Effect of denial of service attack on IoT Network Performance

Abstract

The denial of service attack is a common attack that causes the network components that are not available to the users of a network specifically the Internet of things (IoT) network, The IoT is a networking service that enables the users to access the internet world irrespective of their geographical location (Yelavarthi, 2019). It is a platform that helps to communicate between different objects that are connected by the internet IoT network. In which the components are self-organized using network identification. So, the uniqueness of this network is the dynamic nature and configured anywhere.

Since the IoT is widespread across the internet there is a chance of various attacks that are performed on the IoT networks such as Denial of service (DoS), DNS Flooding and Privilege escalation. These attacks cause to decrease the reliability speed and power of the network. The main cause for these types of performance deviation is that the Denial of service attacks in which the user is unable to access the system, the DoS attacks can be placed at the server, network components such as router and switches and even in the host systems. And the security measures which are used in the conventional networks are not usable in the IoT networks, because the IoT network does not have a predefined network structure it is connected to the internet and can be changed at any time hence showing a different network behaviour each time.

The objects in the IoT networks are machines so the connection in the IoT is a machine to machine connections and that is the speciality of IoT networks. The population selected for this research project is client workstations and other devices that are connected to the IoT network of an organization. The performance of the network objects and components are measured under normal condition and the Denial of service attack and are compared to find out the effect on the performance.

Introduction

The IoT networks are designed to overcome the limitation of normal wireless and wired networks. Because the IoT is a widespread network across the internet there is a need for measuring the performance under the Denial of service attack which is often caused by the jamming of the networks or by attacks performed by attackers. Advancements in internet communication changed the internet to internet of people to the internet of things. In the IoT network, each object is equipped with actuators or sensors to work it as automated. And the denial of service attack causes the network components available which affect the performance of the network.

The performance can be measured by using the throughput of the testing network which is the subnet of an organization where uses IoT for communication and automation. The objects in the IoT are capable of decision making so the attacks especially Denial of service attack is a large threat to IoT network and its performance. And IoT is being used in multiple applications such as in the Smart Home, Industrial and economical automation, Healthcare automation and Automated transportation. The performance of IoT is greatly affected by the mobility of gateways which reduces the throughput and roundtrip times.

The performance of the IoT network is affected by the behaviour of each node in the network and the routing protocol that is going to be used so the increase in the number of nodes will result in reduced performance by giving space for attackers to exploit. This paper presents the performance

analysis of the IoT network under Denial of Service attack. The mobility and flexibility of the IoT network are obtained by using wireless IoT networks in which testing for performance make easy.

Background

The attacks in the IoT networks and its performance and the mitigation strategies are recently becoming very popular due to the increased demand in automation.

Sriram Sankaran (Sankaran, 2016) analysed the performance of the IoT network under different attacks for that he constructed a Markov model for IoT networks and then constructed a framework for analysing the performance at each node of the network. the model was generic and can be applied to different domains. The probability of an attack is calculated using the framework and model that is developed.

Gaurav Kumar and others (G. Kumar, 2017) analysed the performance of an office network during a DDoS attack in which a group of IoT objects were connected to the WLAN server, the simulated environment was having a high load database application, an access point jammer is used to simulate the denial of service attack and then compared the same traffic with the normal network scenario.

Muraleedharan and others (Osadciw, 2006) analyze the physical layer Denial of Service attack on a wireless sensor network which is the basic part of the IoT network and is attacked by jammers which is a cause for DDos attack when is used at the access point.

Hanumat Prasad Alahari and others (Yelavarthi, 2019) analysed the performance of the application and network layer of IoT which is under Distributed DoS attack and DDoS attack. The attacks were simulated in the Contiki Operating system in Cooja simulation and the attacks were performed on messages that contain data, which in turn reduces resources in the application layer and network layer and making the targets unavailable.

Md. Mahmud Hossain and others (Matthewpirretti, 2006) have proposed “Towards an analysis of security issues, challenges and open problem in the internet of things” which primarily engrossed on to security issues of the IoT. As everybody knew that IoT is well-known and rapidly improving technologies in the internet world. IoT is diffusing its automation and advancement in its technologies to all fields such as hospitality, construction, software development and automotive. But the increase in the technologies caused IoT to face serious attacks like Denial of service attack.

P. Hemalatha and others (P. Hemalatha and J. Vijithaananthi, 2017) analysed an effective performance for denial of service attack detection. In this paper, the performance is analysed using the Artificial Bee Reverse Tracing Algorithm(ARBT) and it will detect the denial of service attack, and the approach was carried out using a network simulator.

Da Yin and others (D. Yin, 2018) analysed the DDoS attack detection and mitigation with software-defined internet of things Framework. They considered the SD IoT framework to find out the attack detection and mitigation algorithm and the key of the proposed algorithm is the calculation of cosine similarity and used the threshold value to calculate to find out whether an attack has occurred

Methods

The different types of attacks that are happening to the internet or the cyberspace are common nowadays. One among those threat is that the denial of service attack or Dos attacks as the name indicates it is the denial of service to a group of users or even a server or some functions of a server. And the denial of service attacks is being used as a mask for so many different types of attacks so that they can dissolve the communication with the outside world. The Dos attacks are mainly done using DNS flooding or by attacking the access point of a wireless network. In this paper, the performance of the IoT network is measured using the throughput of the system that is the total time required for a data frame to reach from source to destination and vice-versa. The denial of service can be of two types the first one is that Dos attack which affects only one client system, and the next one is a distributed denial-of-service attack in which the services are denied for a group of client systems.

For calculating the performance of the network from an organization is selected and an isolated network is created inside that network. The throughput of the network is calculated using the formula $Throughput \leq \frac{RWIN}{RT}$, where RWINis the TCP Receive Window size and RTT is the roundtrip time. The throughput of the normal network is calculated first, then the throughput of the network which is under Denial of service attack is measured at a different time and formulated a data set and compared the data to find out the performance of IoT network under the denial of service attacks.

References

D. Yin, L. Z. a. K. Y., 2018. A DDoS Attack Detection and Mitigation With Software-Defined Internet of Things Framework. *IEEE Access,* Volume 6, pp. 24694-24705.

G. Kumar, E. A. J. H. a. A. P., 2017. Analyzing the effect of DoS attacks on network performance,. *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), New York, NY,* pp. 372-376.

Matthewpirretti, n. v. S. P. a. M., 2006. he Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense. *International Journal of Distributed Sensor Networks,* Volume 2, pp. 267-287.

Osadciw, R. M. a. L. A., 2006. Cross Layer Denial of Service attacks in Wireless Sensor Network Using Swarm Intelligence. *40th Annual Conference on Information Sciences and Systems Princeton University IEEE.*

P. Hemalatha and J. Vijithaananthi, 2017. An effective performance for Denial of Service Attack (DoS) detection. *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam,* pp. 229-233.

Sankaran, S., 2016. Modeling the performance of IoT networks.. *2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS),* pp. 1-6.

Yelavarthi, H. P. A. a. S. B., 2019. Performance Analysis of Denial of Service DoS and Distributed DoS Attack of Application and Network Layer of IoT. *2019 Third International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, ,* pp. 72-81.

C. Pu and T. Song, "Hatchetman Attack: A Denial of Service Attack Against Routing in Low Power and Lossy Networks," *2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, Shanghai, 2018, pp. 12-17.

Y. E. Sagduyu, Y. Shi and T. Erpek, "IoT Network Security from the Perspective of Adversarial Deep Learning," *2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, Boston, MA, USA, 2019, pp. 1-9.

N. Giachoudis, G. Damiris, G. Theodoridis and G. Spathoulas, "Collaborative Agent-based Detection of DDoS IoT Botnets," *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, Santorini Island, Greece, 2019, pp. 205-211.

Z. Liu *et al*., "The Efficiency Comparison Between DDoS and DoS Attack," *2018 9th International Conference on Information Technology in Medicine and Education (ITME)*, Hangzhou, 2018, pp. 1050-1054.

H. P. Alahari and S. B. Yelavarthi, "Performance Analysis of Denial of Service DoS and Distributed DoS Attack of Application and Network Layer of IoT," *2019 Third International Conference on Inventive Systems and Control (ICISC)*, Coimbatore, India, 2019, pp. 72-81.

C. Pu, "Spam DIS Attack Against Routing Protocol in the Internet of Things," *2019 International Conference on Computing, Networking and Communications*, Honolulu, HI, USA, 2019, pp.73-77.

D. Yin, L. Zhang and K. Yang, "A DDoS Attack Detection and Mitigation With Software-Defined Internet of Things Framework," in *IEEE Access*, vol. 6, pp. 24694-24705, 2018.

J. Li, M. Liu, Z. Xue, X. Fan and X. He, "RTVD: A Real-Time Volumetric Detection Scheme for DDoS in the Internet of Things," in *IEEE Access*, vol. 8, pp. 36191-36201, 2020.

M. S. Abdalzaher, L. Samy and O. Muta, "Non-zero-sum game-based trust model to enhance wireless sensor networks security for IoT applications," in *IET Wireless Sensor Systems*, vol. 9, no. 4, pp. 218-226, 8 2019.

M. Roopak, G. Y. Tian and J. Chambers, "Multi-objective-based feature selection for DDoS attack detection in IoT networks," in *IET Networks*, vol. 9, no. 3, pp. 120-127, 5 2020.

T. Gong, A. Gil C. P. Ramos, S. Bhattacharya, A. Mathur and F. Kawsar, "AudiDoS: Real-Time Denial-of-Service Adversarial Attacks on Deep Audio Models," *2019 18th IEEE International Conference On Machine Learning And Applications (ICMLA)*, Boca Raton, FL, USA, 2019, pp. 978-985.

J. Liu, A. Ren, L. Zhang, R. Sun, X. Du and M. Guizani, "A Novel Secure Authentication Scheme for Heterogeneous Internet of Things," *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, Shanghai, China, 2019, pp. 1-6.

C. Pu and B. Groves, "Energy Depletion Attack in Low Power and Lossy Networks: Analysis and Defenses," *2019 2nd International Conference on Data Intelligence and Security (ICDIS)*, South Padre Island, TX, USA, 2019, pp. 14-21.

J. N. Bakker, B. Ng and W. K. G. Seah, "Can Machine Learning Techniques Be Effectively Used in Real Networks against DDoS Attacks?," *2018 27th International Conference on Computer Communication and Networks (ICCCN)*, Hangzhou, 2018, pp. 1-6.

A. Sharma, I. Sharma and A. Jain, "A Construction of Security Enhanced and Efficient Handover AKA Protocol in 5G Communication Network," *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Kanpur, India, 2019, pp. 1-6.