ISSN 2712-0562
Sustainable Engineering and Innovation *Review Article*
Vol. 1, No. 1., June 2019, pp.43-48
https://doi.org/10.37868/sei.v1i1.36

DoS and DDoS vulnerability of IoT: A review

Emina Džaferović*[1], Ajla Sokol[1], Ali Abd Almisreb[1], Syamimi Mohd Norzeli[2]
[1] Department of Computer Sciences and Engineering, International University of Sarajevo, Bosnia
[2] Institute of Energy Infrastructure, University Tenaga National Selangor, Malaysia

*Corresponding author: emina.dzaferovic.95@gmail.com

Abstract
The Internet of Things (IoT) paradigm became particularly popular in the last couple of years in such a way that the devices are present in almost every home across the globe. Using cheap components one can connect any device to the internet and enable information collecting from the environment, making everyday life a lot easier. Even though it does bring multiple advantages to the table, at the same time it brings certain challenges and vulnerabilities that need to be addressed. In this paper, we focus on Distributed Denial of Service (DDoS) and Denial of Service (DoS) attacks and we provide a review of the current architecture of the Internet of Things which is prone to these.

Keywords: IoT, DoS, DDoS, Vulnerability, Review

1. Introduction

Internet of Things (IoT) as a term was firstly introduced in 1999 by Kevin Ashton [1]. It represents a network of devices that has the ability to connect and provide communication for billions of things simultaneously. This kind of network does not require expensive components but can be made out of cheap sensors and interconnected objects, which collect information from the environment and enable the improvements in the way we live. The Internet of Things is the next step in the path to the fourth industrial revolution, where the Internet is extended to include more of the physical world, introducing both more intelligence to everyday objects and hence more control over the physical world. The I in IoT refers to the universal interconnectivity between all perceivable objects, including the traditional computing objects such as computers and smart phones, and the new generation of smart objects. The T in IoT enabled by sensors, actuators, and all embedded computers into everyday objects, from toys and wearable to home appliances, manufacturing equipment, vehicles and up to buildings, power grids and the entire urban city.

Nowadays, IoT is implemented in many domains like transportation, agriculture, healthcare and energy production and distribution due to the fact that it makes our lives easier by making intelligent devices all around us perform daily tasks [2]. Given the above facts, it is only natural to assume that IoT plays the important part in our daily lives which is why it is predicted [3] that IoT devices will reach the usage of 28.1 billion by 2020 thus making the increase for about 30 times of that in 2009 [3].

Looking at this data and being aware of the purpose of IoT devices, we can notice that these devices have access to vast amount of all sort of private data which naturally rises security and privacy concern. The devices are based on client/server centralized model and consist of three-layer architecture with some additional helper layers: perception (collects information from the environment), network (controls processing of information) and application layer (contains business logic) [4]. Certain elements of this architecture are prone to particular attacks that threaten the security of IoT devices. Distributed Denial of Service (DDoS) attack is one of the examples. DDoS is one of the most widespread cyber attacks in the last couple of years. In this type of attack, perpetrator enslaves a number of internet dependent devices into an arrangement called botnet and then for a certain period of time makes simultaneous requests to a server, overwhelming the server

and making it ignore legitimate requests from the user [3]. In this paper we will review current architecture of IoT devices and how it is affected by DoS and DDoS attacks as well as provide some of the possible solutions in which these can be avoided.

The remainder of the paper is organized as follows: Section II presents related works on the topic of Dos, DDoS and IoT; Section III discusses the current architecture of IoT and possible improvements and Section V is devoted to the conclusion.

2. Literature review

In their work, Farooq et al [13] make a review on the Internet of Things and the security concerns behind it. The main security concerns are for data confidentiality, data integrity and data availability. Authors also talk about the security challenges and issues regarding each of the layers, and which security measures could be applicable. Authors [14] have touched upon the analysis of the security challenges and features of Internet of Things. Their work talks about the strategies that could be used in the design and deploy of security mechanisms for IoT. One of those strategies is to group things by location, and implement security system based off of the needs of group, while other strategy can be to focus more on the interaction of human users with the Internet of Things. Authors [1] talked about the security of Internet of Things and possible countermeasures. They discussed about the attacks on Wireless Sensor Networks (WSN) and Radio Frequency Identification (RFID), and the countermeasures available against each of the attacks possible. In the paper, one of the mentioned attacks was jamming, one of the oldest and most famous attacks on the WSN that targets specific packets in each layer, and some of the proposed measures are to regulate transmitted power and frequency hopping spread spectrum (FHSS), which is a way of transmitting radio signal.

Ning et al [5] talk about the future of security architecture of Internet of Things, where they proposed a model for heterogeneous IoT system, which consists of three essential security perspectives, such as information, physical and management. This model is three-dimensional information security model that introduces social layer, intelligence and compatibility for security considerations. Dao et al [19] discussed about the heterogeneous IoT networks, which are characterized by multiple access technologies and mobile edge computing capabilities, and securing them from the intelligent DDoS attacks. The solution they propose as a prevention of DDoS attacks is called MECshield, a framework consisted of central controller and multiple agents located at the edge of each local network, which enables the network to defend against malicious traffic.

In their paper, authors Peraković et al [29] analyze data that they collected from the domestic company regarding the trends in DDoS attacks. Through their research, it is stated that the Simple Service Discovery Protocol (SSDP) is the most common when it comes to conducting DDoS attacks. They also analyzed the amount of these attacks happening in regarding IoT, and concluded that the rise in IoT devices also mean rise in the DDoS attacks. Simple study on handling DDoS attacks has been conducted by the Oh et al [15], where they presented four major approaches that can be considered in order to defend against these attacks. Given approaches for defense against DDoS attacks are by rate limit framework, defense by offense, by active filtering and by IP traceback. In the research conducted by Khalil [27], the main topic was the security of Internet of things against DDoS attacks, where he talked about the security measures by using machine-learning algorithms. Author provides algorithm that helps in monitoring, analyzing, and recognizing attack patterns [17].

In the paper, authors [8] touched upon the malwares in IoT with DDoS capabilities. The malware, such as Linux. Hydra, PsybOt, Chuck Norris, Tsunami, Aidra, Spike, Mirai, show the growth in popularity and are able to hit the targets with much more attacks than in past. This research is conducted in order to raise the awareness for the researchers to look more into the higher security measures in this field. Authors Bhardwaj et al [26] explore the option of DDoS attacks prevention in IoT using edge computing, where the edge computing, by their definition, is usage of computing resources near the end devices. They develop a solution called ShadowNet, which serves as the defense against DDoS attacks by making the edge computing a first line of defense. Solution is based on the edge functions that establish fast path between networks that send packets with information about the traffic in IoT to their main service. The authors Hallman et al [11] discussed about the details behind IoT security vulnerabilities and IoT-based botnets and botnet malware used in DDoS attacks. They mentioned some of the cyber security vulnerabilities of Internet of Things. This paper also talks about Mirai botnet malware, which is a part of Trojan malware family that serves as a DDoS attack

on the IoT devices [28]. After the analysis, authors showed that this newly released malware has a soft spot that can be research into much deeper, which is regarding the SQL injection attack, where the counterattack is possible to be implemented. Tamanna [18] discussed about the cloud computing, the form of IoT, that has taken the computing from the desktop to the Internet, and the DDoS attacks that happen in this cloud environment. This author proposes a solution against the DDoS attacks in the form of Software Defined Networks (SDN) features, since SDN is flow based concept with standardized API and support for IDSs and Intrusion Prevention Systems (IPSs). Javaid et al [22] conducted a research in the field of DDoS attacks on the IoT devices, and their prevention using blockchain technology, a technology that serves as online distributed ledger consisted of list of blocks. For the proposed model online software platform called Ethereum was used, that helps with the generation of addresses of devices, as well as the customized smart contract that enabled the defense mechanism against DDoS attacks. Authors have conducted experiments to prove that their model is capable of better detection and prevention of DDoS attacks.

Authors Kasinathan et al [30] proposed a solution for detection of DoS attacks in Internet of Things, specifically in 6LoWPAN based networks. The most important components of their solution were IDS Probe, which operates with custom firmware and is used to detect the incoming packets with incriminating properties, and IDS, which provides many benefits, such as multithreading and intrusion prevention system. This proposed method was tested by making the simulation of five different IPv6 UDP flooding attacks on a targeted 6LoWPAN node. Results and graphs that they came up with showed that their solution can detect DoS attacks in IoT structures with 6LoWPAN protocol. Authors [29] research the security of Internet of Things in regards to the electronic healthcare, where the solution given should enhance the abilities of server to observe attack patterns. In their proposed solution, they used the assumption that the communication nodes are present in specific geographical locations and proposed an algorithm for checking the DoS attack by comparing the packet buffer utilization rate of a server and Time to Live (TTL) value of arriving packet.

3. Discussion

3.1. Layers of architecture

Architecture of Internet of Things is hierarchical, and consists of three main layers. Those layers are application layer, network layer and sensor (perception) layer [5].

The main purpose of application layer is to provide different applications for different scenarios that the IoT may find itself. Layer provides Quality of Service (QoS) by managing and processing data from the middleware layer. Due to the fact that application layer holds sensitive data, if the perpetrator gains access to the layer he will be able to maliciously modify the data [2].

Middleware layer is additional layer located between network layer and application layer that acts as an intermediary between the two. It takes the data from the network layer after which it links the system to cloud and database, and processes and stores the data. One of the main purposes of middleware layer is provision of APIs that are used to meet the demand of the application layer [6].

Network layer has the purpose to collect data from sensor layer and send it to the upper layer using wired or wireless medium. Attacks on the network layer are very common and diverse. Usually, they impose threat to coordination of work and information being shared between the devices.

Perception layer is all about identification of objects and collection of necessary data which are then transformed into digital signals. Tech which is present in this layer includes sensors and RFID tags which are the main components [7]. In case of an attack on sensors, there would be an interference with the collection of data. Even though the generic architecture of IoT is described and illustrated in Figure 1, it is not a standardized architecture.

Denial of Service (DoS) attack is a cyber-attack where the perpetrator tries to exhaust resources or bandwidth of a legitimate user. In case that this kind of attack is coordinated, meaning a perpetrator is trying to perform the above using several compromised nodes than it is called a Distributed Denial of Service (DDoS) [8]. DoS is nothing more but flooding vast amount of traffic in order to spend network resource, bandwidth, target CPU time etc. Different types of these attacks are present but some of the most important ones include SYN flood, DNS flood, Ping flood, UDP flood and ICMP broadcast [9].

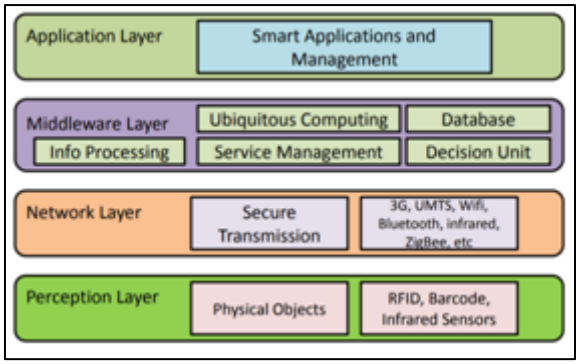

Figure 1: IoT Generic Architecture (as illustrated in [7])

3.2. DoS/DDoS attacks and IoT

Denial of Service (DoS) presents a major attack in the field of computer networks. They take over the target by exhausting its resources. Their purpose is to disable service or slow the performance of the service with numerous different existing attack techniques.[23] This attack influences network in order for victim not to be able to access it. When attacker tries to use DoS as attack mechanism, it has three things in mind to compromise – confidentiality, integrity and availability [25].

Distributed Denial-of-Service, more known as DDoS, presents one of the most dangerous threats for the Internet. The amount of these types of attacks increases in size annually. In order to perform DDoS attack, three steps need to be applied here, and they are. Scanning is the first step, where the attacker scans the vulnerable machine by different scanning strategies. Next step is propagation, where the attacker recruits machine in order to generate stream of packets that will perform the attack onto the vulnerable machine. The third and final step is communication, where the two different models can be applied, Agent-Handler model or IRC model. [10]

Generally, two types of techniques for DDoS attacks ar used. The first one is reflection, where attackers send packets to different destinations with the IP address of target as the source address of packets. Main purpose behind this technique for attacker is to hide the trail. Another technique called amplification, large numbers of packets are sent to the victim's machine [24]. Both types of attacks generally tend to attack on the weaknesses in TCP/IP protocol using different types of attacks, such as TCP Syn Flood, UDP Flood, ICMP flood and similar [21].

In recent period, with rise of use and applications of IoT devices, the various DoS and DDoS attacks have start to take place as threats. These attacks happen in different protocol layers in IoT networks. Those protocol layers are physical layer, MAC layer, 6LoWPAN layer, network layer and application layer.

In physical layer, there are several different attacks that can occur, such as node capturing, jamming and spamming. All of these attacks have distinct name, hence the function of those is explained by it. The most popular is jamming attack, where the attacker creates interference to the signal transmitted in the physical layer. MAC layer has many types of Dos/DDoS attacks that can be performed. Some of those are CCA manipulation, ACK attack and PANID conflict. CCA or Clear Channel Assessment manipulation is the way of skipping CCA mechanism which can cause collisions. ACK or Acknowledgment attack is caused by interference in ACK frames. PANID conflict is the way to attack user by placing coordinates with same Personal Area Network ID next to each other in that way causing conflict.

When it comes to 6LoWPAN layer, mainly fragment duplication and buffer reservation are kind of the attacks used in order to infiltrate IoT network. Fragment duplication is duplicating single fragment of a packet, while buffer reservation is reserving buffer space with incomplete packets, and keeping that space occupied. In network layer of IoT, two specific types of attacks can be performed. Those are RPL-Specific attack, and non-RPL-Specific attack. RPL-Specific attack is used to attack RPL protocol design, while the attacks not specific to RPL are those that are applicable to RPL protocol design, such as neighbor, sinkhole or cloneID. Neighbor is retransmission of routing control message. Sinkhole attack is the one where attacker finds good routing parameters, and show the node created as a good parent. In cloneID attack, the attack clones nodes to a

multiple positions in the network. When it comes to the final layer, which is application layer, several different attacks may occur. Flooding and desynchronization are one of those [20].

All of these protocols in IoT network are vulnerable and opened to the attacks by hackers. These attacks are also shown in the form of malware-based botnets, like Mirai, XOR and BillGates. These malwares use DoS/DDoS attacks as their base attacking different layers and performing same types of attacks on those layers. Malwares and Dos/DDoS attacks are becoming more difficult to fight against, since with their growth, the current security mechanisms are not good enough [20].

4. Conclusion

This paper has touched upon the topic of Internet of Things security architecture and security issues regarding Dos and DDoS attacks. The issue of security in IoT does not cover only a single piece of software, but it is connected to the whole system. Architecture of solution to a security issue in IoT can be found when the issues are specified, which means that the general security framework cannot be applied to every case. [12] Although the field of IoT has been attractive in the research field in the recent years, it has attracted new difficulties and challenges with it. In time, the development in Internet of Things field will bring new issues to its security [16]. There have been many researches done in the field of security and applicable solutions for defense against different attacks. Unfortunately, rise in the attacks means rise in the difficulties in securing systems against them. The need for researching different security measures have grown, and currently, researchers are in great need of others to try to find solution for current problems. Several of those solutions have been presented in the literature review, but even more of those are needed.

References

[1] O. El Mouaatamid, M. Lahmer, and M. Belkasmi, “Internet of Things Security : Layered classification of attacks and possible Countermeasures,” Electron. J. Inf. Technol., vol. 9, no. 9, pp. 66–80, 2016.

[2] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, “Internet of things (IoT) security: Current status, challenges and prospective measures,” 2015 10th Int. Conf. Internet Technol. Secur. Trans. ICITST 2015, pp. 336–341, 2016

[3] K. Angrishi, “Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets,” pp. 1–17, 2017

[4] [4] K. Sonar and H. Upadhyay, “A survey on ddos in Internet of Things,” Int. J. Eng. Res. Dev., vol. 10, no. 11, pp. 58–63, 2014.

[5] H. Ning and H. Liu, “Cyber-Physical-Social Based Security Architecture for Future Internet of Things,” Adv. Internet Things, vol. 02, no. 01, pp. 1–7, 2012

[6] K. Chen et al., “Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice,” J. Hardw. Syst. Secur., vol. 2, no. 2, pp. 97–110, 2018

[7] R. Khan, “Future Internet : The Internet of Things Architecture , Possible Applications and Key Challenges Future Internet : The Internet of Things Architecture , Possible Applications and Key Challenges,” no. April 2017, pp. 257–260, 2012

[8] A. Spognardi, M. De Donno, N. Dragoni, and A. Giaretta, “Analysis of DDoS-Capable IoT Malwares,” vol. 11, pp. 807–816, 2017

[9] N. Tripathi, “DoS and DDos Attacks: Impact, Analysis and Countermeasures,” Natl. Conf. Adv. Comput. Netw. Secur., no. December 2013, 2013

[10] A. Sriyastava, B. Gupta, A. Tygai, A. Sharma and A. Mishra, “A Recent Survey on DDoS Attacks and Defense Mechanisms”, pp. 570-580, January, 2011

[11] R. Hallman, J. Bryan. G. Palavicini, J. Divita and J. Romero-Mariona, “IoDDoS – The Internet of Distributed Denial of Service Attacks: A Case Study of the Miraj Malware and IoT-Based Botnets”, SCITEPRESS, pp. 47-58, California, USA, 2017

[12] Q. Jing, A. Vasilakos, J. Wan, J. Lui and D. Qui, “Security of the Internet of Things: Perspectives and Challenges”, Springer Science + Business Media, New York, USA, 2014

[13] M. Farooq, M. Waseem, A. Khairi and S. Mazhar, “A Critical Analysis on the Security Concerns of Internet of Things (IoT)”, International Journal of Computer Application, vol. 111, February, 2015

[14] R. Roman, J. Zhou and J. Lopez, “On the features and challenges of security and privacy in distributed internet of things”, Computer Network, 2013, http://dx.doi.org/10.1016/j.comnet.2012.12.018

[15] D. Mukhopadhyay, B. Oh, S. Shim and Y. Kim, "A Study on Recent Approaches in Handling DDoS Attacks", International Journal of Computer Science Trends and Technology, vol. 3, 2015
[16] H. Suo, J. Wan, C. Zou and J. Lui, "Security in the Internet of Things: A Review", IEEE International Conference on Computer Science and Electronics Engineering, 2012
[17] M. Kolinsyk, V. Kharchenko, I. Piskachova and N. Bardis, "A Markov Model of IoT System Availability Considering DDoS Attacks and Energy Modes of Server and Router"; ICTERI, vol. 14, Ukraine, 2017
[18] T. Tamanna, "DDoS Attack in "Cloud of Things" environment, Software Defined Networking (SDN) and a research on defense mechanism against DDoS using SDN", International Journal of Scientific & Engineering Research, vol. 7, 2016
[19] N. Dao et al, "Securing Heterogeneous IoT with Intelligent DDoS Attack Behaviour Learning", IEEE Communications Magazine, 2017
[20] A. Aris, S. Oktug and T. Voigt, "Security of Internet of Things for a Reliable Internet of Service", Autonomous Control for a Reliable Internet of Service, pp. 337 – 370, 2018
[21] A. Wod and J. Stanković, "Denial of Service in Sensor Networks", Computer, vol. 35, 2002
[22] U. Javaid, A. Siang, M. Aman and B. Sikdar, "Mitigating IoT Device based DDoS Attacks using Blockchain", CryBlock'18, pp. 71-76, Germany, 2018
[23] Q. Gu and P. Liu, "Denial of Service Attacks", 2008
[24] S. Specht and R. Lee, "Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures", International Workshop on Security in Parallel and Distribted Systems, pp. 543-550, September, 2004
[25] N. Tripachi and B. Mehtre, "Dos and DDoS Attacks: Impact, Analysis and Countermeasures", National Conference on Advances in Computing, Networking and Security, 2013
[26] K. Bhardwaj, J. Miranda and A. Gavrilovska, "Towards IoT – DDoS Prevention Using Edge Computing", 2018
[27] T. Khalil, "IoT Security against DDoS Attacks Using Machine Learning Algorithms", International Journal of Scientific and Research Publications, vol. 7, June, 2017
[28] R. Ullah, M. Asif and M. Ahmad, "DoS/DDoS Detection for E-healthcare in Internet of Thigns", International Journal of Advanced Computer Science and Applications, February, 2018
[29] D. Peraković, M. Periša and I. Cvitić, "Analysis of the IoT Impact on Volume of DDoS Attacks", PosTel 2015, Belgrade, December, 2015
[30] P. Kasinathan, C. Pastrone, M. Spirito and M. Vinkovits, "Denial-of-Service detection in 6LoWPAN based Internet of Things", IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications, 2013.