# Review of PPM, a Traceback Technique for Defending Against DDoS Attacks

Satwinder Singh[#1], Abhinav Bhandari[*2]

[#]*M. Tech & Ucoe & Punjabi University Patiala*
*Punjab India*

***Abstract*— Distributed denial-of-service (DDoS) is a swiftly growing problem. Denials of Service (DoS) attacks add up to one of the major fear and among the hardest security problems in today's Internet. DDoS attacks are more difficult to handle because their traffic can be made highly similar to the legitimate traffic. With little or no advance notice, a DDoS attack can easily wear out the computing and communication resources of its victim within a short period of time. This paper presents classification of DDoS tools and IP Traceback technique to configure the actual source of attacker. The attack classification criteria were selected to highlight commonalities and important features of attack strategies. The goal of this paper is to place some order into the existing attack and defence mechanisms, so that a better thoughtful of DDoS attacks can be achieved and then more efficient and effective algorithms, techniques and procedures to fighting these attacks may be developed.**

***Keywords*— DoS, DDoS,PPM, IP, Traceback .**

## I. INTRODUCTION

Denial of Service (DoS) attacks is certainly a very serious problem in the Internet, whose impact has been well verified in the computer network literature. The main aim of DoS is the disorder of services by attempting to bound access to a machine or service instead of subverting the service itself. This kind of attack aims at picture a network incapable of providing normal service by targeting either the network's bandwidth or computer resources. These attacks attain their goal by sending at a victim a stream of packets that swamps his network or processing capacity denying access to his regular customers. In the not so distant past, there have been some large-scale attacks targeting most common Internet sites [1–3]. Distributed Denial of Service (DDoS), is a comparatively simple, yet very powerful method to attack Internet assets. DDoS attacks add the many-to-one aspect to the DoS problem making the prevention and improvement of such attacks more difficult and the impact proportionally severe.

DDoS attacks are comprised of packet streams from different sources. These attacks engage the power of a vast number of coordinated Internet hosts to consume some critical resource at the target and deny the service to legitimate clients. Traffic of DDos attack is behaved like a normal legitimate traffic. The traffic is usually so aggregated that it is difficult to distinguish legitimate packets from attack packets. More significantly, the attack volume can be larger than the system can handle. Unless special care is taken, a DDoS victim can suffer from damages ranging from system shutdown and file corruption, to total or partial loss of services. Attackers constantly modify their tools to bypass security systems developed by system managers and researchers, who are in a constant alert to modify their approaches to handle new attacks.

## II. HISTORY OF DOS

### A. *The Morris Worm*

On November 2 1988 the first DoS attack was launched on the electronic world. As a result about 15% (about 6.000) of the systems connected to the network were infected and stopped running. It was self replicating and self propagating.

### B. *SYN Floods*

SYN Floods have existed since TCP has existed. They are a direct consequence of TCP specifications. It is therefore possible to say that SYN Floods are part of TCP just as spoofing is part of UDP. Easy to implement, effective and hard to traceback to the actual source, Denial of Service attacks are still appreciated by malicious Internet abusers, managing to launch 100's of megabits, sometimes more than one gigabit, of SYNs targeted to a single service.

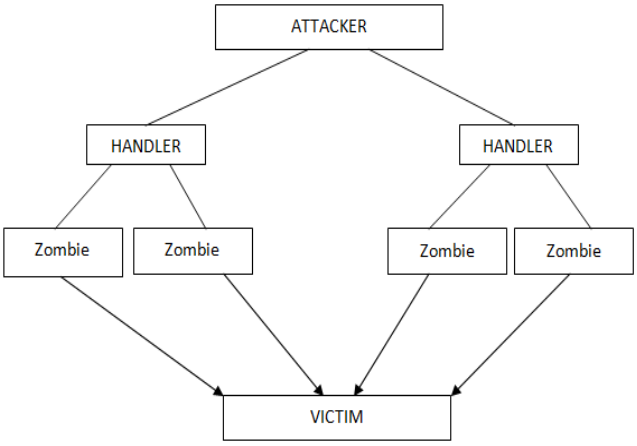
## III. DDOS ATTACK

In network security, a denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its planned users. While the means to carry out and targets of a DoS attack may vary, it normally consists of the efforts of one or more people to temporarily or forever interrupt or suspend services of a host connected to the Internet. Perpetrators of DDoS attacks typically target sites or services hosted on high-profile web servers such as Internet banking, credit card payment gateways, and even root servers. The term is generally used linking to computer networks, but is not limited to this field. One common method of attack involves saturating the target machine with external communications requirements such that it cannot take action to legitimate traffic, or responds so gradually as to be rendered basically unavailable. Such attacks usually lead to a server overload. In common terms, DDoS attacks are implemented by either forcing the under attack computer to reset, or overpowering its resources so that it can no longer provide its intended service or obstructing the communication media

between the intended users and the victim so that they can no longer communicate sufficiently.

## IV. DDOS ARCHITECTURE

A Distributed Denial of Service Attack is Calm of four elements.




1.1: Architecture of a DDoS Attack [4]

• The real attacker.
• The handler or master, which is compromised hosts with a special program running on them, capable of controlling multiple agents.
• The attack daemon agents or zombie hosts, who are compromised hosts that are running a special program and are responsible for generating a stream of packets towards the proposed victim. Those machines are commonly external to the victim's own network, to avoid efficient response from the victim, and external to the network of the attacker, to avoid liability if the attack is traced back.
• A victim or target host.

## V. DDOS ATTACK CLASSIFICATION

There are many DDoS attack tools. The architecture of these tools is very similar to each other and in fact some tools have been constructed through minor modifications of other tools.

### *A. Trinoo*

Trinoo [5] is certified with being the first DDoS attack tool to be widely spread and used. Trinoo [5] is a bandwidth depletion attack tool that can be used to launch coordinated UDP flood attacks against one or many IP addresses. The attack uses constant-size UDP packets to target random ports on the victim machine. Early versions of Trinoo appear to packets with spoofed source IP addresses and also randomize the target ports. It is capable of spoofing either one or all 32 bits of the IP source address, or just the last eight bits. Some of the attacks that can be launched by TFN include: Smurf, UDP flood, TCP SYN flood, ICMP echo request flood, and ICMP directed transmit on air.

### *B. Stacheldraht*

Stacheldraht [10] (German term for ''barbed wire'') is based on early versions of TFN and attempts to remove some of its weak points. It combines features of Trinoo (handler/agent architecture) with those of the original TFN. It also has the ability to perform updates on the agents repeatedly. This means that the attacker can offer the installation file on an secret server and when each agent system turns on (or logs on to the Internet), the zombies will automatically look for updates and install them. Stacheldraht also provide a protected telnet connection via symmetric key encryption between the attacker and the handler systems. Communication is performed through TCP and ICMP packets. Some of the attacks that can be launched by Stacheldraht include UDP overflow, TCP SYN flood, ICMP echo request overflow, and ICMP directed broadcast. The attack daemons for Stacheldraht implement Smurf, SYN Flood, UDP Flood, and ICMP Flood attacks. Support IP source address spoofing. Typically, the Trinoo agent gets installed on a system that suffers from remote buffer flooded utilization. This ''bug'' in the software allows an attacker to remotely compile and run the agent installation within the secondary victim's system buffer. The handler uses UDP or TCP to communicate with the agents so intrusion detection systems can only find them by sniffing for UDP traffic. This channel can be encrypted and password protected as well. However currently the password is not sent in encrypted format, so it can be ''sniffed'' and detected. Trinoo does not spoof source addresses although it can easily be extended to include this capability. Trinoo attack daemons implement UDP Flood attacks against the target victim.

### *C. Tribe Flood Network*

Tribe Flood Network (TFN) [6], written in 1999, is a DDoS attack tool that provides the attacker with the ability to earnings both bandwidth depletion and resource depletion attacks. It uses a command line interface to communicate between the attacker and the control master program but offers no encryption between agents and handlers or between handlers and the attacker. In addition to Trinoo's UDP flooding it also allows TCP SYN and ICMP flood as well as smurf attacks. Handlers are accessed using regular TCP connections like telnet. Other alternatives are ICMP tunnelling tools like LOKI [7,8]. Communication between the handler and the daemons is expert with ICMP ECHO REPLY packets, which are harder to detect than UDP packets and can often pass firewall systems. TFN launches coordinated Denial of Service attacks that are especially difficult to counter as it can generate multiple types of attacks and it can generate packets with spoofed source IP addresses and also randomize the target ports. It is capable of spoofing either one or all 32 bits of the IP source address, or just the last eight bits. Some of the attacks that can be launched by TFN include: Smurf, UDP flood, TCP SYN flood, ICMP echo request overflow, and ICMP directed broadcast.

### D. TFN2K

TFN2K [9] is a DDoS attack tool based on the TFN architecture. This attack tool add encrypted messaging between all of the attack components. Targets are attacked via UDP, TCP SYN, ICMP_ECHO overflow or smurf attack, and the attack type can be varied during the attack. Information is sent from the master to the agent via TCP, UDP, ICMP, or all three at random, making it harder to detect TFN2K by scanning the network. Communication between the real attacker and control master program is encrypted using a key-based CAST-256 algorithm. TFN2K attack daemons implement Smurf, SYN, UDP, and ICMP Flood attacks. Targets are attacked via UDP, TCP SYN, ICMP_ECHO overflow or smurf attack, and the attack type can be varied during the attack All communication between handlers and agents is encrypted and base-64 encoded. There is one additional attack form called TARGA attack. TARGA mechanism is achieved by sending malformed IP packets known to slow down or hang-up many TCP/IP network stacks.

## VI. DDOS DEFENSE PROBLEMS AND CLASSIFICATION

DDoS attacks are difficult problem to solve. First, there are no common characteristics of DDoS streams that can be used for their detection. Besides, the distributed nature of DDoS attacks makes them extremely difficult to conflict or traceback. In addition, the automated tools that make the operation of a DDoS attack possible can be easily downloaded. Attackers may also use IP spoofing in order to hide their true identity, and this makes the traceback of DDoS attacks even more difficult. Finally, there is no sufficient security level on all machines in the Internet, while there are constant security holes in Internet hosts. We may classify DDoS defence mechanisms [11] as

- Intrusion Prevention,
- Intrusion Detection,
- Intrusion Tolerance and Mitigation, and
- Intrusion Response.

## VII. INTRUSION RESPONSE (DEFENSE MECHANISM)

Once an attack is predicted, the immediate response is to find out the attack source and block its traffic accordingly. The jamming part is usually performed under manual control (e.g. by contacting the administrators of upstream routers and enabling access control list) since an automated response system might cause additional service dreadful conditions in response to a false alarm. Automated intrusion response systems do exist, but they are deployed only after a period of self-learning (for the ones that employ neural computation in order to discover the DDoS traffic) or testing (for the ones that operate on static rules). Improving attack source identification, techniques can speed up the capture of attackers and deter other attack attempts. There are many approaches that target the tracing and identifying of the real attack source [12].

## VIII. IP TRACEBACK

IP traceback traces the attacks back towards their origin, so one can find out the true identity of the attacker and achieve detection of asymmetric routes, as well as path characterization. Some actors that render IP traceback difficult is the stateless nature of Internet routing and the lack of source accountability in the TCP/IP protocol. For efficient IP traceback it is necessary to compute and construct the attack path. It is also necessary to have a low router overhead and low false positive rate. Furthermore, a large number of packets is required to reconstruct the attack path. It is also important the robustness against multiple attacks, the reduction of the privacy of IP communication, the incremental deployment and the backward compatibility. At a very basic level, you can think of this as a manual process in which the administrator of the network under attack places a call to his Internet Service Provider (ISP) asking for the direction from which the packets are coming. Since the manual traceback is very tedious there have been various proposals in the recent past to automate this process.

## IX. PROBABILISTIC PACKET MARKING (TECHNIQUE FOR IP TRACEBACK)

In packet marking, the router marks forwarded IP packets with its identification information. Because of the limited space in packet header, routers probabilistically choose to mark packets so that each marked packet carries only partial path information. The network path can be regenerated by combining a modest number of packets containing mark. This approach is known as probabilistic packet marking (PPM) [13]. Burch and Cheswick [14] proposed this algorithm and was designed carefully later it was implemented by Savage for solving the trace back problem present with IP address. The PPM algorithm consists of two procedures: The packet marking procedure and graph building procedure. In the packet marking procedure the packets randomly code every edge of the attack graph and the graph reconstruction procedure obtains the constructed graph from this encoded information. Here the constructed graph should be the same as the attack graph. The constructed graph is the graph obtain by the PPM algorithm and attack graph is the set of paths the attack packets has been traversed. In this methods, the packets are marked with the router's IP address from which they traversed or the path edges from which the packet is being transmit. Packets are marking with the router's address is the best approach when compared to the two alternatives provided here, where if a packet is lost of affected with any attack, the source router address can be fetched and send back to the actual router. Now the router checks the packets and retransmits the packet to the actual destination. With this implementation, an accuracy of 95% can be achieved to identify the actual attack path.

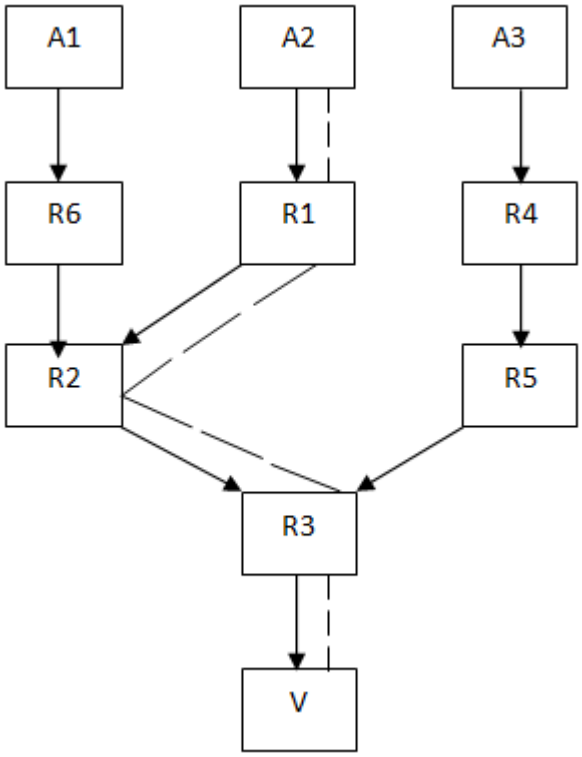



Figure 1.2: An attack graph containing attack path.

The view of network can be defined as a directed graph having G = (V, E), here E represents the edges set, and V represents the nodes set. The single host that is under attack can be considered as V or device that one present at the border of a network which may be firewall or a system that is intrusion detected representing a number of paths. The origin of all the Potential attacks is at Ai which is represented as a leaf in tree that is being embedded at V, and there are routers in the path namely Ri that are present among Ai as well as V. The routers ordered list that is between Ai and V having the packets traversed is considered as the "attack path" which is represented in the figure 1.2 with a dotted line it is (R1, R2, R3). The number of routers that are present in between the Ri and V in a path is considered as the "distance" which is represented in the figure 1.2 for the path R3, R1, R2. Those packets that are utilized in the attacks of DDoS are considered as the 'attack packets'.

Marking procedure at router R

If x is smaller than the predefined marking probability pm, the router choose to initiate encoding an edge. The router sets the initiate field of the incoming packet to the routers address and resets the distance field to zero. If x is greater than pm, the router chooses to end encoding an edge by setting the router's address in the end field.

```
for each packet w
let x be a random number from [0..1)
if x < pm then
write R into w.start and zero into w.distance
else
if w.distance = 0 then
write R into w.end
increment w.distance
```

Attack Graph building Procedure at victim V

A victim V, upon receiving packets, initial needs filtering of unmarked packets (since they don't carry any information in the attack graph construction). The victim needs to execute the graph construction algorithm for all the collected marked packets and re-construct the attack graph.

```
let G be a tree with root being victim V ;
let edges in G be rows (start,end,distance);
for (each received marked packet w)
{
if (w.distance==0) then
insert edge (w.start,V ,0) into G ;
else
insert edge (w.start, w.end, w.distance) into G ;
}
remove any edge (x,y,d) with d _ distance from x to V in G ;
extract path (Ri…Rj) by enumerating acyclic paths in G ;
```

Disadvantages of PPM technique

1. In this technique affected packets are more than normal packets.
2. Path reconstruction of the lost packets requires many computation cycles in this method and this is not practically possible for the systems with low resources..

## X. Conclusion

The impending threats imposed by DDoS attacks call for efficient and fast traceback schemes. Some of the desirable features of a good attack traceback scheme are providing accurate information about routers near the attack source rather than those near the victim. Avoiding the use of large amount of attack packets to construct the attack path or attack tree and low processing and storage overhead at intermediate routers.

References

1. CERT Coordination Center, Denial of Service attacks, Available from <http://www.cert.org/tech_tips/denial_of_service.htl.
2. Computer Security Institute and Federal Bureau of Investigation, CSI/FBI Computer crime and security survey 2001, CSI, March 2001, Available from <http://www.gocsi. com>.
3. D. Moore, G. Voelker, S. Savage, Inferring Internet Denial of Service activity, in: Proceedings of the USENIX Security
4. W. Stallings, "Cryptography and Network", 4th ed, Pearson Education, 2006.
5. D. Dittrich, the DoS Project_s ''trinoo'' Distributed Denial of Service attack tool, University of Washington, October 21, 1999,

Available from <http://staff.washington.edu/ dittrich/misc/trinoo.analysis.txt>.
6. D. Dittrich, the Tribe Flood Network Distributed Denial of Service attack tool, University of Washington, October 21, 1999, Available from <http://staff.washington.edu/ dittrich/misc/trinoo.analysis.txt>.
7. Phrack Magazine 7 (49), File 06 of 16 [Project LOKI], Available from <http://www.phrack.com/search.phtml? View&article¼p49-6>.
8. Phrack Magazine 7 (51) September 01, 1997, article 06 of 17 [LOKI2 (the implementation)], Available from <http:// www.phrack.com/search.phtml?
9. J. Barlow, W. Thrower, TFN2K—an analysis, 2000, Available from <http://security.royans.net/info/posts/ bugtraq_ddos2.shtml>.
10. D. Dittrich, The _Stacheldraht_ Distributed Denial of Service attack tool, University of Washington, December1999, Available from<http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt>.
11. Christos Douligeris, Aikaterini Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the art, Received 9 October 2003; accepted 13 October 2003.
12. P. Zaroo, A survey of DDoS attacks and some DDoS defense mechanisms, Advanced Information Assurance (CS 626).
13. S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Network support for IP traceback," *IEEE/ACM Transactions on Networking*, vol. 9, June 2001.
14. Burch, Hal; Bill Cheswick, "Tracing Anonymous Packets to their Approximate Source", LISA, pp. 319–327, 2000.