JURNAL UPI

Journal of Computers for Society

Journal homepage: https://ejournal.upi.edu/index.php/JCS

Journal of Computers for Society

Security Analysis and The Effect of Codec Changes on Quality of Service of Encrypted Voice Phones on Voice Over IP Freepbx

Asep Saepul Achmad[1,], Muhammad Nursalman[2], Rizky Rachman J[3]*

Department of Computer Science Education, Universitas Pendidikan Indonesia, Indonesia.
*Correspondence: E-mail: aasepsaepul947@student.upi.edu

ABSTRACT

VoIP is one of the technologies as communication with audio and video media online. The server secures voice phone data on VoIP supporting VoIP phone data encryption. In addition to security, in order to improve sound quality FreePBX also uses the latest codecs such as Alaw, Ulaw, G722, G729. The purpose of this study was to display the results of VoIP voice phone security testing on FreePBX Server, analyze the Quality of Service of voice codecs on VoIP phones, and compare encrypted and unencrypted VoIP voice phones. The Quality-of-Service criteria of voice telephony consist of packet loss, jitter, and delay or delta. Then, test VoIP security using the Man in The Middle Attack (ARP Poisioning) attack method on the Cain and Abel application. Next, analyze the comparison between encrypted and unencrypted phones using SoftPhone SIPSoercery. Test results for QoS of encrypted VoIP phones with different audio codecs are very good and this assessment is based on the TIPHON QoS standard. The best delta value is found in the Ulaw codec and the best jitter value is found in the Alaw codec. After VoIP phones are attacked with ARP Poisoning, there is a decrease in QoS quality. For all codecs tested, the delta value decreased from 9.34% to 104.12%, the jitter value decreased from 235.49% to 767.97%, and the packet loss value decreased from 5.56% to 181.82%.

ARTICLE INFO

Article History:
Submitted/Received 20 Feb 2023
First Revised 18 Apr 2023
Accepted 12 Jun 2023
First Available Online 13 Jun 2023
Publication Date 15 Sep 2023

Keyword:
ARP Poisoning,
Codec,
FreePBX,
MITM.
QoS,
SDP,
SIP Sorcery,
SIP,
SRTP,
TLS,
VoIP,

1. INTRODUCTION

Everyone can exchange information with the internet in the form of voice, images, text, and video. The rapid development of the internet makes it easier for users to send data in the form of voice to each other via Voice over Internet Protocol (VoIP). In short, VoIP is a telephone communication technology connected through an Internet Protocol (IP) network that converts voice into digital code and is transferred towards the caller's destination (Uys, 2009). VoIP is not only used to communicate with voice, but users can also communicate via video (video calls), and text messages (Gawarle, 2017). Digital voice communication typically uses a Public Switched Telephone Network (PSTN). However, this technology began to be abandoned because of its high cost and low sound quality. VoIP networks governed by Private Branch Exchanges (PBXs) are seen as the next major evolution in telecommunications that will accelerate PSTN convergence. One PBX software that many companies use is Asterisk (Maar *et al*., 2017). Usually, PBXs are installed on VoIP servers, one of the well-known open-source VoIP servers is FreePBX.

FreePBX is one of the Voice Over IP management systems used by many companies and uses VoIP as the company's internal communication technology. FreePBX servers implement encryption of VoIP communication with TLS and SRTP. The application of encryption of VoIP voice telephone communication by FreePBX needs to be tested and analyzed for security, then prove that VoIP telephone communication using FreePBX is secure, and the confidentiality of telephone voice media data is maintained. In the industrial world, security is an important part that must be present in VoIP systems and is an important topic (Wang, & Zhang, 2011). VoIP security hackers usually manipulate computer systems by gaining unauthorized access to VoIP systems and obtaining information illegally. There are several VoIP security studies showing that hacking events occur because of the perpetrator's need for sabotage, revenge, extortion, to greed (Martin *et al*., 2005).

In addition to security, VoIP communication requires good quality VoIP telephony. One method of measuring the quality of VoIP phones is to use Quality of Service. Media quality in VoIP voice telephone communication is usually supported by codecs. The VoIP communication system in FreePBX uses a variety of media codecs that can be used and according to the wishes of the VoIP communication client. Therefore, VoIP communication in FreePBX that uses various codecs requires testing with quality-of-service parameters.

To avoid security hackers on voice communication on Voice Over IP, there are security solutions that can be done. One of them is to encrypt voice communication on Voice Over IP. Voice over IP encryption is the process of converting a telephone packet into a telephone packet that cannot be understood by the recipient of a regular telephone plan. Because the packet is encrypted, the security of a data can be guaranteed because it cannot be read by just anyone. In addition to security, good voice is also needed so that communication between users is also good and smooth.

Based on the problems just discussed, an analysis and testing of VoIP voice phone security on FreePBX was carried out. The analysis was conducted to see the stages of voice phone encryption on VoIP using TLS and SRTP protocols. VoIP voice phone security analysis is also carried out by comparing VoIP communication flows carried out by encrypted and unencrypted VoIP voice phones. Security testing is carried out by attacking VoIP voice phone systems with the Man in The Middle Attack method. Then, in this study also the VoIP system in FreePBX will be tested and analyzed Quality of Service from the use of selected codecs by encrypted and encrypted VoIP voice phones that are attacked.

DOI: http://dx.doi.org/10.17509/xxxx.xxx
p- ISSN xxxx-xxxx e- ISSN 2723-4088

2. METHODS

Research methods are a framework used as a guide in carrying out research. In this section, the author will explain the framework from the beginning of the research to the end. The design of this study can be seen in **Figure 1**.

Figure 1. Desain Penelitian.

2.1. Hardware and Software Installation

In carrying out research, hardware and software are needed which can be seen in **Table 1** and **Table 2**.

Table 1. Hardware Specifications

Specifications	Client 1 (Laptop)	Client 2 (Laptop)	Server (Raspberry Pi 4)
Processor	Intel Core i7-6500U	Intel Core i3-3217U	Quad core Cortex-A72
RAM	8 GB	6 GB	4 GB
Harddisk	125 GB	250 GB	32 GB
Audio Driver	Realtek HD Audio	Microsoft HD Audio	-
Operating System	Windows 10	Windows 10	Raspbian GNU/Linux 10

DOI: http://dx.doi.org/10.17509/xxxx.xxx
p- ISSN xxxx-xxxx e- ISSN 2774-7891

Other hardware such as:

- Cable LAN
- Switch HUB
- Router Internet
- USB Headset dbE GM-180 dan Logitech G633s
- Realme Buds Classic Earphones with Audio Jack Port

Table 2. Software

Device	Software	Information
Server	FreePBX,	FreePBXTesting as server VoIP .
	Asterisk	Asterisk as a VoIP PBX application.
Client (SoftPhone)	MicroSIP	MicroSIP for encrypted voice phones.
	SIPSorcery	SIPSorcery for VoIP communication without encryption. Only make a blind transfer call. The result is a SIP *call flow* that will be compared to the SIP in an encrypted phone.
Testing	Wireshark,	Wireshark is used as a security test in terms of the use of encryption algorithms and VoIP security support protocols
	Cain and Abel	Cain and Abel is used as a security test in the event of hacking or attacks on VoIP communications

2.2. Test Design

The test was conducted with 3 scenarios, namely 1) VoIP voice phone testing without encryption (**Figure 4**); 2) VoIP voice phone testing with SRTP encryption (**Figure 2**); 3) VoIP voice phone testing with encryption and attacked using Man In The Middle Attack method (**Figure 3**).

DOI: http://dx.doi.org/10.17509/xxxx.xxx
p- ISSN xxxx-xxxx e- ISSN 2723-4088

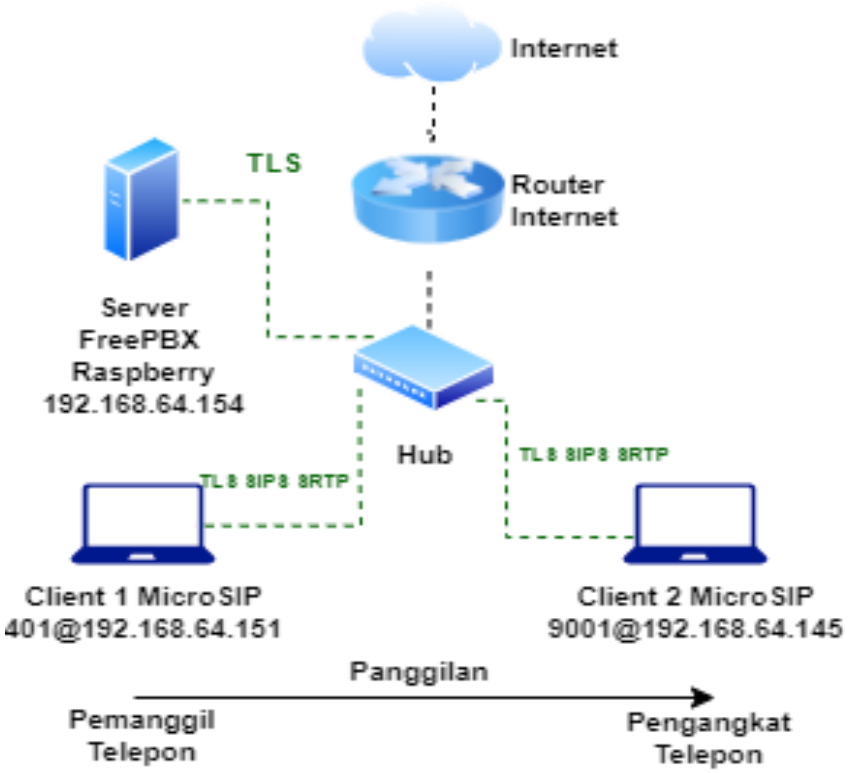

Figure 2. Encrypted Phone.

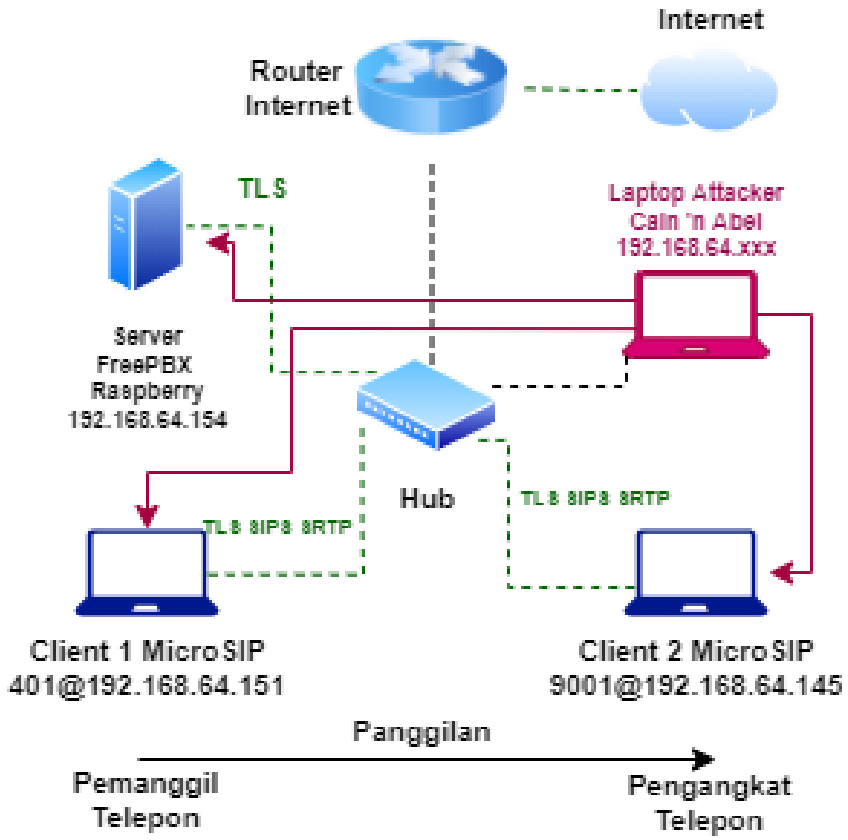

Figure 3. Encrypted Calls and MiMA Attacks.

DOI: http://dx.doi.org/10.17509/xxxx.xxx
p- ISSN xxxx-xxxx e- ISSN 2774-7891

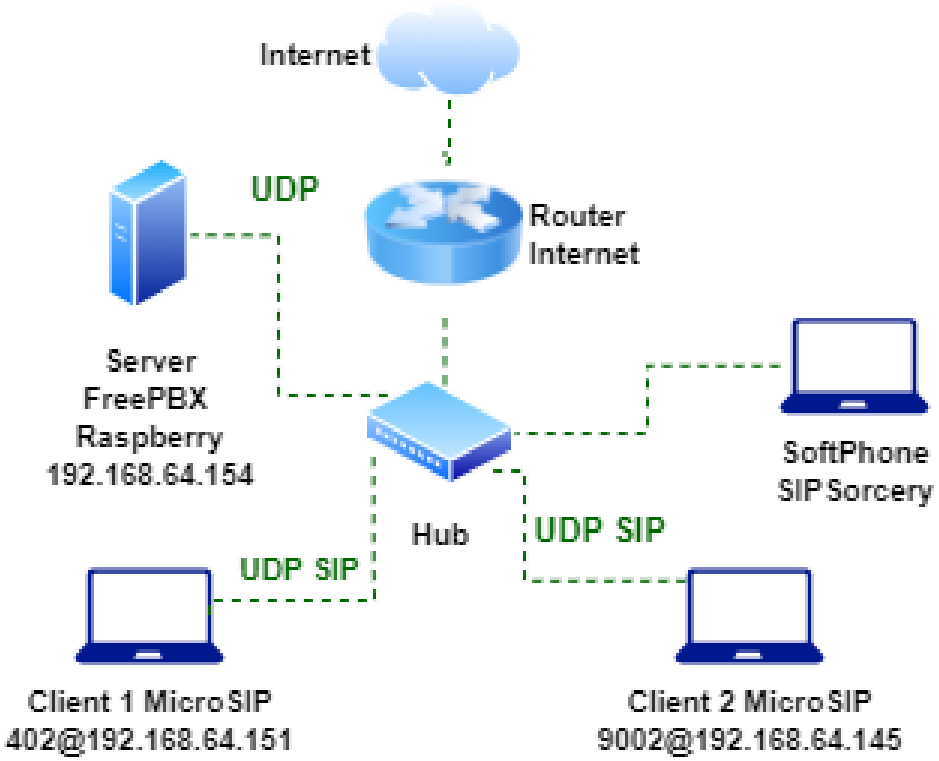

Figure 4. VoIP Without Encryption.

In the scenarios of Figure 2 and Figure 3, for the encrypted call, data capture will be carried out on the voice telephone communication between Client 1 and Client 2. Here is a scenario of testing conducted using several scenarios to prove VoIP security on FreePBX.

• Encrypted VoIP Voice Phone System with TLS SRTP Testing:
  - Phone conversation duration of 45 seconds
  - Conducted 4 calls, calls with codecs Alaw, Ulaw, G729, G722
  - The contents of the phone come from 2 microphones that are held close to the speaker of the mobile phone that is playing dialogue.
  - Data packet tapping using Wireshark

• VoIP Voice Phone System Encrypted with TLS SRTP and Attacked using Cain and Abel Testing:
  - Phone conversation duration of 45 seconds
  - Conducted 4 calls, calls with codecs Alaw, Ulaw, G729, G722
  - The contents of the phone come from 2 microphones that are held close to the speaker of the mobile phone that is playing dialogue.
  - Data packet tapping using Wireshark

• VoIP Voice Phone System Without Encryption Testing:
  - Communication duration is 45 seconds.
  - Conducted 4 calls, calls with codecs Alaw, Ulaw, G729, G722.
  - SIPSorcery sends data in the form of RTCP, this data is similar to RTP but this data has no media.
  - No interception of data packets using Wireshark.

Then, the telephone scenario for all encrypted phones is depicted in **Figure 5**.

DOI: http://dx.doi.org/10.17509/xxxx.xxx
p- ISSN xxxx-xxxx e- ISSN 2723-4088

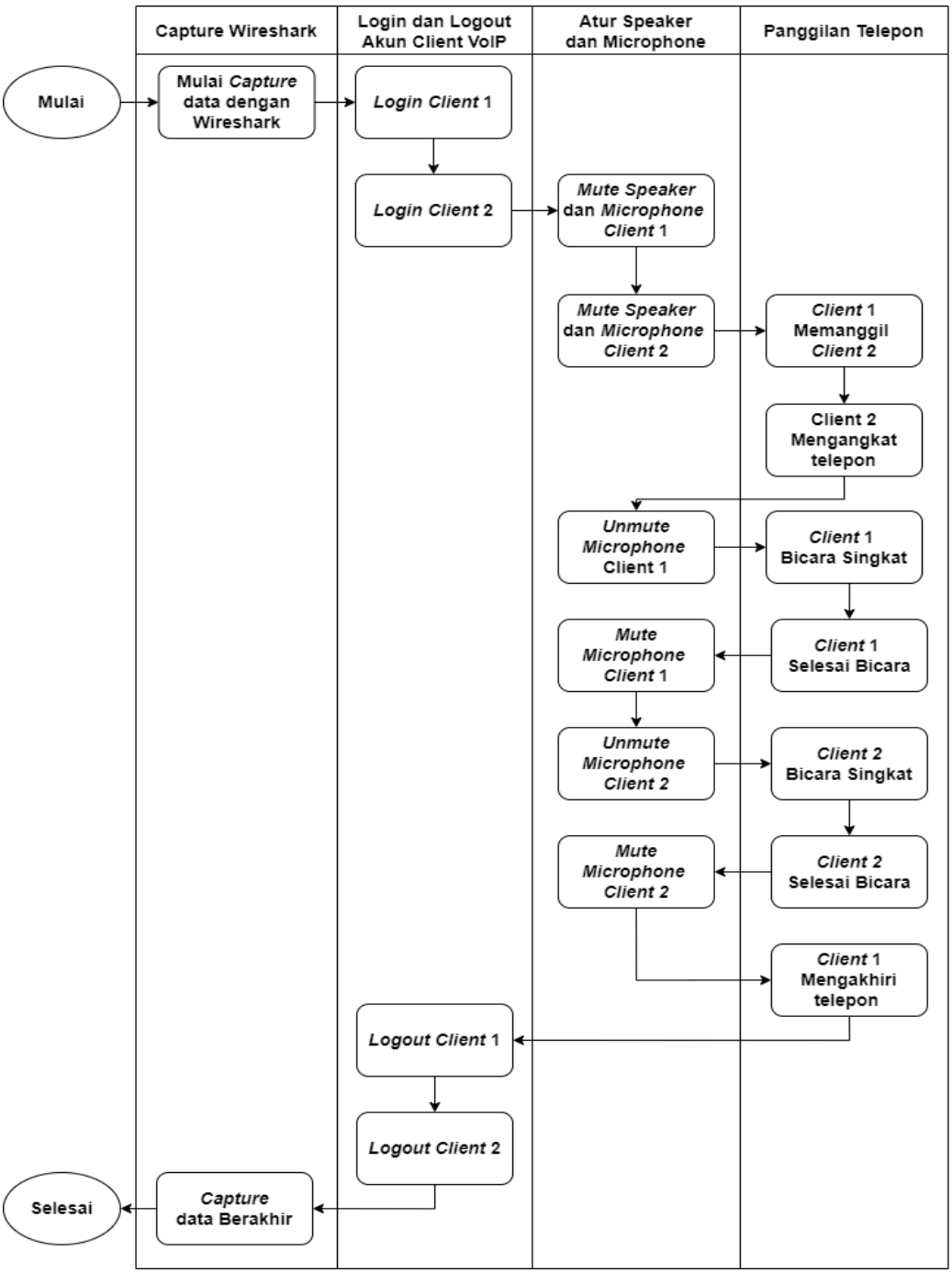

Figure 5. VoIP Phone Process

2.3. Instalasi Server FreePBX

The FreePBX VoIP server installation steps are as follows:

- Install the FreePBX .iso file on the MicroSD installed on the Raspberry
- Initial configuration after OS installation, i.e. localhost address, time and language, VoIP server account and password.
- Update all applications on the VoIP server with the raspbx-upgrade command.

DOI: http://dx.doi.org/10.17509/xxxx.xxx
p- ISSN xxxx-xxxx e- ISSN 2774-7891

2.4. VoIP Phone Account Creation

Phone accounts on VoIP are set in Extensions. The following in Table 3 are the extensions used in this study.

Table 3. Extension VoIP

IP Address	Extension	Information
192.168.64.151	401	VOIPCALLCLIENT2
192.168.64.151	402	VOIPCALLCLIENTNOENCRYPT2
192.168.64.145	9001	VOIPCALLCLIENT1
192.168.64.145	9002	VOIPCALLCLIENTNOENCRYPT1

Each extension number has its own configuration. Table 4 showing the configuration of VoIP extension numbers on FreePBX Servers.

Table 4. Extension Configuration

Extension	Configuration	Extension	Configuration
401	• allow=g722,alaw, g729,ulaw callerid=VOIPCALLCLIEN T2 <401> • dtmf_mode=info • transport=0.0.0.0-tls media_encryption=sdes extension_driver=pjsip rtp_timeout=30 rtp_timeout_hold=300 password= • VOIPCALLCLIENT2	**402**	• allow=g722,alaw,g729,ulaw • callerid=VOIPCALLCLIENTNOENCRYPT2 <402> • password= • VOIPCALLCLIENTNOENCRY • PT2 • transport=0.0.0.0-udp • rtp_timeout=30 • rtp_timeout_hold=300 • extension_driver=pjsip

DOI: http://dx.doi.org/10.17509/xxxx.xxx
p- ISSN xxxx-xxxx e- ISSN 2723-4088

Extension	Configuration	Extension	Configuration
9001	• allow=g722,alaw,g729,ulaw • callerid=VOIPCALLCLIENT1 <9001> • dtmf_mode=info • transport=0.0.0.0-tls media_encryption=sdes extension_driver=pjsip rtp_timeout=30 rtp_timeout_hold=300 password= • VOIPCALLCLIENT1	**9002**	• password= • VOIPCALLCLIENTNOENCRYPT1 • transport=0.0.0.0-udp • callerid=VOIPCALLCLIENTNOENCRYPT2 <402> • allow=g722,alaw,g729,ulaw • rtp_timeout=30 • rtp_timeout_hold=300 • extension_driver=pjsip

3. RESULTS AND DISCUSSION

3.1. VoIP Phone Analysis Without Encryption

Sniffing Packet on VoIP phones without encryption aims to see the content of communication messages related to VoIP and compare the content of messages in the form of VoIP protocols, namely Session Initiation Protocol, Session Description Protocol, and RTP Control Protocol. SIPSorcery sends data in the form of RTCP to Clients who provide QoS feedback through repeated statistical data communication. However, RTCP does not stream media data (Han *et al*., 1998) like SRTP on Encrypted VoIP phones. SIP and SDP protocols are used in unencrypted VoIP communications or encrypted VoIP voice calls. The SIP protocol is used as a signaling protocol in VoIP. SDP protocol is a protocol that supports multimedia sessions in communication that aims to convey media stream information that can be understood by participants in the communication (Kang, *et al*., 2004). All these protocols will be compared to encrypted VoIP voice phones.

```
v=0
o=- 3868669554 3868669555 IN IP4 192.168.64.151
s=pjmedia
b=AS:84
t=0 0
a=X-nat:0
m=audio 4000 RTP/AVP 8 101
c=IN IP4 192.168.64.151
b=TIAS:64000
a=rtcp:4001 IN IP4 192.168.64.151
a=sendrecv
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ssrc:2705443 cname:39b32d12074d4dc8
```

```
v=0
o=- 1554553297 0 IN IP4 127.0.0.1
s=sipsorcery
c=IN IP4 192.168.64.151
t=0 0
m=audio 18000 RTP/AVP 0 8 9 18 101
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:9 G722/8000
a=rtpmap:18 G729/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=sendrecv
a=ssrc:1267401709 cname:e1c51705-9702-41a7-91c7-33a433987e1f
```

Figure 6. Phone Media Information in SDP Protocol

DOI: http://dx.doi.org/10.17509/xxxx.xxx
p- ISSN xxxx-xxxx e- ISSN 2774-7891

3.2 VoIP Phone Analysis Without Encryption

Phone encryption was performed 4 times with the voice codecs Alaw (8 kHz, 64 kbit/s), Ulaw (8 kHz, 64 kbit/s), G722 (16 kHz, 64 kbit/s), and G729 (8 kHz, 8 kbit/s). Encrypted VoIP calls use TLS and SRTP protocols. The TLS protocol secures data from the beginning of the connection between the client and server until the connection is complete. The start of the connection between client and server is done by logging in or registering a VoIP extension account from MicroSIP Softphone. Termination of TLS connections is done by logging out or offline the VoIP extension account. While the SRTP protocol initiates security after communication with the SIP protocol is successful and the VoIP phone is ready to call the destination.

3.2.1 VoIP Phone Analysis Without Encryption

TLS and SRTP protocols use a cipher suite which is a set of encryption algorithms to secure data (McGrew, D., & Rescorla, E., 2010). TLS protocol cipher suite information is obtained from the results of packet sniffing using Wireshark. Cipher information of the SRTP protocol suite was recovered from the MicroSIP SoftPhone log file. Table 5 follows the cipher suites used in encrypted VoIP communication in this study.

3.2.2. VoIP Phone Analysis Without Encryption

RTP Stream contains media data on VoIP. RTP serves as a transport protocol for audio and video on VoIP. When Wireshark siniffs VoIP communication, Wireshark can retrieve RTP information i.e. QoS from RTP Stream, RTP specification in the form of codecs, etc. (Sinam *et al*., 2014). When Wireshark fails to sniffing VoIP data, the VoIP voice data packets obtained are only UDP data packets as shown in Figure 7. In this picture there are contents of 2 Wireshark applications and displays package number 2954. The top Wireshark failed to sniffing RTP packets marked for those packets using the UDP protocol, while the bottom Wireshark successfully sniffed RTP packets.

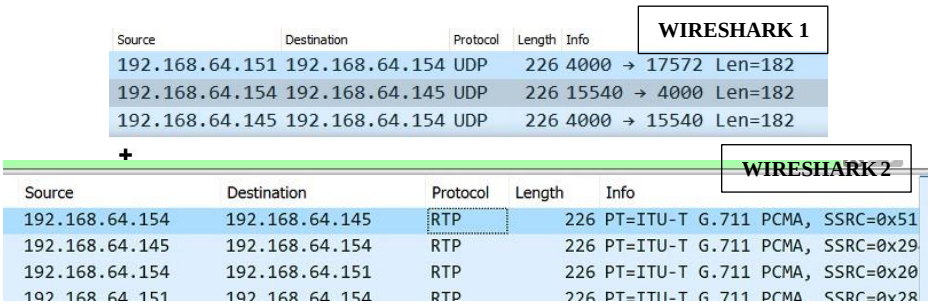

Figure 7. Sniffing Paket RTP with Wireshark

3.2.3 Quality of Service voice telephony on VoIP

Quality of Service is a method of measuring the ability and quality of a network so that the network can be better than before for user needs (Nisar, 2010). In this study, the QoS parameters to be analyzed are packet loss, delta / delay, and jitter.

Delay or Delta is the time delay in processing data packets (Molitorisová, A., & Šístek, P., 2021). Delays can occur in data packets on VoIP due to the coding process, transmission between communication participants, the digital voice packet process, the existence of data packet service queues, the existence of buffers to overcome jitter. Good Delay value quality if the delay time ranges from 0 – 150 ms (Zheng, 2021).

DOI: http://dx.doi.org/10.17509/xxxx.xxx
p- ISSN xxxx-xxxx e- ISSN 2723-4088

Table 6. Delay parameter based on TIPHON TR 101 329

Delay Value	Information
< 150 ms	Very good, slight echo
150 - 250 ms	Good
250 - 350 ms	Enough
> 450 ms	Bad

Jitter which is a variation of delay is the occurrence of a delay in the interval of arrival between data packets at the destination. Jitter is caused by a sudden increase in traffic which results in the emergence of many queues and narrowing bandwidth (Sheikh, 2023). Good jitter times range from 0 – 20 ms (Ekstedt *et al*., 1974).

Table 7. Jitter parameters based on TIPHON TR 101 329

Jitter Value	Information
< 10 ms	Very good
10 - 15 ms	Good
15 - 20 ms	Enough
> 20 ms	Bad

Packet loss which means loss of data packets during communication is usually caused by excessive queues on data packets and then causes collisions, noise, and congestion [Deng, *et al*., 2009). A good value for packet loss is around 0 – 0.5% (Balogh, *et al*., 2018).

Table 8. Parameter Packet Loss

Packet Loss Value	Information
< 0.5 %	Very good
0.5 – 1.5 %	Good
> 2 %	Bad

The following is the result of this study in the form of Quality of Service from 4 encrypted voice phone calls on VoIP with Codecs Alaw, Ulaw, G722, and G729 listed in the table below.

Table 9. Quality of Service Encrypted VoIP Voice Phone

Codec	Max Delta (ms)	Valuation Delta	Max Jitter (ms)	Valuation Jitter	Pocket Loss (%)	Valuation Pocket Loss
G729	160.218	Good	4.663	Very Good	0.32	Very Good

DOI: http://dx.doi.org/10.17509/xxxx.xxx
p- ISSN xxxx-xxxx e- ISSN 2774-7891

Alaw	127.045	Very Good	1.929	Very Good	0.18	Very Good
Ulaw	109.713	Very Good	2.802	Very Good	0.11	Very Good
G722	143.577	Very Good	4.064	Very Good	0.15	Very Good

3.3 Analyze Encrypted VoIP Phones Attacked with Man in The Middle Attack

In security testing on encrypted VoIP voice phones, the telephone stages are the same as the VoIP phone stages depicted in Figure 5. An addition to the VoIP phone process flow is that before the call is made, an attack using the Cain and Abel App begins. Attack on VoIP phones using APR Poisinong. APR Poisinong is a form of attack that manipulates ARP Tables by sending fake APR packets to the network so that the original APR Table is overwritten with fake ones (Almaarif, A., & Yazid, S., 2018). The contents of the ARP Table are data mapping IP network addresses to MAC addresses (Chandramohan, 2012). IP addresses can change, while MAC is a unique address for each device. The following in Figure 8 is the process of attacking VoIP phones with APR Poisoning in this study.

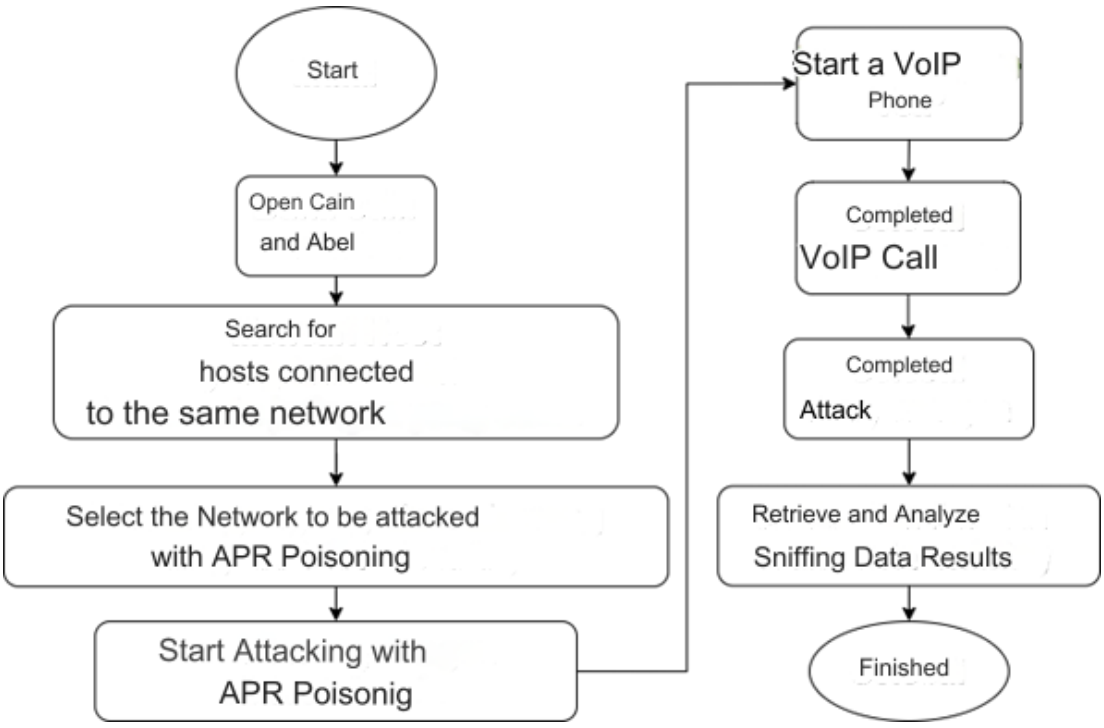

Figure 8. Poisoning on VoIP phone networks

3.3.1 Results of Data Sniffing with APR Poisoning

When APR Poisoning runs, the Cain application retrieves information related to VoIP communications. The data obtained is in the form of server certificates used for TLS protocols, SIPS protocol information, and VoIP audio data. The certificate data was successfully retrieved intact, namely the certificate file format .crt. SIP data was successfully retrieved from 4 VoIP calls (Alaw, Ulaw, G722, G729). The Cain and Abel application managed to get TLS information, SIPS information, and RTP voice data information which was then stored in the

DOI: http://dx.doi.org/10.17509/xxxx.xxx
p- ISSN xxxx-xxxx e- ISSN 2723-4088

Attacker's laptop. Then for the telephone conditions of 401 and 9001 are the telephone conditions (the telephone process is done as in Figure 5) when the attack uses ARP Poisoning.

3.3.1.1 Codec Alaw

TLS information: The TLS server certificate (.crt) file was successfully retrieved.

- SIP Information:
- SIP Handshake information was successfully obtained.
- Cipher Suite information on SDP is obtained.
- RTP (Voice Packet) Information: - Codec information obtained.
- RTP voice data is obtained and stored in mp3 form. The sound obtained cannot be decrypted or is not the same as the asl soundi.
- Phone Condition from Client 401 - Login = Normal.
- Calling destination = normal.
- Voice Phone = Normal.
- Call ended = normal.
- Phone Condition from Client 9001 - Login = Normal.
- Calling destination = normal.
- Voice Phone = Normal.
- Call ended = After 401 ends call, 9001 cannot End Call. End Call is done by the user.
- The recording file of the MicroSIP SoftPhone is corrupted

3.3.1.2 Codec Ulaw

- TLS information:
- The TLS server certificate (.crt) file was successfully obtained.
- SIP Information:
- SIP Handshake information was successfully obtained.
- Cipher Suite information on SDP is obtained.
- RTP (Voice Packet) Information: - Codec information obtained.
- RTP voice data is obtained and stored in mp3 form. The sound obtained cannot be decrypted or is not the same as the original sound.
- Phone Condition from Client 401 - Login = Normal.
- Calling destination = normal.
- Voice Phone = Normal.
- Call ended = normal.
- Phone Condition from Client 9001 - Login = Normal.
- Calling destination = normal.
- Voice Phone = Normal.
- Call ended = After 401 ends call, 9001 cannot End Call. End Call is done by the user.
- The recording file of the MicroSIP SoftPhone is corrupted.

3.3.1.3 Codec G722

- TLS information:
- The TLS server certificate (.crt) file was successfully obtained.
- SIP Information:
- SIP Handshake information was successfully obtained.
- Cipher Suite information on SDP is obtained.
- RTP (Voice Packet) Information: - Codec information obtained.
- RTP voice data is obtained and stored in mp3 form. The sound obtained cannot be decrypted or is not the same as the original sound.
- Phone Condition from Client 401 - Login = Normal.

DOI: http://dx.doi.org/10.17509/xxxx.xxx
p- ISSN xxxx-xxxx e- ISSN 2774-7891

- Calling destination = normal.
- Voice Phone = Normal.
- Call ended = normal.

• Phone Condition from Client 9001 - Login = Normal.

- Calling destination = normal.
- Voice Phone = Normal.
- Call ended = Normal.
- The recording file from SoftPhone MicroSIP can be opened and there is sound

3.3.1.4 Codec G729

• TLS information:

- The TLS server certificate (.crt) file was successfully obtained.

• SIP Information:

- SIP Handshake information was successfully obtained.
- Cipher Suite information on SDP is obtained.

• RTP (Voice Packet) Information: - Codec information obtained.

- RTP voice data is obtained and stored in mp3 form. The sound obtained cannot be decrypted or is not the same as the original sound.

• Phone Condition from Client 401 - Login = Normal.

- Calling destination = normal.
- Voice Phone = Normal.
- Call ended = normal.

• Phone Condition from Client 9001 - Login = Normal.

- Calling destination = normal.
- Voice Phone = Normal.
- Call ended = Normal.
- The recording file of the MicroSIP SoftPhone can be opened and there is sound.

3.3.2 QoS of encrypted VoIP voice phones attacked by ARP Poisoning Here in Table 12 are QoS of VoIP voice phones from 4 VoIP calls (Alaw, Ulaw, G722, G729) attacked by ARP Poisoning

Table 9. QoS of encrypted phones attacked with ARP Poisoning

Codec	*Max Delta (ms)*	Delta *Assessment*	*Max Jitter (ms)*	Jitter *Assessment*	*Packet Loss (%)*	Packet Loss Assessment
G729	240.179	Good	22.465	Bad	0.15	Very Good
Alaw	154.277	Good	16.739	Enough	0.19	Very Good
Ulaw	223.944	Good	19.649	Enough	0.31	Very Good
G722	156.981	Good	13.635	Good	0.42	Very Good

3.4 RTP Packet Analysis from VoIP Voice Phones

On a VoIP voice phone call, Wireshark and Cain and Abel successfully intercepted an RTP packet containing the phone's audio. When both audios are listened to, it will emit a sound that does not match the audio recorded from the client's microphone while on the phone. The Cain and Abel application used to intercept audio from RTP packets was unable to decrypt the data. In the 2 images below, each image has 2 paired charts and 1 graph. The first paired graphic at the very top is the RTP packet audio graph of an encrypted VoIP voice phone and

DOI: http://dx.doi.org/10.17509/xxxx.xxx
p- ISSN xxxx-xxxx e- ISSN 2723-4088

attacked with ARP Poisoning. The second paired graphic in the middle position is the RTP packet audio graph of an encrypted VoIP voice phone. The bottom graphic is a packet RTP audio graph from the SoftPhone Client audio recording, can be seen in the following **Figure 9** and **Figure 10.**

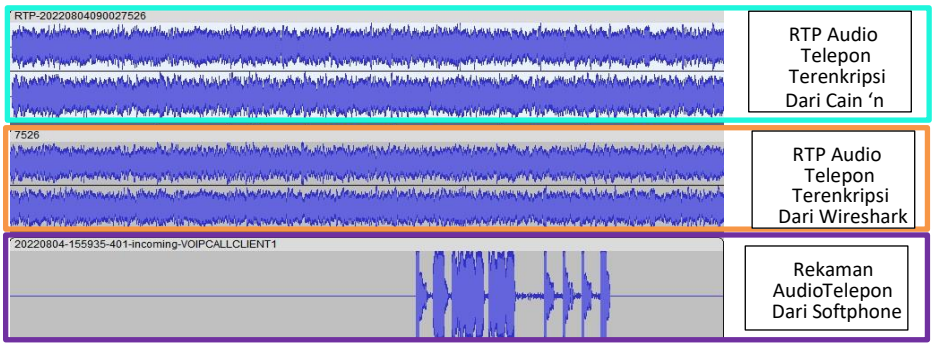

Figure 9. Audio Graphics RTP VoIP phone from 401 using Codec G729

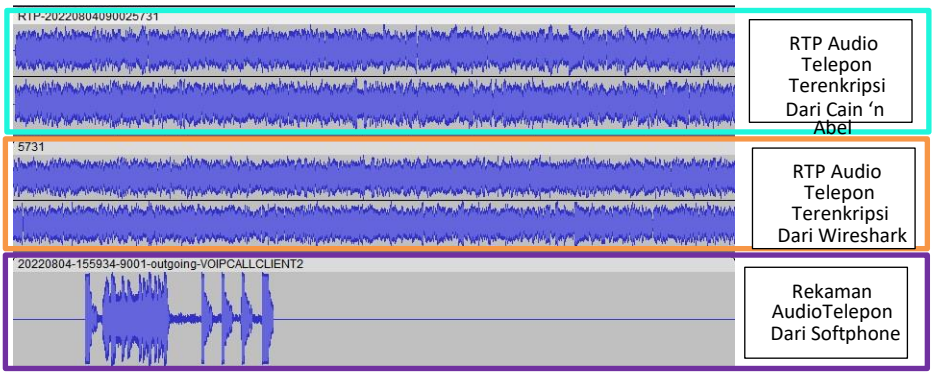

Figure 10. RTP Audio Graphics of VoIP phones from 9001 using Codec G729

3.5 Encrypted and Unencrypted VoIP Phone Analysis

Encrypted VoIP telephony starts from connecting the Server with the Client with the TLS protocol. Transport Layer Security will send a TLS Handshake message as the initial communication and make an agreement between Client and Server that after this TLS handshake is complete, the communication will continue with data that has been encrypted by TLS. Client and Server use cipher suites as a set of encryption algorithms and use TLS certificates as public keys and authentication for encryption [19]. After the TLS Handshake is complete, the Client and Server will initiate VoIP communication with the SIP protocol. The SIP protocol sends a SIP handshake or call flow message which contains information on VoIP Client A and Client B, Extension and IP used by the Client, checking the Extension by the server, etc. In the SIP protocol, there is an SDP protocol that is used as a store of VoIP media information. SDP also has a crypto attribute that is used to store cipher suite information that will be used for RTP voice data encryption (SRTP).

VoIP telephony without encryption starts from connecting Server and Client with UDP protocol (Kazemi, *et al*., 2010). After that, the server and client can communicate and initiate VoIP telephone communication with the SIP protocol. Clients A and B start handshake or SIP call flow. Unencrypted phones also use the SDP protocol. The difference between encrypted and unencrypted phones is; In SDP protocol phone encryption has a crypto attribute, while in SDP protocol phone without encryption there is no crypto attribute. Proof of the SDP protocol can be seen from the MicroSIP Softphone log file for encrypted VoIP phones and for VoIP

DOI: http://dx.doi.org/10.17509/xxxx.xxx
p- ISSN xxxx-xxxx e- ISSN 2774-7891

without encryption can be seen from the output of the SIPSorcery Softphone VoIP blind call program, can be seen in the following **Figure 11**.

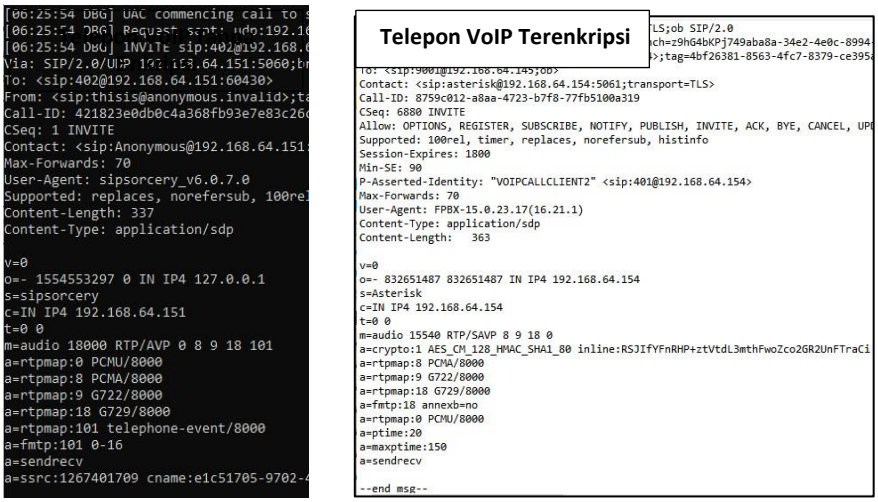

Figure 11. SDP Protocol Image on Encrypted and Unencrypted VoIP Phone.

4. CONCLUSION

Voice phone encryption on VoIP is very useful for securing telephone communications. In addition to security, VoIP voice phones must maintain the quality of voice data on the phone so that the voice can be heard clearly, voice data is not damaged / defective. The authors analyze the security as well as the effect of Codec changes on encrypted voice telephony on VoIP. The analysis uses Wireshark software. Then, the encrypted phone was also tested for security using the Cain and Abel application with the APR Poisoning attack. In this test, several audio codecs were also used, namely Alaw, Ulaw, G722, and G729.

After these tests were conducted on the SoftPhone MicroSIP application and FreePBX server with different audio codecs, the Quality-of-Service results of encrypted voice phones were very good and there was no significant loss in quality. Delta, jitter, and packet loss are rated very well based on TIPHON QoS standards. The best Delta value is found in the Ulaw codec, the best packet loss value is in the Ulaw codec, and the best jitter value is found in the Alaw codec.

After VoIP phones are attacked with APR poisoning, there is a decrease in QoS quality. Despite the decrease in quality, the sound from client 1 to and still is clearly heard by client 2. The increase and decrease in QoS quality in encrypted VoIP voice phones can be seen in the following **Table 10**.

Table 10. Percentage Increase and Decrease in QoS

Codec	Delta	Jitter	Packet Loss
G729	↓ 49.91%	↓ 381.77%	↑ 53.13%
Alaw	↓ 21.43%	↓ 767.97%	↓ 5.56%
Ulaw	↓ 104.12%	↓ 601.14%	↓ 181.82%
G722	↓ 9.34%	↓ 235.49%	↓ 180.00%

DOI: http://dx.doi.org/10.17509/xxxx.xxx
p- ISSN xxxx-xxxx e- ISSN 2723-4088

5. AUTHORS' NOTE

The authors declare that there is no conflict of interest regarding the publication of this article. The authors confirmed that the paper was free of plagiarism.

7. REFERENCES

Almaarif, A., and Yazid, S. (2018). ARP Cache Poisoning sebagai Teknik Alternatif untuk Membatasi Penggunaan Bandwidth berbasis Waktu. *Jurnal Rekayasa Sistem and Industri (JRSI), 5*(02), 108-113.

Maar, M., Sitarova, J., and Orgon, M. (2017). Enterprise network with software Asterisk PBX based on the PLC technology. *International Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems*, *6*(1), 1-10.

Chandramohan, D., Veeraiah, D., Shanmugam, M., Balaji, N., Sambasivam, G., and Khapre, S. (2012). SVIP-enhanced security mechanism for SIP based VoIP systems and its issues. *In Advances in Computing and Information Technology: Proceedings of the Second International Conference on Advances in Computing and Information Technology (ACITY) July 13-15, 2012, Chennai, 1*, 81-86.

Deng, D. J., Cheng, R. S., Chang, H. J., Lin, H. T., and Chang, R. S. (2009). A cross-layer congestion and contention window control scheme for TCP performance improvement in wireless LANs. *Telecommunication Systems, 42*, 17-27.

Gawarle, A. S. (2017). Design a Free Voice Calling System Using Raspberry Pi. *International Journal of Research in Engineering and Applied Sciences (IJREAS), 7*(6), 10-14.

Kang, T. G., Bae, H. J., Kim, D. Y., and Kim, D. U. (2004). SIP/SDP signaling of media gateway with transcoding function in converged network. *In The 6th International Conference on Advanced Communication Technology, 2004, 2*, 842-845.

McGrew, D., and Rescorla, E. (2010). Datagram transport layer security (DTLS) extension to establish keys for the secure real-time transport protocol (SRTP) (No. rfc5764).

Molitorisová, A., and Šístek, P. (2021). Reimagining Electronic Communications Regulatory Environment with AI: Self-Regulation Embedded in 'Techno-Regulation'. *European Journal of Law and Technology, 12*(1), 1-27.

Ekstedt, J., Nilsson, G., and Stålberg, E. (1974). Calculation of the electromyographic jitter. *Journal of Neurology, Neurosurgery and Psychiatry*, *37*(5), 526-539.

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

Uys, L. (2009). Voice over internet protocol (VoIP) as a communications tool in South African business. *African Journal of Business Management, 3*(3), 89.

Sheikh, W. (2023). Jitter-sensitive data communication in emerging wireless networks. *Transactions on Emerging Telecommunications Technologies*, *34*(5), e4746.

Wang, X., and Zhang, R. (2011). Voip security: vulnerabilities, exploits, and defenses. *In Advances in Computers, 81*, 1-49.

DOI: http://dx.doi.org/10.17509/xxxx.xxx
p- ISSN xxxx-xxxx e- ISSN 2774-7891

Han, T., Zhu, G. X., Zhu, Y., and Yao, W. (1998, September). Implementation and analysis of stream-oriented protocol-based RTP/RTCP within video conference. In *International Symposium on Multispectral Image Processing (ISMIP'98)*, *3545*, 286-289.

Zheng, L., Zhang, L., and Xu, D. (2001, June). Characteristics of network delay and delay jitter and its effect on voice over IP (VoIP). *In ICC 2001. IEEE International Conference on Communications. Conference Record (Cat. No. 01CH37240),1*, 122-126.

Martin, M. V., and Hung, P. C. (2005, May). Towards a security policy for VoIP applications. In *Canadian Conference on Electrical and Computer Engineering, 2005,* 65-68.

Kazemi, N., Wijesinha, A. L., and Karne, R. (2010, April). Evaluation of IPsec overhead for VoIP using a bare PC. *In 2010 2nd International Conference on Computer Engineering and Technology, 2*, V2-586.

Nisar, K., Said, A. M., and Hasbullah, H. (2010, June). Enhanced performance of packet transmission using system model over VoIP network. *In 2010 international symposium on information technology, 2*, 1005-1008.

Balogh, Z., Koprda, Š., and Francisti, J. (2018, October). LAN security analysis and design. *In 2018 IEEE 12th International Conference on Application of Information and Communication Technologies (AICT), 2018*, 1-6.

DOI: http://dx.doi.org/10.17509/xxxx.xxx
p- ISSN xxxx-xxxx e- ISSN 2723-4088