Design and Development of Proactive Solutions for Mitigating Denial-of-Service Attacks

#Nagesh H.R[1], K. Chandra Sekaran[2]

[1]*Department of Computer Engineering*
P.A. College of Engineering, Mangalore, Karnataka, INDIA
Email: hrnagesh2001@rediffmail.com

[2]*Department of Computer Engineering*
National Institute of Technology Karnataka, Surathkal, Karnataka, INDIA
Email: kch@nitk.ac.in

ABSTRACT

Denial of Service attacks, orchestrated by a single host or multiple hosts in a coordinated manner, has become an increasingly frequent disturbance in today's Internet. Generally, attackers launch 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 [4].This paper deals with Denial of service (DoS) and Distributed DoS (DDoS) attacks. In the first part, we categorize existing defense mechanisms, and analyze their strengths and weaknesses. In the second part of our investigation, we develop and evaluate two defense models for DoS 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 third part of our investigation, we assess the effectiveness of our defense models for different types of DoS attack.

KEYWORDS
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 [4].

A. 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 [4].

Types of DoS attacks

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

B. 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.

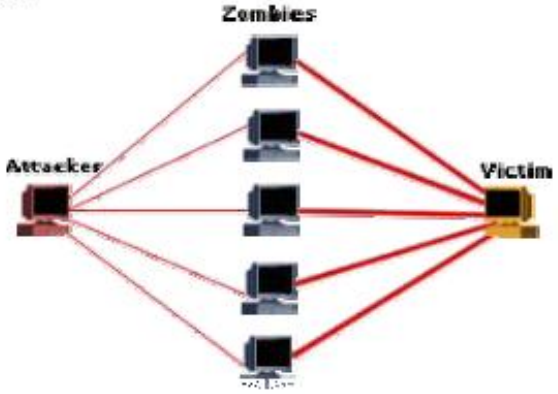

Figure 3 DDoS Attack

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 [8].

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 Denial-of-Service (DoS) attack defense techniques, we find that the major challenges of DoS 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 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 attacks 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.

A. 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]:

- 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.

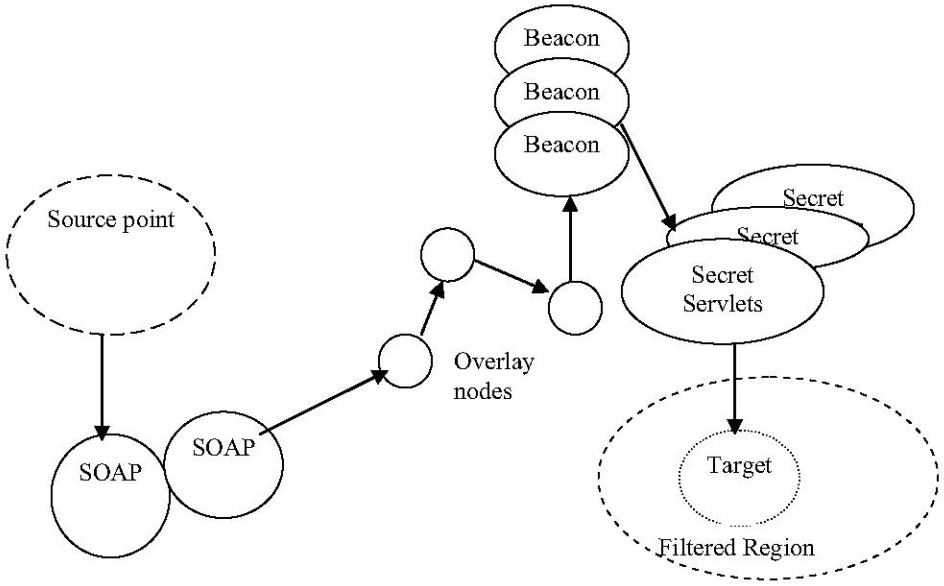

Figure 2 Secure Overlay Services architecture

B. 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 the framework for moving one end point of a live connection from one location and reincarnating 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.

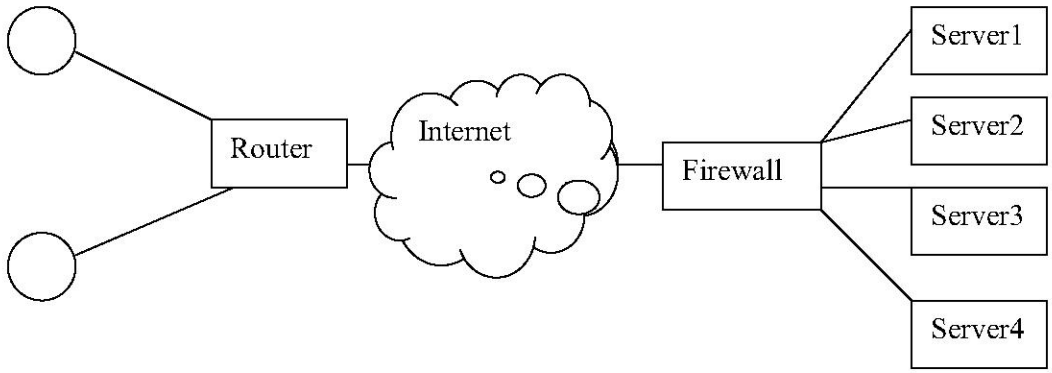

Figure 3 Server Hopping Architecture

3. SIMULATIONS CARRIED OUT

A simple network before DDoS attack is as shown in Fig. 4.

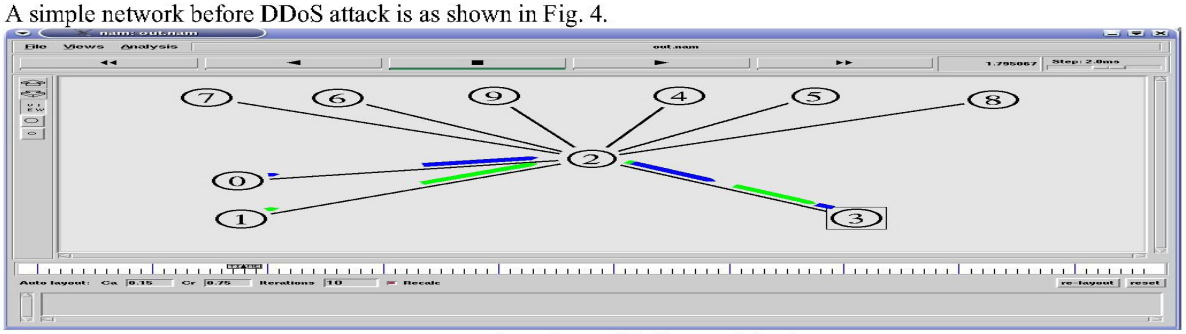

Figure 4 Network before DDoS Attack

Nodes 0,1 are legitimate nodes communicating with server node 3. Node 2 is the router being compromised. In the simulation we use a TCP CBR traffic generator. The node 0 and 1 send packets to node 3 at regular intervals. The queue stack of the router node 2 is set to allow only legitimate traffic i.e. from node 0 and 1. The node 3 is a TCPSink, which accepts all traffic. Acknowledgements may be included. In The network during DDoS attack is as shown in Fig. 5.

this simulation acknowledgements are not included since our aim is to demonstrate damage done by zombies in one direction only. Nodes 4, 5, 6, 7,8and 9 are zombie nodes. They are compromised nodes, which act as slaves to a central event for e.g. particular dates or actions by user. When the zombies are activated they collectively attack the target node.

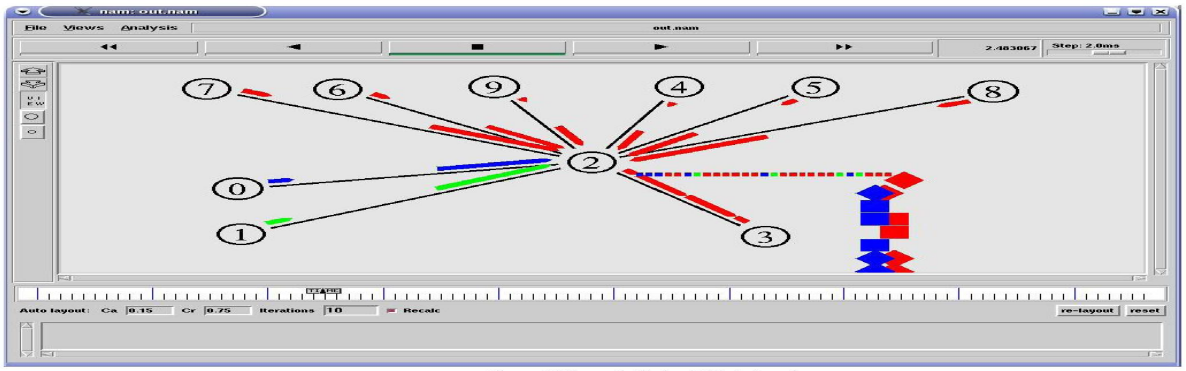

Figure 5 Network during DDoS Attack

- Nodes 4, 5, 6, 7, 8 and 9 are zombie nodes, which attack router node 2.
- The DDoS attack causes the link 2-3 to overflow. This leads to packet losses as shown in Fig. 5
- The density of attack determines amount of legitimate packet loss.

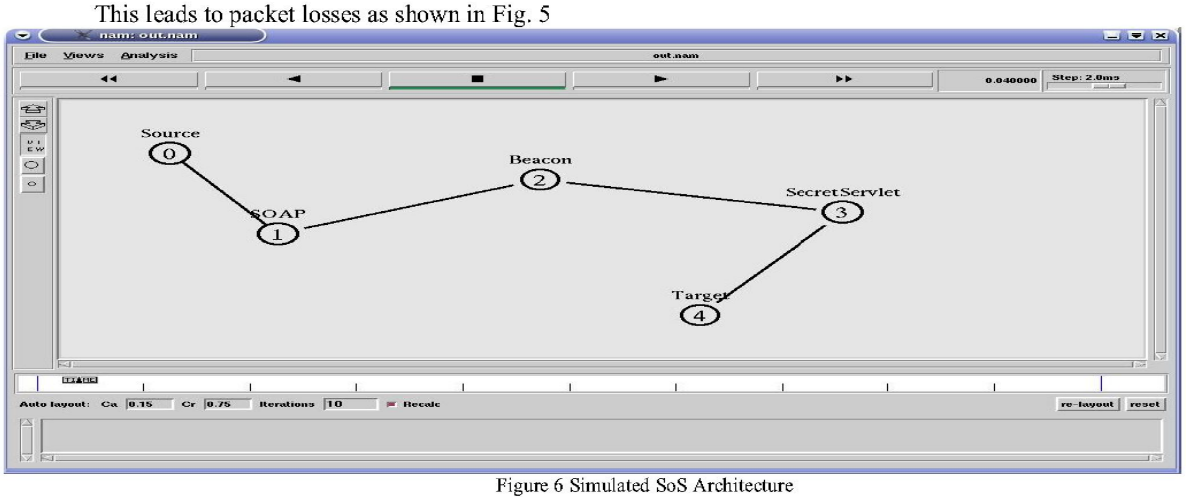

Figure 6 Simulated SoS Architecture

The packet movement follows the path: Source → SOAP → Beacon → SecretServlet → Target. The Server hopping architecture is simulated using the network shown in the Fig. 7.

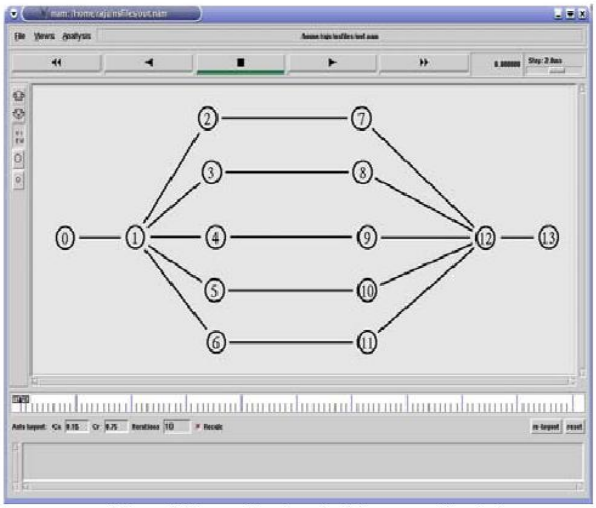

Figure 7 Server Hopping Architecture - Simulation

The packet movement is as follows: Source → Router → Firewalls → Target as shown in Fig. 8.

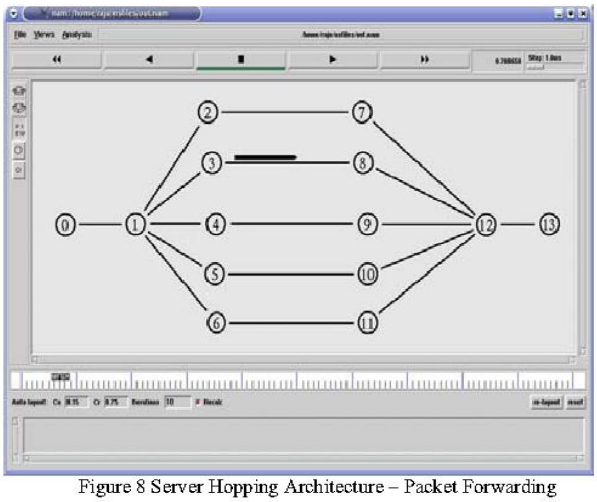

Figure 8 Server Hopping Architecture – Packet Forwarding

4. RESULTS

The following Fig. 9 shows the simulation results of SoS, which depict time at each point.

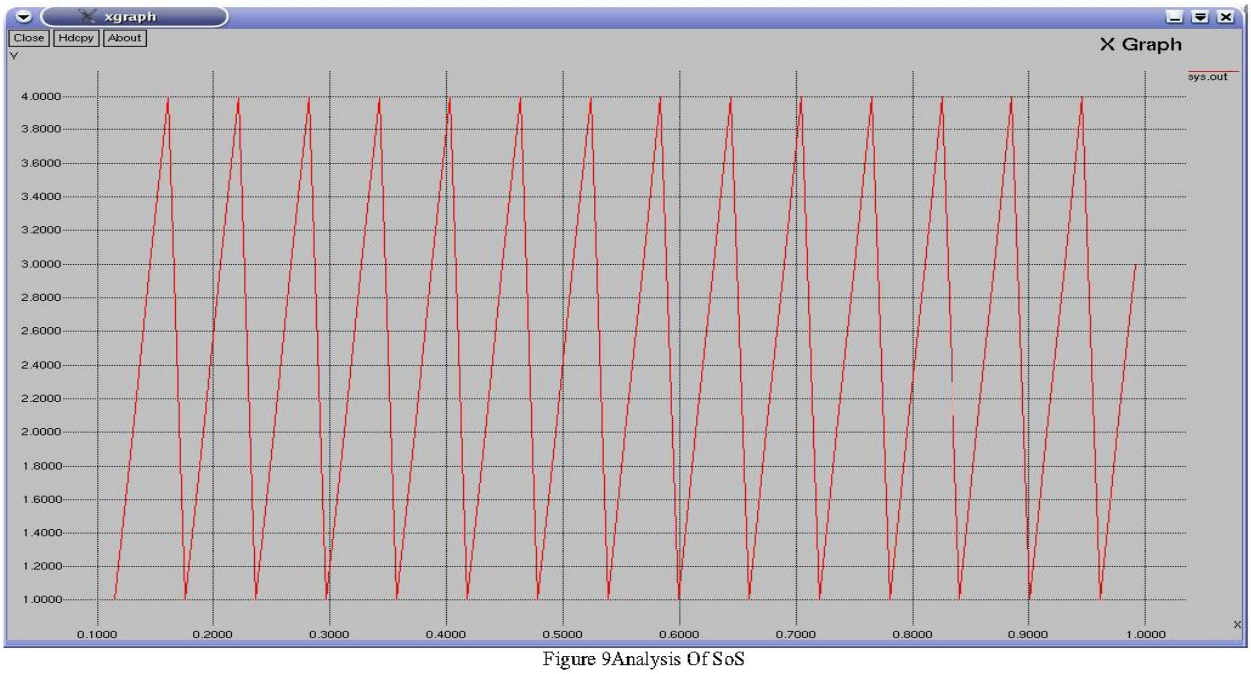

Figure 9Analysis Of SoS

Through simple analytical models we show that DoS attacks directed against any part of the SOS infrastructure have negligible probability of disrupting the communication between two parties: for instance, when only ten nodes act as beacons, ten nodes act as secret servlets, and ten nodes act as access points, for an attack to be successful in one out of ten thousand attempts, approximately forty percent of the nodes in the overlay must be attacked simultaneously. Furthermore, the resistance of a SOS network against DoS attacks increases greatly with the number of nodes that participate in the overlay. The server selected at each time instant is shown in Fig. 10 (using modulo as hash function)

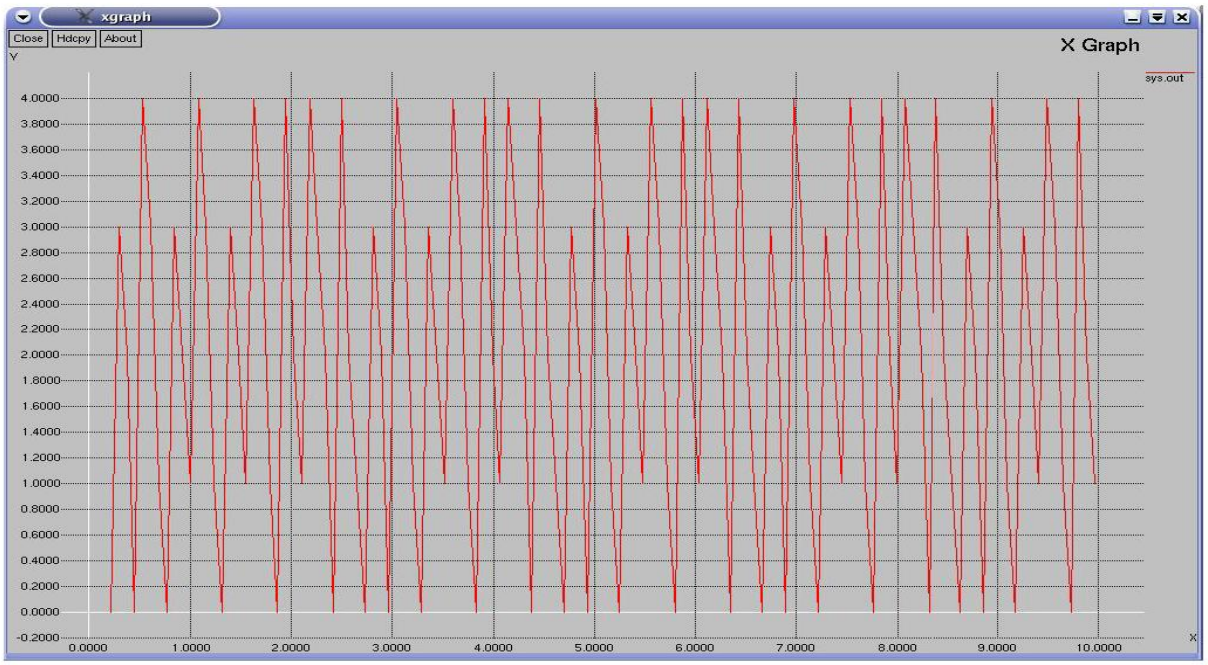

Figure 10 Analysis of Server Hopping

The benefit of the server roaming outweighs the cost of the roaming and the loss caused by the attacks. The migrating connections from the attacked server to a non-attacked server increase the opportunity for the transfers to be completed a lot quicker than leaving them with the stalled server.

5. CONCLUSIONS

Distributed denial-of service is a grave problem that requires a complex solution. Distributed denial-of-service requires a distributed solution. The architectures present a crucial building block of this solution by implementing systems that provide a selective and dynamic response.

We believe that our approach is a novel way of countering DoS attacks, especially in service-critical environments. It provides good service to legitimate traffic during the attack, which is the ultimate goal of DDoS defense.

The contribution of these architectures provides a range of defenses that can severely limit the damage caused by DoS attacks. This itself 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.

ACKNOWLEDGMENT

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

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.

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

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