Survey On Taxonomy Of Ddos Attacks With Impact And Mitigation Techniques

Ms. Chandni M Patel[*1], *Asst. Prof. Viral H Borisagar*[#2]

** C.S.E. Department, Government College of Engineering, Sector-28,Gandhinagar Gujarat Technology University, Gujarat, India.*

 # C.S.E. Department, Government College of Engineering, Sector-28, Gandhinagar Gujarat Technology University, Gujarat, India

Abstract

Recently many prominent web sites face so called Distributed Denial of Service Attacks (DDoS). DDoS attacks are a virulent, relatively new type of attack on the availability of Internet services and resources. To avoid denigration most of the commercial sites do not expose that they were attacked that is the biggest challenges of the researchers. In this paper survey on taxonomy of DDos attacks with Impact and mitigation techniques are done.

Keywords: — DOS, DDos, zombies, botnets, deplition, incidents, factors affecting DDos, Mitigation techniques.

1. Introduction

An aim of an internet is to provide scalable, open [1] and secured network. Confidentiality, authentication, message integrity and non repudiation are the basic aspects of the internet security. As the Internet is breeding in size and complexity its visibility and diversity is also increased which gives the impressions to attract a variety of highly damaging attacks. A Denial of Service (DoS) attack can be characterized as an attack with the purpose of preventing legitimate users from using a victim computing system or network resource. Distributed denial of service (DDos) attack targets the availability of services on the Internet. It is one kind of Denial of service attack. A DDoS attack can be characterized as a simultaneous network attack on a victim from large numbers of hosts, well distributed throughout the network [2]. Many to one nature of DDoS attack makes it more powerful and difficult to prevent. DDoS attacks are a case where several hundreds of zombies or botnets (compromised machines) are involved in the generation of attack traffic. In most of the cases, the owners of the zombie machines are not even aware that their systems are compromised and being used to generate DDoS attacks [3]. As defined by the World Wide Web Security FAQ*:"* A Distributed Denial of Service (DDoS) attack uses many computers to launch a coordinated DoS attack against one or more targets. Using client/server technology, the perpetrator is able to multiply the effectiveness of the Denial of Service significantly by harnessing the resources of multiple unwitting accomplice computers which serve as attack platforms"[4]. DDoS attack first appears in July, 1999. At that time, it is just one theoretical research on the hacker network. But through the rapid development of internet since February, 2002. DDoS attack becomes more and more serious get along with the increase of network speed and bandwidth. Because the DDoS attack is harmful to the users, detection and defense has the vital significance.[5]

In this paper survey on section 2 describes what is DDos attack and DDos attack process.In section 3 various types of DDos attacks are described.Section 4 illustrates the various factors which causes DDos attacks.Section 5 gives related information regarding various DDos Incidents, losses due to attack ,threat landscap of DDos attacks and impact of DDos attack in network.Section 6 describes DDos attack mitigation techniques. So overall paper comprises the taxonomy of DDos attack and impact analysis with DDos mitigation strategies.

2 DDos Attacks

DDoS attacks are highly distributed, well coordinated, offensive assaults on services, hosts, and infrastructure of the Internet. Effective defensive countermeasures to DDoS attacks will require equally sophisticated, well coordinated, monitoring, analysis, and response.[2]

DDos Overview

"Distributed denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include: [24]
1) attempts to "flood" a network, thereby preventing legitimate network traffic
2) attempts to disrupt connections between two machines, thereby preventing access to a service
3) attempts to prevent a particular individual from accessing a service
4) attempts to disrupt service to a specific system or person

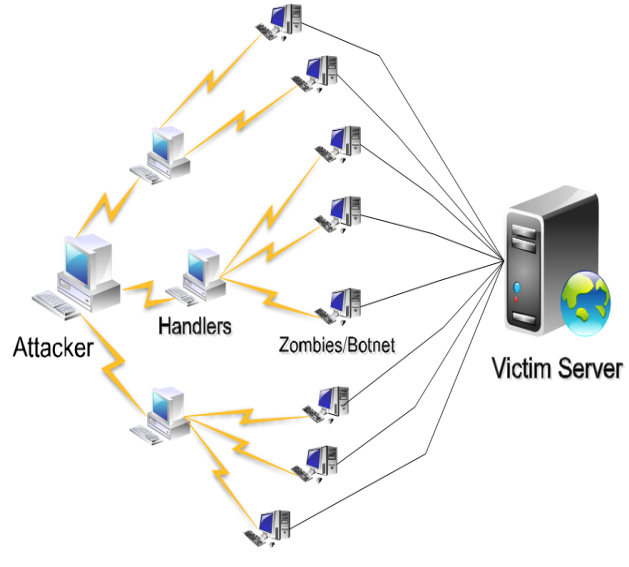

Fig. 1 DDos Architecture

As shown in fig.1 A typical DDoS attack contains two stages, the first stage is to compromise susceptible systems that are accessible in the Internet and install attack tools in these compromised systems. This is known as turning the computers into "zombies." In the second stage, the attacker sends an attack command to the "zombies" through a secure channel to launch a bandwidth attack against the targeted victim(s).[6]

DDoS Attack Process [5]

Step 1)Information Collection of Target Host

Before invade the network, attacker needs to collect and understand the host's condition. Attacker cares such as host quantity and address configuration, system layout and performance, bandwidth and so on. For instance, if attacker attacks at one website, he must confirm how many hosts are supporting this website. Because one big website might need many hosts to support the services by using load balance technology. On the basis of host quantity, attacker can assure the attack quantity to achieve the attack.

Step 2) Host Occupation

Attacker need to use the scan or other equipments to chose one or more zombie computers to carry out the attack. In order to avoid the efficient effect of network as well as the tracked monitoring attack, zombie host usually stand outside the attack network and target network. Zombie host must be fragility enough to control and need to equip with enough resource to create the powerful attack data flow. Attacker can use them to send attack data package to the targets.

Step 3) Initiate Actual Attack

After former 2 stage preparations, attacker can bring the attack into operation. In the first place, log in the control zombie and send attack orders to the entire attack zombies. And the hided DDOS attack programs will send out amount of data packages to the host with the speed which beyond the host management. Then the hosts will dead halt or no response to the normal requirements. Some expert attackers will attack and monitor the attack effect with different measures at the same time so that can make the relative modulations. The simplest method is open so much windows to ping the hosts. When receive the responses, it will crease the flow rate or more hosts to attack until the target host breakdown. From the process we can know that attacker can falsify the IP address to avoid the tracking.

Attacker can off line when send out the attack orders or after the attack computer respond. So even find out the zombie host, get hold of the attack is still a difficulty.

3 Taxanomy Of DDos Attacks

There are different types of DDos attacks Techniques. There are two main classes of DDoS attacks: bandwidth depletion and resource depletion attacks.

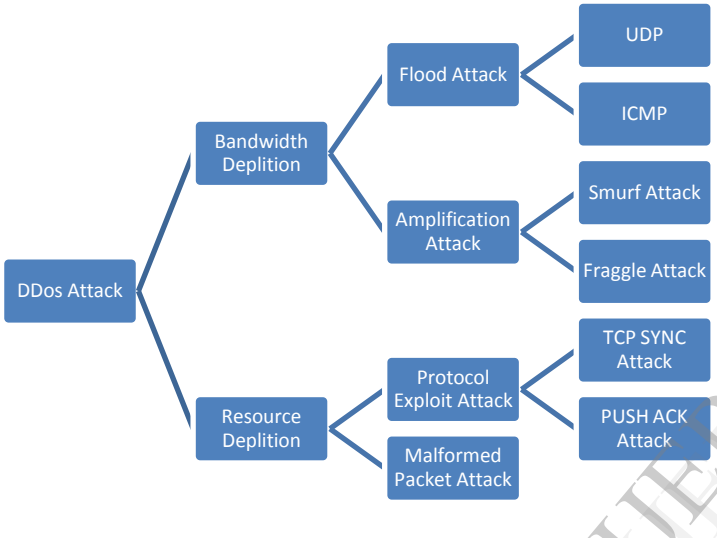

Fig.2 Taxonomy of DDos Attacks

3.1) Bandwidth Depletion attack

A bandwidth depletion attack is designed to flood the victim network with unwanted traffic that prevents legitimate traffic from reaching the (primary) victim system.

Flood Attack [27]

In a DDoS flood attack the zombies flood the victim system with IP traffic. The large volume of packets sent by the zombies to the victim system slows it down, crashes the system or saturates the network bandwidth. This prevents legitimate users from accessing the victim.

Smurf Attack [27]

In a DDoS Smurf attack, the attacker sends packets to a network amplifier with the return address spoofed to the victim's IP address. The attacking packets are typically ICMP ECHO REQUESTs, which are packets 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.

Mail bomb attack [6]

A mail bomb is the sending of a enormous amount of e-mail to a specific person or 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 working. This attack is also a kind of flood attack [9].

Spam Attack

This type of attack is used for targeting the various mail services of corporate as well as public users. DDoS attack through spam has increased and disturbed the mail services of various organizations. Spam penetrates through all the filters to create DDoS attacks, which causes serious trouble to users and the data. But these mail services are frequent target of hackers and spammers.[6,10]

Fraggle Attacks [27]

A DDoS Fraggle attack is similar to a Smurf attack in that the attacker sends packets to a network amplifier. Fraggle is different from Smurf in that Fraggle uses UDP ECHO packets instead of ICMP ECHO packets. There is a variation of the Fraggle attack where the UDP ECHO packets are sent to the port that supports character generation with the return address spoofed to the victim's echo service creating an infinite loop The UDP Fraggle packet will target the character generator in the systems reached by the broadcast address. This attack generates even more bad traffic and can create even more damaging effects than just a Smurf attack

DNS request attack [6]

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 [6,8]

Algorithmic complexity attack [6]

It's a class of low-bandwidth DDoS attacks that exploit algorithmic deficiencies in the worst case performance of algorithms used in many mainstream applications. For example, both binary trees and hash

tables with carefully chosen input can be the attack targets to consume system resources greatly [6,9].

3.1.2) Resource Depletion attack

A resource depletion attack is an attack that is designed to tie up the resources of a victim system. This type of attack targets a server or process on the victim system making it unable to process legitimate requests for service.[6]

TCP Reset Attack [6]

TCP reset also utilize 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 [6,7].

TCP SYN Attack [27]

In a DDoS TCP SYN attack, the attacker instructs the zombies to send such bogus TCP SYN requests to a victim server in order to tie up the server's processor resources, and hence prevent the server from responding to legitimate requests. Eventually, if the volume of TCP SYN attack requests is large and they continue over time, the victim system will run out of resources and be unable to respond to any legitimate users.

PUSH + ACK Attacks [27]

The PUSH + ACK attack is similar to a TCP SYN attack in that its goal is to deplete the resources of the victim system The attacking agents send TCP packets with the PUSH and ACK bits set to one. These packets instruct the victim system to unload all data in the TCP buffer and send an acknowledgement when complete. If this process is repeated with multiple agents, the receiving system cannot process the large volume of incoming packets and it will crash.

Malformed Packet Attacks [27]

A malformed packet attack is an attack where the attacker instructs the zombies to send incorrectly formed IP packets to the victim system in order to crash the victim system. There are two types of malformed packet attacks. In an IP address attack, the packet contains the same source and destination IP addresses. This can confuse the operating system of the victim system and cause the victim system to crash. In an IP packet options attack, a malformed packet may randomize the optional fields within an IP packet and set all quality of service bits to one so that the victim system must use additional processing time to analyze the traffic. If this attack is multiplied using enough agents, it can shut down the processing ability of the victim system.

UDP storm attack [6]

This kind of attack can not only impair the hosts. Services, but also congest or slow down the prevailing network. When a connection is established between two UDP services, each of which produces a very huge number of packets, thus cause an attack.[6]

4 Factors affecting DDos Attack

One of the major reasons that make the DDoS attacks wide spread and easy in the Internet is the availability of attacking tools and the powerfulness of these tools to generate attacking traffic [12]. As per [11], [13] various reasons that create opportunities for attackers to use attack tools easily and launch a successful attack are:[1]

1) Internet security is highly interdependent: The susceptibility of DDoS attacks depends upon global internet security rather than the security of victim.

2) Internet resources are limited: Each Internet host has limited resources that can be consumed by a sufficient number of users.

3) Accountability is not enforced: With mechanisms like IP spoofing, the perpetrator can conceal his real identity and hence, real source of attack cannot be judged.

4) Control is distributed: Since Internet management is distributed and each network runs as per particular policies and regulations defined, it is almost impossible to deploy a certain global security mechanism and moreover due to privacy concerns it is sometimes nearly impossible to investigate the cross network behavior.

5) Simple Core and Complex Edge: One of the design principles is that the Internet should keep the core networks simple and push any complexity into the end hosts [1,13,14]. Hence, core routers don't make necessary authentication checks. The void of authentication checks at network level encourages undesired unauthorized attempts like IP spoofing, which is the major way of doing DDoS attack.

6) Multipath Routing: Multipath routing makes authentication difficult hence, it may encourage unauthorized activities. Intermediate router routes IP

packet from source to destination & has no way of knowing that whether the IP packet it is forwarding is the legitimate packet or a spoofed one [1,13].

5 DDos Incidents

Attack communities are well coordinated and synchronized with each other and hence, have high potential.They use the distributed traffic to create the botnet and flood the packets targeting victim. This makes tracing of the identity of attacker difficult and thus attacker escapes the witty eye. The DDoS attacking programs have very simple logic structures and small memory requirements which make them easy to implement and hide. Besides, many tools for DDoS attacks are available, high qualification is not required to use them. Hence, DDoS attacks have emerged as a weapon of choice for disruption on the Internet.

Any one on the network is prone to DDos attack, it may be financial institutes or banks or multinational corporations or government or defense agencies etc. Even very high profile websites like Yahoo, eBay, E Trade, Buy, Amazon, Twitter, Facebook etc were Web sites fell victim to DDoS attacks [15]. In January 2001, Register.com was targeted, DNS servers were used as reflector in that attack [16]. On two occasions to date, attackers have performed DNS Backbone DDoS Attacks on the DNS root servers. The first occurred in October 2002 and disrupted service at 9 of the 13 root servers. The second occurred in February 2007 and caused disruptions at two of the root servers [17], [18]. Even CERT/CC, one of the Internet's leading network security sites, was also suffered from DDoS attack in May, 2001 [19].In the same year, DDoS attack was launched targeting Whitehouse.gov domain [20].In January 2004, MyDoom attacked 1 million computers [21]. In February 2007, more than 10,000 online servers in games such as such as Return to Castle Wolfenstein, Halo, Counter- Strike and many others were attacked [17]. After one year, WordPress.com was attacked resulting in 15 minutes of outage [15]. The incidents citing DDoS attacks are endless. These attacks demonstrate the potential of attacks.

Table 1 [1, 26]

Recent DDos Attack Incidents		
Date	**DDos Incidents**	**Description**
October 21,2012	HSBC Bank of America	disrupted daily operations for banks
September 25,2012	Bank of America website	disrupted daily operations for banks
September 11,2012	GoDaddy takes down	Millions of website are out of service
March , 2012	South Korea and United states Websites	It is similar to those launched in 2009.
January 1,2012	Official Web-site of the office of the vice president of Russia	It caused the site to be down by more than 15 hours.
November 5 to 12 , 2011	Asian Ecommerce Company	Flood of Traffic was launched and 250,000 Computers are infected with malware participated.
October ,2011	Site of National Election Com-mission of South Korea	Attacks were launched during the morning when citizens would look up information .and attack leads to fewer turnouts.
March 3,2011	On Blogging Platform Live Journal	Experienced serious functionality problems for over 12 Hours
December 8,2011	Master Card, PayPal, Visa and Post Finance	Attack was launched in support of WikiLeaks.ch and its founder.
November 30,2011	Whistleblower site Wikileaks	Attack size was 10Gbps. Caused the site unavailable to visitors.
November 12,2011	Domain registrar Regis-ter.com	Impacted DNS, hosting and webmail clients.
November 2,2010	Burma's main Internet provider	Disrupted most network traffic in and out of the country for 2 days.

October.2010	MPAA & Indian tech firm Aiplex software	At least hundreds of 4chan users at once executed at-tack in Pro-piracy protest. Simple application Low Orbit Ion Cannon (LOIC) was used.
September,2010	Fast growing botnet	Botnet's motive was to provide commercial service
June,2010	Broadband forum Whirlpool	Flooding DDoS attack
May,2010	Vocus	Caused connectivity disruptions across multiple web-sites.
May,2010	Web24	Caused Connection issues for users of the Vocus net-work
April,2010	Optus	Sourced from China. 4 hours of outage.
February,2010	Australian Parliament House website (www.aph.gov.au)	Attack was the part of protest by a group.
December 23,2009	DNS services provider Neustar	Amazon, Wal-Mart, and Expedia were affected
August 6,2009	Twitter, Facebook, Livejournal, and Google blogging pages	Hundreds of millions of Internet users affected.
October,2009	40 Swedish sites	About 40 websites belonging to police & media went down.
April 1,2009	Cloud computing provider GoGrid	Service was disrupted to about half of its 1,000 customers
January,2009	GoDaddy.com	Affected
		thousands of its shared hosting customers.

Financial Loses Incurred Due To Attack Incidents

As proof of these disturbing trends, 2003 to 2006 FBI/CSI surveys [22,23] concluded that DoS/DDoS attacks are one of the major causes of financial losses [26]as depicted in Figure 3 below:

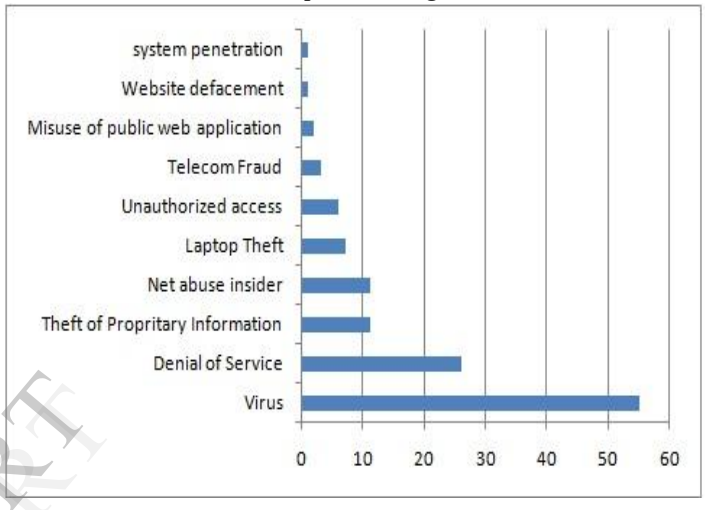

Fig.3 Financial Loss

Threat landscape of DDoS attacks [28]

Below Fig 4 shows a flow of DDoS attacks, surpassing all previous records. Amazingly a majority of these distributed denial-of-service attacks were not recognized due to bandwidth constraints. In the supplementary graph it is clearly seen that network-based DoS attacks were fewer than application-level DDoS attacks. A majority of the attacks exploited the HTTP and its sibling HTTPS protocols. Attackers recognize that volumetric attacks can be mitigated by use of scrubbers on the cloud, so they opt for slow and low DoS attacks, choosing applications as the target instead of networks.

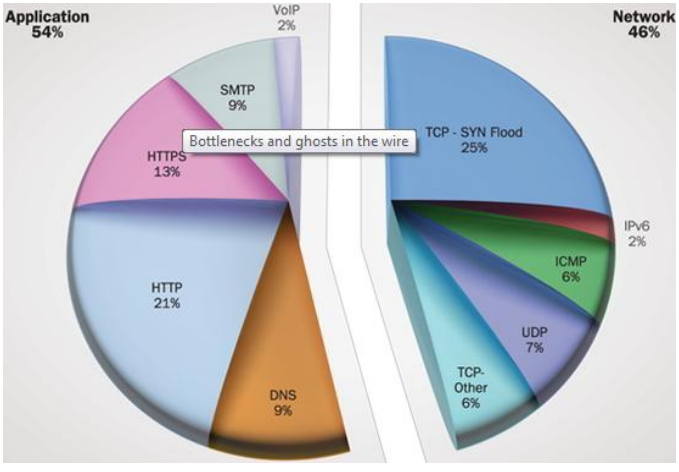

Fig.4 Threat Landscape [28]

6 DDos attack mitigation tequniques [27]

Load Balancing

For network providers, there are a number of techniques used to mitigate the effects of a DDoS attack. Providers can increase bandwidth on critical connections to prevent them from going down in the event of an attack. Replicating servers can help provide additional failsafe protection in the event some go down during a DDoS attack. Balancing the load to each server in a multiple-server architecture can improve both normal performance as well as mitigate the effect of a DDoS attack.

Throttling

One proposed method to prevent servers from going down is to use Max-min Fair server-centric router throttles. This method sets up routers that access a server with logic to adjust (throttle) incoming traffic to levels that will be safe for the server to process. This will prevent flood damage to servers. Additionally, this method can be extended to throttle DDoS attacking traffic versus legitimate user traffic for better results. This method is still in the experimental stage, however similar techniques to throttling are being implemented by network operators. The difficulty with implementing throttling is that it is still hard to decipher legitimate traffic from malicious traffic. In the process of throttling, legitimate traffic may sometimes be dropped or delayed and malicious traffic may be allowed to pass to the servers.

Honeypots

Honeypots are systems that are set up with limited security to be an enticement for an attacker so that the attacker will attack the Honeypot and not the actual system. The goal of this type of honeypot is to attract a DDoS attacker and get him to install either handler or agent code within the honeypot. This prevents some legitimate systems from getting compromised and allows the honeypot owner to track the handler or agent behavior and better understand how to defend against future DDoS installation attacks.

7 Conclusion

The major contributions of this paper are the survey of overview of DDos attack, the main security defects which causes the DDos attack, taxonomy of DDos attacks, recent DDos attack incidents, DDos attack incidents history from 2009-2012 ,impact analysis of attack and financial loss incurred due to attack and DDos attack mitigation techniques are done.

References

[1] Ketki Arora, Krishan Kumar, Monika Sachdeva "Impact Analysis of Recent DDoS Attacks" International Journal on Computer Science and Engineering (IJCSE)ISSN : 0975-3397 Vol. 3 No. 2 Feb 2011

[2] Christos Papadopoulos, Robert Lindell, John Mehringer, Alefiya Hussain, Ramesh Govindan" COSSACK: Coordinated Suppression of Simultaneous Attacks" Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX'03) 0-7695-1897-4/03 © 2003 IEEE

[3] Udaya Kiran Tupakula ,Vijay Varadharajan, Sunil Kumar Vuppala"SBAC: Service Based Access Control" 14th IEEE International Conference on Engineering of Complex Computer Systems978-0-7695-3702-3/09 © 2009 IEEE

[4] Lincoln Stein and John N. Stuart. "The World Wide Web Security FAQ", Version 3.1.2, February 4, 2002. http://www.w3.org/security/faq/ (8 April 2003).

[5] Liang Hu, Xiaoming Bi" Research of DDoS Attack Mechanism and Its Defense Frame" 978-1-61284-840-2/11©2011 IEEE

[6] Akash Mittal "A Review of DDOS Attack and its Countermeasures in TCP Based Networks"International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.4, November 2011 DOI : 0.5121/ijcses.2011.2413

[7] Robert Vamosi, "Study: DDoS attacks threaten ISP infrastructure," Online at http://news.cnet.com/8301-1009_3-10093699-83.html, CNET News, Nov. 2008.

[8] A. Yaar, A. Perrig, and D. Song, "PI: A path identification mechanism to defend against DDoS attacks," in proceedings of the IEEE symposium on Security and Privacy, pp. 93-109, May 2003.

[9] Elinor Mills, "Radio Free Europe DDOS attack latest by hactivists," Online at http://news.cnet.com/8301-10784_3-9933746-7.html, CNET News, May. 2008.

[10] Dhinaharan Nagamalai, Cynthia Dhinakaran, Jae Kwang Lee. "Multi Layer Approach to Defend DDoS Attacks Caused by Spam". In aaXiv.org (Cornell university Library),arXiv: 1010.1583v1 [cs.CR]

[11] J. Mirkovic, and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," Computer Journal of ACM SIGCOMM,vol. 34, no. 2, pp. 39-53, Apr. 2004.

[12] B. Gupta, R. Joshi, and M. Misra, "Distributed Denial of Service Prevention Techniques," International Journal of Computer and Electrical Engineering, Vol. 2, no. 2, pp. 268-276, April, 2010.

[13] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network based defense mechanisms countering the DoS and DDoS problems," Computer Journal of ACM Computing Surveys, vol. 39, no. 1, pp. 123-128, Apr. 2007.

[14] J. Mirkovic, "D-WARD: source end defense against distributed denial of service attacks," Ph.D. thesis, University of California,2003.

[15] M. Sachdeva, G. Singh, K. Kumar, and K. Singh, "DDoS incidents and their impact :A review,"International Arab Journal of Information Technology, vol. 7, no. 1, pp. 14-19, Jan. 2010.

[16] Washington.edu, "A DNS reflection attack on register.com,"[Online].Available:http://ww.staff.washington.edu/dittrich/misc/ ddos/

[17] Wikipedia, "Denial-of-service attack," [Online]. Available: http://en.wikipedia.org/wiki/Denial-of-service_attack.

[18] ICANN. "Factsheet - Root server attack on 6 February 2007,"[Online].Available:http://ww.icann.org/announcements/factsheet-dns-attack-08mar07.pdf.

[19] A. Bennett. (2001) ITworld.com,"CERT hit by DDoS attack for a third day,"[Online].Available: http://www.itworld.com/IDG010524CERT2.

[20] R. Lemos. (2001) Cnet.com, "Hackers cripple white house site," [Online]. Available: http://news.cnet.com/2100-1001-257068.html.

[21] Parabon.com, "Distributed Denial of Service (DDoS) attack timeline," [Online]. Available: http://www.parabon.com/faqs/ddostimeline.html

[22] Cichardson R., "Computer Crime and Security Survey," http://www.crime-research.org/ news/ 11.06.2004 /423/, 2007

[23] Gordon A., Loeb P., Lucysgyn W., and Richardson R., CSI/FBI Computer Crime and Security Survey, CSI Publications, 2006.

[24] Priya Metri, Jayshree Ghorpade, Santaji Ghorpade," DDOS Attacks and Defense Mechanisms: An Overview", International Journal of Advances in Computing and Information Researches ISSN: 2277-4068, Volume 1– No.1, January 2012, 1 to 5

[25] Daljeet Kaur, Monika Sachdeva , Krishan Kumar," Recent DDoS Incidents and Their Impact" International Journal of Scientific & Engineering Research Volume 3, Issue 8, August-2012 1 ISSN 2229-5518,1 to 6

[26] Monika Sachdeva,Gurvinder Singh,Krishan Kumar,Kuldip Singh" DDoS Incidents and their Impact: A Review", The International Arab Journal of Information Technology, Vol. 7, No. 1, January 2010, 14 to 24

[27] Stephen Specht, Ruby Lee "Taxonomies of Distributed Denial of Service Networks, Attacks, Tools, and Countermeasures" http://www.princeton.edu

[28] Website http:// searchsecurity.techtarget.in / photostory/2240164376 /Five-DDoS-attack-tools-that-you-should-know-about/9/Threat-landscape-of-DDoS-attacks#contentCompress