University of Sindh Journal of Information and Communication Technology
(USJICT)
Volume 5, Issue 1, March 2021

ISSN-E: 2523-1235, ISSN-P: 2521-5582
Website: http://sujo.usindh.edu.pk/index.php/USJICT/

Invite Internet Users to Honeynet Security to Improve VoIP Streaming Services

Muhammad Faisal Shaikh[1], Pinial K. Butt[1], Bisharat Rasool Memon[2],
Zulfikar Ahmed Maher[1], Ghulam Mujtaba Khushk[1]

[1]Information Technology Centre, Sindh Agriculture University, Tandojam, Pakistan
[2]Department of Information Technology, University of Sindh, Jamshoro, Pakistan
E-mail: muhammad.faisal@admin.muet.edu.pk, pinial@sau.edu.pk, zamaher@gmail.com,
khushk.ghulammujtaba@gmail.com

Abstract: Several challenges have been identified in security and quality of service in VoIP based communications, and a number of studies have been conducted in this context, including IPSec security on VoIP, VoIP Honeypot architecture, and on the issue of cryptography techniques adopted for secure transmission of information streams over the network. However, it is inherently hard for network communication security to be perfect or be guaranteed at 100% level. For the time being we can aim to minimize or mitigate security threats but at the same time as the technology changes and as new areas for network communication are being developed, there are new threats that are also having a potential impact on the security on quality of service. Researchers have applied different patterns, techniques, and scenarios to prevent some specific threats and adopted security frameworks for securing VoIP communication. However, there is a dearth of studies which analyze the impact of Honeynet security on VoIP streaming communication. In this research, we have analyzed the quality of service of VoIP streaming communication under the application of a Honeynet security framework.

Keywords: ATA Analog Telephone Adapter; QoS Quality of Service; SIP Session Initiation Protocol

I. Introduction

Voice over Internet Protocol (VoIP) has been a rapidly growing technology due to the convergence, with minimum costs and less configuration, of voice and data traffic over the current networks.

People have been trying to connect and communicate in every possible way in the modern hectic environment, making use of technologies and platforms such as, smartphones, pagers, video conferencing, voice calls, instant messaging and email, plus mobile computers, personal digital assistants (PDAs). At the same time, these technologies are also helping the enterprises to be faster, more competitive, and more open.

Some pioneers began selling PC-to-phone and phone-to-phone VoIP applications since 1998 [1]. Voice over IP design requires specific hardware to provide the service at each site on both ends of network devices Siemens, Cisco, Avaya, Alcatel-Lucent, Nortel and Mitel will do so in order to accomplish the removal of conventional PBX systems and IP switching technologies based on their ability. The only device driver is an IP solution. A Voice over IP or IP telephony is a solution that only uses a telephone service over IP rather than a PBX system [2].

The Internet as a network is highly shielded by various networking equipment, such as routers, firewalls, IPS, IDS, DMZ, proxy servers, Honeynet, and many more. Honeynet is a security architecture or framework used as the intrusion detection/prevision device can be viewed as part of it [3]. By building a fake area inside the actual world, any security breaches or break-in attempts will be diverted to this honey region when any malicious activity is detected, and we can find who is attempting to hack and how [3, 4].

The configuration of a Honeynet is deliberately vulnerable. The key goal is to allow hackers to target the infrastructure so that it is possible to track hacking operations and to research their techniques and trends. For IT professionals to secure the intranet of a real organization, knowledge of Honeynet infrastructure may be useful. Honeypots can function to some degree as a lightweight intrusion-detection method to deflect hackers from targeting a real intranet and its infrastructure, a Honeynet is often used. Their interest could be distracted until hackers felt they had what they wanted.

The rest of the paper is structured as follows: In Section II, we present the related work, discussing results from relevant literature. Section III describes the experimental setup adopted in this study, including the various QoS parameters of VoIP streaming communication. Section IV presents and discussed the results from the real physical Honeynet framework setup that was adopted in this study. Finally, Section V concludes the paper and provides some directions for future work.

II. Related Work

There have been several studies to compare the performance of VoIP communication in various network topologies, such as ring, bus, and star. For example, there are several advantages and disadvantages to each of these topologies, and therefore, to find out which topology will enforce VoIP optimally a study is required [5]. Researchers have introduced VoIP in multiple topologies and efficiency tests were done for each topology.

The impact of SIP call control signaling on QoE for Voice over Internet Protocol (VoIP) service signaling has also been analyzed. It has been investigated whether SIP call control signaling load has an impact on the human perception of SIP signaling, the underlying QoE performance and to identify the significance of separate SIP-based performance metrics for signaling performance [6]. In addition, their intention was to determine whether the SIP call control signaling load alters its effect if the previously proposed algorithm for differentiated SIP message handling is activated and quantify mutual relationships of considered user perceptions and QoE.

Another study that analyses the factors of providing confidentiality, integrity and authentication is the context of network security is [7] which show that VoIP data can be protected by IPSec encryption as it moves around the network. When someone break or bypass security limits and try to disturb VoIP communication, the encrypted content will not be decipherable. VoIP communications can be made safer by IPSec. While IPsec is a prevalent protection software in VoIP security. However, because of the added overheads involved with IPSec, it affects VoIP performance.

Security in VoIP communication systems is especially problematic with respect to specify types of attacks when VoIP is implemented on a large scale. For example, analyzing reliability and security of VoIP communication systems and have proposed the solution of VPN in VoIP to overcome these challenges [8]. In the architecture they have proposed, the fundamental functionality of VoIP is established during the transmitting of packets. VoIP nodes first send their packets to the IPBX server, then it routes the packet to the targeted client. The Virtual Private Network offers secure communication to the VoIP services, and it safely routes the encrypted voice packets into a VPN tube. Another VoIP user decodes the speech at the remote site and transforms the digital voice to an analog signal for transmission to the handset.

Some key threats to VoIP calls are identified by [9], which include spoofing or identity theft and call redirection, making the integrity of data a major risk. Authentication is first implemented in this security framework to authenticate the true user with his voice, and then cryptography techniques are used to securely transmit the stream of information over the network. Cryptography offers high and adjustable levels of security, biometrics does not repudiate it, and eliminates the need to remember passwords. In cryptographic, biometric cryptosystems, a key is generated so that the key cannot be disclosed without biometric authentication being effective from the biometric template of the user stored in the database.

Another study has developed three different patterns for VoIP implementation related to specific security issues [6], namely (i) secure negotiation of NATs and firewalls, (ii) identifying DDoS attacks, and (iii) eavesdropping. In first pattern they describe the ad-hoc but efficient strategies used by most VoIP vendors to bypass firewalls and NATs. The second pattern describe how to keep “Man-in-the-Middle” attacks from disrupting VoIP connections. Finally, the third pattern, describes how to protect VoIP against eavesdropping.

There are a few studies such as [10—14] which have demonstrated VoIP quality analysis from two common 3G and 4G social network technologies, covering both fixed and mobility. 4G was found to have no greater VoIP performance than 3G., based on stationary studies, while 4G's downlink speed is faster than 3G by around 5-7 times. However, it can be seen, based on mobility testing called semi-dynamic tests, that 4G simply offers better VoIP efficiency than 3G.

A few studies have analyzed quality of service of VoIP communications on such social networking platforms Skype, GoogleTalk, Windows Live, Yahoo Messenger, etc. [2, 16—19]. However, these are mostly stationary tests and semi-dynamic tests using the SILK codec and LINE using a proprietary codec.

III. Experimental Setup

The proposed system diagram for experimental setup is shown in Fig. 1. It is a real-life setup involving a campus network, contains VoIP Server, Honeynet firewall, wired and wireless VoIP users, and IP Phones.

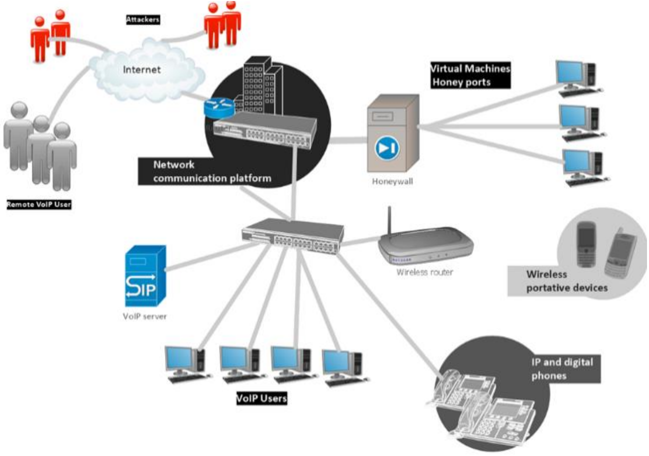


Figure 1. System diagram.

A. Method of Implementation

Overall, we carry out an experimental approach that spans over multiple stages. We start by the installation of VoIP server and its configuration and subsequently testing is carried out. Next step is to carry out the installation and configuration of Honeynet security framework.

In the last phase, analyses of the results and measurement of various QoS parameters which affects VoIP quality are carried out. These are described later in this section, and included sample rate, bitrate, bandwidth, jitter and lag.

B. Honeynet setup and configuration

The classification of Honeynet can also be based on its method of implementation: physical and virtual honeypots. On another system, physical honeypots are hosted and have no unique IP address. They are challenging to deploy and maintain; they are often time exhaustive and expensive. There is also a great deal of administrative work to be done to ensure proper security and tracking. Virtual honeypots do not require the implementation of additional computer systems; they can be hosted on another machine. It is easier to populate the network, inexpensive and less time consuming.

For our Honeynet setup we used an open-source solution called Glastopf which is primarily a low-interaction network emulator. As per recommended practice, the honeypot is placed in the DMZ of the network, such that, it is out of the main network but it is still behind a router and provides an interface to the Internet. This makes the honeypot effective so that any malicious traffic passes through the firewall and is trapped by the honeypot.

C. *VoIP Codecs*

In order to achieve VoIP best quality we need to select from a number of common VoIP codecs. A good understanding of codecs will help us to select best codec for a particular setup and configuration combination. Table 1 lists out and briefly describes the common VoIP codes. A codec is prospect that transforms an audio signal (own voice) for communication into a compressed digital format (VoIP) and returns it for re-execution to an uncompressed audio signal.

TABLE I. COMMON VOIP CODECS, THE TABLE SHOWS THE DIFFERENT CODECS USED IN VOIP PBX FOR VIDEO AND AUDIO.

Codec	Bandwidth/Kbps	Comments
G.711	64	Distribute accurate audio transmission. Processor requirements are very low. Bidirectional requires over 128 kbps
G.722	48/56/64	Adjusted to fluctuating compression, bandwidth is kept with network jamming.
G.723.1	5.3/6.3	Great compression with high quality voice. Can use with dial-up. High processor power.
G.726	16/24/32/40	Upgrade version of G.721 and G.723 (diversified from G.723.1)
G.729	8	Excellent bandwidth consumption. Inaccurate tolerance. A license is required.
GSM	13	Free access is available on many hardware and soft- ware platforms. The same encoding is used for GSM mobile phones (Enhanced version is being used fre- quently at the present time

D. *VoIP Protocols*

There are several protocols used to provide VoIP facilities. H.323 is a standard defined by the ITU to allow user of PSTN network to talk with the VoIP network user. H.323 standard used different protocols for different task as given below:

- H.255: It used for the call signaling.
- Q.931: It used also used call signaling but rented from the ISDN.
- H.245: It used for the purpose of authentication and security.
- Real Time Transfer Protocol (RTP): RTP carries the data of real time communication.
- H.450.x: It is used for the extra services like follow me, call transfer etc.

E. *Measures of Voice Quality*

To many organizations today, a stable VoIP setup has become critical. Fidelity is the backbone of outstanding corporate correspondence, which is why audio fidelity on the telephone is a big concern. These are some audio terminologies in which the quality of voice is dependent.

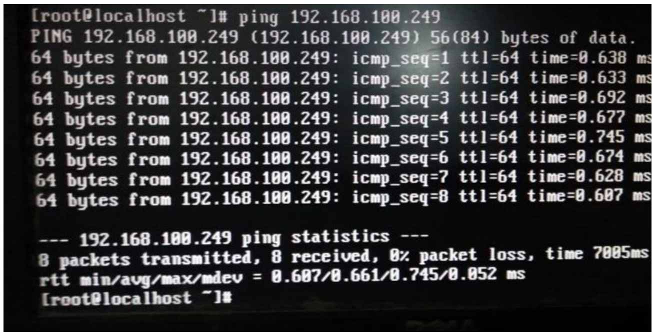
Sample Rate: It corresponds to the audio samples taken per second, often referred to as sample frequency. Each independent measurement will tell you the overall amplitude value of the signal waveform for a given duration. The larger the sampling rate, the higher the quality of the recording.

Bitrate: Speed of encoding (compressed) digital audio and video files, measured in kilobits (Kb) and megabits (Mb) per second. Higher bitrate implies better sound quality.

Bandwidth: While bandwidth defines the maximum data transmission of network or internet. It calculates how much information can be transmitted in each period over a particular connection.

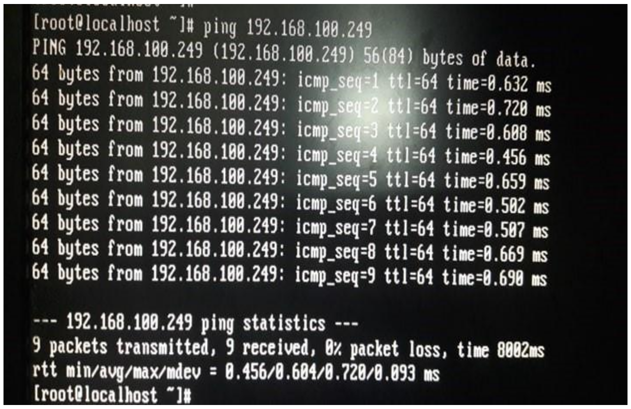
IV. EXPERIMENTAL RESULTS

This research is not on a test bench; it is a real physical setup of VoIP and Honeynet configuration as shown in Fig. 1 to investigate the impact of Honeynet security framework on VoIP quality. There are some parameters like packet loss, jitter, latency which we have measured before applying Honeynet security with the help of ping utility, Wireshark.



```
[root@localhost ~]# ping 192.168.100.249
PING 192.168.100.249 (192.168.100.249) 56(84) bytes of data.
64 bytes from 192.168.100.249: icmp_seq=1 ttl=64 time=0.638 ms
64 bytes from 192.168.100.249: icmp_seq=2 ttl=64 time=0.633 ms
64 bytes from 192.168.100.249: icmp_seq=3 ttl=64 time=0.692 ms
64 bytes from 192.168.100.249: icmp_seq=4 ttl=64 time=0.677 ms
64 bytes from 192.168.100.249: icmp_seq=5 ttl=64 time=0.745 ms
64 bytes from 192.168.100.249: icmp_seq=6 ttl=64 time=0.674 ms
64 bytes from 192.168.100.249: icmp_seq=7 ttl=64 time=0.628 ms
64 bytes from 192.168.100.249: icmp_seq=8 ttl=64 time=0.607 ms

--- 192.168.100.249 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7005ms
rtt min/avg/max/mdev = 0.607/0.661/0.745/0.052 ms
[root@localhost ~]#
```

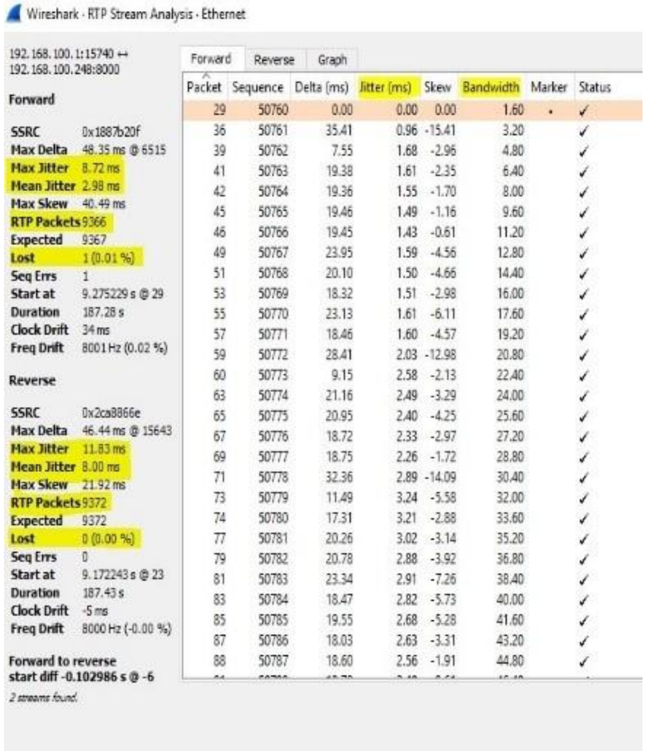
Figure 2. Ping from VoIP server to IP-phone



```
[root@localhost ~]# ping 192.168.100.249
PING 192.168.100.249 (192.168.100.249) 56(84) bytes of data.
64 bytes from 192.168.100.249: icmp_seq=1 ttl=64 time=0.632 ms
64 bytes from 192.168.100.249: icmp_seq=2 ttl=64 time=0.720 ms
64 bytes from 192.168.100.249: icmp_seq=3 ttl=64 time=0.608 ms
64 bytes from 192.168.100.249: icmp_seq=4 ttl=64 time=0.456 ms
64 bytes from 192.168.100.249: icmp_seq=5 ttl=64 time=0.659 ms
64 bytes from 192.168.100.249: icmp_seq=6 ttl=64 time=0.502 ms
64 bytes from 192.168.100.249: icmp_seq=7 ttl=64 time=0.507 ms
64 bytes from 192.168.100.249: icmp_seq=8 ttl=64 time=0.669 ms
64 bytes from 192.168.100.249: icmp_seq=9 ttl=64 time=0.690 ms

--- 192.168.100.249 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8002ms
rtt min/avg/max/mdev = 0.456/0.604/0.720/0.093 ms
[root@localhost ~]#
```

Figure 3. Ping from VoIP server to wireless user.

Figure 2 shows the result of 0% packet loss when the call established between two users. We have some more results of wireless users. Same result in Figure 3 with wireless user when the call established. Figure 4 shows the result from Wireshark, it displays the jitters packet lost and received when call established.



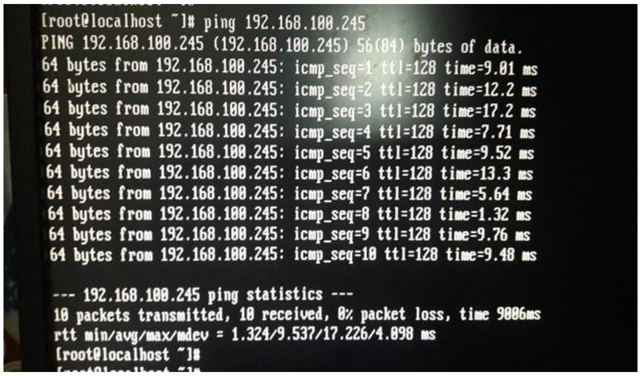
Wireshark · RTP Stream Analysis · Ethernet

```
192.168.100.1:15740 ↔
192.168.100.248:8000

Forward

SSRC          0x1887b20f
Max Delta     48.35 ms @ 6515
Max Jitter    8.72 ms
Mean Jitter   2.98 ms
Max Skew      40.49 ms
RTP Packets   9366
Expected      9367
Lost          1 (0.01 %)
Seq Errs      1
Start at      9.275229 s @ 29
Duration      187.28 s
Clock Drift   34 ms
Freq Drift    8001 Hz (0.02 %)

Reverse

SSRC          0x2ca8866e
Max Delta     46.44 ms @ 15643
Max Jitter    11.83 ms
Mean Jitter   8.00 ms
Max Skew      21.92 ms
RTP Packets   9372
Expected      9372
Lost          0 (0.00 %)
Seq Errs      0
Start at      9.172243 s @ 23
Duration      187.43 s
Clock Drift   -5 ms
Freq Drift    8000 Hz (-0.00 %)

Forward to reverse
start diff -0.102986 s @ -6

2 streams found.
```

Packet	Sequence	Delta (ms)	Jitter (ms)	Skew	Bandwidth	Marker	Status
29	50760	0.00	0.00	0.00	1.60	•	✓
36	50761	35.41	0.96	-15.41	3.20		✓
39	50762	7.55	1.68	-2.96	4.80		✓
41	50763	19.38	1.61	-2.35	6.40		✓
42	50764	19.36	1.55	-1.70	8.00		✓
45	50765	19.46	1.49	-1.16	9.60		✓
46	50766	19.45	1.43	-0.61	11.20		✓
49	50767	23.95	1.59	-4.56	12.80		✓
51	50768	20.10	1.50	-4.66	14.40		✓
53	50769	18.32	1.51	-2.98	16.00		✓
55	50770	23.13	1.61	-6.11	17.60		✓
57	50771	18.46	1.60	-4.57	19.20		✓
59	50772	28.41	2.03	-12.98	20.80		✓
60	50773	9.15	2.58	-2.13	22.40		✓
63	50774	21.16	2.49	-3.29	24.00		✓
65	50775	20.95	2.40	-4.25	25.60		✓
67	50776	18.72	2.33	-2.97	27.20		✓
69	50777	18.75	2.26	-1.72	28.80		✓
71	50778	32.36	2.89	-14.09	30.40		✓
73	50779	11.49	3.24	-5.58	32.00		✓
74	50780	17.31	3.21	-2.88	33.60		✓
77	50781	20.26	3.02	-3.14	35.20		✓
79	50782	20.78	2.88	-3.92	36.80		✓
81	50783	23.34	2.91	-7.26	38.40		✓
83	50784	18.47	2.82	-5.73	40.00		✓
85	50785	19.55	2.68	-5.28	41.60		✓
87	50786	18.03	2.63	-3.31	43.20		✓
88	50787	18.60	2.56	-1.91	44.80		✓

Figure 4. VoIP server to IP-phone.

Now, we will apply Honeynet security firewall in VoIP setup. Then analyses the results of wired, wireless and remote VPN users. There is no change in quality measures after applying Honeynet firewall within same network. In Figure 5 it shows the same result.



```
[root@localhost ~]# ping 192.168.100.245
PING 192.168.100.245 (192.168.100.245) 56(84) bytes of data.
64 bytes from 192.168.100.245: icmp_seq=1 ttl=128 time=9.01 ms
64 bytes from 192.168.100.245: icmp_seq=2 ttl=128 time=12.2 ms
64 bytes from 192.168.100.245: icmp_seq=3 ttl=128 time=17.2 ms
64 bytes from 192.168.100.245: icmp_seq=4 ttl=128 time=7.71 ms
64 bytes from 192.168.100.245: icmp_seq=5 ttl=128 time=9.52 ms
64 bytes from 192.168.100.245: icmp_seq=6 ttl=128 time=13.3 ms
64 bytes from 192.168.100.245: icmp_seq=7 ttl=128 time=5.64 ms
64 bytes from 192.168.100.245: icmp_seq=8 ttl=128 time=1.32 ms
64 bytes from 192.168.100.245: icmp_seq=9 ttl=128 time=9.76 ms
64 bytes from 192.168.100.245: icmp_seq=10 ttl=128 time=9.48 ms

--- 192.168.100.245 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9006ms
rtt min/avg/max/mdev = 1.324/9.537/17.226/4.098 ms
[root@localhost ~]#
```

Figure 5. No change in quality measures.

A. *Effect of Packet Failure on Protection of the Honeynet*

These following results demonstrate that, the remote users dial the campus network through VPN before honeynet security applies.

Normally the delays of packet are 5% to 10% percent and after apply security the result are 10% to 20% packet losses. This is illustrated in Figures 6 and Figure 7.

V. Conclusion and Future Work

Security is much like a race between hackers and security accountable, even by using Honeynet and other techniques we have to understand the efforts that hacker do to slip through by observing the latest security tools and creating more sophisticated ways to accomplish their goals. So, the security administrator must continue to work to enhance security techniques and create multi-layer security policies and systems, so if one of the layers passes the threat of the attacker, we can still catch him and prevent him on the next layer.

The main purpose of this project is to investigate the results of quality of VoIP setup after deploying the honeynet security framework. It is mostly affected on remote users of different networks which are connect through VPN.

The project provides the security framework to detect hacker actions for enterprises, schooling, hospitals, banking environments and individuals and prevents them at the beginning of the network.

There is a need to explore the fact and figures which are causing the impact of honeynet security architecture.

References

[1] Shivankar, S. J., & Tembhurkar, M. P. (2015, February). Comparative analysis on security techniques in VoIP environment. In 2015 2nd International Conference on Electronics and Communication Systems (ICECS) (pp. 1176-1180). IEEE.

[2] Wuttidittachotti, P., & Daengsi, T. (2015, July). QoE of social network applications: A study of VoIP quality from Skype vs LINE over 3G and 4G. In 2015 Seventh International Conference on Ubiquitous and Future Networks (pp. 462-464). IEEE.

[3] Kyriakou, A., & Sklavos, N. (2018, October). Container-based honeypot deployment for the analysis of malicious activity. In *2018 Global Information Infrastructure and Networking Symposium (GIIS)* (pp. 1-4). IEEE.

[4] Ren, J., Zhang, C., & Hao, Q. (2021). A theoretical method to evaluate honeynet potency. Future Generation Computer Systems, 116, 76-85.

[5] Prasetyo, Junaedi Adi, and I. Wayan Suardinata. "Comparison of Voice over Internet Protocol (VoIP) Performances in Various Network Topologies." Buletin Pos dan Telekomunikasi 18.1 (2020): 65-74.

[6] Baraković, Sabina, and Seudin Kasumović. "The Influence of SIP Call Control Signalling on VoIP Quality of Experience." Tehnički vjesnik 26.6 (2019): 1537-1544.

[7] Kurniawati, N., & Agoes, S. (2020). Analysis of Voice Captured Packet Using Wireshark. Jetri: Jurnal Ilmiah Teknik Elektro, 17(2), 205-216.

[8] Kumar, V., & Roy, O. P. (2020). Reliability and Security Analysis of VoIP Communication Systems. In Rising Threats in Expert Applications and Solutions (pp. 687-693). Springer, Singapore.

[9] Kurniawati, N., Affandi, A., Pratomo, I., & Gyoda, K. (2018, August). Raspberry Pi-Based VoIP System for Rural Area. In 2018 International Seminar on Intelligent Technology and Its Applications (ISITIA) (pp. 33-38). IEEE.

[10] Kolahi, S. S., Mudaliar, K., Zhang, C., & Gu, Z. (2017, July). Impact of IPSec security on VoIP in different environments. In 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN) (pp. 979-982). IEEE.

[11] El Kafhali, S., & Hanini, M. (2017). Stochastic Modeling and Analysis of Feedback Control on the QoS VoIP Traffic in a single cell IEEE 802.16 e Networks. IAENG International Journal of Computer Science, 44(1), 19-28.

[12] “Secure VoIP Transmission through VPN Utilization” International Journal of Engineering Research and General Science Volume 3, Issue 2, Part 2, March-April, 2015 ISSN 2091-2730PrashantKhobragade, Disha Gupta Department of Computer Science & Engineering RGCER Nagpur, India.

[13] Singh, M., & Sharma, N. (2015). A Proposed Security Framework for VoIP. International Journal of Computer Science and Mobile Computing, 4(5), 424-431.

[14] “VoIP over WLAN Networks”International Journal of Scientific & Engineering Research, Volume 6, Issue 5, May-2015ISSN 2229-5518 Pankaj Kumar, ArunVerma, ShailiSinghal, ShobhitUniversity,U.PIIT, Mumbai RCVGIT, GHAZIABAD, U.P

[15] Sat, B., & Wah, B. W. (2007, October). Evaluation of conversational voice communication quality of the Skype, Google-Talk, Windows Live, and Yahoo Messenger VoIP systems. In 2007 IEEE 9th Workshop on Multimedia Signal Processing (pp. 135-138). IEEE.

[16] Anwar, Z., Yurcik, W., Johnson, R. E., Hafiz, M., & Campbell, R. H. (2006, April). Multiple design patterns for voice over IP (VoIP) security. In 2006 IEEE International Performance Computing and Communications Conference (pp. 8-pp). IEEE.

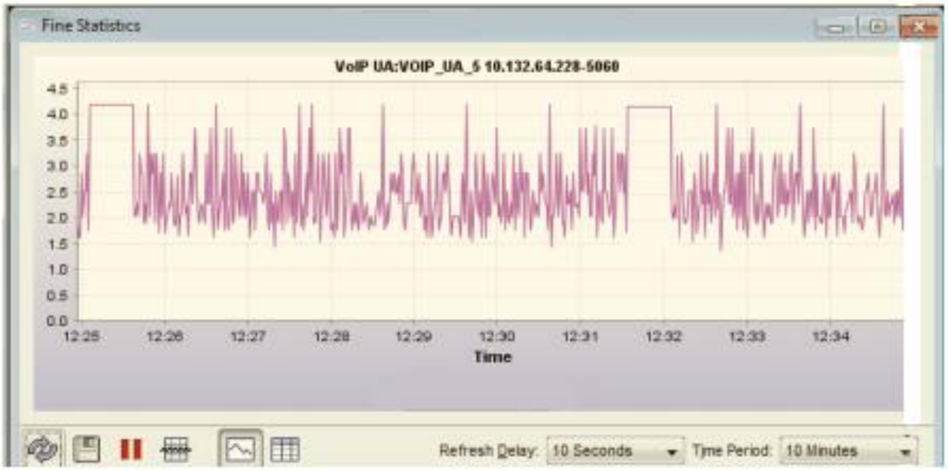
[17] Yeun, C. Y., & Al-Marzouqi, S. M. (2009, October). Practical Implementations for Securing VoIP Enabled Mobile Devices. In 2009 Third International Conference on Network and System Security (pp. 409-414). IEEE.

[18] ABDALLA, M. E. M. (2017). Performance Evaluation of VoIP QoS in WiMAX Networks (Doctoral dissertation, Sudan University of Science and Technology).

[19] Edreva, P. J., & Georgieva, T. N. POSSIBLE PROBLEMS AND FACTORS AFFECTING QoS IN TRANSMISSION OF VOICE OVER IP NETWORK. КОМПЮТЪРНИ НАУКИ И ТЕХНОЛОГИИ, 99.

[20] Tomić, D., Martinović, G., & Čuljak, A. (2017, October). Comparison of QoS influence to VoIP traffic into native and tunnel mode IPv6 networks. In 2017 International Conference on Smart Systems and Technologies (SST) (pp. 109-114). IEEE.

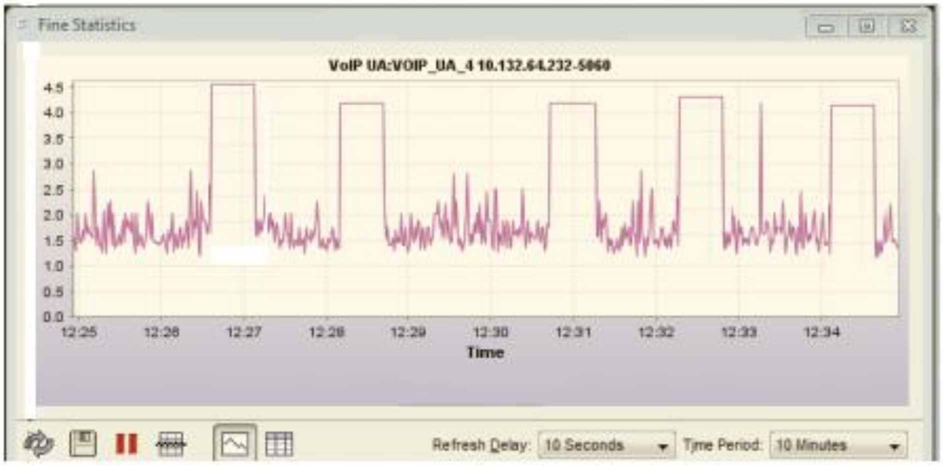
[21] Hassine, K., & Frikha, M. (2017, June). A VoIP focused frame aggregation in wireless local area networks: Features and performance characteristics. In 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC) (pp. 1375-1382). IEEE.



Refresh Delay: 10 Seconds

Time Period: 10 Minutes

Figure 6. It shows the delay of 5 to 10%.



Refresh Delay: 10 Seconds

Time Period: 10 Minutes

Figure 7. It shows the delay of packaets 10 to 20%.