SDN 과 Honeypot 을 활용한 DoS 공격 차단 기법

문성식, 김미희*
한경대학교 컴퓨터웹정보공학과
door55ik@gmail.com, mhkim@hknu.ac.kr

DoS Attack Defense Using SDN and Honeypot

Sungsik Mun, Mihui Kim*
*Department of Computer & Web Information Engineering, HanKyong National University

요 약

SDN(Software Defined Networking)은 효율적인 방법과 저렴한 비용으로 네트워크를 직접 프로그램 하여 즉각적인 제어를 할 수 있다. 본 논문에서는 SDN 의 특성을 활용, SDN 구성요소인 컨트롤러와 스위치를 활용하여 공격 정보를 수집하고 이를 기반으로 공격을 탐지하는 위협 레벨 관리 모듈, 공격 탐지 모듈, 패킷 통계 모듈 등을 설계하여 프로그래밍하고 허니팟을 적용하여 서비스 거부(DoS, Denial of Services)공격을 차단하는 방법을 제시한다.

1. 서론

서비스 거부 (DoS, Denial of Services) 공격은 사용자의 자원을 고갈시켜 시스템의 작동을 방해하려 하는 악의적인 행위로서 이를 해결하기 위한 다양한 연구가 수행되어 왔다[1]. 기존 연구 [2]에서는 DoS 공격에 대한 N-IDS 를 이용한 탐지 방법을 제시하였다. 하지만 침입 탐지 시스템 (IDS)은 추가적인 장비를 필요로 하고 IDS 의 네트워크에서의 위치에 따라 관점이 달라질 수 있다는 단점이 있다[3]. 연구 [4]에서는 SDN 을 활용하여 DoS 공격을 완화시키는 두 가지 방법인 FLOWSEC 기법과 BLACKBOX 기법을 제시하였다. FLOWSEC 은 정상적인 패킷 또한 차단할 가능성이 크고 BLACKBOX 는 지능적인 공격자가 차단 기법을 파악하여 이를 우회하여 공격할 수 있는 가능성이 있다.

최근, 기술의 발달로 급증하는 데이터에 의해 네트워크 관리는 더욱 어려워졌고, 이러한 관리의 효율성을 향상시키기 위해 SDN(Software Defined Networking) 기술이 고안되었다[5]. SDN 스위치는 유연한 패킷 제어를 위해 네트워크 동작을 프로그래밍할 수 있도록 설계되었다. SDN 은 관리자가 기민한 트래픽 분석을 가능하게 하고, 네트워크 동작을 직접 프로그래밍할 수 있게 한다. 따라서 많은 데이터를 간단하고 효율적으로 처리할 수 있는 장점을 가진다.

본 논문에서는 이러한 SDN 의 특성을 활용하여 DoS 공격을 차단하는 방법을 제시한다. 이는 SDN 구성요소인 컨트롤러와 스위치를 활용하여 공격 정보를 수집하고 이를 기반으로 공격을 탐지하며 효율적으로 DoS 공격을 차단한다. 각각의 SDN 컨트롤러와 스위치에는 프로그래밍된 위협 레벨 관리 모듈, 공격 탐지 모듈, 패킷 통계 모듈 등을 배치하여 DoS 공격을 분석하고 차단한다. 또한 공격 패킷은 허니팟으로 전달하여 분석하고 분석된 정보는 컨트롤러에 전달하여 공격 탐지 기준에 적용되는 시스템을 제안한다.

2. 관련 연구

2. 1. SDN

SDN 은 통합되어 있던 데이터 플레인(Data plane)과 제어 플레인(Control plane)을 분리하여 컨트롤 부분을 중앙 집중하고 네트워크 동작을 프로그램화 하여 효율적인 제어를 할 수 있도록 하였다. SDN 은 SDN 컨트롤러와 SDN 스위치로 구성되고 SDN 프로토콜을 통해 통신하며 Flow Rule 을 통해 데이터 패킷을 처리한다. 이는 관리자가 기민한 트래픽 분석을 가능하게 하고 직접 프로그래밍을 할 수 있으며 많은 데이터를 간단하고 효율적으로 처리할 수 있도록 한다[6].

본 논문에서는 SDN 의 특징인 유연한 패킷 제어를 활용해 효율적으로 DoS 공격을 탐지하고 차단하는 기법을 제안한다. 제안된 구조는 스위칭과 모니터링 기능을 함께 할 수 있는 SDN 스위치[7]를 사용하며, IDS 등을 사용하는 기존 기법 대비 작은 오버헤드로 DoS 공격을 탐지 및 차단할 수 있다.

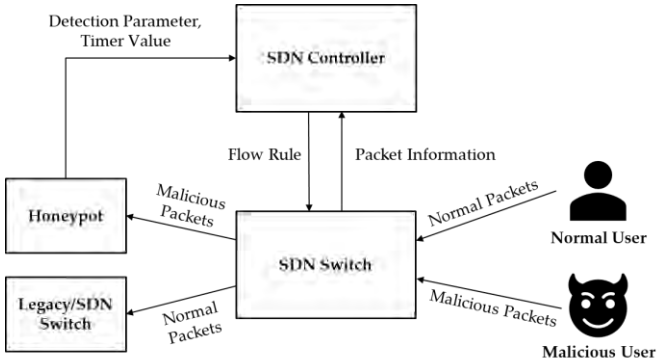
2. 2. 기존 연구

기존 연구로서 Snort, WinPCap 등을 활용하여 N-IDS 를 구축함으로써 DoS 공격을 탐지하고 차단하는 방법이 제시되었다[2]. 하지만 침입 탐지 시스템(IDS)은 추가적인 장비를 필요로 하고, IDS 가 네트워크 상에서 어느 부분에 위치하는지에 따라 관점이 달라질 수 있다는 문제가 있다[3].

또 다른 기존 연구로서 SDN 컨트롤러에 대한 DoS 공격을 완화하기 위해 FLOWSEC 과 BLACKBOX 를 이용한 방안이 제안되었다[4]. FLOWSEC 은 공격자가 시간당 전송할 수 있는 패킷에 수를 제한하여 공격을 완화시키고자 하였지만 이는 일반적인 사용자의 패킷 또한 제한할 수 있는 문제점을 가지고 있다. BLACKBOX 는 위협이 되는 단계를 정의하는 유한 상태 머신을 활용하여 공격을 차단하는 방법을 고안하였다. 하지만 지능적 공격자가 방어의 동작을 파악하여 이를 피해 공격을 할 수 있는 약점이 있고 본 논문에서는 BLACKBOX 에서 제시한 유한 상태 머신을 활용하고 허니팟이라는 공격 우회 장치를 추가하여 더욱 동적으로 공격에 대응할 수 있는 방법을 제시한다. 허니팟을 사용하여 공격 탐지 시스템의 탐지 기준 등을 조정함으로써 지능적 공격에도 유연하게 대응할 수 있다[8].

3. 제안 시스템

3. 1. 제안 시스템 구조

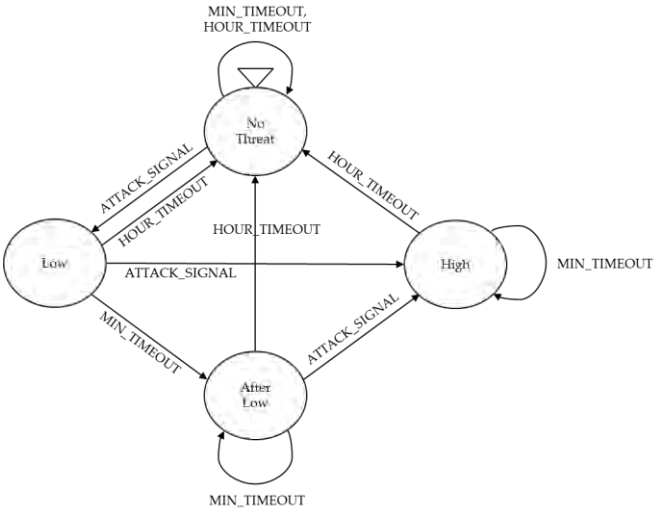


(그림 1) 제안 시스템 구조도.

(그림 1)은 본 논문에서 제안하는 시스템의 구조를 도식화한 것이다. 제안 시스템은 SDN 컨트롤러와 SDN 스위치, 허니팟, 사용자으로 구성된다. 사용자는 정상 사용자와 악의적 사용자로 구분할 수 있다. SDN 컨트롤러는 SDN 스위치가 수집한 트래픽 정보를 기반으로 악의적 사용자를 판단하고, 악의적 사용자의 트래픽을 폐기하는 플로우 규칙을 생성한다. SDN 스위치는 트래픽 정보를 수집하여 SDN 컨트롤러로 전달하고, 플로우 규칙에 따라 트래픽을 포워딩한다. 허니팟은 악의적 사용자에 대한 정보를 수집해 이를 기반으로 적응형 공격 탐지를 수행할 수 있도록 한다.

3. 1. 1. SDN 컨트롤러

SDN 컨트롤러는 공격 탐지 모듈(Attack Detection Module)과 플로우 규칙 생성기(Flow Rule Generator), 위협 레벨 관리 모듈(Threat Level Management Module)을 포함한다. 공격 탐지 모듈은 SDN 스위치가 수집한 패킷 데이터를 기반으로 악의적 사용자를 판단한다. 단위 시간 당 특정 사용자로부터 발생한 패킷의 수가 정해진 기준보다 많은 경우, 해당 사용자를 악의적 사용자로 판단하고 허니팟 유도 플로우를 생성한다. 플로우 규칙 생성기는 악의적 사용자의 패킷을 허니팟으로 유도하기 위한 플로우 규칙을 생성한다.



(그림 2) BLACKBOX 에서 사용된 유한 상태 머신[4]

(그림 2)는 논문 [4]에서 제안된 BLACKBOX 의 유한 상태 머신이다. 본 논문은 이를 활용하여 컨트롤러의 위협 레벨 관리 모듈로 사용하였다. 위협 레벨 관리 모듈은 공격이 탐지되면 위협 레벨을 조정한다. 위협 레벨 관리 모듈의 위협 레벨은 위협 없음(No Threat), 낮은 위협(Low), 경계(After Low), 높은 위협(High)로 구분되며, 위협 레벨에 따라 공격 탐지 기준을 다르게 조정함으로써 다양한 공격 상황에 유연하게 대응할 수 있도록 한다. 초기 상태인 위협 없음 단계에서 최초 공격이 탐지된 경우 위협 수준을 낮은 위협로 변경하고, 분 단위 타이머와 시간 단위 타이머를 가동한다. 분 단위 타이머는 각 위협 레벨 간의 상태 전이의 기준이 되는 타이머로, 세밀한 위협 레벨 조정을 위해 사용한다. 시간 단위 타이머는 공격 여부에 따른 상태 전이의 기준이 되는 타이머로, 현재의 위협 레벨이 어느 단계에 있더라도 시간 단위 타이머가 종료되면 더 이상 공격 위협이 없는 것으로 판단하고 위협 레벨을 위협 없음(No Threat)으로 변

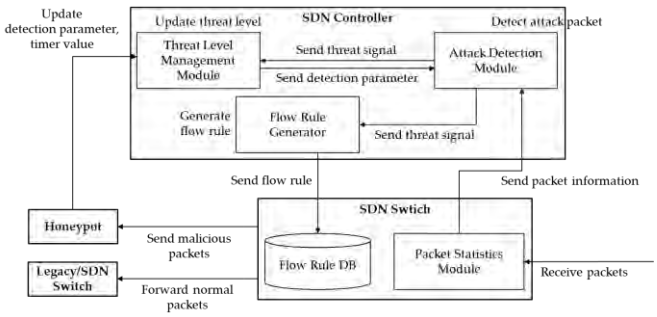
경한다. 각 타이머의 타임아웃 값은 네트워크 관리자가 적절한 값으로 설정한다. 위협 수준 Low 단계에서 추가 공격이 탐지되면 위협 수준을 High 로 조정한다. 추가 공격이 감지되지 않고 분 단위 타이머가 종료된 경우, 위협 수준을 After Low 로 조정한다. 위협 수준 After Low 단계에서 추가 공격이 탐지되면 위협 수준을 High 로 조정한다. 추가 공격이 감지되지 않고 시간 단위 타이머가 종료된 경우 위협 수준을 No Threat 로 조정한다. 위협 수준이 High 인 경우 높은 수준의 공격 탐지를 수행하고, 시간 단위 타이머가 종료되면 위협 수준을 No Threat 로 조정한다.

허니팟은 공격 탐지 모듈이 공격으로 판단한 패킷을 수집하고 이를 분석한다. 공격자들의 공격 패턴, 시간 유형들을 분석하고 이를 바탕으로 SDN 컨트롤러에 포함된 위협 레벨 관리 모듈의 타이머를 조정한다.

3. 1. 2. SDN 스위치

SDN 스위치는 패킷 수집 모듈과 플로우 규칙 데이터베이스를 포함한다. 패킷 수집 모듈은 사용자들의 패킷을 수집하여 SDN 컨트롤러로 전송한다. 플로우 규칙 데이터베이스는 SDN 컨트롤러부터 전송받은 플로우 규칙을 저장한다. SDN 스위치는 플로우 규칙 데이터베이스에 저장된 플로우에 따라 스위치로 들어오는 패킷을 포워딩 한다. 플로우 규칙 데이터 베이스는 기본적으로 모든 패킷을 다음 스위치로 전달하는 포워딩 플로우를 포함한다. 공격 패킷 폐기 규칙은 포워딩 플로우보다 높은 우선순위를 가지도록 생성되어 악의적 사용자의 패킷이 목적지로 전달되지 않도록 한다.

4. 2. 공격 탐지 흐름



(그림 3) 공격 탐지 및 차단 흐름도

사용자로부터 패킷이 수신되면 패킷 수집 모듈은 패킷 정보를 SDN 컨트롤러로 전달한다. 패킷 정보는 패킷의 송신자 주소, 패킷 종류, 플래그를 포함한다. 플래그는 SYN Flooding 공격 등 플래그를 사용한 DoS 공격에 사용한다. 패킷 전체를 전달하는 대신, 패킷 일부만을 전달함으로써 트래픽 부담을 최소화할 수 있다. SDN 컨트롤러는 SDN 스위치의 패킷 수집 모듈로부터 패킷이 전달되면 공격 감지 모듈은 SDN 스위치가 수집한 패킷 데이터를 기반으로 악의적 사용자를 판단한다. 악의적 사용자 판단에는 단위 시간 당 패킷 수, 대역폭 사용량, 패킷 종류별 비율 등의 판단 기준을 사용할 수 있다. 악의적 사용자 판단에는 단위 시간 당 패킷 수, 대역폭 사용량, 패킷 종류별 비율 등의 판단 기준을 사용할 수 있다. 악의적 사용자로 의심되는 사용자가 탐지된 경우, 플로우 규칙 생성기와 위협 레벨 관리 모듈에게 위협 신호를 각각 전달한다. 위협 신호는 공격자 주소를 포함한다. 위협 레벨 관리 모듈은 위협 신호를 분석하여 위협 단계를 업데이트 한 후 위협 단계에 따른 위협 감지 파라미터를 공격 감지 모듈에게 전달한다. 위협 감지 파라미터는 단위 시간 당 패킷 개수, 대역폭 사용량, 패킷 종류에 따른 비율 등이 될 수 있다 플로우 규칙 생성기는 위협 신호를 파악하여 플로우 룰을 생성하고 이를 SDN 스위치로 전송한다. SDN 스위치는 SDN 컨트롤러로부터 플로우 규칙이 전달되면 이를 플로우 규칙 데이터 베이스에 저장하고 플로우 규칙에 따라 정상 플로우 규칙에 따라 악의적 사용자에 의한 패킷은 허니팟으로 전달하고, 정상 패킷은 다음 스위치로 전달한다. 허니팟은 수집된 공격자의 공격 방식, 공격 패턴, 공격 유형, 공격 범위, 공격 시간 등을 분석하여 이를 위협 레벨 관리 모듈에 반영한다.

5. 결론

본 논문에서는 SDN 의 특징인 유연한 플로우 규칙 설정을 활용해 악의적 패킷을 허니팟으로 전달함으로써 DoS 공격을 차단하는 방법을 제시했다. SDN 을 활용하면 기존의 공격 탐지 시스템과 달리 SDN 스위치가 직접 플로우 규칙에 따라 패킷을 목적지로 포워딩 또는 허니팟으로 전송하도록 할 수 있다. 허니팟은 전송된 공격 패킷을 분석하여 SDN 컨트롤러에 포함된 공격 탐지 모듈과 위협 레벨 관리 모듈이 지능적 공격 상황에도 유연하게 대응할 수 있도록 한다. 향후 연구에서는 여러 종류의 DoS 공격에 대응할 수 있도록 위협 레벨 관리 모듈, 공격 탐지 모듈 등을 상세 설계하고, 이를 구현하여 제안 시스템의 성능을 보이고자 한다.

6. Acknowledgement

"이 논문은 2015 년도 정부(교육부)의 재원으로 한국연구재단 기초연구사업의 지원을 받아 수행된 연구임(No. NRF-2018R1A2B6009620)", 교신저자 김미희.

참고문헌

[1] Specht, S. M. and Lee, R. B., "Distributed denial of service: taxonomies of attacks, tools and countermeasures," Proceedings of the International Workshop on Security in Parallel and Distributed Systems, CA, USA, 2004, pp.543-550.

[2] 천우성, 박대우, "DoS 공격에 대한 N-IDS 탐지 및

패킷 분석 연구," 한국컴퓨터정보학회논문지, 한국컴퓨터정보학회, 13, 6, 217-224, 2008.

[3] Tommy, M., Xenia, M., Xiangyang L. and Kaiqi X., "Selective Packet Inspection to Detect DoS Flooding Using Software Defined Networking (SDN)," IEEE 35th International Conference on Distributed Computing Systems Workshops, OH, USA, 2015.

[4] Yun, T., Vincent, T. and Mutalifu, K., "DOS Attack Mitigation Strategies on SDN Controller," IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, USA, 2019.

[5] Kreutz, D., Ramos, F. M., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S. and Uhlig, S., "Software-defined networking: A comprehensive survey," Proceedings of IEEE, 103, 1, 14-76, 2014.

[6] Software Defined Networking (SDN), ONF, https://www.opennetworking.org/onf-sdn-projects

[7] Zha, Z., Wang, A., Guo, Y., Montgomery, D. and Chen, S., "Instrumenting open vSwitch with monitoring capabilities: designs and challenges," Proceedings of the Symposium on SDN Research, LA, USA, 2018.

[8] Alata, E., Nicomette, V., Kaaniche, M., Dacier, M. and Herrb, M., "Lessons learned from the deployment of a high-interaction honeypot," In 2006 Sixth European Dependable Computing Conference, Coimbra, Portugal, 2006, pp. 39-46.