A SELECTIVE SURVEY OF DISTRIBUTED DENIAL-OF-SERVICE (DDOS) ATTACKS AND DEFENSE MECHANISMS

Gupta B.B
Department of Electronics and Computer Engineering
Indian Institute of Technology, Roorkee
E-mail: brijgdec@iitr.ernet.in

Abstract

Distributed Denial of Service (DDoS) attacks, one of the latest and most powerful threats that have appeared to the Internet can disrupt the availability of Internet services completely, by eating either computational or communication resources through sheer volume of packets sent from distributed locations in a coordinated manner or graceful degradation of network performance by sending attack traffic at low rate. An overview of DDoS problem, Vulnerabilities in Internet Architecture, Attack: Modus Operandi, different types of DDoS attacks, recent defense mechanisms and their effectiveness are presented. This provides better understanding of the problem, current solution space and future to defend against DDoS attacks.

Key words: Distributed Denial-of-Service (DDoS), Attack mechanisms, Defense mechanisms, Internet Security.

I. INTRODUCTION

The Internet has become increasingly important to current society. It is changing our way of communication, business mode, and even everyday life. Hence the availability of Internet and its resources is very critical for the socio-economic growth of nation and the whole humanity. Unfortunately, security problems are major obstacles to the further development of Internet. According to [38], a mere 171 vulnerabilities were reported in 1995 which boomed to 8064 in 2006. Already, the number for the same for the merely the first quarter of 2007 has gone up to 2176. Apart from these, a large number of vulnerabilities go unreported every year. In particular, today distributed denial-of-service (DDoS) attacks are a major threat to the Internet.

Distributed Denial-of-Service (DDoS), is a relatively simple, yet very powerful technique to attack Internet resources. The primary goal of these attacks is to prevent access to a particular resource like DNS server [1, 13]. DDOS attacks can be carried out either as a Flooding or a Logical attack. In Flooding DDOS attacks, legitimate looking but error data packets are send to victim as much as possible, thus reduce a legitimate user's bandwidth, prevent access to a service to a legitimate user. A logical attack is based on an intelligent exploitation of vulnerabilities in the target [6].As per recent survey conducted by FBI/CSI, these attacks are second most dreadful attacks in terms of revenue losses after information thefts [12]. Mölsä et al. [6], Xiang et al. [3], Douligeris et al. [7, 10], Chen et al. [8], and Mircovik et al. [9] have reviewed various DDoS attack, and defense methods. Möl! sä et al. [6] Describes what Denial of Service (DoS) attacks are, how they can be carried out in IP networks, and how one can defend against them. Here, goal is not to implement all possible defenses. Instead, one should optimize the trade-off between security costs and acquired benefits in handling the most important risks. Xiang et al. [3] describes evolution and classification of DDoS attacks. They propose a novel concept of *active* defence against DDoS attacks to mitigate the infamous DDoS attacks in the Internet. Douligeris et al. [7,10] presents a structural approach to the DDoS problem by developing a classification of DDoS attacks and DDoS defense mechanisms and. Chen et al. [8] propose a characterization of distributed denial-of-service (DDOS) defenses where reaction points are network-based and attack responses are active and compared different attack detection algorithms on the basis of Granularity of detection used, Network information monitored, specific characteristics of attack traffic, source of false positives and limitations. Mircovik et al. [9] gave good direction for DDoS research by providing comprehensive taxonomies of attack and defense mechanisms. Moreover they critically brought forward weaknesses of various DDoS defense classes which are useful for future work in DDoS.

The remainder of this paper is organized as follows: section II gives overview of DDoS, section III discusses Vulnerabilities in Internet Architecture, section IV discusses Attack: Modus Operandi, section V contains various Attack Mechanisms, section VI discusses various defense approaches, Section VII finally concludes the paper.

II. DDOS OVERVIEW

DDoS is basically a resource overloading problem. The resource can be bandwidth, memory, CPU cycles, file descriptors and buffers etc. The attackers bombard scare resource either by flood of packets or a single logic packet which can activate a series of processes to exhaust the limited resource [2]. Here in the Fig .1 packets drop due to congested access link in victim network and buffer overflow at victim due to large number of requests are depicted [3,10]. Figure 1 shows that packets coming from traffic sources are stored in queues. When queues fill up to its capacity, it starts dropping packets.

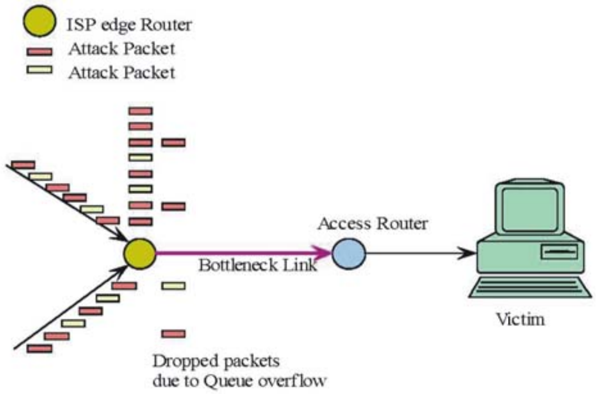

Fig .1 Packets drop under DDoS attack

The attacker/malicious users waste their energy and effort to create attack network (botnet) comprising of weekly secured machines to launch such attacks. The main motives behind DDoS Attacks are either of *criminal*, *commercial* or *ideological* nature. There are usually four types of attackers:

(a) Criminals who blackmail their victims and demand high ransom payments.

(b) Competitors who aim to damage their rivals businesses and reputation.

(c) Terrorists who carry out ideologically motivated attacks.

(d) Script kiddies who are testing their abilities or for publicity.

Extremely sophisticated, user friendly and powerful DDoS toolkits are available to potential attackers increasing the danger of becoming a victim. DDoS attacking programs have very simple logic structures and small memory sizes making them relatively easy to implement and hide [11].

III. VULNERABILITIES IN INTERNET ARCHITECTURE

The Internet has grown without an overall architectural design. This architecture paradigm is beneficial to the rapid growth of the Internet. However, such architecture opens several security issues that provide opportunities for the attackers. The fundamental characteristic of the Internet that allures DDoS attack is that the Internet security is highly interdependent [14]. DDoS attacks are commonly launched from systems that are subverted by an intruder via a security-related compromise rather than from the intruder's own system or systems [15]. Thus no matter how well secured the victim system may be, its susceptibility depends on the state of security of the rest global environment. It is easy for attackers to hide their identities from tracing back in different networks. Another characteristic of the Internet comprising of limited and consumable resources is also an inherent reason that attracts the attacks. Bandwidth, processing power, and storage capacities! are all targets of attacks. Each host or network has limited resources that can be exhausted by a sufficient number of users. Moreover, the Internet provides a target rich environment. There are millions of hosts and networks in the Internet with vulnerabilities that can be exploited to launch an attack [4]. With the well developed DDoS tools, even an inexperienced user can start an attack easily.

IV. ATTACK: MODUS OPERANDI

Here we describe a typical DDoS attack scenario and its strategy. Fig .2 shows a hierarchical model of a DDoS attack. The most common attacks involve sending a large number of packets to a destination, thus causing excessive amounts of endpoint, and possibly transit, network bandwidth to be consumed [5]. The attack usually starts from multiple sources to aim at a single target. In order to launch a DDoS attack, the attacker first scan millions of machines for vulnerable service and other weakness that permits penetrations, then gain access and compromise these machines so called handlers, and zombies or slaves. After being installed the malicious scripts, such as scanning tools, attack tools, root kits, handler and zombie program, and lists of vulnerable and previously compromised hosts, etc., these infected machines can recruit more machines.

This propagation phase is quite like computer viruses. Then the communication channels between the attacker and the handlers and between the handlers and zombies are established [16]. These control channels are designed to be secret to public, in order to conceal the activity of attacker. TCP, UDP, ICMP, or a combination of these protocols is used to perform the communication [17]. Staying behind the scenes of attack, the real attacker sends a command to the handlers to initiate a coordinated attack. When the handlers receive the command, they transfer it to the zombies under their control. Upon receiving attack commands, the zombies begin the attack on the victim. The real attacker is trying to hide himself from detection, for example, by providing spoofed IP addresses [2].

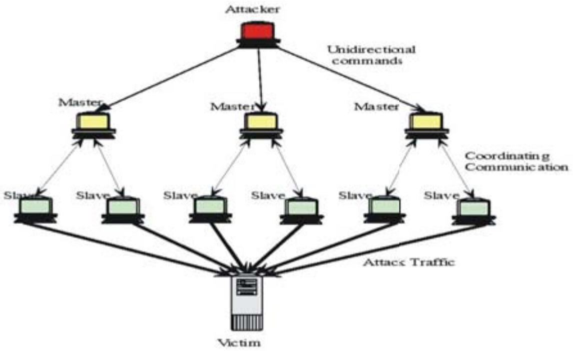

Fig .2 A hierarchical model of a DDoS attack

It makes difficult to trace the real source of attacker and filter malicious packets from the legitimate traffic.

In short, A DDoS attacks compose of following phases:

Recruitment: The attacker chooses the vulnerable agents, which will be used to perform the attack.

Compromise: The attacker exploits the vulnerabilities of the agents and plants the attack code, protecting it simultaneously from discovery and deactivation.

Communication: The agents inform the attacker via handlers that they are ready.

Attack: The attacker commands the onset of the attack [7].

V. ATTACK MECHANISMS

Various attack mechanisms can be used by attackers that can be classified as follows:

A. Based on attacking methods

From the technical point of view, we classify the attacks by attacking methods in this section. The resources consumed by attacks include network bandwidth, disk space, CPU time, data structures, printers, tape devices, network connections, etc.

1) *TCP SYN flooding:* SYN flood sends a flood of TCP/SYN packets, often with a forged sender address. Each of these packets are handled like a connection request, causing the server to spawn a half-open connection, by sending back a TCP/SYN-ACK packet, and waiting for an TCP/ACK packet in response from the sender address. However, because the sender address is forged, the response never comes. These half-open connections consume resources on the server and limit the number of connections the server is able to make, reducing the server's ability to respond to legitimate requests until after the attack ends [18,19,20,21].

2) *TCP reset:* TCP reset also exploit the characteristics of TCP protocol. By listening the TCP connections to the victim, the attacker sends a fake TCP RESET packet to the victim. Then it causes the victim to inadvertently terminate its TCP connection [22,23].

3) *UDP flooding:* This type of attack, most commonly exploits the chargen or echo services, creating an infinite loop between two UDP services. When a connection is established between two UDP services, each of which produces output, these two services can produce a very high number of packets that can lead to a denial of service on the machine(s) where the services are offered. Anyone with network connectivity can launch an attack; no account access is needed [23, 6, 24].

4) *ICMP attack:* Smurf attack sends forged ICMP echo request packets to IP broadcast addresses. These attacks lead large amounts of ICMP echo reply packets being sent from an intermediary site to a victim, accordingly cause network congestion or outages [23,25].

5) *DNS request Attack:* In this attack scenario, the attack sends a large number of UDP-based DNS requests to a name server using a spoofed source IP address. Then the name server, acting as an intermediate party in the attack, responds by sending back to the spoofed IP address as the victim destination. Because of the amplification effect of DNS response, it can cause serious bandwidth attack [1,26].

6) *Ping of Death:* The Ping of Death is a typical TCP/IP implementation attack. In this assault, the DDoS attacker creates an IP packet that exceeds the IP standard's maximum 65,536 byte size. When this fat packet arrives, it crashes systems that are using a vulnerable TCP/IP stack. No modern operating system or stack is vulnerable to the simple Ping of Death, but it was a long-standing problem with Unix systems [27].

7) *CGI request:* By simply sending multiple CGI request to the target server, the attacker consumes the CPU resource of the victim. Then the server is forced to terminate its services [28].

8) *Mail bomb:* A mail bomb is the sending of a massive amount of e-mail to a specific system. A huge amount of mail may simply fill up the recipient's disk space on the server or, in some cases, may be too much for a server to handle and may cause the server to stop functioning. This attack is also a kind of flood attack [29].

9) *Land Attacks:* A Land attack is similar to a SYN attack, the only difference being that instead of a bad IP Address, the IP address of the target system itself is used. What this means is that in a Land Attack, the attacker sends SYN packets to a particular port of the target system with the source address and source port number of these SYN packets, being same as the destination IP Address and port number. This creates an infinite loop between the target system and the target system itself and hangs, crashes etc it [30].

B. Based on Attack Traffic Distribution

In order to defeat aggregate based defense, attackers try to distribute attack traffic uniformly throughout all ingress points of attacked autonomous system. This is called isotropic distribution of attack traffic whereas if attack traffic is aggregated in certain parts of Internet more then it called Non-isotropic distribution of attack traffic [2].

C. Based on Attack packets used

Third classification is on the basis of attack packets used. Semantic DDoS attacks are normally launched with control packets like TCP SYN, TCP FIN, ICMP echo packets whereas for launching brute force DDoS attacks control as well as data packets like HTTP, FTP (involving TCP), UDP, and ICMP bogus packets can be used.

D. Based on Protocol used

On the other hand network protocols based classification of DDoS attacks basically divide DDoS attacks into TCP, UDP, and ICMP protocols as for semantic and brute force attacks either of these protocol packets are used.

VI. DEFENSE MECHANISMS

Various defense mechanisms are given to defend against these attacks, which can be classified as follows:

A Basic defense Mechanisms

There are some basic issues to defend against DoS attacks. These issues should be taken care of by any organization or individual having hosts connected to the Internet. All defense mechanisms listed here are effective in preventing or making it more difficult to exploit logic DoS attacks [6].

1) *Disabling Unused Services:* In general, if network services are unneeded or unused, the services should be disabled or removed to prevent tampering and attacks. The less there are applications and open ports in hosts, the less there are vulnerabilities to be exploited by an attacker. Default installations of operating systems often include many applications not needed by a user. Especially many home-users do not even know, what services are running on their systems. A vulnerability scanner can be used to detect what network services (open ports) are available in a network.

2) *Using firewall*: A firewall or a filtering router with similar abilities should be used to Filtering all packets entering and leaving the network protects the network from attacks conducted from neighboring networks, and prevents the network itself from being an unaware attacker. Even if there are many services available from local hosts, not all of these services need to be accessible from the public Internet. This measure requires installing ingress and egress packet filters on all routers.

3) *Disabling IP Broadcasts:* By disabling IP broadcasts, host computers can no longer be used as amplifiers in ICMP Flood and Smurf attacks. However, to defend against this attack, all neighboring networks need to disable IP broadcasts.

4) *Applying Security Patches:* To guard against denial of service attacks, host computers must be updated with the latest security patches and techques.

5) *Removing known security holes:* The DDoS tool deployment phase and many logic DoS attacks are based on exploiting vulnerabilities in host software. Removing known security holes prevents re-exploitation of vulnerabilities for example with publicly available scripts. In practice, this important defense is often neglected which makes it possible for available exploits to have lifetimes up to several years.

6) *Strong password:* Attackers should not be able to get unauthorized access to hosts, e.g., by exploiting weak passwords. A minimum requirement is to use passwords which are difficult to guess with or without existing password cracking tools.

7) *Antivirus software:* The antivirus software should be using the most recent virus definition database. This helps detecting known worms and viruses. Antivirus software can thus be considered as IDS [2, 3, 6, 10].

B. Defense based on Activity

There are basically four approaches to combat with DDoS attacks: Prevention, Detection and Characterization, Traceback, and Tolerance & Mitigation.

1) *Attack prevention:* Prevention aims to fix security holes, such as insecure protocols, weak authentication schemes and vulnerable computer systems, which can be used as stepping stones to launch a DoS attack [36]. This approach aims to improve the global security level and is the best solution to DoS attacks in theory. There are three precautions against DDoS attacks. First, the ISPs are strongly recommended to install ingress filters to stop IP address spoofing. Second, the end host should repair their security holes as soon as possible, especially for some well-known software and protocol bugs. Third, the end hosts are encouraged to install the Intrusion Detection System (IDS) to prevent from being compromised by the adversary [37,9].

2) *Detection and Characterization:* The next approach to deal with DDoS attacks is to find novel ways for detection and characterization of attacks so that they are completely filtered. The process of identifying that a network or server is under attack after launch of the attack is called detection. Detection can be passive, proactive, and On-time. Characterization means differentiating attack packets from legitimate packets by looking at some feature/header of packets which are derived from monitoring and analysis at various times and points of the Internet evaluations criteria exist which can compare different approaches [2].

a) *Anomaly detection*: The most common used DDoS detection and characterization schemes are anomaly based. Anomaly detection relies on detecting behaviors that are abnormal with respect to some normal standard. Many anomaly detection systems and approaches have been developed to detect the faint signs of DDoS attacks [4, 6, 7].

b) *Misuse based detection:* It is normally applied in prevention techniques as in this case the packets which are intelligently crafted to exploit end point protocols and operating systems are easily identified by their unique header or payload values or in other terms attack signatures. Misuse detection identifies well-defined patterns of known exploits and then looks out for occurrences of such patterns [32, 36, 9].

c) *Congestion based Detection:* It is normally used when we look for broad attack signatures however aggressive flows are also successfully identified in However congestion based schemes are found to be suitable only for high bandwidth attacks [2,10].

3) *Traceback:* Tracing is one of the best strategies to not only curb the menace of DDoS attacks but also arranging enough evidence to prove the identity of attacker so that he should be punished in such a manner that next time nobody should dare doing these attacks[10]. Once an attack has been detected, an ideal response would be to block the attack traffic at its source and identify complete Botnet. In all traceback solutions input debugging, state keeping, extra resource requirement, ICMP messages and IP packet marking overheads are involved. Moreover security of this communication so that these control messages should not be forged in terms of Confidentiality, Authentication, Integrity, and freshness is a big hurdle to tackle. Co-operation between ISPs is always bump to bear with. At the moment traceback in combination with tolerance and mitigation is popular methodology to defend DDoS! attacks. A number of approaches have been proposed for IP traceback, such as link testing, controlled flooding, ICMP-based iTrace, probabilistic packet marking (PPM), and so on [34]. By compared with other IP traceback approaches on management cost, additional network and router load, and the ability to trace multiple simultaneous attacks, PPM has more advantages [35].

4) *Tolerance & Mitigation:* The last but mostly used strategy assumes that because of limitations of prevention, detection and characterization, and finally tracing it is almost impossible to prevent, accurately detect and characterize without false positives and negatives, and trace back to ultimate attacker when attack is in progress or passive when attack is over[7]. It focuses on minimizing the attack impact and on maximizing the quality of its services. The idea of fault tolerance is that by duplicating the network's services and diversifying its access points, the network can continue offering its services when one network link is congested by flooding traffic [32, 33]. So in Tolerance and mitigation, we try to rate limit traffic from the sources mostly ingress edges of ISPs from where we suspect more attack traffic to enter.

C. Defense based on Deployment Location

Based on the deployment location, we divide DDoS defense mechanisms to the following categories:

1) *Victim-Network Mechanisms:* Most of the systems for combating DDoS attacks have been designed to work on the victim side. This is understandable since the victim suffers the largest damage from a DDoS attack and is therefore motivated to invest in a

defense system. A victim-end DDoS defense system facilitates easy detection because it can closely observe the victim, model its behavior and notice any anomalies. But, The defense system is on the path of the full-force attack, and may be overwhelmed by a large traffic volume. Examples of these systems are resource accounting, and protocol security mechanisms [31].

2) *Intermediate-Network Mechanisms:* An intermediate-network defense system, usually installed at a core router, detects the attack through anomalies observed at this router. As core routers handle large-volume, highly aggregated traffic, they are likely to overlook all but large-scale attacks. However, response is likely to inflict collateral damage as core routers can only accommodate simple rate-limiting requests and cannot dedicate memory or processor cycles to traffic profiling. Examples of these mechanisms are traceback and pushback [31,7].

3) *Source Network Mechanisms:* DDoS defense mechanisms at the source network can stop attack flows before they enter the Internet core and before they aggregate with other attack flows. Further, as it may monitor only a small portion of the attack, the defense system has difficulties in detecting anomalies. On the other hand, response effectiveness increases with proximity to the sources. A small attack volume enables an effective response as it is unlikely to overwhelm the defense system. An example of these mechanisms is proposed in [9,10]**.**

VII. CONCLUSION

An overview of DDoS problem, Vulnerabilities in Internet Architecture, Attack: Modus Operandi, different types of DDoS attacks, recent defense mechanisms and their effectiveness are presented in this paper.

DDoS attacks are a serious problem for which numerous defense mechanisms have been proposed, but none of them give reliable protection. Here we tried to present a methodology that would allow a classification of the DDoS attack problem in order to be able to find more effective solutions.

REFERENCES

[1] S. Cheung, “Denial of Service against the Domain Name System”, IEEE Security & Privacy, Jan/Feb. 2006, vol. 4 no. 1 pp. 40-45.

[2] K. Kumar, R.C. Joshi and K. Singh, “An Integrated Approach for Defending against Distributed Denial-of-Service (DDoS) Attacks”, iriss, 2006, IIT Madras.

[3] Y. Xiang, W. Zhou, M. Chowdhury,” A Survey of Active and Passive Defense Mechanisms against DDoS Attacks”, Technical report, TR C04/02, School of Information Technology, Deakin University, Australia, 2004.

[4] P. Zaroo, "A Survey of DDoS attacks and some DDoS defense mechanisms", *A part of course textbook Advanced Information Assurance (CS 626) in Purdue University*, 2002.

[5] F. Lau, S. H. Rubin, M.H. Smith, L. Trajkovic “Distributed Denial of Service Attacks” IEEE International Conference, 2000, VOL 3, pages 2275-2280.

[6] J. Molsa “Mitigating denial of service attacks: A tutorial”, Journal of computer security 13 (2005) 807-837 IOS Press.

[7] C. Douligeris, and A. Mitrokotsa, “DDoS attacks and defense mechanisms: classification and state-of-the-art,” *Computer Networks*, 2004, pp.643–666.

[8] Li-Chiou Chen, Thomas A. Longstaff, and Kathieen M. Carley, “Charterization of defense mechanisms against distributed denial of service attacks,” *Computer & Security 23,* 2004, pp.665-678.

[9] 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.

[10] C. Douligeris and A. Mitrokotsa**, “**DDoS attacks and defense mechanisms: classification”, ISSPIT 2003. Proceedings of the 3rd IEEE International Symposium on, pg. 190- 193.

[11] Felix Lau, Rubin H. Stuart, Smith H. Michael, and et al., "Distributed Denial of Service Attacks", Proceedings of 2000 IEEE International Conference on Systems*,* Man, and Cybernetics, Nashville, TN, Vol.3, pp.2275-2280, 2000.

[12] S. Crocker “Protecting the Internet from DDoS Attacks: A Proposal”,proc. of IEEE, vol. 92, No. 9, sept,2004.

[13] B. Gupta, K. Kumar, R. Joshi, K. Singh, “A Distributed approach using Entropy to detect DDoS attacks in ISP Domain”, proceeding of ICACS,2007.

[14] A. Householder, A. Manion, L. Pesante, George M. Weaver and R. Thomas, "Managing the Threat of Denial-of-Service Attacks", *CERT, http://www.cert.org/archive/pdf/Managing_DoS.pdf*, October, 2001.

[15] A. Garg, and A.L.N. Reddy, "Mitigating Denial of service Attacks using QoS regulation," *Proceedings of the Tenth IEEE International* Workshop on Quality of Service, pp. 45–53, 2002.

[16] X. Geng, and A.B. Whinston, "Defeating Distributed Denial of Service attacks," *IEEE IT Professional* ,pp 36–42, 2002.

[17] K. J. Houle and G. M. Weaver, "Trends in Denial of Service Attack Technology", *CERT, http://www.cert.org/archive/pdf/DoS_trends.pdf*, October, 2001.

[18] R. Farrow,"TCP SYN Flooding attacks", http://www.networkcomputing.com/unixworld/security/004/004.txt.html.

[19] CERT, "CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks," September 1996.

[20] Touch, J., "Defending TCP Against Spoofing Attacks," Internet- Draft (work in progress), draft-ietf-tcpm-tcp-antispoof-05, Oct, 2006.

[21] Eddy, W., "TCP SYN Flooding Attacks and Common Mitigations," Internet-Draft (work in progress), draft-ietf-tcpm-syn-flood-00, July 2006.

[22] TCP Reset, http://www.cisco.com/univercd/cc/td/doc/Product/voice/c_callmg/sec_vir/sec-up/tcpreset.htm.

[23] R. Azrina, R. Othman, "Understanding the Various Types of Denial of Service Attack", www.niser.org.my/resources/dos_attack.pdf.

[24] Javvin network management & security "UDP Flood attack",http://www.javvin.com/networkSecurity/UDPFloodAttack.html.

[25] Huegen, Craig A. "The Latest in Denial of Service Attacks: "Smurfing" Description and Information to Minimize Effects". 8 Feb, 2000.

[26] DNS request attack,http://en.wikipedia.org/wiki/DNS_cache_poisoning.

[27] M. Kenney, "Ping of Death", http://insecure.org/sploits/ping-o-death.html.

[28] CGI, http://cpan.uwinnipeg.ca/htdocs/CGI.pm/CGI.html.

[29] CERT® Coordination Center, http://www.cert.org/tech_tips/email_bombing_spamming.html.

[30] ikipedia,http://en.wikipedia.org/wiki/LAND.

[31] J.Ioannidis,S. M. Bellovin, "Implementing Pushback Router- Based Defense Against DDoS Attacks': hoc. EEE INFOCOMM Anchorage, AK, USA. pp. 878-886. Apr. 2001

[32] A. Garg, and A.L.N. Reddy, "Mitigating Denial of service Attacks using QoS regulation,"proceeding of tenth IEEE International *Workshop on Quality of Service*, pp. 45–53, 2002.

[33] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, "An architecture for differentiated services," *IETF, RFC 247 5*, 1998.

[34] Stefan Savage, David Wetherall, Anna Karlin et al, "Practical network support for IP traceback1", In Proc. ACM SIGCOMM Conf '00, Sweden, 2000,pp. 295-306.

[35] DQ Li, YD Xu, PR Su, DG Feng, "Adaptive packet Marking for IP Traceback", Acta lectronica Sinica, 2004, 32(8):1334~1337.

[36] X. Geng, and A.B. Whinston, "Defeating Distributed Denial of Service attacks," *IEEE IT Professional* ,pp 36–42, 2002.

[37] T. Peng, C. Leckie, and K. Ramamohanarao, "Protection from Distributed Denial of Service attack using history-based IP filtering," *Proceedings of IEEE International Conference on Communications (ICC 2003)*, *Anchorage, AL, USA*, 2003.

[38] CERT statistics, available at, http://www.cert.org/stats/cert_stats.html.

Mr. B.B.Gupta Research scholar, Department of Electronics and Computer Science IIT Roorkee. His area of research is Distributed Denial-of-Service and Defense Mechanisms. He has presented several papers in national and international conferences.