Distributed Denial of Service Attack and its Countermeasures

Akash Sharma, Deepanshu Batra, Rajat Pandey, Priti Narwal, Vinay Kumar
Manav Rachna International University
Faridabad, India
akash97sharma10@gmail.com
deepanshubatra1997@gmail.com
rajatp91gmail.com
preeti.fet@mriu.edu.in
vinay.kumar@accendere.co.in

ABSTRACT: *Since past few years, there has been a rapid increase in use of attacks or cyber crime over the cyber space and one of the most common attacks used is the distributed denial of service attack. These attacks leads for use in the variety of both the attacks and the defence approaches. In this paper, classification of the available mechanisms which are proposed in the literature on how to keep the cyber space away from the possible DDoS attacks and discuss the strong and weak points of each mechanism. This provides the better understanding of the problem and enables a security administrator to effectively equip his storages with proper prevention mechanisms for fighting against DDoS attacks. The paper investigated multiple nature of the problem and look for its causes, further presenting brief insights and suggested approaches for defending against DDoS attack.*

Keywords: DDoS attacks, TCP Synchronization, Flood Attacks, DDoS Installation

Received: 26 April 2018, Revised 25 May 2018, Accepted 4 June 2018

DOI: 10.6025/ijwa/2018/10/3/91-99

1. Introduction

As the days are passing the role of internet has been consistently increasing in our life, every little thing we do on our devices is connected to the network internet has become a very major part of our life, the increase in the amount of work over the network has lead to an increase in the cyber crimes[1]. However, nowadays cyberspace is full of DDoS(distributed denial of service attack), email spamming, financial frauds over the internet and many more. Cyberspace is becoming the heaven for the intelligent criminals. Among all the attacks over the internet most commonly practiced attack are DDOS attacks, distributed denial of service attack is also known as DDoS attack in these multiple systems which are infected or compromised are used to target a single system which leads a Denial of Service (DoS) attack the systems can be infected using a Trojan.

2. Literature Overview

From a technical point of view, the network insecurity, on the one hand, because of all the resources through a network share, on the other hand, its technology is open. In general, network security threats are the following[2]:

• **Inadvertent Human Error:** Improper use of operators, security configuration vulnerabilities, the user with poor security awareness, choosing inadvertently a password will pose a threat to network security.

• **Man-made Malicious Attacks:** Such attacks are divided into two kinds: one is the active attacks, its purpose is to tamper with the information contained in the system, or to change the system's state and operation in variety of ways and to destroy it validity, integrity, and authenticity; the other is a passive attack, it does not affect the normal work of the network, intercept and theft information, strong threat confidentiality of the system.

• **Non-authorized Access:** The use of network or computer resources without their consent is seen as a non-authorized access. Mainly in the following forms: the illegal users by impersonating the identity access the network for illegal operation; authorized users in a lawful manner operate and so on.

2.1 DDOS Attack Networks

This section deals with classification of two major DDoS attack network models.In the next section we'll discuss the types of DDoS attack network i.e. the agent handler model and the Internet relay chat based model (IRC model).

2.1.1 Agent Handler Model

Agent handler model is divided into three parts known as clients, handlers, and agents. Clients platform is where the DDoS attacks the network, handlers are the software packages which are located on computing systems throughout the Internet that is used by the attacker to communicate indirectly with the agents. The agent software exists on the compromised systems that will ultimately carry out the attack on the victim's system[3].

The attacker using the help of software packages which are located on the computing system over the internet also known as the handlers to communicate with the agents present on the compromised systems which will be later used to attack on the victim system[4].

2.1.2 IRC Based DDoS Attack Model

IRC stands for the Internet Relay Chat ,a multi-user, online chatting system. It allows the users to create two party or multi-party interconnections and type messages in real time[3]. The IRC network architectures consist of IRC servers that are located throughout the cyber space with channels to help in communication with each other across the Internet. The internet relay chat networks allow their users to create public, private and secret channels. Public channels are the channels where multiple users can chat and share messages and files with each other[5].

The Public channels allow the user of the channel to see or access all the IRC names and messages of users in a channel. Private and secret channels are set up by users to communicate with only other designated users secretly and privately[6]. Both the private and the secret channels protect the names and messages of users that are logged on from users who do not have access to the channel[5].In this the content of private channels is hidden, certain channel locator commands can allow users not on the channel to identify if it exists or not, whereas the secret channels are much harder to locate unless the user is a member of a channel[7].

2.2 DDoS Attack Taxonomy

There are a wide variety of DDoS attack techniques. There are two classes of DDoS attacks: bandwidth depletion attacks and resource depletion attacks[6].

2.2.1 Bandwidth Depletion Attacks

The flooding of victim network with unwanted traffic that prevents legitimate traffic from reaching the victim system happens using bandwidth depletion attacks. A bandwidth attack can be divided into flood attack and amplification attack[7]. A flood attack involves the zombie system sending traffic in large volumes to a particular victim system which congests the bandwidth of the victim's system. What an amplification attack does is that it broadcast messages to Ip addresses inturn using all the

system in the network to send messages to the victim system[8].

2.2.2 Flood Attacks

Zombies are created to flood a victim system with a large amount of IP traffic. Large volumes of data packets which are in turn sent by the zombies to a particular system which slows down the system gradually resulting in crashing the system and lower down and saturates the network bandwidth[2]. Which prevents legitimate users from accessing the network[7-9].

This is also divided into two types: UDP Flood Attacks and ICMP Flood Attacks.A UDP flood attack may fill the bandwidth of connection located around the victim systems. This basically impacts the systems located near the victim system. An ICMP flood attack occurs when the zombies send large volumes of ICMP_ECHO_REPLY packets to the victim systems[10].

2.2.3 Amplification Attacks

It uses the broadcast IP address feature which can easily be found on most of the routers to amplify the attack. This feature manages the router that serves those data packets within the network to all addresses in the broadcasted address range. This can be distinguished into Smurf and Fraggle attacks. A DDoS Smurf Attack is an attack where the attacker sends packets to a network amplifier with the returned address spoof to the victim IP address. Another DDoS attack is Fraggelattack where the attacker sends packets to a network amplifier using UDP ECHO packets[13]. This attack can generate more bad traffic and cause more damage than a Smurf attack[11].

2.3 Resource Depletion Attacks

Resource depletion attacks prevent the victim system from using its resources. In this type of DDoS attack the attacker sends those packet which misuse the network protocol communication[8].

2.3.1 Protocol Exploit Attacks

TCP Synchronization

The Transfer Control Protocol which includes a three-way handshake between the receiver and the sender before sending the data packets.The initiating system sends an SYN request. The receiving system acknowledges (ACK) the SYN request, and in turn, sends its own SYN request. The initiating system therefore sends back its ACK and hence the communication begins between the two systems[7].

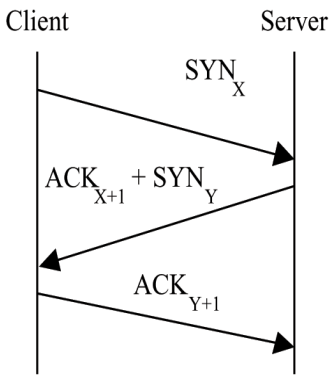

Figure 6a. TCP Synchronization

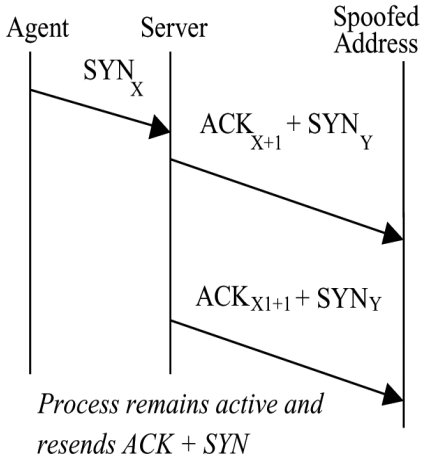

Figure 6b. TCP SYN Attack

Figure 1. DDoS TCP SYN Attack

In this attack the attacker makes zombies and instructs them to send malicious TCP SYN requests to a victim server to tie up the resources of the server's processor, thus preventing the server to acknowledge legitimate request[14]. The TCP SYN attack the three-way handshake between both the sending and the receiving system.At the end, if the volume of these attacks request is larger, the victim system will eventually run out of their resources[15].

3. Software Used For DDoS Attacks

3.1 DDoS Agent Setup

Active and Passive techniques are used to install malicious code or data on a victim system, to set up an Agent Handler on an IRC based DDoS attack network. Active methods include scanning various system on the network for vulnerabilities. Once a vulnerable system is identified the attackers tries to break into the system[16]. The passive method involves the attacker sharing corrupt files or building web sites that take advantage of known vulnerabilities in a secondary victim's web browser[17-18].

3.2 Active DDoS Installation

3.2.1 Scanning

Before launching a DDoS attack, attackers must first set up the DDoS attack network.One common tool attackers use to scan for ports is a software program called Nmap[16]. Nmap is used to identify which os version is running and who is hosting the network.

3.2.2 Software/Backdoor Vulnerability

There are many sources on the Internet, such as the Common Vulnerabilities and Exposures (CVE) organization, which publicly list all the known vulnerabilities of different systems [18]. This research information is available so network administrators can make their systems more secure; however, it also provides attackers with data about which vulnerabilities exist.

3.2.3 Trojan Horse Program

Trojan horse program is installed on a victim's system by the attacker and allow the attacker to gain control of a user's computer without the user knowing[20]**.** In the case of a DDoS attack tool setup, Trojan horse programs already installed on a victim system might be used by the attacker to gain access to a secondary victim's system allowing the attacker to install the DDoS agent code[19].

3.3 Passive DDoS Installation

3.3.1 Bugged Web Site

The attacker is allowed to create websites with code or commands to lure in a victim in this method. When the victim tries to access the webpage or its content, the web page voluntarily installs malicious code. The malicious HTML code could include the DDoS agent, and takes the form:

<object classid="clsid:XXXXXXXX" codebase = http://www.webpage.com/myactivex.cab></object>

3.3.2 Corrupted File

This method is used to alter files and include malicious code embedded inside them. When the victim system tries to execute or even view these files, they will get infected by the malicious code.When a user launches the file, his machine will become infected with the DDoS agent software. Some attackers are skilled enough to include a text box to open, so the victim will think the file was legitimate and will not realize that it contained the DDoS agent.

4. DDoS Attack Software Commands

(i) Agent Commands

Command	Description
Turn On	Agent to turn on and wait for other commands.
Turn Off	Instructs the agent to shut down
Initiate Attack Download	This command is used to make the agent to launch an attack against a specified target.
Upgrades	This command is used to make the agent to download an upgrade package, usually an executable file that can be uploaded from a web location.

Set Attack Time	Instructs Agent with time to begin an attack.
Set Attack Duration It	Instructs Agent with time to end an attack.
Set Packet Size	It Instructs the Agent to set the number of bytes in each attacking packet.
Info	Prints information (some type of help/command listing)

Table 1.Agent commands and description

(ii) Handler Commands

Command	**Description**
Log On	This command is for the attacker to log on to the handler (usually password protected).
Turn On	This command instructs the handler to turn on and wait for other commands.
Log Off	This command is used by the attacker to log off of the handler.
Turn Off	Instructs the handler to shut down. If the handler was actively polling the network looking for agents, this command stops the handler from continuing this action.
Initiate Attack	Instructs the handler to contact all agents and have them launch an attack against a specified target.
List Agents	Instructs the handler to poll the network looking for all active agents (usually involves a ping of the agents).
Kiss Agents	Remove agents from the DDoS attack network.
Add Victim IP Address	Add a new victim IP address to the list of addresses for agents to attack.
Download Upgrades	Instructs the handler to download an upgrade package, usually an executable file that can be uploaded from a web location.
Set IP Address Spoofing	Instructs the handler to turn IP Spoofing on to the agents. This allows the attacker to set the spoofed IP address.
Set Attack Time	Instructs the handler to set a time when it should communicate to the agents to begin the attack.
Set Attack Duration	Instructs the handler to set a time when it should communicate to the agents to end the attack.
BufferSize	Set the buffer size for packets sent during a flood attack.
Info	Print information (some type of help/command listing)

Table 2. Handler commands and description

5. Challenges

One of the most important issues that will impact how countermeasures against DDoS attacks are deployed will be the cost of solutions and preventive measures. If DDoS prevention strategies cost companies and individuals huge sums of money than these systems will not see quick or wide-scale deployment. It will take time before industry and government agencies buy new

products. Additionally, attackers build methods to counter specific security measures. This leads to a cyclical pattern of new security systems being deployed, and new attacks being designed.

For the DDoS attacks, what is desirable is a more comprehensive solution that can defend against both known attacks and new variants. The following list summarizes and discusses technical challenges for DDoS defense:

• **Need for a Distributed Response at Many Points on the Internet.** There are many possible DDoS attacks, very few of which can be handled only by the victim. Thus, it is necessary to have a distributed, possibly coordinated, response system. It is also crucial that the response is deployed at many points on the Internet to cover diverse choices of agents and victims.

• **Lack of Detailed Attack Information.** It is widely believed that reporting occurrences of attacks damage the business reputation of the victim network. Therefore, very limited information exists about various attacks, and incidents are reported only to government organizations under obligation to keep them secret. It is difficult to design imaginative solutions to the problem if one cannot become familiar with it. Note that the attack information should not be confused with attack tool information, which is publicly available at many Internet sites. Attack information would include the attack type, time and duration of the attack, number of agents involved (if this information is known), attempted response and its effectiveness, and damages suffered. Appendix C summarizes the limited amount of publicly available attack information.

• **Lack of Defense System Benchmarks:** Many vendors make bold claims that their solution completely handles the DDoS problem. There is currently no standardized approach for testing DDoS defense systems that would enable their comparison and characterization. This has two detrimental influences on DDoS research:

(1) Since there is no attack benchmark, defense designers are allowed to present those tests that are most advantageous to their system.

(2) Researchers cannot compare the actual performance of their solutions to existing defenses; instead, they can only comment on design issues.

• **The Difficulty of Large-Scale Testing:** DDoS defenses need to be tested in a realistic environment. This is currently impossible due to the lack of large-scale test beds, safe ways to perform live distributed experiments across the Internet, or detailed and realistic simulation tools that can support several thousand nodes. Claims about defense system performance are thus made based on small-scale experiments or simulations and are not credible.

6. Countermeasures for DDoS Attacks

After consulting to different research papers a conclusion can be drawn regarding the countermeasures related to DDoS attacks that no complete solution is being so far discovered by anyone that can cure all forms DDoS attacks.Although a no. of partial proposals or solutions are available today to prevent, divert and mitigate the effects of these attacks.

Every now and then attackers develop new ways of bypassing each of the countermeasures in use. Understanding the nature, the scope of a DDoS attack can help in developing the techniques and attack tools (software oriented) to help in developing better preventive methods[6].

There are three essential components of DDoS countermeasures :

• Preventing the DDoS attack which includes preventing secondary victims and detecting and neutralizing handlers

• Dealing with a DDoS attack while it is in progress including detecting and preventing the attack, mitigating or stopping the attack and deflecting as well.

• The final component is post- attack component which involves network forensics.

7. Prevention of Secondary Victims

7.1 Individual Users

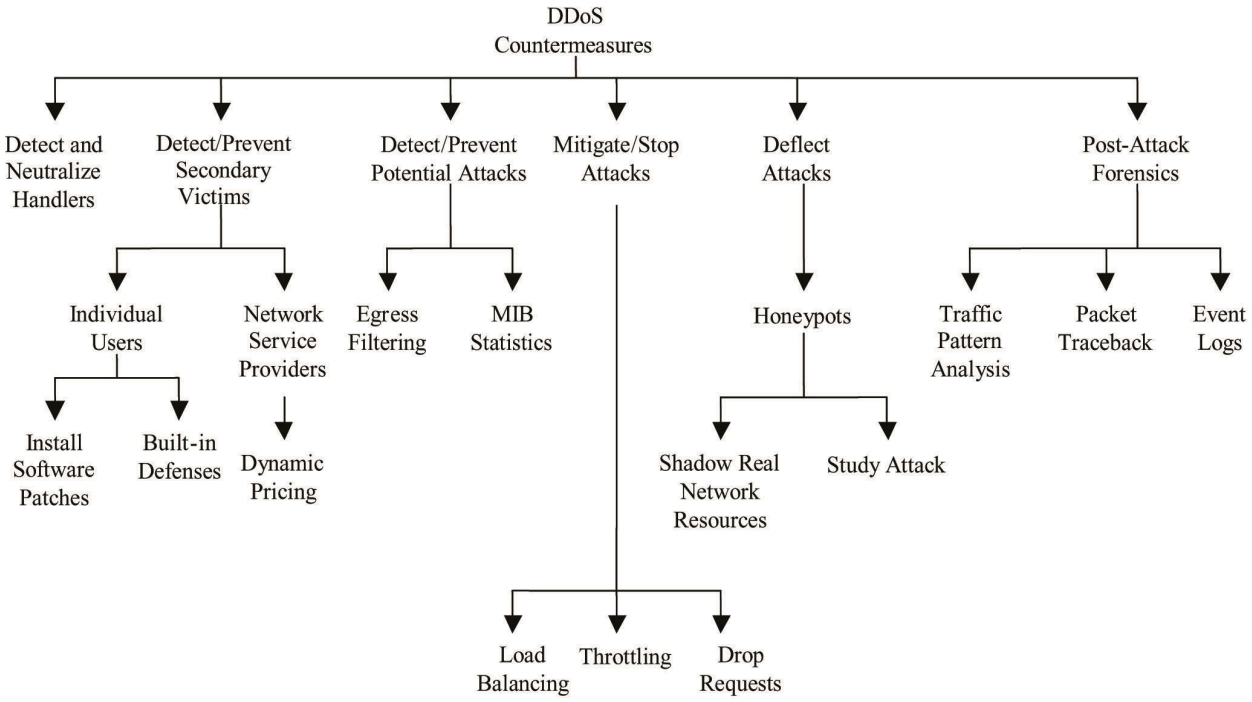

Figure 2. Flowchart for Countermeasures for DDoS attacks

One of the best methods to prevent DDoS attacks is for the secondary victim systems to prevent themselves from participating in the attack. This requires a heightened awareness of security issues and prevention techniques from all Internet users. Ifattackers are unable to break into and make use of secondary victim systems, then the attackers will have no "DDoS attack network" from which to launch their DDoS attacks.

In order for secondary victims to not become infected with the DDoS agent software, users of these systems must continually monitor their own security. They must check to make sure that no agent programs have been installed on their systems and that they are not sending DDoS agent traffic into the network. The Internet is so de-centralized, and since there are so many different hardware and software platforms, it is quite difficult for typical users to implement the right protective measures. Typically this would include installing anti-virus and anti-Trojan software and keeping these up to date. Also, all software patches for discovered vulnerabilities must be installed.This can significantly reduce the probability of a system being compromised as a secondary victim in setting up a DDoS attack network.

• **Network Service Providers**: This strategy is currently in the discussion phase and it emphasizes on adding pricing the network usage by the providers. If providers chose to charge a significant amount of money for some of the resources or access to some services, this will allow legitimate customers on to their network and will increase their conscious to send traffic they send into a network.

• **Protocols**: This strategy is still in discussion phase, it is still a challenge to design protocols that do not offer opportunities for DDoS attacks. Its main objective is to preventing server's resources from establishing a large no. of spoof TCP connections. Modifications are to be made in high-bandwidth routers of ISP networks.

• **Zombie Prevention**: It is an important step towards preventing the secondary victims from being a part of an army of attacked computers or zombie computers. If hosts that are connected to the public internet are being prevented from buffer overflow that can be mitigated using either software and hardware mechanisms.

7.2 Detect and Neutralize Handlers

One important method for stopping DDoS attacks is to detect and neutralize handlers. Since the agent-handler DDoS attack tools require the handler as an intermediary for the attacker to initiate attacks, finding and stopping the handlers is a quick method to disrupt the DDoS attack network. This can possibly be done by studying the communication protocols and traffic patterns between handlers and clients or handlers and agents in order to identify network nodes that might be infected with a handler. Also, there are usually far fewer DDoS handlers deployed than there are agents, so neutralizing a few handlers can possibly render multiple agents useless, thus thwarting DDoS attacks.

7.3 DetectPotential Attacks

• **Egress Filtering**: It is a method in which scanning of packet headers of IP packets leaving is done and checked that if they follow certain criteria. This prevents from IP address spoofing which is one of the main features of DDoS attack. It works like if a given packet passes a particular criteria it will be routed outside it originated network otherwise it will not be transferred to the intended user. One can use firewalls or packet sniffer for this purpose

• **MIB Statistics:** Another method currently being looked at to identify when a DDoS attack is occurring uses the Management Information Base (MIB) data from routers. The MIB data from a router includes parameters that indicate different packet and routing statistics. Current research has focused on identifying statistical patterns in different parameters during a DDoS attack. It looks promising for possibly mapping ICMP, UDP, and TCP packet statistical abnormalities to specific DDoS attacks.

Accurate statistical models based on the MIB parameters from routers are still being studied to understand how accurately they can monitor DDoS attack traffic and predict when a DDoS attack is happening. Work in this area could provide important information and methods for identifying when a DDoS attack is starting and how to filter or adjust the network to compensate for the attacking traffic.

9. Conclusions

A number of conclusions can be drawn from understanding DDoS attacks and from looking at some of the countermeasures that are being researched or implemented.

• DDoS attacks are quite advanced methods of attacking a network system to make it unusable to legitimate network users.

• These attacks are an annoyance at a minimum, and if they are against a critical system, they can be severely damaging. Loss users. The negative effects of a DDoS attack make it important that solutions and security measures be developed to prevent these types of attacks.

• Detection, prevention, and mitigation DDoS attacks(as discussed earlier) is important for national security.

The Prime purpose of this paper will be to know more about DDoS attacks and tools and main countermeasures for the same. The need for us is to understand is that internet being an important component of our lifestyle has become user-friendly over the years which has attracted government agencies, businesses etc which gives a chance to lead towards hacking and disturbing network traffic. According to researchers conducted worldwide, it has been concluded that although remote cracking once required a fair amount of skill set and computer knowledge, hackers have now access to all attack scripts and protocols which can be down-loaded from the World Wide Web and launch them against victim sites. In short, it can be concluded that as the sophistication of attacking tools has increased, the access and controlling of them are easier to use.

10. Future Scope

DDoS attacks that have occurred using www (world wide web) in recent times have led to some serious damages which are now being considered as legal issues. Since victims of the attacks usually cannot trace back to the attacker, there is a question of which other parties may be liable in terms of contributory negligence. Since some DDoS attacks can be traced back to the secondary victims, can the owners or corporations responsible for secondary victim computers be held liable for participating in an attack? Are software vendors liable for vulnerabilities in their code? Are hardware vendors responsible for not providing defenses against malicious intrusion and use of the machines they sell by remote parties other than the owners? Do network providers have an obligation to prevent their networks from allowing secondary victims to send DDoS packet traffic into the network?

References

[1] Karig, D., & Lee, R. (2001). A remote denial of service attacks and countermeasures. *Princeton University Department of Electrical Engineering Technical Report CE-L2001-002*, *17*.

[2] Stein, L. D. (2002). *World Wide Web Security FAQ*. Lincoln D. Stein..

[3] Criscuolo, P. J. (2000). *Distributed denial of service: Trin00, tribe flood network, tribe flood network 2000, and stacheldraht ciac-2319* (No. CIAC-2319). CALIFORNIA UNIV LIVERMORE RADIATION LAB..

[4] Specht, S. M., Lee, R. B. (2004, September). Distributed Denial of Service: *Taxonomies of Attacks, Tools, and Countermeasures*. In *ISCA PDCS,* 543-550.

[5] Bridis, T. (2002). Powerful attack cripples majority of key Internet computers. *SecurityFocus News, The Associted Press, http://www. securityfocus. com/news/1400*.

[6] Specht, S., & Lee, R. (2003). Taxonomies of distributed denial of service networks, attacks, tools and countermeasures. *Princeton University Technical Report CE-L2003-03*.

[7] Nicolas Pioch. "A Short IRC Primer". Edition 1.2, January 1997. http://www.irchelp.org/irchelp/ircprimer.html#DDC. (21 April 2003).

[8] Kleinpaste, Karl, Mauri Haikola, and Carlo Kid. "The Original IRC Manual". March 18, 1997. http://www.user-com.undernet.org/documents/irc-manual.html#seen (21 April 2003).

[9] Kevin J. Houle. "Trends in Denial of Service Attack Technology". *CERT Coordination Center, Carnegie Mellon Software Engineering Institute.* October 2001. www.nanog.org/mtg-0110/ppt/houle.ppt. (14 March 2003).

[10] TFreak. "smurf.c", *www.phreak.org*. October 1997. http://www.phreak.org/archives/exploits/denial/smurf.c (6 May 2003).

[11] Federal Computer Incident Response Center (FedCIRC), "Defense Tactics for Distributed Denial of Service Attacks". *Federal Computer Incident Response Center.* Washington, DC, 2000.

[12] TFreak. "fraggle.c", *www.phreak.org*. http://www.phreak.org/archives/exploits/denial/fraggle.c (6 May 2003).

[13] Martin, M. J. (2002). Router Expert: Smurf/Fraggle Attack Defense Using SACLS. *Networking Tips and Newsletters, www. searchnetwork. techtarget. com*..

[14] Chen, Y. W. (2000). Study on the prevention of SYN flooding by using traffic policing. In *Network Operations and Management Symposium, 2000. NOMS 2000. 2000 IEEE/IFIP* (pp. 593-604). IEEE.

[15] Kumar, R., Arun, P., Selvakumar, S. (2009, March). Distributed denial-of-service (ddos) threat in collaborative environment-a survey on ddos attack tools and traceback mechanisms. *In*: *Advance Computing Conference, 2009. IACC 2009. IEEE International* (1275-1280). *IEEE*.

[16] Nessus Documentation", *Nessus*. 2002. http://www.nessus.org/. (8 April 2003).

[17] Specht, S., Lee, R. (2003). Taxonomies of distributed denial of service networks, attacks, tools and countermeasures. *Princeton University Technical Report CE-L2003-03*.

[18] "Girma, A., Garuba, M., Li, J., Liu, C. (2015, April). Analysis of DDoS attacks and an introduction of a hybrid statistical model to detect DDoS attacks on cloud computing environment. *In*: *Information Technology-New Generations (ITNG), 2015 12th International Conference on* (212-217). *IEEE*.

[19]. Pelaez, C. E., & Bowles, J. (1991, March). Computer viruses. In *System Theory, 1991. Proceedings., Twenty-Third Southeastern Symposium on* (513-517). *IEEE*.