Impact Analysis of Recent DDoS Attacks

Ketki Arora
Department of Computer Science & Engineering
LLR Institute of Engineering & Technology
Moga-142001, Punjab, India

Krishan Kumar, Monika Sachdeva
Department of Computer Science & Engineering
SBS College of Engineering & Technology
Ferozepur-152004, Punjab, India

***Abstract*— In the present era Internet has changed the way of traditional essential services such as banking, transportation, power, health, and defence being operated. These operations are being replaced by cheaper, more efficient Internet-based applications. It is all because of rapid growth and success of Internet in every sector. Unfortunately with the growth of Internet, count of attacks on Internet has also increased incredibly fast. Denial-of-service attack is one of them, which poses immense threat on the availability. Since, the World is highly dependent on the Internet, availability of the Internet is very critical for the socio-economic growth of the society. Denial-of-service attacks occur almost every day, and the frequency and the volume of these attacks are increasing day by day. One of the biggest challenges before researchers is to find the details of such attacks because due to damaging reputation issues, most of the commercial sites do not even disclose that they were blitzed by such attacks. Details of attacks can guide very well in the formulation of comprehensive defensive solution for such attacks. In this paper, an overview on DDoS problem, major factors causing DDoS attacks are demonstrated, brief detail of most recent DDoS incidents on online organizations is outlined and finally, the need for a comprehensive distributed solution is highlighted.**

Keywords- Availability; Botnet; DoS; DDoS incidents; vulnerability

I. INTRODUCTION

The original aim of Internet was to provide an open and scalable network, which could offer easy, fast and inexpensive communication mechanisms, and it was indeed very successful in accomplishing this particular goal. During Internet design, the functionality aspect was of much concern rather than security, due to which this design opens up several security issues that create a room for various attacks on the Internet. Internet security has several aspects such as confidentiality, authentication, message integrity and non repudiation. Availability is one of the main aspects of Internet security. Attacks such as denial of service and its variant distributed denial of service attack target the availability of services on the Internet. Threat to the Internet availability is a big issue and hampering the growth of online organizations those rely on having their websites 100% available to visitors, users and customers. DDoS attacks are not new assaults against the Internet. DDoS attacks marked their presence in August 1999 and continuing to attack various Web sites (including high-profile) since then. Due to the lack of a comprehensive and effective solution to combat such DDoS attacks, they are growing in frequency and volume.

This paper outlines DoS and DDoS attack overview and highlights some of the DDoS incidents occurred from 1999 to 2008 and briefs DDoS incidents occurred in the year 2010-2009 and also demonstrates the need of a comprehensive DDoS solution due to flood of incidents occurred in past few years.

The remainder of this paper is organized as follows. Section II discusses Internet attack and classification of Internet attacks according to unauthorized result is discussed. Section III demonstrates DoS and DDos overview and DDoS attack modus operandi. Section IV discusses factors which open the door for DDoS attacks on the Internet. Section V gives the details of various DDoS incidents from year 1999 to 2008 and highlights some recent DDoS incidents in year 2009-2010 in chronological order, also briefs monetary and non monetary impacts on online organizations due to DDoS attacks. Section VI highlights need of the comprehensive DDoS combat solution. Finally, section VII concludes the paper.

II. INTERNET ATTACKS OVERVIEW

The current architecture of Internet carries many security holes in it, which creates opportunities for attacker to launch a successful attack.

Before going through the detail about DDoS attacks, it is useful to have an overview and classification over internet attacks.

As per [1], definition of an attack can be a series of steps taken by an attacker to achieve an unauthorized result.

An attacker uses a tool to exploit a vulnerability to perform an action on a target in order to achieve an unauthorized result. Thus, attack is an assault against a computer system or network as a result of deliberate, intelligent action.

A. General Attack Classification

A possible classification of Internet attacks according to unauthorized result could be [1]

1) *Increased Access:* An unauthorized increase in the domain of access on a computer or network.
2) *Disclosure of Information*: Dissemination of information to anyone who is not authorized to access that information.
3) *Corruption of Information* - Unauthorized alteration of data on a computer or network. This may result in loss of information.
4) *Denial of Service*: Intentional degradation or blocking of computer or network resources. Its main goal is to disrupt the services to legitimate user.
5) *Theft of Resources*: Unauthorized use of computer or network resources.

III. DOS AND DDOS OVERVIEW

According to the WWW Security FAQ, a DoS attack can be described as an attack designed to render a computer or network incapable of providing normal services. A DoS attack is characterized by an intentional attempt by malicious users/attackers to completely disrupt or degrade availability of services/resources to legitimate/authorized users [2]. Hence, legitimate users are deprived of available services/resources they would normally expect to have. These attacks do not necessarily damage the data directly or permanently, but they deliberately compromise availability of the resources and thus, can cost the target a great deal of time and money. Some well known DoS attacks are SYN flood, Teardrop, Smurf, Ping of Death, Land, Finger Bomb, Black Holes, Snork, Octopus ARP Cache Poisoning and the Misdirection.

With the advent of time after the launch of denial-of -service attacks, the attackers became aware of defense mechanisms that were implemented to prevent and mitigate DoS attacks and to trace the identity of attackers. Moreover, with the evolution of technology ISPs became aware of how to prevent DoS attacks from blitzing their networks. Earlier DoS attacks were well known and can be defended by robust networking equipment and proper security practices. To overcome the downfalls of aggregate DoS attacks, the attackers launched Distributed DoS, which uses distributed traffic to attack victim also called Isotropic distribution. Distributed denial-of-service (DDoS) attack is the multitude form of denial of service (DoS) attack. DDoS is relatively simple, yet more powerful technique. It is a large-scale, coordinated attack on the availability of Internet services and resources. It uses same techniques as regular DoS, but on a much larger scale. It is a denial of service attack that occurs from more than one source, and/or more than one location, at the same time [8].The primary goal of these attacks is to prevent access to a particular resource like a Web site [3]. DDoS attack attains its goal by flooding the victim with great volume of packets that consumes its network or processing capacity and thus denying access to its legitimate users. There are varieties of DDoS attacks as classified in [4], [5]. However, the most common form of DDoS attacks is a packet-flooding attack, in which a large number of seemingly legitimate TCP, User Datagram Protocol (UDP), or Internet Control Message Protocol (ICMP) packets are directed to a specific destination.

A. DDOS Attack Method

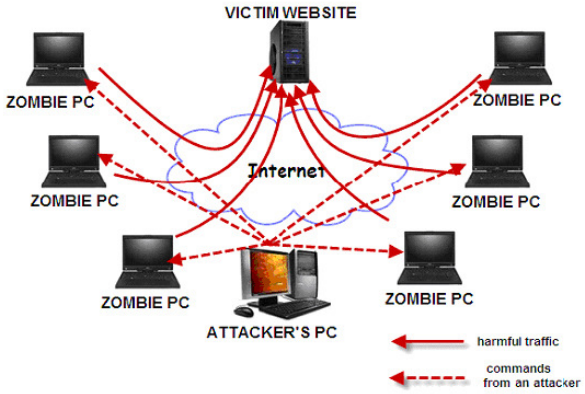

Figure 1. DDoS attack architecture

DDoS attack does not rely on particular network protocol or system weakness. It simply exploits the huge resource asymmetry between the Internet and the victim [7]. Since Internet architecture is open in nature, any machine attached to it is publically visible to another machines attached to enable the communication. The hacker or attacker community takes the unhealthy advantage of this open nature to discover any insecure machine connected to the Internet. The discovered machine is thus infected with the attack code. The infected machine can further be used to discover and infect another machine connected and so on. The attacker thus gradually prepares an attack network called botnet. Depending upon the attacking code the compromised machines are called Masters/Handlers or zombies. Hackers send control instructions to masters, which in turn control zombies. The zombies under the control of masters/handlers transmit attack packets as shown in Fig. 1, which converge at victim to exhaust its resources. DDoS attack basically targets victim's computational or communicational resources [11], such as bandwidth, memory, CPU cycle, file descriptors and buffers etc.

DDoS attack can be flooding attack or vulnerability attack [4], [9]. Flooding attack eats up the victim resources by flooding the large volume of packets. Vulnerability attacks use the expected behavior of protocols such as TCP and HTTP to the attacker's advantage.

During flooding attack as shown in Fig. 2, the attackers congest the link between ISP edge router and victim's access router by flooding packets towards victim. This results in the consequence that the legitimate clients are denied of the service due to limited bottleneck bandwidth.

When the total request rate becomes more than total service rate the requests will start buffering at victim server and with the passage of time incoming requests are dropped due to buffer overflow. The congestion and flow control signals [16], [17] force the legitimate clients to decrease their rate of sending packets, however, attack packets continue to come at the distribution rate specified by attacker. Hence, a stage comes when whole of bottleneck bandwidth is seized by attack packets. As per [12], as attack strength grows by using multiple sources, the computational requirements of even filtering traffic of malicious flows become a burden at the target. The distributed nature of DDoS makes it very difficult to prevent and mitigate. The effects of DDoS attacks are very severe. It enables attacker to conceal its identity very well.

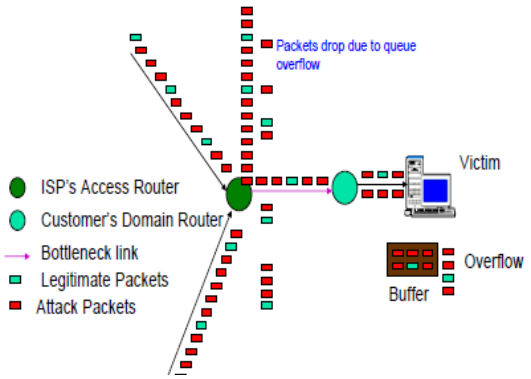

Figure 2. Packets drop during DDoS attack

IV. MAJOR FACTORS CAUSING 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 [6]. As per [4], [9] various reasons that create opportunities for attackers to use attack tools easily and launch a successful attack are:

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 [9], [10]. 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 [9].

V. DDOS INCIDENTS

Attack communities are well coordinated and synchronized with each other and hence, have high potential. The Distributed denial-of-service attackers are mischievous and use the best effort method to prevent them from being traced out. 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. As the strength of attackers is growing by the use of multiple sources, the methods to mitigate and prevent the distributed denial-of-service attacks are becoming a great challenge for the defenders.

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 distributed denial-of-service 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 [13]. In January 2001, Register.com was targeted, DNS servers were used as reflector in that attack [14]. 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 [15], [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 [15]. After one year, WordPress.com was attacked resulting in 15 minutes of outage [13]. The incidents citing DDoS attacks are endless. These attacks demonstrate the potential of attackers.

A. Recent DDOS Incidents

DDoS attacks are launched almost every day. Even the most prominent Websites like Twitter, Facebook, g Google etc couldn't escape themselves from being hit by it, which caused millions of their users affected. The most eye opener case was the DDoS incident that targeted White house, Federal Trade Commission and the Department of the Treasury. Washington Post and the New York Stock exchange, NASDAQ. A Botnet comprised of 30,000 – 60,000 infected computers were used. The attack traffic consumed 20-40 gigabytes of bandwidth per second. It was the largest attack traffic observed. Such attack caused target outage for 4-5 days which was the longest outage duration ever. The observed DDoS incidents in the year 2010-2009 are outlined in Table I. in the chronological order.

TABLE I. RECENT DDOS INCIDENTS

S.No	Date	DDoS target/ incident	Consequences/Description
1.	December 8, 2010	MasterCard, PayPal, Visa. and PostFinance	Attack was launched in support of WikiLeaks.ch and its founder. Attack lasts for more than 16 hours.
2.	November 30, 2010	whistleblower site Wikileaks	Attack size was 10 Gbps. Caused the site unavailable to visitors. Attack was launched to prevent release of secret cables.
3.	November 28, 2010	whistleblower site Wikileaks	Attack size was 2-4 Gbps. Attack was launched just after it released confidential US diplomatic cables.
4.	November 12, 2010	Domain registrar Register.com	Impacted DNS, hosting and webmail clients. 24 hours of outage
5.	November 2, 2010	Burma's main Internet provider	Disrupted most network traffic in and out of the country for 2 days. Geopolitical motivated attack. Attack size was of 1.09 Gbps (average) & 14.58 Gbps (maximum) . Attack vectors were TCP Syn/rst 85%, flooding 15%.
6.	October 2010	MPAA & Indian tech firm Aiplex software	At least hundreds of 4chan users at once executed attack in Pro-piracy protest. Simple application Low Orbit Ion Cannon (LOIC) was used.
7.	September 2010	Fast growing botnet "IMDDOS" was discovered	Botnet's motive was to provide commercial service for launching DDoS attacks against any target.
8.	July and August, 2010	Irish Central Applications Office server	Attack was hit on four different occasions.
9.	June 2010	Broadband forum Whirlpool	Flooding DDoS attack. 9 hours of outage.
10.	June 2010	UK- based Jewish Chronicle	Website had to shut down its balanced coverage of the "Ashdod flotilla incident" immediately.
11.	May 2010	Botnet consisting of web servers was discovered	Rrather than individual PCs,servers were being used. An attacker named "Exeman" has infected around 400 web servers with a simple 40-line PHP script.
12.	May 2010	Vocus	Caused connectivity disruptions across multiple websites. 80 minutes of disruption.
13.	May 2010	Web24	Caused Connection issues for users of the Vocus network More than 12 hours of outage.
14.	April 2010	Optus	Sourced from China. 4 hours of outage.
15.	February 2010	Australian Parliament House website (www.aph.gov.au)	Attack was the part of protest by a group. 50 minutes of outage.
16.	December 23, 2009	DNS services provider Neustar	Amazon, Wal-Mart, and Expedia were affected. 60 minutes of outage.
17.	August 6,2009	Twitter, Facebook, Livejournal, and Google blogging pages	Hundreds of millions of Internet users affected. Geopolitical motivated attack. Aimed at knocking Giorgi "cyxymu" off the web. 120 minutes of outage.
18.	October,2009	40 Swedish sites	About 40 websites belonging to police & media went down.
19.	July, 2009	Major websites in South Korea and the United States	Attack traffic consumed 20-40 gigabytes of bandwidth /sec Botnet of 30,000- 60,000 computers was used. Aimed at White House, Federal Trade Commission and the Department of the Treasury, Washington Post and NASDAQ. 4-5 days of outage.
20.	June 2009	The Pirate Bay	Provoked by sellout to Global Gaming Factory X AB
21.	June 2009	Iranian government ahmedinejad.ir	Cut off internet access for protesters inside Iran.
22.	April 1, 2009	Cloud computing provider GoGrid	Service was disrupted to about half of its 1,000 customers
23.	April 6-7, 2009	Web host The Planet	Caused disruption for 8 hours.
24.	April 2-5, 2009	Domain registrar Register.com	Caused 48 hours of disruptions for its customers.
25.	March 2009	UltraDNS	Affected small subset of its customers. Caused several hours of disruption.
26.	January 2009	GoDaddy.com	Affected thousands of its shared hosting customers. Resulted into uptime of 64.26% and downtime of 4d 14h 7m.

The costs of DDoS attacks are monumental. Annually these attacks cost millions of dollars to various companies and represent a serious threat to any computer system. DDoS attack results in long system timeouts, lost revenues, large volumes of work to identify attacks and to prepare adequate response measures [22].

Depending on the type of business, revenue losses can range from $100,000 to tens of millions of dollars per hour when services are down. Forrester, IDC and the Yankee Group estimate that the cost of a 24-hour outage for a large e-Commerce company can approach US $30 million [23]. Further, not only do these attacks cost online organizations monetary losses, they may also cause irreparable damage to reputations and customer relationships [24]. A series of DDoS attacks against Amazon, Yahoo, eBay and other major sites in February 2000 caused an estimated cumulative loss of US $1.7 billion, according to the Yankee Group [23]. Analysts estimated that during the three hours Yahoo was down, it suffered a loss of e-commerce and advertising revenue that amounted to about $500,000. According to bookseller Amazon.com, its widely publicized attack resulted in a loss of $600,000 during the 10 hours it was down.

According to a survey conducted by CSI in 2007, DDoS attacks were found to be one of the major reasons for financial losses [25] as depicted in Fig. 3, incurred almost $2,888,600 which is remarkable high sum of financial loss.

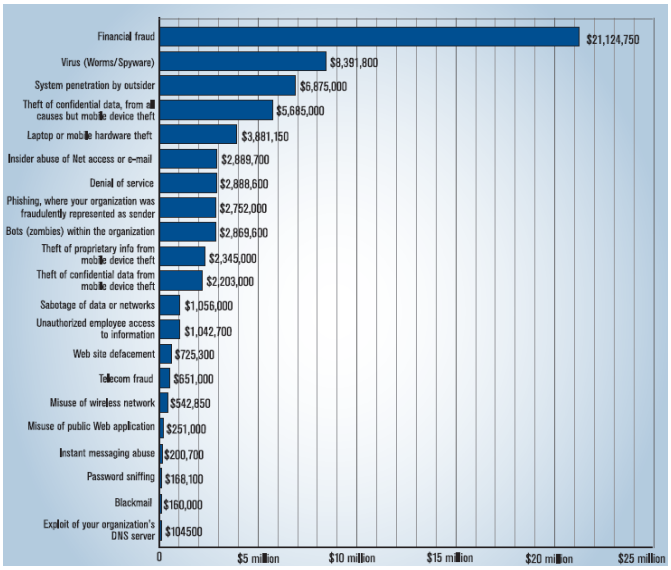

Figure 3. Financial losses incurred due to various attack incidents in 2007

DDoS attacks are growing larger and more destructive as demonstrated in CISCO annual security report 2009 [26] depicted in Fig. 4. Over the last eight years, DDoS attacks have increased in both volume and frequency. The volume of DDoS attacks has increased by more than 1,000 times and has become a real threat for hosting companies and websites that require 100% uptime. In 2005, DDoS attacks averaged several hundred per day. Reports indicate that by the middle of 2007, as many as 8,000 DDoS attacks were seen on a daily basis [23] which consume up to 3%-5% of all internet traffic. While the largest attacks in 2005 were 3.5 gigabit per second (Gbps), attack sizes in 2008 were measured to be 80 Gbps and larger. Attack sizes have increased to 80 Gbps in 2008 vs. 20 Gbps in 2007, 10 Gbps in 2006, and 3.5 Gbps in 2005 and show no signs of slowing down. New types and variations of attacks are being continuously launched, including complex layer-7 HTTP and low- and slow logic attacks [27].

A survey of CSI conducted in 2007 also showed that DDoS attacks were among major reasons of economical losses. While most companies are often reluctant to publicize the attacks they incur [27]. The increased numbers of DDoS attacks in volume and frequency have led to development of numerous defense mechanisms. Still, the growing number of attacks and their financial implications highlighted the need of a comprehensive solution. Distributed defense is the only workable solution to combat DDoS attacks [28]. There is a need of better ways to elicit the details of these attacks, only then a comprehensive distributed defense against DDoS attacks can be devised.

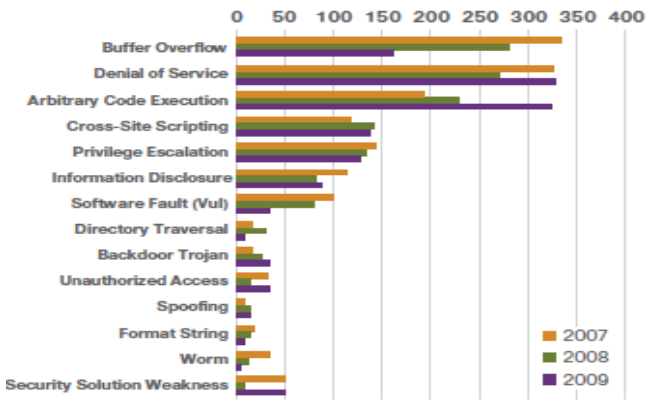

Figure 4. Vulnerabilities and threat categories

VII. CONCLUSIONS

There is an alarming increase in the number of DDoS attack incidents. Not only, DDoS incidents are growing day by day but the technique to attack, botnet size, and attack traffic are also attaining new heights. Effective defense measures needed to prevent and mitigate these attacks is the current need of the hour.

The major contributions of this paper are

- It gives overview of DoS and DDoS problem.
- It briefs the main security holes that create room for these attacks.
- Information about important DDoS incidents from year 1999-2008.
- Chronological brief about recent DDoS incidents is provided.
- Latest scenario of DDoS attacks, DDoS attack traffic, botnet size is explored.
- Financial loss incurred due to DDoS attacks is also explored.
- The need for comprehensive methods to elicit information of DDoS attack and effective preventive and mitigation methods are highlighted.

REFERENCES

[1] J. Howard, and T. Longstaff, “A common language for computer security incidents,” [Online]. Available: www.cert.org/research/ taxonomy_988667.pdf.

[2] (2000) CERT. [Online]. Available: http://www.cert.org/advisories/CA-2000-01.html.

[3] S. Gibson. (2002) grc.com, “The strange tale of the denial of service attacks against GRC.COM,” [Online]. Available: www.grc.com/ dos/grcdos.htm, 2007

[4] 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.

[5] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state of the art," *Computer Journal of Networks*, vol. 44, no. 5, pp. 643-666, Apr.2004.

[6] 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.

[7] R.K.C. Chang, "Defending against flooding-based distributed denial-of-service attacks: A Tutorial,” *Computer Journal of IEEE Communication Magazine*, vol. 40, no. 10, pp. 42-51, Oct.2002.

[8] T. Roebuck. (2005) Crime-research.org, “Network security: DoS vs. DDoS attacks,” [Online]. Available: http:// www.crime-research .org/articles/network-security-dos-ddos-attacks.

[9] 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.

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

[11] K. Kumar, R. Joshi, and K. Singh, “An integrated approach for defending against distributed denial of service attacks,” *IRISS-2006*, IIT Madras. [Online]. Available: http://www.cs.iitm.ernet.in/~iriss06/paper.html.

[12] M. Robinson, J. Mirkovic, M. Schnaider, S. Michel, and P. Reiher, "Challenges and principles of DDoS defense," *Computer Journal of ACM SIGCOMM*, vol. 5, no. 2, pp. 148-152, 2003.

[13] 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.
[14] (2009) Washington.edu, "A DNS reflection attack on register.com," [Online]. Available: http:// www.staff.washington.edu/dittrich/ misc/ ddos/
[15] Wikipedia, "Denial-of-service attack," [Online]. Available: http://en.wikipedia.org/wiki/Denial-of-service_attack.
[16] M. Kisimoto, "Studies on congestion control mechanisms in the Internet– AIMD- based window flow control mechanism and active queue management mechanism," Master Thesis, Osaka University, 2003.
[17] S. Floyd, K. Fall, "Router mechanisms to support end-to-End congestion control", Lawrence Berkeley National Laboratory, USA, Tech. Rep., February 1997.
[18] (2007) ICANN. "Factsheet - Root server attack on 6 February 2007," [Online]. Available: http:// www.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/ddos-timeline.html.
[22] V. Golubev. (2005) Crime-research.org, "DoS attacks: crime without penalty," [Online]. Available: http://www.crime- research.org/ articles/1049/
[23] (2010) Blacklotus.net, "Stopping DDoS Attacks: Cost Management Analysis," [Online]. Available: http://www.blacklotus.net/pdf/ whitepaper.pdf.
[24] (2009) Intermap.com, "Managed Anti DDoS Service Protection," [Online]. Available: http://www.internap.com/wp- content/uploads/ WP-Managed-Anti-DDoS.pdf.
[25] (2007) gocsi.com, "The 12th annual computer crime and security survey," [Online]. Available: http://www.sis.pitt.edu/~jjoshi/courses/ IS2150/Fall09/CSIFBI2007.pdf.
[26] (2009) CISCO. "Annual Security Report, Dec 2009," [Online]. Available: http://www.cisco.com/en/US/prod/collateral/ vpndevc/ cisco_2009_asr.pdf.
[27] (2009) Level3.com, "Managed DDoS Protection," [Online]. Available: http://www.level3.com/downloads/Managed_ DDoS_ Protection_whitepaper.pdf.
[28] M. Sachdeva, G. Singh, K. Kumar, and K. Singh, "A comprehensive survey of distributed defense techniques against DDoS attacks," *International Journal of Computer Science and Network Security*, vol. 9,no. 12, pp. 7-15, Dec. 2009.

AUTHORS PROFILE

Ketki Arora has done BTech computer science and engineering from Shaheed Bhagat Singh College of Engineering & Technology SBSCET, Ferozepur in 2005.Currently she is a MTech student in Department of Computer Science and Engineering at Lala Laj Pat Rai Institute of Engineering & Technology LLRIET, Moga, India.

Krishan Kumar has done BTech computer science and engineering from National Institute of Technology NIT, Hamirpur in 1995. He finished his MS software systems from BITS Pilani in 2001. In 2008, he finished his PhD from Department of Electronics and Computer Engineering at Indian Institute of Technology, Roorkee. Currently,he is an assistant professor at SBS College ofEngineering and Technology, Ferozepur, India.

Monika Sachdeva has done BTech computer science and engineering from National Institute of Technology NIT, Jalandhar in 1997. She finished her MS software systems from BITS Pilani in 2002. Currently she is a PhD student in Department of Computer Science and Engineering at Guru Nanak Dev University, India.