Studies on WSN Models for IoT-based Monitoring Systems in the Critical Infrastructure of the State

Sergiy Gnatyuk[1,2,3], Dauriya Zhaksigulova[4], Oksana Zhyharevych[5], Dinara Ospanova[6], and Iryna Chuba[1]

[1] *National Aviation University, 1 Liubomyra Huzara ave., Kyiv, 03058, Ukraine*
[2] *State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, 3 M. Zaliznyaka str., Kyiv, 03142, Ukraine*
[3] *Yessenov University, 32 microdistrict, Aktau, 130000 Kazakhstan*
[4] *D. Serikbayev East Kazakhstan Technical University, 19 D. Serikbayev str., Ust`-Kamenogorsk, 070004, Kazakhstan*
[5] *Lesya Ukrainka Volyn National University, 13 Voli ave., Lutsk, 43025 Ukraine*
[6] *Kazakh Humanitarian Juridical Innovative University, 11 Mengilik str., Semey, 070000, Kazakhstan*

Abstract

It has been established that the IoT concept has three interrelated basic issues: providing information security (IoT Security), scaling up the growing volume of technical devices and data (IoT Scalability), and IoT Technical Solutions and Low-Power Consumption. Also, the analysis of protocols for solving IoT tasks was carried out: MQTT: protocol for collecting data of devices and transmitting their servers (D2S); XMPP: protocol for connecting devices to humans, partial case of D2S-schemes when people connect to servers; DDS: fast bus for integrating smart devices (D2D); AMQP: The system organizes queues for connecting servers (S2S). Stochastic models of the functioning of wireless sensor networks that use randomized network parameters (with variable number of nodes and random participation of nodes in separate groups of network nodes) have been improved. It allowed us to estimate the probability of collision of signals and to more effectively design communications protocols of the IoT. These models allowed us to estimate the probability of collision of signals: the maximum number of nodes that provide the quality of transmission at the level of the probability of collision no higher than 10^{-2} is 50, with the number of nodes involved in the collision is negligible in comparison with the average number of transmissions, in particular, the ratio of the average number involved in the collision of nodes to the average number of transmissions is 10^{-7}. Given results can be used for developing an effective environment monitoring system.

Keywords

IoT, monitoring, WSN, stochastic model, information security, collision, S2S.

1. Introduction

Today there is an urgent need to control and measure almost all physical quantities in large quantities and in almost all areas of human activity. The use of sensors and related communication nodes gives an idea of the universality of the problem of Wireless Sensor Networks (WSN) [1], in particular, in homes and buildings; industrial facilities; warehouses; in the natural environment (forests, fields, over rivers, in the mountains, in the soil, in the air, etc.); in an environment affected by biological and chemical weapons; in cars and planes; at moving intersections; at the bottom of the ocean; inside large machines, rotating spheres, balls; on the ocean surface during a tornado; on

CPITS-2023-II: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2023, Kyiv, Ukraine
EMAIL: s.gnatyuk@nau.edu.ua (S. Gnatyuk); dauriya.dzh@gmail.com (D. Zhaksigulova); o.zhyharevych@gmail.com (O. Zhyharevych); d.ospanova@gmail.com (D. Ospanova); i.chuba@ukr.net (I. Chuba)
ORCID: 0000-0003-4992-0564 (S. Gnatyuk); 0000-0003-0646-2823 (D. Zhaksigulova); 0000-0002-1979-4168 (O. Zhyharevych); 0000-0002-6131-4113 (D. Ospanova); 0000-0003-3336-5105 (I. Chuba)

the battlefield behind the front line; as an indicator for animals and goods; in rivers in combination with water energy, etc.

2. Related Paper Analysis

The development of electronics, Information, and Communication Technologies (ICT) has given grounds for the realization of the idea of measuring and controlling any necessary physical quantities of the environment, industrial processes, control processes, monitoring, etc. Such a huge number of applications of measuring technology, which is also implemented in mobile (mobile) objects, require solutions related to the technique of collecting, transmitting, and processing information for different types of processes used. Many network solutions have been developed and implemented based on previous experience in the implementation of ICT in the concept of the Internet of Things (IoT) [2–5], which are computer networks of physical objects (i.e. things), that are equipped with technologies to interact with each other. These solutions are dominated by deterministic access algorithms for network operation. The number of solutions is quite large and diverse—LAN, MAN, WAN, WLAN, SDH, Wi-Fi, mobile telephony, Bluetooth, ZeegBee etc [6–8].

However, for some applications, previous solutions, such as deterministic solutions [9], are not very suitable (equipment costs, complexity, high energy requirements, complexity of algorithms, wide radio bandwidth)—this significantly limits their applicability. At the same time, the search for stochastic solutions opens up a wide range of add-ons that were previously unsuitable for network solutions in some applications (for hitherto impossible implementations). They extend the category of solutions for modern applications, such as environmental monitoring [10–11], hospital monitoring [12], and more. Given this, the development of information technology for environmental monitoring in the concept of IoT is an urgent scientific and technical task that has important scientific and practical significance. The main objective of this study is the development and simulation of the WSN models for IoT-based monitoring systems that can be implemented for various critical situations.

3. IoT Concept Problems

The IoT concept has been identified as having three interrelated underlying issues: information security (IoT Security), scaling up the growing volume of technical devices and data (IoT Scalability), and addressing IoT Technical Solutions and Low-Power Consumption). Also, protocols for solving IoT tasks were analyzed [13–14]:

1. MQTT: protocol for data collection of devices and transmission of their servers (D2S);
2. XMPP: protocol for connecting devices with people, partial case of D2S-scheme, when people connect to servers;
3. DDS: fast bus for the integration of intelligent devices (D2D);
4. AMQP: a queuing system for connecting servers (S2S).

Fig. 1 shows the ecosystem of a typical IoT architecture according to the international standard ITU-T Y. 2060 “Overview of the Internet of Things” [15].

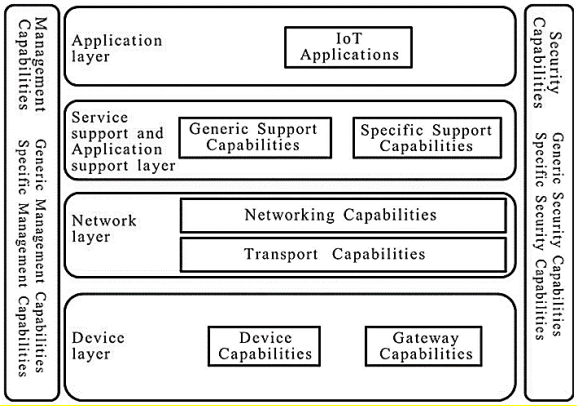

Figure 1: IoT Architecture by ITU-T Y. 2060 [16]

These shortcomings of IoT negatively affect its basic functions, in particular, its monitoring application, in addition to security problems, faces the problem of collisions during scaling, as well as the high energy needs of known solutions, most of which are deterministic.

Thus, the first section identifies the shortcomings of the known approaches and proves the need for mathematical models, methods, and communication protocols of WSN networks with random access and appropriate monitoring information technology to ensure high performance, quality, and survivability of their operation.

4. Modern WSN Deployment

The concept of a sink network [16], which in particular can be a wireless sensor network, is that the sources of information that are distributed in space, both stationary and mobile, and which can be very many, transmit information directly to the base station (information collection center). These are single-hop networks. If the network is organized in such a way that it can transmit information through other nodes, to some extent indirectly, then it is a multi-hop network. Single-hop networks are characterized by a star topology in which individual channels can be implemented simplex or duplex depending on the number of required channels: frequency (available frequencies) or frequency-time, in which this frequency is additionally multiplexed with time division (or temporary compaction), increasing the number of available communication channels. An example is the DCS 1800 system in cellular telephony. In contrast, multi-hop networks are often characterized by mesh architecture.

In all collection networks, which are characterized by all-in-one technology, there is a fundamental problem. At this time, the selected frequency channel can be occupied by only one network user. Therefore, the main task of such networks is the collision-free organization of access to information from individual nodes to the information collection center (base station). Therefore, it is necessary to develop special algorithms and access protocols and prepare communication nodes to operate in an environment of many sensors that try to access one information collection center (base station). That is, the task is to develop a control protocol for the network itself. Considering this issue, we must also mention the problem of electromagnetic compatibility. Using space as a transmission medium, the analyzed wireless network is not an isolated structural unit in space, and due to the use of radio frequencies, its operation, as well as other users of radio communication are interdependent.

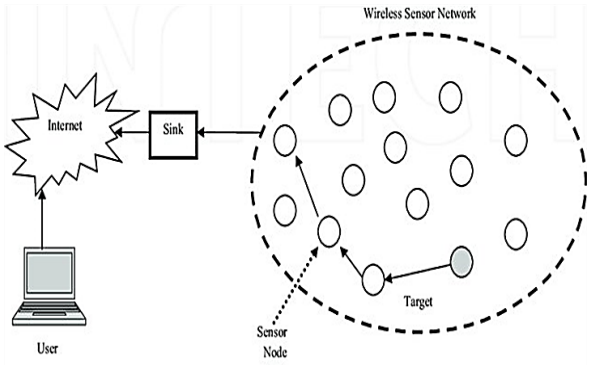

Figure 2: WSN Architecture [17]

The issue of compatibility covered by the standards indicates the limited possibilities of using arbitrary frequencies and the use of arbitrary radiation powers (Effective Isotropical Radiated Power, EIRP). This issue is regulated legally, through the justice systems of states, taking into account international norms. Moreover, it can be said that the electromagnetic spectrum is divided into bands that are subject to special legal protection, and its use in these bands requires a license. Then the guarantee of trouble-free operation of devices operating on licensed frequencies is taken over by the relevant government agencies. Unlicensed bands are also available, such as 27 MHz for Citizen Band, 35 MHz for modeling control, 2.4 GHz for wireless computer WLANs and Wi-Fi, or 433 MHz for remote controls for cars and other automation and control devices. In practice, the use of these bands does not require a license, although the principles of maximum radiated EIRP power and bandwidth used must also be followed. However, unlicensed bands do not guarantee the operation of devices without interference. Today, in practice, for example, the above frequencies are used quite intensively and widely, and the implementation of new network solutions on these frequencies is fraught with a very serious risk of correct action, taking into account the space used. There are also bands in the spectrum of electromagnetic waves that are still not covered by the norms. These are the main bands in the region of very high frequencies—above 100 GHz, infrared, and visible area [18].

Topological and communication specifics of wireless collecting measuring sensor networks. The sensor network consists of many nodes, which are located both inside the measuring medium and outside near the

studied physical quantities. It is accepted that individual communication nodes associated with sensors can move in the field of study of physical effects controlled by sensors. Thus, the mobility of nodes is assumed, which in turn often causes changes in the configuration of the network, and especially leads to changes in the propagation of electromagnetic waves. These requirements are imposed on very important and necessary features and characteristics for the considered nodes of wireless networks, namely: algorithms and protocols must have the ability to self-organize [19]. This means that the node on the hardware side must be equipped with a processor that will often implement very complex maintenance algorithms in a changing environment. The use of ad hoc spontaneous networks for this purpose, despite the many protocols and algorithms available in these networks, does not address the unique needs of sensor networks, which arise from differences between seemingly universal solutions in standard ad hoc networks and the actual needs of measuring networks. This specificity and uniqueness of wireless sensor measuring networks is due to the following components [20]:

- The number of nodes in the sensor network is usually several orders of magnitude higher than in the ad hoc network.
- Nodes in sensor networks, as a rule, are densely placed.
- Sensors with the units with which they cooperate—are often an integral means—are more susceptible to accidents.
- There are frequent changes in the network topology.
- The sensor usually uses node communication solutions, generally more complex than in the case of ad hoc, where communication is generally based on the point-to-point model.
- Nodes in the sensor network, in principle, have a limited power supply, which is a limitation for computing power, available memory, antenna radiation power, and frequency of activation of providers ("wake-up" sensors).
- Nodes cannot have a global ID due to the huge number and space allocated for tasks.

Among the many significant factors that affect the architectural and communication aspects, as well as the use of the network, are the task assigned to the network, environmental impact (environment), resistance to interference and errors, network architecture, hardware constraints, translation algorithms, the need for power supply, the factors that affect the means of production. These factors are the subject of many studies for different applications of wireless networks. The above factors that affect network solutions are important guidelines for designing communication protocols and network algorithms. The following essential conditions in the design of wireless sensor networks can be abbreviated [20]:

- Bandwidth capability and communication frequencies.
- The need for power, for example, for communication and data processing.
- External constraints related to the environment.
- Hardware limitations.
- Scalability.
- Range of resistance to errors.

In a wireless collection network with several nodes, errors or interruptions in the transmission occur, which is the result of many reasons. In the case of radio communication, a significant impact is caused by problems associated with the propagation of radio signals (electromagnetic waves), which is caused primarily by the physical conditions of the environment that surrounds the supply points (nodes). Thus, the presence of signal reflection on local interference, climatic conditions, interference, insufficient signal strength or excessive signal level, and several others. Transmission of information by radio waves is the most difficult task in broadcasting using wired means—copper cables, fiber optics, etc.

By [9–14], we can declare that today it is necessary to create a new class of wireless networks that allow to fill certain gaps in the development of WSN networks related to solving problems such as:

a) obtaining low financial costs in terms of network nodes equipped with sensors for general and simple applications.

b) ease of operation, in particular, sensor algorithms and ease of connecting and disconnecting new components.
c) a significant limitation of the occupied band of radio frequencies in the context of the growing deficit of the radio frequency spectrum.
d) significant energy savings at the nodes (reduction of nodes for data processing, no receiver signal, autonomous operation of nodes in the intervals of very short activity and short-term radio radiation), especially due to lack of energy replenishment directly related to node operation time.
e) complete independence of the nodes from each other.

5. WSN Stochastic Models

WSN stochastic models were developed to assess the probability of signal collision in the system (by concepts [17, 20]).

Let's mark A_s' as an event, that means collision absence in the interval $[0, s]$ $(s > 0)$. Also, let's mark $P(A_s')$ as the probability of collision absence in the interval $[0, s]$. Let's consider $[0, s]$, where $s > t_p$. Suppose that $N(s) = j$, that is the quantity of transmissions in the interval $[0, s]$ equals j $(j \geq 1)$. Random vector $(U_1, \dots, U_j)$ of the time between transmissions is even distributed in the set $\Omega_t^* = \{(u_1, \dots, u_j): u_1 + \dots + u_j \leq s\}$ with conditional density $f(u_1, \dots, u_j | N(s) = j) = j!/s^j$ for $(u_1, \dots, u_j) \in \Omega_t^*$, and also 0 beyond that. In this way conditional density of collision absence in the interval $[0, s]$, supposing $N(s) = j$, is equal:

$$P\left(\frac{A_s'}{N(s)} = j\right) = P(U_1 > t_p, \dots, U_j > t_p) = \left(1 - \frac{jt_p}{s}\right)_+^j ,$$

where expression x_+ determines as $x_+ = x$ for $x \geq 0$ and $x_+ = 0$ for $x < 0$.

The conditional probability of collision in the length interval s, where $s > t_p$, by condition $N(s) = j$, forms by the following expression:

$$P(A_s / N(s) = j) = 1 - \left(1 - \frac{jt_p}{s}\right)_+^j . \qquad (1)$$

The probability of collision in the length interval s, where $s > t_p$, determined by the following expression:

$$P(A_s) = \sum_{j=2}^{\infty} e^{-n\frac{s}{T}} \frac{(n\frac{s}{T})^j}{j!} [\,1 - (1 - j\,\frac{t_p}{s})_+^j], \qquad (2)$$

where n is the number of nodes, T is the average time between node transmissions, t_p is the time of protocol transmission.

The question of the number of nodes that remain in collision in the length interval s is also analyzed for $s > t_p$. The probability of collision in the length interval s is investigated for $s > t_p$. Below are models that characterize the lower and upper estimates of the conditional probability of the number of gears that remain in conflict, in the length interval s, assuming that the number of gears in the transmission interval is in the length interval s $(s > t_p)$ equals j.

Let's mark Y_s as number of transmissions in collision in the length interval s. In this case, we will have an expression:

$$(j\frac{t_p}{s})^{\kappa-1}(1 - j\frac{t_p}{s})^{j-\kappa} \leq P(Y_s = \kappa / N(s) = j) \leq (j\frac{t_p}{s})^{\left[\frac{\kappa+1}{2}\right]}(1 - \frac{t_p}{s})^{j-\left[\frac{\kappa+1}{2}\right]},$$

$$\sum_{j=2}^{\infty} e^{-n\frac{s}{T}} \cdot \frac{\left(n\frac{s}{T}\right)^j}{j!} \left(j\frac{t_p}{s}\right)^{\kappa-1} \left(1 - j\frac{t_p}{s}\right)_+^{j-\kappa} \leq P(Y_s = \kappa) \leq \sum_{j=2}^{\infty} e^{-n\frac{s}{T}} \frac{\left(n\frac{s}{T}\right)^j}{j!} (j\frac{t_p}{s})^{\left[\frac{\kappa+1}{2}\right]} (1\frac{t_p}{s})_+^{j-\left[\frac{\kappa+1}{2}\right]} .$$

Models that characterize the lower and upper estimates of the expected number of gears in conflict and the variance of the number of gears in conflict in the length interval s $(EY_s, D^2(Y_s))$. Let's suppose $s > t_p$.

Then

$$\sum_{\kappa=2}^{\infty} \kappa \sum_{j=2}^{\infty} e^{-n\frac{s}{T}} \cdot \frac{\left(n\frac{s}{T}\right)^j}{j!} \left(j\frac{t_p}{s}\right)^{\kappa-1} \left(1-j\frac{t_p}{s}\right)_+^{j-\kappa} \leq EY_s$$

$$\leq \sum_{\kappa=2}^{\infty} \kappa \sum_{j=2}^{\infty} e^{-n\frac{s}{T}} \cdot \frac{\left(n\frac{s}{T}\right)^j}{j!} (j\frac{t_p}{s})^{\left[\frac{\kappa+1}{2}\right]} (1-j\frac{t_p}{s})_+^{j-\left[\frac{\kappa+1}{2}\right]},$$

$$\sum_{\kappa=2}^{\infty} \kappa^2 \sum_{j=2}^{\infty} e^{-n\frac{s}{T}} \cdot \frac{\left(n\frac{s}{T}\right)^j}{j!} (j(\bar{1}-\left[\sum_{\kappa=2}^{\infty} \kappa \sum_{j=2}^{\infty} e^{-n\frac{s}{T}} \cdot \frac{\left(n\frac{s}{T}\right)^j}{j!} (j\frac{t_p}{s})^{\left[\frac{\kappa+1}{2}\right]} (1-j\frac{t_p}{s})_+^{j-\left[\frac{\kappa+1}{2}\right]}\right]^2$$

$$\leq D^2(Y_s) \leq$$

$$\sum_{\kappa=2}^{\infty} \kappa^2 \sum_{j=2}^{\infty} e^{-n\frac{s}{T}} \cdot \frac{\left(n\frac{s}{T}\right)^j}{j!} (j(\bar{1}-\left[\sum_{\kappa=2}^{\infty} \kappa \sum_{j=2}^{\infty} e^{-n\frac{s}{T}} \cdot \frac{\left(n\frac{s}{T}\right)^j}{j!} (j\frac{t_p}{s})^{\kappa-1} (1-j\frac{t_p}{s})_+^{j-\kappa}\right]^2 .$$

Thus, two dependencies are obtained for the probability of collision (Fig. 2–3). The first expression (1) describes the probability of collision in the short time t_p of providing the protocol, determining the probability of intact provision of the protocol. The second expression (2) is derived using other properties of the Poisson process concerning the probability of collision over a sufficiently long transmission time.

The graphs illustrate the probability of collision depending on the number of sensors for the set average time between messages (Fig. 3), and also show the dependence on the average time of protocol transmission, if the number of nodes is set (Fig. 4). For the average time between transmissions of a node equal to 10 s, the maximum number of nodes, which ensures the quality of transmission at a probability level not exceeding 10^{-2}, is 10, and for the average time between transmissions of a node equal to 30 s, the maximum number of nodes is 50. Further increase in the average time between node transmissions allows you to increase the maximum number of nodes. For a given number of nodes, increasing the average time between collisions causes a decrease in the probability of collision.

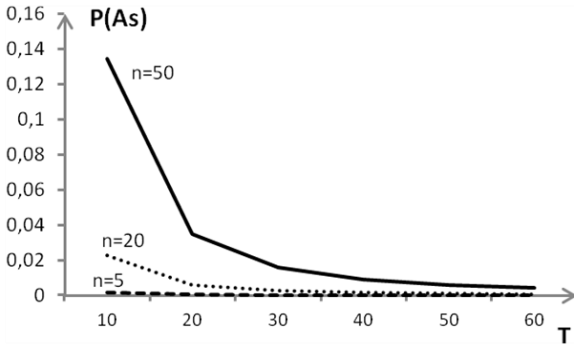

Figure 3: Collision probability in the interval s, where $s > t_p$ depending on observation time $s = 180$ s. and the average time between transmissions of a node for $n = 5, 20, 50$

Using graphs, you can find the optimal values of the parameters that affect the correctness of the transfer (n, T, t_p). Graphs make it possible to determine in which range the transmission quality is provided at a given level or for which values (n, T, t_p) the probability of collision increases sharply. You can determine the order of collision probability values for arbitrarily selected parameters: for example, for $t_p = 3.2\times10^{-5}$, the number of transducer sensors equal to 10, and providing each sensor with an average transmission time every $T = 60$ s the collision probability is 1.65×10^{-4}.

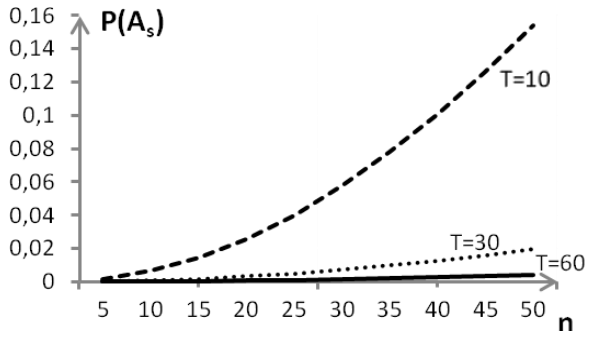

Figure 4: Collision probability in the interval s, where $s > t_p$ depending on observation time $s = 180$ s. and nodes number where $T =$ 10 s., 30 s., 60 s.

The three-dimensional coordinate system (Fig. 5) shows a set of end devices $A = \{a_1, \ldots, a_m\}$ and a set of endpoints of the system $B = \{b_1, \ldots, b_m\}$ from the beginning of a set of coordinators of network $K = \{k_1, \ldots, k_m\}$ (for begin $n = 1$).

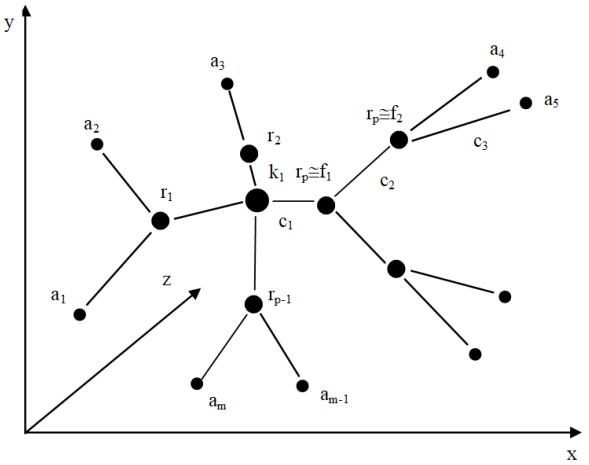

Figure 5: Model of end topology WSN (primary information sources)

Distance between points $a(x_i, y_i, z_i)$ and $b(x_j, y_j, z_j)$ equals:

$$c_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2 + (z_i - z_j)^2}.$$

There are a set of such distances $C = \{c_{11}, \ldots, c_{m1}, \ldots, c_{1n}, \ldots, c_{mn}\}$. The distance between the nodes should not exceed the maximum data transmission range. We will assume that the maximum transmission range between any WSN nodes is the same and equal to $c_{\max}$.

6. Experimental Study and Discussion

6.1. Software Technical Complex Based on WSN

The software technical complex includes subsystems: data collection; communication support; primary processing of the received data and analytical work with information; cartographic display of information; maintaining and maintaining a database [20–22].

1. The data collection subsystem includes a set of automated workstations for the staff of remote users (automated workstations of the monitoring system entities) that perform data and information collection work by certain monitoring functions and transmit to the SU center by established protocols for exchanging information with access to the global Internet.
2. The communication support subsystem includes a communication center, including a set of communication networks and information exchange protocols and external communication servers to implement functions: receiving data from automated workstations of remote users, pre-control, processing, and input of data and information to relevant databases; providing information communication with the information-analytical center; providing information communication with persons who make management decisions; providing access to information of wide use. A system server built on the ideology and requirements of similar structures in terms of reliability, performance, and memory to provide, inter alia, service for numerous user requests with high-speed Internet access channels.
3. The subsystem of primary data processing and analytical work with information includes automated workstations of the database administrator and automated workstations of the Center's specialists who receive, process, and analyze data and information, and can perform modeling and forecasting work. The database administrator implements

support for the functioning of the database; distribution of levels of access to information; maintaining the consistency of the receipt and issuance of data and information displayed on the server of external communications with the content of information in the database; and support for security and information recovery. Automated workplaces of the Center's specialists provide control over the receipt and preliminary analysis of data and information received from remote users; unification of data and information received from remote users for entry into the database; performing tasks of complex analysis, assessment, and modeling of crises; providing operational and consolidated information on the results of monitoring. Automated workstations of specialists are equipped with hardware and software for the rapid solution of data processing problems and high-speed communication channels with the server of information resources and the server of external communications, equipped with equipment for working with graphics.

4. The subsystem of cartographic display and data analysis is designed: to conduct a comprehensive analysis and assessment of the state and possible consequences of the impact on the zones, taking into account the geographical features of the region; visualization of information on the location of networks for monitoring the state of the region and sources of anthropogenic pressure. The subsystem includes a digital map by the level of tasks performed (locality and globality); an information retrieval subsystem developed based on a geographic information system; modules that provide information combination of digital map and database of information resources; a subsystem of cartographic analysis of the ecological situation of the region; modules for providing results of cartographic search and analysis.
5. The subsystem of maintaining and maintaining the database is designed to create, store, and provide access to information resources of the management system, including a separate server of the bank of information resources and special software. The subsystem provides the function of saving data in non-standard situations, including archiving and duplication.

The monitoring system based on this software technical complex can be switched into the following four operation modes [23]:

1. Normal (standard operation, normal operation). The tasks of normal operation consist of emergency planning, the main purpose of which is to gather information to predict the possible occurrence and development of the crisis regime and control its consequences, determine the resources of telecommunications networks and tools needed to resolve crises, develop special forecasts to respond effectively in anticipation of the problem, taking into account all the forces and means to implement the objectives. In this mode, regulatory, legislative, and other mechanisms aimed at minimizing the risk and damage from the crisis are identified and created.
2. Increased preparedness (non-standard operation, active preparation, and practical implementation of several preventive/precautionary measures). To do this, collect and use in the monitoring system data on the state of internal and external structure, data for current and retrospective analysis with the possibility of preventive planning of trends in the current situation, as well as planning resources, forces, and means necessary to neutralize, stabilize and reduce the severity of the consequences of the crisis. Lack of necessary information often becomes a major obstacle to the functioning of the monitoring system to prevent possible consequences. In many cases, this is due to the untimely provision of data, detection, and use of the necessary resources of interconnected, sensory means and telecommunications networks of different operators.

3. Crisis (actions in a crisis). In a crisis mode, the monitoring system should provide a real-time operational mode. Tasks must be implemented on a limited time interval quickly and continuously. In the event of crises in the monitoring system, there may be problems of peak load on all elements, in connection with which they may significantly exceed the functional limitations for their use.
4. Post-crisis (elimination of long-term consequences of the crisis regime). The post-crisis regime is transitional to the usual and includes analysis of the crisis, features for its elimination, modification of the content of databases and knowledge bases, and restoration of normal modes of operation of the components of the monitoring system.

6.2. Simulation of the IoT-based Monitoring System

An experimental study of the results obtained on the example of an IoT system for monitoring air parameters (Fig. 6).

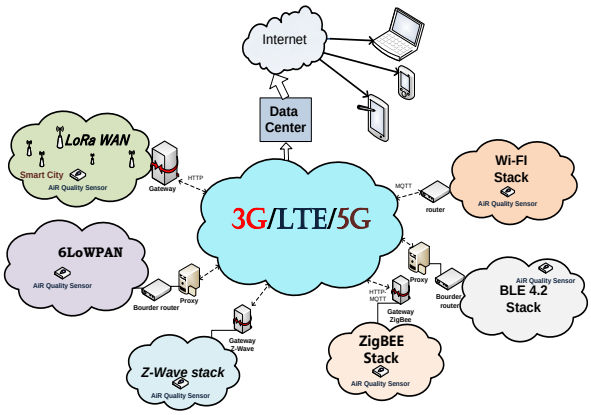

Figure 6: IoT network architecture of air parameters monitoring system

Fig. 6 displays architectures using a variety of wireless technologies, such as LoRAWAN, 6LoWPAN, Z-Wave, ZigBee, and more. When transmitting data over short distances (for example, indoors), devices can use the PAN provided by wireless data technologies such as BLE (Bluetooth Low Energy), ZigBee, 6LoWPAN, and a wired USB interface. If you are talking about data transmission over long distances (for example, in the office), you can use a local area network. Leading LANs in most cases are based on Ethernet and fiber and wireless based on Wi-Fi technology. Wi-MAX, LTE and LPWAN technologies can be used to organize a global computer network (WAN) [1, 6].

According to the method of the experiment, the study was conducted indoors. Fig. 7–8 shows the change in humidity and temperature during the day in a separate room. The monitoring system is based on IoT network architecture, presented in Fig. 6. These graphs are built in real-time mode using specialized software, proposed by authors in their previous studies.

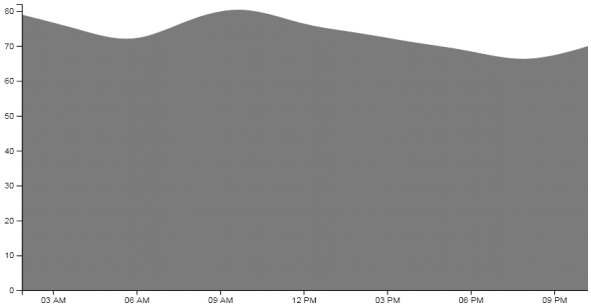

Figure 7: Graph of humidity change

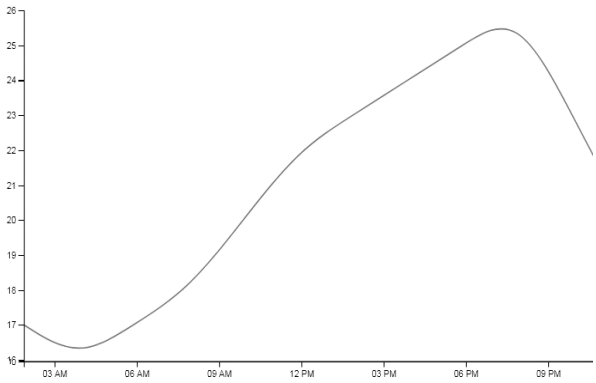

Figure 8: Graph of temperature change

Thus, the studied complex of real-time environmental parameters monitoring can be used as a prototype for the organization of monitoring in dynamically changing environments and the event of critical situations of different natures [24–25].

6.3. Quality Analysis of the IoT-based Monitoring System

By the recommendations of E.430, E.800, X.134, and others of the International Telecommunication Union, the Quality of Service (QoS) is understood as a generalized (integral) beneficial effect of the service, which is determined by the degree of satisfaction the user both from the received service and from

the service system itself. The QoS criterion in the telecommunications business is usually determined by a set of indicators of the properties of both the provided telecommunications service and the network resources used. Service quality indicators are called service QoS parameters, and network resource quality indicators are called network performance parameters. To quantify most of the properties of the quality of telecommunications services defined in the recommendations of TL 9000 and E.800, the corresponding indicators are introduced, which are determined based on the performance characteristics (parameters) of the network. The analysis of recommendations I.350 showed that the quality of the provided telecommunication services is ensured at three stages:

1. Access to information transfer (connection establishment).
2. Transfer of user information.
3. Termination of the information transfer session (disconnection).

Each part of the service, in turn, is characterized by three main indicators:

1. *Efficiency* (connection establishment time, time (effective rate) of user information transmission, probability of timely delivery of user information, and connection disconnection time).
2. *Security* is a property that characterizes the ability of the system to withstand accidental or intentional, internal or external influences, which may result in its undesirable state or behavior (the probability of imposing false connections, the probability of entering false data, the probability of false shutdown, etc.).
3. *Reliability* (certainty of connection establishment, data transmission, and disconnection of the connection, characterized by the probability of refusal to establish a connection, the probability of loss of user information, the probability of refusal to disconnect a connection, etc.).

Many applications of the proposed random access network solution indicate the possibility of dividing the total number of nodes into groups with different average times between transmissions. Such a division has its technical justification, namely if the WSN receives data relating to different physical quantities with different rates of change of their parameters. For example, monitoring the parameters of the environment, in particular the measurement of daily changes in soil temperature and wind speed. This example already indicates the possibility of different frequencies of maintenance of measurements of such quantities. The task deserves attention because the ability to reduce the intensity of the movement of radio packets always has a beneficial effect in this method to improve the quality of transmission. The graphs below in this section present the results of experimental studies of WSN behavior for different percentages of nodes with different mean times between transmissions [20–21].

The study was performed for the following percentages: 10% of nodes with average intervals between transmissions every 10 s and 90% with average intervals between transmissions every 30 s (10%/10 s+90%/30 s were recorded for reduction). In the future 10%/10 s +90%/60 s. The following studies are for 1/3(33%)/10 s+2/3(67%)/30 s and two studies are 50%/10 s+50%/30 s and 50%/10 s+ 50%/60 s. (Fig. 9–13).

In the presented (mentioned) task the time of communication protocol is $t_p = 3{,}2 \cdot 10^{-5}\ s$. The simulation results are obtained, which are compatible with the expected ones, which follow from the earlier dependences presented by the authors.

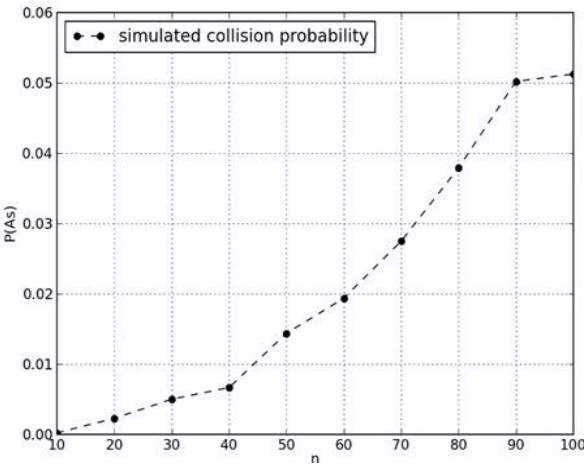

Figure 9: Influence of the number of nodes with different average times between transmissions on the probability of collision: the number of nodes with an average time between transmissions T = 10 s is 10% of the total number of nodes, and 90% of nodes work with an average time between transmissions T = 30 s

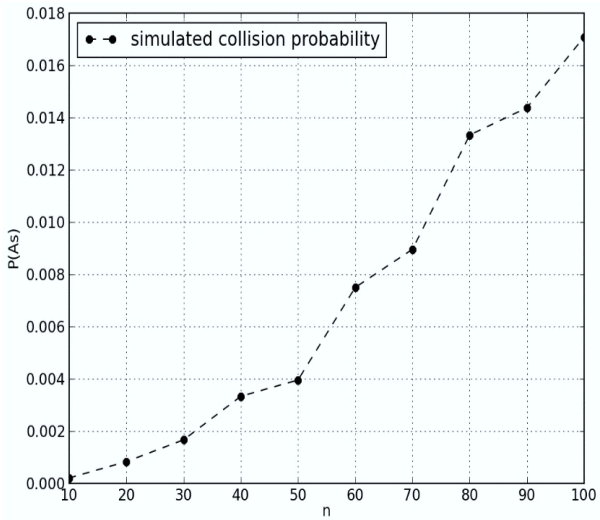

Figure 10: Influence of the number of nodes with different average times between transmissions on the probability of collision: the number of nodes with an average time between transmissions T = 10 s is 10% of the total number of nodes, and 90% of nodes operate with an average time between transmissions T = 60 s

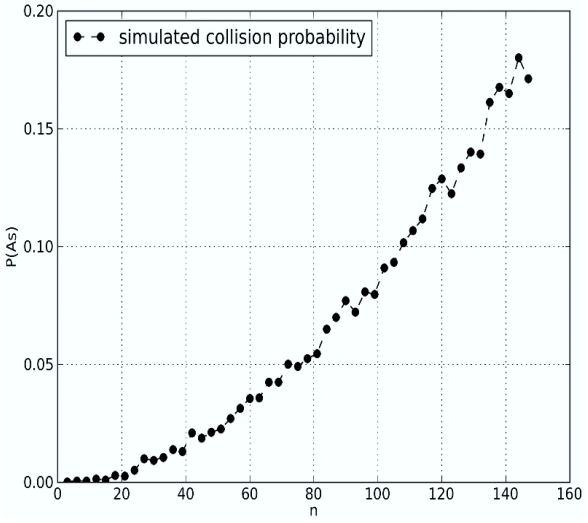

Figure 11: Influence of the number of nodes with different average times between transmissions on the probability of collision: the number of nodes with an average time between transmissions T = 10 s is 1/3 of the total number of nodes, and 2/3 of nodes works with an average time between transmissions T = 30 s

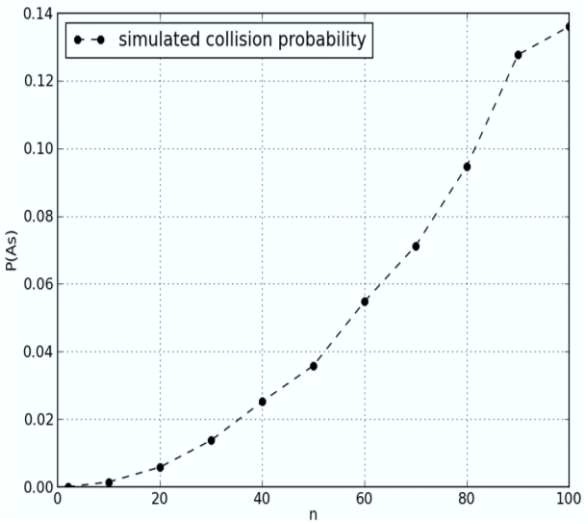

Figure 12: Influence of the number of nodes with different average times between transmissions on the probability of collision: the number of nodes with an average time between transmissions T = 10 s is 50% of the total number of nodes, the remaining 50% of nodes work with an average time between transmissions T = 30 s

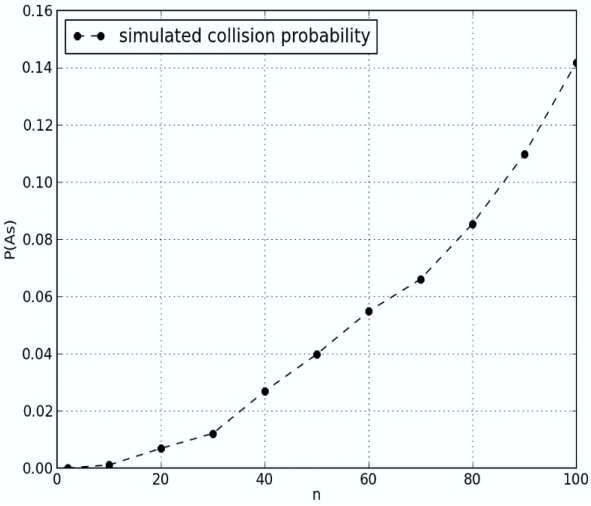

Figure 13: Influence of the number of nodes with different average times between transmissions on the probability of collision: the number of nodes with an average time between transmissions T = 10 s is 50% of the total number of nodes, the remaining 50% of nodes work with an average time between transmissions T = 60 s

This indicates that the longer the average time between transmissions of node *T*, the better the network works (with fewer collisions). An essential condition is that the duration of the communication protocol t_p is much shorter than the average time between transmissions of nodes *T*. Therefore, if a significant part of

packets in the radio space can be broadcast as infrequently as possible, the better for the overall result. quality of radio transmission. Therefore, the division into percentage groups of nodes with different average times between transmissions is quite justified. A further consequence of this fact, which can be seen in the graphs below compared to the results obtained if the nodes have only one average broadcast time, is the ability to increase network capacity (*n* nodes) for a stable transmission quality expressed by the probability of collision.

Based on the results of the computer simulation of WSN, the correspondence of the obtained theoretical dependences of collision probability for:

a. the same mean times between data transmissions.
b. the case of the division of nodes into groups with different mean times between data transmissions.

The quality of data transmission in WSN with random access depending on the different percentages of nodes in the groups was evaluated and analyzed. The influence of groups of nodes with variable average times between transmissions on the quality of data transmission in WSN with random access is investigated. Based on the results of model studies, the convergence of theoretical positions with the data obtained by computer simulation of WSN with random access was confirmed.

7. Conclusion

Based on the results of the analysis it was proved today it is necessary to create a new class of wireless networks that allow filling certain gaps in the development of WSN networks related to solving problems such as: obtaining low financial costs in terms of network nodes equipped with sensors for general and simple applications, ease of operation, in particular, sensor algorithms and ease of connecting and disconnecting new components, significant limitation of the occupied band of radio frequencies in the context of the growing deficit of the radio frequency spectrum; significant energy savings at the nodes (reduction of nodes for data processing, no receiver signal, autonomous operation of nodes in the intervals of very short activity and short-term radio radiation), especially due to lack of energy replenishment directly related to node operation time, complete independence of the nodes from each other.

Stochastic models of the functioning of wireless sensor networks that use randomized network parameters (with variable number of nodes and random participation of nodes in separate groups of network nodes) have been improved. It allowed us to estimate the probability of collision of signals and to more effectively design communications protocols of the IoT for critical infrastructures of the state [26–28]. These models allowed us to estimate the probability of collision of signals: the maximum number of nodes that provide the quality of transmission at the level of the probability of collision no higher than 10^{-2} is 50, with the number of nodes involved in the collision is negligible in comparison with the average number of transmissions, in particular, the ratio of the average number involved in the collision of nodes to the average number of transmissions is 10^{-7}.

Monitoring information technology was further developed, which through the use of stochastic models of wireless sensor networks and advanced monitoring methods, allowed to development of software and hardware (using Arduino, JavaScript, NodeJs, HTML, and CSS) monitoring of real-time environmental parameters in real-time IoT concepts. This complex of real-time environmental parameters monitoring can be used as a prototype for the organization of monitoring in dynamically changing environments and the event of various critical situations.

Based on the developed mathematical models of WSN, model studies were conducted to verify the theoretical dependences of the collision probability basis of the collision probability modeling, which allowed to verification of the proposed models. Based on the results of the computer simulation of WSN, the correspondence of the obtained theoretical dependences of collision probability for:

a. the same mean times between data transmissions.
b. the case of the division of nodes into groups with different mean times between data transmissions.

The quality of data transmission in WSN with random access depending on the different percentages of nodes in the groups was evaluated and analyzed. The influence of groups of nodes with variable average times between transmissions on the quality of data transmission in WSN with random access is investigated. Based on the results of model studies, the convergence of theoretical positions with the data obtained by computer simulation of WSN with random access was confirmed.

Future studies in this direction will be focused on the security problems [27–30] of the WSN models and IoT-based systems (encryption, incident response, DoS/DDoS security, and other up-to-date security challenges).

References

[1] G. Rahman, K. Wahid, LDCA: Lightweight Dynamic Clustering Algorithm for IoT-Connected Wide-Area WSN and Mobile Data Sink Using LoRa, IEEE Internet Th. J. 9(2) (2022) 1313–1325. doi: 10.1109/JIOT.2021.3079096.

[2] B. Mazon-Olivo, A. Pan, Internet of Things: State-of-the-art, Computing Paradigms and Reference Architectures, IEEE Latin America Transactions 20(1) (2022) 49–63. doi: 10.1109/TLA.2022.9662173.

[3] I. Kuzminykh, et al., Investigation of the IoT Device Lifetime with Secure Data Transmission, Internet of Things, Smart Spaces, and Next Generation Networks and Systems, vol. 11660 (2019) 16–27. doi: 10.1007/978-3-030-30859-9_2.

[4] V. Sokolov, et al., Method for Increasing the Various Sources Data Consistency for IoT Sensors, in: IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PICST) (2023) 522–526. doi: 10.1109/PICST57299.2022.10238518.

[5] Z. Hu, et al., Bandwidth Research of Wireless IoT Switches, in: IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (2020). doi: 10.1109/tcset49122.2020.2354922.

[6] M. Hadidi, et al., ZigBee, Bluetooth and Wi-Fi Complex Wireless Networks Performance Increasing, Int. J. Commun. Antenna Propag. 7(1) (2017) 48–56. doi: 10.15866/irecap.v7i1.10911.

[7] A. Mukesh, et al., Design and Analysis of an Edge Truncated Flexible Antenna for Wi-Fi Applications, Int. Conf. Electron. Renew. Syst. (2022) 1861–1864. doi: 10.1109/ICEARS53579.2022.9752032.

[8] M. Hadidi, et al., Adaptive Regulation of Radiated Power Radio Transmitting Devices in Modern Cellular Network Depending on Climatic Conditions, Contemp. Eng. Sci. 9(10) (2016) 473–485. doi: 10.12988/ces.2016.629.

[9] S. Soni, G. Kaur, Performance Analysis of Four Layer Clustering Network Using Enhanced Deterministic Energy-Efficient Clustering Protocol in Wireless Sensor Network, Fifth Int. Conf. Adv. Comput. Commun. Technol. (2015) 679–685. doi: 10.1109/ACCT.2015.120.

[10] L. Hernández-Alpizar, A. Carrasquilla-Batista, L. Sancho-Chavarría, Monitoring Adjustment Based on Current Data of an IoT-COTS Monitor for Environmental Chemical Analysis, IEEE 12th Latin America Symp. Circuits Syst. (2021) 1–4. doi: 10.1109/LASCAS51355.2021.9459119.

[11] T. Tsmots, O. Kuzmin, S. Kuzmin, Simulation of Environmental Monitoring Using Wireless Sensor Networks, IEEE 15th Int. Conf. Comput. Sci. Inf. Technol. (2020) 361–364, doi: 10.1109/CSIT49958.2020.9322054.

[12] M. Zaliskyi, et al., Method of Traffic Monitoring for DDoS Attacks Detection in E-Health Systems and Networks, in: Informatics & Data-Driven Medicin vol. 2255 (2018) 193–204.

[13] A. Carrasquilla-Batista, et al., IoT Applications: On the Path of Costa Rica's Commitment to Becoming Carbon-Neutral, Int. Conf. Internet Th. Global Community (2017) 1–6. doi: 10.1109/iotgc.2017.8008975.

[14] M. Onibonoje, An IoT Design Approach to Residential Energy Metering, Billing and Protection, IEEE Int. IoT Electron. Mechatron. Conf. (2021) 1–4. doi:

10.1109/IEMTRONICS52119.2021.9422580.
[15] ITU-T Y.2060:Overview of the Internet of Things (06/2012).
[16] P. Shrivastava, A Hybrid Sink Repositioning Technique for Data Gathering in WSN, Wireless Sensor Networks—Insights and Innovations (2017). doi: 10.5772/intechopen.70335.
[17] A. Nayak, I. Stojmenovic, Sink Mobility in Wireless Sensor Networks, Wireless Sensor and Actuator Networks: Algorithms and Protocols for Scalable Coordination and Data Communication, IEEE (2010) 153–184. doi: 10.1002/9780470570517.ch6.
[18] S. Glisic, Sensor Networks, Advanced Wireless Networks: Technology and Business Models, Wiley (2016) 194–243. doi: 10.1002/9781119096863.ch5.
[19] J. Al-Azzeh, et al., Analysis of Self-Similar Traffic Models in Computer Networks, Int. Rev. Modelling Simul. 10(5) (2017) 328–336. doi: 10.15866/iremos.v10i5.12009.
[20] M. Karpmski, et al., Wireless Sensor Networks with Randomized Parameters, 16th Int. Conf. Control Autom. Syst. (2016) 1470–1475, doi: 10.1109/ICCAS.2016.7832497.
[21] M. Assim, A. Al-Omary, Design and Implementation of Smart Home using WSN and IoT Technologies, Int. Conf. Innovation Intell. Inform. Comput. Technol. (2020) 1–6. doi: 10.1109/3ICT51146.2020.9311966.
[22] M. Lazarescu, Design of a WSN Platform for Long-Term Environmental Monitoring for IoT Applications, IEEE J. Emerging Selected Topics Circuits Syst. 3(1) (2013) 45–54. doi: 10.1109/JETCAS.2013.2243032.
[23] A. Singh, P. Kumar, Advancement in Quality of Services in Wireless Sensor Networks, 3rd International Conference On Internet of Things: Smart Innovation and Usages (2018) 1–5. doi: 10.1109/IoT-SIU.2018.8519842.
[24] V. Grechaninov, et al., Decentralized Access Demarcation System Construction in Situational Center Network, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3188, no. 2 (2022) 197–206.
[25] V. Grechaninov, et al., Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center, in: Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things, vol. 3149 (2022) 107–117.
[26] S. Gnatyuk, V. Sydorenko, M. Aleksander, Unified Data Model for Defining State Critical Information Infrastructure in Civil Aviation, IEEE 9th Int. Conf. Dependable Syst. Services Technol. (2018) 37–42.
[27] S. Gnatyuk, Critical Aviation Information Systems Cybersecurity, Meet. Secur. Chall. Thr. Data Anal. Decis. Support 47(3) (2016) 308–316. doi: 10.3233/978-1-61499-716-0-308.
[28] Yu. Danik, R. Hryschuk, S. Gnatyuk, Synergistic Effects of Information and Cybernetic Interaction in Civil Aviation, Aviation 20(3) (2016) 137–144. doi: 10.3846/16487788.2016.1237787.
[29] S. Ismail, D. Dawoud, H. Reza, A Lightweight Multilayer Machine Learning Detection System for Cyber-attacks in WSN, IEEE 12th Annu. Comput. Commun. Workshop Conf. (2022) 0481–0486. doi: 10.1109/CCWC54503.2022.9720891.
[30] H. Tao, et al., Secured Data Collection with Hardware-Based Ciphers for IoT-Based Healthcare, IEEE Internet Th. J. 6(1) (2019) 410–420. doi: 10.1109/jiot.2018.2854714.
[31] Z. Hu, et al., Method for Optimization of Information Security Systems Behavior under Conditions of Influences, Int. J. Intell. Syst. Appl. 9(12) (2017), 46–58. doi: 10.5815/ijisa.2017.12.05.
[32] A. Singh, N. Kushwaha, Software and Hardware Security of IoT, IEEE Int. IOT, Electron. Mechatron. Conf. (2021) 1–5. doi: 10.1109/IEMTRONICS52119.2021.9422651.