서비스 거부 공격 탐지 및 방어를 위한 SDN 기반 IoT 게이트웨이 설계

신 응억 뉘엔, 이윤기, 이왕광, 신기원, 김경백
전남대학교 전자컴퓨터공학부
sinhngoc.nguyen@gmail.com, negee1564@naver.com,
kwang9092@gmail.com, giwonie@gmail.com kyungbaekkim@jnu.ac.kr

Design of SDN based IoT Gateway for Detecting and Preventing DoS attack

Sinh Ngoc Nguyen, Yungee Lee,
Wangkwang Lee, Giwon Shin, Kyungbaek Kim
Department of Electronics and Computer Engineering,
Chonnam National University

요약

최근 IoT 개념 확산과 IoT 기반 서비스 활성화에 따라, 다양한 형태의 기기 및 단말 장치가 실생활에 보급 되고, 주요 개인 정보 및 시스템에 활용되고 있다. 이와 동시에, 단말의 보안 취약점을 악용한 대규모 서비스 거부 공격 (DoS)의 가능성이 높아지고, 그 공격 방법이 다양해지고 있다. 또한, IoT 환경에서는 다양한 기기 및 단말이 공격 목표가 됨과 동시에 공격 도구로 악용될 수 있으므로, 다양한 상황의 DoS공격에 대한 대응책 마련이 필요하다. 이 논문에서는 이와 같은 다양한 DoS공격을 탐지하고 방어하는 IoT 게이트웨이를 위한 SDN기반 설계를 제안한다. 제안된 IoT 게이트웨이는 네트워크 플로우 관리의 유연성을 향상시켜주는 SDN기반 스위치를 탑재하고, 해당 IoT 게이트웨이를 통과하는 트래픽을 샘플링하여 네트워크 플로우의 DoS공격 관련 여부를 탐지한다. 탐지된 DoS공격 정보를 기반으로 SDN 컨트롤러는 자동으로 공격과 관련된 네트워크 플로우를 차단함으로써 DoS공격 방어를 수행한다. 또한 IoT 환경의 특성상 무선 통신을 통해 데이터를 주고받는 장치들이 많다는 점을 고려하여, 무선 DoS공격시 단말 및 기기의 무선 연결을 최소한으로 유지시키기 위해 장치 관리자 및 SDN 기반 스위치와 연동하는 네트워크 큐 관리자를 IoT 게이트웨이에 포함한다. 샘플링 기반의 DoS공격 탐지 및 방어 기능을 탑재한 IoT게이트웨이 프로토타입을 라즈베리파이, OpenWRT, Open vSwitch, 그리고 OpenDaylight를 통해 구현하였고, 그 동작을 검증하여 해당 설계의 가능성을 확인하였다.

1. 서 론

언제 어디서나 네트워크와 연결되는 미래의 모습, 공상과학 영화에서나 보던 '유비쿼터스 시대'가 어느덧 우리의 생활과 가까워지면서 'IoT' 기술 또한 뜨거운 관심을 받고 있다[3].

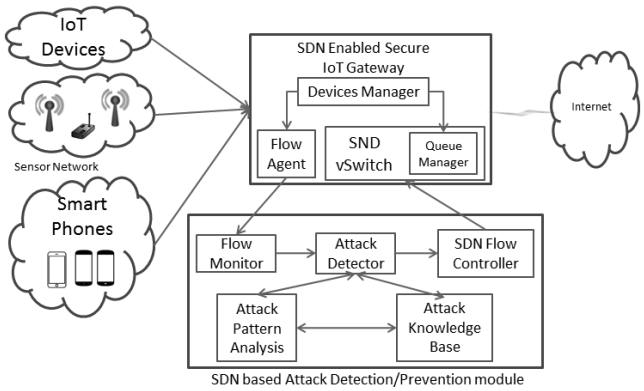
인터넷을 기반으로 모든 사물을 연결하여 사람과 사물, 혹은 사물과 사물 간의 정보를 상호 소통하는 지능형 서비스인 사물인터넷(IoT)는 인공지능(AI)와 함께 종종 4차 산업혁명을 이끌 주요 기술로 꼽히곤 한다. 인체를 인식하여 자동으로 켜지는 가로등부터 스마트폰, 냉장고, IPTV 등 그 종류는 굉장히 다양해졌고 우리의 생활과 밀접한 사물들과 결합되면서 IoT는 손바닥 안에서 모든 것을 통제할 수 있게 되었다고 해도 과장이 아니다.

하지만 이렇게 편리하게 모든 것을 통제할 수 있는 반면, IoT환경은 역으로 기본적인 보안 허점 등의 문제로 인해 DoS 공격에 노출되기 쉬운 것이 사실이다[2]. 실제로 IoT 기반의 스마트 홈 서비스는 대부분 집안의 하나의 무선 공유기를 통하여 연결이 되어 있는 경우가 많아 무선 공유기 하나에만 침투에 성공하면 그에 연결되어 있는 모든 스마트 기기들이 노출되어 DoS공격 수단으로 이용될 수 있다[3][4][5]. 지난 9월, 수십만 대의 사물 인터넷 디바이스를 감염시켜 대규모 DoS 공격을 일으킨 트로이목마 프로그램 미라이(Mirai)의 소스 코드가 온라인에 공개되기도 하면서 향후 더 많은 사물 인터넷 봇넷이 생겨날 가능성이 커졌다. 이와 같이 IoT 산업이 발전함에 따라 네트워크와 연결된 사물과 데이터의 이동 역시 갈수록 많아지고 IoT 환경에서의 DoS 공격이 증가하고 있다.

본 논문에서는 이러한 IoT 환경에서 위협의 되고 있는 DoS공격 탐지 및 방어를 수행하기 위한 IoT게이트웨이를 SDN기반으로 설계하고, 그 프로토타입을 구현하여 가능성 검증 결과를 소개한다. 제안된 IoT 게이트웨이는 유, 무선 네트워크 인터페이스를 관리하는 SDN기반의 스위치를 포함한 유무선 네트워크 AP기능을 기본으로, 네트워크

트래픽 샘플링 에이전트, 연결된 장비/기기 관리자, 네트워크 큐 관리자로 구성된다. DoS공격을 탐지하고 방어하기 위한 SDN기반 공격 탐지 및 방어 모듈은 네트워크 플로우 모니터, DoS공격 탐지기, SDN 컨틀로러, 공격 패턴 분석기 그리고 공격 지식 기반으로 구성된다. 설계된 SDN기반 IoT보안 게이트웨이의 가능성 검증을 위해, 라즈베리파이, OpenWRT[1], OpenVSwitch, 오픈데이라이트, SNORT, 그리고 SFLOW를 이용한 프로토타입을 구현하고, TCP SYN Flooding공격의 탐지와 방어에 대한 동작을 확인하였다.

2. DoS공격 탐지/방어 SDN기반 IoT게이트웨이



(그림 1) DoS공격 탐지 방어를 위한 SDN기반 IoT 게이트웨이 구조

IoT환경에서는 다양한 네트워크 인터페이스를 가진 기기들이 서로 정보를 주고 받게 된다. 이를 지원하기 위해 일반적으로는 다양한 네트워크 인터페이스를 지원하는 게이트웨이가 사용된다. 이러한 IoT 게이트웨이에서는 유무선 네트워크 인터페이스를 통해 연결된 다양한 기기 및 장치들이 보내는 네트워크 트래픽이 흐르게 된다.

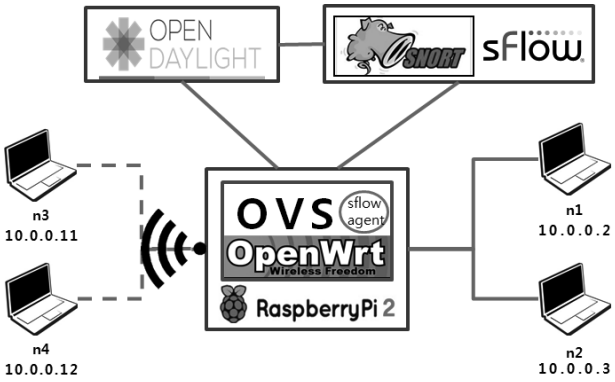
우리는 이러한 다양한 네트워크 인터페이스에서 흘러들어오는 네트워크 트래픽을 관찰하여 DoS공격을 탐지하고, 이 탐지 정보를 사용해 자동으로 네트워크 플로우를 관리할 수 있는 SDN 컨트롤러의 기능을 포함하는 SDN기반 공격 탐지 방어 모듈을 IoT 게이트웨이에 탑재 또는 연결시키고자한다. 그림 1에서는 이러한 DoS공격 탐지 방어를 위한 SDN기반의 IoT게이트웨이의 기본 구조를 나타내고 있다.

SDN기반 공격 탐지 방어 모듈을 활용하기 위해서는, IoT 게이트웨이는 OpenFlow 프로토콜을 이해하는 SDN기반의 스위치가 탑재 되어야 한다. 이 스위치는 유 무선 네트워크 인터페이스를 관리하게 되고, 해당 스위치 상에서 흘러가는 네트워크 트래픽은 SDN 컨트롤러에 의해서 플로우(flow)단위로 관리할 수 있다. 이러한 네트워크 플로우에서 발생되는 패킷을 분석하여 공격을 탐지하기 위해서, 플로우 에이전트와 플로우 모니터가 필요하다. 다양한 DoS공격의 분석 정도와 IoT게이트웨이의 성능문제를 고려하여, 플로우 에이전트는 분석을 위한 네트워크 트래픽의 샘플링 정도를 조절할 수 있다. 이렇게 관찰된 네트워크 패킷들의 패턴을 공격 탐지기를 통해 분석하고, 분석된 결과는 향후 새로운 공격 패턴을 예측하기 위한 지식기반 구축을 위해 저장된다.

또한, IoT환경의 특성상 무선으로 연결되는 기기가 많다는 점을 고려하면, 무선 채널에서의 DoS공격의 영향을 고려한 설계가 필요하다. 무선 상에서는 Queensland DoS attack, Deauth Flood attack, EAP Start Flood attack등 무선 채널을 장악하여 다른 무선 기기들의 통신을 원천적으로 방해하는 공격이 가능하다. 이러한 취약점에 대응하기 위해서, SDN기반의 IoT게이트웨이에서는 무선으로 접속하고 있는 장비들을 관리하는 관리자와 네트워크 플로우에 적용 가능한 네트워크 큐 관리자가 필요하다. 즉, IoT 게이트웨이에 연결된 모든 무선 기기들을 파악하고, 해당 무선 연결 정보를 유지하기 위한 최소한의 네트워크 채널을 보장하는 큐를 해당 네트워크 플로우에 매핑시킨다. 이를 통해 무선 DoS공격의 영향을 약화 시키고 해당 무선 DoS 공격의 탐지와 방어를 가능하게 한다.

3. 프로토타입 구현 및 동작 검증

제안된 DoS공격 탐지/방어 SDN기반 IoT게이트웨이의 동작을 검증하기 위해 라즈베리파이, OpenWRT, Open VSwitch, 오픈데이라이트, SNORT, 그리고 SFLOW를 이용한 프로토타입을 구현하고, TCP SYN Flooding 공격에 대한 탐지와 방어에 대한 IoT게이트웨이 동작을 확인하였다. 그림 2에서는 구현된 프로토타입의 구조를 나타낸다.



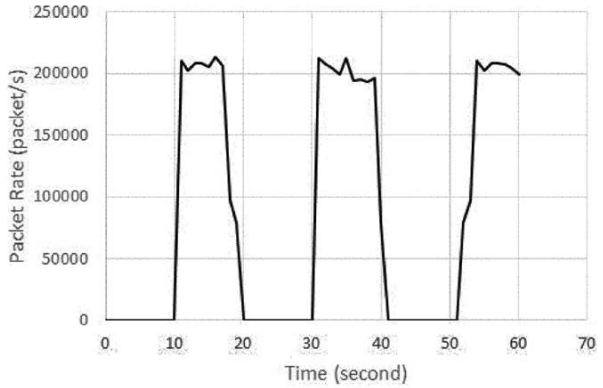
(그림 2) SDN기반 IoT 게이트웨이 프로토타입 구조

프로토타입은 세 개의 이더넷 인터페이스와 하나의 WiFi 인터페이스를 가지고 있다. 하나의 이더넷 인터페이스는 오픈데이라이트 및 스노트와 연결하기 위해 사용된다. 나머지 두 개의 이더넷 인터페이스는 각각 임의의 기기에 연결하였고, 두 개의 무선 기기를 WiFi 인터페이스에 연결하였다.

이러한 상황에서 n1을 공격자로 가정하고, n1에서 n2로

TCP SYN공격을 시작하면, 다른 일반 노드들 간의 ping 시간이 급격하게 증가하는 것을 확인 할 수 있었다. 즉 IoT 게이트웨이가 n1이 생성하는 과도하게 많은 네트워크 트래픽을 처리하기 위한 과부하가 걸리면서 다른 노드들의 네트워크 트래픽 처리가 늦어지게 된다.

이 때, SDN기반 공격 탐지 방어 모듈을 IoT 게이트웨이에 연결한 경우, n1이 공격을 시작하면 sflow의 샘플링 주기에 맞추어 해당하는 공격이 탐지되고 자동적으로 공격으로 사용되는 네트워크 플로우가 막히게 된다.



(그림 3) DoS공격 탐지 방어에 따른 네트워크 패킷량

그림 3에서는 sflow의 샘플링 주기를 10초로 하였을 때, 네트워크 공격 탐지 및 방어가 진행되는 과정에서의 네트워크 패킷량을 보여준다. 현재 10초가 경과되는 시점에서 n1은 TCP SYN flooding공격을 시작하였고, 네트워크 트래픽이 급격히 증가하는 것을 확인할 수 있다. 하지만 약 10초 경과후 해당 공격은 제안된 공격 탐지 모듈에서 탐지되고, 공격에 이용된 네트워크 플로우는 SDN 컨트롤러에 의해서 자동으로 중단된다. 해당 공격 탐지 및 방어 모듈의 기능을 확인하기 위해서, 이 실험에서는 SDN 컨트롤는 네트워크 플로우를 중지 시킬 경우 10초 후에 다시 해당 플로우를 활성화 시키도록 하였다. 따라서, 공격이 막힌 시점에서 10초후에 네트워크 공격이 재개되는 것을 확인 할 수 있고, 마찬가지로 공격이 감행된 후 다시 공격이 탐지 및 방어되는 현상을 볼 수 있다.

이러한 프로토타입 기반 검증을 통해, 제안된 설계의 동작을 검증할 수 있었다.

4. 결론

이 논문에서는 IoT환경에서 위협이 되는 DoS공격을 탐지하고 방어하기 위한 SDN기반의 IoT게이트웨이의 설계와 그 동작의 검증 결과를 소개 하였다. 간단한 L2, L3에서의 플러딩 기반 DoS공격에 대한 탐지 및 방어는 제안된 SDN기반 IoT 게이트웨이를 통해 탐지되고 자동으로 방어할 수 있다. 이러한 SDN기반의 IoT게이트웨이는 향후 IoT환경 구축 및 확산에 있어서 매우 필수적인 구성요소가 될 것이다.

향후, 무선 DoS공격의 영향을 최소화 하고, 해당 공격시 다른 무선 기기들의 연결을 보장하기 위한 장지 관리자 및 큐 관리자의 구체적 내용을 연구할 계획이다. 또한, 변현된 DoS 공격 또는 어플리케이션 계층에서의 DoS공격을 탐지 및 방어하기 위한 방안을 연구할 계획이다.

Acknowledgements

이 논문은 2016년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (R0110-16-1001, IoT 기기 서비스 거부 공격 방어를 위한 리소스 보호용 시큐어 하드웨어 컨테이너 기술)

참 고 문 헌

[1] “What is OpenWrt?”, (https://openwrt.org/)

[2] Needham, Roger M. Denial of service Proceedings of the 1st ACM Conference on Computer and Communications Security. ACM, 1993. APA

[3] Kalliola A, Lee K, Lee H, Aura T, Flooding DDoS mitigation and traffic management with software defined networking InCloud Networking (CloudNet), 2015 IEEE 4th International Conference on 2015 Oct 5 (pp. 248-254). IEEE.

[4] Valdivieso Caraguay L, Benito Peral A, Barona Lpez LI, Garca Villalba LJ SDN: evolution and opportunities in the development IoT applications, International Journal of Distributed Sensor Networks, 2014 May 4, 2014.

[5] 이윤기, 김승욱, 부 둑 티엡, 김경백, SDN을 위한 샘플링 기반 네트워크 플러딩 공격 탐지/방어 시스템, 한국스마트미디어학회 스마트미디어저널 4권 4호, pp. 24-32, December 31, 2015