ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

# Scrutiny of DDoS Attacks Defense Mechanisms

[I]Ms. Diksha Kale, [II]Prof. Vijay Bhosale
M. E. (Computer), MGM College of Engineering and Technology,
Dept. of Computer Engineering, MGM College of Engineering and Technology
Email : [I]dikshakale88@gmail.com

**Abstract**
*With the growing use of internet in today's world security is one of the major aspect. And one such security concern is Denial of service attack, rendering computer or network incapable of providing normal services to its users. DDoS is more severe than DoS enhancing capabilities of DoS adding multiple ways at one time. It has capability to exhaust processing and communication resources of victims system without any warning. This paper strongly focuses on classification of DDoS attacks and its Defense Mechanisms. Also, this paper describes significant characteristics of each attack and defense mechanisms. Moreover, paper also outlines the pros and cons of proposed defense schemes. The main aim of this paper is to give clear understanding of DDoS attacks and its counter measures so that one can develop efficient and effective algorithms, procedures or even schemes to counter such attacks.*

**Keywords**
*Amplification, Attack, Defense Mechanisms, Denial-of- Service (DoS), Packet Filtering.*

## I. Introduction

Denial of Service attack denies access of users to particular services. The main aim of DoS attack is to make the system or network unable to provide regular services to its legitimate users by flooding the network bandwidth or connectivity by huge number of packets.

It is very difficult to identify, avoid and minimize impact of DDoS attack due to its many to one configuration. Large numbers of coordinated internet hosts are crooked to utilize some critical resource at target and it denies the service to legitimate users. Attack volume is very much large than system can handle. Attack traffic is in such a way that we cannot distinguish it from normal traffic.

What makes DDoS attacks possible?

- Internet Security is highly dependent
- Difficulty in tracing back the attack to the source
- Limited Resources
- A target rich environment
- Easier to break systems than to make them

Organization of the paper is as follows. Section II describes history and trends in DDoS attack. Section III elaborates overview of DDoS. Section IV discusses classification of DDoS attack and Section V introduces and discusses various defense mechanisms as counter measure against DDoS attack. Section VI concludes the paper and suggests future directions.

## II. History and trends in ddos attack

The DDoS attacks gained very widespread notoriety and media exposure with the three days of DoS attacks ( Feb 7-11, 2000) that were launched against major internet sites like CNN, Yahoo, EBay and Datek [6].

Multiple attack tools like Trinoo, TFN, StachleDraht and TFN2K were used in these attacks. Some attacking tools are agents based in which agents and handlers know each other's identity while in IRC (Internet relay chat) based attacking tools, communication is done indirectly. Some of the tools that are been practiced are described below.

### A. Trin00

Trin00 was discovered as product of IRC Channel takeover. This attack consists of UDP flood. It does not use Source IP spoofing.

### B. Tribe Flood Network (TFN)

TFN is a mixture of Smurf attack, UDP, TCP SYN Flood and ICMP Flood. Masters and agents communicate with ICMP ECHO REPLY packets, so it is difficult to identify than UDP packets and can easily pass firewall.TFN generates coordinated attacks with IP spoofing.

### C. TFN2K

TFN2K attack agents implement Smurf, SYN, UDP, and ICMP Flood attacks. Supplementary provides encryption of messaging. Targets are violated via UDP, TCP SYN, ICMP_ECHO flood or Smurf attack.

Table. 1 : Comparison Of DDoS Tools [5]

| S. No | Tool Name | Reported In Year | Possible Attacks | Packet Format Used To Launch Attacks | Channel Encryption | Model Used |
|---|---|---|---|---|---|---|
| 1. | Trinoo [36] | February 2000 | Bandwidth Depletion | Udp | Yes | Agent Based |
| 2. | Tfn(Tribe Flood Network) [37] | April 2000 | Bandwidth And Resource Depletion | Udp, Tcp-Syn, Icmp Echo Request, Directed Broadcast | No | Agent Based |
| 3. | Tribe Floodnet (Tfn2k) [40] | June 2000 | Targa And Mix Attack | Udp, Tcp-Syn, Icmp | Yes | Agent Based |
| 4. | Stacheldrahr [38],[41] | June 1999 | Bandwidth And Resource Depletion | Udp, Tcp-Syn, Icmp, Directed Broad Cast | Yes | Agent Based |
| 5. | Mstream [42], [43] | April 2000 | Bandwidth Depletion | Tcp-Ack, Icmp, Tcp-Rst | No | Agent Based |
| 6. | Shaft [44], [45] | November 1999 | Bandwidth And Resource Depletion | Udp, Tcp, Icmp | No | Agent Based |
| 7. | Trinity [46], [47] | August 1999 | Bandwidth And Resource Depletion | Udp, Tcp-Syn, Tcp-Ack, Tcp-Rst | No | Irc Based |
| 8. | Knight [48] | July 2001 | Bandwidth And Resource Depletion | Syn, Udp | No | Irc Based |
| 9. | Kaiten [48] | August 2001 | Bandwidth And Resource Depletion | Udp, Tcp-Syn, Tcp-Push+Ack | No | Irc Based |
| 9. | Owasp Http Post Tool [49] | December 2010 | Resource Depletion, Slow Post, Slow Get | Http | No | Agent Based |
| 1o | Davoset [50] | July 2010 | Resource Depletion | Xss | No | Agent Based |
| 11 | Ufonet [51] | 2013 | Resource Depletion | Web Abuse | No | Agent Based |

## III. Overview Of Ddos

### A. DDoS Architecture

A Distributed Denial of Service Attack is composed of four elements, as shown in Fig.1

- The real attacker.
- The handlers or masters, which are compromised computers with a special program running on them, capable of controlling multiple agents.
- The attack agents or zombie hosts, running a special program generates a stream of packets towards the deliberate victim.
- A victim or target host.

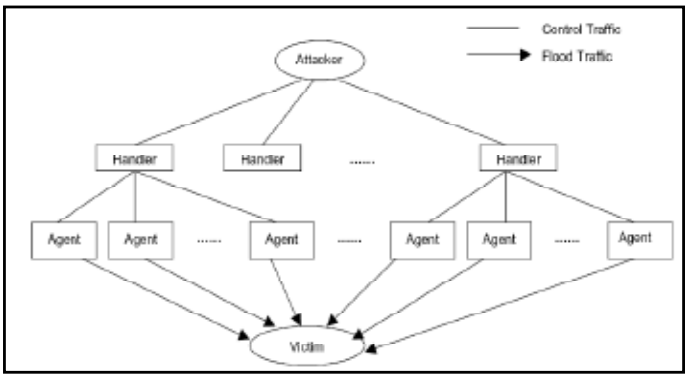


Fig. 1: DDoS Attack Architecture

### B. Strategy steps of DDoS attack

#### (i). Choice of agents

Selection of agent is done here by attacker. Attacker can get an access to agents through some vulnerability. Agent should have huge resources in order to generate high volume of stream of packets.

#### (ii). Compromise

By getting access through the security holes, attacker plant code into agents. Self-propagating tools such as the Ramen worm and Code Red soon automated this phase.

#### (iii). Communication

TCP, UDP, or ICMP protocols are used as communication mediums between attacker-handler and handler-agents.

#### (iv). Attack

Here, attacker launches the attack. The victim, the duration of the attack as well as special features of the attack such as the type, length, TTL, port numbers etc, can be adjusted [3].

## IV. Classification Oo DDoS Attack

There are various ways in which we can classify DDoS attacks, but according to the exploited vulnerability DDoS attacks can be divided in the following categories: flood attacks, amplification attacks, protocol exploit attacks and malformed packet attacks.

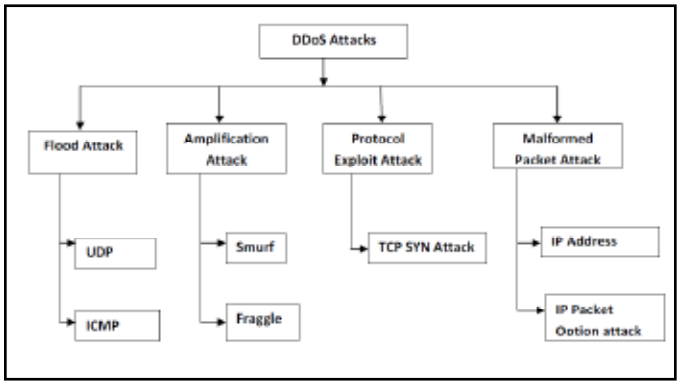


Fig. 2: Classification of DDoS Attack

### A. Flood attack

In this type of attack the victim system bandwidth is congested by sending large volume of IP packet traffic. The impact of packet streams sent by the zombies to the victim system varies from slowing it down or crashing the system to saturation of the network bandwidth [3]. Some of the well-known flood attacks are UDP flood attacks and ICMP flood attack.

#### (i). UDP Flood attack

Achieve saturation of network and bandwidth of victims system by sending large number of UDP packets. In this attack, an attacker sends a UDP packet to a arbitrary port on the victim system. If enough UDP packets are delivered to ports of the victim, the system will go down.

#### (ii). ICMP Flood attack

Internet Control Message Protocol (ICMP) is misused in this attack. During this attack, the agents send large volumes of ICMP_ECHO_ REPLY packets (‘‘ping’’) to the victim. These packets request reply from the victim and this has as a result the saturation of the bandwidth of the victim’s network connection.

### B. Amplification attacks

Broadcast IP Address feature of most of the routers is exploited to reproduce and amplify the attack and send messages to a broadcast IP address. Some well known amplification attacks are Smurf and Fraggle attacks.

#### (i). Smurf attack

Firstly victims IP address is spoofed and with that spoofed IP address, attacker send ICMP echo request traffic to a number of IP broadcast addresses. In IP network, several machines accept ICMP echo requests and respond to the source address, which is the actual target victim. Each of these machines will reply to victims IP address and thus flood victims system with huge traffic.

#### (ii). Fraggle attacks

Fraggle attack uses UDP echo packets instead of ICMP echoes. Fraggle attacks generate even more terrible traffic and can create even more destructive effects than just a Smurf attack.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

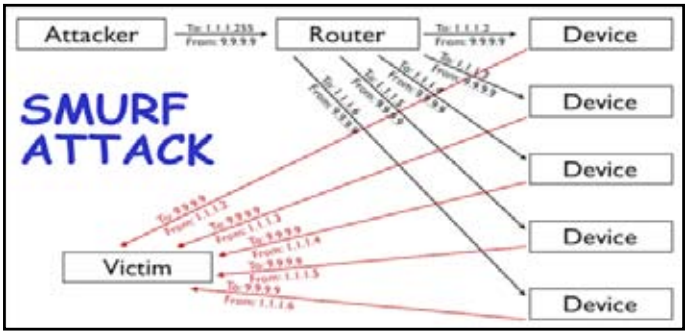

Fig. 3: Smurf Attack

### C. Protocol Exploit attack

Exploit a precise feature or realization bug of some protocol installed at the victim in order to consume excess amounts of its resources. A representative example of protocol exploit attacks is TCP SYN attacks.

### (i). TCP SYN attack

Weakness of the three-way handshake involved in the TCP connection setup is abused in this attack. An attacker starts a SYN flooding attack by sending a large number of SYN packets and never acknowledges any of the replies, essentially leaving the server waiting for the nonexistent ACKs.

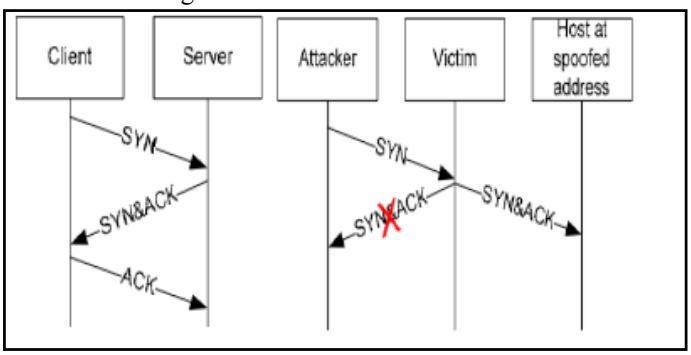

Fig. 4: TCP SYN Attack [4]

### D. Malformed Packet Attack

Improperly formed IP packets are sent from agents to the victim in order to crash the victim system. Types of malformed packet attacks are: IP address attack and IP packet options attack.

### (i). IP address attack

In this attack, the packet contains the same source and destination IP addresses. This has as a result the confusion of the operating system of the victim system and the crash of the victim system.

### (ii). IP packet options attack

During this attack, the optional fields of an IP packet are randomized and all quality of service bits is set to one. This would have as a result the use of additional processing time by the victim in order to analyse the traffic.

## V. DDoS Defense Mechanisms

There are various ways in which DDoS attacks are implemented. Moreover, the automated tools that make the deployment of a DDoS attack possible can be easily downloaded. According to the activity performed during attack discovery, traceback and mitigation DDoS Defense mechanisms can be classified as follows.

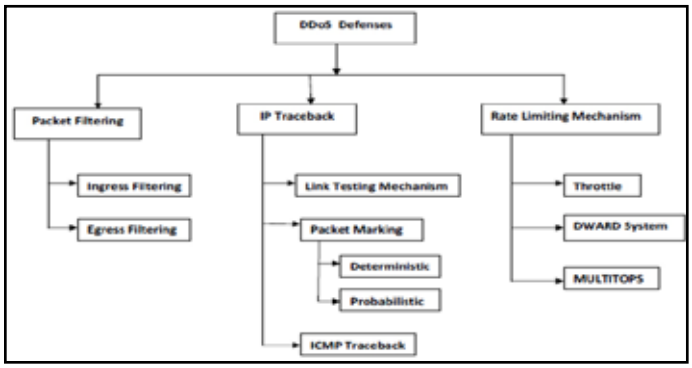

Fig. 5: DDoS Defense mechanisms

### A. Packet filtering Mechanism

It makes difficult to generate an attack with IP spoofing. Attacking packets are stopped, before they aggregate to fatal size. Packet filtering mechanisms can be divided into the following categories.

### (i) Ingress filtering

Ingress filtering is an approach to setup a router such that to disallow incoming packets with illegitimate source addresses into the network. The firewall should apply ingress filtering on the external interfaces and drop all packets that have the source address which belongs to its internal network,

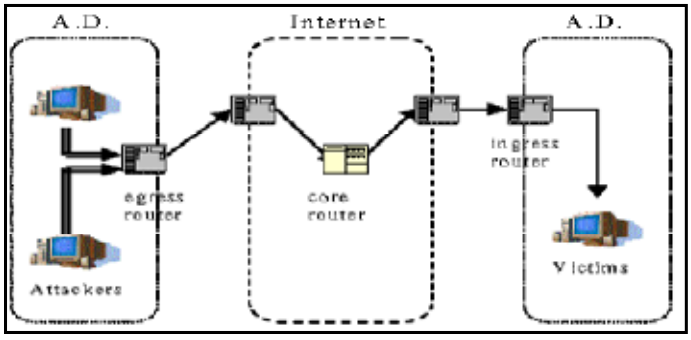

Fig. 6: Ingress & Egress Filtering [4]

### (ii) Egress filtering

An outbound filter, ensuring that only allocated IP address space leaves the network. The firewall drops all the packets that have source addresses that do not belong to their local network. This stops an attacker from using hosts within that network as DDoS agents.

### B. IP Traceback Mechanisms

With the help of IP traceback one can trace the original attacker as well as path used to launch the attack.

### (i) Link Testing Scheme

Each arriving link is tested as probable link of DDoS attack. In this each link is flooded with tremendous traffic and checked for any behaviour change. The idea being that the loaded link will

suffer from the most behaviour change. Link testing mechanisms work best when there is a single attacking source.

### (ii) Packet Marking Scheme

While forwarding packet router insert a mark that is a unique identifier in the packet. As a result the victim can find out all the intermediate hops for each packet by observing the inserted marks [1]. There are 2 variants to this marking scheme.

### 1. Deterministic packet marking scheme

Here router assigns a unique identifier to each arriving packet due to which reconstruction of attack path at victim becomes easy. Drawbacks are large packet header size and router performance overhead.

### 2. Probabilistic packet marking scheme

It uses just a single entry in the IP header to store markings. Each router on the path from the source to the destination writes down its unique identifier in the entry in the packet header with some probability. By writing into the entry, routers overwrite any previous entry that was present there.

### (iii) ICMP Traceback messages

Routers send recently proposed ICMP messages to the destination, with the information about the previous hop. The scheme proposes sending an ICMP message for every 20,000 packets forwarded. Here overhead is minimal but, to collect path information multiple packets should be forwarded.

### 3. Rate Limiting Mechanisms

Limit the rate of packet arrival which matches the criteria for DDoS attacks. It is important that rate limiting mechanisms only limit the rate of malicious packets and do not harm legitimate flows. Examples are as below.

### (i). Throttles

It is used to protect servers from high traffic rates. A server under stress should install rate throttles at a subset of its upstream routers.

### (ii). DWARD Systems

It should be installed at the edge routers for a network. The system monitors the traffic being sent to and from the hosts in its interior.

### (iii). MULTOPS

A MULTOPS data structure can be used for keeping track of attacking hosts or hosts under attack.

### (iv). MANAnet's Reverse firewall

The reverse firewall protects the outside network from packet flooding attacks that originate from within a network.

Table.2 : Comparison of DDoS Defense Mechanisms [5]

| S.No | Defense Mechanisms | Advantages | Shortcomings |
|---|---|---|---|
| 1 | Ingress/Egress filtering at source's edge router | Detect and filter packets with spoofed IPaddresses at the source's edge routers based on the valid IPaddress range internal to the network | Spoofedpackets will not be detected if their addresses are still in the Valid internal IP address range |
| 2 | D-WARD | Stop attack traffic originating From a network at the border of the source network | It consumes more memory space and CPUcycles than some of the network-based defense mechanisms |
| 3 | MULTOPS | Detects and filtersddosflooding attacks based on significant difference between themes of traffic going to and coming from a host or subnet | It uses a dynamic tree structurefor monitoring packet rates for each IP address which makesit a vulnerable target of a memory exhaustion attack |
| 4 | MANAnet's reverse firewall | Limits the rate at which it forwards packets thatare not replies to other packets that recently were forwardedin the other direction | It is manual and requires the administrators' involvement |
| 5 | IP Traceback mechanisms | Traces back the forged IP packets to their true sources ratherthan the spoofed IP addresses | Serious deploymentand operational challenges, most of thetrace back mechanisms have heavy computational, network onmanagement overheads |
| 6 | Packet marking and filtering mechanisms | Mark legitimate packetsat each router along their path to the destination so thatvictims' edge routers can filter the attack traffic | Dependent in part on the strength of the attackers, andwhen it increases, filters become ineffective and they cannotproperly be installed |

## VI. Conclusion

Through review of the all relevance detection and defense mechanisms against DDoS, we can conclude that ways are different in many aspects such as ease of implementation, amount of traffic it drops. Each Mechanism has some features as well as drawbacks that make it suitable or difficult to implement in particular situation. There should be some mechanisms in which features of multiple defenses can be combined to combat DDoS attacks.

## References

[1] *DDoS: Survey of Traceback Methods A.John1, T Sivakumar.2" International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009*

[2] *Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions" Monowar H. Bhuyan1, H. J. Kashyap1, D. K. Bhattacharyya1and J. K. Kalita2*

[3] *"DDoS attacks and defense mechanisms: classification and state-of-the-art"Christos Douligeris *, Aikaterini Mitrokots Computer Networks 44 (2004) 643–666a*

[4] *"Survey on DDoS Attacks and its Detection & Defence Approaches" Nisha H. Bhandari International Journal of Science and Modern Engineering (IJISME) ISSN: 2319-6386, Volume-1, Issue-3, February 2013*

[5] *"A Survey on Latest DoS Attacks: Classification and Defense Mechanisms"Rajkumar1, Manisha Jitendra Nene2 International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 1, Issue 8, October 2013*

[6] *CNN. Cyber-attacks batter Web heavyweights, February 2000. Available at http://www.cnn.com/2000/TECH/computing/02/09/cyber.attacks.01/index.html.*