VoIP: Making Secure Calls and Maintaining High Call Quality

ABSTRACT

Modern multimedia communication tools must have high security, high availability and high quality of service (QoS). Any security implementation will directly impact on QoS. This paper will investigate how end-to-end security impacts on QoS in Voice over Internet Protocol (VoIP). The QoS is measured in terms of lost packet ratio, latency and jitter using different encryption algorithms, no security and just the use of IP firewalls in Local and Wide Area Networks (LAN and WAN). The results of laboratory tests indicate that the impact on the overall performance of VoIP depends upon the bandwidth availability and encryption algorithm used. The implementation of any encryption algorithm in low bandwidth environments degrades the voice quality due to increased loss packets and packet latency, but as bandwidth increases encrypted VoIP calls provided better service compared to an unsecured environment.

1. 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 and web-casting through Voice over IP (VoIP). The key benefits of VoIP are low cost, blended voice and network services, and multimedia based communication on a single network [3].

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 [4]. 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 [5]. As organizations begin to combine voice and data traffic into a single converged network, they must ensure manageability, performance and full security including authorization, authentication, confidentiality and integrity [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 public internet [6]. Security issues will arise as long as IP networks are developed on shared public communication infrastructure. Attackers can easily hack into the network to gain access to user data or to disrupt the voice call. Data encryption has been presented as a potential solution to the security problems with VoIP. However, little research has been undertaken to determine the affect of encryption on QoS in VoIP.

This paper presents the results of laboratory tests to measure the affect encryption based security have on QoS in real world VoIP implementations. The discussion commences with coverage of the security issues faced, and an explanation of the QoS factors in VoIP implementations in Section 2. Section 3 provides an overview of the research method undertaken and the test network design. Section 4 presents the analyses of data. The discussion on findings is in Section 5 followed by the conclusion.

2. VOIP SECURITY AND QOS ISSUES

2.1 VoIP Security Issues

One of the first security concerns voiced by organizations implementing VoIP is 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 Local Area Network (LAN) or Wide Area Network (WAN). Even an unsophisticated attacker can intercept and decode voice conversations [7].

As VoIP uses the IP infrastructure, it is also susceptible to malicious service interruptions caused by denial of service (DoS) attacks. By generating excessive traffic, attackers can overwhelm network services making VoIP communication unusable by legitimate users.

Hence, the migration of business communication to IP (Internet Protocol) infrastructure, has given rise to security problems such as Denial of Services, Call Hijacking, Eavesdropping, Snooping, Man-in-The-Middle, and Phishing. As VoIP becomes more popular, the concern for security will increase.

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 malicious service disruptions. Some of these solutions use one or more techniques such as end device protection using firewalls, and transit communication protection via Virtual Private Network (VPN) and encryption [2].

A VPN is a security mechanism that establishes a security association through tunnelling. A VPN can create a secure connection in Layer 2 and Layer 3 of the Open System Interconnection (OSI) communication stack. 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 more robust and effective tools for securing communications. The end-to-end encryption employed is based on the exchange of a secret key pair used for data encryption. After this operation, all data between the two nodes are encrypted [8].

© ACM, 2010. This is the author's version of the work.
It is posted here by permission of ACM for your personal use. Not for redistribution. The definitive version was published
in the 8th International Conference on Advances in Mobile Computing & Multimedia, ISBN: 978-1-4503-0440-5, MoMM 2010. http;//dx.doi.org/10.1145/1971519.1971532

Encryption is the process of rendering information unreadable by everyone except the recipient. Encryption keys work through encryption algorithms to convert plaintext into ciphertexts (encrypt) and vice versa (decrypt). There are two broad categories of encryption keys: asymmetric key, where more than one set of keys is utilized, and symmetric key using the same key to encrypt and decrypt communication packets. This study only looks at symmetric encryption algorithms, such as DES, Triple DES (3-DES), Blowfish-256, AES-128, AES-256 and RC2 because these encryption algorithms perform their operations faster than asymmetrical algorithms. Speed in encryption and decryption is important for real-time VoIP communication.

Cipher encryption speed can be considered a very important factor when assessing an encryption algorithm in terms of strength or weakness. The speed measure includes the amount of time for ciphering/deciphering that supports variable parameters such as data length, which is the length of a plaintext or ciphertext, and key length [9].

Figure 1 shows a comparison of cipher encryption speeds for the chosen encryption algorithms. Another important feature of encryption algorithms is key size, which contributes directly to the strength of the encryption, and whether key size affects speed. Table 1 presents a comparison of the selected encryption algorithms with regard to key size and speed.

2.2 VoIP Quality of Service (QoS)

QoS is a major requirement in VoIP implementations. In VoIP, quality means listening and speaking in a clear and continuous voice, without unwanted noise, long delays, and dropped sound. In order to obtain suitable quality voice conversation and delivering real time data for VoIP over the Internet, the network needs to minimize loss and delay of VoIP packets and also reduce jitter [10]. Issues such as these must be factored into measuring QoS [2].

QoS can be measured in terms of lost packets, latency and jitter (unwanted noise) in a VoIP packet as suggested by Talevski and colleagues (2008) [4]:

- Latency or delay is measured by the time taken for voice packets to travel between two endpoints. It is the time taken for a VoIP call to get from the speaking person to the listener at the other end [11]. The latency should be as low as possible as high latency will disrupt bi-directional conversations as they speakers will not be in sync with each other [12].

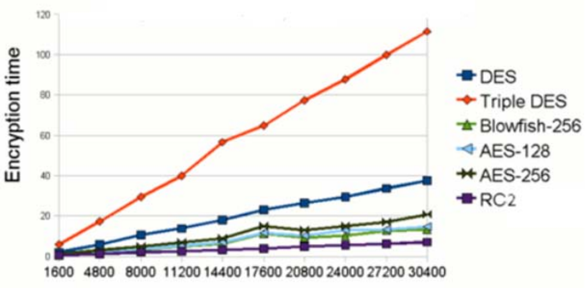

Figure 1: Cipher Encryption Speeds [1].

- Lost packets is the failure of one or more packets of data travelling across the network to reach their destination. Packet loss is one of the important error types in digital communications [13]. In VoIP, loss packets will cause a call to break up, and too much of this will make the conversation uncomprehendable.

- Jitter is the variation of a periodic signal. In VoIP, jitter is the variation in time between packets arriving that is usually caused by delays inside router queues, due to congestion or a change in network path [14]. No jitter occurs where a network has no variation in packet arrival times. High jitter means the voice quality is inconsistent during a VoIP call session.

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 a good voice quality with limited and often shared bandwidth [15].

(b) Codec is a signalling format for sending and receiving information when a call is made over the Internet [16]. A codec with a higher compression ratio and faster algorithm 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

Table 1: The main features of each encryption algorithm [2].

Algorithm	Key size(s)	Speed	Speed depends on key size?	Security / comments
RC2	40-1024	Very fast	No	May be secure for moderate numbers of encrypted sessions of moderate length.
Blowfish (BF)	128-448	Fast	No	Believed secure.
AES	128,192, 256	Fast	Yes	Secure
DES	56	Slow	No	Insecure
Triple DES (3DES)	112/168	Very slow	No	Moderately secure

logical interconnection between nodes of network elements [17], commonly applied as LANs (Local Area Networks), WANs (Wide Area Networks) and MANs (Metropolitan Area Networks).

2.3 Impact of Security on QoS

The implementation of security protocols in VoIP applications would require additional resources, which will impact on the quality of the voice call. 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 [18].

Previous works have only measured the impact of encryption algorithms on VoIP applications in three different bands in WANs [19]. In this paper, the impact of encryption algorithm in terms of lost packet ratio, latency and jitter on both LAN and WAN with different bandwidths are examined. The best encryption algorithm that provides acceptable security along with acceptable quality of services, has been nominated and discussed.

3. RESEARCH METHODOLOGY

The research method applied for this research is a laboratory experiment. It entails the gathering of data from experiments and the analysis of that data to build findings that answer the research question and are meaningful in the context of the research.

Encryption Algorithm and Bandwidth are the independent variables. These characteristics have been chosen from previous literature on QoS in VoIP. The dependent variables are Latency, Jitter and Lost packets. These variables define the quality of a VoIP call. In the context of this research “Unacceptable bandwidths” is defined as that which cannot provide an average latency of less than 0.050ms seconds as well as that bandwidth, which generates more than 20% lost packet ratios. "A significantly detrimental impact on QoS" is defined as any impact, which reduces QoS to the point where VoIP communication is unacceptably poor.

3.1 VoIP Network Design

Two network areas have been configured in the test network representing a LAN and WAN. The LAN was represented by two computers connected via a cross cable and the WAN was represented by connecting two groups of computers via two Cisco 2500 routers 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 a LAN to each router, the two computers from two different area networks were able to communicate with each other (see Figure 2). The configuration of the test network is as follow:

- 100 Mbps bandwidth for the LAN.
- Three different bandwidths of 19k, 38k and 64k for the WAN.

For measurement of impact of implementation of encryption algorithms to VoIP, different scenarios were conducted in the test network at 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 Windows operating system from Microsoft along with its Firewall feature. Netmeeting was used as the VoIP client as it allows for peer-to-peer communication and it allows the use of different encryption algorithms through a VPN client.

Each packet carrying voice data travelling between the sender and receiver was captured using Wireshark. The Wireshark output was then converted to XML.

For calculating these three factors such as lost packet ratio, latency and jitter, the XML file was 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 was used 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) No Security: Running Netmeeting, Wireshark and disabling Windows Firewall on both PC. No encryption algorithm was used for the VoIP calls.

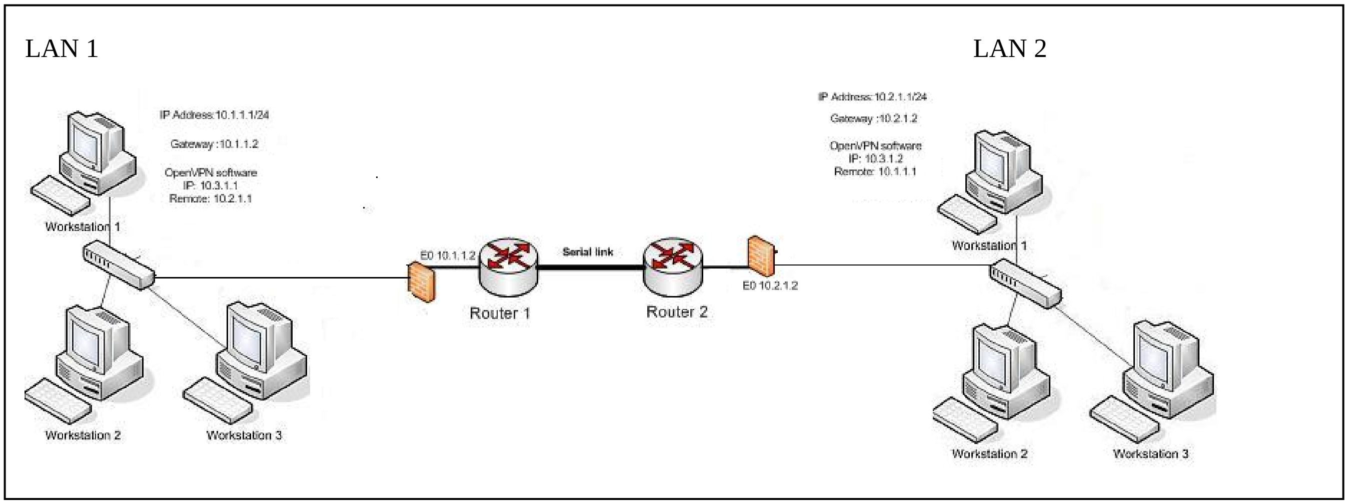

Figure 2: The WAN Test Network Design

(b) Firewall Only: Running Netmeeting, Wireshark and enabling Windows Firewall on both PC. No encryption algorithm was used for the VoIP call.

(c) With Windows Firewall and different encryption algorithms: Running Netmeeting, Wireshark, enabling Windows Firewall and OpenVPN with different encryption algorithms for VoIP calls between the sender and receiver.

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. As this research was conducted in an isolated laboratory, it was not necessary to measure the dependent variable regularly many times. Once the experiment recorded consistent average latency time, jitter and lost packet for each scenario, the results were reliable throughout the experiments.

4. DATA ANALYSIS

Five different encryption algorithms were implemented with three different bandwidth speeds in the laboratory to measure the degree of latency, jitter and lost packet ratio by different encryption algorithms.

The lab experiment results in a low bandwidth situation, where the bandwidth is 19kbps, show that implementation of encryption algorithms causes a high degree of latency of around 0.50ms and that the lost packet ratio jumps to around 50%. However, implementing No Security has slightly less jitter than implementing encryption algorithms. As such a low bandwidth makes it difficult to implement sufficient quality in VoIP calls, the results of 19kbps bandwidth speed is not presented it this section.

4.1 Latency

Figure 3 shows the degree of latency for three different bandwidth using different security encryption algorithms, “Firewall” and “No Security”.

As it can be seen from Figure 3, the degree of latency is improved by increasing bandwidth.

As the diagram shows, implementing the BF and AES encryption algorithms in the 38kbps bandwidth generate a great deal of latency, which is about 0.040ms. In contrast, other encryption algorithms and scenarios does not largely impact on QoS in terms of degree of latency.

The diagram also indicates that in 64kbps, the degree of latency would not be influenced by implementing the security schemas. This figure reveals that implementing a 3DES encryption algorithm is the worst encryption in terms of high latency, which is around 0.016ms and is the greatest degree of latency in comparison with other encryption algorithms in 64k bandwidth, while AES encryption has the least degree of latency.

In addition, the degree of latency for a LAN is shown in 100Mbps. It indicates that implementation of security schemas such as encryption algorithms and firewall does not negatively affect the degree of latency.

Overall, the degree of latency is not influenced by implementing encryption algorithms and firewall where the bandwidth is increased from 38Kbps to 64Kbps or 100Mbps,

4.2 Jitter

Figure 4 shows the degree of jitter ratios. It reveals that the degree of jitter is improved by increasing bandwidth except in scenario of Firewall Only security implementation. This means, the degree of jitter is risen by changing the bandwidth from 38kbps to 64kbps. However, in a LAN (100Mbps) the amount of jitter is dropped to almost 0ms.

As can be observed from the figure, implementing RC2 encryption algorithm decreased the degree of jitter dramatically, while the degree of jitter is higher when no encryption algorithm is used.

In a WAN, the degree of jitter is reduced drastically for DES,AES and RC2 encryption algorithms when the bandwidth increases to 64kbps, whereas the jitter is high for VoIP communication without any encryption algorithms and activating Windows Firewall only. In a firewall only scenario, the degree of jitter increases to 0.032ms when the WAN bandwidth increases, which is the greatest degree of jitter among all scenarios.

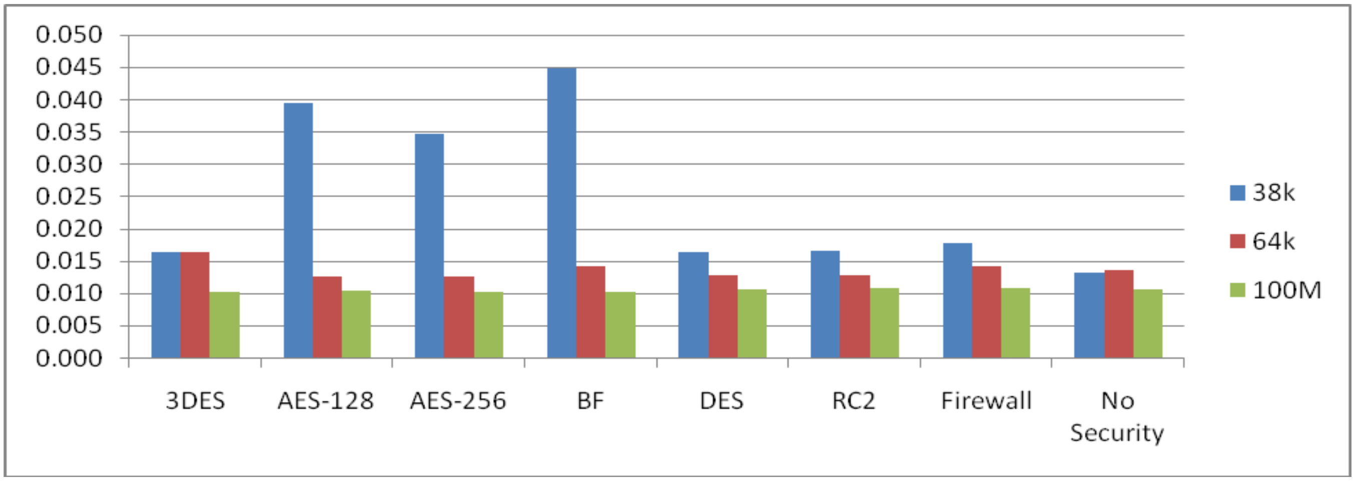

Figure 3: Degree of Latency

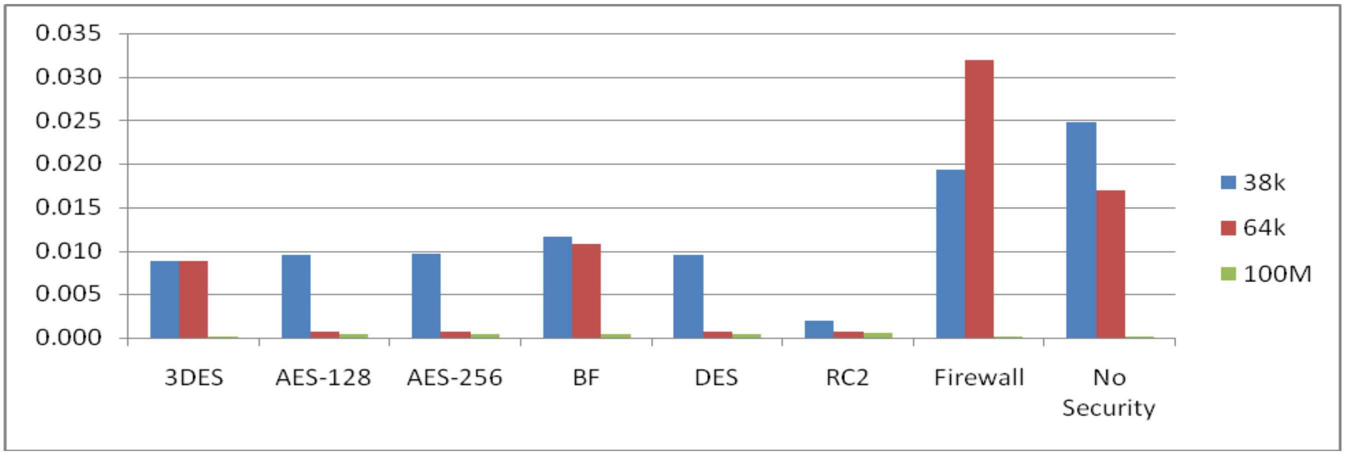

Figure 4: Degree of Jitter

In a LAN with high bandwidth (100Mbps), the degree of jitter is decreased to almost 0ms for 3DES, No Security and Firewall Only implementations.

4.3 Lost Packet

Figure 5 shows the degree of lost packets and bandwidth has a very important role in measurement of lost packet ratios.

As can be seen, implementing the BF and AES encryption algorithms in the 38kbps bandwidth WAN generate a great deal of lost packet ratio, which is more than 10%. However, implementing 3DES encryption algorithm decreased the number of lost packet. 3DES implementations only have 4% loss packets, lower than all other scenarios.

In 64kbps, 3DES encryption algorithm along with Firewall Only scenario has the highest loss packet ratio, which is around 4%. AES-128 and RC2 encryption algorithms only generate less than 1% lost packet which is negligible in VoIP communication..

In a LAN with 100Mbps, the increased bandwidth should have improved QoS. However, implementation of RC2 algorithm generates more lost packets in comparison with other scenarios in this bandwidth. The RC2 implementation generates more lost packets in a LAN than in 64kbps WAN and even more than implementing AES and BF encryption algorithm in 64kbps WAN.

5. 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.

The results indicate that bandwidth speed has a very important role in selecting an encryption algorithm. The figures in section 4 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 and different networks (LAN and WAN). 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).

The log files from the laboratory experiments demonstrate that the initial application of the AES encryption algorithm results in a high ratio of lost packets which reduces the quality of voice, but improves as the procedure continues. For example, implementing AES encryption algorithms in 38k bandwidth (WAN), which is an acceptable and minimum bandwidth for implementing encryption algorithms in this research, generates significant lost packets at the beginning of the connection. However, it should be mentioned that the encryption standard of the United States National Institute of Standards and Technology (NIST), and the United States government reportedly approves AES encryption algorithm for encrypting top-secret documents (NIST 2008). This algorithm affects the quality of voice more than the BF encryption algorithm. As a result, if a completely secure communication is desirable, the implementation of AES encryption algorithms is essential because the impact of AES on quality of voice is acceptable.

Findings from this research indicate that DES and 3DES should be rejected because DES encryption is not secure and 3DES only provides *Moderate Security* while being very slow in terms of

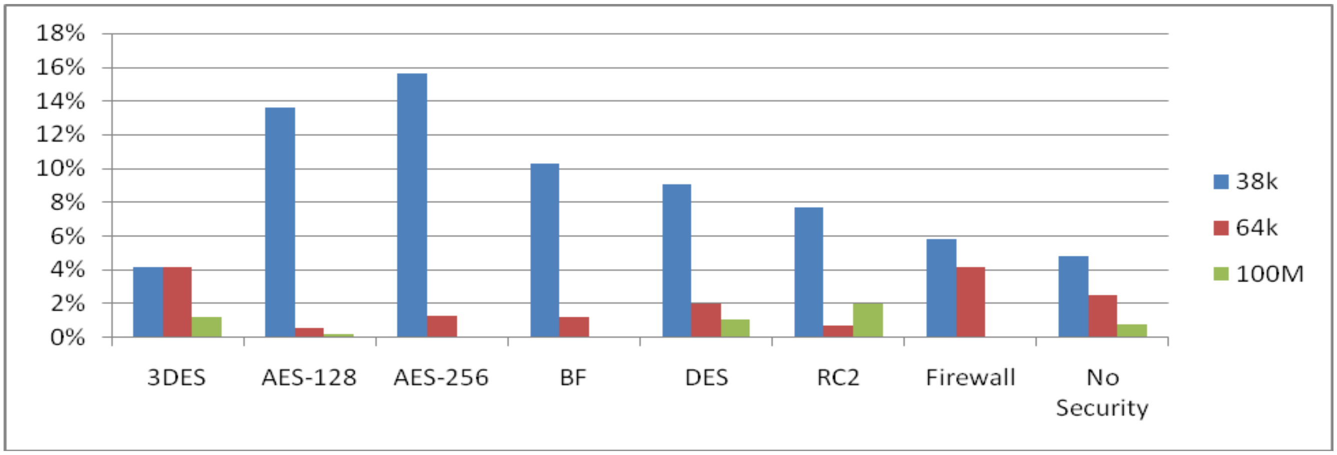

Figure 5: Lost Packet Ratio

speed of encrypting and decrypting. However, these two encryption algorithms have slightly less impact on voice quality than AES.

Table 2: The encryption algorithm assessments

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

Results in laboratory shows that by increasing bandwidth, a great deal of lost packet ratio is dramatically decreased and by removing encryption algorithms and the firewall the lost packet ratio is improved. According to the log files, there are a great numbers of Not Found packets at the beginning of connection, which implemented by AES encryption algorithms, whether 128 or 256 key lengths. It means, the reason that increases lost packet ratios in these two encryption algorithms, is the establishing connection at the beginning.

Encryption affects voice traffic in two ways. It increases packet size because of the headers added to the original IP packet for confidentiality and the new IP header added for the tunnel. The second is the time required to encrypt the payload and headers and construct the new header. There are undoubtedly many other factors that affect QoS and these have not been included in this research.

6. 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 increased bandwidth.

However experiments in the laboratory demonstrated that by implementing encryption algorithms the amount of jitter is decreased, but significantly raises 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. This will be presented in future work.

7. REFERENCES

[1] A. Klein, "Comparison of ciphers," in http://www.javamex.com/tutorials/cryptography/ciphers.shtml, [Accessed: 1 May 2009].

[2] Z. A. Barnes, "Is implementation of voice over internet protocol (voip) more economical for businesses with large call centers," Bowie State University 2005.

[3] E. T. Aire, B. T. Maharaj, and L. P. Linde, "Implementation considerations in a sip based secure voice over IP network," in *Proc of the 7th AFRICON Conference in Africa (AFRICON)*, Botswana, 2004, pp. 167-172.

[4] Cisco Systems, "Cisco IP communications solutions," in http://www.cisco.com/application/pdf/en/us/guest/netsol/ns165/c643/cdccont_090, [Accessed: 23 October 2008].

[5] A. Rouse, "Voice over IP revolutionizing the way businesses communicate," in *The Communicator*. vol. 1: NetLojix, Available at: http://www.netlojix.com/whitepapers/voip.pdf, 2004.

[6] A. Talevski, E. Chang, and T. Dillon, "Secure and mobile voip," in *Proc. of the International Conference on Convergence Information Technology*, Korea, 2007, pp. 2108-2113.

[7] P. Thermos and A. Takanen, *Securing voip networks: Threats, vulnerabilities, and countermeasures*. Boston, USA: Pearson Education, Inc., 2008.

[8] R. Weaver, "Vpn implementations," in *Guide to network defense and countermeasures*, 2nd ed USA: Thomson Course Technology, 2007, pp. 203-230.

[9] Y. Zheng, "The speed cipher," in http://labs.calyptix.com/files/speed-paper.pdf, [Accessed: 4 May 2009].

[10] Cisco Systems, "Understanding delay in packet voice networks," in Document Id: 5125, Available at: http://www.cisco.com/application/pdf/paws/5125/delay-details.pdf, [Accessed: 23 October 2008].

[11] N. Sulaiman, R. Carrasco, and G. Chester, "Impact of security on voice quality in 3g networks," in *Proc. of the 3rd IEEE Conference on Industrial Electronics and Applications (ICIEA)*, Singapore, 2008, pp. 1583-1587.

[12] A. P. Markopoulou, F. A. Tobagi, and M. J. Karam, "Assessing the quality of voice communications over internet backbones," *IEEE/ACM Transactions on Networking*, Vol. 11, No. 5, 2003, pp. 747-760.

[13] M. Minasi, "Locking up the ports: Windows firewall," in *Mastering windows server 2003, upgrade edition for sp1 and r2* Indianapolis, USA: Sybex, 2006.

[14] M. Manousos, S. Apostolacos, I. Grammatikakis, D. Mexis, D. Kagklis, and E. Sykas, "Voice quality monitoring and control for voip," *IEEE Internet Computing*, Vol. 9, No. 4, 2005, pp. 35- 42.

[15] S. Na and S. Yoo, "Allowable propagation delay for voip calls of acceptable quality," in *Proc. of the 1st International Workshop (AISA)*, Seoul, Korea, 2002, pp. 47-55.

[16] Ciso Systems, "Understanding codecs: Complexity, hardware support, mos, and negotiation," in http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a00800b6710.shtml, [Accessed: 4 May 2009].

[17] S. Tanenbaum, *Computer networks*, 4th ed. New Jersey, USA: Pearson Education, 2003.

[18] R. Barbieri, D. Bruschi, and E. Rosti, "Voice over ipsec: Analysis and solutions," in *Proc. of the 18th Annual Computer Security Applications Conference*, San Diego, USA, 2002, pp. 261- 270.

[19] P. Radmand and A. Talevski, "Impact of encryption on qos in voip," in *Proc of 2nd IEEE International Conference on Information Privacy, Security, Risk and Trust (PASSAT)*, USA, 2010, p. (accepted for publication).