International Journal of Circuit, Computing and Networking

E-ISSN: 2707-5931
P-ISSN: 2707-5923
IJCCN 2022; 3(1): 33-42
Received: 17-02-2022
Accepted: 10-04-2022

DDOS attack on IOT devices

Amit, Akshaya Dhingra, Anil Sangwan and Vikas Sindhu

Amit
Electronics & Comm. Engineering UIET, Maharshi Dayanand University, Rohtak, Haryana, India

Akshaya Dhingra
Electronics & Comm. Engineering UIET, Maharshi Dayanand University, Rohtak, Haryana, India

Anil Sangwan
Electronics & Comm. Engineering UIET, Maharshi Dayanand University, Rohtak, Haryana, India

Vikas Sindhu
Electronics & Comm. Engineering UIET, Maharshi Dayanand University, Rohtak, Haryana, India

Corresponding Author:
Amit
Electronics & Comm. Engineering UIET, Maharshi Dayanand University, Rohtak, Haryana, India

DOI: https://doi.org/10.33545/27075923.2022.v3.i1a.41

Abstract

The Internet of Things (IoT) is a way of connecting everyday objects to the internet to make life easier for everyone. The need for (IoT) in our daily lives keeps this industry growing at an ever-increasing rate. As a result, anything linked to the internet would be vulnerable to hacking [1]. As the demand for (IoT) devices develops, so does the potential for malevolent usage. One of the most prevalent IoT violations is a Distributed Denial of Service (DDoS) assault, and we'll look at how it affects these devices in this article to help us better manage our use and understand the need of protecting them against DDoS attacks.

Keywords: Component, IoT devices, DDoS attacks, networks defense, IoT protocold, cyber security

Introduction

The Internet of Things has faced a number of challenges since its inception because of security concerns. Hardware, software, operating systems, and networks all have vulnerabilities that may be exploited. These devices and systems have been successfully attacked by hackers to get access to resources, damage these equipment, and prohibit legitimate users from using them. When it comes to a DDoS assault on IoT devices, we'll examine the mechanism that enables this attack, as well as the best methods for defending our devices from DDoS attacks.

Literature review

Every electronic device (such as sensors and actuators) has its own unique place in the internet of things because of this. These gadgets can be managed from anywhere over the internet [7]. The three-layer design described by researchers is the most fundamental of the IoT architectures [8]. This design may be seen in Figure 1. The sensors and hardware at the perception layer are chosen according to the product's requirements and are responsible for gathering data about the world around it. The network layer serves as a bridge between the physical and logical layers of the OSI model. Last but not least, end users engage with the application layer, which offers them services tailored to their individual needs as an end user.

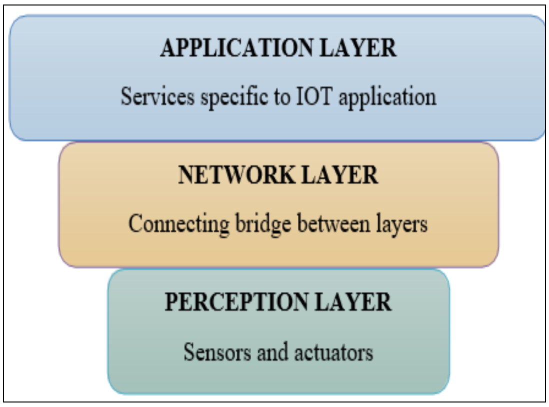

APPLICATION LAYER
Services specific to IOT application
NETWORK LAYER
Connecting bridge between layers
PERCEPTION LAYER
Sensors and actuators

Fig 1: The three IoT layer architecture

The major role of the network layer is to transfer data between the network's various nodes. A wired or wireless medium is used to transmit this information [9]. Additionally, procedures must be followed in order for this process to take place. It is easy to attack the network layer because it serves as a link between the perception and application levels. It is true that the majority of DoS assaults take place at the network level. There are a variety of ways in which these assaults might drain the layer's resources or disrupt the flow of traffic.

Extensive background

▪ 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.

1) 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",

- 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)

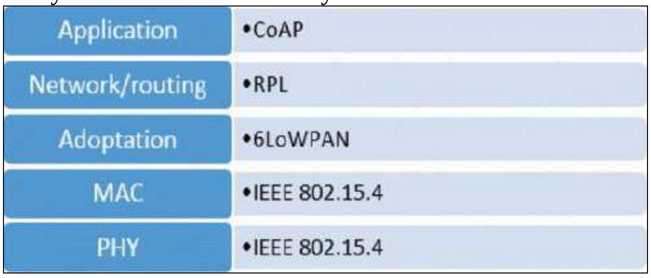
- Network layer using IPv6.
- Provides confidentiality and integrity of the message.

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.



Application	•CoAP
Network/routing	•RPL
Adoptation	•6LoWPAN
MAC	•IEEE 802.15.4
PHY	•IEEE 802.15.4

Fig 2: IoT Protocol

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.

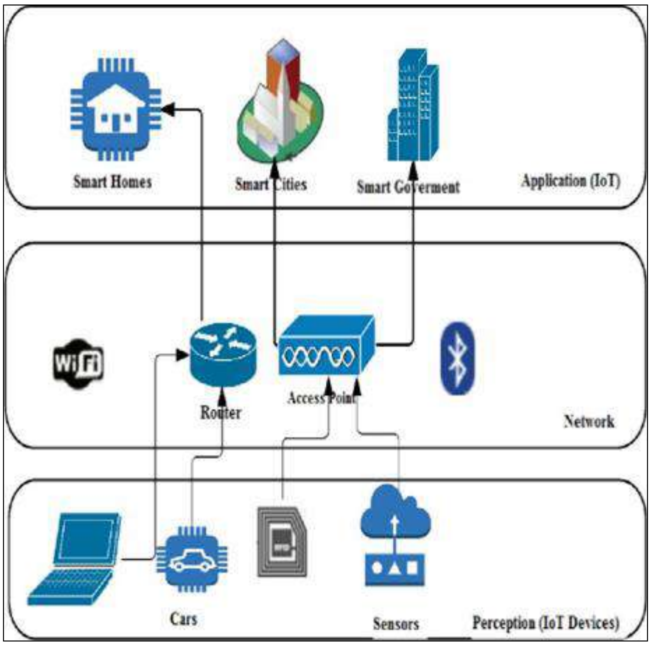


Fig 3: Internet of Things Architecture

▪ 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.

▪ 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".

- 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.

Example of DDoS Attack on IoT Devices [6]

Because the Internet of Things IoT devices, connected to

- 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 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.

Current Trends

DoS types

DoS attacks have many different types and methods for locking up a targeted server, which may be an IoT device, and it is essential to understand each type in order to mitigate and prevent them. Various kinds of DoS attacks might also occur for IoT networks such as the Smurf attack and the SYN flood attack [12].

A Smurf attack uses Internet Control Message Protocol (ICMP) requests for deluging the targeted server through a spoof Internet Protocol (IP) address. The ICMP's purpose is to provide the sender with the status of the sending requests, whether they are reaching the destination or not. ICMP is used by network devices such as the router. The working principle of a Smurf attack is as follows: the attacker creates a spoofed packet by setting its source as the IP address of the target server, and it is sent to an IP broadcast address of a router. Then, the router sends requests to host devices inside the network that respond by sending ICMP packets to the spoofed address of the target. Consequently, the target server will be overloaded with many requests [13].

On the other hand, the SYN flood is considered as a half-open attack because the attacker never completes the connection after requesting the server. Therefore, it aims to consume all available server resources. This attack works by taking advantage of the handshake process of a Transmission Control Protocol (TCP) connection. The TCP works synchronously with the IP to maintain the order of data between sender and receiver. In the handshake, the receiver receives an SYN packet from the sender to initialize the connection. It responds by sending acknowledgment (ACK), and then receives ACK again from the sender. In the SYN flood attack, the attacker will receive ACK from the server after sending a spoofed packet without replying with a final ACK. The attacker will continue sending SYN packets until all the server's available ports are exploited [13]. According to [14], the highest occurring type of DoS attack is the SYN flood threat, and the majority (85%) of DoS attacks happen using TCP protocol.

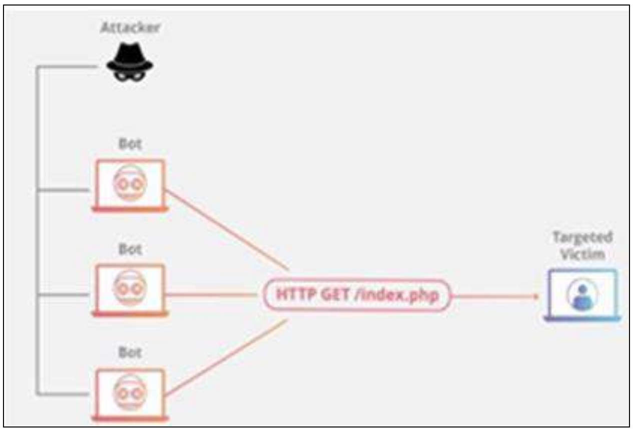


Fig 4: DDoS attack work

The impact of DoS attacks

DoS is one of the most significant and severe attacks from the starting of the digital era. Since the beginning of IoT, DoS exposed huge vulnerabilities of IoT systems. Many sensitive and critical IoT environments could be affected by this attack since the IoT system requires a high level of reliability. The DoS attack affects the whole network by preventing the accessibility of the server or any IoT components, therefore violating one of the essential components of cybersecurity: the availability. One of the hackers' aims is to compromise the availability since it does not require administrative privilege compared to compromising the confidentiality and integrity components for getting and modifying confidential information. DoS has a more harmful effect on high profile organizations such as banks and governments, leading to considerable losses in finances and time.

Lohachab and Karambir [15] demonstrate many impacts and exploited-IoT properties based on different distributed denial- of-service (DDoS) types. For instance, DDoS over the ZigBee network showed a low awareness of security problems with limited resource devices. It resulted in the manipulation of privileged nodes. Another example is flooding attacks. The specific IoT property exploited is a collection of malicious connected devices and network congestion in addition to resource consumption produced as impacts. Furthermore, the protocol attack type used the vulnerability features in IoT protocols, leading to unexpected and abrupt protocol functionality.

As the number of connected devices increases, such as printers, fridges, sensors, and routers with limited security capabilities, attackers would take advantage of the weaknesses of those devices to affect the whole IoT network. Such devices play a significant role in different industries and have crucial impacts on many people's lives—for instance, healthcare monitoring devices and control valves of power plants.

Organizations and enterprises must possess an awareness regarding DoS attacks and their impact on different aspects. Therefore, they should implement robust defense methods and develop solutions against those attacks as well as consider cybersecurity strategy as a priority in their policies. Furthermore, the wireless traffic of the IoT system should be monitored and analyzed periodically to detect and prevent abnormal behavior. Implementing a comprehensive authentication mechanism, such as controlling the received packets and using full headers, could also strengthen the network communication protocol. Another crucial point is the high importance of choosing a robust Internet Service Provider (ISP). ISPs must provide sufficient DoS defense mechanisms to protect their enterprise customers from downtime, therefore minimizing the risk of affecting clients' IoT systems and earning a higher level of trust from them [16].

Enterprises should outline ethical IoT foundations and frameworks while designing their systems and have the responsibility of delivering an IoT-based solution that satisfies the ethics. Businesses that provide IoT products must maintain an ethical culture during production while ensuring high-quality services that deploy a high level of security, and, at the least, provide a backup plan in case of an attack. Such as providing another way of accessing data instead of the service going offline completely.

Examples

Smart homes utilize IoT devices such as sensors, cameras, and appliances to make people's lives easier. Sensors can read the house's temperature, monitor air smoke, and even monitor a baby's health. Moreover, sensors and cameras can be used to monitor a home's entry points and alert the owners in case there was a breach. The devices in an IoT smart home communicate by using IP addresses, and a gateway achieves the management of these devices. If a DoS attack targets the gateway, all the devices become jammed and are unable to perform their functions [17].

IoT has granted the industry the opportunity to perform remote management of their services that can be realized from desktops, servers, or point-of-sale systems. Remote management is applied in industries such as retail stores, factories, and healthcare units. The management of a package in transit, the monitoring of a patient's health, and the tracking of a truck's movement are examples of remote management. All of these elements are prone to DoS attacks where the eavesdropper can spam the server with false data causing jamming and blocking to the legitimate users, which leads to tremendous losses for the organization [18]. In 2016, A Mirai botnet attack was launched on IoT devices by perpetrating them, jamming their servers, and causing a traffic overload. This attack caused damage to popular websites like Netflix, Reddit, and Twitter [19].

In the medical applications of IoT, personal medical devices can be used to report the health status of patients and their medical reports. A DoS attack can gain access to the communication channel that the IoT system uses to utilize its resources and drain them, making the system shut down. IoT based health sensors can report medical data to a cloud via a channel or middleware. This middleware can be breached by a DoS attack making the data transmission delayed or indefinitely terminated [17].

1.1 Current Proposed Solutions

Due to the broad range of IoT applications and services, it is difficult to provide one distinct solution that protects all IoT systems. In this section, three different types of DoS attack mitigation and prevention methods are discussed.

A graph-based method can detect DoS attacks in smart homes. In the graph technique, nodes represent the connected devices, and edges represent the communication between these devices. A DoS attack may shut down one device, and yet, the whole system may appear as if it is fully functioning. The Novel Graph-Based Outliner Detection in Internet of Things (GODIT) claims to analyze each entity (node) in the IoT network and study its performance with respect to the whole system. The GODIT approach requires only the source IP and destination IP to create the graph of the network's flow of data/traffic, which makes the GODIT efficient compared to other DoS detection methods that require more elements such as protocols and the packet size [20].

A Honeypot system mimics the behavior and features of the targeted main server and acts as s decoy. The decoy requires three components to operate: a computer, an application program, and some specific data. The DoS attack is forwarded to this decoy protecting the intended target server. The protection is achieved by tracking the attackers and tracing their activities to further study and analyze them to prevent future attacks [11].

Kajwadkar and Jain [21] proposed a novel solution to detect DoS attacks that target constrained devices. The detection occurs at an early stage at the Border Router node that guarantees the network devices in any IoT network will be unharmed. The detection method consists of two stages: the primary stage and secondary stage. In the primary stage, the source IP and packet size are checked, and the algorithm decides whether the source is a confirmed threat or suspicious. In the secondary stage, the legitimacy of the suspicious input is verified.

Market Strategy

As IoT technologies advance, companies are taking the initiative in developing various solutions and tools to help users have a better, safer experience in addition to forming dynamic, productive teams to develop these innovations in IoT. Examples of such innovations are presented.

Extreme Networks applies the BGP (Border Gateway Protocol) Flowspec (Flow Specification) Route Reflector feature to mitigate DoS attacks. The BGP is deployed on routers to monitor and analyze the flow of data traffic between the end devices and the internet. The authenticity of the data traffic is verified by comparing its parameters such as the source, destination, and L4 with a specific pre-known flow. The flow (data packets) of the DoS attack can be redirected from the victim host to another node to be dropped and flushed [22, 23].

VDOO offers its customers a customizable user experience where the IoT devices can be protected depending on their architecture and requirements. The VDDO ERA agent's firmware binary file is tailored using the Vision, VDDO's analysis platform to analyze and study the desired device to discover its vulnerabilities and protect devices from threats. The VDOO agent is automatically configured for the device. In addition, it provides run-time protection that does not compromise the device's resources and functions [24].

Simulation Results

On the basis of the analysis of statistical data we assess the main indicators of dependability and built a graph shown in Fig. 5-10. As an example, we give graphical dependencies for different technical states of the server. We constructed the dependence of the system availability function (we denote it AC) from the transitions rates to different states (λij, αij, γij, where $i = \overline{\overline{1,22}}$, $j = \overline{\overline{1,22}}$), which depend on events occurrence time. Figures 5-10 shows the changing of availability function AC from changing the transitions rates from one state to another in the Markov's model. The analysis of the Markov's model simulation results shows decreases the value of SBC availability function AC with increase of: - the transition rate λ218 from an active-power mode of the server 2 to a state of the server fail 18 (fig. 9),

- the transition rate λ1317 from active-power mode of the router 13 to a state of the router failure 17 (fig. 5), - the transition rate λ26 from server's active-power mode 2 to a state of the server failure 6 and the transition rate λ36 from server's low-power mode 3 to a state of the server failure 6 (fig. 6, fig.7).

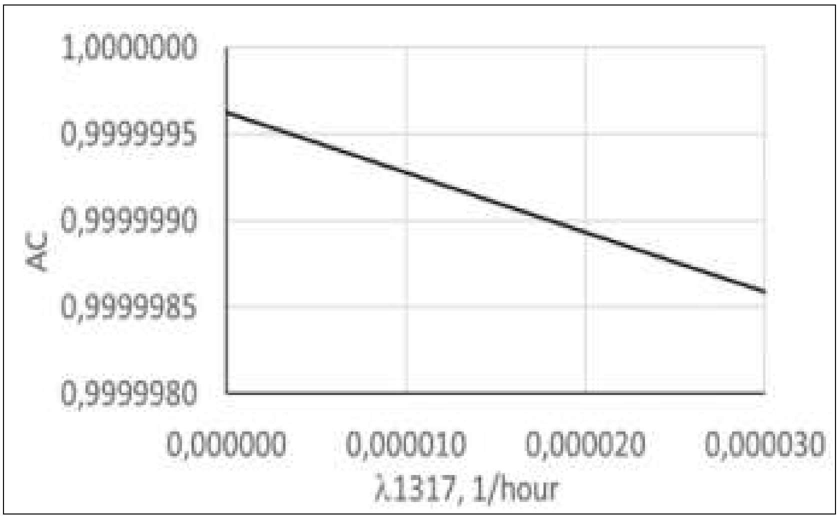


Fig 5: Graph of dependence of SBC AC on the transition rate λ1317 from active power state of the router 13 to a state of the router failure 17

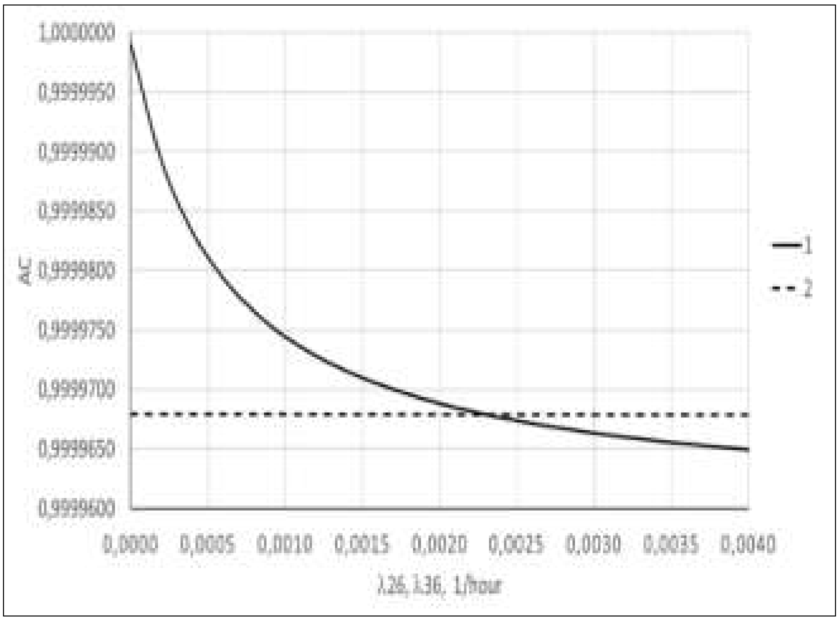


Fig 6: Graph of dependence of SBC AC on the transition rate λ26 from active power state of the server 2 to a state of the server failure 6 and the transition rate λ36 from server's low-power mode 3 to a state of the server failure 6 if γ12=30 1/hour; µ61=0,02083 1/hour; µ67=60 1/hour; µ71=20 1/hour

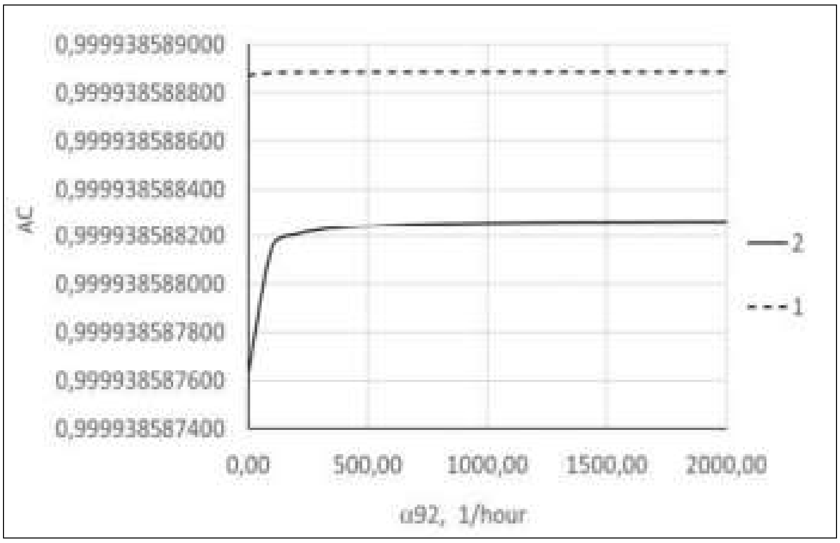


Fig 7: Graph of dependence of SBC AC on the transition rate α92 from the state of successful DDoS-attack on the server after the firewall failure 9 to state of active-power state of the server 2

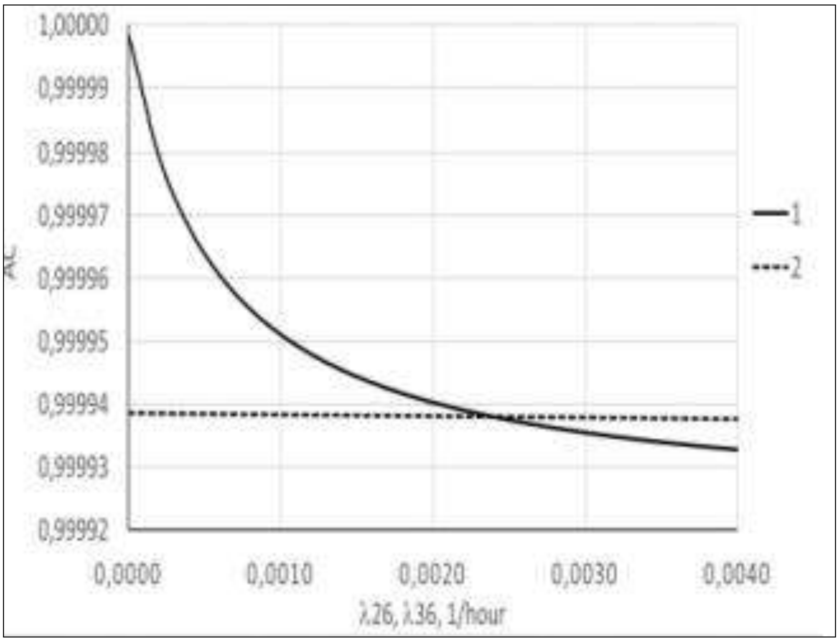


Fig 8: Graph of dependence of SBC AC on the transition rate λ26 from active power state of the server 2 to a state of the server failure 6 and the transition rate λ36 from server's low-power mode 3 to a state of the server failure 6 if γ12=100000 1/hour; μ61=20 1/hour; μ67=1000 1/hour; μ71=50 1/hour

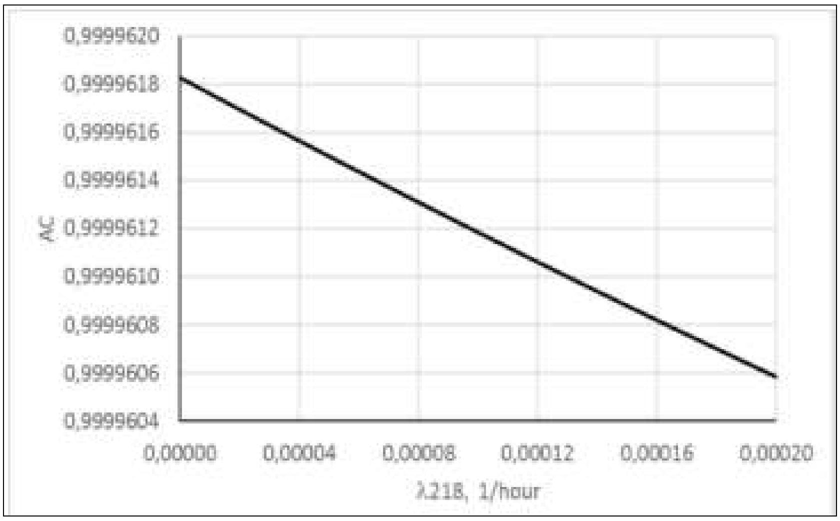


Fig 9: Graph of dependence of SBC AC on the transition rate λ218 from active power state of the server 2 to a state of the server fail 18

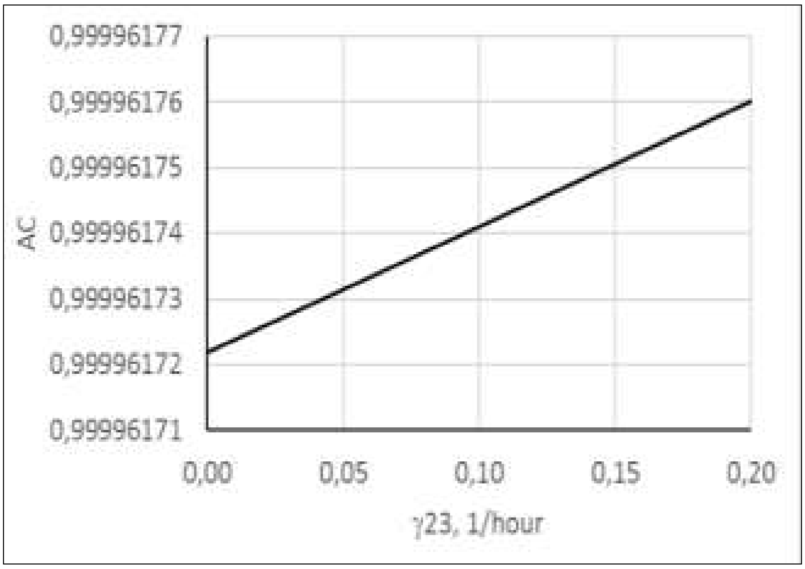


Fig 10: Graph of dependence of SBC AC on transition rate γ23 from active-power state of the server 2 to a state of the low power mode of the server 3

Increase the transition rate from a good state of a server with full power consumption 2 to a server failure state 6 (λ26); from a good state of a server with a reduced power consumption 3, to the server's failure state 6 (λ36) results to AC decrease. With an increase of the transition rate from a good state 1 to a state with full power consumption 2 (γ12), increase the nominal value of AC(t). Moreover, at a high intensity of the transition from the defective state of the server 6 to the working state 1 (μ61), and also to the reconfiguration state 7 (μ67), a smoother change in the availability function is observed than values of μ61, μ67 are low. Moreover, at a high transition rate from the server failure state 6 to the working state 1 (μ61), and also to the reconfiguration state 7 (μ67), a smoother change in the availability function is observed than at low values of μ61, μ67. With the transitions rates γ12=30 1/hour; μ61=0,02083 1/hour; μ67=60 1/hour; μ71=20 1/hour (fig. 9) – the value of AC with λ26=0,004 1/hour is about equal to 0,9999340. If γ12=100000 1/hour; μ61=20 1/hour; μ67=1000 1/hour; μ71=50 1/hour (fig. 10) availability function value with λ26=0,004 1/hour is equal to 0,9999650. Therefore, it is necessary to choose such values of SBC parameters at which the availability factor of the proposed system for any changes in parameters taking into account the power consumption modes and under states of DOS and DDoS attacks will not change significantly. Reducing the availability function when increasing the transition rate from a good state with a high power consumption of the server into a software fail mode occurs due to the impact of external influences (Dos- and DDoS-attacks), and because of internal causes associated with defects in the software and/or hardware of the server (fig. 6). The initial value of the AC is less than 1 when the transition rate from state 9 to state 2 (α92) changes (by the Dos- and DDos-attacks influence on the state of the server with high power consumption if there is a vulnerability in the server firewall), because the AC is influenced both by external influences (attack), and internal causes (defects of software and/or hardware). With the increase in the attack flow to the server through the firewall vulnerability, it is perceived as a simple increase in the flow of data to the server, which leads to the server's transition into a good state of high energy consumption. With a further increase in α92, the change in AC ceases. Fig. 3 shows how the AC varies depending on α92 for different values of the transition rate of the system from good state 1 to the vulnerability state of the server firewall 9. Analysis of the dependences for λ19 = 0.000001 1/hour (line 1) and λ19 = 0.001 1/hour (line 2) showed that an increase in the value of λ19 leads to a decrease in the AC. Besides, increasing of the transition rate from active-power mode of the server to a state of the low-power mode of the server γ23 (fig. 10) insignificantly increase the AC function. Behavior of the availability function AC (γ23) (fig. 10) is justified by the fact that when switching from an active mode of operation of a server with full power consumption to a low power consumption mode, the AC increases depending on the transition rate (γ23) by reducing the load on the power supply equipment increases its availability. Under the influence of DDoS attacks, the server, which is in one of the energysaving modes, will switch to the mode of increased power consumption. The practical significance of the results is the following. They allow to assess the availability factor and to develop recommendations for the design SBC for reduce the vulnerability of the system from DoS- of DDoS-attacks, as well as reducing SBC energy consumption.

Future Trends

As organizations and enterprises improve their security policies and significantly increase their awareness and protection methods against denial-of-service attacks, attackers continue to adapt to these security improvements and respond by reinforcing and enhancing their attack methods.

One of the challenges associated with deploying different protection mechanisms proposed by cyber security experts is the architecture of the current IoT system. Such as open IoT devices, resource-constrained devices, weak networking protocols, and poor quality of hardware components. The opportunity of improving the security of the network by implementing the proposed solution of changing the packets authentication technique is also bounded by difficulties. First is an unsupported lightweight encryption algorithm by standard cryptographic libraries of embedded hardware.

Second is the chance of increasing the overhead of messages due to the addition of required information to the packets for the authentication method. Despite many proposed defending mechanisms for securing the hardware of devices, unfortunately, it could increase the power consumption and the chip size of those devices. The resource limitations of IoT devices increase the challenges of implementing effective solutions [25]. However, the continuous improvement of the IoT devices and networking architecture will promise more securing IoT systems even for critical implementation.

Eaper

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.

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.

- 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.

- **Defend DDoS Attack on IoT Devices classification**
- **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**

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.

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.

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 KD Tree 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 block chain.

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.

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.

Conclusion

The IoT is rapidly developing and becoming a major 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.

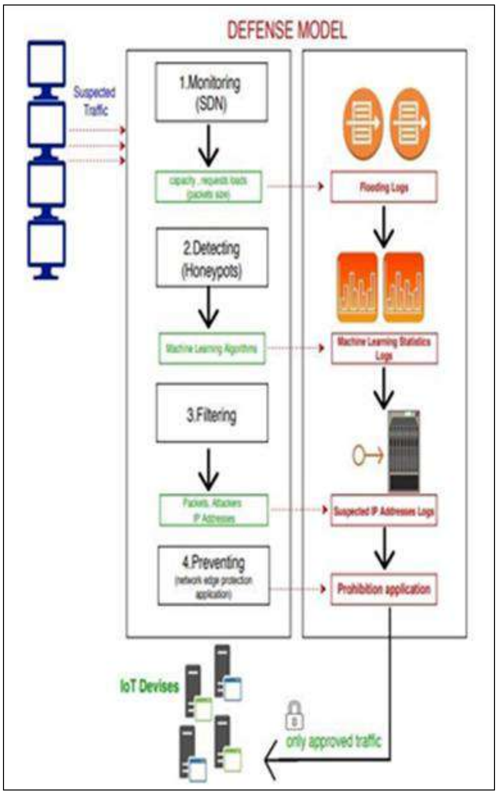

DEFENSE MODEL
Suspected Traffic
1.Monitoring (SDN)
capacity , requests loads (packets size)
Flooding Logs
2.Detecting (Honeypots)
Machine Learning Algorithms
Machine Learning Statistics Logs
3.Filtering
Packets, Attackers IP Addresses
Suspected IP Addresses Logs
4.Preventing (network edge protection application)
Prohibition application
IoT Devises
only approved traffic

Fig 11: Defense Model of DDoS attack on IoT Devices.

References

1. Bhardwaj K, Miranda JC, Gavrilovska A. Towards IoT-DDoS prevention using edge computing. in {USENIX} Workshop on Hot Topics in Edge Computing (HotEdge 18), 2018.
2. Vishwakarma R, Jain AK. A survey of DDoS attacking techniques and defence mechanisms in the IoT network. Telecommunication Systems, 2019, 1-23.
3. Rahman RA, Shah B. Security analysis of IoT protocols: A focus in CoAP. In 2016 3rd MEC international conference on big data and smart city (ICBDSC). IEEE, 2016.
4. Mirkovic J, Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms. ACM Sigcomm Computer Communication Review. 2004;34(2):39-53.
5. Sonar K, Upadhyay H. A survey: DDOS attack on Internet of Things. International Journal of Engineering Research and Development. 2014;10(11):58-63.
6. Pajila PB, Julie EG. Detection of DDoS Attack Using SDN in IoT: A Survey. In Intelligent Communication Technologies and Virtual Mobile Networks. Springer, 2019.
7. Ahmed ME, Kim H. DDoS attack mitigation in Internet of Things using software defined networking in 2017 IEEE Third International Conference on Big Data Computing Service and Applications (Big Data

Service). IEEE, 2017.

8. Upreti N. DDoS Attack and Mitigation, 2019.
9. Anirudh M, Thileeban SA, Nallathambi DJ. Use of honeypots for mitigating DoS attacks targeted on IoT networks in 2017 International Conference on Computer, Communication and Signal Processing (ICCCSP). IEEE, 2017.
10. Doshi R, Apthorpe N, Feamster N. Machine learning ddos detection for consumer internet of things devices. In 2018 IEEE Security and Privacy Workshops (SPW). IEEE, 2018.
11. Minoli D, Occhiogrosso B. Blockchain mechanisms for IoT security. Internet of Things. 2018;1:1-13.