Impact of Encryption on QoS in VoIP

Pedram Radmand
Digital Ecosystem Business Intelligence
Curtin University of Technology
GPO Box U1987, Perth, Western Australia 6845
Email: pedram.radmand@postgrad.curtin.edu.au

Alex Talevski
Digital Ecosystem Business Intelligence
Curtin University of Technology
GPO Box U1987, Perth, Western Australia 6845
Email: Alex.Talevski@cbs.curtin.edu.au

***Abstract*— This paper studies the impact of different encryption algorithms on the quality of Voice over Internet Protocol (VoIP). Assuring Quality of Service (QoS) is one of the primary issues in any IP based application that examines the voice quality of VoIP. This paper examines QoS in terms of lost packet ratio, latency and jitter using different encryption algorithms along with firewalling at the IP layer. The results of laboratory tests indicate that the impact on the overall performance of VoIP depends upon the bandwidth available and encryption used. Findings include the need for the provision of bandwidth for encryption, and even when adequate bandwidth is provided encryption algorithms can increase lost packet ratios and packet latency, and reduce. Overall, the results indicate the implementation of encryption algorithms may degrade the voice quality even if bandwidth is adequate.**

I. INTRODUCTION

The recent tendency towards geographically dispersed telecommunication and the migration of business communication to IP (Internet Protocol) infrastructure, has given rise to better methods of collaboration and interaction between personnel. This greater requirement is provided by video-conferencing, web-casting and instant messaging through Voice over IP (VoIP) because the capabilities of the internet and many private networks have ensured that all these functions are able to run across existing infrastructure with less cost. In other words, the key benefits of VoIP are very low cost, integrated voice and network of data, and voice and video on a single network [1].

One of the most attractive reasons for implementing VoIP is cost savings. The definition of costs is more involved than a simple phone bill at the end of the month and includes hardware requirements, training costs, potential switch over costs and loss of business in transition [2], but there are several ways that VoIP helps to reduce the business costs through lower usage cost, lower costs of maintenance and support, and reduced network infrastructure [3]. Most current VoIP applications provide a reasonable voice Quality of Service (QoS) that is currently lacking in practical security solutions. When VoIP technology is used in the workplace, it provides a good opportunity for hackers to access voice information during a VoIP call, because these are routed using insecure methods over the internet or any network [4]. Security issues will arise as long as IP networks are developed on shared media communication. Attackers try to hack into the network to gain access to user data or to disrupt the network services. Over the past, encryption has been presented as a potential solution to the security problems with VoIP decade. However little has been undertaken to determine the affect of encryption on QoS in VoIP.

This paper presents the results of laboratory tests to determine the affect of encryption on the QoS in VoIP. The discussion commences with coverage of the security issues faced, and an explanation of the QoS factors in VoIP implementations. An overview of the research method undertaken is presented followed by the data analyses and discussion of findings.

II. VOIP SECURITY ISSUES

One of the first security issues voiced by organizations implementing VoIP is the issue of confidentiality of voice conversations. Unlike traditional telephone networks, which are circuit-switched and relatively difficult to eavesdrop, voice traffic on converged networks is packet-switched and vulnerable to interception with the same technique used to sniff data on a LAN or WAN. Even an unsophisticated attacker can intercept and decode voice conversations [5].

By generating excessive traffic, attackers are also able to cause service disruption. This excessive traffic generated by the malicious user competes in terms of accessing the network resources along with the voice traffic, thereby causing a reduction in the voice quality. Hence the migration of business communication to Internet Protocol (IP) infrastructure, has given rise to security problems such as Denial of Services, Call Hijacking, Eavesdropping and Snooping, Man-in-The-Middle, and Phishing. As VoIP becomes more popular, so also does the concern for security.

In order to prevent these security problems a number of security solutions have been developed to protect the network infrastructure and user data as well as mitigate the risk of attack, such as firewalls, the Virtual Private Network (VPN) and encryption[6].

978-0-7695-4211-9/10 $26.00 © 2010 IEEE
DOI 10.1109/SocialCom.2010.112

VPN is a security mechanism that establishes a security association through tunneling. VPN can create a connection in Layer 2 and Layer 3 of the Open System Interconnection (OSI). A layer 2 connection does not need to perform an exclusive privacy protecting technique due to its mechanism that provides basic privacy. In contrast, a layer 3 VPN connection provides high security and protects user privacy through an IPSec tunnel and Secure Socket Layer (SSL) or Transport Layer Security (TSL), which are the most robust and effective tools available for securing communications [7].

Encryption is the process of rendering information unreadable by everyone except the recipient. Encryption keys work through encryption algorithms to convert plaintext into ciphertexts to encrypt and decrypt data. Although there are two broad categories of encryption keys: asymmetric, where more than one set of keys is utilized, and symmetric using the same key to encrypt and decrypt, this study used only the symmetric encryption algorithms DES, Triple DES, Blowfish-256, AES-128, AES-256 and RC2.

Cipher encryption speed can be considered a very important factor when assessing an encryption algorithm in terms of strength or weakness. Speed is a private key block cipher that supports variable parameters such as data length, which is the length of a plaintext or ciphertext, and key length [8].

Other features of encryption algorithms that are important to consider are key size, which contributes directly to the strength of the encryption, and whether key size affects speed. Table 1 presents a comparison of the chosen algorithms with regard to key size and speed.

Table 1: The main features of each encryption algorithm [6].

Algorithm	Key size(s)	Speed	Speed depends on key size	Security comments
RC2	40-1024	Very fast	No	May be secure
BF	128-448	Fast	No	Believed secure.
AES	128,192, 256	Fast	Yes	Secure
DES	56	Slow	No	Insecure
Triple DES	112/168	Very slow	No	Moderately secure

III. QUALITY OF SERVICES

QoS is a major issue in VoIP implementations. Overall voice quality is a function of many factors that include lost packets, jitter and latency. In VoIP quality means listening and speaking in a clear and continuous voice, without unwanted noise (jitter) and delays, and dropped sound. Obtaining suitable quality voice conversation and delivering real time data for VoIP over the Internet is required to minimize loss and delay of VoIP packets and also to reduce the jitter [10]. Issues such as these must be factored into measuring the QoS [6].

Another aspect of QoS refers to security of the conversations and reliability. Security or privacy of phone calls becomes exceptionally important for law enforcement officials [11] and those involved in national security. QoS can be measured in terms of lost packets, latency and jitter in a VoIP packet as suggested by Talevski and colleagues (2008) [4].

- Latency is measured by the time taken by voice packets to travel between two endpoints. Latency occurs when packets of data take longer than expected to reach their destination and causes some problems in voice quality [12]. In other words, latency is the time taken for data to get from the speaking person to the listener at the other end[13] .
- Lost packets is the failure of one or many packets of data travelling across the network to reach their destination. Packet loss is one of the important error types in digital communications [14].
- Jitter is unwanted variation of a periodic signal. In VoIP jitter is the variation in time between packets arriving that is usually caused waiting insider router queues caused by congestion or a change in path [15]. No jitter occurs where a network has no variation in packet arrival times.

QoS for IP networks, especially VoIP is one that has received significant amount of attention in recent years. There are a number of factors, some controllable and some uncontrollable, that affect voice quality and need to be considered.

(a) Bandwidth is the key for voice quality and adequate bandwidth is the most important factor in guaranteeing quality for VoIP. This is one of the greatest challenges in networks today; how to achieve good voice quality with limited and often shared bandwidth [16].

(b) Codec is a signaling format for sending and receiving information when a call is made over the Internet [17]. A codec with a higher bandwidth provides better voice quality and less lost packets and latency.

(c) Area network is the arrangement or mapping of the network elements in the network. Area network is the physical and logical interconnection between nodes of network elements [18], commonly applied as LANs (Local Area Networks), WANs (Wide Area Networks) and MANs (Metropolitan Area Networks).

IV. IMPACT OF SECURITY ON QUALITY OF SERVICES

During the implementation of security protocols in VoIP applications, QoS protocols must be adopted to meet the requirements of transmission parameters such as lost packets, jitter and latency. In fact, QoS protocols try to meet the imposed requirements using different features such as packet classification, queuing mechanisms, header compression, and congestion avoidance strategies. Unfortunately, such features cannot be used to advantage in combination with security protocols as they utilize fields in the IP header. Therefore, when security protocols are implemented, the possible choices of QoS protocols are limited [19].

V. DESIGN

Two LAN network areas connected via two Cisco 2500 routers were used as the base platform. The two routers were connected via a serial link enabling them to ping each other. By also configuring the Ethernet interfaces of the routers to establish a connection from the attached computer from LAN to each router, the two computers from two different area networks were able to ping each other (see Figure 2).

Each packet carrying voice data travelling between the sender and receiver was captured using Wireshark. The Wireshark output was then converted to XML. It means, for capturing the payload of each packet, which travels between two computers and carries the voice data, the Wireshark file should be converted to XML file and then XHTML. Different scenarios were conducted in the test network at three different bandwidth speeds. This design used Netmeeting as the Conferencing software, Wireshark as the packet sniffer, OpenVPN as the VPN software, which enables us to implement different encryption algorithms and

For calculating these three factors such as lost packet, latency and jitter, the XHTML file should be exported to an Excel file. These factors are calculated through two tags such as data and timestamp. In fact, data helps to find the lost packet ratio and timestamp can be applied for calculating latency and jitter.

Three scenarios were conducted in the test network to measure the impact of the different encryption algorithms on VoIP:

(a) Without encryption and Windows Firewall: Running Netmeeting, Wireshark and disabling Windows Firewall on both laptops.

(b) With Windows Firewall: Running Netmeeting, Wireshark and enabling Windows Firewall on both laptops.

(c) With Windows Firewall and different encryption algorithms: Running Netmeeting, Wireshark, enabling Windows Firewall and OpenVPN with different encryption algorithms on both laptops.

The measurement of the dependent variables, latency, jitter and lost packet in the test network was used to assess the impact of different area networks and bandwidths on QoS using the above three scenarios.

VI. DATA ANALYSIS

Five different encryption algorithms were implemented with three different bandwidth speeds in the laboratory to measure the degree of latency by different encryption algorithms.

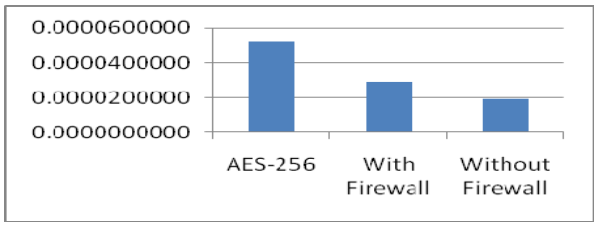

Figure 3: Latencies at 19kbps using AES-256 vs no encryption

Figure 3 shows the degree of latency in the 19k bandwidth in three different scenarios: AES-256, With Firewall and Without Firewall. As can be observed from the diagram, implementing encryption in the 19k bandwidth generates a greater degree of latency of around 0.0000050 seconds. Meanwhile, if any security schemas such as encryption or firewalls are removed, the latency is reduced to less than 0.0000020. It should be mentioned that implementing firewalls in this bandwidth generates latency of 0.0000030 seconds.

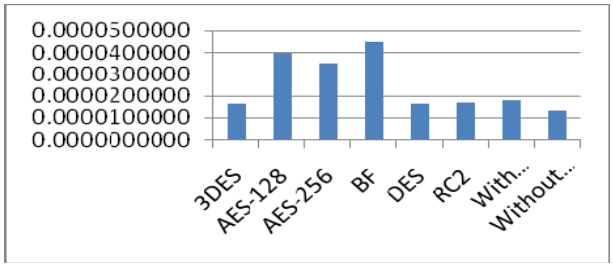

Figure 4: Latency 38kbps

Figure 4 shows the degree of latency in the 38k bandwidth. The latency was measured in eight different scenarios including the six different encryption algorithms, and With Firewall and Without Firewall. As the diagram shows, implementing the BF encryption algorithm in the 38k bandwidth generates a great deal of latency, nearly 0.00004500 seconds and also generates the most amount of latency in comparison with others. On the other hand, implementing without any encryption algorithms or firewall (Without Firewall) has the least degree of latency.

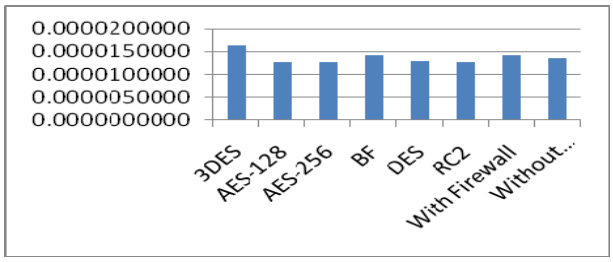

Figure 5: Latency 64k

Figure 5 shows the degree of latency in the 64k bandwidth when implementing different encryption algorithms, and With Firewall and Without Firewall. As can be seen, implementing a 3DES encryption algorithm in the 64k bandwidth is the worst scenario in terms of latency because it generates 0.00001600 seconds which is the greatest degree of latency in comparison with other encryption algorithms and scenarios.

Five different encryption algorithms have been implemented in five different bandwidth speeds in the laboratory to measure the degree of jitter by different encryption algorithms.

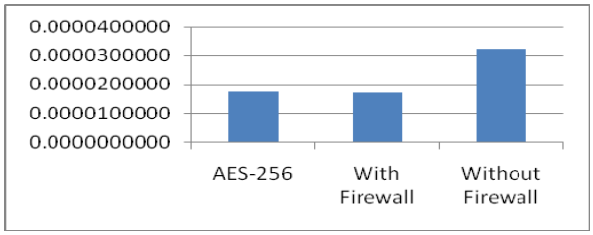

Figure 6: Jitter 19kbps vs no encryption

Figure 6 shows the degree of jitter in three different scenarios: AES-256, With Firewall and Without Firewall in the test network in the 19k bandwidth. As can be seen, the degree of jitter is increased when both firewall and encryptions are removed, exceeding more than 0.00003000 seconds. Meanwhile, if an encryption algorithm such as AES-256 as well as a firewall are implemented, the degree of jitter is reduced to almost half. Implementing a firewall without any encryption algorithms has slightly less jitter than implementing encryption algorithms.

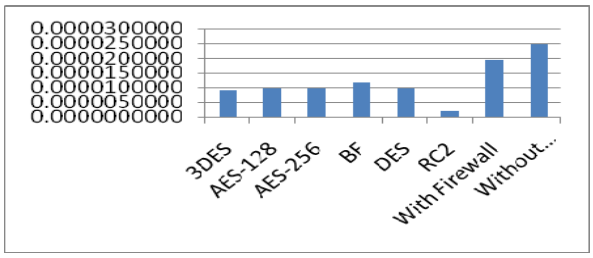

Figure 7: Jitter 38k

Figure 7 shows the degree of jitter in the selected encryption algorithms, With Firewall and Without Firewall in the test network in the 38k bandwidth. This figure shows that implementing encryption algorithms decreases the degree of jitter. In particular, the RC2 encryption algorithm has the least degree of jitter in comparison with other encryption algorithms. Meanwhile, removing encryption algorithms along with firewalls dramatically increased the amount of jitter in the 38k bandwidth and the Without Firewall had the most degree of jitter in this bandwidth.

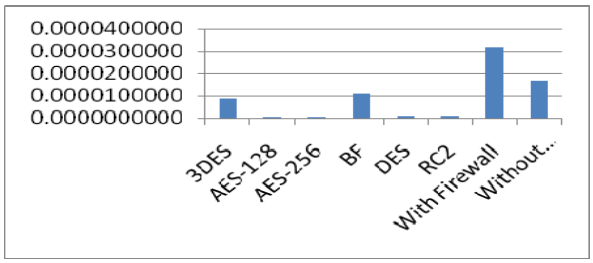

Figure 8: Jitter 64k

Figure 8 illustrates the degree of jitter in many different encryption algorithms, With Firewall and Without Firewall in the test network in the 64k bandwidth. As can be seen,

the degree of jitter is negligible when encryption algorithms are implemented and when they are removed the degree of jitter is increased. With Firewall generates the most degree of jitter in the 64k bandwidth. However, removing the firewall generates less jitter than running the firewall, but it still generates a significant degree of jitter in comparison with implementing encryption algorithms in this bandwidth. The best case scenario in terms of the degree of jitter, is implementing AES, DES and RC2 encryption algorithms.

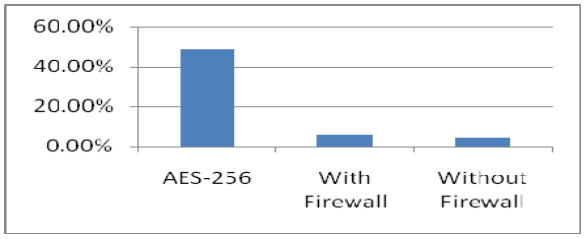

Figure 9: Lost Packet Ratio at 19k using AES vs no encryption

Figure 9 shows the degree of lost packet ratios in the chosen encryption algorithms, With Firewall and Without Firewall in the test network in the 19k bandwidth. It is clear that the lost packet ratio jumps to around 50% when AES-256 is run. The lost packet ratio is significantly reduced when the encryption algorithm is removed and this is reduced more when the firewall is removed as well. Without Firewall has the least lost packet ratio in the 19k bandwidth.

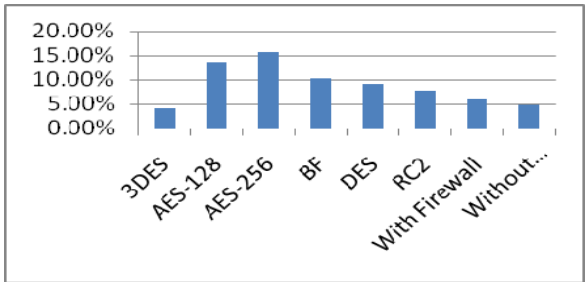

Figure 10: Lost Packet Ratio at 38k using AES versus no encryption.

Figure 10 illustrates the degree of lost packets in the chosen encryption algorithms, and With Firewall and Without Firewall in the test network in the 38k bandwidth. As can be seen, when encryption algorithms except 3DES are implemented, the lost packet ratio is increased. However, the lost packet ratio is improved by implementing 3DES encryption in this bandwidth, but it appears that by removing encryption algorithms and the firewall the lost packet ratio is improved. According to the Excel files, there are numerous Not Found packets at the beginning of connection with the two AES encryption algorithms. This increases their lost packet ratio due to establishing the connection at the beginning.

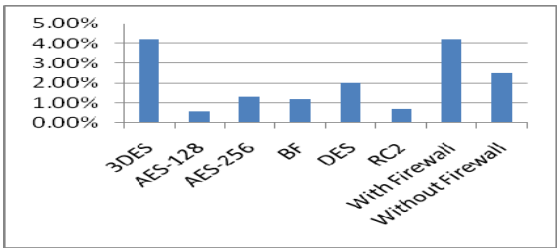

Figure 11: Lost Packet Ratios at 64k

Figure 11 indicates the degree of lost packet ratio in the encryption algorithms used, With Firewall and "Without Firewall in the test network in the 64k bandwidth. It can be seen from the diagram, in contrast with bandwidth of 38k in which 3DES has the lowest lost packet ratio, the 3DES encryption algorithm generates the greatest lost packet ratio in comparison with the others. By implementing AES-128 encryption in this bandwidth, the lost packet ratio is reduced. This encryption has the least lost packet ratio in the 64k bandwidth.

VII. DISCUSSION

Information security is a trade-off between ease of use and convenience and restriction for protection from misuse. Similarly security in VoIP can be defined as the process of achieving a balance between secure communications and high quality communications.

Table 2: The encryption algorithm assessments

Rating	Security	Speed	Latency	Jitter	Lost packets
1	DES	3DES	BF	BF	AES-128
2	3DES	DES	AES-128	AES-256	AES-256
3	RC2	AES-256	AES-256	AES-128	RC2
4	BF	AES-128	3DES	DES	DES
5	AES-128	BF	DES	3DES	3DES
6	AES-256	RC2	RC2	RC2	BF

The bar charts above illustrate the effects of implementing the chosen encryption algorithms on voice quality in VoIP in an effort to establish which encryption algorithm is most effective in different bandwidths. Table 2 summarizes the results showing desired factors of security, speed, latency, jitter and lost packets for the selected encryption algorithms, rating the effectiveness of each in ascending order (1=low and 6=high).

VIII. CONCLUSION

This research examined the impacts of implementing a number of encryption algorithms on the quality of service in VoIP with the affects being measured in terms of latency, jitters and lost packets. Bandwidth limitation is one of the major issues in the VoIP network, so different area networks, bandwidths and encryption algorithms have been investigated in this research. The results show that the three factors of QoS, latency, jitter and lost packets, are all improved through increasing bandwidth. However experiments in the laboratory demonstrated that by implementing encryption algorithms the amount of jitter is decreased, but significantly raised the degree of latency and lost packets that sometimes depend on the bandwidth speeds, leading to VoIP becoming unusable. Employing encryption algorithms in a VoIP environment completely depends on required applications and a single answer is not forthcoming and much depends upon the desired factor rated most important.

In the search for the encryption algorithm providing an acceptable level of security and in addition to the best quality of voice the following recommendations are offered.

The RC2 encryption algorithm is recommended as the most suitable encryption algorithm, when users are seeking features such as speed, least latency and jitter. The RC2, unlike DES, algorithm is very fast and provides the least latency and jitter as well as an acceptable level of lost packets. It means if speed is desired then the RC2 is the most effective. However, this encryption algorithm provides only moderate security, but is recommended in some environments where speed and voice quality have priority over security. It is concluded form the results that DES is the most ineffective encryption algorithm in terms of security and speed among those which have been examined in this paper.

In addition, this paper indicated that the BF and AES encryption algorithms present the best security among those examined in this research. Therefore, in a situation where security is the most important objective, then AES-256 is the most effective and DES the most ineffective. Where latency or jitter is the most important, then RC2 is superior and BF is the most inferior.

Also, this research demonstrated that BF is the most effective algorithm for minimizing lost packets ratios in contrast to AES-128 which rates the lowest for this factor. Furthermore, it should be mentioned that the BF encryption algorithm provides an acceptable level of security, which is *Believed Secure*, as well as less impact on voice quality than the AES encryption algorithm. Both encryption algorithms are recommended in some situations where security is desirable, such as financial and army applications. However, the AES encryption algorithm provides better security than BF, but AES has a greater impact on QoS in VoIP applications than BF. Further research is needed to identify factors that may affect voice quality, such as congestion, routing protocol, different codec and type of network determine the effects these have upon the QoS in VoIP.

REFERENCE

[1] E. T. M. Aire, B.T. Linde, L.P. , "Implementation Considerations in a SIP based secure Voice over IP Network," in *AFRICON, 2004. 7th AFRICON Conference in Africa*. vol. 1 Dept. of Electr., Electron. & Comput. Eng., Pretoria Univ, 2004, pp. 167-172.

[2] Cisco, "Cisco IP communications solutions." vol. 2008, 2005.

[3] NetLojix., "Voice Over IP Revolutionizing the way Businesses Communicate." vol. 2009, 2004.

[4] A. Talevski, Chang, E., and Dillon, T, "Secure and Mobile VoIP," in *Convergence Information Technology, 2007. International Conference on*, 2007, pp. 2108-2113.

[5] T. B. B. Porter, M. Cross, j. Kanclirz, A. Rosela, C. Shim, and A. Zmolek, "VoIP Threats." vol. 2009, 2006.

[6] Z. A. Barnes, "Is Implementation of Voice over Internet Protocol (VoIP) More Economical for Businesses with Large Call Centers," Bowie State University 2005.

[7] R. Weaver, "VPN," in *Network Defense and Countermeasures*. Perth: Thomson, 2006.

[8] Y. Zheng, "The Speed Cipher." vol. 2009, 2009.

[9] A. Klein, "Comparison of ciphers." vol. 2009, 2008.

[10] Cisco, "Understanding Delay in Packet Voice Networks,." vol. 2008, 2007.

[11] N. P. Thanthry, R. Namuduri, K. , "Voice over IP security and law enforcement," in *Security Technology, 2005. CCST '05. 39th Annual 2005 International Carnahan Conference on* Dept. of Electr. & Comput. Eng., Wichita State Univ., KS;, 2005, pp. 246-250.

[12] N. Unuth, "What Affects Voice Quality in VoIP Calls. ." vol. 2009, 2009.

[13] N. C. Sulaiman, R. Chester, G. , "Impact of security on voice quality in 3G networks," in *Industrial Electronics and Applications, 2008. ICIEA 2008. 3rd IEEE Conference on*, 2008, pp. 1583-1587.

[14] TechTarget., "Microsoft Windows Firewall security.." vol. 2009, 2007.

[15] M. A. Manousos, S. Grammatikakis, I. Mexis, D. Kagklis, D. Sykas, E. , "Voice Quality Monitoring and Control for VoIP," *IEEE Internet Computing, ,* vol. 9, pp. 35- 42, 2005.

[16] N. Unuth, "Delay In VoIP. Retrieved October ". vol. 2009, 2009.

[17] W. ISP, "VoIP Codecs." vol. 2009, 2008.

[18] S. Tanenbaum, "Area Network," in *Computer Networks, Fourth Edition.* Perth: Prentice Hall, 2003.

[19] R. B. Barbieri, D. Rosti, E. , "Voice over IPSec: Analysis and Solutions," in *Computer Security Applications Conference, 2002. Proceedings. 18th Annual* Dipt. di Sci. dell'Informazione, Univ. di Milano, Italy;, 2002, pp. 261- 270.