DoS Attacks in IoT Systems and Proposed Solutions

Nada Abughazaleh
Department of Electrical and Computer Engineering
FOE, King Abdulaziz University, Jeddah, KSA

Ruba bin Jabal
Department of Electrical and Computer Engineering
FOE, King Abdulaziz University, Jeddah, KSA

Mai Btish
Department of Electrical and Computer Engineering
FOE, King Abdulaziz University, Jeddah, KSA

Hemalatha M.
Department of Electrical and Computer Engineering
FOE, King Abdulaziz University, Jeddah, KSA

ABSTRACT

The internet of things (IoT) has been gaining attention in the past decade, and this rapid growth is due to the many different advantages delivered towards achieving a smart world. However, security is one of the biggest challenges, as it builds upon the internet. This article surveys denial-of-service (DoS) attacks that occur in the network layer of IoT systems and the impact on various aspects. The Smurf and SYN flood attacks are briefly discussed along with several distinct DoS attack mitigation methods. Two DoS mitigation technologies implemented by IoT security companies are discussed as a case study.

General Terms

Denial of Service, Internet of Things, IoT Architectures, Smurf attack, SYN flood, Honeypot

Keywords

IoT, DoS, DDoS, network, Smurf attack, SYN flood

1. INTRODUCTION

Technology has seen significant advancements and developments, particularly in the last decade. The most evident effect of this growth is how the internet has become an integral part of people's daily lives. Thus, internet-based technologies, such as the internet of things (IoT), spread around the globe. IoT enables devices to work and communicate together within a specific environment in order to serve a definite purpose with the minimum human intervention [1]. These devices are connected to the internet and possess different characteristics and features, and while they facilitate machine-to-machine communication, their capabilities can reach beyond it [2].

The reason the internet of things has become popular is the many benefits it provides, such as making various aspects of people's lives simpler, increasing the level of autonomy in tasks, and, simply, providing better experiences for businesses and consumers [3]. However, despite its countless benefits, IoT is facing challenges that hinder it from reaching the high potential it is expected to reach. The design of the majority of IoT devices does not consider the security and privacy of users which became a huge concern [4]. One of the most common risks in IoT systems is the denial-of-service (DoS) attacks, which interrupt the smooth operation of IoT devices and cause inconveniences to their users and processes [5].

With the 20.4 billion IoT devices expected to be connected to the internet in 2020, it is necessary to provide consumers and businesses with safe and secure IoT services [6]. Thus, this paper focuses on the denial of service attacks to IoT systems. Types of DoS attacks are presented, the impact of this attack, globally and ethically, is discussed. Then, current strategies and solutions that organizations have developed, and possible future innovations are reviewed.

2. LITERATURE REVIEW

The main characteristic of the internet of things is that it is a system comprised of electronic devices (i.e., sensors and actuators) of all sizes and capabilities. These devices are connected to the internet and controlled from any location [7]. Researchers have formulated different IoT architectures; the proposed three-layer architecture is the most basic one [8]. Figure 1 illustrates this architecture. The perception layer has the sensors and hardware, selected as per the needs of the product, that collect information about its surrounding environment. The network layer acts as a middle layer that connects devices together and transfers data between the other two layers. Finally, end-users interact with the application layer which provides them with application-specific services.

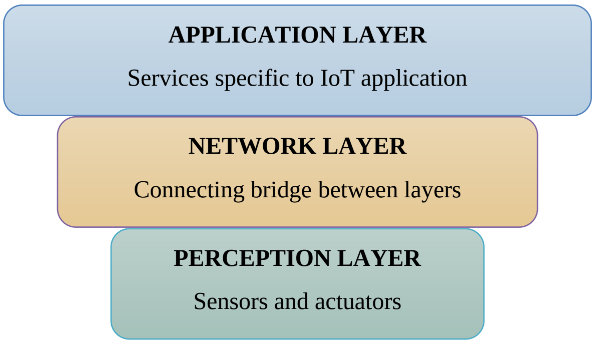
APPLICATION LAYER
Services specific to IoT application
NETWORK LAYER
Connecting bridge between layers
PERCEPTION LAYER
Sensors and actuators

Fig. 1: The three IoT layer architecture

The primary function of the network layer is the transmission of data between nodes in the network. This transmission occurs through a wired or wireless medium [9]. Furthermore, for this process to occur, protocols must be utilized. Since the network layer functions as the communicating bridge between the perception and application layers, it is quite vulnerable to attacks. In fact, most DoS attacks occur on the network layer [10]. These attacks may deplete the layer's resources, divert the flow of traffic, or even eavesdrop on nodes.

A DoS attack occurs when the attacker sends too many requests to the main server/host making the real users of the server unable to use it. The attacker keeps pinging the host with spam requests until it gets overloaded and shuts down as a result [11]. DoS attacks can affect several IoT applications, such as smart homes, personal medical devices, and industrial applications. Due to the broad field of IoT applications, different security measures must be taken depending on the requirements of the IoT system.

2.1 Current Trends

2.1.1 DoS types

DoS attacks have many different types and methods for locking up a targeted server, which may be an IoT device, and it is essential to understand each type in order to mitigate and prevent them. Various kinds of DoS attacks might also occur for IoT networks such as the Smurf attack and the SYN flood attack [12].

A Smurf attack uses Internet Control Message Protocol (ICMP) requests for deluging the targeted server through a spoof Internet Protocol (IP) address. The ICMP's purpose is to provide the sender with the status of the sending requests, whether they are reaching the destination or not. ICMP is used by network devices such as the router. The working principle of a Smurf attack is as follows: the attacker creates a spoofed packet by setting its source as the IP address of the target server, and it is sent to an IP broadcast address of a router. Then, the router sends requests to host devices inside the network that respond by sending ICMP packets to the spoofed address of the target. Consequently, the target server will be overloaded with many requests [13].

On the other hand, the SYN flood is considered as a half-open attack because the attacker never completes the connection after requesting the server. Therefore, it aims to consume all available server resources. This attack works by taking advantage of the handshake process of a Transmission Control Protocol (TCP) connection. The TCP works synchronously with the IP to maintain the order of data between sender and receiver. In the handshake, the receiver receives an SYN packet from the sender to initialize the connection. It responds by sending acknowledgment (ACK), and then receives ACK again from the sender. In the SYN flood attack, the attacker will receive ACK from the server after sending a spoofed packet without replying with a final ACK. The attacker will continue sending SYN packets until all the server's available ports are exploited [13]. According to [14], the highest occurring type of DoS attack is the SYN flood threat, and the majority (85%) of DoS attacks happen using TCP protocol.

2.1.2 The impact of DoS attacks

DoS is one of the most significant and severe attacks from the starting of the digital era. Since the beginning of IoT, DoS exposed huge vulnerabilities of IoT systems. Many sensitive and critical IoT environments could be affected by this attack since the IoT system requires a high level of reliability. The DoS attack affects the whole network by preventing the accessibility of the server or any IoT components, therefore violating one of the essential components of cybersecurity: the availability. One of the hackers' aims is to compromise the availability since it does not require administrative privilege compared to compromising the confidentiality and integrity components for getting and modifying confidential information. DoS has a more harmful effect on high profile organizations such as banks and governments, leading to considerable losses in finances and time.

Lohachab and Karambir [15] demonstrate many impacts and exploited-IoT properties based on different distributed denial-of-service (DDoS) types. For instance, DDoS over the ZigBee network showed a low awareness of security problems with limited resource devices. It resulted in the manipulation of privileged nodes. Another example is flooding attacks. The specific IoT property exploited is a collection of malicious connected devices and network congestion in addition to resource consumption produced as impacts. Furthermore, the protocol attack type used the vulnerability features in IoT protocols, leading to unexpected and abrupt protocol functionality.

As the number of connected devices increases, such as printers, fridges, sensors, and routers with limited security capabilities, attackers would take advantage of the weaknesses of those devices to affect the whole IoT network. Such devices play a significant role in different industries and have crucial impacts on many people's lives—for instance, healthcare monitoring devices and control valves of power plants.

Organizations and enterprises must possess an awareness regarding DoS attacks and their impact on different aspects. Therefore, they should implement robust defense methods and develop solutions against those attacks as well as consider cybersecurity strategy as a priority in their policies. Furthermore, the wireless traffic of the IoT system should be monitored and analyzed periodically to detect and prevent abnormal behavior. Implementing a comprehensive authentication mechanism, such as controlling the received packets and using full headers, could also strengthen the network communication protocol. Another crucial point is the high importance of choosing a robust Internet Service Provider (ISP). ISPs must provide sufficient DoS defense mechanisms to protect their enterprise customers from downtime, therefore minimizing the risk of affecting clients' IoT systems and earning a higher level of trust from them [16].

Enterprises should outline ethical IoT foundations and frameworks while designing their systems and have the responsibility of delivering an IoT-based solution that satisfies the ethics. Businesses that provide IoT products must maintain an ethical culture during production while ensuring high-quality services that deploy a high level of security, and, at the least, provide a backup plan in case of an attack. Such as providing another way of accessing data instead of the service going offline completely.

2.1.3 Examples

Smart homes utilize IoT devices such as sensors, cameras, and appliances to make people's lives easier. Sensors can read the house's temperature, monitor air smoke, and even monitor a baby's health. Moreover, sensors and cameras can be used to monitor a home's entry points and alert the owners in case there was a breach. The devices in an IoT smart home communicate by using IP addresses, and a gateway achieves the management of these devices. If a DoS attack targets the gateway, all the devices become jammed and are unable to perform their functions [17].

IoT has granted the industry the opportunity to perform remote management of their services that can be realized from desktops, servers, or point-of-sale systems. Remote management is applied in industries such as retail stores, factories, and healthcare units. The management of a package in transit, the monitoring of a patient's health, and the tracking of a truck's movement are examples of remote management. All of these elements are prone to DoS attacks where the eavesdropper can spam the server with false data causing jamming and blocking to the legitimate users, which leads to tremendous losses for the organization [18]. In 2016, A Mirai botnet attack was launched on IoT devices by perpetrating them, jamming their servers, and causing a traffic overload. This attack caused damage to popular websites like Netflix, Reddit, and Twitter [19].

In the medical applications of IoT, personal medical devices can be used to report the health status of patients and their medical reports. A DoS attack can gain access to the communication channel that the IoT system uses to utilize its resources and drain them, making the system shut down. IoT based health sensors can report medical data to a cloud via a channel or middleware. This middleware can be breached by a DoS attack making the data transmission delayed or indefinitely terminated [17].

2.2 Current Proposed Solutions

Due to the broad range of IoT applications and services, it is difficult to provide one distinct solution that protects all IoT systems. In this section, three different types of DoS attack mitigation and prevention methods are discussed.

A graph-based method can detect DoS attacks in smart homes. In the graph technique, nodes represent the connected devices, and edges represent the communication between these devices. A DoS attack may shut down one device, and yet, the whole system may appear as if it is fully functioning. The Novel Graph-Based Outliner Detection in Internet of Things (GODIT) claims to analyze each entity (node) in the IoT network and study its performance with respect to the whole system. The GODIT approach requires only the source IP and destination IP to create the graph of the network's flow of data/traffic, which makes the GODIT efficient compared to other DoS detection methods that require more elements such as protocols and the packet size [20].

A Honeypot system mimics the behavior and features of the targeted main server and acts as s decoy. The decoy requires three components to operate: a computer, an application program, and some specific data. The DoS attack is forwarded to this decoy protecting the intended target server. The protection is achieved by tracking the attackers and tracing their activities to further study and analyze them to prevent future attacks [11].

Kajwadkar and Jain [21] proposed a novel solution to detect DoS attacks that target constrained devices. The detection occurs at an early stage at the Border Router node that guarantees the network devices in any IoT network will be unharmed. The detection method consists of two stages: the primary stage and secondary stage. In the primary stage, the source IP and packet size are checked, and the algorithm decides whether the source is a confirmed threat or suspicious. In the secondary stage, the legitimacy of the suspicious input is verified.

2.3 Market Strategy

As IoT technologies advance, companies are taking the initiative in developing various solutions and tools to help users have a better, safer experience in addition to forming dynamic, productive teams to develop these innovations in IoT. Examples of such innovations are presented.

Extreme Networks applies the BGP (Border Gateway Protocol) Flowspec (Flow Specification) Route Reflector feature to mitigate DoS attacks. The BGP is deployed on routers to monitor and analyze the flow of data traffic between the end devices and the internet. The authenticity of the data traffic is verified by comparing its parameters such as the source, destination, and L4 with a specific pre-known flow. The flow (data packets) of the DoS attack can be redirected from the victim host to another node to be dropped and flushed [22], [23].

VDOO offers its customers a customizable user experience where the IoT devices can be protected depending on their architecture and requirements. The VDDO ERA agent's firmware binary file is tailored using the Vision, VDDO's analysis platform to analyze and study the desired device to discover its vulnerabilities and protect devices from threats. The VDOO agent is automatically configured for the device. In addition, it provides run-time protection that does not compromise the device's resources and functions [24].

3. FUTURE TRENDS

As organizations and enterprises improve their security policies and significantly increase their awareness and protection methods against denial-of-service attacks, attackers continue to adapt to these security improvements and respond by reinforcing and enhancing their attack methods.

One of the challenges associated with deploying different protection mechanisms proposed by cybersecurity experts is the architecture of the current IoT system. Such as open IoT devices, resource-constrained devices, weak networking protocols, and poor quality of hardware components. The opportunity of improving the security of the network by implementing the proposed solution of changing the packets authentication technique is also bounded by difficulties. First is an unsupported lightweight encryption algorithm by standard cryptographic libraries of embedded hardware. Second is the chance of increasing the overhead of messages due to the addition of required information to the packets for the authentication method. Despite many proposed defending mechanisms for securing the hardware of devices, unfortunately, it could increase the power consumption and the chip size of those devices. The resource limitations of IoT devices increase the challenges of implementing effective solutions [25]. However, the continuous improvement of the IoT devices and networking architecture will promise more securing IoT systems even for critical implementation.

4. CONCLUSION

This paper reviewed types and examples of DoS attacks, proposed solutions, and the impact of such attacks. Two types of DoS attacks were discussed: the Smurf attack and SYN flood, and three proposed solutions were reviewed. Additionally, strategies currently employed in the market, and possible future IoT security trends are presented.

IoT has improved many aspects of people's lives. Nevertheless, their privacy and security may still be compromised with the ongoing development of the IoT environment without the implementation of appropriate security measures. Malicious attacks on IoT systems pose a threat that must be addressed by developers and designers of IoT services. In order to achieve maximum security in an IoT system, the security of all three layers, not only the network layer, must be guaranteed to ensure a safe and positive experience for all users.

5. REFERENCES

[1] S. Rizvi, A. Kurtz, J. Pfeffer and M. Rizvi, "Securing the Internet of Things (IoT): A Security Taxonomy for IoT," in 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th

IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE , New York, 2018.

[2] M. H. Miraz, M. Ali, P. S. Excell and R. Picking, "A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT)," in 2015 Internet Technologies and Applications (ITA), 2015.

[3] M. Burhan, R. A. Rehman, B. Khan and B. S. Kim, "IoT Elements, Layered Architectures and Security Issues: A comprehensive Survey," Sensors (Switzerland), vol. 18, no. 9, pp. 1-37, 2018.

[4] M. A. Razzaq, M. A. Qureshi, S. H. Gill and S. Ullah, "Security Issues in the Internet of Things (IoT): A Comprehensive Study," International Journal of Advanced Computer Science and Applications, vol. 8, no. 6, pp. 383-388, 2017.

[5] L. Liang, K. Zheng, Q. Sheng and X. Huang, "A Denial of Service Attack Method for an IoT System," in 2016 8th International Conference on Information Technology in Medicine and Education (ITME), Fuzhou, 2016.

[6] NETSCOUT, "NETSCOUT Threat Intelligence Report," 2019.

[7] A. K. Gomez and S. Bajaj, "Challenges of Testing Complex Internet of Things (IoT) Devices and Systems," in 2019 11th International Conference on Knowledge and Systems Engineering (KSE), Da Nang, 2019.

[8] P. Sethi and S. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," Journal of Electrical and Computer Engineering, vol. 2017, pp. 1-25, 2017.

[9] K. Chopra, K. Gupta and A. Lambora, "Future Internet: The Internet of Things-A Literature Review," in 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (Com-IT-Con), Faridabad, 2019.

[10] A. Roohi, M. Adeel and M. A. Shah, "DDoS in IoT: A Roadmap Towards Security & Countermeasures," in 2019 25th International Conference on Automation and Computing (ICAC), Lancaster, 2019.

[11] [1M. Anirudh, S. A. Thileeban and D. J. Nallathambi, "Use of Honeypots for Mitigating DoS Attacks targeted on IoT Networks," in IEEE International Conference on Computer, Communication, and Signal Processing (ICCCSP-2017), Melmaruvathur, 2017.

[12] "Cybersecurity: What you need to know about phishing, ransomware, and DoS attacks.," January 2019. [Online]. Available: https://revenuecycleadvisor.com/membership-check?destination=/node/5939. [Accessed 14 3 2020].

[13] CloudFlare, "Smurf DDoS Attack," CloudFlare , [Online]. Available: https://www.cloudflare.com/learning/ddos/smurf-ddos-attack/. [Accessed 14 3 2020].

[14] D. Peraković, M. Periša and I. Cvitić, "Analysis of the IoT Impact on Volume of DDoS Attacks," 2015.

[15] A. Lohachab, "Critical Analysis of DDoS—An Emerging Security Threat over IoT Networks," Journal of Communications and Information Networks, vol. 3, no. 3, pp. 57-78, 2018.

[16] Z. Liu, Y. Cao, M. Zhu and W. Ge, "Umbrella: Enabling ISPs to offer readily deployable and privacy-preserving DDoS prevention services," IEEE Transactions on Information Forensics and Security, vol. 14, no. 4, pp. 1098-1108, 2019.

[17] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu and D. Qiu, "Security of the Internet of Things: perspectives and challenges," Wireless Networks, vol. 20, no. 8, pp. 2481-2501, 2014.

[18] P. K. Chouhan, S. McClean and M. Shackleton, "Situation Assessment to Secure IoT Applications," in 2018 Fifth International Conference on Internet of Things: Systems, Management and Security (IoTSMS), Valencia, 2018.

[19] G. V. Hulme, "6 DoS attacks that made headlines," CSO, 22 9 2017. [Online]. Available: https://www.csoonline.com/article/3226399/6-dos-attacks-that-made-headlines.html#slide7. [Accessed 14 3 2020].

[20] R. Paudel, T. Muncy and W. Eberle, "Detecting DoS Attack in Smart Home IoT Devices Using a Graph-Based Approach," in 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, 2019.

[21] S. Kajwadkar and V. K. Jain, "A Novel Algorithm for DoS and DDoS attack detection in Internet of Things," in 2018 Conference on Information and Communication Technology, CICT 2018, Madhya Pradesh , 2018.

[22] "BORDER ROUTING," Extreme Networks, [Online]. Available: https://www.extremenetworks.com/solution/border-routing/. [Accessed 31 3 2020].

[23] CISCO, "Implementing BGP Flowspec," in Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide, Release 5.2.x, San Jose, Cisco Systems, 2014, pp. 175-201.

[24] "ERA Embedded Runtime Agent Protection," [Online]. Available: https://assets.ctfassets.net/u50eda8fk490/5KjRe7c29xsgajzzPyDRj5/0ccc9e586bdb3f815ff68affb4a00438/VDOO_ERA.pdf. [Accessed 31 3 2020].

[25] F. Meneghello, M. Calore, D. Zucchetto, M. Polese and A. Zanella, "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8182-8201, 2019.