International Journal of Future Generation Communication and Networking
Vol. 13, No. 1, (2020), pp. 959-969

A STUDY ON DENIAL OF SERVICE (DOS) AND DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS

Akash Hegde[1], Krithika L[2], Dr. Sowmyarani C. N[3], Dr. Dayananda P[4]
[1,2,3]*Department of Computer Science and Engineering, R. V. College of Engineering, Bengaluru, India*
[4]*Department of Information Science and Engineering JSS Academy of Technical Education Bengaluru, India*

Abstract

A Denial of Service (DoS) attack is a type of cyber-attack wherein the attacker cripples the users of a machine or a network by making it unavailable temporarily or disrupting the services of a host indefinitely. A Distributed Denial of Service (DDoS) attack is a type of DoS attack in which there are multiple sources for the attack and these sources can flood the target with unnecessary packets, thereby bringing down the target. It is extremely difficult to stop DDoS attacks because it involves multiple sources and blocking a single source is ineffective. In this paper, a thorough study of the existing types of DDoS attacks and their defense mechanisms is presented. Scope for future work in terms of defending against such large-scale attacks is also provided.

Keywords: *denial of service; distributed denial of service; network attacks; cyber security; cyber-attacks; network security; flooding; packets; large scale attacks*

1. INTRODUCTION

In the current world, information and network security is one of the most trending domains due to the abundance of information available. Cyber security is a much needed aspect in any IT infrastructure in recent times. The number of cyber-attacks has increased a lot over the past few years, ranging from simple passive attacks to monitor transactions to large scale deployment of denial-of-service (DoS) attacks to bring down entire networks. When a DoS attack takes place in a co-ordinated fashion with multiple perpetrators launching the attack at the target at once, this is called as a distributed denial-of-service (DDoS) attack.

There lies a major difference between the DoS and DDoS attacks. In a DoS attack, a computer and an internet connection is used to overload a server or the network with more number of data packets, with the only intention of overwhelming the victim's bandwidth and also the other set of available resources. The DDoS attack is a little more amplified. Instead of a computer and an internet connection, it usually involves large number of systems that is used in the distributed fashion to have the effect of shutting down a website or a web application or even a network. In both the cases, the victim is flooded with the data requests which results in disablement of its functionality.

The very first DDoS attack reportedly occurred in 1999, and the frequency and sophistication of these attacks have been increasing since then. The primary objective of these attacks is to cause huge revenue losses to the victim organization or corporation. This was first observed in 2000, when Yahoo! had their services shut down for about 2 hours due to a large scale DDoS flooding attack. In 2002, 9 out of the total 13 domain name system (DNS) servers were shut down for over an hour due to the DDoS attack performed on them. Many such cases have been observed over the recent past and thus, security has become a major concern. Most of these

ISSN: 2233-7857 IJFGCN

attacks are targeted towards high-profile servers, such as those which are used for banking or as payment gateways for credit or debit card transactions, for example. The motivation behind these attacks can be blackmail, revenge, activism or sometimes, even just for fun.

Keeping this in mind, the paper is written in which we have effectively tried to make a comprehensive list of all the DDoS attacks and their known defense (if any). The paper includes information taken from various sources and attempts to provide the reader with ample knowledge about DDoS attacks. This would help researchers to either improve the existing systems or to identify new prototype defense mechanisms for reducing the effect of damage that are caused by the DDoS attacks. Fig. 1 shows how a DDoS attack generally occurs over the Internet.

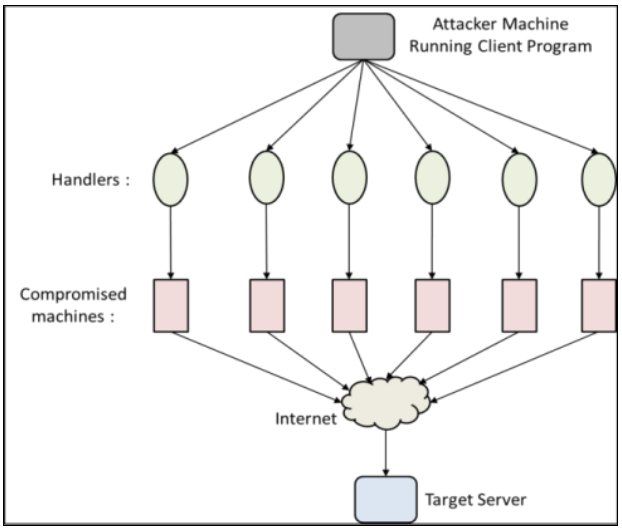

Fig. 1. **General depiction of a DDoS attack**

Section 2 features the related work that have taken place so far in terms of DDoS attacks and their descriptions. Section 3 features the types of DDoS attacks, followed by Section IV which describes the existing defense mechanisms for DDoS attacks. Finally, the conclusions that can be drawn from this study are presented in Section 5.

2. RELATED WORK

The study of DDoS attacks is very popular in recent times and has drawn the attention of many researchers. A brief account of the work referred to, when writing this paper, is given in this section.

A paper presented by A. Wang, S. Chen, W. Chang and A. Mohaisen [1] describes the DDoS attacks that are carried out by botnets over the Internet. Based on the observations, the characteristics of the attacks are analysed and categorised. The analysis were carried out on approximately 51000 DDoS attacks all over the world that were implemented by 674 botnets. It was found that the geolocationanalysis of the attackers always showed that their geospatial distribution followed a set of patterns and hence have made it easier to deploy the defence mechanism in the future.

X. An, X. Lu, J. Su and F. Lin [2] have presented a paper which describes their analysis on intrusion detection systems in fog computing. They have proposed a hypergraph clustering model that works on apriori algorithm. They state that their model describes how the fog nodes

ISSN: 2233-7857 IJFGCN

are associated with respect to the DDoS attacks. They conclude that the amount of usage of the resources of the system can be increased by using the association analysis of DDoS.

S. Hameed and U. Ali [3] have presented a paper which describes their framework HADEC, which is used for detecting DDoS attacks using Hadoop. They state that their framework can be used to analyze flooding attacks efficiently by using MapReduce and HDFS concepts of Hadoop. Furthermore, they state that they have implemented a detection algorithm for DDoS attacks by using counters for TCP-SYN flood, HTTP GET flood, UDP flood and ICMP flood attacks. They evaluated the performance of their HADEC framework and concluded that their framework can process and detect DDoS attacks in almost real-time.

J. Gera and B. P. Battula [4] have presented a paper in which they have proposed a methodology which can be used to find out the DDoS attacks that are spoofed and non-spoofed and also differentiate these from the flash crowds. They say that these flash crowds consist of an enormous traffic that is generated because of Flash Events (FEs), which are extremely similar to DDoS attacks. They have carried out their simulations on NS-2 and they have used the same to validate their methodology.

Z. Liu, Y. Hu, H. Jin and M. Bailey [5] have presented a paper in which they have proposed a proactive prevention mechanism for DDoS attacks. Their proposed model MiddlePolice is designed such that it does not require the Internet core and the stack of clients on the network to change. This yields instant deployability on to the present architecture of the Internet. Their model also guarantees the delivery of victim-desired traffic not considering the attacker strategies as it uses a destination driven traffic control.

J. W. Seo and S. J. Lee [6] have presented a paper in which they have conducted a study for detecting the network-based IP spoofing DDoS along with the malware infected systems effectively. This study will try to calculate the frequency of the packet attributes and will also try to analyse the anomalies if present for detecting the IP-spoofed attacks. It also proposes a method to detect the injection of malware into the systems that trigger the attack on the edge of the network.
Research papers [7], [8], [9], [10], [11] and [12] further describe the different types of DoS and DDoS attacks, their analyses and countermeasures. These papers served as a guideline for the survey done.

3. TYPES OF ATTACKS

DoS attacks occurring on the networks are either the bandwidth attacks or the connectivity attacks. Bandwidth attack is one of the kind of Denial of Service attack which always impacts the network traffic largely; this causes the available network resources to be depleted, which in turn leads to legitimate users not being serviced properly. Connectivity attacks are another form of attacks where the target system gets flooded by a lot of connection requests; this causes the exhaustion of the available resources of the target's operating system, which will lead the server to be unavailable to process legitimate requests. Fig. 2 shows how DoS and DDoS attacks are classified in terms of the layers that they affect.

ISSN: 2233-7857 IJFGCN

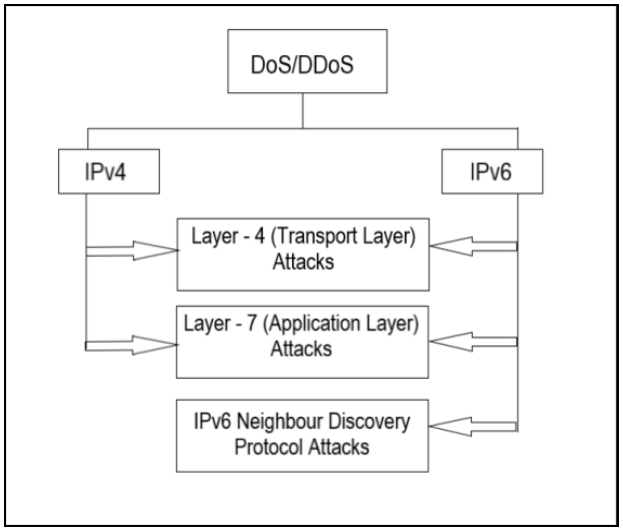

Fig. 2. **Classification of DoS and DDoS attacks**

A. Layer 4 Attacks

Here, the various types of Layer 4 attacks under IPv4 and IPv6 are explained. Layer-4 attacks include the following:

1. TCP-SYN Flood Attack

The SYN flood always uses the 3-way handshake property of TCP for the attack purpose. In order to establish a connection with the destination, initially SYN packets are sent. After the SYN-ACK is received, the destination will not send any responses further. In order to receive the data from the source, a connection queue is used at the destination host. As the matter of fact that there will no further responses from the destination, the queue will have to be maintained all the time which results in the wastage of the compute resources and the inability to service the legitimate requests. Fig. 3 shows how a SYN flooding attack usually occurs.

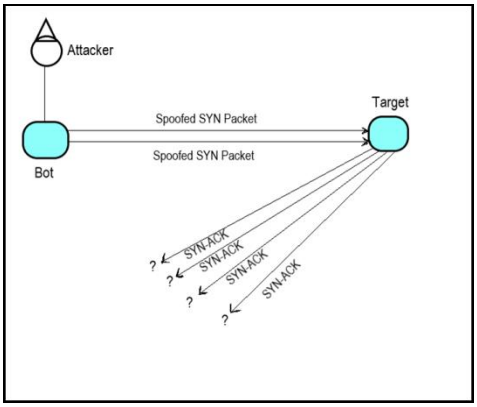

Fig. 3. Depiction of a TCP-SYN Flood Attack

2. UDP Flood Attack

A UDP flooding is caused when an attacker will continuously send a large amount of UDP packets to the target port in a random fashion such that, the target will receive the UDP packets and will confirm the application that is waiting to be sent at the destination

ISSN: 2233-7857 IJFGCN

port. When the absence of existence of such ports at the source is found out, then the ICMP packets are generated in order to reach the original source. This huge amount of packets will cause the target to crash and the attack will become successful. Fig. 4 depicts a general scenario of how a UDP flood attack occurs.

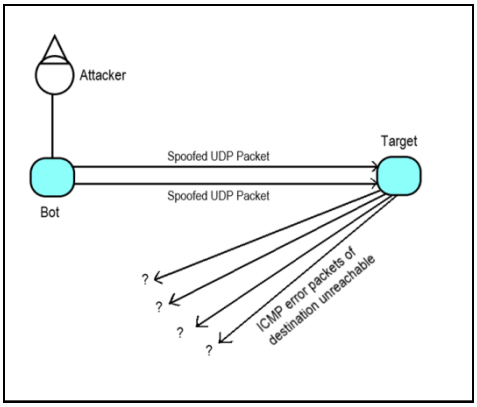

Fig. 4. Depiction of a UDP Flood Attack

3. ICMP (Ping) Flood Attack

In this attack, initially the router that responds to the ICMP requests is found out by the attacker. Knowing this router, the attacker will send the requests to the router's broadcast address that contains the spoofed source IP address. When the message is broadcasted to all the devices in the network by the router, they send back their responses immediately. This will cause the generation of a large amount of traffic making the bandwidth to choke within the network. Fig. 5 depicts how an ICMP flood attack occurs.

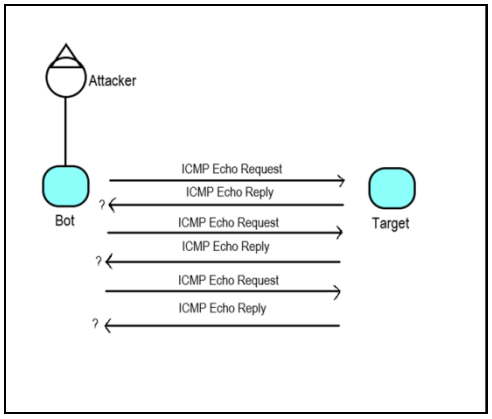

Fig. 5. Depiction of an ICMP Flood Attack

4. Ping of Death Attack

A Ping of Death attack occurs when a attacker tries to transmit a large amount of ping request to a target; these requests contain a huge packet size, which makes the target crash or continuously respond with ICMP echo replies to the attacker. This forces other clients to wait indefinitely. Fig. 6 shows how a Ping of Death attack occurs.

ISSN: 2233-7857 IJFGCN

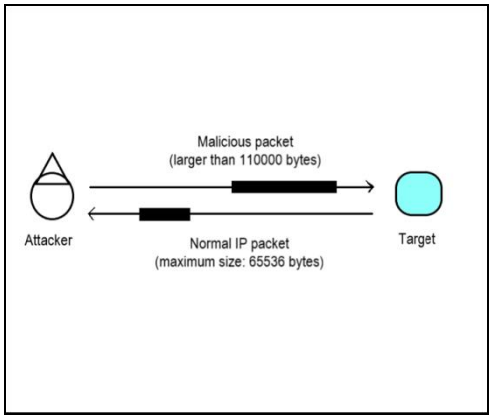

Fig. 6. Depiction of a Ping of Death Attack

5. Teardrop Attack

In a teardrop attack, the manipulated IP fragments that contain the overlapped fragments as well as oversized payloads, are sent by the attacker to the target. As a result of this, the target system may crash and lose huge amount of data. This kind of attack will affect almost all the operating systems and the all types of servers.

6. Low-rate Denial-of-Service Attack

The attacker in the Low-rate DoS attack will create the TCP overflow by continuously sending high-rate, intensive bursts of TCP packets, and trying to enter the re-transmission timeout (RTO) state. All this is done with a very slow time scale which causes the TCP throughput to be reduced heavily at the target's end.

7. Peer-to-Peer Attacks

In this peer-to-peer (P2P) attack, the target system is injected with the useless data. This can be called as poisoning the network. It is for the attacker to inject a huge amount of bogus look-up key-value pairs into the index of the target system as all the P2P networks use a look-up service; this may cause the target system to become slow ,will introduce a delay in producing the query results and also may produce invalid results. Fig. 7 shows how a P2P poisoning occurs.

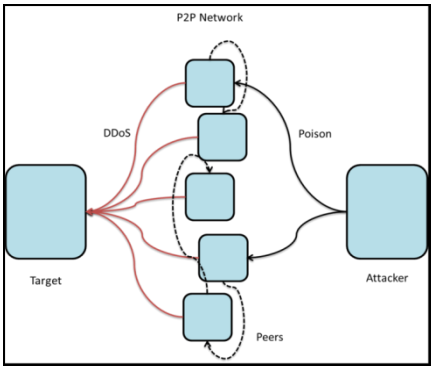

Fig. 7. Depiction of a Peer-to-Peer Attack

8. Smurf Attack

ISSN: 2233-7857 IJFGCN

Smurf attack is a similar kind of ICMP flooding which uses the ICMP echo response process. In such kind of attacks, the attacker will broadcast packets along with the source address that is spoofed towards the victim system. As it is the broadcast address, it will be received by the nodes that are connected in the network. Due to this, every other node in the network will respond to the target machine as the spoofed source IP will be the target's IP address. This causes a lot of response packets to be sent to the victim, which exhausts its sources. According to the RFC2463, the response is generated only if the packet has a IPv6 multicast address or a broadcast address or a link-layer multicast. Thus we can say that smurf attacks are not effective over IPv6.

9. DDoS Reflector Attack

This form of attack is difficult to defend as a matter of fact that the target would be flooded by the traffic from multiple servers over the Internet. This attack would work using the SYN-ACK that are received when TCP SYN request packets are sent. These packets are used by the attackers as a reflector. In a reflector the server response maybe misused after request packet is received. The packets are sent by the reflector agents to the target using the spoofed source address i.e., the address of the non-compromised servers. In every other stage of the attack, the amplification of the rate and size of the packets is done. Due to this, the trace-back or detection of the attacker becomes very difficult. Fig. 8 depicts how a DDoS reflector attack usually occurs.

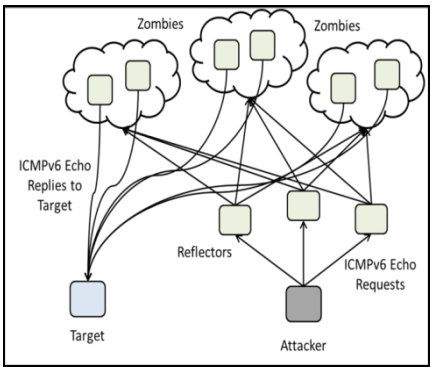

Fig. 8. Depiction of a DDoS Reflector Attack

B. Layer-7 Attacks

In this section, the different Layer-7 attacks that are possible under IPv4 and IPv6 have been explained. Some of these attacks are:

1. Incomplete HTTP Requests using GET Method

This attack will show how data is sent to the web server by the client while there is communication going on between them. Here, the client will send the HTTP requests differently to a web server. HTTP header is not sent completely during the request rather the client sends just a small portion of the header. The subsequent headers are sent by the client continuously to keep the socket alive, at regular intervals of time. The resources of the server are exhausted by the multiple incomplete requests sent by the client.

As a result of this all the available resources of the server is consumed by these requests which leads to denying the requests of the legitimate user. These forms of attacks are quite dangerous as they can be launched using minimum amount of bandwidth and also does not

ISSN: 2233-7857 IJFGCN

require large amount of systems to attack. But as soon as the attack is stopped the server will restore back within few seconds.

2. Incomplete HTTP Requests using POST Method

This form of attack is quite similar to the one with the GET method. The basic difference here is that the client uses the POST method rather than using GET for sending the HTTP requests that are incomplete.

3. HTTP Requests using HEAD Method

The only difference between the HEAD method and the GET method is that using HEAD method. The message body is not sent in response by the server. This helps to save the resources at the attacker's end. Using the HEAD method, the attacker would target the page that is very expensive to build for the server, e.g. a search.

C. IPv6 Neighbour Discovery Protocol Attacks

In this sub-section, we have explained different Neighbour Discovery Protocol-based DoS attacks which are possible under IPv6.

1. Duplicate Address Detection Attack

The ability of configuring with the IP addresses that are global automatically without using a DHCP server is given to the nodes by IPv6, known as a Stateless Address Configuration. In this method, when the node tries to get an IPv6 address and allot the address to itself permanently, first it tries to find whether that address is being used by some other node. This is ensured by multicasting the Neighbour Solicitation Messages with an unspecified source address (::) by focusing that server which has to be checked. If any Neighbour advertisement messages are received by the node for that address then it means that the address is being used by some other node. If none of such messages are received then the checking nodes considers that the address is available and uses that address for its further communications. The above process is called as Duplicate Address Detection (DAD). For launching the attack using this mechanism, the attacker would send the spoofed neighbour advertisement messages as a response to the DAD Neighbour Solicitation Messages along the IP address of the source. This will make a legitimate node to not receive the address for its communication.

2. Neighbour Solicitation/Advertisement Spoofing

The neighbour solicitation attack is same as that of the IPv4 ARP poisoning. In such kinds, the Neighbour advertisement messages that are spoofed are sent as the response to the legitimate neighbour solicitation messages. This would result in redirecting the legitimate traffic towards an invalid destination. This is usually used to get the MITM (Man in the middle) position between a conversation.

D. Attacks based on Router Discovery Mechanism

In the following sub-section, the router discovery mechanism based attacks have been explained.

1. Killing the Default Router

ISSN: 2233-7857 IJFGCN

Every node in the network maintain the set of the IP addresses of those on-link routers that are eligible to become default routers and which also send the router advertisement messages. If this list becomes empty, then the attacker will assume the default router to be absent and all other routers are on-link. This form of attack can be initiated from the attacker by continuously sending the spoofed router advertisements with a lifetime of zero that causes the target system to send all the packets directly to the destination nodes rather through the routers. As the target system or the destination system will not be on-link node, the packet will not reach the destination.

2. Bogus Address Configuration Prefix Attack

The IPv6 addresses are configured by the on-link nodes with the help of the on-link prefixes that are advertised by the router in the router advertisement, in the absence of DHCPv6. Usually these messages are advertised periodically. In order to launch this attack, the attacker can send the spoofed router advertisements with invalid prefixes. Using these prefixes the addresses are configured to the nodes automatically. As a result of this auto configuration of the invalid addresses there will be a loss of communication between the nodes. This attack results in the complete consumption of the CPU resource on the nodes using the Windows operating system but however it doesn't make any effect for the host using the Linux operating system.

4.DEFENSE MECHANISMS

DoS/DDoS attacks require other attacks to be performed in order for them to be executed. Some of the attacks that have to be performed before hand are ARP spoofing/poisoning, IP spoofing, MITM attacks and MAC spoofing. It will not be easy for the attackers to initiate the DoS attacks if the above attacks can be prevented. The countermeasures/defenses against the DoS attacks are described in the following section.

A. Rate Limit

Rate Limiting method uses three processes: detection of the attack, decision on the rate limits and application of the rate limit closer to the sources over the traffic that is due to attack. This method uses some of the agents such as Attack Detection Agent (ADA), Defense Service Provider (DSP), and Rate Limiter (RL). As soon as the attack is detected, ADA will send the alert of the attack along with the request to DSP for defense. It can be installed either as hardware or software on the victim machine or host machine firewalls. The DSP will be used to provide defense services and to process the service orders for defense. Whenever a request from ADA is received, its authenticity is verified in order to confirm that it is not a new attack. Later the decision on rate limiting is done and these commands will be further sent to RL. Limiting the rate of the particular flow is done by the RL. Then the real-time information about the rate is collected approximately and will be reported by RL to the DSP. The RL will be deployed by the ISP and is managed by the local DSP server of the given domain.

B. Aggregation and Push-back Approach

This approach is a process of detection and control of high bandwidth aggregate that results from the DDoS attacks that take place. The collection of the packets that have the similar properties, from one or more flows is called the aggregate. The properties maybe a broader one (e.g. TCP traffic) or even a narrow one (e.g. HTTP traffic) which always

ISSN: 2233-7857 IJFGCN

depends on the specific host. Push-back is a type of co-operative mechanism that is used to manage the upstream aggregation of the traffic. In the given method, the router that is congested will send the command to rate-limit the aggregate to its adjacent upstream routers. These commands will be sent only to such neighbours who are responsible for contributing to the major portion of the aggregate traffic. The push-back method not only saves the upstream bandwidth by dropping the packets early which would be dropped further by the congested router in the downstream, but also tries to limit the rate of the attack traffic within the aggregate.

C. Defense by Offense

Sending higher volume of traffic would offer a remedial measure at the application level for the DDoS attacks. This will not only help the bad clients to be slowed down, but will also help the good clients to increase the amount of traffic to be sent. It is assumed that, if most of the bandwidth is being used by the bad clients, then by helping increase the traffic volume will help to change the volume of the good clients. To measure the bandwidth used, a mechanism is needed by the speak-up. The major responsibility of the given scheme is to help the clients to send larger volume of traffic. A front end tool called thinner will be used for implementing the given mechanism by the speak-ups. The control is implemented by the thinner by sending the requests to the server.

D.Active Filtering

It includes a defense mechanism that is used to detect and also control the attack traffic. It occupies the main body of the traffic and hence protects the TCP friendly traffic. In order to perform the traffic control, gateways are deployed at different locations in the network. It uses new filtering mechanism based on Raspberry Pi. This scheme consists of a packet marking algorithm which holds a complete Raspberry Pi in every packet and also a filtering algorithm which helps in finding out how effectively the scheme is being used by the victim.

E.IP Traceback

IP traceback is a traceback system that uses multiple stages for handling the DDoS attacks. Such a construct is also called as Stealthy Tracing Attackers Research Light Trace (STARLITE). It is a version that is extended from the Source Path Isolation Engine (SPIE). This forms a prototype that integrates the traceback of the single packet and the stepping stone detection. In this context, stepping stones are the attack paths which are traced using the laundering hosts. For this purpose the list of connections are constructed. SPIE is a kind of traceback method that is log based. The capabilities of the IP packet trace-back is mainly dependent on the auditing of the routers in the network. The SPIE Trace-back Manager (STM) is mainly used for managing the whole system. The stepping stone detection process is integrated onto the SPIE system by the STARLITE system for utilising the rich communication infrastructure of the SPIE.

5. CONCLUSION

A Denial of Service (DoS) attacks occur when the target is being crippled by the attacker system in terms of network and resource unavailability. A Distributed Denial of Service (DDoS) attacks will occur when the multiple sources try to attack the target and bring it down. This paper

ISSN: 2233-7857 IJFGCN

has explored the different types of DoS and DDoS attacks and has given an account of how they work. It also briefly describes the possible counter measures that can be considered while defending these attacks.

The intention of this paper is to provide researchers a handy list of attacks and countermeasures such that they can be inspired to improve upon the existing solutions or even propose a new solution for the problem of DoS and DDoS attacks.

REFERENCES

[1] A. Wang, W. Chang, S. Chen and A. Mohaisen,"Delving Into Internet DDoS Attacks by Botnets: Characterization and Analysis", IEEE/ACM Transactions on Networking, IEEE, 2018.

[2] X. An, J. Su, X. Lu and F. Lin,"Hypergraph Clustering Model-based Association Analysis of DDoS Attacks in Fog Computing Intrusion Detection System", EURASIP Journal on Wireless Communications and Networking, Springer, 2018.

[3] S. Hameed and U. Ali, "HADEC: Hadoop-based Live DDoS Detection Framework", EURASIP Journal on Information Security, Springer, 2018.

[4] J. Gera and B. P. Battula, "Detection of Spoofed and Non-spoofed DDoS Attacks and Discriminating Them from Flash Crowds", EURASIP Journal on Information Security, Springer, 2018.

[5] Z. Liu, Y. Hu, H. Jin and M.Bailey, "Practical Proactive DDoS-Attack Mitigation via Endpoint-Driven In-Network Traffic Control", IEEE/ACM Transactions on Networking, IEEE, 2018.

[6] J. W. Seo and S. J. Lee,"A Study on Efficient Detection of Networkbased IP Spoofing DDoS and Malwareinfected Systems", SpringerPlus, Springer, 2016.

[7] N. Tripathi and B. M. Mehtre,"DoS and DDoS Attacks: Impact, Analysis and Countermeasures", 2013.

[8] Z. Chao-yang, "DoS Attack Analysis and Study of New Measures to Prevent", International Conference on Intelligence Science and Information Engineering, 2011.

[9] D. Mukhopadhyay, B. Oh, S. Shim and Y. Kim,"A Study on Recent Approaches in Handling DDoS Attacks", 2010.

[10] M. B. Apsara, P. Dayananda, and C. N. Sowmyarani, "A Review on Secure Group Key Management Schemes for Data Gathering in Wireless Sensor Networks", Eng. Technol. Appl. Sci. Res., vol. 10, no. 1, pp. 5108-5112, Feb. 2020.

[11] K. M. Elleithy, D. Blagovic, W. Cheng and P. Sideleau,"Denial of Service Attack Techniques: Analysis, Implementation and Comparison", 2006.

[12] Bhawna Nigam, Himanshu Dugar, Niranjanamurthy M, "Effectual Predicting Telecom Customer Churn using Deep Neural Network" , International Journal of Engineering and Advanced Technology (IJEAT), Volume-8 Issue-5, June 2019

ISSN: 2233-7857 IJFGCN