IOSR Journal of Computer Engineering (IOSRJCE)
ISSN: 2278-0661, ISBN: 2278-8727 Volume 6, Issue 2 (Sep-Oct. 2012), PP 35-41
www.iosrjournals.org

Performance Analysis of VoIP by Communicating Two Systems

Ms. V. Yagna Prabha[1], Ms.R.Amsaveni[2]
[1] *(Research Scholar, PSGR Krishnammal College for Women/Bharathiyar University, India)*
[2]*(InformationTechnology Department, PSGR Krishnammal College for Women/Bharathiyar University, India)*

Abstract: *VoIP is a technology that digitizes voice packets and enables telephony communication by using internet as a backbone. In this paper we introduce and explore the problems that occur in our day to day life in sending voice and data with different windows. The paper evolves in the VoIP environment. Sending of text and voice along single window is possible. In earlier days VoIP merges over devices like IP Telephony, Palms, PDAs, etc over IP network for communication. But less security is provided with packet loss, retransmission, end to end delay and overhead. VoIP is composed of Signalling and Media. The use of Signalling is for controlling communication and it does the call set up, locate users, and tear down sessions. Media is used for transporting the voice packets. Ad hoc wireless networks are formed by a set of mobile nodes that communicate with each other over a wireless channel. Perceived Voice Quality can be achieved in terms of NS-2 Simulator. The work focuses with the combined forward error correction, layered coding and multiple. VoIP is a term used for a set of facilities for managing the delivery of voice information using the Internet Protocol. With VoIP there is no dedicated connection between the communicating devices. In addition to IP VoIP uses parameters such as residual packet loss rate and average burst length for secured delivery of voice and data. The protocols used are SIP and RTP. Our task in this work is to configure and create the test bed to simulate the working of Voice over IP (VoIP) Network. Also detailed and scrutinized study is made to test the performance of the proposed configuration. Two systems are installed with Client software and the third one with Server and the settings are made in such a way that Call from Client A will pass to the server and then server transfers to client B. NS-2 is used to analyse the network communication among the three machines*
Keywords: *ABL, IP, NS – 2, PDA, RPLR, RTP, SIP, Telephony, VoIP.*

I. Introduction

VoIP is a technology that digitizes voice packets and enables telephony communication by using internet as a backbone. The broad development of Internet had witnessed the concept of VoIP and the technology is evolving to replace the Public Switched Telephone Network. VoIP is composed of Signalling and Media. The use of Signalling is for controlling communication and it does the call set up, locate users, and tear down sessions. Media is used for transporting the voice packets. Ad hoc wireless networks are formed by a set of mobile nodes that communicate with each other over a wireless channel.

The work focuses on providing voice over ad hoc wireless networks. When transmitting voice data, continuous delivery with limited packet loss rate is of primary importance. For a packet to be useful at its destination the destination should receive the packet before its deadline. Playout time is defined as the time instant at which the packet should be played out at the destination. VMware Software is used such that an operating system can be installed within another operating system. The voice and data networks are existing separately, along their separate paths. One of the main reasons is the technology used for voice and data communication. To overcome this problem, voice over ad hoc wireless networks can be applied. Hence by avoiding the packet loss overhead, retransmission and end to end delay can be eliminated.

VoIP is a term used for a set of facilities for managing the delivery of voice information using the Internet Protocol. With VoIP there is no dedicated connection between the communicating devices. In addition to IP VoIP uses parameters such as residual packet loss rate and average burst length for secured delivery of voice and data. The protocols used are Session Initiation Protocol and Real Time Transport Protocol. Both the client and server use different software. Two systems are installed with Client software and the third one with Server and the settings are made in such a way that Call from Client A will pass to the server and then server transfers to client B. NS-2 is used to analyse the network communication among the three machines

Client Softwares are used to generate and terminate calls. Some of the free source softwares are listed below:

- *Ekiga*
- *Empathy*
- *Jisti*
- *Kphone*
- *Linphone*
- *MicroSIP*

- *QuteCom*
- *Twinkle*

Servers are used to response to the client's request and forward to the destination. Some of the open source server softwares are listed below:

- *Asterisk*
- *Elastix*
- *FreeSWITCH*
- *Kamilio*
- *OpenSIPS*
- *OpenSER*
- *sipX*

II. Related Work

Works focus on optimizing packet length, employing forward error control with a packet and retransmission strategies. Separate windows are needed for sending and receiving text as well as voice. In Yahoo server the voice is stored in a file and then it is converted into packets and it is transmitted by the use of Half Duplex Communication. Both the windows for voice and text cannot be used simultaneously. In single hop network, every node is within the radio range of every other node and hence time-delay occurs. In multi hop network, end-to-end delay and performance overhead occurs. The interaction between call participants become more difficult to establish. Some of the limitations are

2.1 Limitations

- Retransmission is done frequently.
- End-to-end delay occurs.
- Network traffic and congestion occurs.
- Packet loss rate is maximum in older days.
- Separate environment is necessary for both voice and text.

III. Proposed Work

In our proposed work, we have evaluated the performance of various open source softwares and results are studied. From the results, tools that are used are

Ubuntu - Operating System
NS-2 - Network Traffic Analyser
LinPhone - Client Software
OpenSIPS - Server Software

Our task in this work is to configure and create the testbed to simulate the working of Voice over IP (VoIP) Network. Also detailed and scrutinized study is made to test the performance of the proposed configuration. Two systems are installed with Client software and the third one with Server and the settings are made in such a way that Call from Client A will pass to the server and then server transfers to client B. NS-2 is used to analyze the network communication among the three machines

Steps taken to install Client and Server Software:

Installation of Linphone

- Install the dependencies from Synaptic Package Manager: speex, libosip2, libeXosip2
  - *sudo apt-get install speex*
  - *sudo apt-get install libosip2*
  - *sudo apt-get install libXosip2*
- Still from Synaptic Package Manager, install : linphone
- After installation, you can find the app in your menu : Applications > Internet > Linphone
- To setup your account, go to the menu : Linphone > Preferences > 'Manage SIP Accounts'
- Account details are added as per our scenario.

Installation Of openSIPs

The backbone of VoIP network lies in the efficiency and task performed by the Server.

Here are steps that are followed to install Server on Ubuntu system

1 sudo apt-get install bison bison++ bisonc++
2. sudo apt-get install flex
3. sudo apt-get install libsctp1
4. sudo apt-get install mysql-server

5. sudo apt-get install libmysqlclient-dev
6. sudo apt-get install libxml2-dev
7. sudo apt-get install libexpat1-dev
8. sudo apt-get install libradius-ng2 libradius-ng-dev
9. sudo apt-get install libcurl3-dev
10. sudo apt-get install libxmlrpc-c3 libxmlrpc-c3-dev
11. sudo apt-get install libperl-dev
12. sudo apt-get install libsnmp-dev
13. sudo apt-get install libconfuse0 libconfuse-dev
14. sudo apt-get install build-essential
15. sudo tar xvfz opensips-1.5.0-tls_src.tar.gz
16. edit opensips-1.5.0-tls/Makefile/
change : #TLS=1
to : TLS=1
remove : – jabber
- cpl-c
- xmpp
- rls
- mi_xmlrpc
- xcap_client
- db_mysql
- presence
- presence_xml
- presence_mwi
- presence_dialoginfo
- pua
- pua_bla
- pua_mi
- pua_usrloc
- pua_xmpp
- pua_dialoginfo
- perl
- snmpstats
- peering
- carrierroute
from : exclude_modules=
17. sudo make
18. sudo make install
19. sudo cp opensips-1.5.0-tls/packaging/debian-etch/opensips.default /etc/default/opensips
sudo cp opensips-1.5.0-tls/packaging/debian-etch/opensips.init /etc/init.d/opensips
20. sudo nano /etc/default/opensips
change : RUN_OPENSIPS=no
to : RUN_OPENSIPS=yes
21. sudo nano /etc/init.d/opensips
change : DAEMON=/usr/sbin/opensips
RUN_OPENSIPS=no
to : DAEMON=/usr/local/sbin/opensips
RUN_OPENSIPS=yes
22. sudo chmod +x /etc/init.d/opensips
23. sudo groupadd opensips
sudo useradd -g opensips opensips
24. sudo mkdir /var/run/opensips
sudo chmod 777 /var/run/opensips
25. sudo chmod 777 /usr/local/etc/opensips/
26. sudo apt-get install bind9
27. sudo nano /etc/bind9/named.conf
add : zone “opensips.org” {
type master;
file “/etc/bind/db.opensips”;
};

zone “18.14.10.in-addr.arpa” {
type master;
file “/etc/bind/db.18.14.10″;
};
28. Create new RR file
sudo nano /etc/bind9/db.opensips
write :
;
; BIND data file for opensips.org
;
$TTL 604800
@ IN SOA opensips.org. root.opensips.org. (
2 ; Serial
604800 ; Refresh
86400 ; Retry
2419200 ; Expire
604800) ; Negative Cache TTL
;
IN NS opensips.org.
opensips.org. IN A 10.14.18.56
29. Create new RR file
sudo nano /etc/bind9/db.18.14.10
add :
;
; BIND data file for opensips.org
;
$TTL 604800
@ IN SOA opensips.org. root.opensips.org. (
2 ; Serial
604800 ; Refresh
86400 ; Retry
2419200 ; Expire
604800) ; Negative Cache TTL
;
IN NS opensips.org.
opensips.org. IN A 10.14.18.56
30. sudo nano /etc/bind9/named.conf.option
add : recursion no;
in : option { }
31. sudo /etc/init.d/bind9 restart
32. sudo nano /usr/local/etc/opensips/opensipsctlrc
uncomment : # SIP_DOMAIN=opensips.org
DBENGINE=MYSQL
DBHOST=localhost
DBNAME=opensips
DBRWUSER=opensips
DBRWPW=”opensipsrw”
DBROUSER=opensipsro
DBROPW=opensipsro
DBROOTUSER=”root”
USERCOL=”username”
INSTALL_EXTRA_TABLES=ask
INSTALL_PRESENCE_TABLES=ask
uncomment and change :
PID_FILE=/var/run/opensips.pid
to : PID_FILE=/var/run/opensips/opensips.pid
33. sudo mysqladmin -u root password ‘root’
34. sudo opensipsdbctl create
35. sudo nano /usr/local/etc/opensips/opensips.cfg
uncomment : #loadmodule “db_mysql.so”

#loadmodule “auth.so”
#loadmodule “auth_db.so”
#modparam(“usrloc”, “db_mode”, 2)
#modparam(“usrloc”, “db_url”,
“mysql://opensips:opensipsrw@localhost/opensips”)
#modparam(“auth_db”, “calculate_ha1″, yes)
#modparam(“auth_db”, “password_column”, “password”)
#modparam(“auth_db”, “db_url”,
“mysql://opensips:opensipsrw@localhost/opensips”)
comment : modparam(“usrloc”, “db_mode”, 0)
36. sudo nano mysql -u root -p
mysql> GRANT ALL PRIVILEGES ON *.* TO opensips@localhost IDENTIFIED BY ‘opensipsrw’;
mysql> GRANT ALL PRIVILEGES ON *.* TO opensips@127.0.0.1 IDENTIFIED BY ‘opensipsrw’;
37. start opensips, choose one of these method:
1. sudo opensipsctl start
2. sudo /etc/init.d/opensips start
38. sudo opensipsctl add 1001 1001

IV. Performance Analysis Using NS – 2

Fig.1 is the process of converting user originated inputs to a computer based format. It can be designed as the information that is to be provided to the system. It should be easily understandable and should be tested with various combinations of inputs.

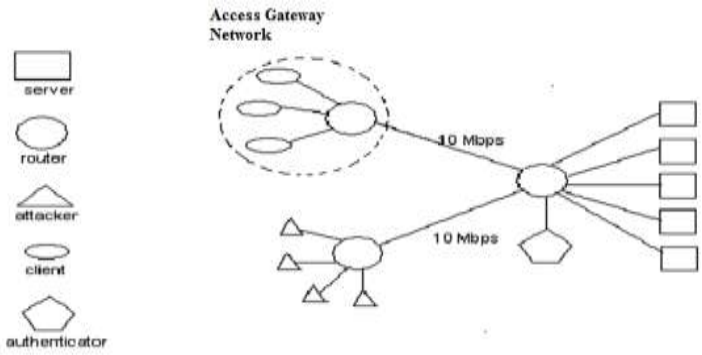

Fig.1 Simulation Topology

With the help of Honeypots tool the performance can be analysed. We utilize our roaming honeypots scheme to mitigate the effects of service-level DoS attacks, in which many attack machines acquire service from a victim server at a high rate, against back-end servers of private services. The roaming honeypots scheme detects and filters attack traffic from outside a firewall and also mitigates attacks from behind a firewall by dropping all connections when a server switches from acting as a honeypot into being active.

Through ns-2 simulations, we show the effectiveness of our roaming honeypots scheme. In particular, against external attacks, our roaming honeypots scheme provides service response time that is independent of attack load for a fixed number of attack machines.

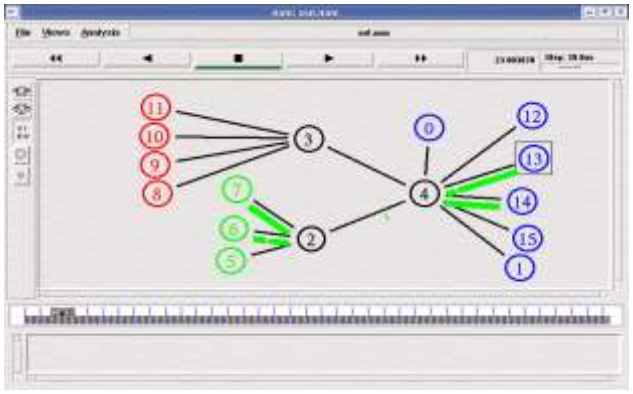

Fig.2 Honeypots in Active Servers

In Fig.2 the roaming mechanism of honeypots, which is a secure and light weight mechanism to proactively change the location of the active server lies within a server pool. Legitimates clients keep track of roaming times and location of the roaming server using light-weight one way hash functions. The roaming honeypots scheme is two- fold: Firstly, idle servers detect attacker addresses so that all their subsequent requests are filtered out. Secondly, each time a server switches from idle to active, it drop all its current connections, opening a window of opportunity for legitimate request before the attack re-build up.

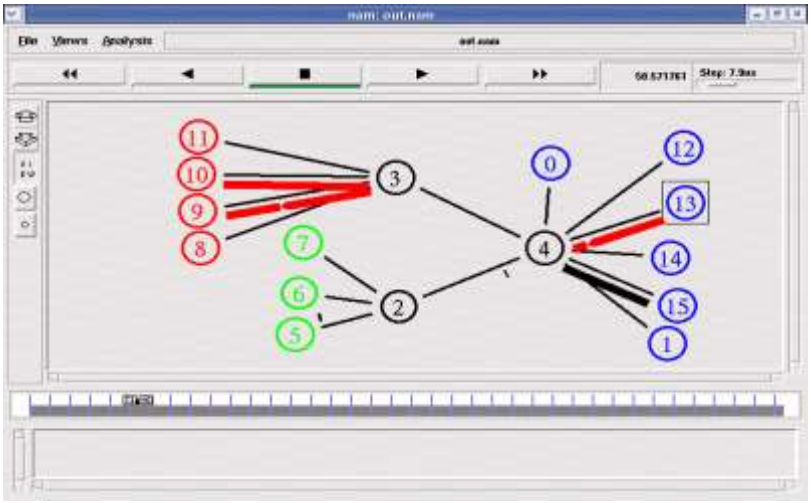

Fig 3. Honeypots Providing Lifeline

Fig.3 explains that once if an attacker or an intruder hits the tool its server requests are dropped. Since the locations of honeypots are unpredictable the tracers are trapped easily.

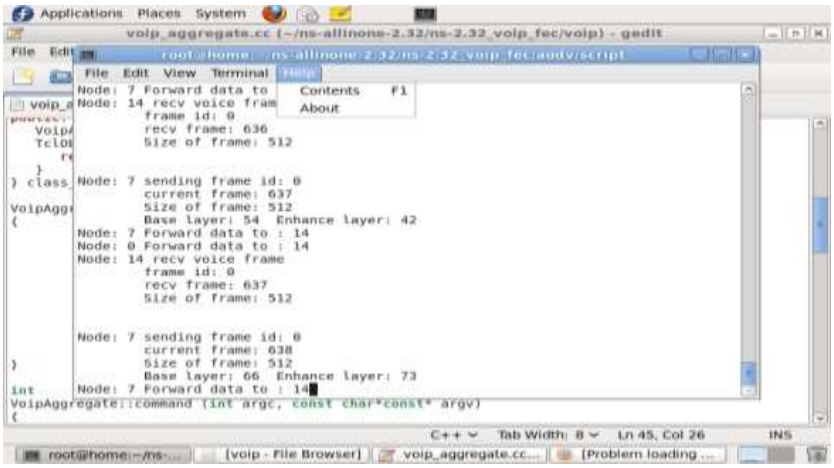

Fig4. VoIP Mechanism of Authentication

Fig.4 explains that the substreams are send with the help of frame id. The EL substream is encoded into two descriptions using MD Coder and each description is sent along with BL substreams. Each voice packet contains adaptive FEC protected BL and one of the two BL descriptions. Hence an authenticated voice communication can be provided. Hence an authenticated mechanism can be achieved by communicating two systems with Linux OS and VMware Software. Once after providing communication between two systems with the client tool and the server tool, the performance can be analyzed with the help of NS – 2 Simulations.

V. Conclusion

Though there are several threats in our network security different technologies were invented to overcome those problems. Technologies like, Honeypots, RFID, Snort, Wireshark, etc. are invented to increase the performance of our conference or communication. Today there are major methods for electronic communication like Voice (Telephone), Fax, Email, etc. if the same network carries these messages to the devices over IP or AWN then in future there is no reason why one device can receive all of them. Thus a voice call would be automatically sent to speakers or headphone, while a fax message could be sent to the printer or the monitor for printing or display and e-mail message on the other hand would be stored in e-mail client. The features like,

- Unified inbox must be bought into existence.
- Designing attacker model to trace hackers must be done.
- Non Real Time traffic must be analysed.
- Firewalls in the CDN should allow traffic sourced at the secret gateways.
- The idea of indirection to defend against DoS must be presented.

References

[1] ITU-T Recommendation, G.114, *One Way Transmission Time, Feb. 1996.*

[2] J.D. Gibson, A. Servetti, H. Dong, A. Gersho, T. Lookabaugh, and J.C. De Martin, *"Selective Encryption and Scalable Speech Coding for Voice Communications over Multihop Wireless Links," Proc. IEEE Military Comm. Conf. (MILCOM '04), vol. 2, pp. 792-798, Nov. 2004.*

[3] C.-h. Lin, H. Dong, U. Madhow, and A. Gersho, *"Supporting Real-Time Speech on Wireless Ad Hoc Networks: Inter-packet Redundancy, Path Diversity, and Multiple Description Coding," Proc. Second ACM Int'l Workshop Wireless Mobile Applications and Services on WLAN Hotspots (WMASH '04), pp. 11-20, Oct. 2004.*

[4] X. Yu, J.W. Modestino, and I.V. Bajic, *"Modeling and Analysis of Multipath Video Transport over Lossy Networks," Proc. 11th Int'l Conf. Distributed Multimedia Systems (DMS '05), pp. 265-270, Sept. 2005.*

[5] L. Munoz, M. Garcia, J. Choque, R. Aguero, and P. Mahonen, *"Optimizing Internet Flows over IEEE 802.11b Wireless Local Area Networks: A Performance-Enhancing Proxy Based on ForwardError Correction," IEEE Comm. Magazine, vol. 39, no. 12, pp. 60-67, Dec. 2001.*

[6] S. Aramvith, C.-W. Lin, So. Roy, and M.-T. Sun, *"Wireless Video Transport Using Conditional Retransmission and Low-Delay Interleaving," IEEE Trans. Circuits and Systems for Video Technology (CSVT '02), vol. 12, no. 6, pp. 558-565, June 2002.*

[7] G. Rubino and M. Varela, *"Evaluating the Utility of Media- Dependent FEC in VoIP Flows," Proc. Fifth Int'l Workshop Quality of Future Internet Services (QofIS '04), pp. 31-43, Sept. 2004.*