A Simulation based analysis study for DDoS attacks on Computer Networks

Mariam Abojella Msaad, Reema A. Saad
Faculty of Information Technology, University of Tripoli,
Tripoli, Libya
Meemee_02@yahoo.com, Ranem_reem@yahoo.com

Azeddien M. Sllame
Faculty of Information Technology, University of Tripoli,
Tripoli, Libya
Aziz239@yahoo.com

Abstract— **A denial of service attacks are usually employed to interrupt the system's activity by getting a large number of fake requests, which leads to slowing down and stopping information system or network operations. This paper outlines the basic principles of DDoS attacks, explains how DDoS attack works. The paper presents an experimental using OPNET simulation tool in which traffic from three different applications VoIP, FTP, and HTTP is used to make the practical model with a firewall shield to model and simulate DDoS over Internet. However, three scenarios have been developed to illustrate different aspects of the DDoS over networks. The results clearly demonstrate how firewalls can be configured to mitigate DDoS attacks.**

Keywords: DoS attacks; DDoS attacks; Firewall; Network security; modeling, simulation.

I. NTRODUCTION

Networks connect people, simplify the use of software and services, and provide access to tools that make businesses around the world run efficiently. So, computer networks are now as the Internet industry's most valuable assets. They form the foundation of data centers for the delivery of data between consumers, companies, government agencies and social and scientific communities. Documents, data files, data collected by information processing facilities, controlled and processed by other organizations, and multimedia streaming might be that information, which handled inside networks during their lifetime. Network architectures, however, are becoming relatively complex to meet the everyday supplies of businesses in order to satisfy availability and security. Therefore, applications for network protection or hardware devices, such as firewalls are used to defend computer networks from multiple network attacks that consume a target network's incoming bandwidth. However, network security aims to: monitoring physical accessibility to the computer network, preventing accidental deletion, preventing data modification or compromise, detecting and preventing planned internal security breaks; and noticing and stopping unapproved exterior interventions and hacking [1].

One of the commonly disturbing network attacks is the *Denial of Service* attacks (DoS), which created by flooding the network medium with fabricated packets that prevent the proper operation of networks. However, one of the network devices used to prevent and mitigate an attacker from initiating DoS attacks on network resources is firewalls. Unauthorized access is a common weakness found in both wired and wireless networks, where an attacker may connect a computer to the network through unsecured ports of a switch or a poorly protected wireless router. In addition, an attacker can use weak points when interconnecting with the network to lead dangerous attacks on the network, such as: *sniffing* the users' data to hijack valuable information, or launching a DoS attack to an account of authorized users on any network by overflowing entire network by injecting streams of incorrect data, and spoofing the physical information of validated *Media Access Control* (MAC addresses) of network's hosts to securely take-out important data or to conduct a 'man-in-the-middle' attack.

Network security is therefore designed to look after the protection of networks and to keep computers, communications, and communication devices save against unintended users. In addition, network security aims to develop tools, protection strategies, and procedures to make sure that data are transmitted with confidentially and received with integrity across computer networks. Furthermore, business continuity (i.e. availability) is one primary objective that must be achieved in entire networks by providing extra protection to maintain data usable and consistent with efficient integrity and security levels. Finally, information security aims include: regulating and securing physical security to computers and networks, protecting data's access; protecting transfer of information across networks; ensuring secured accessibility to network' assets; discovering and stopping unintentional data removal, preventing data modification or destruction; monitoring and put away any internal security attempts; doing risk management and controlling incident response procedures [1].

This paper is organized as follows: Previous work is reported in section 2. Principles of information security and definitions are briefly described in section 3. Types of computer networks attacks are summarized in section 4. Essentials of DDoS attack is described in section 5. Section 6 demonstrates the experimental results. Section 7 clarifies the conclusion.

II. PREVIOUS WORK

There are many related research papers published in many international conferences and scientific journals. Authors in [2] evaluated the capabilities of the firewall in mitigating the DDoS attacks. However, in [3] the authors presented some researches on DoS attacks and detection programming, while in [4] the authors reported an integrated DDoS Attack Defense Infrastructure for Effective Attack Prevention method.

III. DEFINITIONS AND PRINCIPLES OF INFORMATION SECURITY

Information security is a set of procedures and tools proposed to protect data and prevent any illegal access or alteration to data and its related facilities such as networks and

data centers, often referred as *info sec*, both when it is stored, processed and when it is transmitted from one device to another through networks.

The following definitions are related to paper context [5] [6] [7]:

- *Attack:* A deliberate or accidental act that can harm information and/or the structures that sustain it or otherwise damage it. Attacks can be active or passive.
- *Threat*: A category of objects, people, or other entities that present a danger to the assets of the information systems.
- *Distributed denial of service (DDoS)*: Efforts to make the capabilities of computers or networks unavailable for their intended use. DDoS generally consists of organized attacks, malicious attempts by an attacker to discourage or stop the successful operation of a website or service at all, permanently or temporary.
- *Malicious code (malware)*: piece of software is designed to penetrate or damage a computer or network system without the informed consent of the owner. Viruses, worms, backdoors, and Trojans are the most widely identifiable forms of malware.
- *Social engineering*: The process of manipulating people to perform actions or to share sensitive data.
- *Industrial espionage*: Industrial espionage defines practices such as theft of trade secrets, bribery, blackmail and technological surveillance, as well as spying on corporate entities and often government entities.
- *Spam, phishing, and hoaxes*: Although spamming and phishing exist, they are often produced together. The misuse of electronic messaging networks, many of which contain hoaxes or other inappropriate content, such as links to phishing websites, is spamming. Phishing is the criminally deceptive practice of attempting to access sensitive information such as usernames, passwords, and credit card information.
- *Intrusion detection*: It is the process of recording events that occur on a computer system or networks to examine them for signs of possible accidents that signify failures or imminent threats of infringement of security policies, appropriate usage policies, or normal security practices of computer networks.
- *Intrusion prevention:* It is a mechanism that effectively prevents threats from targeting the network even before they enter the target host while they are online on the network.
- *Firewalls:* It is a device that implements the security policy of an entity at the boundary between two different networks. Most firewalls are designed to block (prevent) any traffic that is not authorized by the corporate security policy.

IV. Types of computer networks attacks

In computer networks some attacks, such as eavesdropping and phishing, acquire information from the device or personal information. Attacks may also interfere, such as viruses, worms, and Trojans, with the intended purpose of the system. The other kinds of attack are that they can be activated by DDoS attacks when the system's resources are used in a useless way. Other types of network intrusions, such as land assaults, *smurf* attacks and *tear-drop* attacks, are also available [4]. Attacks can be categorized into "*Passive*" when data passing through the network is intercepted by a network attacker and "*Active*" when an intruder initiates commands to interrupt the network's normal activity [8][9] [10].

A. Active attacks

Active attacks are attacks carried out by malicious nodes that carry a certain energy cost to carry out the attacks. Any data manipulation, streaming, or creating a false stream include active attacks. Spoofing attacks, wormhole attacks, alteration, DoS, Sinkhole, and Sybil attacks are several types of active attacks [8] [10].

B. Passive attacks

The names of some passive attacks are traffic analysis, Eavesdropping, and Monitoring. In traffic analysis: an attacker tries to sense the communication path between the sender and receiver. There is no modification in data by the traffic analysis. Traffic analysis, Eavesdropping, and Monitoring are the names of certain passive attacks. Whereas, eavesdropping as a passive attack on the ad-hoc mobile network tries to uncover any knowledge from contact that is classified or confidential. This confidential information may be the sender or receiver's private or public key, or any secret data. In Monitoring, the confidential data can be accessed by the attacker, but the attacker cannot alter the data or change the data [8][9] [10].

C. Advanced attacks

There are many reported advanced attacks such as black hole, rushing, replay, byzantine, and location disclosure attacks [10]. Black hole attacks are one of the developments in attacking methods in which the routing protocol is used by the attacker to advertise himself as having the best route to the node whose packets he wants to intercept. Rushing attacks occur when a sender sends a packet to the receiver; the packet is altered and forwarded to the receiver by an attacker. In replay attacks, the data may be replicated or delayed by a malicious node. This can be accomplished by an originator who intercepts and retransmits the information. An attacker is able to intercept the password at that time. Whereas, in byzantine attacks a group of intermediate nodes operate between the sender and the receiver and making certain modifications, such as creating routing loops. However, location disclosure attacks are accomplished by computing and tracking the traffic, a malicious node collects information about the node and the path. So, further attacks on networks could be carried out by malicious nodes [10] [11].

V. DDoS attacks

A DDoS attack uses many computers to launch a coordinated DoS attack against one or more targets. Using client/server technology, using the resources of several unknown accomplice machines, which function as attack bases, the attacker will greatly improve the efficiency of the attack. The most advanced form of DoS attack is the DDoS attack. It is differentiated from other attacks by its ability to spread its

arms over the Internet in a “distributed " way to generate venomous traffic [10]. DDoS attacks never attempt to crack the framework of the victim, where the primary objective of a DDoS attack is to damage the structures of a target [11]. However, a DDoS is carried out in several phases. First, multiple agents (slave) machines are employed by the attacker. Usually, this process is performed automatically by remote machine scanning, searching for security susceptible holes that allow supervision. The Week devices are then attacked using the vulnerabilities identified and infected with the code of the attack. The exploit/infect process is also automated. Thus, the infected machines can be used to further train new agents. Then, agent machines are used to send packets for an attack [10]. The DDoS attack is composed of four elements, as shown in Fig. 1, for more details see [11].

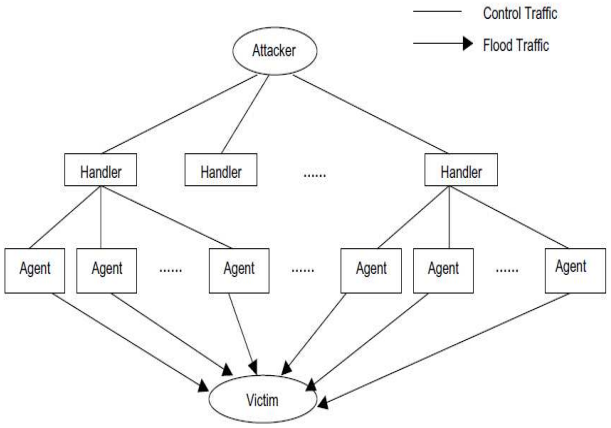

Fig. 1. Architecture of DDoS attacks [11]

Fig.1 includes the following:

(1) The real attacker;

(2) Handlers or masters are compromised hosts with a special program running on them that can monitor multiple agents.

(3) Attack node agents or zombie hosts who are the hacked hosts whose running a special program and are responsible for producing a packet stream to the systems of the intended target. However, those machines are commonly external to the victims own network in order to avoid efficient response from the victim, and external to the network of the attacker, to avoid liability if the attack is traced back.

(4) A victim or target host.

The following steps are usually taken during planning and conducting of a DDoS attack [9]:

(1) Selection of agents: The attacker selects the agents who will execute the attack. Such devices need to have any vulnerability that can be exploited by the attacker to access them. They should also have sufficient resources that will allow them to create powerful streams of attack.

(2) Compromise: The attacker exploits the agent machines' security holes and vulnerabilities, and implants the attack code. In addition, an intruder may attempt to protect the code from detection and deletion. Usually, the owners and users of the agent systems have no idea that their device has been compromised and that they can engage in a DDoS attack. Each agent software uses only a small number of resources (both in memory and bandwidth) when engaging in a DDoS attack, so that computer users experience limited performance changes.

(3) Communication: To determine the agents are up and running, when to plan attacks, or when to update agents, the attacker interacts with any number of handlers. Depending on how the attacker configures the DDoS attack on a network. Users can communicate between the attacker and the handler and between the handler and agents using TCP, UDP or ICMP protocols.

(4) Attack: The attacker starts the attack at this stage. It is possible to change the victim, the duration of the attack, as well as special attack characteristics such as form, length, TTL, port numbers [10][11].

VI. Experimetial Study

The OPNET simulation tool is used to model and simulate the DDoS attack over a wide area network based on MPLS technology. OPNET is a Discrete Event Simulation (DES) tool that offers detailed and lifelike implementations for a wide range of applications. However, OPNET can be used to evaluate the performance of different technologies including a wide range of devices and links applied to various network’s infrastructures with many processes, protocols and procedures for many network nodes in several reliable and identical implementations [12]. Thus, OPNET simulation tool is chosen to carry out the performance evaluation study in this paper.

In this simulation’s study there are three different scenarios as shown in the baseline design model shown in Fig.2; with considering the same network topology. However, the experimental study carried out in this paper by applying three different applications namely; Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP) and Voice over Internet protocol (VoIP) in order to make the simulation study more realistic over a wide area network with MPLS technology. During the simulation the network is tested through a random injection of traffic of all types (VoIP, HTTP, and FTP) from all nodes to all nodes randomly. However, DDoS attacker uses HTTP and FTP heavy-traffic from attacker’s network which is 25 PCs, as seen in Fig.3, which describes the paths of DDoS traffic attacking the whole network. Fig.4 shows the HTTP generation windows on OPNET tool. In addition, VoIP traffic is generated between nodes applying the menu icon "*create traffic flow*" from OPNET simulation tool using the next input constraints:

- Call rate: 100 calls per hour for every scenario resulted in a 210 voice traffic flows.
- Average call duration: 300s (5 min).
- Voice flow duration: 3600s (60 min).
- Encoder scheme: G.711.
- Type of Service: Interactive voice (6) with delay, throughput, and reliability.
- Including Overhead (bytes): RTP/UDP/IP.

Therefore, the network scenarios are:

(1) Scenario 1 is baseline network with operational firewall without DDoS attack.
(2) Scenario 2 is with operational firewall with DDoS attack.
(3) Scenario 3 is with operational firewall blocking HTTP coming from attacker network.

From these illustrations we can see that a very huge traffic calculated in Giga Bytes values is supplied to the network to demonstrate more realistic simulation performance study

which also illustrates the efficiency of employing MPLS networks in handling different traffic efficiently. Furthermore, the configuration of the firewall is shown in Fig.5.

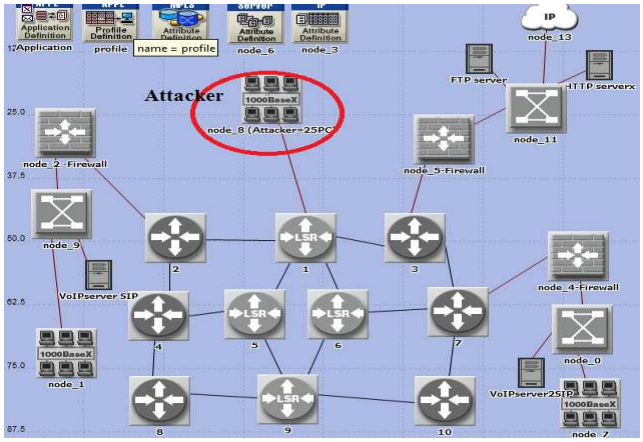

Fig.2 .The case study topology with of DDoS path selected

Simulation results

The following results will show different performance metrics used with the three applications; FTP, HTTP, and VoIP applications to evaluate the performance of the different situations in different scenarios under DDoS attack.

FTP Profile

Fig.6 describes FTP download response time with the three scenarios, which shows that FTP download response time is increased with DDoS attack. It is higher with DDoS attack (red line in Fig. 6) where it is increased by factor of 3 than DDoS attack case with attack blocking of (blue line), while it is 4 times higher than normal traffic network (green line).

Fig. 7 describes FTP upload response time with the three scenarios, which shows that FTP upload response time is higher with DDoS attack during blocking (blue line in the Fig. 7) where it is approached 15 seconds, which is much higher than DDoS attack and normal network case.

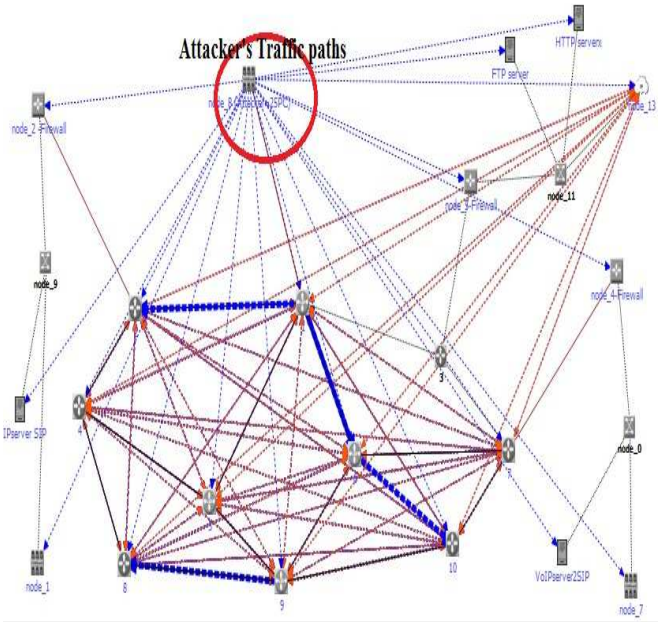

Fig.3 DDoS attacker's traffic and paths sent to all nodes of the case study

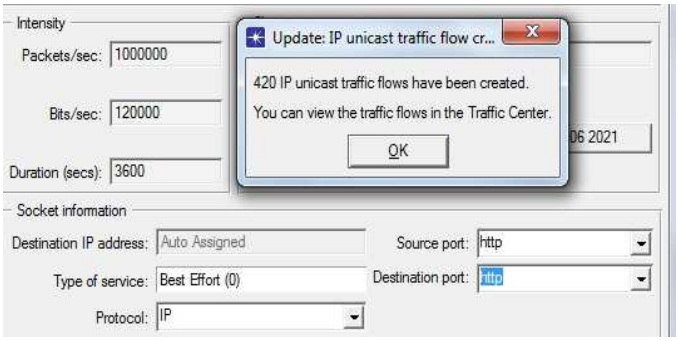

Fig.4 DDoS attacker's traffic and paths with all nodes

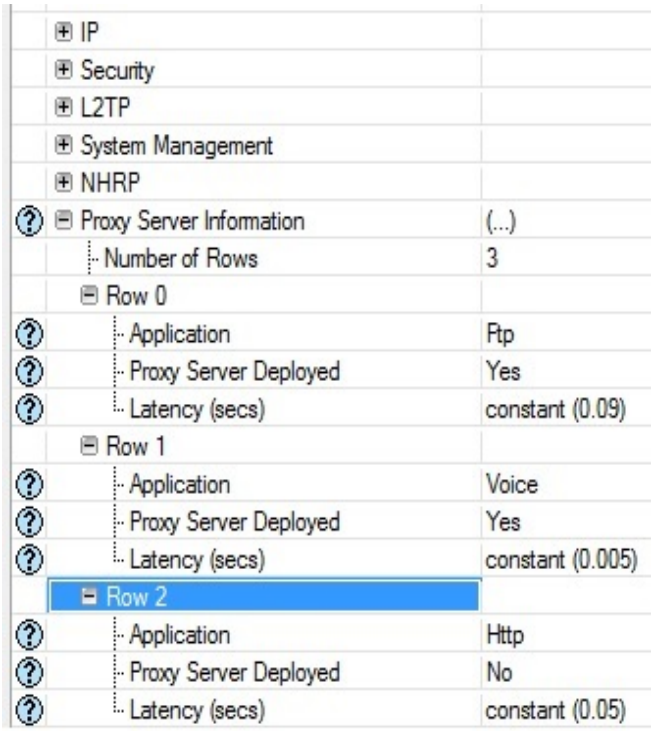

Fig.5 The configuration of Firewall to prevent HTTP traffic of DDoS attacker's traffic

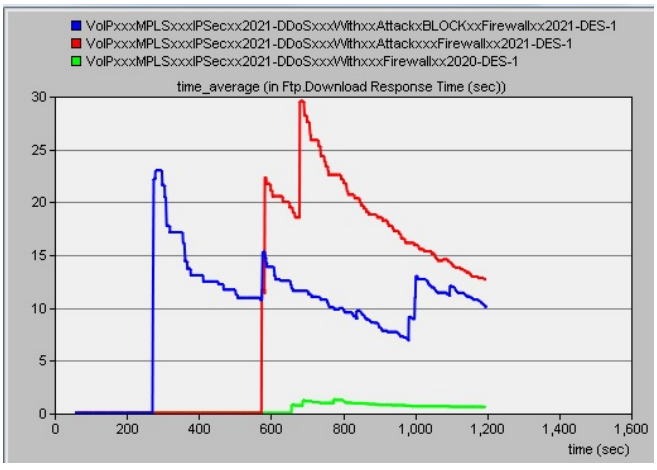

Fig.6 FTP download response time (Sec)

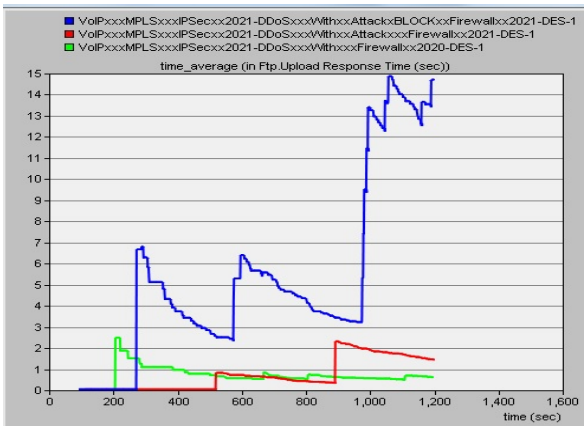

Fig.7 FTP upload response time (Sec)

HTTP profile

Fig. 8 refers to HTTP object response time in seconds; it seen from the Fig. 8 that the HTTP object response time within normal network (no attack) is around zero (very very small value) (Fig.8 in the down place). Whereas, HTTP object response time is about 0.001 second with DDoS attack but firewall working to block attacker's traffic (Fig. 10 in the upper place). However, HTTP object response time with DDoS attack without any traffic blocking from firewall is around 2 seconds and approaching 4 seconds, which is very high value compared to other cases (Fig. 8 in the middle).

Fig. 9 demonstrates the simulation results of HTTP page response time in seconds; it is clear from Fig.9 that the HTTP page response time when using a network without DDoS attack behavior (normal network); where no DDoS attack is around 0.094 seconds, but at the beginning reaches the maximum of 1 second (Fig. 9 in the down place). However, HTTP page response time is about 0.003 of second with DDoS attack but firewall working to block attacker's traffic (Fig.9 in the upper place). Furthermore, HTTP page response time with DDoS attack without any traffic blocking from firewall is around 3 seconds and approaching 9 seconds in some period of time, which is a very high value compared to other cases (Fig. 9 in the middle).

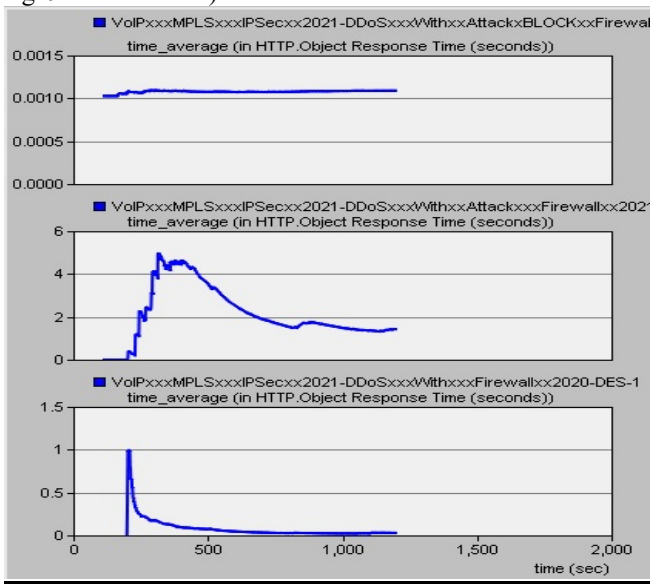

Fig.8 HTTP object response time (Sec)

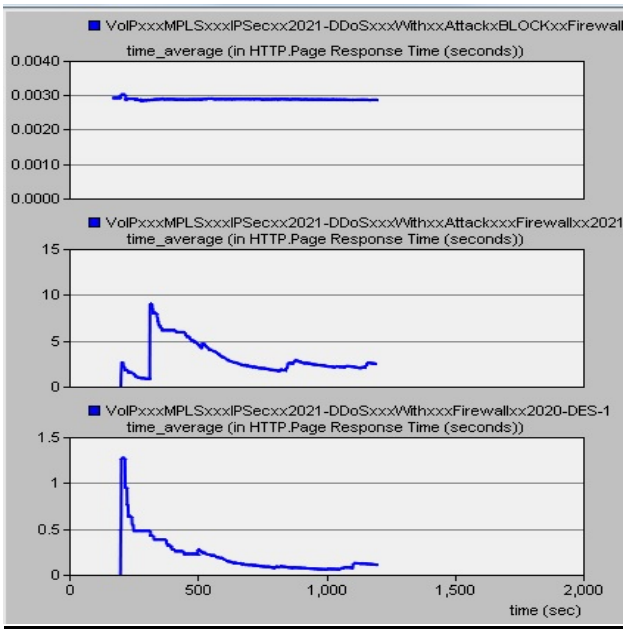

Fig.9 HTTP page response time (Sec)

Fig.10 makes evident of the HTTP injected into the scenarios with and without DDoS attack. The red line shows the DDoS traffic which looks higher than the other two scenarios.

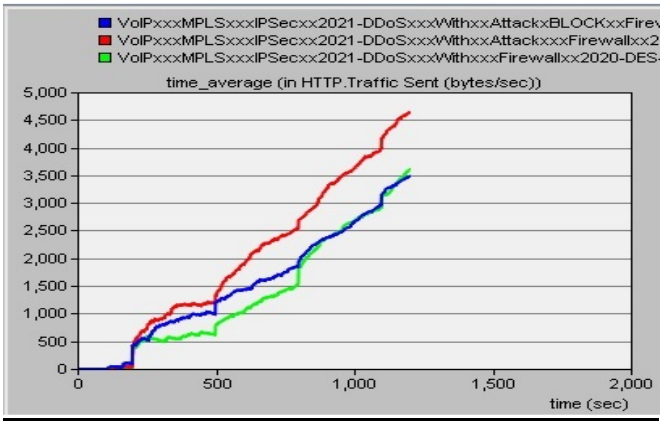

Fig.10 HTTP traffic injected to experimnets of DDoS attacks (bytes/secs)

Fig.11 illustrates the Transport Control Protocol (TCP) segment delay in seconds for the three scenarios. The Fig. 11 clearly shows that the TCP segment delay is much higher in the case of DDoS attack than the other two cases where it is approaching 25 seconds while the normal case in which there is no DDoS attack it is around 0.02 seconds and at the maximum was 0.12 seconds. However, the TCP segment delay with the DDoS attack block case was 0.5 seconds on average.

VoIP profile

Fig.12 describes the VoIP packet delay variation within the scenarios with and without DDoS attack. The red line of Fig. 12 expresses the VoIP packet delay variation with DDoS attack, which approximately increases linearly with the time of attack and it is more than the other two cases which looks higher than the other two scenarios with factor of 2.

Point-to-point Throughput

Fig.13 describes the Throughput of the attacker's traffic generated during the DDoS with two scenarios of DDoS attack and the blue line shows the firewall blocking of attack.

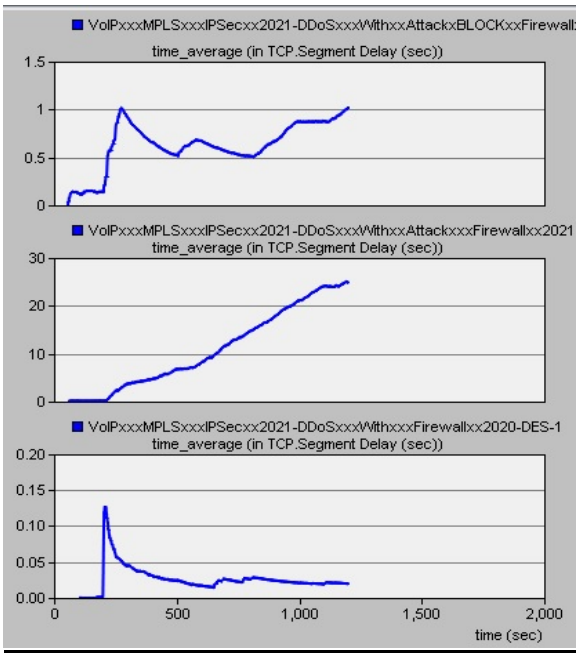

Fig.11 TCP segment delay (Sec)

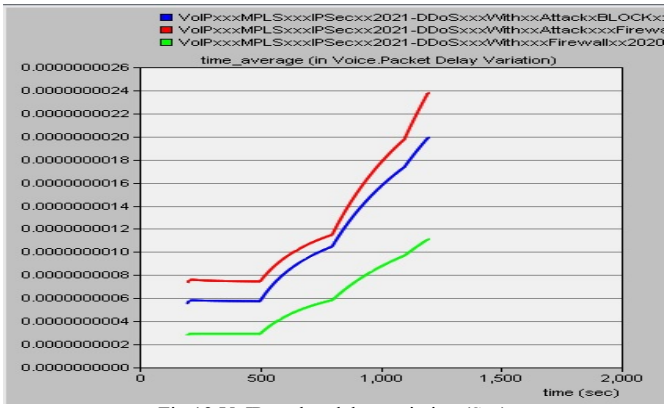

Fig.12 VoIP packet delay variation (Sec)

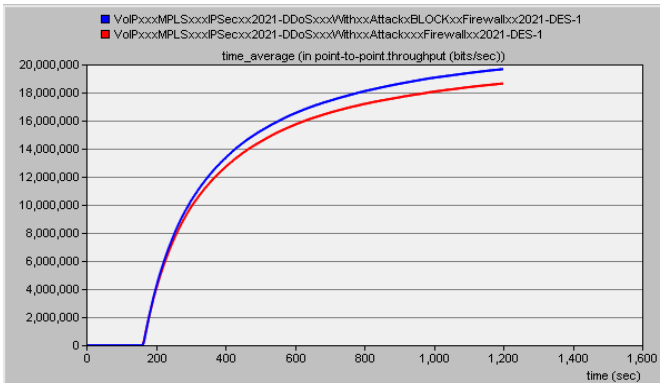

Fig.13 point-to-point throughput (bits/sec) under DDoS attack

VII. Conclusion

DDoS are from the group of the most commonly dangerous security threats disturbing the business continuity. Because of such importance, this paper is an attempt to model and simulate DDoS attacks over Internet using OPNET tool. A set of applications contains VoIP, FTP, and HTTP is used in the presented experimental study to make the model more realistic practically. The paper results showed a model and detailed simulation results with three scenarios that have been developed to demonstrate different aspects of the DDoS over WAN networks. The presented results clearly show how firewalls can be used to mitigate DDoS attacks. However, the firewalls when employed with a correct configuration and proper security policy provides suitable defense fence against DDoS attacks.

Reference

[1] James F. Kurose and Keith W. Ross: Computer Networking: A Top-Down Approach Featuring the Internet, 2012.

[2] Wael Alosaimi, Mazin Alshamrani, Khalid Al-Begain: *Simulation-Based Study of Distributed Denial of Service Attacks Counteract in the Cloud Services*, in WSEAS Transactions on Computer Research, Volume 4, 2016, E-ISSN: 2415-1513, pp.19-30.

[3] W. Liu, "Research on DoS Attack and Detection Programming," in 2009 Third International Symposium on Intelligent Information Technology Application, 2009, pp. 207–210.

[4] Y. Choi, J. Oh, J. Jang, and J. Ryou, "Integrated DDoS Attack Defense Infrastructure for Effective Attack Prevention," in Proceedings of the Second IEEE International Conference on Information Technology Convergence and Services (ITCS), 2010, pp. 1–6.

[5] Albert Caballero: "Information Security Essentials for IT Managers: Protecting Mission-Critical Systems", 2nd edition, Elsevier publisher, 2014.

[6] Bhavya Daya ."Network Security: History, Importance, and Futue" ,University of Florida Department of Electrical and Computer Engineering , FL, USA, 2013.

[7] Kuldeep Sharma, Neha Khandelwal, Prabhakar.M ."*An Overview Of security Problems in MANET*".

[8] Amol S. Rajpure ,swami chincholi ,Pune Sachin S. Bere Asst.,swami chincholi ,Pune ,"*Network Security with its Thesaurus Attacks and feasible Security Technology* ", 2019, IJRAR journal, May 2019.

[9] Mohan V. Pawar , Anuradha J. "*Network Security and Types of Attacks*", Network International Conference on Intelligent Computing, Communication & Convergence (ICCC-2014), India, Procedia Computer Science 48 (2015) 503 – 506, Elsevier publisher.

[10] Jelena Mirkovic, Peter Reiher. "*A taxonomy of DDoS attack and DDoS Defense mechanisms*", ACM SIGCOMM Computer Communication Review, Vol. 34, Issue 2, April 2004, pp.

[11] Christos Douligeris, Aikaterini Mitrokotsa , "*DDoS attacks and defense mechanisms: classification and state-of-the-art* ", in Computer Networks: The International Journal of Computer and Telecommunications Networking 44 (2004), issue 5, pp.643–666, Elsevier publisher.

[12] OPNET product documentation v.11.0.A, OPNET Technologies, Inc., Bethesda, MD, 2004.