International Journal of Multidisciplinary Research and Publications
ISSN (Online): 2581-6187

DoS and DDoS Attacks at OSI Layers

Hadeel S. Obaid[1], Esamaddin H. Abeed[2]
[1]College of engineering, University of Information Technology and Communications, Baghdad, Iraq
[2]Civil Aviation Authority, Baghdad International Airport, Baghdad, Iraq

Abstract*— *Among different online attacks obstructing IT security, Denial of Service (DoS) and Distributed Denial of Service (DDoS) are the most devastating attack. It also put the security experts under enormous pressure recently in finding efficient defiance methods. DoS attack can be performed variously with diverse codes and tools and can be launched form different OSI model layers. This paper describes in details DoS and DDoS attack, and explains how different types of attacks can be implemented and launched from different OSI model layers. It provides a better understanding of these increasing occurrences in order to improve efficient countermeasures.

Keywords*— *DoS, DDoS, OSI Layers, OPNET.

I. INTRODUCTION

The Internet has changed the style of communication, the way of running a business [1]. And it provides many services for various fields such as education, entertainment, banking transactions, medicine, research, etc. Development of the network technologies allows intruders and hackers to discover illegitimate methods to enter a system.

Network security is frequently discussed as part of computational infrastructure [2]. The commitment of safeguarding critical data, information and services placed on internet and computer networks is a key focus of research today. Many new threats have appeared and defences against them are constantly being developed. Computational threats can be classified into four classes: password attack, malware, denial of service (DoS) attacks and reconnaissance attacks. For the DoS type of threat, securing the network from a denial of service attack becomes critical, because this attack is very easy to perform.

Since 1995, San Francisco Federal Bureau of Investigation (FBI) and Computer Security Institute (CSI) are produced an annual survey [3]. This survey found that, the third most significant attack that causes computer crime losses is the DoS attack, which comes after unauthorized access to information and Virus attacks. The total approximate loss of DoS attack is more than 7 million dollars for 639 respondents that wanted and capable of estimation losses in 2005.

Annually, Distributed Denial of Service attack (DDoS) costs businesses about $3.5 million as reported by Ponemon Institute's research [2]. 54 minutes is the average downtime after a DDoS attack and each minute of downtime cost approximately $22,000. Estimations from the Yankee Group, IDC and Forrester expect the 24 hours for a big E-commerce business outage cost about $30 million.

Today, many network facility and application servers can be under DoS and DDoS attacks [4]. The major aim of these two attacks is to block legitimate users from online services. The users may have to pay for these services. An assailant does not distinguish due to the fee of the service. The purpose behind DoS attacks is not to abuse or take data, but the purpose is to flood the server by sending a huge amount of traffic. In general, the attacker prevents legal users from using an online service by draining the server resources. In addition, the Internet of Things (IoT) has recently been presented as the next revolution and a part of the internet of the future [29]. DoS can be also used to pull down any IoT network as well [30].

The rest of the paper is ordered as following: in section 2 includes the related work. Section 3 explains the DoS attacks. section 4 presents DDoS attacks. OSI layers and their attacks are in Section 5. Finally, the Conclusion in section 6.

II. RELATED WORK

Koc and Carswelll have implemented experiments using Naïve Bayesian (NB), KDD99 dataset, and its variables; Tree (NBTree), Averaged One-Dependence Estimators (AODE), Weightily AODE (WAODE), Tree-Augmented Naïve Bayesian (TAN), Decision DTNB, and Hidden Naïve Bayesian (HNBNB) [5]. The results of their experiments indicate that Proportion K-Interval discretization techniques, along with HNB, offer high accuracy to detect DDoS attack.

Machine learning (ML) is a known area of computer science that mainly deals with the discovery of data patterns and data-related irregularities [31]. Lohit Barki et al. have proposed an IDS to detect DDoS attack in Software Defined Network (SDN) using machine learning algorithms such as K-Nearest neighbour, Naive Bayes, K-medoids and K-means to categorise incoming traffic into regular and irregular categories [6]. The detection rate and efficiency parameters are used to measure these algorithms. The algorithm has more accuracy in choosing to implement Signature IDS; its results are then processed by Advanced IDS, where the intent is to detect anomalous behaviour using open connections. This helps to provide accurate results of the hosts involved in the DDOS attack.

Katkar and Bhatia have performed an experiment for intrusion detection using REPTree classifier and assess the variation in its performance when it is combined with different data pre-processing and feature selection techniques [7]. Experiment results show that the accuracy of REPTree classifier in detecting intrusion is better when used with Numeric to Binary pre-processing technique on the data set of KDD99.

Zhiyuan Tan et al. have presented detection system to detect DoS attack using multivariate correlation analysis (MCA) [8]. By extracting geometrical correlations between different features of network traffic, MCA can be used for network characterization. Such a detection system uses

Hadeel S. Obaid and Esamaddin H. Abeed, "DoS and DDoS Attacks at OSI Layers," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 2, Issue 8, pp. 1-9, 2020.

anomaly based detection in its attack recognition. The advantage is it makes the solution able to detect identified and unidentified DoS attacks through learning normal patterns of the network traffic. Additionally, to improve and to accelerate MCA processes, a triangle-area-based method is suggested. The efficiency of this suggested detection system is assessed using the data set of the KDD Cup 99. The effects of both regulated and non-regulated data on the performance of the proposed detection system are tested.

Detection methods such as Client Puzzle Protocol (CPP) and Ingress filtering are used to detect DoS and DDoS attacks at the Application layer [4]. In internet communication, CPP algorithm is used and aims to stop misuse of server resources. CPP requires that all clients that want to connect to the server to resolve a mathematical puzzle before the connection is to be established. When the puzzle is solved, the client passes the solution of the puzzle to the server. If the client failed to solve the puzzle, the server refuses the connection. The puzzle is not hard to solve but the attacker attempt to establish a huge number of connections with the target and this will be difficult because of the time delay. The Ingress filtering technique is used to ensure that the arrival packets do not have fake source IP addresses in their header. Every packet is sent with the IP source address in the header. If this IP address is fake, this is considered as an attack. In Ingress filtering, packets are examined based on the information from the past so that the server will not be allowed to respond to packets from possible attacking IP addresses.

III. Denial of Service Attacks

Availability, Confidentiality and Integrity are the main aims of computer security [9]. Availability is defined as the capability of using the desired resources or information. DoS attacks threaten the resource's availability in the network.

DoS attacks can happen when an attacker attempts to make Internet-based applications or a website and other services unreachable to legitimate users. Also, DoS attacks can be defined as an attack which aims to prevent the users form using an internet-based service by disturbing the usual functionality of a server that hosts an application [10]. DoS attacks include an attacker sending messages to take advantage of particular vulnerabilities which lead to anomaly or disability in the network systems or sending a large amount of messages quickly to a single node to consume the resources of the system that cause a crash in the system see Fig. 1 [11].

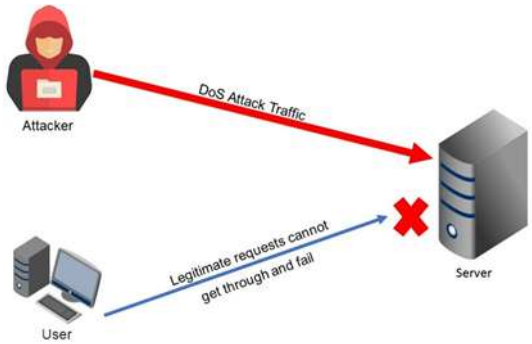

Fig. 1. DoS Attack

IV. Distributed Denial of Service (DDoS) Attack

DoS attack results from many distributed sources is called a Distributed Denial of Service attack (DDoS) [11]. In this type of attack, multiple bots called zombies are used to send a huge amount of traffic to the victim sever.

DDoS attack aims to expand the Dos attack strength by using more than one computer [4]. DDoS attacks are considered to be more efficient than DoS attacks because they raise the attack density through the use of many computers simultaneously. DDoS attacks are a repeated disorder to services in web servers of high profile sites such as insurance companies, credit card payment gateways, banks, etc. DDoS happens when many computers overflow the resources of a victim, making DoS attack further effective and difficult to find the attack creator or origin. DDoS attacks are able to cause a big harm to online services. Because they are able to quickly damage the network performance and make the detection hard. DDoS attacks are considered to be a dangerous security threats to the present Intrusion detection schemes. Discovering DDoS attacks in adequate time would minimize the damage that the attack can cause. Until now, no efficient solutions to overcome all DDoS attacks' characteristics. Thus, detection of DDoS attacks represent an attractive domain for researches. DDoS is typically executed in a logical structure as shown in Fig. 2:

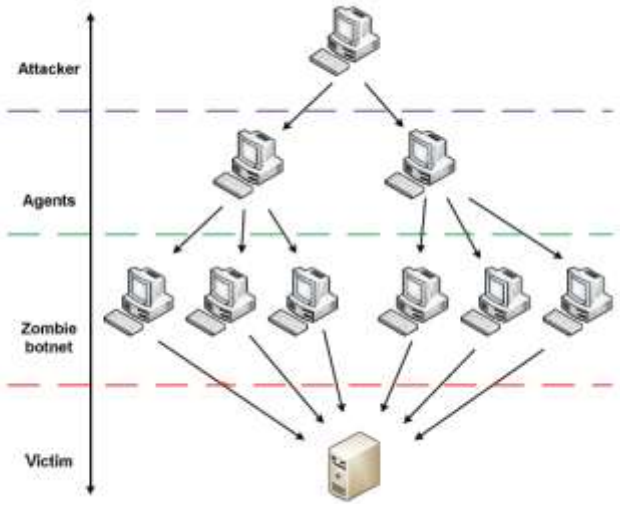

Fig. 2. Structure of DDoS Attack

The structure of DDoS includes a client, who represents the attacker and is connected to a number of cooperated systems called handlers [4]. The handlers direct commands to a number of zombie agents that ease the DDoS onto the victim system. Each handler is able to dominate thousands of zombie agents.

Internet Relay Channel (IRC) is used by the attacker to communicate with agents [12]. The attacker can use (Internet Relay Channel) IRC to communicate with agents rather than installing a handler program on a network server. The IRC channel enables the attacker to use genuine IRC ports to forward instructions to agents. Using genuine ports prevent distributed denial of service command requests to be tracked. Also, IRC servers have huge amount of traffic, allowing

Hadeel S. Obaid and Esamaddin H. Abeed, "DoS and DDoS Attacks at OSI Layers," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 2, Issue 8, pp. 1-9, 2020.

attackers to hide their existence. A malicious node does not need to preserve agents listing, as he is able to directly access the IRC server and check the existing agents. In the IRC network, the agent software sends and receives messages via an IRC channel, where information about the operational is available for the attacker [13].

V. OSI Model in Brief

Open System Interconnection (OSI) is a framework to define the agreements and functions required for communications between network systems [14]. Working on the OSI model started in the late of 1970s by Telephone Consultative Committee or (CCITT) and International Organization for Standardization (ISO). The OSI model applies a structuring technique that is called layering. This partitions communication into a set of vertical layers, where each layer performs functions that apply and enhance the layer that is immediately at a lower level. Fig. 3 shows the OSI Model Layers:

Layer name	Layer number	Layer name
Application layer	7	Application layer
Presentation layer	6	Presentation layer
Session layer	5	Session layer
Transport layer	4	Transport layer
Network layer	3	Network layer
Data link layer	2	Data link layer
Physical layer	1	Physical layer

Fig. 3. OSI Model Layers

There are seven layers to the OSI model. The first, Layer 7, is the Application layer that permits access to resources on the network. It helps to send and receive data between different applications [15]. Message/data are the main communication unit (PDU) at this layer. Layer 6 is the Presentation layer, which is responsible for data formatting to exchange between communication's points such as translation, data compression and encryption. Layer 5 is the session layer, where the layer provides termination, governing and establishing sessions through the network. Layer 4 is the Transport layer, which is responsible for providing reliable data delivery from one procedure to another. It guarantees to have an orderly sequence, being error free and having no repetition of the transmission of packets. Segments, datagrams or packets are the (PDU) or unit of communication this layer is based on. Layer 3 is the Network layer, which is responsible for packets' movement between source and destination. It offers routing and addressing to the packets. The packet is the PDU at this layer. Layer 2 is the Data link layer; it ensures error free of data transmission over physical media. The frame is the PDU at this layer. Layer 1 is the physical layer, which manages the transmission of binary data (0s and 1s) through the transmission media. It translates bits into signals, where the bit is the PDU at this layer. The table displays the most common DoS attacks types at different OSI model layers.

A. Denial of Service Attack at the Application Layer

DoS attacks at the application layer are more complex [11]. They incapacitate features or functions as dissenting to the entire network. Application layer protocols have two main categories: user protocols and support protocols. User protocols provide services to users directly, such as through HTTP, SMTP/POP, FTP, IMAP, XMPP, SSH, IRC, etc. Support protocols aim to provide common system functions. Such as DNS, NTP, SNMP, BOOTP/DHCP, TLS/SSL, RTP, SIP, etc [9]. Any of these protocols can be a means or an object to launching a DoS attack. Most protocols at the application layer are structured in a client-server model. A server is a procedure to implement a particular service, such as email or file transfer services. A client is a procedure to request services from a server. Clients can be classified to make them legitimate or not, that is those who do not have malicious logic and malicious clients who do have malicious logic.

DoS attacks at the Application layer are more disturbing than other layers' attacks because of [11]: -

- High obscurity: these attacks use legitimate UDP or TCP connections, making it hard to distinguish them from legitimate users.
- Highly efficient: DoS attacks at the Application layer require fewer numbers of connections.
- Multiple effects: they can directly or indirectly impact many victims. For instance, DNS attacks at one DNS provider can affect all its users.
- Normal traffic rules: these attacks follow the rules of normal traffic and complete the process of the TCP handshake so that traffic in those attacks look like legitimate traffic.
- Affect multiple applications: they affect different applications because any one of the protocols mentioned above can be used to launch a DoS attack.
- Simplicity in exploitation: they take advantage of the simplicity in Layer 7; for instance, a server may collapse by simultaneously refreshing the browsers by thousands of users.
- Limited resources requirement: they require limited resources. An attacker can achieve a successful attack by a limited investment.
- Highly targeted: These attacks aim at a specific application such as web servers running applications in Java, PHP5, and ASP.NET. Targets are crafted using HTTP requests; there could be collisions with the web server´s hashing operation as non-unique and overlapping responses are returned.

An attacker may exhaust memory or CPU of a victim by sending a vast number of service requests [9]. Each request can cause the victim to execute memory and/or CPU intensive operations. For instance, an attacker may order malicious agents to send HTTP requests to a server for downloading a large file. As the server must read the huge file from the hard disk into the memory and send it to a significant number of packets to the malicious user, a single HTTP request can cause

Hadeel S. Obaid and Esamaddin H. Abeed, "DoS and DDoS Attacks at OSI Layers," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 2, Issue 8, pp. 1-9, 2020.

substantial resource depletion on the server in regarding, CPU, I/O, bandwidth and memory.

HTTP GET, Slowloris and HTTP POST Attacks are examples of DoS attacks in Application Layer. HTTP POST and HTTP GET protocols are usually misused in HTTP or HTTPS [4]. An HTTP GET flood attack can be implemented by the exploitation of a weakness in the HTTP protocol. In this attack, the attacker sends a large number of pernicious attacks using the HTTP protocol. The attacker sends a huge number of malicious HTTP GET requests to the victim. Because of the HTTP payloads of these packets is legitimate, the victim server cannot differentiate the malicious HTTP GET requests from normal requests. Therefore, the server has to treat all requests as legitimate requests, where this process then consumes its resources.

Another type of DoS attack at the application layer is when the attacker executes a Slowloris attack or what is called a Slow Header Attack [16].

The weakness of the HTTP GET request is also used in this attack, but it exploits the time delay in HTTP GET headers rather than flooding the server with spoofed requests. The attacker does not send an HTTP GET request one at a time, however the lines of the header are separated and sent. The connection is built by the web server with the attacker and waits for the request header to finish, where this can take a long time. The malicious request for the request is detained for a long time. A default threshold is setup, indicating a maximum timeout for the next header to arrive, where anything over that time will lead to a closed connection. The default threshold of the Apache web server is 300s. This is put as a pause time to send the next line of the header of the attacker's request. As a result, the attacker can consume the resources of the web server by creating multiple connections with the victim's server [4]. An attacker also can take advantage of the weakness in the HTTP POST request also called a Slow Message Body attack [39]. A message body is included in a POST request which can use any encoding. The HTTP Header includes a filed Content-Length that informs the web server about the message's body size. The HTTP Header portion is sent by the attacker to the web server in full. Then the attacker directs the HTTP message body as 1 Byte per 110 seconds sequentially. Simply the web servers follow the Content-Length that is on the header field while waiting for the remainder of the message. By waiting for the whole message body to be sent allows web servers to backing users with sporadic or slow connections. The server will be under DoS attack, if there are some such connections.

B. Denial of Service Attack at the Presentation Layer

DoS attacks at the presentation layer include deformed Secure Socket Layer (SSL) requests. SSL or TLS offers security for web services such as online shopping, online banking, etc [15]. Because of security advantages, many well-known organizations utilize SSL for securing their services [9]. Currently, most transactions are secured by SSL. However, SSL also has attracted attackers. The TCP protocol and TCP handshake is a frequent victim of DoS attacks. After completing the TCP handshake, the exchange of messages starts to authorize the authenticity of communicating entities. Afterwards, the encryption key for communication is built [15]. Several attacks take advantage of the SSL handshake to consume server resources. The Pushdo botnet performs this by sending incompressible data to the SSL server. The SSL protocol needs sufficient computation time and to produce additional workload on the server to treat the un-useful data as a normal handshake. At this stage, the server may stop processing SSL connections or restart them. Firewalls may fail in such a scenario, as both entities have ended the TCP handshake. Attackers often use SSL to tunnel their HTTP-based DoS attacks, as they appear to be a secure request.

SSL DDoS Attacks can be divided into two classes: -

1- Protocol misuse attacks

These attacks exploit the protocol being used. A DoS attack is mounted without completing the secure connection, potentially lacking the need for secure keys. As one example, THC-SSL-DOS, which can be used to 'renegotiate' in the connection, can be applied without the benefit of a secure channel. Mitigation techniques, such as IPS signatures, help to detect these attacks.

2- SSL Traffic Floods

These attacks send a large amount of traffic over an established secure channel that results in depleting the bandwidth and other resources. Without additional information, mitigation devices are not able to differentiate between normal connections and malicious connections. Such attacks cannot issue a web challenge in attempting to assess source legitimacy. You are prone to false actions because you have either nothing to connect to a rate limit.

C. Denial of Service Attack at the Session Layer

The session layer includes the synchronisation and termination of connections over the network [10]. An attacker takes advantage of log-in and log-off protocols to launch DoS attacks in the session layer; for instance, launching a Telnet DoS attack [15]. A Telnet application permits a terminal to communicate remotely with the counterpart. The Telnet uses the network to send and receive data via a port (e.g.23).

The attacker may execute the DoS attack at this level so that defects in Telnet are misused at the switch level, making the services of the switch unobtainable, whereby the administrator will be prevented from controlling the switch [10].

Attacks in Telnet can be classified into three classes [15]: -

1) Telnet brute force attack: in this attack, the attacker uses a list of frequently used passwords and a program is designed to attempt to create a Telnet session by using each word in the list;

2) Telnet communication sniffing: the lack of encryption is the most serious problem in a Telnet protocol. The transmissions between parties over the network are sent without any encryption. This vulnerability is exploited by the attacker for frame sniffing. It can be easy for the attacker to sniff the plain text that flows over the network.

3) Telnet DoS: this attack is a way to damage the communication between two devices over the network by consuming the bandwidth of their connection. To implement this, the attacker sends a large number of irrelevant and useful data frames, thereby stifling the connection. As a result, a

legitimate communication cannot use this connection. This attack is also used to stop administrators from using Telnet in their devices.

D. Denial of Service Attack at Transport Layer

Layer 4 DoS attacks are based on transmission and generation of an enormous volume of traffic to deactivate or totally block the availability of services or resources in the network for legal clients [15]. These attacks usually include misuse of TCP and UDP protocols for flooding resources in the network.

DoS attacks at Transport layer classified into flooding attacks and de-synchronization attack [17]:

- Flooding

If an attacker is iterating to make a new connection with the same server, which wants to retain status at each end of the connection, the resources that are needed for each one of these connections will be consumed [17]. As a result, any further connections from any other users cannot be served, where they may even be dropped.

- De-synchronization

De-synchronization attack is the disturbance of a current connection [17]. For example, the attacker can spoof messages continually to a node and this causes the node to retransmit the lost frames. End hosts may not be able to exchange data effectively, if the attack is done promptly, where the resources are then wasted in the connection.

To understand DoS attacks at the transport layer, a brief explanation of the TCP/IP protocol is needed [18]. The USA military Defense Department was the first to implement the TCP/IP protocol suite. The Internet, at that time, was very limited and the TCP/IP protocol was capable of providing the required security. However, by time the Internet started to mature, the TCP/IP protocol had not improved. Today, the TCP/IP suite is neither considered secure nor resistant to attacks. An Internet protocol (IP) is defined as a service with packet delivery [19]:

- Delivery without assurances of acknowledgements.
- IP Protocol is connection less i.e. each packet is handled individually from all other packets.
- The Internet makes a reasonable effort to deliver packets to the best of its abilities. Fig. 4 represents the IP header:

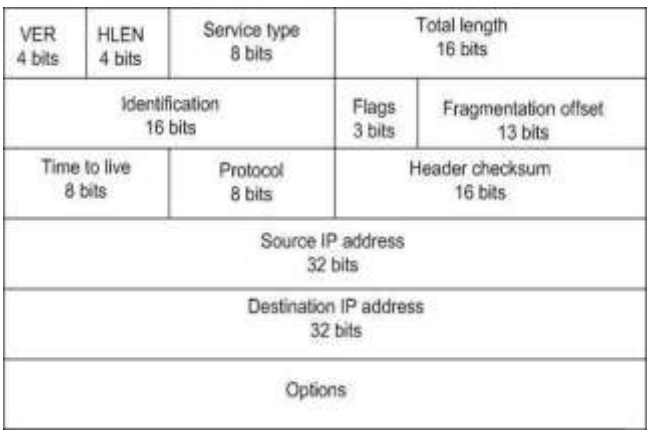

Fig. 4. IP Header

Transmission Control Protocol (TCP) is a process to process protocol [19]. TCP protocol uses port numbers to provide program to program communication. TCP is a connection-oriented; for program A to communicate with program B, there must be a connection has been set up between A and B. This connection allows the sending and receiving processes to deliver and receive data as a stream of bytes. TCP is part of the transport layer above the Network layer; variable length data streams can be sent and received. Fig. 5 shows the TCP header:

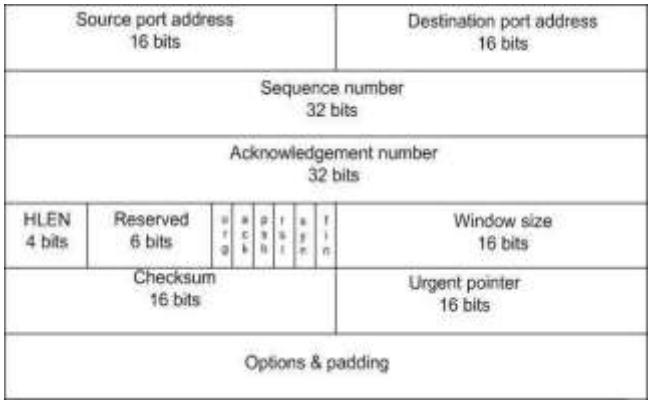

Fig. 5. TCP Header

TCP is a connection-oriented, stream protocol which offers full duplex service where the data can flow over the internet in both directions [20]. To establish the connection, TCP uses the three-way handshake process. In Fig. 6, the illustration shows a three-way handshake process between a TCP server and a TCP client.

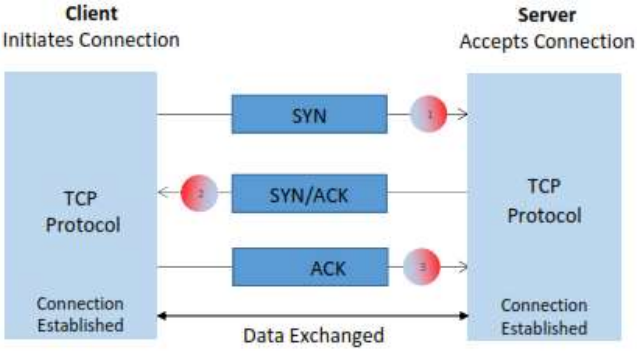

Fig. 6. TCP Three Way Handshake

- First, the client sends a packet marked with SYN to the server.
- After the SYN packet is received from the client, the server sends a SYN+ACK packet to the client.
- The client reply with an ACK packet and the connection is established with the server. Now, the client is able to send the data messages.

A TCP SYN flood attack represents easiest and most dangerous ways to launch DDoS attacks [21]. This attack uses the weaknesses in the TCP protocol, but it was not considered a weakness when the protocol was developed. In 1994, Steve Bellovin and Bill Cheswick discovered the weakness in the

Hadeel S. Obaid and Esamaddin H. Abeed, "DoS and DDoS Attacks at OSI Layers," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 2, Issue 8, pp. 1-9, 2020.

TCP protocol (TCP SYN flood attack).

In such TCP SYN attacks, a synchronize flag in TCP headers is utilized in messages sent [22]. This flag is set when the system sends a packet in a TCP connection; there is an indication that the receipt system has to store the sequence number contained in this packet.

The characteristics of the TCP SYN flood attack are [21]:

- A huge number of server connections are generated by the attacker.
- SYN sets up a RECEIVED state. Then the victim receives a request to form a connection that allocates memory to it.
- The server leaves this half-open connection in the backlog queue and a reply packet to the client with SYN and ACK flags after the server receives a request for connection, which is a packet with SYN flag.
- The server sends the SYN ACK packet again until a timeout finishes when it does not receive any reply from the client. It removes this half-opened connection from the backlog queue.
- The whole procedure of SYN requests may take about three minutes for operating systems.
- TCP SYN flood attack produces a huge amount of half-open connections that the server cannot handle; new requests cannot be received.
- Connections remain at a SYN RECEIVED status until the backlog queue becomes full.
- The operating system is able to serve only some of the half opened connections, depending on the size of the backlog. As an example, 2048 bytes is the default size of the backlog queue of the Debian Squeeze. If it reaches this size, the server cannot receive any connection requests. Fig.7. shows TCP SYN Flood DoS attack network:

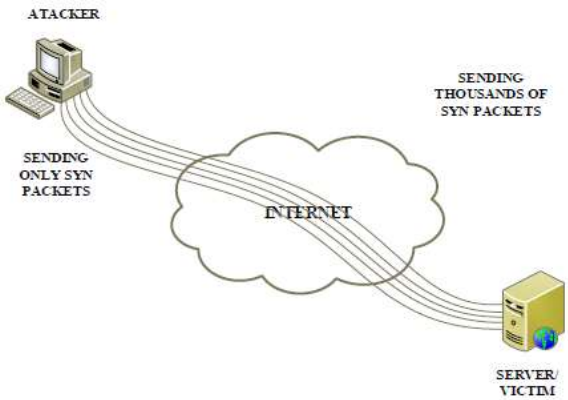

Fig. 7. TCP SYN Flood DoS Attack

If the malicious client quickly sends SYN packets without using the spoofing technique to spoof the IP source address, in this case the attack is called a direct attack [22]. This attack can be implemented by simply sending many TCP connection requests. The operating system of the attacker may not reply to the SYN-ACKs, where RSTs, ICMP, or ACKs messages may move the Transmission Control Block (TCB) from the SYN-RECEIVED state. The attacker can avoid responding to the SYN-ACK packets by setting some of the firewall configurations by which the firewall can filter leaving packets to the listener (i.e., only permitting SYN packets out); the firewall can filter arriving packets so that the SYN-ACK packets are dropped before approaching the processing code of the local TCP.

The source IP address is also can be spoofed to perform the TCP SYN attack; this is more complicated than the direct attack [22]. In such attack, the attacker changes firewall rules, generates and send IP packets that have legal TCP and IP headers. Furthermore, IP address spoofing techniques can be classified into various categories, depending on what spoofed IP source address is used in the attack packet.

The DDoS TCP SYN flood attack is very dangerous to the victim server because it raises the amount of the traffic that is sent to the victim [21]. Chasing the distributed attack is a tough task, which is the major reason that makes the defense against a TCP SYN DDoS attack very hard. User Datagram Protocol (UDP) is a protocol in the transport layer and the application layer uses this protocol widely, including DNS servers [23]. UDP is not like TCP; this protocol is connectionless and there is no guarantee that data reach their destination. Fig.8 represents the UDP header.

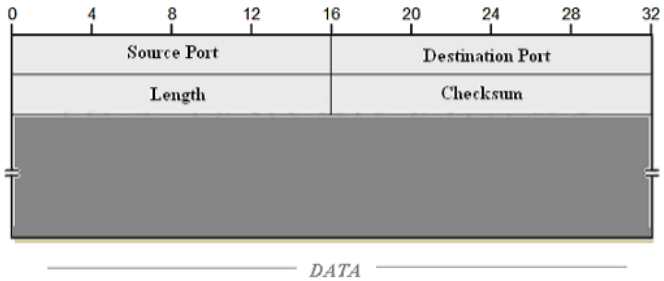

Fig. 8. UDP Header

In UDP flood DoS attacks, the attacker uses the UDP to perform this type of attack [18]. Using the UDP protocol to launch DoS attacks is not as simple as using the TCP protocol. However, the UDP flood attack is executed by sending many UDP packets to random ports of the victim [10]. Consequently, the target server will:

Examine the application which listens at the port.

On that port, if there is no application listening, the server responds with an ICMP packet Destination Unreachable message. Fig.9 shows the UDP Flood Attack.

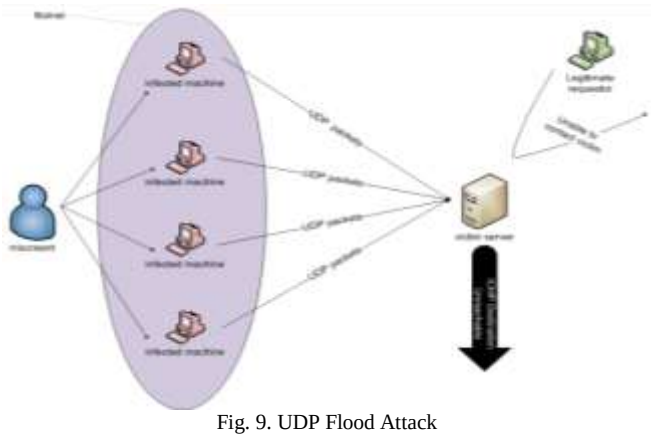

Fig. 9. UDP Flood Attack

Hadeel S. Obaid and Esamaddin H. Abeed, "DoS and DDoS Attacks at OSI Layers," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 2, Issue 8, pp. 1-9, 2020.

E. Denial of Service Attack at the Network Layer

Layer 3 of the OSI model is responsible for data packets' routing and switching to various networks and LANs. It depends on IP, ARP, RIP and ICMP protocols, relying on routers [10]. DoS attacks at the Network layer include injecting the victim's network with a large amount of traffic that it cannot handle. As a result, the victim network begins to respond slowly or it neglects some packets. The loss of some packets can cause an overflow of retransmitted packets and causes extra traffic. Increasing the network traffic overfeeds the network, and it becomes inaccessible for the legitimate users [15]. There are several attacks at the Network Layer:

1- Smurf Attack

Smurf Attack is an old DoS attack where the attacker sends an echo packet to a routing machine in the network, and the source of the data is concealed. By using a broadcast address, the request is sent to all machines over the network. All machines that receive the echo packet send a reply to the sender, which is the victim [6]. Smurfing considers internet control message protocols (ICMP) and Internet protocols. A network administrator uses an ICMP protocol for data exchange, the network status, and pinging devices to define their operational state. The machines that are operative send back an echo packet as a response to ping requests. The Smurf program generates a network packet that seems to have originated from another address; this is called IP spoofing. The packet includes an ICMP ping message, which is sent to all IP addresses in the network by using an IP broadcast. Thus, the echo responses are sent to the IP address of the victim. Many ping requests and echo replies make the network unavailable for real traffic [12]. Fig. 10 shows the Smurf Attack Smurf attack Steps:

1- The attacker determines IP address of the victim.
2- The attacker identifies the intermediate site to help in increasing attack.
3- The attacker sends a huge amount of traffic to the broadcast address at specific intermediate sites.
4- Intermediate sites offer broadcast to all hosts in a subnet.
5- Hosts reply to the victim's address.

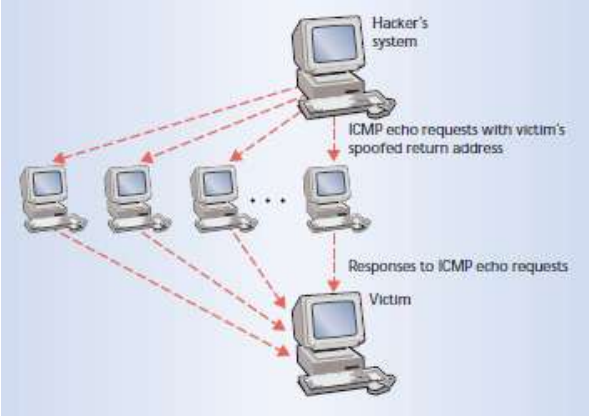

Fig. 10. Smurf Attack

2- ICMP Flood Attack

In ICMP Flood, also called a Ping flood, where the attacker sends an enormous number of ICMP Echo packets to the victim server in order to exhaust all existing bandwidth and prevent legitimate users [24]. The ping command is one example of this attack. The ping command is mainly used for testing the connectivity of the network by examining whether a device can send and receive messages over the network. Fig. 11 represents the ICMP Flood Attack.

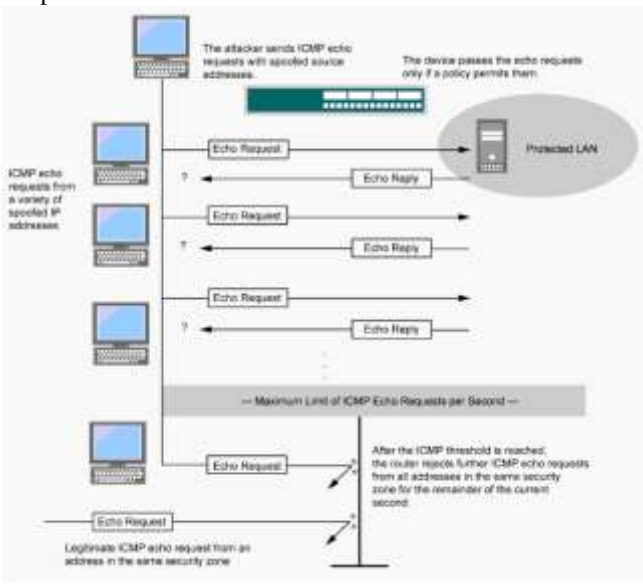

Fig. 11. ICMP Flood Attack

F. Denial of Service Attack at the Data Link Layer

Layer 2 ensures that the data is effectively handed over to the physical layer [10]. The media access control (MAC) or link layer offers channel settlement neighbor-to-neighbor transmission. Cooperative systems, which depend on carrier sense and allows nodes to sense other nodes are communicating, are particularly susceptible to DoS attacks. Attacks such us Collision, Unfairness and Exhaustion are based on attacking data frame detection, medium access control, multiplexing of data-streams and error control [17]. There are well-known attacks at Data Link Layer.

1- Unfairness Attack

Misusing a cooperating MAC layer priority system or sporadic application of those attacks can result in an Unfairness Attack, which is a weak format type of DoS attack [26]. This menace may not completely block legal entry to the channel, however this can reduce service by making clients miss their deadlines in a real time MAC protocol. One mechanism to prevent this menace is using small frames so that a node may access the channel only for a short time. But, this technique can increase framing overhead if the network sends long messages. In addition, an attacker can fail this defense by deception, where competing for access, for example, by replying fast, whilst others delay in a random way.

2- Collision Attack

A collision in one octet may only be needed for a transmission to cause disruption [26]. Any change in the data part may cause a mismatch in the checksum at the receiver end. In some MAC protocols, a distorted ACK control message can produce expensive exponential back off. At any

Hadeel S. Obaid and Esamaddin H. Abeed, "DoS and DDoS Attacks at OSI Layers," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 2, Issue 8, pp. 1-9, 2020.

layer, error-correcting codes offer a good method for bearing changing levels of distortion in messages. These codes can function best as counters to probabilistic or environmental errors. In one encoding, attackers may distort more data than the system can correct at a considerabl cost to the system. Codes for correcting errors themselves can cause further communication and processing overhead. A network may employ collision detection to detect the attacking collisions, but it generates a link layer jamming process and no efficient defense is known. Appropriate communication still need cooperation between machines, which are predictable to prevent distortion of others' packets. Access may be denied through the subservient node, where less energy is expended in fulltime jamming.

3- Exhaustion Attack

A simple implementation of link layer is attempting to retransmit frequently, while even having been produced by a late collision, including such a collision near the end of the frame [26]. An Exhaustion attack is an active DoS attack that can exhaust the resources of the battery in neighboring devices. The attack compromises availableness at little expense to the attacker. The likelihood of unintended collision, can be reduced by random back-offs; therefore, they could not help in stopping such an attack. Each node is offered a slot to broadcast without needing adjudication for each frame by using Time Division Multiplexing Technique. The unlimited delay issue in a back-off algorithm could be resolved by using such a technique, however, it is still vulnerable to collisions. A self-sacrificing node can take advantage of the cooperating nature of most protocols at the MAC layer in an interrogation attack. For instance, Request-to-Send, Data/Ack and Clear-to-Send messages are used by IEEE 802.11 MAC protocols to detain data transmission and channel access. A node could frequently request to access the channel by sending RTS, obtaining a CTS reply from the targeted neighbor. The energy resources of both nodes can be consumed by continuous transmission. The MAC admission can monitor the rate limit as a solution, thus additional requests are disregard on the network without sending costly radio transmissions. This limit should not be less than the predictable maximum data rate that the network can support. Limiting the inessential replies that the protocol needs is an approach to prevent battery exhaustion attack. Engineers often code this ability into the system for generic effectiveness; however, extra logic is needed for coding to deal with possible attacks.

G. Denial of Service Attack at the Physical layer

Jamming attacks are one of the most significant attacks in denial of service attacks [27]. Because wireless networks are dependent on radio channels, jamming attacks overlap with the transmission channels by transmitting semi-valid packets to interrupt the transmission between genuine nodes.

DoS attacks that target the network infrastructure have become more prevalent because of the increase in the number of wireless networks and the importance of such networks [28]. Wireless transmissions are constantly very sensitive to interference. As an example, Microsoft's Xbox is able to interfere with 802.11n networks because they both use 2.4 GHz bands. This interference can be performed using a jammer. Outside the United States, it is legal to use frequency jammers. For example, in France, they allow using frequency jammers to ban cell phone communications in restaurants and theatres. In Italy, jammers are used to decrease the probability of academic dishonesty in exam rooms. In Mexico, jammers are used to maintain the sacredness of religious occasions. In distributed networks, Miniature jammers are used in malicious and intentional disruptions of wireless communication. Nowadays low-power tiny, jammers can be build using Nano Electro Mechanical Systems (NEMS) and Micro Electro Mechanical Systems (MEMS) which can be spread like "dust" constructing a distributed jammer network. Such a jammer has a simple function in comparison to sensors (i.e., transmitting noise signals rather than: filtering, complex modulation, or various other type of signal processing functions). In Iraq, in the second Gulf War, the United States used these techniques [25]. At the Physical layer, there are two types of DoS attacks [26]:

Jamming attack: - which is a well-known attack on wireless communication. The attack frequencies interfere with the regular frequencies that the nodes of the network used. An attacker may interrupt the whole network with jamming nodes, placing the network nodes out of service.

Tampering attack: - A One cannot realistically expect access to many or hundreds of nodes that are spread over a wide area. These networks can be under true brute-force destruction. An attacker may replace or damage sensor and computation hardware; important information could be hacked. Cryptographic keys can be used to obtain unlimited entree to higher levels of communication, where node destruction could become difficult to be differentiated from fail silent behaviour.

VI. CONCLUSION

Attackers attempt to launch DoS and DDoS attacks from different OSI model layers. They take advantage of the security issues involves in this model. Engineers did not consider security when they first developed the OSI model layers. DoS attacks at Application layer are complex and disturbing than the other layers DoS attacks. HTTP GET and HTTP POST Attacks are the most popular DoS attacks at the Application layer. They misuse the HTTP GET and HTTP POST protocols.

DoS attack at the presentation Layer includes the misuse of the Secure Socket Layer (SSL) protocol. While DoS attacks at the Session Layer abuse the of log-on and log-off protocols such as Telnet DoS attack. DoS attacks at the Transport layer often involve misuse of TCP and UDP protocols. Layer 4 DoS attacks can be classified into flooding attacks and de-synchronization attack. The most common DoS and DDoS attacks at the Transport layer are TCP SYN flood and UDP flood attacks. TCP SYN flood uses the weaknesses in the TCP protocol. While UDP flood attacks use the UDP to perform this type of attack but is not as simple as using the TCP protocol. They can be executed by sending many UDP packets to random ports of the target victim. Network layer DoS attacks involve injecting the victim's network with a large

amount of traffic that it cannot handle. Smurf Attack, ICMP Flood and Ping of Death are the most common attacks at this layer. All these attacks based on the ICMP protocol weaknesses. Data Link Layer includes attacks such as Collision, Unfairness and Exhaustion which are based on attacking data frame detection, medium access control, multiplexing of data-streams and error control.

REFERENCES

[1] Razak, T.A.: 'A study on IDS for preventing denial of service attack using outliers' techniques', (IEEE, 2016), pp. 768-775.
[2] Luo, S., Wu, J., Li, J., and Pei, B.: 'A defense mechanism for distributed denial of service attack in software-defined networks' (IEEE, 2015), pp. 325-329.
[3] Loukas, G.: 'Defence against denial of service in self-aware networks', 2006.
[4] Durcekova, V., Schwartz, L., and Shahmehri, N.: 'Sophisticated denial of service attacks aimed at application layer' (IEEE, 2012), pp. 55-60
[5] Koc, L., and Carswell, A.D.: 'Network intrusion detection using a hnb binary classifier', (IEEE, 2015.), pp. 81-85.
[6] Barki, L., Shidling, A., Meti, N., Narayan, D., and Mulla, M.M.: 'Detection of distributed denial of service attacks in software defined networks' (IEEE, 2016), pp. 2576-2581.
[7] Katkar, V.D., and Bhatia, D.S.: 'Experiments on detection of Denial of Service attacks using REPTree', (IEEE, 2013), pp. 713-718.
[8] Tan, Z., Jamdagni, A., He, X., Nanda, P., and Liu, R.P.: 'A system for denial-of-service attack detection based on multivariate correlation analysis', IEEE transactions on parallel and distributed systems, 2013, 25, (2), pp. 447-456.
[9] Abliz, M.: 'Internet denial of service attacks and defense mechanisms', University of Pittsburgh, Department of Computer Science, Technical Report, 2011, pp. 1-50.
[10] Muharish, E.Y.M.: 'Packet filter approach to detect denial of service attacks', 2016.
[11] Kumar, G.: 'Understanding denial of service (DoS) attacks using OSI reference model', International Journal of Education and Science Research, 2014, 1, (5).
[12] Sandeep, R.: 'A study of DoS & DDoS-smurf attack and preventive measures', International Journal of Computer Science and Information Technology Research, 2014, 2, pp. 1-6.
[13] Panicker, A.: 'Botnets and Distributed Denial of Service Attacks', 2008.
[14] Kumar, S., Dalal, S., and Dixit, V.: 'The OSI model: Overview on the seven layers of computer networks', International Journal of Computer cience and Information Technology Research, 2014, 2, (3), pp. 461-466.
[15] Kumar, G.: 'Denial of service attacks–an updated perspective', Systems science & control engineering, 2016, 4, (1), pp. 285-294.
[16] Tripathi, N., Hubballi, N., and Singh, Y.: 'How secure are web servers? An empirical study of slow HTTP DoS attacks and detection', (IEEE, 2016), pp. 454-463.
[17] Xia, Y.: 'Selective Dropping of Rate Limiting Against Denial of Service Attacks', University of Dayton, 2016.
[18] Shah, M., Soni, V., Shah, H., and Desai, M.: 'TCP/IP network protocols—security threats, flaws and defense methods' (IEEE, 2016), pp. 2693-2699.
[19] Maregeli, C.N.: 'A study on TCP-SYN attacks and their effects on a network infrastructure', 2010.
[20] Rana, D.S., Garg, N., and Chamoli, S.K.: 'A Study and Detection of TCP SYN Flood Attacks with IP spoofing and its Mitigations', International Journal of Computer Technology and Applications, 2012, 3, (4), pp. 1476-1480
[21] Bogdanoski, M., Toshe.vski, A., Bogatinov, D., and Bogdanoski, M.: 'A novel approach for mitigating the effects of the TCP SYN flood DDoS attacks', World Journal of Modelling and Simulation, 2016, 12, (3), pp. 217-230.
[22] Bogdanoski, M., Suminoski, T., and Risteski, A.: 'Analysis of the SYN flood DoS attack', International Journal of Computer Network and Information Security (IJCNIS), 2013, 5, (8), pp. 1-11.
[23] Saied, A.: 'Distributed denial of service (ddos) attack detection and mitigation', King's College London, 2015.
[24] Gupta, N., Jain, A., Saini, P., and Gupta, V.: 'DDoS attack algorithm using ICMP flood', (IEEE, 2016), pp. 4082-4084.
[25] Shaker, K.: 'Analyzing DoS and DDos Attacks to Identify Effective Mitigation Techniques', American International University-Bangladesh (AIUB), 2014.
[26] Wood, A.D., and Stankovic, J.A.: 'Denial of service in sensor networks', computer, 2002, 35, (10), pp. 54-62.
[27] Bandaru, S.: 'Investigating the Effect of Jamming Attacks on Wireless LANS', International Journal of Computer Applications, 2014, 99, (14), pp. 5-9.
[28] Akhter, S., Myers, J., Bowen, C., Ferzetti, S., Belko, P., and Hnatyshin, V.: 'Modeling DDoS Attacks with IP Spoofing and Hop-Count Defense Measure Using OPNET Modeler', (2013).
[29] Sabry, S.S., Qarabash, N.A., and Obaid, H.S.: 'The Road to the Internet of Things: a Survey', (IEEE, 2019), pp. 290-296.
[30] Anirudh, M., Thileeban, S.A., and Nallathambi, D.J.: 'Use of honeypots for mitigating DoS attacks targeted on IoT networks', pp. 1-4.
[31] Obaid, H.S., Dheyab, S.A., and Sabry, S.S.: 'The Impact of Data Pre-Processing Techniques and Dimensionality Reduction on the Accuracy of Machine Learning', (IEEE, 2019), pp. 279-283.