IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 3, Ver. IV (May-Jun. 2016), PP 68-76
www.iosrjournals.org

Survey Of DDoS Attacks Based On TCP/IP Protocol Vulnerabilities

Saket Acharya[1], Namita Tiwari[2]
[1](Department Of Computer Science Engineering,MANIT Bhopal,India)
[2](Asstt. Professor,Department Of Computer Science Engineering,MANIT Bhopal,India)

Abstract: *Distributed denial-of-service (DDoS) attacks are one of the key threats and perhaps the toughest security problem for today's Internet.Distributed Denial of Service (DDoS) attack has become a stimulating problem to the availability of resources in computer networks.With brief or no advance warning, a DDoS attack can easily drain the computing and communication resources of its victim within a short period of time. In this paper, DDoS attacks based on the protocols vulnerabilities in the TCP/IP model, their impact on available resources viz CPU,memory,buffer space is investigated. This paper aims to provide a better understanding of the existing tools,methods and comparative analysis of them,and defense mechanisms.*

Keywords: *Cyber-attack, Cyber security,DDoS Attack,DDoS Attack Tools, Mitigation,Vulnerability,*

I. Introduction

Distributed Denial of Service (DDoS) attacks pose a severe problem in the Internet, whose impact has been well exhibited in the computer network literature. The main goal of a DDoS is the disruption of services by attempting to reduce access to a machine or service instead of depraving the service itself..In DDoS attack, the attacker feats any vulnerability in the protocols at different layers.In this way it compromises different systems. These systems are called zombies or bots.[1]DDoS attacks are comprised of packet streams from disparate sources.The DDoS tools do not require technical knowledge to execute them. Hence DDoS are becoming effortless to launch and difficult to detect.DDoS traffic creates a heavy congestion in the internet and hinders all Internet users whose packets cross congested routers.In this paper, we studied ddos attack types at various TCP/IP protocols,application level ddos attack tools ,compare existing GUI tools so that we know the trend of attacking method used by the attackers to launch an attack and various defense mechanisms.DDoS attacks never try to break the victim's system, thus making any old security defense mechanism inefficient. The main goal of a DDoS attack is to cause destruction on a victim either for personal reasons, either for material gain, or for popularity.[2]Application level attacks overflow a computer with such a high volume of connection requests, that all available operating system resources are disbursed, and the computer can no longer process legitimate user requests.

II. Ddos Architecture

A Distributed Denial of Service Attack is encompassed of following terms, as shown in Fig. 1:

- The attacker.
- The handlers or masters, which are conceded hosts with a special program running on them, capable of controlling multiple agents.
- The attack daemon agents or zombie hosts, who are conceded hosts that are running a special program and are responsible for generating a stream of packets towards the intended victim.
- Victim.

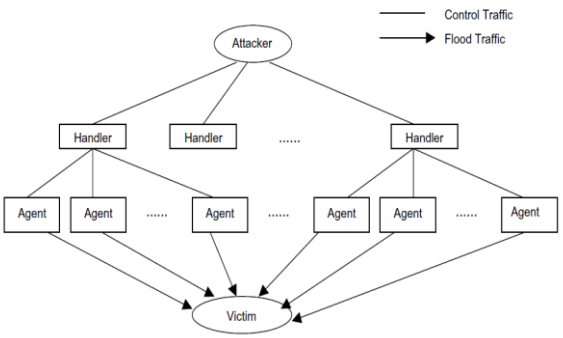

Fig. 1: DDoS Architecture

Following steps take place during DDoS attack:

1. The attacker chooses the machines that have some susceptibility that the attacker can use to gain access to them. Using these machines, the attacker performs attack.
2. The attacker exploits the vulnerabilities of the agent machines and embeds the attack code. When participating in a DDoS attack, each agent program uses only a small amount of resources (both in memory and bandwidth), so that the users of computers experience minimal change in performance.
3. The attacker communicates with handlers to identify which agents are running and when to schedule attacks. In case of direct attack, the attacker directly performs the attack without handlers.

III. Ddos Attacks Classification

On the basis of TCP/IP Protocol vulnerabilities, DDoS attacks are classified as shown in Fig.2

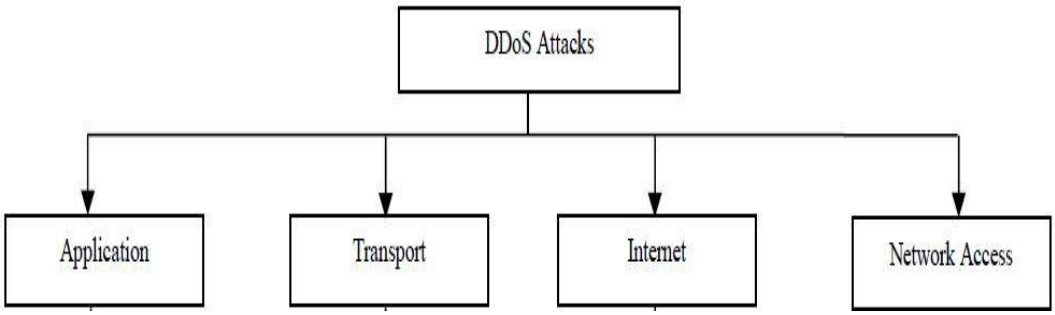

Fig. 2: Classification of DDoS Attacks Based On TCP/IP Vulnerabilites

A. Application Layer DDoS Attacks: An application layer DDoS attack is prepared mainly for explicit targeted purposes, including disrupting transactions and access to databases. They require a smaller amount of resources and often supplement network layer attacks. An attack is masked to look like legitimate traffic, except it targets particular application packets. The attack on the application layer can dislocate services such as the retrieval of information or search function as well as web browser function, email services and photo applications.

Following are some application layer DDoS attacks:

a) HTTP/HTTPS Flooding: HTTP flood is a type of Distributed Denial of Service (DDoS) attack in which the attacker feats HTTP GET or POST requests which looks real to attack a web server or application. HTTP flood attacks are volumetric attacks, frequently using a botnet "zombie army"—a group of Internet-connected computers, each of which has been spitefully taken over, usually with the help of malware like Trojan Horses. An erudite Layer 7 attack, HTTP floods do not use deformed packets, spoofing or reflection techniques, and involve less bandwidth than other attacks to bring down the targeted site or server. This attack is disgrading in nature.

b) FTP Flooding: In this type of attack, the attacker exploits apparently-legitimate FTP requests to outbreak a FTP server or application. This attack is disgrading in nature.

c) Telnet DDoS: In this type of attack, the attacker distantly login into target system and the perform attack. This attack is disgrading in nature.

d) Mail Bombs: Attacker sends a immense amount of e-mail to a specific person or system. A huge amount of mail may solely fill up the recipient's disk space on the server. This attack is degrading in nature.

e) SQL Slammer: It is a computer worm that triggered a denial of service on some Internet hosts and intensely slowed down general Internet traffic.

f) **DNS Flood:** DNS floods are endeavored to exhaust server-side assets (e.g., memory or CPU) with a flood of UDP requests, created by scripts running on several conceded botnet machines.

B. Transport Layer DDoS Attacks: These types of attacks are usually encompassed of volumetric attacks that aim to devastate the target machine, denying or consuming resources until the server goes offline. In these types of DDoS attacks, malicious traffic (TCP / UDP) is used to flood the victim.The major categories of DDoS attacks under transport layer are following:

a) SYN Flooding: It is a form of denial-of-service attack in which an attacker sends a subsequence of SYN requests to a target's system in an attempt to ingest enough server resources to make the system unresponsive to legitimate traffic. It is generally degrading in nature. It is shown below:

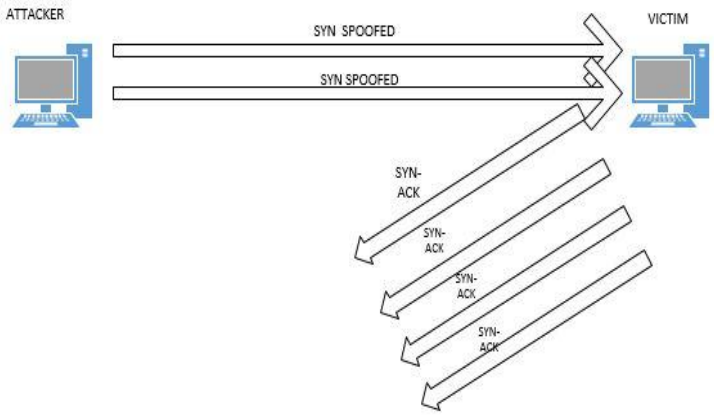

Fig 3: DDoS SYN Flooding

b) UDP Flooding : The attacker sends UDP packets, naturally big ones, to single destination or to random ports.It is generally disruptive in nature.It is shown below:

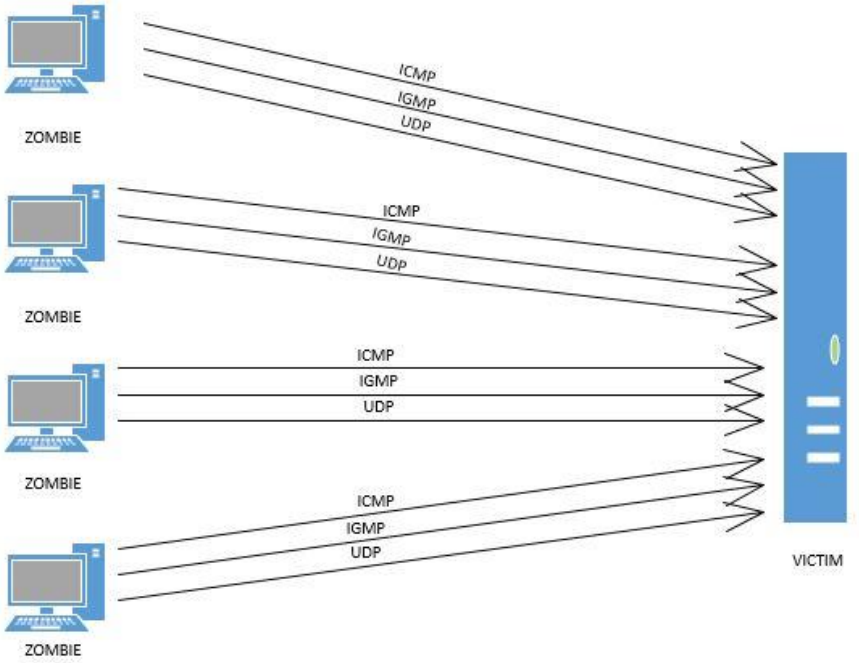

Fig 4: UDP Flooding

c) **TCP Null Flooding:** In this type of attack the invader send packets that have the no TCP segment flags set (six possible) which is invalid. This type of section may be used in port scanning.It is generally degrading in nature.Following are the six TCP flags :

- URG (U) – indicates that the Urgent pointer field is noteworthy
- ACK (A) – indicates that the Acknowledgment field is noteworthy. All packets after the initial SYN packet sent by the client should have this flag set.
- PSH (P) – Push function. Asks to push the buffered data to the receiving application.
- RST (R) – Reset the connection
- SYN (S) – Synchronize sequence numbers. Only the first packet sent from each end should have this flag set. Some other flags and fields modify meaning based on this flag, and some are only valid for when it is set, and others when it is clear.
- FIN (F) – No more data from sender.

C. Internet Layer DDoS Attack: These types of attacks occur due to vulnerability in internet layer protocols of the TCP/IP model. They are following:

a) **Smurf Attack :**In this type of attack, large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP Broadcast address. This attack is disgrading in nature. It is shown below :

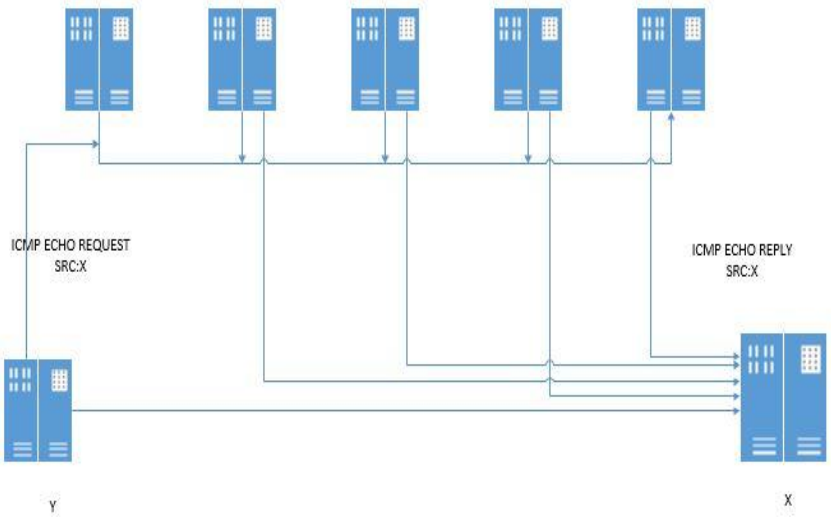

Fig. 5: Smurf Attack

b) **Fraggle Attack :**It is similar to smurf attack but insted of ICMP packets,large numbers of UDP packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP Broadcast address.This attack is disgrading in nature.

c) **TearDrop Attack :**It involves sending fragmented packets to a target machine. Since the machine receiving such packets cannot reassemble them due to a bug in TCP/IP fragmentation reassembly, the packets overlap one another, crashing the target network device.This attack is disgrading in nature.It is shown below :

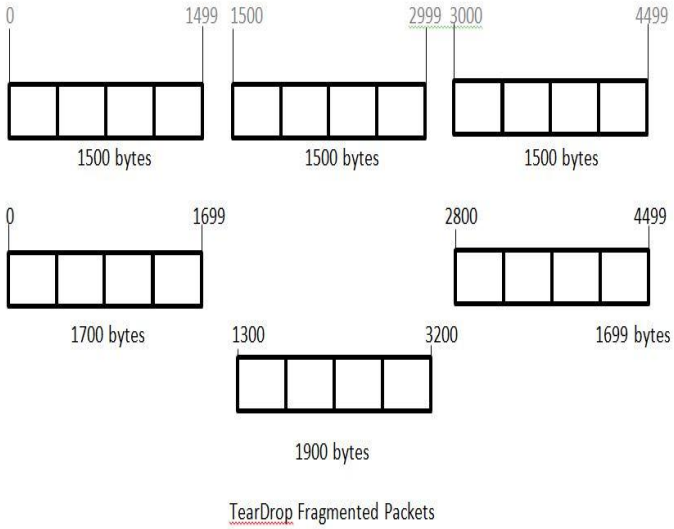

Fig. 6: Tear Drop Attack

In fig 6. there are three normal fragmented IP packets are having size 1500 bytes whereas the teardrop fragmented packets have varying sizes of 1700 bytes,1699 bytes and 1900 bytes respectively.When these teardrop fragmented packets are send to viictim machine,the machine will remain busy in assembling these fragments and will end up in denying services to other legitimate clients.Since these packets have different sizes,the machine is not able to reassemble these packets.

d) **ICMP Flooding:** Attacker overwhelms the victim with ICMP Echo Request (ping) packets.The attacker hopes that the victim will respond with ICMP Echo Reply packets, thus consuming both outgoing bandwidth as well as incoming bandwidth. If the target system is slow enough, enough CPU cycles can be consumed and the user notices a significant slowdown.This attack is disgrading in nature.It is shown below :

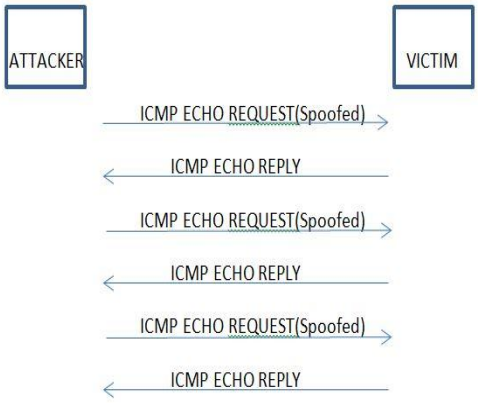

Fig.7: ICMP Flooding

D. Network Access Layer DDoS Attack: These type of attacks exploit the weakness of network layer and its protocols.Followng are the major types of DDoS attacks falls under this category:

a) **VLAN Hopping:** VLAN hopping is a computer security exploit, a method of attacking networked resources on a Virtual LAN (VLAN). This attack is disruptive in nature.As shown in fig 9. the attacker launches VLAN hopping attack by spoffing Dynamic Trunking Protocol(DTP) messages and causes the switch to enter trunking mode.

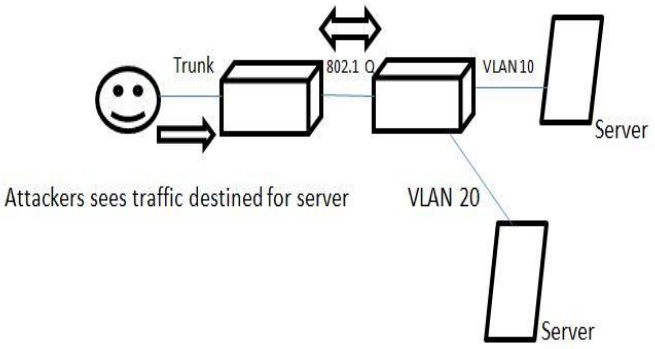

Fig.8: VLAN Hopping

b) **MAC Flooding :** MAC flooding is a method engaged to compromise the security of network switches.This attack is disgrading in nature.

c) **DHCP Attack :** Attacker avert hosts from gaining access to the network by refuting them an IP address by overwhelming all of the available IP address in the DHCP Pool.This attack is disruptive in nature.It is shown below :

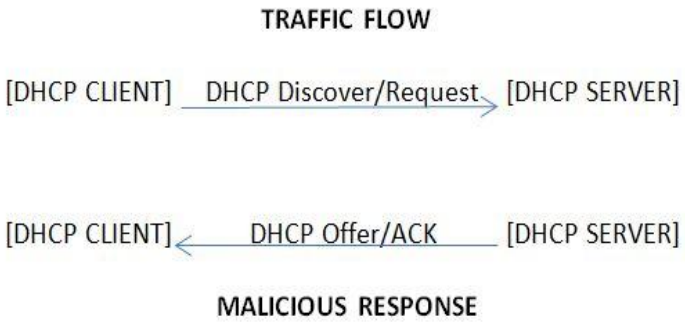

Fig.9: DHCP Attack

d) **ARP Spoofing:** ARP spoofing is a type of attack in which a malevolent actor sends falsified ARP (Address Resolution Protocol) messages over a local area network. This attack is disgrading in nature.Fig. 10 shows normal ARP traffic pattern. The sniffer snorts the traffic and sends malicious ARP messages to the target computer as shown in fig.11

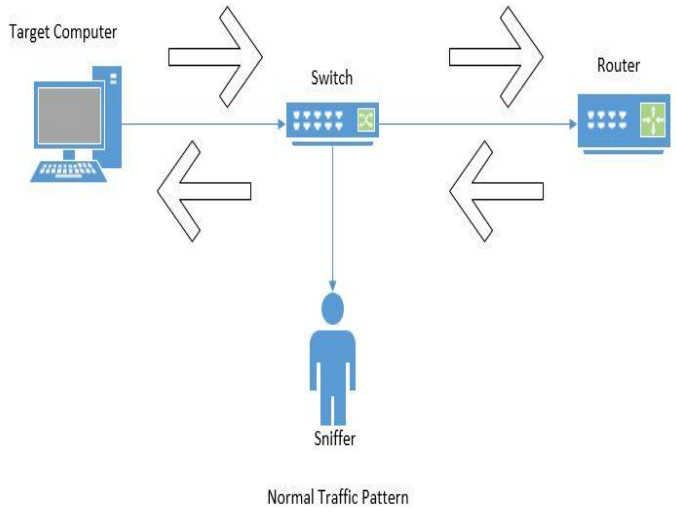

Fig.10 ARP Attack Normal Traffic

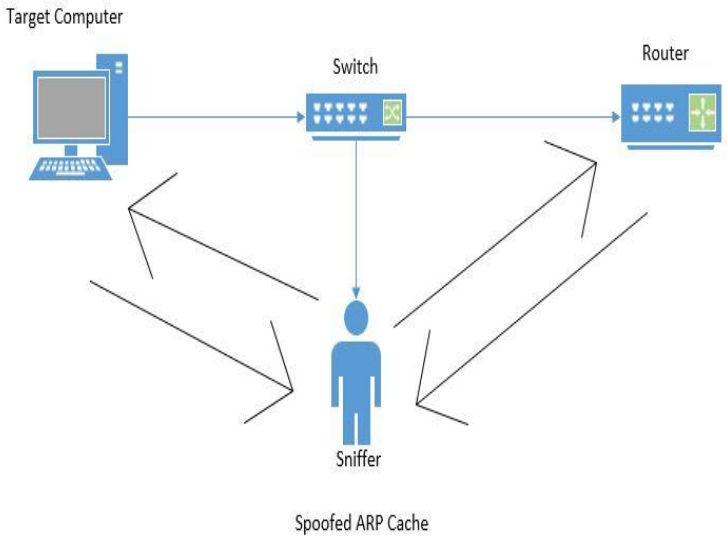

Fig.11: ARP Attack Malicious Traffic

Following are the reasons for speedy growth of Application Layer DDoS Attacks:

- These attacks are some of the most difficult attacks to alleviate against because they impersonate human behavior as they interrelate with the user interface.
- Attacker requires less resources and needs only information of susceptible IP and ports.
- Difficult to stop because they look authentic to classic firewalls which let them pass freely.
- Defending this classification of attack is difficult because network devices like switches,routers etc have no security at application layer.

IV. Existing Tools And Comparison

A. **Low Orbit Ion Canon(LOIC)**: LOIC performs a denial-of-service (DoS) attack (or when used by many individuals, a DDoS attack) on a target site by flooding the server with TCP or UDP packets with the intent of disrupting the service of a precise host. People have used LOIC to connect intended botnets.LOIC unveil a DDoS attack by using the various flooding method e.g. TCP, UDP and ICMP in order to harm the resources such as CPU time, storage and bandwidth of the compromising host.[3]

B. **Mstream:** The purpose of the tool is to enable impostors to utilize multiple Internet connected systems to launch packet flooding denial of service attacks against one or more target systems. The Mstream tool uses tricking method for attacking the target host. For example using small TCP Acknowledge packets to attack the victim site. Mstream tool uses TCP ACK floods that, as a response, can marsh the information used by routing methods in switches.[4]

C. **Switchblade:** It provides three dissimilar types of denial of service situations that can be tested from a single machine[5]

- SSL Half Connect: This type of attack works by driving the server to do tasks that take up a lot of resources over and over again until it runs out of resources to do that task with (often RAM and CPU power) and then clatters or stops doing its envisioned function.
- HTTP Post Attack: The attacker creates hundreds or even thousands of such connections, until all resources for arriving connections on the server (the victim) are used up, hence building any further (including legitimate) connections difficult until all data has been sent.
- Slowloris: This attack works by introducing multiple connections to the targeted web server and keeping them open as lengthy as possible. It does this by constantly sending restricted HTTP requests, none of which are ever accomplished. The confronted servers open more and connections open, waiting for each of the attack requests to be accomplished.

LOIC	**MSTREAM**	**SWITCHBLADE**
LOIC launch a DDoS attack by using the various flooding method e.g. TCP, UDP and ICMP in order to damage the resources such as CPU time, storage and bandwidth of the compromising host.	Mstream tool uses TCP ACK floods that, and gains the Information used by routing methods in switches.	OWASP Switchblade is a denial of service tool used for testing the availability, performance and capacity planning of a web application to be proactive about this type of risk condition.
Types of flooding provided by it are TCP SYN, UDP, ICMP.	It provides TCP SYN , ICMP and RST	It provides UDP, TCP SYN, ICMP
Disruptive in nature.	Degrading in nature	Disruptive in nature

Fig.12: Comparison of DDoS Tools

V. Defense Mechanisms

1. **Ingress/Egress Filtering:** Ingress filtering is an tactic to set up a router such that to prohibit incoming packets with illegitimate source addresses into the network[6].It averts source IP address spoofing of Internet traffic.This mechanism can considerably reduce the DoS attack by IP spoofing if all domains use it. Sometimes legitimate traffic can be rejected by an ingress filtering using Mobile IP[7] **Egress filtering** [8] is an outbound filter, which certifies that only assigned or allocated IP address space leaves the network. Egress filters do not help to save resource wastage of the domain where the packet is originated but it protects other domains from possible attacks.

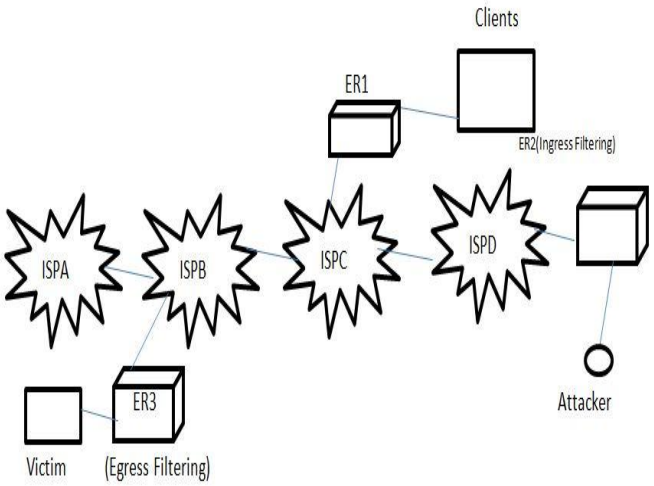

Fig.13: Network Ingress/Egress Filtering

2. **Route Based Distributed Packet Filtering:** This methodology is capable of filtering out a huge portion of deceived IP packets and averting attack packets from accomplishing their targets as well as to help in IP traceback. Route-based filters use the route statistics to filter out spoofed IP packets, making this their main modification from ingress filtering. If route-based filters are partially positioned,a synergistic sifting effect is possible, so that spoofed IP flows are prohibited from reaching other Autonomous Systems.
3. **History Based IP Filtering:** According to this method the edge router disclose the incoming packets according to a pre-built IP address database. The IP address database is based on the edge router former connection history. This scheme is healthy, does not need the support of the whole Internet community, and is appropriate to a wide variety of traffic types and requires little arrangement.[9]
4. **Load Balancing:** Load balancing[10] is a simple method that enables network providers to upsurge the provided bandwidth on serious connections and prevent them from going down in the occurrence of an attack. Additionally the duplication of servers can be done for guaranteed protection during a DDoS attack.
5. **Intrusion Detection:** Intrusion detection systems sense DDoS attacks either by using the database of well-known signatures or by recognizing glitches in system behaviors.[11]Anomaly detection trusts on detecting behaviors that are irregular with respect to some normal standard. Following are some anomaly detection systems and methods have been developed to detect the weak signs of DDoS attacks:

- **Signature Based**
- **Pattern Based**

6. **Deflection:** It includes the following techniques:

- Honeypots: They are the technologies that are not supposed to receive any legitimate traffic. Traffic designed to a honeypot is possibly an ongoing attack that can be investigated to expose vulnerabilities targeted by attackers.
- Attack Study: Honeypots have special software which regularly collects data about the system performance for forensic analysis. Honeypots are permitted to be compromised and behave as a normal machine, noiselessly capturing valuable information about the activities of attacker.
- Roaming Honeypots: Unlike classic honeypots,these can be located at service-level, where the locations of honeypots are unexpectedly changing within a pool of back-end servers.

7. **Data Logging:** Vital information can be obtained from the network components (such as firewalls, packet sniffers, log-servers) as these components registers the incident details about the attack, during forensics analysis. If attacker has done significant financial damage,law enforcement policies can also be assissted.
8. **Congestion Triggered Packet Filtering:** In this technique,a subset of packets which are released due to overcrowding is selected for statistical analysis. If any problem is shown by the statistical results, a signal is sent to the router to filter the detrimental packets.
9. **IP Traceback:** IP traceback hints the attacks back towards their origin, so that the attacker can be validated and mysterious routes can be detected, as well as path categorization. Key factor that makes IP traceback challenging is the homeless nature of Internet routing. Other problem can be lack of source liability in the TCP/IP protocol.[11] At a very simple level, the administrator of the network under attack places a call to his Internet Service Provider (ISP) requesting for the direction from which the packets are coming. Since the manual traceback is very tiresome, process computerization is needed.**Probabilistic packet marking (PPM)** is used to interpret partial route path information proficiently and include the traceback data in IP

packets. This technique can be functional during or after an attack, and it does not need any supplementary network traffic, router storage, or packet size increase. Even though it is not dreadful to reconstruct an well-ordered network path using an unordered collection of router samples, it needs the victim to obtain a large amount of packets.

VI. Conclusion

Internet has touched such places where people could not even think that such kind of network exists which offer any possibly imaginable information.With the increased use of internet, a huge number of attackers are keeping an eye to launch attacks to get entrée to critical information and even crash the complete servers.There are systems whose vulnerabilities can be easily exploited by the attackers and they use them to perform DDoS attacks.We provide a review on DDoS attacks classified according to vulnerabilites in the TCP/IP protocols.We also provide a review on common DDoS attack tools and their comparison.DDoSattacks are difficult to remove completely but they can be prevented and also a review on common DDoS defense mechanisms is given.

References

[1]. Christos Douligeris , Aikaterini Mitrokotsa, DDoS attacks and defense mechanisms: Classification and State-of-the-art,IEEE Journal, 2003, 1-5
[2]. Khan Zeb, Owais Baig, Muhammad Kamran Asif, DDOS Attacks and Countermeasures in Cyber Space,IEEE Journal,2015,1-10
[3]. Astha Keshariya and Noria Foukia.,DDoS Defense Mechanisms: A New Taxonomy,IEEE Journal,2013,4-8
[4]. Mohammed Alenezi, Martin J Reed,Methodologies for detecting DoS/DDoS attacks against network servers,IEEE Journal,2012,3-9
[5]. Abdulaziz Aborujilah,Shahrulniza Musa,Detecting TCP SYN based Flooding Attacks by Analyzing CPU and Network Resources Performance,IEEE Journal,2014,1-6
[6]. OWASP Switchblade Tool,HTTP Post,Available:[Online] :https://www.owasp.org/index.php/OWASP-HTTP-Post-Tool,2015
[7]. Bharti Nagpal,Pratima Sharma,Naresh Chauhan,Angel Panesar,DDoS Tools: Classification, Analysis and Comparison,IEEE Journal,2015,4-10
[8]. Anh Le, Ehab Al-Shaer, Raouf Boutaba,On Optimizing Load Balancing of Intrusion Detection And Prevention Systems,IEEE Journal,2008,1-6
[9]. Ioannis Koniaris, Georgios Papadimitriou, Petros Nicopolitidis, Mohammad Obaida.,Honeypots Deployment for the Analysis and Visualization of Malware Activity and Malicious Connections,IEEE Journal,2014
[10]. Ping Du, Akihiro Nakao,DDoS Defense Deployment with Network Egress and Ingress Filtering,IEEE Journal,2010,1-5
[11]. Masahito Yamana,Katsuhiro Hirata,Hiroshi Shimizu,Simulation Of IP Traceback For DOS Attack,IEEE Journal,2005,1-8