Effect of Distance on Skype VoIP Communication over Wireless Network

Anas Tukur Balarabe[1], Zahriya Lawal Hassan[2]

Senior Lecturer, Sokoto State University, SoKoto, Nigeria

Abstract
The appearance of COVID-19 virus has affected many aspects of our life. These include and not limited to social, financial and economic changes. One of the most important impacts is the economic effects. Many countries have taken actions to continue the teaching process through online teaching platforms. The students are expected to graduate during the next few semesters with certificates that include some online-completed courses and their graduation certificates are called mixed certificates. This paper considers graduation mixed certificates with some online courses and its impact on graduates seeking jobs. First, we study how well the mixed certificates are accepted by job market. In other words, how different companies, organizations and even governmental entities would accept such certificates when hiring. We study the perception of job market for such certificates for different learning fields. Secondly, we study how well the online courses are accepted by the students keeping in mind that these students are used to traditional face to face teaching. Finally, we paper our results and recommendations according to the collected data from the surveys. Some of the results show that about 60% of companies do not have policies to encourage hiring graduates with mixed certificates. Also, colleges are almost divided evenly between preferring face to face and preferring online teaching.

Keywords:
Skype VoIP Communication, Wireless Network, Effect of Distance

1. Introduction

As the name implies, multimedia is a mixture of different forms of data; sound, video, text, graphic and animation. The advancement in the area of communication has reached the stage that people can share video, perform video conferencing and voice communication over the internet. Today, several applications have been developed for VoIP communication, although not all of these applications enjoyed wider acceptance by the growing number of internet subscriber, there are some that have proven to be dominant applications, a typical example of such applications is the Skype.[1, 2]

The IP network has provided the basis on which voice over IP (VoIP) service operates. This technology is growing rapidly by the day, largely because of the alternative it offers to the traditional packet switched telephone network (PSTN), in addition to the increasing access to the wireless internet and the increase in overall data transmission capacity of the internet. The flexible nature of the VoIP communication and its cost saving advantages are of course some of the factors that make it very popular [3].

But the factors that affect the performance of these two technologies are not the same. Because the internet, which is the medium through which VoIP communications are carried out was designed to provide best effort service. However, some packets; like voice packets are real time and therefore require prioritisation in order for the communication to achieve its minimum quality requirements. The fundamental issue with the best effort nature of the internet and the volatility of the communication channels, especially wireless channel; presses the need for development of some techniques that can compensate for the loss that voice packets might suffer during transmission over the internet[3, 4].

The quality of a VoIP communication is measured through delay, jitter, packet loss and sync skew. Applications which are sensitive to delay, such as VoIP do not require retransmission of lost packets and may tolerate certain amount of delay, jitter and packet lost. To achieve the required quality of service and give user a better quality of experience, compression techniques, sophisticated codecs and robust error correction mechanism need to be employed to reduce size of the packets and correct errors [3, 5].

As stated earlier, there are numerous VoIP applications available today, but in this tutorial paper, the spotlight is going to be on the Skype. After describing the application, attention will be given to its requirements and the technical solutions adopted for its implementation.

2. Overview of Skype Technology

Skype is proprietary application that was launched in the end of the 2nd quarter of the 2003. By the end of the year 2005, the company was bought by eBay and now by Microsoft. Ahti Heinla and Priit Kasesalu are brains behind this popular application. Today, there is no VoIP service that is a popular as the Skype, by the 2008 this application attracted enough users to account for 8 percent of the global long-distance call. And after a year, in 2009 there were an estimated 500 million people that are using this application [5].

Manuscript received July 5, 2026
Manuscript revised July 20, 2026
https://doi.org/10.22937/IJCSNS.2026.26.7.19

In contrast with other VoIP services, Skype does not rely on client-server architectural model, rather, it operates on a Peer-to-Peer (P2P) network overlay. The Skype network architecture contains two types of nodes namely: the ordinary node and the super node. These nodes are selected based on certain criteria; for a node to be selected as super node, it has to have enough processing power, storage capacity and network bandwidth. Ordinary node on the other hand, is any Skype application that is used for placing voice calls and messaging [1].

The super nodes play a very vital role in the Skype network overlay, they serve the purpose of the relaying calls among the users and the role of providing directory services. Because of the proxy functionality of these nodes, Skype nodes that are behind the firewalls and the gateways can setup peer-to-peer calls devoid of any distinct arrangements [5].

Another integral component of the Skype network overlay is the Skype login server, the login server is not a Skype node, rather a very important part of the network that holds the login details of the Skype users. Therefore, to establish a Skype connection, an ordinary node needs to make connection to the Skype super node and register with the login server. The server does not only serve the function of storing the user login details, but also perform the function of authenticating the user login. In addition, this server also ensures that Skype login details are unique to each user in the Skype name space [1]

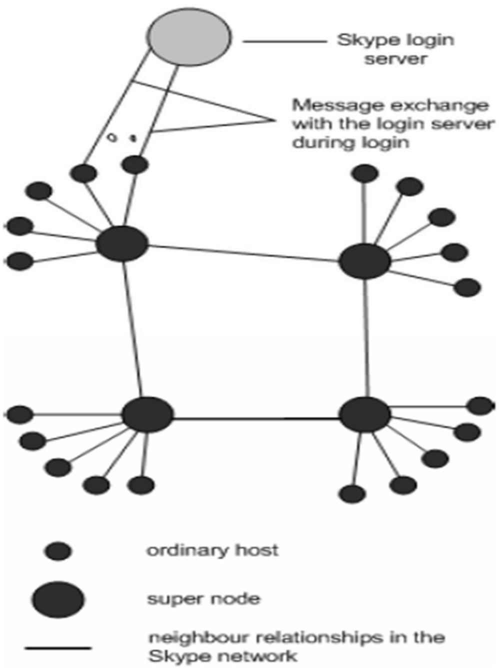

Figure I. Skype Network Architecture [1]

The login server is the only central entity in the Skype network. This implies that user information and search queries are distributed and stored in the Skype network. Skype enjoys it wider acceptance because of the high degree of voice quality it offers, compared to other VoIP applications [1, 5].

Skype has some rather unique features that make it stand out of the rest of the VoIP applications, these features attracted a lot of attention of mobile service and network operators. Unlike other voice over IP applications, Skype uses sophisticated cryptographic techniques; making it impossible to intercept and decrypt its traffic. Furthermore, Skype can pass through firewalls, thus avoiding being blocked by the firewall rule [6]

Apart from the ability of the Skype to traverse firewall and the NAT, this application has unique additional functionalities that further distinguishes it from other VoIP applications. With SkypeOut, a Skype client can make calls to landlines and mobiles phones, receives calls and voicemail messages and perform video calls with SkypeIn. In addition, As specified on the Skype official website, the application has eight call features, two video calls feature, six messaging features, four file sharing features and a list of other features including a feature that allows clients to connect to Skype WiFi at over 2 000 000 public hotspots worldwide and another feature that allows voice, video and instant messaging translation between clients that do not speak similar language. [7, 8] The following sections give highlight of the components of the Skype application.

3. Components of the Skype Software

To establish a connection, a Skype user monitors a specific ports for incoming calls, uses host cache to preserve a list of other skype nodes, it also does the maintenance in addition to encryption of messages and determining either it is behind a firewall or a NAT [1].

3.1 Ports

Skype employs TCP and UDP protocols to transport data packets. Usually a Skype node usually listens to three ports that are configured in the node's configuration dialog box. The node selects a random number during the process of installation. Moreover, two more listening ports are opened by the SC, one at port 80 (HTTP port), and port 443 (HTTPS port). Different form the other internet protocols, such as SIP and HTTP, there is no default TCP or UDP listening port. In order to capture the Skype VoIP traffic in correctly, a new port number needs to be assigned through which the incoming traffic could be captured [6].

3.2 Host Cache

Since the Skype operates on a peer-to-peer network overlay, there is no centralised system that stores the super nodes IP address and the Skype clients port numbers, that are used for communication between Skype clients. Therefore, a host cache (HC) is used, this important component of Skype contains the super node IP address and the port pairs that Skype node builds and refreshes periodically. The host caches is never empty, it most contain at least one record of an active Skype node. This record typically contains the IP address and the port number of this active node. Each Skype client stores host cache in its windows registry, the host cache can contain a maximum of 200 entries. In some cases a different P2P protocol uses a finger table for quick searching of a node. [1, 9]

3.3 Codec

For multimedia applications, minimum bit rate and high quality of audio or video are very important qualities. This can only be achieved with a good codec, a codec is an integral part of a multimedia system that compressed and decompresses a video or audio file. Thereby reducing its bit rate, storage space requirement while maintaining its quality. One of the fascinating features of the Skype application that makes it popular today is the quality of its voice calls, this can undoubtedly be attributed to the sophistication and efficiency of the codec use by the application. [2, 5, 9]

Presently, the available version of Skype uses an internally developed codec called code SILK code. The SILK codec has brought tremendous success to the Skype application, it substituted all other codecs such as, iLBC, ISAC and SVOC. SILK is a very robust and efficient speech and audio codec and has the ability to adapt to the changes in the network by adjusting its sampling rate and compression rate and complexity. The ability of SILK to adjust its sampling and compression rates to match the network condition at any given time makes it a unique codec among the myriad of codecs available. SILK has been designed to support four different distinct modes that exist within the range of 8000 Hz and 24000 Hz sampling rate. Skype proposes that devices cannot support higher sampling rate as well as the packet switch telephony network (PSTN) should be interfaced to with the narrow band mode. On the other hand, IP platforms that has no support for sampling frequency greater than 16×10^3 Hz could be interfaced to with wideband mode. While mediumband (MB) and Super wideband should be used to interface with lower end node and platforms that have the provision for supporting 24×10^3 Hz or more, respectively. In its three years of introduction and incorporation into the Skype software, SILK has been used for serving more 750 billion Skype-to-Skype minutes.[8, 10, 11].

Despite all its huge success story, SILK is certainly not the future codec for Skype. Because the company has since started developing a new codec call Opus, which they intend to develop and standardise for use over the internet. The draft for this new codec has since been submitted to the IETF. As part of the new revolution, Skype revealed that Opus is an adaptable codec with greater efficiency, smartness that can work across exceptional range of bitrates, sampling rates and frame sizes. Opus will have the ability to support seamless handover between different technologies (e.g 3G to WiFi). As a matter of fact the company is working towards a future where Skype clients will perform voice communication over Skype with CD quality.[8]

3.4 Buddy List

Skype uses another feature call buddy list to keep offline users updated with what is happening in the group that they are members. Buddy list data is stored in the OS registry. It is protected with digital signature and strong encryption. Because Skype operates on P2P network architecture, the buddy list is stored locally on each machine. As a result, reconstruction of the buddy list is necessary whenever a user uses Skype client n a different machine to log into the Skype network. [1]

3.5 Encryption

To provide security for user data, voice and video traffic there is need for using an encryption technique that ensure protection of such data. Skype uses a number of cryptographic techniques to provide protection for text, voice and video traffic. According to [12], the cryptographic techniques used by Skype are: AES block Cipher, RSA public key cryptosystem, ISO 9796-2 signature padding scheme, SHA-1 function and RC4 stream cipher. The advanced encryption standard or Rijndel is a very strong encryption technique and is used by American Government organisations for protection of delicate information. Skype employs 256-bit encryption, with a total of 1.1×10^7 keys combination, to dynamically encrypt the data in every Skype call or instant message. Skype authenticate user public keys at the Skype login server with 1536-2048 symmetric keys.[1, 9, 12]

3.6 Skype Error Correction Mechanism

Voice or video communication over a network might encounter some errors, especially if it is over a wireless network, which is very unpredictable. Therefore, it is important to use appropriate error correction schemes that can mitigate the effect of the errors. Error correction mechanisms such as Automatic Repeat Request (ARQ) might not be suitable for bidirectional communication such as VOIP and video telephony, because of the issues of delay and increase overhead. Skype employs forward error correction technique for lost packets recovery, this technique adds redundant bits to the voice data stream. In a research conducted by [13], the authors conducted and experiment in which they induced packet losses in multi-party conferencing using Skype. They observed that there were not retransmission of lost packets, the authors noticed some gaps between the total transmission rates and the video rates. The authors concluded that Skype uses robust Forward Error Correction technique for VoIP and two-party video calls.[1, 13, 14]

3.7 NAT and Firewall

One of the most important traits of Skype is its ability to circumvent firewall and traverse NAT. Determination of Nat and firewall is performed at the transport layer by the Skype. Through this process, NAT settings behind which the SC resides are determined. It is widely hypothesise that Skype client sues a variant of a protocol STUN and TURN to figure out the nature of firewall and NAT use in the network where the SC resides. By using its peer relay, Skype connects clients that are behind NAT, it also uses TCP tunnel to a peer relay to traverse firewall that do not allow UDP to pass through them. [1, 15]

4. Skype Function

4.1 Start-up Function

When a Skype client is ready to go online after successful installation, the SC sends a HTTP 1.1 GET request containing the keyword 'installed'. Subsequently, when the SC attempts to connect it only sends the same GET request to the Skype server with a different keyword requesting for a latest version if there is any available. [1]

4.2 Login Procedure

Login function is undoubtedly the key step in Skype operation. For a Skype client to successfully log in, it has to provide a valid username and password, which are validated by the Skype login server. After passing through the process of authentication by the login server, the SC then goes on to advertise its presence to peers and to the other SCs on its buddy list, determine the nature of NAT and firewall use in the network in which the SC resides before finally discovering other active Skype nodes that have public IP address.[1, 9]

4.3 User Search

As discussed in the introduction, Skype does not have any central entity except the login server. To search for user in the network Skype has a technique, the Global index technology for searching for users. According to [1], Skype confirms that search for user is not centralised and it can find an existing user who logged in the last 72 hours. The research conducted by [1] corroborated with the claim.

4.4 Call Establishment and Teardown

Skype typically employs UDP for voice streams and TCP for exchange of control signals [2]. Baset and Schulzrinne, 2004 analysed the Skype protocol, they used three networks set up and studied the mechanisms used by the SC in establishing connection. In the first set up where the caller and callee were using public IP address, the caller's SC connects to the callee's SC by establishing TCP handshake with the callee's SC. They discovered that during the process of establishing the call, the caller also sent messages over UDP to alternative online Skype nodes, which it detect in the process of login. In another setup, where the callee is port-blocking NAT and the callee was using public IP, the authors discovered that there was not direct flow of traffic between the caller and the callee. Rather, other active Skype node was used as relay by the caller to channel signalling packets over TCP. The intermediary node then forwardes the information to the callee. This node also served as the relay of audio streams over UDP between the caller and the callee and vice versa.

Baset and Schulzrinne, 2004, discovered that it takes more time to establish connection to users that are not in a SC buddy list than it takes to establish with those already in the list. The increased delay is as result of the time it takes for the SC to do user search before finally sending the signal. For the call parties that are both on Public IP or behind NAT, call termination signal is exchanged the TCP [1].

5. Review of Related Work

In a related work carried out by Asiri and Sun, 2013 the performance of skype voice called was analysed. The authors used Wireshark to capture Skype traffic under different network conditions and then measure the QoS parameters of their interest. They studied how the then version of Skype (in 2013) under diverse packet loss ration make adjustment to payload size, inter arrival time and throughput. The authors discovered that Skype uses categorised congestion control algorithm to improve the quality of voice calls under different rates of packet loss. Three categories were identified by the authors, the first category algorithm is used when the range of packet loss is between 0% and 10%. When the loss ratio increase to 10%-14%, a different congestion control algorithm that works in the same manner as the TCP congestion window was adopted. Finally, when the loos increases to from 14% to 20%, Skype uses its third category algorithm to mitigate the effect of the loss.

The objective Mean Opinion Score measurementIII. corroborated with the subjective test, Asiri and Sun, 2013,IV. found out that the performance of the of the Skype voice call deteriorated with the increase in packet loss.

Zhang *et al*., 2012 did a research where they studied Skype rate control and video Quality, the authors used the network emulator to induced random packet losses in the network. They used three different amount of network bandwidth, it was observed that the Skype is can withstand insignificant packet loss and propagation delays. However, when the network condition degraded the Skype reduced the rate at which packets are sent.

6. Experiment Setup and Result Analysis

The experiment is divided into two sections, the first section is the Cisco Packet Tracer implementation of VOIP. The second section describes the methodology followed in setting up the Skype call capturing the packets and analysis of the result.

6.1 Traffic Capture Procedure

In order to capture the traffic and successfully analysed it based on the selected QoS parameter, which is delay in this case. Wireshark will be used to capture Skype voice traffic at four successive distances (10M, 20M, 30M and 40M). To this the following tools will be used:

- Wireless Access Point for accessing the internet (Router)
- Two Laptops with Skype Client for voice traffic generation

I. - Wireshark Software for capturing packets

II. - Measuring Tape to measure distance from the access Point

- Three volunteers for subjective measurement (MOS)

6.2 Objective Measurement

Depending on the number of devices that are connected to an access point and the type of application they are using, different traffic will be captured by the Wireshark. This can make the analysis of the voice packet, which are mainly transmitted over UDP very difficult. To avoid this problem, the IP address of the two laptops were obtained by using ***ipconfig*** command in the command prompt. In this case the two IP address are 192.168.0.6 and 192.168.0.2.

After getting the IP address distance were measured and demarcated in the space of 10M, 20M, 30M, and 40M. Then the volunteers were informed on how to score each call, from 1 to 5. The best quality takes 5, good takes 4, fair takes 3, poor takes 2 and bad takes 1. The filter below was applied to the Wireshark in order to capture only UDP traffic exchanged by the two laptops.

((ip.src==192.168.0.6&&ip.dst==192.168.0.2)|| ip.dst==192.168.0.6&&ip.src==192.168.0.2))& & (udp)

To ensure equal amount of time is spent during each measurement, the two communication parties counted 1, 2, 3, 4, 5 with some short silent in between during each measurement. The link capture is then stopped in the line is dropped, the capture files are then saved.

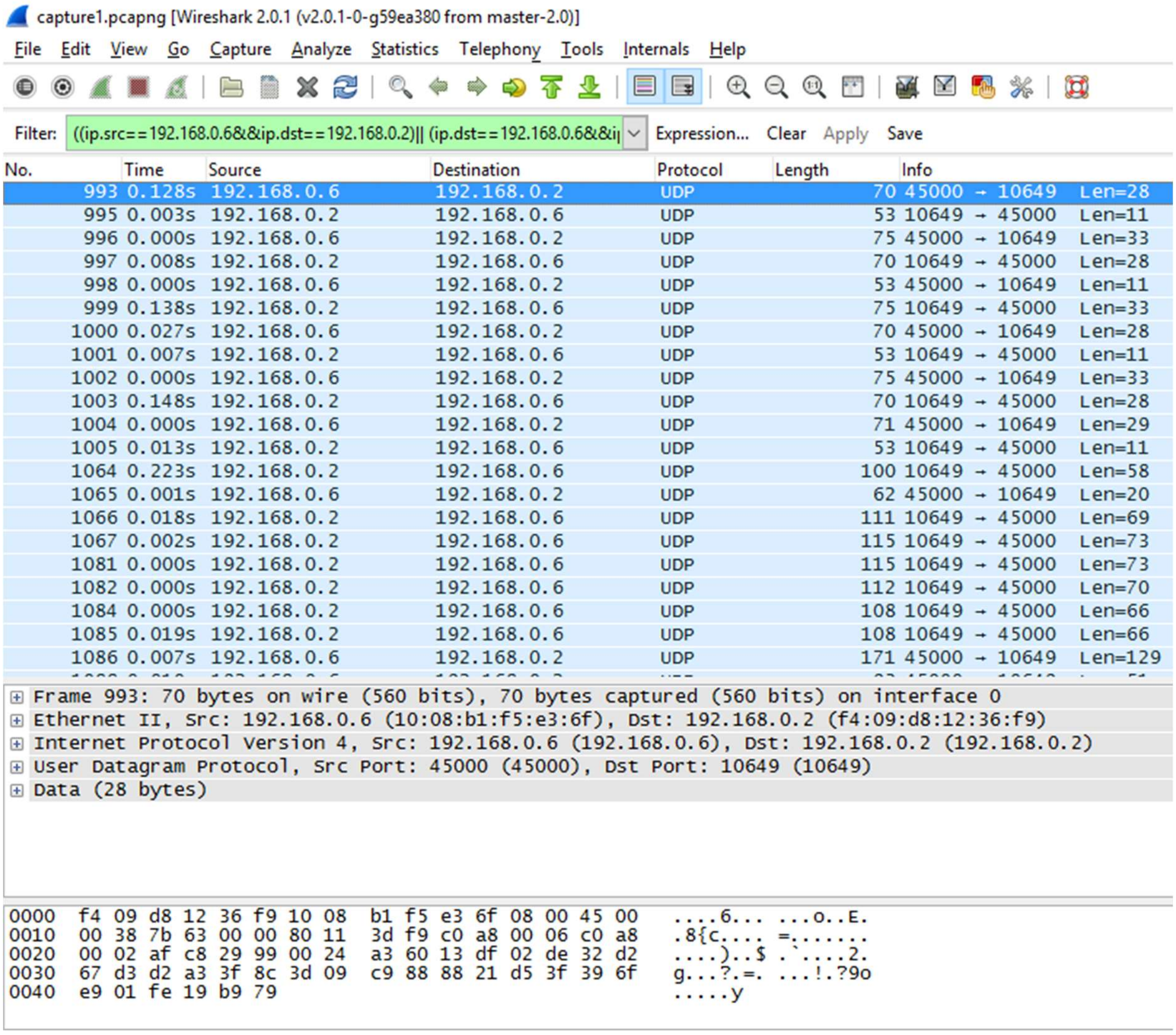

Figure 5: Snapshot of First Capture

The captured file were then stored as text files and later imported into the MS Excel to compute the average the delay of each capture.

Manuscript received July 5, 2026
Manuscript revised July 20, 2026
https://doi.org/10.22937/IJCSNS.2026.26.7.19

capture11 - Notepad

File Edit Format View Help

No.	Time	Source	Destination	Protocol	Length	Info	
993	0.128s	192.168.0.6	192.168.0.2	UDP	70	45000 → 10649	Len=28
995	0.003s	192.168.0.2	192.168.0.6	UDP	53	10649 → 45000	Len=11
996	0.000s	192.168.0.6	192.168.0.2	UDP	75	45000 → 10649	Len=33
997	0.008s	192.168.0.2	192.168.0.6	UDP	70	10649 → 45000	Len=28
998	0.000s	192.168.0.6	192.168.0.2	UDP	53	45000 → 10649	Len=11
999	0.138s	192.168.0.2	192.168.0.6	UDP	75	10649 → 45000	Len=33
1000	0.027s	192.168.0.6	192.168.0.2	UDP	70	45000 → 10649	Len=28
1001	0.007s	192.168.0.2	192.168.0.6	UDP	53	10649 → 45000	Len=11
1002	0.000s	192.168.0.6	192.168.0.2	UDP	75	45000 → 10649	Len=33
1003	0.148s	192.168.0.2	192.168.0.6	UDP	70	10649 → 45000	Len=28
1004	0.000s	192.168.0.6	192.168.0.2	UDP	71	45000 → 10649	Len=29
1005	0.013s	192.168.0.2	192.168.0.6	UDP	53	10649 → 45000	Len=11
1064	0.223s	192.168.0.2	192.168.0.6	UDP	100	10649 → 45000	Len=58
1065	0.001s	192.168.0.6	192.168.0.2	UDP	62	45000 → 10649	Len=20
1066	0.018s	192.168.0.2	192.168.0.6	UDP	111	10649 → 45000	Len=69
1067	0.002s	192.168.0.2	192.168.0.6	UDP	115	10649 → 45000	Len=73
1081	0.000s	192.168.0.2	192.168.0.6	UDP	115	10649 → 45000	Len=73
1082	0.000s	192.168.0.2	192.168.0.6	UDP	112	10649 → 45000	Len=70
1084	0.000s	192.168.0.2	192.168.0.6	UDP	108	10649 → 45000	Len=66
1085	0.019s	192.168.0.2	192.168.0.6	UDP	108	10649 → 45000	Len=66
1086	0.007s	192.168.0.6	192.168.0.2	UDP	171	45000 → 10649	Len=12
1088	0.010s	192.168.0.6	192.168.0.2	UDP	93	45000 → 10649	Len=51
1090	0.001s	192.168.0.6	192.168.0.2	UDP	94	45000 → 10649	Len=52

Figure 6: Snapshot of txt file of Wireshark Trace File

I	J	K	L	M	N	O	P	Q	R	S	T
	Time		Source	Desti	atio	Prot	Le	gth	I	fo	
993	0.128	s	192.168.0.6	192.168.0.2	UDP	70	45000	→	10649	Le	28
995	0.003	s	192.168.0.2	192.168.0.6	UDP	53	10649	→	45000	Le	11
996	0.000	s	192.168.0.6	192.168.0.2	UDP	75	45000	→	10649	Le	33
997	0.008	s	192.168.0.2	192.168.0.6	UDP	70	10649	→	45000	Le	28
998	0.000	s	192.168.0.6	192.168.0.2	UDP	53	45000	→	10649	Le	11
999	0.138	s	192.168.0.2	192.168.0.6	UDP	75	10649	→	45000	Le	33
1000	0.027	s	192.168.0.6	192.168.0.2	UDP	70	45000	→	10649	Le	28
1001	0.007	s	192.168.0.2	192.168.0.6	UDP	53	10649	→	45000	Le	11
1002	0.000	s	192.168.0.6	192.168.0.2	UDP	75	45000	→	10649	Le	33
1003	0.148	s	192.168.0.2	192.168.0.6	UDP	70	10649	→	45000	Le	28
1004	0.000	s	192.168.0.6	192.168.0.2	UDP	71	45000	→	10649	Le	29
1005	0.013	s	192.168.0.2	192.168.0.6	UDP	53	10649	→	45000	Le	11
1064	0.223	s	192.168.0.2	192.168.0.6	UDP	100	10649	→	45000	Le	58
1065	0.001	s	192.168.0.6	192.168.0.2	UDP	62	45000	→	10649	Le	20
1066	0.018	s	192.168.0.2	192.168.0.6	UDP	111	10649	→	45000	Le	69
1067	0.002	s	192.168.0.2	192.168.0.6	UDP	115	10649	→	45000	Le	73
1081	0.000	s	192.168.0.2	192.168.0.6	UDP	115	10649	→	45000	Le	73
1082	0.000	s	192.168.0.2	192.168.0.6	UDP	112	10649	→	45000	Le	70
1084	0.000	s	192.168.0.2	192.168.0.6	UDP	108	10649	→	45000	Le	66
1085	0.019	s	192.168.0.2	192.168.0.6	UDP	108	10649	→	45000	Le	66

Figure 7: Snapshot of Wireshark Trace File in MS Excel

Table 1: Delay for each Measurement

Measurement	Distance (M)	Delay (ms)
1	10	0.01409
2	20	0.02794235
3	30	0.033424242
4	40	0.071642857

Manuscript received July 5, 2026
Manuscript revised July 20, 2026
https://doi.org/10.22937/IJCSNS.2026.26.7.19

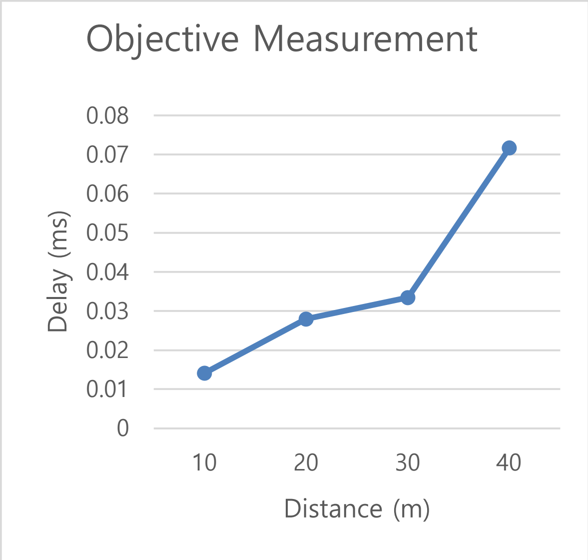

Figure 8: Graph of Delay (ms) vs Distance (m)

Table 1 and the graph above show the delay per distance, it is clear that as the distance increases the delay increases. Therefore, the quality of voice communication deteriorates as we move further away from the access point.

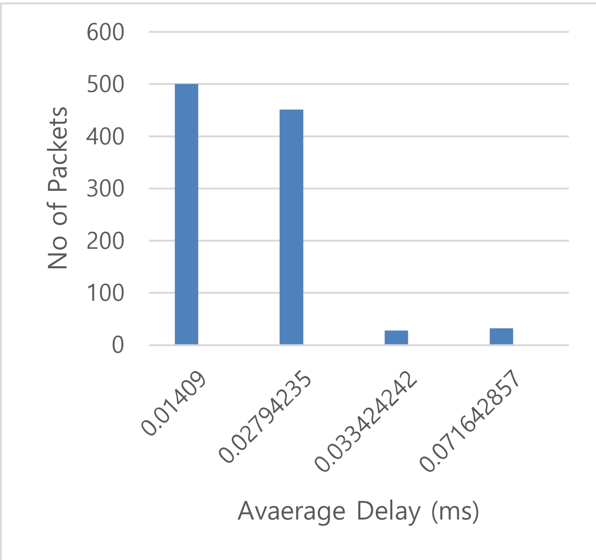

Figure 9: Graph of packets and average delay

It can also be observed from the figure 9 above, that the more packets were received when the close to the access point. This implies that there were not packets drop due to delay, reduction in throughput or other impairment.

6.3 Subjective Measurement

Subjective measurement needs to be carried out in a controlled environment. However, the environment in which this experiment was carried out not controlled. There was interference, deflection, reflection and scattering of the signal by wall and other objects that came between the computer and the access point. Despite that the volunteers were able to grade the quality of voice for at each distance. One of the constraints in this experiment is the approximation made during the distance measurement at certain points, because of the walls.

Table 2 and the figure 10 below show the MOS values for the four measurements, it verified the result of objective measurement. The volunteers observed that as we move away from access point, the quality of communication drops down.

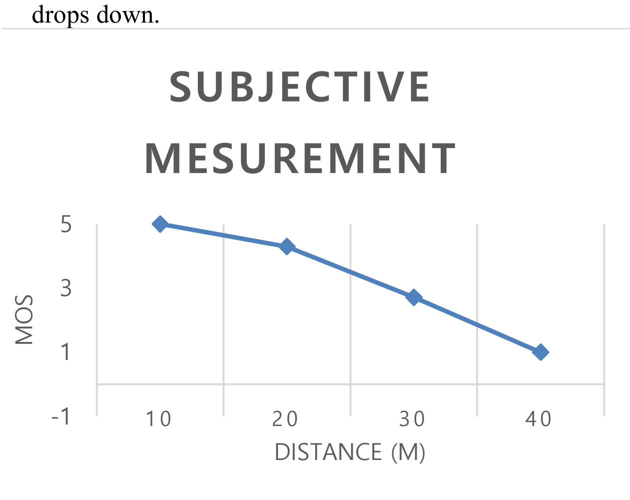

Figure 10: MOS against Distance

Table 2: MOS for the Calls

Measurement	Volunteer 1	Volunteer 2	Volunteer 3	Average
10	5	5	5	5
20	4	5	4	4.3
30	2	3	3	2.71
40	1	1	1	1

5 Conclusion

Conclusively, it has been observed that distance from the access point affects the quality of communication by increasing the delay of packets arrival and reducing the quality of the communication significantly. Thus, it is safe to conclude that the more the distance from the access point, the more the delay and the number of packets dropped. This affects both QoS as indicated by the increase in the delay and the QoE as indicated by the MOS given by the volunteers.

References

[1] S. A. Baset and H. Schulzrinne, "An analysis of the skype peer-to-peer internet telephony protocol," *arXiv Preprint Cs/0412017,* 2004.

[2] Z. Li, M. S. Drew and J. Liu, *Fundamentals of Multimedia.* Springer, 2004.

[3] W. Chiang, W. Xiao and C. Chou, "A performance study of voip applications: Msn vs. skype," *Proceedings of MULTICOMM,* pp. 13-18, 2006.

[4] M. Arranz and C. Aurello, "IP Telephony: Peer-to-peer versus SIP," 2005.

[5] T. Huang, P. Huang, K. Chen and P. Wang, "Could Skype be more satisfying? a QoE-centric study of the FEC mechanism in an internet-scale VoIP system," *Network, IEEE,* vol. 24, pp. 42-48, 2010.

[6] T. Sinam, I. T. Singh, P. Lamabam, N. N. Devi and S. Nandi, "A technique for classification of VoIP flows in UDP media streams using VoIP signalling traffic," in *Advance Computing Conference (IACC), 2014 IEEE International,* 2014, pp. 354-359.

[7] T. Sinam, I. T. Singh, P. Lamabam and N. Ngasham, "An efficient technique for detecting skype flows in udp media streams," in *Advanced Networks and Telecommuncations Systems (ANTS), 2013 IEEE International Conference On,* 2013, pp. 1-6.

[8] (). *Skype and a New Audio Codec*.

[9] L. Ptácek, "Analysis and detection of Skype network traffic," *Masaryk University Faculty of Informatics, Master Thesis, Brno, Czech Republic, Spring,* 2011.

[10] M. Goudarzi, L. Sun and E. Ifeachor, "Modelling speech quality for nb and wb silk codec for voip applications," in *Next Generation Mobile Applications, Services and Technologies (NGMAST), 2011 5th International Conference On,* 2011, pp. 42-47.

[11] K. Vos, S. Jensen and K. Soerensen, "Silk speech codec," *IETF Standards Track Internet-Draft,* 2009.

[12] R. F. Rights, "SANS Institute InfoSec Reading Room," *Risk,* vol. 1, pp. 27, 2001.

[13] Y. Xu, C. Yu, J. Li and Y. Liu, "Video telephony for end-consumers: Measurement study of google , iChat, and skype," in *Proceedings of the 2012 ACM Conference on Internet Measurement Conference,* 2012, pp. 371-384.

[14] W. Lizhong, W. Muqing, W. Lulu and L. Mojia, "An adaptive forward error control method for voice communication," in *2010 International Conference on Networking and Digital Society,* 2010, pp. 186-189.

[15] H. Wang, "Skype VoIP service-architecture and comparison," in *INFOTECH Seminar Advanced Communication Services (ASC),* 2005, pp. 4.