UDC 510.83/.86: [004:658] (02) **doi:** https://doi.org/10.20998/2522-9052.2025.4.05

Oleg Barabash[1], Valentyn Sobchuk[2], Andrii Sobchuk[3], Andrii Musienko[1], Oleksandr Laptiev[2]

[1] National Technical University of Ukraine “Ihor Sikorskyi Kyiv Polytechnic Institute”, Kyiv, Ukraine
[2] Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
[3] State University of Information and Communication Technologies, Kyiv, Ukraine

TOPOLOGICAL ASPECTS OF DESIGNING FUNCTIONALLY ROBUST WIRELESS SENSOR NETWORKS

Abstract. Research objective: To develop and analyze topological approaches for constructing functionally stable wireless sensor networks (WSNs) that ensure uninterrupted monitoring and control under the influence of destabilizing factors, particularly in critical infrastructure systems and the manufacturing sector. **Research object:** The operation and management processes of wireless sensor networks, as well as their resilience to external and internal disruptions. **Research subject**: The topological aspects of wireless sensor network design that impact their functional stability, including structural self-organization, connectivity metrics, and mechanisms for minimizing data transmission collisions. **Research results.** This article explores topological strategies for designing functionally robust WSNs in the context of monitoring and managing facilities, especially within critical infrastructure and industrial environments. Key challenges such as high energy consumption, latency, and vulnerability to interference are identified, necessitating thorough analysis at the design stage. The significance of properly formulating the synthesis task and selecting appropriate performance criteria is emphasized to ensure effective WSN operation. An analysis of existing systems based on current solutions highlights the capabilities of remote control and monitoring. The study investigates the features and advantages of such networks, including self-organization, energy independence, self-diagnostics, and scalability. However, it also reveals a low level of functional robustness in existing hierarchical WSNs, due to a limited number of alternative routes, low vertex and edge connectivity, and a low probability of connectivity between structural components. The proposed directions for further research include a comparative analysis of topologies, development of modified topologies for WSNs in critical infrastructure applications, evaluation of their stability, exploration of collision minimization mechanisms, and estimation of communication channel costs. The findings of this study aim to enhance the reliability and efficiency of wireless sensor networks under challenging operational conditions.

Keywords: network topology; functional stability; wireless network; sensor network; structure synthesis.

Introduction

Among the general challenges of building wireless sensor networks (WSNs), the task of managing and monitoring both the target objects and the system components themselves represents a central aspect in the design and development of complex systems. Effective control over key network performance indicators enables optimized distribution of information flows, as well as efficient management of data processing and transmission channels with minimal consumption of system resources. At the same time, it allows for various forms of redundancy – both in components and resources – to ensure stable system operation in the presence of internal and external destabilizing factors.

However, implementing these tasks in practice can be challenging due to the specific operational characteristics of WSNs and the nature of the assigned tasks. Therefore, it is essential to consider the individual characteristics and operational conditions of each WSN during the design stage, including potential negative environmental influences.

Certain functional features of WSNs—such as high energy consumption during data reception, processing, and transmission; significant time delays caused by long distances between nodes or transmission errors due to channel noise; interference; or node malfunctions – can adversely affect overall system performance. These factors necessitate more in-depth analysis during the planning and design phases.

One of the key approaches to studying the control and operational processes of a WSN involves formulating the synthesis problem and selecting appropriate performance indicators and evaluation criteria for the system under consideration.

Overview of sources by research topic. In [1], algorithms for the synthesis of functionally stable wireless sensor networks (WSNs) are presented; however, the study does not address the topological aspects and their influence on the design and operation of such networks. The authors of [2] focus on the architectures of information systems, network resources, and network services, providing a conceptual foundation for understanding how different WSN components interact and how architecture influences their functional stability.

In [3], a method for improving routing efficiency in self-organizing networks is proposed – an approach that is critically important for WSNs, as efficient and adaptive routing significantly enhances functional stability, especially under dynamic conditions.

A number of studies [4–9] explore the mathematical and topological foundations of dynamical systems, metrics, algebras, and impulse processes. These works provide a theoretical basis for analyzing the stability of complex technical information systems in terms of their temporal behavior and response to external influences.

Studies [10, 11] are dedicated to system analysis and methods for ensuring the functional stability of information systems, including those used in critical infrastructure and industrial processes. These contributions are closely related to the concept of functional stability and its application to WSNs.

Article [12] presents an approach for enhancing the functional stability of production processes using neural networks, demonstrating the potential of artificial intelligence in improving WSN resilience. Furthermore, the authors of [13] propose an AI-based algorithm for detecting anomalies in network traffic—an essential element in strengthening WSN cybersecurity. In [14], a comprehensive intrusion detection system (IDS) for IoT/IIoT cybersecurity is introduced, based on the Zero-Trust principle, highlighting the critical importance of security in building functionally robust WSNs.

The reviewed studies cover a wide range of topics related to the functional stability, optimization, and security of information systems, including WSNs. However, they do not sufficiently investigate topological features and their specific impact on the synthesis and operation of functionally stable wireless sensor network.

Research results

Description of the properties of a wireless sensor network. This paper addresses the general synthesis problem for a wireless sensor network (WSN) based on the self-organization of its structure and presents calculations of specific performance characteristics of the network according to the defined problem.

For analysis, a system used in the automation of critical infrastructure facilities and agricultural production was selected. Its primary function is the remote monitoring and control of production environments. The solution is based on Advantech technologies, including the ADAM-62xx Ethernet I/O series, wireless sensor nodes, and WebAccess 8.0 HMI/SCADA software. This setup enables users to monitor and control the environment in real time via a virtual control panel accessible from a PC, tablet, smartphone, or other device.

The system incorporates a standalone set of controllers and sensors (e.g., for temperature, humidity, soil pH), as well as IP cameras, automatic dispensers, ventilation units, and more. It also supports remote monitoring and control through a custom-developed user interface.

The remote monitoring and control system for critical infrastructure facilities-essentially a wireless sensor network, provides:

- remote monitoring of the temperature of the processor, fan and other equipment parameters using the system management and maintenance software client;
- use of a widget library and a dashboard editor to customize a cross-platform dashboard page to display dynamic data on end-user devices (PC, tablet, smartphone, etc.);
- setting thresholds for temperature, humidity, soil pH level, etc., as well as reading and transmitting data from end nodes;
- analysis of measurement results, maintenance of an archive of measurement results.

A feature of such a wireless sensor network is:

- the ability to self-organize and autonomously operate the network in the event of a temporary or complete failure of individual system elements;
- non-volatile operation over a long period of operation, which is achieved by using autonomous power supply (batteries) by the end nodes of the network;
- the presence of a built-in self-diagnostics system;
- - the use of dedicated servers (main and backup) for storing and processing the main observed parameters of the studied environment; the possibility of using wired and wireless methods of information transmission.

The advantages of this system are:

- - autonomous operation and self-organization of the system in the event of failure of its individual elements under the negative influence of external or internal destabilizing factors before the intervention of qualified personnel;
- remote management and monitoring of the state of network elements to ensure timely analysis and change of the limit values of the studied parameters if necessary;
- distributed analysis and processing of data, both on dedicated servers and on end nodes.

Components of the system:

- wireless end nodes, concentrators, coordinators;
- dedicated servers for collecting and processing information;
- software for data analysis and managing the wireless sensor network.

It should be noted that this system can be scaled (wireless sensor networks based on ZigBee or Threat technologies support up to several hundred devices), which will not negatively affect the overall efficiency of network management and operation. However, the analysis results show that these networks are characterized by a low level of functional stability, namely:

- hierarchical construction of a wireless sensor network (tree topology) with a small number of alternative routes;
- low degree of vertex connectivity of the structure $\chi(G) \leq 2$, which does not ensure the operation of the system in the event of a complete or temporary failure of more than two network elements;
- low degree of edge connectivity of the structure $\lambda(G) \leq 2$, which does not ensure the operation of the system in the event of a complete or temporary failure of more than three *communication channels* (CCh);
- low probability of connectivity of structural elements, which does not allow maintaining its connectivity under the influence of internal and external destabilizing factors.

Comparative characteristics of the topology of sensor wireless networks of critical infrastructure facilities. That is why, to solve this problem, it is necessary to adhere to the developed methodology for ensuring the functional stability of a wireless sensor network (analysis of the level of functional stability, synthesis of the WSNs structure) at the stages of system design and operation.

The choice of network topology can serve as an additional factor that will help minimize energy consumption, while leaving unchanged or maximizing the range, without delay in data transmission. The best characteristics of the network topology, in this case, are obtained with a circular arrangement of network nodes (in the center and at the ends of the diameter) [15]. In Fig. 1, the vertices of the graph mean sensor nodes, and the edges of the graph are communication channels between them.

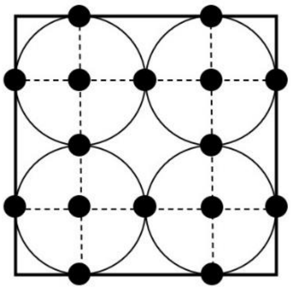

Fig. 1. Circular topology of a wireless sensor network

This arrangement of elements allows not only to maintain the overall efficiency and reliability of the network, but also requires a smaller number of elements used in its deployment.

To calculate the number of network nodes in a certain area (network coverage) according to the network topology, we use the following formulas:

$$N_s = 1.15 \cdot \frac{A_{total}}{d_{sense}^2}, \tag{1}$$

$$N_s = \frac{A_{total}}{d_{sense}^2}, \tag{2}$$

$$N_s = 0.77 \cdot \frac{A_{total}}{d_{sense}^2}, \tag{3}$$

$$N_s = \left(\frac{L}{2d_{sense}}\right) \cdot \left(\frac{B}{d_{sense}} + 1\right) + \\ + \left(\frac{L}{2d_{sense}} + 1\right) \cdot \left(\frac{B}{d_{sense}}\right), \tag{4}$$

where N_s is total number of wireless sensor network elements; A_{total} is total coverage area of the wireless sensor network; a_{sense} – distance between elements of a wireless sensor network.

Formulas (1)–(4) allow you to calculate the total number of network elements depending on the selected topology, in particular, formula (1) for a triangular network topology, formula (2) for a square network topology, formula (3) for a hexagonal network topology and formula (4) for a circular topology with a node in the center. Taking into account the network topology, we will calculate the number of elements that can be placed on 1 ha. ZigBee technology (IEEE 802.15.4) has a range of 10 to 100 meters, but it will be sufficient to consider the smallest values with a placement interval of 10 meters. The calculation results are given in Table 1.

Table 1 – **Calculating the number of network elements based on its topology**

Network topology	Required number of network nodes		
	***r* = 10 m**	***r* = 20 m**	***r* = 30 m**
Triangular	115	29	13
Square	100	25	12
Hexagonal	77	20	9
Circular with a knot in the center	75	17	9

Based on the data obtained, it can be concluded that a circular topology with an additional node in the center will require the least number of elements, which will have a significant effect if significant network coverage is required.

Assertion 1. *The redundancy of the triangular topology, compared to the circular one with a node in the center, is estimated to be at least 31%.*

This indicator is important not only from the point of view of reducing costs, both time and financial, when deploying a network, but also allows you to maximize the network uptime.

Fig. 2 shows the dependence of the router's operating time, which processes information transmitted by network elements [16]. The above values clearly demonstrate that with a larger number of network elements, its overall operating time will decrease in accordance with the router's electricity consumption (power consumed in standby mode).

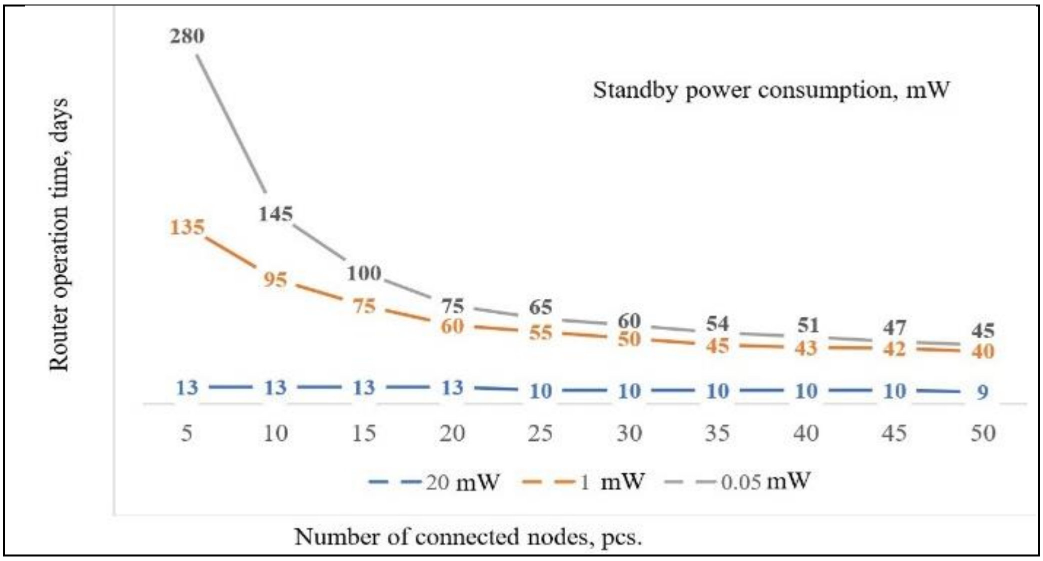

Fig. 2. Dependence of the operating time of a router processing data on the number of network elements

Fig. 3, a presents a conventional layout of the elements of a wireless sensor network for automation of critical infrastructure facilities for the purpose of remote monitoring and control of facility parameters, in which existing types of redundancy are used: in particular, an excessive number of network elements, as well as communication channels between them.

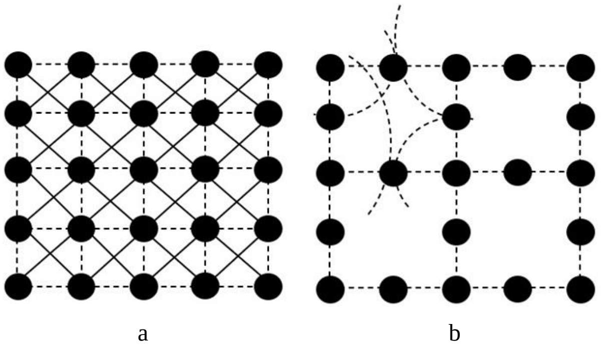

Fig. 3. Conventional diagram of the location of wireless sensor network elements and connections between them

Modified topology of a wireless network of critical infrastructure facilities. The approach described above can be quite expensive, as using each additional sensor in the system will have low efficiency. It is also very expensive to scale such a system.

In Fig. 4, after certain transformations (removal of nodes) shown in Fig. 3, b, a modified topology of a wireless sensor network is presented, covering the same area, without a significant decrease in the efficiency of the system, while using a significantly smaller number of elements.

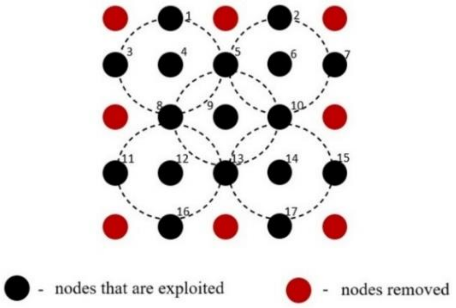

Fig. 4. Modified topology of a wireless sensor network

This approach, in turn, allows you to optimize the costs of implementation and operation, especially when scaling the system.

It should be noted that in addition to the location of network elements, the location of the end server to which data is transmitted for further processing, as well as the network coordinator, which is provided by most short-range wireless data transmission technologies, is also important. Let us consider topologies where vertices 1 and 9 were selected as network coordinators. Fig. 5 shows possible variants of the wireless sensor network topology based on the self-organization of its structure in the automation of critical infrastructure facilities for remote monitoring and control of territories.

This topology involves the implementation of coordinator nodes that serve to control and manage the network, however, in the event of a failure of the selected node, other nodes can perform this function to ensure the normal functioning of the system as a whole. Such a scheme for building a wireless sensor network has predefined communication channels and actually has a hierarchical structure (the head node is given). For clarity, such a structure is presented in Fig. 6.

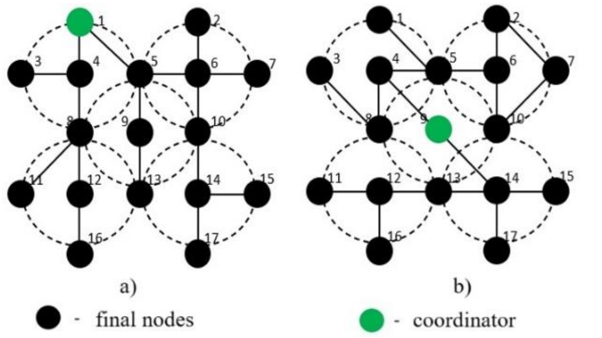

Fig. 5. Diagram of connections between elements of a wireless sensor network

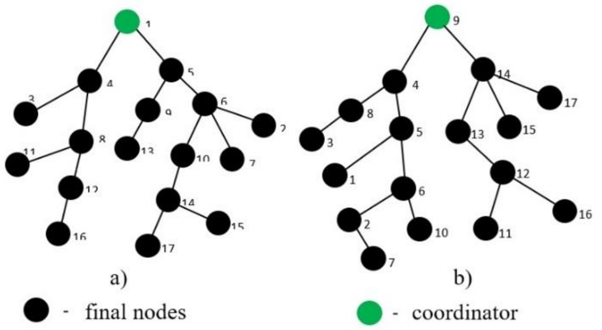

Fig. 6. Modified diagram of connections between elements of a wireless sensor network

Stability analysis of a modified wireless sensor network topology. Let us consider case b) of the network element layout, and analyze its structure in more detail. Let us analyze this structure of the proposed topology of the wireless sensor network to provide a more detailed assessment of the functional stability characteristics of the system.

1. The initial structure of the presented topology is (Fig. 6, b)) a hierarchical structure with defined information transmission channels. The graph of the structure is single-component, connected.

2. The number i of sensor node locations. The structure consists of $N = 17$ network elements, which includes end nodes and a defined coordinator.

3. Communication channels. In the presented structure of the wireless sensor network, there are $M = 16$ communication channels. The adjacency matrix of the graph is presented in Table. 2.

To estimate the probability of connectivity P_{ij} the value of the probability of the existence of communication channels (the probability of information transmission between adjacent v_i and v_j via communication channel e_{ij}) varies within $p \in [0{,}5;\ 0{,}95]$.

4. Indicators of functional stability. Vertex connectivity measure $\chi(G)$ and the edge connectivity measure $\lambda(G)$: $\chi\ (G) = 1; \lambda(G) = 1$.

5. Functional endurance reserve. Peak functional endurance reserve Z_V and rib margin of functional stability Z_E: $Z_V\ =\ 0;\ Z_E\ =\ 0$.

6. Structural parameters of the graph: redundancy coefficient, graph diameter, centrality coefficient.

Table 2 – **Location of elements of the selected topology WSN**

Node No.	Local measure δi	Adjacency of elements
1	1	5
2	2	6, 7
3	1	8
4	3	5, 8, 9
5	3	1, 4, 6
6	3	2, 5, 10
7	2	2, 10
8	2	3,4
9	2	4,14
10	2	6,7
11	1	12
12	3	11, 13, 16
13	2	14, 16
14	4	9, 13, 15, 17
15	1	14
16	1	12
17	1	14

Technological solutions for the application of wireless sensor networks. A common solution in the field of wireless sensor networks is to use the following hardware solution:

- RISC processor with a frequency of 8 to 32 MHz;
- RAM capacity from 8 to 192 KB;
- External flash memory capacity from 0.5 to 8 MB.

Particularly important are the characteristics of power consumption in different modes. Typical values are given in Table 3.

Table 3 – **Operating modes of WSN wireless modules**

Operating mode	Power designation	Typical value, mW
Reception	P_{rx}	52
Transmission	P_{tx}	45
Processing	P_a	20
Sleep mode	P_s	0,03

Energy efficiency is determined by how rationally a system uses the energy supplied to it from the outside.

Energy efficiency is determined by how efficiently a system uses the energy supplied to it from outside

$$E = \frac{w_n}{w_{\text{п}} + w_{\text{нп}}},$$

where $w_{\text{п}}$ this is energy that is used efficiently; $w_{\text{нп}}$ this is unproductive energy consumption.

In general, a node in a wireless data collection network can be considered operational as long as it is capable of accurately reading sensor data, performing the necessary computations, and transmitting the results to the network. When designing and deploying such a network, it is important to estimate the expected operating time of each node before its battery requires replacement. This requires identifying the key factors that influence the duration of autonomous operation and ensuring appropriate mechanisms are in place to notify maintenance personnel when a sensor's battery reaches a critical charge level.

Knowing the initial battery energy E_0 and the power P consumed by the device, we can approximately estimate its life time using the formula

$$t = E_0/P.$$

The end device is designed to read readings from its own sensors and transmit them to the network. Its main difference from a repeater is the lack of the ability to transmit data from other devices through itself. When using the event model or the scheduled transmission model, it usually operates cyclically Fig. 7:

$$P_{ed} = \frac{P_f t_f + P_a t_a + P_s(t_c - t_f - t_a)}{t_c},$$

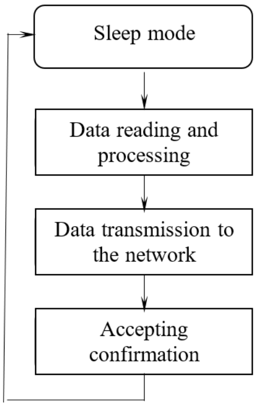

Fig. 7. End device operation cycle

where t_c is the duration of one operating cycle of the device [c]; P_f is the average power consumed during data transmission and subsequent acknowledgment reception [W]; t_f is the time spent on data transmission and acknowledgment exchange [c]; P_a is the power consumption during data processing (e.g., reading sensor values) [W]; t_a is the total time required for reading sensor data, processing it, and preparing it for transmission [c]; P_s is the power consumption in sleep mode [W].

It is assumed that $t_a + t_f < t_c$ meaning that the end device has sufficient time to enter sleep mode during each cycle.

Time spent transmitting all frames including sending acknowledgements [17]

$$k_{tx} = \sum_{i=1}^{n} \tau_i \lambda_i + t_{ACK} \sum_{i=1}^{n} \lambda_i,$$

where τ_i is time spent on transmitting one packet; t_{ACK} – is time required to send an acknowledgement for each frame.

Mechanisms for minimizing data transmission collisions in wireless sensor networks. The mechanism for preventing collisions at the channel level involves the use of a guard interval (also known as a backoff interval—a temporary delay before data transmission), which ultimately increases the overall transmission delay. Another important factor is the calculation of the total probability of collisions during data transmission, as well as the potential need to establish a connection between nodes in advance (if required by the network's communication services) and to periodically renegotiate that connection at predefined intervals.

Due to the potential for significant transmission delays, network elements may switch between different operating modes to conserve energy, especially since nodes rely on autonomous power sources. Moreover, a given wireless sensor network node can receive data addressed to it only during specific, periodically repeated time windows when the node is in an active state. While this approach helps reduce power consumption, it can also increase the total time required for data exchange between two nodes in the system [18]

$$\bar{t} = \bar{t}_{MAC} + \bar{\tau},$$

where $\bar{t}_{MAC}$ is time required to implement data transmission of the corresponding data link layer protocol; $\bar{\tau}$ is average waiting time for a node to be active to receive or transmit data.

When implementing the standard IEEE 802.15.4 [19] average data transmission time between two nodes of the system, in a free communication channel, according to [19] can be represented as

$$\bar{t}_{MAC} = T_{backoff} + T_{data} + T_{ack} + T_{trt}.$$

where $T_{backoff}$ is time $backoff$ interval (default 2.368 ms); T_{data} is data transfer time (4.256 ms); T_{ack} is confirmation transmission time, regarding the establishment of a connection between a pair of nodes (0.352 ms); T_{trt} is time to receive confirmation (0.192 ms).

In the case where different frequency channels are used for reception and transmission by a transit node (not the source or final destination of data transmission) [30], the throughput is approximately half of the possible data transmission rate over a given communication channel.

If a scenario is implemented using different frequency channels for data transmission, the possible packet delay in one service phase can be determined

$$\bar{t}_{mfmac} = 2\bar{t}_{MAC}.$$

The average waiting time for a network node to be active τ can vary depending on its size and the services it uses [20].

Characteristics of packet retransmission in wireless sensor networks. An equally important indicator of the performance of a wireless sensor network is the average number of packet retransmissions, which may be due to collisions in the data transmission channel, errors during reception and transmission of information, data integrity violations, etc. Let b_e and p_e be the probability of a bit error (BER – *Bit Error Rate*) and a packet transmission error (PER – *Packet Error Rate*), respectively. Based on the size of the packet length (which depends on the service and technology of short-range wireless data transmission), which is equal to L bits, the probability of a packet transmission error between network elements is equal to

$$p_e = 1 - (1 - b_e)^L.$$

As mentioned earlier, a packet transmission error leads to its retransmission (if the service used requires it). Retransmission improves network reliability, but increases latency, which negatively affects the efficiency of the network as a whole. That is why the maximum number of data retransmissions can be limited to a certain number of attempts K (including attempts to establish or restore a connection with the corresponding network node), after which the node is considered unavailable and an attempt is initiated to establish an alternative route between the nodes.

The average number of retransmission attempts can be calculated as follows [21]

$$n_r = \sum_{i=1}^{K-1} i p_e^i (1 - p_e) + K p_e^K.$$

Determining and minimizing the bit error rate (BER) is a critical task in short-range wireless sensor networks, as the data transmission environment is often susceptible to errors and distortion caused by natural or artificial interference and general signal instability. For such networks, a commonly accepted threshold for the bit error rate is no more than 10^{-3} per bit, which is considered acceptable in many practical scenarios.

However, in cases where a lower BER is required, error correction mechanisms are typically employed. These methods can reduce the number of bit errors by one to three orders of magnitude. Nevertheless, the use of error-resilient coding comes at a cost: increased computational load, higher energy consumption, and a reduction in data transmission speed by approximately 1.5 to 2 times. These trade-offs may not be acceptable in all applications.

Experimental results on data transmission in wireless sensor networks. In an experimental environment during data transmission in a point-to-point topology, it was found that when using noise-tolerant coding, the bit error probability approximately reaches the level of $10^{-6} - 10^{-7}$. However, in a more complex topology, where message retransmission is possible, the bit error probability increases, but usually does not exceed 10^{-5} [22].

Assertion 2. *During packet data transmission with a packet length of less than* 1 *kbit, no more than* 1% *of bits will be lost, which should not affect the efficiency of the system.*

Evaluating the cost of communication channels in wireless sensor networks. The cost of the given costs for communication channels is also a variable (this implies the use of additional hardware modules to establish 2 or more communication sessions at the same time). The total cost of data transmission costs between nodes of a wireless sensor network can be calculated as

$$C_{\text{CCH}} = \sum_{i=1}^{N} \sum_{j=1}^{N} C_{ij} \cdot a_{ij}, \qquad (5)$$

where a_{ij} is elements of the structure adjacency matrix; C_{ij} is cost of capital investment and operation of a direct communication channel between sensor nodesv_i and v_j

$$C_{ij} = \left(k_{\text{cap}} \cdot l_{ij} + C_{ij}^{\text{oper}}\right) \cdot \left[h_{ij}/\rho\right], \qquad (6)$$

where k_{cap} s the capital investment required to establish a single communication channel, depending on the channel type; for calculations, it is assumed that $k_{\text{cap}} =$ 33,6 n.c.u. (*nominal conventional units*); l_{ij} is the distance between nodes v_i and v_j; h_{ij} is the intensity of information exchange between nodes v_i and v_j; ρ is the bandwidth of a single communication channel; it is assumed that $\rho > h_{ij}$; C_{ij}^{oper} is the operating cost of the information transmission channel between nodes.

The redundancy coefficient of connections (the ratio of the difference between the number of connections in the structure M and the minimum required number $M_{\min}$ of connections to ensure the connectivity of the graph to the value $M_{\min}$ is determined by the ratio

$$K_{\text{exces}} = \frac{M - M_{\min}}{M_{\min}} = \frac{M}{N-1} - 1, \qquad (7)$$

where $M_{min} = N - 1$ is the number of edges of a tree graph; N is the number of vertices of the graph. For the graph (Fig. 6):

$$K_{\text{exces}} = \frac{16}{17-1} - 1 = 0. \qquad (8)$$

The diameter of the graph characterizes the number of communication channels included in the route of maximum length

$$D = \max_{ij}\{d_{ij}\}, \quad i, j = \overline{1, N}, \quad i \neq j, \qquad (9)$$

where d_{ij} is the number of communication channels included in the shortest route between v_i and v_j.

Considering that a wireless sensor network consists of end devices, routers and coordinators, the set of network devices $\mathcal{N}$ can be divided into three subsets that combine all elements of the sensor network [23]:

$$\mathcal{N} \subset \mathcal{K},\ \mathcal{N} \subset \mathcal{R},\ \mathcal{N} \subset \mathcal{E},$$

where $\mathcal{K}$ is a subset of coordinators in the network; $\mathcal{R}$ is a subset of routers in a network; $\mathcal{E}$ is a subset of end devices in a network.

Then the total number of nodes in the network can be described as

$$\mathcal{N}_{all} = \sum_{i=1}^{n} \mathcal{N}_i = \sum_{j=1}^{k} \mathcal{N}_j + \sum_{l=1}^{r} \mathcal{N}_l + \sum_{s=1}^{e} \mathcal{N}_s,$$

where k is the number of coordinators in the network; r is the number of routers in the network; e is the number of end devices in the network; $\mathcal{N}_j$ is the j-th coordinator in the wireless sensor network; $\mathcal{N}_l$ is the l-th router of the network; $\mathcal{N}_s$ is the s-th terminal node of the network.

Let the maximum distance between $\mathcal{N}_i$ and $\mathcal{N}_j$, where $\mathcal{N}_i$ is in radio visibility $\mathcal{N}_j$, is called *the communication radius R_{radio}* nodes $\mathcal{N}_i$, and determines the connectivity of a wireless sensor network node (Fig. 8) [24].

Nodes $\mathcal{N}_i$ and $\mathcal{N}_j$ of a wireless sensor network can have direct radio communication if and only if [25]

$$\mathcal{N}_i \in M_{radio}(\mathcal{N}_i) \cap \mathcal{N}_j \in M_{radio}(\mathcal{N}_j),$$

where $M_{radio}(\mathcal{N}_j)$ is the set of radio neighbors.

In this case, two nodes are called neighbors if the intersection of their radiuses is not an empty set

$$R_s(\mathcal{N}_i) \cap R_s(\mathcal{N}_j) \neq \emptyset,$$

where $R_s(\mathcal{N}_i)$ is the radius of action of the sensor node $\mathcal{N}_i$; $R_s(\mathcal{N}_j)$ is the radius of action of the sensor node $\mathcal{N}_j$ for all $i, j = 1, 2, \dots, n$, $i \neq j$.

A connectivity-based criterion for the functional stability of wireless sensor networks. For a complete assessment of a sensor network from the point of view of the theory of functional stability, it is necessary to consider the criteria of network connectivity. Since the implementation of functional stability is achieved by using various, already existing types of redundancy (functional, structural, temporal, informational, etc.) in complex technical systems, it is necessary to ensure the redistribution of network resources for its uninterrupted functioning.

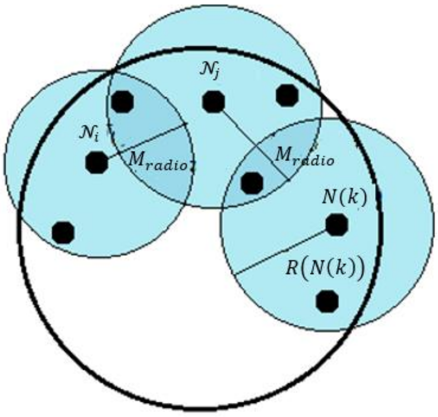

Fig. 8. Radio visibility zone of sensor network nodes

The relationship between the information transmitted and received by the sensors is described by the inverse square law [26].

$$P_{\text{пр}} \sim \frac{P_{\text{пер}}}{d^2}.$$

Here $P_{\text{пр}}$ is the power of the received signal, $P_{\text{пер}}$ is the power of the transmitted signal, d is the distance between the receiver and the transmitter.

The distance between nodes can be estimated based on the transmitter output power, receiver sensitivity, and antenna characteristics, along with empirical data. At the same time, it is important to consider that wireless sensor network elements may be affected by radio interference of both natural and artificial origin, which can significantly impact the effectiveness of data transmission and reception by reducing sensitivity.

The placement of WSN elements should be carefully planned during the design phase and subsequently refined during the initial setup and operational stages to ensure maximum functional stability – provided that all other system requirements are also met.

Introducing various types of redundancy helps maintain system performance even in the event of partial failures of nodes or services.

For theoretical estimations, the Friis free-space equation is used

$$P_r = P_t + G_t + G_r + 20\lg\left(\frac{\lambda}{4\pi}\right) - 20\lg d.$$

or

$$P_r = \frac{P_t G_t G_r \lambda^2}{(4\pi d)^2}, \qquad d = \frac{\lambda}{4\pi}\sqrt{\frac{P_t G_t G_r}{P_r}},$$

where P_t is the transmitter power; P_r is the signal sensitivity; G_t, G_r these are the gain coefficients of the antennas for transmitting and receiving information; d is the distance between nodes; λ is the wavelength.

All elements of a wireless sensor network (WSN) transmit information to a central gateway or a dedicated server for data processing, enabling a wide range of monitoring and control functions for individual network components.

Let us examine in more detail the structural criterion of WSN functional stability. Ensuring vertex and edge connectivity of network elements requires meeting specific technical parameters, particularly under destabilizing conditions.

Quality criterion for WSN operation. One of the key structural criteria for vertex connectivity is the implementation of energy-saving mechanisms by WSN nodes. As shown in [27], there is a *direct relationship between overall energy consumption and the number of active nodes in the network*. Therefore, it is essential to reduce and optimize total energy usage in order to maintain the network's functional stability and prolong its operational lifetime.

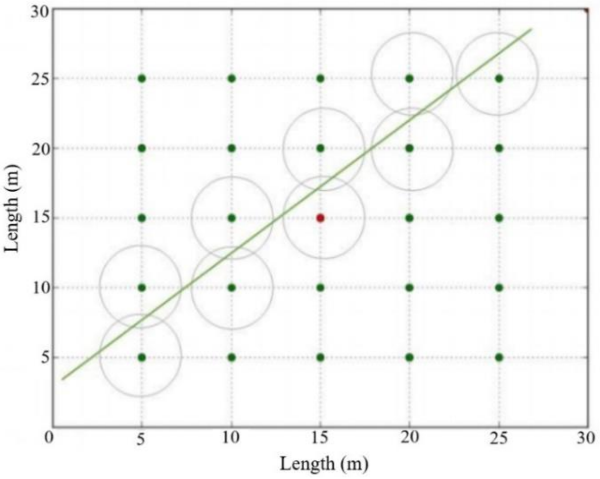

Fig. 9. Tracking a target moving along a given linear trajectory by a wireless sensor network

One of the main criteria for the functioning of a wireless sensor network is the period of its high-quality operation. In situations where it is necessary to ensure constant monitoring, such as monitoring and control of industrial processes, monitoring the state of production facilities or the environment. In this case, one of the key indicators of the functioning of the sensor network is the energy consumption of each of its components, to ensure long-term autonomous and uninterrupted high-quality functioning of the sensor network.

If we describe a wireless sensor network as a directed graph, it is worth noting that the search for the shortest data transmission route between nodes and network components plays an important role. The energy consumption of WSN elements can be conditionally divided into use in standby mode and during transmission/reception of information between nodes.

Let us assume that all nodes have the same energy charge and spend an identical percentage of the charge on data transmission and reception.

The goal, in this case, is to minimize the amount of energy consumed during a more active phase of energy consumption.

Let us describe the function that minimizes the amount of total energy consumed in all nodes as [28]

$$\sum_{i\in\mathbb{N}} e_{i0} - \sum_{\substack{i\in\mathbb{N},\\ i\neq n}} E_{i(et)} \to \min\ ,$$

where e_{i0} is the initial energy indicator of node i for all $i \in \mathbb{N}$ ($e_{i0} > 0$); $E_{i(et)}$ is the energy indicator of node i in time period t for $i \in \mathbb{N}$, $t \in T$; i, j, k these are the indices of the network nodes.

On the condition that

$$\sum_{\substack{i\in\mathbb{N}\\ ij\neq k}} X_{ikt} - \sum_{\substack{i\in\mathbb{N}\\ j\neq k}} X_{kjt} = 0$$

for all $i, k \in \mathbb{N}$, $t \in T$; $k \neq s$, $k \neq n$, where: X_{ikt} is a binary network status indicator equal to 1 if node i and j are related in time period t; 0 otherwise; s is the index of the source node for information transmission; N is the set of network nodes; T is the set of time periods;

$$X_{ijt} - X_{jit} \leq 1$$

for all $i, j \in \mathbb{N}$, $t \in T$, $i \neq j$;

$$\sum_{\substack{j\in\mathbb{N}\\ j\neq s}} X_{sjt} = 1$$

for all $t \in T$;

$$\sum_{\substack{i\in\mathbb{N}\\ i\neq n}} X_{int} = 1$$

for all $i \in \mathbb{N}$, $t \in T$;

$$d_{ij} \cdot X_{sjt} \leq ld$$

for all $i, j \in \mathbb{N}$, $t \in T$, where d_{ij} is the distance between nodes i and j for all $i, j \in \mathbb{N}$;

$$E_{it} - E_{it-1} + cw \cdot \sum_{\substack{j\in\mathbb{N}\\ i\neq j}} X_{ijt} + ct \cdot \sum_{\substack{j\in\mathbb{N}\\ i\neq j}} d_{ij} \cdot X_{ijt} = 0$$

for all $j \in \mathbb{N}$, $i \neq n$, $t \in T$, where: cw is the amount of energy consumed by a node during activation for data transmission or reception; ct is the constant rate of energy consumption (power) during data transmission or reception;

$$X_{ij} \in \{0,1\}$$

for all $i, j \in \mathbb{N}$;

$$E_{it} \geq 0$$

for all $i \in \mathbb{N}$, $t \in T$.

Data transmission reliability in wireless sensor networks. As criteria for edge connectivity, we can consider the reliability of data transmission, which is expressed by the ratio of the number of lost and received packets, and the useful bandwidth for operating network elements.

When transmitting information between WSNs nodes to the base station, some of them act as transit nodes.

Each of the WSNs transit nodes contains a buffer for storing a limited amount of received data to be transmitted to the next node of the route.

The route as a whole is a multi-phase queuing system formed by a sequence of models of individual sections.

The probability of data packet loss during transmission between WSNs nodes can be defined as [29]

$$p = 1 - \prod_{i=1}^{w}(1 - p_i).$$

In this case, p_i can be defined as

$$p_i = \frac{1-p}{1-p^{\frac{2}{C_a^2+C_s^2}\cdot n_b+1}} \cdot p^{\frac{2}{C_a^2+C_s^2}\cdot n_b},$$

where C_a^2 snd C_s^2 are the quadratic coefficients of variation of the distributions of the input data flow and the service time for the i-th node; n_b this is the buffer size; p is the load of the i-th node.

The delivery route of data packets in a WSNs from the data source S to the base station D may have several transmission routes w formed by individual network nodes.

The optimization problem for data transmission with redundancy is formulated as follows. Let there be N independent routes, each of which is described by vectors (p_i, E_i, T_i), along which a message consisting of k packets needs to be sent. In this case, the transmission error $P_e(k, N)$ must not exceed the specified value p. To do this, you need to find the number of packets that will be transmitted along each route, that is, find such a set $(n_1, \ldots, n_N)$, $(n_i \in N)$, for which the following constraints will be satisfied:

1. Number of data transmission errors

$$P_e(k, N) = P(n_1, n_2, \ldots, n_N) \le p,$$

where the value of the function P depends on the selected data transmission algorithm.

2. Total energy consumption during data transmission

$$E(n_1, n_2, \ldots, n_N) = \sum_{i=1}^{N} E_i \cdot n_i \to \min{}_i.$$

3. Total message transfer time

$$T(n_1, n_2, \ldots, n_N) = \max_{i=1\ldots N}\{T_i + r \cdot n_i\} \to \min .$$

The probabilistic criterion states that the connectivity probability of each pair of vertices must be at least a given value to ensure the functional stability property of the WSNs.

Conclusions

The results of the study make it possible to draw key conclusions regarding the topological aspects of constructing functionally robust wireless sensor networks (WSNs), addressing both current challenges and potential solutions.

It was found that traditional hierarchical WSNs – particularly those based on tree topologies-exhibit a low degree of functional robustness. This limitation is due to a restricted number of alternative routing paths, low vertex and edge connectivity, and a reduced probability of maintaining connectivity between structural elements under destabilizing conditions. Such networks are unable to operate effectively if more than two nodes or three communication channels fail.

The study underscores the critical importance of topological design in ensuring WSN resilience. Although systems such as the examined Advantech solution demonstrate partial self-organization and autonomous operation during failures, their underlying topology constrains overall system reliability. To develop truly resilient WSNs, the synthesis of network structures must incorporate resilience-related indicators and criteria from the design phase. This approach lays the foundation for uninterrupted operation under both internal and external threats.

The findings suggest that future research should focus on designing and analyzing modified WSN topologies, particularly for use in critical infrastructure.

This includes increasing vertex and edge connectivity, expanding the number of redundant communication paths, and implementing efficient mechanisms for minimizing data transmission collisions. These strategies will contribute to the creation of more reliable and fault-tolerant systems for monitoring and control.

The results of this work have practical relevance for improving the efficiency and reliability of WSNs deployed in critical domains such as infrastructure automation, security and defense systems, and the manufacturing sector. Topology optimization can help reduce the risk of data loss, ensure process continuity, and minimize resource expenditure for network maintenance.

By implementing these strategies, wireless sensor networks can attain enhanced functional stability, making them well-suited for deployment in critical infrastructure environments. The proposed topological enhancements, energy-efficient protocols, and resilience mechanisms ensure that such networks can maintain operational integrity even under conditions of partial failure, electromagnetic interference, or cyber threats. As a result, the overall reliability, safety, and efficiency of critical infrastructure operations can be significantly improved.

Acknowledgements

This study has been partially supported by Ministry of Education and Science of Ukraine: R&D Projects No 25БП064-01 and No. 24БФ038-01 at Taras Shevchenko National University of Kyiv.

References

1. Barabash, O., Sobchuk, V., Sobchuk, A., Musienko, A. and Laptiev, O. (2025), "Algorithms for Synthesis of Functionally Stable Wireless Sensor Network", Advanced Information Systems, vol. 9, no. 1, pp. 70–79, doi: https://doi.org/10.20998/2522-9052.2025.1.08
2. Dovgiy, S., Kopiika, O. and Kozlov, O. (2021), "Architectures for the Information Systems, Network Resources and Network Services", *CEUR Workshop Proceedings*, vol. 3187, Cybersecurity Providing in Information and Telecommunication Systems II, CPITS-II-1, pp. 293–301, doi: https://ceur-ws.org/Vol-3187
3. Kuchuk, N., Mohammed, A.S., Shyshatskyi, A. and Nalapko, O. (2019), "The Method of Improving the Efficiency of Routes Selection in Networks of Connection with the Possibility of Self-Organization", *International Journal of Advanced Trends in Computer Science and Engineering*, 2019, vol. 8,. no. 1.2, pp. 1–6, doi: https://doi.org/10.30534/ijatcse/2019/0181.22019
4. Sushchanskii, V.I. and Bezushchak, O.E. (1991), "l-Wreath products and isometries of generalized Baire metrics", *Ukr Math J*, vol. 43, pp. 964–971, doi: https://doi.org/10.1007/BF01058702
5. Kuchuk, H., Mozhaiev, O., Kuchuk, N., Tiulieniev, S., Mozhaiev, M., Gnusov, Y., Tsuranov, M., Bykova, T., Klivets, S., and Kuleshov, A. (2024), "Devising a method for the virtual clustering of the Internet of Things edge environment", *Eastern-European Journal of Enterprise Technologies*, vol. 1, no. 9 (127), pp. 60–71, doi: https://doi.org/10.15587/1729-4061.2024.298431
6. Kashkevich, S., Litvinenko, O., Shyshatskyi, A., Salnyk, S. and Velychko, V. (2024), "The Method of Self-Organization of Information Networksin the Conditions of the Complex Influenceof Destabilizing Factors", *Advanced Information Systems*, vol. 8 (3), pp. 59–71, doi: https://doi.org/10.20998/2522-9052.2024.3.07
7. Kapustyan, O., Fedorenko, J. and Temesheva, S. (2025), "Asymptotic behavior of impulsive parabolic problem with infinite-dimensional impulsive set", *Georgian Mathematical Journal*, doi: https://doi.org/10.1515/gmj-2025-2017
8. Asrorov, F., Sobchuk, V. and Kurylko, O. (2019), "Finding of bounded solutions to linear impulsive systems", Eastern-European Journal of Enterprise Technologies, vol. 6, no. 4, 2019, pp. 14–20, doi: https://doi.org/10.15587/1729-4061.2019.178635
9. Kapustyan, O., Bezushchak, D., Stanzhytskyi, O. and Korol, I. (2024), "Global Solutions and Their Limit Behavior for Parabolic Inclusions With an Unbounded Right-Hand Part", *Carpathian Math. Publ.*, vol. 16, pp. 414–426, doi: https://doi.org/10.15330/cmp.16.2.414-426
10. Barabash, O., Sobchuk, V., Musienko, A., Laptiev, O., Bohomia, V. and Kopytko, S. (2023), "System Analysis and Method of Ensuring Functional Sustainability of the Information System of a Critical Infrastructure Object", *System Analysis and Artificial Intelligence. Studies in Computational Intelligence*, vol. 1107, pp. 177–192, Springer, Cham, doi: https://doi.org/10.1007/978-3-031-37450-0_11
11. Pichkur, V., Sobchuk, V., Cherniy, D. and Ryzhov, A. (2024), "Functional Stability of Production Processes as Control Problem of Discrete Systems with Change of State Vector Dimension", *Bulletin of Taras Shevchenko National University of Kyiv. Physical and Mathematical Sciences*, vol. 1 (78), pp. 105–110, doi: https://doi.org/10.17721/1812-5409.2024/1
12. Sobchuk, V., Olimpiyeva, Y., Musienko, A. and Sobchuk, A. (2021), "Ensuring the properties of functional stability of manufacturing processes based on the application of neural networks", *CEUR Workshop Proceedings*, 2845, pp. 106–116, available at: https://ceur-ws.org/Vol-2845/Paper_11.pdf
13. Laptiev, O., Musienko, A., Nakonechnyi, V., Sobchuk, A., Gakhov, S. and Kopytko, S. (2023), "Algorithm for Recognition of Network Traffic Anomalies Based on Artificial Intelligence", *5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications*, HORA, 08-10 June 2023, doi: https://doi.org/10.1109/HORA58378.2023.10156702
14. Sobchuk, V., Pykhnivskyi, R., Barabash, O. and Korotin, S. (2024), "Sequential IDS for Zero-Trust Cyber Defence of IoT/IIoT Networks", *Advanced Information Systems*, vol. 8, no. 3, pp. 92–99, doi: https://doi.org/10.20998/2522-9052.2024.3.11
15. Cancela, H. and Urquhart, M.E. (2002), "Adapting RVR simulation techniques for residual connectedness network reliability models", *IEEE Transactions on Computers*, vol. 51, iss. 4, pp. 439–443, doi: https://doi.org/10.1109/12.995453
16. Carlier, J., Li, Yu and Lutton, J.L.(1997), "Reliability evaluation of large telecommunication networks", Discrete Applied Mathematics, vol. 76, iss. 1–3, pp. 61–80, doi: https://doi.org/10.1016/S0166-218X(96)00117-5
17. Chae Young, Lee and Hee Kwun, Cho (2001), "Multicast routing considering reliability and network load in wireless ad-hoc network", *Vehicular Tech-nology Conference*, VTC 2001 Spring., vol.3, IEEE VTS 53rd, pp. 2203–2207, doi: https://doi.org/10.1109/VETECS.2001.945087
18. Chen, Y. and Nasser, N. (2014), "Energy-balancing multipath routing protocol for wireless sensor networks", *Proceedings of the 3rd international conference on Quality of service in heterogeneous wired/wireless networks*, QShine '06, ACM, New York, USA, pp. 216–224, doi: https://doi.org/10.1145/1185373.1185401
19. Chiang, M., Hande, P., Lan, T., Wei T. C. (2008), "Power Control in Wireless Cellular Networks", *Foundations and Trends in Networking*, vol. 2, is. 4, pp. 381–533, doi: https://doi.org/10.1561/1300000009
20. (2013), *Co-existence of IEEE 802.15.4 at 2.4 GHz Application Note*, NXP Laboratories UK. 2013, available at: https://www.nxp.com/docs/en/application-note/JN-AN-1079.pdf
21. Dunkels, A. (2011), "The ContikiMAC Radio Duty Cycling Protocol", *SICS Technical Report*, ISSN 1100-3154, no 2011:13, doi: https://www.dunkels.com/adam/dunkels11contikimac.pdf
22. Dotson, W., Norwood, F. and Taylor, C. (1993), "Reliability polynomial for a ring network", *IEEE Transactions on Communications*, vol. 41, iss. 6, pp. 825–827, doi: https://doi.org/10.1109/26.231902
23. Dressler, F. (2008), "A Study of Self-Organization Mechanisms in Ad Hoc and Sensor Networks", *Computer Communications*, vol. 31, no. 13, pp. 3018–3029, doi: https://doi.org/10.1016/j.comcom.2008.02.001
24. Eiselt, H.A., Gendreau, M. and Laporte, G. (1996), "Optimal location of facilities on a network with an unreliable node or link", *Information Processing Letters*, vol. 58, iss. 2, pp. 71–74, doi: https://doi.org/10.1016/0020-0190(96)00024-5
25. Kuchuk, H., Chumachenko, I., Marchenko, N., Kuchuk, N., Lysytsia, D. (2025), "Method for calculating the number of IoT sensors in environmental monitoring systems", *Advanced Information Systems*, vol. 9, no. 3, pp. 66–32, doi: https://doi.org/10.20998/2522-9052.2025.3.08
26. Erdos, P. and Reyi, A. (1959), "On random graphs", *Publ. Math. (Debrecen)*, vol. 6, pp. 290–297, available at: https://snap.stanford.edu/class/cs224w-readings/erdos59random.pdf

27. Esau, L.R. and Williams, K.C. (1966), “On teleprocessing system design. Part 2. A method for approximating the optimal network”, IBM System Journal, vol. 5, no 3, pp. 142–147, doi: https://doi.org/10.1147/sj.53.0142
28. Karger, D.R. (1995), “A randomized fully polynomial time approximation scheme for the all terminal network reliability problem”, *SIAM Review*, vol. 43, is. 3, pp. 499–522, doi: https://doi.org/10.1137/S0036144501387141
29. Kansal, M.L., Kumar, Arun and Sharma, P.B. (1995), “Reliability analysis of water distribution systems under uncertainty”, *Reliability Engineering & System Safety*, vol. 50, iss. 1, pp. 51–59, doi: https://doi.org/10.1016/0951-8320(95)00051-3
30. Ramanathan, A. and Colbour, C.J. (1987), “Counting almost minimum cut sets with reliability applications”, *Mathematical programming: Series A*, vol. 39, no. 3, pp. 253–261, doi: https://doi.org/10.1007/BF02592076

Надійшла (received) 26.06.2025
Прийнята до друку (accepted for publication) 10.09.2025

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Барабаш Олег Володимирович – доктор технічних наук, професор, професор кафедри інженерії програмного забезпечення в енергетиці, Національний технічний університет України “КПІ імені Ігоря Сікорського”, Київ, Україна;
Oleg Barabash – Doctor of Technical Sciences, Professor, Professor of the Department of Software Engineering in Energy, National Technical University of Ukraine “Ihor Sikorskyi Kyiv Polytechnic Institute”, Kyiv, Ukraine;
e-mail: bar64@ukr.net; ORCID Author ID https://orcid.org/0000-0003-1715-0761;
Scopus Author ID https://www.scopus.com/authid/detail.uri?authorId=36724076700.

Собчук Валентин Володимирович – доктор технічних наук, професор, професор кафедри інтегральних та диференціальних рівнянь, Київський національний університет імені Тараса Шевченка, Київ Україна;
Valentyn Sobchuk – Doctor of Engineering, Professor, Professor of the Department of Integral and Differential Equations, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine;
e-mail: sobchuk@knu.ua; ORCID Author ID https://orcid.org/0000-0002-4002-8206;
Scopus Author ID https://www.scopus.com/authid/detail.uri?authorId=25123261200.

Собчук Андрій Валентинович – доктор філософії, доцент кафедри інформаційної та кібернетичної безпеки, Державний університет інформаційно-комунікаційних технологій, Київ Україна;
Andrii Sobchuk –PhD, Associate Professor of the Department of Information and Cyber Security, State University of Information and Communication Technologies, Kyiv, Ukraine;
e-mail: anri.sobchuk@gmail.com; ORCID Author ID https://orcid.org/0000-0003-3250-3799;
Scopus Author ID https://www.scopus.com/authid/detail.uri?authorId=58724606300.

Мусієнко Андрій Петрович – доктор технічних наук, доцент, професор кафедри інженерії програмного забезпечення в енергетиці, Національний технічний університет України “КПІ імені Ігоря Сікорського”, Київ, Україна;
Andrii Musienko– Doctor of Technical Sciences, Associate Professor, Professor of the Department of Software Engineering in Energy, National Technical University of Ukraine “Ihor Sikorskyi Kyiv Polytechnic Institute”, Kyiv, Ukraine;
e-mail: mysienkoandrey@gmail.com; ORCID Author ID https://orcid.org/0000-0002-1849-6716;
Scopus Author ID https://www.scopus.com/authid/detail.uri?authorId=55901154800.

Лаптєв Олександр Анатолійович – доктор технічних наук, старший науковий співробітник, доцент кафедри кібербезпеки та захисту інформації, Київський національний університет імені Тараса Шевченка, Київ, Україна;
Oleksandr Laptiev – Doctor of Technical Sciences, Senior Researcher, Associate Professor of the Department of Cyber Security and Information Protection, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine;
e-mail: olaptiev@knu.ua; ORCID Author ID https://orcid.org/0000-0002-4194-402X;
Scopus Author ID https://www.scopus.com/authid/detail.uri?authorId=57216163849.

Топологічні аспекти побудови функціонально стійких бездротових сенсорних мереж

О. В. Барабаш, В. В. Собчук, А. В. Собчук, А. П. Мусієнко, О. А. Лаптєв

Анотація. Мета дослідження: Розробка та аналіз топологічних підходів до побудови функціонально стійких бездротових сенсорних мереж для забезпечення безперебійного моніторингу та управління в умовах впливу дестабілізуючих факторів для систем критичної інфраструктури та виробничого сектору. **Об’єкт дослідження:** Процеси функціонування та управління бездротовими сенсорними мережами, а також їхня стійкість до зовнішніх та внутрішніх впливів. **Предмет дослідження**: Топологічні аспекти побудови бездротових сенсорних мереж, що впливають на їхню функціональну стійкість, включаючи самоорганізацію структури, показники зв'язності та механізми мінімізації колізій передачі даних. **Результати дослідження.** У статті розглядаються топологічні аспекти побудови функціонально стійких бездротових сенсорних мереж (WSNs) в контексті управління та моніторингу об'єктів, зокрема критичної інфраструктури та виробничого сектору. Визначаються ключові виклики, пов'язані з високими енерговитратами, часовими затримками та вразливістю до перешкод, що вимагають детального аналізу на етапі проектування. Наголошується на важливості постановки задачі синтезу та вибору критеріїв для забезпечення ефективного функціонування WSNs. Представлено аналіз існуючої системи на базі сучасних рішень, що демонструє можливості віддаленого контролю та моніторингу. Досліджено особливості та переваги таких мереж, включаючи їхню здатність до самоорганізації, енергонезалежність, наявність самодіагностики та можливість масштабування. Водночас, виявлено низький рівень функціональної стійкості існуючих ієрархічних WSN через обмежену кількість альтернативних маршрутів, низьку вершинну та реброву зв'язність, а також низьку ймовірність зв'язності елементів структури. Запропоновано напрямки подальших досліджень, що включають порівняльний аналіз топологій, розробку модифікованих топологій для WSNs об’єктів критичної інфраструктури, аналіз їхньої стійкості, а також вивчення механізмів мінімізації колізій передачі даних та оцінку витрат на канали зв'язку. Результати роботи сприятимуть підвищенню надійності та ефективності бездротових сенсорних мереж у складних експлуатаційних умовах.

Ключові слова: топологія мережі; функціональна стійкість; бездротова мережа; сенсорна мережа; синтез структури.