BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **11**, No 4

Sofia • 2011

MAC Based Routing Table Approach to Detect and Prevent DDoS Attacks and Flash Crowds in VoIP Networks

N. Jeyanthi[1], *N.Ch. Sriman, Narayana Iyengar*[2]

[1] *School of Information Technology and Engineering*
[2] *School of Computing Science and Engineering,*
VIT University, Vellore, Tamilnadu – 632014, India
Email: njeyanthi@vit.ac.in

***Abstract*:** *The Hype Cycles for Consumer Technologies announced that the level of "Slope of Enlightenment" was achieved by Voice over Internet Protocol (VoIP) in 2007. This stable growth rate expects that the level of "Plateau of productivity" will be achieved in the forthcoming years. While marching towards the exponential growth by balancing other promoting technologies, security becomes the pressing factor. VoIP should not compromise for security which may depreciate its growth rate. Since the rate of the users using VoIP services increases more than the expected, it is vulnerable to all types of attacks that Internet is now facing.*

The approach proposed includes a new framework, with which the Distributed Denial of Service (DDoS) attacks generated by a reflector attack using a spoofed IP address and impersonation in the VoIP networks can be detected and prevented. MAC based routing table, maintained by the server, can detect the DDoS attacks generated by a reflector attack. MD5 and RSA were used to generate the certificates for the legitimate users. This generated certificate and the routing table enable this approach to rightly detect DDoS attacks and to generate a block list of IP addresses. The next time, when there is a connection establishment request from the block listed IP address, the request will be denied. Hence, the network can be protected from being attacked in the initial phase itself. The experimental setup and the NS-2 simulation results support the method.

Keywords: *Voice over Internet Protocol, DDoS attack, reflector attack, MAC, Routing table, MD5, RSA.*

1. Introduction

In VoIP systems the general network carriers are used to transmit multimedia data with the support of the signaling protocol Real Time Protocol (RTP). Most of the network carriers are shifting their network to VoIP based networks; our model improves security and reliability in their networks. Ease of use and implementation of RTP [3] made it less vulnerable to the implementation based attacks. At the same time it suffers from flood based attacks. As VoIP has been mostly [2] used for online communications, the communicating parties expect original quality like a face-to-face chat. Flood based attack causes either the message or the victim unavailable to the communicating party at the other end, thereby it degrades the expected quality of transmission. A large [4] class of threats, such as call rerouting, toll fraud and conversation hijacking incur deviations in the protocol state machines and can be detected through monitoring of the protocol state transitions.

Distributed Denial of Service (DDoS) can acquire different faces. Ultimately it aims at the deterioration of the services to be provided to the right end users. Consequences of DDoS lead to the absolute deprivation of the resources when it is badly needed. DDoS is a kind of a security attack [9] on the availability of Internet services and resources. This type of attack can be implemented using flooding techniques like SYN flooding, ICMP flooding, UDP flooding. The attacker will be sending continuously a bunch of data packets that will occupy the network bandwidth and thus creating congestion in the network, making the resources of the provider unavailable to its users.

1.1. Faces of DDoS attacks

DDoS has different [12-15] transformations on IP based networks, such as:

Implementation flaw DDoS takes place when the malicious user creates a single or multiple number of attack packets to intrude the minor defects while implementing the components of VoIP.

Flood DDoS happens due to flooding or sending a huge number of packets aimed towards the victim VoIP component.

Application-level DDoS happens at a time one of the attributes of the services is vulnerable, like Registration hijacking.

Platform DDoS occurs when the malicious user generates an attack focusing mainly on the support services.

Signaling and Media DDoS occur due to the exposure in the software components of VoIP, such as signaling, media processing software.

1.2. Vulnerable phases in the existing system

The major problem is with the *session initiation* and *session termination.*

1.2.1. Session initiation

This session is highly prone to spoofed IP address attack [10]. Generally this attack can be generated by two different scenarios like Spoofed with an “INVALID” IP address, Spoofed with a “THIRD PARTY” IP address.

1.2.1.1. Spoofed with an INVALID IPv4 address

The attacker sends an INVITE request with an INVALID IPv4 address as a source IPv4 address to the server. The server sends an acknowledgement and a sequence number; ACK+SEQ, to that invalid IP address and waits for the ACK message. Since the Destination IP address is invalid, there will not be any reply from the other end. This increase in the waiting time before terminating the connection at the server end will increase the overhead and prevents the server from delivering [18-20] the resources to the legitimate users.

1.2.1.2. Third party IP v4 address

The attacker sends an INVITE message with a THIRD PARTY IP address as a source IP address. The server sends an ACK+SEQ to that third party IP address and waits for the ACK message. Since the Destination address is unknown, the server checks the packet and discards it since it is not useful.

1.2.2. Session Termination

The Session Termination is mainly prone to the attack "*impersonation*". An attacker lies in the same network as any one of the parties that are engaged in the VoIP call. The attacker will impersonate the party as if he is presented in the network and sends a "BYE" message to the victim end, which will create an abnormal termination of the call and the other who doesn't know about his existence will keep on sending the data presented in Fig. 1.

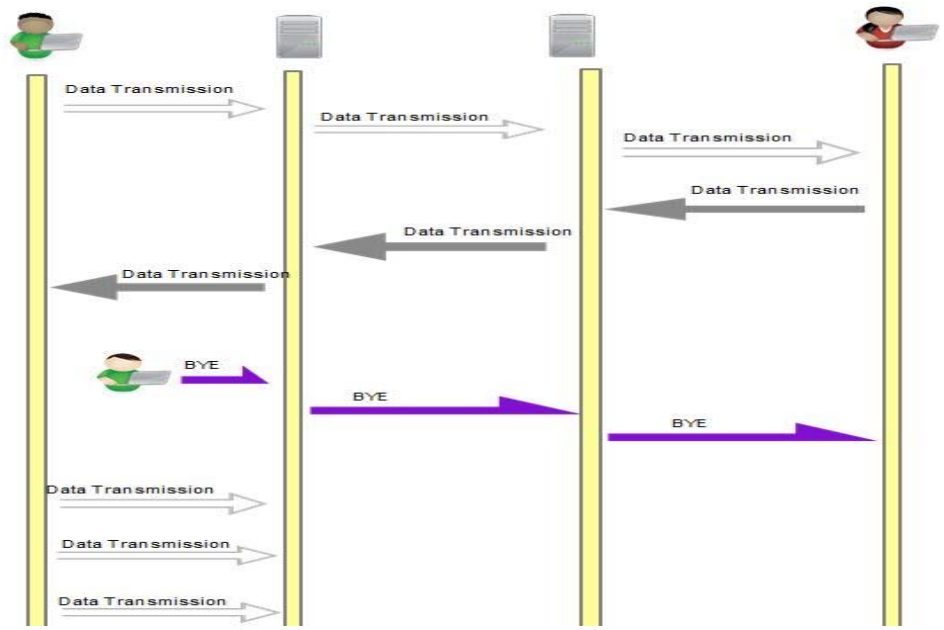

Fig. 1. Session Termination due to Impersonation

2. Architecture of the proposed solution

The solution is provided in such a way that the back lacks in the previously existing solutions are avoided. A new framework is developed in rightly identifying the spoofed IP address.

Also, the user's authentication is introduced to further strengthen the security. Authentication is achieved using the session keys that are generated and exchanged using "hybrid key distribution". This will help in the identification of the third person in the call.

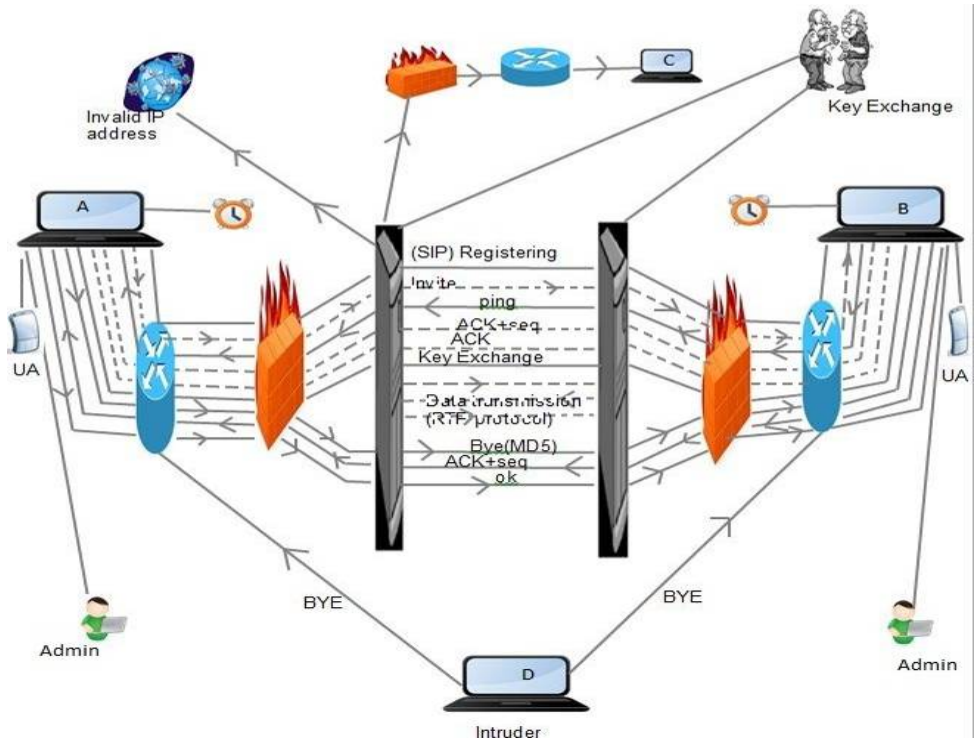

Fig. 2. Framework of the proposed approach

2.1. Discrimination between valid and invalid IP addresses

The most prominent network command, PING command is used to find out the invalid IP address. Consider the scenarios shown in Fig. 3. Let us say that **A** sends a spoofed INVITE packet to **B** with an invalid IP address. Before sending the ACK+SEQ packet, **B** will ping the source IP address present in the INVITE packet. If there is a reply to the command, the host at the destination address to **B** is alive and it is a valid address. If there is no reply, then **B** can determine that it is a spoofed IP and will drop the connection.

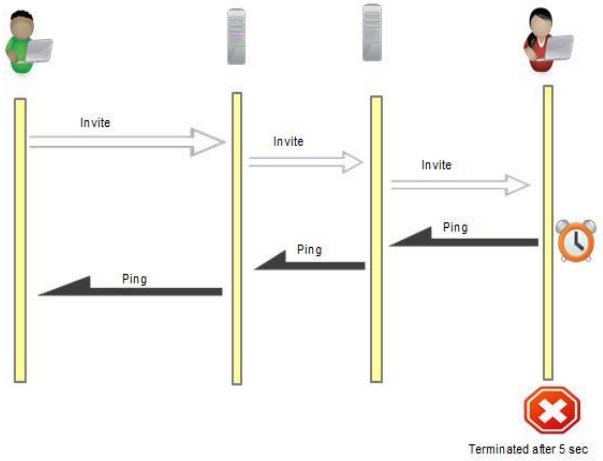

Fig. 3. PING with an invalid IP address

2.2. MAC address for detecting the Spoofed IP address

The attacker uses automated tools to generate numerous spoofed packets; he can change the IP address to the third party IP address, on which he intended to perform a DDoS attack.

The attacker cannot change the MAC address as easily as he is changing the IP address. A new routing table is introduced at each node with a MAC address as one of the parameters shown in Table 1.

Table. 1. New routing tables

IP v4 Address	MAC Address
192.31.67.56	00-00-45-00-00-15
192.31.67.56	00-00-45-00-00-15
192.45.78.91	00-00-45-00-67-15

The server stores the MAC address during the session invitation stage, thereafter every time the router checks the MAC address of the coming packets with the MAC address that is stored, previously shown in Fig. 4. If the MAC address is the same as in the new routing table, the connection is established, summarized pseudo code shown below.

A: A → B
B: Create Routing Table, RT (MAC, IP)
Register A (MAC, IP) in RT
PING A
A: Reply
B: Register Reply (MAC, IP) in RT
Check MAC, IP
MAC mismatch; Create Block list (IP)
Otherwise allow access

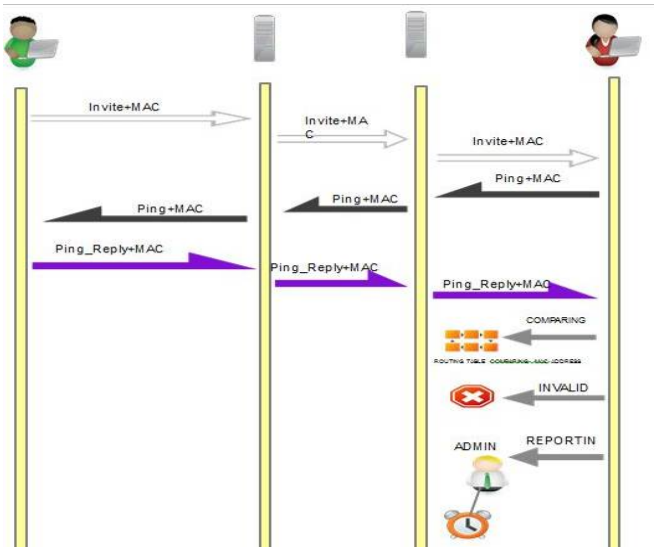

Fig. 4. Invalid MAC address

If the MAC address differs from the routing table, then the connection is terminated and the administrator is notified about the attack and the MAC in the routing table is kept in the watching list. So that further connections from this watch list will be terminated till the enquiry succeeds. Fig. 5 gives a detailed explanation of the working environment.

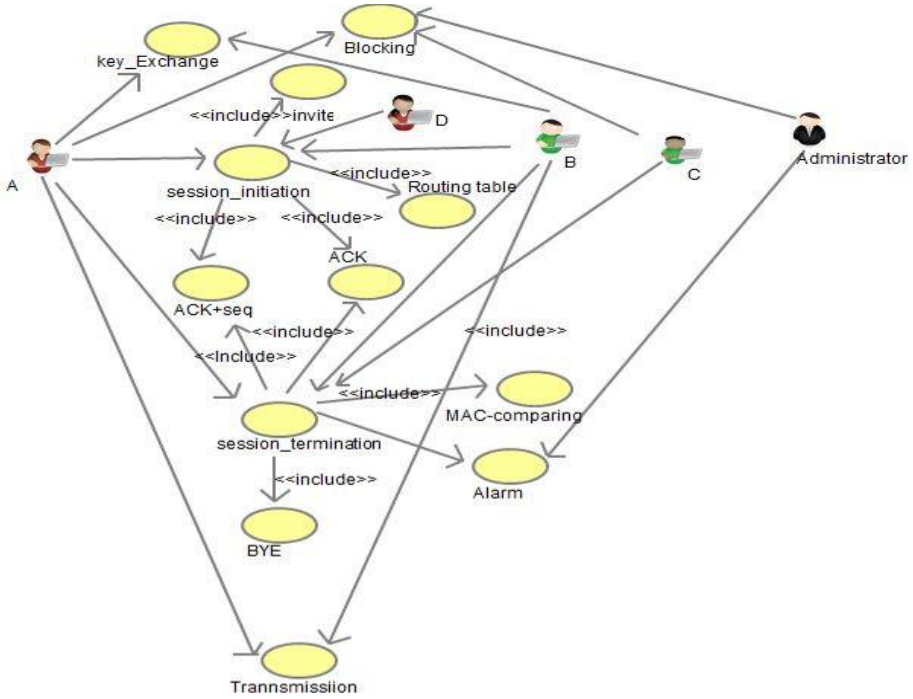

Fig. 5. Identification of a spoofed IP address

When the ping reply is back from the user, the server checks the MAC address in the ping packet with the MAC address registered in the routing table. Upon detection of discrepancy in the MAC address, the server will terminate the connection and alarm the administrator and will place the previously registered MAC in the black list for further enquiry.

2.3. Introducing a key exchange – hybrid key distribution

This proposed method retains the use of a private-key KDC. The Master Key is kept secret and shared among the registered users on demand. These exchanged secret keys help in the distribution of session keys. The Master keys are shared with the aid of a public key. It is especially useful with widely distributed users with salient features like rational performance and backward compatibility.

The media session is the same as in the previous method. It uses the same "RTP" protocols as before. RTP [13] carries multimedia data which must be delivered in real-time to be usable for quality dialogue, at the same time it is vulnerable to flood-based attacks. For example, an attacker can flood a media gateway, IP Phone, shared WAN link, or other media-processing VoIP component, interfering with the processing of normal packets. If this attack causes the target to drop or ignore legitimate RTP packets, then the audio quality may be unacceptable for conversations. The floods were very efficient, resulting in severe or total degradation of the audio. While these attacks did spoof packet values, such as MAC address, IP address, and RTP sequence numbers, it was observed that most IP Phones did not even check these values. It was also observed that when very large RTP packets (of approximately 1500 bytes), were sent to ports on certain IP phones, they crashed and had to be manually rebooted.

The impersonation is the main problem in the SESSION TERMINATION. This can be avoided by using encryption and certificate techniques. Here a combination of RSA and MD5 algorithms are used.

3. Experimental setup

The approach proposed has been supported by simulation using the network simulator ns-2.

3.1. Ping and MAC based routing table

A typical ping command is used by the server in the session initiation stage to find if the destination IP address, from which the request came, is alive or not. The Round Trip Time (RTT) is calculated for further use. After the ping reply is received by the server, the server stores the MAC address in the newly proposed routing table.

3.2. Finding the Spoofed IP Address

After the server receives the ping reply, it will check the previously registered MAC address of a request in the routing table with the ping reply MAC. If two different IP addresses are having the same MAC address, then a flooding attack is detected.

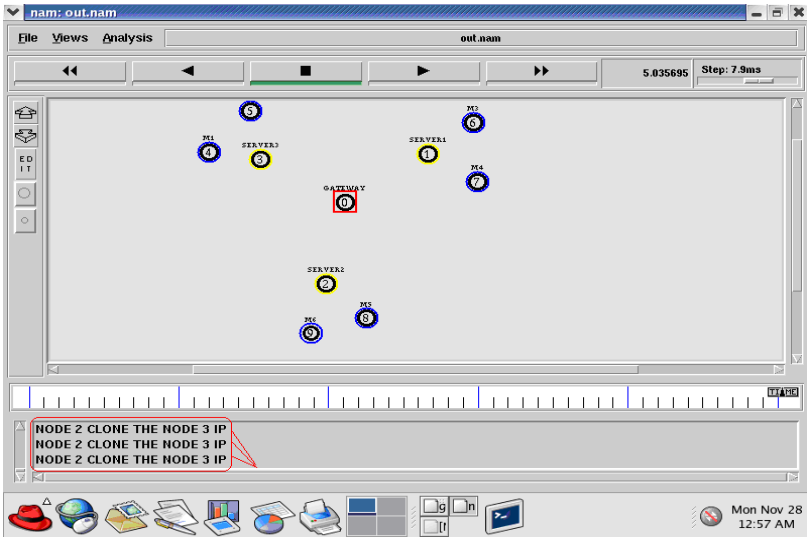

Fig. 6. A Spoofed IP address

From Fig. 6, node 2 cloned the node 3 IP address. Here the MAC address of node 2 will be kept in the black list. When the flooding attack is detected, the server will terminate the connection between the clients and will place the IP address of the attacker in the black list.

3.3. Generation of keys using RSA algorithm and certificates

Using RSA algorithm, both a public and a private key are generated for the parties participating in the connection, to overcome the overhead incurred by other authentication [21] schemes. The generated keys are used along with MD5 hash algorithm to create a certificate for the parties involved in the connection. The certificate is generated by using MD5 along with RSA algorithm.

Once the bye message is sent by any one of the clients, that message is attached with the respective certificate. The other party before terminating the connection checks the certificate with the sent party public key. If the certificate is true, then the connection is terminated. If the certificate is an error, then it will warn the administrator and will not discontinue the connection.

4. Performance analysis of the proposed solution

The analysis of the proposed solution is divided into three stages, such as the existing system, DDoS attack on the existing system and improvements in the proposed framework.

4.1. Throughput in the existing systems

The existing system is a simple system with valid users with minimal traffic.

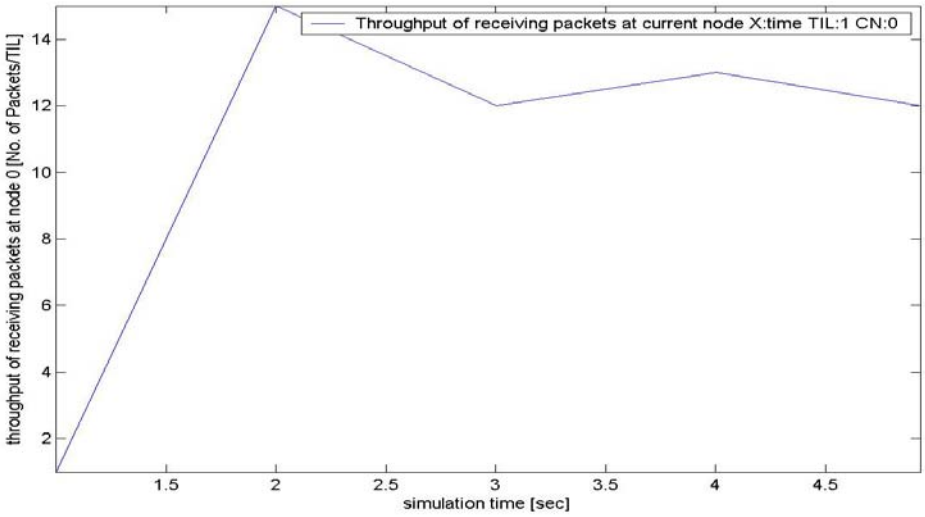

Fig. 7. Throughput of the received packets vs. simulation time

As presented in Fig. 7, the throughput of the system increases as the simulation time increases. Since no attack is deployed on the network, the throughput is generally high, as illustrated in the above graph.

4.2. Throughput in the existing systems during a DDoS attack

Throughput will increase when the DDoS is in its initial stage. As the simulation time increases, the throughput of the system also decreases. During peak time the whole throughput of the system becomes zero and the server is crashed or overloaded with DDoS. Since the DDoS is a wave attack, the graph is again raised.

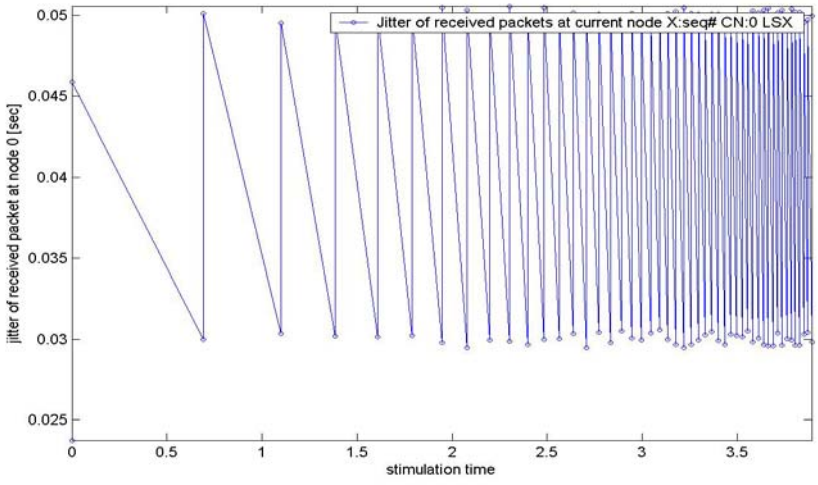

Fig. 8. Jitter vs. simulation time

From Fig. 8 it follows that the jitter of the network increases as the DDoS attack is generated. In the initial state of a DDoS attack, the jitter of the network will be less and less oscillating. But as the impact of DDoS increases, the jitter in the network also increases.

4.3. Throughput in the proposed systems during a DDoS attack

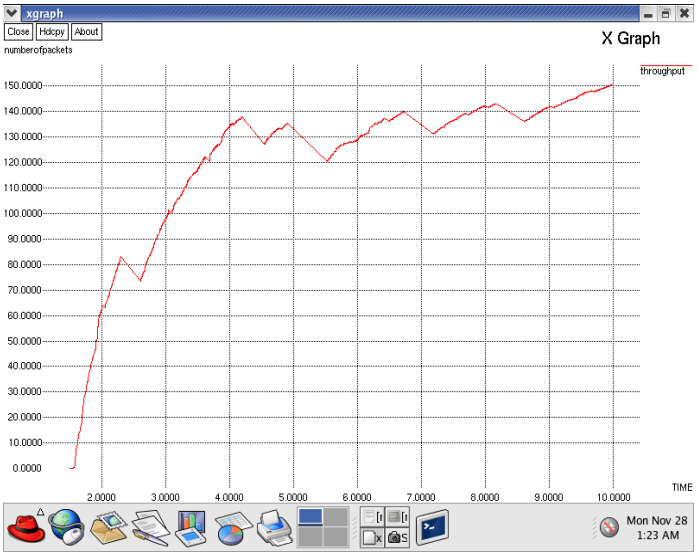

Fig. 9. Throughput vs. simulation time

From Fig. 9 it can be seen that the network in its initial state, the throughput increases with the simulation time as usual. Upon identification of a new framework of the DDoS attack, it prevents the attack and restores the network to its normal state. So the graph again increases as can be observed in the above graph. At the same time the prevention also is alerted and a throughput increase takes place.

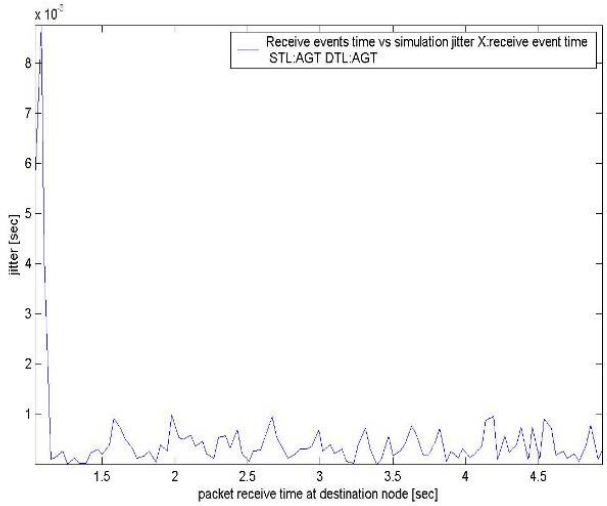

Fig. 10. Jitter vs. simulation time

Once the DDoS attack is generated the jitter of the network also decreases. The framework detects DDoS and terminates the connection between the parties; the jitter of the network comes to its normal level, as seen in Fig. 10**.**

As the simulation time increases, the end to end delay of the packets also increases as the jitter in the network increases due to the increase in the impact of the DDoS attack. After detection of a DDoS attack by the network, the connection between the parties is discontinued. So that the end to end delay is decreased since there is less jitter in the network.

5. Conclusion

DDoS is drawing a large part of the researchers' attention nowadays in all types of networks, from which VoIP is not exempted. To meet the customer's expectation concerning quality, as well as security in par with other emerging communication technologies, VoIP should excel. The packet loss or out-of-delivery will drag the people back from using this technology. VoIP is more widely deployed and thus most of the enterprises start to interconnect their internal networks via untrusted networks. The research study has shown that many VoIP components are vulnerable to DDoS. The threat to these components will increase. The required well-designed VoIP components, the use of strong authentication and VoIP firewalls best mitigates this threat.

By identifying and protecting against an intruder into the network, security can be achieved. The analysis of the approach proposed confirms its efficiency and robustness. This model could differentiate the attacker by the mismatch in their MAC address. The use of the developed code allows us to test numerous distributed denials of service attack scenarios in regard to the ability of the new framework to detect and prevent them. The usage of the newly generated black list also helps in protecting the network.

References

1. Barbieri, R., D. Bruschi, E. Rosti. Voice over IPsec: Analysis and Solutions. – In: 18th Annual Computer Security Applications Conference (ACSAC), 2002, 261-270.
2. Goode, B. Voice over Internet Protocol (VoIP). – Proc. of the IEEE, Vol. **90**, September 2002, No 9, 1495-1517.
3. Liu1, Chung-Hsin, Chun-Lin Lo. The Simulation for the VoIP DDoS Attack. – In: International Conference on Multimedia and Information Technology, 2008, 280-283.
4. Nassar, M., R. State, O. Festor. VoIP Malware: Attack Tool &Attack. – In: Proc. of the IEEE ICC, 2009, 1-6.
5. Chen, E. Detecting DoS Attacks on SIP Systems. – In: Proc. of 1st IEEE Workshop on VoIP Management and Security, San Diego, CA, USA, 2006, 53-58.
6. Ehlert, S., C. Wang, T. Magedanz, D. Sisalem. Specification-Based Denial-of-Service Detection for SIP Voice-Over-IP Networks. – In: Third International IEEE Conference on Internet Monitoring and Protection, 2008, 59-66.
7. Hongyu, C. VoIP Internet Phone Technology. Songgang, 2005, August, the First Edition of a Brush.

8. Liu, Chung-Hsin, You-Sheng Li. The Study of Botnet Attack on VoIP. – In: Sixth International IEEE Conference on Networked Computing and Advanced Information Management, 2010, 636-640.
9. Tang, Jin, Yong Hao, Yu Cheng, Chi Zhou. Detection of Resource-Drained Attacks on SIP-Based Wireless VoIP Networks. – In: IEEE Globecom Proceedings, 2010, 1-5.
10. J. Rosenberg, H. Schulzrinne, G. Camarillo. SIP: Session Initiation Protocol. IETF RFC 3261, June 2002.
11. Abdelnur, H., T. Avanesov, M. Rusinowitch Radu. State Abusing SIP Authentication. – In: The Fourth IEEE International Conference on Information Assurance and Security, 2008, 237-242.
12. Thermos, P., A. Takanen. Securing VoIP Networks: Threats, Vulnerabilities and Countermeasures. Addison-Wesley Professional, 2007.
13. Sengar, H., R. Dantu, D. Wijesekera. Securing VoIP and PSTN from Integrated Signaling Network Vulnerabilities. – In: IEEE Workshop, 3 April 2006, 1-7.
14. Vuong, S., Y. Bai. A Survey of VoIP Intrusions and Intrusion Detection Systems. – In: 6th International Conference on Advanced Communication Technology, 2004, 317-322.
15. Sisalem, D., J. Kuthan, S. Ehlert. Denial of Service Attacks Targeting a SIP VoIP Infrastructure – Attack Scenarios and Prevention Mechanisms. – IEEE Network, Vol. **20**, 2006, No 5 – Special Issue on Securing VoIP, 26-31.
16. Sengar, H., D. Wijesekera, H. Wang, S. Jajodia. VoIP Intrusion Detection through Interacting Protocol State Machines. – In: IEEE DSN'2006, June 2006, 393-402.
17. Nassar, M., R. State, O. Festor. Intrusion Detection Mechanisms for VoIP Applications. – In: 3rd Annual VoIP Security Workshop, Berlin, Germany, 2006.
18. Jeong, J. T. Lee, S. Yoon, H. Jeong, Y. Won, M. Kim. A Phased Framework for Countering VoIP SPAM. – International Journal of Advanced Science and Technology, Vol. **1**, 21-29.
19. Shevtekar, A., N. Ansari. A Proactive Test Based Differentiation Technique to Mitigate Low Rate DoS Attacks. – In: IEEE 16th International Conference on Computer Communications and Networks, ICCCN, 2007, 639-644.
20. Dantu, R., P. Kolan. Detecting Spam in VoIP Networks. – In: Proc. of USENIX, SRUTI (Steps for Reducing Unwanted Traffic on the Internet) Workshop, July 2005, 31-38.
21. Lee, Cheng-Chi. Security of an Efficient Nonce-Based Authentication Scheme for SIP. – International Journal of Network Security, Vol. **9**, November 2009, No 3, 201-203.