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.

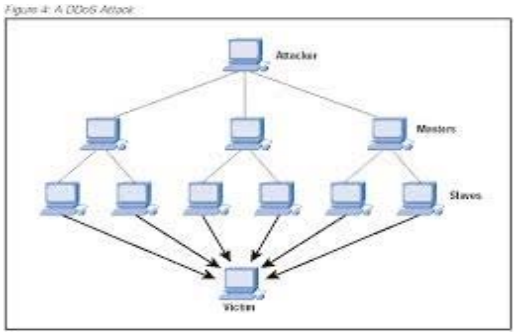


Figure 2: DDoS ATTACK

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.

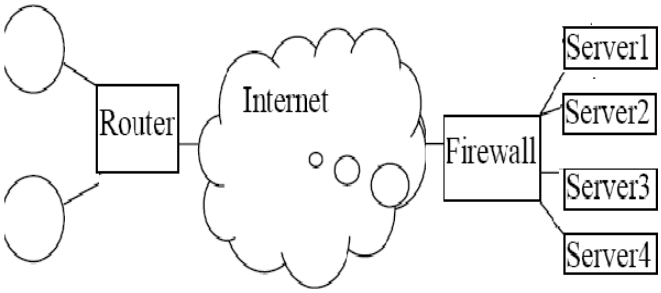


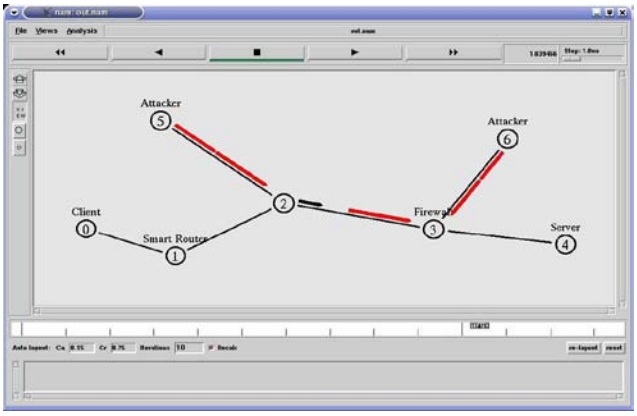
Figure 3: Server Hopping Architecture

The mechanism must deal with four issues:

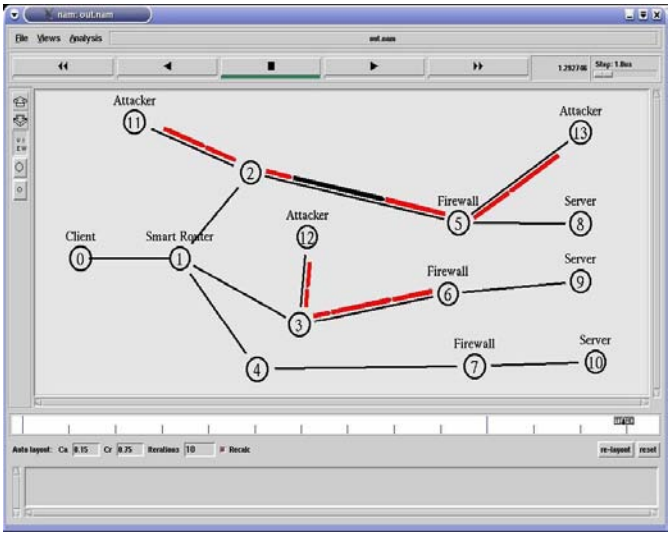
- How the connection is continued between the new end points
- Impact on the network stack and application layer in both the server and the client sides
- How to recover both connection and application states
- When to trigger the migration mechanism

8. Result

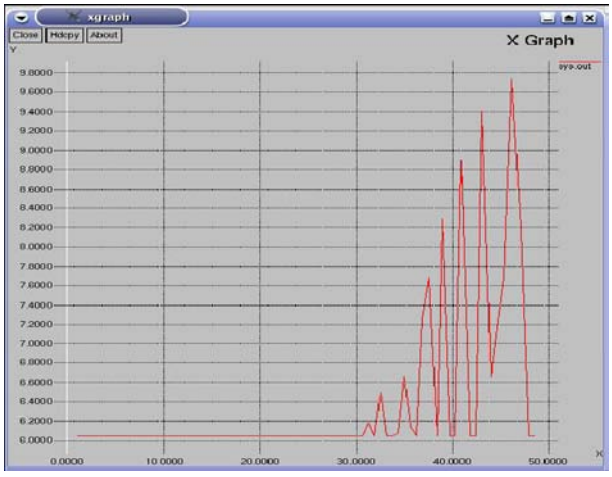
The following Fig. 4. represents the network used for simulating Server hopping architecture for DoS



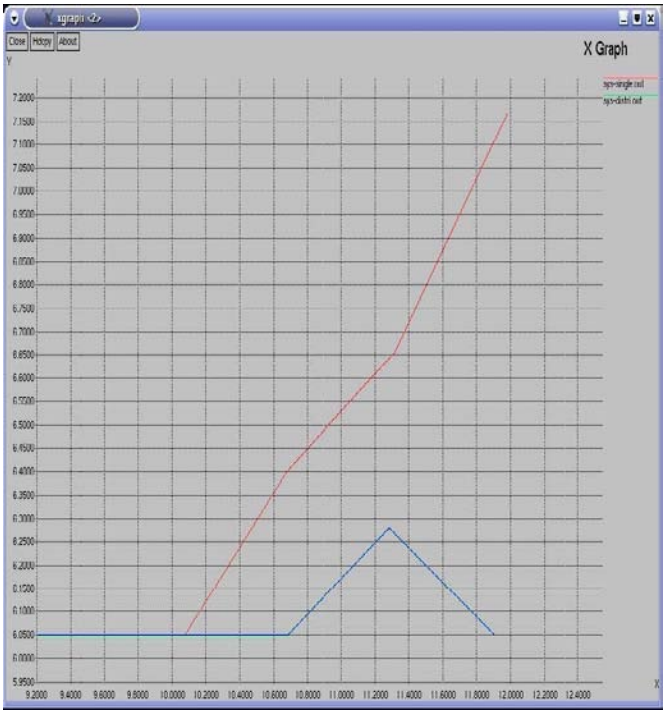
The following Fig. 5. represents the network used for simulating Server hopping architecture for DDoS



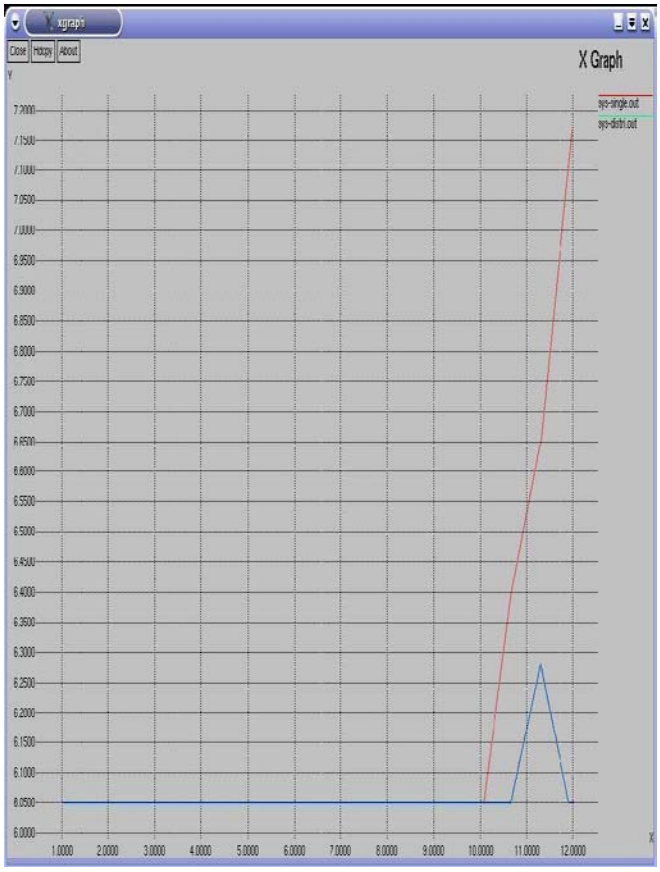
Graphs showing the effect of DoS attack .The following Fig. 6. represents analysis of DoS /DDoS attack without any defense models.



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.