Chapter 65
Internet of Things (IoT)-Based Distributed Denial of Service (DDoS) Attack Using COOJA Network Simulator

Harshil Joshi and Dushyantsinh Rathod

Abstract The revolution in Internet of Things (IoT) technology has carried the astonishing ability to interconnect various devices that are traditionally known as "dumb" devices. On the contrary side, it has also welcomed hazard of billions of unprotected and easily hackable devices. These unexpected flooding of newly added vulnerable devices has welcomed unsought threats like distributed denial of service (DDoS) attacks. In this paper, a brief introduction of the IoT has been given, and broader categories of DDoS attacks have been explained. This paper is mainly focused on various types of DDoS attacks which are done in the recent era and chance to make unwanted damage in nearby future. At the end of paper, DDoS attack is implemented using Contiki operating system-based Cooja network simulator. Care must be taken till a strong intrusion detection system or any other technique is developed for the IoT-based network.

65.1 Introduction

The Internet of Things (IoT) in the twenty-first century stands unquestionably the most important development that can connect devices beyond personal computer or phone. IoT devices play a noteworthy responsibility in a world that are dominated by digital technology (i.e., automation). From a tiny device to a large driverless car, everything has become achievable because of the implementation of the IoT. The Internet of Things and its application can turn any object into a smart object, and these objects can be remotely available. Contrarily, at present time, the enterprise or the firms are in the race to quickly develop the IoT devices. Due to this rush in the development of the new IoT devices, the security of the devices is poorly designed [1, 2]. It can be claimed that this rush and competition in the revolution in the Internet

H. Joshi (✉)
Gujarat Technological University (GTU) and Devang Patel Institute of Advance Technology and Research (DEPSTAR), Charotar University of Science and Technology (CHARUSAT), Anand, Gujarat, India

D. Rathod
Sakalchand Patel Institute of Technology, Visnagar, India

T. Senjyu et al. (eds.), *IOT with Smart Systems*, Smart Innovation, Systems and Technologies 251, https://doi.org/10.1007/978-981-16-3945-6_66

of Things could lead to a potential disaster [3]. An increase in the number of linked or unsecured devices in the market can increase the potentials of hackers to access critical data of IoT devices by targeting them and as a result oversee our devices and control our lives [4–6]. This shift in the Internet of Things toward insecurity could take us back to distributed denial of service (DDoS) attacks powerful and more complex than earlier which could even not be identified or traced. Because of this increase in insecured Internet of Things devices, the number of those attacks has grown to a large extent, and this can lead to more and more criminal activities [7, 8].

The year 2016 was remembered as the year of Mirai as it was the critical point in which the combination of the DDoS and the insecured Internet of Things devices was piled up to create the largest DDoS attack ever noted. Thousands of connected devices were infected, and the major DDoS attack was seen which reached the nasty capability to about 1.2 terabytes (TB) per second [9, 10].

Interestingly, the impressive thing about the Mirai attack is not only the power of attack but was how the worm was able to infect those large ranges of devices or units. Those devices were affected by a very simple dictionary attack which was based on only sixty entries approximately. The attack was made only a very simple fact that the infected devices never changed the default login credentials, and some devices were not able to change because of technical reasons.

Recently in January 2019, an undisclosed client of Imperva experienced an outsized DDoS attack that received 500 million packets per second on their network. In the January 2019 attack, each packet was around 800–900 bytes in size. This means 500 packets of 850 bytes resulting in approximately 3.4 trillion bits of data targeting the Web site and resulting in an unresponsive one. This could affect the thousands of Internet of Things devices that were connected to it. All the above things lead to the unquestionable need to face the Internet of Things security problems.

65.2 How Does a DDoS Attack Work?

The Internet itself makes the DDoS attacks possible and more powerful. When the aim is to improve the functionality of the Internet and not the security, the Internet becomes inherently vulnerable to various security issues. Due to these security issues, the DDoS attacks are possible [11, 12].

To carry out a DDoS attack, an attacker needs to gain control of a network of online machines. These machines (Internet of Things devices) are infected with malware, and thus, each machine turns into a bot. This group of bots forms a “botnet”, and the attacker has complete remote control over this botnet.

Once the attacker has complete remote control over this botnet, the attacker can send the updated instructions to each bot. Each bot from the botnet will send a request to the IP address of the victim and hence causing the network to overflow capacity.

As these bots are also legitimate Internet devices, they cannot be separated from the traffic and it results in the denial of service to the normal traffic. The DDoS needs to go throughout the following states to be struck [11, 12].

1. **Recruitment**: The attacker scans for the bots that can later be used to penetrate the attack to the victim machine. Previously, the attackers manually recruit the bots, but nowadays, there are many scanning tools available that can be used for this purpose.
2. **Forming a botnet**: Malicious code is injected into the vulnerable machines, and a botnet is created. At present, this stage is also been automated (the bots are recruited by self-propagating tools).
3. **Command and Control**: The attacker communicates with the bots via command-and-control architecture. In this way, the attacker gets to know about the active bots, upgrades the bots, and schedules an attack.
4. **Attack**: The attacker sends the command to the botnet, and the bots start sending malicious packets to the target. The attacker adds the parameters such as victim, number of packets, and duration of the attack. The attackers hide the IP address of the agent machines (bots); hence, machines, during the attack, will remain undiscoverable.

65.3 Distributed Denial of Service (DDoS) Attacks

There are many different types of DDoS attacks that are noted in today's life, and a very extensive range of classification is suggested in literature today. Elements that are seen in DDoS attack are as below.

1. The attacker is the main person behind the attack and on which the whole attack is based.
2. The organizer which is negotiable hosts a program running on them that can control many operators.
3. The person or the online work which is attacked by the attackers.

65.3.1 Types of Distributed Denial of Service (DDoS) Attacks

The DDoS attack can be categorized into three types, which are as below.

65.3.1.1 Volume-Based Attack

The volume-based attacks are also called volumetric DDoS attacks. In this attack, the attackers consistently surge the sufferer with the immense volume of vast connecting equipment, networks, high-frequency resources, and servers. This is called the most common DDoS attack. This attack includes various spoofed-packet floods like UDP floods and ICMP floods. The motive of the attacker is to consume the bandwidth of the victim's site. The degree of the attack is deliberate in bits per second (bps).

65.3.1.2 Protocol-Based Attacks

Protocol-based attacks mainly target manipulating a deficiency in Layer 3 or Layer 4 of the OSI layer. The motive of the attacker is to consume resources of the actual server. The degree of the attack is deliberate in packets per second.

65.3.1.3 Application Layer Attack

The application layer attack is also called the Layer 7 attacks. This attack refers to the type of malignant act which is designed to target the application layer of the OSI model where the common Internet requests such as HTTP POST and HTTP GET occur. The motive of the attacker is to target the Apache, Windows, or open BSD vulnerabilities, and more.

65.3.2 Examples of DDoS Attack

In today's era, we can find various DDoS attacks; few of them are described here.

65.3.2.1 UDP Flood

This is a subtype of volume-based attack. UDP is an abbreviation for User Datagram Protocol. UDP is a type of attack in which the attacker crushes random ports on the targeted host. UDP runs with lower overhead as it does not require a three-way handshake like TCP.

65.3.2.2 ICMP Flood

This is also a subtype of volume-based attack. ICMP flood is an abbreviation for Internet Control Message Protocol. It is also called the ping flood. In ping flood, an attacker takes control of the a victim's computer by sending ICMP echo requests.

65.3.2.3 TCP SYN Flood

This flood attack, a subtype of protocol-based attack, which exploits part of the normal TCP three-way handshake to consume resources on the targeted server and revive it passively. In a SYN flood attack, the targeted server is flooded with the repeated SYN packets sent by the attacker using a fake IP address.

65.3.2.4 HTTP Flood

This is a subtype of the application layer attack. During this, a web server or application is flooded via HTTP GET or POST requests sent by the attacker. HTTP flood attacks are volumetric attacks, habitually employing a botnet "zombie army."

65.3.2.5 Hydra

An open-source prototype malware that appeared in 2008 was the router that worked as an open-source tool by their own. The main purpose of the malware was to access the routers by using brute-force methods for performing DDoS attacks. The access to the router was possible by either with dictionary attack or with the use of the D-Link authentication bypasses method [13].

65.3.3 Implementation of DDoS Attack

In this paper, Contiki operating system-based Cooja network simulator is used to implement DDoS attack in the IoT network. Cooja network simulator provides environment that is nearer to real-time IoT network.

As shown in Fig. 65.1, we have created IoT network scenario with 25 nodes. In this network, Node 1 acts as server and Node 2 to Node 25 act as client. Server node is indicated by green color, and client node is indicated by yellow color.

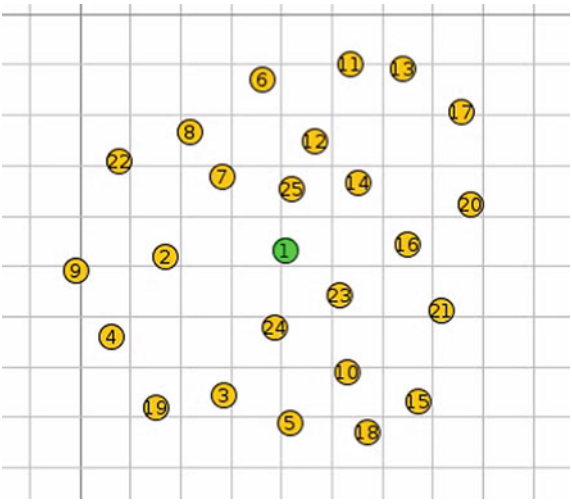

Fig. 65.1 IoT network scenario when simulation is not initialized

As shown in Fig. 65.2, each node starts communication with each other via sending HELLO packet. When any attacker node is connected, it may start to send multiple packets to each node (as shown in Fig. 65.3).

As we all know, IoT devices have limited amount of computational power which is not sufficient to handle large amount of packet simultaneously. Processing of such a huge amount of data will affect IoT devices badly. We must provide some lightweight solution which can work for the IoT network.

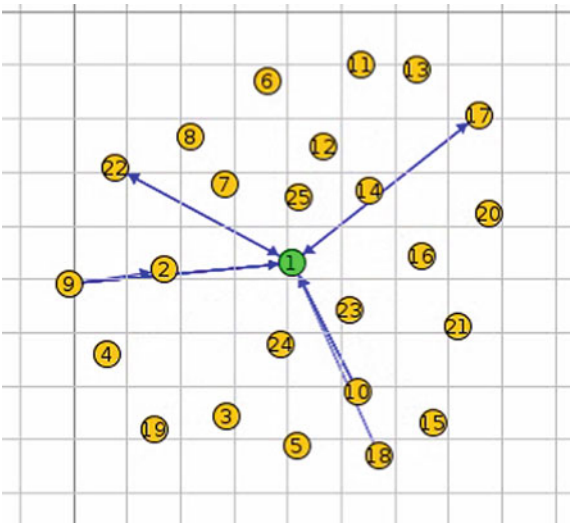

Fig. 65.2 IoT network scenario when simulation is initialized

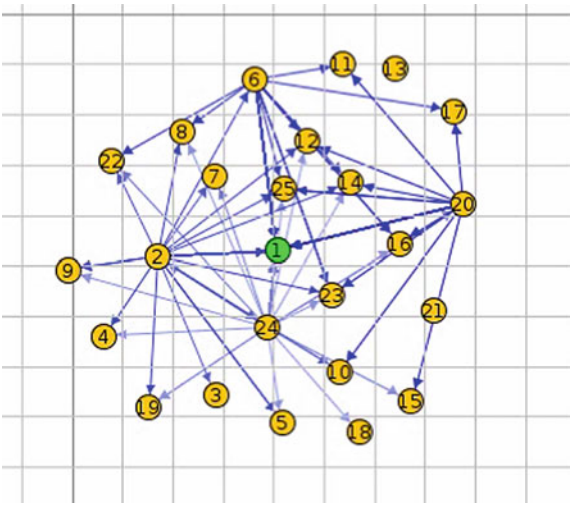

Fig. 65.3 IoT network is flooded with multiple packets sent via attacker node

65.4 Conclusion

In the recent era, we have seen insignificant growth in the IoT devices which are poorly designed and with limited security features. Due to lack of attention, fundamental urgency has been emerged in the market to redesign security parameter that can work with IoT devices with limited computational power and heterogeneously designed IoT network. Inspired by the intensified situation, various taxonomy of DDoS attack has been indentified and represented in the paper. Moreover, small scenario has been implemented to provide nearly real-time scenario of IoT-based network during DDoS attack. However, some techniques need to develop such as lightweight instution detection system for IoT-based network.

References

1. Granjal, J., Monteiro, E., Sa Silva, J.: Security for the internet of things: a survey of existing protocols and open researchissues. IEEE Commun. Surv. Tutorials **17**(3), 1294–1312 (2015)
2. Arias, O., Wurm, J., Hoang, K., Jin, Y.: Privacy and security ininternet of things and wearable devices. IEEE Trans. Multi-Scale Comput. Syst. **1**(2), 99–109 (2015)
3. Dragoni, N., Giaretta, A., Mazzara, M.: The internet of hack able things. In: Ciancarini, P., Litvinov, S., Messina, A., Sillitti, A., Succi, G. (eds.) Proceedings of the 5th International Conferencein Software Engineering for Defense Applications (SEDA16), Advances in Intelligent Systems and Computing. Springer, Berlin (2017)
4. Hughes, D.: Silent risk: new incarnations of longstanding threats. Netw. Secur. **2016**(8), 17–20 (2016)
5. Shukla, S.K.: Editorial: cyber security, IoT, block chains—risks and opportunities. ACM Trans. Embedded Comput. Syst. (TECS) **16**(3, article 62), 1–2 (2017)
6. Goyal, R., Dragoni, N., Spognardi, A.: Mind the tracker youwear: a security analysis of wearable health trackers. In: Proceedingsof the 31st Annual ACM Symposium on Applied Computing (SAC'16), pp. 131–136, Pisa, Italy (2016)
7. Bertino, E., Islam, N.: Botnets and internet of things security. IEEE Comput. **50**(2), 76–79 (2017)
8. Kolias, C., Kambourakis, G., Stavrou, A., Voas, J.: DDoS in the IoT: mirai and other botnets. IEEE Comput. **50**(7), 80–84 (2017)
9. York, K.: Dyn statement on 10/21/2016 DDoS attack, Dyn Blog (2016). http://dyn.com/blog/dyn-statement-on-10212016-ddosattack/
10. Hilton, S.: Dyn analysis summary of Friday October 21 attack, Dyn Blog (2016). http://dyn.com/blog/dyn-analysis-summary-offriday-october-21-attack/
11. Mirkovic, J., Reiher, P.: A taxonomy of ddos attack and ddos defense mechanisms. Comput. Commun. Rev. **34**(2), 39–53 (2004)
12. Douligeris, C., Mitrokotsa, A.: DDoS attacks and defensemechanisms: classification and state-of-the-art. Comput. Netw. **44**(5), 643–666 (2004)
13. Janus, M.: Heads of the hydra. Malware for network devices. Tech. Rep. Securelist (48) (2011)