DOI 10.31489/2019Ph 3/64-70
UDC 621.391.26

M.Z. Yakubova[1], T.G. Serikov[2]

[1]*Almaty University of Power Engineering & Telecommunications, Kazakhstan;*
[2]*Karaganda State Technical University, Kazakhstan*
(E-mail: Tansaule_s@mail.ru)

For the security of telecommunication networks on the application program package OPNET Modeler v.14.5 and the use of the «NetDoctor» module

The work is focused on modeling in OPNET Modeler v.14.5 wireless subscriber access network for its analysis and research by using and applying the NetDoctor module to ensure the security of the built network. Wireless communication is used, as it is accepted, in networks, connecting and wired (cable) means, and give the opportunity to take a convenient, fast and economical solution of problems arising in the process of solution and modernization of cable networks. Wireless communications, therefore, should be considered not a complete alternative to cable networks, but only an alternative technology for the implementation of individual segments or even entire levels of the designed, extensible or modernizing computer network. Detection of used erroneous technologies in the process of building and modeling of telecommunication networks ensures the security of their functioning and predicts their reliable building structure at their design. In our work we use the NetDoctor module of the program package of OPNET Modeler v.14.5 to test the security of the built wireless network.

Keywords: OPNET Modeler v. 14.5, LAN, program package, networks, NetDoctor, traffic, wireless communication.

In foreign countries, wireless subscriber access networks (WSAN) are widely used by corporate networks located inside buildings, on the territory of industrial enterprises as well as for communication of remote offices among themselves. Typical customers of such solutions are hospitals, warehouses and trade organizations. This includes non-stationary networks deployed for an indefinite period of time activities such as exhibitions or scientific and other seminars. In Russia, WSAN work outside of buildings, providing high-speed data transfer services to users located at a distance of several kilometers and even tens of kilometers [1].

In Kazakhstan, the wireless local area network (WLAN) sometimes expresses the only economically viable solution – when the cable system is geographically impossible and lacking or of poor quality. In this regard, the research proposed in the work is *relevant.*

The novelty involves the developed modeling technique on the module APP OPNET Modeler structure of its building and its research.

Wireless communication is used, as it is accepted, in networks, connecting and wired (cable) means, and gives the opportunity to take a convenient, fast and economical solution of problems arising in the process of solution and modernization of cable networks. Wireless communications, therefore, should be considered not a complete alternative to cable networks, but only an alternative technology for the implementation of individual segments or even entire levels of the designed, extensible or modernizing computer network.

The analysis shows that the IEEE 802.11 standard compliant technologies for WLAN have the following four levels of security features: Physical, Service Set ID, MAC ID-Media access control ID, and encryption.

This technology is predetermined for the transmission of data in the frequency range 2.4 Ghz at the present phase is widely used in military communication to enhance the security of wireless transmission. In the area of DSSS schema, the flows that cause the data transfer are «deployed» over a 20-Mhz bandwidth within the ISM range using the Complementary code Keying's scheme. The user must establish a reliable frequency channel and apply the same CCK scheme to decode the received information. Then, the technology on the basis of DSSS provides the first line of protection against unclaimed access to the transmitted information. In addition, DSSS is a «silent» interface, so almost all listening devices will filter it out as «white noise».

The SSID allows you to distinguish the certain WLAN that can act in the same place or region. It is a unique network name included in the header of the IEEE 802.11 data and control packages. Wireless clients

and access points use it to filter and accept only those requests that are related to their SSID. Therefore, the user will not be able to refer to the access points unless it is given the correct SSID.

The probability of accepting or rejecting a request to a network may also depend on the value of the MAC ID being a unique number assigned to each network card during production. When a client PC tries to access a wireless network, the access point must first check the MAC address for the client. Similarly, the client PC must know the name of the access point.

For an invasion of the wireless network, it is enough to be in the radio network visibility zone with equipment of the same type on which the network is built. The access check by MAC addresses of devices and the same WEP is provided in WLAN for reducing of probability of unauthorized access. Because access check is performed by using an access point, so it is only possible with an infrastructure network topology. The inspection technology involves pre-compiling the MAC addresses tables of allowed clients at the access point, and provides the only transfer between fixed wireless adapters. The access control at the level of the radio network is not foreseen in the «ad-hoc» technology (each with each).

In order to enter the WLAN, the intruder must:

– have the equipment for WLAN compatible with the used in the network (in relation to the standard equipment-the appropriate technology of wireless networks – DSSS or FHSS);

– recognize the non-standard sequences of frequency jumps at application in FHSS equipment;

– know the network ID, scrambling the infrastructure and a single for the entire logical network (SSID);

– know (in the case of DSSS) which of the 14 possible frequencies the network operates in, or enable the automatic scanning mode;

– be included in the allowed MAC addresses table in the access point of the network infrastructure technology;

– know the 40-bit WEP cipher key if there is an encrypted transmission in the wireless network. It is almost impossible to solve all this, so the probability of unauthorized entry into the wireless network, in which the standard security measures are taken, can be considered as very low.

We will note the following advantages of WLAN compared to wire:

– Speed and simplicity of deployment and wireless network settings;

– Saving investments in the local network when changing the office;

– Flexibility: quick structure change, configuration modification and network scale;

– Mobility of users in the network distribution zone;

– WLAN functions where the cable is not functioning.

The most elementary way to organize workplaces in the WLAN is the «each with each» (ad-hoc) way. The Network Adapter is entered into each computer and the conditions of direct radio visibility with neighboring points are provided. This method can be used to rapidly deploy a network in small areas where wired networks cannot be deployed for technical reasons.

The Figure 1 shows the developed model of the WSAN on the APP OPNET Modeller V.14.5.

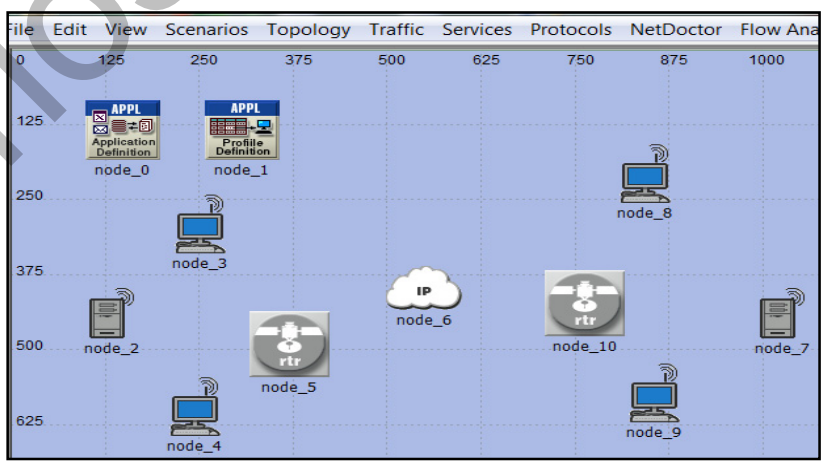


Figure 1. The window of the developed model WSAN on the RFP opnet Modeller V. 14.5

The model consists of the following devices which are wireless: servers, workstations, routers, IP clouds.

We will research the changes of traffic value when different codecs are used in modeling in such a network, for example, G711and G729 standardized in the 90s and used in wireless communications, PSTN networks and VoIP systems. The G.729 is based on an algorithm with a high degree of compression. In general, it allows to compress traffic more strongly, reaching an 8-fold result. Both methods have evolved over the past decades and have a number of versions in accordance with the ITU-T standard.

The research requires an experiment using the following APP OPNET Modeller V.14,5 technologies:

– selection and settings of network equipment;

– from the main menu of the package OPNET Modeller V. 14.5 «Traffic» selection of traffic: VoIP, IP.

As a result of the experiment we get the following data shown in Figure 2 when the codec G711 is used to modify the traffic in its transmission.

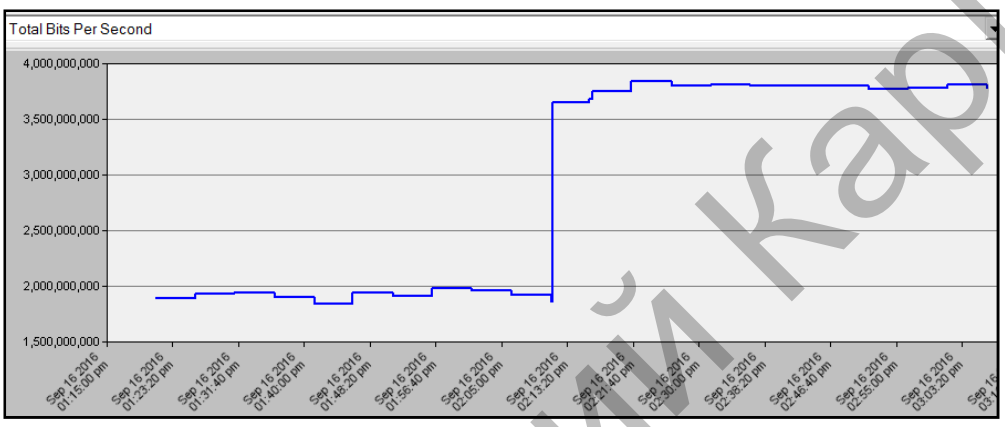


Figure 2. The result of the experiment on distribution of traffic for the model time using codec G711

The Figure 2 shows that at the beginning of the model time the traffic value has changed upward, then from the time of 02. 13.20 sharply increased to 3 800 000 000 bits and then changed very slightly. It can be said that starting from this time there is a steady traffic value in the channel.

We will consider how the traffic value changes by using the G729 codec to modify the traffic. We will use the G729 codec instead of the G711 codec before the modeling as shown in Figure 3.

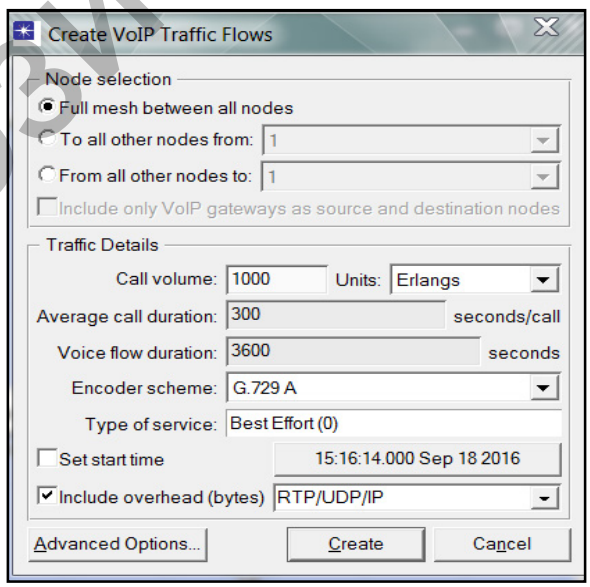


Figure 3. VoIP traffic creation using the G729 codec

The Figure 4 shows the modeling results with the use of the G729 codec from which you can see that from the time of 02. 21.40 there is an almost steady traffic value in the channel and the traffic value thus reaches 1 600 000 000 bits, i.e. by comparing the traffics values it turns out that the value of the transferred traffic using the G729 codec is less than with the G711 codec.

This is explained by the fact that the rate of traffic transmission using the G711 codec is more than G729 almost in 8 times.

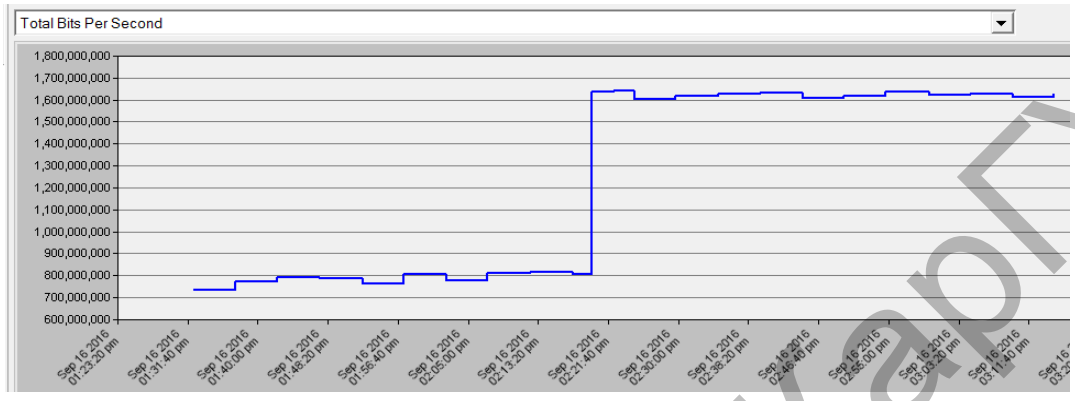


Figure 4. Traffic distribution for the model time using the G729 codec.

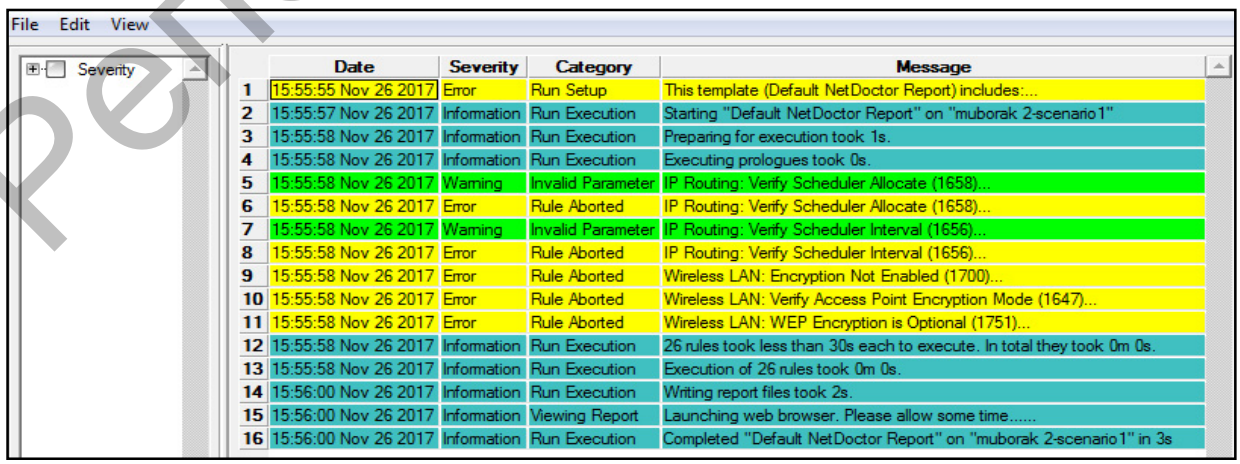
The used encrypting methods are used in communications and are standardized by the ITU-T Association. Both methods use 8000 cycles per second to read the signal using the Nyquist frequency theory, by consuming the bandwidth of 64 Kbit/sec for G.711 and 8 Kbit/sec for G.729.

The G.729 uses special compression methods to reduce the cost of the width of the information transmission, while G.711 will require low computational power compared to G.729, thanks to a simple encrypting methods. The analyzed encrypting and decrypting methods have their own extended versions with small variations. Despite the fact that G.729 provides a lower scope of information, it is necessary to pay attention to the issues of the license [1-4]. The G.729 includes program patents from several companies and is licensed on behalf of Sipro Lab Telecom. Sipro Lab Telecom is an authorized representative of the rights to the G.729 technology and patent portfolio. In a number of countries, it may be required a license fee and/or royalty fee using G.729 The G.729 codec is completely free in Russia.

Based on the above listed, the fact that G.711 is supported by a large number of devices. The systems based on it are easier to use.

We use the NetDoctor module of the program package of OPNET Modeler v.14.5 to test the security of the built wireless network.

For this experiment, we will turn to the main menu OPNET Modeler and clicking on the module NetDoctor we will open its window and run this module. Then we will check its results shown in Figure 5 by modeling WLAN on this module.



	Date	Severity	Category	Message
1	15:55:55 Nov 26 2017	Error	Run Setup	This template (Default NetDoctor Report) includes:...
2	15:55:57 Nov 26 2017	Information	Run Execution	Starting "Default NetDoctor Report" on "muborak 2-scenario1"
3	15:55:58 Nov 26 2017	Information	Run Execution	Preparing for execution took 1s.
4	15:55:58 Nov 26 2017	Information	Run Execution	Executing prologues took 0s.
5	15:55:58 Nov 26 2017	Warning	Invalid Parameter	IP Routing: Verify Scheduler Allocate (1658)...
6	15:55:58 Nov 26 2017	Error	Rule Aborted	IP Routing: Verify Scheduler Allocate (1658)...
7	15:55:58 Nov 26 2017	Warning	Invalid Parameter	IP Routing: Verify Scheduler Interval (1656)...
8	15:55:58 Nov 26 2017	Error	Rule Aborted	IP Routing: Verify Scheduler Interval (1656)...
9	15:55:58 Nov 26 2017	Error	Rule Aborted	Wireless LAN: Encryption Not Enabled (1700)...
10	15:55:58 Nov 26 2017	Error	Rule Aborted	Wireless LAN: Verify Access Point Encryption Mode (1647)...
11	15:55:58 Nov 26 2017	Error	Rule Aborted	Wireless LAN: WEP Encryption is Optional (1751)...
12	15:55:58 Nov 26 2017	Information	Run Execution	26 rules took less than 30s each to execute. In total they took 0m 0s.
13	15:55:58 Nov 26 2017	Information	Run Execution	Execution of 26 rules took 0m 0s.
14	15:56:00 Nov 26 2017	Information	Run Execution	Writing report files took 2s.
15	15:56:00 Nov 26 2017	Information	Viewing Report	Launching web browser. Please allow some time.....
16	15:56:00 Nov 26 2017	Information	Run Execution	Completed "Default NetDoctor Report" on "muborak 2-scenario1" in 3s

Figure 5. WLAN modeling results using NetDoctor

The Figure 5 shows that positions 6, 8-11 indicate used incorrect technologies in the modeling process beginning with the words «ERROR» in English.

To resolve these errors, we use Configure/Run NetDoctor from the NetDoctor submenu and remove the ticks using IP Multicast and IP Routing and modeling without them as shown in Figure 6.

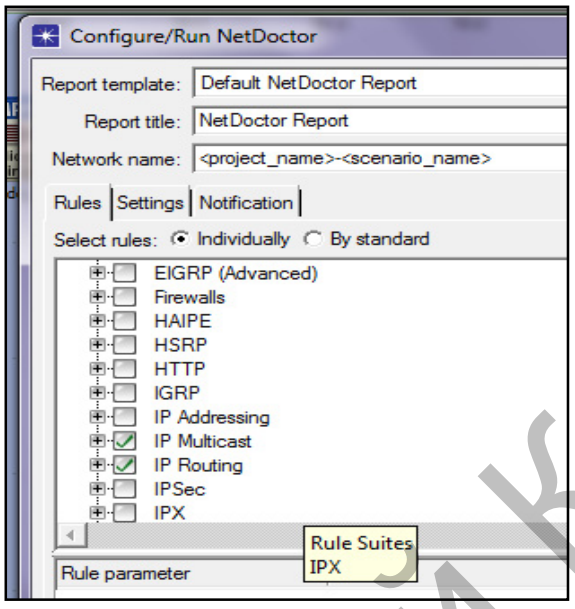


Figure 6. Removal of IP Multicast and IP Routing

As a result, we get the technologies shown in Figures 6–11 where there are no errors

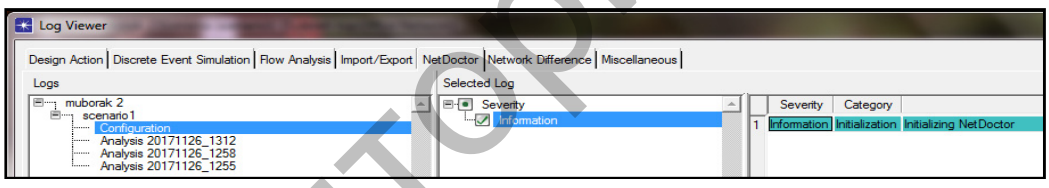


Figure 7. The result of removing the 6th error in the network configuration

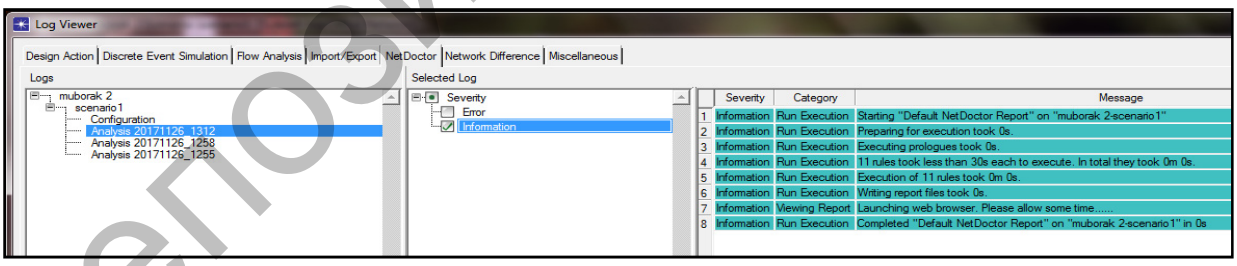


Figure 8. The result of the error 1312 removal analysis

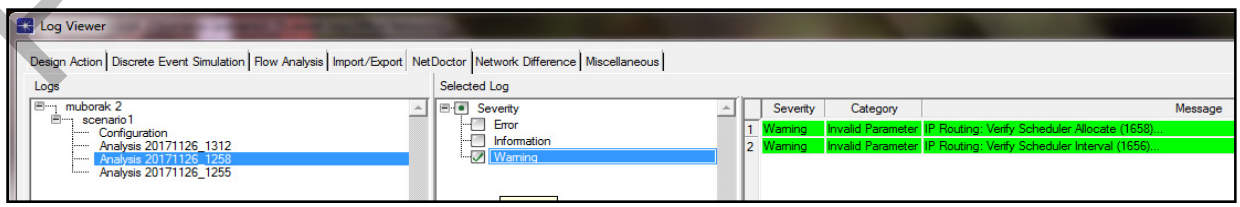


Figure 9. The result of the error 1258 removal analysis

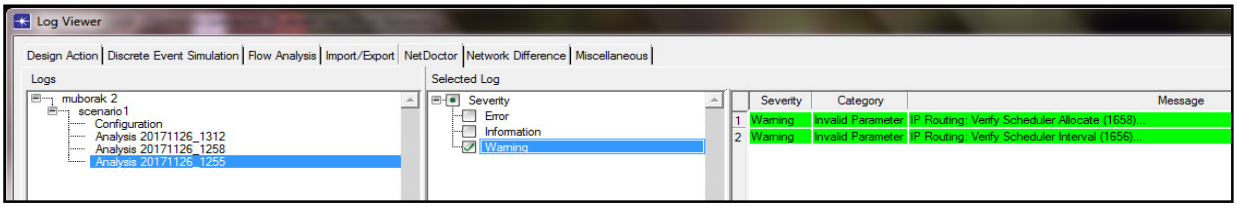


Figure 10. The result of the error 1255 removal analysis

Conclusions

The used codecs in the conducted experiments encrypt data in the researched telecommunication networks.

The G.729 uses less bandwidth for data transmission as opposed to G.711, while the voice quality retains with complex encrypting methods that increase the cost of computational power in encrypting and decrypting processes. Experiments conducted on application program packages show that while comparing the value of the transferred traffic the use of the G729 codec is less than the G711 codec.

Application of the NetDoctor module of the application program package of the APP OPNET Modeller V14.5 showed the errors which were made in the selection of some technologies in modeling, for example, the use of IP Multicast load and the selection of IP technology Routing and others. Detection of used erroneous technologies in the process of building and modeling of telecommunication networks ensures the security of their functioning and predicts their reliable building structure at their design.

References

1 Якубова М.З. Исследование MPLS сетей на основе построения имитационных моделей / М.З. Якубова // Высшая школа Казахстана. — 2016. — № 3. — С. 13–23.

2 Якубова М.З. Имитационное моделирование коммутированных ЛВС / М.З. Якубова // Высшая школа Казахстана. — 2016. — № 3. — С. 30–40.

3 Кислов Д.В. IP-телефония, мобильные телефоны / Д.В. Кислов // ГроссМедиа. — 2007.

4 Сайт журнала «Технологии OPNET» [Электронный ресурс]. — Режим доступа: http://www.opnet.com/services/university/itguru_acadmic_edition.html.

М.З. Якубова, Т.Г. Сериков

NetDoctor модулін қолдану арқылы OPNET Modeler v.14.5 қолданбалы бағдарламасы мен жүйенің қауіпсіздігін қамтамасыз ету

Мақалада құрылған жүйенің қауіпсіздігін құмтамасыз ету үшін NetDoctor модулін қолдану арқылы OPNET Modeler 14.5-те сымсыз абоненттік қатынас жүйесін модельдеу мен оны талдап және зерттеуге арналған. Коммутатордың негізгі кемшілігі — шығыстардың жіберу жолағының шектеулігі. Егер де белгілі бір шығысқа арналған коммутаторға келіп түсіп және оның жылдамдығы және өткізу қабілеттілігінен жоғары болса, пакеттердің қақтығысу проблемасы пайда болады. Бұл жағдайда коммутатор пакеттерді сақтауға немесе пакеттерді кезекке жібереді. Бұл жұмыста екі коммутациялайтын құрылғылардың қолданылуы арқылы, коммутацияланатын жергілікті-есептеуіш желілер құрылады: концентраторлар мен коммутаторлар. Концентратор кірісіне келіп түскен пакеттерді барлық шығыстарына жібереді. Әртүрлі желілерді талдау және модельдеу үшін коммерциялық түрінің қызметін атқаратын OPNET Modeler v.14.5 қолданбалы бағдарламасы пайданылады. Бұл бағдарламада дайын модельдердің көптігіне байланысты қазіргі таңдағы барлық байланыстырушы желілерді модельдеуге және олардың кірістерін өзгертуге мүмкіндік береді.Сонымен қатар OPNET Modeler 14.5 бағдарламасы мен оның кеңейтілуіндегі жергілікті-есептеуіш желілерді модельдеудің тәсілдері мен кеңейтілеген коммутацияланған желілерді зерттеу қарастырылды. Бұл жұмысты зерттеу кезіндегі желілердің жұмыс істеуін тексеру және үлкен коммутацияланатын желілерді құру үшін қолдануға болады.

Кілт сөздер: OPNET Modeler v.14.5 сымсыз жергілікті желі, қосымшалар пакеті, жергілікті желілер, NetDoctor, трафик, модельдеу.

М.З. Якубова, Т.Г. Сериков

Обеспечение безопасности сетей на основе пакета прикладных программ OPNET Modeler v.14.5 с использованием модуля NetDoctor

Статья посвящена моделированию в OPNET Modeler v.14.5 беспроводной сети абонентского доступа, для ее анализа и исследования при использовании и применения модуля NetDoctor для обеспечения безопасности построенной сети. Авторы создавали коммутированные локально-вычислительные сети, с использованием двух различных коммутирующих устройств: концентраторов и коммутаторов. Концентратор передает пакет, прибывший на один из его входов, на все выходы вне зависимости от назначения пакета. Для анализа и моделирования разнообразных сетей применялся пакет прикладных программ OPNET Modeler 14.5, исполняющий собой роль коммерческой версии, предлагаемой бесплатно для использования в образовательных целях. В связи с тем, что у него большая библиотека различных готовых моделей используемых объектов по оборудованию, можно моделировать почти все существующие на сегодняшний момент сети связи и при моделировании можно изменять входные параметры модели. Также рассмотрены методы моделирования локально-вычислительных сетей на OPNET Modeler 14.5 с последующим ее расширением и проведены исследования моделированной расширенной коммутированной сети. Данную работу можно использовать при проведении исследования функционирования сетей с коммутаторами и при построении крупных коммутируемых сетей.

Ключевые слова: OPNET Modeler 14.5, беспроводная локальная сеть, пакет прикладных программ, локально-вычислительные сети, NetDoctor, трафик, моделирование.

References

1 Yakubova, M.Z. (2016). Issledovanie MPLS setei na osnove postroeniia imitatsionnykh modelei [Study of MPLS networks based on the building of simulation models]. *Vysshaia shkola – High School, No. 3,* 13– 23 [in Russian].

2 Yakubova, M.Z. (2016). Immitatsionnoe modelirovanie kommutirovannykh system LVS [Simulation modeling of the switched LAN]. *Vysshaia shkola – High School, No. 3,* 30–40 [in Russian].

3 Kislov, D.V. (2007). IP-telefoniia, mobilnye telephony [IP-Telephony, mobile phones]. *HrossMedia – GrossMedia* [in Russian].

4 Sait zhurnala «Tehnolohii OPNET». [Sait of the magazine «OPNET Technologies»]. *opnet.com.* Retrieved from http://www.opnet.com/services/university/ itguru_acadmic_edition.html [in Russian].