KNOM Review '17-01 Vol.20 No.01
https://doi.org/10.22670/knom.2017.20.1.24

SDN기반 IoT 게이트웨이에서 DoS 공격 영향 평가

최진태◆, 뉘엔 신 응억*, 김경백°

Assessing the impact of DoS Attack on SDN based IoT Gateway

Jintae Choi◆, Sinh-Ngoc Nguyen*, Kyungbaek Kim°

요 약

최근 IoT 디바이스가 보편화 되면서 그 수가 빠르게 증가하고 있다. 또한, CCTV, 난방기기, 자동차, 냉장고 등 인간의 삶에 매우 중요한 기기 또한 IoT에 포함되고 있다. 이러한 상황에 2016년 9월 미라이 공격은 수십만대의 IoT 디바이스를 감염시키고, 이를 이용하여 대규모 DDoS 공격을 감행하였다. 이는 저사양의 IoT 기기에서 발생하는 대량의 공격 트래픽에 대한 대책 마련이 매우 중요함을 보여준다. 또한, IoT 환경에서 발생하는 트래픽은 IoT 기기들 간의 통신에 악영향을 끼쳐, IoT 시스템의 정상적인 동작을 방해할 수 있다. 최근 연구에서 DoS 공격이 IoT 디바이스들의 통신에 미치는 영향에 대해 분석하여 무선 IoT 기기가 특히 DoS 공격에 영향을 많이 받는 것이 확인되었다. 본 논문에서는 DoS공격이 유무선 IoT 통신 환경에 미치는 영향을 더욱 자세히 분석하기 위해, 다양한 구성요소를 가지는 SDN기반 IoT 게이트웨이 환경에서 DoS 공격의 영향을 측정하고 분석하였다. 또한, DoS 공격 발생시 IoT 네트워크 트래픽의 QoS를 유지하기 위해 SDN기반 IoT 게이트웨이에 Queue 관리 기능을 적용하고, 이를 통해 DoS 공격상황에서 IoT 기기 간의 통신 성능 개선이 가능함을 확인하였다.

Key Words : IoT, DoS, SDN (Software Defined Networking), Gateway, AP, Queue, Management

ABSTRACT

Recently, the number of IoT devices has been increasing rapidly. Also, devices such as CCTV, heaters, cars and refrigerators are also included in the IoT. In September 2016, the Mirai botnet infected with hundreds of thousands of IoT devices and launched a huge scale DDoS attack. This shows that preventing heavy attack traffic on IoT devices with limited resources is very important. In addition, traffic in an IoT environment may adversely affect the communication between IoT devices and interfere with normal operations of the IoT system. A recent study found that the impact of DoS attacks on the communication of the IoT devices is severe to the wireless IoT devices. In this paper, we measure and analyze the effect of DoS atack on SDN based IoT gateway with various scenarios to access the impact of DoS attacks in wired and wireless IoT Communication environment in detail. In addition, in order to maintain the QoS of the IoT network traffic during a DoS attack, Queue management technique is applied to SDN based IoT gateway and the viability of improving the performance of IoT communication under DoS attack by using adaptive Queue management.

※이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (NRF-2017R1A2B4012559). 본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2017-2016-0-00314).

◆ First Author : Chonnam National University Department of Information Security, jefroh1100@gmail.com
° Corresponding Author : Chonnam National University of Department of Electronics and Computer Engineering, kyungbaekkim@jnu.ac.kr

논문번호 : KNOM2017-01-05, Received May 20, 2017; Revised June 30, 2017; Accepted August 15, 2017

Ⅰ. 서 론

IoT(Internet of Things)는 주변 사물이 유선 또는 무선으로 네트워크에 연결하여 정보를 공유할 수 있는 기술이나 환경을 뜻한다. 최근 이러한 IoT 디바이스가 보편화 되면서 그 수가 빠르게 증가하고 있다. IT 분야의 리서치 기업 가트너는 2014년 64억 개의 IoT 디바이스가 2020년에는 135억 개에 달할 것으로 추측한다. 더불어 2014년을 기준으로 2015년에는 IoT 디바이스의 사용률이 30%나 증가하였다. [1,2,4] IoT 디바이스의 증가와 함께 IoT의 영역 또한 점차 늘어나 CCTV, 난방기기, 냉장고, 자동차등과 같이 인간의 삶에 밀접한 기기들도 IoT 디바이스의 영역에 포함 될 것으로 예상된다. [3,4]

이렇게 IoT 디바이스의 수는 날이 갈수록 증가하고, 인간의 삶에 더욱 중요한 기기가 되어가고 있지만 IoT 디바이스에 대한 보안은 여전히 취약한 상태이다. 이러한 상황에 2016년 9월, 수십만 대의 IoT 디바이스를 감염시켜 대규모 DDoS 공격을 일으킨 미라이 봇이 등장하였다. 또한, 미라이 봇의 소스코드가 공개되어 앞으로 더 많은 변종 IoT 봇이 등장할 것으로 예상된다. [5] 이와 같이, 다수의 IoT 디바이스를 감염시킬 수 있는 봇이 등장함으로서 이를 악용하여 IoT 네트워크 자체를 마비시킬 수 있는 공격 또한 고려해야 한다.

이에 따라, 최근 논문에서는 유, 무선으로 연결된 IoT 디바이스에 DoS 공격이 가해질 경우 IoT 디바이스들의 통신에 미치는 영향을 실험 하였다. 실험 결과, 무선으로 연결된 IoT 디바이스로 DoS 공격이 가해질 경우 모든 무선 IoT 디바이스들이 매우 큰 영향을 받는 것으로 나타났다. 이 디바이스들은 통신 속도가 느려지기도 하였으며, 통신 불능 상태가 되는 경우도 발생하였다. 이는 앞으로 실생활에 사용될 무선 IoT 디바이스에 대한 DoS 공격의 대비가 매우 중요하다는 것을 보여준다. 특히, IoT 기반의 홈서비스에서는 1개의 공유기에 모든 IoT 기기가 무선으로 연결되는 경우가 많기 때문에 앞으로 나타날 다양한 IoT 게이트웨이 환경에서의 실험은 더욱 더 중요하다. [4,6]

본 논문에서는 다양한 IoT 게이트웨이 환경에서 실험하기 위해 2개의 무선 네트워크 인터페이스를 가진 SDN 기반 IoT 게이트웨이를 구현한다. [6,12] 이와 같은 새로운 환경에서의 실험에 앞서, 먼저 1개의 무선 네트워크 인터페이스를 가지는 SDN기반 IoT 게이트웨이 환경에서 실험을 진행한다. 이를 위해, 유선 IoT 디바이스에서 무선 IoT 디바이스로 DoS 공격을 수행하는 동안 공격을 수행하거나 받지 않는 유선-유선, 무선-유선, 무선-무선 IoT 기기들의 통신 상태에 대해 측정한다. [4,6] 다음으로 2개의 무선 네트워크 인터페이스를 가진 SDN기반 IoT 게이트웨이 환경에서 실험을 진행하여 서로 다른 무선 네트워크 인터페이스가 DoS 공격에 어떠한 영향을 받는지 측정하고 분석한다. 또한, IoT 네트워크 환경에서 DoS 공격의 영향을 최소화하여 IoT 네트워크 통신의 QoS를 유지할 수 있도록 Queue 관리를 적용한 결과를 측정하고 분석한다. [12]

Ⅱ. 관련 연구

2.1 SDN

SDN(Software-Defined Networking)은 소프트웨어로 정의된 네트워크를 의미한다. 이는 기존의 라우터나 스위치와 같은 네트워크 장비의 제어 평면과 데이터 전달 평면을 분리하여 SDN 컨트롤러를 통해 데이터 전달 평면을 제어 및 관리 하는 개념이다. 또한 SDN은 네트워크 장비의 기능을 정의할 수 있는 API를 외부에 개방하여 다양한 네트워크 제어 기술과 라우팅 프로토콜을 개발하여 동작할 수 있도록 한다. [5]

SDN 구조는 크게 데이터 전달 평면 (Data Plane), 제어 평면 (Control Plane), 응용 평면 (Application Plane)으로 구성된다. 제어 평면에서는 SDN 컨트롤러를 이용하여 데이터 전달 평면의 네트워크 장비들을 제어 및 관리한다. 기존의 네트워크에서는 각 네트워크 장비마다 제어하고 관리해야 했지만, SDN은 SDN 컨트롤러에서 통합적으로 네트워크 장비를 관리하기 때문에 네트워크 관리 및 제어에 매우 효율적이며, 편리한 서비스를 제공한다. 이를 위해, 제어 평면과 데이터 전달 평면을 상호 연결 시켜주는 표준화된 프로토콜인 Open southbound API가 필요하다. 현재 가장 많이 사용되는 프로토콜은 OpenFlow이다. 이러한 표준화된 프로토콜을 통해 특정 장비에 국한되지 않고 네트워크망을 제어 및 관리할 수 있다. [5]

또한, SDN 컨트롤러의 네트워크 OS 기능을 자유롭게 개발할 수 있도록 제어 평면과 응용 평면

간에 Northbound API를 제공한다. 이를 통해 네트워크 관리자는 자신의 목표에 맞는 라우팅 프로토콜, 트래픽 엔지니어링, QoS 관리 등을 제공할 수 있다. [5]

데이터 전달 평면은 네트워크 하드웨어 장비로 구성된다. 이러한 장비들은 기존의 네트워크 장비들과 다르게 패킷제어 및 관리 기능 없이 패킷 포워딩 기능만을 가지고 있으며, SDN 컨트롤러에 의해 제어 및 관리 된다. [5]

2.2 DoS 공격

DoS (Denial of Service) 공격이란 서비스 거부 공격을 뜻한다. 이는 악의적으로 유명 사이트나 목표가 되는 시스템의 자원을 점유하여 목표 시스템의 서비스를 원하는 사람이 서비스 받지 못하도록 하는 공격 기법이다. 이러한 DoS 공격은 DDoS (Distributed Denial of Service)공격과 DRDoS (Distributed Reflection Denial of Service)공격으로 발전하였다.

DDoS 공격은 분산 서비스 공격으로, 여러 대의 PC를 좀비 PC로 감염시킨 후 좀비 PC를 사용하여 목표가 되는 시스템을 공격하는 공격 기법이다. 최근에는 좀비 PC대신 IP를 가지며 인터넷에 연결 할 수 있는 다수의 IoT 기기들을 사용하여 DoS 공격을 감행하였다. 이에 따라 IoT 디바이스 또한 DoS 공격에 매우 위험한 위치해 있으며, 이에 대한 피해 정도와 대응방법을 구상할 필요가 있다.

DR-DoS 공격이란 분산 반사 서비스 거부 공격으로, DDoS의 발전된 형태이다. 이 공격기법은 좀비 PC가 직접 목표물을 공격하지 않고 DNS 서버나 NTP서버를 반사 서버로 이용하여 목표물을 공격하는 공격기법이다. 이러한 반사 서버에 목표물의 IP로 스푸핑된 소스 IP를 사용하여 공격 요청 패킷을 전송하게 되면, 공격 요청 패킷을 받은 반사 서버는 스푸핑된 IP를 가진 목표물에 대량의 패킷을 전송함으로써 공격이 감행된다. 또한, 최근에는 SSDP공격과 같은 IoT 프로토콜을 이용한 DR-DOS 공격 또한 등장하고 있다. [8,9,10]

Ⅲ. 실험 환경 구축

최근 연구에서는 상용 게이트웨이에 존재하는 1개의 무선 네트워크 인터페이스를 사용하여 실험하였다. [4] 하지만, 본 논문에서는 다양한 IoT 게이트웨이 환경에서의 실험 및 DoS 공격의 영향을 줄이기 위한 Queue 관리 기능 적용을 위해 2개의 무선 네트워크 인터페이스를 가진 SDN 기반 유무선 IoT 게이트웨이를 구현하였다.

3.1 SDN 기반 IoT 게이트웨이

SDN은 다양한 유, 무선 네트워크 인터페이스와 프로토콜을 제공하며 사용자 정의대로 게이트웨이를 관리 할 수 있다. 이러한 이유로 SDN을 사용하여 유무선 IoT 게이트웨이를 구성한다. 이를 위해 H/W로 라즈베리파이3를 사용했으며, OS로는 라즈비안, SDN 스위치 기능을 사용하기 위해 openvswitch를 설치한다. Open vSwitch는 OVS 라고 불리며, OpenFlow 프로토콜을 지원하며 스위치기능을 가진 프로그램이다.

3.2 실험 환경 구성

SDN기반 IoT 게이트웨이 환경에서 DoS 공격이 발생했을 경우 IoT 디바이스들의 통신에 대한 영향을 측정하기 위해 그림 1과 같은 SDN 기반 스위치 네트워크 토폴로지를 구성하였다. 그림 1의 구성요소는 다음과 같다. SDN 컨트롤러인 OpenDayLight(ODL) Beryllium, 5개의 OVS-Switch, Vswitch로 구현한 1개의 SDN 기반 IoT 게이트웨이를 사용하였다. 무선 네트워크 인터페이스는 usb wifi dongle을 사용하였다. 표 1은 무선 네트워크 인터페이스의 세부 특성을 보여준다. [6,11,12]

무선 네트워크 인터페이스를 활용하는 SDN기반 IoT 네트워크의 구현을 위해 라즈베리파이3에 라즈비안 운영체제를 사용한다. 그리고 유선 네트워크와 무선 네트워크를 연결하기 위해 OVS를 설치하여 브릿지를 생성한다. 이를 위해 hostap tool을 사용하

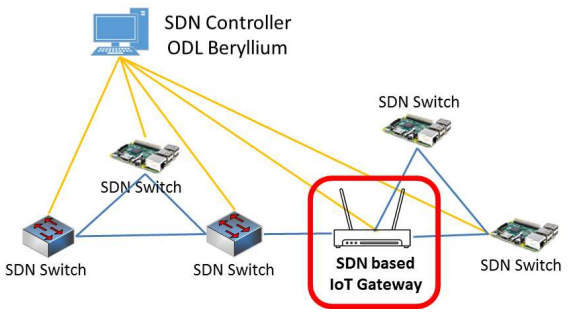


그림 1. SDN 기반 스위치 네트워크 토폴로지
Fig. 1. SDN-based switch network Topology

표 1. 무선 랜 usb wifi dongle 세부 특성
Table 1. Wireless LAN usb wifi dongle Details

카테고리	특징
CPU	리얼텍 RTL8188
인터페이스	USB 2.0
무선 주파수 대역폭	2.4 GHz
무선 지원 규격	IEEE 802.11n/b/g
무선 속도	N150
무선 수신 채널	싱글 밴드

여 IoT 게이트웨이를 설정하였다. 또한, 무선 IoT 디바이스의 연결을 위해 isc-dhcpserver를 사용하여 자동으로 ip를 제공하도록 만들었다.

추가적으로, DoS 공격 트래픽을 제한하기 위해, SDN기반 IoT 게이트웨이에 플로우별 Queue 관리 기능을 적용한다. Queue 기능을 적용하게 되면 각 개별 트래픽의 최소, 최대 전송률을 설정할 수 있다. 이후에 ovs-ofctl 명령어를 이용하여 지정된 입력 port와 출력 port로 구분되는 플로우에 Queue를 설정한다. 예를 들어 다음 그림 2와 같이 Queue1은 Host1에서 Host3로 가는 플로우에, Queue2는 Host2에서 Host3로 가는 플로우에 설정된다. Queue1은 0.1Kb/s로 트래픽을 제한하며, Queue2는 10Kb/s로 트래픽을 제한한다.

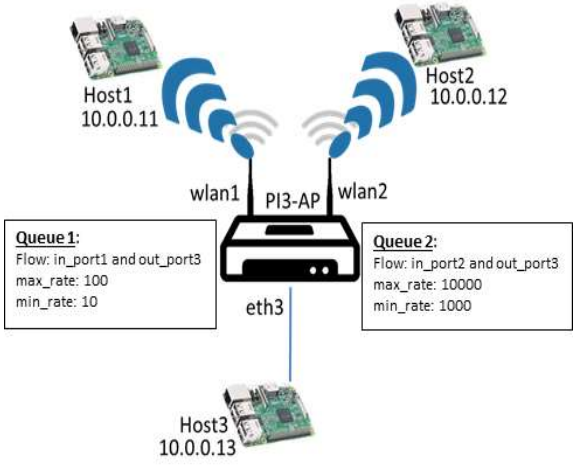


그림 2. SDN network QoS 구현
Fig. 2. SDN network QoS implementation

Ⅳ. 실험 및 분석

4.1 실험 측정 방법

그림 3, 5와 같은 실험환경에서 유선에서 유선 공격, 무선에서 무선 공격, 유선에서 무선 공격, 무선에서 유선 공격에 대한 각 IoT 디바이스들의 통신 상태를 비교한다. DoS 공격은 hping3 DoS 공격 툴을 사용한다. 공격 실행 시에는 표2와 같이 공격 속도 옵션을 각각 다르게 하여 IoT 디바이스의 통신 상태를 측정한다. IoT 디바이스의 통신 상태 측정은 1초당 1개의 Ping을 60번씩 보내어 주고받은 패킷 왕복시간인 Ping RTT(Round Trip Time)의 최솟값, 평균값, 최댓값과 손실률을 측정한다. 4.2 섹션에서는 한 개의 무선 네트워크 인터페이스를 가지는 SDN기반 IoT 게이트웨이 환경에서 유선에서 무선으로 DoS 공격을 수행하였을 경우 각 IoT 디바이스의 통신 상태를 측정한다. 4.3 섹션에서는 두 개의 무선 네트워크 인터페이스를 가지는 SDN기반 IoT 게이트웨이 환경에서 상황별 DoS 공격에 대한 각 IoT 디바이스 사이의 통신 상태를 측정한다. 4.4 섹션에서는 4.2와 4.3에서 분석한 결과를 토대로 Queue 관리 기능을 적용하여 DoS 공격에 대한 IoT 디바이스의 통신 개선이 가능함을 보인다.

4.2 IoT GW with one wireless network interface

첫 번째 실험에서는 1개의 무선 네트워크 인터페이스를 가진 SDN기반 IoT 게이트웨이 환경에서 DoS 공격에 대한 영향을 분석한다. 선행 연구에서는 IoT 게이트웨이 환경에서 DoS 공격이 이루어졌을 경우, 각 IoT 디바이스들의 통신 상태를 측정하였다. [4] 하지만 측정할 당시 DoS 공격을 받는 IoT 디바이스와의 통신 상태를 측정하였기 때문에 공격을 수행하거나 받지 않는 IoT 디바이스들의 통

표 2. hping3 공격 속도 옵션
Table 2. Attack speed option of hping3.

옵션	공격속도 (packet for second)
u1000	100
u100	1000
u50	5000
u10	10000

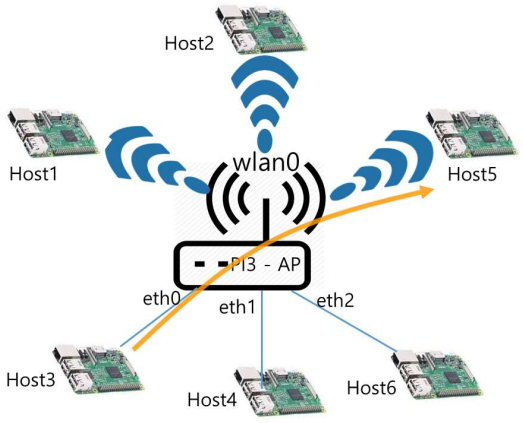


그림 3. 1개의 무선 네트워크 인터페이스 IoT 게이트웨이 구성 및 공격 경로
Fig. 3. Gateway Configuration with one wireless network interface and attack a path

신에 대해서는 정확히 알 수가 없었다. 이에 따라 본 논문의 첫 번째 실험에서는 선행 연구에서 DoS 공격의 영향을 많이 받았던 유선 IoT 디바이스에서 무선 IoT 디바이스로 DoS 공격이 발생할 경우, 공격을 수행하거나 공격을 받지 않는 다른 IoT 디바이스간의 통신 상태를 측정한다. 이를 위해 그림 3과 같은 1개의 무선 네트워크 인터페이스를 가진 SDN 기반 IoT 게이트웨이 환경을 구성한다. Host1, Host2, Host5는 무선 네트워크 인터페이스인 wlan0에 연결하였고, Host3, Host4, Host6은 유선으로 SDN 기반 IoT 게이트웨이에 연결하였다.

그림 4는 유선에서 무선으로 DoS 공격을 수행할 경우, 공격을 수행하거나 받지 않는 IoT 디바이스들 사이의 Ping RTT와 손실률을 측정한 그래프이다. 공격은 Host3에서 Host5로 수행하였다.

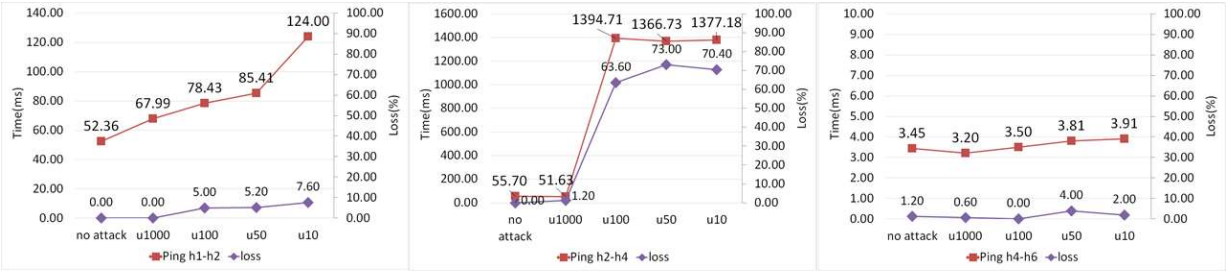
그림 4-(a)는 DoS 공격을 받지 않는 무선 IoT 디바이스들 사이의 Ping RTT를 나타낸 그래프이다. Ping h1-h2 보면 직접적으로 공격을 하거나 받지 않았음에도 불구하고 Ping RTT가 2배 이상 느려졌으며, 손실률 또한 최고 7.6%로 측정되었다.

그림 4-(b)는 DoS공격을 수행하거나 받지 않는 유선 IoT 디바이스와 무선 IoT 디바이스 사이의 통신을 나타내는 그래프이다. Ping h2-h4에서는 25배 가까이 통신 속도가 느려졌다. 하지만, 유선-유선 통신을 나타내는 그림4의 (c) Ping h4-h5 에서는 DoS 공격에 대한 영향이 전혀 없는 것으로 나타났다.

이를 통해, 유선에서 무선으로 DoS 공격이 발생하는 상황에서, 무선 IoT 디바이스와의 통신은 모두 DoS 공격에 큰 영향을 받는 것을 알 수 있다. 또한 공격을 수행하거나 받지 않는 유선 IoT 디바이스들 사이의 통신에는 전혀 영향을 받지 않음을 알 수 있다.

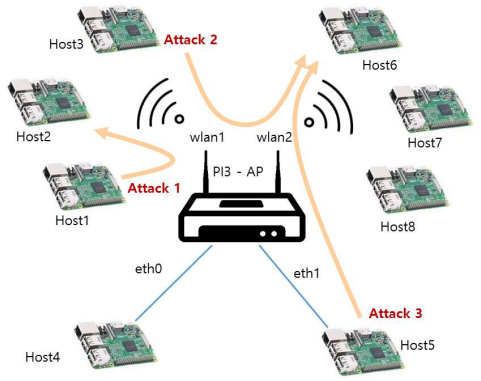
4.3 IoT GW with two wireless network interfaces

앞의 실험에서는 다수의 유선 네트워크 인터페이스와 1개의 무선 네트워크 인터페이스를 가진 IoT 게이트웨이 환경에서 실험하였다. 하지만, 앞으로 등장할 다양한 IoT 게이트웨이 환경에 대한 대비 또한 필요하다. 이를 위해, 두 번째 실험에서는 2개의 무선 네트워크 인터페이스를 가지는 SDN기반 IoT 게이트웨이 환경에서 DoS 공격이 발생했을 경우 각 IoT 디바이스의 통신 상태를 실험한다. 이 경우에도 공격을 수행하거나 수행하지 않는 IoT 디바이스 사이의 통신 상태를 측정한다. 이를 위해, 그림 5와 같이 2개의 무선 네트워크 인터페이스 wlan1, wlan2를 가진 SDN 기반 IoT 게이트웨이



(a) 무선-무선 통신 (b) 유선-무선 통신 (c) 유선-유선 통신

그림 4. 1개의 무선 네트워크 인터페이스 IoT 게이트웨이 환경에서 유선에서 무선(h3->h5) DoS 공격 상황의 실험 결과
Fig. 4. Experiment result on from wired to wireless(h3->h5) in an IoT gateway with one wireless network interface



Attack 1 : Attack within a single wireless network interface (Section 4.3-1)
Attack 2 : Attack between different wireless network interfaces (Section 4.3-2)
Attack 3 : Attack between wireless interface and wired interfaces (Section 4.3-3)

그림 5. 2개의 무선 네트워크 인터페이스 IoT 게이트웨이 구성도 및 각 공격 경로
Fig. 5. Gateway Configuration with two wireless network interfaces and attack paths

환경을 구성한다. Host1, Host2, Host3은 무선 네트워크 인터페이스인 wlan1에 연결하였고, Host6, Host7, Host8은 또 다른 무선 네트워크 인터페이스인 wlan2에 연결하였다. Host4, Host5는 유선으로 SDN 기반 IoT 게이트웨이에 연결하였다.

1) 하나의 무선 인터페이스 내의 DoS 공격

그림 6은 wlan1에 연결된 무선 IoT 디바이스에서 같은 무선 네트워크 인터페이스에 연결된 다른 무선 IoT 디바이스로 DoS 공격이 발생했을 경우 각 디바이스의 Ping RTT와 손실률을 측정한 그래프이다. DoS 공격은 Host1에서 Host2로 수행하였다.

그림 6-(a)의 Ping h3-h6은 wlan1에 연결된 공격을 수행하거나 받지 않는 무선 IoT 디바이스에서 wlan2에 연결된 무선 IoT 디바이스와의 통신 상태를 측정한 결과이다. 이 통신에서는 공격이 없는 상황에 비해 4배 가까이 통신 속도가 느려졌으며, 손실률 또한 0%에서 7.6%로 증가하는 것을 볼 수 있다.

그림 6-(b)의 Ping h7-h8은 wlan2에 연결된 무선 IoT 디바이스들 사이의 통신 상태를 나타낸다. 이 실험 결과에 따르면, wlan2에 연결된 무선 IoT 디바이스들 사이의 통신에는 DoS 공격의 영향이 없음을 확인하였다.

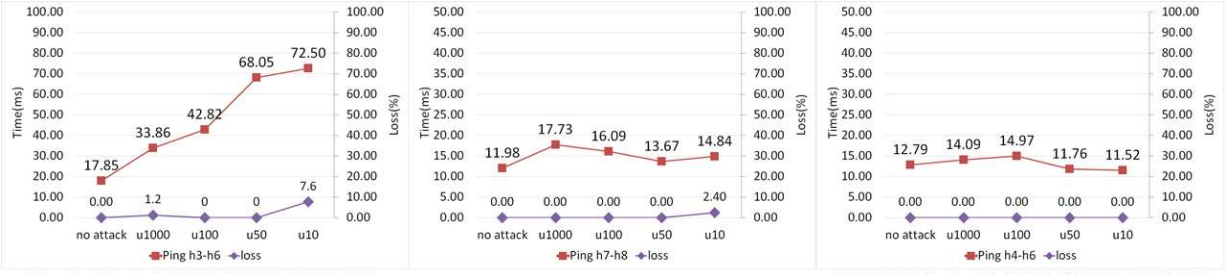
그림 6-(c)의 Ping h4-h6는 wlan2에 연결된 무선 IoT 디바이스와 유선으로 연결된 IoT 디바이스 사이의 통신 상태를 보여준다. 이 통신에서도 영향이 없음을 볼 수 있다.

이를 통해, 두개의 서로 다른 무선 네트워크 인터페이스 사이에 직접적인 DoS 공격이 발생하지 않을 경우, DoS 공격을 받지 않는 무선 인터페이스에 연결된 무선 IoT 디바이스들 사이의 통신은 DoS 공격에 영향을 받지 않는 것을 알 수 있다.

2) 서로 다른 무선 인터페이스 사이의 DoS 공격

그림 7은 wlan1에 연결된 무선 IoT 디바이스에서 wlan2에 연결된 다른 무선 IoT 디바이스로 DoS 공격이 발생했을 경우, 각 IoT 디바이스들 사이의 Ping RTT와 손실률을 측정한 그래프이다. DoS 공격은 Host3에서 Host6로 수행하였다.

그림 7-(a)의 Ping h1-h2는 같은 무선 네트워크 인터페이스 wlan1에 연결된 무선 IoT 디바이스들 사이의 통신 상태를 나타낸 그래프이다. 이 그래프에서 Ping h1-h2의 Ping RTT는 19.90ms에서 74.32ms로 4배 가까이 느려졌으며, 손실률은 0%에서 7.6%로 증가하였다. 이 두 디바이스는 공격을 직접적으로 수행하거나 받지 않는 상황이지만, DoS 공격이 이루어지는 무선 네트워크 인터페이스에 함



(a) wlan1와 wlan2 기기들 사이의 무선-무선 통신 (b) wlan2에 연결된 무선 기기들 사이의 통신 (c) 유선 기기와 wlan2에 연결된 무선 기기 사이의 통신

그림 6. 하나의 무선 네트워크 인터페이스 내의 DoS 공격 실험 결과.
Fig. 6. Results of DoS attacks Experiment within a single wireless network interface.

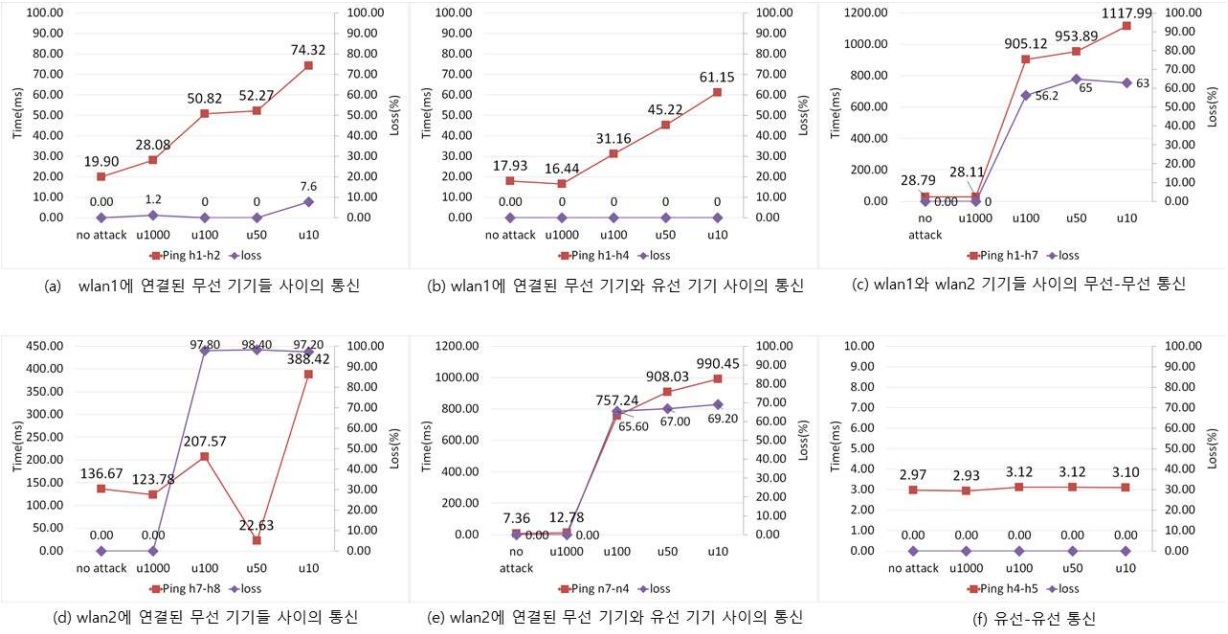


그림 7. 서로 다른 무선 네트워크 인터페이스 사이의 DoS 공격 실험 결과.
Fig. 7. Results of DoS attacks Experiment between different wireless network interfaces.

께 연결되어 있어 많은 영향을 받는 것을 알 수 있다.

그림 7-(b)의 Ping h1-h4는 무선 네트워크 인터페이스 wlan1에 연결된 무선 IoT 디바이스와 유선으로 연결된 IoT 디바이스와의 통신 상태를 나타낸다. 이 경우에는 손실률은 발생하지 않았지만, Ping RTT는 17.93ms에서 61.15ms로 4배 가까이 증가하였다.

그림 7-(c)의 Ping h1-h7은 wlan1에 연결되어 있는 무선 IoT 디바이스와 wlan2에 연결되어 있는 무선 IoT 디바이스와의 통신 상태와 손실률을 나타내는 그래프이다. 이 그래프에서 Ping RTT는 평상시 28.79ms에서 최고 1117.99ms로 40배 가까이 느려졌으며, 손실률 또한 0%에서 최고 65%까지 증가하였다.

그림 7-(d)의 Ping h7-h8은 무선 네트워크 인터페이스 wlan2에 연결되어 있으며, DoS 공격을 받지 않는 무선 IoT 디바이스들 사이의 Ping RTT와 손실률을 나타낸 그래프이다. 이 그래프에서 Ping RTT는 136.67ms에서 최고 388.42로 2배 증가하였으며, DoS 공격속도 u1000부터는 손실률이 97%이상을 기록하였다.

그림 7-(e)의 Ping h7-h4는 유선 IoT 디바이스와 wlan2에 연결되어 있는 무선 IoT 디바이스와의 통신 상태와 손실률을 나타낸 그래프이다. 이 그래프에서 Ping RTT는 평상시 7.36ms에서 최고 990.45ms로 135배 가까이 느려졌으며, 손실률은 0%에서 최고 69.2%로 증가하였다.

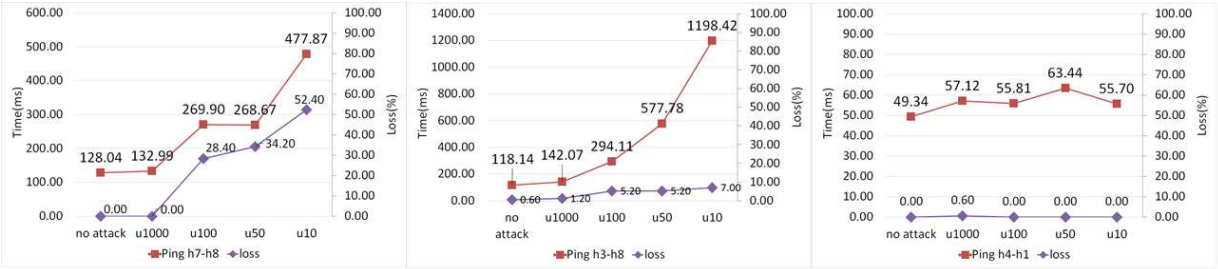
그림 7-(f)의 Ping h4-h5는 유선 IoT 디바이스 사이의 통신 상태와 손실률을 나타낸 그래프이다. 이 그래프에 따르면 무선에서 무선으로 DoS 공격을 하는 경우, 유선 IoT 디바이스사이의 통신은 영향받지 않음을 볼 수 있다.

이를 통해, 서로 다른 무선 네트워크 인터페이스 사이에서 DoS 공격이 일어날 경우, 공격이 발생하는 인터페이스의 무선 IoT 디바이스들의 통신은 DoS 공격에 많은 영향을 받으며, 공격받는 인터페이스에 연결된 무선 IoT 디바이스들은 거의 통신 불가에 가까운 결과를 볼 수 있다.

3) 유선에서 무선 인터페이스로의 DoS 공격

그림 8은 유선 IoT 디바이스에서 wlan2의 무선 IoT 디바이스로 DoS 공격이 발생 했을 경우, 각 IoT 디바이스들 사이의 Ping RTT와 손실률을 측정한 그래프이다. DoS 공격은 Host5에서 Host6로 수행하였다.

그림 8-(a)의 Ping h7-h8 과 손실률은 DoS 공격이 발생했을 때의 h7과 h8 사이의 통신 상태를 나타낸다. 이 두 무선 IoT 디바이스는 직접적으로 공격을 받고 있지는 않지만, 공격받고 있는 무선 네트



(a) wlan2에 연결된 무선 기기들 사이의 통신 (b) wlan1와 wlan2 기기들 사이의 무선-무선 통신 (c) wlan1에 연결된 무선 기기와 유선 기기 사이의 통신

그림 8. 유선 네트워크 인터페이스와 무선 네트워크 인터페이스 사이의 DoS 공격 실험 결과.
Fig. 8. Results of DoS attacks Experiment between wired interface and wireless interface

워크 인터페이스에 연결되어 있어 DoS 공격에 매우 큰 영향을 받고 있다. Ping RTT는 128.04ms에서 477.87ms로 4배 가까이 증가하였고, 손실률은 최고 52.4%에 달했다.

그림 8-(b)의 Ping h3-h8은 공격받지 않는 wlan1에 연결된 무선 IoT 디바이스와 공격받고 있는 wlan2에 연결된 무선 IoT 디바이스와의 통신 상태를 나타낸다. 이 경우의 Ping RTT는 118ms에서 1198ms로 10배 가까이 통신 속도가 느려졌으며, 손실률은 최고 7%에 달했다.

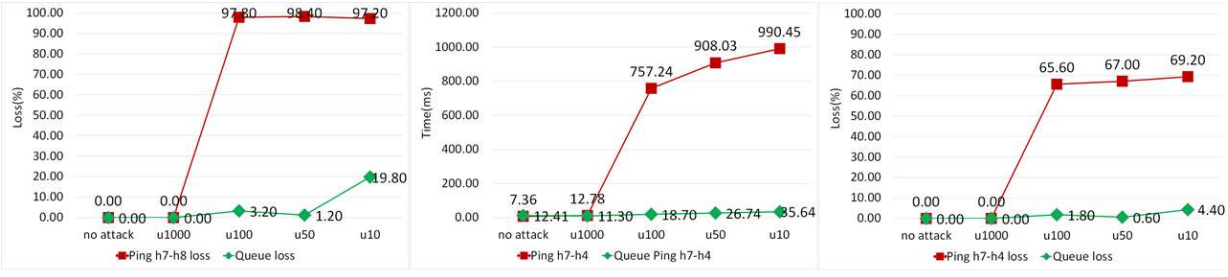
그림 8-(c)의 Ping h4-h1은 유선 IoT 디바이스와 공격받지 않는 무선 네트워크 인터페이스인 wlan1에 연결된 무선 IoT 디바이스와의 통신 상태를 나타낸다. 이 경우에는 DoS 공격에 대한 영향이 전혀 없을 알 수 있다.

이를 통해, 유선 인터페이스와 무선 인터페이스 모두 DoS 공격을 직접 받지 않는다면, DoS 공격에 대한 영향이 없음을 알 수 있다.

4.4 QoS 기능 적용

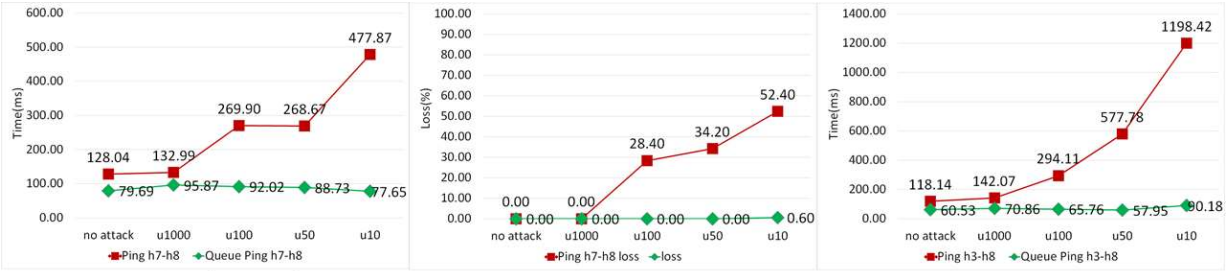
이번 절에서는 DoS 공격의 영향을 많이 받은 공격 상황을 선택하여 Queue 관리 기능을 적용하고, 그에 따른 결과를 산출한다. Queue 관리 기능은 IoT 디바이스에서 생성된 공격 플로우에 적용하였다. Queue 기능을 적용할 시에는 각 공격 플로우마다 최대 bit 전송률을 0.1Kb/s로 설정하였고, 최소 bit 전송률을 0.01Kb/s로 설정한다. 예를 들어, 그림 7처럼 Host 3에서 Host6로 DoS 공격이 이루어지는 경우는 DoS 공격 플로우가 무선 네트워크 인터페이스인 wlan1과 wlan2를 거쳐 흘러가게 된다. 이러한 플로우에 위와 같은 Queue 관리 기능을 적용한다. 이러한 방법으로 플로우의 최대 bit/s 전송률을 설정하게 되면 네트워크 인터페이스에 대량의 DoS 공격 플로우가 입력되는 즉시 제한하기 때문에 다른 네트워크 인터페이스의 QoS를 보장할 수 있다.

그림 9는 그림 7의 공격 상황에서 Queue 관리를 시행한 결과를 보여준다. 그림 9-(a)를 보면, Queue 관리를 시행하기 전에 100%에 가까운 손실률이 최소 1.2%, 최고 19.80%로 현저하게 낮아지는 것을 볼 수 있다. 또한, 그림 9-(b)를 보면 990.45ms 였던 Ping RTT가 최고 35.64ms까지 속도가 빨라지는 것을 볼 수 있다. 그림 9-(c)를 보면 69.20%에 달했던 손실률이 최고 4.40%로 현저하게 줄어든 것을 볼 수 있다.



(a) 그림7-(d)의 손실률 비교 (b) 그림7-(e)의 Ping RTT 비교 (c) 그림7-(e)의 손실률 비교

그림 9. 서로 다른 무선 네트워크 인터페이스 사이의 DoS 공격 상황에 Queue 관리 기능 적용 결과.
Fig. 9. The result of the Queue Management Function applying for DoS attacks between different wireless network interfaces.



(a) 그림8-(a)의 Ping RTT 비교 (b) 그림8-(a)의 손실률 비교 (c) 그림8-(b)의 Ping RTT 비교

그림 10. 유선 네트워크 인터페이스와 무선 네트워크 인터페이스 사이의 DoS 공격 상황에 Queue 관리 기능 적용 결과.
Fig. 10. The result of the Queue Management Function applying for DoS attacks between a wired network interface and a wireless network interface.

그림 10-(a)를 보면, 477ms에 달했던 Ping RTT가 Queue 관리 기능 적용이후 최고 95.87ms로 매우 빨라졌다. 그림 10-(b)를 보면 52.4%에 달했던 손실률이 거의 0%에 가까워졌다. 그림 10-(c)를 보면 1198.42ms에 달했던 Ping RTT가 최대 80.18ms까지 매우 빨라진 것을 확인 할 수 있다.

이를 통해, IoT 게이트웨이 환경에서 DoS 공격이 발생하였을 때 IoT 게이트웨이의 Queue 관리를 통해 DoS 공격으로 인한 IoT 디바이스의 통신 영향을 줄일 수 있음을 증명하였다.

Ⅴ. 결 론

본 논문에서는 다양한 구성요소를 가지는 SDN기반 IoT 게이트웨이 환경에서 DoS 공격에 대한 영향을 알아보기 위하여 2개의 무선 네트워크 인터페이스를 가진 SDN기반 유무선 IoT 게이트웨이를 구현하였다. 이후 IoT 게이트웨이 환경에 DoS 공격이 발생할 경우 각 IoT 디바이스들의 통신 상태를 실험하였다. 실험 결과, 한 개의 무선 네트워크 인터페이스 내부에서 DoS 공격이 발생 했을 경우에는 다른 무선 네트워크 인터페이스에 연결된 IoT 디바이스들은 영향을 받지 않는 것으로 나타났다. 그러나, 한 무선 네트워크 인터페이스에서 다른 무선 네트워크 인터페이스로 공격이 가해질 경우, 두 인터페이스에 연결된 무선 IoT 디바이스들이 영향을 받는 것으로 나타났으며, 무선에서 무선 공격 상황에서는 유선-유선 통신은 영향을 받지 않는 것으로 나타났다. 이러한 결과를 종합하여 보면, 무선 IoT 디바이스가 DoS 공격을 받거나 공격을 수행한다면 같은 무선 네트워크 인터페이스에 연결된 무선 IoT 디바이스들은 통신에 영향을 받는 것으로 나타났다.

이러한 결과에 따라, DoS 공격 발생시 IoT 디바이스의 QoS를 유지하기 위해 Queue 관리 기능을 적용하였다. 적용 후의 결과와 이전 결과의 통신 속도와 손실률을 비교하여 DoS 공격 발생시 IoT 게이트웨이의 Queue 관리가 충분한 효과가 있음을 증명하였다. 하지만, 이러한 Queue 관리는 네트워크 인터페이스 단위로 수행되기 때문에, 다수의 무선 IoT 디바이스가 1개의 무선 네트워크 인터페이스에 연결되는 특성상 하나의 무선 네트워크 인터페이스에 연결된 무선 IoT 디바이스 각각의 QoS를 보장하기 힘들다. 때문에, 중요한 무선 IoT 디바이스의 QoS를 유지하기 위해서는 무선 IoT 디바이스를 다수의 무선 네트워크 인터페이스에 분산시켜 연결시킨 후, Queue 관리를 수행한다면 더 효과적일 수 있다. 이에 따라, Queue 관리를 동적으로 수행하는 기술을 연구하여 더욱 효과적인 Queue 관리 기능을 구현할 계획이다.

References

[1] 유성경, " 미라이 봇넷, IoT의 DDoS 공격 ①" (2017), 접속일시(8. 28. 2017), http://news.grayhash.com/category/malware/%EB%AF%B8%EB%9D%BC%EC%9D%B4%20%EB%B4%87%EB%84%B7.

[2] http://www.gartner.com/newsroom/id/3165317.

[3] 현대경제연구원. "사물인터넷(IoT) 관련 유망 산업 동향 및 시사점". 2016. 07. 11.

[4] Jintae Choi, Kyungbaek Kim, "Analysis of wireless and wired DDoS Attack under IoT environment", knom, 2017.

[5] 한국인터넷진흥원, "2016년 Mirai 악성코드 동

향” 2016. 12

[6] Yungee Lee, Wangkwang Lee, Giwon Shin, Kyungbaek Kim, “Assessing the Impact of DoS Attacks on IoT Gateway.” 11th KIPS International Conference on Ubiquitous Information Technologies and Applications (CUTE 2016), December 19-21, 2016, Bangkok, Thailand

[7] 백상헌, 장인선, 서동은, 이종화 (2015). 미래 네트워크의 새로운 패러다임 SDN/NFV에 대하여. 한국통신학회지(정보와통신), 32(7), 82-92.

[8] Ki-Taek Lee, Seung-soo Baek, Seung-joo Kim, "Study on the near-real time DNS query analyzing system for DNS amplification attacks." Journal of the Korea Institute of Information Security & Cryptology 25(2), 303-311 (9pages), 2015. 4.

[9] 한국인터넷진흥원, “NTP 서버 보안 가이드”, 2015. 1

[10] Ju-Hye Oh, Keun-Ho Lee. "Attack Scenarios and Countermeasures using CoAP in IoT Environment." Journal of the Korea Convergence Society 7.4 (2016): 33-38.

[11] Seung-Hoon Baek, “Open vSwitch와 Mininet을 이용한 가상 네트워크 생성과 OpenDaylight를 사용한 네트워크 제어 실험” 15. 2015, https://www.slideshare.net/rkawkxms/2015316opendaylight-45868170

[12] Sinh Ngoc Nguyen, Yungee Lee, Wangkwang Lee, Giwon Shin, kyungbaek kim, “Design of SDN based IoT Gateway for detecting and Preventing DoS attack”, 2016년도 한국스마트미디어학회(KISM) 추계학술대회 논문집, pp. 223-225, 호남대학교, 광주, October 28-29, 2016

최 진 태 (Jin-tae Choi)

2017년 2월 : 조선대학교 정보통신공학과 학사

2017년 3월~현재 전남대학교, 정보보안협동과정 석사과정

<관심분야> 네트워크 트래픽 분석, 정보보안

뉘엔 신 응억 (Sinh Ngoc Nguyen)

2009: VietNam National University Ho Chi Minh City - University of Information Technology (B.S. Degree)

2016: Chonnam National University, South Korea (M.S. Degree).

2013~2015: Software Engineer at Integrated Circuit Design Research and Education Center

2016~now : School of Electronics and Computer Engineering

김 경 백 (Kyungbaek Kim)

1999년 : 한국과학기술원 전기 및 전자공학과 학사 졸업

2001년 : 한국과학기술원 전기 및 전자공학과 석사 졸업

2007년 : 한국과학기술원 전기 및 전자공학과 박사 졸업

2007년~2011년 : University of California Irvine, 박사 후 연구원

2012년~2015년 : 전남대학교 전자컴퓨터공학부 조교수

2016년 ~ 현재 : 전남대학교 전자컴퓨터공학부 부교수

<관심분야> 분산시스템, 미들웨어, 피어투피어/오버레이 네트워크, 소셜 네트워크, SDN>