International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
DOI: https://doi.org/10.17762/ijritcc.v11i4.6390
***Article Received**: 02 February 2023 **Revised**: 04 March 2023 **Accepted**: 10 March 2023*

Common Mechanism for Detecting Multiple DDoS Attacks

Kavita S. Kumavat[1], Joanne Gomes[2]
[1]Ph.D. Scholar in Computer Engineering dept., St. Francis Institute of Technology
Mumbai, India
Assistant Professor in Computer Engg. Dept., Vishwakarma University
Pune, India
kavita.kumavat@vupune.ac.in
[2]Information Technology Department,
St. Francis Institute of Technology
Mumbai, India
jgomes@sfit.ac.in

Abstract— An important principle of an internet-based system is information security. Information security is a very important aspect of distributed systems and IoT (Internet of Things) based wireless systems. The attack which is more harmful to the distributed system and IoT-based wireless system is a DDoS (Distributed Denial of Service) attack since in this attack, an attacker can stop the work of all other connected devices or users to the network. For securing distributed applications, various intrusion detection mechanisms are used. But most existing mechanisms are only concentrated on one kind of DDoS attack. This paper focuses on the basic architecture of IoT systems and an overview of single intrusion detection systems. This paper presents a single detection method for different DDoS attacks on distributed systems with an IoT interface. In the future, the system will provide support for detecting and preventing different DDoS attacks in IoT-based systems.

Keywords- Attacks, DDoS, Detection, Internet of Things (IoT), Security, Threats.

I. INTRODUCTION

In an IoT-based system, objects connected to each other using different smart devices, actuators, and sensors are referred to as "things" connected using the internet in a pervasive (anything anywhere at any time) manner. An IoT device has a tracking capability for the location privacy of users. IoT-based systems are becoming ubiquitous and pervasive in nature. Hence cyber-attacks may damage the services in different ways.

In IoT-based devices, privacy protection is the main issue. DDoS (Distributed Denial of Service) attack is an injurious attack in IoT-based systems. In a DDoS attack, the attacker attacks different intermediate zombies or legitimate users and then attacks the system or server. The attacker makes the server busy, so legitimate users cannot get service from the server or system.

The goal of the DDoS is to minimize or even crash and shut down, there by it deny the service or the legitimate users from the multiple compromised sources. Mostly the target of the DDoS attacks are a server, website or other network resource, it cause denial of service for users of the targeted sources. For launching large number of DDoS attack botnets are used, because compromised hosts (zombie) are available. Prevention against DDoS attack is the major concept to make our sources to get rid of DDoS attack. If the DDoS attack is not prevented and it will be detected and mitigated DDoS will flood the organization's servers with fake demand and deny the demand from authentic user The goal of the DDoS is to minimize or even crash and shut down, there by it deny the service or the legitimate users from the multiple compromised sources. Mostly the target of the DDoS attacks are a server, website or other network resource, it cause denial of service for users of the targeted sources. For launching large number of DDoS attack botnets are used, because compromised hosts (zombie) are available. Prevention against DDoS attack is the major concept to make our sources to get rid of DDoS attack. If the DDoS attack is not prevented and it will be detected and mitigated DDoS will flood the organization's servers with fake demand and deny the demand from authentic user.

The motive of a DDoS attack is to diminish or even shut down or crash, thereby it rejects the operations or the valid users from many conceded causes. DDoS attacks target network resources, websites, or servers in which services are not provided properly to the user. Basically, Botnets are used for launching a bulky quantity of DDoS attacks. DDoS attack prevention is the main point to make our sources get clear of DDoS attacks. If the DDoS attack is not prevented and it will be detected and mitigated DDoS will flood the organization's servers with fake demand and deny the demand from the authentic user. There are different types of DDoS attacks possible on IoT-based systems

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
DOI: https://doi.org/10.17762/ijritcc.v11i4.6390
***Article Received**: 02 February 2023 **Revised**: 04 March 2023 **Accepted**: 10 March 2023*

like TCP-SYN flood, ICMP Smurf, ICMP Redirect, DNS amplification, Collision, Jamming, and tampering.

In this paper, the authors quantify security risks and design an intrusion detection system to detect different DDoS attacks. The paper shows a detailed overview of the IoT system and implementation detail with the pseudocode of the intrusion detection system.

Before the discussion of different techniques and algorithms available to detect and prevent DDoS attacks on IoT, first, we discuss the basics of IoT systems. IoT system is developed by using devices and services. IoT devices are the hardware components that permit entities to work in the digital world. By using information and communication technology (ICT) different IoT-based devices can communicate with each other. Privacy and data confidentiality are the two major issues in the security of IoT devices. Different attacks are possible on the IoT system through hardware as well as software. Hence, a security mechanism is needed to detect and prevent different types of attacks on the IoT system [1].

For providing complete security to the system, need to study different layers present in IoT architecture. Q. Jing et. Al. defines IoT security architecture in which three layers are present. Three layers are the Application, Transportation, and Perception layer. The perception layer works for object perception, object control, and information collection. The transportation layer can be subdivided into the following layers: the core network, local area, and access network. The application layer is mainly used for resource allocation in selecting, screening, processing, and producing data, supports intelligent computation, and sorts different business services [2].

An IoT system is a better solution for communication and data transportation. But it may cause a dangerous effect if proper security is not provided. On the IoT system, more chances to introduce eavesdropping in an uncertain location. Hence, the system could not able to find an attacker because the location is uncertain [3]. National Cybersecurity and Communication Integration Center published one report on DDoS attacks on different OSI layers. This report contains details regarding layer-wise attacks like layer description, protocol data unit, and potential impact of attack and mitigation options available for attack type [4]. For the detection of an attack, it is important to find out the anatomy of an attack. Normally, the complete attack has been broken down into 12 discrete steps. Attackers use different ways to break the security of the system by continued reconnaissance, downloading pf multiple sets of tools, controlling many locations, compromising authentication credentials, etc. [5]. For understanding the details of an attack, it is important to find out the reason behind the attack. For that system may categorize the attack into different criteria and after that find out the motive of an attacker. So that the attack can be easy to prevent [6]. Despite growing attacks on IoT devices and alerts from safety experts, utmost organizations do not provide satisfactory privacy and security safeguards for their IoT devices. Sogeti High Tech and Capgemini Consulting delivered wide research to recognize the present state of security for IoT devices [7]. The latest and most dangerous attack on the IoT system is the Mirai botnet. In Mirai Botnet, attackers attack multiple nodes at a time. The Mirai botnet, its variants, and imitators' area unit are warning signs to the trade to a better secure net of Things devices or risk exposing the web infrastructure to progressively disruptive distributed denial-of-service attacks [8]. Using multiple ways, DDOS can influence the distributed system through HTTPS, HTTP, UDP, MAC, ICMP, and SYNFLOOD (using TCP) attacks [9]. To detect and prevent different flooding-based DDoS attacks, the mentioned existing system in the paper developed a mechanism that covers the categorization of flooding-based attacks and the classification of present countermeasures of detection, prevention, and reply to the flooding attack.

For detection and prevention of TCP Syn flood attacks existing FireCol [10] system maintains shields, virtual, or rings of protection, everywhere valid/registered customers. The ring is a collection of a set of IPSs that are at the same distance (number of hops) from the customer. Each FireCol IPS instance analyses aggregated traffic within a configurable detection window. The metrics manager computes the frequencies and the entropies of each rule. TCP SYN Flood attack had been outlined [11] in the network. There are 152 detection different methods of attacks that can be enhanced in a direction to make the detection faster and more effective and alarm the security administration department whenever there is an attack or abnormal behaviors in the flow of traffic. ICMP redirection is normally a task held in reserve for non-host nodes in networks or routers. However, with ARP packets, an attacker can generate them with a definite message. ICMP redirection instructs a target to adjust its routing table with an ICMP type of 5 and a code of 0 [12]. Address Translation Redirection Attack (ATRA) [13] assessment with benchmarks presented that ATRA does not make such obvious performance degradation of OS. As long as this restriction of the hardware-based exterior displays remains unsolved, any upcoming progression in their monitoring capability will be ineffective. V. K. Yadav et. al. proposed Distributed Defense approach (DDA) [14] for the detection of ICMP-based attacks. DDA is distributive and filtering is applied at the end router. The authors propose organizations employ remote hosting for their authoritative DNS servers. Organizations demand an upstream filtering mechanism of entirely DNS traffic, mitigating the DDoS attack. To preserve DNS functionality for the organization, the authors suggest and trial a solution to tunnel DNS queries to a remote DNS resolver, such as a remote VM hosted by a cloud provider or ISP. The authors found that we could routinely initiate a remote DNS resolver, initiate the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
DOI: https://doi.org/10.17762/ijritcc.v11i4.6390
***Article Received**: 02 February 2023 **Revised**: 04 March 2023 **Accepted**: 10 March 2023*

tunnel, and forward all local DNS traffic to the remote node in less than 0.67 s, on average. All queries would then have a median additional latency of 16 ms. Accordingly, our approach will allow organizations to weather extremely high-volume DNS amplification attacks with minimal effort [15]. Bandwidth-distributed denial-of-service (BW-DDoS) [16] attacks work relatively insufficient, crude, brute-force mechanisms. However, several known attacks, which aren't commonly used, let attackers launch sophisticated attacks, which are difficult to detect and might considerably amplify attackers' strength. Under Carrier Sense, Multiple Access with Collision Notification (CSMA/CN) [17]-[18], the receiver uses PHY layer information to detect a collision and immediately notifies the transmitter. The collision notification consists of a unique signature, sent on the same channel as the data. Transmitting adaptive camouflage traffic (TACT) [19] is used to combat jamming attacks. TACT reduces the message delay by producing additional traffic i.e. camouflage to balance the network load at the optimum. Experimentations show that TACT can decline the chance that a message is not sent on time in order of magnitude.

Threshold-based Jamming Countermeasure (TJC) [20] method shows different ways of reactive jamming attacks which spots the jamming in the network and protects the network against reactive jamming attacks. The execution of the proposed method in different conditions shows that TJC saves the network in case of a reactive jamming attack with increased traffic and the number of malicious nodes in a network. The paper simulates the TJC by considering realistic scenarios which shows the adaptability of the algorithm in changing traffic interval and mobility among the normal and malicious nodes.

TamperProof [21] was evaluated on several media to large applications demonstrating it to be both effective and efficient. As TamperProof does not require any changes or analysis of server-side source code, it can be deployed in existing proxies and defend any server-side technology or platform. By offering robust protection that treats the server as a black box, TamperProof offers an attractive option to protect web applications from parameter tampering attacks.

Existing Synchrophasor security protocols [22] are very efficient for detecting tampering attacks. It provides efficient computational capabilities and very low verification delays which is essential for the paramount requirement of availability in synchrophasor networks (i.e., information availability at right time). It also supports the real-time operation.

In Table 1 five different tree-based approaches, Enhanced Very Fast Decision Tree (EVFDT) [23], Attack Tree based Intrusion Detection System (ATIDS) [24], Augmented Attack Tree (AAT) [25], Attribute Tree (AT) [26], and Change Aggregation Tree (CAT) [27] are compared as follows-

TABLE I. COMPARISON OF TREE-BASED APPROACHES

Sr. No.	Tree Specification	Parameter	Attacks Covered
1.	EVFDT has used an adaptive tie-breaking threshold for node splitting. A lightweight iterative pruning technique is used to resolve the tree size expansion under extreme noise [23].	classification accuracy, tree size, time, and memory	DDoS attack on the network Traffic
2.	Attack Tree-based IDS (ATIDS) monitors N/W ADtT (Advanced attack tree) specialized for intrusion detection & with uncertainty assessment [24].	Incoming and outgoing network traffic on the edge device with the appropriate configuration	-ICMP Redirect -Smurf Attack
3.	The augmented Attack Tree Based Detection (AATBD) system is used to identify the incidents from the leaf nodes to the root node [25].	Packet Header Data attack signatures	-ICMP, SYN, UDP Flood
4.	An attribute tree is an optimal data mining-based defense cum protection mechanism [26].	identifies and uses candidate packet attributes	-SYN Flood attack (Active N/W attack)
5.	Change Aggregation Tree (CAT) is used DETER testbed to find DDoS attacks [27].	Packet Size	-TCP SYN /UDP/ICMP flooding

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
DOI: https://doi.org/10.17762/ijritcc.v11i4.6390
***Article Received**: 02 February 2023 **Revised**: 04 March 2023 **Accepted**: 10 March 2023*

In this paper, we have studied multiple existing systems concentrated on any one type of attack but we have developed a single method that is able to detect multiple DDoS attacks.

The paper is set in the following manner:

Section II exclusively provides an IoT system overview which contains the IoT system, IoT model, IoT layered architecture, and IoT 3 Tier architecture. Section III explains the implementation of the detection method for DDoS attacks with pseudocode, Section IV concludes the paper.

II. IoT System Overview

This paper focuses on an overview of IoT systems, to understand IoT systems briefly it is important to know IoT system architecture, IoT model, Layered architecture, and the three-tier of risks in detail.

This Section explains the basic structure of an IoT system that provides services to applications, the IoT model which shows how an entity is used by objects to access resources for providing specific services, and IoT layered architecture. To understand IoT-based systems, it is essential to study the architecture shown in the below paper.

A. IoT System

The IoT system in Figure 1 connects hardware to software through the network to serve different applications to the user.

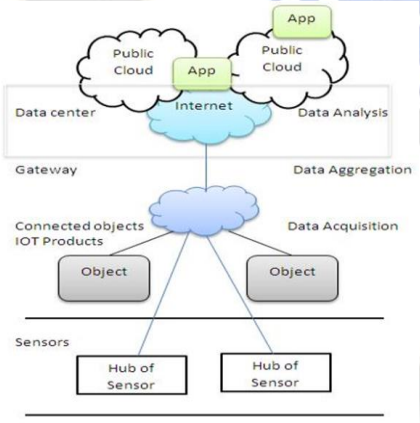


Figure 1. IoT System

Figure 1 shows different sensors connected to a central hub serving multiple services using objects that are connected to the internet or cloud. Connected objects are nothing but IoT products that are used for data acquisition and are connected to the environment or data center using the gateway for data analysis purposes. Data acquisition is used for measuring or converting physical phenomena into an electrical format. Data aggregation is useful for collecting, storing, analyzing, and summarizing information for statistical analysis.

B. IoT Model

It is important to study the IoT model briefly because it gives an idea about the connectivity, association, and access between different devices, entities, resources, and services working combined in an IoT-based system. The IoT model contains different key concepts and their interactions. As shown in Figure 2, an entity is any attribute like an animal, car, human, etc. It is a software thing connected to hardware components called devices by which an entity becomes a part of the digital world. Devices can actuate or sense connectivity to the physical world. An entity is associated with the database using different resources. Services are served using the service provider and service consumer.

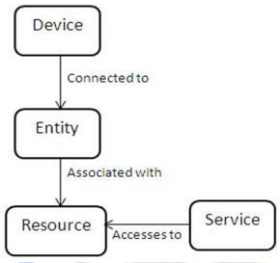


Figure 2. IoT Model.

C. Layered Architecture of IoT

The layered architecture is an important part of IoT based system because it provides a layer-wise comparison between TCP/IP model and with the IoT system. This comparison is needed to understand layer-wise DDoS-based attacks detected on the system. The layered architecture of IoT shown in Figure 3 describes the internal structure, and its working depends on different layers present in the architecture. Here layered architecture is compared with the TCP / IP model for a brief understanding. Figure 3 also shows possible attacks on a particular layer.

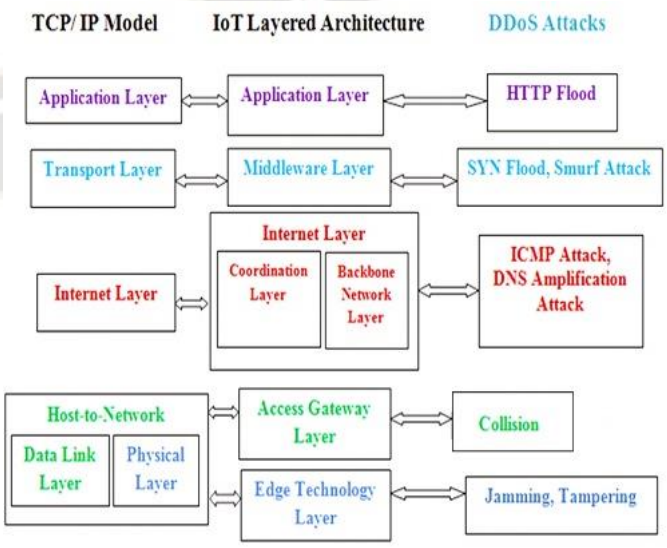


Figure 3. The Layered Architecture of IoT.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
DOI: https://doi.org/10.17762/ijritcc.v11i4.6390
***Article Received**: 02 February 2023 **Revised**: 04 March 2023 **Accepted**: 10 March 2023*

The basic layered structure of IoT contains five layers. Edge Technology Layer also called a Hardware Layer contains embedded system specifications like hardware and software connectivity, sensor network, and different RFID tags. It collects and processes different information which supports communication. Access Gateway Layer provides the functionality of data handling, subscribing, and publishing. It is useful for data access like message routing. The Internet Layer is used for Internet connectivity and online application-based services and processes. The Internet layer is a combination of the backbone network layer and coordination layer. The backbone network layer provides basic internet functionality. Structures of packages are processes and reassembling of different applications in a unified structure takes place in the coordination layer. Middleware Layer has core functionalities like filtering and aggregation of data which is useful for connecting hardware devices, controlling data access, and information discovery. The application Layer delivers services that are served from the middleware layer to the user.

D. Three Tiers of Risks

IoT system has major security issues and there is a risk in developing or handling IoT devices or applications. The three-risk architecture of IoT is shown in Figure 4.
First-tier is related to the additional software and modules or chips that come with preinstalled software. This preinstalled software may be already malicious. It is very difficult to find malware in this tier. Second-tier is related to the connectivity of software and hardware if any of these gets affected then the malware may have a serious effect on the system. Third-tier is related to networking where control and management functions can be directly hacked due to an infected internet connection.

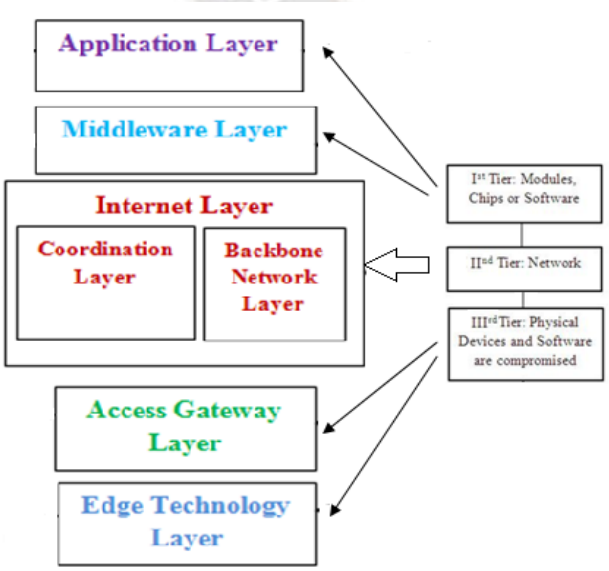


Figure 4. Three-tier Architecture of IoT.

III. Implementation of Detection Method for DDoS Attacks

This paper shows the implementation details regarding the detection of DDoS attacks on distributed systems with an IoT interface.
There are multiple intrusion detection systems available to detect and prevent DDoS attacks. But most of the existing techniques are only able to detect a single attack based on flooding/amplification/ Jamming / Collision / Tampering. Hence there is a need to present a technique that can effectively detect and prevent different types of DDoS attacks with a single approach.
This section presents implementations of TCP SYN flood, ICMP Smurf, ICMP redirect, DNS Jamming, Amplification, Collision, and Tampering-based attacks that are relevant to distribution as well as IoT systems. The detection and prevention technique for these attacks is implemented by a single method using front-end Eclipse and back-end SQL. The proposed intrusion detection system can handle the above-mentioned types of DDoS attacks.

A. TCP SYN Flood Attack

TCP SYN flood also represented by using the half-open connection, is a network-tier attack that continuously bombards a server with connection requests without responding to the respective acknowledgments.

In the proposed system, the IoT application of remote controlling of the Media Player device over the internet. TCP SYN flood attack can be made on this application. Consider one user, acting as an attacker, using the Media Player application as shown in Figure 5(A). An attacker sends the request to the admin to put ‘Media Player ON’, by clicking the ‘ON’ button as shown in Figure 5(B), after which he neither uses it nor sends the request to put it OFF. If at the same time another user wants to access the same Media Player then he finds it unavailable as shown in Figure 5(C). Only when the attacker requests admin to put ‘Media Player OFF’, by clicking the OFF button, then the access to Media Player given to another user.

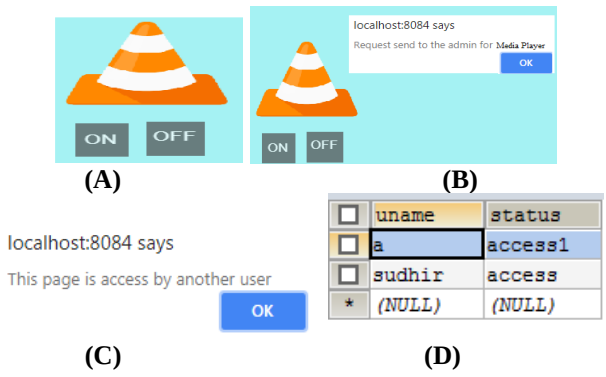


Figure 5. TCP SYN Flood Attack on IoT Application.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
DOI: https://doi.org/10.17762/ijritcc.v11i4.6390
***Article Received**: 02 February 2023 **Revised**: 04 March 2023 **Accepted**: 10 March 2023*

The records of users who are accessing the Media Player application have been stored in the Database as shown in Figure 5(D). It shows that ‘Sudhir’ is an attacker who has access to Media Player and the second user ‘a’ has been denied access. Thus, when the attacker leaves a half-open connection to Media Player, another user cannot access it.

B. ICMP Smurf Attack

In an ICMP smurf attack, an attacker can interrupt the communication and then generate an echo of response.

To illustrate the ICMP Smurf attack on IoT systems here Light-bulb application is shown in Figure 6 (B). In this attack, an attacker can select any valid user IP address as a victim IP address as shown in Figure 6 (A), using that IP address he can take control of the Light application and click on the ON button which will generate echo of the request and will result in Light OFF. If the user clicks a button to put Light OFF it will generate a Light ON response as shown in Figure 6 (C). In this way, the request generates an echo response in the Smurf attack.

(A)

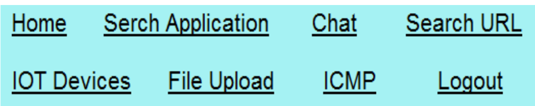
(B) **(C)**

Figure 6. Example: ICMP Smurf Attack.

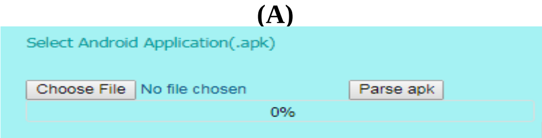
C. ICMP Redirect Attack

In an ICMP redirect attack, the attacker directly attacks the gateway or middleware so that the user and server cannot communicate properly. Hence attackers can able to observe and interrupt communication between user and server as shown in figure 7.

Implementation:



(A)



(B)

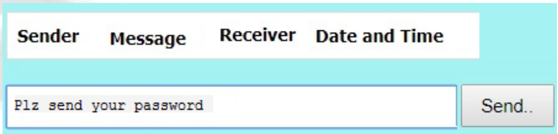
Figure 7. Example: ICMP Redirect Attack.

As shown in Figure 7 (A) when the user clicks on the search URL menu it will redirect the user to the file upload page as in Figure 7 (B).

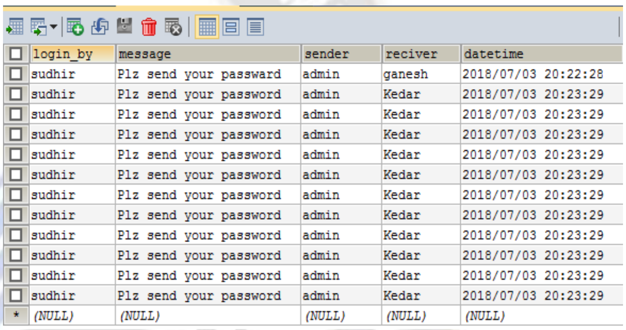
D. DNS Amplification

Implementation:

(A)



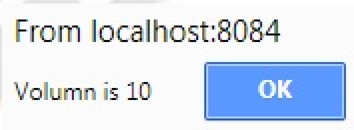
(B)



	login_by	message	sender	reciver	datetime
☐	sudhir	Plz send your passward	admin	ganesh	2018/07/03 20:22:28
☐	sudhir	Plz send your password	admin	Kedar	2018/07/03 20:23:29
☐	sudhir	Plz send your password	admin	Kedar	2018/07/03 20:23:29
☐	sudhir	Plz send your password	admin	Kedar	2018/07/03 20:23:29
☐	sudhir	Plz send your password	admin	Kedar	2018/07/03 20:23:29
☐	sudhir	Plz send your password	admin	Kedar	2018/07/03 20:23:29
☐	sudhir	Plz send your password	admin	Kedar	2018/07/03 20:23:29
☐	sudhir	Plz send your password	admin	Kedar	2018/07/03 20:23:29
☐	sudhir	Plz send your password	admin	Kedar	2018/07/03 20:23:29
☐	sudhir	Plz send your password	admin	Kedar	2018/07/03 20:23:29
☐	sudhir	Plz send your password	admin	Kedar	2018/07/03 20:23:29
☐	sudhir	Plz send your password	admin	Kedar	2018/07/03 20:23:29
*	(NULL)	(NULL)	(NULL)	(NULL)	(NULL)

(C)

(D)



(E)

Figure 8. Example: DNS Amplification Attack.

Implementation of DNS amplification attack uses chat application. In the chat application, the normal user always selects the sender as a self-name but the attacker selects the sender with another user name and sends the message by selecting a particular receiver as shown in Figure 8 (A) and (B). In this attack, multiple copies of a single message are sent to the receiver by clicking one time. As shown in Figure 8 (C)

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
DOI: https://doi.org/10.17762/ijritcc.v11i4.6390
***Article Received**: 02 February 2023 **Revised**: 04 March 2023 **Accepted**: 10 March 2023*

database entries show that 10 times the same message is sent to the receiver. Hence this attack takes up maximum space on the DNS server and limits its capacity of the DNS server.

The IoT application for DNS amplification attack in Figure 8 (D) and (E) shows that when the user clicks on TV volume for increase or decrease volume it will increase or decreases by 10 times on a single click.

E. Jamming Attack

Definition:

A jamming attack is a subset of a DDoS attack in which the attackers prevent other nodes to use the channel.

Explanation:

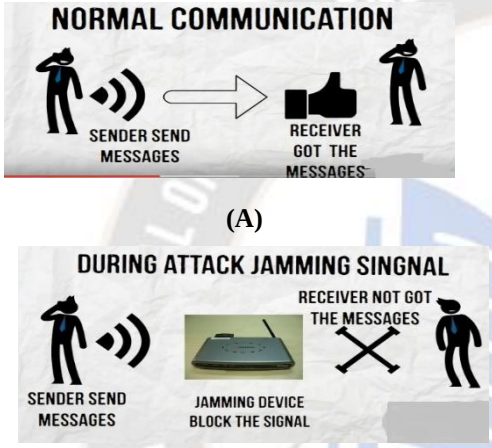


Figure 9. Jamming Attack.

In the usual communication system, the source sends a request and the destination gets a response for that request and communication is successful as shown in Figure 9(A).

But in a jamming attack, the attacker sends multiple requests or a large volume of requests to the server beyond its capacity so that the server is not able to handle it and a jamming attack takes place as shown in Figure 9(B).

Implementation:

Figure 10. Example: Jamming Attack.

The IoT application for jamming attack contains a Light application in which the attacker performs some setting so that if the user clicks on ON then the light is on for one minute and if the user clicks on OFF then the light is OFF for one minute as shown in the figure as shown in figure 10.

Comparison with existing work:

Existing methods provide less accuracy and are only suitable for detecting and preventing collision attacks. The proposed mechanism provides high accuracy and is also useful for finding different DDoS-based attacks.

F. Tampering Attack

Definition:

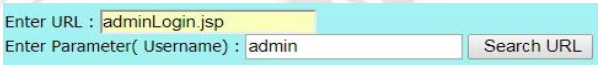
A tampering attack depends on the web in which some parameters of a form field or URL (Uniform Resource Locator) are modified by an attacker or without the permission of that valid user.

Explanation:

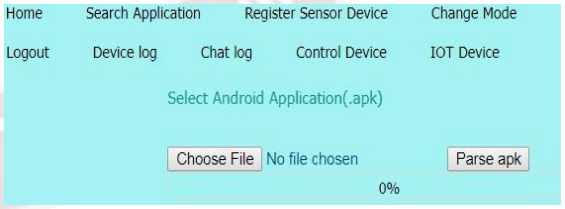
In a URL tampering attack, an attacker may be a normal user who can log in to their own account and just by changing the URL or parameter of the URL can able to access another user account without permission as shown in Figure 11.

Figure 11. Tampering Attack.

Implementation:



(A)



(B)

(C)

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
DOI: https://doi.org/10.17762/ijritcc.v11i4.6390
***Article Received**: 02 February 2023 **Revised**: 04 March 2023 **Accepted**: 10 March 2023*

(D)

Figure 12. Example: Tampering Attack.

IoT application for tampering attacks is implemented on AC. Normal users do login into the system and then click on the search URL menu as shown in Figure 12 (A). By using the admin URL, the user can enter to admin page and gets access to the admin page as shown in Figure 12 (B). In the system, only the admin has the authority to change AC temperature hence users go to IoT devices and access AC as shown in Figure 12 (C). The user will change the temperature of the AC to disturb the system setting as shown in Figure 12 (D). In this way by using a parameter as a URL normal user can get access to the admin page and make damage to the system.

Detection and Prevention Mechanism Code:

The detection and prevention codes for all attacks are given below. Also, the IoT interfacing logic is also mentioned below for reference to how the IoT system will react for particular DDoS attack.

Pseudo Code:

Case I: TCP SYN Flood

```
if (sts.equals("access"))          {  %> <script>
   alert("This page is access by another user");
              window.location="Admin.jsp";  </script>      <%
} else {     System.out.println("in else");
PreparedStatement pst = con.prepareStatement("insert into
tcpsyn (uname,status) values(?,?)");
 pst.setString(1, session.getAttribute("uname").toString());
          pst.setString(2, "access");
         int  i=pst.executeUpdate();
```

IoT Interface Example:

```
If (sts.equals(“access”))
{ alert("This page is access by another user");
\\ media player is accessed by another user
}Else {access (“Media Player”);}
```

The above pseudocode explains the TCP SYN flood attack, in which syn request and ack request are compared. A malicious user cannot send ACK back to the server hence server is not able to provide service to legitimate users.

Case II: ICMP Smurf Attack

```
PreparedStatement pstmt0 = con.prepareStatement("select
status from action where id=1");
 ResultSet rs0 = pstmt0.executeQuery();
while (rs0.next()) {sts = rs0.getString("status");
}      System.out.println("Sts=" + sts);
if (sts.equalsIgnoreCase("No"))
{PreparedStatement pstmt = con.prepareStatement("select ip
from block_ip");
ResultSet rs = pstmt.executeQuery();
while (rs.next()) { String ip1 = rs.getString("ip");
 if(ip.equalsIgnoreCase(ip1))
{   response.sendRedirect("access_denied.jsp");
```

IoT Interface Example:

```
If (enter ip=source ip)
Then ON=Light ON;       OFF=Light OFF;
Else ON=Light OFF;       OFF=Light ON;
```

In ICMP Smurf attack, the eco response is generated for every request.

Case III: ICMP Redirect Attack

```
   if (request.getRemoteHost().equals("0:0:0:0:0:0:0:11")) {
                  then redirect to request page
                              } else {
                          Redirect on wrong page }
                alert ("Attacker try to Redirect Page");
```

IoT Interface Example:

```
If (user request==media player)
 response (TV)
```

In an ICMP redirect attack, the user will redirect randomly to another website.

Case IV: DNS Amplification Attack

Chat application with input as:

```
      Login By, Victim, Receiver, Chatting
      if (request.getRemoteHost().equals ("0:0:0:0:0:0:0:1")) {
      Send message;
            } else {(ip.equalsIgnoreCase(ip1)) {
        response.sendRedirect("access_denied.jsp");
              }
            }
```

IoT Interface Example:

```
      If (request=TV volume increase by 1)
      Response== volume increases by 10
```

In a DNS amplification attack, the attacker amplifies multiple internal devices and by combining send a large amount of request to the DNS server.

Case V: Jamming Attack

If request is send by attacker then request=1,

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
DOI: https://doi.org/10.17762/ijritcc.v11i4.6390
***Article Received**: 02 February 2023 **Revised**: 04 March 2023 **Accepted**: 10 March 2023*

```
 for(int i=0;i<10; i++)
{alert("JAMMING Attack by <%=ip%>");
b1.onclick = function() {b1.style.background = "green";
    alert("Bulb is ON for 1 Min" );
  b2.disabled=true;
    b1.disabled=true;
b2.style.background="";
   setTimeout(function(){b1.disabled = false;},20000);
   setTimeout(function(){b2.disabled = false;},20000);
b2.onclick = function () {
    b2.style.background = "red";
    alert ("Bulb is OFF");
   b1.style.background="";}
```

IoT Interface Example:
If request=attacker to light
then
the bulb on or off for 1 min

In a jamming attack, the attacker sends malicious code or requests so that system will jam for some time.

Case VI: Tampering Attack

```
Enter URL:
<INPUT type="text" name="url"/>
  Enter Parameter (Username):
  <INPUT type="text" name="user"/>
 <input type="submit" value=" Search URL"></input>
Tampattack.jsp
if (request.getRemoteHost().equals("0:0:0:0:0:0:0:11"))
{
            pstmt.setString(2, ip);      }
```

IoT Interface Example:
<<User access==normal user>> || <<user access== admin>>
Access all admin rights

In URL tampering user can change some credentials of the URL to get access to another user page.

IV. Conclusion

Internet-based smart applications are intended to deliver luxury to users. Along with ease, they offer few side effects like various attacks, vulnerabilities, and threats that break down the privacy and confidentiality of users' private information. It is a very serious job to reserve the confidentiality of information in a distributed system. On distributed systems, some attacks cause more impact such as DDoS which is responsible for affecting the working of a system as well as it will affect the connectivity of all nodes to that system's network. Various detection and prevention techniques are available to detect and prevent DDoS attacks, but they do not give assurance to detect and remove all the different reasons for those attacks proficiently. This paper represented a technique that is able to detect and prevent different types of DDoS attacks like Jamming, Tampering, collision, amplification attack, flooding-based attacks (TCP Syn flood), and ICMP-based attacks using a common intrusion detection system.

In the future, this intrusion detection system will support for detection and prevention of other DDoS attacks which is based on application-based IoT systems.

References

[1] M. Abomhara and G. M. Koien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks," Journal of Cyber Security, Vol. 4, pp. 65-88, May 2015

[2] Q. Jing et al., "Security of the Internet of Things: perspectives and challenges," Springer Wireless Netw DOI 10.1007/s11276-014-0761-7, 2014.

[3] Q. Xu et al., "Security enhancement for IoT communications Exposed to Eavesdroppers with Uncertain Locations," IEEE Access, Special section on Internet of Things (IoT) in 5G Wireless Communications, Vol. 4, 2016 .

[4] "DDoS Quick Guide," National Cyber security and Communications Integration Center, Jan 2014.

[5] TrapX Labs - A Division of TrapX Security, Inc, "Anatomy of an Attacks," The Internet of Things (IoT) - The Hidden Danger Exposed, Mar 2017.

[6] "IoT Threat Environment," CISCO, White Paper, 2015.

[7] Capgemini Consulting and Sogeti High Tech, "Securing the Internet of Things Opportunity: Putting Cyber security at the Heart of the IoT," Nov 2014.

[8] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," IEEE Computer, vol. 50, no. 7, pp. 80–84, 2017.

[9] Idris et. al., "HTTP Flood Mitigation Using Gateway Inspection and Second Chance Approach Analysis", International Journal of Cyber-Security and Digital Forensics (IJCSDF), The Society of Digital Information and Wireless Communications (SDIWC), Vol. 6, No. 1, Jan. 2017, pp. 14-22.

[10] J. Francois, I. Aib, and R. Boutaba, "FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks", IEEE/ACM Transactions on Networking, IEEE/ACM, Sept. 2012, 20 (6), pp.1828-1841.

[11] S.H.C. Haris., et. al., "TCP SYN flood detection based on payload analysis", Proc. of 2010 IEEE Student Conference on Research and Development (SCOReD 2010), Putrajaya, Malaysia, Dec 2010, pp. 149-153

[12] Myers, Robbie. "Attacks on TCP/IP Protocols." Last accessed Jan 4, 2016.http://www.utc.edu/center-information-security-assurance/pdfs/course-paper-5620-attacktcpip.pdf.

[13] Daehee Jang et.al., "ATRA: Address Translation Redirection Attack against Hardware-based External Monitors", ACM, Scottsdale, Arizona, USA, CCS'14, November 3–7, 2014.

[14] V. K. Yadav et. al., "DDA: An Approach to Handle DDoS (Ping Flood) Attack",inProc. of International Conference on ICT for

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
DOI: https://doi.org/10.17762/ijritcc.v11i4.6390
***Article Received**: 02 February 2023 **Revised**: 04 March 2023 **Accepted**: 10 March 2023*

Sustainable Development, Advances in Intelligent Systems and Computing, Springer, Singapore, Vol.10, Issue No. 2, Sept. 2016.

[15] D. C. MacFarland et. al., "Characterizing Optimal DNS Amplification Attacks and Effective Mitigation", Springer, Vol. 8, No. 2, Mar. 2015.

[16] M. Geva, A. Herzberg, and Y. Gev, "Bandwidth Distributed Denial of Service: Attacks and Defenses", Article in IEEE Security and Privacy Magazine, Jan. 2013.

[17] S. Sen, R. Choudhary and S. Nelakuditi, "CSMA/CN: Carrier Sense Multiple Access with Collision Notification", proc. In MobiCom'10, ACM, Sept. 2010.

[18] Nicolas Bruneau et. Al., "Stochastic Collision Attack", International IEEE Transactions On Information Forensics And Security, Vol. 12, No. 9, Sept. 2017.

[19] Lu, Zhuo, W. Wang, and C. Wang. "Camouflage Traffic: Minimizing Message Delay for Smart Grid Applications under Jamming." IEEE Transactions on Dependable & Secure Computing, Vol. 12, No.1, Feb. 2015, pp. 31-44.

[20] Sachin D. Babar, Neeli R. Prasad, and Ramjee Prasad, "Activity Modelling and Countermeasures on Jamming Attack", Journal of Cyber Security and Mobility, River Publisher, Vol. 2, No. 1, Apr. 2013.

[21] Nazari Skrupsky et. al., "TamperProof: A Server-Agnostic Defense for parameter Tampering Attacks on Web Applications", Proc. of the Third ACM Conference on Data and Application Security and Privacy (CODASPY'13), San Antonio, Texas, USA, Vol. 7, No. 2, Feb. 18–20, 2013.

[22] M. N. Aman et. al., "Detecting data tampering attacks in synchrophasor network using time hopping", 2016 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), Ljubljana, 2016, pp. 1-6.

[23] R. Latif et al., "EVFDT: An Enhanced Very Fast Decision Tree Algorithm for Detecting Distributed Denial of Service Attack in Cloud-Assisted Wireless Body Area Network", Pub. Hindawi Corporation, Mobile Information Systems (HCMIS), Vol. 2015, Issue 5, Aug. 2015.

[24] J. Wang., "Advanced Attack Tree-Based Intrusion Detection", Pub. In Lough borough University Institutional Repository (LUIR), Leicestershire, UK, Feb 2012.

[25] J. Wang et. al., "Augmented Attack Tree Modeling of Distributed Denial of Services and Tree-Based Attack Detection Method", Proc. in 10th IEEE International Conference on Computer and Information Technology (CIT 2010), Oct. 2010.

[26] P. Jayashree and Dr. K. S. Easwarakumar, "An Effective Defense Cum Prevention Of DDoS Attacks In Active Networks Using Attribute Trees", Ubiquitous Computing and Communication Journal (UCCJ), Jun. 2008.

[27] Yu. Chen et. al., "Distributed Change-Point Detection of DDoS Attacks: Experimen-tal Results on DETER Testbed", Pres. in DETER Community Workshop on Cyber Security Experimentation and Test (DCWCSET), Jul. 2007..