Method to improve information security in fiberoptic systems and networks

Mikola V. Vasylkivskyi[a], Oksana S. Horodetska[a], Liudmyla A. Savytska[a], Nataliia B. Savina[b], Aliya Kalizhanova[c,d], Paweł Komada[e]
[a]Vinnytsia National Technical University, Vinnytsia, Ukraine; [b]National University of Water and Environmental Engineering, Rivne, Ukraine; [c]Institute of Information and Computational Technologies CS MES RK, Almaty, Kazakhstan; [d]Almaty University of Power Engineering and Telecommunications, Almaty, Kazakhstan; [e]Lublin University of Technology, Lublin, Poland

ABSTRACT

The article improves the efficiency of counteracting unauthorised access by using algorithms and a protocol for monitoring information security in fibre-optic transmission systems and access networks with the help of the proposed software, which functions as part of a combined (hardware and software) method of protecting optical information flows in FOCLs. The principles of building network protocols are investigated. The functionality of the developed algorithms and the protocol for monitoring the information security of fibre-optic transmission systems is substantiated. The algorithms for stopping and restoring the transmission mode for the subscriber and linear sections of the optical network based on GPON and GEPON technologies, as well as the protocol for monitoring the information security of fibre-optic transmission systems are developed. The practical significance of the work is to improve information security through the use of a combined security control tool that operates on the basis of the developed algorithms and the information security control protocol.

Keywords: information security, optical access network, fibre-optic systems, fibre optic network

1. INTRODUCTION

Absolutely, securing fiber-optic communication lines (FOCLs) is paramount in modern information and communication networks. An integrated approach combining hardware and software solutions is indeed crucial for enhancing information security and thwarting unauthorized access effectively. Hardware solutions might involve physical security measures such as tamper-resistant enclosures, encryption devices, and intrusion detection systems along the fiber routes. Additionally, techniques like fiber tapping detection mechanisms and secure connectors can further fortify the physical layer of protection. On the software front, robust encryption protocols, authentication mechanisms, and access control policies can be implemented to safeguard data transmitted over the FOCLs. Advanced monitoring and analysis tools can also help in detecting anomalies and potential breaches in real-time, allowing for prompt response and mitigation.

Furthermore, continuous research and development are essential to stay ahead of emerging threats and vulnerabilities in fiber-optic communication systems. Collaboration between industry stakeholders, researchers, and policymakers is vital to foster innovation and establish standards for ensuring the security and reliability of FOCLs in the digital age [1].

FOCLs are integral to modern information and communication networks, offering high-speed data transmission, low signal loss, and immunity to electromagnetic interference. However, like any technology, FOCLs face various security challenges[2]. Addressing the information security issues in fibre-optic communication lines and transmission systems requires a holistic approach that integrates both hardware and software solutions[3]. By focusing on high-accuracy detection methods, ensuring technical feasibility, and developing clear and robust software implementations, it is possible to significantly enhance the security of FOCLs. The combined use of hardware and software protection methods offers a resilient and effective strategy to safeguard against unauthorized access and other security threats in fibre-optic networks[4].

*e-mail: yosup.bilynsky@gmail.com

Photonics Applications in Astronomy, Communications, Industry, and High Energy Physics Experiments 2024, edited by Ryszard S. Romaniuk, Andrzej Smolarz, Waldemar Wójcik, Proc. of SPIE
Vol. 13400, 134000T · © 2024 SPIE · 0277-786X · doi: 10.1117/12.3054856

2. PUBLICATIONS ANALYSIS

Existing methods proposed in[5] prevent the main ways of unauthorised interference with FOCLs, but are characterized by low accuracy of establishing the location of an unauthorised connection in the FOCL route or technical complexity of implementation. It should also be noted that[6] developed and described general procedural steps, and focused on mathematical models that only formally determine the correctness of the proposed algorithms. At the same time, little attention was paid to the software implementation of the algorithms and the subsequent generalisation of the principles of operation in the protocol [7].

Article[8] describes in detail a modified method for monitoring the security of a multichannel FOCL, which allows determining the time and place of unauthorised access (UA). The use of measurement reflectometry technology and statistical analysis methods allows to effectively detect tampering incidents and determine their location in optical channels. The method proposed in this paper is based on a combination of hardware and software, which allows to increase the efficiency of information flow protection by additional processing of signals transmitted over FOCL, as well as to increase the accuracy of determining the location of UA. This paper also provides an overview of the main types of hardware and software tools for protecting FOCLs, reveals the shortcomings of existing methods and creates prerequisites for the use of combined security tools in information systems. The advantages of the proposed method are its versatility and the possibility of implementation in both simple and advanced networks. The use of a computer makes it possible to analyse and predict changes in the power of optical signals and to establish the location of an IPS using a reflectometer that can be operated by a PC using the proposed algorithm. This study also includes an analysis of possible ways of unauthorised access and methods of protection against them. At the same time, structural diagrams of hardware implementation of control devices for the protection of fibre-optic communication lines are proposed.

3. RESEARCH OBJECTIVES AND TASKS

The aim of this paper is to increase the efficiency of counteracting unauthorised access, develop algorithms and a protocol for monitoring information security in fibre-optic transmission systems and access networks by means of the proposed software that operates as part of a combined (hardware and software) method of protecting optical information flows in FOCLs. To achieve a given goal, the following tasks need to be solved:

- analysis of information security problems of fibre-optic lines and transmission systems;
- development of algorithms and protocol for information security control in fibre-optic transmission systems;
- calculation of time parameters of the information security control protocol for fibre optic transmission systems.

4. BASIC RESEARCH MATERIAL

An analysis of existing methods of protecting FOCLs and fibre optic transmission systems (FOTS) has shown that a comprehensive approach is required to ensure a high level of information security. This approach should include both hardware and software security measures. The main areas of security improvement include. Developing methods that ensure high accuracy in detecting unauthorised access points. Ensuring the technical availability of security methods without significant financial and resource costs. Developing a clear software implementation of security algorithms for easy integration with existing systems.

The use of combined security methods will significantly improve the security of FOCLs and transmission systems, ensuring the integrity, confidentiality and availability of information. To ensure a high level of information security for fibre-optic communication lines, it is necessary to improve security criteria such as fibre integrity, fibre condition monitoring, bend protection, and implement hardware and software protection methods. An integrated approach that includes physical, software and cryptographic means will significantly improve the security of information transmitted over fibre optic links[9].

When considering the physical security of FOCLs and OTLs, it is also necessary to pay attention to the security aspects of optical signals. To ensure full protection of information transmitted via optical fibres, it is important to consider optical signal modulation (OS) methods that can make it difficult for unauthorised information to be received. Therefore, modulation of optical signals is an effective method of increasing the security of fibre optics. The use of different types of modulation (by intensity, frequency, phase, polarisation, direction, frequency distribution of modes) makes it difficult to receive an unauthorised optical signal. In addition, the use of different types of control signals for modulation

(electrical, acoustic, mechanical, optical) provides an additional level of protection, making it more difficult for attackers to operate. The integration of such modulation methods into FOCLs can significantly increase the level of information security[1].

When analysing the methods of protecting FOCLs at the physical level, it is also necessary to consider the protection of optical signals transmitted through them. To ensure complete protection of information transmitted through optical fibres, it is important to consider the methods of modulation and coding of optical signals (OS). The security of optical signals is based on the use of modulation and coding methods that make it difficult for intruders to decode signals. This, in turn, reduces the likelihood of unauthorised access to the transmitted information, ensuring a high level of information security in fibre-optic communication lines[2].

The proposed method for controlling the optical signal power and error rate in FOCLs is based on comparing the BER in the optical channel. To do this, a security monitoring device (SMD) is connected to the optical channel of the FOCL using an asymmetric optical splitter (OS). In case of unauthorised connection to the monitored FOCL, the power level of optical signals in the linear path decreases. The change in the power level is detected by an optical receiver with increased sensitivity and transmits the resulting electrical signal to a two-channel BER tester, which simultaneously determines two error rates (Fig. 1). After that, the error rate values are sent to the comparison unit to make a decision on the presence or absence of ND. This control device is advisable to use in small networks because the comparison unit requires manual adjustment (calibration). For networks that are gradually expanding or have the prospect of expansion, the use of this method is not quite profitable, because after each expansion of the network, the comparison unit must be recalibrated. This hardware method can operate in real time. Therefore, for certain types of FOCLs, hardware and software implementation of the proposed method is possible. The generalised structure of the FOCL security monitoring device is shown in Figure 1[6].

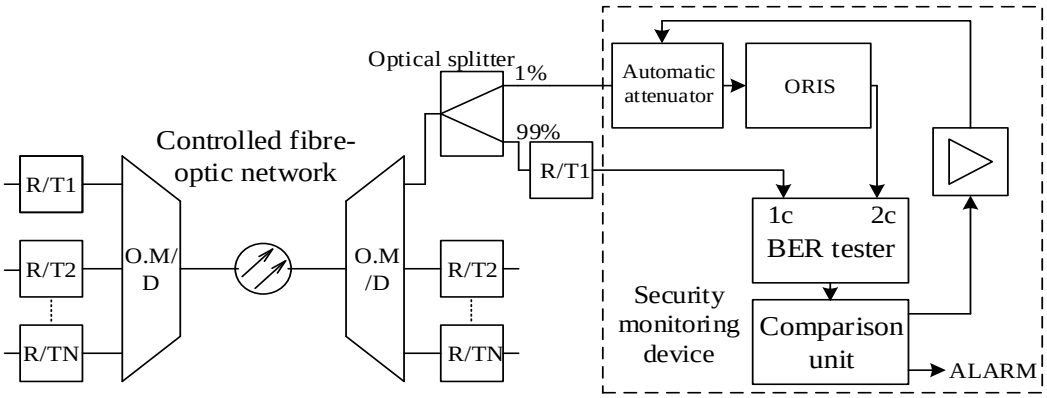

Figure 1. Structure of the FOCL security monitoring device.

The diagram shows an optical splitter (OS) in front of the receiver that divides the input signal: 99%:1% in order to achieve the threshold power at the receiver input, respectively, with any change in power in any part of the communication line, the power at the receiver input will decrease, which will lead to the receiver ceasing to receive this signal, since before this change it was already operating at the threshold of sensitivity. At the same time, the power level decreases, which is detected by the optical receiver with increased sensitivity and transmits the result in the form of an electrical signal to the two-channel BER tester, which simultaneously determines the error rate for two optical channels: the working (reference) and the controlled one. After that, the error rate values are sent to the comparison and difference determination unit, which includes a device for comparing with reference values and a device for generating a signal about the decision on the presence or absence of unauthorised access (UA). This control device is advisable to use in small networks because the result comparison unit requires manual adjustment (calibration). The advantage of the proposed device is that it provides real-time monitoring of FOCL information security. The schematic implementation of the control device is based on serial blocks used in FOCS. The comparison unit consists of a high-performance ADC, a programmable logic integrated circuit (PLIC), which is characterised by high performance, higher than a similar version of the circuit on a microcontroller, RAM, ROM and a control and display unit[7]. Figure 2 shows a generalised structure of an adaptive security monitoring device.

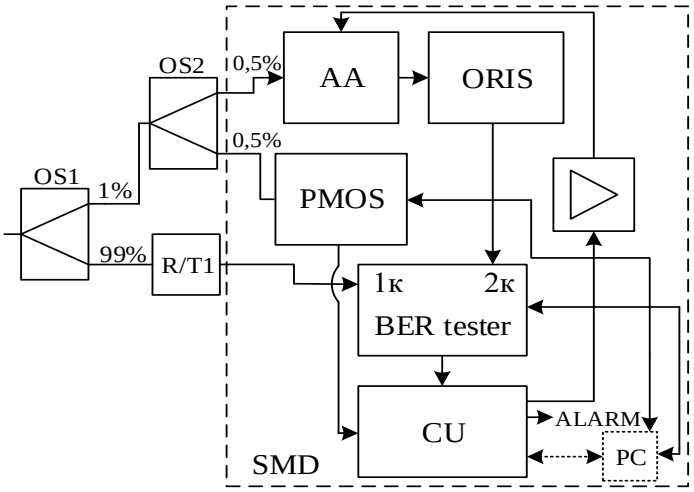

Figure 2. Structure of an adaptive security monitoring device.

For networks that are gradually expanding or have prospects for expansion, the use of this method is not rational, therefore, for such networks, to adaptively adjust the result comparison unit, it is necessary to add another OR and an optical signal power level meter to the structure (Fig. 2) of the PCS. The use of PCs as part of the PCS makes it possible to build an adaptive security control device (SCD).

As a result, we can see that the embodiment shown in Figure 1 is hardware, and the embodiment shown in Figure 2 is hardware and software. To simplify the hardware, software is used that will work according to the algorithm shown in Figure 3.

A modified version of the device circuit is proposed for expanding infocommunication networks with dynamic adjustment of the equipment configuration. For adaptive adjustment of the results comparison unit, it is necessary to add another OR and an optical signal power level meter to the structure of the PCS. The use of a PC as part of the PCS makes it possible to design an adaptive security control device (SCD) for FOCLs based on the proposed hardware and software method, the generalised algorithm of which is shown in Figure 3. This ACS will provide statistics on the operation of FOCLs, on the basis of which it will be possible to predict the functional characteristics of FOCLs in conditionally real time[3].

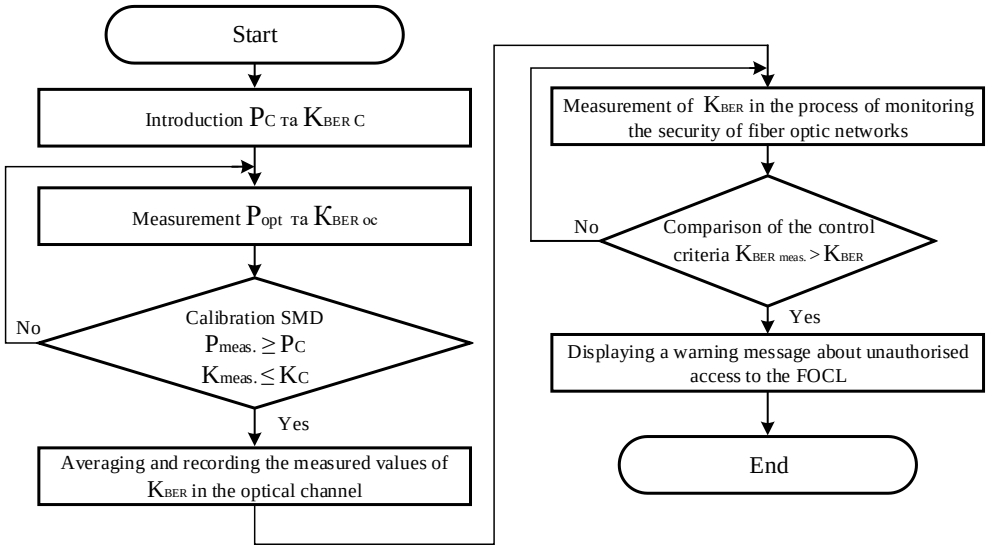

Figure 3. Block diagram of the algorithm of operation of the device for monitoring the protection of FOCL.

The first step is to set the required threshold power and the error rate at this power. Next, a block that checks the correctness of the received data by measuring the actual signal power and error rate, in case of incorrect calibration, the actions are repeated. Then the results are recorded in the program, and the cyclical measurement of the error rate through the power parameter and verification with the recorded averaged data begins. If a discrepancy is detected, a notification is sent and the transmission is stopped[8].

An analysis of the main existing methods of unauthorised access to FOCLs has identified the need to develop and implement methods to counteract and protect information from fraud. The article describes the main types of hardware and software protection, but due to a number of objective shortcomings, it is clear that it is necessary to use combined means of protecting information in FOCLs. The proposed method makes it possible to increase the speed and accuracy of detecting the presence of NS in FOCLs. The advantage of the proposed method is that it can be implemented in both simple and expanding networks. The additional use of a computer makes it possible to analyse and predict possible changes in the power of optical signals and to establish the location of the PD using reflectometers that can operate under PC control according to the proposed algorithm[1, 4].

Analysis of possible problems that may arise during the implementation of algorithms and protocols for monitoring the information security of fibre-optic lines and transmission systems allows us to identify the main areas to be worked on to achieve a high level of security. Choosing the right solutions and implementing them at the early stages of development will ensure effective information protection and reliable operation of fibre-optic communication systems[10,11,12].

The development of algorithms and protocols for information security control in fibre-optic transmission systems is critical to ensure reliable data protection. The use of the UDP protocol reduces overheads and improves performance, while the developed detection and coordination algorithms provide effective protection against unauthorised access and connection. Testing and optimisation of the protocol guarantees its reliable operation in real-world conditions[2,13,14].

The development of algorithms and protocols for information security control based on UDP requires taking into account a number of specific problems associated with its features. To ensure reliable and secure data transmission, it is necessary to implement additional mechanisms that compensate for the shortcomings of UDP, including delivery confirmation, encryption, authentication, data integrity control, flow control, attack detection and session management mechanisms. This will create an efficient and secure protocol that provides high speed and reliability of data transmission without using the traditional client-server model[3,15].

To design a protocol that will take into account the specifics of GEPON and GPON technologies in accordance with IEEE802.3ah and G.984.3 standards, as well as network architecture (station and line), it is necessary to develop algorithms for stopping transmission and checking the network status. These algorithms will ensure effective monitoring and management of fiber-optic transmission systems, reducing the possibility of errors and ensuring stable network operation, taking into account all the specific features of GEPON and GPON technologies[7]. To develop an algorithm for stopping transmission in GPON technology for the subscriber part, where OLTs and ONUs operate, it is necessary to take into account the specifics of the states and interaction between these devices.

The development of an information security control protocol in fibre-optic data transmission systems (FOTS) is an important task, given the high requirements for performance and security of data transmission. Therefore, the implementation of such a protocol will ensure high security and reliability of FOTS, which is critical in today's information security environment.

Let's start the calculation for GEPON technology. Figure 4 shows the time structure of the PON flow.

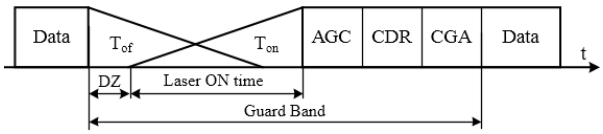

Figure 4. Temporal structure of the PON flow.

The main values in this structure are: T_{on}, T_{off} - time of switching the laser on/off; Automatic Gain Control (AGC) - automatic power control; Clock-and-Data Recovery (CDR) - time of fixing the phase and frequency; Code Group Align (CGA) - alignment time; Data - information field; Dead Zone (DZ) - "dead" zone.

According to the IEEE802.3ah standard, the values of AGC and CDR parameters can be: 96 ns, 192 ns, 288 ns, 400 ns. Laser on/off time: 512 ns. CGA alignment time: 32 ns[10].

Thus, we can calculate the maximum and minimum time required to detect the ND/ND according to the expression:

$$T = T_{on} + AGC + CDR + CGA + DATA + T_{resp} \quad (1)$$

where T_{resp} – processing time, μs.

Let's determine the minimum and maximum detection time for GEPON technology using expression (1), taking into account the fact that the transmission time of 1 bit is 1 ns:

$$T_{\min} = 512 + 96 + 96 + 7 + T_{resp} = 711 + T_{resp} \text{ (ns)}$$
$$T_{\max} = 512 + 400 + 400 + 32 + 7 + T_{resp} = 1.351 + T_{resp} \text{ (μs)}$$

It is worth noting that when calculating the minimum value, the alignment time was not taken into account, since the given value is the maximum possible [10]. Given the fact that 1 bit is transferred within 1 ns, we conclude that an attacker can intercept from 89 bytes to 169 bytes of information, which is less than the maximum size of one Ethernet packet (1518 bytes). It is also worth noting that the processing time T_{resp} can vary depending on the equipment involved, so the determining factor of performance is the time it takes for the node to process the information.

Let's calculate the time for detecting UA/UC for GPON technology. GPON technology allocates only 32 bits (25.7 ns) to switch the laser on and off and 44 bits (35.4 ns) for AGC and CDR [11]. The processing time for GPON is known and ranges from 2 μs to 102 μs [12]. At the same time, the alignment (CGA) is not used. In accordance with (1), we calculate the minimum and maximum detection times for UA/UC:

$$T_{\min} = 25.7 \cdot 10^{-9} + 35.4 \cdot 10^{-9} + 5.62 \cdot 10^{-9} + 2 \cdot 10^{-6} = 2.06672 \text{ (μs)}$$
$$T_{\max} = 25.7 \cdot 10^{-9} + 35.4 \cdot 10^{-9} + 5.62 \cdot 10^{-9} + 102 \cdot 10^{-6} = 102.06672 \text{ (μs)}$$

Considering the GPON frame duration of 125 μs and the length of 38880 bytes, we conclude that 311 bytes are transmitted per 1 μs. Thus, the minimum amount of information intercepted by the attacker is 622 bytes, and the maximum is 31743 bytes, which in terms of GPON packets is 0 packets, and in terms of Ethernet packets (which are not transmitted in their pure form over the GPON network) is 21 packets.

As a result, we can say that $T \gg T_{resp}$ and the node processing time becomes the decisive factor in performance. It is also worth noting that the processing time for GEPON technology is definitely longer than for GPON technology, so for more efficient use of security technology, it is better to deploy fibre optic network based on GPON technology, which is characterised by better performance and a number of advantages over GEPON.

5. CONCLUSIONS

The analysis of the development and operation of fibre-optic systems and transmission lines for creating Internet coverage has shown that the issue of information security, namely the security of data of end users of information and communication services, has not received the necessary attention.

The study of the main types of FOCL hardware and software revealed a number of objective shortcomings of existing protection methods. It is established that the level of their protection is not high, and therefore they cannot provide a 100% security guarantee. A combined hardware and software method of protecting fibre-optic lines and communication systems is proposed, which eliminates the shortcomings identified in the analysis, but at the same time, little attention is paid to the software implementation of algorithms and generalisation of the principles of operation in the protocol, so the basic principles of network protocol development were also considered. The rules governing the transmission of messages over the network are defined. Based on the analysed information, it is determined that in order to ensure the possibility of increasing performance by reducing the frame processing time, the protocol frame should be no more than 64 bytes. Algorithms for controlling information security in fibre-optic transmission systems have been developed and described: a transmission stop algorithm for the subscriber part of the GPON network; a transmission stop algorithm for the subscriber part of the GEPON technology; a transmission stop algorithm

for the linear part of the GPON and GEPON technologies; a transmission restoration algorithm for the FOCL section; a transmission restoration algorithm for the OAN. The problem of packet loss due to the protocol operating between pairs of nodes has been solved, while it is impossible to lose the datagram. The problem of simultaneous detection is solved by using dual detection as a double check for the absence of UA/UC. The problem of remapping is solved by clustering subscribers and using the "dual provider" principle.

The Optic System Security Control Protocol (OSSCP), a protocol for controlling the security of optical systems, was developed. The structure of this protocol is organised. The main functions are developed: input of packet types; obtaining the ID of packet fields; serialiser; deserialiser; packet processing. The protocol performance is calculated. The minimum and maximum detection times for NDs are determined: for GEPON technology they are $(711+T_{resp})$ ns and $(1.351+T_{resp})$ ns, respectively, and for GPON technology they are 2.06672 μs and 102.06672 μs, respectively.

REFERENCE

[1] Vasylkivsky, M. V.. "Protection of information in fiber-optic communication systems," Herald of Khmelnytskyi National University, "Technical Sciences" 3, 202-207 (2018).

[2] Vasylkivsky, M. V., "Evaluation of energy parameters of fiber-optic communication lines under the bit error rate criteria," Herald of Khmelnytskyi National University, "Technical Sciences" 1, 216-219 (2019). https://doi.org/10.31891/2307-5732-2019-269-1-216-219.

[3] Vasylkivsky, M. V. and Palamarchuk, R. P., "Protection of information in fiber-optic communication lines," XVIII International Scientific and Technical conference "Measuring and computing equipment in technological processes," Odessa (June 8-13, 2018), 209-211.

[4] Antonyuk, H. L. et al., "High-speed optical access networks," XVII International Scientific and Technical Conference "Measuring and computing equipment in technological processes," Odessa (June 8-13, 2017), 57-62.

[5] Antonyuk, H. L. et al., "Methods of construction of high-speed fiber-optic tracts," XVII International Scientific and Technical Conference "Measuring and computing equipment in technological processes," Odessa (June 8-13, 2017) 187.

[6] IEEE 802.3ah (2004), Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications. Amd: Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks.

[7] Kazovsky, L. G., Cheng N., Shaw, W.-T., Gutierrez, D. and Wong, S.-W., [Broadband optical access networks], John Wiley & Sons, Inc., Hoboken (2011).

[8] Recommendation ITU-T G.984.3 (2014) – Amd. 1 (2020) Gigabit-capable passive optical networks (G-PON): Transmission convergence layer specification.

[9] Ussipov, N., Akhtanov, S., Zhanabaev, Z., Turlykozhayeva, D., Karibayev, B., Namazbayev, T. and Tang, X., "Automatic modulation classification for MIMO system based on the mutual information feature extraction," IEEE Access 12, 68463-68470 (2024). https://doi.org/10.1109/ACCESS.2024.3400448

[10] Turlykozhayeva, D. et al., "Evaluating routing algorithms across different wireless mesh network topologies using NS-3 SIMULATOR," Eurasian Physical Technical Journal 21.2(48), 70-82 (2024).

[11] Turlykozhayeva, D. et al., "Single Gateway Placement in Wireless Mesh Networks," Physical Sciences and Technology 11(1-2), (2024). https://doi.org/10.26577/phst2024v11i1a5

[12] Turlykozhayeva, D. et al., "Routing metric and protocol for wireless mesh network based on information entropy theory," Eurasian Phys. Tech. J. 20(4), 46, (2024).

[13] Azarov, O. D. et al., "Method of glitch reduction in DAC with weight redundancy," Proc. SPIE 9816, Optical Fibers and Their Applications 2015, 98161T (17 December 2015). https://doi.org/10.1117/12.2229045

[14] Azarov, O. D., et al., "Method of correcting of the tracking ADC with weight redundancy conversion characteristic," Proc. SPIE 9816, Optical Fibers and Their Applications 2015, 98161V (17 December 2015). https://doi.org/10.1117/12.2229101

[15] Osadchuk, O. V. et al., "Pressure transducer of the on the basis of reactive properties of transistor structure with negative resistance," Proc. SPIE 9816, Optical Fibers and Their Applications 2015, 98161C (17 December 2015). https://doi.org/10.1117/12.2229211