Journal of Theoretical and Applied Information Technology
31st July 2021. Vol.99. No 14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ANALYSIS AND RESEARCH OF THE SECURITY OF A WIRELESS TELECOMMUNICATIONS NETWORK BASED ON THE IP PBX ASTERISK IN AN OPNET ENVIRONMENT

[1] MANANKOVA O.A, [1] YAKUBOV B.M., [2] SERIKOV T.G., [1] YAKUBOVA M.Z., [1] MUKASHEVA A.K.

[1] Almaty University of Power Engineering and Telecommunications named after Gumarbek Daukeyev, Almaty, Kazakhstan

[2] Kazakh Agrotechnical University named after S.Seifullina, Nur-Sultan, Kazakhstan

E-mail: [1]o.manankova@aues.kz, [1]b.yakubov@aues.kz, [2]tansaule_s@mail.ru, [1]m.yakubova@aues.kz, [1]a.mukasheva@aues.kz

ABSTRACT

To date, widespread is the connection to the Internet, which is a global public IP network with a large number of IP users and increased requirements for the capabilities of IP networks, using them not only for data transmission, but also for interactive video conferencing, transmission of voice information streams and for other real-time applications. Growth of network resources' users entails the emergence of a large volume of transmitted information and the problem of reliable, secure data transmission, that is, to the problem of information security. The solution to this problem is the use of encryption algorithms, as well as the choice of the OS server, configuration and settings of the Asterisk software firewall. In this regard, this publication has developed a simulation model of a wireless telecommunications network based on PBX Asterisk software IP consisting of wireless devices -workstations, border wireless router, Asterisk server, IP cloud, Wireshark traffic analyzer and others. Using the NetDoctor utility of the Opnet environment, the security of the configuration of the built simulation model of the wireless telecommunications network based on the PBX Asterisk IP software was checked. To carry out simulation modeling of the developed network, settings of all network equipment are performed and experiments are carried out on it, as a result of which it is established that when using the G711, G729, G726 and G728 codecs, small delays are obtained in the interval Router 1 - IP Cloud - Router 2 when using the G711. The rest of the codecs have low latency values at other network sites. Also, a passive attack was performed on the network based on the Wireshark traffic analyzer to determine the protocols, connection time, IP addresses of the network to study the security of the wireless network. The obtained results are aimed at using them in the design of new networks or their modernization.

Keywords: *IP PBX Asterisk, NetDoctor, Opnet Environment, Wireshark, Wireless Telecommunications Network, Traffic Analysis, Passive Attack, Codec*

1. INTRODUCTION

IP telephony is a promising and real way of communication. Given the speed of the Internet growth and the geography of users, IP telephony is a rational means of communication, because it has minimal communication costs. IP telephony provides many functions in contrast to traditional telephony. To switch to IP telephony, one needs to select a customer gateway and subscriber network deployment platform.

Today, the use of Cisco IP PBX, Avaya IP Office and IP PBX Asterisk is common.

Cisco IP PBX is designed both for large enterprises with up to 30,000 subscribers and for enterprises with a number of users from 25 to 1000. It has a full set of functions, meets the stability of work and high performance. Cisco offers a number of tools that include auto attendant, instant messaging, voice mail, video conferencing, and other tools available on the Cisco IP PBX platform. The main disadvantage is the cost of the software. Companies that are interested in high performance and mobility have to pay a lot of money.

Avaya IP Office. The IP Office is designed for medium sized networks. The server capacity and the number of licenses limit the number of

users. Expansion cards and applications must be licensed. A variety of programs can be used to manage the server. Avaya IP Office Manager is the most suitable solution because the program is quite easy to use; console control is possible using Avaya Terminal Emulator.

IP PBX Asterisk is a free software product that is easy to set up and use. Asterisk IP telephony PBX IP system, which allows working in internal and external networks. The PBX has unlimited functional space and can be expanded if necessary. The PBX can continue to be configured in various directions; it is possible to optimize the created server for a specifically created server or for a specific task. It is possible to record voices, call forwarding, conferences, etc. software PBX capable of switching both VoIP calls and calls made between IP phones and the PSTN. It is designed for small businesses, the number of subscribers is limited by the server's capabilities, and one of the advantages is customization flexibility. All the necessary functionality can be added independently without financial costs in a short time interval, since one module is applied per task. Compared to Cisco or Avaya, the Asterisk IP PBX has a low deployment cost. Since the program is free, all costs are spent on the purchase of phones and a server necessary for the normal operation of the PBX. Due to these advantages of IP PBX Asterisk, the object of research is the IP-telephony network based on Asterisk.

2. GOAL SETTING

To determine the current state of research in the field of software IP PBX Asterisks, a review of foreign and domestic sources was carried out.

The publication [1] analyzes denial of service or DoS attacks and ways to counter them in a network based on SIP session initiation protocol. In [2], a unique technique for searching video flaws arising during video calls based on MSU VQMT software was developed when searching for defects. It is supposed to carry out testing for any IP-line for transmission of video calls per unit of time in wired and wireless networks

In article [3], sim-real simulation differs from a wireless sensor network model entirely based on OpnetModeler to a real cloud-computing center. The comparison shows that semi-physical modeling is more reliable.

The article [4] assesses the efficiency of web applications between two wireless networks such as WiMAX and WIFI, studies various QoS mechanisms, where it is noted that the WiMAX network has the best QoS parameters.

The purpose of the study [5] was to solve the problems of developing countries in relation to communication costs. By offering a test base using Zoiper and Asterisk server for intranet VOIP applications as a way of solving problems, where the results show that such a solution is efficient and cost-effective for institutions in developing countries.

Real-time launch vehicles must account for latency and noise in wireless environments. The system proposed in [6] will collect information on acceleration obtained from several sensors. This is why the network simulation software evaluates the effectiveness of these sensors in terms of their latency and throughput. The factors are analyzed using the OPNET simulator to understand the operation of the sensors.

Research carried out in [7] reveals methodological recommendations and measures used in the design and implementation of a prototype for observing and monitoring light and electronic devices via PBX, using a IoT-based wireless solution, using both Arduino and Raspberry access and development platforms, obtaining energy cost efficiency.

Article [8] presents the analysis of the program of resistance of the automatic telephone exchange based on Asterisk NOW from unauthorized access to the telecommunication network. An Asterisk based software product is now used as a server. The attacking device is a laptop with CommView for WiFi software installed. Based on the test results, a network vulnerability analysis was carried out. Recommendations on measures of protection against unauthorized access are given. The optimal option of network protection is suggested.

Publication [9] discusses wireless extension of the corporate network. Base stations are connected between PBX to PBX, and then the PBX is connected to the public switched telephone network. An analytical model for ATS resources planning is proposed. Based on the workload of the PBX, the analytical resource-planning model provides recommendations for determining the throughput of the PBX and base stations.

Publication [10] is dedicated to testing a software product necessary to deliver a good product before it enters the market. Test sets are created to automate tests, but also to reduce runtime by running multiple test sets at the same time and providing the developer with a high-end user interface for testing private branch exchange functions.

It is known that the use of IP telephony technology can reduce the cost of designing and maintaining telecommunication networks. When designing an IP network, a minimum set of network equipment is used. To evaluate and select equipment for creating a network, one must first analyze and calculate indicators that affect the network efficiency. Among these indicators, the total load on the network, channel bandwidth, the number of channels and delays in the transmission of information over the network is what has significant effects.

In work [11], a detailed approach to modeling and successful deployment of a network for the transmission of VoIP traffic is presented based on a study of VoIP traffic characteristics and QoS requirements for various simulation configurations.

According to [12, 15], large packet sizes significantly reduce the efficiency of the network, as transmission delays will be high and communication quality will be poor. In turn, small packets increase the share of overhead, since they contain a fixed-length header, and as the packet size decreases, the number of packets into which messages are split increases dramatically, which leads to an increase in the transmitted traffic in the network.

Therefore, it is necessary to have the optimal length of the transmitted packet to ensure maximum efficiency and high quality of service for network users. It is very difficult to determine the optimal parameters with high accuracy, because they depend on many factors, some of which are constantly changing as the network operates. For example, the amount and type of traffic, when transmitting packets over the network, the amount of delays, since when developing a network, developers use the limits within which the packet length, or rather its data field, can be located, while the header, as a rule, has a fixed length [13].

In the publication [14, 16], modeling and research of a telecommunication network based on IP-telephony technology in the transmission of VoIP traffic using various types of codec was carried out. According to the results of the study, it was revealed that the G.711 codec has better parameters compared to G. 723 and G. 729.

Based on this, the analysis and study of the security of a wireless telecommunication network based on IP PBX Asterisk and the development of a simulation model of a wireless network in the Opnet environment, based on the developed methods, based on the results of the experiments, makes it possible to determine the main network parameters, such as packet delay, bandwidth depending on the type of traffic that is relevant. The results obtained are aimed at using them in the design of new networks or their modernization.

3. ANALYSIS OF SYSTEMS FOR SIMULATION OF TELECOMMUNICATION NETWORKS

There are many software packages for simulation modeling that allow you to analyze and study the characteristics of telecommunication networks being developed. The problem of choosing an environment that will meet scientific and modern trends is relevant.

There are the following important points of simulation modeling - system dynamics, discrete-event and the so-called agent-based modeling method (Figure 1). Figure 2 provides discrete and continuous simulation tools.

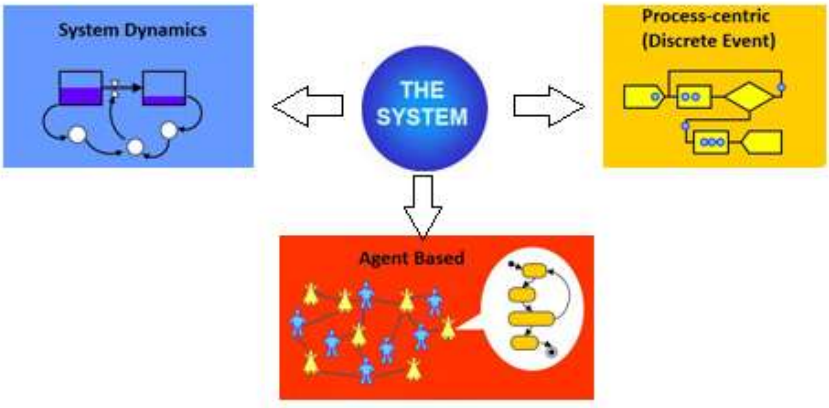

Figure 1: Types of simulation tools

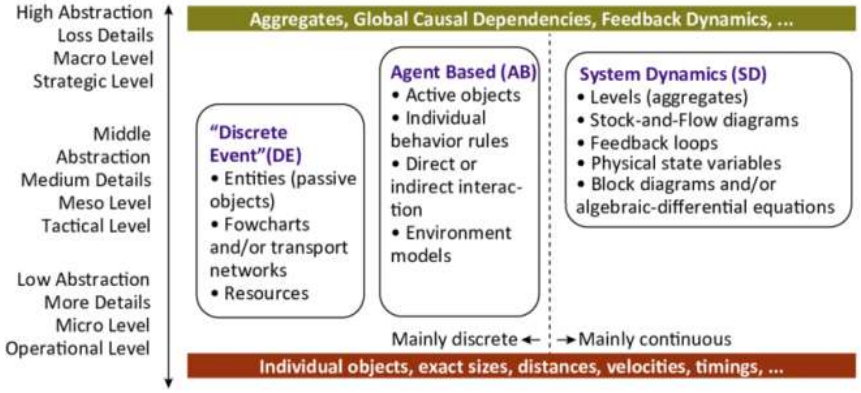

Figure 2: Discrete and continuous simulation tools

Dynamic systems are represented by algebraic equations, differential equations and also block diagrams. The system-dynamic approach, being a powerful toolkit, is intended for the purpose of methods for studying dynamic processes aimed at mastering complex systems with feedback.

Processes are depicted as diagrams, consisting of loops of positive and negative opposite connections. The main focus is on modeling feedbacks. The result of modeling a system-dynamic model is the definition of global dependencies and cause-and-effect relationships in the system under study.

Discrete-event modeling has received the most widespread method of simulation modeling, the range of its use is very wide: logistics, socio-economic processes, communications and others.

The agent-based modeling base shows the "agent" consideration - a creature that has energy at its disposal, independent behavior, which can make decisions in accordance with some set of rules, interact with the sphere, and also modify independently. State maps are considered to be the main parts of agent-based modeling. Agent-based modeling is used to replicate mental, decentralized and partitioned systems in order to acquire knowledge about the impact on the system of activities and the mismatch of elements or analysis.

The most significant are the corresponding parameters of the simulation modeling field.

1. The main characteristics, which include the following features - the use of various paradigms of the IM, the description of the logic of the object's behavior in the built-in language, ease of mastering the modeling environment, support for hierarchical modeling of complex systems, the ability to interactively debug and develop an interface for the user of the model, import and data export, ensuring the development of modeling scenarios, support for continuous-discrete modeling, communication of the IM environment with other software.

2. Hardware and software requirements - the capacity of RAM, type and version of the operating system.

3. Realization of three-dimensional animation and dynamic graphics, which provide visualization of the model and display of its parameters (clock, scales, graphs, and so on).

4. Various statistical capabilities, such as the ability to specify flows of independent random variables, the ability to specify empirical distributions, the implementation of independent runs of the model, the planning of statistical experiments, optimization of the model parameters.

5. Assistance to the user of the sphere (presence of reference material, demos and technical assistance execution, ensuring communication with external applications).

6. Creation of reports with output data, graphs, diagrams, estimation of model parameters, documentation, debugging and analysis, optimization of the simulated system model.

The development of all the considered simulation tools began at the end of the 20th century and is associated with the rapid development of the hardware base of computing systems.

It is necessary to further highlight two features – independence from the operating system (significantly reduces the likelihood of developing and presenting models) and developing an interface for the model user (allows the customer not to purchase the expensive field of simulation and provides model developers with the storage of commercial secrets).

Specialized simulation environments are distinguished by the assistance, as templates, of already built objects that simulate elements and production processes. Universal spheres simulate

production systems, but will take a significant amount of time to develop a model. However, they have the potential to implement custom libraries and templates.

Regardless of the selected approach, the main factors to develop simulation models are possible with the correctly set task, the correctness of the initial data taken and the adequacy of the model.

In addition, during the entire process of developing a simulation model, special attention is required to be paid to documenting and visualizing the acquired results, which makes it possible to facilitate reuse and improve the reliability of the model.

Depending on the required amount of abstraction, different paradigms of simulation modeling can be used to simulate communication systems.

For example, at the level of global interconnections, system dynamics is used. A dynamic systems approach can be used to simulate production processes. It is possible to evaluate the impact of the behavior of elements on the operation of the system with the assistance of agent-based modeling.

At present, there is a whole sequence of well-known simulation modeling systems of a diverse class - from elementary programs assigned to be introduced on an individual computer to large systems that have libraries of many commercially available devices in the communications industry and allow a large extent to automate the research of the analyzed network. The analyzed environments allow you to organize models of continuous and discrete systems with the assistance of a dynamically systematic approach.

Here are the most commonly used simulation software:

OPNET is recommended for virtual networking that simulates the state of authentic networks using routers, switches, protocols, servers, and native applications. Ability to import and export topology and network traffic data. Analysis of the impact of client-server applications and new technologies on network performance. Modeling of hierarchical networks, multi-protocol, local and global networks; accounting for routing algorithms. Object oriented approach. Comprehensive library of protocols and objects.

Packet Tracer is a data network simulator manufactured by Cisco Systems. Allows you to create layouts of networks, check network topology for operability. However, the implemented functionality of the devices is limited and does not provide all the capabilities of real equipment.

GNS3 is an environment for simulating computer networks using network equipment based on processors with an architecture that maintains performance through simple short instructions. These network devices include, among others, most of the network switches and routers manufactured by CISCO.

Table 1 provides a brief comparative description of simulation environments.

Table 1: Characteristics of simulation software

Features	Packet Tracer	GNS3	Opnet
Cost	free	free	silence
Type	simulator	emulator	simulator
Hardware Requirements	High CPU Actual RAM	High CPU 512MB RAM	High CPU 512MB RAM
Language Support	Cisco CLI	Cisco CLI	C++/Java
Visualization	yes	Topology only	yes
Use real-time equipment	no	yes	yes
Graphics data analysis	no	no	yes
Set of programs	no	Wireshark, VirtualBox, QEMU, WinPCAP	NetDoctor, Netbiz, ITGuru, Wireshark

Thus, simulation modeling is one of the most common methods of operations research. This type of modeling is used as a limited method for decision-making in agreements in terms of vagueness, taking into account the presence of heavily formalized technologies in models.

It is well-known that a simulation model is a computer program that depicts a configuration device and depicts the behavior of a genuine object over a period of time. The model produces a detailed picture of the system under study. To provide maximum flexibility in modeling, there is simulation modeling. The simulation model usually allows obtaining detailed statistics on various aspects of the functioning of an object, determined by various input parameters.

When carrying out simulation modeling of a wireless telecommunications network, the OPNET tool was chosen, which allows you to build networks and select equipment from the library and, after setting them up, conduct experiments on the developed simulation model of the network with obtaining graphical results.

4. SIMULATION OF A WIRELESS TELECOMMUNICATIONS NETWORK IN THE OPNET ENVIRONMENT

In this publication, a simulation model of a wireless telecommunications network using IP PBX Asterisk software is built on the basis of the Opnet Modeler modeling tool.

Table 2 shows the content of the studied network by elements, Cisco equipment, the number of interfaces, formed streams and one IP cloud and other configuration elements.

At the heart of any IP telephony network is a network switch. All devices, ip-phones, gateways, IP PBX, personal computers, etc. are connected through this switch.

Table 2: Elements of the designed network

Quantity	Component	Resource Base	Description
10	wlan_wkstn (Mobile node)	wireless_lan	Computers (mobile node)
2	Sip_proxy_server	Fixed node	Asterisk Server
1	IP32_cloud	Node models	Cloud Internet over IP
2	Rtr_CS_3600	Cisco (node models)	Router
2	wlan_ethernet_router	wireless_lan	Wireless LAN и Ethernet IP Router
5	100BaseT	internet_toolbox	Interconnections
1	Application Config	wireless_lan	Defines standard and custom applications used in simulation modeling, including traffic and QoS parameters
1	Profile Config	wireless_lan	Defines the modes of use of the application by a user or a group of users
1	Attacker	SITL link	OC with an installed Wireshark Software

Figure 3 shows that traffic is transmitted from end nodes consisting of wireless PCs, using a switch as an access point, an Asterisk PBX server, and to access the global network and transfer it from one local network to another, an edge router.

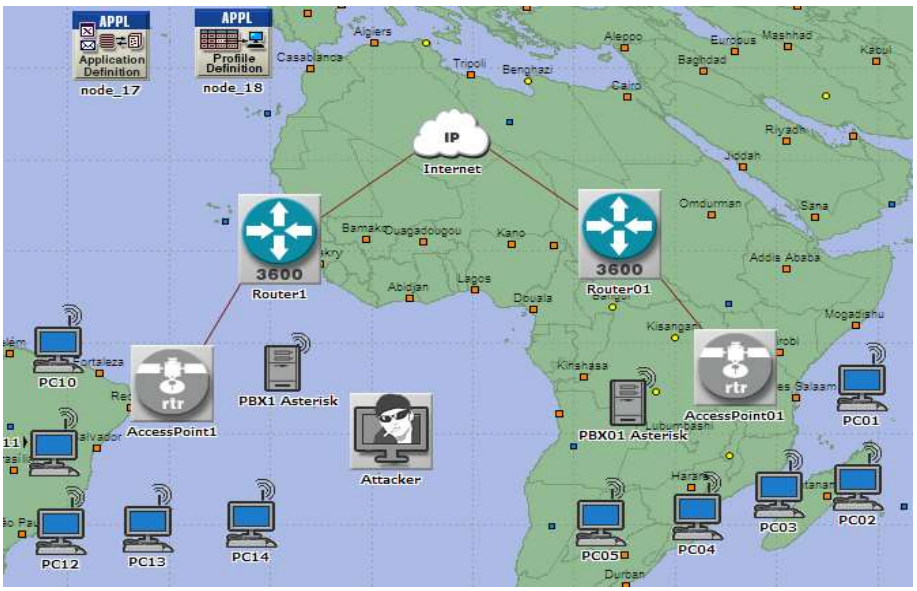

Figure 3: Simulation Model Of A Wireless Telecommunications Network

For communication and simulation in two local area networks, the IP network cloud, the "IP_cloud" object, was taken. The Asterisk PBX server is configured to serve VoIP traffic (Figure 3), depending on the selected scenario, the equipment in the network was configured with

parameters using the G711, G729, G726 and G728 codecs (Figure 9).

It is known that very often when building telecommunication networks on the desktop of the Opnet Modeler software package, questions arise about the reliable and safe construction of a simulation model of the analyzed network, shown in Figure 3. To solve this problem, the NetDoctor utility is used in Opnet Modeler. Therefore, we are going to consider and use its purpose and capabilities for the network we built, shown in Figure 3.

The NetDoctor software module is included in several Opnet products, such as Opnet IT Guru, SP Guru, Opnet Modeler, and is designed to analyze the settings of network nodes. It allows you to detect incorrect settings and parameters, violations of the security policy for the network segment, inefficient use of equipment, and more.

NetDoctor helps to uncover hidden network problems that can be difficult to pinpoint due to the distribution of configuration information across multiple network devices. The devices themselves, as a rule, are separated in space, which also does not contribute to the ease of access to their settings for analyzing and compiling an overall picture of what is happening on the network. With the help of NetDoctor, we can judge how our network meets the required parameters and characteristics given in its design and operation [18, 19].

Network administrators and integrators can use this utility to solve the following groups of tasks:

- finding network nodes whose settings are causing poor network performance, when it is often possible to identify specific configuration details that are causing problems. This information contains the Errors message from NetDoctor Reports.

- finding latent problems that may affect the network in the future, subject to the occurrence of a certain event or series of events (for example, a successful DoS attack on the network firewall). This information contains the Warnings message from NetDoctor Reports.

- checking that the network settings are in accordance with the policy adopted for the organization.

In a network administrator's environment, when it comes to policies, security policies are usually implied, and there are many varieties of them. You can operate with the policy in this case, - the configuration. The latter tell administrators and analysts how much everything conceived by designers and installers has been translated into reality. Therefore, a network can consist of routers in the core of its network, but due to inaccuracies in the settings of the routing protocols, the overwhelming majority of traffic flows will pass through less efficient devices. On the one hand, this leads to the appearance of bottlenecks in the network; on the other hand, it indicates the ineffective use of the network equipment fleet.

NetDoctor allows one to check the performance of the settings of network nodes before they are fully deployed in real conditions, helping to prevent possible errors.

Examples of using NetDoctor include identifying duplicate IP addresses of network nodes, finding links to nonexistent routes in the configuration files of routers, detecting inconsistencies in the settings of their network interfaces, and so on.

For operation, NetDoctor primarily uses information from configuration files of devices that make up the network under investigation for the case when network topology is created by importing node settings files, or device parameters from the project editor, when the topology and all additional settings are performed manually.

However, for some rules, this information is not sufficient. For example, to determine the correctness of the firewall, if there is no idea about the traffic flows passing through it, you may additionally need to run the Flow Analysis module or perform discrete modeling to provide NetDoctor with “material” for further analysis. In general, sequential processing of the network by several utilities (Flow Analysis, NetDoctor, etc.) is practiced, since this allows one to obtain comprehensive information about the network under study, and therefore, to develop solutions for its construction or modernization that are closest to optimal.

The NetDoctor module operates following two types of rules - verification and summary.

Validation rules generate error messages, warning messages and other messages that allow us to judge about incorrect settings, the existence or possible occurrence of conflicts in the network and other events that, according to NetDoctor, do not fit into the pattern of normal operation.

The summary rules display information about the settings of network nodes and the performance of network operations. For example, one of these rules can provide information about the operating systems installed on client machines, or you can determine the number of routers on which BGP is configured.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

All NetDoctor verification messages can be divided into three categories:

- Error – indicates that the identified problem is critical for the network, and will negatively affect the deployment of a real network configuration. Such problems must be identified and eliminated without fail, otherwise no correct operation of the network can be guaranteed.

- Warning – this problem is not critical for the network, but may lead to a deterioration in its characteristics, and decreased quality of service, etc.

- Note – additional information about network objects that may be useful.

Let's simulate NetDoctor for our network shown in Figure 3. To do this, run this module from the Opnet Modeler main menu and get the data in Figure 4.

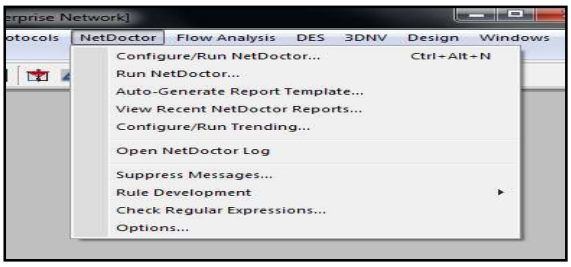

Figure 4: NetDoctor Startup

Figure 4 shows all the submenus of the NetDoctor utility, but to check the network configuration, you must run the Open NetDoctor Log submenu. While starting it, we get Figure 5.

Figure 5: Results of using the NetDoctor module of the Opnet Modeler software package

In Figure 5, you can see that the Error characteristic indicating that the identified problem is critical for the network and will negatively affect the deployment of a real network configuration. It is absent and when such a problem an English word Error appears on the right, Error appears and the color of the line turns yellow instead of green. But in this case the data on the right indicates that the configuration is correct and there are no errors in the network segments. Such problems must be identified and eliminated without fail, otherwise the correct operation of the network cannot be guaranteed.

5. RESULTS OF SIMULATION OF A WIRELESS TELECOMMUNICATIONS NETWORK IN THE OPNET ENVIRONMENT

The collection of statistical data on delays and throughput values was carried out when traffic passes through various scenarios using codecs from one node to another throughout the IP network using Asterisk PBX during a model time of 1 hour. Based on these data, graphs are built (Figure 7-8).

Analyzing the works [8, 15], the G.711 compression codec was selected for the simulation of multimedia traffic. The simulation results are shown in Figure 6.

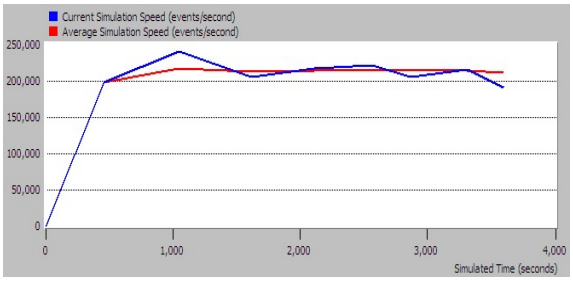

Figure 6: Distribution of traffic speed

Figure 6 shows simulation results when the packets pass through the telecommunications network:

- current value of the speed of traffic passing through the network (blue curve),

- average speed value (red curve)

Journal of Theoretical and Applied Information Technology
31st July 2021. Vol.99. No 14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

In Figure 6, the current and average values of speeds are close to each other in magnitude; this indicates a stable operation of the network when modeling.

As a result of simulation and study of traffic transmission scenarios, indicators of the distribution of traffic passing through different equipment were obtained (Figure 7), which shows on which network section from router 1 - IP router 2 more traffic passed at a higher speed.

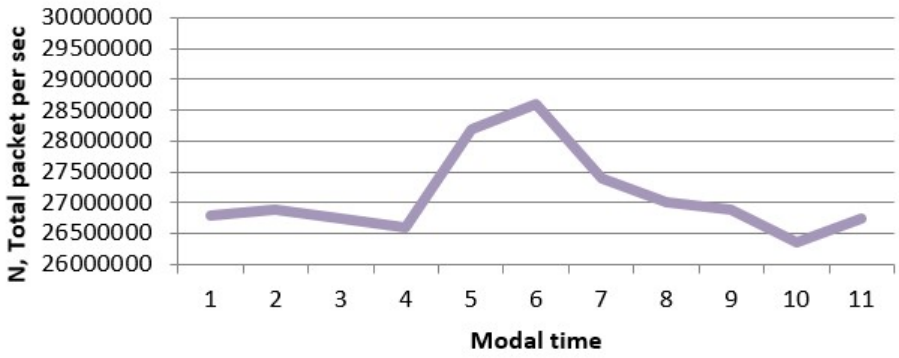

Figure 7: Graph Of The Result Of Modeling The Distribution Of Traffic Passing Through Different Equipment

Figure 8 shows a comparative analysis of total load distribution graphs by type of codecs, as well as the total value of the network delay (ms) for different codecs in Figure 9, the average speed of the process simulation for different codecs, Figure 10 and the efficiency of the bandwidth values by the type of codecs, respectively, in Figure 11.

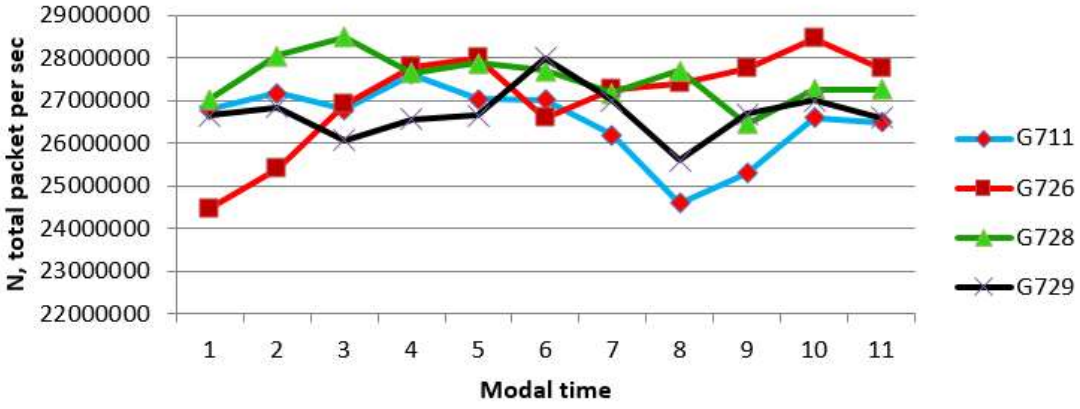

Figure 8: Distribution Of The Total Load By Type Of Codecs

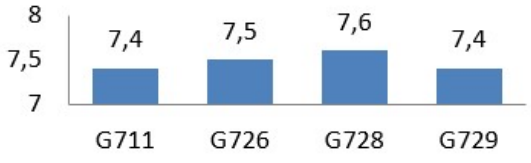

Figure 9: Total network delay (ms) by codec type

Figure 10: Average process modeling speed by type of codecs

Figure 11: BW Efficiency

A comparative analysis of the use of various codecs showed that the most suitable codec in terms of minimum delays for network design is the G711 codec.

6. COMPARATIVE ANALYSIS OF THE EFFICIENCY OF USING CODECS FOR TRAFFIC TRANSMISSION BASED ON THE PEARSON CRITERION

The analysis is based on the method of calculating the Pearson criterion, which allows one to calculate the agreement not only of the practical and theoretical distribution values, but also to calculate the homogeneity of two independent experimental samples.

The values of the basic load during traffic transmission in the wireless network were taken as independent experimental samples. Let us compare the samples made up of the base load values when transmitting traffic in a wireless network. The initial data of the samples are contained in Figure 11 and have, at first glance, similar data. It is necessary to check whether this data is sufficient to assert that the load when using different types of codec is not the same. For this, the $\chi 2$-square method or Pearson criterion was used, with the help of which the distribution of the total load when transmitting information over a wireless network is subjected to statistical analysis. Let us express a hypothesis that the values of the total load for the G711 codec are a theoretical value, and the rest are investigated ones and we will calculate the Pearson criterion according to the formula (1):

$$\chi 2 = \sum \frac{(f_э - f_т)^2}{f_т}, \qquad (1)$$

where $f_э$ – empirical selection values; f_m – theoretical selection values.

Based on the calculation results a histogram was built based on the Pearson criterion, shown in Figure 12.

Figure 12: Distribution of the total load by type of codecs

Figure 12 shows that G729 codec has the best speech transmission quality in a comparative analysis with the G711 codec.

7. CALCULATION OF THE CHANNEL BANDWIDTH WHEN PASSING VOIP TRAFFIC

Voice over the studied network is transmitted using IP-telephony technology. The bandwidth allocated for this type of traffic takes into account the following parameters:

- codec type and voice sample size;
- size of IP/UDP/RTP head labels;
- type of information transmission network technology.

The selected codec type is G.711 with a sample size of 50 packets per second. The choice of the codec type affects the quality of the transmitted voice information and its transmission delay. The size of voice samples packed into a packet also affects delays and required channel bandwidth [18].

Bandwidth is one of the most important characteristics of a network when choosing equipment, and is calculated using the following formula:

$$B_{1phone-IP} = (Ethernet_{overhead} + IP/UDP/RTP_{overnead} + PL) \times N_{packet} \times 8 \qquad (2)$$

where $Ethernet_{overhead}$ – total Ethernet head labels; a $IP/UDP/RTP_{overhead}$ – total IP/UDP/RTP head labels; PL – volume of voice payload in bytes based on the duration of the sample in the packet; N_{packet} – the number of voice samples per 1 second of time.

The payload volume is calculated using the following formula:

$$PL = \frac{B}{N_{packet}}, \qquad (3)$$

B is the coding rate of one voice channel at the output of a certain type of codec.

According to [12], IP / UDP / RTP packet headers in total occupy 40 bytes per packet. The Ethernet header is a total of 38 bytes per packet.

The size of voice information in one IP packet depends on the frame length and the codec transmission rate. The maximum output rate of the G.711 codec is 64kbit/s. We translate this value into bytes:

64kbits ≈ 8 kB = 8000 bytes/s.

This value means that 8000 bytes are received in 1s.

Then the payload will be: PL=(8000/50)=160 bytes

Therefore, the bandwidth will be equal to:

$$B_{1phone-IP} = (38 + 40 + 160) \times 50 \times 8 = 95200 \text{ bit/s}$$

Calculation of the channel bandwidth when video traffic is passing.

The video stream width is the number of video bits processed per second of time. According to [12], usually, the wider the video stream, the better the video quality. For video stream passing in the network, MPEG codecs are used. Video packets are in the range of 800-1500 bytes, and audio packets are smaller - about 480 bytes. This means that the average travel time of an audio stream is less than that of a video stream.

From here, we determine how many packets pass through the network in 1 second using the following formula:

$$N=V/L, \quad (4)$$

where V – video stream throughput; L – video packet length.

The video stream throughput is 3.75 Mbit/s; the length of the video packet is 800 bytes (6400 bits).

Then: N=3932160/6400=615 pack/sec

Now, plugging the data into formula (2), we get the value of the bandwidth for video traffic: Now, substituting the data into formula (2), we get the value of transmission range for video traffic:

$$B_{1phone-IP} = (38 + 40 + 615) \times 615 \times 8 = 3409560 \text{ bit/s}$$

This method determines the data transmission range, taking into account that the packet length is in the range from 46-1500 bytes [12].

Let's consider the case when the packet length is 512 bytes or 4096 bits. Considering that the speed over the data transmission channel is 2×220=2097152 bit/s, we have 512 packets per second. Hence the throughput will be 2,416,640 bps.

Let's find the total traffic:

C=2416640+3409560+95200=5921400 bit/sec

Let us determine the number of channels that can simultaneously serve the number of users, if the throughput of the entire network is 54 Mbps. Then the number of channels Nchannel is:

$$N_{channel} = \frac{56623104}{5914680} = 9{,}6 \approx 10 \; channel$$

8. SECURITY ANALYSIS OF WIRELESS TELECOMMUNICATION NETWORK

Consider the case where security is violated by an external impact on the network, the Wireshark software analyzer, when simulation occurs when the VoIP traffic passes. But first, let's note that Wireshark is a program that analyzes traffic designed for Ethernet computer networks and others. Having a graphical interface, it allows one to analyze all traffic passing through the network in real time,

Wireshark “knows” the structure of different network protocols, and therefore parses the network packet, reflecting the meaning of a certain protocol field of any layer.

Wireshark can handle many input data formats, so it is possible to open data files captured by other programs; this increases the chances of being captured. Looking at an interface such as an http packet, you can see that HTTP takes up space in the header in TCP (transport layer), TCP in the header takes the place of IP (network layer), and IP in turn takes place in the Ethernet header.

The traffic analyzer can be placed in several places: locally, on one’s host or remotely.

To implement an attack on the designed network, one needs to run the Wireshark program as an agent and capture packets passing through the Opnet network. To do this, configure the agent in the Opnet program from the Aplication Capture Manager submenu.

After selecting the Aplication Capture Manager menu, we get a window that displays a list of possible agents for capturing traffic, Figure 13.

Journal of Theoretical and Applied Information Technology
31st July 2021. Vol.99. No 14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

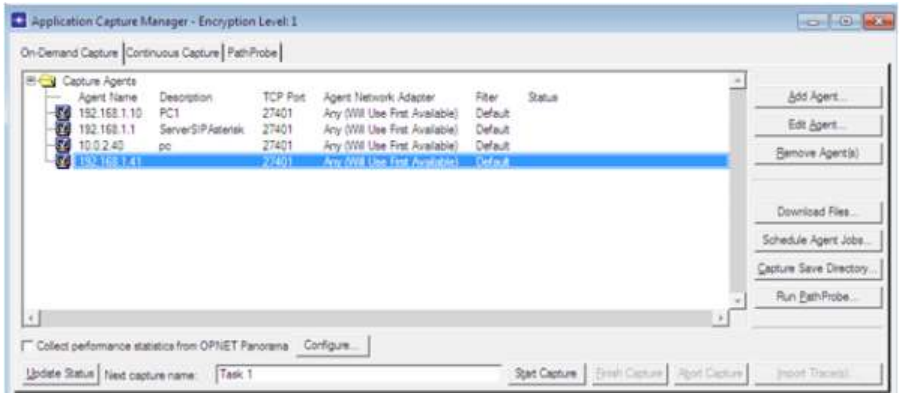

Figure 13: Capture Agents Activation Window

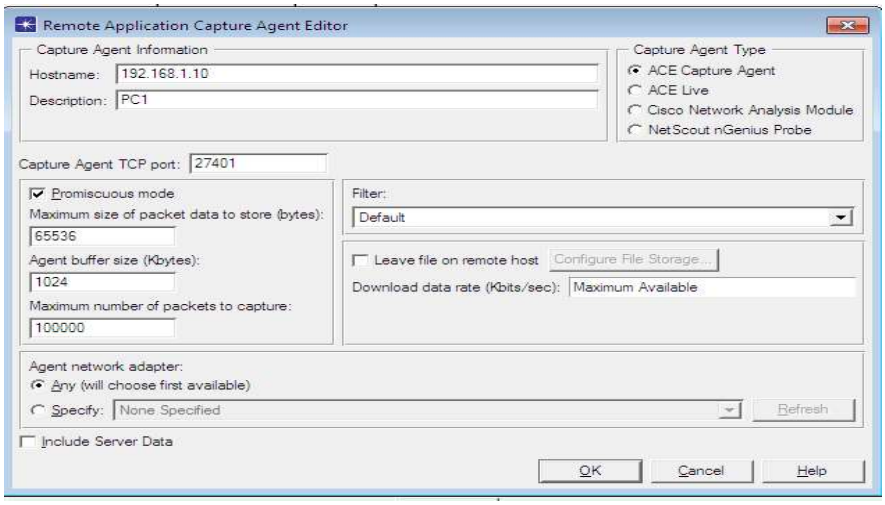

Figure 14: Agent Settings Window

After opening Wireshark, the interface of the Opnet-agent program appears and this is where we carry out the traffic capturing procedure. In the "Statistics" tab in the main menu of the Wireshark program, select the submenu graph and get the captured packets, which are shown in Figure 15.

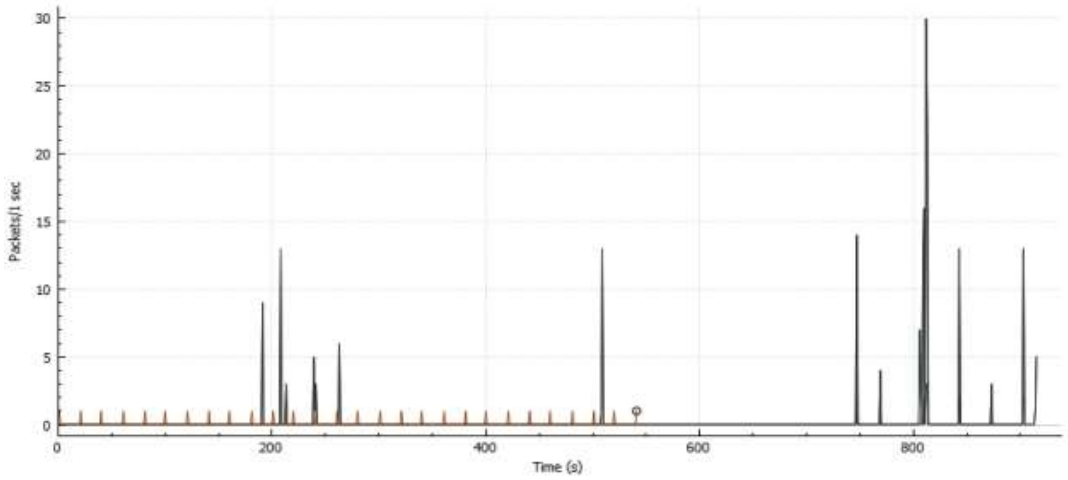

Figure 15: Result Of A Passive Attack Of The Developed Wireless Network Based On The Wireshark Program

Figure 15 shows that with a passive wireless attack based on the Wireshark program, the graph obtained during the simulation shows that the capture of the largest number of packets occurs at a time of 800 seconds.

9. CONCLUSIONS

The introduction analyzes articles primarily published in English and other languages to select the purpose of research.

Analysis of the characteristics of simulation tools is conducted.

The developed network for carrying out simulation model for the security of the configuration of its construction was tested using the NetDoctor utility and it was found that the network was built without errors.

The result of simulation modeling on the distribution of traffic passing through different equipment shows that more traffic passes on the network section from R1 - IP-R2, and at a higher speed.

A comparative analysis of the use of various types of codecs showed that with the G711 codec, network delays are of the least importance and therefore it can be recommended for use in networks built on the basis of IP PBX Asterisk design or upgrade networks.

The result of simulation when using different types of codec showed that the average speed of the simulation process when using the G711 codec is higher than that of others.

The performed comparative analysis based on the Pearson criterion showed that the G729 has the best speech transmission quality in the comparative analysis between the G711 codec and the rest.

Calculated channel bandwidth when VoIP traffic passes.

With a passive wireless attack based on the Wireshark program, it showed that on the graph obtained during the simulation, the greatest time is allocated during the capture of the simulation process-taking place in the network; for example, this is at a time equal to.

REFERENCES:

[1] R. Islam, S. Ghosh, N.J. Ahmed, "Analysis of Conflict DoS Attacks Process and Counter Measure on SIP Based VoIP Network", *International Journal of Advanced Research in Computer Science.* Vol. 3 issue 3, Mandsaur, India 2012, pp. 433-437.

[2] L. Kapicak, P. Nevlud, M. Mikulec, J. Zdralek, "Objective assessment of IP video calls with Asterisk", *Information and communication technologies and services*. Vol. 10 issue 4, Ostrava-Poruba, Czech Republic 2012, pp. 246-250.

[3] J. Wang, X. Shi, M. Alhussein, L. Peng, Y. Hu, "SPSIC: Semi-Physical Simulation for IoT Clouds", *Mobile Networks and Applications*. Vol. 21 issue 5, 2016, pp. 856-864.

[4] A. Khiat, A. Bahnasse, M. Khaili, J. Bakkoury, "Wi-Fi and Wi-Max QoS Performance Analysis on High-Level-Traffic using OPNET Modeler", *Pertanika Journal of Science and Technology*. Vol. 5 issue 24, Selangor, Malaysia, 2017, pp. 1343- 1356.

[5] E.N. Odjidja, S. Kabanda, W.A. Agangiba, R.K. Annan, "Wireless Enabled Voice over Internet Protocol (VoIP) Network Application Using Asterisk PBX", *EAI Endorsed Transactions on Internet of Things*. Vol.4 issue 5, 2018, pp.1-7.

[6] E.N. Odjidja, S. Kabanda, W.A. Agangiba, R.K. Annan, "Wireless Enabled Voice over Internet Protocol (VoIP) Network Application Using Asterisk PBX", *EAI Endorsed Transactions on Internet of Things*. Vol. 4 issue 15, 2018.

[7] M. Razfar, J. Castro, L. Labonte, R. Rezaei, F. Ghabrial, P. Shankar, "Wireless network design and analysis for real time control of launch vehicles", *IEEE International Conference on Wireless for Space and Extreme Environments*. Baltimore, MD, USA, 2013, pp.1-2.

[8] L. Hernandez, M. Ospina, "Scheme and Creation of a Prototype for the Supervision of Lights and Electronic Devices with a PBX, Using a WLAN Solution Based on IoT", *IEEE Colombian Conference on Communications and Computing* (COLCOM), 2019.

[9] T.G. Serikov, M.Z. Yakubova, A.D. Mekhtiev, V.V. Yugay, A.K. Muratova, V.P. Razinkin, A.V. Okhorzina, A.V. Yurchenko, A.D. Alkina, "The analysis and modeling of efficiency of the developed telecommunication networks on the basis of IP PBX asterisk now", *11th International Forum on Strategic Technology (IFOST)*, 2016, pp. 510-515.

[10] W.R. Lai, Y.B. Lin, "Resource planning for wireless PBX systems", *Proceedings of IEEE Enterprise Networking Mini-Conference*

(ENM-97) in conjunction with ICC 97. IEEE. Montreal, Quebec, Canada, Canada, 1997.

[11] R. Manoranjitham, B.N. Jagdale, "Designing an automation framework to improve the performance of SIP based test suites in PBX feature testing", *IEEE Global Conference on Wireless Computing & Networking (GCWCN),* Lonavala, India, 2014.

[12] K. Salah, A. Alkhoraidly, "An Opnet based simulation approach for deploying VoIP", *International Journal of Network Management, John Wiley & Sons Ltd*. V.16 issue 3, 2006, pp. 159-183.

[13] M.Z. Yakubova, "Calculation of Trafic Volume and Type in Asterisk IP PBX Network", *Modern Challenges and Decisions of Globalizations*. *Internationai Conference*. New York, USA, 2013.

[14] S. Khan, N. Sadiq, "Design and configuration of VoIP based PBX using Asterisk server and OPNET platform", *IEECON* 2017, pp.1-4.

[15] A.-B.R. Suleiman, A. Hameed, "Simulation of SIP-Based VoIP for Mosul University Communication Network", *College of Electronics Eng., University of Mosul,* Mosul, Iraq, 2012.

[16] T.Z. Teshabayev, M.Z. Yakubova, T.N. Nishanbaev, B.M. Yakubov, T.V. Golubeva, G. Sadikova, "Analysis and research of capacity, latency and other characteristics of backbone multiservice networks based on simulation modeling using different routing protocols and routers from various manufacturers for using the results when designing and modernization of multiservice networks", *International conference on information science and communications technologies ICISCT 2019 applications, trends and opportunitie*s. Tashkent, Uzbekistan, 2019.

[17] T.Z. Teshabayev, M.Z. Yakubova, T.N. Nishanbayev, M. Amreev, G.S. Sadikova, "The formation of the structure of a multiservice network based on communication equipment from different manufacturers", *International conference on information science and communications technologies ICISCT 2019 applications, trends and opportunitie*s. Tashkent, Uzbekistan, 2019.

[18] M.Z. Yakubova, O.A. Manankova, K.A. Tashev, G.S. Sadikova, "Methodology of the determining for Pearson's criterion based on researching the value of delays in the transmitting of information over a multiservice network", *International Conference on Information Science and Communications Technologies,* Tashkent, Uzbekistan, 2020.pp. 1-5.

[19] M.Z. Yakubova, T.G. Serikov, "IP PBX Asterisk NOW telecommunication network and choice of tools for carrying out attacks. Development and research of the attack scheme to the developed client–server network on the basis of Wi-Fi", *Bulletin of Karaganda State University. Physics Series*. Vol. 2 issue 82, Karaganda, Kazakhstan, 2016, pp. 73-80.

[20] M.Z. Yakubova, T.G. Serikov, A.K. Muratova, "Protection of IP-telefony networks on the basis of Asterisk from interception of data", *Bulletin of Karaganda State University*, *Physics Series*. Vol. 4 issue 84, Karaganda, Kazakhstan, 2016, pp. 24-30.