World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:3, No:10, 2009

VoIP Networks Performance Analysis with Encryption Systems

Edward Paul Guillen, Diego Alejandro Chacon
Telecommunications Engineering, GISSIC investigation group
Military University "Nueva Granada"
Bogotá, Colombia
edward.guillen@unimilitar.edu.co, gissic@unimilitar.edu.co

***Abstract*—**The VoIP networks as alternative method to traditional PSTN system has been implemented in a wide variety of structures with multiple protocols, codecs, software and hardware–based distributions. The use of cryptographic techniques let the users to have a secure communication, but the calculate throughput as well as the QoS parameters are affected according to the used algorithm. This paper analyzes the VoIP throughput and the QoS parameters with different commercial encryption methods. The measurement–based approach uses lab scenarios to simulate LAN and WAN environments. Security mechanisms such as TLS, SIAX2, SRTP, IPSEC and ZRTP are analyzed with μ-LAW and GSM codecs.

***Keywords*—**VoIP, Secure VoIP, Throughput Analysis, VoIP QoS evaluation

I. Introduction

THE promise of VoIP networks is to maintain a reliable voice communications in a broadband scenario improving the best cost-benefit relationship. The QoS parameters guarantee a specific measurement and let providers and users accomplish Service Level Agreements –SLA–. In the VoIP networks design, the desired QoS and the necessary channel capacity vary according to the used codec or the compression technique but when security along the channel is required, the encryption method is a variable that modifies the throughput and sometimes the compression rate. In fact, secure VoIP offers mechanisms for signaling and key management but it's difficult to evaluate the throughout and therefore to design a reliable network.[1]

The throughput analysis is made by the practical measurement of traffic and QoS parameters in predefined VoIP network scenarios with the use of commercial encryption systems.

A brief description of VoIP parameters is given in the second part of the paper. The third part shows encryption protocols and subsystems used in VoIP systems divided onto three subtopics: Signaling encryption, medium encryption, and key management using symmetric and asymmetric methods.

The probed scenarios, the implemented server, and the measurement tools are explained in the fourth section. Finally, the fifth section shows results by analyzing statistical results between codecs, encryption algorithms, QoS parameters, networking scenarios, and required bandwidth according to the throughput results.

II. Key VoIP Features

The QoS parameters and the throughput on VoIP networks have a closed relationship with the used codec. The required bandwidth is selecting according to the parameters and the desired service.

A. Quality of Service Parameters

The common parameters used in VoIP service are delay, jitter and packet lost. Although the thresholds of those parameters could be subjective, their characteristics are well defined.

1) Delay

The time that is taken by a packet to arrive to the end point in a VoIP Network. The network infrastructure affects the latency and also the delay, caused by packets, and the queuing at switches and routers. [2], [3]

A VoIP call total delay is given by equation (1), and it's described by three parameters: transmitter delay, network delay and receiver delay.

$$D = D_{transmitter} + D_{network} + D_{receiver} \quad (1)$$

$D_{transmitter}$ is produced by the packetization process at the information source. Other variables included in this delay are sampling codification delay and packet encapsulation delay at the source terminal.

Network delay is composed by three components: transmission, queuing and propagation. In a LAN, the propagation delay is very lower than the others delays and is usually negligible, but in a WAN, it is not.

For $D_{receiver}$, the value includes playback delay, delay for buffer-jitter and processing delay.

2) Jitter

The jitter is the variation in the time between the time the packet is supposed to arrive and the time when the packet arrives. The RFC3550 [4] explains the jitter by analyzing the equation (2)

$$J_{(i)} = J_{(i-1)} + \frac{D_{(i-1,i)} - J_{(i-1)}}{16} \quad (2)$$

Where,

$J_{(i)}$ is the mean jitter of the ith packet

$J_{(i-1)}$ is the mean jitter of the *(i-1)* packet, and

$D_{(i-1,i)}$ is the delay between the packet *(i)* and *(i-1)*

3) Packet Lost

In the VoIP network, the packet lost could be produced in a network congestion condition with different traffic types. It's important to remember that nowadays network equipment can prioritize VoIP packets but they cannot do so when there is signaling encryption, because those packets are recognized just as simply DNS traffic.

Buffer-Jitter overload can cause packet lost and it increases with the rise of concurrent calls. Under this condition, the source stops sending packets to the destination because there is not sequence in the connection.[5]

Some codecs have the capacity of predicting packet lost and replace them. The general condition is that the lost must be less than 5%. To do so, there are two methods. The first one is interpolation, where the first and the third packet are used to reconstruct the missing packet. For the second method, called substitution, the missing packet is replaced with an equal packet to the last packet. [6]

B. Bandwidth

The capacity of transmit effective data in the complete network or in a segment.

The VoIP bandwidth is affected by parameters like packet flow, packet length and the compression method.

1) Codec

The codec can vary the compression rate over the digitalized signal in order to be send to the channel. The main codec characteristics are compression rate, packet length, and frame time. The Fig. 1 shows the packetization process, and some equation involved. [7]

C_r = Compression factor (times)

T_t = Frame Time (ms)

L_t = Frame Lenght (Bytes)

H = Header Lenght (Bytes)

D_{Rd} = Digital Voice Rate (Kbps)

D_{Rc} = Codified Voice Rate (Kbps)

N = Number of Frames per packet, and

BW = Bandwidth (Kbps)

The analog voice bandwidth is assumed to be 3700 Hz, although for some codecs this value can be a little bit different from 3100 Hz to 4000 Hz.

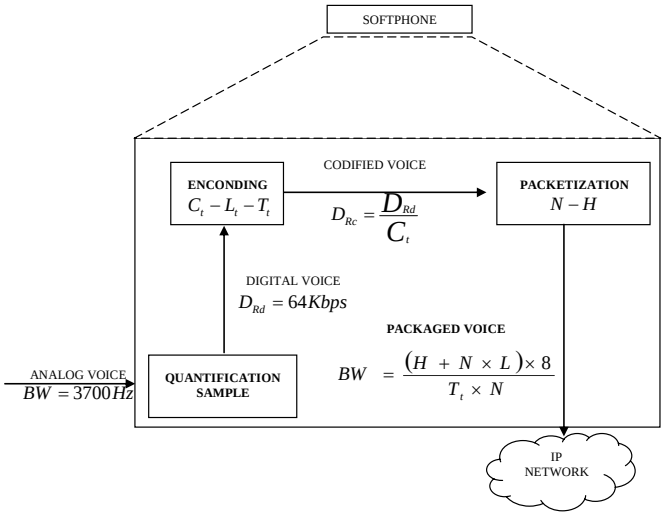

Fig. 1 Voice Packetization Proccess

2) Voice Packet Length

It's the result of the payload plus the lower layer headers as is shown in table I.

TABLE I. VOICE PACKET STRUCTURE

Protocol	Size (Bytes)
Voice	variable (codec)
RTP	12 (variable)
UDP	8
IP	20 (variable until 60)
L2	variable

Two codecs were used for the lab scenarios. The first codec is ITU G.711 standard known as μ-law, and the second codec is GSM used in mobile telephony. A brief characteristics summary about used codecs are shown in table II

TABLE II. USED CODECS CHARACTERISTICS

Codec	Sample Time	Payload (bytes)	Packets per second	Call BW	Objective MOS
G.711	20 ms	160	50	80 kbps	4,3
GSM	20 ms	33	50	29,2 kbps	3,7

The bandwidth is the product of packet transmission rate and the voice packet length as can be seen in equation (3). The encryption algorithm ciphers the payload or lower layer data affecting the total voice packet length.[7]

$$BW = P_l \times R_p \quad (3)$$

Where,

P_l is the packet length (Bytes), and

R_p is the packet transmission rate (pps)

The total supported calls in the system is described by the equation (4). The variables involved are: total link bandwidth – BW_{total}– in bps and call required bandwidth –BW_c–.

$$C = \frac{BW_{total}}{BW_c} \quad (4)$$

III. Encription Alghoritms for VoIP Networks

The information confidentiality is achieved with the use of encryption tools. It is necessary to establish security requirements for every network elements and functions with a risk analysis [9]. There are three functions to be protected over IP networks in VoIP applications: signalling, physical media, and key management.[8]

In the next section, the encryption methods supported by the protocol IETF SIP are described.

A. Signalling Encription Alghoritms

These algorithms cipher signalling messages to establish internetworking communication over the IP network according to the security polices [10].

Session Initiation Protocol –SIP– is an IETF signalling protocol used to create, modify, and to end call sessions over IP networks. The SIP protection is usually achieved by the use of two protocols: Transport Layer Security –TLS– and Secure/Multipurpose Internet Mail Extensions –S/MIME –. TLS is recommended by the IETF in the RFC 4346 [11] in order to prevent evesdropping attacks, message manipulation, and message recurrence.[12]

TLS offers authentication between clients and servers to achieve confidentiality and integrity during information exchange. TLS is composed by two layers. TLS record layer protocol maintains secure connection between terminals. The cryptographic certified negotiation must be completed before the data transmission beginning and it is a responsibility of the upper layer, TLS handshake protocol.[13]

Voice traffic usually goes over UDP but TLS goes over TCP and/or SCTP. In fact, secure SIP recommendations used TLS to guarantee secure signalling messages with secure and encrypted transport.

SIP secure, also known as SIPS, is the use of SIP supported by TLS and it's different to SRTP because TLS develops authentication between clients and servers, not end to end components, that's why it's necessary to establish a TLS session per each connected segment.[14], [15]

B. Media Encription Algorithms

Multimedia applications with audio, video or combination, uses encryption algorithms for secure transmission and establish the secure channel between end to end users [10].

1) Secure Real Time Protocol

SRTP is a protocol that stands for real time authentication, confidentiality and integrity for multimedia traffic [8], and it is described by the RFC 3711 [16]. SRTP provides protection with encryption keys for wired and wireless networks including bandwidth limited channels.[14], [15]

2) Secure Inter-Asterisk Exchange Protocol v2

IAX is an asterisk native protocol and the last version is IAX2. The protocol was designed to route signalling and voice traffic by a single port according to the RFC 5456. IAX2 can establish trunk links with servers that support the same protocol. The operation modes are composed by connection, exchange and end of connection.

SIAX2 is the encryption application over IAX2. The approach uses Advanced Encryption Standard –AES– algorithm with 128 bits over Asterisk servers.[2]

3) IP secure

IPsec uses UDP or TCP as transport layer protocol and can protect the call in establishing, control and information. Two services are provided: authentication header –AH–, and Encapsulating Security Payload –ESP–. Both methods increase the packet size after the IP header.

It's possible to have two operation modes. Transport mode encrypts the payload in each single packet, and tunnel mode provides encryption to the header and payload. The used algorithm is 3DES with a previously established key.

C. Key Management Encryption Algorithms

The key management and creation can be symmetric and asymmetric. The symmetric key needs a private key and an initialization vector. The keys are restricted to the involved nodes. The asymmetric key requires a private and a public key. The public key could be known by anyone but the private key must be hidden in the key generator node. The encryption is made with one key and the decryption with the other key, but both keys has a mathematical relationship.

The protocol used for cryptographic key agreement was ZRTP. The protocol has a negotiation with Diffie-Hellman algorithm and a previously shared secret key [8], [19]. ZRTP works with P2P communications but it doesn't support interconnection with different VoIP networks nor connection with traditional PSTN. The ZRTP practical implementation was done with a client-server application called ZFone.[10], [21]

IV. Network Scenarios

The network implementation was made in two scenarios. The first scenario was a traditional LAN where users are sharing the channel within a switch and the VoIP connections are controlled by an Asterisk server. The network scenario can be seen in the Fig. 2. The second scenario was a WAN with to independents Asterisk servers connected to individual LANS. The interconnection is made with a 2048 kbps PPP channel. The WAN scenario is showed in Fig. 3.

The measurements over the channels are implemented with a network analyzer attached to the servers and to the network clients.

Every single physical and logical scenario has a secure configuration with encryption algorithms. The QoS parameters and the bandwidth are measured with Wireshark using simultaneous calls as traffic generator. The throughput is analyzed after each probe.

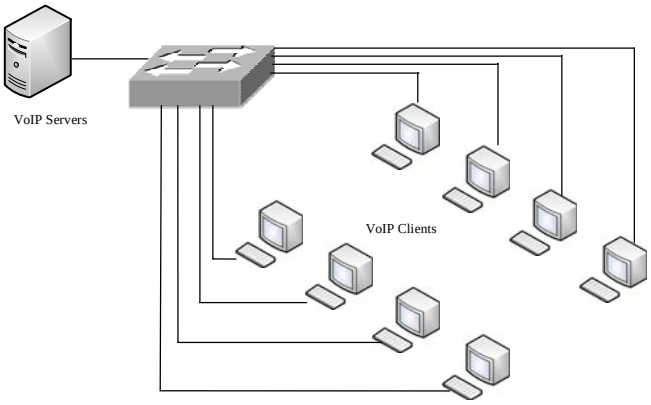

Figure 2 LAN scenario

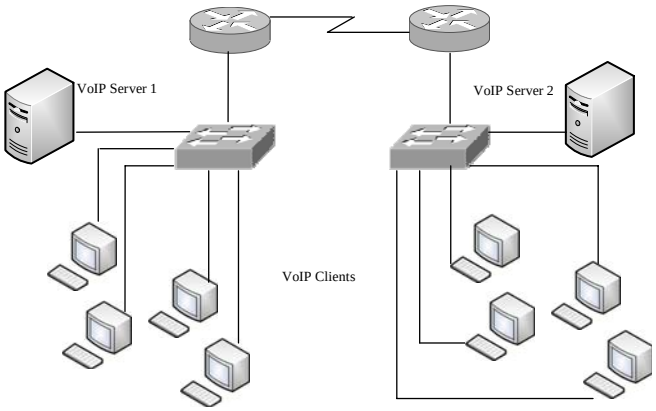

Fig. 3 WAN Scenario

The variables are evaluated in a bidirectional way. The outgoing traffic is represented by client-server communication (CLI-SER), and the ingoing traffic is represented by server-client communication (SER-CLI).

A. Used Software

Asterisk is the VoIP server. The encryption algorithms are implemented according to the server requirements and to the supported softphone. Table III summarizes the encryption software requirements.

B. Setting the Scenarios Up

The logical scenarios are designed based on the network scenarios of the Fig.2 and Fig.3. The tests try to analyze the bandwidth and the QoS parameters.

1) Tests on LAN

TLS, SRTP, ZRTP, IPSec and TLS+ZRTP are configured with compatibility in order to achieve a communication inside the same network. The measurements are made using the G.711 µ-law codec and GSM codec subsequently.

2) Tests on WAN

An IAX2 trunk channel is used between servers with mutual authentication as clients. Asterisk server has IAX2 as native protocol and it can offer encryption with SIAX2. Afterwards, TLS, ZRTP and TLS+ZRTP are implemented in client-server mode for each network.

As in the tests for LAN, The measurements are made with µ-law codec and GSM codec subsequently.

TABLE III. ENCRYPTION ALGORITHMS REQUIREMENTS

Encryption Protocol	*Operation Mode*	*Asterisk Version*	*Required Libraries*	*Softphone and Platform*
SRTP	Client-Client	Trunk-r61760	Minisip, libsrtp	Snom - Win
SIAX2	Server-Server	1.6	N/A	N/A - Win
TLS	Client-Server	1.6	N/A	Snom - Win
IPSec	Client-Client	N/A	Openssl, ipsec	Ekiga - Linux
ZRTP	Client-Client Client-Server	N/A	N/A	Snom – Win, Linux

V. RESULTS

The measurements were made for each scenario and afterwards the bandwidth and QoS parameters were compared with the used codec. Details at http://gissic.umng.edu.co

A. LAN µ-law Vs. LAN GSM

After the VoIP server configuration is made for transmitting traffic with RTP, the QoS parameters are measured.

1) Delay

With RTP as ideal model, Fig. 4 shows the delay results in the scenario. TLS and ZRTP have an efficient performance with no important delay variations. SRTP has a delay increase of 1.5 ms with G.711 µ-law codec and 0.5 ms with GSM codec.

The communication behavior between the server and client remains stable. For IPSec, the packet length rise dramatically and therefore the delay time increases between 1ms and 2ms. The codec is fundamental in packet delay for some encryption algorithms once the connection is established.

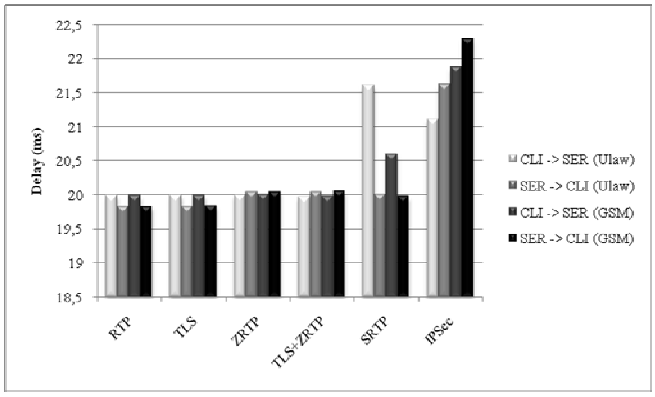

Fig. 4 Packet Delay LAN Scenario

2) Jitter

The jitter really depends on the encryption method as it can be seen in Fig. 5. The value increases in 13ms or even more

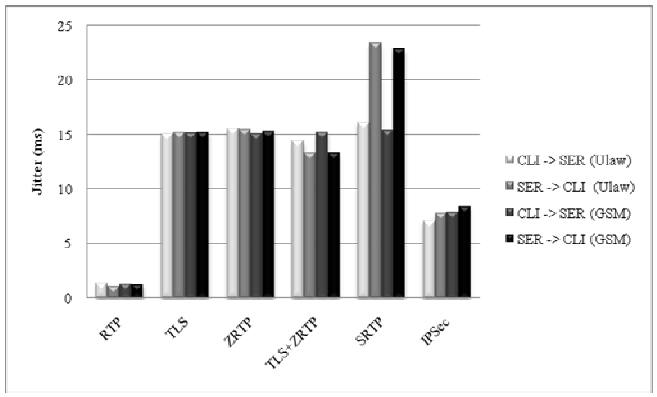

Fig. 5 Jitter LAN Scenario

The SRTP represents the worst case but it is noticeably different for client-server case. The IPSec encryption has the better jitter variation but its variation is bigger than the packet delay

3) Packet Lost

The algorithms developed for applications different than VoIP such as TLS and IPSec did not have significant packet lost. The results are shown in Fig. 6.

The other algorithms shows some packet lost but the number is almost insignificant because in a minute there are around 3000 packets and the results gives a 0.2%

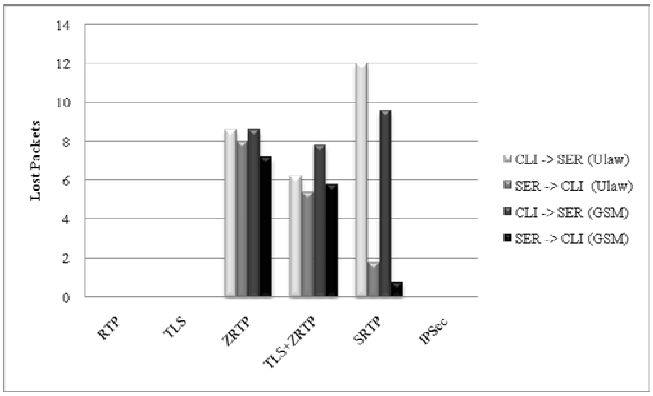

Fig. 6 Packet Lost LAN scenario

B. WAN µ-law Vs. WAN GSM

The communication end to end is ciphered using TLS, ZRTP and ZRTP + TLS. SIAX2 is configured for the trunk channel between the servers.

1) Delay

The outgoing traffic in the client-server mode does not have an appreciable difference compared with LAN scenario because the traffic doesn't have the PPP delay, but the returning server-client traffic is even less than 20 ms because of ZIAX2 protocol. Fig. 7 shows the results.

In fact, ZIAX2 by default has buffer options to achieve a minimum delay.

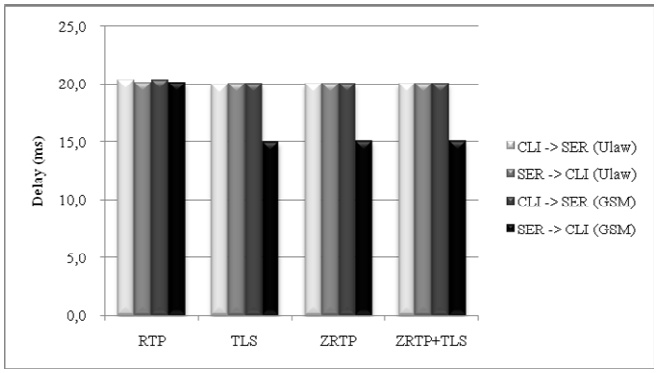

Fig. 7 Delay WAN Scenario

2) Jitter

The jitter results are similar to the LAN scenario but the WAN scenario doesn't have multiple inter-network equipment and neither suffer multipath delay. The GSM codec has a worst jitter time because the processing time is greater. It is owing to the fact that the compression level is better than µ-law.

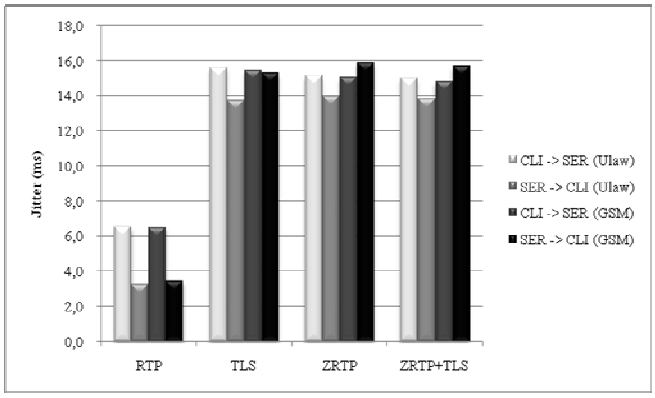

Fig. 8 Jitter WAN Scenario

3) Packet Lost

The PPP channel generates a packet lost between 0.1% and 1% according to Fig. 9. GSM packet lost rate is higher than µ-law because of the GSM packet length but the information lost is equivalent.

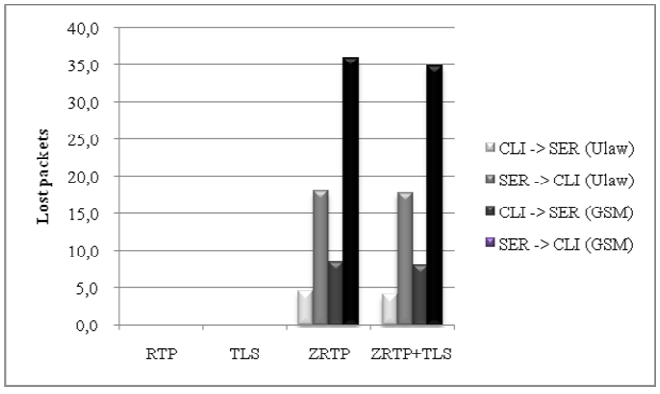

Fig. 9 Packet Lost WAN Scenario

C. LAN Vs WAN

In this section, we consider each codec for single analysis comparing LAN and WAN scenarios with the QoS parameters.

1) µ-law

The G.711 codec results are analyzed in the next section for the QoS parameters.

a) Delay

The difference between LAN in CLI-SER, SER-CLI is around 2 ms, and this difference is very similar with TLS, but delay rise in TLS and TLS+ZRTP and the difference is closer. The general delay is very similar in all tests near to 20 ms. The Fig. 10 shows results.

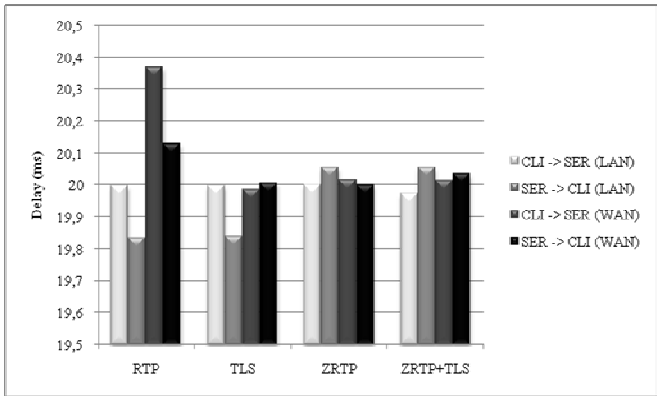

Fig. 10 µ-law codec delay

b) Jitter

Jitter for the µ-law codec in the LAN and WAN comparison can be seen in Fig. 11. The channel capacity between LAN and WAN is almost 97 Mbps, however the results shows very similar jitter with encryption algorithms. The general increase between no encryption and encryption codecs is around 7 times.

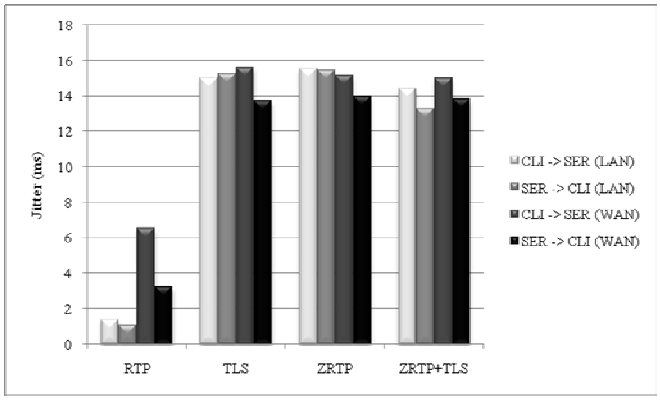

Fig. 11 µ-law codec Jitter

c) Packet Lost

RTP and TLS did not have loss packets in LAN and WAN tests for µ-law, but ZRTP and ZRTP+TLS had significant lost for SER-CLI WAN and LAN, around 0.6 % per minute. The result can be seen in Fig. 12.

2) GSM

As in µ-law codec, GSM codec will be evaluated for every QoS parameter showing the comparison between LAN and WAN.

a) Delay

The results can be seen in Fig. 13. The buffer gets into groups the GSM packets that arrive randomly in order to be sent periodically and as fast as possible. The server processing policies can modify the packet numbers that are transmitted in order to achieve the necessary requirements, by default the packet rate is 50 pps for 20 ms delay.

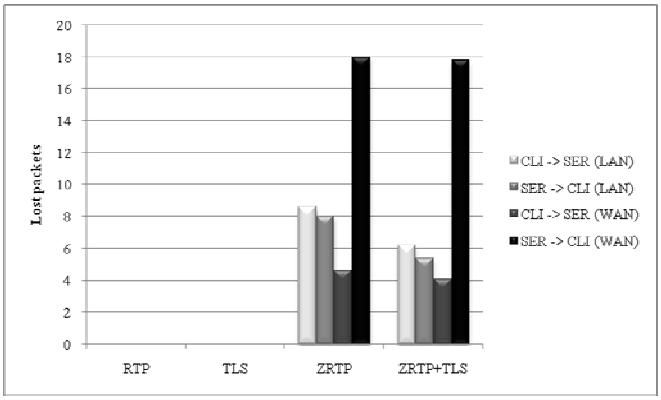

Fig. 12 µ-law codec Packet Lost

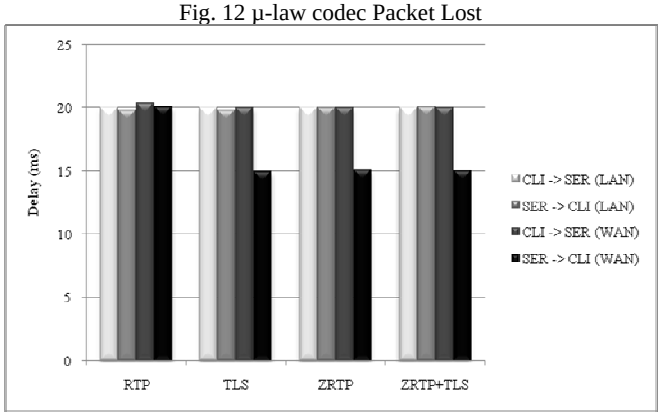

Fig. 13 GSM codec delay

b) Jitter

The cipher packet processing at WAN nodes raise the system jitter in 2 ms according to the Fig. 14. TLS has a stable behavior for every situation in GSM codec.

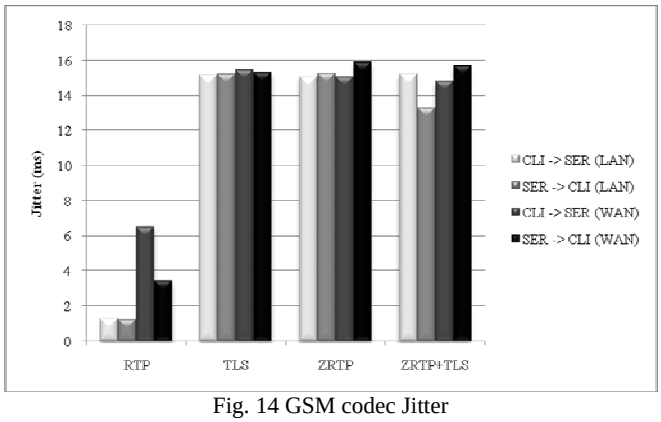

Fig. 14 GSM codec Jitter

c) Packet Lost

WAN had a total packet lost of 1% with ZRTP and ZRTP+TLS. RTP and TLS did not have loss packets. The results can be seen in Fig. 15.

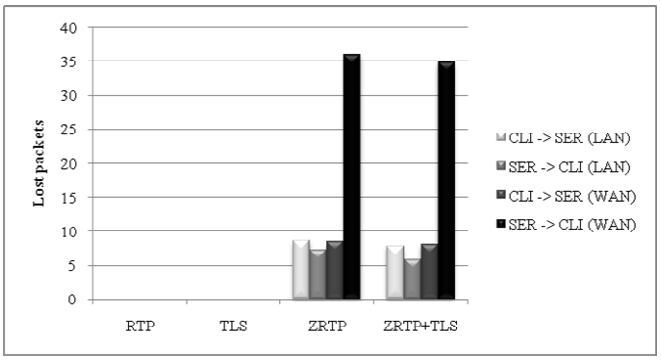

Fig. 15 GSM codec Packet Lost

D. Bandwidth Analysis

The packet voice length without encryption is summarized in table IV. The results were obtained with the network analyzer.

TABLE IV. VOICE PACKET LENGTH WITHOUT ENCRYPTION

	ETHERNET		PPP	
	ULAW	*GSM*	*ULAW*	*GSM*
RTP (Bytes)	226	99	206	79
IAX (Bytes)	218	91	198	71

The required bandwidth was calculated with measurements in a week and it was calculated with the server parameters. Table V shows the required bandwidth per call.

TABLE V. REQUIRED BANDWIDTH PER CALL WITHOUT ENCRYPTION

	ETHERNET		PPP	
	BW ULAW	*BW GSM*	*BW ULAW*	*BW GSM*
RTP (bps)	90400	39600	82400	31600
IAX (bps)	87200	36400	79200	28400

The packet length increases with the use of encryption algorithms and therefore the necessary bandwidth per call is increased too. The payload must to be transmitted with the same frequency with or without encryption generating and overload in the packet length with the use of encryption algorithms. The overload can be calculated for the bandwidth with the known packet length. Table VI shows the overload bandwidth for LAN and Table VII shows the overload bandwidth for PPP channel.

SIAX2 shows low efficiency with GSM codec. It was expected that the SIAX2 packetization would be similar to the traditional cipher methods. Even though, the packet length was of the same size that μ-law, although the payload is lower.

It's possible to calculate the maximum number of simultaneous supported calls in the system if the bandwidth per call is known. The calculations were only made for PPP channel, because the LAN bandwidth is assumed to be infinite for the clients quantity tested in the scenarios.

Table VIII shows the simultaneous supported calls over the WAN channel per encryption algorithm.

TABLE VI. BANDWIDTH OVERLOAD WITH ETHERNET HEADER

METHOD	ALGORITHM	OVERLOAD BW ETHERNET	
		ULAW	*GSM*
Signalling	TLS	0%	0%
Media	SRTP	4,42%	10,10%
	IPSEC	19,47%	43,43%
Keys Management	ZRTP	1,77%	4,04%
Other	ZRTP + TLS	1,77%	4,04%

TABLE VII. BANDWIDTH OVERLOAD WITH ETHERNET HEADER

METHOD	ALGORITHM	OVERLOAD BW PPP	
		ULAW	*GSM*
Signalling	TLS	0%	0%
	SIAX2	15,15%	221,13%
Media	SRTP	4,85%	12,66%
	IPSEC	21,36%	54,00%
Keys Management	ZRTP	1,94%	5,06%
Other	ZRTP + TLS	1,94%	5,06%

The PPP bandwidth was equivalent to an E1 channel of 2.048 kbps

TABLE VIII. PPP CHANNEL ENCRYPTED SUPPORTED CALLS

ALGORITHM	SUPPORTED CALLS	
	ULAW	GSM
ZRTP	24	61
ZRTP + TLS	24	64
IPSEC	20	41
SRTP	23	57
SIAX2	22	22

VI. DISCUSSION AND CONCLUSION

The results show a low performance in secure robust protocols. In fact, it's necessary to establish a relationship between secure polices and bandwidth needs before design the VoIP network. Higher security means low throughput but it's possible to achieve medium security with a reasonable throughput.

REFERENCES

[1] D. Butcher, "Security challenge and defense in VoIP infrastructures" IEEE Transactions on systems, man, and cybernetics. Vol 37, No. 6, pp 1152-1162, Nov 2007

[2] Clayton, Bradley. "Securing media streams in an Asterisk-based environment and evaluating the resulting performance cost". Rhode University. Sudafrica. Jan 2007.

[3] I. Baronák, M. Halás, "Mathematical Representation of VoIP Connection Delay", Dept. of Telecommunications, Slovak University of Technology. Prague, Slovak Republic, April 2008.

[4] Schulzrinne, H., Casner, S., Frederick R., Jacobson, V. "RTP: A Transport Protocol for Real-Time Applications". IETF RFC 3550. July 2003.

[5] Walker, John Q. A. "Handbook for Successful VoIP Deployment: Network Testing, QoS, and More". NetIQ Corporation. 2002

[6] C. Fernández, G. "Voz sobre IP". Departamento de Investigación, Universidad de Belgrano. Argentina. Agosto de 2002.

[7] Newport Networks Ltd., "VoIP Bandwidth Calculation". ISDN 91-052-01-0003-C. 2005.

[8] Gupta, P. Shmatikov, V. VMWare, Inc., Palo Alto. "Security Analysis of Voice-over-IP Protocols". IEEE, Computer Security Foundations Symposium,. 2007.

[9] R. Blom, E. Carrara, F. Lindholm, K. Norrman, M. Naslund, Ericsson Res., Ericsson AB, Stockholm, Sweden. "Conversational IP multimedia security". IEEEMobile and Wireless Communications Network, 2002.

[10] P. Thermos, A. Takanen. "Securing VoIP networks, Threats, Vulnerabilities, and Countermeasures". Addison Wesley. August 2007.

[11] T. Dierks, E. Rescorla. "The Transport Layer Security (TLS) Protocol Version 1.1". IETF RFC 4346. April 2006.

[12] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. SIP: Session Initiation Protocol. IETF RFC 3261, June 2002.

[13] Eren, Evren. Detken, Kai-Oliver. "Voice-over-IP Security Mechanisms – State_of:the:art, risk assessment, concepts and recommendations". Chile, 2007.

[14] L. Wang, P. K. Verma, A Network Based Authentication Scheme for VoIP, School of Electrical and Computer Engineering University of Oklahoma, IEEE, Tulsa, OK, USA.

[15] C. Roberts. "Voice Over IP Security. Centre for Critical Infrastructure Protection". New Zealand. 2005.

[16] M. Baugher, C. McGrew. Naslund, M., Carrara, E., Norrman K. "The Secure Real-time Transport Protocol (SRTP)". IETF RFC 3711. March 2004.

[17] M. Spencer, Digium, Inc.,B. Capouch, S. J.College, E. Guy,E. Truphone, F. Miller, Cornfed Systems, LLC,K. Shumard. IAX: Inter-Asterisk eXchange Version 2. RFC 5456, February 2009.

[18] Feng Cao and Saadat Malik, Cisco Systems, Inc. ."Vulnerability Analysis and Best Practices for Adopting IP Telephony in Critical Infrastructure Sectors". IEEE Communications Magazine. April 2006.

[19] P. Zimmermann. "ZRTP: Media Path Key Agreement for Secure RTP". IETF draft. Sept 2008.

[20] E. Kokkonen, M. Matuszewski,. Nokia Res. Center, Helsinki. "Peer-to-Peer Security for Mobile Real-Time Communications with ZRTP". 5th IEEE Consumer Communications and Networking Conference, 2008.

[21] S. Tangwongsan, and S. Kassuvan. "A Security Model of Voice Eavesdropping Protection over Digital Networks". proceedings of world academy of science, engineering and technology, volume 20, 2007. ISSN 1307-6884