ISSN: 2321-7782 (Online)
Volume 2, Issue 4, April 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Paper / Case Study
Available online at: www.ijarcsms.com

Distributed Denial of Service Attacks and Their Suggested Defense Remedial Approaches

Darshan Lal Meena[1]
(Ph.D. Research Scholar), Department of Computer Science
MP, Bhoj Open University, Bhopal (MP) – 462016
Research Centre: MITS, Gwalior (MP) – 474005
India

Dr. R. S. Jadon[2]
Professor & HOD
Department of Computer Application
MITS, Gwalior (MP)-474005
India

Abstract: Distributed denial-of-service (DDoS) is a rapidly growing problem. The multitude and variety of both the attacks and the defense approaches is overwhelming. This paper is a survey on the problem of denial-of-service (DoS) and Distributed Denial of Service (DDoS) attacks and proposed ways to deal with it. We describe the nature of the problem and look for its root causes, further presenting brief insights and suggested approaches for defending against DDoS. We point out both the positive and negative sides of each potential solution. Future work identifies and justifies open research issues. In conclusion we give a brief summary of what has realistically been achieved so far, as well as what the key missing components still. In this paper, we present a classification of available mechanisms that are proposed in literature on preventing Internet services from possible DDoS attacks and discuss the strengths and weaknesses of each mechanism. This provides better understanding of the problem and enables a security administrator to effectively equip his arsenal with proper prevention mechanisms for fighting against DDoS threat.

Keywords: DoS, DDoS, SYN, CERT, Prevention, Zombie.

I. INTRODUCTION

As organizations continue to incorporate the Internet as a key component of their operations, the global cyber-threat level is increasing. One of the most common types of cyber-threats to these environments is known as a **Denial of Service (DoS**) attack – an attack preventing users from accessing a system for a period of time. Recent DoS attacks have left large corporate and government web sites inaccessible to customers, partners and users for hours or days, resulting in significant financial, reputational, and other losses.

A recent Akamai ‘s Prolexic Quarterly Global DDoS Attack Report Quarter 1 of 2014 came if we compared to the same quarter one year ago,the total number of DDoS attack increased 47% shown in Fig 1.1. Prolexic has introduced a new metric to the DDoS attack report to provide insight the industries targeted by malicious actors in DDoS campaigns. Media and Entertainment took the brunt of DDoS attacks, accounting for 50% of the attack target in first quarter of 2014.Software and technology was the second most often hit at 17%.Security accounted for 12% of attacks. Finance was targeted 9% of the time.Gaming was the last of the top five industry targets with 7% of all observed attacks shown in Fig. 1.2[1]

Prolexic Quarterly Global DDoS Attack Report Quarter 1 of 2014 Compared to Q4 of 2013 then find 18% increase in total DDoS attacks. 39% increase in average attacks bandwidth. 35% increase in infrastructure (Layer 3&4) attacks. 36% decrease in application (Layer 7) attacks. 24% decrease in average attacks duration: 23 vs 17 hours.114% increase in average peak bandwaidth.

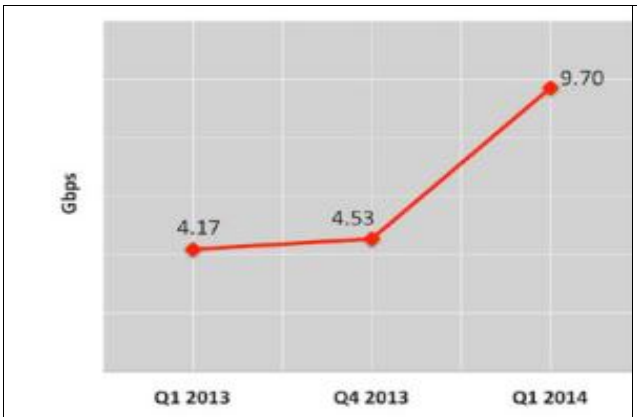


Fig 1.1 Peak bandwidth average(Q1 2014,Q4 2013,Q1 2013)

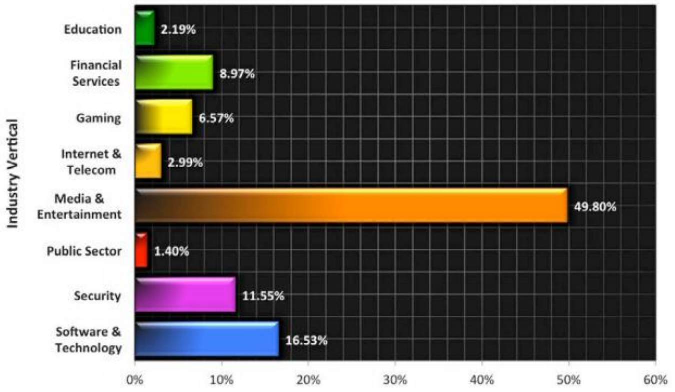


Fig:1.2Distribution of attack targeting key industries

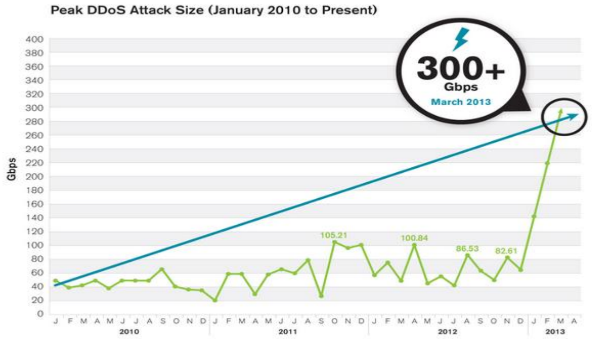


Fig:1.3 Peek DDoS Attack Size Graph as on 2013

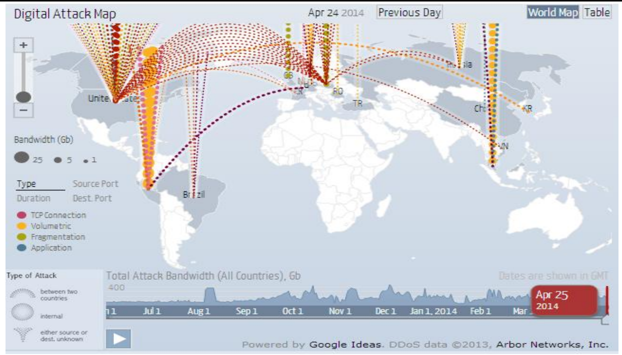


Fig: 1.4 Digital Attack Map as on 24 April 2014

While there have been extensive studies into the details of the former two, until recently denial of service had been disregarded from being a serious threat and had seldom been the focus of attention. Since the number of successive attacks on major commercial Internet sites in February 2000 [2], this topic has been gaining popularity in the research, commercial and even political circles.

A denial of service attack on a network could take one of three possible forms. A malicious party (a.k.a. the attacker) could cause the network not to transmit messages it should be sending in order to offer service to a subset or all of its clients. On the other end of the spectrum, the network could be caused to send messages, which it should not be sending. By far the most common form of DoS in today’s networks is causing excessive bogus traffic (a.k.a. flooding the network) in the direction of a particular server, which in the end will prevent legitimate users from getting the service they could otherwise be receiving from that server.

A simple example of denial of service attack is the popular SYN attack on the TCP protocol. A client sends a request (SYN) to a server announcing its intention to start a conversation. The server responds with an acknowledgement (SYN ACK), accepting the establishment of a connection to the client and simultaneously reserving an entry for the pending connection in its connection queue. Now it is the client’s turn to acknowledge the start of the communication by sending its (SYN ACK ACK) packet. A malicious client may never do that, as a result the server ends up with its connection queue entry tied up (and unused) for a significant amount of time (at least as long as the timeout), before it can be released. If one imagines the above scenario repeating over multiple (almost) simultaneous client requests, it is easy to see how the server could be tricked into initiating bogus “communication“with one of more malicious client(s). Since the maximum processing power of a typical 100 MIPS class server is on the order of 1000 to 2000 connections per second [3] and the minimum standard server TCP connection queue is 2048 slots [4], it becomes clear that overwhelming even a powerful server is within the capabilities of even a very small number of conspiring malicious clients. (Here we should note that a very similar in spirit attack could be mounted against SSL, in the latter case the server’s limited computational rather than memory resources can be most successfully exploited.).

The above patterns are far from contrived, being instead existing weaknesses. An even more credible testimony to the seriousness of the threats these can pose are the real attacks having occurred in the Internet, reported in advisories by the Computer Emergency Response Team (CERT) over the past few years. One study has shown that the number of such attacks has been steadily growing by 50% per year over the past decade [5].

According to ARBOR DDoS & Security Report[6], Arbor's ninth Annual Worldwide Infrastructure Security Report (WISR), released last month, the size of attacks in 2013 eclipsed previous peaks by over 200 percent, with the largest reported attack at 309 Gbps, and with multiple respondents reporting attacks larger than 100 Gbps – the previous largest reported attack size describe in Fig 1.3 and Google ideas has teamed up with Arbor Network to bring the data to life then Digital Attack Map is a live data visualization of Distributed Denial of Service (DDoS) attaks taking place around the globe, built using the anonymous information supplied by Arbor Networks' ATLAS global threat monitoring System describe in Fig 1.4.

According to Arbor network report more than 2,000 DDoS attacks are mounted every single day, with one third of all downtime incidents attributable to DDoS attacks.

This all should serve as a motivation for tackling denial of service attacks the best we can without future delay. In the next section we look into the details of the problem and search for the root causes for it. In this paper Section 2 describe DoS and DDOs attack Overview and Section 3 cover deeper of the attcks problem and in section 4 including Suggested General Remedial Approaches and digest of proposed approaches for eliminating, mitigating or following up on attacks. Finally, in section 5 describing CLASSIFICATIONS OF DDOS PREVENTION MECHANISMS and we briefly identify directions where future work is needed and conclude by summarizing in Section 6 that what the state of- the-art in the research on denial of service attacks is and what still remains on our wish list. Finally in this research paper can be used by researchers to answer many important questions related to DDoS attack and their Novel solutions.

II. DOS AND DDOS ATTACK OVERVIEW

Denial of service attack is a form of cybercrime in which attackers overload computing or network resources with so much traffic that legitimate users are unable to gain access to those resources. Attacks are called " Distributed"(DDoS) because in most case the attack traffic originates from multiple hosts. Any computing service which is accessible via the internet is potentially subject to DDoS."Distributed Denial Of service(DDos) Attacks are attacks on availability " Says **Rakesh Shah,Arbor Networks Director** of product marketing and strategy."The goal of the attacker is to disrupt or shut down an organization's business critical services such as ecommerce transactions, financial trading, email or web site access. By overwhelming network infrastructure, servers or applications with excessive communications requests, an attack means services are unavailable to legitimate users."

A Distributed Denial of Service attack is commonly characterized as an event in which a legitimate user or organization is deprived of certain services, like web, email or network connectivity, that they would normally expect to have. DDoS is basically a resource overloading problem. The resource can be bandwidth, memory, CPU cycles, file descriptors, buffers etc. The attackers bombard scare resource either by flood of packets or a single logic packet which can activate a series of processes to exhaust the limited resource [**7**]. In the Fig. 2.1 simplified Distributed DoS attack scenario is illustrated. The figure shows that attacker uses three zombie's to generate high volume of malicious traffic to flood the victim over the Internet thus rendering legitimate user unable to access the service. Recent DDoS attacks have exploited vulnerabilities in web-hosting companies and other large data centers to launch DDoS attacks on computer systems and websites describe in fig 2.2

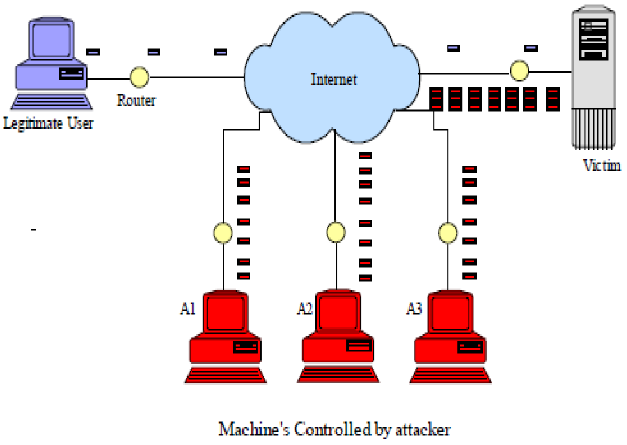


Fig:2.1 Illustration of the DDoS attack scenario

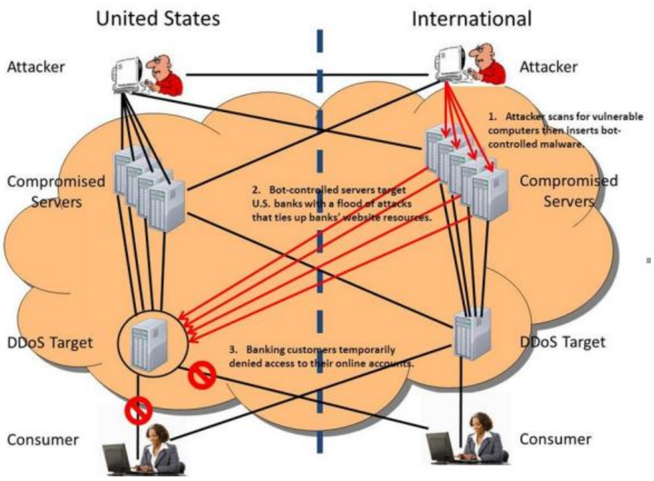

United States
International
Attacker
Attacker
1. Attacker scans for vulnerable computers then inserts bot-controlled malware.
Compromised Servers
Compromised Servers
2. Bot-controlled servers target U.S. banks with a flood of attacks that ties up banks' website resources.
DDoS Target
DDoS Target
3. Banking customers temporarily denied access to their online accounts.
Consumer
Consumer

Fig:2.2An Illustrative Example of DDoS Attack

Extremely sophisticated, user friendly, automated and powerful DDoS toolkits are available for attacking any victim, so expertise is not necessarily required that attract naive users to perform DDoS attacks. Although DoS attacking strategies differ in time, studies show that attackers mainly target the following resources to cause damage on victim [8, 9].

2.1 What makes DDoS attacks possible? Current Inter- net design focuses on effectiveness in moving packets from the source to the destination. This design follows the *end-to- end paradigm*: the intermediate network provides the bare minimum, best-effort packet forwarding service, leaving to the sender and the receiver the deployment of advanced protocols to achieve desired service guarantees such as quality of service, reliable and robust transport or security. The end-to-end paradigm pushes the complexity to end hosts, leaving the intermediate network simple and optimized for packet forwarding. There is one unfortunate implication. If one party in two-way communication (sender or receiver) misbehaves, it can do arbitrary damage to its peer. No one in the intermediate network will step in and stop it, because Internet is not designed to police traffic. One consequence of this policy is the presence of IP spoofing [1]. Another are DDoS attacks. The Internet design raises several security issues concerning opportunities for DDoS attacks.

- ***Internet security is highly interdependent***. DDoS attacks are commonly launched from systems that are subverted through security-related compromises. Regardless of how well secured the victim system may be, its susceptibility to DDoS attacks depends on the state of security in the rest of the global Internet [10].
- ***Internet resources are limited***. Each Internet entity (host, network, service) has limited resources that can be consumed by too many users.
- ***Intelligence and resources are not collocated.*** An end-to-end communication paradigm led to storing most of the intelligence needed for service guarantees with end hosts, limiting the amount of processing in the intermediate network so that packets could be forwarded quickly and at minimal cost. At the same time, a desire for large throughput led to the design of high bandwidth pathways in the intermediate network, while the end networks invested in only as much bandwidth as they thought they might need. Thus, malicious clients can misuse the abundant resources of the unwitting intermediate network for delivery of numerous messages to a less provisioned victim.
- ***Accountability is not enforced***. IP spoofing gives attackers a powerful mechanism to escape accountability for their actions, and sometimes even the means to perpetrate attacks (reflector attacks[2] [11], such as the Smurf attack [12]).
- ***Control is distributed***. Internet management is distributed, and each network is run according to local policies defined by its owners. The implications of this are many. There is no way to enforce global deployment of a particular security

mechanism or security policy, and due to privacy concerns, it is often impossible to investigate cross-network traffic behavior.

2.2 How are DDoS attacks performed? A DDoS attack is carried out in several phases. The attacker first *recruits* multiple agent machines. This process is usually performed automatically through scanning of remote machines, looking for security holes that will enable subversion. The discovered vulnerability is then *exploited* to break into recruited machines and *infect* them with the attack code. The exploit/infect phase is frequently automated, and the infected machines can be used for further recruitment of new agents. Another recruit/exploit/infect strategy consists of distributing attack software under disguise of a useful application (these software copies are called Trojans). This distribution can be performed, for instance, by sending E-mail messages with infected attachments. Subverted agent machines are *used* to send the attack packets. Attackers often hide the identity of subverted machines during the attack through spoofing of the source address field in attack packets.

Note: [1] putting a fake source address in a packet's header to hide the sender's identity.

[2]During reflector attacks, the attacker fakes the source address of the victim in legitimate service requests directed at several servers, e.g., DNS requests. The servers then reply to the victim, overwhelming it. However, that spoofing is not always required for a successful DDoS attack. With the exception of reflector attacks [11], all other attack types use spoofing only to hinder attack detection and characterization, and the discovery of agent machines.

2.3 Why do people perpetrate DDoS attacks? The main goal is to inflict damage on the victim. Frequently the ulterior motives are personal reasons (a significant number of DDoS attacks are perpetrated against home computers,

Presumably for purposes of revenge), or prestige (successful attacks on popular Web servers gain the respect of the hacker community). However, some DDoS attacks are per- formed for material gain (damaging a competitor's resources or blackmailing companies) or for political reasons (a country at war could perpetrate attacks against its enemy's critical resources, potentially enlisting a significant portion of the entire country's computing power for this action). In some cases, the true victim of the attack might not be the actual target of the attack packets, but others who rely on the target's correct operation.

III. Deeper into the Problem

3.1 Culprits

One obvious problem in the TCP SYN attack scenario is that all the preliminary communication takes place *before authentication*, so the server cannot tell a legitimate request from a fake one. There is nothing much that can be done about this, since trying to put authentication from the very start would be a denial of service attack in its own right, since the server would be preoccupied verifying (digital) signatures. Regardless of whether the signatures are fake or not, the very action of doing the computationally intensive verification would use up all spare computational resources of the server. A less obvious cause of denial of service as a phenomenon lies in the *lack of accounting* for the resources consumed by each client [13]. Spats check and Peterson argue that there are three key ingredients for protecting against attacks of that kind:

- ***Accounting*** for all consumed resources per client;
- ***Detection*** when the resources consumed by any given client exceed some limit;
- ***Containment*** – the ability to reclaim the tied resources after detecting an attack by dedicating minimum additional server. Resources to the task and thus avoiding falling for a follow-up denial of service attack.

3.2. Types of attacks or DDoS attack classification:

In terms of the number of malicious entities involved in an attack, we distinguish:

- ***Uni-source attacks*** – launched by and originating from a single source;

- ***Distributed attacks*** – originating from multiple coordinated sources, though not necessarily involving more than one malicious end user. Architecture of DDoS depict in Figure 3..1.There are two main classes of DDoS attacks **(Figure 3.2.):** (i) Bandwidth depletion and (ii)Resource depletion attacks.

3.2.1 Bandwidth depletion attack is designed to flood the victim network with unwanted traffic that prevents legitimate traffic from reaching the victim system. Bandwidth attacks can be divided to(i)**Flood attack** (ii) **Reflect attack**

3.2.1.1Flood Attack In a direct attack, zombies flood the victim system directly with IP traffic. The large amount of traffic saturates the victim's network bandwidth so that other legitimate users are not able to access the service or experience severe slow down. Normally in those attacks, the following packets are used.

-TCP floods A stream of TCP packets with various flags set are sent to the victim IP address. The SYN, ACK, and RST flags are commonly used

-ICMP echo request/reply (e.g., ping floods) A stream of ICMP packets are sent to a victim IP address.

-UDP floods: A stream of UDP packets are sent to the victim IP address.

3.2.1.2 Reflected Attack or Amplification: A reflected denial of service attack involves sending forged requests of some type to a very large number of computers that will reply to the requests. Using Internet protocol spoofing, the source address is set to that of the targeted victim, which means all the replies will go to (and flood) the target. ICMP Echo Request attacks can be considered one form of reflected attack, as the flooding host(s) send Echo Requests to the broadcast addresses of mis-configured networks, thereby enticing a large number of hosts to send Echo Reply packets to the victim

3.2.2. Resource depletion Attacks:

3.2.2.1 TCP SYN Attack :The TCP SYN attack exploits the three-way handshake between the sender and receiver by sending large amount of TCP SYN requests with spoofed source address. If those half-open connection binds resources on the server or the server software is licensed per-connection, all these resources might be taken up.

3..2.2.2 Malformed Packet Attack a ping of death (abbreviated "POD") is a type of attack on a computer that involves sending a malformed or otherwise malicious ping to a computer. A ping is normally 64 bytes in size; many computer systems cannot handle a ping larger than the maximum IP packet size which is 65,535 bytes. Sending a ping of this size often crashes the target computer

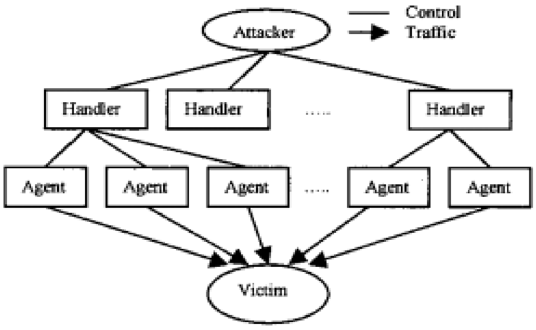


Figure 3.1- Architecture of DDoS attack

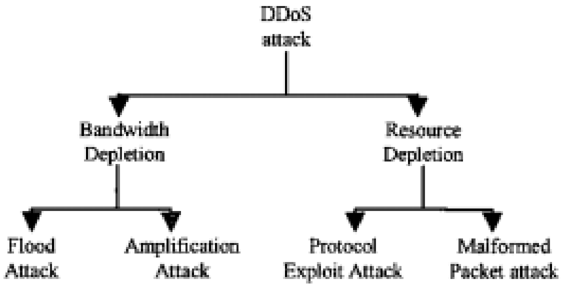


Figure:3.2. - DDoS attack classification

Denial of service broadly can be divided into three forms:

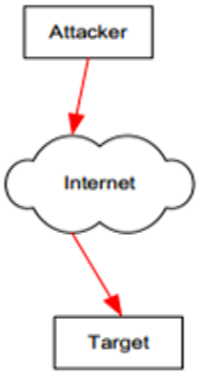


Fig-3.3 DoS Attacks

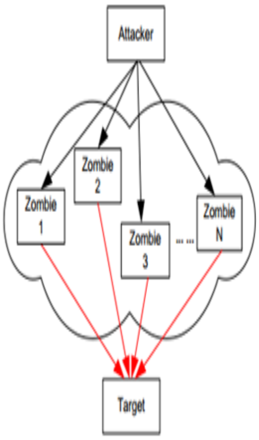


Fig :3.4 DDoS Attacks

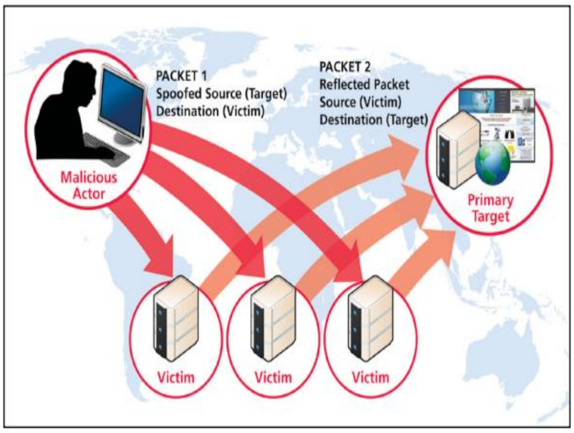


Fig-3.5 DRDoS Attacks

3.2.1 DoS Attacks: DoS attacks (refer to Figure 3.3), a large number of malicious packets are sent from a single machine, with the aim of exhausting the target's computational and networking resources, or crashing the target. The purpose of such attacks is to deprive legitimate users of access to the target's services**.** In a DoS attack, one computer and one internet connection is used to flood a server with packets, with the aim of overloading the targeted server's bandwidth and resources[**14**].

3.2.2 DDoS attack: A distributed denial of service attack (DDoS) (refer to fig 3.4) occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. This is the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic. When a server is overloaded with connections, new connections can no longer be accepted [**15**]. Distributed DoS attacks operate on a much broader scale (with practically limitless number of launch sites) and can considerably add to the severity, length and scale of an attack, making it possible to practically disable even very powerful servers over prolonged periods of time. Such was the case with the servers of large commercial sites like Yahoo!, eBay.com, etc. in early February 2000. Since then, distributed attacks have turned from a theoretical possibility to a major concern for Internet servers of any size and computing power

3.2.3 DR-DoS attacks : distributed reflector denial of service (DRDoS) **(refer to** Figure 3.5) Illustrates another type of bandwidth attack called a **distributed reflector denial of service** (DRDoS) attack, which aims to obscure the sources of attack traffic by using third parties (routers or web servers) to relay attack traffic to the victim. These innocent third parties are also called the reflectors. Any machine that replies to an incoming packet can become a potential reflector.

3.3 IP "spoofing": When an attack is detected and hopefully recorded, the next thing the victim wants to do is to find out who

the originator was. This turns out to be a really hard problem in the Internet. Much like in the case with Alice calling from a public payphone thereby not leaving a trace of who she was, it is possible (and easy) to disguise your identity in today's Internet. Ironically, it is the senders who put in their source address in an IP packet, so a malicious client could choose to stick any IP address in (a technique known as "*spoofing*") and pretend to be sending from somewhere else. To make matters even worse, in the case of a distributed attack the zombie sources are many and their addresses likely to be spoofed. In order to get the real attacker, three additional important steps are necessary, all of which need to be satisfactorily resolved and none of which (to date) have an engineered and deployed solution:

- ➢ ***Tracing back to the sources*** **(zombies)**. Savage et al. [16] have proposed a scheme for doing this which we will briefly discuss in the next section. It needs to be recognized that zombies are unlikely to be reused by an attacker – it would be too risky for her and there are sufficiently many ill-secured zombie-to-be candidate end hosts out there. Hence, relying on correlating recorded traces from many different attacks may prove to be an all-too-optimistic expectation;

- ***Tracing back to the original source* of an attack**. Finding out where the seeds were initially planted is another challenge. This can be achieved by examining the logs of the corresponding ISPs. A drawback of that approach is that it is bound to take much human effort and is therefore unlikely to be a viable solution, except for only a few critical cases of attacks against victim customers willing to invest in pursuing the attacker. In addition, innocent launch-pad end users may be unwilling to cooperate and be monitored, especially over the course of a longer period of time;
- **T*racking down the attacker* herself**. This last step involves not so much technical challenges, but rather successful coordination of efforts between ISPs, telecommunication companies and law enforcement agencies. In [17] Needham points out that in all security matters there are two objectives – to make violations difficult and to make them known to authority when they happen. With the case of denial of service, meeting the first objective is somewhat limited (at least based on the current state of the art), so in the meantime it is essential to be effective in meeting the second objective..

3.4 DDoS DEFENSE CHALLENGES: Launching DDoS attacks on the victim machine is only a matter of few keystrokes for the attacker. With the present technology, many challenges are involved in designing and implementing an effective DDoS defense mechanism. Some of them are as follows[32]

(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.

3.5 Five Principal for DDos defense to build an effective solution: following five principles [33] are recommended by robinson et al. in order to build an effective solution.

- First: 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
- Second:, High Normal Packet Survival Ratio (NPSR) hence less collateral damage is the prime requirement for a DDoS defense
- Third, 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.
- Fourth, as there is no centralized control for autonomous systems (AS) in Internet, a partially and incrementally deployable defense model which does not need centralized control will be successful
- Fifth, a defense system must take into account future compatibility issues such as interfacing with other systems and negotiating different defense policies

3.6 Significance: Finally, let us consider the importance of coping with denial of service as a security phenomenon. Denial of service attacks could disable servers for potentially long periods of time. During that time between the onset of such an attack and the time when the breach is actually detected and recovered from, the victim server is unable to handle any requests by legitimate non-malicious users. For large commercial servers this translates to a significant loss of income, and which they consider even more serious – a loss of reputation. To be concrete, one report estimated the total loss due to the distributed attacks we mentioned in the range of $1 billion it equals to 100 crores in Indian currency.

There is also another important dimension for assessing the damage from such attacks. Although denial of service itself does not directly affect data residing on the server under attack, there is no reason not to anticipate it being used as a first step to another follow-up attack, which actually does steal, alter or somehow manipulate that data. And the data could be mission- or life-critical in some occasions. This kind of chained attack can realistically happen if the protocol the server executes is not fail-stop (or at least fail safe) [18]. In a little more detail, a protocol is considered fail-stop if it automatically halts in response to any active attack that interferes with the protocol execution. The notions of fail-stop and fail-safe protocols are quite useful for formal verification of certain properties of security protocols, as discussed at length by Gong and Syverson. For instance, Bro [19] is an intrusion detection system in use, which is fail-open (due to the need to operate in real-time). Under normal traffic conditions the system looks at packets (headers) and decides which ones to let within a designated administrative boundary it serves to protect.

However, if Bro becomes overloaded, it simply lets packets through while trying to catch up on processing a queue of outstanding ones. This can be used by skillful attackers to penetrate into the domain and do further (more serious) damage there.

IV. Suggested General Remedial approaches

Naturally, as with every kind of security breach, there are three general approaches for dealing with the attack – eliminating it completely, mitigating the effects of the attack on the victim, and discouraging the attacker. Those do not have to be exclusive to one another, but can and should be used as complementary, whenever possible. We will look at each strategy separately in more detail, considering the variety of solutions proposed in literature and pointing out what we think are the strong and weak sides of each.

4.1 Eliminating the possibility of attack:

This is by far the most desirable strategy for "defending" against any kind of security attack. Unfortunately, the problems are rather complicated and very seldom can a threat be completely eliminated. More often that not, this would be the case with scams, which really only have transient effects.

4.1.1Allowing connections *only* to trusted clients. This is clearly the most conservative approach to communication and as such it has the highest degree of averting security threats. Such a solution is justifiable for deployment only in closed and special-purpose (e.g. military) environments. It is inherently inapplicable and incompatible to an open communication system such as the Internet. A known problem with closed environments is that outside intrusions are both not expected and commonly not anticipated. So, the level of preparedness for a security breach, should it ever occur, is very low and the damage grows proportionally high.

4.1.2Out-of-band signaling. This is not a novel idea, especially in the phone network field. The idea is that control and data signals would travel physically on separate wires and thus any interference and possible confusion is excluded. This was not the case with the phone networks in 1960s, when in-band signaling was in use. One could whistle into the phone receiver and under certain favorable circumstances (the right wavelength and amplitude) the signal, which really was just data, could be interpreted as a control signal (e.g. a free call, etc.). Schneier claims that out-of-band signaling would not only alleviate the existing problems with denial of service attacks, but also aid in defeating other inherent known security problems in the Internet

4.2. Mitigating the effect of the attack on the victim:

While the utmost goal is to avoid being attacked, when and if this happens it is highly desirable to be able to sustain some level of (degraded) performance during the high load, even prior to the actual detection of an attack. The following approaches try to achieve this goal in different ways

4.2.1. Securing all computers on a network: Achieving that would render the existence of zombies impossible and hence an attacker would be reduced to being able to mount only a uni-source attack. In addition, IP trace back schemes would directly lead to the attacker's weapon machine, which in turn would both reduce the management overhead in the post-mortem tracing process and serve as a disincentive for the attacker to start in the first place.

4.2.2. Ingress filtering. This approach is describe details in next section targeted at reducing or completely eliminating the ability to forge source addresses, which if accomplished would ultimately result in much easier tracing back to the true source of an attack and as such would serve as a significant deterrent for attackers..

4.2.3 Client "puzzles" prior to committing resources. The idea, recently proposed by two RSA researchers, is to distribute cryptographic puzzles to clients (whether genuine of fake) when the server comes under pressure from high load [20]. Resources are only committed to connections, for which the clients have successfully solved and submitted their puzzles within a timeout period. This strategy would serve two purposes: damping (i.e. spacing) the client requests and allowing the server to control the number of clients establishing connections with it by sending out harder puzzles (depending on the load conditions and actual number of resource slots available), and thus experiencing *graceful degradation* in performance. A good feature to note is that client puzzles are resistant against IP spoofing..

The main disadvantage of client puzzles, admitted by the authors themselves is the requirement for special client-side software (either built into the browser or distributed in some different way). Another drawback, remarked by Schneider [21] is that client puzzles although reasonable as an approach for dealing with uni-source attacks, fall to distributed denial of service attacks, since generation and distribution of client puzzles is a denial of service attack in its own right. Overall, it seems that the approach is viable, but should only be used with caution and in combination with other such promising approaches

4.2.4 Use progressively stronger authentication: The idea here is to again avoid committing server resources early, trying to instead incrementally gain confidence in the identity of the client and only "promising" resources, proportionate to the level of assurance the server has at any one point during the communication . Starting with weak authentication first (e.g. a cookie) and upon receiving positive feedback (i.e. client responding and following the requested steps), the server progressively chooses stronger authentication up to the point of doing an expensive authentication (e.g. digital signature), at which point the real conversation may start. Note that "strong authentication from the start would be a hook for denial of service attacks". This approach in itself does not prevent malicious parties from launching attacks, but it significantly raises the bar for doing that, making the attackers work harder by first having to dispose of the weaker authentication.

Unlike the approaches for completely eliminating the threat of attacks, the ones for actually dealing with it are in our opinion quite reasonable and realistic, albeit none of them offers a complete set of strategy on how to mitigate denial of service attacks.

Other such possible approaches are discussed and compared in [22].

4.3 Discouraging the attacker: The strategies discussed in this subsection should not be observed as separate from the rest in this and other papers. They are merely meant to augment existing other techniques for mitigating denial of service attacks. Only with the joint effort on all fronts can such a massive breach be ultimately defeated.

4.3.1 IP traceback by coordinating between ISPs. Coordination between ISPs is a feature that is highly desirable for tracking down security problems of all kinds. If accomplished, it could significantly raise the bar, forcing attackers to be even more inventive and resourceful (e.g. forcing them to break into and take over other zombie end hosts). However it is one of the hardest things to manage and in addition requires that (most of) the ISPs keep accurate logs and willingness to share them among each other in order to effectively coordinate a traceback. It seems that this could only be achieved if the ISPs themselves have some incentive in participating in such a joint effort. One such thing could be a form of administrative control and mandating them to cooperate, much like governments cooperate in cracking down on international crime. An even more convincing incentive would be to keep them off the list of ISPs, recommended to avoid for being insecure and careless. Another drawback of the general approach (other than there being no management inter-ISP infrastructure) is that if a tool for cracking passwords is made publicly available (and this could happen) then the effect of raising the bar for attackers would be nullified.

4.3.2 IP traceback by probabilistically marking packets: This last approach is allegedly the most promising direction for discouraging attackers. It is both robust (using randomizing), incrementally deployable and backwards compatible [22]. The method is resistant against IP spoofing and against distributed denial of service attacks. The key idea is to probabilistically mark packets at routers (over which the attackers obviously can have no control) with partial path information, which packets will carry. The entire path could be reconstructed post-mortem at the victim server.

V. Classification of DDOS attacks Prevention mechanisms

Attack prevention methods try to stop all well known signature based and broadcast based DDoS attacks from being launched in the first place or edge routers, keeps 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 there are always vulnerable to novel and mixed attack types for which signatures and patches are not exist in the database.

Techniques for preventing against DDoS can be broadly divided into two categories: (i) General techniques, which are some common preventive measures [23] i.e. system protection, replication of resources etc. that individual servers and ISPs should follow so they do not become part of DDoS attack process. (ii) Filtering techniques, which include ingress filtering, egress filtering, router based packet filtering, history based IP filtering, SAVE protocol etc.

5.1 General Techniques:

5.1.1 Disabling **unused services**: The less there are applications and open ports in hosts, the less there are chance to exploit vulnerabilities by attackers. Therefore, if network services are not needed or unused, the services should be disabled to prevent attacks, e.g. UDP echo, character generation services [23].

5.1.2 **Install latest security patches** today, many DDoS attacks exploit vulnerabilities in target system. So removing known security holes by installing all relevant latest security patches prevents re-exploitation of vulnerabilities in the target system [23].

5.1.3 Global defense infrastructure: A global deployable defense infrastructure can prevent from 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 [23].

5.1.4 IP hopping DDoS attacks can be prevented by changing location or IP address of the active server proactively within a pool of homogeneous servers or with a pre-specified set of IP address ranges [23]. The victim computer’s IP address is invalidated by changing it with a new one. Once the IP addresses change is completed all internet routers will be informed and edge routers will drop the attacking packets. Although this action leaves the computer vulnerable because the attacker can launch the attack at the new IP address, this option is practical for DDoS attacks that are based on IP addresses. On the other hand, attackers can make this technique useless by adding a domain name service tracing function to the DDoS attack tools.

5.1.5 Disabling IP broadcast

Defense against attacks that use intermediate broadcasting nodes e.g. ICMP flood attacks, Smurf attacks etc. will be successful only if host computers and all the neighboring networks disable IP broadcast [24].

5.1.6 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. But some complex attack e.g. 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

5.2 *Filtering Techniques:*

5.2.1 **Ingress/Egress filtering:** Ingress Filtering, proposed by Ferguson et al. [25], is a restrictive mechanism to drop traffic with IP addresses that do not match a domain prefix connected to the ingress router. Egress filtering is an outbound filter, which ensures that only assigned or allocated IP address space leaves the network. A key requirement for ingress or egress filtering is knowledge of the expected IP addresses at a particular port. For some networks with complicated topologies, it is not easy to obtain this knowledge. One technique known as reverse path filtering [26] can help to build this knowledge. This technique works as follows. Generally, a router always knows which networks are reachable via any of its interfaces. By looking up source addresses of the incoming traffic, it is possible to check whether the return path to that address would flow out the same interface as the packet arrived upon. If they do, these packets are allowed. Otherwise, they are dropped.

Unfortunately, this technique cannot operate effectively in real networks where asymmetric Internet routes are not uncommon. More importantly, both ingress and egress filtering can be applied not only to IP addresses, but also protocol type, port number, or any other criteria of importance. Both ingress and egress filtering provide some opportunities to throttle the attack power of DoS attacks. However, it is difficult to deploy ingress/egress filtering universally. If the attacker carefully chooses a network without ingress/egress filtering to launch a spoofed DoS attack, the attack can go undetected. Moreover, if an attack spoofs IP addresses from within the subnet, the attack can go undetected as well. Nowadays DDoS attacks do not need to use source address spoofing to be effective. By exploiting a large number of compromised hosts, attackers do not need to use spoofing to take advantage of protocol vulnerabilities or to hide their locations. For example, each legitimate HTTP Web page request from 10,000 compromised hosts can bypass any ingress/egress filtering, but in combination they can constitute a powerful attack. Hence, ingress and egress filtering are ineffective to stop DDoS attacks.

5.2.2Router based packet filtering: Route based filtering, proposed by Park and Lee [27], extends ingress filtering and uses the route information to filter out spoofed IP packets. It is based on the principle that for each link in the core of the Internet, there is only a limited set of source addresses from which traffic on the link could have originated.

5.2.3 History based IP filtering: Generally, the set of source IP addresses that is seen during normal operation tends to remain stable. In contrast, during DoS attacks, most of the source IP addresses have not been seen before. Peng et al. relies on the above idea and use IP address database (IAD) to keep frequent source IP addresses. During an attack, if the source address of a packet is not in IAD, the packet is dropped. Hash based/Bloom filter techniques are used for fast searching of IP in IAD. History based packet filtering scheme is ineffective when the attacks come from real IP addresses. In addition, it requires an offline database to keep track of IP addresses. Therefore, Cost of storage and information sharing is very high.

5.2.4 Capability based method: Capability based mechanisms provides destination a way to control the traffic directed towards itself. In this approach, source first sends request packets to its destination. Router marks (pre-capabilities) are added to request packet while passing through the router. The destination may or may not grant permission to the source to send. If permission is granted then destination returns the capabilities, if not then it does not supply the capabilities in the returned packet. The data packets carrying the capabilities are then send to the destination via router. The main advantage achieved in this architecture is that the destination can now control the traffic according to its own policy, thereby reducing the chances of DDoS attack, as packets without capabilities are treated as legacy and might get dropped at the router when congestion happens [28]

However, these systems offer strong protection for established network flows, but responsible to generate a new attack type known as DOC (Denial of Capability), which prevents new capability-setup packets from reaching the destination, limits the value of these systems. In addition these systems have high computational complexity and space requirement.

5.2.5 Secure overlay Service (SOS) : Secure Overlay Service proposed by Keromytis et al. [29] defines an architecture called secure overlay service (SOS) to secure the communication between the confirmed users and the victim. All the traffic from a source point is verified by a secure overlay access point (SOAP). Authenticated traffic will be routed to a special overlay node called a beacon in an anonymous manner by consistent hash mapping. The beacon then forwards traffic to another special overlay node called a secret servlet for further authentication, and the secret servlet forwards verified traffic to the victim. The identity of the secret servlet is revealed to the beacon via a secure protocol, and remains a secret to the attacker. Finally, only traffic forwarded by the secret servlet chosen by the victim can pass its perimetric routers. Secure Overlay Service (SOS) addresses the problem of how to guarantee the communication between legitimate users and a victim during DoS attacks. SOS can greatly reduce the likelihood of a successful attack. The power of SOS is based on the number and distribution level of SOAPs

5.2.6 SAVE: Source Address Validity Enforcement: Li et al. [30] have proposed a new protocol called the Source Address Validity Enforcement (SAVE) protocol, which enables routers to update the information of expected source IP addresses on each link and block any IP packet with an unexpected source IP address. The aim of the SAVE protocol is to provide routers with information about the range of source IP addresses that should be expected at each interface. Similarly to the existing routing protocols, SAVE constantly propagates messages containing valid source address information from the source location to all destinations. Hence, each router along the way is able to build an incoming table that associates each link of the router with a set of valid source address blocks. SAVE is a protocol that enables the router to filter packets with spoofed source addresses using incoming tables. It overcomes the asymmetries of Internet routing by updating the incoming tables on each router periodically. However, SAVE needs to change the routing protocol, which will take a long time to accomplish. If SAVE is not universally deployed, attackers can always spoof the IP addresses within networks that do not implement SAVE. Moreover, even if SAVE were universally deployed, attackers could still launch DDoS attacks using non spoofed source addresses. Table I summarizes filtering techniques for DDoS attacks prevention. 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 [31], the percentage of spoofed attacks is declining. Only four 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 in near future. To add on, there exists no way out to enforce global deployment of a particular security mechanism. Therefore, relying on attack prevention schemes is not enough to stop DDoS attacks

Table I Summary of filtering techniques for DDoS attacks prevention

Filtering Technique	Benefits	Limitations
Ingress/ Egress	Prevents IP Spoofing	-Need global development - Attacks with real IP addresses can not be prevented
RPF (Route based Packet Filtering)	Work well with static routing	-Problem when dynamic routing is used -Need wide implementation to be effective
History based	Does not require cooperation of whole Internet Community Gives priority to the frequent packets in case of congestion or attack	-Ineffective when the attacks come from real IP addresses Requires an offline database to keep track of IP addresses -Depend on information collected
Capability based	Provides destination a way to control the traffic it desires Incremental deployment	-Attacks against the request packets can not prevented (e.g. ROC attack) -High computational complexity and space requirement
SOS	Works well for communication of predefined source nodes	-Solution has limited scope e.g. not applicable to web servers -Require introduction of a new routing protocol that itself another security issue
SAVE	-Filtering improperly addressed packets is worthwhile incremental deployment	-During the transient period valid packets can be dropped

VI. Conclusion and Future Scope

Complete elimination of denial of service threats is infeasible given the current Internet infrastructure. Internet, being an open environment with no limits set in stone on the number of users, is inherently vulnerable to attacks of the denial of service type. There is no way to predict the parameters of the largest possible flood. In the phone network the infrastructure is set and it is known what the provisions should be in order to reduce the risks to acceptable levels. Such a provision is hardly imaginable in the Internet, as it is. Discussed approaches and strategies could be combined to offer various levels of mitigation of attacks and disincentive for the attackers, but complete set of tools for defense are currently not available both in the academic and industrial communities. One possible high-investment solution might be in a new Internet where accountability has higher value. Another key idea is to improve the way network servers are implemented, e.g. using lazy receiver processing. A third possible direction to look at is how to discover and mitigate the effects of denial of service attacks when they do not completely flood a server, but still significantly constrain its effective use of resources, overwhelming it with bogus packets. Such an approach would be highly desirable and popular among the companies doing commerce on the Internet. While short-term defenses could be found in the literature, there is a call for longer-term strategies against denial of service attacks.

A distributed form of DoS attack called DDoS attack, which is generated by many compromised machines to coordinately hit a victim. DDoS attacks are adversarial and constantly evolving. Once a particular kind of attack is successfully countered, a slight variation is designed that bypasses the defense and still performs an effective attack. In this paper, we covered an overview of the DDoS problem, available. Defense challenges and principles, and a classification of available DDoS prevention mechanisms. This provides better understanding of the problem and enables a security administrator to effectively equip his arsenal with proper prevention mechanisms for fighting against DDoS threat. The main problem is that there are still many insecure machines over the Internet that can be compromised to launch large-scale coordinated DDoS attack. One promising direction is to develop a comprehensive solution that encompasses several defense activities to trap variety of DDoS attack.

Acknowledgement

I would like to express my gratitude to my Guide Dr.R.S.Jadon,Professor& Head,MITS Gwalior and Dr.Praveen Jain Pre-Ph.D Course work Co-ordinator,MP Bhoj Open University, Bhopal , without their guidance, this Research paper would not be possible. I also wish to record my thanks to all our Resource Persons of Pre-Ph.D. Course Work for her consistent encouragement and ideas. The authors gratefully acknowledge the support of the higher authorities of Kendriya Vidyalaya Sangathan under Ministry of Human Resource Development (MHRD), Government of India for partial work given sufficient time for this paper.

References

1. Akamai‘s Prolexic Quarterly Global DDoS Attack Report Quarter 1 of 2014
2. Computer Emergency Response Team, “CERT advisory CA-2000.01 Denial of service developments”, Jan 2000. (http://www.cert.org/advisories/CA-2000-01.html)
3. The Standard Performance Evaluation Corporation, “SpecWeb96 benchmark results”, 1998.(http://www.specbench.org/osg/web96/results).
4. The Standard Performance Evaluation Corporation, “SpecWeb96 benchmark results”, 1998.(http://www.specbench.org/osg/web96/results)
5. John D. Howard, “An analysis of security incidents in the Internet”, PhD thesis, Carnegie Mellon University, 1998.
6. Arbor’s ninth Annual Worldwide Infrastructure Security Report (WISR), released march ,2014

   mim.umd.edu/wp-content/uploads/2012/10/arbor_networks_issue2-2.pdf
7. K. Kumar, R.C. Joshi and K. Singh, “An Integrated Approach for Defending against Distributed Denial-of-Service (DDoS) Attacks”, iriss, 2006, IIT Madras
8. J. Mirkovic, P. Reiher, “A Taxonomy of DDoS Attack and DDoS defense Mechanisms,” ACM SIGCOMM Computer Communications Review, Volume 34, Issue 2, pp. 39-53, April 2004.
9. B. Wang, H. Schulzrinne, “Analysis of Denial-of-Service Attacks on Denial-of-Service Defensive Measures”, GLOBECOM 2003, pp. 1339-43
10. CERT CC. Trends in Denial of Service Attack Technology, October 2001. http://www.cert.org/archive/pdf/DoS trends.pdf.
11. V. Paxson. An analysis of using reflectors for distributed denial-of-service attacks. ACM Computer Communications Review (CCR), 31(3), July 2001.
12. CERT CC. Smurf attack. http://www.cert.org/advisories/CA-1998-01.html.
13. Oliver Spatscheck and Larry Peterson, “Defending against denial of service in Scout”, In proceedings of 3rd USENIX/ACM Symposium on OSDI, pp.59-72, Feb 1999.
14. Charalampos Patrikakis, Michalis Masikos and Olga Zouraraki, “The Internet Protocol- Vol 7, Number 4”.
15. Jelena Mirkovic,Sven Dietrich,David Dittrich,Peter Reiher, “Internet Denial of Service:Attack and Defencse Mechanisms

16. Stefan Savage, David Wetherall, Anna Karlin and Tom Anderson, “Practical network support for IP traceback”, Technical report UW-CSE-00/02/01, In submission to SIGCOMM’00, Feb 2000

17. Roger M. Needham, “Denial of service: an example”, Communications of the ACM, vol.37, No.11, pp.42-46, Nov 1994.

18. Li Gong and Paul Syverson, “Fail-stop protocols: An approach to designing secure protocols”,1998.

19. Vern Paxson, “Bro: a system for detecting network intruders in real-time”, In proceedings of the 7th USENIX Security Symposium, San Antonio, TX, Jan 1998.

20. Ari Juels and John Brainard, “Client puzzles: A cryptographic countermeasure against connection depletion attacks”, In proceedings of the 1999 Networks and distributed system security symposium (NDSS’99), Internet society, Mar 1999. (http://www.isoc.org/ndss99/proceedings)

21. Bruce Schneier, “Distributed denial of service attacks”, Crypto-gram newsletter, Feb 2000.(http://www.counterpane.com/crypto-gram-0002.html#DistributedDenial-of-ServiceAttacks)

22. Stefan Savage, David Wetherall, Anna Karlin and Tom Anderson, “Practical network support for IP traceback”, Technical report UW-CSE-00/02/01, In submission to SIGCOMM’00, Feb 2000

23. X. Geng, A.B. Whinston, Defeating Distributed Denial of Service attacks, IEEE IT Professional 2 (4) (2000) 36–42.

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

25. P. Ferguson, and D. Senie, “Network ingress filtering: Defeating denial of ser-vice attacks which employ IP source address spoofing,” RFC 2267, the Internet Engineering Task Force (IETF), 1998.

26. Baker, F. “Requirements for IP version 4 routers,” RFC 1812, Internet Engineering Task Force (IETF).Go online to www.ietf.org.

27. K. Park, and H. Lee, “On the effectiveness of router-based packet filtering for distributed DoS attack prevention in power-law Internets," Proceedings of the ACM SIGCOMM Conference, 2001, pp. 15-26, 2001

28. T. Anderson, T. Roscoe, D. Wetherall, “Preventing Internet Denial-of-Service with Capabilities,” In ACM SIGCOMM Computer Communication Review, Volume 34, issue 1, January 2004, pp. 39-44

29. A. D. Keromytis, V. Misra, and D. Rubenstein, “SOS: Secure Overlay Services,” in the Proceedings of. ACM SIGCOMM, pp. 61-72, 2002

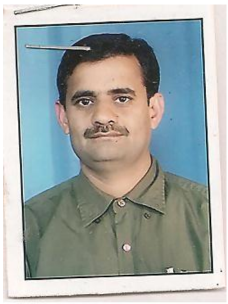
30. J. Li, J. Mirkovic, M. Wang, and P. Reither, “Save: Source address validity enforcement protocol," Proceedings of IEEE INFOCOM, 2002, pp. 1557-1566

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

32. B. B. Gupta, Student Member, IEEE, R. C. Joshi, and Manoj Misra, Member, IEEE International Journal of Computer and Electrical Engineering, Vol. 2, No. 2, April, 2010 1793-8163

33. M. Robinson, J. Mirkovic, M. Schnaider, S Michel, and P. Reiher, “Challenges and principles of DDoS defense,” SIGCOMM, 2003.

AUTHOR(S) PROFILE



Darshan Lal Meena: Received the M.C.A degree from University of Rajasthan,Jaipur in 1998 and M..Tech degrees in Computer Science from Rajasthan Vidyapeeth University ,Udaipur in 2005 and also received the M.Phil degree in Computer Science from MK University,Madurai in 2008.Presently Author is working as a PGT(Computer Science) in Kendriya Vidyalaya ,Sarni under the MHRD,Govt. of India. And presently pursuing Ph.D in Computer Science in Department of Computer Science, MP Bhoj Open University, Bhopal, Madhya Pradesh. Research Centre of Ph.d is MITS, Gwalior. His area of research is Network Security, DDoS Attacks in which he tried to Novel Solution for Distributed Denial of Service Attacks

Dr R.S.Jadon presently working as a Head & Professor in Department Of Computer Application, Madhav Institute of Technology & Science [MITS], Gwalior. Owe the credit of more than 100 research papers published in international & national journals, conference & seminar. His area of expertise is Video Data Processing Techniques