Design and Development of Proactive Models for Mitigating Denial-of-Service and Distributed Denial-of-Service Attacks

Nagesh H.R[†], *K. Chandra Sekaran*[††]

[†]*Department of Computer Engineering, P.A. College of Engineering, Mangalore, Karnataka, INDIA*
[††]*Department of Computer Engineering, National Institute of Technology Karnataka, Surathkal, Karnataka, INDIA*

Summary
Denial-of-Service (DoS) attacks, orchestrated by a single host or multiple hosts in a coordinated manner, have become an increasingly frequent disturbance in today's Internet. Generally, attackers launch Distributed Denial-of-Service (DDoS) attacks by directing a massive number of attack sources to send useless traffic to the victim. The victim's services are disrupted when its host or network resources are occupied by the attack traffic. The threat of DDoS attacks has become even more severe as attackers can compromise a huge number of computers using vulnerabilities in popular operating systems. 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 *Secure Overlay Services (*SOS) Model and the *Server Hopping* Model using distributed firewalls. Each of these models 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 models for different types of DoS and DDoS attacks.

Key words:
Denial-of-Service, Secure Overlay Service, Distributed Denial-of-Service, Server hopping.

1. Introduction

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].

1.1 Denial-of- Service (DoS) Attacks

A DoS attack is a malicious attempt by a single person or a group of people to disrupt an online service. DoS attacks can be launched against both services, e.g., a web server, and networks, e.g., the network connection to a server. The impact of DoS attacks can vary from minor inconvenience to users of a website, to serious financial losses for companies that rely on their on-line availability to do business. As emergency and essential services become reliant on the Internet as part of their communication infrastructure, the consequences of DoS attacks could even become life-threatening. Hence, it is crucial to deter, or otherwise minimize, the damage caused by DoS attacks [1] [2] [3] [7].

Types of DoS attacks

- TCP SYN Flood Attack
- UDP Flood Attacks
- Ping of Death Attacks
- Smurf Attacks
- Teardrop Attacks
- Bonk Attacks
- Land Attacks

1.2 Distributed Denial of Service (DDoS) Attacks

When an attacker attacks from multiple source systems, it is called a *Distributed Denial of Service (DDoS) attack.* If the attacker is able to organize a large amount of users to connect to the same website at the same time, the web server, often configured to allow a maximum number of client connections, will deny further connections. Hence, a denial of service will occur. This is a common method used by 'Hacktivists'.

However, the attacker typically does not own these computers. The actual owners are usually not aware of their system being used in a DDoS attack. The attacker usually distributes *Trojan Horses* that contain malicious

code that allows the attacker to control their system. Such malicious code is also referred to as a *Backdoor*. Once these Trojan Horses are executed, they may use email to inform the attacker that the system can be remotely controlled. The attacker will then install the tools required to perform the attack. Once the attacker controls enough systems, which are referred to as *zombies* or *slaves*, he or she can launch the attack.

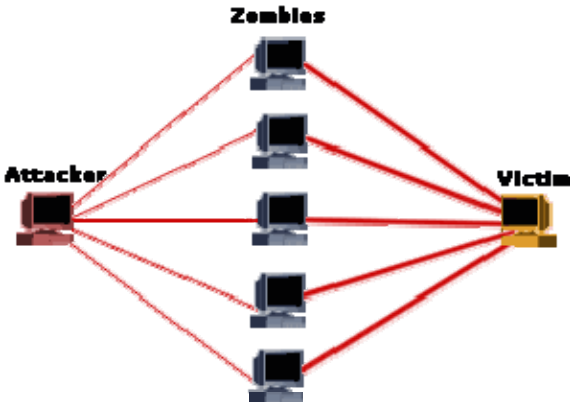

Fig. 1 DDoS Attack

In most cases, it is difficult or even impossible to prevent DDoS attacks entirely. Some routers, firewalls, and IDSs are able to detect DoS attacks and block suspicious connections to prevent a service from being overloaded. When you are the victim of an ongoing DDoS attack, you should contact your ISP to block the IP addresses that seem to be the source of the attack. However, the attacker may forge the source addresses, making it very difficult to trace the actual source(s) of the attack without extensive cooperation of your ISP [11].

A DoS attack aims to stop the service provided by a target. It can be launched in two forms. The first form is to exploit software vulnerabilities of a target by sending malformed packets and crash the system. The second form is to use massive volumes of useless traffic to occupy all the resources that could service legitimate traffic. While it is possible to protect the first form of attack by patching known vulnerabilities, the second form of attack cannot be so easily prevented. The targets can be attacked simply because they are connected to the public Internet. When the traffic of a DoS attack comes from multiple sources, we call it a Distributed Denial of Service (DDoS) attack. By using multiple attack sources, the power of a DDoS attack is amplified and the problem of defense is made more complicated.

The objective of DoS research is to develop practical and scalable mechanisms to detect and react to DoS attacks. These defense mechanisms should detect the DoS attack quickly and accurately, ensure reasonable performance for the networks or systems under attack, and track the attack sources accurately with low computational overhead.

2. Design

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 the SOS architecture we address the problem of securing communication in today's existing IP infrastructure from DoS and DDoS attacks, where the communication is between a pre-determined location and a set of well-known users, located anywhere in the wide-area network, who have authorization to communicate with that location. We focus our efforts on protecting a site that stores information that is difficult to replicate due to security concerns or due to its dynamic nature.

In Server hopping using Distributed Firewalls architecture the proxy server changes its location among a pool of servers to defend against unpredictable and likely undetectable attacks. Only legitimate clients will be able to follow the server as it roams. The main strength of the mechanism lies in the simplification of both the detection and filtering of malicious 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.

2.1 Secure Overlay Services (SOS)

The architecture uses a combination of routing via consistent hashing, and filtering. The forwarding of a packet within the SOS architecture, depicted in Fig. 2. proceeds through five stages [1] [2] [3] [4]:

- A source point that is the origin of the traffic forwards a packet to a special overlay node called a SOAP that receives and verifies that the source point has a legitimate communication for the target.
- The SOAP routes the packet to a special node in the SOS architecture that is easily reached, called the beacon.
- The beacon forwards the packet to a "secret" node, called the secret servlet, whose identity is known to only a small subset of participants in the SOS architecture.
- The secret servlet forwards the packet to the target.

- The filter around the target stops all traffic from reaching the target except for traffic that is forwarded from a point whose IP address is the secret servlet.

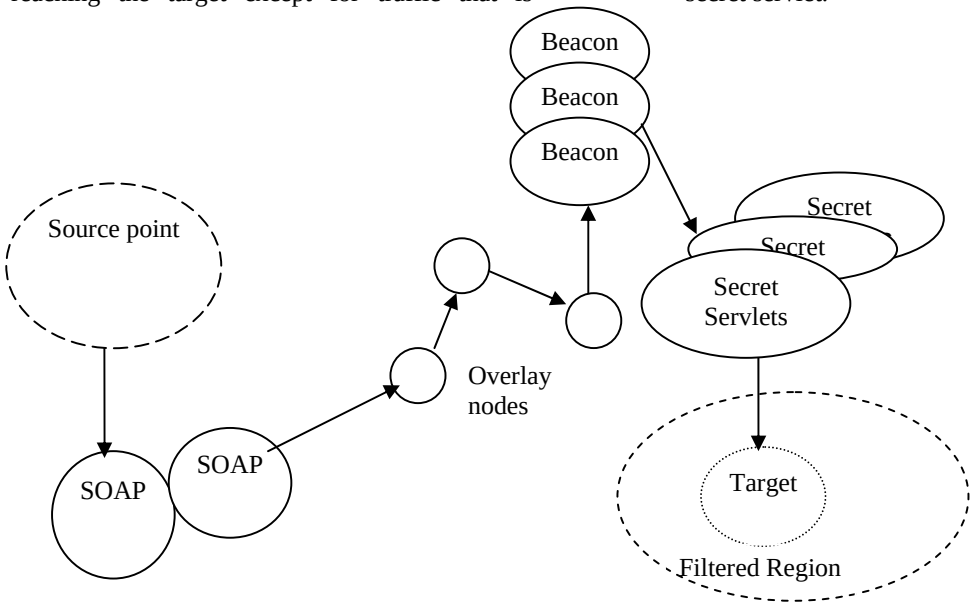

Fig. 2 Secure Overlay Services architecture

2.2 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. This information can be simply obtained by using a series of communication. To avoid the DoS attacks on the Internet, however, clients and servers need a secure communication that 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. 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.

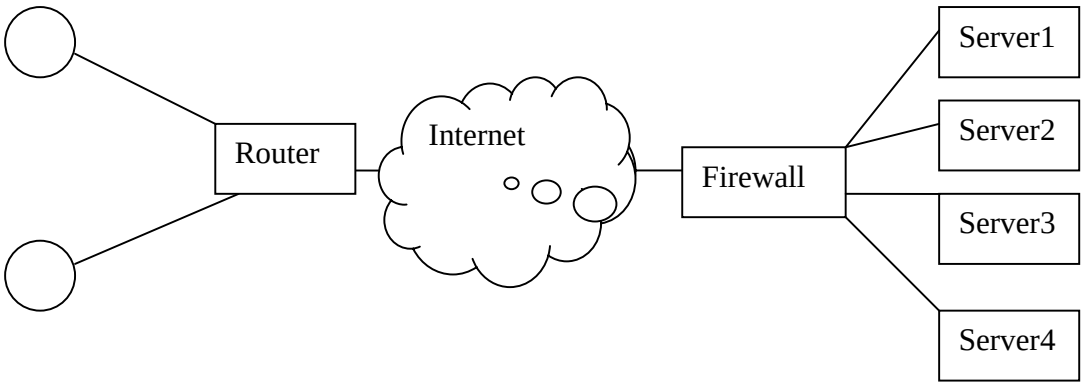

Fig. 3 Server Hopping Architecture

3. Experiments/Simulations, Results and Discussion

3.1 Simulations carried out

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

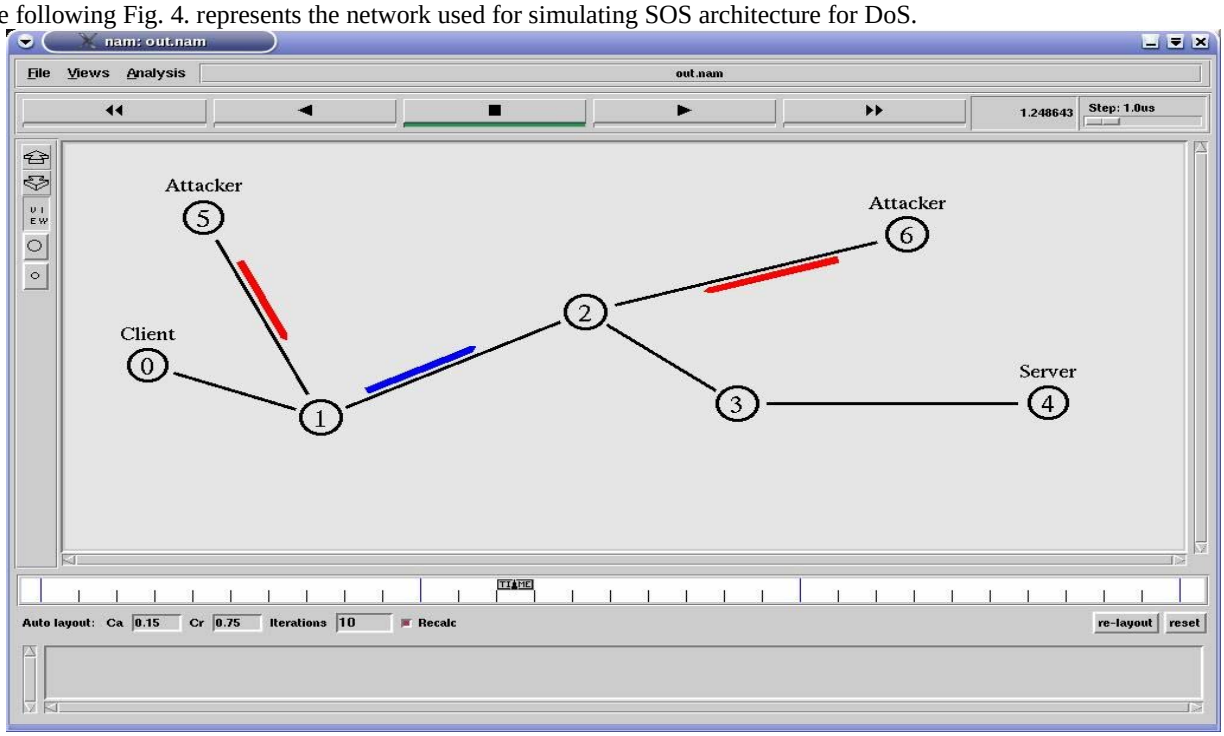

Fig. 4 Network used for simulating SOS architecture for DoS

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

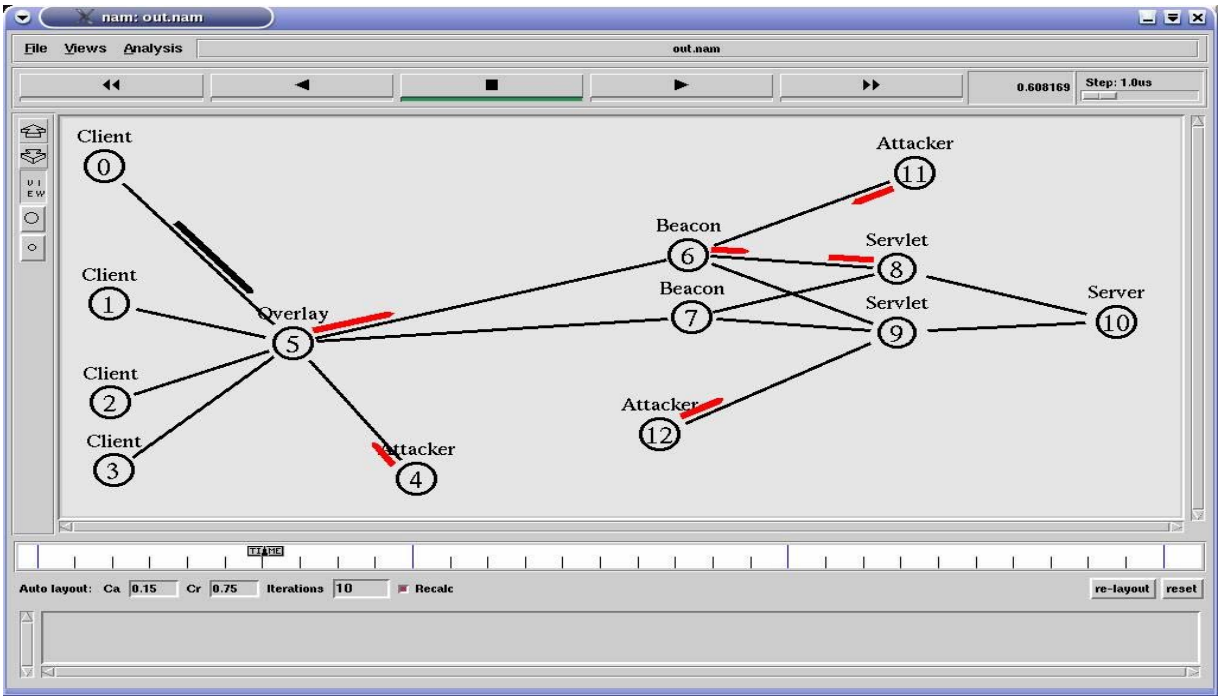

Fig. 5 Network used for simulating SOS architecture for DDoS

The following Fig. 6. represents the network used for simulating Server hopping architecture for DoS

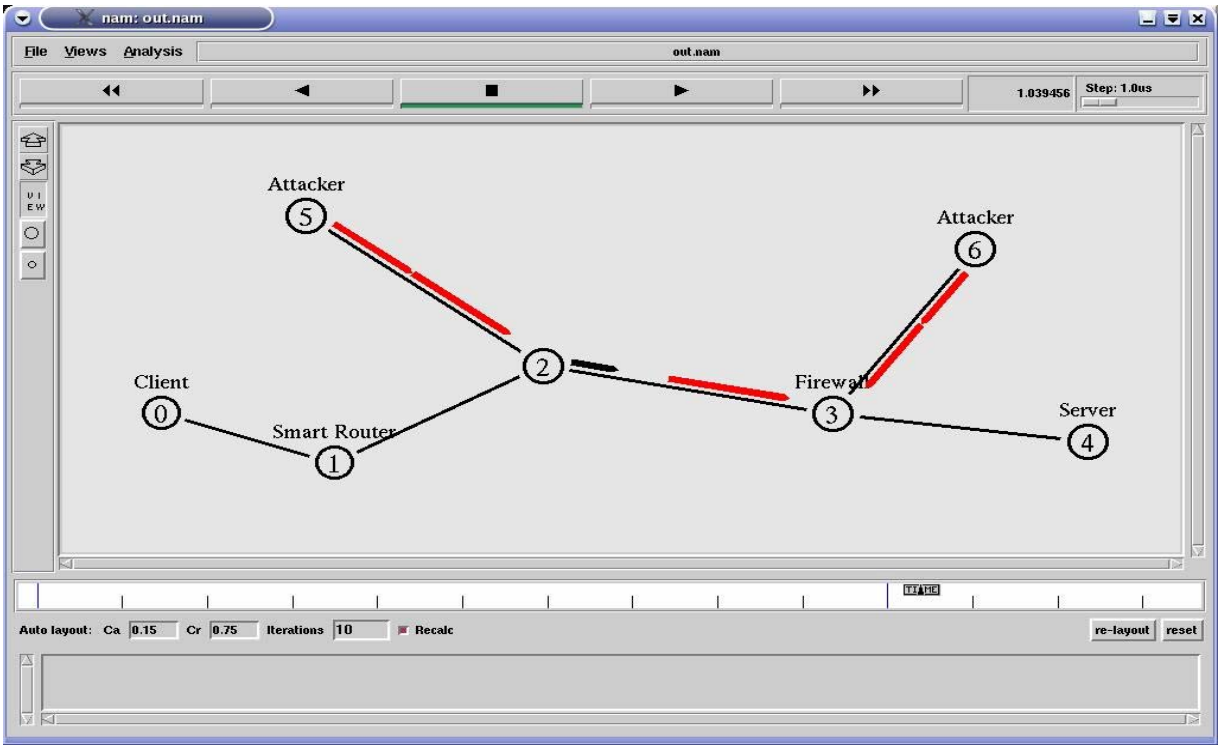

Fig. 6 Network used for simulating Server hopping architecture for DoS

The following Fig. 7. represents the network used for simulating Server hopping architecture for DDoS

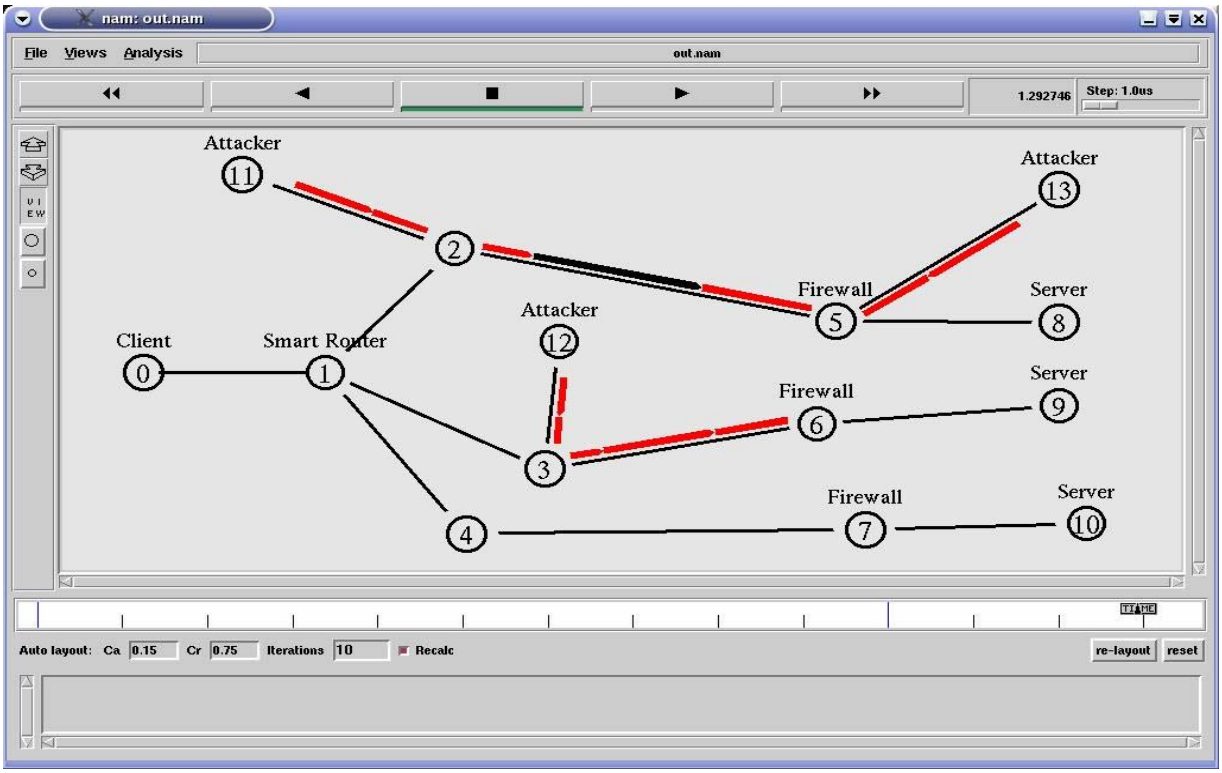

Fig. 7 Network used for simulating Server hopping architecture for DDoS

3.2 Graphs showing the effect of DoS attack

The following Fig. 8. represents analysis of DoS /DDoS attack without any defense models.

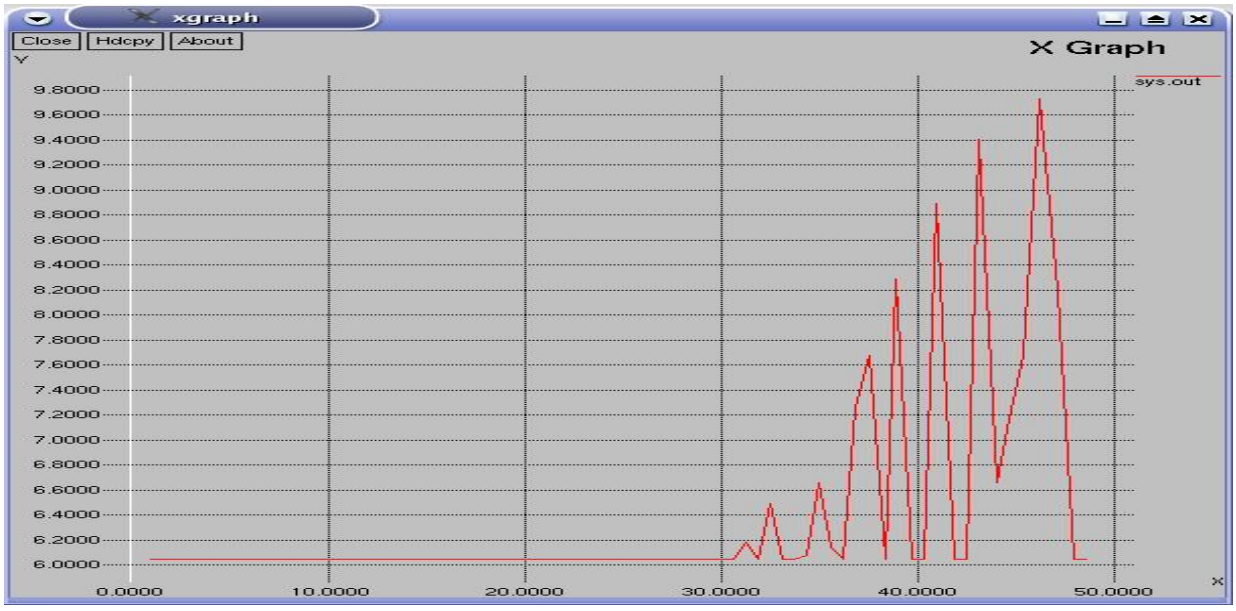

Fig. 8 Analysis of DoS

The following Fig. 9. represents packet delivery time without DoS defense and with DoS defense for SOS architecture.

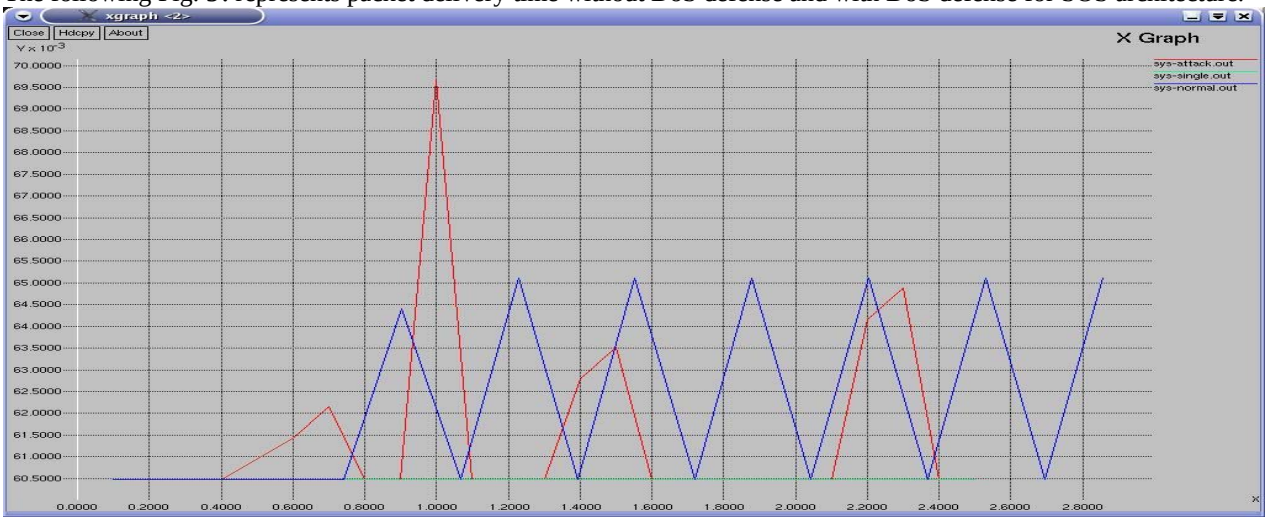

Fig. 9 Packet delivery time without DoS defense and with DoS defense for SOS

The following Fig. 10. represents packet delivery time without DoS defense and with DoS defense for server hopping with distributed firewall architecture.

Fig. 10 Packet delivery time without DoS defense and with DoS defense for Server Hopping

The following Fig. 11. represents the packet delivery time without DDoS defense and with DDoS defense for Server Hopping architecture.

Fig. 11 Packet delivery time without DDoS defense and with DDoS defense for Server Hopping

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 packet 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. 9, 10 and 11 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.

4. Conclusion

We have developed and evaluated two defense models for defending DoS/DDoS attacks. The models are *Secure Overlay Services (*SOS) model and Server Hopping using distributed firewalls model. Each of these models provide defense in a different part of the network, and has different resource requirements. 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 also maintains the constant packet delivery time. But the amount of variation in packet delivery time in SOS is more when compared to server hopping using distributed firewalls model. Through simple analytical models it is identified that DoS attacks directed against any part of the SOS infrastructure have negligible probability of disrupting the communication between two parties due to constant packet delivery time. Furthermore, the resistance of a SOS network against DoS attacks increases greatly with the number of nodes that participate in the overlay.

The SOS and 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.

Acknowledgement

The authors wish to thank the anonymous reviewers for their constructive comments.

References

[1] 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.

[2] 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.

[3] 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.

[4] Angelos Keromytis, Vishal Misra, Dan Rubenstein, Architecture for Mitigating DDoS Attacks, IEEE 2003

[5] Chatree Sangpachatanaruk, Sherif M. Khattaby, Taieb Znatiy, Rami Melhemy Daniel Mossey, A Simulation Study of the Proactive Server Roaming, IEEE 2003

[6] M. Eyrich, A. Hess, G. Sch¨afer, L. Wartenberg, Distributed Denial of Service Protection Framework, IEEE 2002

[7] Tao Peng, Defending Against Distributed Denial of Service Attacks , 2002

[8] Najwa Aaaraj, Sleiman Itani, and Darine Abdelahad , Neighbor Stranger Discrimination 2003

[9] Tanachaiwiwat, S. and Hwang, K. "Differential packet filtering against DDoS flood attacks." ACM Conference on Computer and Communications Security (CCS). Washington, DC, October 2003.

[10] M. Robinson, J. Mirkovic, M. Schnaider, S Michel, and P. Reiher. "Challenges and principles of DDoS defense." SIGCOMM 2003.

[11] Zhang, S. and Dasgupta, P. "Denying denial-of service attacks: a router based solution."International Conference on Internet Computing, June 2003

Biography:

Nagesh H.R received the B.E. and M.Tech. degrees, from Mangalore Univ. in 1996 and 2002, respectively. After working as a lecturer (from 1996), an assistant professor (from 2003) in the Dept. of Computer Science and Engineering, the NMAM Institute of Technology, and an associate professor (from 2005) , a Professor (from 2007) in the Dept. of Computer Science and Engineering , the P.A. College of Engineering., India. His research interest includes computer networks, cryptography, network security and distributed computing. He has published more than 20 publications in International and National proceedings.

K.Chandra Sekaran is a Professor of Computer Engineering at National Institute of Technology Karnataka, India. His research includes Computer Networks, Dependable Network / Distributed computing, Autonomic computing and Community Informatics. He has 20 years of teaching and research and one year Industry experience. He has published more than 86 publications in International and National proceedings and authored two books. He was the Organizing Chair of 14th International Conference ADCOM 2006, International Symposium on Ad Hoc and Ubiquitous Computing ISAHUC'06. He also served as a member of PC in various International conferences, reviewer in many Journals. He has supervised sponsored projects and IT consultant to some corporates in this region of India.