Cyber Security and Distributed Denial of Services (DDoS) Attack Prevention

[1]S. A. Itkar , [2]Chanda Agarwal

[1] professor, Department of Computer Engineering, Modern College of Engineering, Pune -05.

[2] M.E.Student, Department of Computer Engineering, Modern College of Engineering, Pune-05

Abstract - *This paper discusses the role of cyber security in our day-to-day life and explains the DDoS (Distributed Denial of Service) Attack. The legal provisions available to tackle the DDoS attack are also elaborated.*

Cyber security is a broad issue. The millions of devices linked to the Internet have variable levels of safety. There are many known and unknown vulnerabilities in the hardware and software on which these devices run. Technology too is changing at a very high rate. Attackers with poor intent need to be successful only once defenders of cyber security have to be successful all of the time.

With the increase in cyber attacks, there is a growing need to increase skills in the concepts and technology of cyber-security.

Keywords *– DDoS attack, DoS attack.*

INTRODUCTION

The World Wide Web provides the Internet user to collect, accumulate, method, and transfer huge amounts of data, which also includes proprietary and responsive business, transactional, and individual information [1]. With the digital age, businesses and customers have to increasingly rely on such capability. Security fears are evolving as the Internet is expanding rapidly, and the associated risks are becoming global.

Cyber security has a high dependency under workstation network that are available all the time and which have all the essential security components required to give the essentials of a trusted system, viz. privacy, data integrity, transactional non-repudiation, and the capability to recognize the cause of information (validation).

One factor that poses a big risk to national security is that the government trust upon infrastructures that may not be completely secure. Also, because the governments do not own or operate the worldwide networks and infrastructure they depend on; ensuring cyber security becomes a complicated issue. Many government bodies have been advocating cyber security for a long time and have recently faithful significant hard work and resources to strengthening their nation's cyber-posture.

As a head in this domain, the US Federal Government had newly announced their purpose to classify cyber-attacks as acts of conflict. At the similar time, the UK Government had announced a one billion USD project to develop superior capabilities for ensuring safety of the cyber space.

II. WHAT IS CYBER SECURITY?

Cyber security includes technologies, procedures and practices intended to watch information systems, PCs, networks and data from being assaulted, harmed or accessed without authority. [1]. It strives to ensure that safety of the institute and the user's resources is attained and maintained against appropriate safety risk in the cyber location.

Security objectives in broad include Availability, Integrity (including authenticity and nonrepudiation) and Confidentiality. With the rise in cyber attacks, it has been the subject of serious conversation in governments, industries and academia for nearly two decades. Governments and other concerned bodies across the globe are taking proactive actions to reduce or cancel the risks of successful attacks against critical cyber infrastructures.

III. THE ILL-EFFECTS OF CYBER ATTACKS

1. *Attack on Infrastructure :*

Cyber attackers have attempted to break into

important infrastructure like mass transit power grids and nuclear power, although few citizens are aware of it. The increasing number of cyber-attacks is likely to create chaos if not tackled at the right time.

2. *Attack on the banking sector :*

The banking sector is more vulnerable to these kinds of attacks. If the cyber attackers get successful in attacking bank data, sensitive information like user data and passwords will go in wrong hands. Hackers are trying to go into accounts to steal large sums of money.

3. *Attack on Individual :*

According to the recent attacks, hackers are targeting individuals without the person even knowing it. Once the system is infiltrated, hackers can steal unlimited amount of information. Hackers have the ability to capture various kind of information from user's devices like passwords, documents and spreadsheets. Antivirus programs can stop most of the bad stuff but there are always some malware that have no signature and can bypass security.

IV. DDOS ATTACK

Distributed denial-of-service, abbreviated as DDoS, is considered as one of the majority serious attacks over the Internet. It is an attempt by the malicious users to create a networked source busy to its rightful users.

A DDoS attack can be perpetrated either by flooding a network or by interrupting a server by transfer more needs than which it is built to hold, thereby preventing right of entry to a service. Due to the seriousness and ultimate effects of the DDoS attack, its detection and prevention calls for thoughtful attention in the Internet security community across the world [2].

A DDoS enemy uses several machines to commence a co-ordinated denial-of-service assault against one or additional targets. It is initiated by implication through numerous traded off computing systems by exchange a flow of steadily developing movement intended to burst sufferer property. As a consequence, they frequently congest the set of connections all the means from the starting place to the end network and system, thereby disturbing standard Internet function.

The records of DDoS attack have been rising at an alarming rate for the preceding few years. DDoS attacks are carried out by ordered criminals with the intentional of targeting financial institutions, ecommerce, gambling sites etc[2].

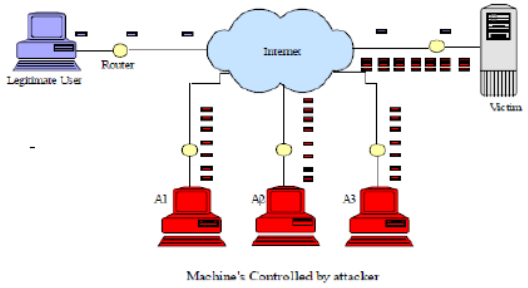

Figure 1:Illustration of DDoS Attack

V. DDOS : ATTACKERS' INCENTIVES

There are various incentives for motivating the DDoS attackers. Based on these incentives, DDoS attacks can be categorized into five categories [4]:

1. *Financial/economical gain* :

These attacks are a major concern to corporations since they involve money. Attackers of this category are usually the most technical and experienced. Attacks that are launched for financial gain are frequently the most unsafe and tough-to-stop attacks.

2. *Revenge* :

Lower technical skills with frustrated individuals are the attackers of this category, who usually carry out attacks as a response to a seeming discrimination.

3. *Ideological belief* :

Attackers in this category are motivated by their ideological attitude to hit their target. This is currently one of the major incentives for the attackers to launch DDoS attacks.

4. *Intellectual Challenge* :

Attackers of this category attack the targeted systems to test and study how to commence different attacks. Nowadays, there exist various easy ways to use attack tools and botnets to rent that even a computer amateur can avail of in order to launch a successful DDoS attack.

5. *Cyber warfare* :

Attackers of this group mostly fit in to armed or revolutionary organizations and are politically annoyed to assault critical resources and infrastructure of another country. Potential targets of these attacks include executive civilian departments and agencies, private and public financial organizations, energy and water infrastructures, and telecommunications and mobile service providers. Attackers are very well trained individuals with ample resources and spend a great deal of time and resources towards disruption of services which may severely paralyse a country and incur significant economic impacts.

VI. DDOS ATTACK : SCOPE AND CLASSIFICATION

The scattered character of DDoS attacks makes them very hard to counter or trace back. Attackers usually use spoofed or false IP addresses to conceal their true personality. Further, there are safety vulnerabilities in several of the Internet hosts that intruders can utilize to their advantage. Additionally, incidents of attacks that target the Application Layer of the OSI model are increasing rapidly. One of the important steps towards deploying a DDoS defense mechanism is to understand all the aspects of DDoS attacks [4].

DDoS flooding attacks can be classified into two categories based on the protocol level that is targeted:

A. Network/transport-level DDoS flooding attacks: These attacks are mostly launched using TCP, UDP, ICMP protocol packets.

A.1. Flooding attacks :

Attackers focus on disturbing legitimate user's connectivity by consuming victim network's bandwidth (e.g., Spoofed/non-spoofed UDP flood, ICMP flood, DNS flood etc.).

A.2. Protocol exploitation flooding attacks :

Attackers exploit specific features or implementation of some of the victim's protocols in order to consume excess amounts of the victim's resources (e.g., TCP SYN flood, TCP SYN-ACK flood, RST/FIN flood, ACK & PUSH ACK flood etc.)

A.3 Reflection-based flooding attacks:

Attackers send false or manipulated requests (e.g., ICMP echo request) instead of direct requests to the reflectors; in return, reflectors send replies to the victim and exhaust victim's resources.

A.4 Amplification-based flooding attacks:

Attackers manipulate services to generate large or multiple messages for each message they receive and amplify the traffic towards the victim. Botnets are usually used for both reflection (generate requests with spoofed source IP addresses) and amplification (exploiting IP broadcast feature of the packets).

B. Application-level DDoS flooding attacks:

These attacks focus on disturbing legitimate user's services by consuming the server resources (e.g. CPU, disk/database, memory, and I/O).Application-level DDoS attacks generally consummate less bandwidth also they are stealthier in nature. However, these attacks usually have the same impact to the services since they are also targeted towards specific characteristics of applications such as HTTP, DNS, or Session Initiation Protocol (SIP).

B.1. Reflection/amplification based flooding attacks :

These assaults use comparative systems as their system/transport-level peers (sending manipulated application-level protocol requests to substantial number of reflectors). For instance, the DNS intensification assault utilizes both reflection and enhancement methods. The attackers (zombies) create little DNS inquiries with vast measure of source IP addresses which can produce an extensive volume of network traffic since DNS response messages might be bigger than DNS query messages. At that point this expansive volume of system activity is guided towards the focused on framework to deaden it.

B.2 HTTP flooding attacks :

There are four types of attacks in this category:

B.2.1. Session flooding attacks :

Session connection requests from the attackers are higher than the requests from the legal users in this type. As a result, the server resources are exhausted. One of the famous examples for this type of attacks is the HTTP GET/POST flooding

attack. In this attack, an immense number of substantial HTTP requests (GET/POST) are sent to victim web server. Assailants for the most part utilize botnets to initiate these attacks. Each of the bots can create countless valid requests (> 10 requests a second), there is no requirement for a substantial number of bots to initiate successful attack. HTTP GET/POST flooding attacks are called non-spoofed attacks.

B.2.2 Request flooding attacks :

Here, attackers send sessions that contain more number of requests which lead to a DDoS flooding attack on the server. The single-session of HTTP get/post flooding is one of the well-known attacks in this category. This is a variation of the HTTP GET/POST flooding attack which uses the feature of HTTP to allow multiple requests within one single HTTP session. Hence, the attacker can limit the session rate of an HTTP attack and bypass session rate limitation defense mechanisms of many security systems.

B.2.3 Asymmetric attacks :

Here, in this type of attack, attackers send sessions that contain high-workload requests.

B.2.4 Slow request / response attacks :

Attackers send sessions that contains high-workload requests. This category has a number of famous attacks which are described as follows:

B.2.4.a Slowloris attack :

This attack uses HTTP GET requests to slow down a Web server using a single/limited number of machines. Partial HTTP requests are sent by the attacker which grow rapidly, update slowly, and never close. The web server becomes inaccessible since the attack continues until the requests take up all available sockets. The source addresses from where the attack in launched are usually not spoofed.

B.2.4.b HTTP fragmentation attack :

This is like Slowloris in nature. HTTP associations are held up for quite a while without raising any alerts. The attackers (bots) which are not spoofed build up a substantial HTTP association with a web server. The bots then fragment genuine HTTP packets into little sections and send every part as moderate as the server time permits out. By utilizing this methodology, by opening numerous sessions on every bot, the attackers can noiselessly cut down a Web server with the assistance of bots.

***B.2.4.c Slowpost attack* :**

In this, the attacker transmits a complete HTTP header which defines the "content-length" field of the POST message body as it sends this request for benign traffic. Data to load the message body is sent at a rate of 8-bits per two minutes. As a result, the server waits to the extent that each message body is completed while Slowpost attack grows quickly. This phenomenon causes the DDoS flooding attack.

B.2.4.d Slowreading attack *:*

In this attack, the responses are read slowly rather than slowly sending the requests. The purpose is achieved by setting a receive window-size smaller than the target server's send buffer.

VII. CLASSIFICATION OF DDoS : PREVENTION MECHANISMS

Well known signature as well as broadcast based DDoS attacks can be stopped from being launched on edge routers using attack prevention methods.

However, these methods may not be successful always since there are machines which are vulnerable to new attack types for which signatures as well as patches do not exist in the database.

The following categories of techniques can be used to prevent DDoS attacks :

(i) General techniques : Use common preventive measures for e.g. using system protection, resource replication etc. that individual servers should follow so that they do not become victim of the DDoS attack process.

(ii) Filtering techniques : These include ingress or egress filtering, router-based packet filtering, history-based IP filtering, SAVE protocol etc [5].

A. General Techniques

1. *Disabling Unused Services :*

Hosts that have less applications and open ports have lesser chance of exploit by attackers. Therefore, if network services are not required or if they are unused, the services should be disabled.

1. *Install latest security patches :*

Installing latest security patches which are relevant prevents exploitation of vulnerabilities in the target system.

2. *Disabling IP broadcast :*

If host computers and their neighbouring networks disable IP broadcast, it will be a good defense against attacks that use intermediate broadcasting nodes e.g. ICMP flood attacks, Smurf attacks etc.

3. *Firewalls :*

The role of a firewall is to allow or deny IP addresses, protocols, and/or ports. Firewalls can prevent attackers from launching simple attacks like flooding. But there are some complex attacks like for example, an attack on HTTP port number 80 which is running the web service, firewalls cannot distinguish that traffic from DDoS attack traffic - hence they cannot prevent that attack.

4. *Global defense infrastructure :*

A global deployable defense infrastructure can prevent from many DDoS attacks by installing certain filtering rules in the most important routers of the Internet. Such type of global defense architecture is not possible in reality as Internet is administered by various autonomous systems in accordance to their own local security policies.

5. *IP hopping :*

DDoS attacks can be kept in check by proactively changing the location/ the IP address of the active server from a pool of homogeneous servers or with a pre-specified set of IP address ranges. All the internet routers should be informed about the change and edge routers will drop the attacking packets. This method is still vulnerable since the attacker can launch the attack at the new IP address. Also, this technique can be made useless by adding a DNS tracing function to the DDoS attack tools.

B. Filtering Techniques

1. Ingress / Egress Filtering

Ingress Filtering is proposed by Ferguson et. al. is a prohibitive system to drop activity with IP addresses that don't coordinate an domain prefix associated with the ingress router. Egress filtering is an outbound channel, which guarantees that lone appointed or apportioned IP address space leaves the system. A key prerequisite for ingress or egress filtering is learning of the normal IP addresses at a specific port. For a few systems with complex topologies, it is not inconvenience allowed to get this information. One strategy surely understood as converse way separating can be utilized to assemble this. This strategy fills in as a switch dependably know which systems are available by means of any of its interfaces, by gazing upward source locations of the internal movement, it is conceivable to check whether the arrival way to that location would stream out the comparative interface as the packets touched base upon. On the off chance that they do, these packets are permitted else they are dropped. This method can't work productively in genuine systems where deviated Internet courses are not remarkable. All the more critically, both entrance and departure sifting can be connected to IP addresses, as well as convention sort, port number, or some other criteria of significance. Both ingress and egress filtering give a few chances to throttle the assault force of DDoS assaults. Be that as it may, it is hard to deploy ingress/egress filtering. If the attacker cautiously chooses a network without ingress/egress filtering to launch a spoofed DDoS attack, the attack can go undetected. Moreover, if an attack spoofs IP addresses from within the subnet, the attack can go undetected as well. Now-a-days DDoS attacks do not 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 not much effective to stop DDoS attacks [5].

1. Router Based Packet Filtering

Route based filtering, proposed by Park and Lee, 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. If an unexpected source address appears in an IP packet on a link, then it is assumed that the source address has been spoofed, and hence the packet can be filtered. However, there are several limitations of this scheme.

2. History based IP filtering :

Generally, the set of source IP addresses that is obtained during normal operation. In contrast, during DDoS attacks, most of the source IP addresses have not been seen earlier. During an attack, if the source address of a packet is not been defined, the packet is dropped. This scheme is robust, and does not need the co-operation of the whole Internet community. However, 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, the cost of storage and information sharing is very high.

3. Capability based method :

Capability based mechanisms provides destination which is 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 it's 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 control the traffic according to its own policy, thereby reducing the chances of DDoS attack. Packets without capabilities are treated as legacy and might get dropped at the router when congestion happens.

6. Secure overlay Service (SOS) :

An architecture called secure overlay service (SOS) is used 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 mapping. The beacon then forwards the traffic to another particular overlay node called a secret servlet for further authentication, and the secret servlet forwards confirmed traffic to the victim. The identity of the secret servlet is revealed to the beacon via a secure protocol, and remains undisclosed to the attacker. Finally, only traffic forwarded by the secret servlet chosen by the victim can pass its routers. Secure Overlay Service 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 SOS is based on the number and distribution level of SOAPs. However, wide deployment of SOAPs is a difficult DoS defense challenge.

7. SAVE : Source Address Validity Enforcement

A protocol called the Source Address Validity Enforcement (SAVE) enable routers to fill in the information of expected source IP addresses on each link and block any IP packet with an unpredicted 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 every interface. Similarly to the existing routing protocols, SAVE continually propagates messages containing valid source address information from the source location to all destinations. Hence, each router along the way is able to put up 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. However, SAVE needs to change the routing protocol, which will take a long time to accomplish. If SAVE is not properly deployed, attackers can always spoof the IP addresses within networks that do not implement SAVE. Moreover, even if SAVE is universally deployed, attackers could still launch DDoS attacks using non spoofed source addresses.

VIII. DDOS ATTACK TOOLS

One of the major reason that make the DDoS attacks wide spread and easy in the Internet is the availability of attacking tools and the powerfulness of these tools to generate attacking traffic. There are a variety of different DDoS attack tools on the Internet that allow attackers to execute attacks on the target system. Some of the most common tools are discussed below:

1. Trinoo *:*

It 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.

2. TFN :

This uses a command line interface to communicate between the attacker and the control master program but offers no encryption between attacker and masters or between masters and slaves. Communication between the control masters and slaves is done through the ICMP echo reply packets. It can implement Smurf, SYN Flood, UDP Flood, and ICMP Flood attack.

Stacheldraht : This 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.

3. Shaft **:**

This has been modelled on Trinoo network. Other than the port numbers being used for communication purpose, working of it is very similar to the Trinoo. Thus, distinctive feature of Shaft is the ability to switch control master servers and ports in real time, hence making detection by intrusion detection tools is difficult. Communication between the control masters and slave machines is achieved using UDP packets. The control masters and the attacker communicate through a simple TCP connection. Shaft can implement UDP, ICMP, and TCP flooding attack.

4. Mstream :

This is more primitive than any of the other DDoS tools. It attacks target machine with a TCP ACK flood. The communication is not encrypted and is performed through TCP and UDP packets and the master connects through 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, here, the masters are informed of access, successful or not, by competing parties.

Knight *:* This uses IRC as a control channel. It has been reported that the tool is commonly being installed on machines that were compromised earlier by the BackOrifice Trojan horse program. Knight can implement SYN attacks, UDP Flood attacks, and an urgent pointer flooder. It is designed to run on Windows operating systems and has some features such as an automatic updater via http or ftp, a checksum generator and more.

6. Trinity **:**

This 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.

IX. CONCLUSION

This paper proposes a comprehensive classification of various DDoS defense mechanisms along with their advantages and disadvantages based on where and when they detect and respond to DDoS flooding attacks. An ideal comprehensive DDoS defense mechanism must have specific features to combat DDoS

flooding attacks both in real-time and as close as possible to the attack sources. This provides better understanding of the problem and enables a security administrator to effectively equip with proper prevention mechanisms for fighting against DDoS threat. The current prevention mechanisms reviewed in this paper are clearly far from adequate to protect Internet from DDoS attack. 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. If one level of defense fails, the others still have the possibility to defend against attack.

REFERENCES

[1] Dale C. Rowe, Barry M. Lunt, and Joseph J. Ekstrom, ``The Role of Cyber Security in Information Technology Education,`` *Proceedings of the 2011 conference on Information technology education*, vol. 20, no. 11, pp. 113-122, 2011.

[2] B. B. Gupta, R. C. Joshi, and Manoj Misra, ``Distributed Denial of Service Prevention Techniques,``*International Journal of Computer and Electrical Engineering*, vol. 2, no. 2, pp. 1793-8163, April 2010.

[3] B. B. Gupta, ``A Selective Survey of Distributed Denial-of-Service (DDOS) Attacks and Defense Mechanisms,`` *International Journal on Information Sciences and Computing, vol.2, no.1, July 2008.*

[4] Saman Taghavi Zargar, James Joshi, and David Tripper, ``A Survey of Defense Mechanisms Against Distributed Denial of Service (DDOS) Flooding Attacks,`` *IEEE Communications Surveys & Tutorials, accepted for publication.*

[5] Mohd Imran, Mr. Shashi Bhshan, and Ms. Anuja Sharma, ``A Protective Model of Distributed Denial-of-Service in Internet For Lack of Variations,`` *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 4, Issue 7, July 2014.

[6] Singel R., ``Cyberwar Hype Intended to Destroy the Open Internet. Wired,`` *March1,2010.http://www.wired.com/threatlevel/2010/03/cyber-war-hype*.

[7] Souza, P. d., Rowe, D. C., Ali, A., et al., ``Cyber Dawn: Libya. Cyber Security Forum Initiative (CSFI),`` May 2011.

[8] Saman Taghavi Zargar, James Joshi, and David Tipper, ``A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks,`` June 2013.

[9] Douligeris, A. Mitrokotsa, ``DDoS attacks and defense mechanisms: classification and state-of-the-art Computer Networks,`` Volume 44, Issue 5, pp. 643-666, April 2004.

[10] C. Douligeris, A. Mitrokotsa, ``DDoS attacks and defense mechanisms: classification, in Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology (ISSPIT 03), Darmstadt, Germany,`` pp. 190-193, Dec. 14- 17, 2003.

[11] D. Moore, C. Shannon, D. J. Brown, G. Voelker, S. Savage. ``Inferring Internet Denial-of-Service Activity,`` *ACM Transactions on Computer Systems*, 24 (2), pp 115-139, 2006.

[12] Juniper Network, ``Combating Bots and Mitigating DDoS Attacks (Solution brief),`` Juniper Networks, Inc, 2006.

[13] J. Mirkovic, P. Reiher, ``A Taxonomy of DDoS Attack and DDoS defense Mechanisms,`` *ACM SIGCOMM Computer Communications Review*, Vol. 34, Issue 2, pp. 39-53, April 2004.

[14] D. Dittrich, ``The Tribe Flood Network Distributed Denial of Service attack tool,`` *University of Washington, October 21, 1999. Available at: http://staff.washington.edu/dittrich/misc/tfn.analysis.txt*.

[15] J. Barlow, W. Thrower, ``TFN2KAn Analysis,`` *Axent Security Team. February 10, 2000. Available at: http://security.royans.net/info/posts/bugtraq_ddos2.shtml.*

[16] D. Dittrich, ``The Stacheldraht Distributed Denial of Service attack tool,`` *University of Washington, December 1999. Available at: http://staff.washington*.

[17] S. Dietrich, N. Long, D. Dittrich, ``Analyzing Distributed Denial of Service tools: The Shaft Case, in Proceedings of the 14th Systems Administration Conference (LISA 2000), New Orleans, LA, USA,`` pp. 329-339, December 3–8, 2000.

[18] D. Dittrich, G. Weaver, S. Dietrich, and N. Long, ``The "Mstream" distributed denial of service attack too,`` *Available at: http://staff.washington.edu/dittrich/misc/mst ream.analysis.txt*.,May 2000.

[19] Bysin, ``Knight.c sourcecode,`` *PacketStormSecurity.nl,. Available at: http://packetstormsecurity.nl/distributed/* knight. C, July 11, 2001.

[20] B. Hancock, ``Trinity v3, a DDoS tool,`` hits the streets, Computers Security 19(7), pp. 574, 2000.

[21] M. Marchesseau, ``Trinity- Distributed Denial of Service Attack Tool`` Available at: http://www.giac.org/certified_professionals/practicals/gsec/0123.php, 11 Sept 2000.

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

[23] 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.

[24] P. Ferguson, and D. Senie, ``Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing,`` *RFC 2267, the Internet Engineering Task Force (IETF)*, 1998.

[25] Baker, F. ``Requirements for IP version 4 routers,``RFC 1812, Internet Engineering Task Force (IETF).Go online to www.ietf.org.

[26] 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*, pp.15-26, 2001.

[27] T. Peng, C. Leckie, K. Ramamohanarao, ``Protection from Distributed Denial of Service *attack using history-based IP filtering,`` in Proceedings of IEEE International Conference on Communications (ICC 2003), Anchorage, AL, USA*, Vol. 1, pp. 482-486, 2003.

[28] T. Anderson, T. Roscoe, D. Wetherall, ``Preventing Internet Denial-of- Service with Capabilities,`` *In ACM SIGCOMM Computer Communication Review*, Vol. 34, Issue 1, pp. 39-44, January 2004.

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

[30] B. B. Gupta, Student , R. C. Joshi, and Manoj Misra, ``Distributed Denial of Service Prevention Techniques,`` *International Journal of Computer and Electrical Engineering*, Vol. 2, No. 2, 1793-8163, April, 2010.