International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Mitigating Denial-of-Service and Distributed Denial-of-Service Attacks Using Server Hopping Model Using Distributed Firewall

Prajyoti P.Sabale[1], Anjali B.Raut[2]

[1]Department of Computer Science &Information Technology, HVPM COET, M.E. First year, Amravati, India

[2]Department of Computer Science, HVPM COET, Amravati, India

Abstract: ***Amongst various online attacks hampering IT security, Denial of Service (DoS) Distributed Denial-of-Service (DDoS) has the most devastating effects. It has also put tremendous pressure over the security experts lately, in bringing out effective defense solutions. These attacks could be implemented diversely with a variety of tools and codes. Since there is not a single solution for DoS, DDoS this attack has managed to prevail on internet for nearly a decade. Hence, it becomes indispensable to carry out these attacks in small test bed environments in order to understand them better. Unlike other theoretical studies, this project lays down the steps involved in implementing these attacks in real time networks. These real time attacks are measured and analyzed using network traffic monitors. The detection and mitigation mechanisms designed here are effective for small network topologies and can also be extended to analogous large domains. This paper deals with proactive models for mitigating DoS and DDoS attacks. In the first part of our investigation, we develop and evaluate two defense models for DoS and DDoS attacks: the Server Hopping Model using distributed firewalls. This model provide defense in a different part of the network, and has different resource requirements. In the second part of our investigation, we assess the effectiveness of our defense model for different types of DoS and DDoS attacks.***

Keywords: Denial-of-Service, Distributed Denial-of-Service, Server hopping

1. Introduction

There are many security threats that pose serious challenge towards the progress of IT economy. Amongst many attacks like Man in the Middle Attack, Session Hijacking, Cross site scripting, Spamming etc, Denial of Service is considered to be the most deadly weapon. In the year 2009, there were several series of Distributed Denial of Service attacks that were carried out against the US information systems and South Korea IT databases. The Internet was initially designed for openness and scalability. The infrastructure is certainly working as envisioned by that yardstick. However, the price of this success has been poor security. On the Internet, anyone can send any packet to anyone without being authenticated, while the receiver has to process any packet that arrives to a provided service. The lack of authentication means that attackers can create a fake identity, and send malicious traffic with impunity. All systems connected to the Internet are potential targets for attacks since the openness of the Internet makes them accessible to attack traffic [1] [2] [3] [7].

2. Classification of Attacks

DOS ATTACK: A DoS attack is a malicious attempt by a single person or a group of people to cause the victim, site, or node to deny service to its customers. When this attempt derives from a single host of the network, it constitutes a DoS attack. On the other hand, it is also possible that a lot of malicious hosts coordinate to flood the victim with an abundance of attack packets, so that the attack takes place simultaneously from multiple points. This type of attack is called a *Distributed DoS*, or DDoS attack.

Denial of Service (DoS) The main goal of the attack is the disruption of service. This can be reached by a variety of ways as we will see later. Intrusion Here the intention is simply to get access to a system and to circumvent certain barriers. People with such an intention meet the classic image of the old style hackers. Normally they try to reach their goal with-out doing severe damage and they inform the system administrator of the bugs found in the system. Information Theft Main goal of this kind of attacks is access to otherwise restricted, sensitive information. Modification Here the attacker actively tries to alter in-formation. DoS attacks are commonly launched from one or more points on the Internet that are external to the victim's own system or network. In many cases, the launch point consists of one or more systems that have been subverted by an intruder via a security-related compromise rather than from the intruder's own system or systems. As such, intrusion defense not only helps to protect Internet assets and the mission they support, but it also helps prevent the use of assets to attack other Internet-connected networks and systems. Likewise, regardless of how well defended your assets may be, your susceptibility to many types of attacks, particularly DoS attacks, depends on the state of security on the rest of the global Internet. Defending against DoS attacks is far from an exact or complete science. Rate limiting, packet filtering, and tweaking software parameters can, in some cases, help limit the impact of DoS attacks, but usually only at points where the DoS attack is consuming fewer resources than are available. In many cases, the only defense is a reactive one where the source or sources of an ongoing attack are identified and prevented from continuing the attack. The use of source IP address spoofing during attacks and the advent of distributed attack methods and tools have provided a constant challenge for those who must respond to DoS attack. against single targets, and multiple source attacks against multiple

targets. Today, the most common DoS attack type reported to the CERT/CC involves sending a large number of packets to a destination causing excessive amounts of endpoint, and possibly transit, network bandwidth to be consumed. Such attacks are commonly referred to as packet flooding attacks. Single source against single target attacks are common, as are multiple source against single target attacks. Based on reported activity, multiple target attacks are less common. The packet types used for packet flooding attacks have varied over time, but for the most part, several common packet types are still used by many DoS attack.

3. Types of DOS Attacks

There are several flavors of Denial of Service that could disrupt a normal service. The attacking methods are classified into two methods according to Erikson Jon [1]. First type would be to flood the network not leaving enough bandwidth for the legitimate packets to get through. This could also be termed as Flooding. The other method is to crash a hardware or software item and make it inoperable. Web servers, routing devices, DNS look up servers are the common targets that could be crashed during an attack. This project has investigated both the scenarios and has analyzed its effects. The DDoS paper published by Lee Garber talks about the mechanisms involved in some common attack types. Following are the most basic attacking methods employed so far [2].Early DoS attack technology involved simple tools that generated and sent packets from a single source aimed at a single destination. Over time, tools have evolved to execute single source attacks against multiple targets, multiple source attacks.

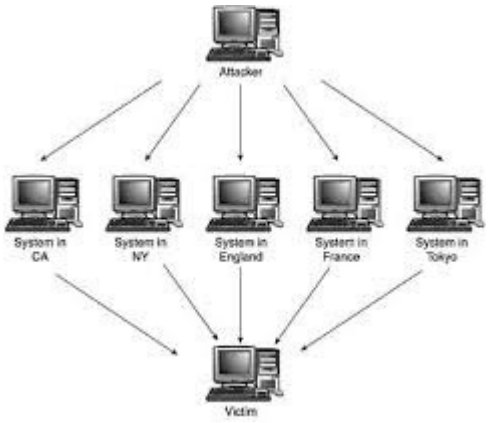


Figure 1: DOS Attack

Smurf Attack

The Smurf Attack is a denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP Broadcast address. Most devices on a network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, flooding the victim's computer with traffic. This can slow down the victim's computer to the point where it becomes impossible to work on.

Ping Flood and Ping of Death:

Ping flood is similar to Smurf wherein the victim is bombarded with thousands of ping packets. In Ping of death, the victim is sent corrupt packets that could crash the system [3].Smurf and ping floods are very easy to craft and any novice attacker could do it with ease. The following command in a Linux terminal could launch an attack [17]. There are enough effective defense mechanisms against Smurf and Ping attacks on the internet lately. However, these attacks could cause considerable damage in small Local Area Networks.

TCP SYN flood

SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic. Normally when a client attempts to start a TCP connection to a server, the client and server exchange a series of messages which normally runs like this:

1) The client requests a connection by sending a SYN (*synchronize*) message to the server.
2) The server *acknowledges* this request by sending SYN-ACK back to the client.
3) The client responds with an ACK, and the connection is established.

This is called the TCP three-way handshake, and is the foundation for every connection established using the TCP protocol. A SYN flood attack works by not responding to the server with the expected ACK code. The malicious client can either simply not send the expected ACK, or by spoofing the source IP address in the SYN, causing the server to send the SYN-ACK to a falsified IP address - which will not send an ACK because it "knows" that it never sent a SYN.

The server will wait for the acknowledgement for some time, as simple network congestion could also be the cause of the missing ACK, but in an attack increasingly large numbers of *half-open connections* will bind resources on the server until no new connections can be made, resulting in a denial of service to legitimate traffic. Some systems may also malfunction badly or even crash if other operating system functions are starved of resources in this way.

4. UDP Flood Attack

A UDP flood attack is a denial-of-service (DoS) attack using the User Datagram Protocol (UDP), a sessionless/connectionless computer networking protocol.

Using UDP for denial-of-service attacks is not as straightforward as with the Transmission Control Protocol (TCP). However, a UDP flood attack can be initiated by sending a large number of UDP packets to random ports on a remote host. As a result, the distant host will:

- Check for the application listening at that port;
- See that no application listens at that port;
- Reply with an ICMP Destination Unreachable packet.

Thus, for a large number of UDP packets, the victimized system will be forced into sending many ICMP packets, eventually leading it to be unreachable by other clients. The attacker(s) may also spoof the IP address of the UDP packets, ensuring that the excessive ICMP return packets do not reach them, and anonymizing their network location(s). Most operating systems mitigate this part of the attack by limiting the rate at which ICMP responses are sent.The software UDP Unicorn can be used for performing UDP flooding attacks. This attack can be managed by deploying firewalls at key points in a network to filter out unwanted network traffic. The potential victim never receives and never responds to the malicious UDP packets because the firewall stops them.

5. DDoSAttack

After analyzing existing DoS and DDoS attack defense techniques, we find that the major challenges of DoS and DDoS attack defense are how to identify the attack traffic accurately and efficiently, and how to locate attack sources and filter attack traffic close to the source.In Server hopping using Distributed Firewalls architecture the proxy server changes its location among a pool of servers to defend against unpredictable and likely DDoS attacks attempt to exhaust the victim's resources. These resources can be network bandwidth, computing power, or undetectable attacks. Only legitimate clients will be able to follow the server as it roams. The main strength of the mechanism lies in operating system data structures. To launch a DDoS attack, the simplification of both the detection and filtering of malicious malicious users first build a network of computers that they will use to produce the volume of traffic needed to deny services to computer users. To create this attack network, attackers discover vulnerable sites or hosts on the network. Vulnerable hosts are usually those that are either running no antivirus software or out- of-date antivirus software, or those that have not been properly patched. Vulnerable hosts are then exploited by attackers who use their vulnerability to gain access to these hosts. The next step for the intruder is to install new programs (known as *attack tools*) on the compromised hosts of the attack network. The hosts that are running these attack tools are known as *zombies*, and they can carry out any attack under the control of the attacker. Many zombies together form what we call an *army* attack packets. In this technique, the proxy server's location changes dynamically as a function of time and a cryptographic key shared between the server and the client. Authorized clients who have the key will be able to determine the current location used by the server, whereas the malicious users will not know the current location. The firewall can then easily filter off illegitimate packets by inspecting the headers.

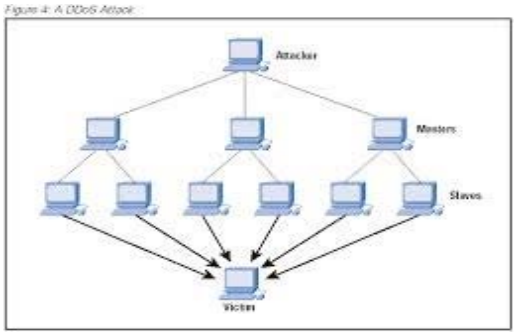


Figure 2: DDoS ATTACK

6. Server hopping using Distributed Firewalls

The effectiveness of the framework relies on how the legitimate clients know where the active server is and how we migrate the in-process connections as shown in Fig. 3.To be able to know the active server location, a client needs to have at least two sets of information: the server address and the time that the server will be active. hisinformation can be simply obtained by using a series of communication.

7. Architectural Design

Provides privacy and integrity to protect the information. The main issue is to provide a framework for moving one end point of a live connection from one location and reincarnate it at another location having a different IP address and/or a different port number.

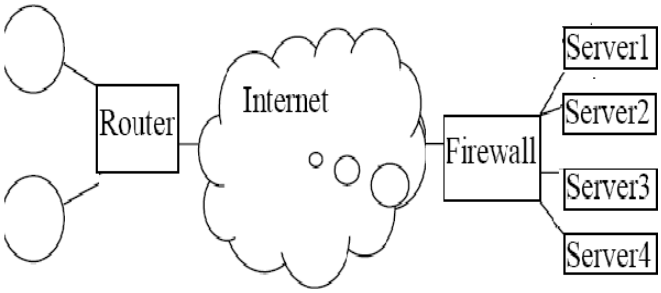


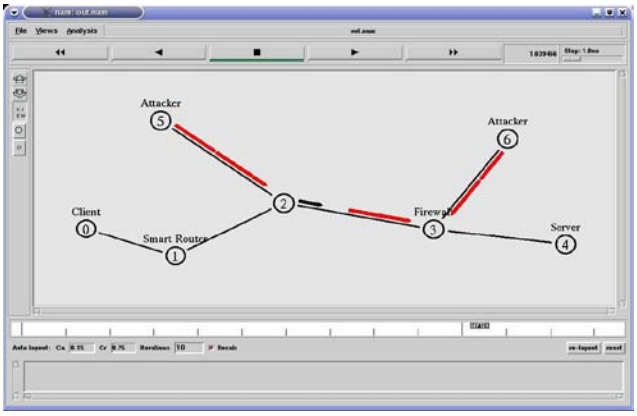
Figure 3: Server Hopping Architecture

The mechanism must deal with four issues:

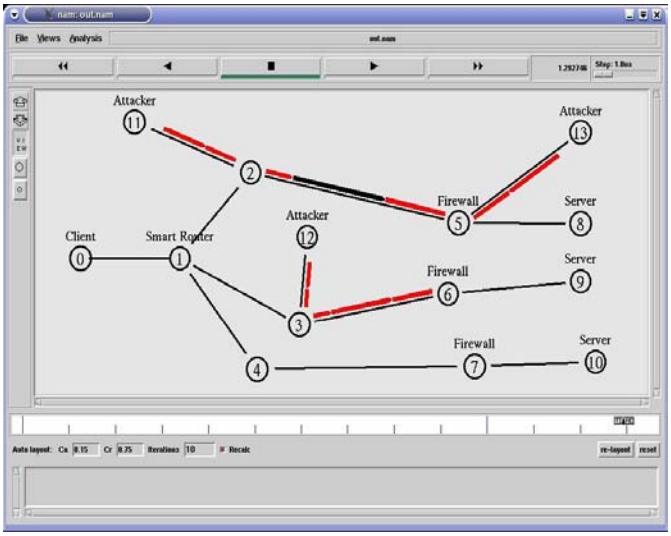
- How the connection is continued between the new end points
- Impact on the network stack and application layer in both the server and the client sides
- How to recover both connection and application states
- When to trigger the migration mechanism

8. Result

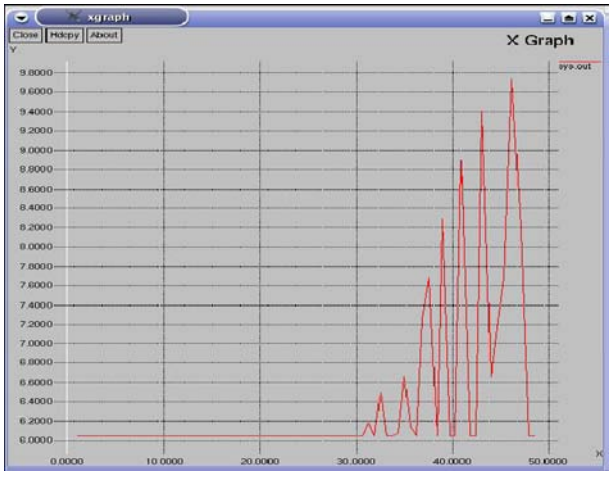
The following Fig. 4. represents the network used for simulating Server hopping architecture for DoS



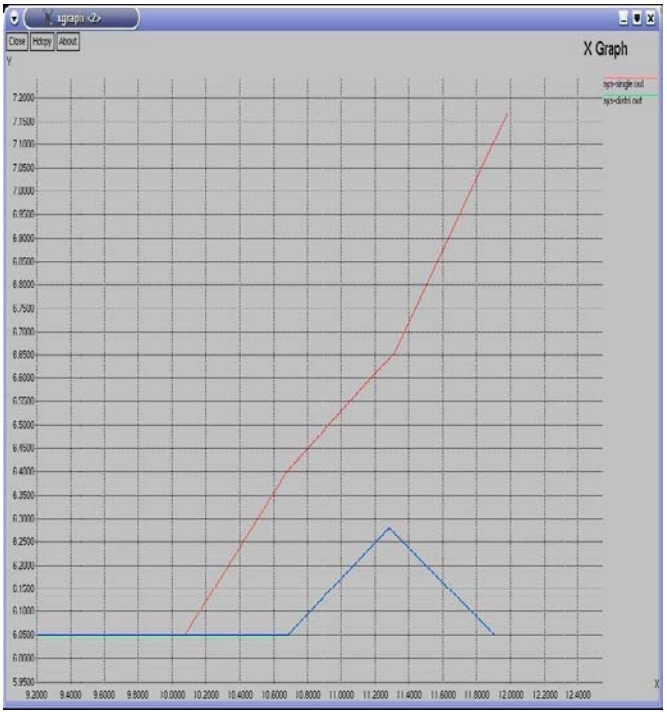
The following Fig. 5. represents the network used for simulating Server hopping architecture for DDoS



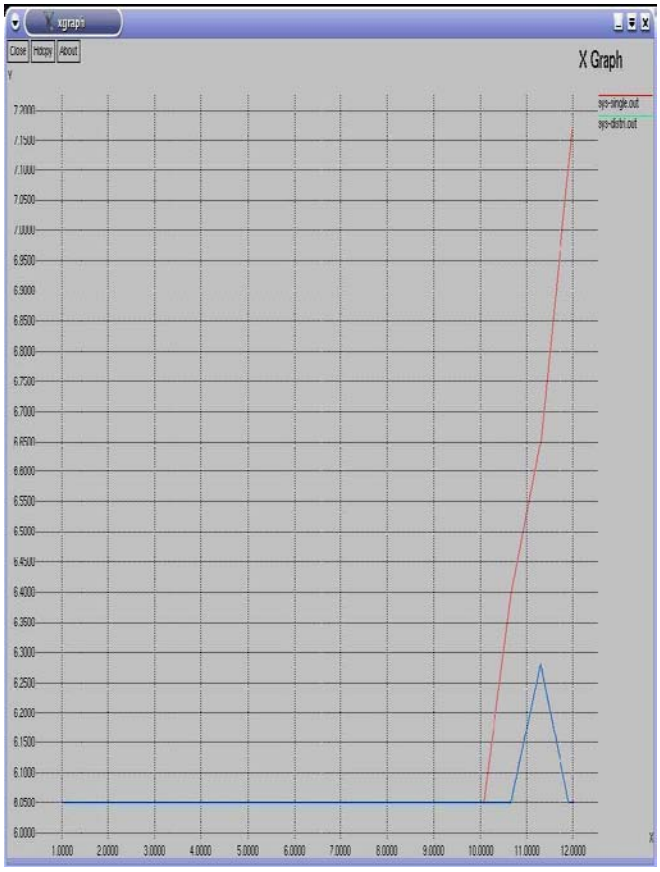
Graphs showing the effect of DoS attack .The following Fig. 6. represents analysis of DoS /DDoS attack without any defense models.



following Fig. 7. represents packet delivery time without DoS defense and with DoS defense for server hopping with distributed firewall architecture.



The following Fig. 8. represents the packet delivery time without DDoS defense and with DDoS defense for Server Hopping architecture.



In the above figure X-axis represents the actual time when running the simulation and Y-axis shows the time taken by the sample packet to reach the server (destination). Simulation is started at 0.0000 and the DoS attack is started at 10.0000. After 10.0000 the attack decays the delivery time. During a normal simulation (i.e.without the DoS attack) it takes 6.000. As the attack begins, the delivery

time increases from 6.000 to infinity at an infinite time. The graph shown in Fig. 7, 8 and 9 depicts the packet delivery time variation between an attacked network and an active network. The upper line (red line) in respective Graph shows the constant increase in delivery time as the attack progresses. The lower line (blue line) in each graph shows the initial increase in packet delivery time when the attack has begun and the active node is registering the attack. As the attack progresses the smart routers can detect the attacking packets and eliminates them from the network. This results in downward slope of the graph. As time progresses the delivery time reaches close to the Actual delivery time with no attack. From the above experimental results plotted in the graph it is proved that the developed architectures for depending DoS and DDoS attacks maintains almost the same packet delivery time as the packet delivery time in the absence of DoS/DDoS attacks.

9. Conclusion

We have evaluated defense models for defending DoS/DDoS attacks. The models is Server Hopping using distributed firewalls model. The simulation results of DoS depicts that the packet delivery time without any defense models increases and the packet delivery to the server will be delayed. In SOS defense model for DoS and DDoS the variation in packet delivery time remains almost constant with the actual packet delivery time. The server hopping model maintains the constant packet delivery time. Server hopping architectures we have developed provide a range of defenses that can severely limit the damage caused by DoS and DDoS attacks. This is a significant step forward in providing a robust Internet service that can be used with confidence for electronic commerce and other on-line services.

10. Acknowledgement

This paper has benefited from conversations with many different people – far more than can be acknowledged completely here. Still we would like to particularly thank, HOD of CS&IT department for his support guidance and support.

References

[1] Angelos Keromytis, Vishal Misra, Dan Rubenstein, Architecture for Mitigating DDoS Attacks, IEEE 2003
[2] Chatree Sangpachatanaruk, Sherif M. Khattaby, Taieb Znatiy, Rami Melhemy Daniel Mossey, A Simulation Study of the Proactive Server Roaming, IEEE 2003
[3] M. Eyrich, A. Hess, G. Sch¨afer, L. Wartenberg, Distributed Denial of Service Protection Framework, IEEE 2002
[4] Tao Peng, Defending Against Distributed Denial of Service Attacks , 2002
[5] Najwa Aaraj, Sleiman Itani, and Darine Abdelahad, Neighbor Stranger Discrimination 2003
[6] Tanachaiwiwat, S. and Hwang, K. “Differential packet filtering against DDoS flood attacks.” ACM Conference on Computer and Communications Security (CCS). Washington, DC, October 2003. M. Robinson, J. Mirkovic, M. Schnaider, S Michel, and P.Reiher. “Challenges and principles of DDoS defense.” SIGCOMM 2003.
[7] Zhang, S. and Dasgupta, P. “Denying denial-of service attacks: a router based solution.”International Conference on Internet Computing, June 2003
[8] Nagesh H.R, K. Chandra Sekaran “Design and Development of proactive solutions for mitigating denial-of-service attacks”, Proceedings of the 14th International Conference on Advanced Computing and Communications, IEEE Press, India, Dec. 2006, pp. 157-162.
[9] Nagesh H.R, K. Chandra Sekaran “Proactive solutions for mitigating denial-of-service attacks”, Proceedings of the International Conference on Information Security and Computer Forensics, Chennai, India, Dec. 2006, pp. 109-116.
[10] Nagesh H.R, K. Chandra Sekaran “Proactive model for mitigating denial-of-service attacks”, Proceedings of 4th International Conference on Information Technology: New Generations, IEEE Computer Society Press, USA, April 2007.