Study of Distributed Denial of Services of Web Server and Network in Cyber Security

Pallavi Sharma[1], Maninder Kaur[2]
[1]M.Tech (Scholar), [2]Assistant Professor
Department of Electronics Communications and Engineering, Doaba Institute of Engineering and Technology, Kharar

Abstract **-** Distributed Denial of Service attack is an incessant critical threat to the internet. Application layer DDoS Attack is resulting from the lower layers. Request layer based DDoS attacks use HTTP requests after formation of TCP three way hands shaking and overwhelms the target resources, such as sockets, CPU, memory, disk, record bandwidth. Network layer based DDoS assaults directs the Synchronize (SYN), User datagram Protocol (UDP) and Internet Control Message Protocol (ICMP) requests to the server and exhausts the bandwidth. The problem found that DDoS attack is an accepted growth from the Synchronize (SYN) Flood. This attack is converging Internet connection bandwidth of many types of machinery upon one or a few machines. Usually, the attacker installs the remote attack database on weakly protected processors using Trojan horses and intrusion methods, and then coordinates the attack from all the different computers at once. The problem is when an attacker will try to attack the system, threat would be detected by Genetic Algorithm and with the help of its fitness function it would harvest an assessment value out of that risk.

Keywords **-** Distributed Denial of services, Internet Control Message Protocol, HTTP and UDP (User Datagram Protocol).

I. INTRODUCTION

A computer system consists of a group of computers, printers & other tools that is connected jointly so that they can communicate with each other. A system consists of 2 or more computers that are associated in order to contribute to resources (such as printers and CDs), replace files or allow electronic connections. The computers on a network may be connected through cables, phone lines, radio waves, satellites or infrared light beams [1**].**

A. Cyber Security

Cyber Safety is the body of technologies, procedures & practices considered to protect system, computers, agenda and data from attack, break or unauthorized admission. In a compute situation, the term safety implies cyber safety. Organization & consumer's assets include linked computing strategy, personnel, transportation, submission, services, telecommunications schemes, and the totality of transferred & stored data in the cyber atmosphere. Cyber security strives to ensure the achievement & maintenance of the safety property of the organization and user's assets against relevant security risks in the cyber atmosphere. The general safety objectives comprise the following:

- Availability
- Integrity, which may take in authenticity & non-repudiation
- Discretion

Cyber security involves protecting that information by preventing, identify, & responding to attacks.[4]

B. Types of Network

1) Local Area Network

The system used to be linked computers in a only space, space within a building or buildings on 1 site are called Local Area Network (LAN). LAN transfer data with a rapidity of several megabits per second (106 bits per second). The broadcast medium is usually coaxial wire. LAN links computers, i.e. software & hardware, in the similar area for the reason of sharing data.

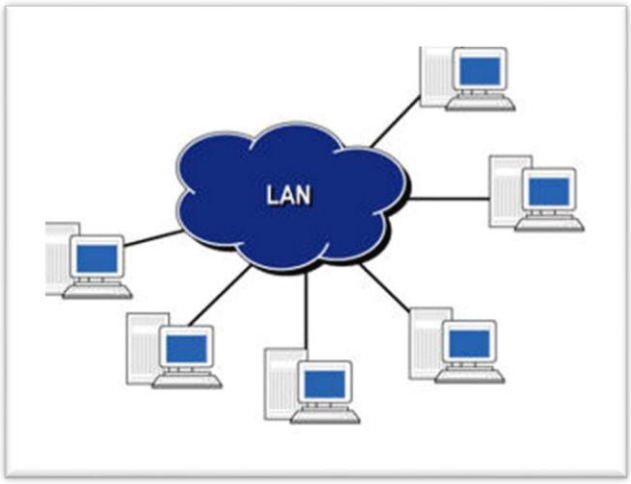

Fig.1 LAN Network

2) Wide Area Network

The term Wide Area Network (WAN) is used to explain a computer system spanning a regional, national or global area. For example, for a great corporation the head quarters might be at Delhi and regional branches at Bombay, Madras and Bangalore. The distance between computers connected

to WAN is better. The broadcast medium used is usually telephone lines, microwaves and satellite links [2]

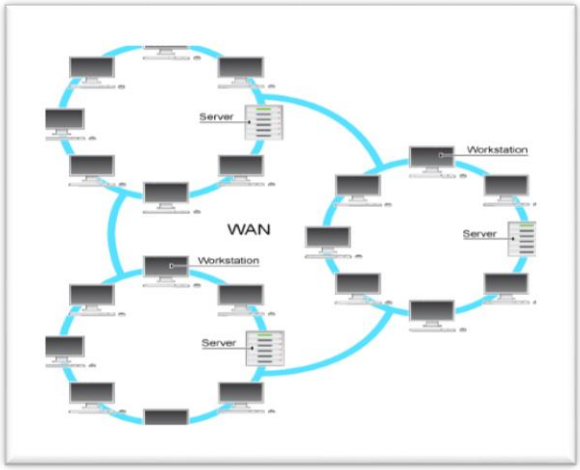

Fig.2 WAN Network

3) Hybrid Network

Between the LAN and WAN structures, hybrid networks are discovered such as campus area nets (CANs) & metropolitan area networks (MANs). In addition, a fresh form of system type is emerging describe home area networks (HANs). The access to business Web sites has produced 2 classifications known as intranets & extranets[3].

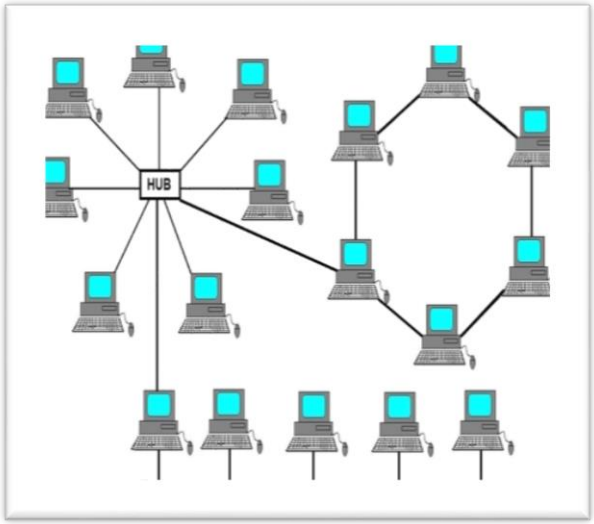

Fig.3 Hybrid Network

II. RELATED WORK

Bing Wang et al. in 2014 [5] proposed by examining the security impact, in particular, the impact on DDoS attack defence mechanisms, in an enterprise system where both technologies are adopted. They found that SDN technology can really help enterprises to defend against DDoS attacks if the defines architecture is designed properly. To that end, they proposed a DDoS attack extenuation architecture that assimilates a highly programmable network monitoring to qualify attack detection & a supple manage organization to allow fast and specific attack reaction.

[8] Shakti Arora et al. in 2014 [6] planned mechanisms that does not outfit to MANET resource constraints because of introduction of substantial traffic load to argument and verifying keys. Because of such problems ad hoc networks have their own vulnerabilities that are not always undertaken by these wired network security solutions. Distributed Denial of Service attacks have also become a problem for Internet using computer system.

[9] Meghna Chhabra et al. in 2014 [7]In this described as, the purpose of this study is to understand the flaws of prevailing solutions to combat the DDoS attack & a novel scheme is being providing with its authentication to reduce the effect of DDoS attack in MANET Environment. As Internet users are growing day by day, it is becoming more prone to attacks and new riding techniques. People are accessing material and communicating with each other on the move.

[10]Sarra Alqahtani et al. in 2015 [8] described a DDoS attack uncovering approach for service clouds & develops effectual algorithms to resolve the creating service for the attack. The detection method had composed of four levels such that each level detects symptoms of DDoS attacks from its local data.

[12] Jae-Hyun Jun et al. in 2015 [9] described a network layer based DDoS attacks which sends the SYN, UDP and ICMP requirements to the server & exhausts the bandwidth. Usual profile is created from user's access behaviour attributes which is the base line to discriminate DDoS attacks as of flash crowd. An irregularity detection mechanism is projected in this weekly to detected DDoS attacks using Enhanced Support Vector Machine with string kernels.

III. FACT AND FIGURES

Distributed denial of service operations remains one of the most popular type of attack, according to a statement from Kaspersky Labs. The occurrences are relatively simple to orchestrate, & extremely difficult to protect against, making them 1 of the most favoured tools for an attacker, be they a nation-state like China or an activist set like Anonymous.

DDoS attacks are used to interrupt a computer network's ability to function by flooding it with information, thus rejecting service to authentic users. DDoS attacks are also highly under-reported, according to Kaspersky's research.

Kaspersky intelligences the following data on DDoS attacks from the second quarter of this year:

- **Figures:** The longest DDoS attack persisted 60 days, 1 hour, 21 minutes and 9 seconds. The highest number of DDoS attacks against a single site was 218.

- **Attacks by Country:**89% of DDoS traffic was generated in 23 countries. The US & Indonesia complete up a combined 11% of attack traffic.

IV. PROBLEM FORMULATION

- DDoS attack is an accepted growth from the SYN Flood. The idea overdue this attack is converging Internet connection bandwidth of many types of machinery upon one or a few machines.
- This way it is likely to use a large array of smaller widely distributed computers to create the big flood effect. Usually, the attacker installs his remote attack database on weakly protected processors using Trojan horses and intrusion methods, and then coordinates the attack from all the different computers at once.
- This makes a brute force flood of malicious "nonsense" Internet traffic to swamp and devour the target server's or its network connection bandwidth. This means packet flood contends with, and overwhelms, the network's valid traffic so that "good packets" have a low probability of enduring the flood. The network's servers become cut off from the rest of the Internet, and their service is denied.

V. TYPES OF ATTACKS

A helpful means of classify safety attack is in relations of Active attack & Passive attack. A passive attack attempts to monitor the information from the scheme but does not affect structure resources. An active attack attempt harms system resources and their operations.

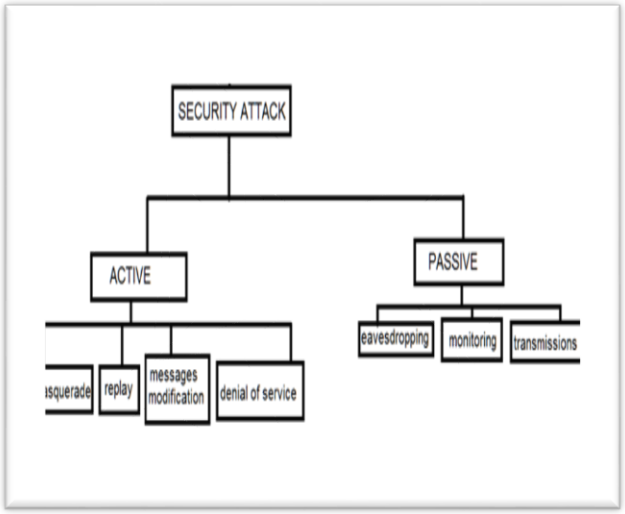

Fig.4 Security attack

- **Passive attack**

Passive attack is in nature of attic dropping on, or monitor of broadcast. Passive attacks contain traffic analysis, checking of unprotected infrastructure, decrypting weakly encrypted transfer, & capturing authentication data such as keys. Passive interception of network procedure enables challenger to see impending actions. Passive attacks effect in the disclosure of information or data archive to an attacker devoid of the consent or knowledge of the user.

- **Active attack**

It involves some adjustment of the information Stream or formation of the false tributary. Attacker tries to avoid or break into secured systems. This can be complete through worms, stealth, or viruses, Trojan horses. Active attacks include attempts to circumvent or crack protection features, to set up malicious code, & to steal or modify data. These attacks are mounted alongside a system backbone, use information in transfer, electronically penetrate an enclave, or attack an authorized remote consumer during a try to connect to a cooperative. Active attacks subdivided into four categories; masquerade, replay, modification of message, and denial of service

- **Spoof attack**

In a spoof attack, the hacker tries to access the network IP address. Before gaining access to the system with applicable IP address, the attacker can modify, reroute, or delete the data.

- **Buffer run over**

A buffer run over attack is when the attacker drives more data to system than is expected. A shield run over attack generally results in the attacker gaining administrative access to the system in a command punctual or shell.

- **Exploit attack**

In this kind of attack, the attacker knows of a security problem within an operating system or a section of software & leverages that information by exploiting the vulnerability.

- **Password attack**

An attacker attempts to break the passwords store in a system account database or a password-protected file. There are three major kind of password attacks: a brute-force attack, a dictionary attack, & a hybrid attack**.[10]**

- **Smurf Attack**

A perpetrator can launch the Smurf attack by sending a spoofed Echo-Request memo to a network's transmitting IP address. The spoofed Echo-Request memo has the victim's IP talk to as the source IP address. Hence, each host receiving the broadcast Echo-apply for message will drive an Echo-Reply memo to the victim. The victim will be overwhelmed with a flood of Echo-Reply post. Thus, the Smurf attack is a type of Denial-of-Service (DoS) attack. Two solutions have been at present adopted in the Internet to avert a Smurf attack : (i) Routers do not forward datagrams having the purpose address as a broadcast IP attend to& (ii) Hosts are configured not to respond for Echo-Request post that were received as a broadcast message.

- **Traffic Redirection**

A cooperation router can propel out route inform messages to all its neighbouring routers inform them that it lays on the direct path to every network in the Internet. The

neighbouring routers onward all of their inward data package to this confrontation router, which will get eventually flooded with the data package& starts reducing them. The information packets do not make it to the destination.

VI. DDOS ATTACK

Distributed Denial of Service attacks have emerged as one of the most severe threats between others. The strength of DDoS attacks has turned into stronger according to advancement of network infrastructure. DDoS attacks are thrown by generating a tremendously large quantity of traffics and they quickly tire resources of target [11] systems, such as system bandwidth and computing control. DDoS defences mechanism can be classified into four classes which are prevention, uncovering, mitigation, and response. When DDoS attack occur, first step to spoil DDoS attacks is the detection and it should be done as fast as possible. However, it is difficult to differentiate between Distributed Denial of Service attack and ordinary traffics, since DDoS attack traffics frequently do not hold horrible contents in the packets. Moreover, attackers copy their source address to cover up their location and to create DDoS attacks more refined. DDoS detection schemes should assurance both short detection delay and high detection rates with low false positives [5].

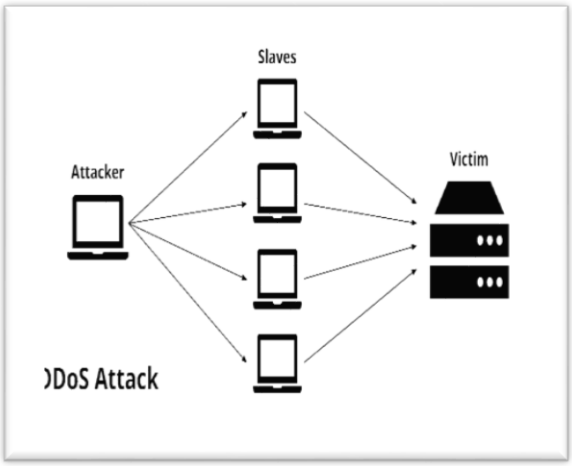

Fig.5 DDoS Attack

Distributed Denial of Service attacks have posed a massive hazard to the Internet. Researching development of recognition and doubt against DDoS attacks results in not only the advance of data security systems, but also continually attack tools enhanced by skilled attacker in order to avoid these safety systems. Various DDoS attack tools and their late publications come to the fore and DDoS field quickly becomes more and more difficult. Thus, it is of huge implication to state DDoS attack in an abstract and formal method and to categorize them in a scalable classification.

VII. CONCLUSION

We implement firstly Initialize the server scenarios or network architecture. Secondly User sent the request of the Web Server if Web server is free then accepts the Request then further request send the application server. Application Server reverts back to the Web server then web server reply the user. Information Transfer user to web server and web server to application server. Attacker will come and hack the information means server will be down or increase the delay and overload of the server. An anomaly detection mechanism is proposed in this paper to detect DDoS attacks. Apply the optimization technique for detect the attack and prevention classification technique

VIII. REFERENCES

[1]. Comer, Douglas E. *Computer networks and internets*. Prentice Hall Press, 2008.
[2]. Chun, Dorothy M. "Using computer networking to facilitate the acquisition of interactive competence." *System* 22.1 (1994): 17-31.
[3]. Wellman, Barry, et al. "Computer networks as social networks: Collaborative work, telework, and virtual community." *Annual review of sociology* (1996): 213-238.
[4]. Moslehi, Khosrow, and Ranjit Kumar. "A Reliability Perspective of the Smart Grid." *IEEE Trans. Smart Grid* 1.1 (2010): 57-64.
[5]. Bhuyan, Monowar H., Dhruba Kumar Bhattacharyya, and Jugal Kumar Kalita. "Information metrics for low-rate DDoS attack detection: A comparative evaluation." Contemporary Computing (IC3), 2014 Seventh International Conference on. IEEE, 2014.
[6]. Anantvalee, Tiranuch, and Jie Wu."A survey on intrusion detection in mobile ad hoc networks." Wireless Network Security.Springer US, 2007.159-180.
[7]. Chhabra, Meghna, and B. B. Gupta. "An Efficient Scheme to Prevent DDoS Flooding Attacks in Mobile Ad-Hoc Network (MANET)." Research Journal of Applied Sciences, Engineering and Technology 7.10 (2014): 2033-2039.
[8]. Alqahtani, Sarra, and Rose Gamble."DDoS Attacks in Service Clouds."System Sciences (HICSS), 2015 48th Hawaii International Conference on.IEEE, 2015.
[9]. Jae-Hyun Jun, Hyunju Oh, andSung Kim."Real time detection and classification of DDoS attacks using Enhanced SVM with string kernels." Recent Trends in Information Technology (ICRTIT), 2015 International journals on. IEEE, 2015.
[10].Stallings, William. *Cryptography and network security: principles and practices*. Pearson Education India, 2006.
[11].Sanmorino, Ahmad, and SetiadiYazid. "Ddos attack detection method and mitigation using pattern of the flow." Information and Communication Technology (ICoICT), 2013 International Conference of.IEEE, 2013.