IJCSBI.ORG

VoIP Security: Improving Quality of Service through the Analysis of Secured Transmission

Uchenna P. Daniel Ani
Federal University Lokoja, Nigeria.

Mohammed Mustapha
INEC, Abuja-Nigeria

ABSTRACT
VoIP as a packet switched system is clearly one of the most important evolving trends in computing and telecommunications. However, just like many other new Information technology trends, VoIP introduces both security risks and opportunities for the IT world, viable solutions of which are required. The use of publically verified cryptographic algorithms to ensure confidentiality of VoIP traffic transmitted over insecure public networks as the Internet cannot be overemphasized. Nonetheless, the uses of cryptographic algorithms yet imposes a delay overhead and packet size overhead on VoIP, which is unconnected to the processing time required to encrypt/decrypt bits or blocks of data and the increase in packet size due the block size of the encryption algorithm. This delay levied is dependent on the mode of operation of the cryptographic algorithms. Mindful of the fact that other components like voice codecs and network bandwidth also contributed delay capabilities on VoIP traffic, and additions of security overheads, there exists a threshold point where an increase in call volume exerts a negative effect on pre-established calls with respect to time and the rate of packet loss. This study sought to determine the combination of cryptographic algorithms, cipher mode and voice codec that holds the uppermost threshold point, before the latency and rate of packet loss of active calls goes past ITU acceptable standards; for one way latency in both plain and encrypted VoIP traffic of 150ms and 200ms respectively and 5% packet loss rate. Through simulation of appropriate scenarios, results indicates that each of the encryption algorithms (AES, DES and 3DES) append additional overhead on the e2e delay and rate of packet loss during VoIP transmission. Also revealing that VoIP-supported codecs are faster and have a higher threshold in terms of the number of calls before the e2e delay and the rate of packet loss exceeds the acceptable limit for encrypted and plain VoIP e2e delay and packet loss rate.

Keywords
VoIP QoS, VoIP Security, VoIP Encryption, Block Cipher Encryption, Stream Cipher Encryption.

1. INTRODUCTION

The use of stream media applications such as Voice over Internet Protocol (VOIP) is of great importance in today's co-operate business strategy, public and private use because it provides a cheap alternative to the

traditional telephoning system for both VoIP service provides in terms of infrastructure cost and user calling cost. A 2010 study by IBISWorld showed that VoIP services have the best growth within the Information Technology industry from 2000 to 2009 with a growth of 179,036% [1]. VoIP is a technology that provides circuit switch like telephone service over an IP based network [2], its involves transmitting voice or media data over the internet by converting analogue signal into digital signals by the means of codec and uses Real-time Transport Protocols as the transport media [3]. Because of the increase in acceptance of VoIP technology, there is a need to secure VoIP traffic as the media networking protocol used in transmitting VoIP packet Real-time Transport Protocols has no security feature [4].

However, the increase in both packet size and processing (Encryption/Decryption) time of each of the encryption algorithms due to the encryption key size, cipher block size of the encryption algorithms creates an added overhead on VoIP packets during VoIP transmission; this will have a clear effect on the QoS in terms of e2e delay and the rate at which packet are dropped depending on the Queue buffer and the jitter buffer algorithms. In today's world where VoIP application users such as Skype, Apple Face Time are growing rapidly especially in the mobile platform sector and these users are competing with each other and other network devices for bandwidth, the need for selecting the best encryption algorithms and best mode of operation (stream/block cipher mode) with the highest threshold in terms of users in order to mitigate the cost of encryption on VoIP transmission and to effectively utilize the available network bandwidth cannot be over stated.

This work is aimed at determining the threshold at which Quality of Service (QoS) will be affected when AES, DES, 3DES encryption algorithms are discretely implemented on the VoIP Crypto-Engine in stream or block cipher mode. This will be achieved by quantifying the overhead produced by stream and block ciphers in terms of latency (e2edelay) and rate of packet loss during a pre-established VoIP transmission. On the specifics, target objectives tend towards; achieving a clear review of related works that shed light on the cryptographic overheads accrued on real time applications such as VoIP. To achieve through critical analysis, the design of well-defined Test parameters for performing the simulated experiment covering parameters such codec, cipher, bandwidth, network topology. Determine through experimental simulation, the encryption (AES, DES, and 3DES) algorithms and the mode of encryption (stream/block mode) with the highest threshold point at which the QoS is affected in a VoIP call system. And finally to a resource pool for network and security computer society in

both academia and industry, for the adequate selection of the best encryption algorithms, the best mode of operation (stream/block), combined with the best voice codec's for implementing in secure VoIP transmission.

Because of the lack of security mechanism in Real-time Transport Protocol (RTP), Secure Real-time Transport Protocol (SRTP) was developed in 2004. SRTP employs the use of cryptographic algorithm and hash functions to provide confidentiality, integrity, authentication and anti-reply of data transmitted over RTP [5]. This discourse will focus strictly on the cryptographic algorithms used by SRTP. By default SRTP supports symmetric encryption algorithm for media transmission of the VoIP packet. VoIP packets are segmented into four sections the IP header, UDP header 8, RTP header and Payload. Packet size may be different depending on the voice codec used which determine the payload size; overall the packet header size is 40 bytes (IP header 20bytes, UDP header 8 bytes, and RTP header 12 bytes). Since SRTP encrypts the payload not header information our focus will be on the payload size.

Although VoIP uses two main protocols; the signalling protocol and media transfer protocol, this work focuses on measuring the effect of encryption algorithms on media transfer protocols (RTP) only for pre-established VoIP transmission. Latency (e2eDelay), Packet Jitter and Packet Loss Ratio are the key network metrics used to determine the QoS of VoIP transmission. Precisely, only the effect of latency (e2eDelay) and the packet loss rate of the encryption algorithms will be determined. Encryption Algorithms to be covered include; Advance Encryption Standard (AES) with 128 bits key, Data Encryption Standard (DES) with 56 bits key and Triple Data Encryption Standard (3DES) with 56 bits key. The effects on latency and packet loss rate of the above listed encryption algorithms will be determined on G.711 and G.729 voice codec support VoIP network.

2. VOIP SECURITY: RELATED WORKS

Voice over Internet Protocols (VoIP) is a technology that transmits real time data such as voice and (or) video over the internet [6]. In other words, VoIP provides a Public Switch Telephone Network (PSTN) or Circuit Switch Telephone Service over a Packet Switch system such as the Internet or Intranet [7]. In the traditional PSTN network, analog voice signals are transmitted over the network, this is not the case in VoIP. VoIP converts voice signals by the use of codec algorithms; codec's converting the analog voice signals into digital packet, thus enabling voice signals to be transmitted over an IP-based network [8]. Unlike PSTN that supports a

dedicated end-to-end connection between the two end users, VoIP packet transmission does not require a directed channel, but rather employs UDP, which is a connectionless transport protocol. In VoIP, how the packets get from source to destination is not as important as the speed taken by packets to reach destination from the source [9]. VoIP supports the use of IP-phones (phones connected to the router), computer-to-computer communication, soft-phones (software based phones such Skype) and also in combination with PSTN or SIP-Based VoIP (internet/intranet), figure 1 shows a basic architecture of a VoIP system [10].

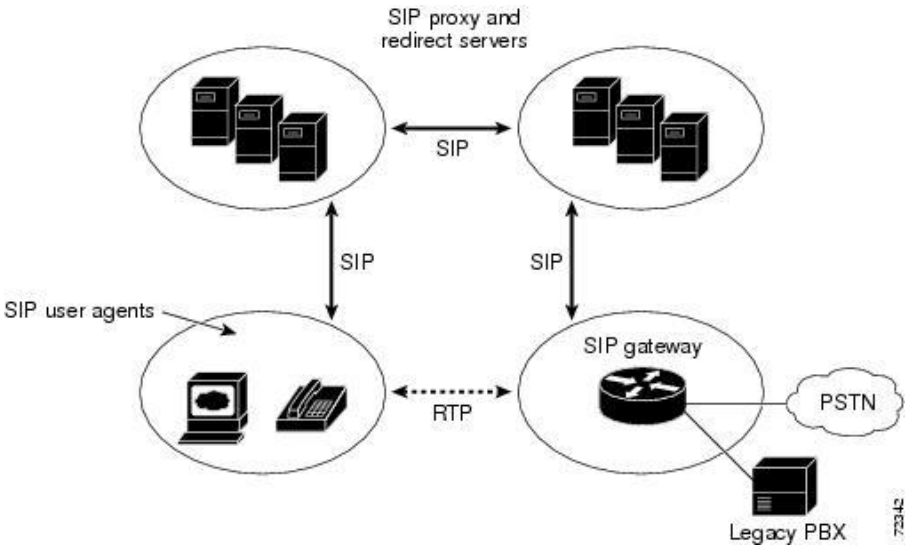

Figure 1: VoIP Architecture 1(VoIP 2005)

Basically, two categories of protocols come functional in the operations of a VoIP system; signalling protocols and media transfer protocols. While signalling protocols help to ensure end-to-end connection and (or) disconnection between two end users [11] , the media transfer protocols aid the actualization of real-time voice and (or) video packet transmission [12] .

2.1 Security Mechanisms for VoIP

It follows that by initial (default) design, both the signalling and media transfer protocols like SIP and RTP respectively have no security features attached, thus needing supporting protocols like SPD and RTCP respectively. This feature makes VoIP an easy target for attackers to eavesdrop on VoIP conversations and modify both the signalling and media transfer protocols [13] . In order to overcome these flaws, the three principles of security (Confidentiality, Integrity and Authentication) are implemented on both protocols.

2.1.1 Confidentiality

This defines a concept protecting data or information from unauthorised accessed. It is achieved by encrypting the media transport protocols using symmetric encryption algorithms running in stream or block cipher modes to encrypt/decrypt VoIP packet or blocks of VoIP packets. SRTP was developed to provide RTP with a means of ensuring confidentiality. SRTP encrypts only the payload section of the VoIP packet, leaving the Header information (IP/UDP/RTP) section unencrypted [14]. All VoIP packets traffic are encrypted at source and decrypted at the destination by a Crypto-Engine.

By way of elaboration, stream ciphers are a family of encryption algorithms where each bits on a plaintext such that $M = m_1 + m_2 + m_3$ are encrypted using a pseudorandom bits generated encryption key called a key stream such that $K = k_1 + K_2 + k_3$ using a XOR Red operation such that $EK(m) = Ek_1\ m_1 \oplus k_1 = C_1$ to create a cipher C_1 [15]. However, block ciphers are encryption algorithms that encrypt blocks of data at a time [16]; instead of one bit at a time like stream ciphers. Block ciphers segment the bits of plaintext into blocks usually a fixed size of 128 bits in the case of AES [17], but may differ with other ciphers. Using mode operation a random bits generated key is combined with bits from the previous successive ciphers to encrypt each block of data [18]. When used in VoIP, packets in blocks of128 bits of size for AES are encrypted and decrypted by the crypto-engine using a random key from each successive block of bits [19] , [20] .

2.1.2 Integrity

This principle saves from unauthorised modification of data or information. The integrity of VoIP traffic is archived by the use of a Hash function algorithm. By default HMAC-SHA1 is used to ensure that VoIP packets have not been altered during transmission. Integrity is also implemented in VoIP when establishing a session in SIP. Typically, hashing the VoIP packet includes both the VoIP payload and the information Header. At the source end a hash value of RPT or SRTP VoIP packets is generated and the integrity is checked at the destination end by generating its own hash value and comparing it against the hash value of the received.

2.1.3 Authentication

The security by Authentication feature used in VoIP is performed on the Session Protocols, in order to authenticate end-to-end establishment of VoIP session, asymmetric encryption algorithms are used. The two end users

negotiate a cipher suite to use in order to create a master key [14]. For instance, the SIP protocol doesn't support any security mechanisms, but by the use of well-known, publically tested internet security mechanisms such as HTTP digests; it provides a mechanism for authenticating VoIP users. The authentication process can be hop-to-hop or end-to-end [21].

2.2 VoIP Operation: Wired and Wireless Modes

In a wired network scenario, VoIP system operates such that the user obtains an IP address from a DHCP server. The VoIP terminal (softphone) registers with a call server (PBX); where voice services access is granted after a completed registration process. For a call to be placed or received with the terminal device, the call server adds the registered device to a Domain Name System (DNS) server, thus enabling a directory lookup on an IP network. When *Paul* dials *Alice*, The destination number (*Alice's*) is routed to a call server which in turns notifies the destination terminal (*Alice*). Once the destination terminal (*Alice*) accepts the call, a notification is sent back to the call server and the call server sends a notification to both terminals that a channel is available to start a conversation.

However, the service flexibility in terms of mobility has seen wireless VoIP (VoIPoW) advancing farther than landline networks. VoIPoW enables mobile devices such as laptops, mobile phones, two way radios etc., to place and receive VoIP calls on a wireless network infrastructure either through Wireless LAN or Wireless WAN. Just like in VoIP wired landline network, in VoIPoW; the user terminal connects and registers with a call server by obtaining an IP address from a DHCP server, while SIP and RTP protocols supported by TCP/UDP helps the user to initiate and engage in a VoIP conversation by routing the compressed voice packet over a gateway to the destination user. Thus, VoIP employs the use of multiple protocols that support IP-based network, wired or wireless radio communication technology and other legacy communication systems such as PSTN and ISDN. It can also be deployed on a multitude of different architectures.
For instance, Session Initiation Protocol (SIP) is a signalling protocol that is an application layer protocol on the TCP/IP network model which is based on request-response. It implies a client/server based architecture usually connecting two end users via a proxy server. The protocol is used to establish, terminate and modify sessions in VoIP over an IP based network [22]. SIP is also supported by Session Description Protocol (SDP); a protocol that carries the session descriptions such as session information and media information [23]. SDP is transmitted with the SIP packet during the first 'INVITE' packet and contains the session information that consists

of the session name and proposes the number of times the session is active, and the contact detail of the source of the session. The media information consists of type of media (voice/video) and the transport protocol information (RTP/UDP/IP).

Real-time Transport Protocol (RTP) is another protocol-instance classified as a Media Transport Protocol. It comes useful when transferring real-time data such as voice or any media over the internet [24] either over a multicast or unicast network, and it is also supported by control protocol called Real-time Transport Control Protocol (RTCP). RTCP carries the description of the data packet being transmitted by RTP and is also used to determine the Quality of Service [25]. It contains information about the RTP packet such as; information about the users, and information that is used to measure Quality of Service parameters like number of packet loss and jitters. Both RTP and RTCP are designed to be completely independent from transport protocol (TCP/UDP) on the TCP/IP layer model [26].

2.3 VoIP Security and QoS: Approaches and Shortcomings

With relativity to VoIP Networks, quality of service (QoS) can be defined as the quality of voice/video during a VoIP transmission [27], and it is measured based on acceptable criteria's set by international standard organizations like the International Telecommunication Union (ITU) and the Internet Engineering Task Force (IETF). In broader terms, network criteria for measuring service efficiency include; latency, packet loss and jitter. These too are applicable to VoIP. However, the economic constraint of an encryption algorithm on QoS depends on the encryption cipher and codec used [28]. In other words, the length of the encryption key and the mode of encryption (stream/block ciphers) combined with the processing time for encoding and decoding of the VoIP payload by the codec determines the budget on the QoS. Thus a logical solution to achieving our goal is to study the effect of voice codec when combined with the encryption algorithms and how they affect latency, packet loss and jitter during VoIP transmission.

2.3.1 Latency

Latency or e2edelay in VoIP is the total round-trip delay time for a bi-directional VoIP packet transmission between two end users [29]. It can be measured in two ways; 250ms for a round-trip from source to destination and back to the source, or 150ms for one-way trip from source to destination, which also includes the delay time for the packet to travel along multiple hops over the internet as specified by the ITU-G 11.4 standards. It is calculated by defining three parameters in VoIP transmission; $D_{transmitter}$,

$D_{network}$, $D_{receiver;}$ where Delay is obtained by summing the three parameters [30]. The size of the encryption key and the mode of operation (stream/block) by the cipher algorithm will lengthen the encoding and decoding processes of the codec which will in turn increase the latency delay of the VoIP packet [19]. A study on the effect of DES/3DES/AES-128-256, RC2 and Blowfish encryption algorithm on latency during a VoIP transmission using different bandwidths (34Kb, 64Kb) shows thus; when using 34kb bandwidth each of the encryption algorithms generate latency when compared with the use of firewall and without the use of firewall. Blowfish generates the highest latency with a time of 0.00001600 seconds. While a 64kb bandwidth, with or without a firewall generates almost the same latency with 3DES yielding the highest latency when compared with the other algorithms [31].

2.3.2. Jitter

Jitter defines the measured variation in each successive packet arrival time due to transmission delay [32]. This occurs when each successive packet have a different latency, since packets are transmitted over the network by the UPD transport protocol each packet will take a different pathway, and the arrival time will differ from source to destination A jitter buffer algorithm is used to assemble the packet but at the cost of time. If the packet cannot be reassembling within 150ms the packet is dropped. The acceptable level of jitter is about 20ms regardless of the number of multiple hops between the source and destination, if the time increases above 20ms the buffer cannot reassemble the packets in correct order making the conversation sound choppy [30].

The study of the impact of security mechanism on VoIP by measuring the effects on the encryption algorithms (3DES/AES-128-256/Blowfish and RC2 on 38k, 64k, 100M network bandwidths) on selected criteria as presented by (Talevski 2011) shows a high ratio of jitter on VoIP when there is no encryption and using a firewall while at 100M the jitter ratio is 0%. However, when using 38kb RC2 records the lowest ratio in comparison with 3DES, Blowfish, AES 128, AES 256 and DES. But when using 64k bandwidth RC2, AES 128, AES 256 and DES all yield lower ratios as compared with 3DES and Blowfish. Interestingly, when the bandwidth is 100Mbps there is no effect on the jitter on any of the encryption algorithms [33].

2.3.3. Packet loss

This defines the ratio of packets dropped due to limited jitter buffer size at the destination end, or packets that did not reach their destination **[34]**. An acceptable percentage of packet loss should be below 5%, which includes multiple hops between source and destination of the VoIP transmission. When the packet loss is greater than 5% the destination end user will only hear air space. The study by **[33]** shows that using 38Kbps of bandwidth in all the encryption algorithms (3DES/AES-128-256/Blowfish and RC2), packet loss ratio is above the acceptable limit of 5% except for 3DES which yields 4% in 64Kbps of bandwidth. However, for 100Mbps speed, the packet of the algorithms is below or within the acceptable limit, with or without a firewall component attached.

Therefore, it follows that the budget of encryption algorithm on QoS generally depends on the type of algorithm used, the length of the encryption key and the network bandwidth. The study presented above shows that only latency and packet loss bear negative impacts on the QoS. Its however amazing to note that the result of the two experiment show that encryption algorithms has a positive effect on the jitter of VoIP packets when compared to plain VoIP packet transmission; this might not be unconnected to network topology setup, since in all the test adopted a single point-to-point connection between the two computers there is no flexibility for VoIP packet taking multiple paths form source to destination

The proliferation of varying VoIP applications with varying platform dependence necessitates a study for the determination of the economic constraints for the implementation of encryption on network performances and CPU cycle performances and the affect it will have on quality of voice or video between two end users.

A comparative study of the effects of AES in both stream and block cipher modes on the QoS results relative to end-to-end delay between two end user [35]. The objectives of the study included; determining the errors generated by the two cipher modes when packets are decrypted at the destination end, and the effect of the errors on the QoS. Secondly, determining the effect of the two cipher modes on packet size, crypto-engine and packet loss on the QoS in terms of end-to-end delay. The authors used a GSM 06.10 Codec and AES algorithm for both stream and block mode to encrypt and decrypt RTP on the crypto-engine. The result showed that the packet size, crypto-engine and the packet loss all bear effects on the end-to-end delay between two end users. This outcome was further consolidated by [36], in his work. He worked on the effect of AES on packet size and the throughput of the crypto-engine when AES is operating on stream and block cipher mode.

Considering packet size scenario, his work showed that that each of the cipher mode has an effect on the packet size but AES operating on block cipher mode has a greater effect on packet size when compared to stream cipher mode, [36]. Considering crypto-engine, AES was used on the two cipher mode and the crypto-engine saturated by increasing the PPS by 25 PPS in every 30 seconds for each four (4) VoIP packet transmitted with the size of 60, 100, 250, and 100 for each of the four packets respectively. While focusing on packet size, the study proves that each of the cipher mode has an effect on the packet size but AES operating on block cipher mode has a greater effect on packet size when compared to stream cipher mode, the outcomes are shown in figures 2 and 3 [36].

The maximum threshold of the two cipher modes before the QoS is affected is indicated by a negative slope. In terms of packet loss, Mean Opinion Score (MOS) was used to evaluate the effect of packet loss on QoS of the two cipher modes on end-to-end delay. As would be noted, AES as stream cipher mode has less packet loss in end-to-end delay compared to block cipher mode, because of the use of key stream by stream ciphers. Summative, it implied that AES on stream cipher mode has a better performance than when run on block cipher mode that is before loss due to synchronization error [36].

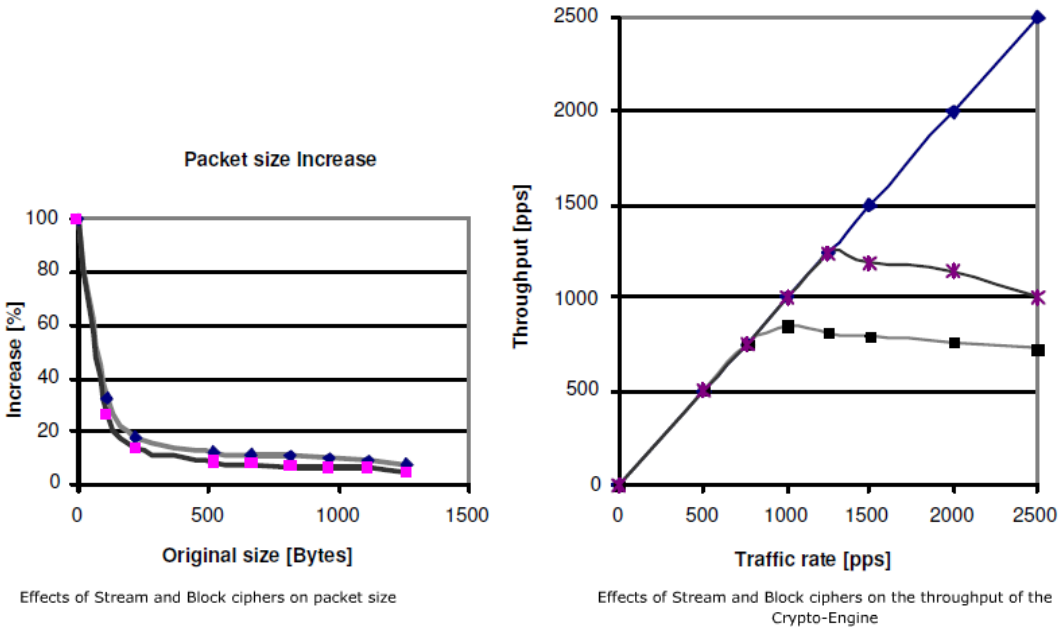

Figure 2: Effects of Stream and Block Ciphers on packet size and throughput [36]

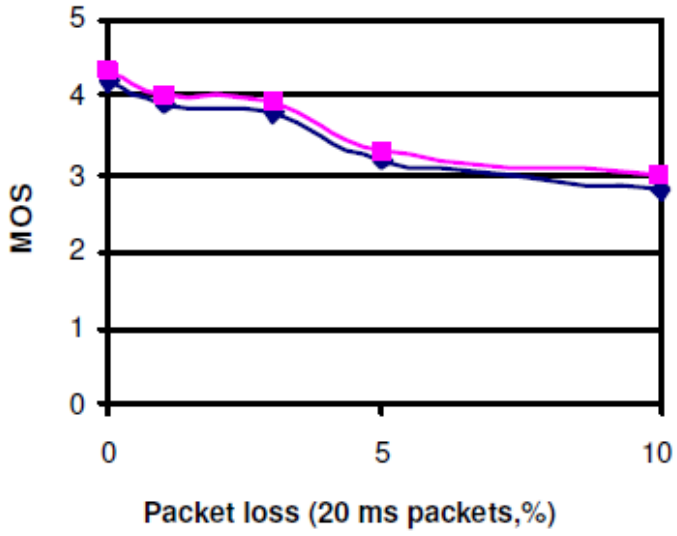

Figure 3: Packet Loss [36]

In another related experiment by [37], the focus was on a family of block ciphers that uses linear prediction as mode of operation. The authors determined the threshold point at which the QoS will be affected based on VoIP traffic in terms of call volume. Using iterative block cipher to encrypt the VoIP packet in a simulated network environment the authors used IPsec for end-to-end transmission of VoIP packets with a total number of 600 users on the network. The users are interconnected using switches, routers and a state full firewall and G.729 codec with DES/3DES/AES encryption algorithms used in block cipher mode. VoIP packet with G.729 codec having a payload size of 10, 20, 30 and 40 bytes for encrypted VoIP packets using DES/3DES and 10 byte, 20 byte and 30 byte for plain VoIP packets were transmitted. The outcome showed that in plain VoIP traffic the packet loss started at about 160 calls when the payload is 10 bytes in size and the end-to-end delay is within the acceptable limit. QoS was unaffected probably due to compression or the reduction of the throughput by the codec and combined with the buffer and the FIFO algorithm used by the authors [37].

The end-to-end delay when encryption was applied was above 200ms which is beyond the acceptable limit. However, packet loss consideration revealed a three-time increase in the payload size; especially when the payload size is 10 bytes and also observed that the rate of packet loss is lower with increased payload size when using DES/3DES encryption algorithm. For

call volume traffic the study revealed that for all payload size when G.729 codec is used with DES/3DES; the rate of packet loss will be above the acceptable loss limit [38].

The works reviewed took differing approaches for answering the question '*which algorithm is better in terms of the effect on the QoS of the VoIP network?'* The outcomes are quite similar with respect to latency, packet loss with each laying emphasis on direct relation between latency, packet loss, and jitter to the type of encryption algorithm in the crypto-engine, the cipher mode of operation, length of the encryption key and the payload size (codec). However, they both bear varied strengths and limitations that basically tended towards methodology, topology and parameters. While the former used a point-to-point network connection between the two hosts; which restricted the results to only VoIP in a peer-to-peer network, and focused on the use of only AES encryption algorithms, without considerations to other encryption algorithms like DES, 3DES, Blowfish, etc. The latter simulated a real world application of VoIP network with routers, switches, and firewall but whose result is only restricted to encryption algorithms running on block cipher modes only.

3. MODEL SIMULATION

This covers a detailed overview of the experiment test-bed and the simulation parameters that will be used to evaluate the effects of encryption algorithms on QoS; when implemented in Stream and Block ciphers mode to secure VoIP communication. The methodology for performing the experiment and the simulation parameters will all be implemented in NS2 network simulation environment. Such parameters as the VoIP codec, the type of encryption algorithms, the length of the encryption key, the mode of encryption (Stream or Block cipher mode), the network topology and the type of transport protocols (UPD/TCP), the media transfer protocol (RTP) and the network bandwidth will be considered. The comprehensive simulation parameters setup is captured in table 1.

3.1 Simulation Parameters

As noted earlier, the key components that constitute the basis for secure SIP-Based VoIP transmission include; voice codec, encryption algorithms, and networking properties such as bandwidth, propagation delay of the network links, queue type and size [39]. Thus, these will be used for the simulation. Table 1 shows the details of the simulation setup as would be used.

3.2 Simulation Scenario

The simulation is divided into two phases; phase **A** involves conducting an experiment with the defined encryption parameters using G.711 voice codec parameter following the process presented in figure 4, while phase B follows the same process, only this time using G.729 voice parameters.

As seen on figure 4, A TCL script is initiated containing networking parameters, voice codec parameters and encryption parameters in NS2. Each of the voice codec is run against the three encryption algorithms (AES, DES, 3DES) in stream or Block cipher mode. The effect of each of the encryption algorithm on the QoS when operating in stream or block cipher mode will be evaluated, and the effect on the QoS will be measured in terms of e2edelay and packet loss rate. An analysis of the collected data will be made, the analysed data will be measured against the acceptable standard define in ITU standards.

1) AES Scenario

The first simulation scenario involves evaluating the cost of AES encryption when implemented in stream or block cipher mode in securing VoIP traffic. The cost of AES encryption with 128 bits key on QoS when used in combination with G.711 and G.729 codec's is quantified by measuring the latency (end2end one way delay) of VoIP packet from source to destination as shown in the figure 5. The figure indicates that simulations will run for 10 minutes, in each successful minute of the simulation ten nodes having two-way VoIP transmission will be initiated. Each VoIP packet during the transmission will be encrypted with AES encryption algorithm.

Table 1: Simulation Setup

Statistics	**Value**			
Test Platform	Ubuntu Virtual Machine			
Simulator	NS2			
Number of scenarios	3			
Number of Nodes	100			
Number of domains	4			
Nodes per domain	25 (To simulate the different geographical locations covering the study.			
Network Properties	Bandwidth Speed (Optional)	2Mbps		
	Queue Type	Drop Tail		
	Queue Size	50		
	Propagation Delay	10ms		
Simulation Parameters	Voice Codec	G.711	G.729	
	Encryption Algorithm	AES (Key length 128 Bits, Block size 128 bits)	DES (Key length 56 Bits, Block size 64 bits)	3DES (Key length 168 Bits, Block size 64 bits)
	Traffic			
Test Metrics	- End-to-End Delay - Packet Loss			
Simulation Scenarios	- AES Scenario - DES Scenario - 3DES Scenario			

e

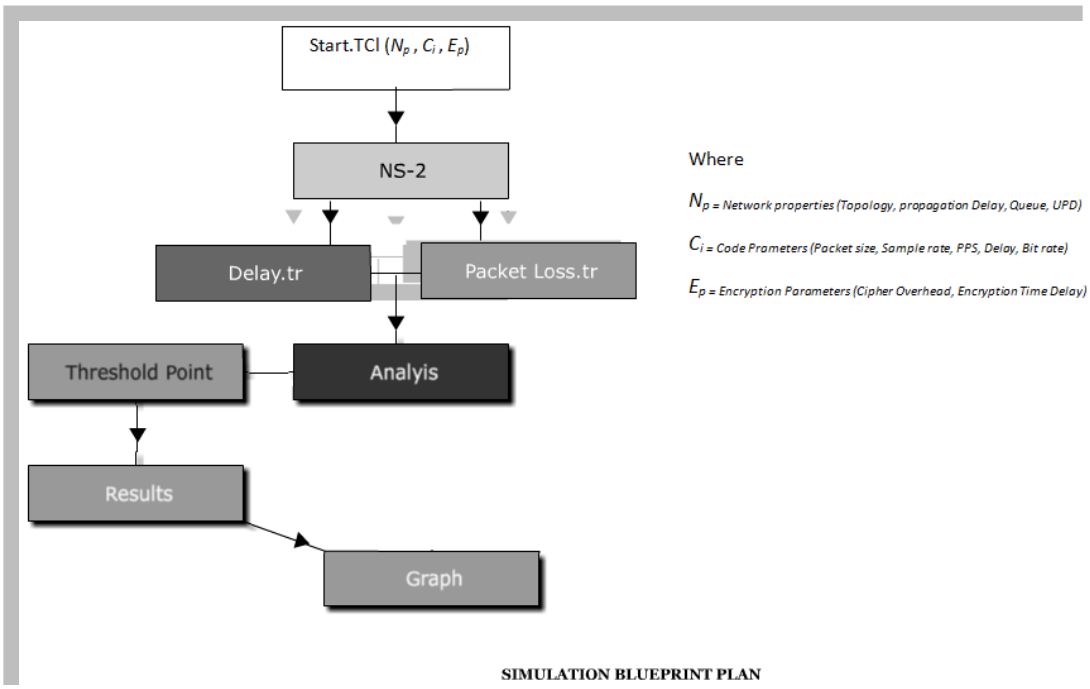

Figure 4: Simulation Blueprint.

The AES simulation will be sub-divided into two experiments in which AES will run on Stream cipher mode and again run on Block Cipher mode. In each of the cipher modes G.711 and G.729 VoIP codec will be encrypted. Using the volume of VoIP traffic, the threshold point at which the QoS will be affected with respect to the two cipher modes will be determined. The criteria that will be used to measure the effect on the QoS are; end2end delay and the rate of packet loss when the number of VoIP traffic is increased in each successful 1minute of the 10 minutes of the simulation.

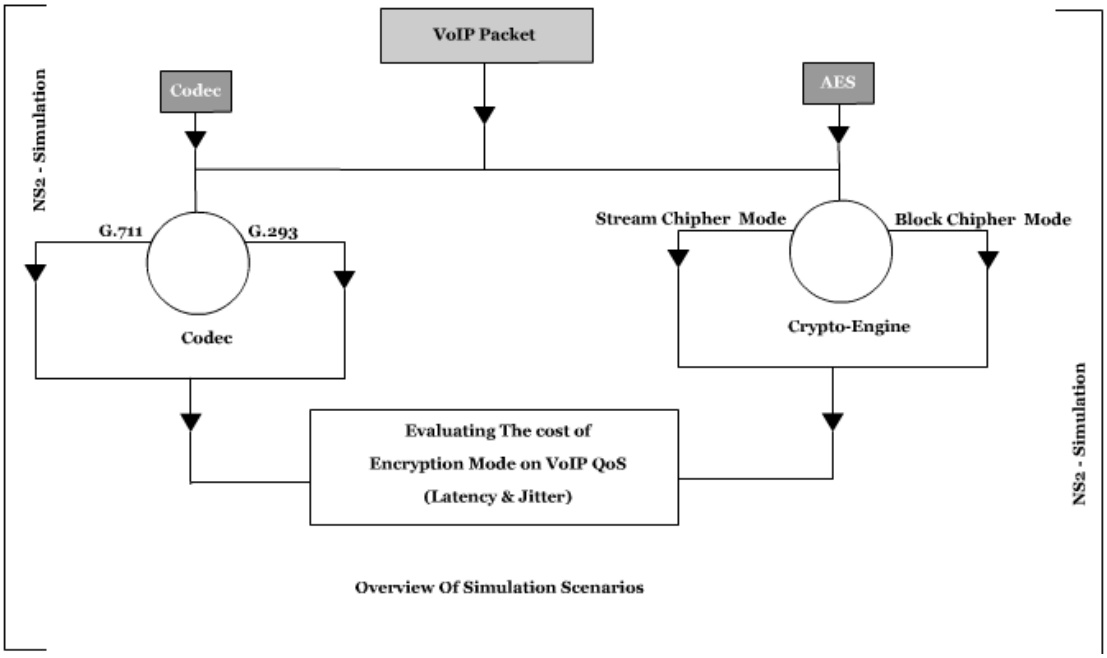

Figure 5: AES Simulation Scenario

2) DES Scenario

This involves using DES encryption algorithm with 54 bits encryption key and 64 bits block size to encrypt the VoIP packet. G.711 and G.729 codecs will also be used in a similar scenario as depicted in figure 5.

Adopting the similarities, DES simulation will run for 10 minutes, in each successful minute of the simulation, ten nodes each having two-way VoIP transmission will be initiated with each VoIP packet during the transmission encrypted with DES 54 bit encryption key algorithm. The scenario is also segmented into two experiments in which DES runs on Stream cipher mode and on Block Cipher mode, with each of the cipher modes utilizing G.711 and G.729 VoIP codecs in encrypted forms. Using the volume of VoIP traffic, the threshold point at which the QoS will be affected in respect to the two cipher mode will be determined. Similar criteria as the AES are also adopted here for the simulation timeline.

3) 3DES Scenario

This third simulation adopts Triple DES (3DES) encryption algorithms to encrypt VoIP traffic. Akin to DES in the second simulation, 54 bits encryption key length and 64 bit block size will be used in combination with

G.711 and G.729 codecs, with a simulation runtime of 10 minutes. In each successful minute of the simulation, ten nodes having a two-way VoIP transmission will be initiated with each VoIP packet during the transmission encrypted with 3DES 54 bit encryption key algorithm.

And just like the prior tests, 3DES will run on both Stream cipher and Block Cipher modes with each of the cipher modes utilizing G.711 and G.729 VoIP codecs in encrypted form. All other criteria similar to prior test.

4. RESULTS AND ANALYSIS.

Based on defined parameters for the study, focused is directed on the threshold point at which the QoS of active VoIP calls exceed the acceptable limits as a result of overheads created by each encryption algorithms in stream and block cipher mode during VoIP transmission.

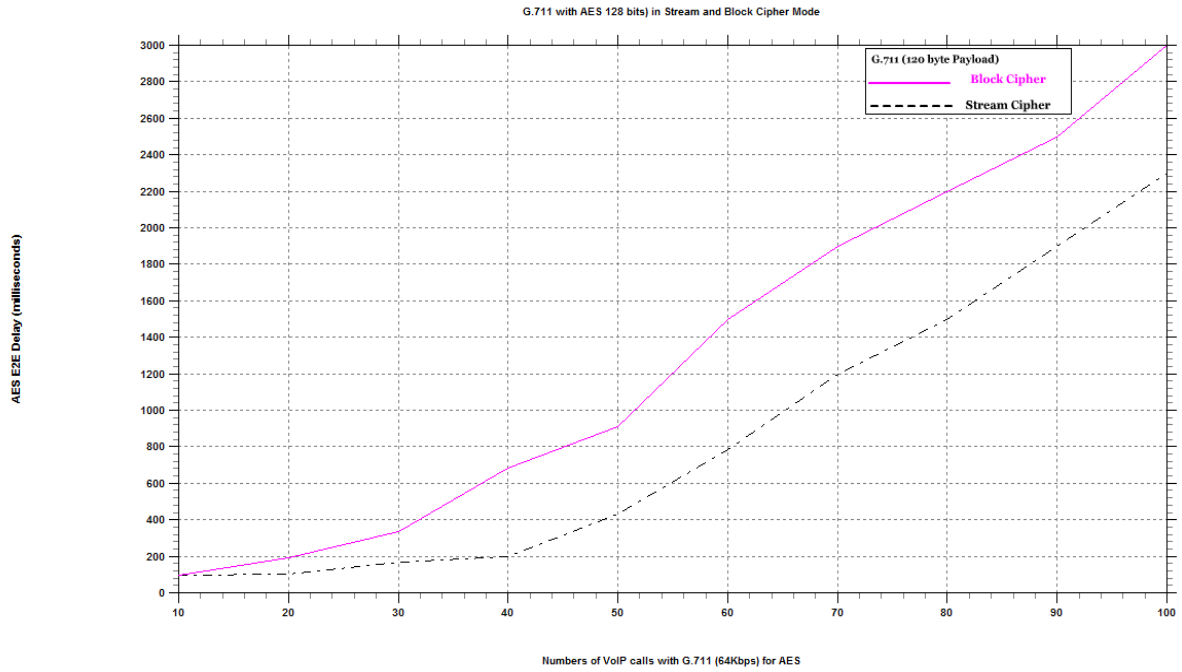

Figure 6: AES using G.711 (64Kbps) in Stream and Block Cipher mode

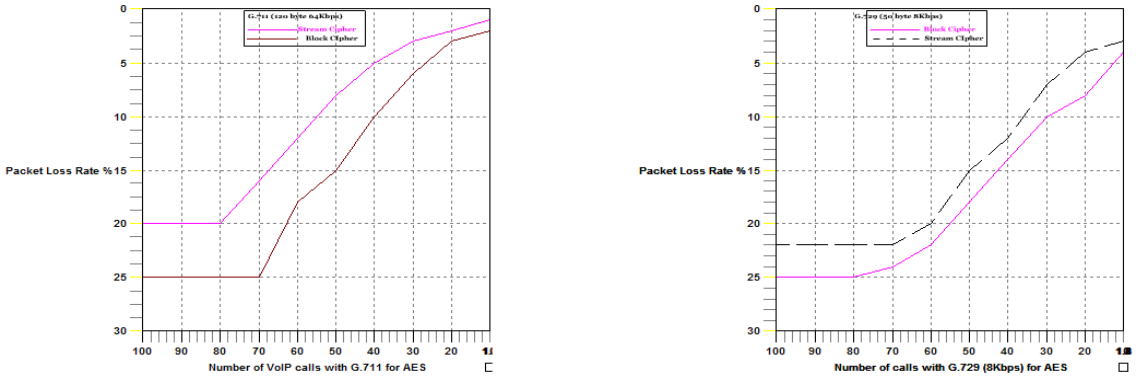

Figure 7: Packet Loss Rate for AES using G.711 (64Kbps) |G.729 (8Kbps)

4.1 AES E2E Delay and Packet Loss Rate

Comparing the effects on e2e delay and packet loss rate for AES (128 bits) operating in stream and block cipher modes on G.711 (64Kbps) and G.729 (8Kbps). The implementation of AES (128 bits) in stream cipher mode performs better and faster when compared with AES (128 bit) in block cipher mode as shown in figure 6. The results shows that AES (128 bits) in stream mode has a higher threshold point before the e2e delay exceeds the acceptable standard defined by ITU with 40 VoIP calls for encrypted VoIP traffic and 30 VoIP calls for plain VoIP traffic which are about 200ms and 150ms respectively. AES (128 bits) in block cipher on G.711 (64Kbps) has a lower threshold point with 20 VoIP calls for encrypted VoIP traffic with 200ms and 10 VoIP calls for plain VoIP traffic with 150ms respectively. Similarly, AES (128 bits) using G.729 (8Kbps) on stream and block ciphers modes shows parallel results with G.711 (64Kbps) both in stream mode and block cipher mode.

On the other hand, results show that AES using G.729 (8Kbps) codec in stream mode perform better in block mode, with a threshold of 40 VoIP calls for encrypted VoIP traffic which is 201ms and 30 VoIP calls for plain VoIP traffic which is 155ms, and in block cipher mode the threshold of 20 VoIP calls for encrypted VoIP traffic which is 200ms and 15 VoIP calls for plain VoIP calls which is 150ms.

The high threshold of AES (128 bits) in stream cipher mode on both G.711 (64Kbps) and G.729 (8Kbps) codecs can be directly linked to, how stream ciphers encrypt and decrypt data using an XORed operation, in which each bits of data is encrypted using a key stream. The voice codec delay, the network propagation delay, network bandwidth and the FIFO queue buffer

at each particular time of the simulation are also a major contributing factor to the increase in e2e delay in each of the cipher modes.

Considering the rate of packet loss for AES (128 bits) with G.711 (64Kbps) and G.729 (8Kbps), results as shown in figure 7 shows that AES (128 bits) in both G.711 (64Kbps) and G.729 (8Kbps) codecs on stream and block cipher mode has a drastic effect on the rate of packet loss. Although the results indicates that AES (128 bits) in stream cipher mode has a lowest packet loss rate when compared with AES (128 bits) in block cipher mode which yields 40 VoIP calls before the acceptable packet loss rate of 5% is exceeded . While in block cipher mode yields a threshold of 25 VoIP calls before 5% packet loss rate is exceeded. For G.729 (8Kbps) codec, it indicates that AES (128 bits) has little significant difference in stream and block cipher mode with respect to packet loss rate. Specifically, AES (128 bits) in stream mode has a threshold of 22 VoIP calls before the packet loss rate exceeds 5%, and a threshold of 12 VoIP calls in block mode. Increase in packet size, and FIFO queue algorithms on each of the routers all contribute to the rate of packet loss.

4.2 DES E2E Delay and Packet Loss Rate

Looking at the effect of DES (56 bits) on e2e delay and packet loss rate using G.711 (64Kbps) and G.729 (8Kbps) codecs, results show that the implementation of DES (56 bits) in stream cipher mode performs better and faster when compared with block cipher mode. DES (56 bits) in stream mode yields a higher threshold point before the e2e delay exceeds the acceptable limit with 40 VoIP calls for encrypted VoIP traffic and 25 VoIP calls for plain VoIP traffic which are about 200ms and 150ms respectively, compared to the block mode which yields a threshold point with 25 VoIP calls for encrypted VoIP traffic with 200ms and 15 VoIP calls for plain VoIP traffic with 150ms respectively. Correspondingly, DES (56 bits) with G.729 (8Kbps) on stream and block cipher shows similar results with G.711 (64Kbps) both in stream mode and block mode as shown in figure 8. Threshold variations are linked to how stream ciphers encrypt and decrypt data using a XORed operation, in which each bits of data is encrypted using a key stream. All other contributors to delay and specifically, discontinuous e2e delay remain the same as in AES scenario.

For rate of packet loss on G.711 (64Kbps) and G.729 (8Kbps) codec with DES (56 bits) encryption, results in figure 9 show that DES (56 bits) in both G.711 (64Kbps) and G.729 (8Kbps) on stream and block cipher mode has a sweeping outcome on the rate packet loss. On G.711 (64Kbps), DES (56 bits) in stream cipher mode has a less packet loss rate when compared with

DES (56bits) in block cipher mode with 20 VoIP calls before the acceptable packet loss rate of 5% is exceeded. While in block cipher mode, the threshold point at which the acceptable packet loss rate exceeds 5% is at 15 VoIP calls. While On G.729 (8Kbps), it indicates that DES (56 bits) has no significant difference in stream and block cipher mode with respect to packet loss rate, this is because the rate of packet loss of the two cipher mode is drastic in less than 10 VoIP calls for acceptable packet loss of 5%; all other conditions remaining unchanged as with AES (128bits).

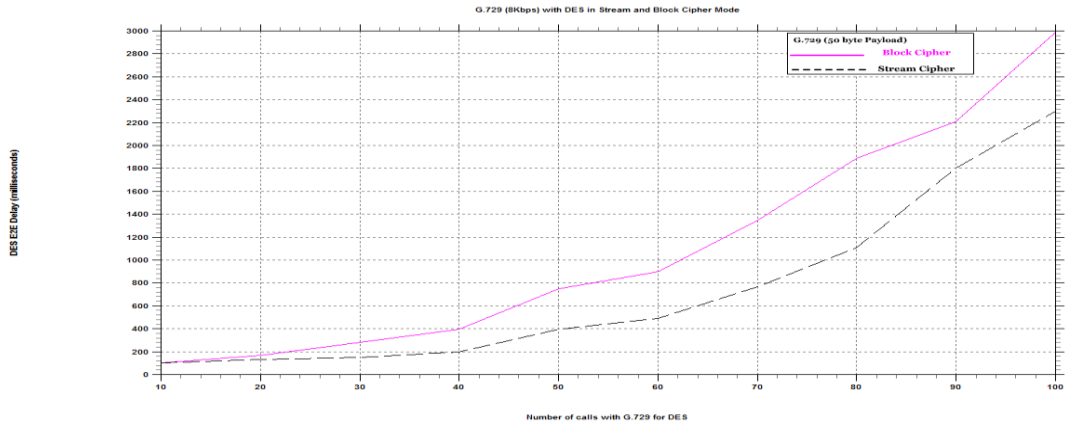

Figure 8: DES with G.729 (8Kbps) in Stream and Block Cipher mode

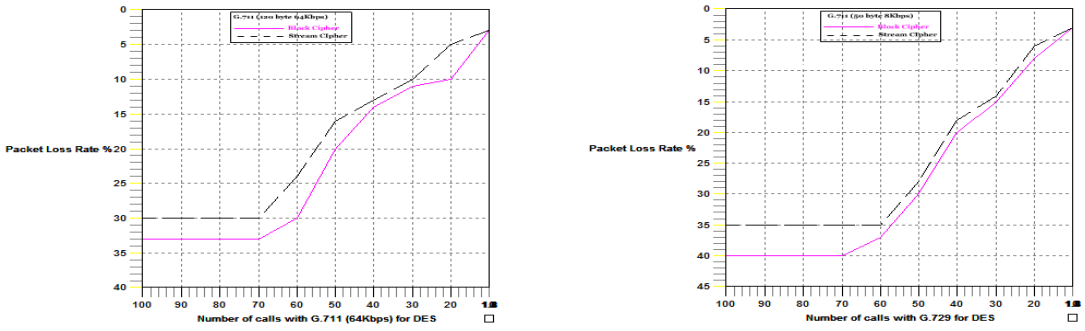

Figure 9: Packet Loss Rate for AES with G.711 (64Kbps) |G.729 (8Kbps)

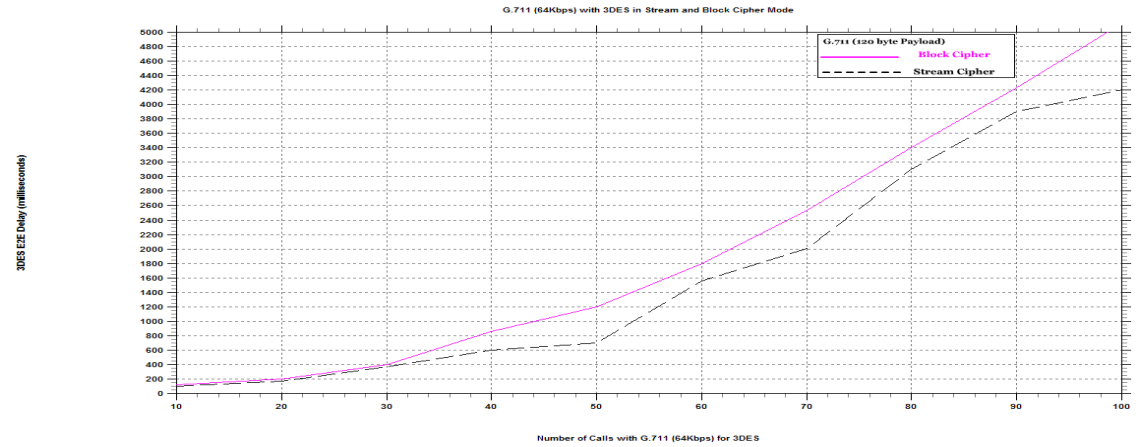

Figure 70: 3DES with G.711 (64Kbps) in Stream and Block Cipher mode

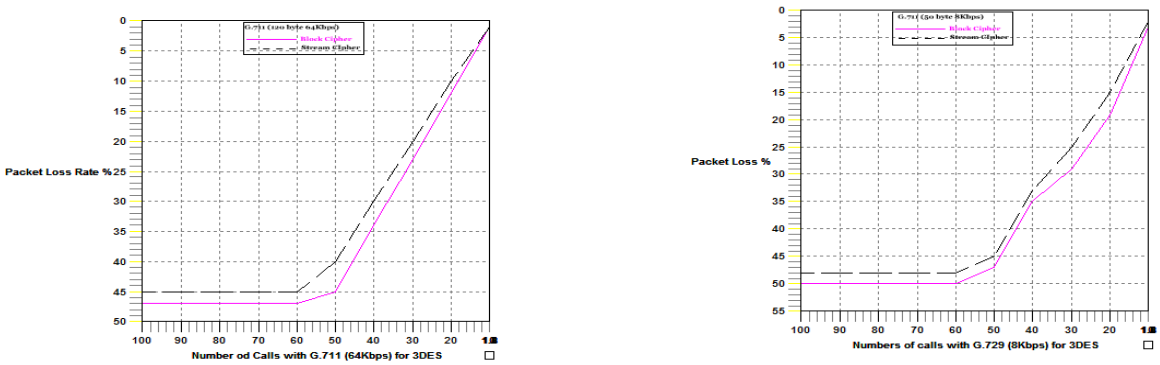

Figure 81: Packet Loss Rate for AES with G.711 (64Kbps) |G.729 (8Kbps)

3DES E2E Delay and Packet Loss Rate

Underscoring the effects of 3DES on e2e delay and packet loss rate using G.711 (64Kbps) and G.729 (8Kbps) codec, the outcome shows that 3DES (56 bits) in stream cipher and block cipher mode has no significant difference as shown in figure 10. The difference can only be noticed when the number of VoIP calls exceeds 40 calls. 3DES (56 bits) in both stream and block cipher mode on G.711 (64Kbps) all yield a threshold point of 20 VoIP calls encrypted VoIP traffic with 200ms and 10 VoIP calls for plain VoIP traffic with 150ms in stream mode, the results for block cipher mode was not farfetched. 3DES (56 bits) with G.729 (8Kbps) on stream and block cipher show similar results with G.711 (64Kbps) both in stream mode and block mode. The low threshold of 3DES (56 bits) in stream and block cipher mode on both G.711 (64Kbps) and G.729 (8Kbps) can be directly

linked to the large computational time required to encrypt and decrypt bits and blocks of data.

For the rate of packet loss for DES (56 bits) with G.711 (64Kbps) and G.729 (8Kbps), 3DES (56 bits) in both G.711 (64Kbps) and G.729 (8Kbps) on stream and block cipher mode has a far-reaching outcome on the rate of packet loss. This is shown in figure 11. On G.711 (64Kbps), the results indicates that 3DES (56 bits) in both stream and block cipher mode packet loss rate are negligible between the two cipher modes; with each of the cipher mode exceeding 5% packet loss at about 5 VoIP calls. However, using G.729 (8Kbps); the results indicates that 3DES (56 bits) has no significant difference in stream and block cipher modes with respect to packet loss rate. This is because the rate of packet loss of the two cipher mode is drastic in less than 5 VoIP calls for acceptable packet loss of 5%.

5. CONCLUSION AND FUTURE WORKS

The results of the simulations shows that using AES (128 bits) and DES (56 bits) in stream cipher mode yields a better and faster performance compared to when implemented in block cipher using G.711(64Kbps) and G.729(8Kbps) codec's supported VoIP network. Whereas in 3DES there are no significant differences in stream or block cipher when implemented using G.711 (64Kbps) and G.729 (8Kbps) supported VoIP networks.

Truthfully, cryptographic algorithms and hash functions are used to guarantee confidentiality, authentication, and integrity and anti-replay of VoIP packets. However the use of cryptographic algorithms on real time applications such as VoIP comes with a cost in terms of delay and increase in packet size, which is due to the processing time required encrypted and decrypt VoIP packets before transmission at the source and after transmission at the destination. Couple of components on the VoIP system like voice codec, Jitter buffer algorithms, routers queue size and the network bandwidth all impose transmission delays, which apparently pose performance and productivity setbacks to VoIP service providers and developers. When all this delay factors are combined with the cryptographic delay there will be a point at which latency and rate of packets loss due to the cryptographic delay and increase in packet size will have a negative effect on the QoS of active calls.

Undoubtedly, the results of the study strongly indicates that each of the encryption (AES, DES, 3DES) algorithms append an additional overhead on the e2e delay and rate of packet loss during VoIP transmission. However

when calculating and comparing the overhead of each of the three encryption algorithms, it demonstrates that AES and DES (in stream cipher mode on G.711 (64Kbps) and G.729 (8Kbps). VoIP support codec are faster and have a higher threshold in terms of number of calls before the e2e delay and the rate of packet loss exceeds the acceptable limit for encrypted and plain VoIP e2e delay and packet loss rate. The simulation also implies that there no significant difference in both e2e delay and packet loss rate for 3DES in stream and block ciphers modes on G.711 (Kbps) and G.729 (8Kbps) VoIP supported codec, this is because 3DES has a drastic effect both the e2e delay and packet loss rate at similar number of calls. Although the study only focuses at measuring the effects of stream and block ciphers on VoIP in terms of e2e delay and the rate of packet loss during VoIP transmission. It did not address the issues of the effect of Synchronization and Bit Explanation errors generated by stream and block ciphers respectively. Future work can tend towards measuring the cost of errors generated by both cipher modes on pre-established VoIP transmission.

REFERENCES

[1] B Boguhn. (2009, June) A Compare Business Products Web site. [Online]. http://www.comparebusinessproducts.com/phone-systems/business-voip/voip-named-as-fastest-growing-technology-of-the-past-decade.

[2] N Wittenberg. (2009) Understanding Voice Over IP Technology, Cengage Learning. Document.

[3] D J Wright. (2001) Voice over packet networks. Document.

[4] O Hersent, *IP Telephony: Deploying VoIP Protocols and IMS Infrastructure*.: John Wiley & Sons, 2010.

[5] M Leggieri and E Gambi, "Quality assessment of secure VoIP communications," in *16th International Conference on Software, Telecommunications and Computer Networks, 2008. SoftCOM 2008*, 2008.

[6] J Fischl and H Tschofenig, "Making SIP Make Cents ," *Queue*, vol. 5, no. 2, pp. 42-49, 2007.

[7] C Shiping and W Xinyuan, "On the anonymity and traceability of peer-to-peer VoIP calls," *Network*, vol. 20, no. 5, pp. 32-37, 2006.

[8] A S.W Marzuki and C Yu Ka, "Performances analysis of VoIP over 802.11b and 802.11e using different CODECs," in *2010 International Symposium on Communications and Information Technologies (ISCIT)*, 2010.

[9] N Sulaiman and R Carrasco, "Performance Evaluation of Voice Call over an IP based Network," in *41st Annual Conference on Information Sciences and Systems, 2007. CISS '07*, 2007.

[10] M B VoIP. (2005) A Business Voip Website. [Online]. http://mybusinessvoip.com/what-is-voip

[11] K K Tam and H L Goh, "Session Initiation Protocol," in *IEEE International*

Conference on Industrial Technology, IEEE ICIT '02, 2002.

[12] N Kara and V Planat, "Performance analysis of IP multimedia services over HSDPA mobile networks," in *Intern ational Conference on IP Multimedia Subsystem Architecture and Applications, 2007*, 2007.

[13] D Geneiatakis and T Dagiuklas, "Survey of security vulnerabilities in session initiation protocol," *IEEE Communications Surveys & Tutorials*, vol. 8, no. 3, pp. 68-81, 2006.

[14] Cisco. (2011) A Cisco Corporation Website. [Online]. http://www.cisco.com/web/about/security/intelligence/securing-voip.html

[15] F Shang and K Sun, "An Efficient MPEG Video Encryption Scheme Based on Chaotic Cipher," in *Congress on Image and Signal Processing, 2008. CISP '08*, 2008.

[16] O Chung-Ming, "Design of block ciphers by simple chaotic functions," *Computational Intelligence Magazine*, vol. 3, no. 2, pp. 54-59, 2008.

[17] P Jun and Y Mingying, "Research on a Block Encryption Cipher Based on Chaotic Dynamical System," in *Third International Conference on Natural Computation, 2007. (ICNC 2007)*, 2007.

[18] P Sarkar, "Pseudo-Random Functions and Parallelizable Modes of Operations of a Block Cipher," *IEEE Transactions on Information Theory*, vol. 56, no. 8, pp. 4025-4037, 2010.

[19] A L Alexander and A L Wijesinha, "An Evaluation of Secure Real-Time Transport Protocol (SRTP) Performance for VoIP," in *Third International Conference on Network and System Security, 2009. NSS '09*, 2009.

[20] G Paul and S Maitra. (2011) Rc4 Stream Cipher and Its Variants. Document.

[21] Geneiatakis Dimitris, Dagiuklas Tasos, K G, Costas Lambrinoudakis, and Stefanos Gritzalis. (2004) SIP Security Mechanisms: A state-of-the-art review. Document.

[22] D R Wisely, "SIP and Conversational Internet Applications," *BT Technology Journal*, vol. 19, no. 2, pp. 107-118, 2001.

[23] T Guenkova-Luy and H Schmidt, "Service Mobility with SIP, SDP and MPEG-21," in *9th International Conference on Telecommunications, 2007. ConTel 2007*, 2007.

[24] X Mochna, "Simulation of packet losses in video transfers using real-time transport protocol," in *20th International Conference on Radioelektronika (RADIOELEKTRONIKA), 2010*, 2010.

[25] L Associates. (2003) An L Associates Website. [Online]. http://www.l1associates.com/VoIP%20Protocols.pdf.

[26] J F Ransome and J W Rittinghouse, "VoIP Security," Elsevie Report 2005.

[27] A Meddahi and H Afifi, ""MOSQoS": Subjective VoIP Quality for Feedback Control and Dynamic QoS Adaptation," in *IEEE International Conference on Communications, 2006. ICC '06*, 2006.

[28] R M Dansereau and S Jin, "Reducing Packet Loss in CBC Secured VoIP using Interleaved Encryption," in *Canadian Conference on Electrical and Computer Engineering, 2006. CCECE '06*, 2006.

[29] K Gonia, "Latency and QoS for Voice over IP," SANS Institute, SANS Institute, 21., White Paper 2004.

[30] D. A. C Edward Paul Guillen, "VoIP Networks Performance Analysis with Encryption Systems," *World Academy of Science, Engineering and Technology*, vol. 58, no. 15, 2009.

[31] M Rawashdeh and A Karmouch, "Seamless video handoff in session mobility over the IMS network," in *IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks & Workshops, 2009*, 2009.

[32] L Atzori and F Boi, "IP Telephony over Mobile Ad Hoc Networks: Joint Routing and Playout Buffering," in *IEEE International Conference on Communications, 2008. ICC '08*, 2008.

[33] A Talevski et al., "The Impact of Security on VoIP Call Quality," *Mobile Multimedia*, vol. 7, no. 1, pp. 113-128, April 2011.

[34] M F Tuysuz and H A Mantar, "Evaluation of cross layer QoS aproachs for improving voice quality over multi-rate WLANs," in *2010 International Conference on Computer Engineering and Systems (ICCES)*, 2010.

[35] Ashraf D Elbayoumy and Simon J Shepherd, "Stream or Block Cipher for Securing VoIP?," *International Journal of Network Security*, vol. 5, no. 2, pp. 128–133, September 2007.

[36] A. D. E. a. S. J Shepherd , "Stream or Block Cipher for Securing VoIP?," *International Journal of Network Security*, vol. 5, no. 2, pp. 128–133, 2007.

[37] Gregory Epiphaniou, Carsten Maple, Paul Sant, and Peter Norrington, "The effects of encryption on VoIP streams under the code-excited linear prediction coder G.729," in *2010 International Conference for Internet Technology and Secured Transactions (ICITST)*, 2010.

[38] G Epiphaniou, C Maple, P Sant, and P Norrington , "An experimental analysis on iterative block ciphers and their effects on VoIP under different coding schemes," in *2010 International Conference on Signal Processing and Multimedia Applications (SIGMAP)*, 2010.

[39] Mohammed Mustapha, "Measuring the Security Overhead of Stream and Block Ciphers on SIP-Based VoIP Transmission," Department of Computer Science and Technology, University of Bedfordshire, Bedfordshire, MSc. Thesis 2012.

This paper may be cited as:
Ani, U. P. D. and Mustapha, M. 2015. VoIP Security: Improving Quality of Service through the Analysis of Secured Transmission. *International Journal of Computer Science and Business Informatics, Vol. 15, No. 1, pp. 66-90.*