# DoS and DDoS Attack Types and Preventions

Muhammad Tariq

*Information Security Department, NUST, Pakistan*

*m_tariq23@yahoo.com*

***Abstract.*** **Internet services are commonly facing unpleasant, slow down and denial of service (DoS) attack since its spread and popularity from the mid 90s. Distributed Denial of Service (DDoS) is specialized attack amongst the DoS attacks and more hazardous in nature. . It is carried out at massive level employing army of zombies and disguising identity of the attacker. DDoS have become a real danger / threat for the internet security. The IP spoofing and the destination based routing of the internet has made it more cumbersome to counter this type of attacks. A number of solutions have been proposed to safe guard against DoS attacks but none can claim to be a perfect protection for a reasonable time.**

***Keywords*— DoS, DDoS, Types of Attack, TCP SYN, Hop count, IP Traceback**

## I. INTRODUCTION

The Denial of Service attack emerged in the last dacade of the 20th century and adopted a more sophisticated shape of Distributed Denial of Service attacks in start of 21st century. It incorporated multiple compromised machines and resources at a time (to include master and slave zombies) to attack a sole target. This increases the intensity of the attack and results in complete shutdown of the target services. The DDoS has emerged more sophisticated and lethal in last few years due to automation in attack techniques. Now a day, novice users are very comfortable in launching a massive attack beyond their knowledge and technical scope due to availability of automated and functional attack softwares and programs in the market.

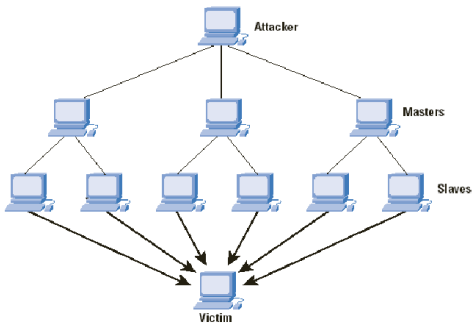


Fig. 1 Concept of DDoS attack

DDoS attack ruthlessly consumes internet resources under the garb of genuine internet user access as it is very difficult to differentiate between malicious and authenticated access at transport and network layers. For example, in July 2009, 48 web sites were made victim to DDoS attack in South Korea and USA. The attack pattern and botnet methods used were quite different from the previous techniques hence detection was made more difficult. Similarly DDoS attacks were even successful in damaging the YAHOO and AMAZON companies in the past. In this article I will discuss varius types of DoS attacks and protections / defenses against them. However the focus will remain on major types and their solutions. Typical DDoS attack includes A) Smurf Attack that generates ICMP echo request. B) TCP SYN attack in which attacker sends connection request to victim using unreachable network address. C) UDP, TCP and ICMP attacks flood the target by continuously sending packets at very high rate and asking the target to forward reply [1,2,3].

## II. GENERAL CATEGORIES OF DOS ATTACKS

The DoS attacks can be categorised in the following 3 major groups [1].

### *A. Bandwidth Attacks*

The attack is aimed to consume all the resources / bandwidth of the target system so that the legitimate users could not access it. The 1st DDoS attack was a flooded attack that occupied complete bandwidth of the system, hence legitimate users were unable to get the services. Typical TCP SYN and ICMP echo attack are aimed to capture all resources of the victim. [2].

### *B. Protocol attacks.*

This type of DDoS attacks are focussed onto inherent protocol designs and their exploitation.

### *C. Software Vulnerability attacks.*

These attacks take advantage of the inbuilt flaws of the software programs in the target computer and exploit their vulnerabilities [1].

## III. TYPES OF DOS ATTACKS

A DoS attack may appear under any of the following forms and techniques.

### A. Direct Flooding Attack

In this type of attack, attacker generate huge amount of packets which are directly sent to the victim. In year 2000, YAHOO and AMAZON were attacked using this technique. The address of attacker can be disguised using IP spoofing. In this DDoS attack the detection of attack is comparatively easy by

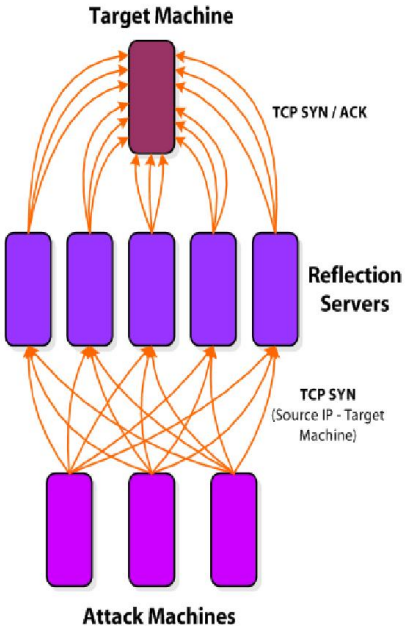


Fig.2 A typical flooding attack

analysing the traffic flow, however blockade to malicious traffic is difficult as differentiation between malicious and legitimate traffic is a cumbersome job. There are several tools available to generate such type of huge traffic like Synhose, Synk7, TFN and TFN2K [2][3]. The most typical attacks like SYN flood and ICMP flood are the common examples.

### B. Remote Controlled Network Attacks

This type of attacked are accomplished through a number of compromised computers and placing an application or agent on them. These compromised computers can be controlled either directly or through the malicious program already installed for the same purpose. It consists of a Master controller, command & control (C&C) and botnet [4]. In this type of attacks traceback to the original attacker is often impossible. The control channels include IRC channel, direct port communication, Smurf, TCP-SYN and ICMP ping packets [1,3].

### C. Reflective Flooding Attack

The reflective flooding attack is generated using several zombies and well known public servers as reflectors. The attacker instead of just spoofing own IP send the packets to reflector with IP address of the victim. The reflectors send back the reply to original IP holder (victim) thus flooding the victim. The amplification technique is also employed to multiply the packets so generated for effectiveness (from 3 to many hundreds) depending upon the protocol and configuration involved [1,4,5].

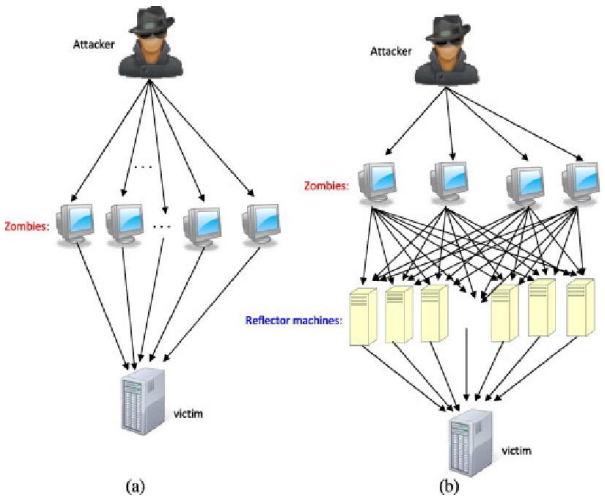


Fig.3 A diagrammatical layout of Reflector DDoS attack

### D. Virus

Viruses are spread through the emails to enhance the zombie network. Generally emails are circulated containing alerts of some fictitious virus / program and receiver is asked to circulate this message to maximum friends. Thus the hidden viruses are installed on the machines and activated as per requirements. Although viruses are not directly a significant threat to the internet but they keep clogging the email systems.

### E. Worms

Worms are distinguished from virus as they are not dependent on human intervention for operation. Worms are significantly used to create large scale zombies network and automated DDoS events. They are intelligent enough to scan for vulnerable machines and automatically start owning it. The well known worms include Code Red, Slammer and MS Blaster [1,2].

### F. Tear drop attack

This type of denial of service attack is generated by transmitting a packet with oversized payload. The size is so selected that is sufficient enough to crash the target machine.

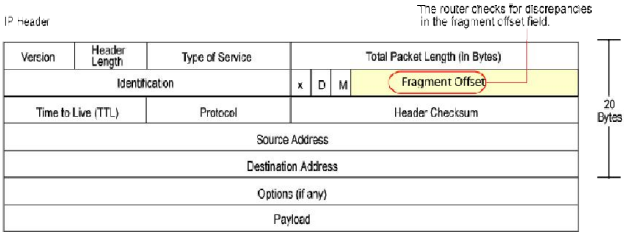


Fig.4 IP header of Teardrop attack packet

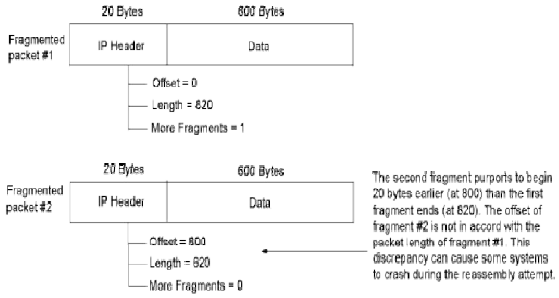


Fig.5 IP header of Teardrop attack packet

### G. Protocol violation attack

When an attacker intentionally violates the transmissi protocols and crafts the packets for negative usage, it characterised as protocol violation attack. The inter protocols are having the vulnerabilities and attacker exploit the same. However this is not the case every time. The protections designed for internet attack specially the trace route programs using ICMP return codes also fall in the same category but purpose is much different [1][2].

### H. Fragmentation attack

The fragmentation attacks are primarily adopted by attackers to avoid detection due to IDS systems in practice now a days and as DoS mechanism. As a DoS mechanism fragmentation is used to exhaust the system resources to assemble the fragmented packets thus making the system unavailable for other uses. This type of attacks occurs against windows operating computers, routers and check point firewalls.

### I. Network attack

The attacks that are aimed to target network infrastructure are more dangerous in nature. This may include attacks on DNS, root name server and RADIUS. The effects that can be generated out of this type of attack are regional and may cause unavailability of service, slow down or unpleasant effects in the service within a given region.

## IV. PROTECTIONS

A number of solutions are available as defence against the DDoS attack however none can be a solution in standalone form and for longer time. The protection elements are integrated and interrelated in nature. These defence mechanisms are very helpful to enhance the detection, prevention, mitigation and absorption of a DDoS attack. Here are few techniques that can offer a great safe guard against the Denial of Service attack.

### A. Hop count filtering

Generally an attacker spoofs the IP and use a number of zombies to disguise his own address while attacking. The hop count method is a source based solution which used TTL segment in the header field of packet and records it in a table.

for each packet:
  extract the final TTL $T_f$ and the source IP address $S$;
  infer the initial TTL $T_i$;
  compute the hop-count $H_c = T_i - T_f$;
  index $S$ to get the stored hop-count $H_s$;
  **if** $(H_c \neq H_s)$
    the packet is spoofed;
  **else**
    the packet is legitimate;

Fig.5 Hop count filtering

If any packet arrives with TTL significantly different than the stored one, it is filtered out and the packet is dropped. This method becomes ineffective if the attacker uses the IPs of zombies in the botnet having approximately similar TTL field. It is relatively unreliable as the working and discarding of the packets is based on assumptions [3,4].

### B. Router base solution[5]

The malicious traffic of the internet can also be traced out by the intelligent routers. When a router is modified with added intelligence and capability of encryption, digital signature and tracesback the source of a packet, it is called hardened router. The network designed with such routers is called a hardened network. Preferably such routers should be installed at border and access point of an autonomous system. When a packet arrives at 1st hardened router, it is encrypted along with one byte of IP address and then forwarded. This continues until the packet reaches its destination. However, the complexity, cost and replacement of already installed router is biggest hurdle in implementing the hardened network. By the working technique this method can be described as very effective method.

### C. StackPi [5]

This method forms unique pairs of adjacent routers and and mark the packets with hash function. The data is stored in a table as reference. Subsequently it drops packet having different marking as already stored in its table. It is done in 2 stages.

1) *Marking*: It is done with the concatenation of MD5 hash of the next node in the network with current node's IP. The result is calculated and placed in IP identification field of the IP header. This is calculated

for each pair of routers and placed in a table at each host end.

2) *Filtering*: The node then compares each packet with the data stored in the table of marking scheme. All the packets on arrival are matched with already calculated IP data and only the packets matching with marking scheme are allowed to flow in the network. This method reasonably reduces the undesired traffic on the network.

### D. Implementing push back – router based defence

In case of DoS attack, the flow of traffic from one node to other is abruptly increased. This can be checked at each node.

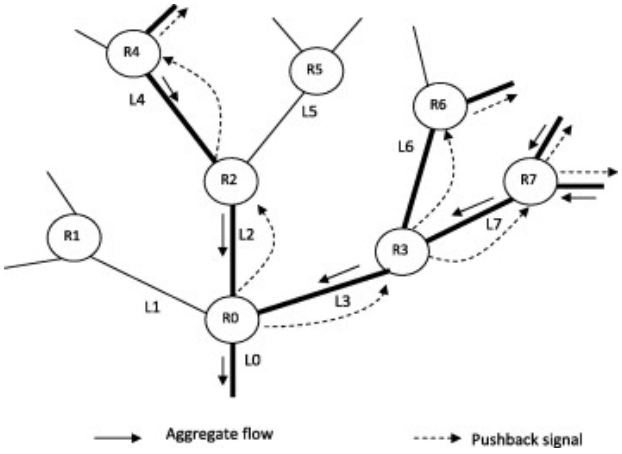


Fig.7 Understanding of pushback signal

In the push back method, router on reaching maximum allowed traffic rate start dropping the packets and also intimate the sender node to reduce the traffic. The router by counting the number of times a particular packet is dropped can also differentiate between legitimate and illegitimate packet. This pushback signal keep flowing upstream unless traffic flow is brought to an acceptable level.

### E. Differential packet filtering

This method is used to filter the traffic once attack has been detected by the host. It works on probability of a packet being malicious and drops it. Certainly few legitimate packets are also dropped in this scheme however it is always adaptive to traffic flow and tends to provides quality of service.

### F. Traceback through marking [5-7]

Traceback means reaching back to the attacker's address. The major challenge to counter the DDoS is traceback of the IP address which is often spoofed by the attacker. The other hurdle is the excessive use of reflectors and zombies network. In the traceback there are two common methods used and both require injection of marks on each packet by the routers to be used for traceback of the original sender of the packet.

1) Probabilistic packet marking (PPM): PPM is used within a small network or by an ISP and we cannot traceback a packet out of the network. It is vulnerable to hacking typically known as packet pollution.
2) Deterministic packet marking (DPM): This technique is relatively wider in nature and traceback out of the local network is possible. However it requires all routers to be updated for marking. It is vulnerable to packet pollution.

### G. Traceback using entropy variations[5,7,8]

This is a novel approach and new method to traceback the DDoS attack. The technique is evolved due to shortcomings of traceback through marking. It requires no marking but routers to manage data of entropy variation during peace time. Once DDoS has been detected the victim is required to initiate a pushback process to identify the address of zombie. This pushback process is initiated only with the router which is involved in flow of undesired traffic by observing flow entropy variations. The router then forwards the pushback process to the next upstream router after analysing its local entropy variations and process is extended to next upstream router and so on. The procedure is repeated in parallel and distributed fashion until the zombie or source of attack is reached. It can counter and mitigate an attack with very high accuracy.

### H. Bloom filter technique[9,10]

Bloom filter is a probabilistic algorithm primarily used to enhance the computation capability of a machine. It was initially used to reduce the access time of different files and applications stored on a disc like spell checkers. It comprises of Vector *V* having *m* bits, all set to position *0* in the start. We have different independent hash function say *k* starting from *h1, h2……hk,* each with range from *0 to m-1*. If the bits at position *h1(a), h2(a)….hk(a)* in vector *V* are set to *1*. The vector *V* can read and show the presence of an element in *A* if $a \in A$. For example if we want to check that whether *x* is present in *A* or otherwise, we have to see the values of *h1(x), h2(x)…hk(x)*. If any one of them is *0, x* is not member of *A* otherwise we assume that *x* is member of *A*.

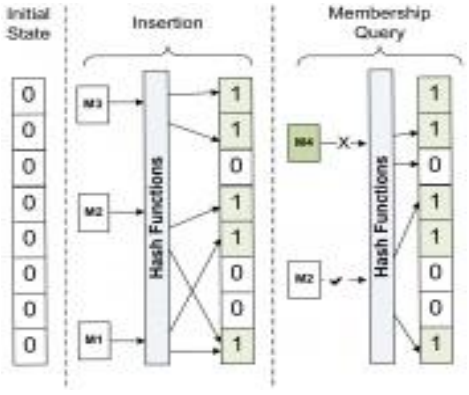


Fig.8 Basic function of bloom filter

## V. CONCLUSIONS

Denial of service attacks and specially Distributed Denial of service attack are hazardous for the internet and web services. According to the surveys, the percentage of attacks is at exponential rise with new and sophisticated techniques. The traceback technique can be helpful in reaching to an attacker but memory-less quality of the web routing is a hurdle in successful traceback. As a result, there are no proficient and successful methods to handle the problem so far. The solutions discussed here still hold certain loopholes and vulnerabilities which need to be addressed. At present preparation and prevention is the best solution to sage guard against attacks. This requires a dedicated network administrator team with latest knowledge and techniques to keep the system up to date and up graded. We must be preparing to deal with attack if encountered to mitigate in efficient and economical way. This requires from service provider and vendors to be adaptive to modern landscape in commensuration in running time frame. Special attention must be paid to the system configuration, correct routing technique, regular monitoring and strict auditing of the traffic and system performance. A lot of work is still required in the field of traceback methods. They all must be weighed against pros and cons and improvement should be a permanent feature of the efforts.


## ACKNOWLEDGMENT

I am grateful to all my friends and family members for tolerating my absence from events even during Eid days.


## REFERENCES


*[1]* Reeta Mishra, Amit Asthana and Jayant Shekhar, *Distributed Denial of Service Attacks Prevention;* VSRD International Journal of Computer Science & Information Technology,ISSN No.2231-2471, *Vol.1(1), page* 1-8, *2011*

[2] Yang-Seo Choi, Jin-Tae Oh, Jong-Soo Jang, *Integrated DDoS Attack Defense Infrastructure for Effective Attack Prevention*: Information Security Division ETRI, Daejeon, Republic of Korea; ©2010 IEEE

[3] Rahul Kumar(B.Tech ),Rahul Karanam(B.Tech), Rahul Chowdary Bobba(B.Tech), Raghunath. S (B.Tech); *DDOS defence mechanism;* International conference on future networks*,* IEEE Computer society - 2009

[4] Simon Liu, surviving *distributed denial of service attacks*; Published by the IEEE computer society; 1520-9202/09/$26.00 © 2009

[5] Shui Yu, Robin Doss, Wanlei Zhou, Weijia Jia, *Traceback of DDoS attack using entropy variations*, IEEE transactions on parallel and distributed systems, vol. 22, no. 3, march 2011

[6] Chirala Lokesh, Raveendra Naick, G. Nagalakshmi, *ETM: a novel efficient traceback method for DDoS attacks;* International Journal of Computer Science and Management Research. ISSN 2278-733X, Vol 1 Issue 3, October 2012

[7] 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

[8] P,R Nidhya,Mr K. Gunasekar: *An efficient way of IP traceback of DDoS attacks based on entropy variation*; International Journal of Communications and Engineering, Volume 02– No.2, Issue: 04 March 2012

[9] Akash Mittal1, Prof. Ajit Kumar Shrivastava2, Dr. Manish Manoria, *A review of DDoS attack and its countermeasures in TCP based network*; International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.4, November 2011

[10] Huan-rong Tang, Chao Xu, Xin-gao Luo, Jian-quan OuYang; *Traceback based bloomfilter IPS in defending SYN flooding attack*; 978-1-4244-3693-4/09/$25.00 ©2009 IEEE