VoIP Codec Performance Evaluation on GRE with IPsec over IPv4 and IPv6

Article · October 2021

DOI: 10.25046/aj060528

CITATIONS
0

READS
114

5 authors, including:

Oluwaseun Alausa
Redeemer's University
1 PUBLICATION **0** CITATIONS
SEE PROFILE

Mba Odim
Redeemer's University
19 PUBLICATIONS **21** CITATIONS
SEE PROFILE

Bosede O. Oguntunde
Redeemer's University
10 PUBLICATIONS **6** CITATIONS
SEE PROFILE

Adewale Opeoluwa Ogunde
Redeemer's University
28 PUBLICATIONS **229** CITATIONS
SEE PROFILE

ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 6, No. 5, 260-266 (2021)

www.astesj.com

ASTESJ

ISSN: 2415-6698

VoIP Codec Performance Evaluation on GRE with IPsec over IPv4 and IPv6

Oluwaseun Ayokanmi Alausa, Samson Afolabi Arekete*, Mba Obasi Odim, Abosede Oyenike Oguntunde, Adewale Opeoluwa Ogunde

Department of Computer Science, Redeemer's University, Nigeria

ARTICLE INFO

Article history:
Received: 10 October, 2020
Accepted: 26 May, 2021
Online: 11 October, 2021

Keywords:
VoIP
IPv4
IPv6
GRE

ABSTRACT

Scientists succeeded in implementing conventional public switch telephone network (PSTN) into internet protocol by launching H.323 IP telephony. The irrelevant and unknown captions in H.323, computer scientists have replaced H.323 by Session Initiation Protocol (SIP) for Voice-over-IP (VoIP). However, the security of voice communication over IP is still a major concern. Besides, security and performance contradict features. VoIP exhibits a quality-of-service requirements that are sensitive to time. Example of such QoS requirements are delay, jitter, and packet loss. Integrating Internet Protocol Security (IPsec) with Generic Routing Encapsulation (GRE) encrypts and authenticate packets from the sender to receiver, but that raises the question of performance as VoIP is time sensitive. Consequently, three codecs were evaluated to determine the efficiency of each on GRE and IPsec implementation on Internet Protocol version 4 and Internet Protocol version 6 (IPv4 and IPv6), respectively. The topology design and device configuration in this study adopted Graphic Network Simulator 3 (GNS3) and Distributed Internet Traffic Generator (D-ITG) to generate VoIP traffic. The evaluation revealed that the G.723.1 codec achieved better results on IPv4 and IPv6 over GRE with IPsec than other codecs used in the experiment. Furthermore, the codec of choice is a major factor in IPsec VoIP deployment, as also revealed in this study.

1. Introduction

There is a budding interest among network providers in deploying a converged IP network that is more cost-effective and more comfortable to manage [1]. Voice communication over IP leverages the packet-switched network architecture, allowing both voice and data packet to negotiate the IP infrastructure simultaneously. The IP architecture supports the carriage of any traffic (voice, video, and text) using best effort carriage devices. As reasonably priced as the IP network is, it poses some threat and challenges for Voice communication [2]. Tunnelling protocol such as Generic Routing Encapsulation Protocol provides packet-level encapsulation only with support for IPv4 and IPv6. Network packets are more susceptible to attack and sniffing using only GRE. Hence, the need for Internet Protocol Security (IPsec); a standard responsible for packet authentication and encryption at layer 3 with support for IPv4 and IPv6 [3, 4].

The use of IPsec is ubiquitous in Virtual Private Networks today for a two-way authentication between hosts at the start of a session and crypto keys for negotiation during an established session [5, 6]. IPsec can secure packet flows between host-to-host, network gateways, and network to host communication [4]. Implementing VoIP over such a reliable and secure protocol ensures a high level of security and privacy.

GRE is a packet encapsulation protocol that supports multicast traffic [6]. GRE provides support for both IP protocol and non-IP protocols. GRE requires IPsec to provide reliable security attributes like encryption and authentication as it is not a secure protocol on its own [7].

Encryption converts data to a cypher-text format that makes data unreadable to sniffers. The appropriate algorithm and key are required to access the cypher-text content. Examples of cryptographic algorithms include Triple Encryption Standard (3DES) and Advanced Encryption Standard (AES) [8].

However, VoIP has time-sensitive traffic, which exhibits a bounded quality of service requirement, such as delay, jitter, and packet loss [9]. It is crucial to verify that adding an extra layer of security on the VoIP packet does not degrade the QoS requirements.

*Corresponding Author: Samson Afolabi Arekete, Email: areketes@run.edu.ng

Related works [5, 10–12] reviewed have investigated GRE and IPsec over IPv4 with little concentration on IPv6, thus a Motivation to understand better the effect of IPsec and GRE on VoIP codec over IPv4 and IPv6.

2. Objective of the study

The objective of this study includes:

1. Evaluate the performance of three VoIP codec on GRE with IPsec considering their effect on delay, jitter, and packet loss.
2. Compare the performance of each codec in (1) above over IPv4 and IPv6.

3. Significance of the study

This study's findings helped verify the appropriate codec suitable for GRE with IPsec network, staying within the limits of ITU-T recommended VoIP quality standard [13]. Through its experiment, the study has established that the choice of voice codec plays a significant role in VoIP IPsec deployment. With the right voice codec, IPsec does not in any way degrade the quality of voice communication.

4. IP Protocols and Voice Codecs

Two IP protocols are discussed in this section, namely IP version 4 and IP version 6. Three codecs developed by the ITU's Telecommunication unit for audio compression and decompression were highlighted: G.711, G.723.1, and G.729.3 codecs.

IPv4 – Internet Protocol version 4

Currently, the Internet Protocol version 4 is mainly used to communicate over the Internet, although deployment of a successor protocol, IPv6, is ongoing. Usually, an IP address holds two different data types, such as the host address and the network address. IPv4 address was structured based on 32-bit values and typically expressed in dotted decimal notation with four octets separated by decimals, for example, 192.168.120.80. IPv4 addresses were divided into five different classes; however, classes A, B and C are generally used. Class A provides the highest amount of IP addresses, while class B provides less than class A and class C offers the least amount of IP addresses [14,15]

IPv6 – Internet Protocol version 6

IPv4 has been used in the Internet world for over two decades. Unfortunately, this is approaching the limit of its capacity of hosting, which is 2^{32} bit addresses. To improve capacity, IPv6 was planned and structured with enhanced features to provide better services than IPv4. With its improved capacity, IPv6 is capable of delivering 2^{128} bit addresses. In addition, IPv6 eliminates the use of Network Address Translation (NAT) and Variable Length Subnet Mask (VLSM) since it has enough IP addresses for all the users around the globe [16].

G.711 Codec

Hypothetically, G.711 codec delivers an exceptional class of voice service that requires higher processing and bandwidth [17]. According to [18], G.711 codec uses 80-bytes of the frame for voice encoding over a 10ms interval. The G.711 codec uses about 64kbps for a one direction call and 128kbps for two-way communication.

G.723 Codec

For voice and multimedia, the ITU-T developed another codec called the G.723 codec, which is an extension of the G.721 codec. In theory, G.723 codec is not suitable for sounds because of its lower-quality output [19]. In [20] the author noted that the G.723 codec was especially fashioned for voice encoding at low transmission capacity. The G.723 codec can operate at 6.4kbps and 5.3kbps with 24-bytes and 20-bytes, respectively.

G.729 Codec

The G.729 codec ITU-T standard engages the Conjugate-structure algebraic-code-excited linear-prediction (CS-ACELP) algorithm to compress a payload for a low bit rate. In theory, G.729 codec delivers reasonably high speech performance [21]. The author in [22] noted that G.729.1 codec has an in-built scalable design set up as an extension of an existing specification. The G.729 codec can interoperate at 8kbps.

In Table 1, the VoIP codec specifications illustrate and compare three ITU-T codecs showing their features, namely, bandwidth, sample period, frame size, and rate.

Table 1 VoIP codec specifications [13]

Codec	G.711	G.723.1	G.729
Bandwidth (Kbps)	64	5.3/6.4	8
Sample period (ms)	20	30	20
Frame size (payload)	160	20/24	20
Rate (Packets /s)	50	33	50

Generic Routing Encapsulation Protocol

GRE, a tunnelling protocol developed by Cisco, which was later standardized by the Internet Engineering Task Force (IETF) [23,24], works by encapsulating layer packet within another IP datagram. It supports broadcast, multicast and other non-IP protocol traffic. GRE tunnels are not secured as data payload are not encrypted and verified. Hence, in real-time, IPsec is integrated with GRE to guarantee the security and integrity of packets.

Internet Protocol Security

In 1998, the IETF drafted the Internet Protocol Security in Request for comments 2411 [25], which was obsoleted by RFC 6071 [26]. IPsec ensures the security of layer three packets for both IPv4 and IPv6. IPsec provides level peer verification, data source validation, data privacy, and data integrity [27–31]. It supports encryption protocol such as DES (Data encryption standard), 3DES (Triple data encryption standard), AES (Advanced encryption standard), authentication protocol such as MD5 (Message Digest 5) and SHA (Secure hash algorithm) [32].

The codecs and IP protocols explained in this section were used in this study. The following section discussed the performance metrics used for evaluation in this study, such as delay, jitter and packet loss.

5. Traffic Generating Tool

D – ITG (Distributed Internet Traffic Generator)

A packet-level traffic generator developed by [33] allows the simultaneous generation of multiple flows of traffic. It can generate realistic traffic patterns from Internet protocols like TCP, UDP, ICMP, and VoIP. Delay, Jitter, Packet Loss are metrics supported by D-ITG. It is a multi-platform application as it works on Linux and Windows. D-ITG can send traffic via UDP or TCP, supporting various voice codecs [1]. According to [34] distributed Internet traffic generator can generate IPv4 and IPv6 traffic that precisely imitates the forms explicated by the Inter Departure time (IDT) and the packet size (PS) stochastic process. Embedded in D-ITG are some statistical models proposed to replicate traffic related to Voice activity detection, DNS, Telnet and VoIP. D-ITG's architecture and components are depicted in Figure 1. The Sender and Receiver are used to generate traffic. The traffic report is held by the ITGLog and can be decoded using the ITGDec, which is the analyzer. The controller controls the activities of each component of the D-ITG.

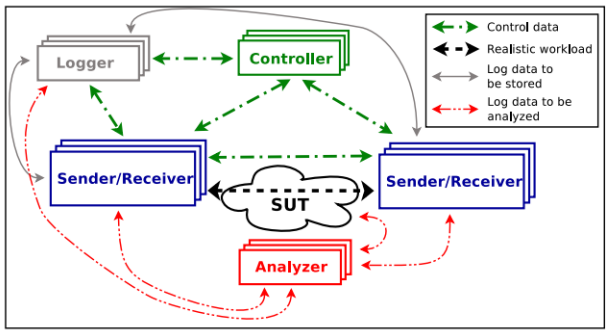

Figure 1: Architecture of D-ITG and its components [33]

6. Performance Metrics

Delay

The time elapsed for a block of data to transit from the sender through the receiver's network infrastructure is regarded as delay. Voice packets can be degraded if it takes a long time to deliver packets from end-to-end [35]

D_t, the total voice packet delay, is calculated thus:

$$D_t = D_n + D_e + D_d + D_c + D_{de} \quad (1)$$

where the components are delays due to:

D_n = Network

D_e = Encoding

D_d = Decoding

D_c = Compression

D_{de} = Decompression

Jitter

Delay variation, often referred to as jitter, is a vital QoS metric in voice communication. It is the measurement of the time difference between packets sent and packets arriving. According to [36,37] a jitter of above 30ms will adversely affect call quality. Jitter can be expressed as follows:

$$J_{(i)} = J_{(i-1)} + \frac{|D_{(i-1,i)}| - J_{(i-1)}}{16} \quad (2)$$

where:

$J_{(i)}$ =jitter of the i^{th} packet

$J_{(i-1)}$ =jitter of the *(i-1)* packet, and

$D_{(i-1,i)}$ = delay between the packet *(i)* and *(i-1)*

Packet Loss

When a packet in transit between two or more hosts on a network fails to reach their destination, packet loss is said to have occurred. It occurs due to an error in data transmission or congestion in the network [38]. ITU-T recommends a maximum of 3% packet loss for VoIP [39]. The Packet Loss rate is computed using the number of RTP packets anticipated and acknowledged from each source. The number of packets is counted as they arrive. The receiver computes the number of packets expected using the difference between the highest segment received and the first segment [40]. Packet loss can be expressed as follows:

$$P_l = P_e - P_r \quad (3)$$

where:

P_l = Packet loss

P_e = Packet expected

P_r = Packet received

In Table 2, the VoIP QoS requirement as recommended by the ITU is given as follows:

Table 2: VoIP Quality Requirement [13]

QoS requirement	Good	Acceptable	Poor
Delay (ms)	0 – 150	150 – 300	>300
Jitters (ms)	0 – 20	20 – 50	>50
Packet Loss (%)	0 – 1	1 – 3	>3

7. Literature Review

A review of related studies is carried out in this section. A comparison of the performance VoIP over BGP/MPLS, VPN and MPLS network was carried out in [5]. The study was simulated under OPNET Modeler using the G.711, G.723.1, and G.729A codecs. The study submitted that the G.729A codec gave a

superior performance over the BGP/MPLS VPN network. The author in [41] noted that encryption is not a standard service in BGP/MPLS VPN, thus not immune to DoS attacks or intrusion.

Furthermore, Performance analysis of IPsec VPN over VoIP network was investigated in [42]. The experimental result showed a rational decline in performance due to the encryption and authentication process carried out by IPsec. Besides, no VoIP codec was evaluated in the study.

The performance of VoIP over GRE tunnel, which provides no extra layer of security, was simulated in [11]. The study submitted that GRE did not lead to a substantial rise in the QoS parameters such as delay and call setup time. GRE being a transparent tunnelling protocol, is not suitable for conveying sensitive traffic such as VoIP. Traffic going over the GRE tunnel is very prone to DoS attack and packet sniffing.

Evaluation of VoIP over multiple Multiprotocol Label Switching (MPLS) tunnelling was carried out in [43]. The study adopted various MPLS architecture with IPsec Secure Hash Algorithm (SHA) and AES for encryption. According to the study, giving the extra layer added by IPsec, VoIP becomes unusable and results in poor speech quality.

Furthermore, an analytical evaluation of layer three tunnelling protocols using VoIP traffic was conducted in [12]. The study attributed the stability of delay variation for non-IPsec scenarios to the non-verification of layer three packets by IPsec encryption and integrity controls. The study concluded that the high delay value reported was a result of IPsec encryption and authentication.

IPv4 to IPv6 and IPv6 to IPv4 transition mechanism was evaluated in [44] with and without virtual private network like IPsec. The codecs were evaluated over Point-to-Point Protocol and IPsec over 4to6 and 6to4 transition mechanism. The metric assessed for the VoIP codec is throughput. The study reported that G.711.2 and G.723.1 codec had the highest throughput.

In [10] the author adopted the riverbed modeller to evaluate SIP performance first with VPN and without VPN. The study evaluated the G.711 codec. The study results revealed that VPN does not lead to higher call set up time as opposed to the submission of [45]. QoS metric like delay, jitter, and packet loss was not evaluated in the study.

The authors in [46] evaluated the performance of the G.711 codec using Open Shortest Path First (OSPF) and Routing Information Protocol (RIP) on IPv4 and IPv6. According to the study, the quality of voice communication in an IP network is dependent on variables such as codec, delay, jitter, packet loss, and routing protocols to reduce convergence time in the case of a link failure. OSPFv3 and RIP next generation (RIPng) performed better in terms of packet delay disparity, end-to-end delay and jitter when compared with OSPFv2 and RIPv2. No tunnelling protocol like GRE was used in the study.

The performance of VoIP over IPv4 and IPv6 was simulated in [47] using the OPNET modeller. The experiment was conducted using the G.711 codec with no tunnelling protocol employed. The study submitted that VoIP on IPv6 had superior performance compared to IPv4.

The study in [48] evaluated three MPLS architecture, IP MPLS, MPLS VPN and MPLS IPsec. IP Service Level Agreement (IP SLA) was used to generate VoIP traffic with delay, jitter, loss rate used as evaluation parameters. The study adopted GNS3 as the network simulator, with G.711 codec being the only codec evaluated over the three MPLS architecture. The study reported that MPLS IPsec resulted in the degradation of voice communication while IP MPLS and MPLS VPN gave acceptable latency and jitter results.

This present study seeks to expand the scope to include IPv4 and IPv6 based on the literature reviewed. Three codecs were used (G.711.1, G.723.1, G.729.3) in this study. The methodology is discussed in the next section.

8. Methodology

This study was carried out in an emulation environment using GNS3. Distributed Internet Traffic Generator (D-ITG) installed on Ubuntu Linux 16.04LTS was used to generate VoIP traffic. The G.711.1, G.723.1, G.729.3 codec were evaluated on the GRE with IPsec tunnel over IPv4 and IPv6.

In this study, a site-to-site VPN topology was used, as depicted in Figure 2. The study considered the performance evaluation of VoIP codec on GRE with IPsec encryption and authentication features over IPv4 and IPv6 Protocol.

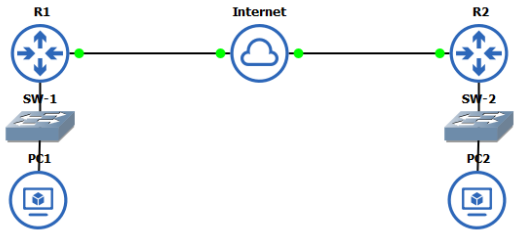

Figure 2: Network topology for the experimental testbed

The study considered three QoS parameters: delay, jitter, and packet loss. Table 3 shows the VoIP parameters used in the study, while Table 4 shows the IPsec configuration Profile.

Table 3: VoIP Parameters

Traffic	VoIP
Codec	G.711.1; G.723.1; G.729.3
Number of packets	100 – 1000 p/s

Table 4 – IPsec Configuration Profile

Encryption	3DES
Packet integrity	MD5
Authentication	Pre-Share

Lifetime	86400s
Cisco IOS	c7200

9. Result and Discussion

The result of this study is subdivided into sections A, B, C. Section A discusses the results for the delay on GRE with IPsec over IPv4 and IPv6. Section B discusses the result for Jitter on GRE with IPsec over IPv4 and IPv6. Section C discusses Packet Loss on GRE with IPsec over IPv4 and IPv6. Table 5, 6, and 7 presents the summary of results for the delay, jitter, and packet loss.

Table 5: Delay (ms) performance summary for GRE with IPsec over IPv4 and IPv6

Codec	G.711.1	G.723.1	G.729.3
GRE with IPsec (IPv4)	196.785	69.186	64.583
GRE with IPsec (IPv6)	389.306	78.056	95.333

From the result in Table 5, the G.723.1 codec gave superior performance compared to the other two codecs. On GRE with IPsec for IPv6, the G.723.1 codec gave a superior performance for delay at 78.056ms compared to G.711.1 at 389.306ms and G.729.3 at 95.333ms. High delay often leads to low speech quality in a VoIP network. The lower the delay, the better the voice quality. According to [13], the ITU-T recommended that VoIP delay should not exceed 300ms. The result in Table 5 clearly shows that the G.711.1 codec exceeds the ITU requirement for the delay on IPv6. Of the three codecs evaluated, the G.723.1 and the G.729.3 codec stood out on IPv4 and IPv6.

Table 6: Jitter (ms) performance summary for GRE with IPsec over IPv4 and IPv6

Codec	G.711.1	G.723.1	G.729.3
GRE with IPsec (IPv4)	18.038	4.561	4.968
GRE with IPsec (IPv6)	48.31	4.588	11.018

In Table 6, the result for jitter is presented for GRE with IPsec over IPv4 and IPv6. The performance of the three codecs on the GRE with IPsec over IPv4 was superior to IPv6. In Table 2, the acceptable QoS requirement for jitter is 50ms. In Table 6, the G.711.1 codec reported a high delay variation on GRE with IP sec over IPv6 at 48.31ms, making the codec not suitable for IPv6 GRE with IPsec deployment. However, the G.711.1 codec fared better on GRE with IPsec over IPv4 with a reported value of 18.038ms. On the other hand, the G.723.1 codec and the G.729.3 codec gave a superior performance over IPv4 GRE with IPsec deployment. The reported value for both codecs were 4.561ms and 4.968ms, respectively. On the GRE with IPsec over IPv6, the G.723.1 codec gave superior performance compared to the two other codecs. The G.723.1 codec reported a performance value of 4.588ms on the GRE with IPsec over the IPv6 protocol. Comparing both the IPv4 and IPv6 results, it is safe to submit that the G.723.1 is preferred to the other two codecs.

Table 7: Packet loss (%) performance summary for GRE with IPsec over IPv4 and IPv6

Codec	G.711.1	G.723.1	G.729.3
GRE with IPsec (IPv4)	67.53	0.1	1.34
GRE with IPsec (IPv6)	86.06	0.45	22.56

For packet loss, the acceptable range is 3% maximum as depicted in Table 2. From Table 7, the G.711.1 had the highest packet loss at 67.53% on IPv4 and 86.06% on IPv6. Hence, the G.711.1 codec becomes unusable on both IP Protocols. Furthermore, on the GRE with IPsec over IPv4, the G.723.1 codec and G.729.3 codec reported a value of 0.1% and 1.34%, respectively, which fall within the acceptable range of the ITU recommendations as depicted in Table 2. For the G.723.1 codec and G.729.3 codec, it is safe to submit that both codecs are suitable for the GRE with IPsec over IPv4 deployment.

On the other hand, the G.729.3 codec exceeded the ITU requirement for packet loss on the GRE with IPsec IPv6 deployment with a reported value of 22.56%. Hence the G.729.3 codec is not fit for use on the IPv6 GRE with IPsec deployment. On the GRE with IPsec over IPv6 deployment, the G.723.1 codec gave a superior performance at 0.45%, which is within the acceptable limits of the ITU recommendation as depicted in Table 2. For the packet loss metric, this study submits that the G.723.1 codec is suitable for IPv4 and IPv6 deployment of GRE with IPsec while G.729.3 codec is suitable for IPv4 GRE with IPsec deployment.

10. Conclusion

This study has provided quantitative evidence by evaluating the performance of three VoIP codecs on GRE with IPsec over IPv4 and IPv6. VoIP codec has a vital role in IPsec enabled network architecture. Delay, jitter, and packet loss were the three QoS parameters evaluated in the study. Since these QoS metrics cannot independently determine the quality of voice communication over IP networks, then the codec that gave a superior performance across the three QoS metric would be considered an efficient codec for GRE with IPsec implementation.

The only codec in this study that efficiently balances acceptable delay, jitter, and packet loss across the IPv4 and IPv6 deployment is the G.723.1 codec. The G.723.1 codec has proved to be usable for IPsec implementations on GRE with IPsec. This study agrees with [49] that regardless of IPsec, the codec of choice influences the voice communication quality output over the IP network. Low bandwidth codec such as G.723.1 and G.729.3 are better choices for IPsec enabled VoIP implementations.

Specific limitation exists in the present study which the methodology could not accommodate. Codecs like Speex, Silk, iLBC, OPUS, and CELT were not evaluated as the traffic generating tool (D-ITG) does not support them. Other IPsec encryption algorithm like AES can also be evaluated in further studies alongside SHA. The present study did not consider any routing protocol like OSPF, EIGRP, and RIP in IPv4 and IPv6 environment. These areas would be addressed in further studies.

Conflict of Interest

The authors declare no conflict of interest.

Acknowledgement

We would like to appreciate the Department of Computer Science, Redeemer's University, for the privilege to conduct this research.

References

[1] H. Sathu, M.A. Shah, "Performance comparison of VoIP codecs on multiple operating systems using IPv4 and IPv6," International Journal of E-Education, e-Business, e-Management and e-Learning, **2**(2), 122, 2012.

[2] S. V. Subramanian, R. Dutta, Measuring SIP proxy server performance, Springer International Publishing, 2013, doi:10.1007/978-3-319-00990-2.

[3] S. Kent, R. Atkinson, RFC2402: IP authentication header, 1998.

[4] R. Atkinson, "IP Encapsulating Security Payload (ESP)," RFC 4303, (1827), 1–44, 1995, doi:10.17487/RFC4303 M4 - Citavi.

[5] I.S.I. Alsukayti, T.J. Dennis, C. Edwards, "Performance analysis of VoIP over BGP-MPLS VPN technology," in PGNet conference, 2011.

[6] K.A. Ogudo, "Analyzing generic routing encapsulation (GRE) and IP Security (IPSec) tunneling protocols for secured communication over public networks," in icABCD 2019 - 2nd International Conference on Advances in Big Data, Computing and Data Communication Systems, Institute of Electrical and Electronics Engineers Inc.: 1–9, 2019, doi:10.1109/ICABCD.2019.8851004.

[7] S. Jahan, M.S. Rahman, S. Saha, "Application specific tunneling protocol selection for Virtual Private Networks," in Proceedings of 2017 International Conference on Networking, Systems and Security, NSysS 2017, Institute of Electrical and Electronics Engineers Inc.: 39–44, 2017, doi:10.1109/NSysS.2017.7885799.

[8] J.G.M. Srivastava, R. Sheeja, "Design and Implementation of Crypto based Water Marking Techniques for EHR Security," Test Engineering and Management, **82**, 10788–10792, 2020.

[9] K. Salah, Deploying VoIP in Existing IP Networks, CRC Press: 19–40, 2018, doi:10.1201/9781420070217.pt1.

[10] A.A. Eskandar, M.R. Syed, M.B. Zarei, "SIP over IP VPN : Performance Analysis," in Proceedings on the International Conference on Internet Computing (ICOMP), 1, 2014.

[11] A.A. Eskandar, M.R. Syed, Z.M. Bahareh, "Performance analysis of VOIP over GRE tunnel," International Journal of Computer Network and Information Security, **7**(12), 1, 2015.

[12] F. Bensalah, N. El Kamoun, A. Bahnasse, "Analytical performance and evaluation of the scalability of layer 3 tunneling protocols: case of voice traffic over IP," IJCNS International Journal of Computer Science and Network Security, **17**(4), 361–369, 2017.

[13] J. Yu, I. Al-Ajarmeh, "Call admission control and traffic engineering of VoIP," in 2007 Second International Conference on Digital Telecommunications (ICDT'07), 11, 2007, doi:https://dx.doi.org/10.1109/ICDT.2007.44.

[14] Y. Rekhter, B.M. Chrysler, D. Karrenber, G.J. de Grooe, E. Lear, Address Allocation for Private Internets, Journal of Chemical Information and Modeling, **5**(9), 1689–1699, 2013.

[15] J. Davies, A. Northrup, Windows Server 2008 networking and network access protection (NAP), Microsoft Press, 2008.

[16] S. Deering, R. Hinden, others, Internet protocol, version 6 (IPv6) specification, 1998.

[17] L. Roychoudhuri, E. Al-Shaer, H. Hamed, G.B. Brewster, "Audio transmission over the Internet: Experiments and observations," in IEEE International Conference on Communications, 2003. ICC'03., 552–556, 2003.

[18] Y. Jeong, S. Kakumanu, C.L. Tsao, R. Sivakumar, "VoIP over Wi-Fi networks: Performance analysis and acceleration algorithms," Mobile Networks and Applications, **14**(4), 523–538, 2009, doi:10.1007/s11036-009-0157-6.

[19] H. Cui, K. Tang, T. Cheng, "Audio as a support to low bit rate multimedia communication," in ICCT'98. 1998 International Conference on Communication Technology. Proceedings (IEEE Cat. No. 98EX243), 544–547, 1998.

[20] M. Menth, A. Binzenhöfer, S. Mühleck, "Source models for speech traffic revisited," IEEE/ACM Transactions on Networking, **17**(4), 1042–1051, 2009, doi:10.1109/TNET.2008.2006222.

[21] L. Ding, R.A. Goubran, "Assessment of effects of packet loss on speech quality in VoIP," in Proceedings - 2nd IEEE International Workshop on Haptic, Audio and Visual Environments and their Applications, HAVE 2003, Institute of Electrical and Electronics Engineers Inc.: 49–54, 2003, doi:10.1109/HAVE.2003.1244724.

[22] I. Varga, S. Proust, H. Taddei, ITU-T G.729.1 scalable codec for new wideband services, IEEE Communications Magazine, **47**(10), 131–137, 2009, doi:10.1109/MCOM.2009.5273820.

[23] D. Farinacci, T. Li, S. Hanks, D. Meyer, P. Traina, "Generic Routing Encapsulation (GRE)," Request for Comments, 1–9, 2000, doi:http://dx.doi.org/10.17487/RFC2784.

[24] G. Dommety, Key and Sequence Number Extensions to GRE, Request for Comments, 1–7, 2000, doi:http://dx.doi.org/10.17487/RFC2890.

[25] R. Thayer, N. Doraswamy, R. Glenn, {IP} Security Document Roadmap, 1998.

[26] S. Frankel, S. Krishnan, "RFC6071: IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap," Request for Comments, **6071**, 1–63, 2011, doi:10.17487/rfc6071.

[27] S. Ariga, K. Nagahashi, M. Minami, H. Esaki, J. Murai, "Performance evaluation of data transmission using IPSec over IPv6 networks," in Proc. INET, 18–21, 2000.

[28] N. Ferguson, B. Schneier, A cryptographic evaluation of IPsec, 1999.

[29] R. Yuan, W.T. Strayer, Virtual private networks: technologies and solutions, Addison-Wesley Longman Publishing Co., Inc., 2001.

[30] W.B. Diab, S. Tohme, C. Bassil, "Critical VPN security analysis and new approach for securing VoIP communications over VPN networks," in WMuNeP'07: Proceedings of the Third ACM Workshop on Wireless Multimedia Networking and Performance Modeling, 92–96, 2007, doi:10.1145/1298216.1298238.

[31] J. Wu, "Implementation of virtual private network based on IPSec protocol," in 2009 ETP International Conference on Future Computer and Communication, IEEE: 138–141, 2009, doi:https://dx.doi.org/10.1109/FCC.2009.16.

[32] R. Weerawarna, TCP/UDP network performance evaluation of various IPSEC algorithms: an empirical test-bed analysis of a virtual private network protocol., 2013.

[33] A. Botta, A. Dainotti, A. Pescapé, "A tool for the generation of realistic network workload for emerging networking scenarios," Computer Networks, **56**(15), 3531–3547, 2012, doi:10.1016/j.comnet.2012.02.019.

[34] A. Botta, A. Dainotti, A. Pescapè, "Multi-protocol and multi-platform traffic generation and measurement," INFOCOM 2007 Demo Session, **2010**, 4–5, 2007.

[35] K. Kim, Y.J. Choi, "Performance comparison of various VoIP codecs in wireless environments," in Proceedings of the 5th International Conference on Ubiquitous Information Management and Communication, ICUIMC 2011, 2011, doi:10.1145/1968613.1968718.

[36] A. Culleton, "Evaluation of Voip Technologies As a Replacement for Traditional Pstn Based Pbx Systems," 2006.

[37] M. Ahmed, M.A. Suhaimi, Q.S. Md Faisal, S. Haseeb, "Evaluating QoS performance of streaming video on both IPv4 and IPv6 protocols," in Proceedings of the 2007 spring simulaiton multiconference-Volume 1, 109–116, 2007.

[38] Y. Ennaji, M. Boulmaif, C. Alaoui, "Experimental analysis of video performance over wireless local area networks," in International Conference on Multimedia Computing and Systems -Proceedings, 488–494, 2009, doi:10.1109/MMCS.2009.5256645.

[39] B. Goode, "Voice over Internet Protocol (VoIP)," Proceedings of the IEEE, **90**(9), 1495–1517, 2002, doi:10.1109/JPROC.2002.802005.

[40] A.-V.T.W. Group, H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, others, RFC1889: RTP: A transport protocol for real-time applications, RFC Editor, 1996.

[41] M. Behringer, "Analysis of the Security of BGP/MPLS IP Virtual Private Networks (VPNs) Status," RFC 4381, 1–22, 2006.

[42] M. Babu, "Performance Analysis of IPSec VPN over VoIP Networks Using OPNET," International Journal of Advanced Research in Computer Science and Software Engineering, **2**(9), 38–44, 2012.
[43] F. Bensalah, N. El Kamoun, A. Bahnasse, "Scalability evaluation of VOIP over various MPLS tunneling under OPNET modeler," Indian Journal of Science and Technology, **10**(29), 1–8, 2017.
[44] S. Narayan, S. Ishrar, A. Kumar, R. Gupta, Z. Khan, "Performance analysis of 4to6 and 6to4 transition mechanisms over point to point and IPSec VPN protocols," in IFIP International Conference on Wireless and Optical Communications Networks, WOCN, IEEE Computer Society: 1–7, 2016, doi:10.1109/WOCN.2016.7759027.
[45] G. Salama, M. Shehab, A. Hafez, M. Zaki, "Performance Analysis of Transmitting Voice over Communication Links Implementing IPsec," International Conference on Aerospace Sciences and Aviation Technology, **13**(AEROSPACE SCIENCES), 1–12, 2009, doi:10.21608/asat.2009.23489.
[46] M. Syed, I.Y. Ambore, "Performance evaluation of OSPF and RIP on IPv4 & IPv6 technology using G.711 codec," International Journal of Computer Networks and Communications, **8**(6), 1–15, 2016, doi:10.5121/ijcnc.2016.8601.
[47] M. Ahmed, A.T. Litchfield, S. Ahmed, A. Mahmood, M.E.H. Meazi, "VoIP performance analysis over IPv4 and IPv6," International Journal of Computer Network and Information Security, **6**(11), 43, 2014.
[48] F. Bensalah, N. El Kamoun, A. Bahnasse, "Evaluation of tunnel layer impact on VOIP performances (IP-MPLS-MPLS VPN-MPLS VPN IPsec)," International Journal of Computer Science and Network Security (IJCSNS), **17**(3), 87, 2017.
[49] E. Antwi-Boasiako, E. Kuada, K. Boakye-Boateng, "Role of codec selection on the performance of IPsec secured VoIP," in 2016 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2016, Institute of Electrical and Electronics Engineers Inc.: 2508–2514, 2016, doi:10.1109/ICACCI.2016.7732434.

.