Taylor & Francis
Taylor & Francis Group

Automatika

Journal for Control, Measurement, Electronics, Computing and Communications

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/taut20

# Countermeasures against large-scale reflection DDoS attacks using exploit IoT devices

Yong-joon Lee, Hwa-sung Chae & Keun-wang Lee

**To cite this article:** Yong-joon Lee, Hwa-sung Chae & Keun-wang Lee (2021) Countermeasures against large-scale reflection DDoS attacks using exploit IoT devices, Automatika, 62:1, 127-136, DOI: 10.1080/00051144.2021.1885587

**To link to this article:** https://doi.org/10.1080/00051144.2021.1885587



Published online: 19 Feb 2021.

AUTOMATIKA
2021, VOL. 62, NO. 1, 127–136
https://doi.org/10.1080/00051144.2021.1885587



# Countermeasures against large-scale reflection DDoS attacks using exploit IoT devices

Yong-joon Lee [a], Hwa-sung Chae [b] and Keun-wang Lee [c]

[a]Department of Cyber Security, Far East University, Chungbuk, Republic of Korea; [b]IT Nomads Co., Ltd, Seoul, Republic of Korea; [c]Department of Multimedia Science, Chungwoon University, Incheon, Republic of Korea

**ABSTRACT**
With the of utilizing IoT devices increasing recently, such devices are being infected with malicious codes and being used to carry out DDoS attacks. In particular, there have been cases of large-scale DDoS reflex attacks of 100GB or more using IoT devices such as wireless sharing devices, CCTVs and smart cars. There is a vulnerability that is being exploited for attacks through Simple Service Discovery Protocol (SSDP) to search for IoT devices. This study examines different types of IoT devices used in DDoS attacks, and conducts experiments in which reflection DDoS attacks are carried out on IoT devices in order to measure the attack threat levels. This study also suggests methods that IoT service operators can employ to remove IoT device vulnerabilities, as well as effective countermeasures that Internet service operators can apply to address reflection DDoS attacks that exploit IoT devices.

**ARTICLE HISTORY**
Received 19 October 2019
Accepted 27 January 2021

**KEYWORDS**
IoT (Internet of Things); SSDP (Simple Service Discovery Protocol); DDoS (Distributed Denial of Services) attack; reflection DDoS attack

## 1. Introduction

It's not surprising that the Internet of Things (IoT) market continues to grow at a rapid pace. According to a 2018 research report by Bain & Company, the IoT market is expected to be worth USD 520 billion by 2021, which is twice the size of the 2017 market. This means that connections for IoT devices are expected to increase by 127 connections per second and, that such connections areexpected to grow for years to come [1].

According to an analysis conducted by the Internet and Television Association (NCTA), the number of IoT devices is expected to surpass 50 billion by 2020 [2]. Since IoT devices are particularly vulnerable to hacking, this increase in IoT devices gives attackers ample opportunity to attack, letting them set up large-scale botnets via malware-infected IoT devices and facilitating large-scale DDoS attacks [3]. According to research conducted by Eurecom, hackers have already developed a new type of malware specifically targeting IoT devices. This development serves as further proof that the era of IoT-based DDoS attacks is already upon us [4].

Additionally, some IoT malwares have already become notorious around the globe. One example is Mirai malware, which rendered several high-profile websites such as Reddit and GitHub inaccessible [5]. According to the DDoS Weapon Report, published in the 4th quarter of 2018, five of the top-ranking malwares for IoT devices that are blocked by security systems belong in the Mirai category. Reported attacks on Xbox Live and the PlayStation Network are from a sixth type of malware [6].

Most of these IoT malwares are from the United States, Italy, the United Kingdom, and Germany. Since the use of wired/wireless routers, IP cameras, smart home appliances, and other IoT systems and devices is so widespread in these countries, they are almost never safe from malware [7]. The threat of malware is compounded by the fact that many IoT device manufacturers still don't take security vulnerabilities into serious consideration when releasing their products in the market. It has even been found that some devices are extremely susceptible to outside attacks via their Telnet port, and attackers can simply download and run malware on such devices [8]. At the very least, most IoT devices are vulnerable to potential DDoS attacks at anytime [9].

As IoT devices have become smaller, they have become more vulnerable to attacks, and recently, there have been increased reports of DDoS attacks that spoof the source IP address of IoT devices [10]. DDoS attacks using IoT devices are cyber attacks that cause bandwidth overload by increasing traffic on the network to make services unavailable. These types of attacks, targeting national broadcasting, financial, and Internet-based services, have been increasing. Recently, DDoS attacks via SSDP (Simple Service Discovery Protocol), used by IoT devices such as home appliances, wireless routers, or CCTVs (Closed-Circuit Televisions), have been increasing [11].

DDoS attacks that use the vulnerabilities of SSDP for searching for IoT devices such as smart TVs, printers, scanners, IP-based CCTVs, and wireless routers, which

**CONTACT** Yong-joon Lee yjlee4279@gmail.com Department of Cyber Security, Far East University, Chungbuk, 27601, Republic of Korea

are major devices on a smart home network, have been growing rapidly [12]. Unlike existing DDoS attacks, which infect IoT devices using malware, this type of DDoS attack exploits the vulnerabilities of the device's communication protocol [13]. South Korea is particularly vulnerable to DDoS attacks using IoT devices as it has the third largest number of IoT-connected devices in the world, after China and the United States [14].

In this type of DDoS attack, the attacker intentionally exploits the vulnerabilities of SSDP for IoT devices [15]. SSDP allows a device to search for and communicate with other devices connected to the same network. The attacker constantly sends packets to the system using the vulnerabilities of SSDP. These types of attacks can easily generate over 50 gigabytes of traffic [16].

This study is intended to present a multi-level defense system for communication protocol L2 and L7 to counteract DDoS attacks using IoT devices. Additionally, this study presents a method to remove the vulnerabilities of IoT devices to DDoS attacks, which is necessary for the operation of a multi-level defense system. Furthermore, this study demonstrates the suggested method by using actual tests that apply DDoS attack blocking patterns.

Additionally, the tests conducted as part of this study showed that the multi-level DDoS countermeasures proposed in this study can successfully protect actual IoT devices against DDoS attacks. As such, this study can contribute to the development of effective countermeasures against the rapid increase of IoT device-based DDoS attacks.

In Chapter 2 of this study, the features and characteristics of SSDP—an IoT device searching protocol—and DDoS attacks are analyzed against the backdrop of previous studies, and in Chapter 3, a multi-level DDoS attack blocking measure and blocking patterns are presented. In Chapter 4, actual methods used to block DDoS attacks that target IoT devices and generate DDoS attack traffic are analyzed through tests. The results of this study and final conclusions are presented in Chapter 5.

## 2. Previous studies

DDoS attacks on IoT devices typically proceed as follows. The attacker identifies the type of IoT device on the Internet, and then identifies the vulnerabilities of the communication protocol used by the IoT device. Finally, the attacker makes a service request to the vulnerable IoT device, and concentrates the responses of the device(s) on the target server to interrupt the service. In order to identify the progression of DDoS attacks, analyses have been conducted on UPnP middleware, which searches for IoT devices, and SSDP, which exchanges IoT device information. Research has also been conducted on the methods and characteristics of DDoS attacks as they relate to SSDP [17].

Under normal circumstances, the SSDP protocol is used to allow UPnP devices to broadcast their existence to other devices on the network. For example, when a UPnP printer is connected to a typical network, after it receives an IP address, the printer is able to advertise its services to computers on the network by sending a message to a special IP address called a multicast address. The multicast address then tells all the computers on the network about the new printer. Once a computer hears the discovery message about the printer, it makes a request to the printer for a complete description of its services. The printer then responds directly to that computer with a complete list of everything it has to offer. An SSDP attack exploits that final request for services by asking the device to respond to the targeted victim.

### 2.1. UPnP

Figure 1 UPnP (Universal Plug and Play) combines TCP/IP, UDP, HTTP and XML technologies and has a middleware structure that is connected using a Peer-to-Peer method. In this structure, the device sends notifications to itself via the UDP broadcast and registers the information of other nearby devices. This type of technology is used by DLNA (Digital Living Network Alliances), PlayStation, Xbox, printers, and scanners [18].

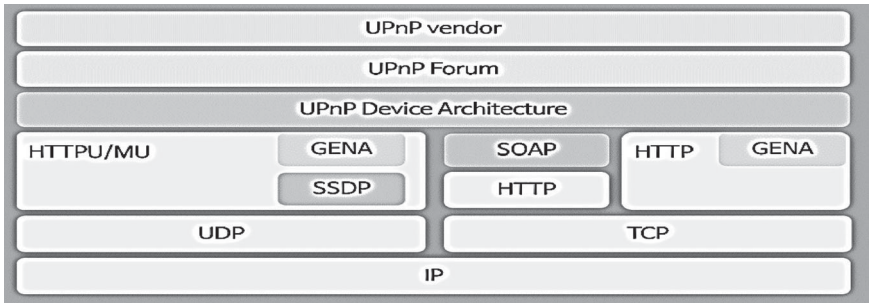


**Figure 1.** UPnP (Universal Plug and Play) middleware.

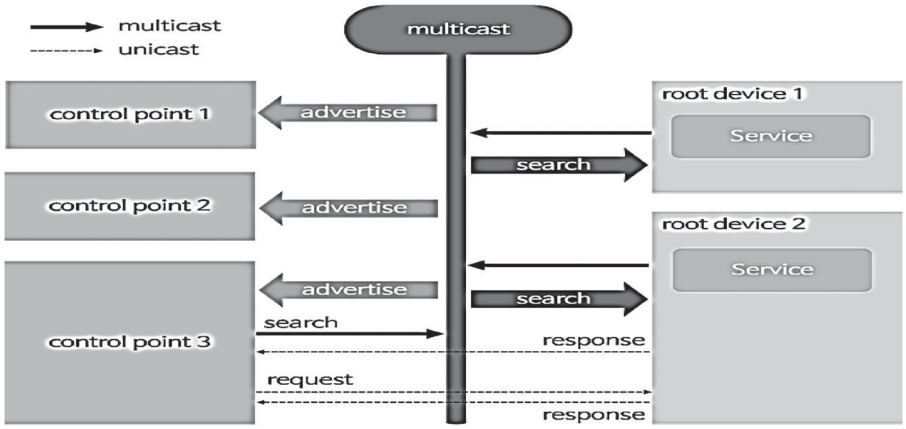


**Figure 2.** SSDP (Simple Service Discovery Protocol).

```
M-SEARCH * HTTP/1.1
Host:239.255.255.250:1900
ST:urn:schemas-upnp-org:device:InternetGatewayDevice:1
Man:"ssdp:discover"
MX:3
```

**Figure 3.** SSDP M-SEARCH request.

```
HTTP/1.1 200 OK
ST:upnp:rootdevice
SERVER: Custom/1.0 UPNP/1.0 Proc/ver
USN:uuid:b830ce10-7277-11e3-8730-
```

**Figure 4.** SSDP M-SEARCH response.

### 2.2. SSDP

Figure 2 SSDP (Simple Service Discovery Protocol) is a protocol used to search services or information on the same network. SSDP, which is a UDP-based HTTP, uses HTTPU and communicates all data in text and takes the UDP 1900 port for IP multicast address [19].

The multicast address for IPv4 is 239.255.255.25, and that for IPv6 is generally ff0x::c. Generally, SSDP is used when a UPnP device performs a network search [20].

As seen in Figure 3, the SSDP header field makes a request for M-SEARCH ∗ HTTP/1.1 information to Host: 239.255.255.250:1900, which is an IoT device that is searched in the form of a general HTTP communication defined in RFC 2610.

As seen in Figure 4, the IoT device responds to the HTTP/1.1 200 0 K and provides information of UPNP [21].

### 2.3. SSDP reflection attacks

IoT devices communicate with each other using SSDP, which utilizes UDP as an underlying transport protocol. UDP does not require any authentication procedures for communication, and for IoT devices, security settings are generally not configured and/or default settings are applied [22]. This renders any device that uses SSDP vulnerable to reflection DDoS attacks. SSDP for IoT devices uses a UDP/1900 port number, and UDP is vulnerable in that it responds to communication requests without any separate authentication procedures. Therefore, an SSDP reflection attack that exploits the vulnerabilities of IoT devices can proceed as shown below in Figure 5 [23].

(1) The attacker transmits a command to multiple zombie PCs through C&C (command & control).
(2) A zombie PC that has received a command from the hacker spoofs the IP address of the original PC as a target IP and makes a large-scale communication request to multiple IoT devices.
(3) The IoT devices that receive the communication request respond to the spoofed IP address without any separate authentication procedures, due to the nature of UDP. The target server goes into a state of service denial due to the large-scale response from the IoT devices, and this eventually depletes the network bandwidth.

### 2.4. Characteristics of SSDP reflection attacks

In an SSDP reflection attack, the source port is 1900, which is taken by the device that is used for the attack. Although UDP is used for this type of attack, an HTTP header is included. UPnP Server information is also included, and the size of the response varies depending on the device being used for the attack [24].

The reason SSDP is often exploited for DDoS attacks is because it is easy to spoof the source IP address using UDP, and consequently, the attack is hard to track. Since SSDP notifications can be sent by broadcast or multicast, a single UDP packet can be sent throughout the entire system, and even when a request is made, the

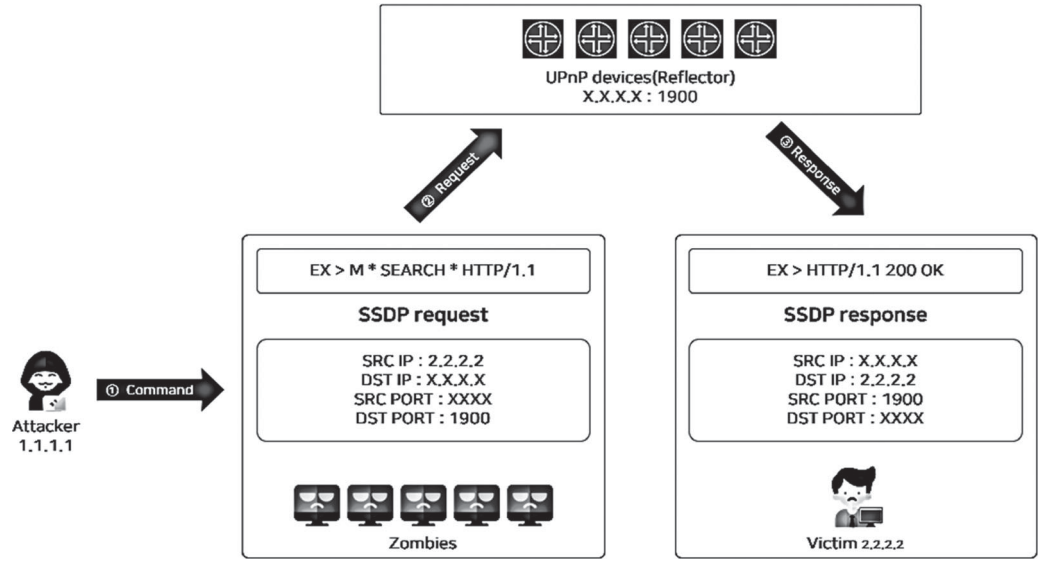


**Figure 5.** SSDP reflection attacks procedures.

system must interpret the URL of the related device using the location header, which leads the system into a LooP, making it use up its CPU resources [25].

## 3. Response system to DDoS attacks that exploit IoT devices

In order to protect IoT devices from DDoS attacks, it is necessary to set up a multi-level defense system with multi-hierarchical security equipment. To effectively defend against UDP and HTTP information exchange, which is a key characteristic of IoT DDoS attacks, it is necessary to establish security equipment for each communication layer, and an integrated defense system through data analysis specific to each level of the hierarchy. A multi-level defense system should be set up for the L3 hierarchy and the L7 hierarchy, and information should be shared between these two hierarchies to ensure an effective defense against IoT DDoS attacks [26].

### *3.1. Multi-level defense system against IoT DDoS attack*

Figure 6 illustrates the concept of safeguarding against IoT DDoS attacks using each level of the communication hierarchy. If a DDoS attack packet is identified, the UDP defense is activated at L3, Stage 1, and the HTTP defense is activated at L7, Stage 2 to reduce attack traffic.

In an L3 hierarchy defense, attacks on the L3 hierarchy, mainly large-scale flooding, are neutralized. Examples of attacks corresponding to the L3 hierarchy include TCP, UDP, ICMP, and IGMP flooding attacks. The defense mechanisms used against these types of attacks mainly include blocking large-scale flooding [27]. Since IoT DDoS attacks involve UDP, defense mechanisms are activated in the L3 hierarchy. The multi-level defense mechanism is intended to efficiently defend the upper levels of the hierarchy (L7) from attack, and the defense mechanism against L3 attacks can be engaged prior to engaging the multi-level defense mechanism [28]. The multi-level defense mechanism blocks attacks in the optimal hierarchy, where attacks can be neutralized the most effectively.

This study proposes procedures for a multi-level defense mechanism as shown in Figure 7. Unlike TCP, UDP packets are not connection-oriented, so thus UDP communication sessions are stored in the system's memory from beginning to end to check communications. In UPD communications, the initial communication history can be stored, and the IP address can be identified. If the IP address constantly generates requests, this stored information can be used to determine whether the requests are part of a DDoS attack. If traffic is continuously transmitted from the same IP address, a threshold can be set to control the traffic [29].

It is also possible to defend against DDoS attacks using SSDP HPPT codes. This method can be easily implemented by reconfiguring the preference settings of the web server. Using this method, if an IoT DDoS attack is suspected, it is possible to check whether the SSDP has been modified and to block the attack [30].

### *3.2. Countermeasures against IoT DDoS attacks*

- **Countermeasures for IoT device vulnerabilities**

As shown in Figure 8, many IoT device users don't change the default settings of their devices after purchase.

If the IoT device manufacturer activates the UPnP function and then releases the product to the market, the UPnP function remains activated until the user deactivates it. If this function remains activated, the device can easily be exploited as a reflector for SSDP

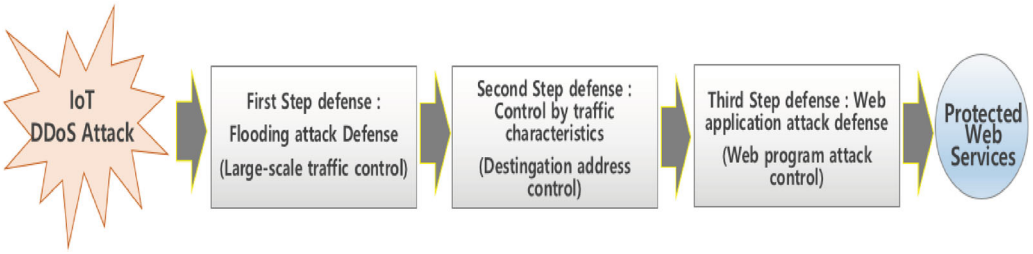


**Figure 6.** Multi-level response to IoT DDoS attacks.

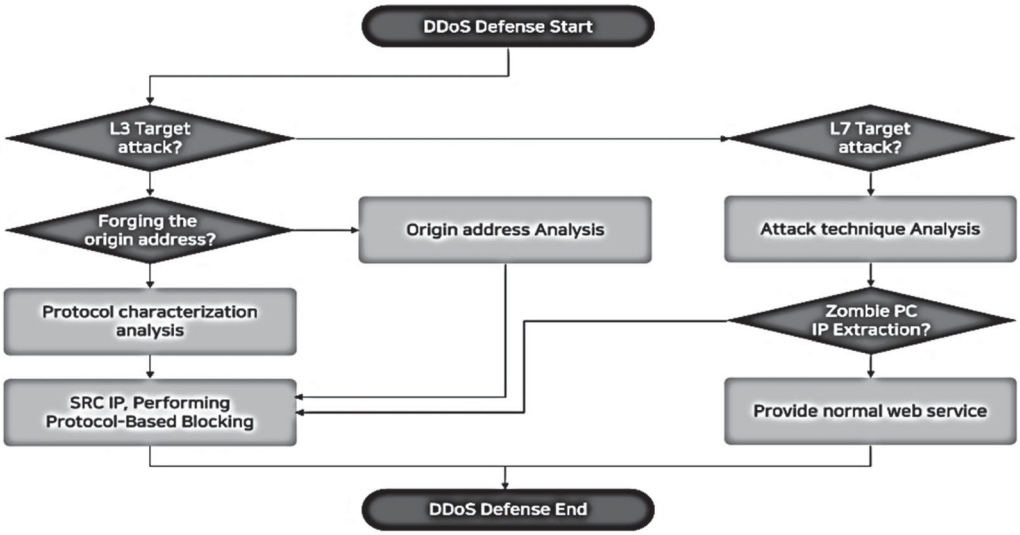


**Figure 7.** IoT DDoS attack defense system.

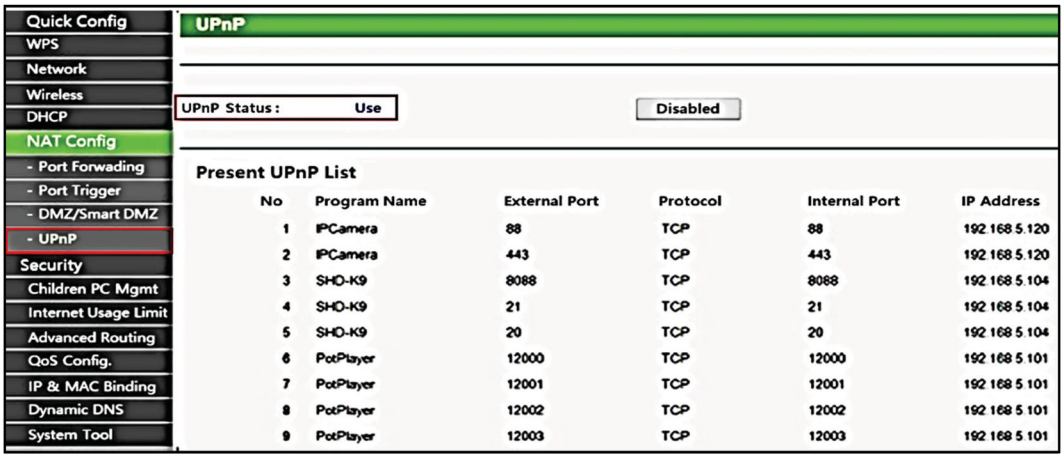


**Figure 8.** UPnP settings of an IoT device.

reflection attacks. Therefore, the UPnP function for IoT devices should be deactivated before the devices are released into the market in order to prevent the devices from being used as a reflectors for SSDP reflection attacks [31].

The UPnP function can be deactivated using the preferences or settings menu if the function is not necessary for device utilization. If the UPnP function is necessary for the use of the device, the settings should be configured to allow only authorized users.

• **Countermeasures for target of attack**

To defend against IoT DDoS attacks, the service provider can block traffic from the UDP port of origin (port 1900) among inbound traffic. Although SSDP is essentially the same protocol as UDP, it uses HTTP, which is a UDP-based HTTP protocol, as the HTTP header is included in the packet. Using this feature, it is possible to block SSDP reflection attacks. Among inbound traffic, packets containing HTTP/1.1 2000k strings can be blocked.

For network administrators, a key mitigation is to block incoming UDP traffic on port 1900 at the firewall. Provided the volume of traffic isn't enough to overwhelm the network infrastructure, filtering traffic from this port will likely be able to mitigate such an attack [32].

• **Countermeasure for ISP(Internet Service Providers)**

Unused protocols in actual services can be blocked in the ISP section when a large-scale attack occurs. The ISP can respond to the DDoS attack by null-routing the target IP address to prevent the network from being affected. To respond to DDoS attacks, the ISP simultaneously uses multiple ISP lines via the CDN service and distributes DDoS attacks using Anycast. Anycast maintains services using the networks that are functioning properly, even if one ISP or multiple networks fail. This distributed countermeasure is the best way to fight against attacks involving large volumes of traffic [33].

ISP eliminates SSDP attacks by stopping all the attack traffic before it reaches it's target. UDP packets targeting Port 1900 are not be proxied to the origin server, and the load for receiving the initial traffic falls on ISP's network. We offer full protection from SSDP and other layer 3 amplification attacks. Although the attack will target a single IP address, our Anycast network will scatter all attack traffic to the point where it is no longer disruptive.

## 4. IoT device forged traffic detection test

### 4.1. Data preparation of vulnerable IoT devices

The term "reflector" refers to an IoT device that is exploited for reflection DDoS attacks. IoT devices are vulnerable to being used as reflectors since their security settings or configurations do not employ SSDP, DNS, NTP, or SMMP protocol for UDP services on the Internet.

Not all IoT devices that use SSDP can be exploited as reflectors for reflection DDoS attacks. If the IoT device is connected to a private IP address, the device cannot be accessed by outside parties, and therefore it cannot be exploited as a reflector. If the user connects the IoT device to a public IP address, an attacker can perform a port scan to collect a list of IoT devices that are readily accessible. It is highly probable that the attacker will then use the exposed IoT devices as reflectors.

The IoT devices that can be exploited as reflectors can be identified using a port scan, as seen in Figure 9. The response packet of the SSDP reflection attack contains a location header, and the information in the header shows the path to the XML file, which has information on the IoT device. The IP address in the location header is set as private IP address, but if the address is changed to a public IP address, it is possible for hackers to gain access to the XML file containing information on the IoT device. Through this way, very detailed information about IoT devices can be accessed.

**Table 1.** Types of IoT devices exploited for SSDP reflection DDoS attacks.

| Number | IoT device | Number of devices | Proportion |
|---|---|---|---|
| 1 | Wired/Wireless Router | 1,482 | 98.2% |
| 2 | Printer | 8 | 0.5% |
| 3 | NAS | 7 | 0.5% |
| 4 | CCTV | 6 | 0.4% |
| 5 | Audio Player | 2 | 0.3% |
| | DVD Player | 2 | |
| 6 | Receivers | 1 | 0.1% |
| | TV | 1 | |
| Total | | 1,509 | 100.% |

**Table 2.** Country distribution of IoT's IP.

| Classification | Distribution by country | Number of devices | Proportion |
|---|---|---|---|
| 1 | South Korea | 1,425 | 94.4% |
| 2 | Japan | 32 | 2.1% |
| 3 | Taiwan | 21 | 1.4% |
| 4 | United Kingdom | 11 | 0.7% |
| 5 | United States | 8 | 0.5% |
| 6 | Canada | 5 | 0.4% |
| 7 | Tanzania | 1 | 0.5% |
| | Sweden | 1 | |
| | New Zealand | 1 | |
| | Ireland | 1 | |
| | Fiji | 1 | |
| | Denmark | 1 | |
| | China | 1 | |
| Total | | 1,509 | 100.% |

As seen in Figure 10, when changing the private IP address (192.168.0.1) in the path in the location header below to the actual origin IP address (121.66.111.171), it is possible to get detailed information about the IoT device from the XML file of the device—this information can then be used for reflection attacks.

This study analyzes reflection DDoS attacks on websites while exploiting IoT devices.

As seen in Table 1, this study analyzed about 1,500 IoT devices. According to the analysis results, most (98%) of the IoT devices exploited for reflection DDoS attacks were wired and wireless routers, followed by NAS and CCTVs. Electronic devices such as audio players and TVs were also victims of attack [30].

As seen in Table 2, an analysis of IP addresses of IoT devices exploited for reflection DDoS attacks showed that, among the attacks that occurred in South Korea, most of the attacks originated from within the country, followed by attacks from Japan and Taiwan.

### 4.2. Design of scenario for SSDP reflection attacks

A test was conducted on 1,509 IoT device searches using an attacking tool developed using Python. The command format was as follows: ssdp.py Victim_IPVictim_portSSDPlist the number of threads, attack duration. The reflection attack test was executed with ./ssdp.py 1.1.1.80 ssdp_100.txt 10 10. As seen in Figure 11, an attack was made on IoT devices using SSDP search requests.

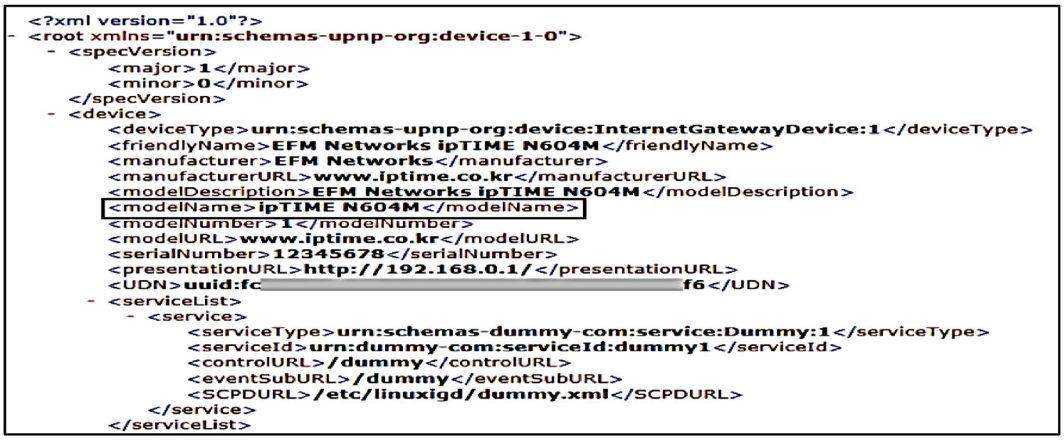


**Figure 9.** IoT device information in the SSDP packet location header.

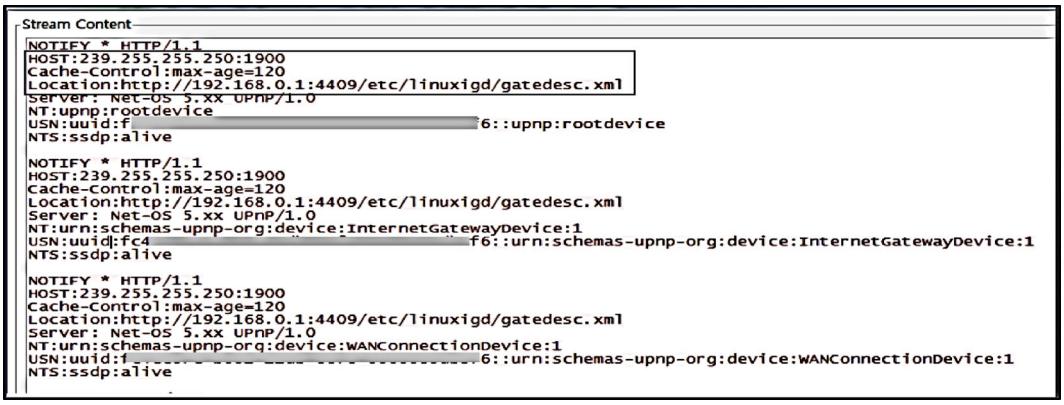


**Figure 10.** Structure of the SSDP packet.

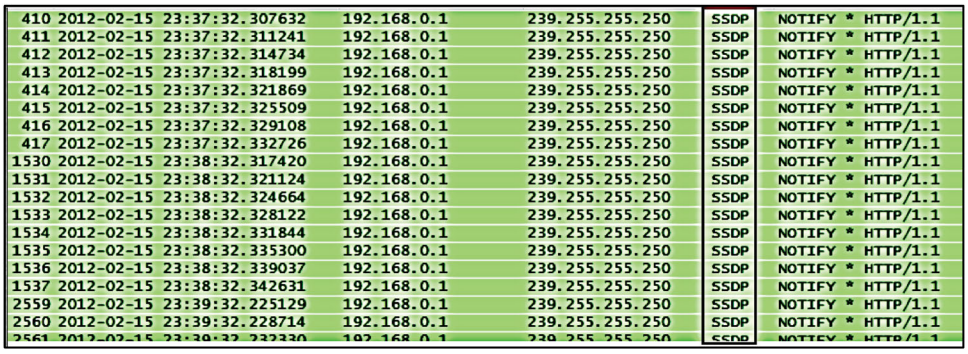


**Figure 11.** SSDP reflection DDoS attack request packet.

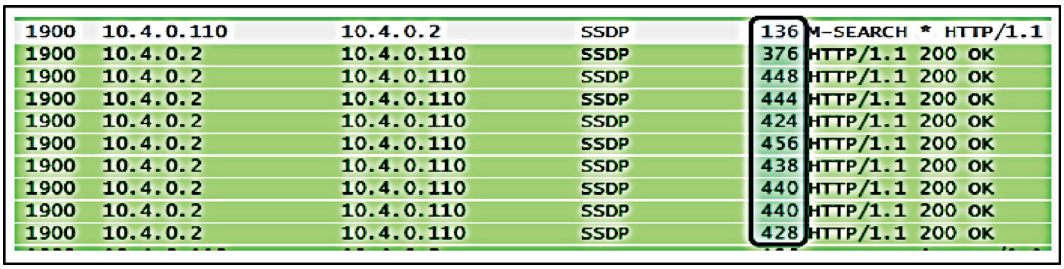


**Figure 12.** SSDP reflection DDoS attack packet.

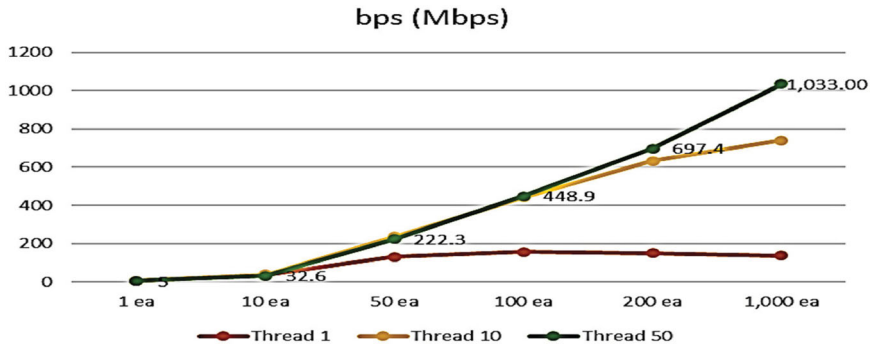


**Figure 13.** Comparison of IoT device DDoS attack volumes (BPS).

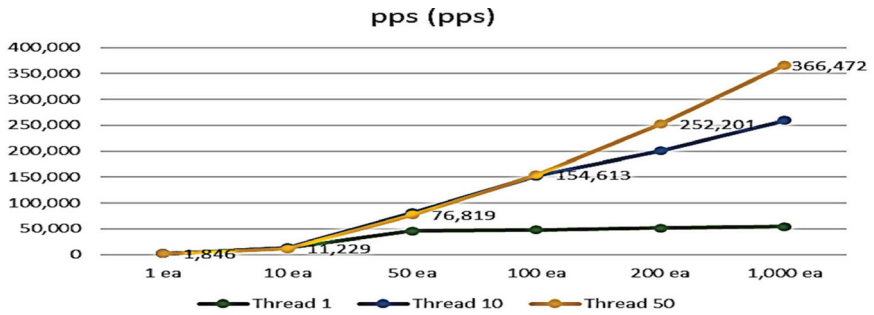


**Figure 14.** Comparison of IoT device-based DDoS attack volumes (PPS).

**Table 3.** Defense against DDoS attacks exploiting IoT devices.

| Attack number | Attack type | Attack volume (Gbps) | Attack requests (pps) | Number of IoT devices attacked |
|---|---|---|---|---|
| 1 | SSDP and GET | 1.9 | 1,846 | 79,107 |
| 2 | SSDP and ICMP | 1.6 | 11,229 | 76,423 |
| 3 | SSDP and ICMP | 2.5 | 76,819 | 269,625 |
| 4 | SSDP, ICMP, and UDP | 4.6 | 154,613 | 53,229 |
| 5 | SSDP and ICMP | 2.2 | 252,201 | 102,805 |
| 6 | SSDP,ICMP, GET, and SYN | 10.0 | 366,472 | 752,771 |
| 7 | SSDP and UDP | 1.2 | 252,201 | 152,751 |
| 8 | SSDP and NTP | 2.3 | 366,472 | 115,153 |

Figure 12 shows the responses of IoT devices to an SSDP search request, from which a DDoS attack of the target server was generated.

DDoS attack traffic was increased from 1 to 50 threads, while the number of IoT devices was increased to 1,000—the increase in attack traffic was expressed in BPS (Bytes Per Second). The results of these generated increases can be seen in Figure 13. In this part of the analysis, it was found that a large-scale DDoS attack equivalent to 1G was generated when the thread was set to 50 for 1,000 IoT devices.

Figure 13 shows a comparison of DDoS BPS attack volumes. As seen in the figure, DDoS attacks rapidly increased to about 500 Mbps when the thread was set to 10 with over 100 IoT devices.

When DDoS attack traffic was increased from 1 to 50 threads and the number of IoT devices was increased to 1,000, the PPS (Packet Per Second) results were as shown in Figure 14. In this part of the analysis, it was found that about 36,000 requests were generated when the thread was set to 50 with 1,000 IoT devices.

Figure 14 shows a comparison of DDoS PPS attack volumes. As can be seen in the figure, DDoS attacks rapidly increased to over 15,000 counts when the thread was set to 10 with over 100 IoT devices.

### 4.3. Analysis of response results against IoT DoS attacks

In this study, a multi-level defense system for actual DDoS attacks targeting IoT devices was developed and tested.

As seen in Table 3, the system effectively protected the devices from a total of eight IoT DDoS attacks. Attack types included combinations of SSDP and ICMP as well as SSDP and GET. The total attack volume ranged from 1.6 Gbps to 10 Gbps, and the number of attack requests increased from 1,846–366,472. The number of exploited IoT devices ranged from about 80,000–750,000. The proposed mechanism successfully protected the devices from the attacks.

It was also found that embedded Linux-based IoT devices were more susceptible to DDoS attacks than other IoT devices. Given that 127 new IoT devices are registered per second, it is highly probable that the scale and occurrence of DDoS attacks will continue to

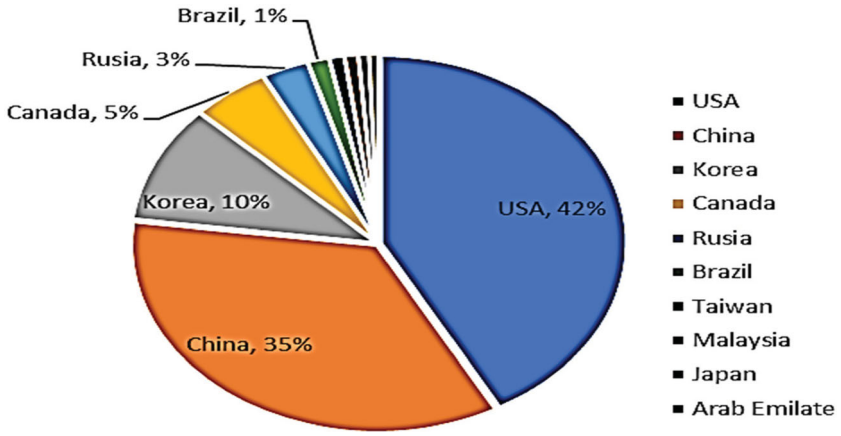


**Figure 15.** Ranking of countries by the number of IoT devices exploited for DDoS attacks.

increase. Recently, an attack with a scale of over 1.6 Gbps occurred through amplified reflection. Amplified reflection attacks use the attributes of UDP and spoofing among servers. These attacks use SSDP, SNMP, and UDP-based services.

SSDP is a protocol used for UPnP devices to share data, and a certain part of the SSDP payload is generated from unexpected ports. It is possible to disguise a port using UPnP, and it is also possible to amplify and conduct reflection attacks using SSDP. UPnP devices can be identified through rootDesc.xml, and these devices can easily become the target of attacks.

As seen in Figure 15, We analyzed each countries where the IoT devices was located. DDoS attacks targeting IoT devices are most often generated in the United States, followed by China, South Korea, Canada, and Russia.

## 5. Conclusion

SSDP for IoT devices has certain characteristics that make it vulnerable to DDoS attacks. SSDP allows devices to search for and communicate with other devices connected to the same network. Attackers generate DDoS attacks using the vulnerabilities of SSDP.

To analyze the ways in which IoT devices are used for DDoS attacks, we identified the types of IoT devices being used online and the vulnerabilities of the communication protocols of each IoT device. We also conducted a test and made service requests to vulnerable IoT devices, and concentrated the device responses on the target server with the aim of shutting down the web service. During tests, we were able to generate over 50 GBs of attack traffic.

This study presents a multi-level defense system for communication protocol L2 and L7 to counteract DDoS attacks using IoT devices. Additionally, this study suggests a method involving DDoS attack blocking patterns that can be used to remove IoT vulnerabilities in DDoS attacks, which is necessary for the effective implementation of a multi-level defense system.

Additionally, the tests conducted as part of this study showed that the multi-level DDoS countermeasures proposed in this study can successfully protect actual IoT devices against DDoS attacks. As such, this study can contribute to the development of effective countermeasures against the rapid increase of IoT device-based DDoS attacks.

## Disclosure statement

No potential conflict of interest was reported by the author(s).

## ORCID

*Yong-joon Lee* http://orcid.org/0000-0002-4655-0302

## References

[1] Xu T, Wendt JB, Potkonjak M. Security of IoT systems: design challenges and opportunities. In Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD '14), (2014): 417–423.

[2] Hee KN. Standard technology trends for Internet security of things. J Korean Inst Commun Sci. 2014;31(9): 40–45.

[3] Lee KH, Park JP. A software vulnerability analysis system using learning for source code weakness history. J Korea Acad Indust Coop Soc. 2017;18:46–52. doi:10.5762/KAIS.2017.18.11.46.

[4] Peng T, Leckie C, Ramamohanarao K. Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Comput Surv (CSUR). 2007;39(1):3.

[5] Ryba FJ, et al. Amplification and DRDoS attack defense-a survey and new perspectives. arXiv preprint arXiv:1505.07892 (2015).

[6] Saboor A, Aslam B. Analyses of flow based techniques to detect distributed denial of service attacks. in Proc. of Applied Sciences and Technology, (2015): 354–362.

[7] Min SY, Jung CS, Lee KH, et al. Design of comprehensive security vulnerability analysis system through efficient inspection method according to necessity of upgrading system vulnerability. J Korea Acad Ind Coop Soc. 2017;18:1–8. doi:10.5762/KAIS.2017.18.7.1.

[8] Manusankar C, Karthik S, Rajendran T. Intrusion detection system with packet filtering for IP spoofing. Commun Comput Intell (INCOCCI). 2010: 563–567.

[9] Deng S, Xiang Z, Zhao P, et al. Dynamical resource allocation in edge for trustable iot systems: a reinforcement learning method. IEEE Trans Ind Inf. 2020. doi:10.1109/TII.2020.2974875.
[10] Al-Duwair B, Daniels TE. Topology based packet marking. The 13th International Conference on Computer Communications and Networks(ICCCN), (2004): 146–151.
[11] Li L, Shen S-B. Packet track and traceback mechanism against denial of service attacks. J China Univ Posts Telecommun. 2008;15(3):51–58.
[12] Wang J, Gao Y, Liu W, et al. Energy efficient routing algorithm with mobile sink support for wireless sensor networks. Sensors. 2019;19(7):1494. doi:10.3390/s19071494.
[13] Oh SH, Kim TE, Kim HK. Technology analysis on automatic detection and defense of SW vulnerabilities. J Korea Acad Ind Coop Soc. 2017;18:94–103. doi:10.5762/KAIS.2017.18.11.94.
[14] Wan Z, Zhang Y, Cao T, et al. A novel authenticated packet marking scheme for IP Trace-back. Computer Science and Information Technology, ICCSIT 2009. 2nd IEEE International Conference, (2009): 150–153.
[15] Bremler-Barr A, Levy H. Spoofing prevention method. Proc IEEE INFOCOM. 2005;1:536–547.
[16] Yaar A, Perrig A, Song D. Stackpi: new packet marking and filtering mechanisms for DDoS and IP spoofing defense. IEEE J Sel Area Comm. 2006;24(10):1853–1863.
[17] Yu J, Zhang B, Kuang Z, et al. iPrivacy: image privacy protection by identifying sensitive objects via deep multi-task learning. IEEE Trans Inf Forensics Secur. 2017;12(5):1005–1016.
[18] Hong S. Efficient and secure DNS cyber shelter on DDoS attacks. J Comput Virol Hacking Tech. 2015;11(3):129–136.
[19] Wang J, Gao Y, Liu W, et al. An intelligent data gathering schema with data fusion supported for mobile sink in WSNs. Int J Distrib Sens Netw. Mar. 2019;15(3).
[20] Yu S, et al. Discriminating DDoS attacks from flash crowds using flow correlation coefficient. IEEE Trans Parallel Distrib Syst. 2012;23(6):1073–1080.
[21] Vaidyanathan R, Ghosh A, Sawaya Y, et al. On the use of Enhanced Bogon Lists (EBLs) to detect malicious traffic. Comput Netw Commun (ICNC). 2012;2012:1–6.
[22] Li Y, Kumar M, Shi W, et al. Falcon: an ambient temperature aware thermal control policy for IoT gateways. Sust Comput-Inform Syst. 2017;16:48–55.
[23] Meidai S, Keisuke I. Validating packet origin using external route information. Inf Telecommun Technol (APSITT). 2010: 1–6.
[24] Paxson V. An analysis of using reflectors for distributed denial-of-service attacks. ACM SIGCOMM Comput Commun Rev. 2001;31(3).
[25] Wang H, Jin C, Shin KG. Defense against spoofed IP traffic using hop-count filtering. IEEE/ACM T Networking (TON). 2007;15(1):40–53.
[26] Wang J, Cao J, Simon Sherratt R, et al. An improved ant colony optimization-based approach with mobile sink for wireless sensor networks. J Supercomput. Dec. 2018;74(12):6633–6645.
[27] Yin Y, Chen L, Xu Y, et al. Qos prediction for service recommendation with deep feature learning in edge computing environment. Mobile Netw Appl. 2019. doi:10.1007/s11036-019-01241-7.
[28] Yu J, Kuang Z, Zhang B, et al. Leveraging content sensitiveness and user trustworthiness to recommend fine-grained privacy settings for social image sharing. IEEE Trans Inf Forensics Secur. 2018;13(5):1317–1332.
[29] Jia G, Han G, Jiang J, et al. Dynamic cloud resource management for efficient media applications in mobile computing environments. Pers Ubiquitous Comput. 2018;22(3):561–573.
[30] Wang J, Gao Y, Liu W, et al. An asynchronous clustering and mobile data gathering schema based on timer mechanism in wireless sensor networks, computers. Mater Con. 2019;58(3):711–725.
[31] Wang J, Gao Y, Yin X, et al. An enhanced PEGASIS algorithm with mobile sink support for wireless sensor networks. Wirel Commun Mob Com. 2018;2018:Article ID 9472075.
[32] Zhang N, Duan Z, Tian C. Model checking concurrent systems with MSVL. Sci China Inform Sci. 2016;59(11):118101:1–118101:3.
[33] Xiaoxian Y, Sijing Z, Min C. An approach to alleviate the sparsity problem of hybrid collaborative filtering based recommendations: the product-attribute perspective from user reviews. Mobile Netw Appl. 2020;25(2):376–390.