QoS Measurement of VoIP Codec Usage on Limited Bandwidth Network over UDP-based VPN

Billy Susanto Panca

***Abstract* — The usage of internet protocol for voice communication is widely used and more efficient rather than an analog signal. However, there is no security guaranteed on IP-based voice communication. The voice payload can be easily tapped or even manipulated. In the case of improving the security aspect, communication quality should be also considered. VoIP requires sufficient bandwidth to get proper communication quality. The ITU-T released a standard unit of communication quality, known as Mean Opinion Score (MOS) which is made from the subjective judgments of some individuals. However, MOS method takes time and is expensive. In this research, we measure VoIP communication which is secured by using VPN and build a tool for analyzing the voice packet between communication peers. The tool has capabilities to measure delay, jitter, and packet loss. Since VoIP has a QoS standard by ITU-T, the usage of VPN for security purpose needs to be considered. The sound quality might be decreased due to the addition of header for tunneling method, as well as the additional delay when the encryption processing is carried out. We used 3 types of codec: a-Law, GSM, and iLBC which will be passed on 4 types of bandwidth (256, 128, 64, 32 kbps) through the UDP-based VPN that use 3 types of encryption method (3-DES, Blowfish, AES).**

***Keywords* — qos, voip, codec, bandwidth, vpn, udp, encryption.**

I. Introduction

Communication trends, such as text chatting, voice, and video calls are sent through the internet. Besides gain flexibility by using IP-based communication, the security and quality of service (QoS) aspect needs to be considered. Voice over IP (VoIP) communication has some threads that divide into several techniques. It can be attacked on the data transmission process, and the hardware or service provider. The voice payload can be sniffed, or even manipulated by using man-in-the-middle (MTM) attack. Besides that, the server or service provider also has a vulnerability that can be attacked by denial of service (DoS) attack.

On the one hand, VoIP communication can be easily secured by using data encryption to prevent sniffed against voice payload and create a tunnel for restricting direct access to the service provider. On the other hand, we need to consider the drawback of the quality of service (QoS) after implementing the security method. There will be an increase in delay, due to addition of information on the packet header for tunneling method, and algorithm delay on data encryption. VoIP communications have a QoS standard by ITU-T for the delay, jitter, and packet loss. The QoS must be preserved when implementing the security aspect.

The usage of certain codecs might be used to improve VoIP communication quality in a certain way. The codec selection might influence the output of voice quality. It is used to compress voice data and make it smaller to send through the network. The codec can be either a hardware or software, in this research we use codec in the form of software, and choose a-law, GSM, and iLBC. After codec compressed the voice payload and sent it into WAN, we cannot control the actual bandwidth on the public network. In this work, we tested the chosen codec for a limited bandwidth (256, 128, 64, 32kbps) with/without VPN and measured the communication delay, jitter, and packet loss.

We build a tool to measure delay, jitter, and packet loss on VoIP communication. The tool was built using Java, which can capture every packet that crossed over the network and sniffed the packet header and payload. It can also detect which codec is used when the voice data is captured.

II. Related Work

There are several researches which focused on voice communication performance and security over the network. Tymchenko et al [1] measured the packet loss in VoIP by using PSQM. Ghiata et al [2] used a neural network and neuro shell to give a capability to learn very accurate MoS. Butcher et al [3] examined and investigated the concerns and requirements of VoIP security by listing the defense sector and generic attack on it. Gupta [4] presents a structured security analysis of the VoIP protocol stack such as SIP, SDP, key establishment, and secure media transport protocols. Yang et al [5] provided a reputation system that monitors VoIP activity, analyzes global traffic patterns, and distinguishes between wanted and unwanted participants. Alouneh et al [6] present a security analysis overflow or limited bandwidth networks using the multipath approach and data encryption using AES. Patrick et al [7] discuss various security VoIP threats. Chandel et al [8] analyze the usage of various routing protocols on WAN with different codecs (G.711, G.729A, G.723.1). They simulated their research by using EXata/Cyber 2.1 simulator and emulator and measure the delay, jitter, packet loss, MoS. VPNs are widely used to establish a secure communication of VoIP.

Paper received February 02, 2020; revised May 16, 2020; accepted June 19, 2020. Date of publication July 31, 2020. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Zorica Nikolić.

Billy Susanto Panca. Faculty of Information Technology, Maranatha Christian University, Indonesia (e-mail: billy.sp@it.maranatha.edu).

Some researchers measure the usage of VPN and analyze the results on the quality of communication. Wafaa et al [9] provide research about the comparison of VPN technologies and used it for securing VoIP communication with considering its weaknesses. They use AVISPA (Automated Validation of Internet Security Protocols and Applications) tool for building and analyzing security protocols. There is research that used a Java-based tool to measure SIP (Session Initialization Protocol) on its delays and jitter at the receiver end [10]. We have proposed the measurement of QoS on the usage of UDP-based VPN for securing VoIP communication with the combination of various bandwidths and codecs. We created a Java-based tool that has capabilities to sniff VoIP packet and analyzed the QoS (delay, jitter, and packet loss).

III. VoIP Codec Characteristics

We proposed 3 kinds of codecs to be measured which will be used on VoIP communication over VPN. GSM was chosen because it has a high compression ratio (create 13kbps stream). GSM is also available in many hardware and software platforms. The second chosen codec is iLBC, which stands for internet low bit rate codec (create 15kbps stream). The third chosen codec is G.711 a-law which creates a 64kbps stream. We proposed 256kbps, 128kbps, 64kbps, and 32kbps bandwidth on this research, considering the variations of available bandwidth on the used network and VPN configuration. Since GSM and iLBC are created a stream lower than our lowest proposed bandwidth on 32kbps the test should be going well. The a-law is creating a 64kbps stream that is not going to work well on 32kbps bandwidth. However, Karapantazis et al [11] measure the codec delay such as algorithm and codec delay on VoIP codec. The a-law has very low processor requirements, compared to iLBC and GSM. iLBC just need 0.125ms for algorithm delay and 0.25msfor codec delay. It means a-law has a hundred times faster than GSM and iLBC on delay values.

TABLE 1: CHARACTERISTICS OF CODECS [11]

Codec	*Bitrate (kbps)*	*Algorithm Delay*	*Codec Delay (ms)*	*MoS*
a-law	64	0.125	0.25	4.1
iLBC	15.2	25	60	3.8
GSM-FR	13	20	40	3.6

Since we focused on measuring QoS of VoIP communication over VPN, the chosen codec isn't just picked by the ideal value of bitrate, but also its algorithm and codec delay. The highest MOS value of VoIP codec is on a-law even it needs at least 128kbps for two-way communication.

IV. VoIP QoS Measurement

In this work, we measure three parameters of VoIP QoS: delay, jitter, and packet loss. Delay or latency measures the length of time it takes between when information is sent and when it is received. Jitter is a variation of delay, and it shows the network consistency. Packet loss is a packet that is broken up when it is being sent. Since VoIP used Real-Time Protocol (RTP) that typically runs over User Datagram Protocol (UDP), when there is a broken package during transmission it did not act on packet loss to send back the packet as TCP did. It is left to the application to take an appropriate action.

We created a software (called VoA core) based on Java which has capabilities to sniff every packet through the network interface (the concept of man-in-the-middle attack). By using the WinPcap library, VoA core might authorize itself to get into a low-level network access. We took the packet frame by sniffing every packet which passes through the network interface and analyzes what kind of packet it is. It also gave us the capability to look up codec information on VoIP communication and help up to analyze the packet. We installed the VoA core on both sides of the communication peer to calculate the delay, jitter, and packet loss value.

Delay value consists of processing, packetization, and network delay. Processing delay in VoIP communication is known as a coder's delay that is the time needed to compress and decompress voice data. The second is the packetization delay which is created during the establishment of the Real-Time Protocol (RTP) packet. And the third is the delay of the network which specifies the time needed to send data from one point into another.

For 3 kinds of codec that are measured in this research, here is the constant's value of delay processing and packetization to be added with network delay to get a total delay:

A. Delay Processing (Coder)

Processing (Coder) delay
= (Compression time) + (Decompression time)

- a-law
  Compression Time
  = 3 * frame-size + look-ahead
  = 3 * 0.125 + 0ms = 0.375ms

  Decompression Time
  = 10% * Compression Time = 0.0375ms

  Total a-law Processing Time = 0.4125ms

- GSM
  Compression Time
  = 3 * frame-size + look-ahead
  = 3 * 20 + 0ms = 60ms

  Decompression Time
  = 10% * Compression Time = 6ms

  Total GSM Processing Time = 66ms

- iLBC
  Since the iLBC used a 15.2kbps bitrate, the processing delay measured by GL Communication inc is 20ms, using a block independent linear-predictive coding (LPC) algorithm. [12]

Refer to ITU-T G.144 [13], the a-law and GSM codec have 0 (zero) delay look ahead.

B. Packetization Delay

Packetization delay is also known as transmission delay. We calculate the packetization delay with the following equation [14]:

$$DT=N/R$$

where:

DT is transmission/packetization delay in seconds
N is number of bits, and
R is bit per seconds transfer rate.

To calculate packetization delay, we already know bitrate for a-law, GSM, and iLBC (shown in Table 1). Next, we get the number of bits for every used codec:

VoicePayload = IP PacketLength − (PacketHeaders)

where packet headers consist of:

Ethernet header = 14 bytes,
IP header = 20 bytes,
UDP header = 8 bytes, and
RTP header = 12 bytes

Then, we can simply calculate voice payload by subtraction of IP packet length with 54 bytes (the sum of ethernet, IP, UDP, and RTP header).

- a-law
  The VoA Core got 214bytes of IP packet length on a-law codec. Voice payload on a-law obtained from the subtraction of 214 bytes with 54 bytes, means a-law have 160 bytes of voice payload that consist of 1280 bits.
  a-law Packetization delay = 1280bit / 64000bps = 0.02seconds (20ms)
- GSM
  We analyzed GSM packet by using VoA core and got 87bytes of IP packet length. Then, the voice payload on GSM codec is 87bytes - 54 bytes = 33 bytes that consist of 264 bits.
  Packetization delay = 264bits / 13000bps = 0.0203 seconds (20ms)
- iLBC
  The GL Communication measured iLBC with 15.2kbps bitrate that have 30ms packetization delay. [12]

The network delay value will be calculated using the VoA core by creating an ICMP packet that is modified to be similar as VoIP packet in size and send it to another peer along with voice packets. VoA core in the computer peer on the other side will sniff the incoming packet and sorting out between voice packet and ICMP packet. We build a small LAN topology that only has 3 hops of a router between client peers. We also make sure, there is only 20% maximum traffic utilization on the network during the test for every proposed bandwidth scenario. Communication measurement over VPN will be done by setup OpenVPN on the edge's router, every testing scenario used 3 types of encryption algorithms (3DES, AES, and Blowfish).

Since we are using a personal lab (LAN) that used a symmetrical path with the same hop count between send and receive data between node, the network delay on ICMP on Syn and Syn-Ack might have a similar value. ICMP gets a time value from a turn-around trip, and to get one-way trip value time, VoA core will simply divide ICMP Syn and Ack. We ignore the value of CPU processing time since ICMP consumes a very short CPU time. Since we can calculate the delay (latency) value, we also can calculate the jitter value.

The VoA core took every incoming packet on the network interface and checked its sequence number. It will check the null or missing packet and detect that as packet loss. We make sure there is a non-blocking process by using multiple threads to handle the I/O process and calculate the QoS values.

V. Analysis and Results

We tested 3 proposed codecs by limiting the bandwidth on the client-side with 254kbps, 128kbps, 64kbps, and 32kbps with and without VPN. There are 3 kinds of encryption algorithms used on VPN: AES, Blowfish, and 3DES. Tables 2 to 4 show the test results of QoS measurement by using the VoA core. Each row presents the average of QoS on 10 times VoIP communication, with approximately 10 minutes on each call.

A. Delay Measurement

With regard to ITU-T standards (Rec G.114) [13], the acceptable delay end-to-end for VoIP communication is less than 150ms. The test result in Table II shows the average of communication delay by using codecs and 3 kinds of VPN encryption. For 3 kinds of codecs tested, all codecs got an acceptable delay on 256kbps with and without VPN. The a-law codec only has an excellence delay on 256kbps, when GSM and iLBC still got an excellence delay until tested on 32kbps bandwidth. The usage of a VPN for communication encryption does not have a high impact on the delay factor. We experience a slight reduction in delay due to the usage of a VPN on a certain codec. The test result in Table 2 shows communication delay changes due to VPN usage.

a-law's delay: The results show that the usage of a-law codec over VPN on all encryption methods gave an additional delay value on 256kbps bandwidth with approximately only 1ms. However, the usage of VPN encryptions on 128kbps becomes better. We experience a reduction in delay value with approximately 100ms even if the basic communication is already unacceptable on approximately over 1150ms. The test result at 32kbps cannot be present due to 100% packet loss on the usage of a-law codec. Prajwala et al [15] also experience the same result, G.711 (a-law) gives more delay compared to other codec on 128kbps bandwidth test.

GSM's delay: The usage of VPN on GSM codec gave an additional delay value. On 256kbps until 64kbps bandwidth, the additional delay made the communication still acceptable on excellent quality (less than 100ms). Approximately, the additional delay only takes 0.5ms on 3DES and Blowfish, and 1ms on encryption by the AES algorithm. Since communication by using GSM on 32kbps bandwidth got a poor delay value, the usage of VPN is not fit to reckon with. However, 3DES usage indicates a reduction in delay value when AES and Blowfish increased on 32kbps bandwidth.

iLBC's delay: We experience the best delay when using iLBC compared with two other codecs on 256-64kbps bandwidth test which stabled on approximately 55ms. Same

as GSM, iLBC becomes unacceptable once tested on 32kbps bandwidth. However, the test scenario on 32kbps bandwidth shows there is a reduction in delay values on every encryption algorithm even though the base communication takes approximately 1000ms which is unacceptable. The test result shows the AES algorithm increases the differential delay value exponentially between the 254kbps until 32kbps with 5 multiplicity (0.49ms, 2.09ms, 8.67ms, 23.87ms).

TABLE 2: DELAY MEASUREMENT RESULT

Codec	*Bandwidth*	*Plain*	*3DES*	*AES*	*Blowfish*
a-law	256kbps	28.48	29.86	30.03	29.08
	128kbps	1,124.88	1,020.11	1,017.92	1,028.07
	64kbps	2,544.16	2,540.97	2882.11	2,536.85
	32kbps	-	-	-	-
GSM	256kbps	89.99	90.50	91.23	90.55
	128kbps	90.12	90.69	91.18	90.72
	64kbps	90.73	91.54	91.78	90.85
	32kbps	1,164.45	1,146.65	1,299.73	1,167.86
iLBC	256kbps	55.56	55.72	56.05	55.76
	128kbps	54.37	55.69	56.46	55.34
	64kbps	54.69	55.60	63.37	55.64
	32kbps	1,014.16	990.21	990.30	1,011.88

B. Jitter Measurement

Jitter is a variation in packet latency for voice communication. Jitter value might appear because of a different route to the destination, network congestion, or improper configuration. Since this research was tested on our own lab and created with an asymmetrical path, the jitter might appear because of network congestion while we limit the communication bandwidth. Ideally, jitter should be less than 30ms for VoIP communication [16]. We present the measurement result of jitter values that appears because of network congestion and the addition of the encryption process in Table 3.

a-law's jitter: The a-law codec got excellence jitter within 256kbps and 128kbps and became unacceptable when tested on 64kbps bandwidth. As we mentioned before, we did not present results on 32kbps since we experience 100% packet loss on 32kbps bandwidth. The results show that the usage of three encryption algorithms gave an additional jitter value yet still got excellent results. The addition of jitter values varies depending on the type of encryption used. The 3DES algorithm gave the best performance for jitter value compared with AES and Blowfish. Test results on 64kbps show a-law codecs are not on excellence but are still acceptable with 39ms jitter while not using VPN. The usage of the 3DES algorithm on 64kbps bandwidth made jitter value increase approximately 4ms, however, AES and Blowfish algorithms make the jitter value better.

GSM's jitter: On the three codec tests performed, GSM codec got the smallest jitter value without using a VPN, when compared with two other tested codecs. The test on 256kbps,128kbp, and 64kbps, shows excellent results (less than 3ms) and becomes unacceptable once tested on 32kbps. After used encryption algorithms, there is a small additional jitter value with approximately less than 1ms on 64-256kbps bandwidth. The smallest addition jitter on 256kbps and 128kbps is performed by the 3DES algorithm, followed by Blowfish and AES. The used Blowfish algorithm on GSM within 64kbps bandwidth made the jitter value become better. The 3DES algorithm gave the best performance for jitter value while using GSM codec when compared with AES and Blowfish.

iLBC's jitter: The same as the other 2 previous codecs, iLBC got excellence jitter from 256kbps to 64kbps bandwidth. The jitter test results in Table 3 show that iLBC on 256kbps got a better value when VPN is used. However, it got additional jitter on three encryption algorithms while using 128kbps bandwidth. On 64kbps bandwidth, 3DES gave a better jitter value when compared with AES and Blowfish which got additional jitter. Since the test on 32kbps got a poor jitter value that is over 50ms, the test result shows that the usage of VPN encryptions made the jitter become better. The 3DES algorithm gave the best performance for jitter value while using iLBC codec compared with AES and Blowfish.

TABLE 3: JITTER MEASUREMENT RESULT

Codec	*Bandwidth*	*Plain*	*3DES*	*AES*	*Blowfish*
a-law	256kbps	2.235	2.914	2.443	3.219
	128kbps	14.805	23.907	27.383	24.467
	64kbps	39.275	43.467	37.363	34.382
	32kbps	-	-	-	-
GSM	256kbps	1.833	1.920	2.840	2.520
	128kbps	1.732	1.952	2.370	2.367
	64kbps	2.706	3.875	3.498	2.157
	32kbps	81.757	95.787	66.985	94.342
iLBC	256kbps	3.409	1.205	2.776	3.047
	128kbps	1.462	1.660	3.186	2.756
	64kbps	2.001	1.738	16.466	2.908
	32kbps	52.190	52.137	45.288	51.204

C. Packet Loss Measurement

Since voice communication uses UDP, it makes the possibility to gain a packet loss. The UDP packet will not resend the lost or broken packet that occurs to maintain the communication performance. The VoIP communication will be excellent if the packet loss takes less than 1% [16].

a-law's packet loss: Regarding the result in Table 4, the a-law codec got excellent packet loss on 256kbps bandwidth, even after the implementation of a VPN. The usage of a VPN made the a-law codec packet loss on 256kbps become better. The test result on 128kbps shows the packet loss value is poor that more than 5%, so are on the 64kbps test. The blowfish algorithm gave a significant decrease on 128kbps bandwidth to 37.66% packet loss. On the three bandwidth test scenarios, the usage of AES algorithm did not give any difference on the a-law codec. Prajwala et al [15] also got the same result in codec G.711 is more prone to error compared with others.

GSM's packet loss: Packet loss on GSM codec is excellent on 256, 128, and 64kbps bandwidth. The tests got nearly 0% packet loss. But once we test on 32kbps bandwidth, it got over 15% packet loss that means poor communication appears. The usage of the 3DES algorithm increases the packet loss on GSM codec. The same as 3DES, the usage of the Blowfish algorithm makes packet loss worse on every test. The 3DES and Blowfish make approximately 0.15-0.40% packet loss yet still are excellent. However, the AES algorithm makes a slight improvement on 256 and 128kbps test. On 32kbps bandwidth test, 3DES and Blowfish gave a slight additional

packet loss. The AES algorithm makes the packet loss gain approximately 60% on the 32kbps bandwidth test.

iLBC's packet loss: The test result on all bandwidth scenarios of iLBC codec shows a poor performance for the packet loss aspect. On 256, 128, and 64kbps it takes approximately 15% packet loss and over 30% loss on 32kbps test. The iLBC stands for internet low bitrate codec, that permits graceful speech degradation in the case of lost frame [17]. The high packet loss might appear because the low bitrate codecs exploit dependencies between speech frames, which cause errors to propagate when packets are lost or delayed. However, iLBC codec is supported by packet loss concealment (PLC) that makes frames independent and so this problem will not occur and compensating for the loss of voice packet. The usage of VPN makes overall iLBC's packet loss improved on the four bandwidth test scenarios.

TABLE 4: PACKET LOSS MEASUREMENT RESULT

Codec	*Bandwidth*	*Plain*	*3DES*	*AES*	*Blowfish*
a-law	256kbps	0.31%	0.09%	0.31%	0.22%
	128kbps	5.91%	7.84%	5.91%	0.66%
	64kbps	36.41%	36.36%	36.41%	37.66%
	32kbps	100%	100%	100%	100%
GSM	256kbps	0.02%	0.43%	0.00%	0.35%
	128kbps	0.04%	0.42%	0.03%	0.17%
	64kbps	0.03%	0.31%	0.09%	0.29%
	32kbps	15.65%	16.07%	75.16%	17.23%
iLBC	256kbps	16.85%	12.49%	9.86%	9.86%
	128kbps	15.38%	13.83%	9.23%	9.23%
	64kbps	14.36%	13.84%	15.84%	15.84%
	32kbps	30.20%	28.45%	28.59%	29.71%

VI. CONCLUSION AND FUTURE WORK

We evaluated QoS on 3 types of VoIP codecs communication over VPN with 3 encryption algorithms. After implementing the VPN and setting the encryption algorithm, there is a degradation of delay obtained only on the communication that is excellence (150ms). However, once the delay value becomes worse (approximately 1000ms) due to the lower bandwidth adjustment, the results show there are improvements in delay when the VPN is implemented. 3DES encryption algorithm gave the smallest impact on delay value on GSM and iLBC codec. The minimum impact of delay for G.711 (a-law) codec occurs during the usage of the Blowfish algorithm. Additional security aspects of VPN encryption did not make much impact on jitter values. The test results show the 3DES algorithm gave the smallest impact on jitter for three tested codecs. We experienced there are slight improvements in jitter values on the iLBC codec since the usage of VPN. There are improvements in packet loss when we implemented VPN on all tested encryption algorithms, especially on iLBC and G.711 a-law codecs. There are slight improvements on GSM codec on 64kbps bandwidth, still mostly test results show degradation on packet loss. Additional encryption algorithm processes and tunneling do not have a significant impact due to the QoS. There is some improvement in our research due to the usage of VPN over UDP. We are looking forward to the linkage between codec characteristics, encryption algorithms, and VPN over UDP. The QoS degradation and improvement are not significant, but it still will be better if we can get the benefits from VPN usage and also improve communication quality.

REFERENCES

[1] Olexander Tymchenko and Maxim Zayarnyuk, "Modeling of Packets Loss in VoIP Networks andMeasurement of Speech Quality," presented at the TCSET, UkraineModeling, 2008.

[2] N. Ghiata and M. Marcu, "Measurement methods for QoS in VoIP review," in *2011 3rd International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, Oct. 2011, pp. 1–6.

[3] D. Butcher, X. Li, and J. Guo, "Security Challenge and Defense in VoIP Infrastructures," *IEEE Transactions on Systems, Man and Cybernetics, Part C (Applications and Reviews)*, vol. 37, no. 6, pp. 1152–1162, Nov. 2007, doi: 10.1109/TSMCC.2007.905853.

[4] P. Gupta and V. Shmatikov, "Security Analysis of Voice-over-IP Protocols," presented at the Computer Security Foundations Symposium, 2007.

[5] W. Yang and P. Judge, "VISOR: VoIP Security Using Reputation," 2008, pp. 1489–1493, doi: 10.1109/ICC.2008.288.

[6] S. Alouneh, S. Abed, and G. Ghinea, "Security of VoIP traffic over low or limited bandwidth networks," *Security Comm. Networks*, vol. 9, no. 18, pp. 5591–5599, Dec. 2016, doi: 10.1002/sec.1719.

[7] P. C. K. Hung and M. V. Martin, "Security Issues in VOIP Applications," in *2006 Canadian Conference on Electrical and Computer Engineering*, May 2006, pp. 2361–2364, doi: 10.1109/CCECE.2006.277789.

[8] S. T. Chandel and S. Sharma, "Experimental analysis of various protocols on VoIP traffic with different CODECs in Wireless LAN," in *2016 Fifth International Conference on Eco-friendly Computing and Communication Systems (ICECCS)*, Dec. 2016, pp. 109–113, doi: 10.1109/Eco-friendly.2016.7893252.

[9] Wafaa Bou Diab and Samir Tohme, "VPN Analysis and New Perspective for Securing Voice over VPN Networks," presented at the Fourth International Conference on Networking and Services, 2008.

[10] J. M. da Silva and R. D. Lins, "Analyzing the QoS of VoIP on SIP in Java," in *2006 International Telecommunications Symposium*, Sep. 2006, pp. 576–581, doi: 10.1109/ITS.2006.4433340.

[11] S. Karapantazis and F.-N. Pavlidou, "VoIP: A comprehensive survey on a promising technology," *Computer Networks*, vol. 53, no. 12, pp. 2050–2090, Aug. 2009, doi: 10.1016/j.comnet.2009.03.010.

[12] GL Communication Inc, "VoIP Codec," *https://www.gl.com/voice-codecs.html*, Feb. 12, 2018. https://www.gl.com/voice-codecs.html.

[13] International Telecommunication Union, "Series G: Transmission Systems and Media, Digital Systems and Networks," ITU-T Rec. G.114 (05/2003), 2003.

[14] K. R. James Kurose, *Computer Networking: A Top-Down Approach, 7th Edition*, vol. 2017. Pearson.

[15] J. Prajwala, R. Mathew, and N. Taj, "Analysis of VoIP Traffic over LTE for different Codecs," in *2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, Bangalore, India, May 2018, pp. 1858–1862, doi: 10.1109/RTEICT42901.2018.9012408.

[16] ETSI, "Telecommunications and Internet ProtocolHarmonization Over Networks (TIPHON) Release 3," TR 101 329-7 V2.1.1 (2002-02).

[17] S. Andersen, Aalborg University, and A. Duric, Telio, H. Astrom, R. Hagen, W. Kleijn, J. Linden, "rfc3951," rfc3951, Dec. 2004.