SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks (2016)
Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1719

RESEARCH ARTICLE

Security of VoIP traffic over low or limited bandwidth networks

Sahel Alouneh[1]*, Sa'ed Abed[2] and George Ghinea[3]

[1] German Jordanian University, Amman, Jordan
[2] Kuwait University, Kuwait City, Kuwait
[3] Brunel University, London, UK

ABSTRACT

The early days of voice over IP (VoIP) adoption were characterized by a lack of concern and awareness about security issues related to its use. Indeed, service providers and users were mostly preoccupied with issues related to its quality, functionality, and cost. Now that VoIP is a mainstream communication technology, security has become a major issue. This paper investigates the major security threats for VoIP communications and proposes a multipath approach solution, especially targeted for low bandwidth networks. Results show that security has an effect on VoIP quality especially for a large distance between communicating nodes and packet size. Results also show that our proposed multipath solution reduces significantly packet losses and performs better than single routing techniques in networks with low bandwidth capacities.

KEYWORDS

VoIP; security; threats; reliability; cost; quality

***Correspondence**

Alouneh, Sahel, German Jordanian University, Amman, Jordan.
E-mail: sahel.alouneh@gju.edu.jo

1. INTRODUCTION

Voice over IP (VoIP) is rapidly replacing traditional telephony networks such as the public switched telephone network as the main method of communication between remote users. One of the main challenges of VoIP is the unreliable quality of such a communication method. In many cases, congestion on IP and internet networks prevents service providers and users from delivering an excellent quality for VoIP communications. It is worth to note that there exist considerable research proposals and solutions tackling the quality of service issues in VoIP networks [1–10,12–17]. However, there is a paucity of research on VoIP security threats. This is of special concern especially bearing in mind when we think that VoIP is becoming mainstream.

Traditionally, the most important factors that affect VoIP quality are its latency, jittering, and available bandwidth. It is worth noting that there is a rising concern about the quality and efficiency of VoIP communication when adding and implementing functionalities targeting its security. The level of security services applied to a VoIP commination plays a role in determining its quality. Therefore, the following security services are the main factors that should be considered in any VoIP communication [2,4,7,8,12,13]:

- Confidentiality: It is the protection of communicated VoIP packets from attacks. In other words, the content of information cannot be revealed if being sniffed by an attacker in the middle of transmission. For example, a video conversation between two state presidents is considered as needing to be confidential to the utmost degree. Therefore, the content of this conversation should not be revealed.
- Integrity: It assures that the VoIP packets have been received as being sent with no modification.
- Non-repudiation: It prevents communicating parties either sender or receiver from denying a transmitted VoIP conservation. Thus, after a VoIP conversation, the receiver can prove that the assumed sender has in fact led the VoIP conversation.

It is worth noting that security threats related to VoIP communications can be accomplished by different

techniques. A list of these security threats include identity theft, eavesdropping, denial of service, VoIP phishing, call interfering, and flooding. In addition, one of the main concerns of VoIP is the changeable quality of such a communication technique. In many cases, congestion on IP networks prevents service providers and users from delivering an excellent quality on voice over IP communications. Therefore, this paper investigates the effect of security on the reliability of VoIP communications. This paper also discusses research literature related to VoIP and security and concludes with a proposed solution based on multipath routing to provide security for low or limited bandwidth networks.

This paper is organized as follows. Section 2 discusses the related work on Voice Over IP (VoIP) networks. We present the analysis of security impact on VoIP quality in Section 3. The design model and implementation issues, and results of our multipath approach solution to provide VoIP security in low or limited bandwidth networks are then discussed in Section 4. Finally, we conclude the paper and present some future trends in Section 5.

2. RELATED WORK

The widespread usage of VoIP applications and their integration with personal computing in different fields has changed the model of how security of VoIP should be handled. Indeed, there have been a growing number of research initiatives, designs, and implementations that have explored the use of security in this regard. When considering security, the quality and performance of VoIP communications are the critical issues that need to be considered. For example, Reason and Messerschmitt [2] have introduced this issue more than a decade ago. Anwar *et al.* [3] started research that aims to document three design patterns for VoIP implementations related to specific VoIP security problems. In related work, Kunze *et al.* [4] have considered the non-repudiation security issue for the content of VoIP communication by applying digital signature; however, this approach does not secure the confidentiality of the VoIP content. Palmieri *et al.* [5] addressed the security of VoIP from an end-to-end perspective taking into the account the three security factors (confidentiality, authentication of users, and authentication of voice content). Nevertheless, reviews on this approach show a problem resulted from public key infrastructure (PKI) infrastructure requirement. Another approach that considers the heaviness of applying encryption techniques on VoIP communication was proposed in [6]. This approach put forward an adaptive lightweight encryption algorithm that takes into account CPU capabilities of participating parties. The performance of this approach with regard to delay, packet loss, and jittering has not been evaluated and tested, however.

It is worth noting that the analyses and proposals for VoIP secure quality are still under discussion and debate. A recent approach that considers the performance of VoIP has been published by Cioponea *et al.* [7]. The authors used a dedicated hardware (a firewall) to test the quality of VoIP; however, it can be noticed that this work focuses only the authentication of VoIP content. Hanifan and Bandung [8] have considered the security of VoIP communications, but the scope of their implementation is limited to enterprise networks only. This kind of solutions cannot be generalized as usually VoIP communications are performed through the internet, and therefore, the effects of security applications are more critical than those in local networks. One recent interesting approach for Son *et al.* [9] has tested the Advanced Encryption Standard (AES) encryption and PKI by using RSA Rivest Shamir and Adelman algorithm on VoIP communications quality, but they only consider the delay factor. Moreover, Wanga and Liu [10] also tested the AES and elliptic curve Diffie–Hellman for key exchange on VoIP quality. Their results included the delay and packet loss. Angrisani *et al.* [11] have also tested VoIP secure communications and checked the impact of security on quality factors such as delay and jittering. The authors in [12] have evaluated the overhead impact of IPSec on VoIP. Their implementation was limited to LAN networks and only via mobile test cases. The work in reference [13] investigates the three major factors (delay, jittering, and packet loss) that influence the quality of service (QoS) for VoIP. The results obtained show that VoIP over a virtual private networks gives better QoS over traditional firewall for VoIP communications; however, these results were obtained by using a test on OPNET. For P2P VoIP communications, Jiang *et al*. proposed a secure key agreement for P2P VoIP Session Initiation Protocol.

Research has also focused on possible attacks on VoIP communications and their impact [15–17,21,22]. Such attacks may include theft of service, masquerading, IP spoofing, call interception, non-repudiation attacks, call hijacking, denial of service, call setup and signaling attacks, and attacks on smartphones.

It is worth observing that the literature on VoIP security is not mature. On the other hand, to the best of our knowledge, the issue of VoIP security in low bandwidth networks has not been previously examined and forms the focus of this paper. In Table I, we provide a comparison of some literature work related to VoIP security. The factors presented in the comparison table concentrate on the five factors: security protection type, for example, is confidentiality considered or not, and the network type, for example, is it local, wide, internet, generalized MPLS (GMPLS), or low bandwidth networks. The remaining factors are jittering, delay, and packet loss.

3. ANALYSIS OF SECURITY IMPACT ON VOIP QUALITY

The main observation from the previous section is the potential negative impact of implementing security functionality on VoIP applications' quality, such as the delay,

Table I. Comparison summary of literature related to voice over IP security.

Approach	Security protection type	Network type	Delay	Jittering	Packet loss
Cioponea *et al.* [7]	Authentication	Enterprise/local networks	N/A	N/A	N/A
Hanifan *et al.* [8]	Confidentiality	Enterprise/local	N/A	N/A	N/A
Son *et al* [9]	Confidentiality	Internet	Yes	N/A	N/A
Wanga *et al.* [10]	Confidentiality	Enterprise	Yes	N/A	Yes
Angrisani *et al.* [11]	N/A	N/A	Yes	Yes	N/A
Kazemi *et al.* [12]	IPSec	Local LAN	N/A	N/A	N/A
Our proposed work	Confidentiality	LAN/WAN/internet/low bandwidth networks/GMPLS	Yes	Yes	Yes

GMPLS, generalized multiprotocol label switching.

packet loss, and jittering. Our objective in this section is to test by simulations and analyze the impact that adding security considerations has on the quality of VoIP calls. These simulations consider the delay, packet loss, and jittering as main performance evaluation parameters. Table II shows the simulation details and security parameters for two different scenarios. The first one is when sending the VoIP traffic in one single path, while the second is when sending the VoIP traffic in multipath. The simulations were conducted by using the NS2 simulation tool (NS-2.35) [20]. The first scenario in Table II applies the AES as an encryption technique to encode VoIP data. The key management protocol that is used to exchange the security keys is the PKI (RSA) based on 1024 bits key size. We have chosen different network topologies with variable distances between nodes ranging from 100 m to 4000 km in the context of wired networks (LAN, WAN, MAN). Indeed, the purpose of making the distance between node variable is to help measure the distance effect on VoIP quality. The employed protocol as a routing agent for single-path routing is the Open Shortest Path First (OSPF), while we used M-OSPF for multipath routing. We used the G.711 and G.729 compression techniques to send VoIP traffic between participating nodes. The simulation takes into consideration different scenarios for traffic rate and variable packet sizes.

Simulation results in Figures 1–3 show the effects of distance, packet sending frequency, packet size, network infrastructure type, and number of nodes along with security on the quality of VoIP traffic with concentration on delay, jittering, and packet loss as quality of service factors.

The second part of the simulations considers the packet size effect and security on VoIP communication quality. Figure 4 concludes these findings. The main observation found is that the packet size has a strong impact on VoIP delay performance, especially when a packet size exceeds the threshold of 120 bytes. In addition, the packet size has also an impact on the packet loss and jittering. Most of the results obtained so far show that the effect of applying security is acceptable as long as the packet delay does not exceed 150 ms [13], which is the case for all testing results except for the case of AES 256 bit encryption and for node distance exceeding 4000 km.

It is worth highlighting that the previous testing findings apply only to computer networks with sufficient bandwidth capabilities. However, these results cannot be valid or applicable in low or limited bandwidth networks [13,17]. Therefore, in the next section, we will discuss this case and propose a solution.

Table II. Simulation parameters.

Parameter	Type/value	Parameter	Type/value
Encryption technique	AES 128, 192, 256 bits	Network infrastructure type	Wired, LAN, WAN, MAN
PKI	RSA, 1024 bits	Number of nodes	2, 4, 6, 10, 20
Simulation area:	100 m, 1 km	Traffic	UDP
distance between nodes	10 km, 100 km 1000 km, 2000 km 4000 km		
Routing agents	OSPF, M-OSPF	Signaling protocols	SIP, SDP, RTP
VoIP Codec	G.711, G.729		
Sending frequency	30 Pkts/s 50 Pkts/s 100 Pkts/s	Traffic throughput	CBR
Packet size	100 bytes/200 bytes 300 bytes	Simulation time	400 s

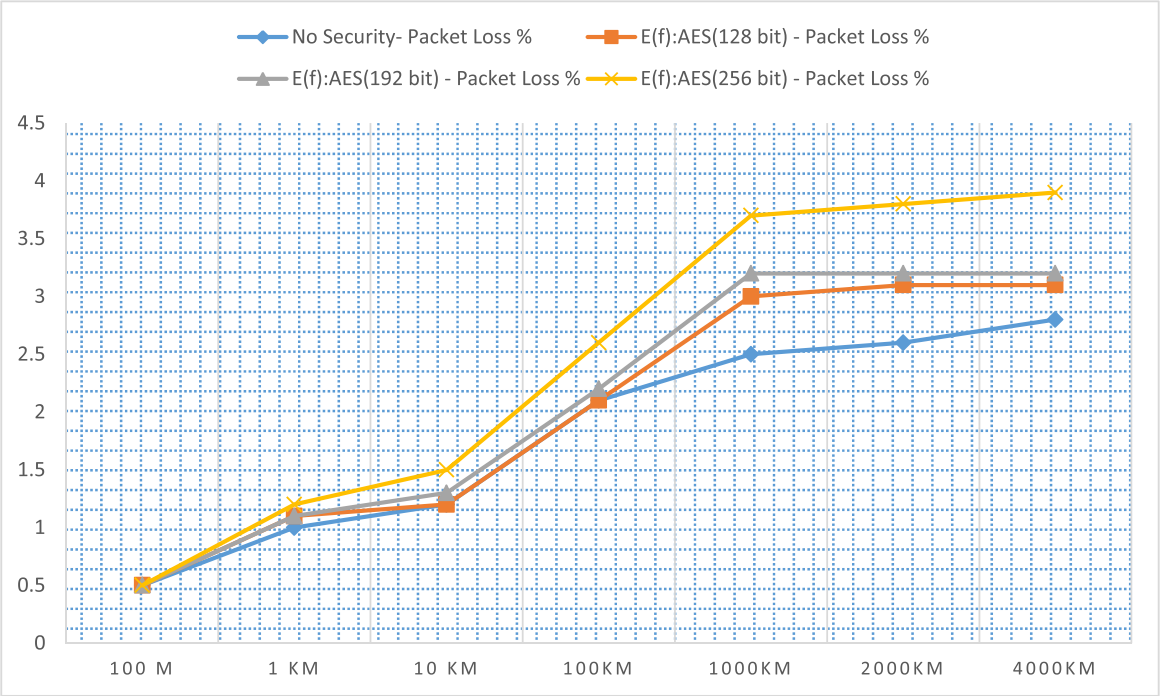

Figure 1. Effect of security on packet delay with regard to variable distance between nodes.

4. A MULTIPATH APPROACH SOLUTION TO PROVIDE SECURITY IN LOW OR LIMITED BANDWIDTH NETWORKS

In some network infrastructures, the bandwidth capacity of links can be variable, that is, some have high bandwidth capacities, and others have low or limited capacities. In addition, some links are more reliable than others, for example, wired links are more reliable than wireless links, and therefore, packets traversing through them are more vulnerable to packet loss and attacks. In such cases, the VoIP quality may be affected, especially if security applications are involved.

We propose a multipath approach based on network coding to protect the content of VoIP communication and increase its quality. The basic idea is to divide VoIP traffic arriving at network gateway (i.e., Ingress Gateway) and distribute the traffic into multipaths toward the outgoing gateway (i.e., Egress Gateway). Figure 5 shows the structure model for our proposed VoIP multipath approach. The multipath routes between Ingress and Egress gateways are assumed to be disjoint. To illustrate more, disjoint paths require having no common routers or links between any of the participating multipath routes. This assumption increases the effectiveness of security and reliability of transmitted data. However, it is also possible to have maximally or partially disjoint multipaths, which means that there are some shared router(s) and/or link(s) between any of the participating nodes in the multipath routes. It is expected to have a decrease in the performance of the networking system when having partially multipath routes. A direct explanation for this decrease can be expected due to the fact that a failure or an attack on a shared node will affect and involve more than one path and therefore could lower the performance of the system.

Our multipath approach relies on three algorithms to accomplish this task. Algorithm 4.1 in the succeeding texts illustrates how our approach distributes the VoIP traffic at the Ingress Gateway. Algorithm 4.1 is responsible for partitioning the VoIP traffic arriving at the Ingress Gateway into multipaths toward the Egress Gateway. The reconstruction of multipath VoIP traffics arriving at the Egress Gateway is illustrated in algorithm 4.2. Both algorithms 4.1 and 4.2 rely on the GMPLS to support the multipath route between Ingress and Egress gateways. Algorithm 4.3 illustrates the MPLS role in distributing and reconstruction of multipath traffics. The term GMPLS is used to refer for a generalized label formats implemented in networking switching technologies such as IP network switching, time network switching, wavelength, or space network switching. In this paper, we focus on the IP networking, and therefore, we use the MPLS term because it is the commonly used term in IP networks.

Algorithm 4.1 *[Partitioning the VoIP traffic at the Ingress Gateway]*
Input: VoIP traffic *S*
Output: *n* sub-VoIP traffic depending on the number of multipaths available toward the Egress Gateway.
Step 1: *Initialization*
·Divide the VoIP IP packet traffic into *sub-VoIP IP packets*.
·Set the fragmentation bit and enforce fragmentation to divide the original VoIP packet into *n* fragments. Indeed, the fragmentation is not enabled for small size packets; therefore, we can

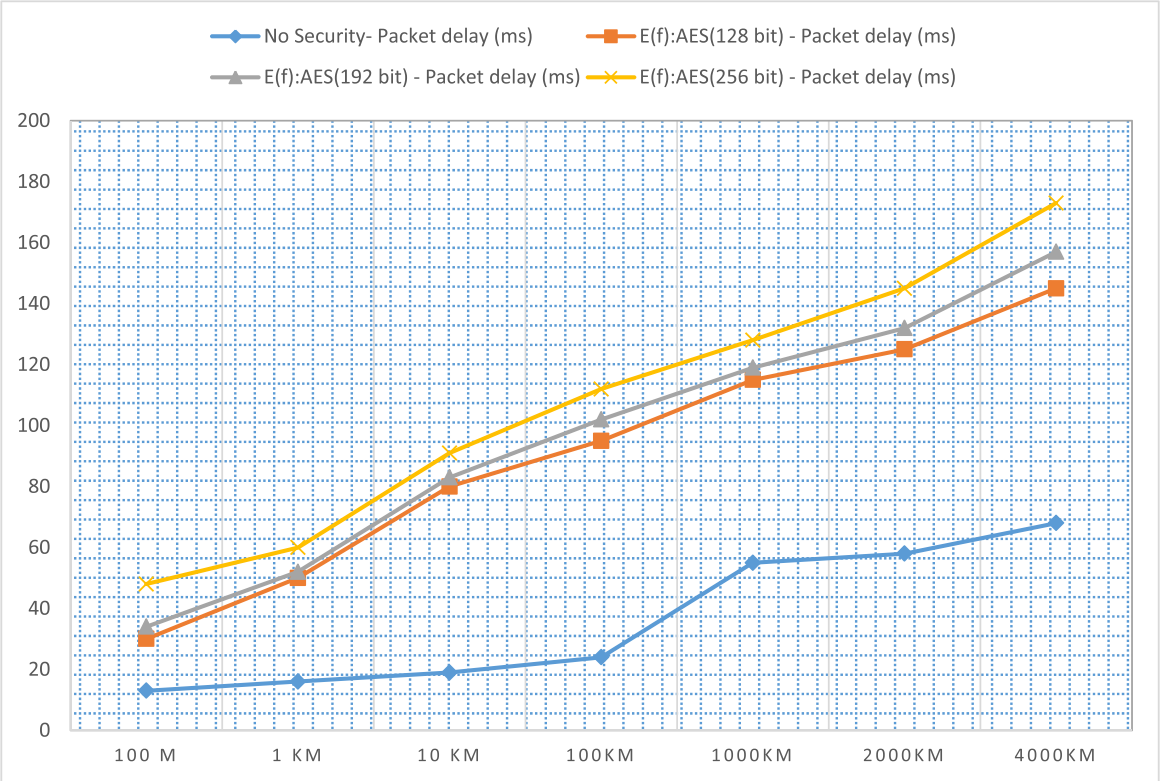

Figure 2. Effect of security on packet loss with regard to variable distance between nodes.

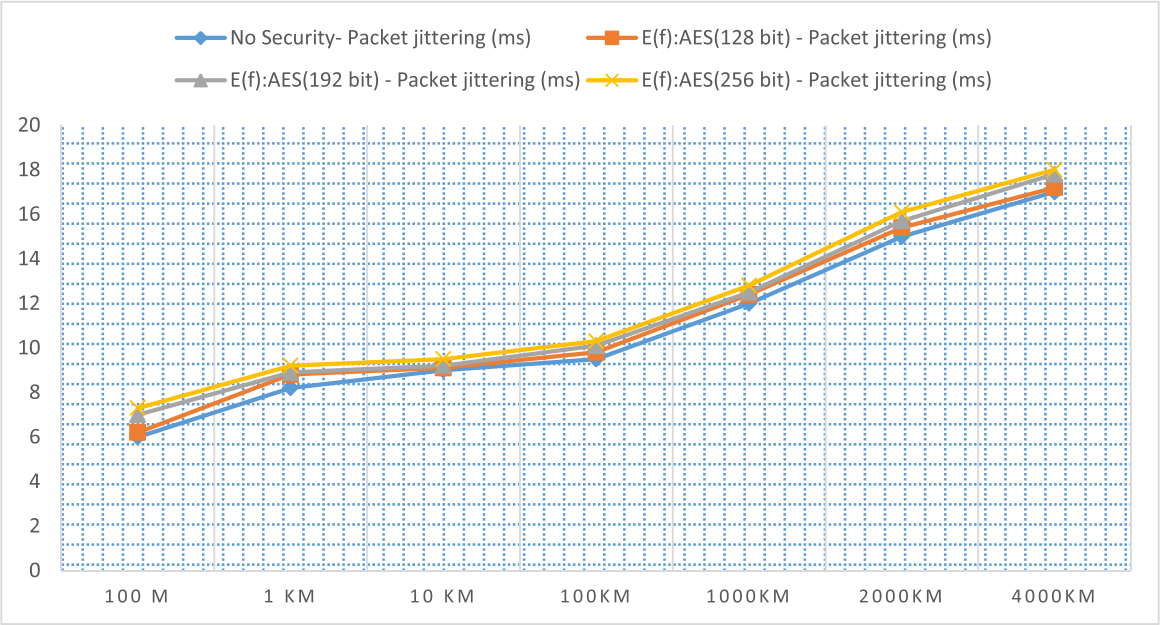

Figure 3. Effect of security on packet jittering with regard to variable distance between nodes.

use the fragmentation field's information such as the fragmentation ID to help in reconstructing these multipaths' VoIP packets at the Egress Gateway.

Step 2: *Processing VoIP traffic*

·*Break* the VoIP packet into blocks of fixed lengths B_1, B_2, …, B_i, where $0 \leq i \leq U$, and U is the total number of blocks in a VoIP packet.

·Block size should be divisible over $n-1$ with no remainder, that is, $(Bi/k) \neq 0$.

·*Padding*, in the last block in VoIP IP packet, is required if the

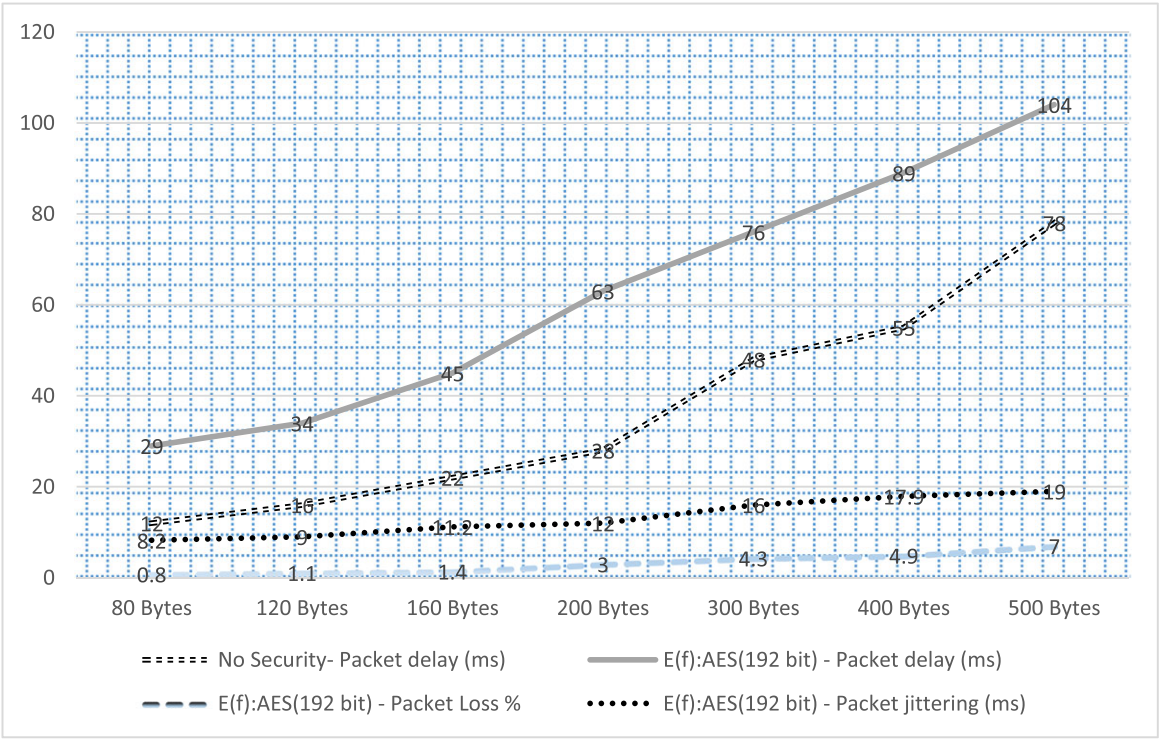

Figure 4. Effect of security on packet delay, loss, and jittering with regard to variable packet size.

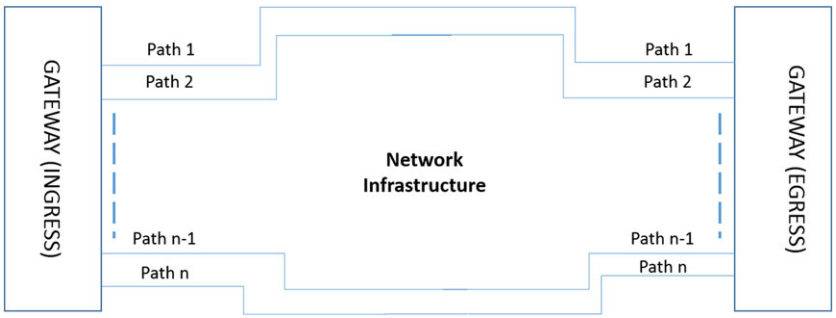

Figure 5. A multipath structure model for voice over IP.

number of bytes in the block is not divisible by k.
·In each block, *all* bytes are fed *to all* coefficients of the polynomial function represented in $GF(2^8)$ finite field.
·Break the resultant VoIP into n sub-VoIP packets.
·For every n sub-VoIP packets, produce a redundant sub-VoIP packet by using the XOR calculation in $GF(2^8)$.
·Save and distribute the calculated n values to n multipaths.
Step 3:*Repetition 1*
Repeat step 2 for all bytes in B_i
Step 4: *Repetition 2*
Repeat steps 2 and 3 for all blocks in a VoIP packet.
Step 5: *Finish* or *wait* for another VoIP to be processed.

Algorithm 4.2 *[Reconstruction of VoIP from sub-multipath routes at the Egress Gateway]*
Input: multipath VoIP sub-IP packets
Output: VoIP traffic S
Step1: *Select* any k = n − 1 out of n sub-VoIP packets.
Step 2: *Perform* the reconstruction by defragmentation process
·*If* : one fragmented sub-VoIP packet is lost or has errors, *then* : Recover it from the redundant VoIP sub-packet.
·Reconstruct the original block B_i from blocks of each sub-VoIP packet, where B_{sub} is the block size in each sub-VoIP packet.
Step 3: *Repetition*
Repeat step 3 until all blocks from sub-VoIP IIP packets are reconstructed, and finally, the original VoIP packet is reconstructed.
Step4: *Repetition*
Repeat steps 2 and 3 until all VoIP traffics are reconstructed
Step5: *Finish* or *wait* for another VoIP traffic.

Algorithm 4.3 *[VoIP sub-IP packet distribution and reconstruction at gateways and network infrastructure handling]*
Input: multipath VoIP sub-IP packets
Output: labeled VoIP sub-IP packets
Requirements: MPLS supported by the network core infrastructure
Step 1: *Select* multipath label switched paths (LSPs) for n sub-VoIP packets (between Ingress and Egress gateways)
Step 2: At Ingress Gateway, *assign* MPLS labels for each VoIP sub-IP packets and distribute it to the assigned LSP.
Step 3: At Egress Gateway, *extract* MPLS labels received from LSPs and *Defrag*.
Step 4: *Reconstruct* original VoIP packet
Step 5: *Repetition*

Repeat steps 1 and 4 *until* all VoIP traffics are processed at Ingress and Egress gateways.
Step 5: *Finish* or *wait* for another VoIP traffic.

In order to test our multipath approach for VoIP communications, we made some modification to the label distribution protocol traffic engineering protocols [18][19] to support extensions for M-OSPF multipath routing protocol. It can be clearly noticed that new objects have to be introduced in the label distribution protocol traffic engineering signaling messages. Therefore, we have defined new Forwarding Equivalence Class called forward error correction VoIP, management information base, EXPLICIT-ROUTE objects for multipath routing for M-OSPF routing protocol, route request object, and route reply objects.

Now, our goal in this section is to test by simulations and analyze the impact of using the multipath approach on the quality of VoIP communication. In addition, we measure the impact of using the multipath approach toward enhancing the security of VoIP. These simulations consider the delay, packet loss, and jittering as main performance evaluation parameters. We have used the same simulation setup as shown in Table II with two testing scenarios; the first one is when sending the VoIP traffic in one a single path, while the second is when sending the VoIP traffic in multipath routes. The simulations were conducted by using the NS2 simulation tool (NS-2.35). Figure 6 shows that multipath delays between two Ingress and Egress gateways are very close to the single-path routing with more delay encountered in the multipath routing due to the fact of having longer paths than the others. However, Figure 7 shows a significant improvement in respect of packet loss when using multipath routing, which is to be expected due to its having redundant packets sent over the multipath VoIP communication.

Nevertheless, the multipath option comes with a cost. The option to find multiple paths between two communicating gateways may not always be available. Moreover, buffering at the receiving gateway is also required because it has to wait for slower paths. To allocate the required buffer size, the following calculations are required:

Consider an original VoIP traffic T with n sub-VoIP traffic T_n. The end-to-end delay for each share toward an Egress gateway G_e is given by

$$d^{T_{n,Ge}} = \sum_{(i,j)\in M_n} d_{ij} \tag{1}$$

where according to our description d_{ij} is the delay of each link (i, j) in a path M_n. The delay for the slowest T_n belonging to Egress gateway G_e is

$$d^{T_{n,Ge}}_{slowest} = \max\left(\left\{d^{T_{n,Ge}}\right\}\right) \text{ for all } M_n \text{ in } M \tag{2}$$

Therefore, the buffer size $Q^{T_{n,Ge}}$ required for each T_n traffic is

$$Q^{T_{n,e}} = \left(d^{T_{n,Ge}}_{slowest} - d^{T_{n,Ge}}\right).RT_n \tag{3}$$

where R_{T_n} is the bit rate arrival for gateway G_e from traffic T_n. It is noticed that a buffer for the slowest path is not required. The total buffer size required at an egress router G_e for an original VoIP traffic T is

$$Q^{Te} = \sum_{\forall M_n \in M} Q^{T_{n,Ge}} \tag{4}$$

5. FUTURE WORK AND CONCLUSION

In this paper, we focused on VoIP communication and the security impact for wired infrastructure networks.

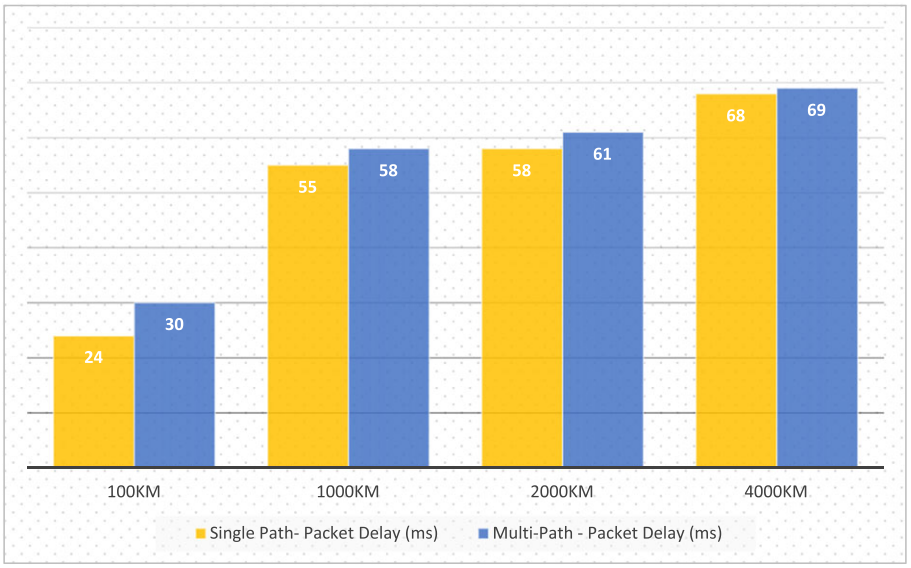

Figure 6. Packet delay evaluation for single and multipath voice over IP communications.

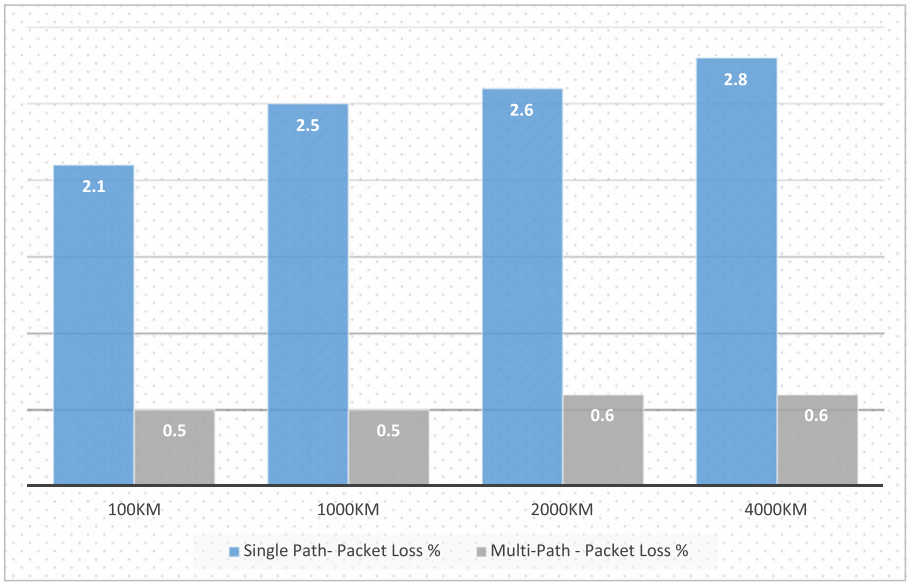

Figure 7. Packet loss evaluation for single and multipath voice over IP communications.

Therefore, our next step will target the same objectives mentioned in the preceding texts but with focus on wireless network infrastructures, which require different testing and simulation environment. Moreover, the visibility of VoIP application in distributed systems/cloud computing environments will also be investigated.

In this paper, we have studied the effect of security on VoIP communications. Our simulation results have shown that adding security on top of a VoIP communication may result in adding more delay, jittering, and packet loss, especially when applying high encryption standards such as AES (256 bits). This paper also investigates the application of VoIP in multipath environment. Our analysis has shown that multipath networking can reduce the VoIP packet loss with a slight delay incurred. We also, suggested the use of MPLS as core infrastructures for multiple path networking as MPLS is able to provide multipath routing with simple implementation and less networking overhead.

REFERENCES

1. Endler D, Collier M. Hacking exposed VoIP: voice over IP security secrets & solutions. McGraw-Hill, Inc.: New York, NY, USA, 2006.
2. Reason J, Messerschmitt D. The impact of confidentiality on quality of service in heterogeneous voice over IP networks. *Management of Multimedia on the Internet, Lecture Notes in Computer Science Volume* 2001; **2216**:175–192.
3. Z. Anwar, W. Yurcik, R.E., Johnson, M. Hafiz, R.H. Campbell, "Multiple design patterns for voice over IP (VoIP) security", Performance, Computing, and Communications Conference, 2006. IPCCC 2006. 25th IEEE International, vol., no., pp.8 pp.,492, 10-12 April 2006.
4. Kuntze N, Schmidt AU, Hett C. Non-repudiation in internet telephony. *Proc. IFIP International Information Security Conference* May 2007:361–372.
5. Palmieri F, Fiore U. Providing true end-to-end security in converged voice over IP infrastructures. *Computers & Security* September 2009; **28**:433–449.
6. A. Elbayoumy and S. Shepherd, "A high grade secure VoIP system using the tiny encryption algorithm," in Proc. 7th Annual International Symposium on Advanced Radio Technologies, pp. 342–350, March 2005.
7. C. Cioponea, M. Bucicoiu, D. Rosner, "Analysis of VoIP encryption performance using dedicated hardware," Roedunet International Conference (RoEduNet), 2013 11th, vol., no., pp.1,4, 17-19 Jan. 2013.
8. Y. Hanifan, Y. Bandung, "Designing VoIP security system for organizational network," ICT for Smart Society (ICISS), 2013 International Conference on, vol., no., pp.1,5, 13–14 June 2013.
9. Son B, Nahm E, Kim H. VoIP encryption module for securing privacy. *Multimedia Tools and Applications, Springer* 2013; **63**(1):181–193.
10. Wanga C, Liu Y. A dependable privacy protection for end-to-end VoIP via elliptic curve Diffie-Hellman and dynamic key changes. *Journal of Network and Computer Applications* 2011; **34**:545–1556.
11. N. Kazemi, A. Wijesinha, R. Karne, "Evaluation of IPsec overhead for VoIP using a bare PC", Computer Engineering and Technology (ICCET), 2010 2nd

International Conference on, vol.2, no., pp.V2-586, V2-589, 16-18 April 2010.
12. Mohammed H, Ali A. Effect of some security mechanisms on the Qos VoIP application using OPNET. *International Journal of Current Engineering and Technology* 2013; **3**(5).
13. H. Jiang, Y. Jia, and X. Wang, "An identity-based security mechanism for P2P VoIP," IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS), vol., no., pp.481,485,-25, June 2010.
14. Gruber M, Schanes C, Fankhauser F, Moutran M, Grechenig T. Architecture for trapping toll fraud attacks using a VoIP honeynet approach. *Network and System Security, Lecture Notes in Computer Science Volume* 2013; **7873**:628–634.
15. M. Ronniger, F. Fankhauser,C. Schanes, and T. Grechenig, "A robust and flexible test environment for VoIP security tests", Internet Technology and Secured Transactions (ICITST), 2010 International Conference for, vol., no., pp.1,6, 8-11 Nov. 2010
16. E. Coulibaly, and L. Liu, "Security of Voip networks", 2nd International Conference on Computer Engineering and Technology (ICCET), vol.3, pp.V3-104-V3-108, April 2010.
17. L. Angrisani, R. Moriello, M. Di Lelio, P. Morabito, and M. Vadursi, "Design and implementation of a reconfigurable test-bed for real-time security measurements in VoIP systems" **46**, 9, 3691–3700, 2013.
18. Zhang L, Tang S, Zhu S. A lightweight privacy preserving authenticated key agreement protocol for SIP-based VoIP. *Peer-to-Peer Networking and Applications* 2016; **9**(1):108–126.
19. German P. Counting the security cost of cheap calls. *Journal of Network Security* 2015; **2015**(11):9–11.
20. NS2 Simulation tool, *www.isi.edu/nsnam/ns/*
21. L. Anderson, B. Thomas, "LDP specification", RFC 5036, IETF, 2007
22. Alouneh S, Abed S, Jamil Mohd B, Kharbutli M. MPLS technology in wireless networks. *Journal of Wireless Networks (WINET), Springer* 2014; **20**(5).