How To Mitigate And Defend Against DDoS Attacks In IoT Devices

Basak Comlekcioglu
Department of Electrical and Electronics Engineering,
Institut Supérieur d'Électronique de Paris
Paris, France
basak.comlekcioglu@eleve.isep.fr

María Pilar Bezanilla
Department of Indsutrial and Systems Engineering,
Institut Supérieur d'Électronique de Paris
Paris, France
maria-pilar.bezanilla-casanueva@eleve.isep.fr

Ifiyemi Leigha
Department od Digital Security and Networks,
Institut Supérieur d'Électronique de Paris
Paris, France
ifiyemi.leigha@eleve.isep.fr

***Abstract*—The rapid increase and widespread adoption of Internet of Thing (IoT) in all spheres and facets of human endeavor has led to the emergence of new security threats, including Distributed Denial of Service (DDoS) attacks. This has become a major concern to the world owing to the significant disruptions it can cause to critical infrastructure and services. IoT devices have become popular targets for attackers due to their vulnerability and the ease of compromising them (Botnets). This paper aims to present the different solutions provided by different literatures on how to detect, mitigate and defend against DDoS attacks on IoT devices. First, we explain how this kind of attack work, highlighting the Mirai attack as a notable example and relevant statistics. Next, we present the different solutions found by researchers on how to mitigate, protect and defend against this type of attack such as Software-Defined Network (SDN) and Edge Computing. In addition, we try to reflect on this challenge from a theoretical perspective by explaining how IPV6 Unique Local Address can be used to defend and mitigate against DDoS attacks.**

Keywords—Internet of Things (IoT), Distributed Denial of Service (DDoS), Mirai Attack, Botnets, Network Anomaly Detection, Neural Network, Artificial Intelligence, Edge Computing, Public Key Infrastructure (PKI).

I. Introduction

Indeed, the rapid advancement of The Computer Network technology has given rise to the possibility of interconnecting physical devices such as vehicles, computers, phones, appliances and other everyday objects embedded with sensors, software and network connectivity such that these devices can collect and exchange data with each other and with their environment [1]. This network of interconnected devices is termed Internet of Things (IoT). The problem is that these IoT devices have some security lapses such as: inadequate security measures (improper authentication mechanisms, encryption), default or weak credentials, lack of firmware updates, large attack surface, bandwidth amplification, limited processing power and memory and lack of user awareness [2].

These weaknesses have paved the way for attackers to attack these devices. One of the most notable attacks on these devices used by attackers is Distributed Denial of Service (DDoS) attack. DDoS is a coordinated attack in which an attacker sends commands through a command and control (C&C) server to zombie agents (botnets – infected IoT devices) so that they can perform malicious activities like flooding a server [4]. An example of such attack is the Mirai botnet attack which took down the infrastructure of Dyn, a major Domain Name System (DNS) provider. As a result, popular websites like Netflix, Twitter and so on experienced massive disruptions. It implemented the attack with an estimated amount between 100,000 – 200,000 botnets [5]. The three types of DDoS attacks include volumetric attacks, protocol attacks and application layer attacks. So many defense mechanisms and strategies have been identified by researchers which can be used to defend and mitigate against this type of attack. Such strategies include Software-Defined Networks (SDN) [9] and Edge Computing [6]. In the subsequent sections, we fully discuss these strategies and as well reflect on this challenge and propose a theoretical solution. Our solution involves employing IPv6 Unique Local Addressing (ULA) as a means of communication among the connected devices. Honestly, this strategy proofs good because devices can communicate using this method without having to go through the Global Internet, which is really the propeller of DDoS attacks. Our solution can contribute greatly to the defense mechanism by adding an additional layer of network isolation and reducing the attack surface. Our solution proposes the use of multiple defense strategies, with ULA, as the core communication means in the network. We segment the network of IoT devices with ULAs based on device type and we implement several other strategies like Firewalls and Access Control List (ACL), ingress and egress filtering at the network edge devices (routers and firewalls), rate limiting and traffic shaping strategies, intrusion detection and prevention systems (IDS/IPS) and continuous monitoring and incidence reporting.

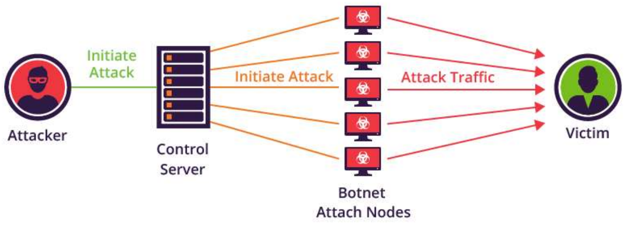

Fig 1: The MIRAI Botnet

II. Literature Review

Distributed denial-of-service (DDoS) attacks pose a significant threat to the availability and integrity of online services and networks. These attacks overwhelm the target system with a massive volume of malicious traffic, rendering it unable to handle legitimate user requests. This literature review aims to explore the solutions on how to mitigate and defend against DDoS attacks already presented by other researchers in their papers.

According to [8], machine learning based detection framework can be used to predict the possibility of an abnormal activity based on a log file generated by a honey pot, using a light weighted classification algorithm, preferably an unsupervised one. In this case, a honey pot is intentionally used to lure in attackers who will attempt to inject malware into the system through an open port say Telnet port 23 or 2323. The purpose of this is to capture the malware properties and its style of invading the security of IoT devices. This log file can contain information such as new malware families and their variants, type of targeted devices, server IP address, port numbers etc. These information on the log files are transformed into a proper table format that will work as data sets so that it can be used to train their machine learning model, which in turn is implemented in the network to detect traffic patterns like the data they were trained with. [7] takes the approach of leveraging computational resources at the edge of the network to accelerate the defense from IoT-DDoS attacks and arrest them before they can cause considerable damage. They propose ShadowNet - an architecture that makes the edge the first line of defense against IoT-DDoS. [3] proposed building the IoT architecture as a Software-Defined Network (SDN)-based traffic monitoring and abnormally detection framework so that since IoT devices normally have reasonably predictable traffic pattern during normal operations, if there is any abnormally, it can be detected. Typical components of such systems include SDN (Software Defined Networking) controllers, switch and IoT devices. This system setup tris to learn the IoT device's normal patterns to block communication that is out of ordinary.

III. Our Model

Our model involves two key processes:

A. Segmentation of IoT devices using IPv6 unique local addresses (ULAs)

IPv6 unique local addresses (ULAs) help devices in a local private network to communicate securely. ULAs are not reachable from the Global Internet. So, in this model, we divide our network into different segments based on certain criteria like device type and assign ULAs to each segment. No matter how large the private network is, ULAs can help departments, sites and so on to communicate securely.

B. Implement the edge paradigm at the network perimeter

At the network perimeter, we implement access control and filtering mechanisms. This can include firewalls, intrusion detection systems, intrusion prevention systems or access control lists that monitor and filter traffic entering or leaving the private IoT network. We set up ingress and egress filtering mechanisms, implement rate limiting and traffic shaping mechanisms to control the flow of traffic to and from the IoT segments. We also set up appropriate thresholds to limit the maximum number of connections, packets per second, or bandwidth allocated to each segment.

In Fig 1 below., the Gateway which is also a firewall acts as the network perimeter and provides access control and filtering capabilities. The IoT devices are assigned unique IPv6 ULAs and communicate with each other within the private network. The firewall monitors the traffic and applies security measures to mitigate DDoS attacks.

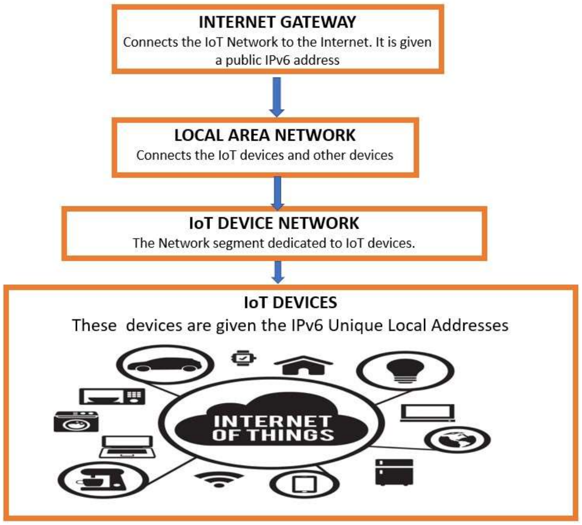
INTERNET GATEWAY
Connects the IoT Network to the Internet. It is given a public IPv6 address
LOCAL AREA NETWORK
Connects the IoT devices and other devices
IoT DEVICE NETWORK
The Network segment dedicated to IoT devices.
IoT DEVICES
These devices are given the IPv6 Unique Local Addresses
INTERNET OF THINGS

Fig 2. IPv6 ULA in IoT

IV. Conclusion

In conclusion, by using IPv6 ULAs and implementing appropriate security measures, the IoT environment can benefit from enhanced security and isolation, reducing the impact of potential DDoS attacks. Researchers, industries and academicians can make further research about this concepts.

References

[1] M. Alshamkhany, W. Alshamkhany, M. Mansour, M. Khan, S. Dhou and F. Aloul, "Botnet attack detection using Machine Learning," 2020 14th International Conference on Innovations in Information Technology (IIT), Al Ain, United Arab Emirates, 2020, pp. 203-208.

[2] M. H. Rohit, S. M. Fahim and A. H. A. Khan, "Mitigating and detecting DDoS attack on IoT Environment," 2019 IEEE International Conference on Robotics, Automation, Artificial-intelligence and Internet-of-Things (RAAICON), Dhaka, Bangladesh, 2019, pp. 5-8.

[3] K. M. Shayshab Azad, N. Hossain, M. J. Islam, A. Rahman and S. Kabir, "Preventive determination and avoidance of DDoS Attack with SDN over the IoT Networks," 2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI), Rajshahi, Bangladesh, 2021, pp. 1-6.

[4] [4] Al-Begain, Khalid, et al. "A DDoS detection and prevention system for IoT devices and its application to Smart Home environment." *Applied Sciences*, vol. 12, no. 22, MDPI, Nov. 2022, p. 11853.

[5] Z. Ahmed, S. M. Danish, H. K. Qureshi and M. Lestas, "Protecting IoTs from Mirai Botnet attacks using Blockchains," 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Limassol, Cyprus, 2019, pp. 1-6.

[6] Bhatia, Sajal, et al. "Distributed denial of service attacks and defense mechanisms: current landscape and future directions." Advances in Information Security, Springer Nature, 2018, pp. 55–97.

[7] Bhardwaj, Ketan, Joaquin Chung Miranda, and Ada Gavrilovska, "Towards IoT-DDoS prevention using edge computing." Workshop on Hot Topics in Edge Computing (HotEdge 18), 2018.

[8] R. Vishwakarma and A. K. Jain, "A Honeypot with Machine Learning based detection framework for defending IoT based Botnet DDoS attacks," 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2019, pp. 1019-1024.

[9] Jing, Hengchang, and Jing Wang. "Detection of DDoS Attack within Industrial IoT devices based on Clustering and Graph Structure features." *Security and Communication Networks*, vol. 2022, Hindawi Publishing Corporation, Mar. 2022, pp. 1–9.