Journal of Mobile Multimedia, Vol. 7, No.1 (2011) 113-128
© Rinton Press

# THE IMPACT OF SECURITY ON VOIP CALL QUALITY

PEDRAM RADMAND, JAIPAL SINGH, ALEX TALEVSKI

*Digital Ecosystems and Business Intelligence Institute,*

*Curtin University of Technology, Perth, Australia*
*pedram.randmand@postgrad.curtin.edu.au, {J.Singh, A.Talevski}@curtin.edu.au*

MARC DOMINGO-PRIETO, JOAN ARNEDO-MORENO

*Estudis d'Informàtica, Multimèdia i Telecomunicació, UOC, Barcelona, Spain*
*{mdomingopr, jarnedo}@uoc.edu*

Received March 4, 2011
Revised April 4, 2011

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) in the lab and in the real world. 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.

*Key words*: Voice over IP (VoIP), Quality of Service (QoS), data encryption

## 1 Introduction

The Internet has changed the way people communicate with each other. It pioneered text based communication from e-mails to instant messaging to the more recent use of social networking blog and sites. With the increase in network bandwidth capacity and better compression techniques, more and more consumers and businesses are using Voice over IP (VoIP) as a replacement for the traditional telephony systems.

VoIP started a means of making cheap/free voice calls from one computer to another over the Internet. VoIP technology improved to allow for calls from computers to existing telephony infrastructure. More recently, softphones or traditional handsets with a special adaptor allow for VoIP to be used to call anyone cheaply through the Internet. Even the upcoming 4G mobile standard will make use of VoIP for voice communication, thus replacing the existing circuit-switched networks currently being used for traditional telephony [3, 4].

The key reasons for this switch from traditional circuit-switching to VoIP over packet-switching networks are are low cost, blended voice and network services, and multimedia based communication on a single network [5].

The take up of VoIP by all parties, infrastructure providers, service providers and consumers, is due to its lower cost compared to traditional telephony. This lower cost goes beyond the monetary value of a consumer's phone bill and includes hardware costs, training costs, potential switch over costs and loss of business in transition [6]. VoIP can help in several ways to reduce the business costs through lower usage cost, lower costs of maintenance and support, and reduced network infrastructure [7]. 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 [5].

Current VoIP applications try to provide reasonable audio Quality of Service (QoS) that is lacking in practical security solutions. As more and more workplaces employ VoIP technologies, it provides an opportunity for hackers to access voice information during a VoIP call, because these are routed using insecure methods over the public internet [8].

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 is important as VoIP service providers need to select the best encryption algorithm to safeguard their customer's privacy while ensuring that the VoIP call quality is not unduly impacted by the high processing load of the encryption algorithm.

Therefore, this paper presents the results of laboratory and real-world tests to measure what affect does different encryption based security have on the VoIP call quality. 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 used in the laboratory and real-world implementation. Sections 4 and 5 present the analyses of data from laboratory and real-world experiments. Section 6 provides a discussion on findings followed by the conclusion.

## 2 VoIP Security and QoS Issues

Some typical attacks on VoIP system, the quality of service (QoS) requirements for VoIP and the impact of Security on QoS are outlined below.

### *2.1 VoIP Security Issues*

Organizations are concerned about implementing VoIP due to the lack of confidentiality in voice conversations. Traditional telephone networks are circuit-switched and relatively difficult to eavesdrop because an attacker needs physical access to the telephony network. The packet-switched nature of VoIP makes it more vulnerable to interception as the information travels on public network infrastructure. Similar techniques used to sniff data on a Local Area Network (LAN) or Wide Area

Network (WAN) can be used to intercept VoIP transmissions, allowing even an unsophisticated attacker to intercept and decode voice conversations [9].

VoIP systems are also vulnerable to malicious service interruptions caused by denial of service (DoS) attacks. An attacker can generate excessive traffic to 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 Eavesdropping, Man-in-The-Middle, Call Hijacking, Denial of Services and Phishing attacks. The security of VoIP will become more important as the number of users 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 used to protect the confidentiality of information transmitted between a sender and receiver over a public network. It establishes a security association through tunnelling and can be implemented 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). This tunnel provides end-to-end encryption where any nodes intercepting this communication on the public network will be unable to extract the encrypted message. This encryption is based on the exchange of a secret key pair which is used solely by the sender and receiver to encrypt and decrypt the communication [10].

Encryption is the process of rendering information unreadable by everyone except the recipient. An encryption algorithm will use an encryption key to convert plaintext into ciphertexts (encrypt) and vice versa (decrypt). There are two broad categories of encryption keys: asymmetric key, which uses different keys to encrypt and decrypt a message, and symmetric key, which used the same key to encrypt and decrypt communication packets.

Due to the added complexity of asymmetrical key encryption, this paper will only investigate symmetrical encryption algorithms for VoIP communication. The symmetrical encryption algorithms can be classified into stream ciphers and block ciphers. A stream cipher encrypts one plaintext bit at a time and it combines plaintext bits with a pseudorandom cipher bit stream. Block ciphers encrypt plaintext in a fixed encryption blocks. Stream ciphers have lower hardware complexity and execute faster than block ciphers. However, block ciphers provide stronger encryption compared with stream ciphers.

This paper will only look selected 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 and has less infrastructure overheads than asymmetrical algorithms. Speed is an important consideration for real-time VoIP communication, as it must balance speed with security requirements. A popular VoIP service provider, Skype employs AES-256 to provide end-to-end communication security to safeguard its user's conversations from being overhead by unauthorised parties [11].

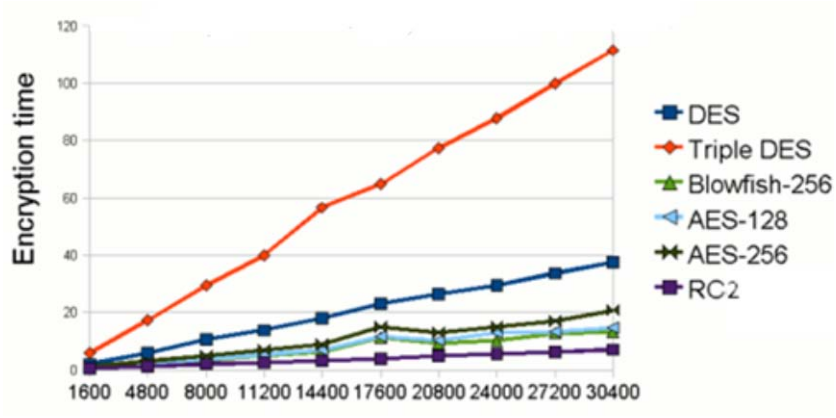

Figure 1: Cipher Encryption Speeds [1].

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 [12].

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.

Table 1: Key features of selected encryption algorithm [1].

| Algorithm | Key size (bit) | Speed | Key size affect speed | 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 | 112/168 | Very slow | No | Moderately secure |

### *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 [13]. 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) [6]:

- 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 travel from the speaking person to the listener at the other end [14]. The latency should be as low as possible as high latency will cause sound echoes which disrupts bi-directional conversations as the speakers will not be in sync with each other [15]. The ITU-T recommended that VoIP calls should have a maximum one-way latency of 150 ms.
- 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 [16]. In VoIP, loss packets will cause a call to break up, and too much of this will make the conversation incomprehendable. In VoIP, packet loss of 1 percent or more can cause calls to break up.
- Jitter is the variation of a periodic signal. In VoIP, jitter is the variation in time between packets arriving and can cause strange sound effects. Jitter is usually caused by network congestion or a change in transmission path [17]. No jitter occurs where a network has no variation in packet arrival times. Network providers accept jitter between 0.5-2 ms in a network. A jitter buffer is used to handle jitter but this will lead to higher end-to-end delay or latency.

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 [18].

(b) Codec is a signalling format for sending and receiving information when a call is made over the Internet [19]. 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 [20], commonly applied as LANs (Local Area Networks), WANs (Wide Area Networks) and MANs (Metropolitan Area Networks).

(d) Another aspect of QoS, which is optional, refers to security of the conversations and reliability. Security or privacy of phone calls becomes exceptionally important for law enforcement officials [21] and those involved in national security. It would be dangerous if police communication can be intercepted and decoded by unauthorised agents.

### 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 multiple strategies such as packet classification, priority queuing mechanisms, header compression, and congestion avoidance strategies. Unfortunately, some of these strategies cannot be used in combination with security protocols as they modify fields in the IP header which invalidates the integrity of security in VoIP. Therefore, when security protocols are implemented, the possible choices of QoS protocols are limited [22].

Previous works have only measured the impact of encryption algorithms on VoIP applications in three different bands in LANs and WANs [23, 24]. In this paper, the impact of encryption algorithm in terms of lost packet ratio, latency and jitter on LAN, WAN and real-world implementations with different bandwidths are examined. Based on the results, the best encryption algorithm that provides acceptable security along with acceptable quality of service will be nominated and discussed.

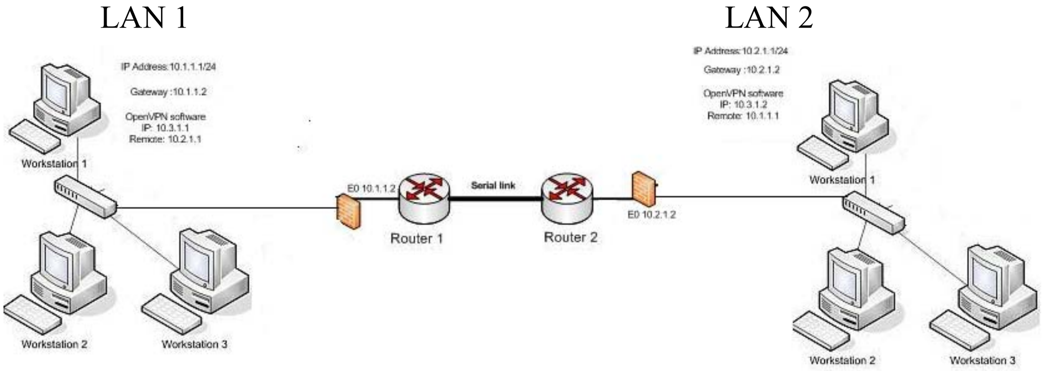

Figure 2: The WAN test network design

## 3. Research Approach

The paper applies an experimental research methodology to measure the impact of security of VoIP call quality. 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 provides an average latency of more than 150 ms, generates more than 1% lost packet ratios and 0.5 ms of jitter. "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*

The VoIP communication was conducted in a test network representing a LAN, a WAN and the Internet infrastructure. The LAN and WAN network was designed and implemented in a network laboratory. The LAN was represented by two computers connected via a cross cable while 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 laboratory based test network is as follows:

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

The real world VoIP implementation was conducted by establishing a VPN connection between two computers, one located in Perth, Australia and the other one in Barcelona, Spain. This experiment applied internet infrastructure to transmit VoIP voice data through a VPN tunnel. In the laboratory setting, the VPN was established in a peer-to-peer network while the real-world implementation established the VPN using a client-server approach. The experiments were conducted multiple times at different time of day and the results were averaged.

### *3.2 Capturing Voice Traffic*

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. The packet payload data and timestamp tags were used to calculate the three QoS factors – latency, jitter and loss packets. The payload data was used to find the lost packet ratio and timestamp was used for calculating latency and jitter.

VoIP communication was initiated between two computers on the test networks according to the scenarios below:

(a) No Security: Both sender and receiver were running Netmeeting, Wireshark packer sniffer and the Windows Firewall were disabled. No encryption algorithms were used for the VoIP calls. We used this setting as our benchmark.

(b) Firewall Only: Both sender and receiver were running Netmeeting, Wireshark packet sniffer and the Windows Firewall were enabled. No encryption algorithms were used for the VoIP call.

(c) With Windows Firewall and VoIP encryption: Both sender and receiver were running Netmeeting, Wireshark packet sniffer, with Windows Firewall enabled and OpenVPN with different encryption algorithms for encrypting/decrypting VoIP calls between both parties.

The measurement of the dependent variables - latency, jitter and lost packet - in the test networks were used to assess the impact of encryption security on QoS under different network situations and bandwidths using the above three scenarios.

## 4. Results of VoIP Security on QoS in LAN & WAN Environments

Five different encryption algorithms - DES, Triple DES (3DES), AES-128/256, Blowfish (BF), and RC2 - were implemented on two different network topologies providing three different bandwidth speeds – 38 kbps, 64kbps and 100 Mbps - in the laboratory to measure the degree of latency, jitter and lost packet ratio by different encryption algorithms.

### *4.1 Latency*

Figure 3 shows the degree of latency for three different bandwidth settings. As can be seen in the figure, the degree of latency is improved by increasing the network bandwidth.

As the diagram shows, implementing the BF and AES encryption algorithms in the 38kbps bandwidth generate higher latency, about 40 ms, compared with other encryption algorithms. Implementation of simple security such as firewall only is shown to have latency similar to DES, 3DES and RC2.

The diagram also indicates that in 64kbps networks, the degree of latency would not be influenced by implementing the encryption schemas. This figure reveals that implementing a 3DES encryption algorithm is the worst performing encryption schema in terms of latency compared while AES encryption has the least degree of latency.

We find that in a LAN setting, where the bandwidth is very high (100Mbps), the VoIP packet latency is similar for implementation with an encryption schema or without any security.

Overall, the degree of latency is not influenced by implementing encryption algorithms and firewall security when the bandwidth is at 64kbps or higher (100Mbps). We also found that even at low bandwidths, 38kbps, the latency is below the maximum threshold of 150 ms for VoIP traffic.

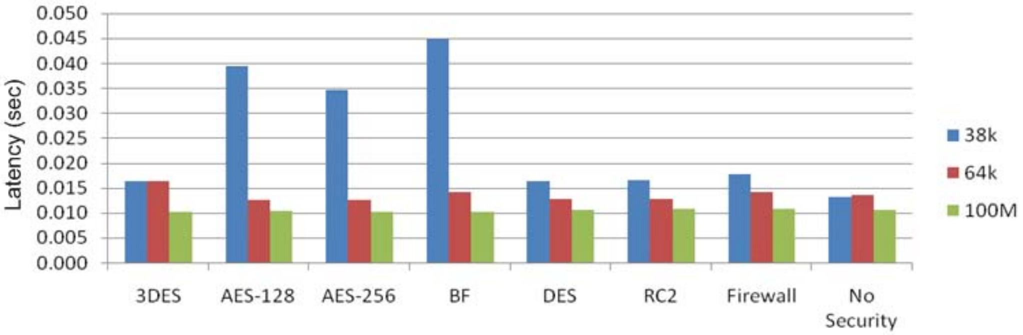

Figure 3: VoIP Latency in LAN & WAN

### 4.2. Jitter

Figure 4 shows the degree of jitter ratios. It reveals that the degree of jitter is reduced by increasing network bandwidth except in Firewall Only security implementation. However, in a LAN (100Mbps), the amount of jitter is dropped to almost 0 ms when 3DES, no security or firewall only security is implemented.

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 for low to moderate bandwidth scenarios.

In a WAN, the degree of jitter is reduced drastically for DES, AES and RC2 encryption algorithms when the bandwidth is increased to 64kbps, whereas the jitter is high for VoIP communication without any security and Windows Firewall only security. In a firewall only scenario, the degree of jitter increases to 32 ms when the WAN bandwidth increases, which is the greatest degree of jitter among all scenarios. This is most probably caused by higher variation in packet arrival time due to the firewall. The firewall does not drastically vary the VoIP packet arrival time when used in conjunction with an encryption schema.

Our experiments show that using a security scheme generally has a lower degree of jitter compared with not using security or using simple security such as firewall only. This shows that better call quality in terms of reduced jitter is provided when encryption security is used for VoIP communication.

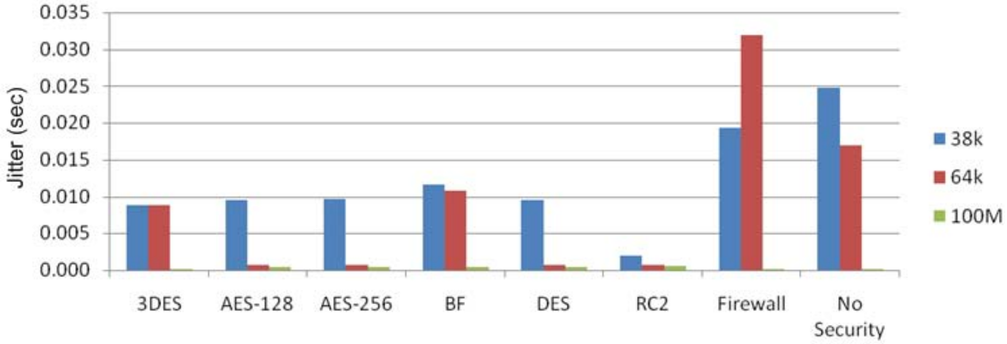

Figure 4: VoIP Jitter in LAN & WAN

### 4.3. Lost Packet

Figure 5 shows that bandwidth has a very important role in the 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. Unfortunately, no network scenario meets the VoIP loss packet requirement of less than 1% in the low bandwidth scenario.

In a moderate bandwidth network of 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 meets the VoIP communication requirements. This provides better performance compared with VoIP implementation without any security.

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.

We find that the AES security schema meets the VoIP loss packet requirements of less than 1% in moderate to high bandwidth networks.

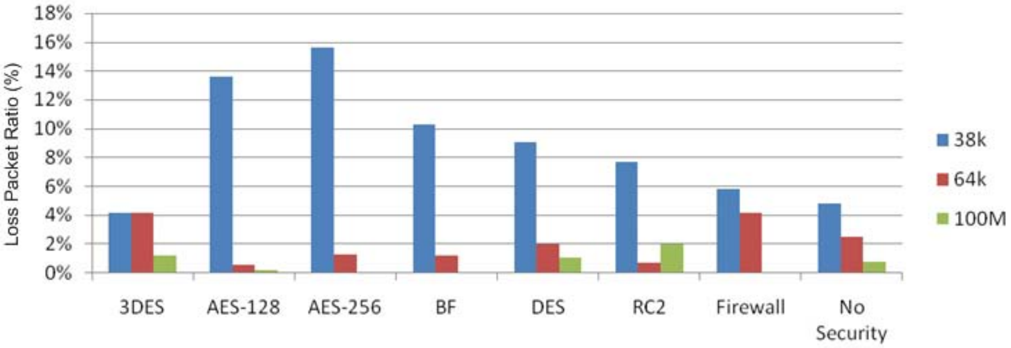

Figure 5: Loss Packet Ratio for VoIP in LAN & WAN

## 5. Results of Security on QoS in Internet Voice Communication

The same five encryption algorithms were implemented to measure the call quality of VoIP running on a commercial ADSL2+ connection from Perth, Australia to Barcelona, Spain. This experiment was conducted at different times of day and the results were averaged to measure the degree of latency, jitter and lost packet ratio by different encryption algorithms in an environment similar to most home networks. We found a huge difference in latency, jitter and loss packets in the real world compared with the laboratory setting. Even with such a high reduction in quantitative performance, there was no noticeable impact in voice quality between sender and receiver. This will be explain in detail in section 6.

### *5.1 Latency*

Figure 6 shows the degree of latency for VoIP traffic between Australia and Spain. As it can be seen, all different encryption, minimum security and no security scenarios have almost the same degree of latency. Due to the great distance between the two computers, the degree of latency is significantly higher compared to the experiments conducted in the laboratory. The real-world experiments show that the latency exceeds the maximum threshold by 6 times. This is the same even if no security scheme is used in VoIP traffic. As the results are similar, the authors cannot recommend the best or worst security schema for reducing latency in VoIP traffic.

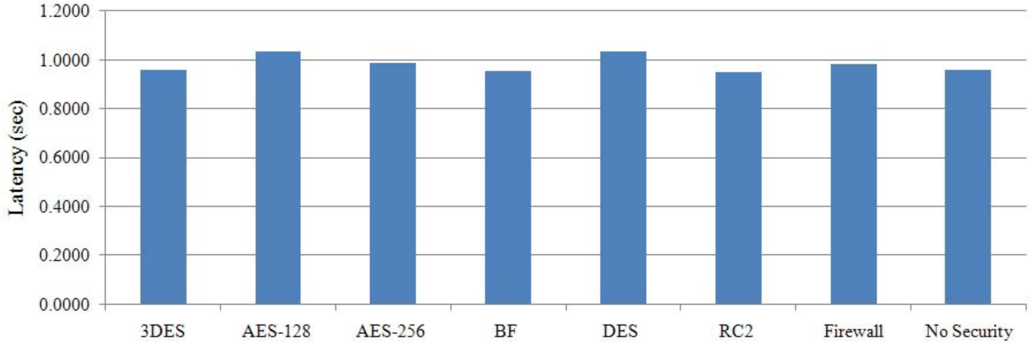

Figure 6: Degree of Latency for VoIP in Internet

### *5.2 Jitter*

Figure 7 shows the degree of jitter ratios for VoIP traffic over the Internet between Spain and Australia. Similar to the laboratory experiments, we find that VoIP with no security or minimal security has higher jitter compared with VoIP using most security schemas. Like the latency results, the jitter measured in 150 times the maximum threshold recommended by the ITU-T. It should be mentioned that implementing any one of the encryption schemas will not affectedly change the degree of jitter as the difference between the best encryption algorithm (BF) and worst algorithm (AES-128) is only less than 1 ms. This high jitter is due to the network architecture between Australia and Spain. However, as the results show, some encryption algorithms actually reduces jitter in VoIP traffic compared to no security implementations. Therefore, security should be implemented for VoIP communication to reduce jitter.

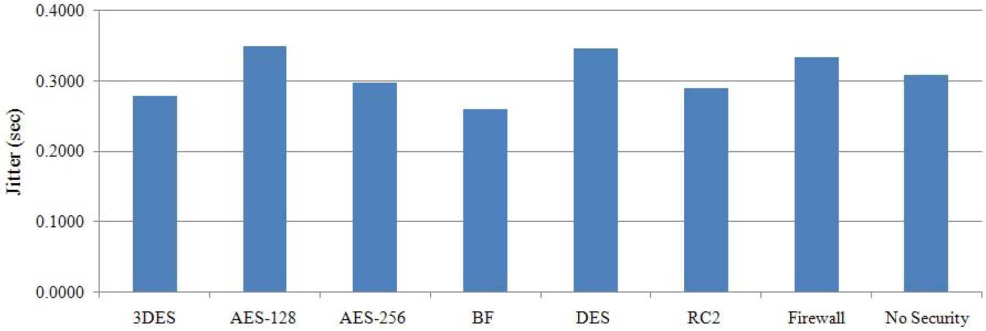

Figure 7: Degree of Jitter for VoIP in Internet

### *5.3 Lost Packet*

Figure 8 shows the lost packets ratio for VoIP traffic between Spain and Australia using the Internet. We found that the packet loss ratio for VoIP without any security is around 1.6%, similar to using the DES encryption algorithm. VoIP using 3DES encryption generates a great deal of lost packets, more than 3.5%. This result is worse than the laboratory experiments and exceeds the recommended loss packet ratio for VoIP, namely 1 percent packet loss. The average packet loss was between 1.6% to 3.5%. Even though the packet loss was higher than the recommended packet loss for VoIP, we rarely noticed call degradation. Based on these results, the DES encryption algorithm comes closest to meeting the packet loss requirement threshold for VoIP. However, this encryption algorithm is not as secure, has higher latency and higher jitter compared with other encryption algorithms that were examined in this research.

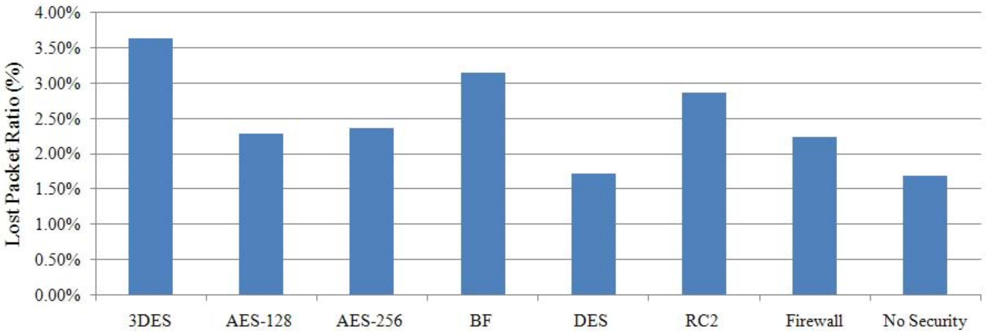

Figure 8: Lost Packet Ratio for VoIP in Internet

## 6. Impact of Security on VoIP Call Quality

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.

Our experimental results indicate that bandwidth speed plays an important role in VoIP quality of service (QoS), in some cases more so than the encryption algorithm speed. We found that in some cases, an encryption algorithm that takes a longer time to encrypt/decrypt messages might have lower latency compared with algorithms that perform an encrypt/decrypt quickly. For example, 3DES takes the longest to encrypt/decrypt but performs moderately better in terms of latency and jitter compared with faster algorithms like AES.

We found that some encryption algorithms work as well as or better compared with unsecured VoIP implementations. In terms of latency, VoIP systems running DES or RC2 encryption perform similarly with an unsecured VoIP implementation. The important finding is when measuring jitter, VoIP implementations using some forms of encryption generally outperforms an unsecured VoIP implementation or that using simple firewall protection. This is because the encryption/decryption process ids in normalising the packet arrival time at the receiver, thus making the VoIP packets arrive in a more uniform manner compared with regular network traffic (no security). We also found that bandwidth directly influenced packet loss. The lower the bandwidth, the higher the packet loss when encryption was used. However, when the network bandwidth increases, the packet loss when using encryption dropped sharply, in some cases less packets failed to arrive when using encryption compared with implementations without encryption.

An interesting observation of call quality on the Internet is relevant to the QoS thresholds provided by ITU-T. We found that an ADSL2+ connection between Perth, Australia and Barcelona, Spain failed to meet the QoS thresholds for acceptable call quality in VoIP traffic (with security and without security implementations). However, the call was clear and easily understood by both parties. The only audio disruptions occurred when both sides tried to speak at the same time. Other than that, there were no issues in terms of call quality. This experiments shows that exceeding the QoS thresholds, even by up to 6 times for latency and 150 times for jitter did not affect the call quality at all.

The experiments conducted in this research clearly shows that security implementations for VoIP do not adversely affect the call quality, and in some cases even improve it. This research, while not exhaustive, provides an understanding of which encryption algorithm should be used in different network conditions, i.e. using 3DES for lower bandwidth networks while AES for medium to high bandwidth networks. We also found that stream cipher do no better than block cipher in terms of QoS in VoIP traffic, particularly when the network has medium to high bandwidth.

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 descending order (1=high and 6=low). This table gives higher weightage to results from the Internet compared with LAN/WAN results. This is because the Internet would be a better guide to actual network conditions for VoIP communication. This table can be used to select an encryption algorithm based on the perform that is important for call quality, namely latency, jitter or packet loss. Lower latency will reduce echoes in VoIP conversation while lower jitter will eliminate audio artefacts and less packet loss will make the audio quality smoother. Knowing this, the user can select the best encryption algorithm to achieve the best call quality.

Table 2: The encryption algorithm assessments

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

*Performs better in LAN/WAN Environments

Encryption algorithms affect 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.

Findings from this research indicate that DES performs better in LAN/WAN environments and poorly over the Internet although it achieved the lowest packet loss. 3DES performs inversely to DES on the Internet, with better latency and jitter but worse packet loss rations. However, as DES and 3DES algorithms provide the least security, we recommend that they should not be used at all for VoIP communication.

The AES encryption algorithm provides the strongest encryption compared with the other algorithms tested in this paper. It is widely adopted for encrypting top-secret documents by the United States government and is adopted by Skype for VoIP communication. AES provides middle-range performance in terms of latency and jitter but has very strong security and very little packet loss. Therefore, AES-256 should be adopted for highly confidential/secured voice communication. The second choice would be RC2 encryption as it provides moderate security but least amount of latency and moderate jitter and packet loss.

Our results indicate that distance plays a very important role in QoS for VoIP. The results demonstrated that by implementing security schemas through VPN along with firewall, the degree of latency and jitter are not changed and only the last packet ratios are a bit affected. In fact, the results demonstrate that initial application of the 3DES encryption algorithm result in a high ratio of lost packet, where the bandwidth is constant, is around 3.5%. However, the lost packet ratios were lower when implementing DES encryption algorithm. However, the authors do not recommend DES and 3DES as they are not very secure encryption algorithms.

## 7. Conclusion

This research examined the impact 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 in a laboratory and real world (Internet) environment. Based on our experiments, we found that network bandwidth plays an important role in ensuring call quality in VoIP communication. Our results show that the three factors of QoS - latency, jitter and lost packets - are all improved, when the bandwidth is higher.

However, due to the great distance between Perth, Australia and Barcelona, Spain, the network was unable to meet the recommended QoS thresholds for VoIP. Even so, we found no degradation in call quality and the security schemas did not adversely affected the network QoS.

We found that the ratio of lost packet in the real world is far less than lost packet ratios in the laboratory settings, particularly when the network bandwidth is 38k. The network QoS improves as the bandwidth increases. The results demonstrate that adequate bandwidth is a more important factor than distance, which is very effective in generating latency and jitter, and in situations where the amount of bandwidth is high, the lost packet ratios are dramatically dropped. For example, the ratio of lost packet, where the bandwidth in the lab is 38k, is between 4% to 16%, while the ratio of lost packets on the

Internet is between 1.7% to 3.5%. This demonstrates that adequate bandwidth is the most important factor in QoS for VoIP in terms of lost packet ratios.

Our experiments demonstrated that some encryption algorithms actual decrease the amount of jitter compared with an unsecured VoIP implementation. Most encryption algorithms would increase call latency in low bandwidth environments but perform as well as unsecured networks in medium to high network bandwidths. 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.

The experiments revealed that the RC2 algorithm is very fast and provides the least latency and an acceptable level of lost packets and jitter. 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 from the results that DES is the most inefficient encryption algorithm in terms of security and speed among those encryption algorithms which were examined in this paper.

This paper indicated that the AES encryption algorithms provides the best security without impacting overall QoS too much of all the tested algorithms. Therefore, in situations where security is the most important objective, then AES-256 is the most effective. Where latency or jitter is the most important, then RC2 or BF is superior.

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.

It is recommended to implement security schemas, where two computers have a great distance to each other because the impact on QoS by implementing security schemas and encryption algorithms are negligible. As there is no one encryption algorithm that meets all requirements, the type of security schema to be implemented will greatly depends on the requirements of the user. This paper provides recommendations on which security algorithm should be applied for different user requirements when using VoIP for voice communication.

Further research is needed to identify additional factors that may affect voice quality, such as network 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.

## References

1. Klein, A., Comparison of ciphers. http://www.javamex.com/tutorials/cryptography/ciphers.shtml, Vol. 2009, (2008).
2. Barnes, Z.A., Is implementation of voice over internet protocol (VoIP) more economical for businesses with large call centers. Bowie State University, (2005).
3. Santhi, K.R., Kumaran, G.S., Migration to 4G: Mobile IP based solutions. in Advanced International Conference on Telecommunications and International Conference on Internet and Web Applications and Services (AICT/ICIW). IEEE Computer Society, Guadeloupe, French Caribbean, (2006).
4. Badard, B., Diascorn, V., Boulmier, G., Vicard, A.D., Renard, V., Dimassi, A.H., Migration to VoIP over mobile networks: Technical challenges and economic opportunity analysis. in 14th

International Telecommunications Network Strategy and Planning Symposium (NETWORKS), Warsaw, Poland, (2010), 1-7.

5. Aire, E.T., Maharaj, B.T., Linde, L.P., Implementation considerations in a SIP based secure voice over IP network. in 7th AFRICON Conference in Africa, Vol. 1, Botswana, (2004), 167-172.
6. Cisco Systems, Cisco IP communications solutions. http://www.cisco.com/application/pdf/en/us/guest/netsol/ns165/c643/cdccont_090, Vol. 2008, (2005).
7. Rouse, A., Voice over IP revolutionizing the way businesses communicate. The Communicator, Vol. 1. NetLojix, Available at: http://www.netlojix.com/whitepapers/voip.pdf, (2004).
8. Talevski, A., Chang, E., Dillon, T., Secure and mobile VoIP. in International Conference on Convergence Information Technology, Korea, (2007), 2108-2113.
9. Thermos, P., Takanen, A., Securing VoIP networks: Threats, vulnerabilities, and countermeasures. Pearson Education, Inc., Boston, USA, (2008).
10. Weaver, R., VPN implementations. in Guide to Network Defense and Countermeasures. Thomson Course Technology, USA, (2007), 203-230.
11. Berson, T., Skype Security Evaluation. http://www.anagram.com/berson/skyeval.pdf. Anagram Laboratories, Palo Alto, USA, (2005).
12. Zheng, Y., The speed cipher. http://labs.calyptix.com/files/speed-paper.pdf, Vol. 2009, (2009).
13. Cisco Systems, Understanding delay in packet voice networks. Document Id: 5125, Available at: http://www.cisco.com/application/pdf/paws/5125/delay-details.pdf, Vol. 2008, (2006).
14. Sulaiman, N., Carrasco, R., Chester, G., Impact of security on voice quality in 3G networks. in 3rd IEEE Conference on Industrial Electronics and Applications (ICIEA), Singapore, (2008), 1583-1587.
15. Markopoulou, A.P., Tobagi, F.A., Karam, M.J., Assessing the quality of voice communications over internet backbones. IEEE/ACM Transactions on Networking, Vol. 11**,** (2003), 747-760.
16. Minasi, M., Locking up the ports: Windows firewall. Mastering Windows Server 2003, Upgrade Edition for SP1 and R2. Sybex, Indianapolis, USA, (2006).
17. Manousos, M., Apostolacos, S., Grammatikakis, I., Mexis, D., Kagklis, D., Sykas, E., Voice quality monitoring and control for VoIP. IEEE Internet Computing, Vol. 9, (2005), 35- 42.
18. Nisar, K., Hasbullah, H., Said, A.M., Internet call delay on peer to peer and phone to phone VoIP network. in International Conference on Computer Engineering and Technology (ICCET), Vol. 2, Singapore, (2009), 517-520.
19. Goode, B., Voice over internet protocol (VoIP). in Proceedings of the IEEE, Vol. 90**,** (2002), 1495-1517.
20. Tanenbaum, S., Area network. Computer Networks, Fourth Edition. Prentice Hall, Perth, (2003).
21. Thanthry, N., Pendse, R., Namuduri, K., Voice over IP security and law enforcement. in 39th Annual International Carnahan Conference on Security Technology (CCST), (2005), 246-250.
22. Barbieri, R., Bruschi, D., Rosti, E., Voice over IPSec: Analysis and solutions. in 18th Annual Computer Security Applications Conference, San Diego, USA, (2002), 261- 270.
23. Radmand, P., Singh, J., Domingo, M., Arnedo, J., Talevski, A., VoIP: Making secure calls and maintaining high call quality. in 8th International Conference on Advances in Mobile Computing & Multimedia (MoMM). ACM Press, Paris, France, (2010).
24. Radmand, P., Talevski, A., Impact of encryption on QoS in VoIP. in 2nd IEEE International Conference on Information Privacy, Security, Risk and Trust (PASSAT). IEEE, Minneapolis, USA, (2010), 721-726.