Information Security Journal: A Global Perspective
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/uiss20

Defending against Distributed Denial of Service Attacks: Issues and Challenges

B. B. Gupta [a] , R. C. Joshi [a] & Manoj Misra [a]
[a] Department of Electronics and Computer Engineering , Indian Institute of Technology , Roorkee, India
Published online: 24 Nov 2009.

To cite this article: B. B. Gupta , R. C. Joshi & Manoj Misra (2009) Defending against Distributed Denial of Service Attacks: Issues and Challenges, Information Security Journal: A Global Perspective, 18:5, 224-247, DOI: 10.1080/19393550903317070

To link to this article: http://dx.doi.org/10.1080/19393550903317070

Information Security Journal: A Global Perspective, 18:224–247, 2009

ISSN: 1939-3555 print / 1939-3547 online
DOI: 10.1080/19393550903317070

Taylor & Francis
Taylor & Francis Group

Defending against Distributed Denial of Service Attacks: Issues and Challenges

B. B. Gupta, R. C. Joshi, and Manoj Misra
Department of Electronics and Computer Engineering, Indian Institute of Technology, Roorkee, India

ABSTRACT Distributed Denial of Service (DDoS) attacks on user machines, organizations, and infrastructures of the Internet have become highly publicized incidents and call for immediate solution. It is a complex and difficult problem characterized by an explicit attempt of the attackers to prevent access to resources by legitimate users for which they have authorization. Several schemes have been proposed on how to defend against these attacks, yet the problem still lacks a complete solution. The main purpose of this paper is therefore twofold. First is to present a comprehensive study of a wide range of DDoS attacks and defense methods proposed to combat them. This provides better understanding of the problem, current solution space, and future research scope to defend against DDoS attacks. Second is to propose an integrated solution for completely defending against flooding DDoS attacks at the Internet Service Provider (ISP) level.

KEYWORDS attack mechanisms, defense mechanisms, Distributed Denial-of-Service (DDoS), network security

INTRODUCTION

The Internet has become increasingly important to current society. It is changing our way of communication, business mode, and even everyday life. The impact of the Internet on society can be seen from Figure 1, which shows an exponential increase in the number of hosts interconnected through the Internet (ISC Internet Domain Survey, July, 2009). Unfortunately, security problems are major obstacles to the further development of the Internet. According to CERT statistics (February, 2009), a mere 171 vulnerabilities were reported in 1995 but increased to 7236 in 2007. Already, that number has increased in the third quarter of 2008 to 6,058, as shown in Figure 2. Apart from these, a large number of vulnerabilities go unreported every year. In particular, today denial-of-service (DoS) attack is one of the most common and major threat to the Internet. It reveals big loopholes not only in specific applications but also in the entire TCP/IP protocol suite.

A DoS attack can be described as an attack designed to render a computer or network incapable of providing normal services. It is considered to take place only when access to a computer or network resource is intentionally blocked or degraded as a result of malicious action taken by another user

Address correspondence to B. B. Gupta, Department of Electronics and Computer Engineering, Indian Institute of Technology, Roorkee 247667, India.
E-mail: bbgupta@ieee.org

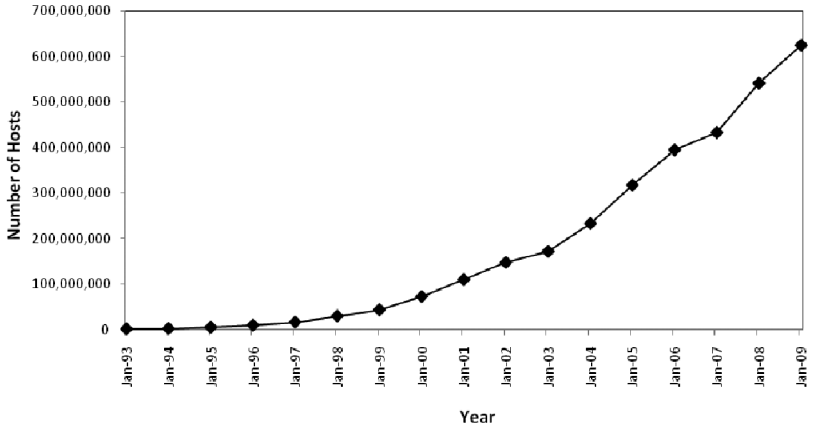

FIGURE 1 **Internet Domain Survey Host Count.**

(Douligeris & Mitrokotsa, 2004). Therefore, as defined by Weiler (2002), it includes any of the following attempts:

- to inhibit legitimate network traffic by flooding the network with useless traffic,
- to deny access to a service by disrupting connections between two parties,
- to block the access of a particular individual to a service, or
- to disrupt the specific system or service itself.

The main aim of such attacks is to prevent the victim either from the benefit of a particular service (in case of client being victim) or from providing its services to others (in case of server being victim). A DDoS attacker uses many computers to launch a coordinated DDoS attack against one or more targets (Douligeris & Mitrokotsa, 2003). This attack is launched indirectly through many compromised computing systems by sending a stream of useless aggregate traffic meant to explode victim resources. As a side effect, these attacks frequently create network congestion on the way from a source to the target, thus disrupting normal Internet operations. Intruder can perform DDoS attack either as brute force/flooding attack or as logical attack. In brute force DDoS attack, legitimate looking but error data packets are sent to victims as much as possible, thus reducing legitimate users' bandwidth and preventing access to a service. Logical attack exploits a specific feature or implementation bug of some protocol or application installed at the target machine in order to consume an excess amount of its resources (Molsa, 2005). The main motives behind DDoS attack are criminal, commercial, or ideological in nature.

Various DDoS attacks against high-profile websites such as Yahoo, Amazon, eBay, CNN News, and E*Trade in early 2000 (CNN Headline News, 2000); the series of attacks on GRC.com in May 2001 (Gibson, 2002); a highly coordinated attack against CERT in May 2001 (Abennett, 2001); a series of attacks against Internet Service Providers (ISPs) in the UK in 2002 (Leyden, 2002); distributed attack against name servers in Akamai's Content Distribution Network (CDN) on June 15, 2004 (Akamai, 2004; Gonsalves, 2004); and the text-to-speech translation application running in the Sun Microsystem's Grid Computing system disabled with a DDoS attack in March 2006 (Galli, 2006) demonstrate how devastating DDoS attacks are and how defenseless the Internet is under such attacks. As proof of these disturbing trends, a computer crime and security survey conducted by FBI/CSI in the United States for the year 2004 (Gordon et al., 2005) found that DoS attack is the second most widely detected outsider attack type in computer networks immediately after virus infections. A computer crime and security survey conducted in Australia for the year 2004 (Australian Computer Emergency Response Team, 2005) shows similar results. By now, DDoS attacks have risen to be the number-one threat on the Internet (Li, Li, & Jiang, 2008). A study has shown that the number of DDoS attacks increased 50% per year (Howard, 1998), and the attacks were also increased in sophistication and severity. The losses caused by DDoS attacks are remarkable particularly to e-commerce sites. According to Jupiter Communications, 46% of consumers report that poor site

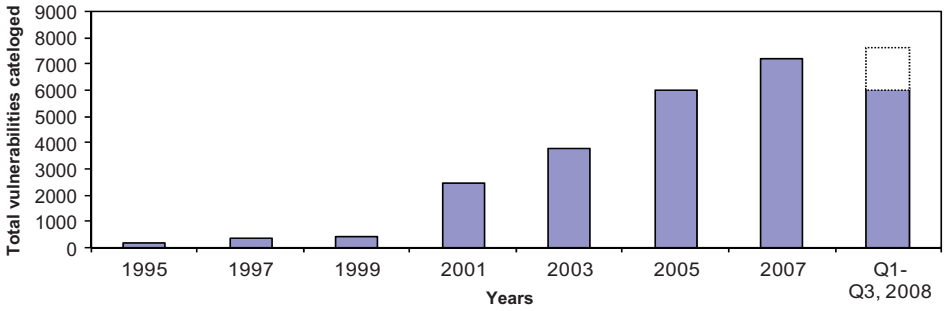

FIGURE 2 Vulnerabilities reported since 1995.

performance drove them away from their preferred sites (Negi, 2001).

DDoS attacks are inevitable. Because the Internet is designed to keep intermediate network as simple as possible to optimize it for packet forwarding (Leiner et al., 2003). This pushes the complexity to the end hosts and causes one unfortunate implication. If one party in two-way communication misbehaves, it can result in arbitrary damage to its peer. No one in the intermediate network will step in and stop it because the Internet is not designed to police traffic. Moreover, Internet security is highly interdependent. Even though, we can use some traditional security mechanisms, such as firewalls (Oppliger, 1997; McAfee, n.d.), IDS (Debar, Dacier, & Wespi, 1999), access lists (Hazelhurst, 2000), etc., to protect victims' machines, the susceptibility to DDoS attacks also depends on the position of security in the rest of the global Internet (Mirkovic & Reiher, 2004). For example, if an attacker is able to exploit an insecure legitimate machine that is authorized to communicate with the victim, that machine can be used to perform an attack against the victim as incoming attack traffic to the victim seems to be normal traffic. The limited availability of resources acts as additional benefit for DDoS attackers. To add on, accountability is not enforced, which leads to variety of reflector attacks (Paxson, 2001; Scalzo, 2006). One of the most dangerous types of reflector attack that is difficult to deal with is a Smurf attack (Papadopoulos et al., 2003; Huegen, 2000). Thus there exists no way to enforce global deployment of a particular security mechanism (Mirkovic & Reiher, 2004).

Recently, several schemes have been proposed to deal with the DDoS problem. Many of them claim to be best in business in absence of benchmarks, but none of them gives a comprehensive solution; they only deal with some part of the DDoS problem. Moreover these attacks are very dynamic to escape from existing defense systems. So how to defend against DDoS attacks has become one of the extremely important research issues in the Internet community. Therefore, the motivation of our work is to develop a robust and effective solution to counteract DDoS attacks. In this paper, we present an overview of the DDoS problem, classifications of DDoS attack types, and discuss strength and weaknesses of the array of state-of-art mechanisms based on common defense principles. This provides better understanding of the DDoS problem, current solution space, and future research scope to defend against DDoS attacks. Finally, an integrated solution is proposed to defend against these attacks completely in ISP domain.

The remainder of the paper is organized as follows. Section 2 contains background and overview of the DDoS problem. Section 3 presents classification of attack mechanisms. Classification of DDoS defense mechanisms is described in section 4. Section 5 describes proposed integrated solution in details. Finally, Section 6 concludes the paper and presents further research scope.

2. BACKGROUND AND DDOS OVERVIEW

Today, DoS attacks and more particularly the distributed ones (DDoS) are one of the latest threat and pose a grave danger to users, organizations and infrastructure of the Internet. In these attacks, the goal of the attacker is to tie up chosen key resources at the victim, usually by sending a high volume of seemingly legitimate traffic requesting some services from the

victim. The first publicly reported DDoS attack appeared in the late 1999 against a university (Garber, 2000). These attacks quickly became increasingly popular as communities of crackers developed and released automated tools to carry them out. This made attack process within inexperienced crackers' capabilities. Thus, these attacks are easiest to implement from an attacker's point of view and definitely one of the costliest for businesses (Molsa, 2005).

2.1 Denial of Service Attacks

A DoS attack is commonly characterized as an event in which a legitimate user or organization is deprived of certain services, such as Web, email, or network connectivity, that the user would normally expect to have (Gupta, Misra, & Joshi, 2008). The formal definition of the term "Denial of Service" is given in (Weiler, 2002; Limwiwatkul & Rungsawang, 2004):

A DOS attack is considered to take place only when access to a computer or network resource is intentionally blocked or degraded as a result of malicious action taken by another user (Douligeris & Mitrokotsa, 2003). In DoS attacks, only one machine is used by attacker to perform attack. Figure 3 depicts a typical denial-of-service attack scenario in which an attacker sends a stream of malicious packets to a victim, denying its service to a legitimate user.

2.2 Distributed Denial-of-Service Attacks

Distributed denial-of-service (DDoS) attack can usually cause more significant damage than DoS attack by performing attack from many compromised machines. Figure 4 depicts a simple DDoS attack scenario in which attacking machines A1, A2, A3 send streams of malicious packets to victim, denying its service to legitimate user. A DDoS attack has two phases: deployment and attack (Molsa, 2005). A DDoS program must first be deployed on one or more compromised hosts before an attack is possible. Therefore, mitigation of DDoS attacks requires defense mechanisms for both phases (Gupta, Misra, & Joshi, 2008).

2.3 The Art of DDoS Attacks

Here we describe a typical DDoS attack scenario, its core elements, and strategy. A DDoS attack is composed of four elements (Xiang, Zhou, & Chowdhury,

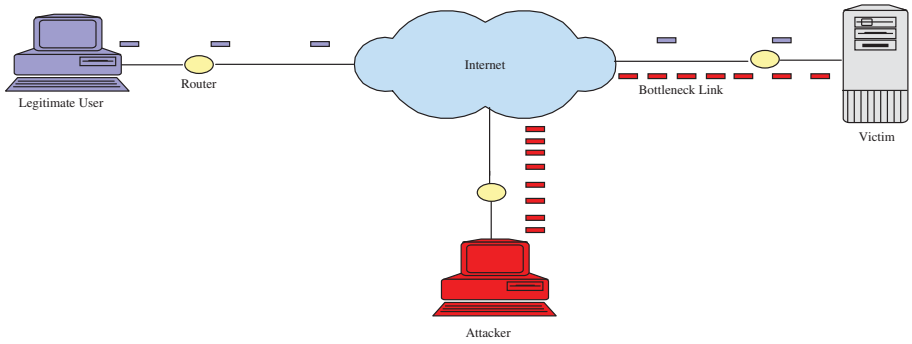

FIGURE 3 Denial of Service attack scenario.

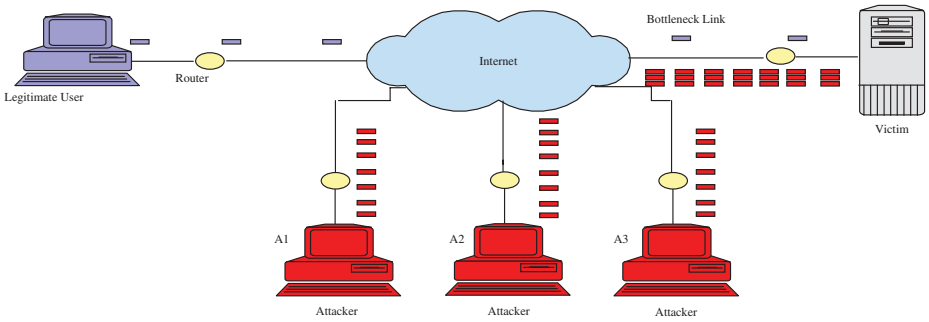

FIGURE 4 Distributed Denial-of-Service attack scenario.

2004; Lau et al., 2000): Attack source, Control masters, Agents, and Victim.

- Attack source: Attack source is the machine, handled by attacker who is the mastermind behind the attack. It is the one who sets every plan about the attack.
- Control masters: Control masters coordinate and control multiple agents and exploit further agent machines on behalf of attack source. Control masters are deployed on one or more host machines.
- Agents: Agents, also known as slaves or attack daemons, are programs that actually conduct the attack on the target victim. Attack daemons are usually deployed on host computers. These daemons affect both the target and the host computers. The task of deploying these attack daemons requires the attacker to gain access and infiltrate the host computers.
- Victim: A victim is a target host that has been chosen to receive the impact of the attack.

Figure 5 shows how these core elements are coordinated to inflict DDoS attack on a targeted victim's machine. DDoS attack is carried out from multiple sources to aim at a single target, in several phases. In order to launch a DDoS attack, the attacker first scans millions of machines for vulnerable services and other weaknesses on the Internet. Machines that are always connected to the Internet through cable modems and often have weak security are easier to compromise. The discovered vulnerabilities are then exploited to gain access and plant malicious codes on these machines so-called handlers, or masters.

After the malicious scripts are installed, these infected machines can repeat the same procedure to recruit more machines, so-called zombies or slaves. In the hacker's community, these exploited machines used as an attack army are collectively called bots and the attack network is known as botnet. Then the communication channels between the attacker and the masters and between the masters and slaves are established. These control channels are designed to be secret to the public (Xiang, Zhou, & Chowdhury, 2004). Staying behind the scenes of attack, the real attacker sends a command to the masters to initiate a coordinated attack. When the masters receive the command, they transfer it to the slaves under their control. Upon receiving attack commands, the zombies or slaves begin the attack on the victim (Lau et al., 2000). The real attacker is trying to hide himself from detection, for example, by providing spoofed IP addresses (Mirkovic & Reiher, 2004; Xiang, Zhou, & Chowdhury, 2004).

2.4 DDoS Attack Tools

It used to be that attackers often tested the network manually to find out vulnerable hosts and installed DDoS attacks tools onto them. Recently, the compromise process has been much more automated. Attackers can use scanning methods to look for the vulnerable hosts. To propagate among vulnerable hosts, DDoS attackers install attack tools on the compromised hosts and use them as the attacking machines for further compromise. There are a variety of different DDoS attack tools on the Internet that

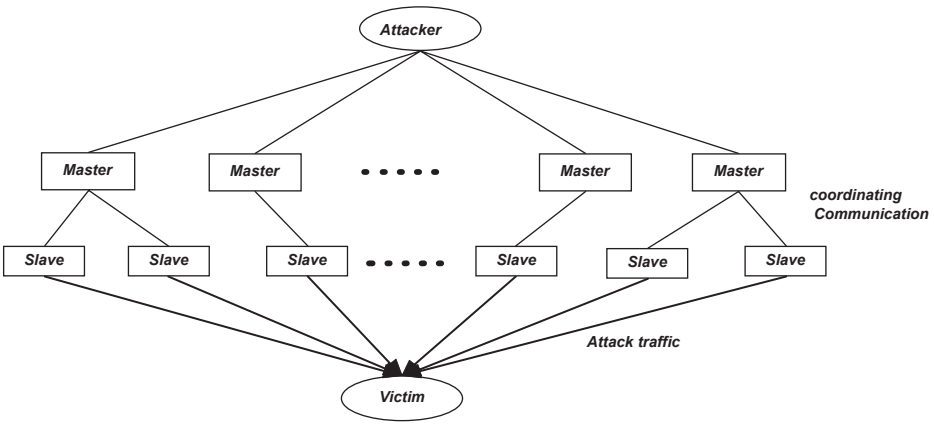

FIGURE 5 A hierarchical model of a DDoS attack.

allow attackers to execute attacks on the target system. Some of the most common tools are discussed below:

- *Trinoo* (Mirkovic & Reiher, 2004; Dittrich, 1999) can be used to launch a coordinated UDP flooding attack against target system. Trinoo deploys master/slave architecture and attacker controls a number of Trinoo master machines. Communication between attacker and master and between master and slave is performed through TCP and UDP protocol, respectively. Both master and slaves are password protected to prevent them from being taken over by another attacker. *Wintrinoo* is a Windows version of trinoo that was first reported to CERT on February 16, 2000.
- *TFN* (Dittrich, 1999) uses a command line interface to communicate between the attack source and the control master program. Communication between the control masters and slaves is done via ICMP echo reply packets. However, it does not offer any kind of encryption between attack source and masters or between masters and slaves. It can implement Smurf (Huegen, 2000; Azrina & Othman, n.d.), SYN Flood (Schuba et al., 1997; Farrow, n.d.; CERT Advisory, 1996), UDP Flood (Azrina & Othman, n.d.), and ICMP Flood (Azrina & Othman, n.d.; Papadopoulos et al., 2003) attacks. Detailed descriptions about these attacks, that is, Smurf, SYN Flood, UDP Flood, ICMP Flood, etc., are presented in Section 3.
- *TFN2K* (Douligeris & Mitrokotsa, 2004; Barlow & Thrower, 2000; CERT Coordination Center, 1999) is a more advanced version of the primitive TFN network. It uses TCP, UDP, ICMP, or all three to communicate between the control master program and the slave machines. TFN2K can implement Smurf, SYN, UDP, and ICMP Flood attacks. Communication between the real attacker and control master is encrypted using a key-based CAST-256 algorithm. In addition to flooding, TFN2K can also perform some vulnerability attacks by sending malformed or invalid packets.
- *Stacheldraht* (Dittrich, 1999) combines best features of both Trinoo and TFN. It also has the ability to perform updates on the slave machines automatically. It uses an encrypted TCP connection for communication between the attacker and master control program. Communication between the master control program and attack daemons is conducted using TCP and ICMP. Stacheldraht can implement Smurf, SYN Flood, UDP Flood, and ICMP Flood attacks.
- *Shaft* (Dietrich, Long, & Dittrich, 2000) has been modeled on Trinoo network. Other than the port numbers being used for communication purpose, working of it is similar to the Trinoo. Thus, a distinctive feature of Shaft is the ability to switch control master servers and ports in real time, making detection by intrusion detection tools difficult. Communication between the control masters and slave machines is achieved using UDP packets. The control masters and the attacker communicate via a simple TCP telnet connection. Shaft can implement UDP, ICMP, and TCP flooding attack.
- *Mstream* (Dittrich et al., 2000) is more primitive than any of the other DDoS tools. It attacks target machine with a TCP ACK flood. Communication is not encrypted and is performed through TCP and UDP packets and the master connects via telnet to zombie. Masters can be controlled remotely by one or more attackers using a password protected interactive login. Source addresses in attack packets are spoofed at random. Unlike other DDoS tools, masters are informed of access, successful or not, by competing parties.
- *Knight* (Cert Coordination Center, 2001) uses IRC (IRC Security, n.d.) as a control channel. It has been reported that the tool is commonly being installed on machines that were previously compromised by the BackOrifice Trojan horse program. Knight can implement SYN attacks, UDP Flood attacks, and an urgent pointer flooder (Bysin, 2001). It is designed to run on the Windows operating system and has features such as an automatic updater via http or ftp, a checksum generator, and more.
- *Trinity* (Hancock, 2000; Marchesseau, 2000) is also IRC based DDoS attack tool. It can implement UDP, IP fragment, TCP SYN, TCP RST, TCP ACK, and other flooding attacks. Each trinity compromise machine joins a specified IRC channel and waits for commands. Use of legitimate IRC service for communication between attacker and agents eliminates the need for a master machine and elevates the level of the threat (Douligeris & Mitrokotsa, 2004).

2.5 Defense Challenges and Principles

With the present technology, many challenges are involved in designing and implementing an effective

DDoS defense mechanism. These challenges include (Kumar, Joshi & Singh, 2006) (a) large number of unwitting participants, (b) no common characteristics of DDoS streams, (c) use of legitimate traffic models by attackers, (d) no administrative domain cooperation, (e) automated tools, (f) hidden identity of participants, (g) persistent security holes on the Internet, (h) lack of attack information, and (i) absence of standardized evaluation and testing approaches.

Thus, the following five principles are recommended by Robinson et al. (2003) to build an effective solution:

- DDoS is a distributed attack and because of high volume and rate of attack packets, distributed instead of centralized defense is the first principle of DDoS defense. A distributed defense mechanism consists of multiple defense nodes, generally with the same functionalities that are deployed at various locations and organized into a network. Nodes are communicated through the network and coordinate their actions to achieve a better overall defense. Therefore, it overcomes the single point failure problem that occurs in a centralized defense mechanism.
- It has a High Normal Packet Survival Ratio (NPSR); hence, less collateral damage is the prime requirement for a DDoS defense.
- A DDoS defense method should provide secure communication for control messages in terms of confidentiality, authentication of sources, integrity, and freshness of exchanged messages between defense nodes.
- As there is no centralized control for autonomous systems (AS) in Internet, a partially and incrementally deployable defense model that does not need centralized control will be successful.
- A defense system must take into account future compatibility issues such as interfacing with other systems and negotiating different defense policies.

3. CLASSIFICATION OF ATTACK MECHANISMS

Here a classification of a wide range of DDoS attacks found in the wild is presented for Internet providers and users. The classification is illustrated in Figure 6 and describes in detail in this section.

A. Classification Based on Attacking Methods

A-1: Flooding

Currently, the majority (90–94%) of DDoS attacks are performed using TCP, and a large portion (52–57%) of them is targeted to flooding attacks (Moore et al., 2006). In flooding DDoS attack, also known as brute force attack (Mirkovic & Reiher, 2004), legitimate looking but garbled packets are sent to victim machine to clogs up computational or communication resources on the target machine so that it cannot serve

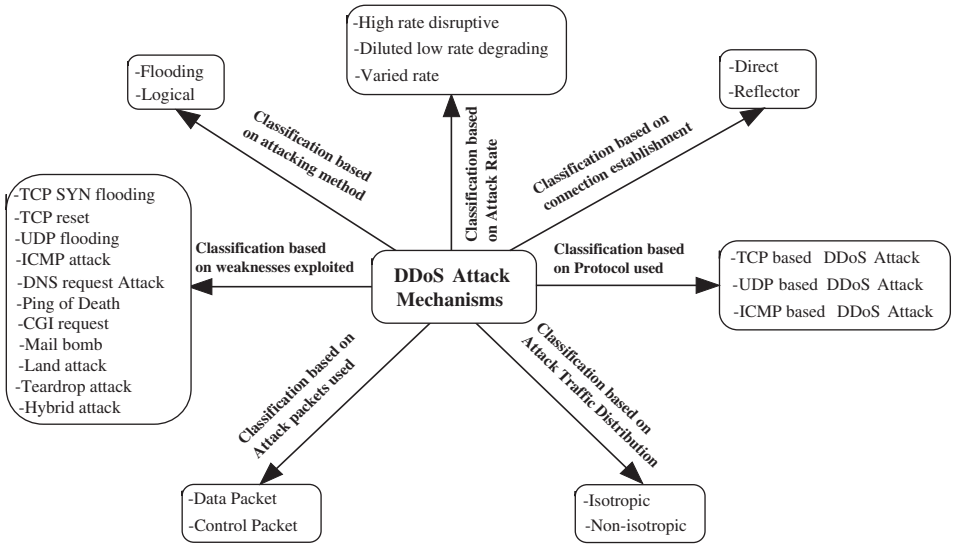

FIGURE 6 Classification of DDoS attack Mechanisms.

its legitimates users. The resources consumed by attacks include network bandwidth, disk space, CPU time, data structures, network connections, and so forth.

A-2: Logical

Logical attacks exploit a specific feature or implementation bug of some protocol or application installed at the target machine in order to consume excess amount of its resources (Gupta, Misra & Joshi, 2008). For example, in the TCP SYN attack, the exploited feature is the allocation of substantial space in a connection queue immediately upon receipt of a TCP SYN request. The attacker initiates multiple connections that are never completed, thus filling up the connection queue.

B. Classification Based on Weaknesses Exploited

B-1: TCP SYN Flooding

Any system providing TCP-based network services is potentially subject to this attack. In normal case, TCP 3-way handshaking is performed as shown in Figure 7(a). The attacker sends a flood of TCP/SYN packets, often with a forged sender address. Each of these packets is 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. The result would be system crash or system inoperative. As shown in Figure 7(b), an attacker B initiates a SYN flooding attack by sending many connection requests with spoofed source addresses to the victim machine D. That causes D to allocate resources, and once the limit of half-open connections is reached, it refuses all successive connection establishment attempts (Schuba et al., 1997; Farrow, n.d.; CERT, 1996).

B-2: TCP Reset

TCP reset also exploit the characteristics of TCP protocol. The main idea behind a TCP reset attack is to falsely terminate an established TCP connection without the consent of the two parties that own the

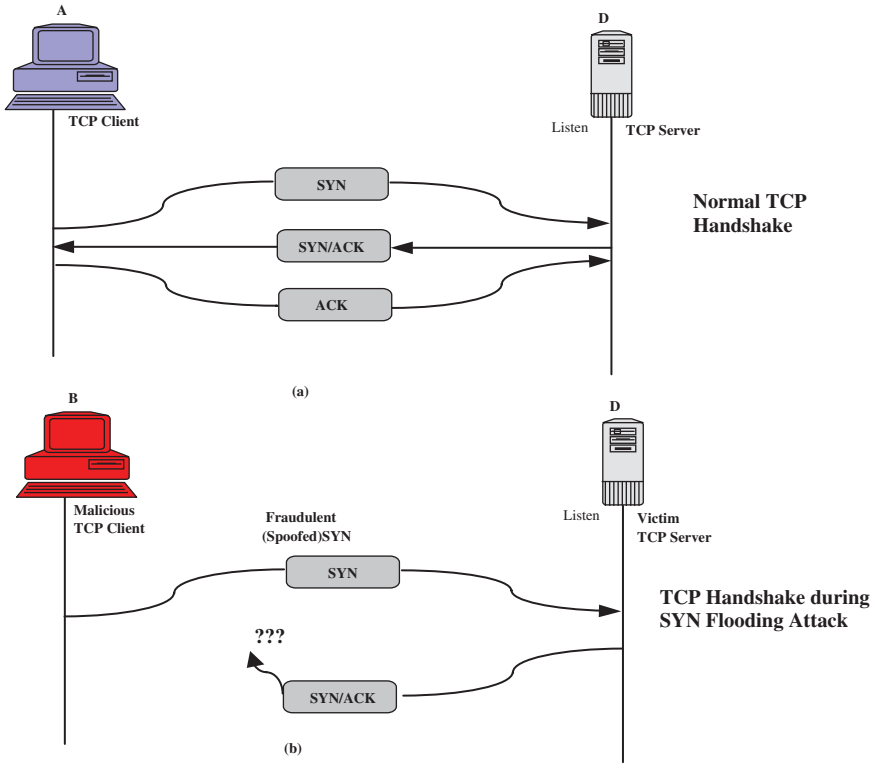

FIGURE 7 (a) TCP 3-way handshaking (b) TCP SYN attack.

endpoints (Andrews, 2004). Let us imagine an established TCP connection from host A to host D. Now, a third host, B, spoofs a packet that matches the source port and IP address of host A, the destination port and IP address of host D, and the current sequence number of the active TCP connection between host A and host D. Then host B sets the RST bit on the spoofed packet, and when this packet is received by host D, host D immediately terminates the connection. This results in a DoS until the connection is reestablished.

B-3: UDP Flooding

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 to the forged source address. If enough UDP packets are delivered to ports on victim, the system will go down. 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, which can lead to a DoS on the machine(s) where the services are offered (Azrina & Othman, n.d.; Jarvin network management, n.d.).

B-4: ICMP Attack

During an ICMP flooding attack, the attacker generates a flood of ICMP ECHO packets directed at the victim. The victim replies to each ICMP request, consuming its CPU resources and network resources. Smurf attack is ICMP flooding attack (as shown in Figure 8). The attacker directs a stream of ICMP ECHO requests to broadcast addresses in intermediary networks, spoofing the victim's IP address in the source address fields. A multitude of machines then reply to the victim, overwhelming its network (Papadopoulos et al., 2003; Huegen, 2000; Azrina & Othman, n.d.).

B-5: DNS Request Attack

In this attack scenario, the attacker 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. In a DNS request attack small queries can generate larger UDP packets in response, which is known as amplification effect of DNS response. Because of this amplification effect of DNS response, it can cause serious bandwidth attack (Cheung, 2006; Wikipedia, n.d.). For example, in the initial DNS specification, UDP packets were limited to 512 bytes. At most, a 60-byte query could generate a 512-byte response for an amplification factor of 8.5. This amplification effect has been used in DNS based attacks for some time.

B-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

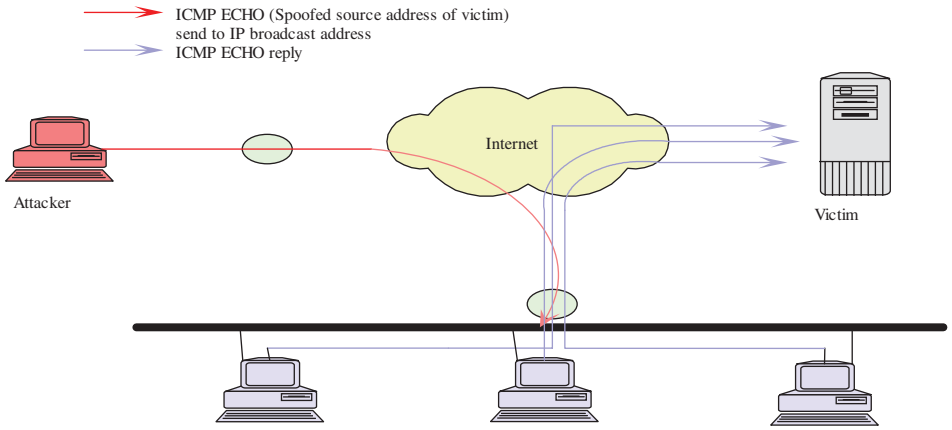

FIGURE 8 Smurf attack.

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 (Kenney, n.d.).

B-7: CGI Request

By simply sending multiple CGI request to the target server, the attacker consumes the CPU resource of the victim. At last, the server is forced to terminate its services (CGI request attack, n.d.).

B-8: Mail Bomb

A mail bomb is the sending of a massive amount of email 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 (CERT Coordination Center, n.d.).

B-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 or crashes it (Wikipedia, n.d.).

B-10: Teardrop Attack

The Teardrop attack exploits the vulnerability present in the reassembling of data packets. It involves sending invalid or garbage IP fragments with overlapping or oversized, payloads to the target machine. A bug in the TCP/IP fragmentation re-assembly code of various operating systems causes the fragments to be improperly handled and forces them to crash, hang, or reboot (Teardrop attacks, n.d.).

B-11: Hybrid Attack

With the large number of countermeasures being employed by a number of organizations on the Internet, recently there has been an emergence of hybrid forms of DDoS attacks. In such attacks, the attacker combines two or more attack types to form a hybrid variety of DDoS attack, for example, teardrop spoofing attack or overlapping land attack.

Teardrop spoofing attack involves spoofed mangled IP fragments with overlapping or oversized payloads to the target machine to crash, hang, or reboot it. Similarly, overlapping land attack involves mangled IP fragments with overlapping or oversized payloads and with the source address and source port number of these mangled IP fragments, being same as the destination IP address and port number to the target machine to crash, hang, or reboot it.

C. Classification Based on Connection Establishment

C-1: Direct

In this case, zombies send huge amount of packet directly targeting victim machine(s). To serve this purpose, attackers often have compromised and gained control over thousands or even millions of vulnerable machines. The attacking packets are routed to the victim from zombies distributed widely on the Internet.

C-2: Reflector

It is more complicated and harder to trace back compared to direct attacks. Instead of sending packets to victims directly, the zombies take advantage of the TCP three-way handshake mechanism. Zombies are instructed to continuously send TCP connection-requesting SYN packets to other innocent IP hosts. Those SYN packets carry a spoofed source IP belonging to the victim. As the second phase of the TCP connection handshake, those innocent hosts reply to the victim with SYN/ACK packets according to the source IP address in the requesting packets they received. In this manner, malicious SYN packets are being "reflected" off innocent nodes and their SYN/ACK responses are being used to flood and attack the victim (Paxson, 2001; Scalzo, 2006).

D. Classification Based on Attack Rate

D-1: High Rate Disruptive

In high rate disruptive attacks, sheer volume of packets at very high rates are sent from distributed

locations in a coordinated manner to completely disrupt the availability of Internet services. As these attacks have a direct impact on ISP networks, the packets are easy to detect and characterize.

D-2: Diluted Low Rate Degrading

In diluted low rate degrading attacks, packets are sent from a large number of infected machines, that is, zombie machines, at low rate in a coordinated manner to gracefully degrade network performance. As these attacks degrade Quality of Service (QoS) of the network slowly, they are difficult to detect and characterize.

D-3: Varied Rate

To make detection of attacks more difficult, attackers can use sophisticated attack tools to generate varied rate attacks in which they use some of the zombie machines to generate packets at high rates while the remaining machines generate packets at low rates. These types of attacks are toughest to detect and characterize.

E. Classification Based on Attack Traffic Distribution

In order to defeat an 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 nonisotropic distribution of attack traffic (Kumar, Joshi, & Singh, 2006).

F. Classification Based on Attack Packets Used

Logical DDoS attacks are normally launched with control packets such as TCP SYN, TCP FIN, and ICMP echo packets; for launching flooding DDoS attacks, control as well as data packets such as HTTP, FTP (involving TCP), UDP, and ICMP bogus packets can be used.

G. Classification Based on Protocol Used

Network protocols-based classification of DDoS attacks basically divide DDoS attacks into TCP, UDP, and ICMP protocol-based attacks, as either of these protocol packets can be used for flooding and logical attacks.

4. DDoS DEFENSE MECHANISMS

Large numbers of defense methods have been proposed to combat DDoS attacks in the literature. Figure 9 summarizes a classification of various defense mechanisms proposed by researchers. Detailed descriptions of the classification are given as follows:

A. Classification Based on Activity Deployed

Classification based on activity deployed categorizes the DDoS defense mechanisms in the following four categories:

A-1: DDoS Attack Prevention

Attack prevention methods (Ferguson & Senie, 2001; Global incident analysis, n.d.; Park & Lee, 2001; Peng et al., 2003; Li et al., 2002; Geng & Whinston, 2000) try to stop all well-known signature- and broadcast-based DDoS attacks from being launched in the first place or edge routers, keep all the machines over Internet up to date with patches, and fix security holes.

Attack prevention schemes are not enough to stop DDoS attacks because they are always vulnerable to novel and mixed attack types for which signatures and patches do not exist in the database. So these are considered forensic defense methods. DDoS attacks prevention techniques can be classified as follows:

A-1-1: Filtering. Filtering approaches(Ferguson & Senie, 2001; Global incident analysis, n.d.; Park & Lee, 2001; Peng et al., 2003; Li et al., 2002; Geng & Whinston, 2000) are used to prevent IP spoofing based DDoS attacks. Incoming packets that have forged IP addresses are assumed as attack signature in this case and filter out at edge routers. A number of approaches are given for preventing IP spoofing-based DDoS attacks in literature, but these approaches require global deployment that is not practical, as Internet is governed in distributed manner and each network has its own local policies to enforce defense mechanisms.

A-1-2: Remove unused services. The less there are applications and open ports in hosts, the less th ere are

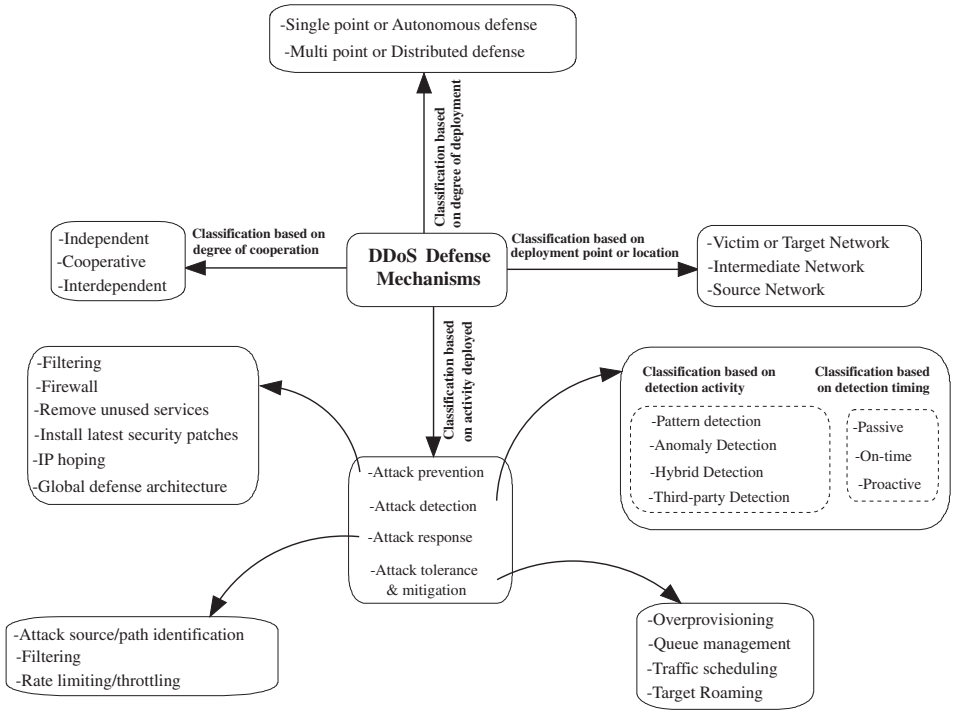

FIGURE 9 **Classification of DDoS Defense Mechanisms.**

chance to exploit vulnerabilities by attackers. So only the necessary services should be open and all others services should be removed, as default installations of operating systems often include many applications not needed by a user (Geng & Whinston, 2000; Molsa, 2005).

A-1-3: Firewalls. Firewalls can effectively prevent users from launching simple flooding type attacks from machines behind the firewall. Firewalls have simple rules such as to allow or deny protocols, ports, or IP addresses. However, some complex attack; for example, if there is an attack on port 80 (Web service), firewalls cannot prevent that attack because they cannot distinguish good traffic from DoS attack traffic (Oppliger, 1997; McAfee, n.d.).

A-1-4: Install latest security patches. Today, many DDoS attacks exploit vulnerabilities in target systems. So removing known security holes by installing all relevant latest security patches prevents re-exploitation of vulnerabilities in the target system (Geng & Whinston, 2000).

A-1-5: Global defense infrastructure. A global deployable defense infrastructure can prevent many DDoS attacks by installing filtering rules in the most important routers of the Internet. As Internet is administered by various autonomous systems according their own local security policies; such type of global defense architecture is possible only in theory (Geng & Whinston, 2000).

A-1-6: IP hopping. DDoS attacks can be prevented by changing the victim computer's IP address with a prespecified set of IP address ranges, thereby invalidating the old address (Geng & Whinston, 2000). This action still leaves the computer vulnerable because the attacker can launch the attack at the new IP address.

To conclude, attack prevention aims to solve IP spoofing, a fundamental weakness of the Internet. However, as attackers gain control of larger numbers of compromised computers, attackers can direct these "zombies" to attack using valid source addresses. Since the communication between attackers and "zombies" is encrypted, only "zombies" can be exposed instead of attackers. According to the Internet Architecture Working Group (2005), the percentage of spoofed attacks is declining. Only 4 out of 1127 customer-impacting DDoS attacks on a large network used spoofed sources in 2004. Moreover, security awareness is still not enough, so expecting installation of security technologies and patches in large base of Internet seems to be an ambitious goal. Also, there exists no way to enforce global deployment of a particular security mechanism. Therefore, relying on attack prevention schemes is not enough to stop DDoS attacks.

A-2: DDoS Attack Detection

Attack detection aims to detect an ongoing attack as soon as possible without misclassifying and disrupting legitimate traffic. We may classify DDoS detection mechanisms using following different criteria:

A-2-1: Classification based on detection timing. Based on detection timing, DDoS detection approaches can be classified as follows:

- A-2-1-1: Passive detection: Detection can be passive if logs are analyzed after attacker fulfills his/her desire and attack is over.
- A-2-1-2: On-time detection: Detection can be on time, if attack can detected when attack is going.
- A-2-1-3: Proactive detection: Detection can be proactive, if attack can be detected either before it reaches target machine or before appreciable degradation of service.

A-2-2: Classification based on detection activity. Based on detection activity, DDoS detection approaches can be classified as follows:

- A-2-2-1: pattern based attack detection: Signature based approach employs a priori knowledge of attack signatures. The signatures are manually constructed by security experts analyzing previous attacks and used to match with incoming traffic to detect intrusions. SNORT (Paxson, 1999) and Bro (Roesch, 1999) are the two widely used signature-based detection approaches. Signature based techniques are only effective in detecting traffic of known DDoS attacks whereas new attacks or even slight variations of old attacks go unnoticed.
- A-2-2-2: Anomaly based attack detection: Anomaly-based system (Gil & Poletto, 2001; Blazek et al., 2001; Cheng et al., 2002; Lee et al., 1999; Mirkovic et al., 2002; Bencsath & Vajda, 2004; Gupta et al., 2008; Chen et al., 2007; Feinstein et al., 2003; Lakhina et al., 2005; Gupta et al., 2007) uses a different philosophy. It treats any network connection violating the normal profile as an anomaly. A network anomaly is revealed if the incoming traffic pattern deviates from the normal profiles significantly. Detecting DDoS attacks involves first knowing normal behavior of our system and then finding deviations from that behavior. Anomaly-based techniques can detect novel attacks; however, it may result in higher false alarms. The common challenge for all anomaly-based intrusion detection systems is that it is difficult to train data to provide all types of normal traffic behavior. As a result, legitimate traffic can be classified as attack traffic, causing a false positive. To minimize the false positive rate, a larger number of parameters are used to provide more accurate normal profiles. However, with increase in number of parameters, the computational overhead to detect attack increases.

Table 1 shows the comparison of various detection approaches, that is, pattern, anomaly, hybrid, and third-party detection.

- A-2-2-3: Hybrid attack detection: Hybrid attack detection combines the positive features of both pattern- and anomaly-based attack detection models to achieve high detection accuracy, low false positives and negatives, and a raised level of cyber trust. Even though hybrid attack detection approach decreases false positive rate, it also increases complexity and cost of implementation (Hwang et al., 2007).
- A-2-2-4: Third party detection: Mechanisms that deploy third-party detection do not handle the detection process themselves but rely on an external third-party that signals the occurrence of the attack (Mirkovic & Reiher, 2004). Examples of mechanisms that use third-party detection are easily found among traceback mechanisms (Savage et al., 2000; Snoeren et al., 2001; Bellovin, Leech, & Taylor, 2001; Dean, Franklin, & Stubblefield, 2002; Xong & Perrig, 2001; Belenky & Ansari, 2003). A detailed description about traceback mechanisms is presented in next sub–section 4.

A-3: DDoS Attack Response

The goal of the attack response is to relieve the impact of the attack on the victim while imposing minimal collateral damage to legitimate clients. We classify attack response mechanisms as follows:

A-3-1: Attack Source/ Path Identification. Once an attack has been detected, an ideal response would be to block the attack traffic at its source. Unfortunately, there is no easy way to track IP traffic to its source due to the stateless of the IP protocol. The attacker can easily spoof the source IP address field in the packets and send the packets to the victim without notice. To address this limitation, several enhancements have been proposed to support IP traceability (Savage et al.,

TABLE 1 Comparison of Various Detection Approaches Classified Based on Detection Activity Used

Detection category	Strategy used	NPSR	Complexity	Detection accuracy	Limitations
Pattern Detection	Store the pattern of the known attacks in the databases and monitor each communication for the presence of these pattern	High	Low	High	Detection of the novel attacks are not possible
Anomaly Detection	Compare the current state of the system with normal system be havior pe riodically	Medium	Medium	Medium	False positives and negatives rate is very high, since defining normal system behavior and setting threshold values is difficult
Hybrid Detection	Combines the positive features of both pattern and anomaly detection models	High-Medium	High	High	Complexity and cost of implementation is very high to deployed in practice
Third party Detection	Rely on an third party to signals the occurrence of attack	Depend on detection approach used by third party	High	Depend on detection approach used by third party	Economic Factor, Security prone

2000; Snoeren et al., 2001; Bellovin, Leech, & Taylor, 2001; Dean, Franklin, & Stubblefield, 2002; Xong & Perrig, 2001; Belenky & Ansari, 2003). Attack source identification mechanisms provide the victim with information about the identity and path taken by the machines that are responsible for performing the attack.

A-3-2: Filtering. Filtering techniques (Darmohray & Oliver, 2000) are used to filter out incoming traffic that has been characterized as malicious by the detection mechanism completely. However, it is always difficult to distinguish malicious packets from legitimate packets; therefore, these techniques cause a high number of false positives.

A-3-3: Rate Throttling. Rate-throttling is a lenient response technique that imposes a rate throttle on the incoming traffic that has been characterized as malicious by the detection mechanism, usually deployed when the detection mechanism has a high level of false positives or cannot precisely characterize the malicious traffic (Papadopoulos et al., 2003; Mirkovic, Prier, & Reiher, 2002; Floyd et al., 2001).

A-3-4: Reconfiguration. Reconfiguration mechanisms (Andersen et al., 2001) change the topology of the victim or the intermediate network to either add more resources to the victim or to isolate the attack machines.

A-4: DDoS Attack Tolerance and Mitigation

Attack tolerance and mitigation approach assumes that it is impossible to prevent or stop DDoS completely. Therefore, it focuses on minimizing the attack impact and tries to provide optimal level of service as per quality of its service requirement to legitimate users while the service provider is under attack. This is not a comprehensive solution in any way; however it can complement other approaches to work in parallel and achieve their goals by providing sufficient assurance and cushion in terms of time to providers that the legitimate clients are being served. Attack tolerance and mitigation approaches can be classified as follows:

A-4-1: Overprovisioning. An abundance of resources, for example, a pool of servers with load balancer, high

bandwidth link between victim machine, and upstream routers are used to tolerate these attacks (Mirkovic & Reiher, 2004; Lee, 2003; Bush et al., 2000).

A-4-2: Router's Queue Management. Router's queue management schemes aim to reduce attack impact or congestion simply without providing fairness between the traffic flows. Therefore, NPSR is very low in these schemes (Floyd & Jacobon, 1993; Floyd & Fall, 1999).

A-4-3: Router's Traffic Scheduling. Router's traffic scheduling algorithm can reduce congestion or attack impact with the fairness between the traffic flows, but they are too expensive in terms of delays and state monitoring (Demers, Keshav, & Shenker, 1990; Mckenny, 1990; Mankin & Ramakrishnan, 1991).

A-4-4: Target Roaming. Active servers change their location within distributed homogeneous servers proactively to eliminate or curtail DDoS attacks impact (Khattab et al., 2003).

B. Classification Based on Degree of Deployment

Classification based on degree of deployment categorizes the DDoS defense mechanisms in the following two categories:

B-1: Single Point or Autonomous Defense

Single point or autonomous defense mechanisms (Bencsath & Vajda, 2004; Gupta et al., 2008; Feinstein et al., 2003; Lakhina et al., 2005) consist of a single defense node that observes the attack and applies response.

B-2: Multipoint or Distributed Defense

Multipoint or distributed defense mechanisms (Chen, Hwang, & Ku, 2007; Savage et al., 2000; Snoeren et al., 2001; Bellovin et al., 2001; Dean et al., 2002; Song & Perrig, 2001; Belenky & Ansari, 2003; Floyd et al., 2001; Keromytis, Misra, & Rubenstein, 2002; Mirkovic, Robinson, & Reiher, 2003) consist of multiple defense nodes, generally with the same functionalities that are deployed at various locations and organized into network. Nodes are communicated through the network and coordinate their actions to achieve a better overall defense.

C. Classification Based on Deployment Point or Location

Classification based on deployment points or locations (as shown in Figure 10) categorizes the DDoS defense mechanisms in the following three categories:

C-1: Victim or Target Network

Most of the existing DDoS defenses systems have been designed to work at the victim network (Bencsath & Vajda, 2004; Gupta et al., 2008; Feinstein et al., 2003; Lakhina et al., 2005; Guupta et al., 2007). This is understandable because it can closely observe the victim system's behavior, model its normal system model that can be used to find a variety of anomalies. So it is best placed to detect DDoS attack; however, these systems may themselves become targets of DoS attacks by sending a sheer amount of traffic from various distributed attack sources that can overwhelmed it. Storage and processing power requirement to store and examine various statistical measures are very high in these systems.

C-2: Intermediate Network

These mechanisms (Savage et al., 2000; Snoeren et al., 2001; Bellovin et al., 2001; Dean et al., 2002; Song & Perrig, 2001; Belenky & Ansari, 2003; Floyd, 2001; Keromytis et al., 2002) are deployed at core routers. Since core routers can handle large volume, highly aggregated traffic, they are likely to overlook all but large scale attacks. However, response to attacks is likely to inflict collateral damages, as core routers can only accommodate simple rate-limiting request and cannot dedicate memory or processing cycle to traffic profiling.

C-3: Source Network

These mechanisms are deployed at source end, that is, edge routers, and can detect DDoS attacks at the source based on the idea that DDoS attacks should be stopped as close to the sources as possible. At this place attack flows are not so aggregated, so it would place less burden on the defense systems to analyze them. Since they would be cut off at the source, it would save transit networks from transporting malicious traffic. This approach, however, requires a large scale deployment in order to be effective. Also, since

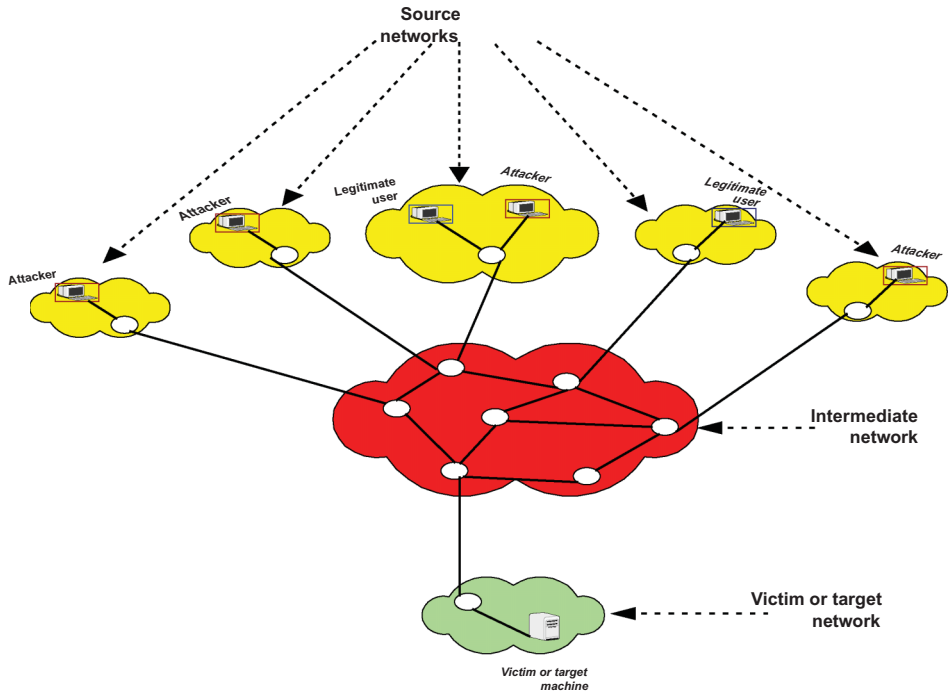

FIGURE 10 DDoS defense deployment points or locations.

attack streams in the source network usually are small in volume, they may be more difficult to detect and a large number of false positives and negatives exist (Gill & Poletto, 2001; Mirkovic et al., 2002).

D. Classification Based on Degree of Cooperation

Classification based on degree of cooperation categorizes the DDoS defense mechanisms in the following categories:

D-1: Independent

As the name suggests, independent defense mechanisms (Oppliger, 1997; Ferguson & Senie, 2001; Global incident analysis, n.d.; Park & Lee, 2001; Peng et al., 2003; Li et al., 2002; Paxson, 1999; Roesch, 1999; Gil & Poletto, 2001; Blazek et al., 2001; Gupta et al., 2008) work independently at the location where they are deployed.

D-2: Cooperative

Cooperative defense mechanisms (Chen, Hwang, & Ku, 2007; Floyd et al., 2001; Keromytis et al., 2002; Mirkovic et al., 2003) are capable of working independently but can cooperate with other entity to increase performance significantly.

D-3: Interdependent

Interdependent defense mechanisms (Savage et al., 2000; Snoeren et al., 2001; Bellovin et al., 2001; Dean et al., 2002; Song & Perrig, 2001; Belenky & Ansari, 2003) cannot operate independently at single deployment point. They either require deployment at multiple networks, or rely on other entities for attack prevention, detection or response.

5. INTEGRATED SOLUTION FOR DEFENDING AGAINST DDOS ATTACKS

Although there are many DDoS solutions proposed by different scholars, literature shows that there has been no effective way proposed to defend against DDoS attacks. This might be due to several reasons, including:

- Solution deployment issue: It is the willingness of major and local ISPs to deploy defense components on their resources for the benefit of others.

- Lack of completeness: Many defense solutions that are proposed so far have focused only on particular DDoS attacks and will not protect against others.
- Collateral damage to legitimate traffic: Defense systems may prevent or delay normal clients request during filtering the attacks.
- Complexity of proposed solutions: Some solutions may require much processing and storage capacity from the available limited resources.

Moreover, these attacks are dynamic and can escape from existing defense systems. With the emergence of sophisticated data collection tools and massive data repositories, there is a need for solutions that will not only detect a wide range of DDoS attacks by simultaneously analyzing heterogeneous data sources but also provide meaningful information to the analysts in real time. In addition, if we see current issues and challenges under a wide range of attacks, we can say that only an efficient integrated solution that encompasses several defense activities can trap a variety of DDoS attacks. If one level of defense fails, the others still have the possibility to defend against attack. A successful intrusion requires all defense levels to fail.

We have tried to address the above mentioned limitations of current research on defending against DDoS attacks. In summary, the problem can be stated as this: *"To defend against a wide range of Distributed Denial-of-Service attacks, there is a need to develop a robust and efficient approach which can prevent known attacks, detect novel attacks with minimum false positives and then respond against these novel attacks in cost effective manner."* Therefore, we propose an incrementally deployable robust and efficient integrated framework as shown in Figure 11, which aims to provide following activities in defending against DDoS attacks at ISP level:

- **Attack prevention:** Prevention from known DDoS attacks.
- **Attack detection:** Detects a wide range of flooding DDoS attacks autonomously in ISP network while victim is being attacked.
- **Malicious flows characterization:** Identifies and tags attack flows accurately in real time.
- **Attack response:** Responds to identified attacks by either filtering or rate throttling according to strength of attacks.

The detailed explanation of proposed framework given in Figure 11 is as follows:

- Input is network packet.
- Check whether packet matches with desired conditional rules, if not it should be declined.
- Monitor the packets statistics for period of ΔT.
- Check for anomaly; if yes, then presence of attack is identified.
- Identify flows responsible for the attack traffic in the network.
- Stop/Rate limit these flows, depending on the strength of attacks.

Various defense principles being satisfied by our proposed approach are explained below:

- While prevention and response engines are placed at edges routers or as a separate module that interact with the edge routers, detection engine is placed at bottleneck router or as separate module that interacts with the bottleneck router. Therefore, it is a distributed defense mechanism.
- Our novel characterization scheme categorizes incoming flows in three categories: normal, suspicious, and confirm attack flows depending on deflection from thresholds. Our system filters only those flows that come under confirm attack category. Rate of the traffic coming through flows that come under suspicious category is throttled according to strength of attack. If rate of incoming attack traffic is high, traffic coming through suspicious flows is throttled with high rate and vice versa. As our system filters only confirmed attack traffic, Normal Packet Survival Ratio (NPSR) is very high.
- For communication between edge routers and bottleneck router, secure control messages are to be exchanged with proper security and routers cryptographically verify its authenticity and integrity in order to prevent new DDoS attacks.
- Proposed framework can be extended easily to multiple ISP domains with help of trusted entities acting as interfaces between two ISPs so that two ISPs can share there information and thus more effectively stop the attack.
- Proposed system has considered future compatibility issues; therefore, it can interact with other systems, if needed.

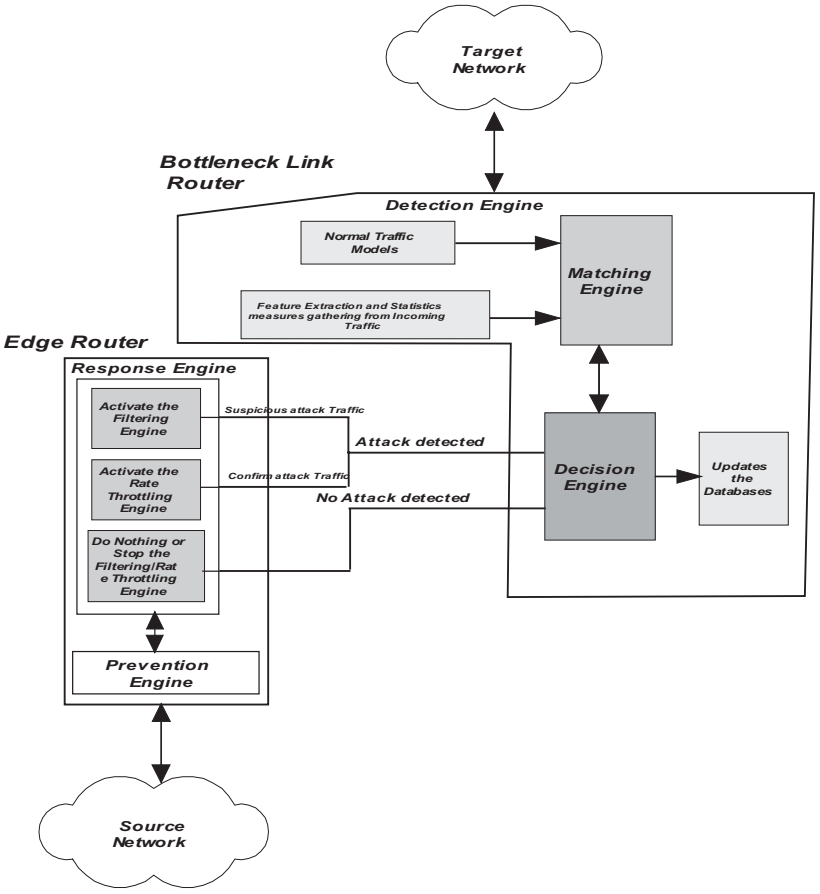

FIGURE 11 Overview of proposed DDoS defense framework.

5.1 Attack Prevention

Prevention system is part of the edge routers or can belong to separate unit that interact with edge routers for DDoS attacks prevention. In prevention, all well known signatures based and broadcast based attacks can be stopped at edge routers. We propose to have a historical logs based approach with a space efficient data structure for prevention. Historical logs are used to contain information of dropped packets due to congestion and history of all the legitimate IP addresses that have previously appeared in the network. Various packet filtering rules are made using this historical logs information to define attack signatures that are stored at edge routers to filter attack traffic. Mining association rule techniques (Lee & Stolfo, 2000; Ramkumar, Ranka, & Tsur, n.d.) are used for making filtering rules. Mining association rules search for interesting relationships among items in a given dataset. Functional diagram of our proposed DDoS attack prevention approach is shown Figure 12. Rule mining engine consists of two phases of development: training and real time traffic phase. Training phase is needed to generate rules from attack free traffic. The real time traffic phase is needed to generate rules from real time traffic.

First various connection features like IP header fields, TCP source and destination ports, UDP source and destination ports, ICMP type, dst_byte, src_byte, service, duration timestamp etc. are extracted from incoming packets header to create filtering rules. Then rule mining engine generates various rules from incoming traffic. Finally, anomalous traffic is find out using matching engine and then filtered. Below are some examples of filtering rules:

"drop | allow {daddr = 70.3.5.1 protocol
= 6 dport = 80 saddr = 14.6.2.1 sport = 45}"

Above packet filter rule will drop/allow packets going to the particular destination IP address 70.3.5.1,

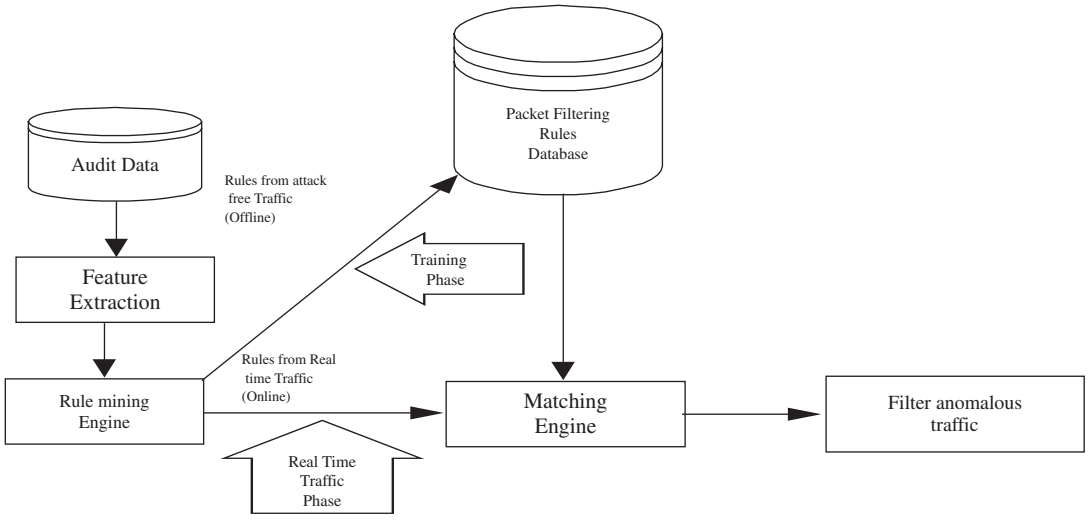

FIGURE 12 **Functional diagram of our proposed DDoS attack prevention approach.**

destination port = 80 from source IP address 14.6.2.1 and source port = 45.

"allow {if (ip.saddr ! = ip.daddr)};"
"allow {if (tcp.sport ! = tcp.dport)};"
"allow {if (udp.sport ! = udp.dport)};"
"allow {if incoming packet's IP address is not
from reserve IP addresses };"

In historical logs-based packet filtering, space requirement at edge routers to store history information is very high. We use bloom filter (Bloom, 1970; Abdelsayed et al., 2003), a space efficient data structure to reduce high space requirement. The Bloom filter, conceived by Burton H. Bloom in 1970, is a space-efficient data structure that is used to test whether an element is a member of a set.

Bloom filters have a strong space advantage over other data structures for representing sets such as binary search trees, hash tables, simple arrays or linked lists of the entries. It allows low and controlled false positives. A Bloom filter for representing a set $S = \{x_1, x_2, \ldots, x_n\}$ of n elements is composed by an array of m bits, initially all set to 0. We use k independent hash functions $h_1, h_2, \ldots, h_k$, each with range {0, 1, . . ., m-1}. For each element $x \in S$, the bits $h_i(x)$ are set to 1 for $1 \leq i \leq k$. Given a query on the existence of y in S, we check whether all $h_i(y)$ are set to 1. If not, then clearly y is not in S. If all $h_i(y)$ are set to 1, we assume that y is in S, although we are wrong with some probability. This probability is referred to as the *false positive* rate, where it suggests that an element x is in S even though it is not.

5.2 Attack Detection

Detection system is part of access router or can belong to separate unit that interact with access router to detect and identify attack traffic. Proposed approach detects DDoS flooding attacks by monitoring the propagation of abrupt traffic changes inside the network. Varieties of metric are available to capture distribution changes in traffic features. A traffic feature is a field in the header of a packet. Normally focus is on four fields: source IP address, destination IP address, source port, and destination port. This 4-tuple of 96 bytes is called flow.

Detecting DDoS attacks involves first knowing normal behavior of our system and then to find deviation from that behavior. Normal profile is build off line using traces collected for the network without attack, whereas for attack detection, on line monitoring, analysis and comparison with normal profile is done under attack. Some of the statistical measures (or metrics) are described as follows:

Volume based metric:
It is used to count the number of packet occurring during a period of Δ T time.

Volume = (Total number of packet/ Δ T).

$$\text{Volume} = \sum_{i=1}^{N} n_i / \Delta T.$$

Flow based metric:

It is used to measure the total number of distinct flows during a period of ΔT time.

Flow = (Total number of distinct flows/ ΔT).

Ratio based metric:

It is used to calculate ratio of total incoming packets with total outgoing packets.

Ratio = (Total number of incoming packet/ Total number of outgoing packets).

Entropy based metric:

It is used to calculate degree of dispersal or concentration of a distribution.

$$\text{Entropy} = -\sum_{i=1}^{N} (p_i) \times \log_2 (p_i)$$

where $p_i = n_i / S, \ \ i = 1, \ldots\ldots, N$ and $S = \sum_{i=1}^{N} n_i$ is the total number of packets during a period of ΔT time. The value of sample entropy lies in the range $0 - \log_2 N$. The metric takes on the value 0 when the distribution is maximally concentrated. Sample entropy takes on the value $\log_2 N$ when the distribution is maximally dispersed.

All these metrics have different advantage and disadvantage. Volume-based metric is suitable for the high rate DoS and DDoS attack, which is easy to detect. However, for low rate DDoS attack, its abilities will be reduced. Flow-based metric work well when the attack is performed in distributed manner, such as Smurf Attack or ICMP Flood attack. Distribution of source IP addresses during the attack is easy to recognize, but it is difficult to measure volume of the attack. Therefore, high rate DoS attacks are undetectable using flow metric. Ratio analysis plays its role for the attack well, and that creates high difference of attack ratio such as TCP SYN Flood and Smurf Attack. However, it is less effective in low rate DDoS attacks. Entropy-based metrics work well against high and low rate DDoS attacks. It is not effective in dealing with varied rate DDoS attacks. Therefore, combining use of these metrics may increase the efficiency of detection. In our system, we will use two metrics, namely, volume and flow in combination to detect a wide range of DDoS attacks.

5.3 Characterization of Malicious Flows

After detecting that DDoS attacks are occurring, the next thing to do is separate traffic coming through malicious flows from legitimate traffic to respond to attacks correctly. We observed number of bytes arrival for each flow during the monitoring period, and flows that cross predefined thresholds are classified as either suspicious or attack traffic flows depending on deflection from thresholds. Six-sigma concept (Raisinghani et al., 2005; Kim, 2006) is used to calculate the Upper Control Limit (UCL) and Lower Control Limit (LCL) values in order to differentiate the normal, suspicious, and attack state of the total number of bytes arrival for each flow.

5.2.1 Six-Sigma Method

Six-Sigma scheme is proposed by Motorola to address quality problem and business improvement. Six-Sigma claims that focusing on reduction of variation will solve process and business problems. By using a set of statistical tools to understand the fluctuation of a process, management can begin to predict the expected outcome of that process. If the outcome is not satisfactory, associated tools can be used to further understand the elements influencing that process. Using Six-Sigma, there would be approximately 3.4 or fewer failures per billion attempts. This is an extremely low rate of failure. To find Six-Sigma, calculate sigma or standard deviation, multiply by 6, and add or subtract the result to the calculated mean.

5.4 Response to Attacks

Response system is part of edge routers of the ISP or can belong to separate unit that interact with edge routers to responds to attacks traffic. Our system can respond to the malicious flows either by filtering confirmed attack flows or by rate throttling suspicious flows. Rate of packets coming through suspicious flows is throttled according to strengths of attacks. If incoming rate of attack traffic is high, packets coming through suspicious flows are throttle with high rate and vice versa.

6. CONCLUSIONS AND SCOPE FOR FURTHER RESEARCH

DDoS attack is currently amongst the latest and most problematic trends in network security threats. It is an attack on availability in the Internet, wireless network, and other infrastructures as well. In this paper, we have presented overview of the DDoS problem, various attack methods, and current defense mechanisms. This provides better understanding of the problem, current solution space, and future scope to defend against DDoS attack.

The current defense mechanisms reviewed in this paper are clearly far from adequate to protect the Internet from DDoS attack. The main problem is that there are still many insecure machines over the Internet that can be compromised to launch a large-scale, coordinated DDoS attack. One promising direction is to develop a comprehensive solution that encompasses several defense activities to trap a variety of DDoS attacks. If one level of defense fails, the others still have the possibility to defend against attack. A successful intrusion requires all defense level to fail. Therefore, an integrated solution is proposed to defend against flooding DDoS attacks completely. The proposed framework can be implemented incrementally and does not disrupt current Internet users. Implementation of proposed framework is a future work. However, this is only the first step toward realizing the secure Internet paradigm.

Currently, the proposed framework is limited to a single ISP domain, but it can be extended to multiple ISP domains with the help of trusted entities acting as interfaces between two ISPs so that two ISPs can share their information and thus more effectively stop the attack.

For future research, we have addressed a number of research issues. The major research issues are being listed as follows:

- **Technical and economic model:** The longer-term challenge for defense against DoS attacks is to find a technical and economic model to achieve cooperation between ISPs in order to combat a wide range of DDoS attacks collaboratively.
- **Analytical solution:** A large number of simulation-based schemes are proposed in the literature, but an effective analytical solution to defend against DDoS attacks is still a pending issue.
- **Solution to deal with unresponsive traffic flows in regard to fairness:** In general, we observe the arriving rate for the monitored traffic flow after the dropping probability increases. If the arriving rate does not slow down, we can regard this traffic flow as unresponsive traffic flow. However, there are some false positives, in that we could identify some traffic flows which actually are responsive. The arrival rate of a flow at the router depends not only on the drops at that router, but also on the demand from the application, and drops elsewhere along the path. In addition, the router does not know the round-trip time or the other factors, for example, equation-based congestion control mechanism, multicast, etc., that affect the timeliness of the flow's response to congestion. At the same time, we might not detect some traffic flows which are not responsive. We should find a proper way to test the unresponsiveness of the traffic flow or improve the accuracy.
- **Distributed solution:** The mammoth volume generated by DDoS attacks pose the biggest challenge in terms of memory and computational overheads as far as monitoring and analysis of traffic at single point connecting victim is concerned. To address this problem, an effective distributed cooperative technique is required to be proposed that distributes memory and computational overheads to many points e.g. all edge routers for detecting a wide range of DDoS attacks at early stage.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the financial support of the Ministry of Human Resource Development (MHRD), Government of India for partial work reported in the paper.

REFERENCES

Abdelsayed, S., Glimsholt, D., Leckie, C., Ryan, S., and Shami, S. (2003). An efficient filter for denial-of-service bandwidth attacks. In *Proceedings of IEEE Global Telecommunications Conference (GLOBECOM'03)*, Volume 3, pp 1353–1357.

Abennett. (2001, May). CERT hit by DDoS attack for a third day. Available at http://www.itworld.com/IDG010524CERT2

Akamai. (2004, June). Press release: Akamai provides insight into Internet denial of service attack. Available at http://www.akamai.com/en/html/about/press/press459.html

Andersen, D.G., Balakrishnan, H., Kaashoek, M.F., and Morris, R. (2001, October). Resilient overlay networks. In *Proceedings of 18th ACM SOSP*, pp. 131–145, Banff, Canada.

Andrews, J. (2004). Understanding TCP reset attacks. Available at http://kerneltrap.org/node/3072

AusCERT. (2005). 2005 Australian computer crime and security survey. *Tech. Report*, Australian Computer Emergency Response Team. Available at http://www.auscert.org.au/crimesurvey

Azrina, R., and Othman, R. (n.d.). Understanding the various types of denial of service attack. Available at www.niser.org.my/resources/dos_attack.pdf

Bai, Y., and Kobayashi, H. (2003, March). Intrusion detection system: Technology and development. In *Proceedings of the 17th International Conference on Advanced Information Networking and Applications (AINA)*, pp. 710–715.

Barlow, J., and Thrower, W. (2000, February 10). TFN2K—an analysis. Axent Security Team. Available at http://security.royans.net/info/posts/bugtraq_ddos2.shtml

Belenky, A., and Ansari, N. (2003). IP traceback with deterministic packet marking. *IEEE Communication Letter*, 7(4), 162–164.

Bellovin, S., Leech, M., and Taylor, T. (2001, October). ICMP traceback messages. *Internet draft: draft*-ietf-itrace-01.txt, *work in progress*.

Bencsath, B., and Vajda, I. (2004). Protection against DDoS attacks based on traffic level measurements. In *Proceedings of the Western Simulation Multi Conference*, San Diego, CA, pp. 22–28.

Blazek, R.B., Kim, H., Rozovskii, B., and Tartakovsky, A. (2001). "A novel approach to detection of denial-of-service attacks via adaptive sequential and batch sequential change-point detection methods," in *Proceedings of IEEE Systems, Man and Cybernetics Information Assurance Workshop*, pp. 220–226, 2001.

Burton, H. Bloom. (1970, July). Space/time trade-offs in hash coding with allowable errors. *Communications of the ACM (CACM)*, 13(7), 422–426.

Bush, R., Karrenberg, D., Kosters, M., and Plzak, R. (2000, June). Root name server operational requirements. *BCP 40*, RFC 2870.

Bysin. (2001, July 11). Knight.c sourcecode. PacketStormSecurity.nl. Available at http://packetstormsecurity.nl/distributed/knight.c

CERT. (1996, September). CERT advisory CA-1996-21 TCP SYN Flooding and IP spoofing attacks.

CERT Coordination Center (1999). Denial of service tools. Available at http://www.cert.org/advisories/CA-1999-17.html

CERT Coordination Center. (n.d.). Mail bomb attack. Available at http://www.cert.org/tech_tips/email_bombing_spamming.html

CERT Coordination Center. (2001). Carnegie Mellon Software Engineering Institute, CERT Advisory CA-2001-20 Continuing threats to home users, 23. Available at http://www.cert.org/advisories/CA-2001-20.html

CERT Statistics. Available at http://www.cert.org/stats/cert_stats.html

CGI request attack. (n.d.). Available at http://cpan.uwinnipeg.ca/htdocs/CGI.pm/CGI.html

Chen, Y., Hwang, K., and Ku, W. (2007, December). Collaborative detection of DDoS attacks over multiple network domains. *IEEE Transaction on Parallel and Distributed Systems*, TPDS-0228-0806, 18(12).

Cheng, C.M., Kung, H.T., and Tan, K.S. (2002). Use of spectral analysis in defense against DoS attacks. In *Proceedings of IEEE GLOBECOM 2002*, Taipei, Taiwan, pp. 2143–2148.

Cheung, S. (2006, January/February). Denial of service against the domain name system. *IEEE Security & Privacy*, 4(1), 40–45.

Darmohray, T., and Oliver, R. (2000). Hot spares for DDoS attacks. Available at http://www.usenix.org/publications/login/2000-7/apropos.html

DDoS attacks on Yahoo, Buy.com, eBay, Amazon, Datek, E*Trade. (2000, February 7–11). *CNN Headline News*.

Dean, D., Franklin, M., and Stubblefield, A. (2002). An algebraic approach to IP traceback. *ACM Trans. Inform. System Security*, 5(2), 119–137.

Debar, H., Dacier, M., and Wespi, A. (1999). Towards a taxonomy of intrusion detection systems. *Computer Networks*, 31.

Demers, A., Keshav, S., and Shenker, S. (1990). Analysis and simulation of a fair queuing algorithm. *Journal of Internetworking Research and Experience*, 1(1), pp. 3–26.

Dietrich, S., Long, N., and Dittrich, D. (2000). Analyzing distributed denial of service tools: The Shaft case. In *Proceedings of the 14th Systems Administration Conference (LISA 2000)*, New Orleans, LA, December 3–8, pp. 329–339.

Dittrich, D., Weaver, G., Dietrich, S., and Long, N. (2000, May). The "Mstream" distributed denial of service attack too. Available at http://staff.washington.edu/dittrich/misc/mstream.analysis.txt

Dittrich, D. (1999, October 21). The DoS project's Trinoo distributed denial of service attack tool. University of Washington. Available at http://staff.washington.edu/dittrich/misc/trinoo.analysis.txt

Dittrich, D. (1999, October 21). The tribe flood network distributed denial of service attack tool. University of Washington. Available at http://staff.washington.edu/dittrich/misc/tfn.analysis.txt

Dittrich, D. (1999, December). The Stacheldraht distributed denial of service attack tool. University of Washington. Available at http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt

Douligeris, C., and Mitrokotsa, A. (2003). DDoS attacks and defense mechanisms: Classification. In *Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology (ISSPIT 03)*, pp. 190–193, Darmstadt, Germany, December 14–17.

Douligeris, C., and Mitrokotsa, A. (2004, April). DDoS attacks and defense mechanisms: Classification and state-of-the-art. *Computer Networks*, 44(5), 643–666.

Farrow, R. (n.d.). TCP SYN Flooding attacks and remedies. *Network Computing Unix World*. Available at http://www.networkcomputing.com/unixworld/security/004/004.txt.html

Feinstein, L., Schnackenberg, D., Balupari, R., and Kindred, D. (2003). Statistical approaches to DDoS attack detection and response. In *Proceedings of DISCEX'03*, Washington, DC, Vol. 1, pp. 303–314.

Ferguson, P., and Senie, D. (2001). Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing. *RFC 2827*.

Floyd, S., and Jacobon, V. (1993). Random early detection gateways for congestion avoidance. *IEEE/ACM Trans. on Networking*, 1(4), 397–413.

Floyd, S., and Fall, K. (1999, August). Promoting the use of end-to-end congestion control in the Internet. *IEEE/ACM Trans*. on *Networking*, 7(4), 458–472.

Floyd, S., Bellovin, S., Loannidis, J., Kompella, K., Mahajan, R., and Paxson, V. (2001). Pushback messages for controlling aggregates in the network. Available at *draft-floyd-pushback-messages-00.txt*

Galli, P. (2006, March). DoS attack brings down Sun Grid demo. Available at http://www.eweek.com/article2/0,1895,1941574,00.asp

Garber, L. (2000, April). Denial-of-service attacks rip the Internet. *IEEE Computer*, 33(4), 12–17.

Geng, X., and Whinston, A.B. (2000). Defeating distributed denial of service attacks. *IEEE IT Professional*, 2(4), 36–42.

Gibson, S. (2002, March). The strange tale of the attacks against GRC.COM. Available at http://grc.com/dos/grcdos.htm

Gil, T.M., and Poletto, M. (2001). Multops: A data-structure for bandwidth attack detection. In *Proceedings of the 10th USENIX Security Symposium*, Washington, DC, pp. 23–38.

Global incident analysis center-special notice-egress filtering v 0.2. Available at http://www.sans.org/y2k/egress.htm

Gonsalves, C. (2004, June). Akamai DDoS attack whacks Web traffic. Available at http://www.eweek.com/article2/0,1895,1612739,00.asp

Gordon, L.A., Loeb, M.P., Lucyshyn, W., and Richardson, R. (2005). 2005 CSI/FBI computer crime and security survey. *Tech. Report*, Computer Security Institute. Available at www.GCSI.com

Gupta, B.B., Misra, M. and Joshi, R.C. (2008). An ISP level solution to combat DDoS attacks using combined statistical based approach. *International Journal of Information Assurance and Security (JIAS)*, 3(2), 102–110.

Gupta, B.B., Misra, M., and Joshi, R.C. (2008). FVBA: A combined statistical approach for low rate degrading and high bandwidth disruptive DDoS attacks detection in ISP domain. In *Proceedings of 16th IEEE International Conference On Networks (ICON-2008)*, New Delhi, India, Dec. 12–14, pp. 34–37.

Gupta, B.B., Kumar, K., Singh, K., and Joshi, R.C. (2007). Distributed approach to detect DDoS attacks in ISP domain using entropy. In *Proceedings of International Conference on Advanced Communication System (ICACS-2007)*, India, pp. 101–108.

Hancock, B. (2000). Trinity v3, a DDoS tool, hits the streets. *Computers Security*, 19(7), 574.

Handley, M. (2005). Internet architecture WG: DoS-resistant Internet subgroup report. Available at http://www.communications.net/object/download/1543/doc/mjh-dos-summary.pdf

Hazelhurst, S. (2000). Algorithms for analyzing firewall and router access lists. In *Proceedings of Workshop on Dependable IP Systems and Platforms (ICDSN)*.

Howard, J. (1998, August). An analysis of security incidents on the Internet 1989–1995. PhD thesis, Carnegie Mellon University.

Huegen, C.A. (2000). The latest in denial of service attacks: "SMURFING" description and information to minimize effects. Available at http://www.pentics.net/denial-of-service/white-papers/smurf.txt

Hwang, K., Cai, M., Chen, Y., and Qin, M. (2007). Hybrid intrusion detection with weighted signature generation over anomalous Internet episodes. *IEEE Transaction on Dependable and Secure Computing*, 4(1), 41–55.

IRC Security. (n.d.). Available at http://www.irchelp.org/irchelp/security/

J-063: Domain name system (DNS) denial of service (DoS) attacks. (1999). Available at http://www.securityfocus.com/advisories/1727

Javvin network management & security. (n.d.). UDP Flood attack. Available at http://www.javvin.com/networkSecurity/UDPFloodAttack.html

Kenney, M. (n.d.). Ping of death attack. Available at http://insecure.org/sploits/ping-o-death.html

Keromytis, A.D., Misra, V., and Rubenstein, D. (2002). SOS: Secure overlay services. In *Proceedings of ACM SIGCOMM*, pp. 61–72.

Khattab, S.M., Sangpachatanaruk, C., Melhem, R., Mosse, D., and Znati, T. (2003, August). Proactive server roaming for mitigating denial of service attacks. In *Proceedings of the 1st International Conference on International Technology: Research and Education (ITRE 03)*, Newark, NJ, pp. 500–504.

Kim, D. (2006, August). A study on introducing Six Sigma theory in the library for service competitiveness enhancement. In *Proceedings of the World Library and Information Congress: 72nd IFLA General Conference and Council*, Seoul, Korea, pp. 20–24

Kumar, K., Joshi, R.C., and Singh, K. (2006). An integrated approach for defending against distributed denial-of-service (DDoS) attacks. In *Proceedings of IRISS-2006*, IIT Madras. Available at www.cs.iitm.ernet.in/~iriss06/iitr_krishan.pdf

Lakhina, A., Crovella, M., and Diot, C. (2005). Mining anomalies using traffic feature distributions. *ACM SIGCOMM Computer Communication Review*, 35(4), 217–228.

Lau, F., Stuart, R.H., Michael, S.H., et al. (2000). Distributed denial of service attacks. In *Proceedings of 2000 IEEE International Conference on Systems, Man, and Cybernetics*, Nashville, TN, Vol.3, pp. 2275–2280.

Lee, R.B. (2003). Taxonomies of distributed denial of service networks, attacks, tools and countermeasures. Princeton University. Available at http://www.ee.princeton.edu/~rblee

Lee, W., Stolfo, S.J., and Mok, K.W. (1999). A data mining framework for building intrusion detection models. In *Proceedings of the 1999 IEEE Symposium on Security and Privacy*, Oakland, CA, May 9–12, pp. 120–132.

Lee, W., and Stolfo, S. (2000). A framework for constructing features and models for intrusion detection systems. *ACM Trans. Information and System Security (TISSEC)*, 3(4), 227–261.

Leyden, J. (2002, April). Scottish ISP floored as DDoS attacks escalate. Available at http://www.theregister.co.uk/2002/04/09/scottish_isp_floored_as_ddos/

Leiner, B.M., Cerf, V.G., et. al. (2003). *A brief history of the Internet*. Internet Society. Available at http://www.isoc.org

Li, M., Li, M., and Jiang, X. (2008). DDoS attacks detection model and its applications. *WSEAS Transactions on Computers*, 7(8), 1159–1168.

Li, J., Mirkovic, J., Wang, M. Reiher P., and Zhang, L. (2002). SAVE: Source address validity enforcement protocol. In *Proceedings of IEEE INFOCOM*, pp. 1557–1566.

Limwiwatkul, L., and Rungsawang, A. (2004, October). Distributed denial of service detection using TCP/IP header and traffic measurement analysis. In *Proceedings of IEEE International Symposium on Communications and Information Technology (ISCIT 2004)*, pp. 605–610.

Mankin, A., and Ramakrishnan, K. (1991, August). Gateway congestion control survey. *IETF RFC 1254*. Available at http://www.rfc-editor.org/rfc.html

Marchesseau, M. (2000, September). Trinity-distributed denial of service attack tool. Available at http://www.giac.org/certified_professionals/practicals/gsec/0123.php

McAfee. (n.d.) Personal Firewall. Available at http://www.mcafee.com/myapps/firewall/ov_firewall.asp

Mckenny, P. (1990). Stochastic fairness queuing. In *Proceeding of IEEE INFOCOM*, Piscataway, NJ, pp. 733–740.

Mirkovic, J., Prier, G., and Reiher, P. (2002). Attacking DDoS at the source. In *Proceedings of ICNP-2002*, Paris, France, pp. 312–321.

Mirkovic, J., and Reiher, P. (2004, April). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communications Review*, 34(2), 39–53.

Mirkovic, J., Robinson, M., and Reiher, P. (2003). Forming alliance for DDoS defenses. In *Proceedings of New Security Paradigmes Workshop (NSPW 2003)*, ACM Press, New York, NY, August 11–18.

Molsa, J. (2005). Mitigating denial of service attacks: A tutorial. *Journal of Computer Security*, 13, 807–837.

Moore, D., Shannon, C., Brown, D.J., Voelker, G., and Savage, S. (2006). Inferring Internet denial-of-service activity. *ACM Transactions on Computer Systems*, 24(2), 115–139.

Oppliger, R. (1997). Internet security: Firewall and beyond. *Communications of the ACM*, 40(5), 92–102.

Papadopoulos, C., Lindell, R., Mehringer, J., Hussain, A., and Govindan, R. (2003, April). COSSACK: Coordinated suppression of simultaneous attacks. In *Proceedings of the DARPA Information Survivability Conference and Exposition*, Vol. 1, pp. 2–13.

Park, K., and Lee, H. (2001). On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law Internets. In *Proceedings of the ACM SIGCOMM 2001 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, ACM Press, New York, pp. 15–26, 2001.

Paxson, V. (2001). An analysis of using reflectors for distributed denial-of-service attacks. *ACM SIGCOMM Computer Communications Review (CCR)*, 31(3), 38–47.

Paxson, V. (1999). Bro: A system for detecting network intruders in real-time. *International Journal of Computer and Telecommunication Networking*, 31(24), 2435–2463.

Peng, T., Leckie, C., and Ramamohanarao, K. (2003). Protection from distributed denial of service attack using history-based IP filtering. In *Proceedings of IEEE International Conference on Communications (ICC 2003)*, Anchorage, AL, Volume 1, pp. 482–486.

Raisinghani, M.S., Ette, H., Pierce, R., Cannon, G., and Daripaly, P. (2005). Six Sigma: concepts, tools, and applications. *Journal of Industrial Management & Data Systems*, 105(4), 491–505.

Ramkumar, G.D., Ranka, S., and Tsur, S. (1998). Weighted association rules: Model and algorithm. In *Proceedings of Fourth ACM Int'l Conf. Knowledge Discovery and Data Mining*. Available at http://www.cs.ucla.edu/~czdemo/tsur/Papers/wis.ps

Robinson, M., Mirkovic, J., Schnaider, M., Michel, S., and Reiher, P. (2003). Challenges and principles of DDoS defense. *SIGCOMM*.

Roesch, M. (1999, November). Snort-lightweight intrusion detection for networks. In *Proceedings of the USENIX Systems Administration Conference (LISA '99)*, pp. 229–238.

Savage, S., Wetherall, D., Karlin, A., and Anderson, T. (2000, August). Practical network support for IP traceback. In *Proceedings of ACM SIGCOMM 2000*, Stockholm, Sweden, pp. 295–306.

Scalzo, F. (2006). Recent DNS reflector attacks. VeriSign. Available at http://www.nanog.org/mtg-0606/pdf/frank-scalzo.pdf

Schuba, C., Krsul, I., Kuhn, M., Spafford, G., Sundaram, A., and Zamboni, D. (1997, May). Analysis of a denial of service attack on TCP. In *Proceedings of the 1997 IEEE Symposium on Security and Privacy*.

Singh Negi, C. (2001, September). Using network management system to detect distributed denial of service attacks. Master's thesis, Naval Postgraduate School Monterey, CA.

Snoeren, A.C., Partridge, C., Sanchez, L.A., Jones, C.E., Tchakountio, F., Kent, S.T., and Strayer, W.T. (2001, August). Hash-based IP traceback. In *Proceedings of ACM SIGCOMM 2001*, San Diego, CA, pp. 3–14.

Song, D.X., and Perrig, A. (2001). Advanced and authenticated marking schemes for IP Traceback. In *Proceedings of IEEE INFOCOM*, pp. 878–886.

Teardrop attacks. (n.d.). Available at http://www.physnet.uni-hamburg.de/physnet/security/vulnerability/teardrop.html

The ISC Internet Domain Survey. Available at https://www.isc.org/solutions/survey

Weiler, N. (2002, June). Honeypots for distributed denial of service attacks. In *Proceedings of the Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'02)*, pp. 109–114, Pittsburgh, PA.

Wikipedia. (n.d.). DNS request attack. Available at http://en.wikipedia.org/wiki/DNS_cache_poisoning

Wikipedia. (n.d.). LAND attack. Available at http://en.wikipedia.org/wiki/LAND

Xiang, Y., Zhou, W., and Chowdhury, M. (2004). *A survey of active and passive defense mechanisms against DDoS attacks*. Technical Report, TR C04/02, School of Information Technology, Deakin University, Australia.

BIOGRAPHIES

B. B. Gupta received a bachelor's degree in Information Technology in 2005 from Rajasthan University, India. He is currently a PhD student in the Department of Electronics and Computer Engineering at Indian Institute of Technology, Roorkee, India. His research interests include defense mechanisms for thwarting Denial-of-Service attacks, network security, cryptography, data mining, data structure, and Algorithms.

R. C. Joshi received a bachelor's degree in Electrical Engineering from Allahabad University, India, in 1967. He received his master's and PhD degrees in Electronics and Computer Engineering from University of Roorkee, India, in 1970 and 1980, respectively. Currently, he is working as a Professor at Indian Institute of Technology Roorkee, India. He has served as Head of the Department twice from January 1991 to January 1994 and from January 1997 to December 1999. He has been Head of Institute Computer Centre (ICC), IIT Roorkee, from March 1994–December 2005. Prof. Joshi is in expert panel member of various national committees, including AICTE, DRDO, and MIT. He has vast teaching experience exceeding 38 years at the graduate and postgraduate levels at IIT Roorkee. He has guided more than 25 PhD theses, 150 M.E./M. Tech dissertations, and 200 B.E./B.Tech projects. Prof. Joshi has published more than 250 research papers in national/international journals/conferences and presented many in Europe, the United States, and Australia. He has been awarded Gold Medal by Institute of Engineers for best paper. He has chaired many national and international conferences and workshops. Currently, he is actively involved in research in the field of database management system, data mining, bioinformatics, information security, reconfigurable systems, and mobile computing.

Manoj Misra received a bachelor's degree in Electrical Engineering in 1983 from HBTI Kanpur, India. He received his master's and PhD degrees in Computer Engineering in 1986 and 1997 from University of Roorkee, India, and Newcastle upon Tyne, UK, respectively. He is currently a Professor at Indian Institute of Technology Roorkee. He has guided several PhD theses, M.E./M.Tech. Dissertations, and completed various projects. His areas of interest include mobile computing, distributed computing, and performance evaluation.