Development and Research of a Method for Multi-Level Protection of Transmitted Information in IP Networks Based on Asterisk IP PBX Using Various Codecs

Mubarak Yakubova[1], Tansaule Serikov[2]*, Olga Manankova[3]
Department of Automation and Information Technology,
Almaty University of Power Engineering and Telecommunications named after Gumarbek Daukeev, Almaty, Kazakhstan[1]
Department of Electronics and Telecommunication, S. Seifullin Kazakh AgroTechnical Research University, Astana, Kazakhstan[2]
Department of Cybersecurity, International Information Technology University, Almaty, Kazakhstan[3]

***Abstract*—Research indicates that the utilization of existing symmetric and asymmetric cryptosystems, as well as steganography, fails to ensure the requisite security and reliability in IP networks, where IP PBX Asterisk assumes the role of information transmission facilitator through switching processes. Consequently, this publication undertakes the development and investigation of a four-tiered information protection method when employing various voice codecs in IP networks based on IP PBX Asterisk. The adoption of multi-tiered protection significantly prolongs the cryptanalysis duration for malicious actors, thereby serving as a deterrent to information interception. The primary achievement of this research lies in minimizing the latency incurred during information traversal across the four layers of protection to less than 150 milliseconds, a benchmark widely acknowledged as optimal for assessing voice traffic service quality during transmission. It is noteworthy that a delay parameter of 150 milliseconds in telecommunications networks is pivotal; failure to meet this criterion at the receiving end may result in signal distortion such as jitter, audio degradation, unintelligibility, and other impairments. The devised methodology can be employed in networks transmitting highly classified or business-sensitive information. We contend that the developed encryption enhancement methodology, which prolongs the cryptanalysis duration for malicious entities and the conducted analysis, represents a novel scientific contribution.**

***Keywords*—Asterisk PBX; IP telephony systems; codecs; data security; Python**

I. Introduction

IP PBX Asterisk has become a popular choice for organizations seeking a flexible and cost-effective solution for their telecommunications needs [1-3]. However, the increasing reliance on IP-based communications brings with it new challenges in terms of security and data protection [4-8]. To address these challenges, researchers and developers have focused on improving the security of IP PBX Asterisk systems by implementing advanced security measures [9-14].

Let us consider how IP telephony works. During a conversation, voice signals (the words we speak) are transformed by codecs into compressed data packets, encoded, and transmitted over the Internet to the receiving party. When the data packets reach the recipient, they are decoded back into the original voice signals. Therefore, when building a security system, it is important to be aware of the risks that can arise, which can be presented as follows: distortion of content, due to breach of confidentiality; interception of the passing session; detection of vulnerability in penetrating the organization's network during the deployment of IP telephony; degradation of services based on DoS attacks and resale of traffic, which is one of the convenient ways for hackers to make money by redirecting calls to expensive international destinations when the station is out of order, receiving some reward to their electronic wallets, which, when cashed, turns into real money [15-19].

Unfortunately, such problems have become common lately. As a result, some consider Asterisk an unsafe system. However, this can be disputed if network security is reliably established.

Encryption plays a crucial role in ensuring the confidentiality and integrity of transmitted data [20-24]. The RSA algorithm is commonly used for encryption in IP networks due to its robust security features. Encrypting voice traffic with the RSA algorithm makes it much more difficult for unauthorized users to intercept and decrypt the information, ensuring the confidentiality of communications [25-27].

In addition to encryption, steganography can also be used to increase the security of transmitted information. LSB steganography in particular is well suited to embedding secret messages in voice traffic without significantly impairing the quality of the audio. By using LSB steganography, companies can hide sensitive information in voice traffic, making it difficult for attackers to detect and intercept [28-33].

Authentication is another important aspect of securing IP PBX Asterisk systems. By implementing strong authentication mechanisms, such as two-factor authentication or biometric authentication, organizations can verify the identity of users and devices accessing the system. This helps to prevent unauthorized access and ensures that only authorized users can use the system [34-38].

Finally, traffic analysis techniques can be used to detect and mitigate security threats on IP networks [39-41]. By analyzing

patterns and characteristics of network traffic, companies can identify potential security vulnerabilities and take proactive measures to mitigate them. In this way, attacks such as Denial of Service (DoS) attacks or Man-in-the-Middle (MitM) attacks can be prevented.

Although the implementation of these security measures increases the security of IP PBX Asterisk systems, it can also have an impact on reliability. Encryption and steganography in particular can cause additional latency and bandwidth overhead [42-46]. Therefore, it is important to carefully balance security requirements with performance considerations to ensure optimal system performance.

The research in this article is a continuation [47], in which the security of the Asterisk IP network using the TLS protocol was previously discussed. This article proposes a four-level protection method, which is further implemented as an application module in Asterisk to ensure secure data transfer.

II. Methodologies

This article outlines the following IP network research tasks:

1) Construction of a simulation model of the studied IP PBX Asterisk network in the Opnet Modeler environment to determine the total load depending on the codec used.

2) Study of the security of the developed network model.

3) Selecting a traffic protocol when passing through an IP network, when the role of a switching station is performed by IP PBX Asterisk.

4) Development of a four-level security model based on the selected encryption algorithm.

5) Implementation and testing of a four-level encryption model.

III. Results

A. Construction of a Simulation Model of the Studied IP PBX Asterisk Network in the Opnet Modeler Environment to Determine the Total Load Depending on the Codec used

To study a four-level network security model, a telecommunications network diagram was simulated, which is presented in Fig. 1.

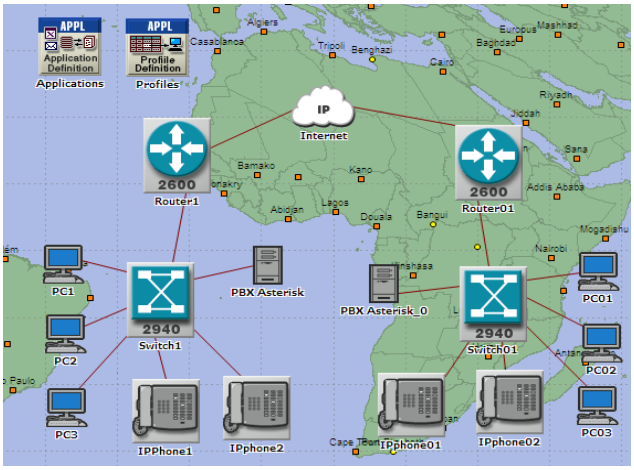

Fig. 1. Diagram of the developed network model using Opnet Modeler.

From Fig. 1 it can be seen that multimedia traffic is transmitted from end nodes consisting of PCs and IP phones using a switch, PBX Asterisk server, and to exit to global network and transmitting it from one local network to another, border router. For communication and simulation in two local area networks, an IP network cloud, the "IP_cloud" object, was taken. The Asterisk PBX server is

configured to serve VoIP traffic.

The developed network model consists of the following devices: IP phones, switches, IP PBX Asterisk servers, routers and IP clouds.

Let's consider the technology of operation of IP phones and conduct a study of the constructed network model shown in Fig. 1.

An IP phone is a device or program that uses Voice over Internet Protocol (VoIP) technology. This technology allows the user to make voice calls over broadband Internet connections rather than the familiar analogue connection.

An IP phone looks like a regular landline phone. The differences lie in the technology of their operation and instead of a pair of copper conductors, VoIP technology uses the Internet to transmit voice calls in the form of data packets.

IP phones use IP packets encoded using codecs to transmit data. IP phones are devices connected to an IP telephony system via a local LAN or the Internet. Please note that analog phones operate on the public telephone network.

By IP address, different gadgets recognize each other and can then transmit data. IP telephony is a telephone connection over the Internet, where telephone numbers are replaced with IP addresses, where it is connected by a provider company that makes calls using special equipment.

What are the advantages: IP telephony has a large capacity; at any time you can connect more lines while uniting all offices into one network. Typically, long-distance and international calls via IP telephony are two to six times less than those made by city and mobile operators.

It is noted that the IP telephony number is a virtual telephone number, that is, the number is not connected to a wired line or device, the IP telephony number is assigned by the IP telephony service provider and allows you to make and receive calls using any internet-connected device, e.g. softphone.

After purchasing the card, dial the telephone number of the IP telephony gateway, you need to switch the phone to tone mode and then dial the card number, its PIN code and the number of the called subscriber with the country and city code. In this case, we do not need a computer or Internet access.

We will conduct a study of such a network after setting up its equipment and selecting the necessary interfaces between them. To do this, we use the buttons of the Opnet modeler main menu located at the top of Fig. 1 and pass VoIP information through the network and launch the modeling process on the network and look at its statistical results.

Fig. 3 shows a graph that, as a result of the simulation, shows the values of packets passed through the network during the

simulated time. It was created as shown in Fig. 2, 156 voice traffic as shown in Fig. 2.

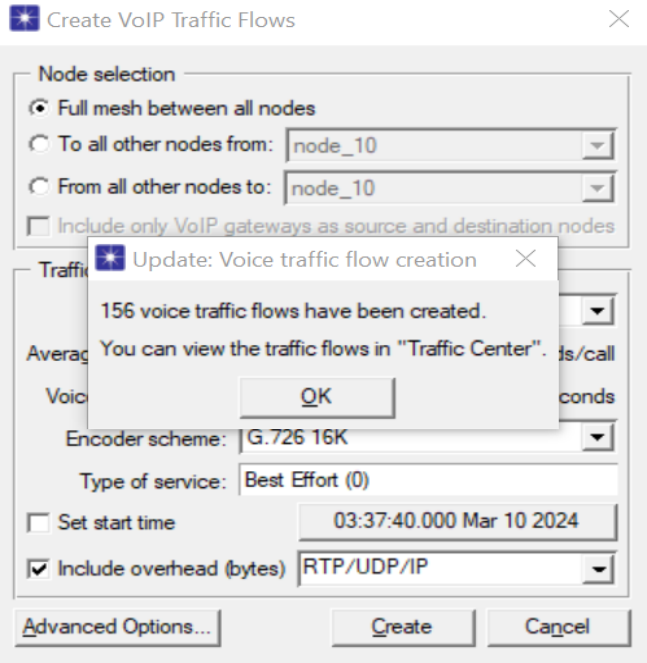

Fig. 2. Result of generating 156 voice traffic of simulation.

As a result of the simulation experiment, voice traffic is created that forms a total load during the simulation time, for example, with the G726.16k codec shown in Fig. 3.

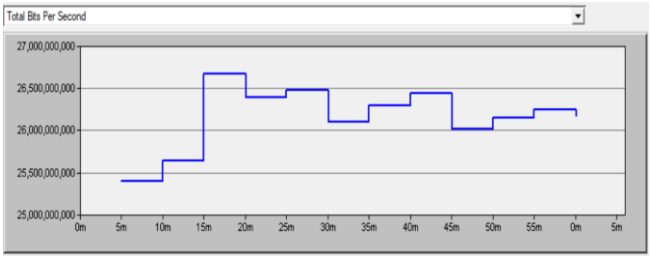

Fig. 3. The result of modeling the traffic passed through the network when the network is operating is based on the G726 codec.

It can be seen from the graph that the total load on the network was more than 26,500,000,000 packets, but the network worked unstably; places in the graph are visible during the model time; as its devices passed through, it increased and then decreased.

This traffic statistics on the network is explained by the fact that various devices, when traffic passed through it, increased or passed fewer packets, and this also depends on what codec is used on the network in IP phones.

For example, when using the G723 codec in IP phones, the number of packets increased to 42,000,000,000, the simulation results are shown in Fig. 4. This is explained by the fact that the number of packets increased due to the fact that the packets became smaller in length, but larger in number and the network worked more stable than with G726.

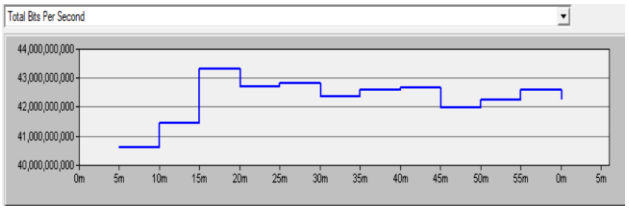

Fig. 4. The result of modeling the traffic passed through the network when network operation based on the G723 codec.

Further research was carried out on the occupied traffic bandwidth depending on the type of voice traffic, the results are shown below in Fig. 5.

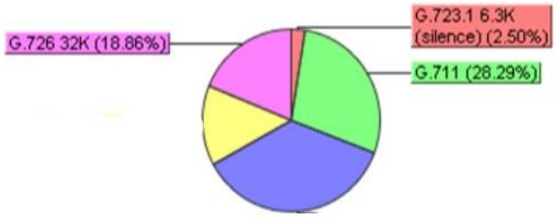

Fig. 5. The result of modeling the traffic passed through the network when network operation.

The result of modeling the occupied volume of voice traffic bandwidth when using codecs: G726. G711. G723.

From Fig. 5 it can be seen that the largest bandwidth in the channel is occupied by the G711 codec, then G726 and the smallest bandwidth by the G723 codec. This is explained by the length of the packet that they form to transmit voice traffic through the channel.

B. Security Study of the Developed Network Model

Now, into the network model presented in Fig. 1, we will introduce the hacker's actions by connecting him to the IP PBX Asterisk server.

Taking into account the risks that were presented at the beginning of the publication, we will conduct a study of the security of such a network. To conduct such a study, it is necessary to connect the Wire Shark program with the Opnet modeler program. To connect these programs, let's launch the ACE module from Opnet modeler to capture packets using Wireshark. To do this, we use the Application Capture Manager module and obtain the results of the attack presented in Fig. 6.

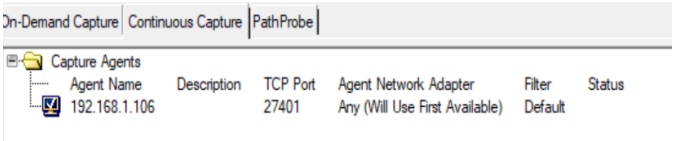

Fig. 6. Result of application capture manager.

By clicking on VoIP traffic and launching Wireshark, a program for capturing packets passing through the network over a certain time, we get the statistics shown in Fig. 6. It is now ready to communicate with Wireshark after it is launched (see Fig. 7).

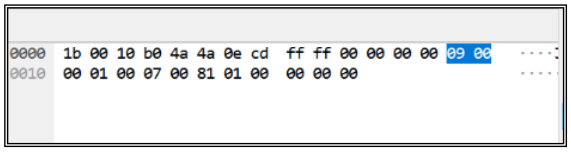

Fig. 7. Packet capture result.

Lastly, by clicking on statistics in the main menu of the Wireshark program, we select the graph submenu and receive captured packets which are shown in Fig. 8.

Fig. 8 shows that the captured packets passed through in a time period from 0 to 3000 seconds and that the packet sizes are different. Packet capture based on Wireshark shows that the network must be protected so that a hacker cannot obtain packets passing through the network, violating confidentiality and integrity voice traffic transmitted over the network.

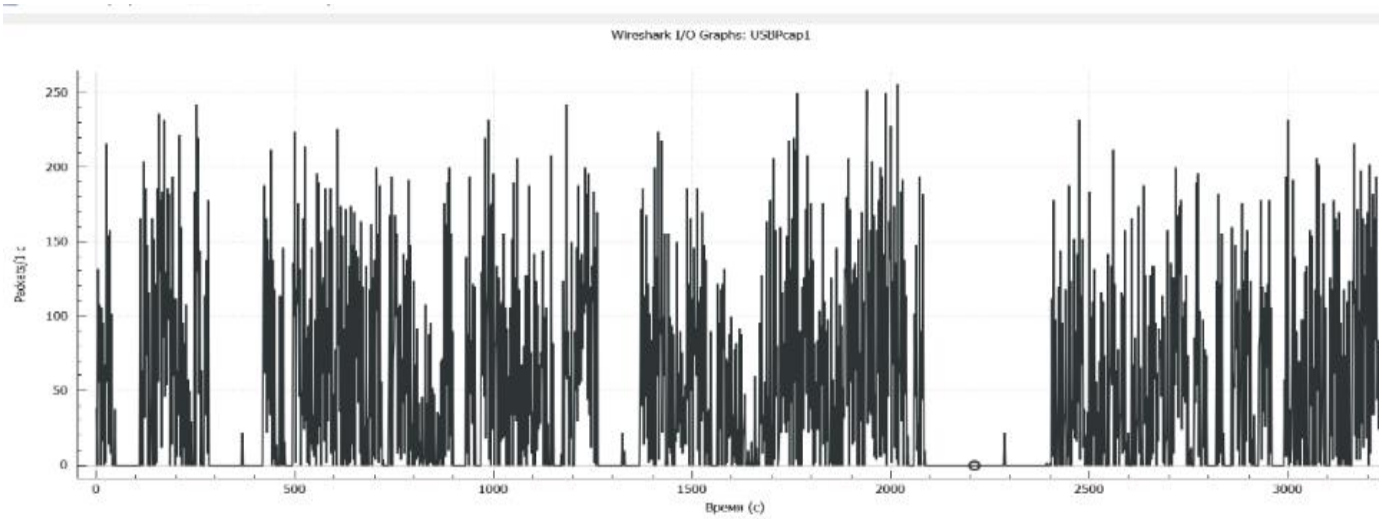

Fig. 8. Packet capture result.

C. *Selecting a Traffic Protocol When Passing Through an IP Network, When the Role of a Switching Station is Performed by IP PBX Acterisk*

Note that among the transport layer protocols UDP and TCP, we prefer the UDP protocol because it is fast. Moreover, the User Datagram Protocol (UDP) is a transport layer network protocol used to establish low-latency and loss-resistant connections between applications on the Internet. It is primarily used for time-critical communications such as DNS (Domain Name System) and Voice over Internet Protocol (VoIP).

In contrast to TCP, which uses handshakes, UDP uses only a minimal number of mechanisms. It provides checksums to ensure the integrity of the data and port numbers to provide other functions and the purpose of the datagram.

The main purpose of UDP is to save time between communication signals, so it uses IP to transfer data from one device to another. It collects data in UDP packets and adds some header information. The data contained in the packet includes destination ports, source, and checksum and packet length.

After the received packets are encapsulated into IP packets, they are sent to the destination based on the packet information. Unlike TCP, which provides feedback, UDP does not send feedback signals to indicate that the packet has reached its destination; instead, it loops the process or stops the sending process.

Unlike TCP, which uses handshakes, UDP uses only a minimal number of mechanisms. It provides checksums to ensure data integrity and port numbers to provide other functions and datagram mappings.

The main purpose of UDP is to save time between communication signals, so it uses IP to transfer data from one device to another. It collects the data in UDP packets and adds some header information. The data contained in the packet includes destination ports, source, and checksum and packet length.

After the received packets are encapsulated into IP packets, they are sent to the destination based on the packet information. Unlike TCP, which provides feedback, UDP does not send feedback signals to indicate that the packet has reached its destination; instead, it performs the process in a loop or stops sending.

UDP Features:

1) Supports connectionless service;
2) Sends packets in large quantities;
3) Mainly used for streaming services and other services such as DNS and NFS;
4) Lack of error control mechanism;
5) No confirmation after sending or receiving package;
6) IP only has inter-process addressing and checksumming built into it;
7) Lack of flow control mechanism;
8) Faster communication than TCP.

As already mentioned, the communication mechanism is ideal for applications such as the Domain Name System (DNS), SNMP, Dynamic Host Configuration Protocol (DHCP) and Routing Information Protocol (RIP).

With this in mind, we choose the UDP protocol for transmitting information over the channel, as the TCP protocol is slow in comparison.

It is known that in the transmission of information over telecommunication networks, an estimation plays a major role - the delay with which the information reaches the receiving end. When transmitting encrypted information, the delays in the channel should not exceed 150 ms. This requirement is fundamental. Therefore, we decided to use the UDP protocol, where the header size of the transmitted packet is 8 bytes, and when using the TCP protocol from 20-80 bytes [44]. In addition, the application area of UDP is: video conferencing, streaming, DNS, VoIP and IPTV.

Protocols are used in tandem to achieve better quality and speed of data transmission and thus the operation of online services. For the transmission of multimedia files, video and audio streaming or streaming, for example, it is better to use UDP technology.

As already mentioned, the communication mechanism is ideal for applications such as Domain Name System (DNS), SNMP, Dynamic Host Configuration Protocol (DHCP) and Routing Information Protocol (RIP). Streaming services also use UDP, as it is generally suitable for video and voice traffic. This is because the use of other protocols such as TCP often results in packet loss in this communication chain, which impairs quality.

D. Analysis and Justification for Ensuring the Security of the Developed Network by Using Multi-level Encryption Technology When Transmitting Information

Note that information security involves practical measures aimed at preventing unauthorized access to stored, processed and transmitted data in networks. In addition, the methods used to ensure it aim to prevent the use, disclosure, falsification, alteration or destruction of data stored on computers, in databases, archives or other storage media.

The main task in creating information security in a company is to protect data, i.e. to ensure its integrity and availability without harming the organization. The information security system is built step by step. Ensuring security is very important when information is transmitted over long distances via different networks. However, we have shown above that if the network is not protected, an attacker can carry out a successful attack and violate the confidentiality, integrity, etc. of the transmitted information.

Therefore, in order to prevent the attacker from accessing the transmitted information, increase the duration of cryptanalysis many times over, for example, by encrypting voice traffic more than once, as usual, and performing encryption in 4 stages.

It is known that even RSA can be hacked to encrypt and decrypt information traversing the network in one layer.

Attackers, for example, had several ways to hack RSA. The most effective attack is to find a private key that matches the required public key.

Another unique application of RSA is to find a method to compute the e-root of mod n. Since $C = M^e \bmod n$, the root of degree «e» of «mod n» is the message M. By computing the root, you can open encrypted messages and forge signatures without knowing the private key, etc.

Source in [45] describes the DES and 3DES cryptosystems and others as they depend on the time of cracking. There are many examples where attackers have tried to obtain encrypted information using various cryptanalysis methods. The important factor here was the time available to the attacker.

For an attacker, the time factor is important when hacking; if it is too long, he cannot obtain the desired transmitted information. It was therefore decided to carry out the encryption in four stages. The time for critical analysis increased 4-fold. The algorithm consisted of the fact that the encryption was performed the first time, i.e. the encrypted text was encrypted a second time. Then the encrypted text was encrypted for the second time for the third time, and finally, the encrypted text was encrypted for the third time for the fourth time. It turned out that the first time the encryption was performed was the length of the packet when it was formed according to a codec, for example G723. The success of attacks depends on the time the attacker spends on cryptanalysis. Therefore, this problem can be solved by increasing this time and at the same time using a cryptosystem for encryption that has not yet been modestly tested in its disclosure and retrieval of the key.

The solution to this problem was to increase the cryptanalysis time for the attacker. In this article, the encryption of packets was performed according to the codec found in IP phones based on the AES cryptosystem in the Python programming language. The key length was set to 128 bits. The UDP protocol was chosen for the reasons mentioned above.

To achieve better quality and speed of data transfer, and, accordingly, the operation of online services, protocols are used in tandem. The block diagram of the program for four levels of encryption is shown in Fig. 9.

The block diagram is built mainly to reflect the four levels of encryption and is very general.

Distribution of encryption time across four levels when operating the G728 codec. Time is located in microseconds on the vertical axis, and different levels are located on the horizontal axis, from the first to the 4th level of encryption in AES in the Python programming language (Fig. 10).

Considering that when encrypting these codecs occurs in a similar way, the experiment of four levels of encryption after codecs G726 G728 and G723 and obtaining the encryption time in microseconds is presented in Table I.

Table I shows that when encrypting information contained in packets of different codecs of the AES cryptosystem on Python, the time from the first encryption level up to and including level 4 changes only slightly.

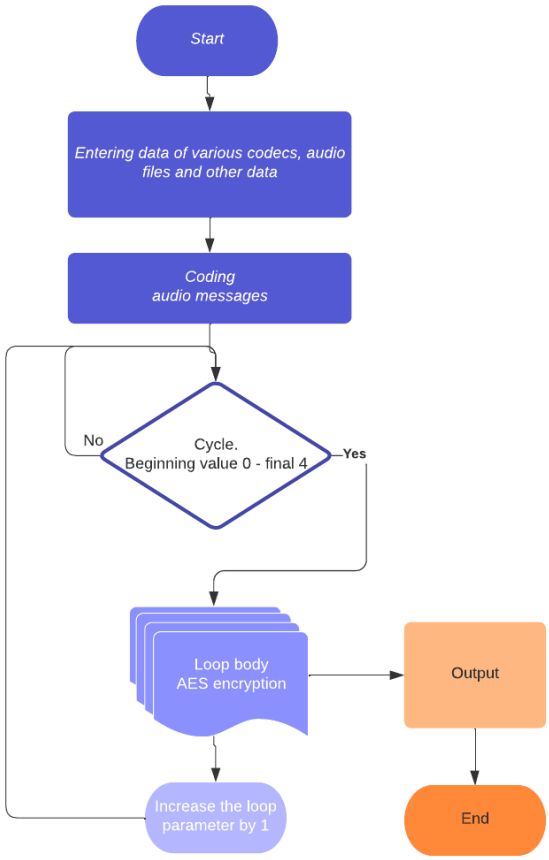

Fig. 9. The block diagram of the four levels of encryption.

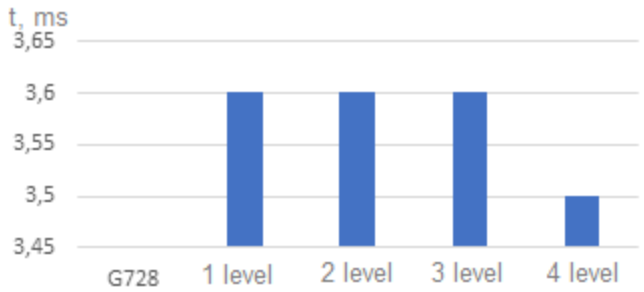

Fig. 10. Encryption time for four levels of G728 codec.

TABLE I. ENCRYPTION TIME FOR THE CODECS IN MICROSECONDS

Levels	Time G726, ms	Time G728, ms	Time G723, ms
1	3,66	3,6	3,67
2	3,62	3,6	3,6
3	3,6	3,6	3,63
4	3,5	3,5	3,4

The encryption time for the G726 codec is only 14.38 ms over four levels, for the G728 codec only 14.3 ms and the G723 codec 14.3 ms.

Decoding the received information takes about the same time. Thus, we conclude that an attacker takes much longer to reveal encrypted information due to the delays in the transmitted encrypted information, so that the information reaches the receiving end while he is busy with cryptanalysis.

The experiment has shown that the encryption and decryption for the G728 codec on four levels is only 14.3 ms x 2 = 28.6 ms, for the G726 codec 14.38 ms x 2 = 28.76 ms and for the G723 ms codec 14.3 ms x 2 = 28.6 ms, as the decryption, i.e. the reverse encryption process, takes the same time as the encryption in Python.

It is known that delays should not exceed 150 milliseconds when transmitting information in a channel. As experiments have shown, when using different speech codecs, the delays achieved on four levels are measured in microseconds.

Therefore, we believe that by increasing the number of encryption levels of the chosen cryptosystem in a programming language and thus increasing the time for cryptanalysis for an attacker, we can achieve a high level of security for IP networks created on the basis of the IP PBX Asterisk used as switches.

The developed technology, in which encryption and decryption is carried out on many levels, is a new technique for increasing the security of IP networks created on the basis of the Asterisk IP PBX, where the encryption and decryption methods were carried out on the basis of the Python programming language4. Discussion Authors should discuss the results and how they can be interpreted from the perspective of previous studies and of the working hypotheses. The findings and their implications should be discussed in the broadest context possible. Future research directions may also be highlighted.

IV. CONCLUSION

The analysis of publications showed that the area of information protection using IP PBX Asterisk has not been fully studied. The article proposes a new protection method based on increasing the number of encryption levels. For this purpose, simulation modeling was carried out on IP network built on IP PBX Asterisk, the Opnet modeler program. For network operation, the UDP protocol is selected for information transmission based on an analysis of sources.

Experiments carried out on a simulation model show that when using various codecs used in IP phones when voice traffic passes, the network operates unstable.

When carrying out an attack on a built network, the hacker captures packets passing through the network, violating its confidentiality and integrity.

An analysis and justification for increasing network security is carried out by developing a new method of protecting IP networks built on IP PBX Asterisk by using multi-level encryption technology when transmitting information.

A new modern method has been developed to increase the security of IP networks built on IP PBX Asterisk by developing multi-level encryption technology of the AES cryptosystem when transmitting information using the Python programming language using G728, G726 and G723 codecs.

The use of four layers of security in a network results in a much longer cryptanalysis time for the hacker, but encryption occurs in a very short time of a few microseconds. Passing

through four encryption and decryption stages occurs in a very short time, e.g. 3 to 4 microseconds when operating various codecs, as the recorded diagrams show. It is assumed that the increase in encryption levels supports the parameter for ensuring the operation of IP networks, when the delays in the transmission of information should not exceed 150 milliseconds.

Thus, the newly developed method of multi-level encryption and decryption of information transmitted over the network can be used in the transmission of confidential information and information that needs to be transmitted in a very short time, when the hacker does not have time to intercept the information, since his efforts will take a lot of time.

ACKNOWLEDGMENT

This research has been/was/is funded by the Science Committee of the Ministry of Education and Science of the Republic of Kazakhstan AP14871745 «Development of a method for improving the security of a telecommunications network based on IP-PBX Asterisk».

REFERENCES

[1] S. S. Kumar, B. Dhivyalekshmi, S. Preethi, and P. Rengaraju, "PBX implementation in LAN using Asterisk open source software," *Int. J. Appl. Eng. Res.*, vol.10, no. 55, pp. 66–69, 2015.

[2] A. Martin, E. Gamess, D. Urribarri, and J. Gomez, "A proposal for a high availability architecture for VoIP telephone systems based on open source software," *Int. J. Adv. Comput. Sci. and Appl*., vol. 9, no. 9, pp. 1–11, 2018. Doi: 10.14569/IJACSA.2018.090901.

[3] M. M. Rahman, and N. S. Islam, "VoIP Implementation Using Asterisk PBX," *J. Bus. Manag*., vol.15, no. 6, pp. 47–53, 2014.

[4] M. F. Anagreh, A. M. Hilal, and T. M.Ahmed, "Encrypted Fingerprint into VoIP Systems using Cryptographic Key Generated by Minutiae Points," *Int. J. of Adv. Comput. Sci. and Appl. (IJACSA)*, vol. 9, no. 1, 2018, doi: 10.14569/IJACSA.2018.090120.

[5] G. Vennila, and M. S. K. Manikandan, "Two stage secure dynamic load balancing architecture for SIP server clusters," *J. of Eng. Sci. and Tech. Review*, vol. 7, no. 3, pp. 1–6, 2014.

[6] P. Kadam, M. Kulkarni, and V. Gaikwad, "Bandwidth Management for VoIP Calling through Asterisk," In Proceedings of the 2nd Global Conference for Advancement in Technology, GCAT 2021. Bangalore, India, 01 – 03 October 2021. doi: 10.1109/GCAT52182.2021.9587544.

[7] D. S. Bhatti, S. Sidrat, Sh. Saleem, A. W. Malik, B. K. Suh, K.-I. Lee, and K.-C. Kim, "Performance analysis: Securing SIP on multi-threaded/multi-core proxy server using public keys on Diffie–Hellman (DH) in single and multi-server queuing scenarios," *PLoS ONE*, vol. 19, no. 1, 2024, doi: 10.1371/journal.pone.0293626.

[8] L. Zhang, X. Hu, W. Rasheed, T. Huang, and C. Zhao, "An Enhanced Steganographic Code and its Application in Voice-Over-IP Steganography," *IEEE Access*, vol. 7, pp. 97187–97195, 2019, doi: 10.1109/access.2019.2930133.

[9] H. Wu, C. Zhu, and G. Cheng, "Real-time Application Identification of RTC Media Streams via Encrypted Traffic Analysis," In Proceedings - International Conference on Computer Communications and Networks (ICCCN 2022), Honolulu, HI, USA, 25-28 July 2022, doi: 10.1109/ICCCN54977.2022.9868928.

[10] C. Shen, E. Nahum, and H. Schulzrinne, "The impact of TLS on SIP server performance," In Proceedings of the IPTComm 2010 - Principles, Systems and Applications of IP Telecommunications 2010, Munich, Germany, 2-3 August 2010, doi: 10.1109/TNET.2011.2180922.

[11] Y. Lu, and D. Zhao, "An anonymous SIP authenticated key agreement protocol based on elliptic curve cryptography," *Math. Biosci. and Eng.* vol. 19, no. 1, pp. 66 – 85, 2022, doi: 10.3934/mbe.2022003.

[12] V. M. Danylchenko, V. R. Mykolaychuk, O. M. Tkalenko, and A.S. Didkivskyy, "Initial setup of PBX server based on Asterisk," *Connectivity*, vol. 148, no. 6, 2020, doi: 10.31673/2412-9070.2020.064448.

[13] H. S. H. Aliwi, and P. Sumari, "IAX-JINGLE Network Architectures Based-One / Two Translation Gateways," *Int. J. of Adv. Comput. Sci. and Appl. (IJACSA)*, vol. 7, no. 5, 2016, doi: 10.14569/IJACSA.2016.070515.

[14] P. Nuno, C. Suarez, E. Suarez, Fr.G. Bulnes, Fr.J. Calle, and J.C. Granda, "A Diagnosis and Hardening Platform for an Asterisk VoIP PBX," *Secur. Commun. Netw.*, 2020, art. no. 8853625, doi: 10.1155/2020/8853625.

[15] Sh. U. Rehman, and S. Manickam, "Denial of Service Attack in IPv6 Duplicate Address Detection Process," ," *Int. J. of Adv. Comput. Sci. and Appl. (IJACSA)*, vol. 7, no. 6, 2016, doi: 10.14569/IJACSA.2016.070630.

[16] W. Nazih, Y. Hifny, W. S. Elkilani, H. Dhahri, and T. Abdelkader, "Countering DDoS Attacks in SIP Based VoIP Networks Using Recurrent Neural Networks," *Sensors*, vol. 20, 2020, doi: 10.3390/s20205875.

[17] A. Zunussov, A. Baikenov, O. Manankova, T. Zheltaev, and T. Zhaksylyk, "Quality of service management in telecommunication network using machine learning technique," *Indonesian J. of Electr. Eng. and Comput. Sci.*, vol. 32, no. 2, pp. 1022–1030, 2023. Doi: 10.11591/ijeecs.v32.i2.pp1022-1030.

[18] P. Krasnowski, J. Lebrun, and B. Martin, "A novel distortion-tolerant speech encryption scheme for secure voice communication," *Speech Commun.*, vol. 143, pp. 57–72, 2022, doi: 10.1016/j.specom.2022.06.007.

[19] S. M. Rosu, M. M.Popescu, G. Dragoi, and I. R. Guica, "Virtual Enterprise Network based on IPSec VPN Solutions and Management" *Int. J. of Adv. Comput. Sci. and Appl. (IJACSA)*, vol. 3, no. 11, 2012, doi: 10.14569/IJACSA.2012.031105.

[20] Q. Shambour, S. N. Alkhatib, M. M. Abualhaj, and Y. Alrabanah, "Effective Voice Frame Shrinking Method to Enhance VoIP Bandwidth Exploitation" *Int. J. of Adv. Comput. Sci. and Appl. (IJACSA)*, vol. 11, no. 7, 2020, doi: 10.14569/IJACSA.2020.0110741.

[21] D. Barison, R.S. Miani, L. De Souza Mendes, "Evaluation of quality and security of a VoIP network based on asterisk and Open VPN," In Proceedings of the International Conference on Security and Cryptography 2009, Milan, Italy, 7–10 July 2009, pp. 144–147, doi: 10.5220/0002228101440147.

[22] O. A. Manankova, M. Z. Yakubova, M. A. Rakhmatullaev, and A. S. Baikenov, "Simulation of the Rainbow Attack on the SHA-256 Hash function," *J. of Theoret. and Appl. Inf. Tech*., vol. 101, no. 4, pp. 1594–1603, 2023.

[23] L.R. Costa, L.S.N. Nunes, J.L. Bordim, K. Nakan, "Asterisk PBX Capacity Evaluation," In Proceedings of the IEEE International Parallel and Distributed Processing Symposium Workshop, 2015, Hyderabad, India, 25–29 May 2015; pp.519–524, doi: 10.1109/ipdpsw.2015.90.

[24] M. Kolhar, "Web Server Performance Evaluation in a Virtualisation Environment" *Int. J. of Adv. Comput. Sci. and Appl. (IJACSA)*, vol. 8, no. 2, 2017, doi: 10.14569/IJACSA.2017.080210.

[25] D. Pal, T. Triyason, V. Vanijja, "Asterisk server performance under stress test," In Proceedings of the IEEE 17th International Conference on Communication Technology (ICCT) 2017, Chengdu, China, 27–30 October 2017; pp.1967–1971, doi: 10.1109/icct.2017.8359973.

[26] S. Deepikaa, and R. Saravanan, "VoIP steganography methods, a survey," *Cybernetics and Inform. Tech.*, vol. 19, no. 1, pp. 73–87, 2019, doi: 10.2478/CAIT-2019-0004.

[27] A. H. Ali, M. R. Mokhtar, L. E. George, "Recent approaches for VoIP steganography," *Indian J. of Sci. and Tech.*, vol. 9, no. 38, 2016, doi: 10.17485/ijst/2016/v9i38/101283.

[28] D. Soundararajan, and S. Ramakrishnan, "Coverless Data Hiding in VoIP based on DNA Steganography with Authentication," *Int. Arab J. of Inf. Techn.*, vol. 20, no. 2, pp. 190–198, 2023, doi: 10.34028/iajit/20/2/5.

[29] S. Yazdanpanah, M. Kheyrandish, and M. Mosleh, "LSBR Speech Steganalysis Based on Percent of Equal Adjacent Samples," *J. of Circuits, Syst. and Comput.*, vol. 31, no. 6, 2022, doi: 10.1142/S0218126622501183.

[30] B. Q. Abd Ali, H. I. Shahadi, M. S. Kod, and H. R. Farhan, "Covert VoIP Communication based on Audio Steganography," *Int. J. of Comput. and Digit. Syst*., vol. 11, no. 1, pp. 821–830, 2021, doi: 10.12785/IJCDS/110167.

[31] H. Moodi, and Ah. R. Naghsh-Nilchi, "A New Hybrid Method for VoIP Stream Steganography," *J. of Comput. and Sec.*, vol. 3, no. 3, pp. 175-182, 2016.

[32] M. Kara, H.R.J. Merzeh, M. A. Aydın, and H. H. Balık, "VoIPChain: A decentralized identity authentication in Voice over IP using Blockchain," *Comput. Communicat.*, vol. 198, pp. 247–261, 2023, doi: 10.1016/j.comcom.2022.11.019.

[33] O. Younes, and U. Albalawi, "Securing Session Initiation Protocol. *Sensors*, vol. 22, no. 23, 2022, doi: 10.3390/s22239103.

[34] J. Peng, and S.Tang, "Covert Communication over VoIP Streaming Media with Dynamic Key Distribution and Authentication," *IEEE Transact. on Industrial Electr.*, vol. 68, no. 4, pp. 3619–3628, 2021, doi: 10.1109/TIE.2020.2979567.

[35] J. Saenger, W. Mazurczyk, J. Keller, and L. Caviglione, "VoIP network covert channels to enhance privacy and information sharing," *Fut. Gener. Compu. Syst.*, vol. 111, no. 2020, pp. 96-106, 2020, doi: 10.1016/j.future.2020.04.032.

[36] Th. Surasak, and H. C.-H. Scott, "Enhancing VoIP Security and Efficiency using VPN," In Proceeding of the International Conference on Computing, Networking and Communications, ICNC 2019, Honolulu, HI, USA, 18-21 February 2019, 8685553, pp. 180 – 184, doi: 10.1109/ICCNC.2019.8685553.

[37] R. Ch. Rao, K. Lakshmi, Ch. Raja, P. Varma, G. R. K. Rao, and A. Patibandla, "Real-Time Implementation and Testing of VoIP Vocoders with Asterisk PBX Using Wireshark Packet Analyzer," *J. Intercon. Netw.*, vol. 22, 2022, doi: 10.1142/S0219265921410309.

[38] Z. Ayan, B. Alimzhan, M. Olga, Z. Timur, Z. Toktalyk, "Quality of service management in telecommunication network using machine learning technique," *Indonesian J. of Electr. Eng. and Comput. Sci.*, vol. 32, no. 2, pp. 1022–1030, 2023, doi: 10.11591/ijeecs.v32.i2.pp1022-1030.

[39] Z. Yang, H. Yang, C.-C. Chang, Y. Huang, and C.-C.Chang, "Real-time steganalysis for streaming media based on multi-channel convolutional sliding windows," *Knowledge-Based Syst.*, vol. 237, 2022, doi: 10.1016/j.knosys.2021.107561.

[40] H. A. Rahman, A-A. Mwaffaqa, and N. Kholoudb, "New RTP packet payload shrinking method to enhance bandwidth exploitation over RTP protocol," *Int. J. of Advanced Comput. Sci. and Appl.*, vol. 11, no. 8, pp. 139 – 143, 2020, doi: 10.14569/IJACSA.2020.0110818.

[41] Sh. Qusaia, N. A. Sumaya, M. A. Mosleh, and A. Yousefa, "Effective voice frame shrinking method to enhance voIP bandwidth exploitation," *Int. J. of Advanced Comput. Sci.and Appl.*, vol. 11, no. 7, pp 313 – 319, 2020, Doi: 10.14569/IJACSA.2020.0110741.

[42] J. Papan, P. Segec, and M. Kvet, "Enhanced Bit Repair IP Fast Reroute Mechanism for Rapid Network Recovery," *Appl. Sci.*, vol. 11, no. 7, 2021, doi: 10.3390/App11073133.

[43] RFC: 793 - Transmission Control Protocol (TCP).

[44] Sh. Varshney, L. M. Gupta, and A. Gupta, "Performance Analysis of Cryptography Algorithms: Blowfish, DES, 3DES, AES, MARS& RC6 with Data Hiding In Images Using Steganography," *Tech. Int. J. of Innovat. Res. in Sci., Eng. and Tech.*, vol. 8, no. 5, pp. 4787 – 4795, 2019, doi:10.15680/IJIRSET.2019.0805007.

[45] A. H. Y.Mohammed, R. A. Dziyauddin, and L. A. Latiff, "Current Multi-factor of Authentication: Approaches, Requirements, Attacks and Challenges," *Int. J. of Adv. Comput. Sci. and Appl. (IJACSA)*, vol. 14, no. 1, 2023, doi: 10.14569/IJACSA.2023.0140119.

[46] S. Ghoul, R.Sulaiman, and Z. Shukur, "A Review on Security Techniques in Image Steganography," *Int. J. of Adv. Comput. Sci. and Appl. (IJACSA)*, vol. 14, no. 6, 2023, doi: 10.14569/IJACSA.2023.0140640.

[47] M. Yakubova, O. Manankova, A. Mukasheva, A. Baikenov, and T. Serikov, "The Development of a Secure Internet Protocol (IP) Network Based on Asterisk Private Branch Exchange (PBX)," *Appl. Sci. (Switzerland)*, vol. 13, no. 19, 2023, doi: 10.3390/app131910712.