Sustainable Engineering and Innovation ISSN 2712-0562
Vol. 3, No. 1, January 2021, pp.23-28 *Review Article*
https://doi.org/10.37868/sei.v3i1.124

Survey of DoS/DDoS attacks in IoT

Rozan Khader[1*], Derar Eleyan[2*]
[1] Department of Higher Studies, Palestine Technical University Kadoorie, Palestine
[2] Department of applied computing, Palestine Technical University Kadoorie, Palestine

*Corresponding author: r.m.khader3@sutedents.ptuk.edu.ps, d.eleyan@ptuk.edu.ps

Abstract

The term internet of things (IoT) has gained much popularity in the last decade, which can be defined as various connected devices over the internet. IoT has rapidly spread to include all aspects of our lives. For instance, smart houses, smart cities, and variant wearable devices. IoT devices work to do their desired goals, which is to develop a person's living with his/her minimal involvement. At the same time, IoT devices have many weaknesses, which attackers exploit to affect these devices' security. Denial of Service (DoS) and Distributed Denial of Service (DDoS) are considered the most common attacks that strike IoT security. The main aim of these attacks is to make victim systems down and inaccessible for legitimate users by malicious malware. This paper's objective is to discuss and review security issues related to DoS/DDoS attacks and their countermeasures i.e. prevention based on IoT devices' layers structure.

Keywords: IoT; DoS; DDoS; Security

1. Introduction

According to Nemade, "The Internet of Things (IoT) is the network of physical objects—devices, vehicles, buildings and other items—embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data" [1]. Despite the fact that this term was invented in 1999 by Kevin Ashton, who was working on Radio Frequency Identification (RFID) technology, it took a decade for IoT to become a popular phenomenon around the world. Nowadays, there are billions of various devices connected to the Internet around us in different applications, such as home automation, social life, education systems, health care, entertainment, and transport systems [2]. The number of devices is expected to exceed 75 billion Internet of Things (IoT) devices by 2025 [3]. Furthermore, the fast and wide development of IoT devices comes with many challenges and security issues in these devices that should be addressed. Because these devices exist in all our life aspects, and gather information about our daily lives, there must be systems and solutions that mitigate the security challenges and security issues [4] which make them prone to different type of attacks. The most common attacks Denial of Service (DoS) and Distributed Denial of Service (DDoS) can be launched via various methods.

DoS aims to prevent services provided by Io applications. This is done by wasting and exhausting network resources by unnecessary traffic [5]. DDoS happens when the host server is flooded with massive number of unnecessary requests by geographically distributed zombie devices [6]. IoT applications do not have a standard architecture layers yet, but most of the researchers divide it into four major layers with some additional helper layers. These layers are: Perception, Network, Middleware, and Application [7]. Each layer has security issues which make it prone to different types of attacks. In this paper, we will discuss IoT architecture and protocols used in each layer, the main challenges and security issues that make IoT prone to different attacks, the major DoS/DDoS attacks that strike different IoT layers and possible countermeasures and prevention techniques that could be used.

1.1. Challenges and security issues in IoT

- Bandwidth and Power Consumption: IoT devices designed to be small, with less powerful computing capability, and less memory capacity. Thus, advanced cryptographic-algorithms cannot be applied to the IoT system, since it demands high computing and memory requirement. Meanwhile, IoT contains many connected sensors to do the desired job with maintaining security issues, which may consume high bandwidth. Therefore, security mechanisms should be applied with minimal overhead on IoT system [8].
- Insufficient authentication and authorization mechanism: Most of IoT devices suffer from weak and default passwords, insecure credentials, and lack of access control. Therefore, attacker might exploit this to threaten privacy and data integrity [9].
- Insecure web interface: Most of IoT devices have web interfaces that do not require the use of strong passwords. Some of them still do not lock out users who have made several failed login attempts. Therefore, these interfaces are prone to several attacks like brute force credentials, injections, and scripting [10].
- Insecure network services: Because all IoT systems rely heavily on network communications, these networks must be secured. Otherwise, network services will be compromised through buffer overflows, fuzzing, DDoS, and other attack forms.
- Poor phys cal security: If any malicious actor gains physical access to IOT device, he could break or remove storage card and use it to extract stored information. Moreover, if the device is equipped with external ports like a USB port, attacker can use it to attack the operating system [9].

1.2. Literature review

An extensive literature study has been conducted and results presented in next section where we present IoT DoS/DDoS attack types based on layered structure. Also some relevant solutions are presented hereby to give wide overview of the existing approaches. Farooq et al [11] review IoT layered architecture and main security goals which is data confidentiality, data integrity and data availability. They also talk about security issues and possible solutions at each layer. Ning et al [12] propose a systematic security architecture (named IPM) that consist of three security aspects: information, physical, and management. This security model introduces social layer, and intelligence and compatibility for security consideration. Authors [13] focus on authentication issue for Wireless Sensor Networks (WSN) in term of security and computational overhead. As a result of this research, sensors and tags limited resource posing a great challenge in mitigating DoS attacks in field of WSN.

1.3. The IoT architecture

As mentioned earlier, there are different architecture proposed for IOT application, but the basic architecture shown in Fig.1 consists of perception layer, network layer, middleware layer and application layer [7] [8]. In IoT architecture design, many things have to be considered, such as scalability and the ability to operate among different devices and models. Therefore devices must be able to interact with each other dynamically [11]. Fig. 1 presents used IoT layered architecture and used technologies and protocols in each layer. IoT consists of heterogeneous technologies used in different layers. This makes various researches to propose different approaches for designing homogeneous, and as possible secured from attacks, infrastructure [6]. In the next section, we will explore security challenges in each layer, famous types of Dos/DDos attacks that happen in each layer, and possible solutions for these problems.

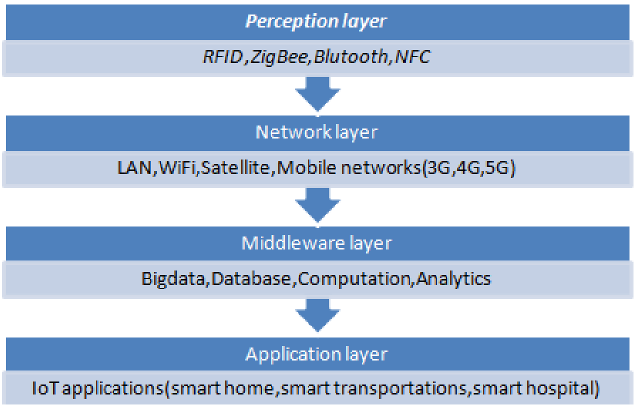
Perception layer
RFID,ZigBee,Blutooth,NFC
Network layer
LAN,WiFi,Satellite,Mobile networks(3G,4G,5G)
Middleware layer
Bigdata,Database,Computation,Analytics
Application layer
IoT applications(smart home,smart transportations,smart hospital)

Figure 1. IoT layers and used technologies and protocols

2. IoT DoS/DDoS attack classification based on layered structure

2.1. Perception layer

2.1.1. Security vulnerabilities at perception layer

This layer, which is sometimes called ‘sensing layer’, depends on physical resources part of IoT. It uses several sensing technologies and devices for collecting data, transforming them to digital signals and forwarding them to the network layer [12]. Perception layer technologies include RFID tags, cameras, wireless sensor network (WSN), GPS, and Bluetooth. These devices are chosen based on IoT applications functionalities. The data collected from the surrounding environment may come in different forms, such as motion, light, change in temperature, and location.

Perception layer sensors and devices are presented to end users. These devices are intended to increase flexibility, reduce the cost, and have limited resources in computing and storage [13]. Moreover, they are limited in data transmission rate [14]. This restriction is exploited by intruders.

Famous types of attacks on this layer:

- RF Jamming attack: Since most of wireless devices are using radio frequency (RF) signals to communicate with others, this signal can be jammed with other stronger signals. The attacker intercepts and denies communication between the sensor, or tag, and the reader of transmitted data [7][15].

- Eavesdropping: mainly affects confidentiality part of IoT device. It is a dangerous attack, because attacker can read and collect secret information committed between tag and the reader of data, and take advantage of the information gathered [16][15]. These confident information could be phone calls, text messages, video conferences [17].

2.1.2. Security solution at perception layer

Authors [15] talk about possible countermeasures available against attacks on RFID, WSN. In the paper, one proposed countermeasure against jamming is to regulate transmitted power and Frequency Hopping Spread Spectrum (FHSS). It is a powerful solution to avoid interference and multi-path fading (distortion), it also decreases narrowband interference, increases signal capacity, and improves the signal to noise ratio[18].

Porambage et al. [19] have discussed a pervasive authentication (PAuthKey) method which is lightweight in nature. This algorithm has been developed keeping in mind the resource scarcity at sensors end. Moreover, key establishment process was also refined in light of it. This PAuthKey system allows users to establish secure connection at lower cost directed towards the sensor nodes.

Lin Hu et al.[20] have researched on secrecy enhancing technique to minimize Secrecy Outage Probability (SOP) that come from eavesdropping at perception layer. It resulted in enhanced security service at minimal cost as compared to other methods available.

2.2. Network layer

2.2.1. Security vulnerabilities at network layer

This layer operates in the same way of TCP/IP network layer, and also faces the same typical communication networks security problems that affect confidentiality, availability and integrity of data [21][14]. It is responsible for transmitting the collected data from the perception layer devices and sensors [17].

Famous types of attacks on this layer:

- Flooding Attacks: In this type of attacks, many useless traffics are sent through the network, causing the target system to become unreachable. More specifically, the system drain is done by huge number of requests from the attacker [22], for instance, UDP flood. Attacker floods different UDP (User Datagram Protocol) packets on different victim ports, therefore, the server host will inspect these ports for incoming requests over and over, causing exhaustion to victim resources [23].
- Reflection-based flooding Attacks: The attacker, in this type of attacks, intercepts the authentic connection, and sends repeated fake requests to reflectors. These reflectors reply at the same time to the target system causing it to become unreachable [23].

2.2.2. Security solution at network layer

As for traditional IPv6, there is tested way to secure normal networks called IPsec. Since IoT devices added to the Internet using IPv6 over Low-power Wireless Personal Area Networks (6LoWPAN), Raza et al. [24] introduced a way to secure the IoT based on the tested IPsec extension added to 6LoWPAN. Moreover, Encapsulation Security Payload (ESP) and Authentication Header (AH) techniques are used to secure the communication from application layer devices to network layer.

2.3. Middleware layer

2.3.1. Security vulnerabilities at middleware layer

This layer is responsible for data manipulation and intelligent decisions based on calculation and processing. The processing is done on massive amount of data collected from sensors and tags. These data is stored in database, also Cloud computing technology could be used in this layer [25][8] . Different attacks and security threats are associated to this layer, because of accumulating large amount of data and using cloud computing [14]. The main aim of these attacks is cloud data to destroy users privacy [26].

Famous types of attacks on this layer:

- Signature Wrapping Attack: For cloud services XML, signatures is used to verify authenticity of connection with another service. Attacker can change the eavesdropped messages and do arbitrary commands on behalf of a legitimate user, without any change in the signature. Likewise, Amazon Elastic Cloud Computing (EC2) uses Simple Object Access Protocol (SOAP) interface for controlling the deployed machine. Attackers exploit weakness in this interface and modify the sent messages or execute arbitrary commands [26].
- Flooding Attack in Cloud: Attackers deplete the resources of the cloud service by sending extensive requests. Cloud system may transfer the affected services to another server causing to exhaust another server. This mainly affecting the quality of service [26],[30-32].

2.3.2. Security solution at middleware layer

Shafagh et al. [33] proposed a mechanism called Encrypted Query Processing Approach, which allow users to initiate encrypted queries on database using cryptographic schema. In this way middleware layer can store data securely on the database and it is feasible in low-power devices.

2.4. Application layer

2.4.1. Security vulnerabilities at application layer

This layer is considered as the top layer; it is responsible for the logical part in IoT application. In other words, this layer will do data manipulation and show it to end users using users interface (UI) [7][23]. This layer face different security challenges, for example, access permissions and authentication are very likely to be hacked, because it is difficult to maintain within different types of applications and users [21]. In addition, hackers may exploits application layer vulnerabilities, such as buffer overflow, cross-site scripting, and SQL injection, as a result, maintaining data privacy and protection is difficult [22].

Famous types of attacks on this layer:

- Reprogramming Attack: Attacker may change the program code if they have unauthorized access, which leads to data leakage. With access to the source-code of the program, they can alter the code to the use. Moreover, if they use infinite loop in the code, it will lead to exhaustion of the server resources [23].
- Path based DoS attack: This attack called PDoS attack , which is done by flooding multi-hop end-to-end communication paths with data packets [27].

2.4.2. Security solution at application layer

For authentication issue in application layer, Cirani et al. [28] proposed an authorization framework based on integration with external Open Authorization Service (OAS). The whole solution denoted as IoT-OAS, Which is targeting HTTP and CAP (Constrained Application Protocol) services. This method provide flexible and easy integration with existing services, in addition to lowering processing load.

3. Conclusions and future work

This paper discusses Dos/DDoS attacks and security solutions with respect to each IoT layer. It shows that every layer have different vulnerabilities exploited by attackers. Security possible solutions for the networks are also discussed, which makes the IoT network more secure. In order to have strong secure structure, we must take care of security issues for all different layers, not only single one. In other word, securing application layer only will not prevent attackers from hack network layer [29]. As declared earlier, perception layer devices characterized with flexibility and ease of use, for reducing costs. This make perception layer the most vulnerable layer and require extended research to identify capabilities [7]. Despite the massive number of DoS/DDoS prevention mechanism given in the literature, they need a lot of work and improvement. Because of IoT applications industry dynamically change. There is massive need to use technologies like machine learning and artificial intelligence to be able to make unified solution against different scenarios with heterogeneous devices, networks and protocols [6]. Furthermore, users of the applications must be aware of importance of using strong passwords and credentials, and update software as necessary.

References

[1] J. Chase, “The Evolution of the Internet of Things,” *Texas Instruments*, vol. 1, no. February, p. 7, 2013.

[2] Y. Perwej, M. Ahmed, B. Kerim, and H. Ali, “An Extended Review on Internet of Things (IoT) and its Promising Applications,” *Commun. Appl. Electron.*, vol. 7, no. 26, pp. 8–22, 2019, doi: 10.5120/cae2019652812.

[3] “Number of IoT devices 2015-2025 | Statista,” 2014. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ (accessed Dec. 11, 2020).

[4] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, “Internet of Things: Security vulnerabilities and challenges,” *Proc. - IEEE Symp. Comput. Commun.*, vol. 2016-Febru, no. August 2017, pp. 180–187, 2016, doi: 10.1109/ISCC.2015.7405513.

[5] S. Sicari, A. Rizzardi, D. Miorandi, and A. Coen-Porisini, “REATO: REActing TO Denial of Service attacks in the Internet of Things,” *Comput. Networks*, vol. 137, pp. 37–48, 2018, doi: 10.1016/j.comnet.2018.03.020.

[6] A. Lohachab and B. Karambir, “Critical Analysis of DDoS—An Emerging Security Threat over IoT Networks,” *J. Commun. Inf. Networks*, vol. 3, no. 3, pp. 57–78, 2018, doi: 10.1007/s41650-018-0022-5.

[7] A. Roohi, M. Adeel, and M. Ali Shah, “DDoS in IoT: A Roadmap Towards Security & Countermeasures,” in *DDoS in IoT: A Roadmap Towards Security & Countermeasures*, 2019, no. September, pp. 5–7.

[8] S. Deep, X. Zheng, A. Jolfaei, D. Yu, P. Ostovari, and A. K. Bashir, “A survey of security and privacy issues in the Internet of Things from the layered context,” *arXiv*, no. March, 2019.

[9] R. Vishwakarma and A. K. Jain, “A survey of DDoS attacking techniques and defence mechanisms in the IoT network,” *Telecommun. Syst.*, vol. 73, no. 1, pp. 3–25, 2020, doi: 10.1007/s11235-019-00599-z.

[10] K. Dineva and T. Atanasova, “Security in IoT systems,” *Int. Multidiscip. Sci. GeoConference Surv. Geol. Min. Ecol. Manag. SGEM*, vol. 19, no. 2.1, pp. 569–577, 2019, doi: 10.5593/sgem2019/2.1/s07.075.

[11] M. U.Farooq, M. Waseem, A. Khairi, and S. Mazhar, “A Critical Analysis on the Security Concerns of Internet of Things (IoT),” *Int. J. Comput. Appl.*, vol. 111, no. 7, pp. 1–6, 2015, doi: 10.5120/19547-1280.

[12] 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, doi: 10.4236/ait.2012.21001.

[13] S. Kumari, M. K. Khan, and M. Atiquzzaman, “User authentication schemes for wireless sensor networks: A review,” *Ad Hoc Networks*, vol. 27, no. November, pp. 159–194, 2015, doi: 10.1016/j.adhoc.2014.11.018.

[14] J. Y. Khan, “Introduction to IoT,” *Internet of Things (IoT)*, no. January 2019, pp. 1–24, 2019, doi: 10.1201/9780429399084-1.

[15] P. Rani and G. S. Lakshmi, “IoT Vulnerabilities and Security,” vol. 2, no. 6, pp. 1–3, 2017, [Online]. Available: http://www.ijasret.com/VolumeArticles/FullTextPDF/166_IJASRET_IoT_Vulnerabilities_and_Securit

y.pdf.

[16] N. C. Luong, D. T. Hoang, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Data Collection and Wireless Communication in Internet of Things (IoT) Using Economic Analysis and Pricing Models: A Survey," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 4, pp. 2546–2590, 2016, doi: 10.1109/COMST.2016.2582841.

[17] I. Cvitić, M. Vujić, and S. Husnjak, "Classification of security risks in the iot environment," *Ann. DAAAM Proc. Int. DAAAM Symp.*, vol. 2015-Janua, no. 2016, pp. 731–740, 2015, doi: 10.2507/26th.daaam.proceedings.102.

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

[19] M. El Beqqal and M. Azizi, "Review on security issues in RFID systems," *Adv. Sci. Technol. Eng. Syst.*, vol. 2, no. 6, pp. 194–202, 2017, doi: 10.25046/aj020624.

[20] M. Burhan and R. A. Rehman, "IoT Elements , Layered Architectures and Security Issues : A Comprehensive Survey," pp. 1–37, 2018, doi: 10.3390/s18092796.

[21] N. Hossein, "Frequency Hopping Spread Spectrum: An Effective Way to Improve Wireless Communication Performance," *Adv. Trends Wirel. Commun.*, 2011, doi: 10.5772/15482.

[22] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "PAuthKey: A Pervasive Authentication Protocol and Key Establishment Scheme for Wireless Sensor Networks in Distributed IoT Applications," *Int. J. Distrib. Sens. Networks*, vol. 2014, 2014, doi: 10.1155/2014/357430.

[23] L. Hu *et al.*, "Cooperative Jamming for Physical Layer Security Enhancement in Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 219–228, 2018, doi: 10.1109/JIOT.2017.2778185.

[24] S. Rizvi, A. Kurtz, J. Pfeffer, and M. Rizvi, "Securing the Internet of Things (IoT): A Security Taxonomy for IoT," *Proc. - 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. Trust. 2018*, no. August, pp. 163–168, 2018, doi: 10.1109/TrustCom/BigDataSE.2018.00034.

[25] K. Somasundaram and K. Selvam, "IOT – Attacks and Challenges," *Int. J. Eng. Tech. Res.*, vol. 8, no. 9, pp. 9–12, 2018, doi: 10.31873/ijetr.8.9.67.

[26] 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.

[27] S. Raza, S. Duquennoy, J. Höglund, U. Roedig, and T. Voigt, "Secure communication for the Internet of Things-a comparison of link-layer security and IPsec for 6LoWPAN," *Secur. Commun. Networks*, vol. 7, no. 12, pp. 2654–2668, 2014, doi: 10.1002/sec.406.

[28] S. Kraijak and P. Tuwanut, "A SURV EY ON INTERNET OF THINGS A RCHITECTURE , PROTOCOLS , POSSIBLE A PPLICATIONS , SECURITY , PRIVA CY , REAL-WORLD IMPLEMENTATION A ND," pp. 26–31, 2015.

[29] 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, doi: 10.1007/s41635-017-0029-7.

[30] J. Deng, R. Han, and S. Mishra, "Defending against Path-based DoS Attacks in Wireless Sensor Networks," 2005.

[31] S. Cirani, M. Picone, P. Gonizzi, L. Veltri, and G. Ferrari, "IoT-OAS: An oauth-based authorization service architecture for secure services in IoT scenarios," *IEEE Sens. J.*, vol. 15, no. 2, pp. 1224–1234, 2015, doi: 10.1109/JSEN.2014.2361406.

[32] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," *Wirel. Networks*, vol. 20, no. 8, pp. 2481–2501, 2014, doi: 10.1007/s11276-014-0761-7.

[33] H. Shafagh, A. Hithnawi, A. Dröscher, S. Duquennoy, and W. Hu, "Poster: Towards encrypted query processing forn the Internet of Things," in *MobiCom '15: Proceedings of the 21st Annual International Conference on Mobile Computing and Networking, September 2015, New York: Association for Computing Machinery, 2015,* pp. 251–253.