Assessing the Impact of DoS Attacks on IoT Gateway

Yungee Lee[1], Wangkwang Lee[1], Giwon Shin[1] and Kyungbaek Kim[1]

[1] Department of Electronics and Computer Engineering,
Chonnam National University, Gwangju, South Korea
negee1564@naver.com, kwang9092@gmail.com,
giwonie@gmail.com, kyungbaekkim@jnu.ac.kr

Abstract. Internet of Things (IoT) becomes more popular, and things are connected to each other through wired or wireless communication methods. Though things are connected with various methods easily, it attracts network attackers who exploit these open and convenient network connections in order to obtain unjustified information and benefits or to subvert various IoT systems. Especially, Denial of Service (DoS) attack becomes a serious problem on IoT system where huge number of devices are connected to. These devices are usually connected to IoT gateways in order to send packets to Internet. However, currently the impact of DoS attack on an IoT gateway, which has various interfaces such as wireless LAN interface and wired LAN interface, is not well examined. In this paper, we assess the impact of DoS attack on an IoT gateway with various scenarios. We implemented a prototype of an IoT gateway which has wired and wireless network interfaces by using Raspberry Pi, OpenWRT, and OVS (Open vSwitch). With this prototype, we evaluated various DoS attack scenarios on this IoT gateway. Through this evaluation, we observed the severity of DoS attack on IoT gateways, especially for wireless connections.

Keywords: Internet of Things, Gateway, Denial of Service attack

1 Introduction

Everything is connected to Internet in anytime and anywhere. The concept of ubiquitous era is not a story of future life any more, but current technology of Internet of Things (IoT) becomes a popular and powerful tool to realize it.

Internet of Things lets everything connect to Internet, and provides communication methods between humans and devices or between devices and devices. Through this rich communication methods and intelligence services with these open and collaborative connections, IoT is considered as one of the essential technologies such as Artificial Intelligence (AI) which will lead the forth industry innovation. An example of intelligent IoT system is a smart streetlamp which monitors human activities, analyze the activities on the centralized server and turns on the lamp automatically under given conditions. Not only this simple example, various life appliances such as smart phones, refrigerators and televisions can collaborate to each other and more intelligence services through network connections. Consequently, IoT technology let people control everything with a small device in their palm.

However, this easy and convenient control of everything may be a serious problem of network security. That is, the IoT intelligence system with basic vulnerability of network security may be exploited by network attackers in order to obtain unjustified information and benefits or to subvert the intelligence system. In practice, a general IoT based smart home service uses a gateway in order to connect the various devices in a house. In this case, if the gateway is manipulated by attackers, every device connected to the gateway becomes target of network attacks or means for various network attacks such as bots for DoS (Denial of Service) attack [1]. Even though the gateway is not manipulated, if some malicious devices are connected to the gateway, they can initiate DoS attack to hamper the communication between the normal devices. Lately, the source code of Mirai, which is a powerful DDoS tool managing over 300K IoT device bots easily, is released, and the possibility of new types of bot nets for IoT DoS attack increases significantly.

Along with the development of IoT industry, the number of devices connected to IoT system and the volume of data traffic in IoT system increases substantially. This increase of complexity of IoT system lead more vulnerability of DoS attacks. In this paper, we evaluate the impact of DoS attacks under IoT gateway in the aspects of communication ability between IoT devices. Through this evaluation we show the importance of DoS attack detection and prevention on IoT gateway.

2 Backgrounds

2.1 Internet of Things (IoT)

Internet of Things (IoT) lets everything in our life environment connected to each other through wired or wireless communication method, and enables these things to exchange data for collaboration. The concept of IoT has been already used in various area such as wearable health care devices and self-managing refrigerators. Recently Korean government selects IoT as a key technology for leading future industry, and early this year Korean government represents a stimulating strategy supporting tax credits to companies for conducting the research and development of IoT up to 30%. Also, many companies including big-size as well as medium size companies focus on developing IoT technologies to preempt the share of IoT Industry.

2.2 Denial of Service (DoS) Attack

Denial of Service (DoS) attack is an attack to make an online service unavailable by overwhelming it with traffic from tens or hundreds of PC in short time. Attackers makes the tons of traffic which is cannot afforded by a server or a network, so general users cannot use the server or the network normally. Generally, attackers install malicious bot control program to other PCes, and control these manipulated PCes in remote. By using this ability of remote control, attackers initiates DoS attack in remote easily by using an automation program for generating heavy traffic from these zombie pc at the same time. The severity of DoS attack is also that it is easy to generate meaningless heavy traffic, and in IoT environment without basic security concerns it is easy that attackers get network connections to many other devices [3].

2.3 OpenWRT

OpenWRT is a Non-Real-Time Linux based open source operating system for a wireless LAN router, and it supports most router platforms [2]. OpenWRT provides various Linux features required by wireless LAN router conveniently as Linux packages. Also, OpenWRT supports ipkg (or opkg) as a package management system for users to install various kinds of software on OpenWRT, and it provides very high flexibility in its usage.

3 Implementation of a prototype of an IoT gateway

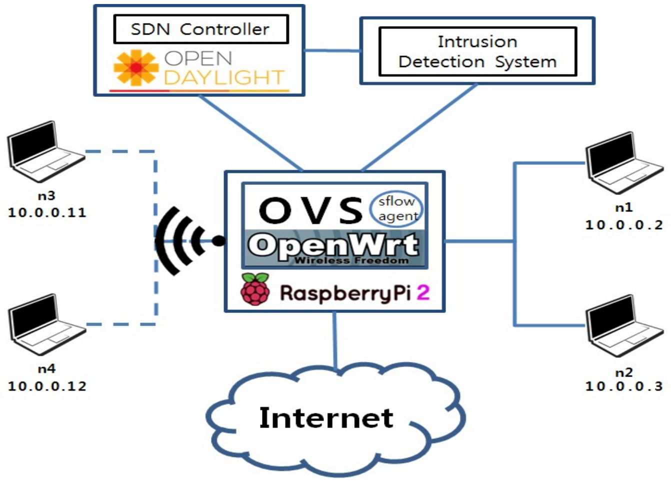


Fig. 1. Architecture of a prototype IoT gateway and connected devices.

To evaluate the impact of DoS attack on IoT gateway, we implemented a prototype of IoT gateway by using Raspberry Pi 2, OpenWRT and Open vSwitch(OVS). The basic architecture of the prototype implementation of our IoT gateway is shown in Fig. 1. The implemented IoT gateway has three Ethernet interface and one Wifi interface. Among these interfaces, two Ethernet interfaces and one WiFi interface are bound in a bridge of OVS, and one Ethernet interface is used for connecting to Internet. With this IoT gateway, we connect four devices (n1, n2, n3, and n4). Two devices, n1 and n2, are connected with Ethernet (wired) interfaces, and other two devices, n3 and n4 are connected with WiFi (wireless) interface.

In this implementation, we consider the ability of DoS detection and prevention discussed in past efforts [4][5][6] and attach an intrusion detection system such as SNORT and a SDN controller for controlling flow traffic to our IoT gateway.

For the implementation of IoT gateway and devices, we use the same WiFi interface module and its detail characteristics are described in Table 1. And for the devices connected with wireless interface, n3 and n4, the distance between the device and the IoT gateway set to 5m.

Table 1. Setup of 802.11 Wireless LAN

Category	Specification
Chipset	Realtek 8188
Bandwidth	20Mhz
Channel	11 (2.462 Ghz), single channel
TX Power	20MHz

4 Evaluation of the Impact of DoS attack on an IoT gateway

By using the implemented IoT gateway, we emulated various scenarios of DoS attack on IoT gateways, and evaluated the impact of different kinds of DoS attack. We consider for difference DoS attack scenarios in the aspect of interfaces of an attacker and a target; wired to wired attack, wireless to wireless attack, wireless to wired attack and wired to wireless attack. We generated the SYN flooding traffic as DoS attack traffic by using hping3 program. Under this DoS attack, we confirm that our intrusion detection system can detect the attack traffic and SDN controller can prevent the flow successively.

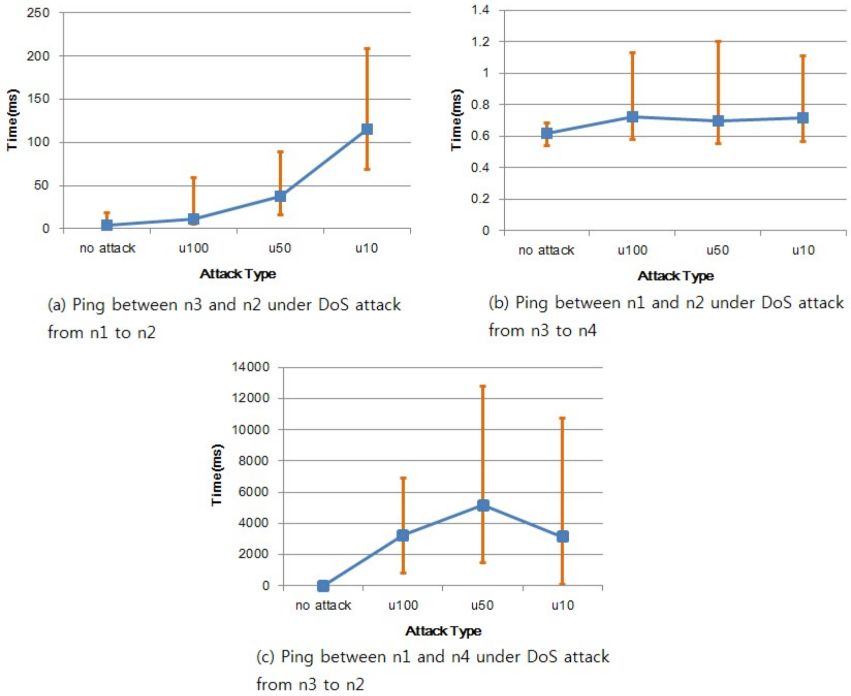
In this evaluation, we focus on assessing the impact of DoS attack, and we turn off the DoS detection functionality of our IoT gateway. Then, we measure the average round trip time of ping messages for 1 minutes between legitimate devices attaches to IoT gateway under various kinds of DoS attack. We tested each DoS attack in three times and obtain the average value of the round trip time.

To evaluate the detail impact of DoS attack, we change the rate of DoS attack by using different rate such as 1000 packets in a sec (u100), 2000 packets in a sec (u50) and 10000 packets in a sec (u10).

Fig. 2 illustrate the average round trip time between legitimate devices under various kinds of DoS attacks. In this figure, we use device notations such as n1, n2, n3 and n4 described in Fig 1.

4.1 DoS attack from wired interface to wired interface

For evaluating wired to wired DoS attack, we initiated a DoS attack from n1 to n2, then measured the round trip time of ping between n3 and n2 like Fig. 2(a). We observed that the ping time increases along with the increase of DoS attack traffic.



(a) Ping between n3 and n2 under DoS attack from n1 to n2

(b) Ping between n1 and n2 under DoS attack from n3 to n4

(c) Ping between n1 and n4 under DoS attack from n3 to n2

Fig. 2. Average round trip time between legitimate devices under various DoS attack

4.2 DoS attack from wireless interface to wireless interface

For evaluating wireless to wireless DoS attack, we initiated a DoS attack from n3 to n4, then measured the round trip time of ping between n1 and n2 like Fig. 2(b). Interestingly, DoS attack between wireless devices does not affect the performance of ping between wired devices. It is because the attack traffic does not bother the legitimate traffic.

4.3 DoS attack from wireless interface to wired interface

For evaluating wireless to wired DoS attack, we initiated a DoS attack from n3 to n2, then measured the round trip time of ping between n1 and n4 like Fig. 2(c). In this case, even though only u100 case DoS attack affects the round trip time between legitimate devices significantly. It is because the packets from wireless interface bother the packets from wired interfaces. Also, we observed lots of packet loss from DoS attack traffic (more than 70%), it is because of the difference of bandwidth between wireless interface and wired interface.

4.4 DoS attack from wired interface to wireless interface

For evaluating wired to wireless DoS attack, we initiated a DoS attack from n1 to n3, then measured the round trip time of ping between n3 and n4. But in this case, we cannot measure the time for ping because n3 and n4 lose their connection to IoT gateway. In this case, the DoS attack traffic which is generated by wired interface overwhelm the queue of wireless interface and drop the heartbeat packets for maintaining wireless connections.

5 Conclusion and Future Works

IoT technology gains huge attentions for future industry, and more and more devices are attached to IoT gateway for collaborating each other with more intelligent services. In this case, DoS attack on IoT gateway may be a critical challenge to maintain intelligent IoT services. Through the implementation based evaluation of DoS attack on IoT gateway, we observed that the wired to wireless type DoS attack is most severe attack on IoT gateway, and realized that it is important to monitor wireless traffic carefully in order to providing effective DoS attack detection and prevention in IoT gateways.

Acknowledgments. This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIP) (R0110-16-1001, Secure hardware containers technology to protect IoT devices from Denial of Service attack)

References

1. ETNEWS, IoT devices are used for DDoS attack, (http://www.etnews.com/20141029000125), 2014
2. OpenWRT, What is OpenWRT?, (https://openwrt.org)
3. Rudman L, Irwin B, Characterization and analysis of NTP amplification based DDoS attacks, In Information Security for South Africa (ISSA), 2015 2015 Aug 12 (pp. 1-5). IEEE.
4. Raza, Shahid, Linus Wallgren, and Thiemo Voigt. SVELTE: Real-time intrusion detection in the Internet of Things, Ad hoc networks 11.8 (2013): 2661-2674.
5. Yungee Lee, Seounguk Kim, Duc Tiep Vu, Kyungbaek Kim, Sampling based Network Flooding Attack Detection/Prevention System for SDN, KISM Smart Media Journal, pp. 24-32, Dec 31, 2015.
6. DucTiep Vu, Kyungbaek Kim, Evaluation of Network Flooding Attack Detection/Prevention System for SDN in KOREN Network, In Proceedings of 2016 KISM, April 29-30, 2016, Silla University, Busan.