Analysis of Different IP Traceback Techniques

Aman Sachdeva
Student
Department of Computer Science & Engineering
World College of Technology & Management, Gurgaon, India

Mr. Binayak Parashar
Assistant Professor
Department of Computer Science & Engineering
World College of Technology & Management, Gurgaon, India

Abstract

Internet usage is increasing day by day as well as the attacks on the sites. Distributed denial of service (DDoS) is one of the such type of attacks. DDoS disable the server by flooding invalid requests with invalid or spoofed addresses, due to this the server's buffer gets overloaded and bandwidth of server get exhausted and server stop its services. Left undetected, can be very dangerous to the entire network. If organizations can detect these types of attack in advance then organizations will be saved from loss of these attacks, there is much prevention techniques which can detect these types of attack but while choosing one of these technique questions arise which technique should be used? Which is the best? IP Traceback technique is a DDoS detection technique, which is used to trace the path of an IP packet to its origin so one can find out the true identity of the attacker and can detect the path characteristics. Different types of IP Traceback Techniques are available. In this paper we study different IP Traceback techniques.

Keywords- DDoS attack, Types of DDoS attack, IP Traceback techniques, link testing, PPM, DPM

I. INTRODUCTION

The Internet has revolutionized the computer and communications world like nothing before. The Internet is at once a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location. [5].We can see in the following fig. that how internet users are increasing every year. [2].Unfortunately with the no. of host increasing the attacks on websites are also increasing. DDoS (distributed denial of service attack) is one of them. Denial of Service (DoS) attacks and a more complicated version known as Distributed DoS (DDoS) is the most common to take advantage of source address spoofing. These attacks deny regular Internet services from being accessed by legitimate users either by blocking service completely or by disturbing it such that users become not interested in the service anymore.[4]

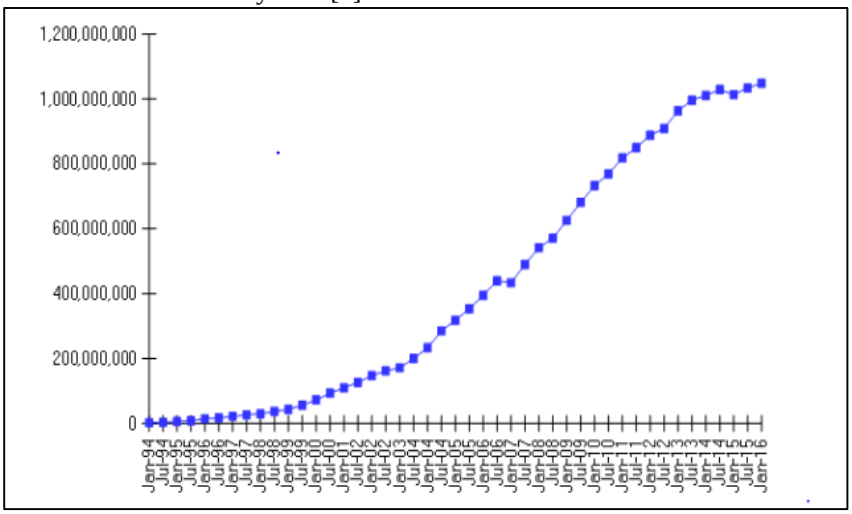

Fig. 1: Internet Domain Survey Host Count

Distributed denial-of-service (DDoS), is a relatively simple, yet very powerful technique to attack Internet resources. With little or no advance warning, a DDoS attack can abruptly drain the computing and communication resources of its victim within a short time, until the attack is resolved or in some cases slowly eat up resources without being noticed. Thus these disruptive or degrading attack flows often lead to complete shutdowns of Internet resources or at least cause performance degradations.[3].

In DDoS attacker uses spoofed source address so it is difficult to detect the DDoS attack traffic because attacker generally hides their identity so tracing the source of attack is difficult. Many techniques and methodologies are used to trace the

DDoS attacks. IP traceback is one of them it identifies the source address of attacker. Goal of this paper is to define different IP traceback techniques and compare them basis on different parameters.

This paper presents overview of DDoS problem, available DDoS attack tools, and a classification of IP Traceback techniques. The paper is organized as follows. Section II contains overview of DDoS problem. Section III describes Types of DDoS attack. Section IV concludes the paper V presents references..

II. OVERVIEW OF DDOS

Distributed Denial of Service (DDoS) is an attack which denies authorized user access to the service provider. The goal of the attacker is to disrupt or shut down an organization's business critical services such as ecommerce transactions, financial trading, email or web site access. By overwhelming network infrastructure, servers or applications with excessive communications requests, an attack means services are unavailable to legitimate users.[14] A Distributed Denial of Service (DDoS) attack is an attack to prevent the users from using the resources of a victim's computer. It is a large scale attack in a co-ordinated fashion, which is typically launched indirectly with the help of other computers in the Internet.[4]

DDOS attack occurs when multiple system resources is not available to network users. A DOS attack floods the remote system with so much traffic that it cannot handle normal, valid requests made from others network systems. One frequently exercised approach is for the attacker to send a stream of packets to a victim; this stream consumes some key resource, thus rendering it unavailable to the victim's legitimate clients. Another common approach is for the attacker to send a few malformed packets that confuse an application or a protocol on the victim machine and force it to freeze or reboot.[1]

To launch a DDoS attack, the attacker(s) first establishes a network of computers that will be used to generate the huge volume of traffic needed to deny services to legitimate users of the victim. [15]To create this attack network, attackers discover vulnerable hosts on the network. Vulnerable hosts are those that are either running no antivirus or out-of-date antivirus software, or those that have not been properly patched. These are exploited by the attackers who use the vulnerability to gain access to these hosts. The next step for the attacker is to install new programs (known as attack tools) on the compromised hosts of the attack network. The hosts running these attack tools are known as zombies, and they can be used to carry out any attack under the control of the attacker. Numerous zombies together form an army or botnet. In a typical DDoS attack, the master computer orders the zombies to run the attack tools to send huge volume of packets to the victim, to exhaust the victim's resources.[4].

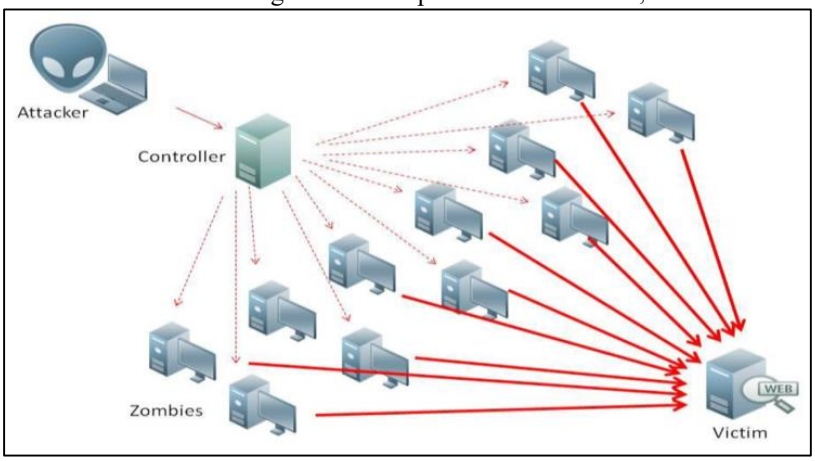

Fig. 2: Illustration of DDoS attack

III. CLASSIFICATION OF DDOS ATTACK

There are three main classes of DDoS attacks:

- Bandwidth/Throughput Attacks
- Protocol Attacks
- Software Vulnerability Attacks

A. Bandwidth/Throughput Attacks

Bandwidth/Throughput attacks are those attacks in which the bandwidth of users is exhausted by flooding the traffic towards victim Bandwidth/Throughput attacks are of two types: flooding attack and amplification attack. Flooding attack can be characterized as-

1) Ping Flood Attack (ICMP echo)
2) SYN Flood Attack (DoS attack)
3) UDP Flood Attacks

1) Ping Flood Attack (ICMP echo)

An ICMP flood attack occurs when the zombies send large volumes of ICMP_ECHO_REPLY packets ("ping") to the victim system. These packets signal the victim system to reply and the combination of traffic saturates the bandwidth of the victim's network connection as described in [1]. During this attack, the source IP address of the ICMP packet may also be spoofed.[6]

2) SYN Flood Attack (DoS attack)

SYN Flood attack is also known as the Transmission Control Protocol (TCP) SYN attack, and is based on exploiting the standard TCP three–way handshake. The TCP three-way handshake requires a three-packet exchange to be performed before a client can officially use the service. A server, upon receiving an initial SYN (synchronize/start) request from a client, sends back a SYN/ACK (synchronize/acknowledge) packet and waits for the client to send the final ACK (acknowledge). However, it is possible to send a barrage of initial SYN's without sending the corresponding ACK's, essentially leaving the server waiting for the non-existent ACK's. Considering that the server only has a limited buffer queue for new connections, SYN Flood results in the server being unable to process other incoming connections as the queue gets overloaded..as described in [7]

3) UDP Flood Attacks

A UDP Flood attack is possible when a large number of UDP packets is sent to a victim system. This has as a result the saturation of the network and the depletion of available bandwidth for legitimate service requests to the victim system. In a DDoS UDP Flood attack, the UDP packets are sent to either random or specified ports on the victim system. Typically, UDP flood attacks are designed to attack random victim ports. A UDP Flood attack is possible when an attacker sends a UDP packet to a random port on the victim system. When the victim system receives a UDP packet, it will determine what application is waiting on the destination port. When it realizes that there is no application that is waiting on the port, it will generate an ICMP packet of ''destination unreachable'' [14] to the forged source address. If enough UDP packets are delivered to ports of the victim, the system will go down. By the use of a DDoS tool the source IP address of the attacking packets can be spoofed and this way the true identity of the secondary victims is prevented from exposure and the return packets from the victim system are not sent back to the zombies.[8]

4) Amplification Attack

An amplification attack involves the attacker or the zombies sending messages to a broadcast IP address, using this to cause all systems in the subnet reached by the broadcast address to send a reply to the victim system. The broadcast IP address feature is found on most routers; when a sending system specifies a broadcast IP address as the destination address, the routers replicate the packet and send it to all the IP addresses within the broadcast address range. In this attack, the broadcast IP address is used to amplify and reflect the attack traffic, and thus reduce the victim system's bandwidth.Example of such types of attacks is-.

5) Smurf Attack

A DDoS Smurf attack is an example of an amplification attack where the attacker sends packets to a network amplifier (a system supporting broadcast addressing), with the return address spoofed to the victim's IP address. The attacking packets are typically ICMP ECHO REQUESTs, which are packets (similar to a "ping") that request the receiver to generate an ICMP ECHO REPLY packet. The amplifier sends the ICMP ECHO REQUEST packets to all of the systems within the broadcast address range, and each of these systems will return an ICMP ECHO REPLY to the target victim's IP address. This type of attack amplifies the original packet tens or hundreds of times.[6]

B. Protocol Attacks

DoS attacks based on protocol features take advantage of certain standard protocol features. For example several attacks exploit the fact that IP source addresses can be spoofed. Example of such attack is:

1) DNS Name Server Attack

Several types of DoS attacks have focused on DNS, and many of these involve attacking DNS cache on name servers. An attacker who owns a name server may coerce a victim name server into caching false records by querying the victim about the attacker's own site. A vulnerable victim name server would then refer to the rogue server and cache the answer [8].

C. Software Vulnerability Attacks

In these types of attack attacker gets the benefit of software vulnerabilities. These attacks are of three types-

1) Land Attack
2) Ping of Death Attack
3) Fragmentation Attack and Teardrop Attack

1) Land Attack

In this attack, an attacker sends spoofed TCP SYN packets, with the same source and destination addresses as the victim's host address. In some TCP/IP stack implementations those kinds of packets may cause the victim's host to crash. Any remote user that can send spoofed packets to a host can crash or "hang" that host.[8].

2) Ping of Death Attack

Ping of Death is an attempt by an attacker to crash, reboot or freeze a system by sending an illegal ICMP (over IP) packet to the host under attack. The TCP/IP specification allows for a maximum packet size of up to 65536 octets. In some TCP stack implementation encountering packets of greater size may cause the victim's host to crash.[6]

3) Fragmentation Attack and Teardrop Attack

Teardrop attacks target vulnerability in the way fragmented IP packets are reassembled. Fragmentation is necessary when IP Datagrams are larger than the maximum transmission unit (MTU) of a network segment across which the Datagrams must traverse. In order to successfully reassemble packets at the receiving end, the IP header for each fragment includes an offset to identify the fragment's position in the original un-fragmented packet. In a Teardrop attack, packet fragments are deliberately fabricated with overlapping offset fields causing the host to hang or crash when it tries to reassemble them. [6]

IV. CLASSIFICATION OF DEFENSE MECHANISM

IP Traceback is a reactive mechanism. IP traceback is the process of identifying the actual source(s) of attack packets. This has the benefit of holding attackers accountable for abusing the Internet. Also, it helps in mitigating DoS attacks either by isolating the identified attack sources or by filtering attack packets far away from the victim as proposed in the IP traceback based intelligent packet filtering technique [4].

Different types of IP Traceback techniques are-

- Link Testing
- Packet Marking
- ICMP Traceback
- Hybrid Schemes

A. Link Testing

The overview of link testing starts from the victim and traces till the attack source via upstream links with the assumption that the attack remains active until the completion of the trace. It determines the upstream of attacking traffic hop-by-hop while the attack is in progress. This scheme, therefore, will not be suitable to identify the attack that occurs intermittently or when the attacker is aware of the trace back scheme [9] two variants of link testing are-

1) Input Debugging[4]:

It is one implementation of the link testing approach. This feature lets the administrator determine incoming network links for specific packets. If the router operator knows the attack traffic's specific characteristics (called the attack signature), then it's possible to determine the incoming network link on the router. The ISP must then apply the same process to the upstream router connected to the network link and so on, until the traffic's source is identified.

2) Controlled Flooding:

This technique [4] works by generating a burst of network traffic from the victim's network to the upstream network segments and observing how this intentionally generated flood affects the attack traffic's intensity. Using a map of the known Internet topology around the victim, these packet floods are targeted specifically at certain hosts upstream from the victim's network; they iteratively flood each incoming network link on the routers closest to the victim's network.

B. Packet Marking

Packet Marking One of the common and significant techniques of IP Traceback is packet marking. The marking utilizes the rarely used fields of IP header, to store the audit trail where the field size used for marking varies from scheme to scheme Packet marking mechanism is broadly classified into following categories[9]-

1) Probabilistic Packet Marking
2) Deterministic Packet Marking

1) Probabilistic Packet Marking (PPM)

Probabilistic packet marking (PPM) was originally introduced by Savage et al. [11], who described efficient ways to encode partial route path information and include the traceback data in IP packets. It is an approach that can be applied during or after an attack, and it does not require any additional network traffic, router storage, or packet size increase. Even though it is not impossible to reconstruct an ordered network path using an unordered collection of router samples, it requires the victim to receive a large amount of packets [10]. In this method, each router marks the packet with some probability say p for example p = 1/100 which implies marking one packet for every 100 packets received. The marking field uses 16 bits identification field in the header, of which 5 bits are used for marking hop count, which would be useful information during reconstruction of attack path, and the remaining bits are used by the router to send its information. [9]PPM is shown in fig4 as below-

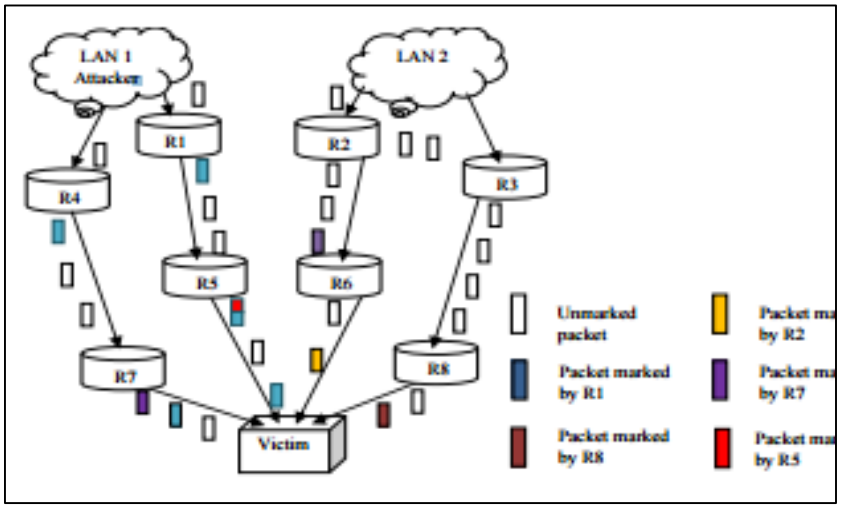

Fig. 4: Probabilistic Packet Marking

The advantage of this approach is that no extra traffic is generated, since the extra information is bound to the packets. Furthermore, there is no interaction with ISPs and this mechanism can be used to trace attacks after an attack has completed.[10] Drawback of this scheme is that it shares similar backwards compatibility problems and is less efficient in the presence of multiple attackers.[4]

2) Deterministic Packet Marking

In deterministic packet marking (DPM), the router embeds its IP address deterministically into the IP packets. The scheme was introduced to overcome some drawbacks of probabilistic packet marking as it has simple implementation and requires less computational overhead on intermediate routers. However, it has its own limitations. In this scheme, the packets are marked with the information of only the first ingress edge router i.e. the complete path is not stored as in PPM. Therefore, it requires even more packets to reconstruct the attack path

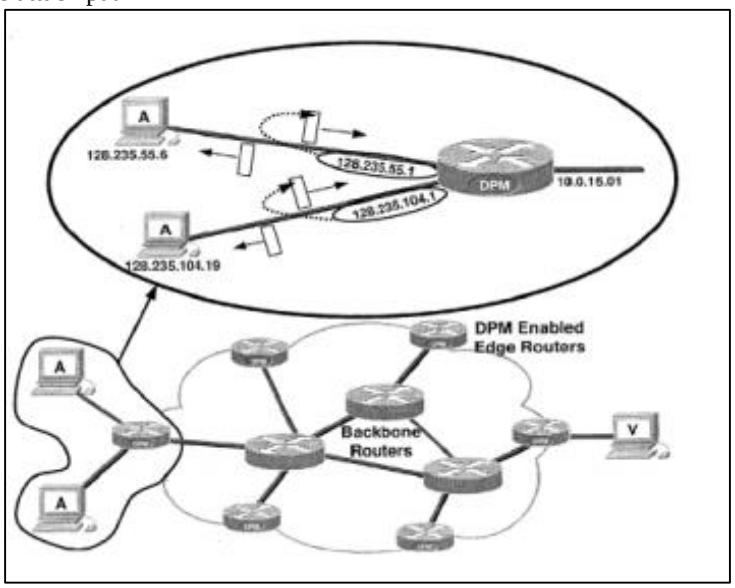

Fig. 4: Deterministic Packet Marking

In figure 4, it is shown that under DPM scheme, packets are marked at the first ingress edge router closest to the source. This marking remains unchanged as long as the packet traverses the network. If the victim is also a part of the internet under single administration (as shown), the same first mark will be available for the victim to traceback the source. The scheme is also more efficient due to deterministic marking of packets as an attempt by the attacker to spoof the mark is overwritten with the correct mark by the first router through which the packet traverses [12].

C. ICMP Traceback

Each router samples the forwarding packets with a low probability (e.g. 1/20000) and sends a special ICMP message including the information like neighboring routers (forward and backward links) on the path to the destination and source along with the original (triggering) packet. Traceback packet also includes an authentication field which guards against spoofed traceback

packets sent from attackers. This field can be null authentication, random strings or even HMACs. TTL is set to 255 for computing distance at the receiving end. During DDoS flooding attack, these ICMP traceback messages are used by the victim to reconstruct the path taken by the attacker. The schematic representation of the scheme is shown in Fig 5.[9]

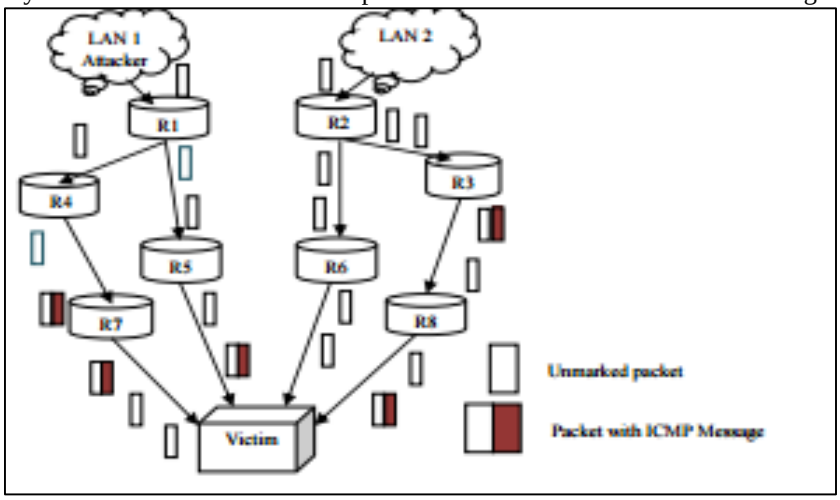

Fig. 5: ICMP Traceback

The updated version of the previous iTrace (ICMP Traceback) scheme was proposed. This technique separates the messaging function between the decision module and the iTrace generation module. A recipient network supplies specific information to the routing table to indicate it requests ICMP traceback message and the decision module would select which kind of packet to use next to generate an iTrace message. Based on this decision, the decision module will set one special bit in the packet-forwarding table and this bit indicates that the very next packet corresponding to that particular forwarding entry will be chosen to generate an iTrace message.[4].The effectiveness of the scheme relies on selecting the appropriate value for the probability exponent which influences the traceback time for attack paths of different length. The iTrace scheme suffers a serious problem on the resource spent on generating the number of traceback packets which turns out to be neither useful nor informative during traceback and this issue is addressed in Intention-driven ICMP traceback which enhances the probability of the router to generate useful trace messages.[9]

D. Hybrid Schemes

The idea of hybrid scheme combining marking and logging has been conceived to overcome the disadvantage of individual marking and logging schemes as stated above and a drastic improvement in traceback has been achieved. Two hybrid schemes of IP traceback are proposed – Distributed Linked List Traceback (DLLT) and Probabilistic Pipeline Packet Marking (PPPM). The first scheme preserves the marking information at the core routers in a precise way such that it can be collected using a linked-list based approach. The second scheme aims at passing the IP addresses of the routers that were involved in marking particular packets by stuffing them into the packets going to the same destination. This mechanism avoids the need for long term storage at the co-routers.

V. CONCLUSION

In this review paper we survey different papers and discuss about the different IP Tracebck techniques. We conclude that the each technique has its advantages and disadvantages. But in these papers the comparative study of different IP Traceback techniques is not described. Also there are many other techniques like ICMP and IP-logging. Study of these techniques and comparison can be done in near future.

REFERENCES

[1] J. Mirkovic, and P. Reiher, "A Taxonomy of DDoS Attack and DDoS defense Mechanisms," ACM SIGCOMM Computer Communications Review, Volume 34, Number 2, April 2004.
[2] ISC Domain Survey jan 2016" https://www.isc.org/network/survey/"
[3] K. Kumar, R.C. Joshi and K. Singh, "An Integrated Approach for Defending against Distributed Denial-of-Service (DDoS) Attacks", iriss, 2006, IIT Madras.
[4] G.Florance, "Survey of IP Traceback Methods in Distributed Denial of Service (DDoS) Attacks International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 7, July 2015.
[5] Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff. A Brief History of the Internet. Internet Society. http://www.isoc.org.
[6] Stephen M. Specht, and Ruby B. Lee, "Distributed Denial of Service:Taxonomies of Attacks, Tools andCountermeasures"Avilableat: http://palms.ee.princeton.edu/PALMSopen/DDoS%20Final%20PDCS%20Paper.pdf.

[7] Felix Lau, Stuart H. Rubin, Michael H. Smith Ljiljana Trajkovic, "Distributed Denial of Service Attacks"Avilableat:http://www2.ensc.sfu.ca/~ljilja/ENSC833/Spring01/Assignments/smc00_edited.pdf
[8] Christos Douligeris *, Aikaterini Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art"Avilable at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.103.7118&rep=rep1&type=pdf
[9] Vijayalakshmi Murugesan, Mercy Shalinie, and Nithya Neethimani, "A Brief Survey of IP Traceback Methodologies", Department of Computer Science and Engineering, Thigarajar College of Engineering, Thiruparankundram, Madurai – 625015, Tamilnadu, India
[10] Christos Douligeris *, Aikaterini Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art", Department of Informatics, University of Piraeus, 80 Karaoli and Dimitriou Str, Piraeus 18534, Greece October 2003
[11] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical network support for ip traceback," in Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, ser. SIGCOMM '00. New York, NY, USA: ACM, 2000, pp
[12] B.B gupta ,R. C. Joshi and Manoj Misra, Member, IEEE"Disrtibuted Denial of Service Prevention Technique" International Journal of Computer and Electrical Engineering, Vol. 2, No. 2, April, 2010 1793-8163.
[13] Darshan Lal Meena, Dr. R. S. Jadon" Distributed Denial of Service Attacks and Their Suggested Defense Remedial Approaches International Journal of Advance Research in Computer Science and Management Studies, Volume 2, Issue 4, April 2014.