AN EXPERIMENTAL ANALYSIS ON ITERATIVE BLOCK CIPHERS AND THEIR EFFECTS ON VOIP UNDER DIFFERENT CODING SCHEMES

Gregory Epiphaniou, Carsten Maple, Paul Sant
Institute for Research in Applicable Computing, University of Bedfordshire, Park Street, Luton, U.K.

Matthew Reeve
Modern Networks, Hitchin, U.K.

Keywords: VoIP, DES, 3DES, AES, HMAC-SHA-1, NS-2.

Abstract: IP telephony (IPTel) refers to the technology to transport real-time media over an IP network. This technology is considered as the key to providing advanced communication for end users at an affordable price whilst also assuring significant cost savings for the Internet Telephony Service Providers (ITSP). As with adoption of any new technology, utilizing VoIP is not without its risks. Digitizing voice that can be routed through hostile environments such as packet switched networks makes VoIP vulnerable to all of the risks of an IP network including viruses, Denial of Service (DOS) attacks and conversation eavesdropping. This paper focuses on the effects of iterative block ciphers on VoIP traffic in terms of average end-to-end delay and packet loss rates. We have tested the majority of voice codecs as well as all the variable payload sizes they can support. Finally, the simulations have been carried out by using the NS-2 network simulator.

1 INTRODUCTION

Applying security protocols to voice traffic may introduce processing overheads to the actual headers added to the VoIP frame. Security protocols such as Encapsulation Security Payload (ESP) and Authentication Header (AH) are found to increase (disproportionally) the ratio between the actual voice payload and the header sizes carried across the network and dramatically reduce the effective bandwidth used (Barbieri et al., 2002). In addition, the total time required to add the appropriate cryptographic functions to the payloads, introduces further delays during transmission. Recent studies have directed towards the proper selection of ciphers (block or stream) for VoIP based on their characteristics (Elbayoumy and Shepherd, 2007).

Authors suggested that in a homogeneous architecture where packet-switched networks are inter-connected, the choice of block cipher option is the most appropriate due to negligible corruption but sufficient loss rates in those architectures. The tradeoff between the packet size used for encryption and the actual throughput of the crypto-enginee has also investigated (Elbayoumy and Shepherd, 2005).

The case of encrypted VoIP streams under variable payload sizes currently supported by G.711 (64 kbps), G.726 (32 kbps),G.726 (24 kbps) G.723.1 (6.3 kbps), G.723.1 (5.3 kbps) and G.729 (8 kbps) have been investigated by using the Pareto ON/OFF traffic model. In voice traffic the packets are generated in active ON state whereas in silent OFF state no packets are generated (Li, 2008), (Bohnert and Monteiro, 2005). The interval periods are taken by the actual codecs' specifications which can effectively produce the required number of packets per second, without changing the codec rate.

The IPSec scenario in transport mode has been used, assuming that the endpoints (IP phones/softphones) can support cryptographic operations. This framework of open standards is widely known for its network layer authentication, data integrity, confidentiality and replay protection (Benvenuto and Keromytis, 2003). IPSec uses the Internet Key Exchange (IKE) process for key exchange consisting of two phases, in which a mutual authentication between the communication parties

Epiphaniou G., Maple C., Sant P. and Reeve M. (2010).
AN EXPERIMENTAL ANALYSIS ON ITERATIVE BLOCK CIPHERS AND THEIR EFFECTS ON VOIP UNDER DIFFERENT CODING SCHEMES.
In *Proceedings of the International Conference on Signal Processing and Multimedia Applications*, pages 17-25
DOI: 10.5220/0002930000170025

takes place based on a secret key and establish a new session key to protect the rest of the transmission. The second phase relies on the session key created at phase one to establish a session two key for protecting the data in the security association (Radia and Kaufman, 2000).

This paper focuses on the effect of iterative block ciphers to VoIP traffic under different coding schemes structured as follows: In section 2 we calculate the overhead in terms of bandwidth and packet size when encryption is applied for the IPSec scenario, by using a mathematical framework proposed (Xenakis et al., 2006). In section 3 the simulation topology and initial parameters related to average end-to-end delay and packet loss rates for each codec, are also presented. In section 4 the main results and discusions are presented and finally in section 5 we withdraw main conclusions and areas of future work.

2 QUANTIFY THE ENCRYPTION OVERHEAD

In terms of quantifying the encryption penalty upon network transmissions, an extended mathematical framework has been proposed by Xenakis et al. (2006). The authors have quantified the impact that different symmetric ciphers such as DES, 3DES, AES and hashing algorithms HMAC-SHA1, HMAC-MD5 may impose in terms of communication quality and consumption (effective bandwidth) used.

The total time for a crypto-engine to encrypt a plain user packet of specific payload size S_d with a processing speed C_p by using DES, 3DES is:

$$t_{DES}(x,C_p) = \left\lceil \frac{8 * S_d}{64} \right\rceil * \frac{T_{DES/3DES}}{C_p} \quad (1)$$

Where $T_{DES} = 3697$ and $T_{3DES} = 8091$ are the number of operations required to encrypt a block of user data with these block ciphers. For *AES* the total time required to encrypt/decrypt one block of data is given below (Xenakis et al., 2006):

$$t_{AES}(x,C_p) = \left\lceil \frac{8 * S_d}{128} \right\rceil * \frac{T_{AES-enc}}{C_p} \quad (2)$$

$$t_{AES}(x,C_p) = \left\lceil \frac{8 * S_d}{64} \right\rceil * \frac{T_{AES-dec}}{C_p} \quad (3)$$

The processing cycles for encrypt/decrypt a user data block for a specific key length with *AES* (Elkeelany et al., 2002):

$$T_{AES-enc}(128) = 6168$$
$$T_{AES-enc}(192) = 7512$$
$$T_{AES-enc}(256) = 8856$$
$$T_{AES-dec}(128) = 10992$$
$$T_{AES-dec}(192) = 13408$$
$$T_{AES-dec}(256) = 15824$$

The ciphering overhead created by padding the original packet in order to create multiple blocks supported by the ciphers. The additional field added has also been addressed by the authors as follows:

$$SP_{ESP-CNF-ATH}(S_d) = \left\lceil \frac{S_d + 22}{Bl} \right\rceil * Bl + 40 \quad (4)$$

Where S_d is the payload size and Bl is the block size of each cipher used (8 bytes for DES/3DES and 16 for AES). Table 1, illustrates the codecs used in the simulations as well as the packet overheads for plain and encrypted traffic for both modes in IPSec operation. The total number of packets produced per second for each codec is given by the following:

$$PPS(pkts/sec) = \frac{\text{Codec bit rate (bits)}}{\text{Payload Size (bits)}} \quad (5)$$

The total bandwidth required per VoIP call has been calculated as follows:

$$Band(kbps) = \text{Voice pkt size (bits)} * \text{PPS} \quad (6)$$

During our simulation there is no voice activity detection (VAD) used since this metric can effectively reduce the utilisation up to 65% of the full rate (Press, 2009). A first observation throughout our calculations is that when G.726 (32 kbps) is used with payload size 20 bytes all ciphers examined seem to add exactly the same overhead in terms of packet size. The total IP packet for this payload size is 88 and 104 bytes and the ethernet bandwidth recorded is 265.5 kbps. Similar results were extracted in the case of G.726 (24 kbps) with payload size 40 bytes and total IP packet size of 104 and 136 bytes for AES (both IPSec modes) and 104 and 128 for DES/3DES. The required bandwidth in that case was measured at 121kbps. No discrepancies in terms of packet overhead and ethernet bandwidth required were noticed either in the case of G.729 (8 kbps) for payload sizes 10, 20, 40 bytes respectively.

3 SIMULATION TOPOLOGY

An access network topology was designed by using NS-2 (NS2, 2001) consisting of 300 user agents (UA) where encryption takes place on an end-to-end fashion (Transport mode)(figure 1). A total number of 600 UA were interconnected by using switches

Table 1: VoIP Ethernet packet overheads for encrypted traffic with AES/DES/3DES and IPSec in two modes of operation.

Codec	P.Size[bytes]	AES trans.	AES tunn.	DES/3DES trans.	DES/3DES tunn.
G.711 (64 kbps)	120	152	168	144	168
	200	232	248	224	248
	280	312	328	304	328
G.726 (32 kbps)	60	88	104	88	104
	120	136	152	128	144
	160	184	216	184	208
G.726 (24 kbps)	120	152	168	144	168
	80	104	136	104	128
	100	136	152	128	144
G.729 (8 kbps)	50	72	104	72	69
	60	88	104	88	104
	70	104	120	96	112
	80	104	136	104	128
	90	120	136	112	136
	100	136	152	128	144
G.723.1 (6.3 kbps)	64	88	120	88	112
	88	120	136	112	136
G.723.1 (5.3 kbps)	60	88	104	88	104
	80	104	136	104	128

and routers and two stateful inspection firewalls at the core entrance points. A script written in python has been created that automates the simulation process. The simulation starts with an initial configuration stored in a file called parameters.dat that the python script reads prior to topology generation. Table 2 illustrates the initial parameters regarding propagation delay, link capacity, payload size and burst/idle times. The idle and burst time is based on the Pareto ON/OFF model and depends totally on each codec individually.

Table 2: Initial simulation parameters.

P.D.[ms]	L.C.[Mb]	P.S.[bytes]	b./i.[ms]
10	5	160	20-10

The parameters.dat file includes the basic configuration details for G.711 (64 kbps). This file is used as an input to the PythonTopology.py script that generates 300 tcl scripts corresponding to each VoIP call to be simulated. The input file is automatically accessed by the python script if the simulation parameters change. We have particularly focused on DES/3DES and AES with HMAC-SHA1. Once tcl topologies have been written, the NS-2 simulator is called and run against each tcl script to extract simulation results. Figure 2 illustrates the simulation process.

During the simulations the total buffer queue size was set to 50 packets and the default first-in-first-out (FIFO) queue management was implemented (Braden et al., 1998). The network was overloaded by VoIP flows gradually increasing from 1 to 300 calls, up to the congestion level where packets were simply

Figure 1: Simulation topology.

dropped. In addition, packet loss concealment (PLC) is not employed, therefore, there is no compensation for dropped packets. We have described packet loss rate as a multiplicative function of each value of the packet loss rate at a specific link during a transmission.

$$Plr_{ij} = \frac{pkts_{lost}}{pkts_{received}} = \frac{pkts_{sent_i} - pkts_{received_j}}{pkts_{received_j}} \quad (7)$$

We have derived the overall packet loss rate of a route with several links for unicast transmissions as follows:

$$PLR_{ij} = 1 - \sum_{f \in F} \Pi_{ij} (1 - Plr_{ij}) \quad (8)$$

Where f denotes a specific traffic flaw within the network flaws F.

$$PLR_{ij} \leq 0.05 * Pkts_{sent_i} \quad (9)$$

Equation (9) is dirived by the National Institute of Standards and Technology (NIST) recommendations

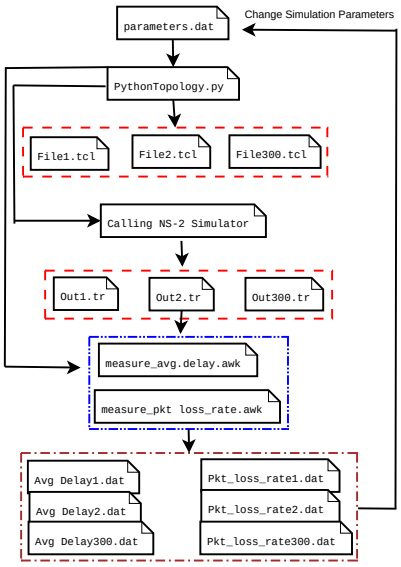


Figure 2: Simulation flow chat.

which suggest the total packet loss for a voice call must not exceed 5% of the total packets transmitted (Kuhn et al., 2005). Although simulations were carried out based on the maximum number of 300 simultaneous calls, there is a point at the delay traces were packets are simply dropped above the acceptable limits. This investigation focuses only on those call volumes where trasmissions are feasible and within the limits posted by the International Telecommunication Union (ITU). The limits posted by ITU-T regarding one-way delay limits are 0-150ms for most network applications and 0-200ms for encrypted transmissions (It, 1993).

4 RESULTS AND DISCUSSION

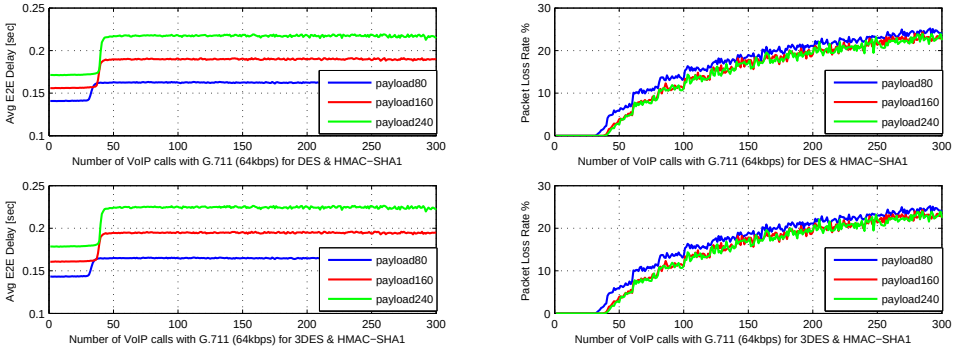
In this section we present the experimental results of our simulations based on the ciphers and codecs introduced in section 2. For the sake of brevity only the most important findings are presented. In the case of G.711 (64 kbps) with plain traffic, a significant trade-off between the actual payload size and e2e delay, as well as e2e delay and packet loss rates has been recorded. Only one third of the total VoIP calls fed into the network are feasible since packet loss dramatically increases after 100 simultaneous calls.

Although e2e delay seems to be constant and below the limits for an unacceptable call, the packet loss rates when G.711 (64 kbps) is used, are catastrophic for the calls above 100 no matter payload size used. In the case of G.723.1 (5.3 kbps) the majority of calls are delivered successfuly with minor effects on e2e delay and packet loss rates. This can be explained mainly due to the low codec rate and the actual link capacity. The buffer queue size at 50 pps is also another factor positively contributes to low packet loss rates. In the case of G.723.1 (6.3 kbps) when the payload size is 24 and 48 bytes the overall average delay and packet loss rates seem to be slightly higher then G.723.1 (5.3 kbps) and its corresponding payload sizes. Even in that scenario, however, effects on delay and packet loss rates seem to be negible in comparison to G.711 where dropping symptoms are rapid after 100 VoIP calls.

The smallest payload size used in both cases seems to create unacceptable dropping rates at the very early stages of 140 and 60 simultaneous VoIP calls respectively in the case of G.726. Throughout the simulations with the selected codecs when payload size of 80 and 120 bytes is used, this modification seems to allow more calls into the network prior to drastic dropping rates. An interesting observation is that with G.726 (32 kbps) and payload size of 20 bytes the overall packet loss rates are higher than any other payload used even with the same codec under different rates. An overall increase of up to 20% dropping rates with 300 VoIP calls has been observed. In the case of plain voice traffic, G.726 (32 kbps) seems to perform better with a given payload size of 120 bytes. For the case of G.729 (8 kbps) this codec seems to inserts the maximum number of VoIP calls into the network mainly due to its low bit rate and packets produced per second. A successful delivery of all VoIP calls with payload sizes of 40, 50 and 60 bytes respectively has recorded. The average e2e delay for the first three payload sizes gradually increases following a step-wise function behaviour, due to the aggregation of the incoming traffic those payloads create in the buffer queue. The default payload size of 10 bytes seems to outperform regarding packets loss rates since its dropping symptoms exceed 5% of the total packets submitted after 200 calls.

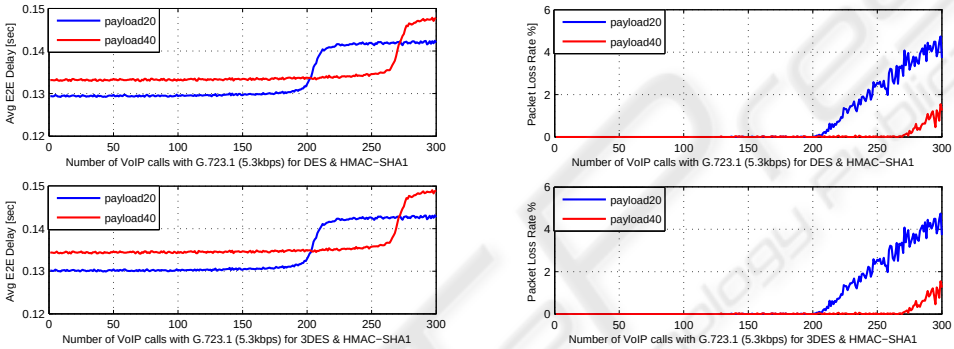
4.1 Encrypted VoIP Traffic with DES/3DES and HMAC-SHA1

Figure 3 illustrates average e2e delays and packet loss rates in the case of encrypted VoIP traffic for G.711 (64 kbps). A direct effect of encryption regarding G.711 operation is the actual increase on average e2e delay suffered from all calls fed into the network. This increase has been measured up to 90 ms higher then plain traffic with the same codec. Although DES and 3DES with HMAC-SHA1 are in place, no significant discripancies were found regarding the two ciphers' effects upon VoIP. The analysis has shown very



(a) (b)

Figure 3: Average e2e delay and packet loss rates for G.711 (64 kbps) with DES/3DES and HMAC-SHA1.

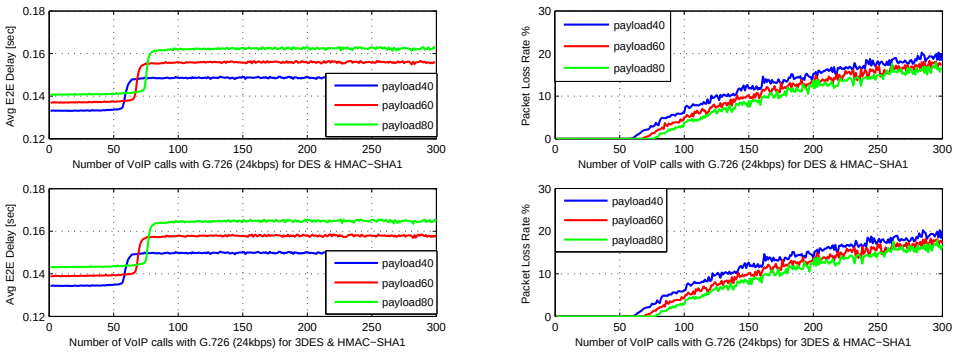


(a) (b)

Figure 4: Average e2e delay and packet loss rates for G.723.1 (5.3 kbps) with DES/3DES and HMAC-SHA1.

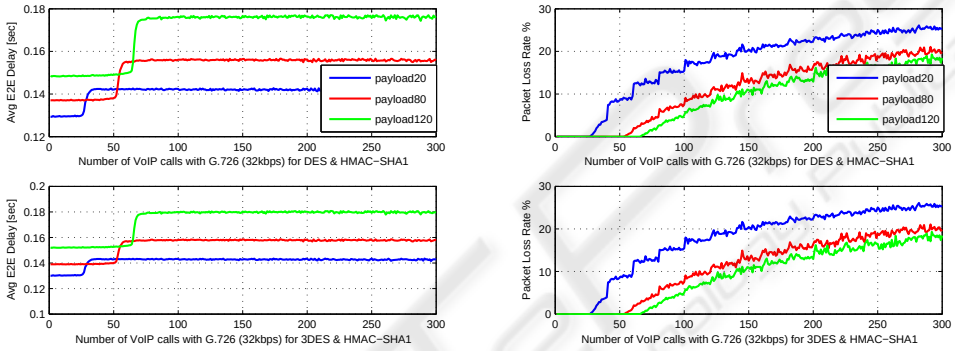
similar behaviour in terms of network impairments, although 3DES is considered to be a computationally more expensive cipher than DES. Both ciphers used have managed to allow less feasible VoIP calls into the network. In figure 3, the overall dropping symptoms started at under 50 simultaneous VoIP calls, allowing up to 50 calls into the network within the acceptable packet loss limits. Figure 4 illustrates the findings for G.723.1 (5.3 kbps). An increase has been noticed regarding e2e delay for up to 70ms in comparison to plain traffic, mainly due to cryptographic operations. As the number of VoIP calls increases, a constant e2e delay recorded up to the level of 200 calls for 20 bytes payload size and 260 calls for 40 bytes. In terms of packet loss rates, for both payload sizes, no value exceeded 5% for either cipher examined. The good behaviour of the VoIP traffic, even in the case where encryption is applied can be partially explained by the low bit rate of the codec, as well as the link capacity.

Figure 5 illustrates the average e2e delay and packet loss rates as measured for G.726 (24 kbps). An overall e2e delay of 43ms has been added as a result of the encryption process. In terms of payload sizes, the actual operation of the codec with 80 bytes payload may contribute to higher rates of e2e delay, however, it seems to feed more calls into the network (Figure 5). The dropping symptoms based on this network topology with the existing characteristics are considered to be dramatic after a certain number of concurrent VoIP calls (60 calls) for all payloads supported. In the case of both DES/3DES, the overall packet loss rate takes place earlier as the VoIP call volume increases in comparison to plain traffic, which is an expected network behaviour due to the additional overhead introduced. Although the actual payload size does not by itself constitute an improvement in terms of packet loss rates, however, with encryption in place and G.726 (24 kbps) as the codec selected, the payload of 80 bytes seems to perform better. This can be partially explained by the relationship between the actual packet size and the cryptographic engine's throughput. A slightly different behaviour has been recorded with G.726 (32 kbps) and its smallest payload size. Although the codec's operation with the specific payload size of 20 bytes presents the low-



(a) (b)

Figure 5: Average e2e delay and packet loss rates for G.726 (24 kbps) with DES/3DES and HMAC-SHA1.



(a) (b)

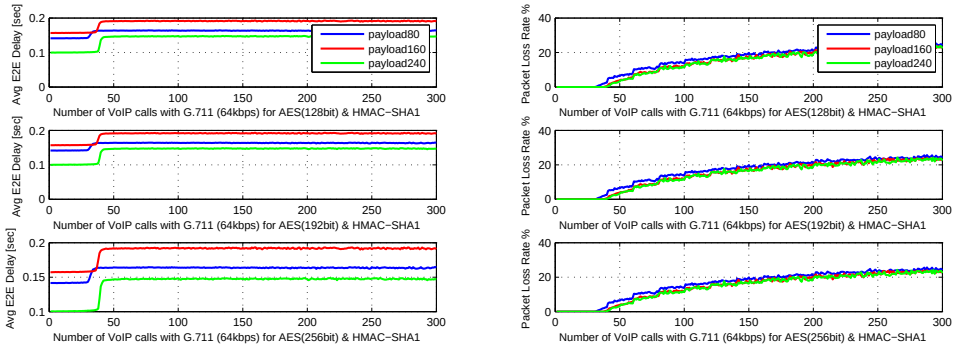
Figure 6: Average e2e delay and packet loss rates for G.726 (32 kbps) with DES/3DES and HMAC-SHA1.

est average e2e delay, it seems to have dispropotionally high dropping symptoms in comparison to the other payloads supported. In the case of encryption the overall precentage regarding packet loss rates has been also increased by up to 10%. The average e2e delay remains constant, mainly due to rapid dropping symptoms. Similarly, the aggregation of the incoming traffic, as well as the total buffer queue size, has contributed negatively to the overall packet loss rates. The area of feasible VoIP calls is illustrated in Figure 6. An interesting observation is that the encryption overhead reduces dramatically the total number of simultaneous VoIP calls fed into the network by 50% for all payload sizes used in comparison to unencrypted traffic for the same scenario.

4.2 Encrypted VoIP Traffic with AES and HMAC-SHA1

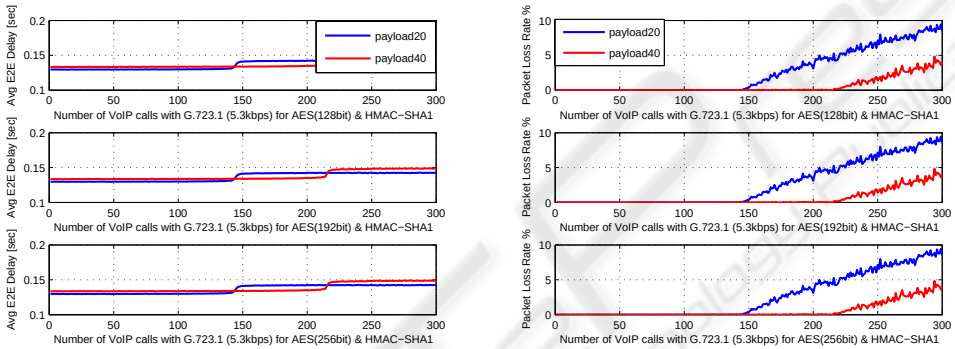
A similar investigation has been carried out with VoIP confidentiality and authentication to be assured with AES and HMAC-SHA1. Figure 6 shows the average e2e delay and packet loss rates for G.711 (64 kbps) for the case of AES and HMAC-SHA1. For all the payload sizes currently supported by the codec, the average e2e delay does not exceed 200ms for the feasible area of calls (1-50). The higher e2e delay values have been recorded with payload size of 160 bytes from a starting point of 170ms up to nearly 200ms for an increased number of calls. The default payload size used by the codec (160 bytes) preserves those values no matter the key length used. It is clear throughout the simulation that the payload size of 240 bytes seems to feed more calls into the network with an acceptable e2e delay and packet loss rate for the feasible area investigated. The average e2e delay is up to 150ms whereas payload size 80 bytes seems to record slightly higher values.

Under the burst traffic conditions, as well as the network parameters as configured in the tcl simulation scripts, G.723.1 (5.3 kbps) seems to behave better in terms of average e2e and packet loss rates when encryption is applied (Fig. 8). In the case that AES & HMAC-SHA1 is used, similar delay traces have been recorded as in the DES/3DES scenario, however, the delay increase has been reported 50 calls



(a) (b)

Figure 7: Average e2e delay and packet loss rates for G.711 (64 kbps) with AES and HMAC-SHA1.



(a) (b)

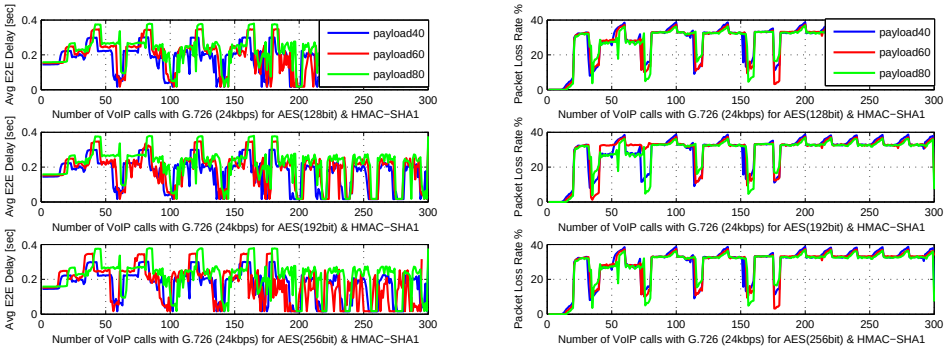
Figure 8: Average e2e delay and packet loss rates for G.723.1 (5.3 kbps) with AES and HMAC-SHA1.

earlier. The same behaviour seems to apply for the dropping symptoms as well. Simply put, in the case of DES/3DES and payload size of 20 bytes the rapid dropping symptoms start at 200 calls whereas in the AES case this behaviour starts 50 calls earlier. In addition, higher dropping rates have been measured for AES than DES/3DES for the same payload size. However, even if AES is used, with this decrease of the feasible area of VoIP calls, the codec seems to behave better than any other codec under investigation for the same scenarios.

Figure 9 clearly shows the devastating effects of AES and HMAC-SHA1 when G.726 (24 kbps) is used under the given simulation scenario. The available area of feasible calls has been reduced to 1-30 simultaneous calls, reduced by almost 20 VoIP calls in comparison to DES/3DES and HMAC-SHA1. An obvious observation is that every call above the feasible area is practically impossible, since for a specific time frame and calls the average e2e delay exceeded 300ms and the corresponding loss rates 35% of the total number of packets transmitted.

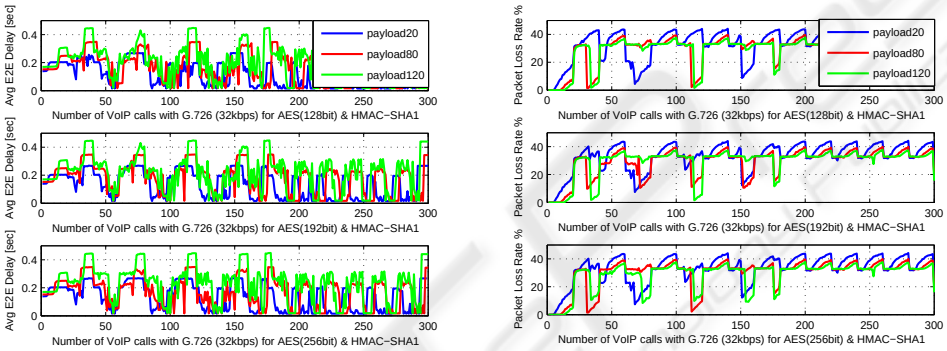
With AES used under pre-defined and strict parameters reported an overall 10% higher dropping rates then the higher dropping rate value recorded with DES/3DES for this codec. This signifies the importance in terms of impact of such modification regarding the encryption level even when the payload size and rates remain constant. The penalty factors contributing to such behaviour except the actual cryptographic overhead, are the relatively small payload size, the rate of the codec as well as the aggregation of the incoming traffic in the buffer queue.

A closer investigation in the area of feasible VoIP calls with the selected codec, has shown that when a payload size of 80 bytes is used, the maximum number of calls is fed into the network with relatively acceptable network impairments suffered during the transmission. However, the use of AES as it is recorded in that case does not constitute a significant improvement regarding VoIP call volume delivery. Finally, even in that particular case, the default payload size supported by the codec does not seems to be the most appropriate selection when encryption is active. Similar results were extracted in the case of G.726 (32 kbps) and its corresponding payload sizes



(a) (b)

Figure 9: Average e2e delay and packet loss rates for G.726 (24 kbps) with AES and HMAC-SHA1.



(a) (b)

Figure 10: Average e2e delay and packet loss rates for G.726 (32 kbps) with AES and HMAC-SHA1.

of 20, 80 and 120 bytes. Figure 10 illustrate that the feasible area of VoIP calls has been reduced to 1-15 and the overall packet loss rates have been increased above 40% for a specific time frame and payload size. Although any call above 15 is practically unfeasible, it is clear from the Figure 10 the tradeoff between the actual packet size, delay and packet loss rates. The spiky waveform of the average e2e delay and packet loss rates is mainly presented due to the codec rate and its resulting packets per second, as well as the queuing mechanism (FIFO) used. A comparison between DES/3DES and AES shows a vast increase in the actual delay, which has been almost doubled as recorded during the simulations.

5 CONCLUSIONS

During our simulations an in depth investigation has been carried out regarding the feasible area of VoIP calls for each codec examined. We have found that in the case of G.711 (64 kbps) the encryption can add up to 90ms average e2e delay for the same streams in comparison to plain traffic with the same codec. The area of feasible transmissions has been measured below 45 simultaneous VoIP calls in the case of encryption with DES/3DES and HMAC-SHA1. Also, the payload size of 240 bytes recorded the highest feasible call volume in comparison to other payload sizes supported by the codec when encryption is applied no matter the cipher used for the same codec.

In the case of G.726 (24 kbps) and G.726 (32 kbps) the payloads of 80 bytes and 120 bytes respectively seem to perform better in terms of e2e delay within the area of feasible VoIP calls (1-65), for both codecs. In contrast, the smallest payload sizes supported by both codecs have reported higher dropping symptoms at earlier stages during our simulations. For G.723.1 (5.3 kbps) and G.723.1 (6.3 kbps), the payload sizes of 40 bytes and 48 bytes have recorded the lowest dropping symptoms, although all calls have managed to feed into the network successfuly. Only in the case of AES with HMAC-SHA1 has the feasible area of VoIP calls been reduces to 1-200 calls for G.723.1 (5.3 kbps) and payload 20 bytes and 1-

260 for payload of 40 bytes. For G.723.1 (6.3 kbps) and AES with HMAC-SHA1 the area of feasible VoIP calls has been reduced to 0-160 for payload size of 24 bytes and 1-240 for payload size of 48 bytes. The dropping rates were almost double than those recorded with DES/3DES and HMAC-SHA1. In general, the crypto-engine seems to perform better with large payload sizes and, in the majority of the cases examined, the default payload size shipped with each codec, is not the appropriate selection when encryption is concerned.

ACKNOWLEDGEMENTS

Special thanks must go to Nikolaos Pavlidis, from Information Services Directorate, University of Bedfordshire, Dr. Peter Norrington from the Centre for Excellence in Teaching & Learning (CETL) at the University of Bedfordshire as well as Dr. Helen Jacobs (Modern-Networks) for all the valuable support and fruitful ideas during the implementation of this work. Finally, acknowledgement must be credited to Engineering and Physical Sciences Research Council (EPSRC) for the financial support of this project.

REFERENCES

Barbieri, R., Bruschi, D., and Rosti, E. (2002). Voice over ipsec: Analysis and solutions. *Computer Security Applications Conference, Annual*, 0:261.

Benvenuto, M. C. and Keromytis, A. D. (2003). Easyvpn: Ipsec remote access made easy. In *LISA '03: Proceedings of the 17th USENIX conference on System administration*, pages 87–94, Berkeley, CA, USA. USENIX Association.

Bohnert, T. and Monteiro, E. (2005). A comment on simulating lrd traffic with pareto on/off sources. In *CoNEXT '05: Proceedings of the 2005 ACM conference on Emerging network experiment and technology*, pages 228–229, New York, NY, USA. ACM.

Braden, B., Clark, D., Crowcroft, J., Davie, B., Deering, S., Estrin, D., Floyd, S., Jacobson, V., Minshall, G., Partridge, C., Peterson, L., Ramakrishnan, K., Shenker, S., Wroclawski, J., and Zhang, L. (1998). Recommendations on Queue Management and Congestion Avoidance in the Internet. RFC 2309 (Informational).

Elbayoumy, A. D. and Shepherd, S. J. (2005). Using the tiny encryption algorithm for securing voice over ip. In *Proceedings of 7th Annual International Symposium on Advanced Radio Technologies*. INSTICC Press.

Elbayoumy, A. D. and Shepherd, S. J. (2007). Stream or block cipher for securing voip? *I. J. Network Security*, 5(2):128–133.

Elkeelany, O., Matalgah, M., Sheikh, K., Thaker, M., Chaudhry, G., Medhi, D., and Qaddour, J. (2002). Performance analysis of ipsec protocol: encryption and authentication. *ICC*, 2(2):3225–3241.

It, U. (1993). ITU-T recommendation G.114. Technical report, International Telecommunication Union.

Kuhn, D. R., Walsh, T., Fries, S., of Standards, N. I., and (U.S.), T. (2005). *Security considerations for voice over IP systems [electronic resource] : recommendations of the National Institute of Standards and Technology / D. Richard Kuhn, Thomas J. Walsh, Steffen Fries*. U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology, Gaithersburg, MD :.

Li, I.-H. (2008). Effects of on-off variability in two-state pareto traffic models on multimedia application transmission performance. *Networked Computing and Advanced Information Management, International Conference on*, 2:426–431.

NS2 (2001). The Network Simulator ns-2 (v2.1b8a). http://www.isi.edu/nsnam/ns/.

Press, C. (2006 (accessed September 23, 2009)). *Voice over IP Per Call Bandwidth Consumption*. http://www.cisco.com/warp/public/788/pkt-voice-general/bwidth_consume.pdf.

Radia, P. and Kaufman, C. (2000). Key exchange in ipsec: Analysis of ike. *IEEE Internet Computing*, 4:50–56.

Xenakis, C., Laoutaris, N., Merakos, L., and Stavrakakis, I. (2006). A generic characterization of the overheads imposed by ipsec and associated cryptographic algorithms. *Comput. Netw.*, 50(17):3225–3241.