ISSN:0975-9646

A Survey on Distributed Denial of Services (DDOS)

Er. Sakshi kakkar , Er. Dinesh kumar

Computer Science Engineering Department,
Giani Zail Singh PTU Campus
Bathinda, India

Abstract—DDoS attacks are a dreadful problem with the internet services and the network. DDoS attacks are the massive attacks launched by distributing malicious computers. The hard problem against the defense of the DDoS attack is to distinguish the legitimate traffic from the attack traffic. In ISP domain, detection of a variety of attacks must be needed to handle. This paper introduces about the major problem occur in the security which is known as DDoS attacks.The objective of this paper is to provide a survey of various mechanisms of distributed denial of service attacks, its detection and various approaches to handle these attacks. Detection of DDOS attack can be on source side as well as on the victim side. Based on the surveyed work it provides the reader to work in the research by using these approaches and features of DDOS attacks.

***Keywords*—DoS,DDoS,network,survey**

I. INTRODUCTION

Distributed Denial of service attack is a defined an attack launched by many attacker's host to one or more victim host, such that victim host is not further capable of providing its services or resources. This is done by sending a large amount of requests simultaneously by attacker's host called flooding to forbid the services to its legitimate users. The target host is either respond poorly or it crashes. DDoS is a propagation of DoS. In Dos attack there is one attacker host to launch the attack to one victim host. But DDoS has the very destructive power to harm the sever than DoS. Handling of DoS is easier than DDoS. An arsenal of computers called botnets are used to perform a DDoS attack. These computers of botnets are employed through the use of viruses, Trojan horses etc. It is very difficult to find the original attacker because of sending spoofed IP addresses by botnets which are under control of attacker. The main target of the DDoS attacks are credit card, banks, websites, social sites. The incentives of the attacker includes financial gain, economical gain,revenge ,competition . The purpose the attacker is to consume the bandwidth and services. DDOS attacks can be launched in two different ways. These are direct ddos attack and indirect ddos attack. In direct DDoS attack the traffic is send directly to the botnets to launch an attack against victim. In indirect DDoS attack the traffic is send indirectly to the botnets to launch an attack .DDoS attacks are very dangerous for the network security.

A. ARCHITECTURE OF DDOS ATTACK

The Architecture consists of main attacker's host and three compromised hosts to launch the coordinate attack through the internet by sending a large number of requests through the network. The network of the target server gets busy and then it will not respond to its legitimate users and will not able to provide services to the other actual hosts.

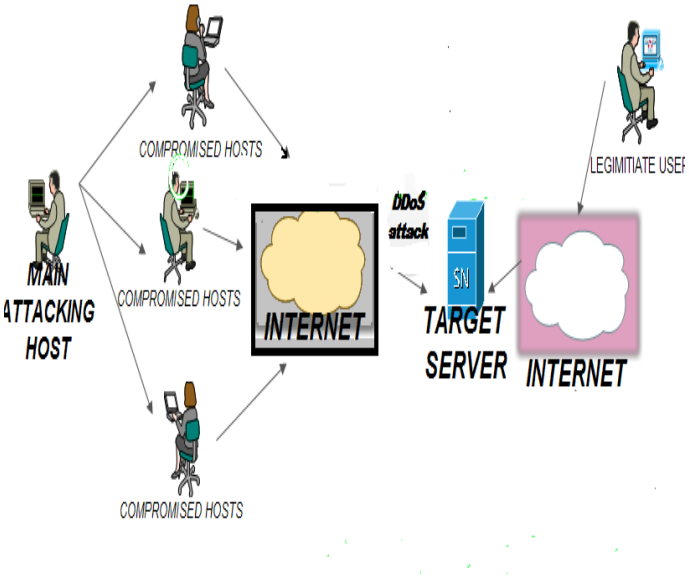

Fig1. Architecture of DDoS attacks

II. LITERATURE REVIEW

Yang Xiang (2011)[1] has discussed about the most destructive type of attack known as low rate DDoS attacks. Two new approaches generalized entropy and information distance approaches are considered to detect the low rate ddos attacks. The previous approaches Shannon entropy and kullback-liebler distance was also studied in this paper and Compare it with the new approaches. The alpha value of generalized entropy and information distance metric was adjusted to improve the detection rate. With the help of these two new metrics, it would be easy to differentiate between the legitimate traffic and the normal traffic. At last IP trace back method is used to find source of the attacker .This method is useful to stop the attack by examining the attacker.so this paper shows that the proposed technique is used to detect the attack low rate traffic and more reduce the attack rate.

M.Vijaylakshmi, Dr.S.Mercy Shalinie, A.Arun Pragash (2012)[2] has studied that IP traceback is the appropriate approach to find the source of the attack. This metric was used to detect the DDoS attacks in the network by tracing the router which is nearer to the incoming traffic. The tracing of the router is done by packet marking scheme in which each incoming packet is marked and then send to the network. This detection technique is used when the attacker launches the attack by sending spoofed IP addresses. These kind of attacks is performed in network and application layer. Proactive traffic shaping and reactive filtering mechanism were also used. It is used to evaluate the efficiency of the system and in this paper the test bed used was NTRO sensor smart and secure environment. The main contribution of this paper is to determine the attacker.

onowar H.Bhuyan (2012)[8] has studied about the issues and the various challenges of the detection schemes which come under DDoS Attacks. The motive of this paper is to compare all the available techniques of detection. This study showed that all the methods of detection are not able to satisfy all needs of the network security or defense. Some possible solutions are also considered in this paper against DDoS attacks. Description of various kinds of tools is also described integrate its protocol and type of attack the tool can launch. This paper gives the revision of all the detection methods, and tools to perform an attack.

Ahmad Sanmorino (2013) [3] has proposed a pattern of matching detection technique that overcome the drawbacks of the other detection techniques of the DDoS attacks. Traffic flows through the network is checked based on the specified pattern and can easily find that packet is malicious or not. This technique of detection has an advantage of lower cost of infrastructure since it only uses routers and switches which exist already. It does not use high technology resources such as multicore CPU technology. This paper shows three topological environment which consists of 3 phases. In the Ist environment normal behavior of the traffic was shown, In the second phase unsecured network with attacks launched on it was shown. In the third phase handling of the attack was shown with firewall and successful dropout the packets.

PyungKoo(2013) [5] has studied that pseudo states in the router are one of the best method to protect the services. As routers, switches and other devices on the network are not much capable to differentiate between all the packets.so the service oriented based detection mechanism using pseudo state (SDM-P) is used to counter the attack packets before it falls into the network. A Hash key algorithm is used to evaluate the performance of this detection scheme. In other techniques the attack is detected when the services accommodation gets down, but proposed technique is used for the detection before entering the data packets. The implementation has done on the NS-2 platform to identify the difference between the packet whether it is legitimate packet out the attacker's packet.

Muhammad Aamir (2013) [4] has studied that with the increasing need of information technology, network security is one of the major issue as number of DDoS attacks are increasing at higher pace The various techniques of DDoS attacks and Defense of DDoS attack on the FTP server. The various parameters are observed using the opnet test bed environment. Observation parameters are a utilization of CPU, TCP Delay, processing time and show the effect of DDoS attacks on these parameters. As the size of botnet increases, the effect on these parameters also increases. 3 botnet sizes 50,100,200 was considered to launch the attack in this paper. How FTP server gets affected has shown in this paper.

Saman Taghavi (2013) [6] has presented about DDOS flooding attack as it is one of the challenging issue to prevent the network security. In this type of attack an armies are set up to launch an attack. Various computers are hired by an attacker, it is called botnets or Zombies, the coordinated attack is performed by all the hired computers. The appropriate defense mechanism is required to bar the DDOS flooding attacks. The purpose of this paper is to seek about DDOS flooding trouble and the various steps to encounter it. The Study is about the consideration of previous counter steps to handle the DDOS Flooding attacks. The main consideration of this paper is to give the survey of traditional and current handling mechanism which helps the research community to develop their DDOS flooding handling problem when or after attack launched.

IlkerOzcelik (2013) [7] has presented about the detection approach on Denial of Services. The detection is based on the anomaly based metrices. The Cumulative Sum (Cusum) approach has applied to detect the effect of the attack on the network. This algorithm is performing at high and low bandwidth of the network. The main purpose of this work is to show the better detection results with the cusum algorithm as it reduces the utilization of the network. This whole work was performed by using the background traffic in the paper's scenario

III. ATTACK TECHNIQUES

DDoS attacks are classified in two ways. These are network based attacks and application based attacks

A Network Based Attacks

1) Tcp Syn Flood

Communication between two nodes required a handshake mechanism for the connection establishment. In handshake mechanism the host which wants to communicate sends the SYN packet to the server host then the server host responds by sending the reply message with the acknowledgement packet. Again the hosts send the SYN packet to communicate with the server by establishing a full connection as shown in fig 2 (a) but in this type of attack the attacker continuously send the sync packets with spoofed IP addresses to the server.The Spoofed IP address is the address which does not exist. After receiving the request by client ,server responds by sending the acknowledgment(ack) packet to the spoofed IP addresses. But there is no actual nodes address present, so the acknowledgement rep packet will never come and the server will wait for a long time until it sends connection timeout messages shown in fig 2 (b).

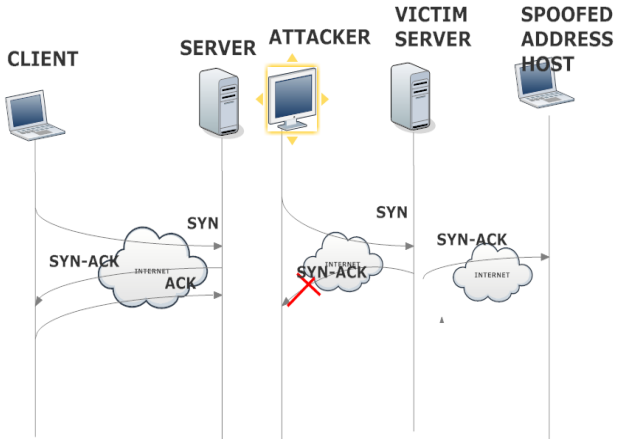

Fig 2(a) Handshake mechanism packet flow (b)TCP SYN ATTACK

2) Icmp Smurf Flood

In this type of attack, the attacker will take the IP address of the victim's IP address as the source and send a number of ICMP echo requests to all the computers which are located on that network. All computers on that network will receive the request packet and respond to the victim with ICMP echo replies and congestion occurs on the victim's network. The victim will no further capablity to provide services.

3) UDP Flood

As there are lots of new techniques now available to defend against TCP and ICMP Flood attacks, the attacker finds a new method to launch the attack. The Attacker sends a huge amount of UDP packets to the victim host.

B Application Based Attack

1) *Slow Read Attacks*

The attacker sends actual host user request message to the victim server. The server reply with the response message but attacker read it very slowly to exhaust server's connection. The requests for the legitimate users will be unanswered due to this attack.

2). HTTP Flood

Through HTTP communication a large number of requests will send by attacker to establish a huge number of connections to the server. The Server will not respond to the other actual host clients due to busy processing cycles.

IV. DEFENSE TECHNIQUES AGAINST DDOS ATTACKS

Defense techniques are described in two phases:

Detection and Mitigation

To enhance the security of the network or the server, the attack must have to be recognized and take further step to stop these attacks. Detection can be classified into two metrics.

Signature based detection and anomaly based detection signature based detection: A prespecified pattern of incoming packet are classified into the entrance router or switch on the network, such that incoming packets pattern like its port number, identification number etc are checked and detect the attack.

Anomaly based detection: This metric observe the normal behavior of the traffic and then it will compare the incoming traffic and evaluate the difference between them.

Various techniques and technologies are developed for detecting and handling the DDOS attacks.

A Firewall:

Firewall is the popular security product which is either hardware or software. Firewall control the traffic towards the network. It filters the traffic and decide whether the traffic should be allowed through or they should be denied. This decision is based on the predefined set of rules in the firewall. The main job of the firewall is the prevention from the unauthorized use of data. For this all the records are maintained in the firewall containing all the records of the connections of the packets which are passing through the firewall. A Firewall is used to filter the traffic and allow to establish the legitimate TCP connections. Firewall is placed between two networks as a barrier. Firewall analyzes the real time to detect and also gives information about duration and rate.

B Routers:

Routers are used to filter the traffic and block the unwanted packets. Routers use the Access Control List which is the collection of predefined rules in a router. The denial of the packets from the router is based on source IP addresses or if the packets header does not match with the predefined policies deployed in the router. ACL checks the incoming IP packets. If they belong to the ACL table ,then it forwards the packet otherwise it discards. ACL can also be applied on switches. ACL rules generation method on the router is very less expensive method than others because it do not need of any extra hardware infrastructure cost.

C IP Trace back Mechanism

To find the origin of the attack IP trace back Mechanism is used. In this method Routers which forward the packets carry the information regarding its header and payload such that it can be easy to traverse the route from where the abnormal traffic arrives. There are two methods of IP trace back mechanism which is Proactive and Reactive method. Proactive mechanism is defined as the tracing the information of the packets when they are traversing. The Reactive method is applied after the attack is found.

V. COMPARATIVE STUDY

This comparative study shows that during different years, various and improved security measurements had been developed to mitigate the effect of DDoS attacks. Till this pattern of matching had been used successfully to filter the packets which improve the overall performance.

Table I

Author(s)	Year	Name of paper	Techniques used	Results
Ahmad sanmorino,et al.	2013	DDoS Attack Detection Method based on Pattern of the Flow	Pattern Matching for Detection,Firewall for mitigation	Successfully filter the packets and dropped the attacker's packet
Ilker Ozcelik,et al.	2013	DoS Detection is Easier Now	Cumulative sum (cusum)algorithm	Better detection of Dos as the network utilization decreases
PyungKoo Park,et al.	2013	Service-Oriented DDoS Detection mechanism using pseudo state in a flow router	Detection Based on Pseudo State in flow router, Bidirectional hash key algorithm	Differentiate between the legimitiate and attacker's traffic
Muhammad Aamir,et al.	2013	Study and Performance Evaluation on Recent DDoS Trends of Attack and Defense	Consideration of FTP Sever under DDoS Attacks	Give an idea that DDoS attacks on Application Layer are Increasing
Saman Taghavi,et al.	2013	A Survey of Defense Mechanisms Against Distributed Denial of Service(DDos) Flooding Attacks	Various Handling Mechanisms of DDoS Flooding Attacks	Overview of various Mechanisms of Defense DDoS Flooding Attacks
M.Vijayalakshmi ,et al.	2012	IP Traceback System for Network and Application Layer Attacks	Traceback System,Anomoly Detection based on New Payload and New Header,Packet Marking scheme	Find the attacker after Detecting the Attacks,Bring down the Attack Traffic
Yang Xiang,et al.	2011	Low-Rate DDoS Attacks Detection and Trace back by Using New Information Metrics	Generalized entropy metric and Information Distance metric	Detection of Low rate DDoS Attack and False Positive Rate is Reduced
Kevin Hattingh,et al.	2011	DoS! Denial of Service	Virtual Network Creation,Wireshark	Demonstration of Denial of service and Response plan List is created

VI. CONCLUSION

As Attack techniques continue to lead, the companies today have to face various threats. DDoS attacks are increasing day by day and their main aim is to harm the every level in the data center of the organization. Smart Companies take steps not only to defend from the attacks ,but also find the origin of the attack. This article attention is on the matter that to take effective counter steps against DDoS attacks.

It is shown in the paper that there are various detection and mitigation mechanisms to prevent the network from various kinds of DDoS attacks. In future some different techniques can be used to detect and mitigate the effect of DDoS attack, like detection technique integrated pattern of matching method with wire shark and mitigation using Access control lists(ACL) with trace route or using a Firewall. So this paper give a survey about various kinds of DDoS attacks and how to handle them. It helps to give a basic idea of the techniques to the reader who wants to get started his research work from network security.

REFRENCES

[1]. Yang Xiang, Ke Li, and Wanlei Zhou, Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics, *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 2, JUNE 2011*.

[2]. Vijayalakshmi, Shalinie, Arun Pragash, IP Traceback System for Network and Application Layer Attacks, *Recent Trends In Information Technology (ICRTIT), 2012 International Conference*

[3]. Ahmad Sanmorino1, Setiadi Yazid2, DDoS Attack detection method and mitigation using pattern of the flow,*2013 International conference of Information and communication technology(ICoICT)*

[4]. Muhammad Aamir , Muhammad Arif, Study and Performance Evaluation on Recent DDoS Trends ofAttack & Defense, *I.J. Information Technology and Computer Science, 2013, 08, 54-65*

[5]. PyungKoo Park, SeongMin Yoo, Chungnam Nat, Service-Oriented DDoS Detection Mechanism Using Pseudo State in a Flow Router , *2013 International Conference on Information Science and Applications (ICISA)*

[6]. Saman Taghavi Zargar, Joshi, Member, IEEE, and David Tipper,A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks, *IEEE COMMUNICATIONS SURVEYS & TUTORIALS, ACCEPTED FOR PUBLICATION* (2013)

[7]. Ilker Ozcelik, Yu Fu , Richard R. Brooks ,DoS Detection is Easier Now, *2013 Second GENI Research and Educational Experiment Workshop.*

[8] Monowar H. Bhuyan1, H. J. Kashyap1,D. K.Bhattacharyya, Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions, *The Computer Journal first published online March 28, 2013* ,