지연시간의 임계값 초과 여부를 확인	임계값
OpenFlow, sFlow	DDoS, 웜의 전파, 포트스캔	FlowTable, 컨트롤러	sFlow를 이용하여 패킷을 수집, 샘플링한 후 사전에 실험을 통해 얻은 Attack Rate를 임계값으로 지정하여 초과 여부를 확인	
Rate Limiting	SYN Flooding	FlowTable	패킷을 지연 큐에 넣고 지연 큐의 길이를 임계값으로 지정하여 초과 여부를 확인	
Maximum Entropy	포트스캔	FlowTable, 컨트롤러	패킷의 포트번호를 기준으로 하여 클래스를 나누고 카운트하여 t초마다 임계값의 초과여부를 확인	

3.2.2 OpenFlow와 sFlow를 이용한 탐지 기법

Giotis는 OpenFlow와 sFlow를 이용하여 DDoS, 웜의 전파, 포트스캔공격을 탐지할 수 있는 기법을 제안했다[9]. sFlow는 패킷 수집 및 트래픽 분석의 기능을 하는 플로우 모니터링 기법이다[10]. sFlow는 네트워크 장비에 유입되는 패킷에서 필요한 정보만을 추출하여 지정된 서버나 기기로 전송해주는 기능과 전체 유입되는 패킷들 중 얼마만큼의 패킷에서 정보를 추출할지 수치를 지정하는 Sampling Rate기능, 추출한 정보들을 카운트하는 기능 등을 가지고 있다. 이 기법은 sFlow기능을 지원하는 OpenFlow스위치에 유입되는 패킷들 중 출발지/목적지 IP 주소, 출발지/목적지 포트번호의 네 가지 정보들을 추출하여 화이트리스트에서 비교하는 단계를 거친다. 이 후 네 가지 정보들을 각각 카운트한 값이 지정된 Attack Rate를 넘어서는 경우 공격으로 판단하는 기법이다. 여기서 Attack Rate는 네트워크의 대역폭에 따라 다르며 sFlow의 Sampling Rate기능을 이용한 실험을 통해 얻은 통계적 데이터로 지정 된다.

이 기법은 sFlow의 데이터 수집기능과 Sampling Rate 기능을 사용하여 트래픽 분석과 함께 이상 트래픽까지 검출할 수 있다는 장점이 있다. 하지만 sFlow에서 수집하는 패킷 데이터들은 OpenFlow에서도 FlowTable 작성을 위해 수집되기 때문에 정보 수집 과정이 두 번 필요하다는 단점도 있다.

3.2.3 Rate Limiting을 이용한 탐지 기법

Mehdi외 3명은 Rate Limiting을 이용한 네트워크 공격 탐지 기법을 제안했다[6]. 이 기법은 스위치에 유입되는 특정 호스트에 대한 새로운 연결요청 패킷들을 화이트리스트기반 워킹셋에서 비교하는 단계를 거친 뒤 스위치의 지연 큐에 저장한다. 지연 큐를 관리하는 Rate Limiter는 일정주기마다 저장된 패킷들 중 제일 오래된 패킷과 동일한 수신IP주소를 가진 패킷들을 묶어서 호스트에게 전송한다. 지연 큐를 감시하는 Queue Length Detector는 패킷이 큐에 저장될 때마다 지연 큐의 길이를 검사하여 미리

이 기법은 유입되는 패킷을 모두 지연 큐에 넣어 관리함에 따른 장단점이 있는데 장점은 패킷이 호스트로 지연 전달됨에 따라 DDoS같은 공격을 효과적으로 탐지하고 막을 수 있다는 것이다. 단점은 정상적인 패킷도 지연 전달되기 때문에 호스트의 입장에서는 서비스가 지연된다는 것이다.

3.2.4 Maximum Entropy를 이용한 탐지 기법

Mehdi외 3명은 Maximum Entropy를 이용한 네트워크 공격 탐지기법을 제안했다[6]. 이 기법은 Dhadialla외 1명이 제안한 클래스 분류 기반 탐지 기법에 기반 한다[11]. 이 기법은 TCP와 UDP의 SYN, RST가 각각 547개의 포트, 총 2,348개의 클래스로 분류하는 것을 시작으로 한다. 이 후 OpenFlow스위치의 FlowTable을 이용하여 각 클래스에 해당하는 포트번호를 카운트하고 일정 주기마다 2,348개 클래스의 카운트 값을 컨트롤러로 전송, 컨트롤러에서 미리 지정해놓은 Maximum값과 비교하여 초과하는 경우 해당 포트(클래스)에 대한 공격으로 판단하는 기법이다. 관리자는 네트워크의 중요도에 따라 주기값인 t초와 Maximum값을 지정한다.

이 기법은 카운트 값을 컨트롤러로 전송하는 주기를 너무 길게 설정할 경우 이미 네트워크가 공격받은 이 후 일 가능성이 높기 때문에 탐지라는 기능이 무의미해지며 반대로 너무 짧게 지정할 경우 컨트롤러로 전송되는 카운트 값들에 의해 네트워크에 혼잡이 발생할 가능성이 있다.

4. 분석 결과

SDN기반 네트워크 공격 탐지 기법들을 분석한 결과는 <표 1>로 나타낼 수 있다. 각 탐지 기법들은 탐지 방법에 따라 패킷 분석 기반과 임계값 기반으로 분류되었다. 보안성 측면에서 결과를 정리하면 다음과 같다. 패킷 분석 기반과 임계값 기반으로 분류된 기법들은 각각 공통적인 장단점이 있다. 그 내용은 <표 2>와 같이 정리할 수 있다. 먼저 패킷 분석 기반 탐지 기법들은 이미 알려진 공격 패턴에 대해서는 빠른 탐지가 가능하다는 장점과 패턴이 알

려지지 않은 공격에 대한 탐지는 불가능 하다는 단점이 있다. 임계값 기반 탐지 기법들은 네트워크의 중요도에 따라 임계값을 지정하여 사용할 수 있다는 장점과 공격 여부를 판단하는 기준이 관리자가 지정한 임계값에 의존한다는 단점이 있다.

<표 2> 패킷 분석과 임계값 기반 탐지 기법 장단점

기반	장점	단점
패킷 분석	패턴이 알려진 공격에 대한 탐지가 빠름	패턴이 알려지지 않은 공격에 대한 탐지가 불가능
임계값	네트워크의 보안적인 중요도에 따라 임계값을 지정	공격 여부를 판단하는 기준이 관리자가 지정한 임계값에 의존

SDN 자원 사용에 대한 효율성 측면에서 결과를 정리하면 다음과 같다. 모든 기법들은 탐지를 위해 SDN의 자원인 컨트롤러나 OpenFlow스위치, FlowTable을 이용한다. 하지만 그 중 패킷 분석을 기반으로 한 공격 탐지 기법들은 SDN의 자원을 패턴 매칭을 위해서만 사용한다는 것을 알 수 있었다. 그에 반해 임계값을 기반으로 한 공격 탐지 기법들은 SDN의 자원을 임계값 지정을 위한 수단으로 사용하는데 이 말은 즉, 공격을 탐지하는 데에 패킷 분석 기반 기법들보다 임계값 기반 기법들이 SDN의 중앙 통제 방식 특성을 더 효율적으로 사용했다는 것이다.

5. 결론

본 논문에서는 SDN을 기반으로 한 네트워크 공격 탐지 기법들을 탐지 방법에 따라 패킷 분석 기반과 임계값 기반으로 분류하고 보안성 측면과 SDN 자원 활용에 대한 효율성 측면으로 분석해 보았다. 분류에 따라 향후 SDN 기반 네트워크 공격 탐지 기법 연구에서는 다음 사항들을 고려해야한다. 패킷 분석을 기반으로 한 탐지 기법들은 알려지지 않은 새로운 공격패턴의 지속적인 갱신이 필요하며 이때, 공격에 대해 자동으로 패턴을 생성하는 기법들이 사용될 수 있겠다[12,13]. 또한 SDN의 자원을 효율적으로 사용하는 방안에 대한 연구가 필요하겠다. 그리고 임계값을 기반으로 한 탐지 기법들은 공격 여부를 판단하는 기준이 되는 임계값을 지정해주는 알고리즘이 필요한데 여기에 패킷 모니터링 기법이 사용될 수 있겠다[14,15].

향후 연구로는 알려진 공격에 대한 패턴 매칭을 1차 탐지로 하고 네트워크 중요도에 따른 임계값 초과 여부를 2차 탐지로 하여 탐지율에 특화된 새로운 탐지 기법을 연구하고 그에 따른 오탐율과 미탐율 분석을 통해 새로운 SDN기반 네트워크 공격 탐지 시스템을 개발하는데에 기틀을 마련한다.

참고문헌

[1] 이승익 “소프트웨어 정의 네트워킹(SDN) 표준화 동향”, ETRI 표준연구센터, 2014.

[2] ONF "SDN Security Considerationsin the Data Center“ ONF Solution Brief, 2013.

[3] McKeown, Nick, "Openflow: enabling innovation in campus networks." ACM SIGCOMM Computer Communication Review, 38.2, 69-74, 2008.

[4] N. McKeown, “openflow (Why Can’t I innovate in my Wiring Closet?),” www.openflow.org/documents/openflow.ppt

[5] Kumar, Suresh, "Open flow switch with intrusion detection system." International J. Schientific Research Engineering & Techonology (IJSRET), 1-1-4, 2012.

[6] Mehdi, Syed Akbar, Junaid Khalid, and Syed Ali Khayam. "Revisiting traffic anomaly detection using software defined networking." Recent Advances in Intrusion Detection, Springer Berlin Heidelberg, 2011.

[7] Mahoney, Matthew V. "Network traffic anomaly detection based on packet bytes", ACM, Proceedings of the 2003 ACM symposium on Applied computing, 2003.

[8] Schechter, Stuart E., Jaeyeon Jung, and Arthur W. Berger, "Fast detection of scanning worm infections" Recent Advances in Intrusion Detection, Springer Berlin Heidelberg, 2004.

[9] Giotis K, "Combining Openflow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments", 2013.

[10] Wang, Mea, Baochun Li, and Zongpeng Li, "sFlow: Towards resource-efficient and agile service federation in service overlay networks", 24th International Conference on IEEE, 2004.

[11] Dhadialla, Prabhjot S, "Maximum-entropy network analysis reveals a role for tumor necrosis factor in peripheral nerve development and function", National Academy of Sciences, 106.30, 12494-12499, 2009.

[12] De Ocampo, Frances Bernadette, Trisha Mari Del Castillo, and Miguel Alberto Gomez. "AUTOMATED SIGNATURE CREATOR FOR A SIGNATURE BASED INTRUSION DETECTION SYSTEM (PANCAKES)." The Second International Conference on CyberSec2013(The Society of Digital Information and Wireless Communication, 2013.

[13] Yin, Pu Tian, Rao Zheng Chan, and Qin Zheng, "Network Attack Characteristics of Automatic Data Extraction Technology", Advanced Materials Research 765 1245-1248, 2013.

[14] Kamijo, Shunsuke, et al. "Traffic monitoring and accident detection at intersections", IEEE Transactions on 1.2(Intelligent Transportation Systems), 108-118, 2000.

[15] Cucchiara, Rita, Massimo Piccardi, and Paola Mell,. "Image analysis and rule-based reasoning for a traffic monitoring system.", IEEE Transactions on 1.2(Intelligent Transportation Systems), 119-130, 2000.