Effect of Distributed denial of service attack on IoT Network Performance

Abstract

The IoT refers to a system of interconnected objects that can gather and transmit data over a network without a human to human or human to computer interaction (Wikipedia, 2020). The availability of information with integrity and confidentiality is a critical parameter in network communications. However recent events which are reported related to security attacks shows vulnerabilities among IoT devices which bring a security risk to the network environment. One common use of this is the distributed denial of service attack that blocks the legitimate users accessing the computers hence affects the availability. Recent research has done in the field of the internet shows the performance is affected inversely, in this regard the current work is new in the field of IoT. This paper mainly concentrated on the various DDoS attacks, their impacts on the IoT network performance and countermeasures to defend against these attacks. The method employed to analyse the performance in calculating the throughput of the network by sending Transmission Control Protocol (TCP) data and calculating the Roundtrip time of the data packet. The experimental result shows there is a significant reduction to IoT network performance while under DDoS attack.

Introduction

The need for information and communication protection has resulted from the sudden increase in the dependence on information and communication technologies in both private and business environment (Dragan Peraković, 2015). In the world with automated and connected devices, the world can be considered as a large network of interconnected devices. Though the network gets bigger and bigger the security risks associated with that also in the ever-increasing phase, one of the major attacks that are significant while considering the availability of information with integrity and confidentiality is the Distributed denial of service attack (DDoS).

The DDoS attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic (Cloudflare, 2020). The most common DDoS attacks are ICMP(Ping) Flood, SYN Flood, Ping of Death, Slow Loris, NTP Amplification, HTTP Flood, Zero-day DDoS attacks and volume-based attacks (Imperva, 2020). By using any of these attacks the attacker can make the network resource, the server or the devices in the IoT infrastructure unavailable.

The goal of this paper is to analyse the network performance of an IoT network under DDoS attack by measuring the throughput of the network so that if the performance of the IoT network is affected then we can discuss and implement the countermeasures or mitigation strategies that can be used to increase the performance of the network. hence the availability of service or the data can be achieved without compromising the security of the network or the devices connected to it.

The IoT network is created in a virtual environment with a server that is used for a city-wide monitoring system which is connected to a Network gateway and then connected to traffic camera on one end and another end the images from the camera are continuously monitored for speeding and other traffic violation. Then partial DDoS attack is implemented on the Network gateway and measured the performance. The full DDoS cannot be implemented because then it is not able to measure the throughput of the network and that is a limitation of the network and the area of interest for this project is the area from the camera sensor to the sensor. Then the effect of network performance is measured, and mitigation strategies are implemented.

Background

The performance of the IoT network under DDoS attack is relatively less spoken as compared with other security issues in IoT Networks. The number of DDoS attacks is regularly growing which requires constant research in the field of IoT network and attacks.

Dragan Peraković (Dragan Peraković, 2015) and others had analysed the impact on the volume of DDoS attacks on IoT networks and show that the DDoS attacks are increasing day by day as the development of IoT infrastructure and hence there is need to analyse the performance of the IoT network.

To measure the network parameters there is a need to find out the required parameters, environment and framework for that the performance analysis of mesh network considered Diego Passos and others (Passos, 2006) measured performance in the mesh network. it was based on the ReMesh Wireless mesh network deployed over a city. It was using a modified version of OSLR and Ad Hoc routing protocols the performance is measured using the Expected Transmission Count (ETX) and Packet Loss Rates (PLR). The ETX is calculated by multiplying forward delivery ratio and reverse delivery ratio. Then the network throughput can be calculated using ETX value.

Christos Douligeris and others (Douligeris, 2004) mentioned different types of DDoS attacks and those are Network device level in which attacker taking advantage of bugs or weakness in the software or by exhausting the hardware, and in OS level the attacker takes advantage of ways the operating system implements protocol one example of this category is Ping of Death attack, Application-level attack is done by setting the machine to out of order by draining the resources on the host, Data flood attack is done by flooding the system with data fragments and protocol feature attack is made possible by DNS flooding and all these attacks are possible in IoT Network.

Pourya Shamsolmoali and others (Zareapoor, 2014) mentioned a countermeasure for DDoS attacks in cloud computing which is based on the statistically-based filtering system. The proposed system analyses the entire data packet hence reduce the number of false-positive detections. And in this done by using the Jensen-Shannon algorithms and calculate the information divergence(D). At first, the algorithm checks for the IP address is spoofed if yes then drops the packet else the packet is sent to next stage in which the information divergence is calculated and is compared with the learned probabilities and if that is positive drops the packet and adds the address to the blacklist, else is sent to the server. In the IoT network is the performance is reduced then this algorithm can be used to mitigate the Distributed Denial of Service attack (DDoS).

The researches conducted up to now shows that devices in the IoT can be utilized to generate a DDoS attack and hence affects the performance of the network. the purpose of this research is to analyse the performance of the IoT network under DDoS attack and to implement countermeasure to improve the network performance.

Methods

The Distributed denial of service attack is the most important risk factor affecting the network performance of the IoT network. the IoT infrastructure is most susceptible to DDoS attacks compared to other networks due to the implementation and environment which it is setup. A network connection on the IoT is composed of several network layers, the Open Systems Interconnection (OSI) model describes it in seven layers as shown in the figure below and each layer, the DDoS attack is possible by disrupting the service of that layer.

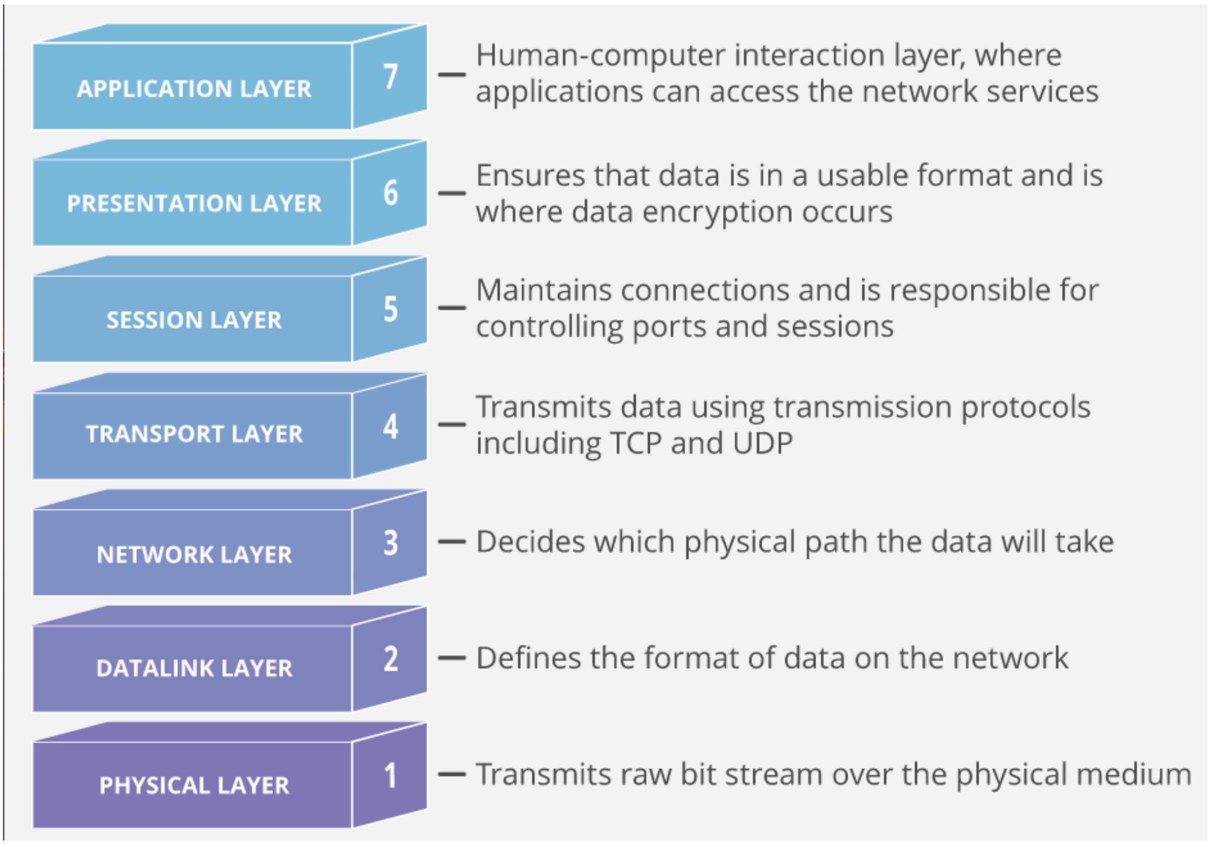
APPLICATION LAYER
7
— Human-computer interaction layer, where applications can access the network services
PRESENTATION LAYER
6
— Ensures that data is in a usable format and is where data encryption occurs
SESSION LAYER
5
— Maintains connections and is responsible for controlling ports and sessions
TRANSPORT LAYER
4
— Transmits data using transmission protocols including TCP and UDP
NETWORK LAYER
3
— Decides which physical path the data will take
DATALINK LAYER
2
— Defines the format of data on the network
PHYSICAL LAYER
1
— Transmits raw bit stream over the physical medium

Fig: OSI model (Cloudflare, 2020)

For the calculation of ETX, PLR and Throughput two networks are selected one in which a simple network of city-wide monitoring system which is created on a virtual machine. And the other network created is a normal LAN network to compare the performance of IoT under the attack of DDoS, the created IoT network is shown below

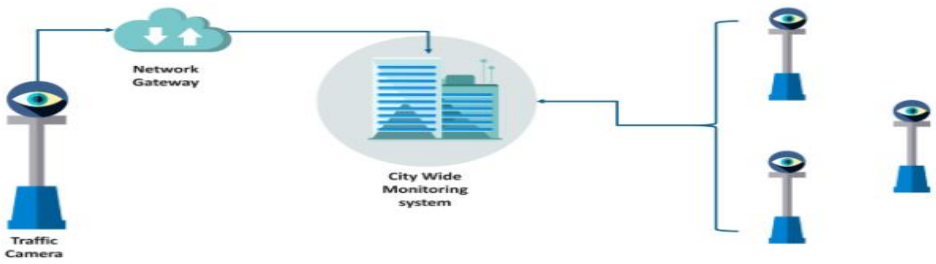

Fig: IoT network implemented on the virtual machine (Priyadarshiny, 2018)

Then the performance of the network is being measured using the Expected Transmission count and Packet loss Rate and the data obtained is recorded under different types of data packets, the Transmission control protocol (TCP) and User datagram protocol (UDP) are used. After obtaining the data, it is compared, and the throughput of the network calculated by sending iperf that is a TCP data packet sent from the server to the destination node.

Then one of the DDoS attacks is partially implemented namely HTTP flooding, the reason for partial implementation is that if the DDoS is implemented completely it causes the service to shut down completely so that the measuring of performance is impracticable. The same attack is implemented in the LAN network as well. Then the results were compared to find out how much the DDoS is affecting the network performance in the IoT infrastructure network. and the PLR indicates the number of packets that are dropped during the transmission from source to destination. Then the average delay, ETX, PLR and throughput is calculated for different data packets and bandwidth and made a dataset.

Mitigation Strategy

if the performance of the network is affected by the DDoS attacks then there is a need for mitigation strategies to overcome the poor network performance. The statistical method of filtering the data packet proposed by Pourya Shamsolmoali for cloud networks (Zareapoor, 2014) can be used in IoT networks as well. In this method, the incoming network traffic is stored in a buffer and then the IP of the received packet is checked with the IP address of the blacklisted attackers, if it finds a match then drops the packet otherwise sends to the next filter and checks for the similarity between different packets send by because in DDoS attacks the attacker mostly sends the same type of packets. The second filter checks for the frequency of packets if it exceeds the threshold value it will be flagged attacker and the IP is sent to the blacklist and Drops the packet, if this filter also passes the data packet then it is sent to the server, by using this method the DDoS attack can be greatly reduced in The IoT network and the performance can be improved.

References

Cloudflare, 2020. *What is a DDoS Attack?.* [Online]
Available at: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/
[Accessed 03 09 2020].

Douligeris, C. a. M. A., 2004. DDoS attacks and defense mechanisms:classification and state-of-the-art.. *Computer Networks,* pp. 643-666.

Dragan Peraković, M. P. I. C., 2015. ANALYSIS OF THE IoT IMPACT ON VOLUME OF DDoS ATTACKS. *XXXIII Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom,* pp. 1-10.

Imperva, 2020. *DDoS Attacks.* [Online]
Available at: https://www.imperva.com/learn/ddos/ddos-attacks/
[Accessed 03 09 2020].

Passos, D. T. D. M.-S. D. M. L. a. A. C., 2006. Mesh network performance measurements. *International Information and Telecommunicatios Technologies Symposium (I2TS),* pp. 48-55.

Priyadarshiny, U., 2018. *Real World IoT Applications in Different Domains.* [Online]
Available at: https://medium.com/edureka/iot-applications-c62cd48b7363
[Accessed 06 09 2020].

Wikipedia, 2020. *Internet of things.* [Online]
Available at: https://en.wikipedia.org/wiki/Internet_of_things
[Accessed 02 09 2020].

Zareapoor, P. S. a. M., 2014. Statistical-based filtering system against DDOS attacks in cloud computing. *International Conference on Advances in Computing, Communications and Informatics (ICACCI),* pp. 1234-1239.