DDOS ATTACK ON IOT DEVICES

Asmaa Munshi, Nouf Ayadh Alqarni, Nadia Abdullah Almalki.
Department of Cybersecurity
College of computer science and engineering
University of Jeddah
Jeddah, Kingdom of Saudi Arabia
Ammunshi@uj.edu.sa
Nalqarni0038.stu@uj.edu.sa
Namalki0001.stu@uj.edu.sa

***Abstract*— Internet of Things (IoT) is an application of the internet correlation with devices that makes human life easy. The need to use (IoT) in our lives makes this field expands every day without stopping. Which would let everything connected to the internet exposure to penetration. As the need for (IoT) devices grows, the horizon of malicious abuse expands [1]. In this paper, we will study one of the most common violations in IoT devices, which is Distributed Denial of Service (DDoS) attack and study its impact on (IoT) devices in order to be aware to control our utilizations and the need to secure the Internet of Things devices in our lives.**

Keywords-component (IoT devices; DDoS attacks; Networks defense; IoT protocold; Cyber security)

I. INTRODUCTION

Since the Internet of Things began, it has been facing many objections, due to concern about security vulnerabilities. Many violations can occur in hardware, software, operating systems or networks. Hackers have successfully exploited these devices and systems, to access resources, harm these devices and prevent service from legitimate users. In this paper, we will study DDoS attack on IoT devices to get know about what is the mechanism that allows occurring, how to defend our devices from DDoS attack and to be aware to protect systems and devices.

II. EXTENSIVE BACKGROUND

A. The Vulnerability of IoT Devices:

TABLE 1:PRESENTS THE LIST OF VULNERABILITIES ON IOT DEVICES [2]

Vulnerability	Weak points
Insufficient validation and authorization	• Poor password • Weak password recovery systems • Unsecured credentials
Untrusted user interfaces	• Low login credentials, plain text credentials • In the absence of encryption, data can be compromised.
Network is not reliable	• Sensitive network facilities can be used to attack target.
Privacy problems	• Untrustworthy end points, not strong authentication,non-encrypted transmitting, and exposed network facilities that let attackers access poorly protected data .
Physical insecurity	• Some ports and memory cards let attack.

B. Protocols on IoT:

There are many researches that have been mentioned as protocols for Internet of things with different advantages and disadvantages [3], we will discuss some of them in this research shown in "Fig1",

1) Constrained Application Protocol(CoAP):

- It is a deployment protocol designed for lightweight machine-to-machine connections in restricted networks.
- Interact easily with http.
- Provide four type of security:
  1. NoSec It is assumed that security is not available in the transmitted message.
  2. PreshardKey support Programmed sensors using Symmetric cipher keys.
  3. RawPublicKey for devices requiring authentication using the public key.
  4. Certificates.

2) Routing Protocol Low Power and Lossy Networks (Routing-RPL):

- Network layer using IPv6.
- Provides confidentiality and integrity of the message.

3) 6LoWPAN:

- It is used in the network layer for direct connection to the Internet and is open source.
- Alternative for IPv6.
- There is no safety in the layer, so it contains many vulnerabilities that can be exploited by the attackers.
- In studies indicating that the proposed solution is used IPsec.

4) 4. 802.15.4 Protocol:

- It works in the physical layer and mac layer.
- It provides protection and security by using encryption cryptography.

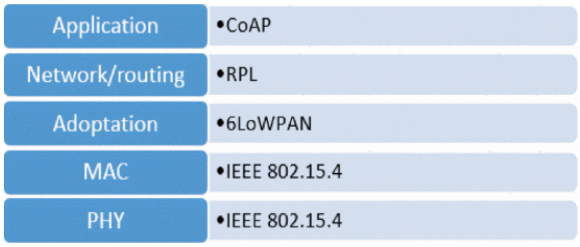

Figure 1. IoT Protocol

C. DDoS Attack Overview:

A denial-of-service attack is characterized by an explicit attempt to prevent the legitimate use of a service. A distributed denial-of-service attack deploys multiple attacking entities to attain this goal [4]. It is a malicious active to prevent traffic of workflow in network, server or hardware. The main goal is to crush the infrastructure and disrupt data flood. This attack can successfully effect when devices and systems are compromised. Generally, DDoS attack achieve its goals by preventing the normal workflow from access required destination.

D. DDoS Attack Work [5]:

The attacker must take control of the network and devices that help to implement a distributed denial of service (DDoS) attack. The malware (like bots or zombies) software helps the hacker to gain control. The hacker sends commands to each bot remotely, and then directed it to IP address of desired source. Hacker send hundreds of commands to the equipped robots, which causes overflow to the target port or server. The service disabled for normal traffic, and this is the aim of DDoS attack. shown in "Fig2".

E. DDoS Attack Classification on IoT:

IoT is separated into key three layers that are Observation Layer, Network Layer, and Application Layer [6] shown in "Fig3", then DDoS attacks varied based on layers:

1) DDoS on Observation Layer:

- RFID: A technique that receives data and reads it from sensors that are included in Internet of Things devices, without any direct interference from humans, and here the possible attack occurs, such as Jamming, Kill Command Attack, etc.
- In the layer relay on Confusion to prevent access to services.

2) DDoS on Network Layer:

The network layer is the area most vulnerable to attacks, targeting wired and wireless networks, where huge data is pumped to carry out the attack. The system that receives the data remains in an attempt to delay the response to requests and the required resources can be made until there are no direct connections, which leads finally to prevent the service. As an example of a network layer attack: ICMP flood, SYN flood attack.

3) DDoS on Application Layer:

In the application layer which contains the basic user interface (smart governments, smart cities, smart devices, mobile applications, web) through which it works using applications. In this layer two types of attacks can occur as Reprogramming Attack, Path based DoS.

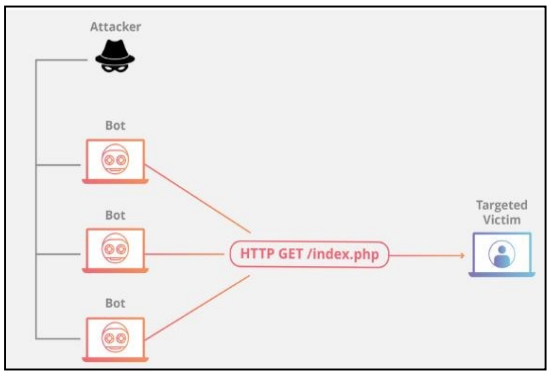

Figure 3. DDoS attack work

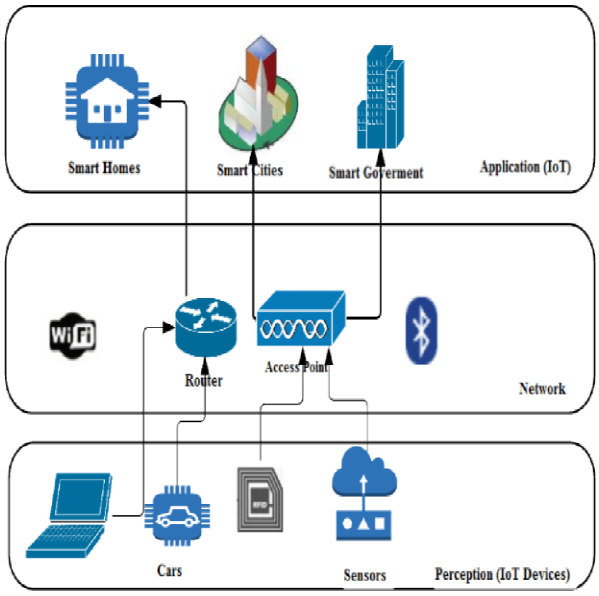

Figure 2. Internet of Things Architecture

F. Example of DDoS Attack on IoT Devices [6]:

Because the Internet of Things IoT devices, connected to each other, This doing to form a suitable area for the occurrence of distributed denial-of-service DDoS attacks, and this is what makes malware implementation (bots, and zombies) distributed on it easily:

1) Mirai:

Infect Linux systems.

2) Wirex:

Infect Android devices. Google addressed the problem and deleted many applications on the Play Store.

3) Reaper:

This bot has the ability to search for vulnerabilities and vulnerabilities in Internet of Things devices, and major companies like Cisco and Linksys have been affected.

4) Torii:

Torii is newly has been covered. It has the ability to objective utmost of today's Most recent computers, smartphones, tablets with having designs similar to (64-bit), x86, ARM, MIPS, etc.

G. Latest General DDoS Attacks:

TABLE 2 :RECENT POPULAR DDOS ATTACKS [7]

Target	DATE	Description
Russian Defense Ministry's website	March 2018	The attack targeted the ministry's website while they were verifying the names of new weapons.
Boston Globe	November 2017	DDoS is interrupting the newspaper phone, and the editing system is down.
UK National Lottery	September 2017	Preventing clients from setting the lottery.
Bank of Greece Website	May 2016	Rrestricted the servers of the Bank to stay passive for 6 hours.

H. Defend DDoS Attack on IoT Devices classification:

1) Classical DDoS Detection:

- Mitigation flooding [8]:

This defense based on the technology of directing the harmful flood to an external server through a mediator, with a fee-based agreement for the mediator to protect IoT devices. This technique used for attacks that its scale is very large.

- Detecting Intrusions:

1. Network traffic detection [2]:

It considered one of the old solutions to prevent the denial of service attacks distributed in the Internet of Things networks, which go towards the system layer model or use a model to cross all layers of the system. To prevent these attacks in all layers of the system and network architecture. This solution goes through successive steps, begins with capturing the attack, then defining the type of hacker and finally the defense operation.

The defense process consists when it detects in the first step that the amount of traffic to service is very large by measuring and comparing with the capacity of traffic. Then the sabotaged device that sends many requests larger than usual identified, and here this device is easily disposed of.

However, due to the failure of this mechanism to prevent all attacks with this technique, machine learning used to obtain more measurements of the attack rate with the normal traffic rate.

2. System workflow detection [9]:

It is also one of the old ways to detect attacks, implemented by creating a honeypot (data base) to store suspected packets aims system workflow." In this proposed scheme, honeypots are used as a trap for the intruders intending to harm the security of the system. A honeypot, as its name suggests, used for luring in attackers with an intention to observe and analyze their method of launching an attack by capturing information about the attacking agent like malware" [10]. So it checks all incoming requests to the server. When one of requests suspected, it directs this request to the honeypots to protect the main server from attack. Also it examines the IP address of the device that sent the attack, and stores it in a separate database away of the main servers.

Based on these logs, each request is examined in future times and compared to the honeypots content, then it will prevented if it found there. And it allowed if detection tool does not find the IP address in it.

2) Modern DDoS attack Detection:

- Malicious software Detection: (using machine learning) [11]

We found a variety of learning machine algorithms that can detect distributed denial of service attacks, as this mechanism works on a rigorous test that reveals the difference in the behavior of networks of Internet of things devices.

Among these algorithms that were tested in a research paper followed by Princeton University, "We tested five machine learning algorithms to distinguish normal IoT packets from DoS attack packets: K-nearest neighbors KDTree algorithm, support vector machine with linear kernel, Decision tree using Gini impurity scores, Random Forest using Gini impurity scores, neural Network (NN)" [11].

Where they stated in their research that these algorithms provided effective results in encouraging them to continue to work on improving them more to monitor networks of IoT devices. By implementing this is in a more real environment to reach accurate numbers. Statistics can be inferred that help detect distributed denial of service attacks.

- Prohibition Techniques: (using middleware like SDN) [7]

It is a technology, which works specifically for IoT devices successfully, where there is software whose mission is defensing (SDN). "detecting malicious packets on the given network path is one of the most challenging problems in the field of network security. We argue that the advent of Software Defined Networking (SDN) provides a unique opportunity to effectively detect and mitigate DDoS attacks[8]. So, SDN middleware It's main objective task is mitigate the attack damage by using this software features, it receives data in the IoT environment while it is working and saves all data related to the interaction of IoT devices with users.

When unexpected interactions detected, alerts sent to make the necessary block later. Because a software created that, its job is to detect any unbalanced transmissions: such as increasing the number of messages, a noticeable increase in packets sent, harmful entries that are recognized at ports, and

then the program detects then it directs the task to another tool to blocks these exploits. Preventing DDoS attacks in this stage be effective using applications that has algorithms and web services execute prohibition successfully. We found a solution implemented to applied this idea in Georgia Institute of Technology. They proposed – an architecture to make the edge defensing as the first line against IoT-DDoS, they called it "ShadowNet" and it achieves its purposes in the attack defense [1].

- Blokchain Defense [12]:

The blockchain mechanism used as a modern defense method to protect IoT devices, as organized records are kept in the blockchain, IoT devices are connected to servers in a sequence. Launched applications for IoT devices built into this blockchain, with the status logged each time an interaction occurs between the server and IoT device.

When IoT devices are major buildings and cities, it would be better to monitor them and protect them using blockchain.

III. Research Gap:

Now, The question that comes to mind Why do IoT devices easily fall into this attack? And what IoT devices are most vulnerable? and What vulnerabilities are IoT devices?

The reason comes from our lack of interest in make safe simple IoT devices. We only care about protecting precious devices, but cheap devices as (web cameras, smart TVs) neglect the protection aspect.

IV. Recommend Solution:

From the above, after we have studied these researches, and we found the most effective techniques for detecting and preventing attack, we have come up with a proposed model that integrates the best technologies from our perspective as shown in "Fig4", which provides us with a reasonable as well as accurate method.

We suggest providing a model for detecting attacks. Preventing distributed service in IoT devices. Based on the initial inspection, it monitors internal traffic to the network using Middleware SDN. When it detects a suspicious traffic, it directs the packet to Honeypots that isolated from the main server of IoT devices systems. Here we want to suggest using machine learning to measure The size of the package and the amount of traffic, and keeping it in the records for future use in the comparison. Finally, it will prevent the attack using the network-edge preventing application.

After researching and studying many mechanisms to defend IoT devices against distributed denial of service attacks, we found learning machine algorithms to be the most useful way because they give the most accurate results in traffic control in IoT networks.

We would really like to test these algorithms on the machine and use the Internet service provider for these devices, to discover the difference between normal traffic and record these numbers. As the machine is put under a real attack test, we can see the results in numbers and network behavior. Of course, we assume that testing will greatly enrich this research. However, we have just introduced the newly available protocols to gain sufficient awareness of the use of the Internet of Things and the prevention of its vulnerabilities.

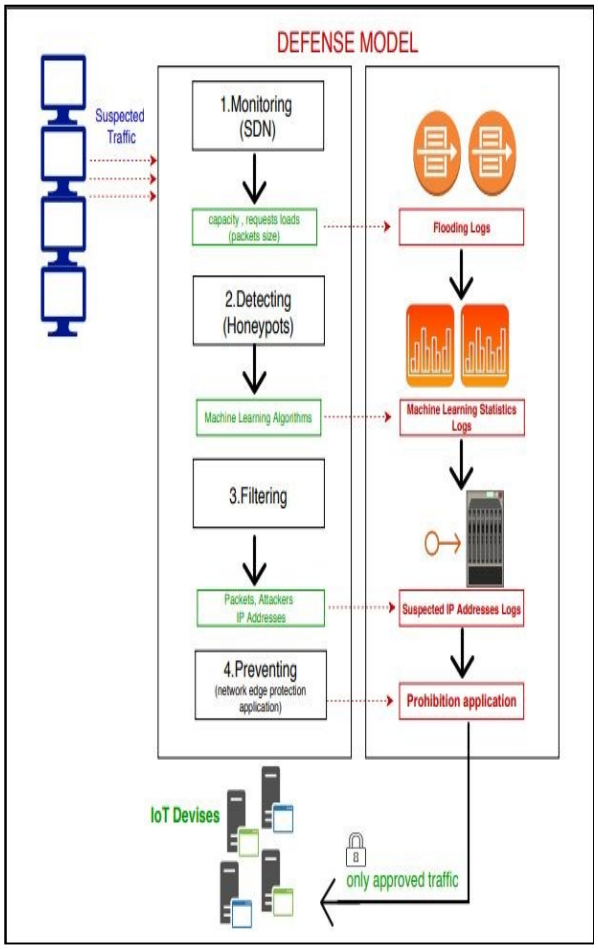

Figure 4. Defense Model of DDoS attack on IoT Devices.

update in the currently, so the issue of security is very important and preventing DDoS attacks is difficult. So in this paper, we talk about some types of this attack and how we can reduce it. The IoT devices must be securing.

References

1. Bhardwaj, K., J.C. Miranda, and A. Gavrilovska. *Towards IoT-DDoS prevention using edge computing*. in *{USENIX} Workshop on Hot Topics in Edge Computing (HotEdge 18)*. 2018.
2. Vishwakarma, R. and A.K. Jain, *A survey of DDoS attacking techniques and defence mechanisms in the IoT network.* Telecommunication Systems, 2019: p. 1-23.
3. Rahman, R.A. and B. Shah. *Security analysis of IoT protocols: A focus in CoAP*. in *2016 3rd MEC international conference on big data and smart city (ICBDSC)*. 2016. IEEE.

4. Mirkovic, J. and P. Reiher, *A taxonomy of DDoS attack and DDoS defense mechanisms.* ACM SIGCOMM Computer Communication Review, 2004. **34**(2): p. 39-53.

5. *What is a DDoS Attack?* 2019; Available from: www.cloudflare.com/learning/ddos/what-is-a-ddos-attack.

6. Sonar, K. and H. Upadhyay, *A survey: DDOS attack on Internet of Things.* International Journal of Engineering Research and Development, 2014. **10**(11): p. 58-63.

7. Pajila, P.B. and E.G. Julie. *Detection of DDoS Attack Using SDN in IoT: A Survey*. in *Intelligent Communication Technologies and Virtual Mobile Networks*. 2019. Springer.

8. Ahmed, M.E. and H. Kim. *DDoS attack mitigation in Internet of Things using software defined networking*. in *2017 IEEE Third International Conference on Big Data Computing Service and Applications (BigDataService)*. 2017. IEEE.

9. Upreti, N., *DDoS Attack and Mitigation.* 2019.

10. Anirudh, M., S.A. Thileeban, and D.J. Nallathambi. *Use of honeypots for mitigating DoS attacks targeted on IoT networks*. in *2017 International Conference on Computer, Communication and Signal Processing (ICCCSP)*. 2017. IEEE.

11. Doshi, R., N. Apthorpe, and N. Feamster. *Machine learning ddos detection for consumer internet of things devices*. in *2018 IEEE Security and Privacy Workshops (SPW)*. 2018. IEEE.

12. Minoli, D. and B. Occhiogrosso, *Blockchain mechanisms for IoT security.* Internet of Things, 2018. **1**: p. 1-13.