Impact of Security on Voice Quality in 3G networks

Norrozila Sulaiman, Rolando Carrasco and Graeme Chester
School of Electrical, Electronic and Computer Engineering,
Newcastle University,
Newcastle Upon Tyne, UK
Norrozila.sulaiman@ncl.ac.uk

Abstract—The aim of this paper is to study the impact of security protocols on the quality of Voice over Internet Protocol (VoIP) in a third generation (3G) network. Long distance calls are expensive and the potential of cost saving is the most attractive feature in VoIP. In VoIP, voice traffic travels using the Internet protocol instead of using a conventional line. Assuring quality of service (QoS) is one of primary issues in an IP based application. Hence, it is essential to evaluate the performance to ensure that the quality is acceptable to the users. This paper discusses the security protocol at the IP layer. It also presents the results of system simulations which provide some insights into the conditions and parameters involved. The results indicate that a security algorithm has a great impact on the overall performance of a voice service which may degrade the voice quality to an unacceptable level.

I. INTRODUCTION

The third generation (3G) network, such as Universal mobile telecommunications system (UMTS), provides high speed data and multiple data rate services. It offers a higher user bit rate and as it can support a variety of services on a single infrastructure, traffic management is crucial [1]. The traffic can be classified into real-time and non-real-time groups. Real-time traffic is time-sensitive which involves information that requires immediate delivery such as video and voice. On the other hand, non-real-time traffic is time-insensitive. Information such as images and data can be stored for later consumption. For the real time services like voice, the end to end delay has to be very low.

Voice over Internet Protocol (VoIP) is a technology that allows voice conversations to be transmitted over a network using Internet technology. To be able to transmit a speech signal on the Internet, it must be digitised. The technology converts the voice into digital unit and sends the packets over the network as shown in Fig 1.

At the receiving end, the packets will be reconstructed into the speech signal. The use of VoIP as a telephony alternative is getting more popular because it can lower the total communication costs especially for a long distance call. However, there are several issues related to VoIP like technology management and security challenges.

Bandwidth limitation is one of the major issues concerning the VoIP network. As the available bandwidth is very limited, the digitised speech is required to be compressed in order to reduce the amount of required bandwidth to transmit the signal. The bandwidth usage depends on the codec type and voice samples per packet. Theoretically, compression techniques can reduce the bandwidth and can maximize the number of users on the system. There are a number of voice coding standards which have different rates, quality and complexity. The speech quality varies with the bit rate of the codes.

According to [2], the performance of the speech coder determines the quality of the speech and the capacity of the system. Low bit-rate coding will enable more users to be accommodated with a limited allocated bandwidth. Implementation of speech coding must consume little power and provide tolerable speech quality. Speech coding aims to transmit the highest quality of speech with the use of the least possible channel capacity while maintaining a certain level of communication delay. In general, the type of codec, voice packet size and delay are some of parameters that have an impact on the VoIP call. These parameters affect the voice packet flow between the nodes in the call.
One of the main problems of IP based applications is the lack of QoS guarantee. Although voice packets can be delivered across a network using the IP, assuring the QoS is one of the issues in the implementation. Packet loss and delays are the undesirable features of voice communication. As VoIP is becoming popular, the concern for security increases too. The quality of voice is affected by the packet size and service capacity as analysed in [3]. Moreover, the network traffic and interference could cause delay and jitter.

In VoIP, packets must arrive quickly and at the same the packets must be secure. The data packets in VoIP may become unusable unless they reach their destination in a restricted time frame. Users would expect the level of QoS to be approximately the same as the traditional telephone lines. It was suggested that the end-to-end delay should be no more than 150 milliseconds (ms) in order to maintain the voice quality [4]. There are several issues that correspond to VoIP such as latency, jitter and packet loss. By introducing security to VoIP, the QoS will drop.

The QoS for each IP application is different and it can be grouped into several categories as shown in TABLE 1. In order to satisfy the end to end service, a user is provided with certain data packet traffic [5].

The end-to-end delay is the time taken for data to get from the speaking person to the listener at the other end. The end-to-end delay for a packet is measured based on the time difference between the created and received time. Jitter occurs when packets have different delays. Let d be the delay, then the variation (V) from source(a) to destination(b) is given by:

\[ \Delta V_{ab} = \sqrt{\Delta d_a^2 + \Delta d_b^2} \] (1)

Some packet arrivals are delayed and must be discarded. Packet loss occurs when packets do not arrive or arrive too late to be processed. It is seen as gaps in the communication. Packet loss is intolerant in VoIP as it may degrade the quality of service in VoIP. A packet loss of 2% is normally acceptable. However, if the losses are more than that, users’ satisfaction will not be achieved. According to [6], the voice quality is intolerable if packet loss is more than 3%.

II. BACKGROUND

There has been some research carried out on VoIP [7-13]. Research on delay performance of VoIP in 3G systems was conducted in [7]. In this study, the network capacity was evaluated under different packet delay budgets associated with radio access channels.

In [8], a new QoS control scheme that uses a simple protocol to detect the end-point CPU capabilities was proposed. A study which aimed to outline the potential security issues faced in transforming the traditional phone systems into VoIP systems was presented in [9].

A similar project has been carried out in [10] where the authors explained the challenges of VoIP security and steps for securing an organization’s VoIP network. A model for carrying out simulations of the performance of secure session initiation protocol was described in [11] and the results of the performance analysis were presented.

A quantitative analysis of the Quality of Service (QoS) based on IPsec was evaluated in [12]. The aim was to analyze whether IPsec is good enough to transmit real time multimedia traffic.

In [13], a study on the integration of standard security schemes with standard VoIP protocols was presented. The effects of firewall and virtual private network (VPN) techniques on the quality of a single Session Initiation Protocol (SIP)-based voice call were carried out. Issues related to implementing a secure and high quality VoIP networks were also discussed in [13].

III. SIMULATION MODEL

The packet arrival rate depends on the link rate mean number of packets in a “talkspurt”. The voice packets contain a payload of 32 bytes/packet and its frame size is approximately 20 ms. The parameters in the simulation are the coding rate, packet length, service rate and frame size. The packet size and the effective bit rate are computed.

Let \( \lambda \), represent arrival rate in the queue with inter-arrival time \( \tau \). The packet arrival rate depends on the link rate and the number of active sessions. In the calculation, the probability of active state \( P(\alpha) \) was used to consider the traffic behaviour which represents the actual arrival rate. The probability of the arrival rate of \( n \) packets can be represented by [3]:

\[ P(n) = \frac{\lambda^n \tau^n (\lambda \tau)^n}{n!} \] (2)

Let \( t \) be the duration of call in seconds and \( h \) be the holding time in seconds. Therefore, the probability of a call arrival in \( t \) seconds is given by:

\[ P(t) = e^{(t/h)} \] (3)

| TABLE I |
|-----------------|-----------------|-----------------|
| QoS Classes | Type of Quality of Service | Example of Applications |
| a) conversational class | real-time connection, nearly symmetric | voice |
| b) streaming class | real-time connection, asymmetric | streaming video |
| c) interactive class | non-real-time packet data, no immediate action expected | web browsing |
| d) background class | non-real-time packet data, no immediate action expected | emails |

Authorized licensed use limited to: Newcastle University. Downloaded on March 17,2010 at 12:29:25 EDT from IEEE Xplore. Restrictions apply.
Handover could occur because of the signal strength falls below certain parameters specified in handover criteria. It could also occur when the traffic capacity of a certain cell has reached its maximum. Thus, the mobile users have to be handed over to neighbouring cells with less traffic load. The simulation was run to analyse the impact of IPSec protocol on a VoIP application and non-IPSec was used as a baseline. The performance was evaluated for a different packet arrival rate over a range of system parameters.

Security is another important issue that needs to be addressed and in some cases voice security could be more important compared to data networks. As protecting sensitive and financial data are crucial, ensuring the security of a conversation is desired. Securing the voice communication includes protecting the voice data as well as the identities of both parties. IP Security (IPSec) is a standard framework for securing IP communication. It is used for encrypting and the authentication of IP packets. IPSec may be used to provide authentication, integrity and confidentiality for the transmitted data. It is necessary to protect the data and it can be achieved by encrypting the packets at the IP level using IPSec.

The basic protocols used are Encapsulating Security Payload (ESP) and Authentication Header (AH). AH is intended to guarantee connectionless integrity and data origin authentication, whereas ESP provides origin authenticity, integrity, and confidentiality of a packet. ESP can be used in tunnel or transport mode. Transport mode encrypts the payload and upper layer headers in the IP packet. In contrast, tunnel mode encrypts the entire IP datagram and places it in a new IP Packet. The different between tunnel and transport modes is as shown in Fig. 2.

As IPSec expands the packet size, encoding and decoding encryption can have a significant impact on delay. Thus, there must be a balance between the desired security and the desired recognised quality. A security solution should be implemented with a minimum delay to ensure the QoS conforms to the standard. IPSec algorithm was deployed at every mobile device for end to end data transfer. IPSec provides the shared key that is required to perform authentication and confidentiality. The 3DES encryption algorithm is widely supported and some implementations can make use of the AES encryption algorithm.

The Advanced Encryption Standard (AES) based on the Rijndael encryption algorithm is used for the encryption scheme. The users will configure a private key. It is assumed that the users of the system know a shared secret key. The base station will send an Authentication Response with a text. The user will answer with the text encrypted with the security key. If the base station can decrypt the message and validates that the text is the same, it will grants access to the user.

IV. RESULT ANALYSIS

IPSec is one way of securing the data however it introduces an additional overhead to the packet size. The impact of implementing a security algorithm and protocols on the performance of VoIP networks is analysed. The simulation was run to analyse the impact of IPSec protocol on a VoIP application and non-IPSec was used as a baseline.

A. End-to-End Delay

Delay in voice communication can be caused by the codec and encryption. Different types of codec have different amounts of delay added to the compressed speech data. Encryption will result in a larger header to payload ratio for each packet which reduces the effective bandwidth. As Fig. 3 shows, the impact of security on end-to-end delay is unacceptable to the user when the interface rate is 32Kbps.

As Fig. 3 shows, the impact of security on end-to-end delay is unacceptable to the user when the interface rate is 32Kbps.
Similarly, Fig. 4 illustrates that the end-to-end delay is slightly noticeable when the interface rate is 64Kbps and it still falls within the recommendation. However, as the traffic increase, the delay increases drastically.

Fig. 4. End-to-end Delay against Arrival Rate

Fig. 5 shows the end-to-end delay of the simulation model with the theoretical model as in [3]. As the traffic increase, the delay maintains at a certain level and at a certain point it increases drastically. The simulation result matches closely to the theoretical result.

Fig. 5. End-to-end Delay against Arrival Rate

C. Packet Loss

Fig. 7 shows the impact of security on percentage of packet loss when the rate is 32Kbps. The average percentage of acceptable packet loss is about 2%. The graph shows that the packet loss is very noticeable and it does not conform to the recommended standard.

Likewise, Fig. 8 shows the impact of security on percentage of packet loss when the rate is 64Kbps. The percentage of packet loss fluctuates as the traffic increase. However, the difference is very small and is almost negligible. The average percentage of packet loss is maintained at a value of about 2%.

Fig. 7. Packet Loss against Arrival Rate

B. Throughput

Fig. 6 illustrates the impact of security on throughput. As the traffic increases, the throughput increases too. However, the graph shows that security does not really affect the throughput for both data rate. This is because although the packet size increased, it does not increase the payload capacity. The increase in packet size is due to the encryption and encapsulation header.
V.  C O NCLUSION

With the convergence of technologies, privacy and security have become more important. VoIP is being approved as a replacement for the traditional circuit switched infrastructure. Nevertheless, voice communication and its security are a relevant concern for the most critical infrastructure. Security aspects of VoIP have emerged as important as QoS. The purpose of this study is to analyse the impact of a security algorithm in the network.

There are a few factors that affect voice traffic over secure IP network such as encrypt payload and increased packet size. The basic QoS such as delay, jitter and packet loss were used in evaluating the impact of the IPSec. These issues arise in VoIP environment because the packet must arrive at the destination fast. If a packet is lost, there is no time to resent the packet. Delay in voice communication can be caused by the codec and encryption. In addition, encryption will result in a larger header to payload ratio for each packet which reduces the effective bandwidth. Due to the nature of VoIP which is time-sensitive, most of the security measures in data networks could not be used in VoIP networks.

The result has indicated that the integration of a security algorithm with VoIP has a great impact on the performance of VoIP in a 3G network. It increases latency and contributes jitter which may degrade the voice quality to an unacceptable level. This is due to a significant increase in packet size cause by the additional header for security. As VoIP uses small packets in a high volume, this may accumulate the total packet size.

From the results, it can be concluded that the overall quality is reduced when security protocol was implemented. Although security results in a degradation of speech quality, there must be a compromise for securing the data. Lastly, VoIP is a technology that would have wide scale implementation in the future and secured communication in IP based networks is a key success for the VoIP evolution.