IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 21 August 2024, accepted 1 September 2024, date of publication 4 September 2024,
date of current version 16 September 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3454367

RESEARCH ARTICLE

Toward Reliability of Long Wireless Sensor Networks

VLADIMIR V. SHAKHOV[1], (Member, IEEE), DENIS A. MIGOV[2], HONGLONG CHEN[3], (Senior Member, IEEE), POLINA V. MISHCHENKO[4], AND INSOO KOO[1], (Member, IEEE)

[1]Department of Electrical, Electronic and Computer Engineering, University of Ulsan, Ulsan 44610, South Korea
[2]Department of Economic Informatics, Novosibirsk State Technical University, 630087 Novosibirsk, Russia
[3]College of Control Science and Engineering, China University of Petroleum (East China), Qingdao 266580, China
[4]Department of Computer Engineering, Novosibirsk State Technical University, 630087 Novosibirsk, Russia

Corresponding author: Vladimir V. Shakhov (shakhov@ulsan.ac.kr)

This work was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education under Grant RS-2023-00250720.

ABSTRACT Wireless sensor networks have become pervasive in various applications, including environmental monitoring, smart cities, precision agriculture, and healthcare. In particular, linear wireless sensor networks that span considerable distances are increasingly deployed for applications such as pipeline monitoring and transportation systems. However, ensuring the reliability of long wireless sensor networks poses significant challenges due to the unique characteristics of the network topology and the constraints imposed by the resource-constrained sensor nodes. There is a notable lack of methods for the analysis and optimization of the reliability of large-scale sensor networks, and in this paper, we partially fill this gap. We propose a method for assessing the tradeoff between redundancy of forward error correction and reliable packet delivery. We also consider approaches to improve the reliability of linear sensor networks based on increasing topology connectivity and provide a corresponding method for the exact calculation of the all-terminal reliability. Numerical experiments demonstrate the relevance and effectiveness of our results. This research contributes to a deeper understanding of the underlying principles governing the reliability of long wireless sensor networks and provides valuable insights for the design, optimization, and management of such networks in real-world applications.

INDEX TERMS Wireless sensor networks, Internet of Things, monitoring system, fault tolerance, system reliability, random graph, all-terminal reliability.

I. INTRODUCTION

Currently, corporations and governments around the world are making serious efforts to research, develop, and patent technologies based on wireless sensor networks (WSNs) for monitoring long critical infrastructure [1], [2], [3], [4]. For example, research on the use of WSNs for pipeline monitoring has been carried out as part of a joint re-search project between Stanford University, Southern California University, and Chevron Corporation [5]. The Pipeline Monitoring Solutions Competition was hosted by an agency of the U.S. federal government (the Bureau of Reclamation) on a crowdsourcing platform. Even for a particular problem such as monitoring water pipes to detect leaks, the market for solutions reaches several billion US dollars and is growing at 5.8% per year, according to an analytical report from GlobeNewswire. WSNs are able to carry out continuous monitoring, detect various faults in real time, and deliver the necessary data to the decision-making center. Monitoring systems for vital infrastructure based on WSNs are one of the most in-demand IoT technologies. However, it is necessary to ensure the reliability of the WSNs.

It should be noted that IT professionals make reasonable claims about the unreliability of IoT technologies, and they doubt the ultimate benefit to society from the introduction of developments whose reliability is not guaranteed.

The associate editor coordinating the review of this manuscript and approving it for publication was Hongwei Du.

This is especially true for the modernization of life-support infrastructure. It is noted that companies specializing in IoT technologies strive to occupy as much of the market as possible as quickly as possible and give priority to the early release of products without paying due attention to issues regarding its reliability. The issue of reliability is particularly acute in large-scale WSNs used to monitor long objects, such as pipelines. Most sensor nodes are geographically distant from the base station and are usually equipped with self-contained low-cost batteries, which have a small capacity. This means that there is a limitation on the use of traditional network reliability protocols.

Moreover, Linear Wireless Sensor Networks (LWSNs) are commonly used to monitor the condition of long linear type infrastructures, such as oil/gas/water pipe-lines, railway/metro, highway, and tourism/heritage sites [6]. The topology of an LWSN is a simple chain graph. A packet sent by a sensor is retransmitted by all nodes between this sensor and the sink. Here, it should also be noted that wireless links are inherently unreliable. If even one channel fails, the network splits into two disconnected segments and data from all sensors of one of the segments is lost. The methods proposed to improve the reliability of LWSNs are based on improving the link reliability or modifying the network topology in order to increase its connectivity. However, even in the most recent works, the analysis of such methods is carried out only for small sized LWSNs [7]. There is an acute lack of efficient methods for analyzing the reliability of long LWSNs, and in this paper, we partially fill this gap.

Thus, the major contributions of this work are summarized as follows. We consider optimization problems for forward error correction schemes in long-distance networks (LWSNs). For a number of scenarios we obtain solutions in closed form. Furthermore, we propose an exact and fast method for calculating the all-terminal reliability, taking into account the nuances of LWSN modification. Finally, we conduct rigorous numerical experiments to demonstrate the significant superiority of the proposed method in terms of computational time.

The reminder of the paper is organized as follows. Section II provides a brief overview of the research background. Section III presents mathematical models that formalize the problem of optimizing the reliability of linear wireless sensor networks and discusses approaches to obtaining a solution. In Section IV, we consider the more general case of elongated wireless sensor networks. Section V concludes the paper.

II. PRELIMINARIES

The literature has extensively focused on approaches to enhance the reliability IoT applications and WSNs [7], [8], [9]. Ensuring the reliability of a network is deemed justifiable even in light of heightened energy consumption, given that the accrued advantages outweigh the associated costs of increased energy usage [8]. A prevailing consensus acknowledges the necessity of striking a balance between energy consumption and reliability. However, to effectively achieve this equilibrium, methods for evaluating reliability are indispensable, particularly in the context of multi-hop communication. Common for all types of wireless networks, is that channels are vulnerable to failures caused by interference, signal attenuation, noise and other related factors. These factors exacerbate reliability concerns, particularly in large-scale networks.

Prominent techniques for ensuring network reliability include Automatic Retry Request (ARQ) and Forward Error Correction (FEC) [9]. ARQ relies on retransmissions to fortify reliability, proving efficacious within shorter distances. However, its feasibility diminishes in expansive networks housing low-power nodes. Furthermore, the latency sensitivity of WSNs applications poses an additional challenge. Therefore, retransmissions should be avoided in these cases. On the other hand, FEC involves the integration of redundant bits prior to packet transmission, enabling the correction of corrupted messages and substantially reducing the necessity for retransmissions. Therefore, we delve into a comprehensive examination of enhancing network reliability through FEC. The paper [10] provides an extensive survey of recent research on FEC in various wireless communication domains, with a specific emphasis on low power wide area networks and IoT technologies.

There is a relationship between message length, error tolerance, and bit error probability. To demonstrate this we use the following notation. The message is encoded into a binary n-tuple: $(x_1, x_2, \ldots, x_n)$. Let the probability of an error in a single bit be equal to p_b. Therefore, the probability of no error of a single bit is $1 - p_b$. A correction code can correct up to k errors. Therefore, if N_e is the number of errors in the message, and $N_e \leq k$, then a transmitted message is successfully recovered by the receiver. The value of k represents the error correction capability and can be defined as a fraction of n [9]. The transmission of bits is assumed to be independent.

Let us introduce the following designation for the binomial cumulative distribution function:

$$B(n, k, p_b) = \sum\nolimits_{i=0}^{k} \binom{n}{i} p_b^i (1 - p_b)^{n-i}, \tag{1}$$

where binomial coefficients are present

$$\binom{n}{i} = \frac{n!}{i!\,(n-i)!} \tag{2}$$

Therefore, the probability of successful message transmission (i.e. the reliability of the link between two nodes) is as follows [9], [11], [12], [13], and [14]:

$$P\,(N_e \leq k) = B(n, k, p_b) \tag{3}$$

FEC mechanisms increase the overall data size, leading to higher energy consumption. In resource-constrained WSNs, this additional overhead may be a significant drawback. Note that FEC has a finite ability to correct errors based on the redundancy introduced. If the level of corruption exceeds the correction capacity, then the FEC may not be able to fully recover the original data, leading to potential data loss. If data packets are transmitted through many intermediate nodes to reach their destination (multi-hop scenario), the reliability situation deteriorates significantly.

It is also possible to increase network reliability through redundant nodes and links. However, the costs associated with each backup facility are typically high. Therefore, network planning must include a cost-benefit analysis that weighs the additional network reliability and the ability to add a backup element against the additional costs. Although the cost of adding a backup node is usually easy to determine, it is much more difficult to predict the additional system reliability gained by adding nodes. Random graph approaches have been proposed in the literature for estimating how much network reliability will increase by adding backup nodes and links. All-terminal reliability is the most commonly used reliability measure defined on random graphs [15], [16]. This metric quantifies the probability that a random graph remains fully connected despite independent edge failures, each occurring with a uniform probability. For the Internet of Things, where WSNs serve as the underlying architecture, the all-terminal reliability is a particularly sought-after criterion [17].

The all-terminal reliability problem is NP-hard [18]. Moreover, it is not known to belong to the NP class [19], primarily because verifying the correctness of a solution could also be computationally intensive, potentially requiring more than polynomial time. For a comprehensive exploration of the computational complexity involved in network reliability analysis, we suggest consulting the paper [20]. For very simple topologies such as trees or cycles, the reliability metric of all terminals can be calculated analytically [16]. However, in more general cases, researchers typically rely on bound estimations [19] or approximate methods [21], which prove ineffective for large-scale networks [22]. This will be further demonstrated below. Even recent works [7], [23], [24] have analyzed only small networks of a few dozen nodes, while geographically extensive networks can contain thousands of nodes. Thus, advancing technique for network reliability analysis that considers the unique properties of network topology are highly promising.

III. LINEAR TOPOLOGY RELIABILITY

In this section, we consider the typical case of traditional LWSNs, where the network topology is described by a simple chain graph. To improve the reliability of the link, a forward error correction mechanism is assumed to be used. By increasing the power of the transmitted signal, it is possible to increase the probability of successfully transmitting one bit, $1 - p_b$. By increasing the message size, we can increase the efficiency of the error-correcting code. This improves the reliability of the channel and the entire network as a whole. However, this also increases the energy consumption and other overhead costs.

Thus, to find the optimal message size, we need to solve the optimization problem as follows:

$$min_n \, C(n) \tag{4}$$

subject to

$$R(p_b, n) \geq \alpha \tag{5}$$

where

- C is a function describing network costs;
- R is a function describing a system reliability;
- α is the required level of reliability.

It is reasonable to assume that $C(n)$ and $R(n)$ are strictly monotonically increasing functions of n. This implies that as n increases, the values of $C(n)$ and $R(n)$ consistently increase. Hence, the optimal message size is as follows:

$$n^* = \left\lceil R^{-1}(p_b, \alpha) \right\rceil \tag{6}$$

where R^{-1} is the inverse function to R. Taking into account the integer nature of n, we obtain

$$n^* = min\{n \in \mathbb{N} : R(p_b, n) \geq \alpha\} \tag{7}$$

Therefore, we obtain the general solution to the optimization problem (4) and (5), and the optimal system cost is $C(n^*)$. In the problem under consideration, the optimal solution depends solely on the constraint defined by the reliability function and not on the specific form of the cost function, provided that the cost function is monotonically increasing. Consequently, the optimization problem is reduced to the computation of the reliability function. For a fixed n, a similar approach can be examined to determine the minimum possible error in the transmission of a single bit. Optimizing the objective function across multiple variables necessitates more advanced techniques, which in turn intensify the demands on both the quality and the precision of the reliability function's calculation.

Let us note that the cost function can be interpreted in terms of energy consumption. For example, in the case of a linear energy consumption function we obtain $C\,(n) = nE_{1b}$, where E_{1b} represents the energy expended for the transmission, processing, and receiving one bit [9].

Likewise, we can consider the problem of maximizing reliability for a given budget constraint, c_0. In this case, we obtain the following solution:

$$n^* = max\,\{n \in \mathbb{N} : C\,(n) \leq c_0\} \tag{8}$$

Although the optimal solution is also determined by the constraint, in order to assess the adequacy of the allocated budget, it is necessary to calculate the reliability function $R(p_b, n^*)$.

Given the scarcity of wireless sensor networks resources, it is desirable to avoid repeated messages and redundant service packets. Since the network topology is a simple chain, the reliability function, R, can be obtained explicitly. The minimum probability of delivering a correct message from any sensor to the sink can be used as an indicator of the system's reliability. Let h be the distance between the sensor and the sink in the term of hops, i.e. h is the count of transmissions occurring between a source and a destination. If the message will be corrected in each intermedia node then the reliability function takes the following form:

$$R(h) = B^{h}(n, k, p_b) \tag{9}$$

In the case of heterogeneous error probability, the formula (9) is modified as follows:

$$R\left(h\right) = \prod\nolimits_{i=1}^{h} B\left(n, k, p_b(i)\right) \tag{10}$$

where $p_b(i)$, $i\epsilon[1, h]$ is the 1-bit error probability in the i-th link from the sensor to the sink.

In multi-hop transmission scenarios, the probability of data loss significantly rises, when corrections are made only at the end node. In this case, the probability of successful transmission equals

$$P\left(N_e \leq k\right) = B\left(n, k, q(h)\right) \tag{11}$$

where $q(h)$ is the following function:

$$q\left(h\right) = 1 - \left(1 - p_b\right)^{h} \tag{12}$$

and in the case of heterogeneous error probability:

$$q\left(h\right) = 1 - \prod\nolimits_{i=1}^{h} \left(1 - p_b\left(i\right)\right) \tag{13}$$

Obviously, the probability of error, characterized by the $q\left(h\right)$ function, is growing rapidly, and the reliability of the network becomes unsatisfactory. A hybrid approach can be used, restoring the message on each j-th intermediate node. Suppose that the sensor is located at a distance h from the sink. Let $h = aj + l$, where a and l are integers, and l is the remainder of dividing h by j. Therefore, the probability is to restore the message on the sink is as follows:

$$P\left(N_e \leq k\right) = \left(B\left(n, k, q(j)\right)\right)^{a} B\left(n, k, q(l)\right) \tag{14}$$

The hybrid approach can be used for medium-distance transmissions, but is not suitable for long-distance networks. In the case of a heterogeneous bit error rate, an analogous formula can be readily derived. However, for performance analysis, researchers typically assume a consistent p_b value. For instance, in the reliability analysis of multi-hop transmissions, the worst-case bit error rate is employed [13], or the typical values for channel availability or failure are used [25], [26], [27]. In applications of long WSNs, such as pipeline monitoring or underwater object tracking, even geographically dispersed sensors are often treated as statistically homogeneous [28], [29], [30]. Moreover, the assumption of statistical similarity among network nodes is a common practice in wireless communications and IoT applications. For example, in the performance analysis of Slotted ALOHA-based MAC protocols for IoT, it is assumed that each sensor has an equal probability of accessing the channel within a specific time slot [31], [32]. Thus, for the purposes of performance analysis, we assume statistical homogeneity among nodes and links. However, it is important to note that the proposed methods are also applicable in the heterogeneous case.

The reliability of message transmission can be increased by using independent routes. If the sensor is between two sinks, at a distance of h_1 from one sink and h_2 from the other sink, and the message is sent to both sinks, then the reliability function becomes

$$R\left(h_1, h_2\right) = R\left(h_1\right) + R\left(h_2\right) - R\left(h_1\right) R\left(h_2\right) \tag{15}$$

The formula can be readily generalized to star topologies as well as other tree topologies. The reliability function allows for the effective optimization of system parameters, thereby enhancing overall system performance and efficiency.

In the aforementioned cases, the network topology is represented by simple chains. Consequently, the calculation of reliability is unimpeded by topological issues, allowing us to accurately determine both the exact value of network reliability and the solutions to inverse problems. These results enable us to provide a clear example highlighting the complexities associated with approximate calculations of network reliability. Let the system parameters be as follows: $\alpha = 0.99$,$p_b = 0.05$, $h = 500$, $k = n/2$, and n will undergo examination with a value of 32. Assume an approximate approach is used instead of formula (9), leading to a 1% underestimation of system reliability. Consequently, if they obtained reliability level is acceptable, messages of size $n = 32$ are used, although $n = 8$ suffices. This results in a fourfold increase in energy consumption. Thus, even advanced approximate methods for calculating system reliability may fail to optimize network parameters. As network size increases, this issue becomes more pronounced, highlighting the need for reliability computing algorithms that are both efficient and precise.

IV. LONGITUDINAL GRAPHS

In this section, we consider the more general case of graphs representing a topology of long-distance wireless sensor networks. An analytical expression for the reliability of a random graph can be easily obtained if a graph can be represented by serial–parallel union of graphs with known reliability polynomials. However, by modifying LWSNs to increase connectivity, we obtain topologies for which a reliability calculation is a challenge. To the best of our knowledge, such computations have exclusively been performed for small-sized systems. We use the special properties of modified LWSNs and develop an efficient and accurate method for calculating the reliability of large networks.

A. NOTATIONS

Let us assume that a topology of a wireless sensor network is modeled by an undirected probabilistic graph $G = (V, E)$. Here V is a set of vertices. These vertices represent the sensor nodes in the network. E is a set of edges (links). Each edge connects two vertices and represents the wireless channel between two adjacent nodes. Each link $e \in E$ works properly with an associated probability p_e. We consider a typical case, when sensor nodes are absolutely reliable and wireless channels are affected by random failures due to noise, signal shielding, weather conditions, and other factors. The reliability of graph G is the probability of connectivity of G, i.e., we focus on all-terminal reliability.

The value of p_e can be determined through the application of formula (9) or by employing other approaches, such as alternative mathematical models [33], experimental procedures, expert interviews, and so on.

Let us introduce a formal definition of longitudinal graphs that have been used to model a topology of WSNs. Let $G_1, G_2 \ldots, G_k$ $(k > 1)$ be a sequence of biconnected graphs with the properties as follows:

1) Graphs G_i and G_{i+1} have exactly two common vertices x_i, y_i and do not have common edges, $1 \leq i \leq k$.

2) If $|i-j| > 1$, then G_i and G_j have no common elements.

The graph

$$G = \bigcup\nolimits_{i=1}^{k} G_i \tag{16}$$

This $G = \bigcup_{i=1}^{k} G_i$ is then called a *longitudinal graph* (Fig. 1). Subgraphs G_i $(1 \leq i \leq k$) are the components of the longitudinal graph G. This graph is a connected graph. Therefore, each pair of vertices $\{x_i, y_i | 1 \leq i \leq k-1\}$ is a vertex cut in G.

In this paper, we define *longitudinal cut* in G as set

$$\bigcup\nolimits_{i=1}^{k-1} \{x_i, y_i\} \tag{17}$$

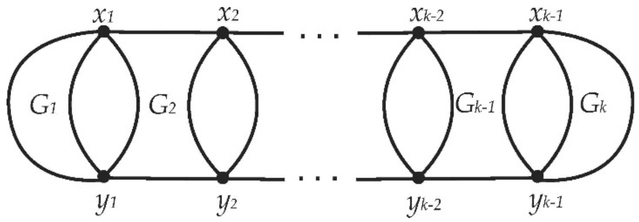


FIGURE 1. Longitudinal graph.

A component of longitudinal cut, x_i, y_i is defined as a *cross-cut* of G. A longitudinal cut is maximal if no 2-vertex cut of G can be added to it so that it remains longitudinal. Any two cross-cuts x_i, y_i and x_j, y_j are *adjacent* if $|i-j| = 1$.

B. PRACTICE EXAMPLE

In practical scenarios, a longitude graph emerges when the LWSN topology is modified to improve network connectivity with auxiliary nodes or networks, extend the transmission range of sensor data, or use of mobile sinks [34], [35]. Next, the WSN topology is naturally described by a longitude graph in environments where sensors are distributed along a quasi-linear path. Practically important cases include border surveillance, road and railway monitoring, vehicle-to-everything (V2X) systems, and bridge or tunnel health monitoring. Clustering and the convergence of multiple networks can also contribute to the formation of longitude graph-like topologies. In [36], the authors propose a few ways to modify LWSNs used for underwater pipeline monitoring, which led to network topologies described by longitudinal graphs.

Let us consider a case when a network contains two-vertex cuts. The corresponding graph is longitudinal. The modified LWSN topology described in [7] and [23] is longitudinal and contains many two-vertex cross cuts (Fig. 2).

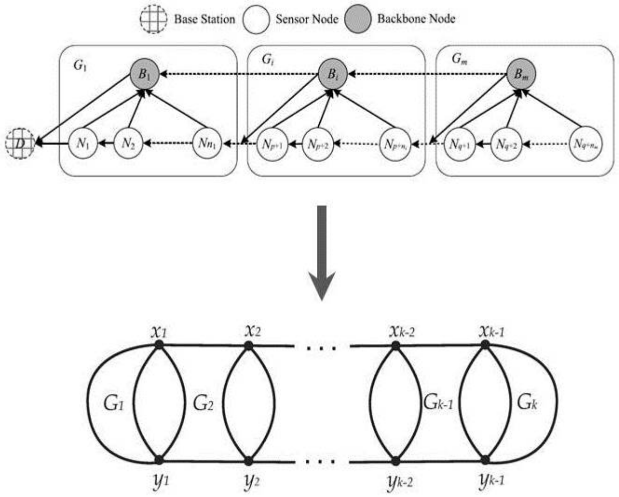


FIGURE 2. Method for modifying LWSNs to improve reliability.

Here, the sensors generate and send data to a single sink. Additional nodes (backbone nodes) have been added to improve connectivity. Without backbone nodes, packets from sensor nodes must rely on multi-hop forwarding along a linear topology to reach the sink. However, with backbone nodes and their interconnections, sensors have additional paths to access the sink, which improves system reliability by improving the network topology connectivity. The components of the corresponding longitudinal graph are subgraphs G_i. The cross-cuts of the longitudinal graph are sets formed by a backbone node and sensors of corresponding G_i.

C. DECOMPOSITION TECHNIQUE

Currently, a number of methods are known for accurate and approximate calculation of network reliability indicators. Taking into account the problem of all-terminal reliability, the most popular approach is the factoring method, which is also called the branching method or the Moore–Shannon method [33], [37]. The method is based on replacing the initial problem with two auxiliary subtasks with a smaller number of random elements. To do this, an arbitrary unreliable edge is selected and the total probability formula is applied to it. Thus, we obtain two new graphs. In one of them, the edge becomes absolutely reliable, i.e., we can contract an edge with vertices incident to it into one vertex. In another graph, an edge has been removed. A similar procedure (factorization) is applied to the resulting graphs. Therefore,

$$R(G) = p_e R\left(G_e^*\right) + (1-p_e) R(G \backslash e) \tag{18}$$

where the graph G_e^* is obtained by contracting edge e in G_e^*, and the graph $G\backslash e$ is obtained by deleting e. We continue the recursion process until we obtain a disconnected graph (its reliability is zero) or a small graph for which the probability of being connected is already known [38]. In addition to the factoring method, other exact and approximate methods have been proposed for calculating the all-terminal reliability of a random graph. A corresponding comprehensive survey can be found in [37].

Reduction and decomposition methods are often used to speed up calculations. They can be used both at the stage of preliminary graph analysis and during the computational process. This technique makes it possible to reduce the computational time and memory used for exact algorithms as well as to improve the estimates obtained by approximate methods. There are attractive prospects for network decomposition through a vertex cut, in particular, a two-vertex cut (2-cut) [38], [39]. Let us consider a biconnected graph G, which can be divided by a 2-cut into two subgraphs G_1, G_2 (Fig. 3).

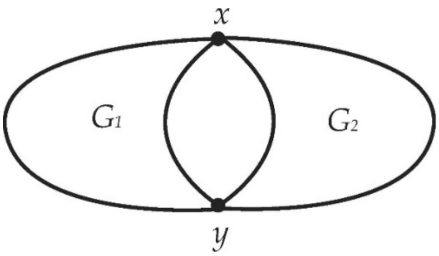


FIGURE 3. A graph G with a two-vertex cut.

For the decomposition of this graph, there is the following formula, which was first derived in [40], and was independently obtained in [41] a decade later:

$$R(G) = R(G_1)\, R\left(G_2'\right) + R(G_2)\, R\left(G_1'\right) - R(G_1)\, R(G_2) \tag{19}$$

where G_i' is a graph obtained by merging the vertices x, y in the graph G_i, $i = 1, 2$.

We use formula (18) as a core idea for creating an efficient approach to calculating the reliability of a longitudinal graph, since such a graph contains a number of 2-cuts. Moreover, the graphs resulting from the decomposition may still contain 2-cuts. At the same time, when formula (19) is used recursively, for some graph components, it is required to recalculate their reliability. These calculations can be avoided. In the next subsection, we describe a method for finding all intersections. Below, we describe a way to find all intersections. Using this result, a method for calculating the reliability of a graph without redundant recalculation is proposed.

D. METHOD

Recursive application of equation (19) for longitudinal graph G leads us to consider its components G_i and the following auxiliary graphs (Fig. 4):

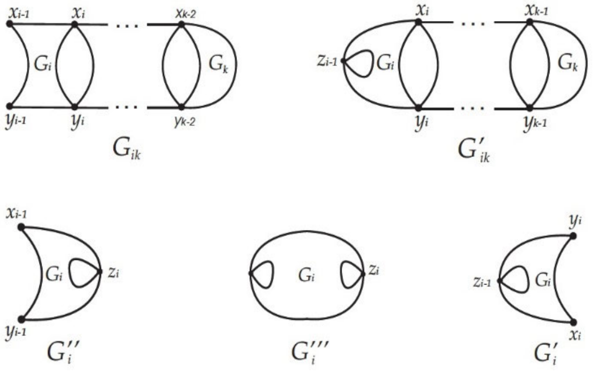


FIGURE 4. Auxiliary graphs. The vertex z_i is obtained by merging vertices x_i and y_i.

Please note that

$$G_{ik} = \bigcup\nolimits_{i \le j \le k} G_j,\ 1 \le i \le k; \tag{20}$$

$$G'_{ik} = G'_i \bigcup\nolimits_{i+1 \le j \le k} G_j,\ 1 < i \le k. \tag{21}$$

Using formula (19), we obtain the recurrent equations as follows:

$$R\left(G_{ik}\right) = \Re\left(G_i, G'_{i+1k}, G''_i, G_{i+1k}\right) \tag{22}$$

and

$$R\left(G'_{ik}\right) = \Re\left(G'_i, G'_{i+1k}, G'''_i, G_{i+1k}\right) \tag{23}$$

where $\mathbb{R}(X, Y, Z, W)$ is the functional defined on graphs $X, Y, Z,$ and W as follows

$$\mathbb{R}(X, Y, Z, U) = R(X)\, R(Y) + R(Z)\, R(U) - R(X)\, R(U) \tag{24}$$

According to the provided definition, $G_{1k} = G$. Thus, we provide the novel recursive algorithm for calculating the reliability $R(G)$.

Now, consider the problem of finding the maximum longitudinal cut. A natural way to solve it is a recursive search for 2-cuts in the components into which the graph is divided according to the 2-cuts already found. The main difficulty is that the set of 2-cuts obtained by this procedure remains a longitudinal cut. This difficulty is trivially solvable for the components G_1, G_k since any of their 2-cuts can be chosen to complement the already formed longitudinal cut. The only thing is to make sure that each vertex from the new 2-cut in G_1 or G_k is distinct from the nodes $\{x_1, y_1\}$ or $\{x_{k-1}, y_{k-1}\}$, respectively.

For an internal component $G_i (2 \le i \le k-1)$, none of its 2-cuts can be added to a current longitudinal cut set (17).

Let there be a cut $\{x, y\}$ in the component G_i, dividing it into subgraphs H_1, H_2. Obviously, the longitudinal cut remains longitudinal due to location of vertices from neighboring cross-cuts with numbers $i, i-1$ to different subgraphs: H_1, H_2. That is,

$$\bigcup\nolimits_{i=1}^{k-1} \{x_i, y_i\} \cup \{x, y \tag{25}$$

is also a longitudinal cut if nodes $\{x_{i-1}, y_{i-1}\}$ are in one subgraph H_i, and the nodes $\{x_i, y_i\}$ are in another. Thus, having a longitudinal cut C in the graph and wanting to complete it to the maximum longitudinal cut, we find an arbitrary two-vertex cut $\{x, y\}$, check where the nodes from neighboring cross-cuts are, and determine whether the cut is longitudinal.

Let us call the algorithm given by formulas (22)-(24) LongCuts. To calculate the reliability of a longitudinal graph using the LongCuts algorithm, it is necessary to calculate the reliability of $4\ (k-2)+4$ graphs: components or contracted components. Using the traditional approach (the 2-Cuts algorithm) based on formula (19) with sequential enumeration of the components of the longitudinal cut, we need to calculate the reliability of the following number of graphs:

$$2+2^{k-1}+4\sum_{i=0}^{k-3}2^i \approx 2^k \tag{26}$$

Thus, the proposed new algorithm is much faster than the traditional 2-Cuts algorithm.

V. PERFORMANCE EVALUATION

First, we consider a case of a linear topology and demonstrate the inadequacy of an approach that implements error correction solely at the terminal node, excluding intermediate nodes. Fig. 5 illustrates the reliability of LWSN for unidirectional packet transmission using the following three approaches: error correction at each node, error correction exclusively at the sink, and a hybrid method in which errors are corrected at every second node, i.e. $j = 2$ in equation (14). The FEC parameters are selected as follows: $= 10, K = 3, p_b = 0.1$. All three plots depict a decreasing function of the distance between the sensor and the sink. However, in the scenario where message correction is performed at each node, the reliability decreases at a significantly slower rate.

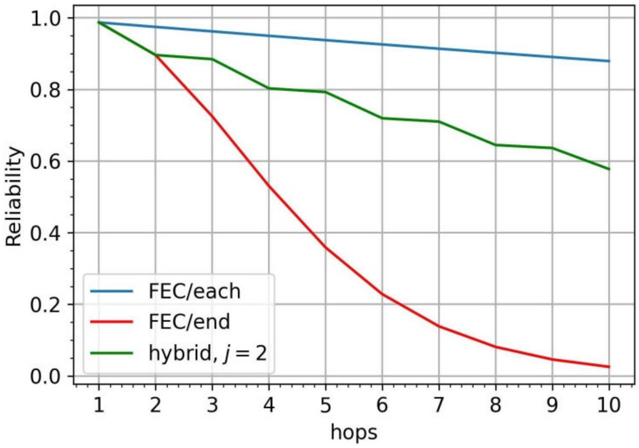


FIGURE 5. FEC performance across different approaches.

For a sensor located one hop from the sink, the results are identical across all approaches. The message is correct with a probability of about 0.99. However, for a sensor located only two hops away from the receiver, implementing message recovery at the intermediate node results in an observed 8% increase in reliability. As the number of hops increases, the disparity between the reliability indicators of the different approaches will become increasingly significant. For the other two approaches, the reliability values coincide; i.e., for $h = 2$, formula (11) and formula (14) are equivalent. With increasing values of h, the reliability of the hybrid approach demonstrates relatively modest degradation and this situation may be partially enhanced through the augmentation of n. However, this method of increasing reliability seems impractical. Indeed, in wireless networks, the ratio of energy costs for data transmission compared to computations at network nodes is typically skewed heavily towards transmission. The energy consumption for packet transmission increases exponentially with distance, while the computational tasks in WSN nodes are usually designed for low energy consumption using energy-efficient microcontrollers. Moreover, the sensor hardware can be optimized to perform the required computations and control functions with minimal energy consumption. Thus, error correction at all intermediate nodes is justified even with some additional energy consumption. Hence, for the remainder of our performance analysis, we adopt the approach wherein error correction is implemented at each node.

In scenarios where the probability of bit errors increases, a practical method for maintaining the requisite level of network reliability involves enlarging the message size. Fig.6 illustrates how network reliability varies with different values of n, demonstrating that increasing the message size can effectively counteract higher bit error rates and ensure robust communication. The remaining parameters are defined as follows: $k = [n/2]$, $h = 100$.

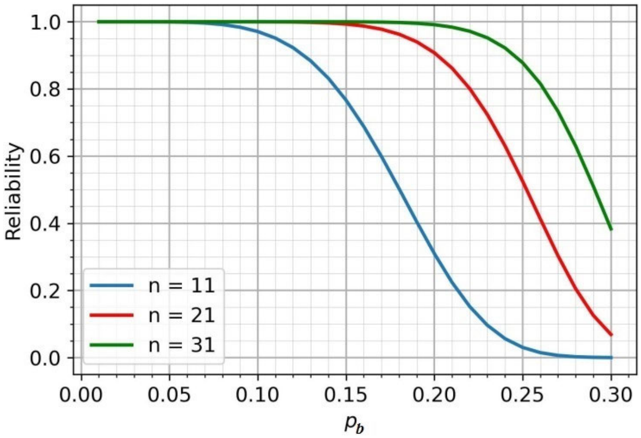


FIGURE 6. Effect of message size on reliability, $h = 100$.

Fig,7 is analogous to Fig.6, differing only in that the number of hops is set to 1000. At low values of p_b, the network reliability remains high.

In the context of long LWSNs, characterized by a relatively high bit error rate of $p_b = 0.1$ and an average message size of $n = 21$, the reliability indicators exhibit exceptional stability.

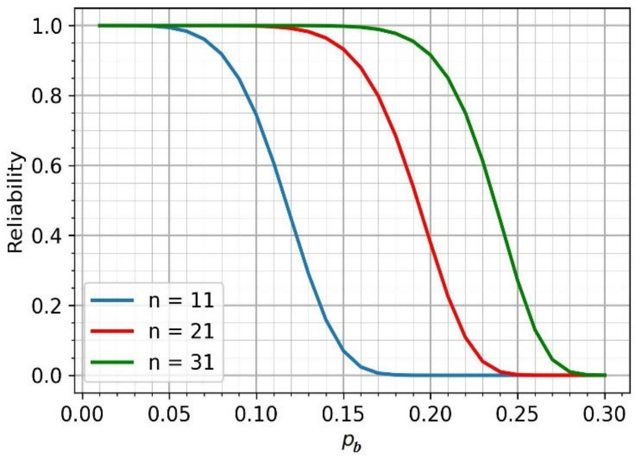


FIGURE 7. Effect of message size on reliability, $h = 1000$.

Remarkably, these indicators remain unchanged to within seven decimal places, notwithstanding a tenfold increase in the number of transitions. Thus, the FEC mechanism demonstrates its ability to maintain a high level of network reliability with a large number of transitions. However, when the parameter k decreases, the situation no longer looks so optimistic.

Fig.8 shows that the reliability of the LWSNs is much more dependent on parameter of error-correction capability, k, than on the network size. In this numerical experiment, we set $n = 21, p_b = 0.1$.

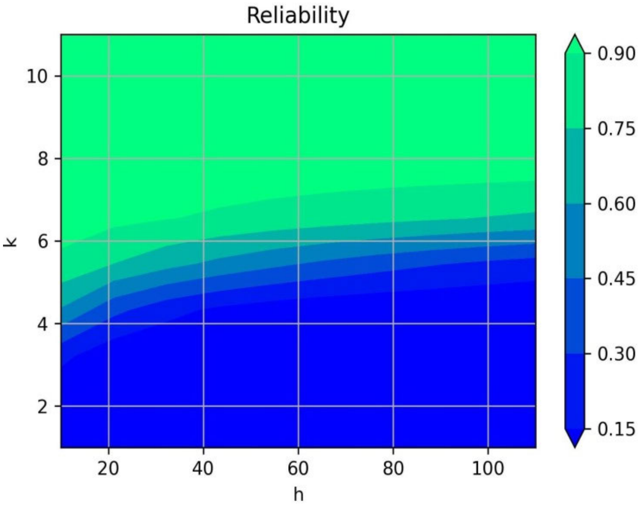


FIGURE 8. Impact of error-correction capability on LWSN reliability compared to network size.

When k values are close to 1, network reliability experiences a significant decline, persisting at notably low levels even with a small number of hops. When the parameter k is set to 4 and the number of hops h is 100, the network reliability index is observed to be at an unsatisfactory level. The situation is radically changed by doubling the value of k, resulting in a dramatic improvement in the reliability index. In contrast, reducing the number of hops by half or more does not produce a nearly comparable effect.

Assume the LWSN comprises 100 nodes utilizing a FEC scheme characterized by parameters: n = 32, p = 0.1, and k = 8. Fig.9 illustrates the delivery rate for each sensor node, indexed from 1 to 100, under two distinct network configurations. In the first configuration, the network incorporates two sinks. The sensor chain is enclosed between these sinks. Each sensor node transmits messages in two directions, targeting both sink nodes. This approach is designed to enhance reliability by providing redundant paths for message delivery; however, it results in a doubling of energy consumption. In the second configuration, the network includes only a single receiver node. Packets are transmitted in one direction towards this sole sink. This configuration is simpler and less expensive, but at the same time sacrifices reliability.

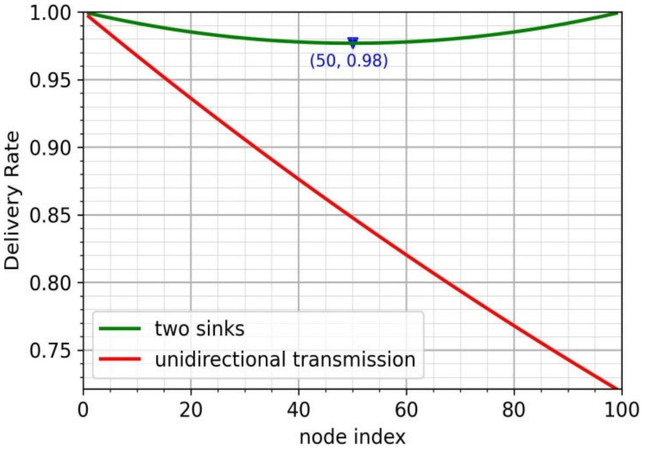


FIGURE 9. Comparison of network reliability in LWSNs with one and two sinks.

As can be seen from Fig.9, the reliability of LWSNs with two sink nodes exhibits a noticeable trend, reaching its minimum value at the midpoint of the network, specifically at the 50th sensor node. The overall reliability of the network with two sinks substantially surpasses that of a system configured with a single sink node.

Next, we consider a more general case where the network topology is described by a longitudinal graph. We present the results of a comparative numerical analysis of our proposed algorithm with two other known algorithms that have the best performance. One of these algorithms is the already mentioned recursive 2-cuts. The remaining algorithm does not use any decomposition based on vertex cut and is based on the factoring method (*Factoring* algorithm) reinforced by a serial-parallel transformation at each step, where a recursive process is performed until a 5-vertex graph with a known reliability polynomial is obtained [21]. To the best of our knowledge, other algorithms for solving a similar problem, even those recently published, have a significantly lower performance. For example, in a paper [42], calculating the reliability of a graph with 15 vertices and 30 edges takes about 13 hours.

Here, decomposition-based testing methods also use the factoring procedure when necessary. Finding the maximum longitudinal cut using the procedure described above requires enumeration of all pairs of nodes along with checking the connectivity of the graph obtained by removing each pair of nodes, i.e., $O(MN^2)$ operations.

For experiments, we have taken longitudinal graphs obtained by the recursive procedure of joining to an already formed graph of the 4-node complete graph K_4 under the assumption that two nodes of these graphs coincide. The longitudinal graph after $k-1$ has iterations we denote as K_4^k (Fig. 5).

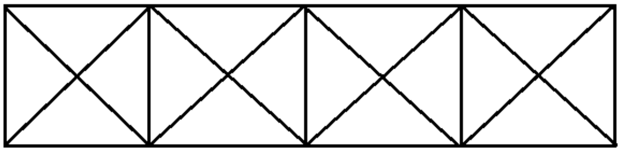


FIGURE 10. Example: graph K_4^5.

Table 1 shows the execution time of algorithms for calculating the reliability for graphs $K_4^j, j \in \{20, 25, 100\}$. The smallest graph, K_4^{20}, contains 40 nodes and 96 edges. For testing, we use 4-core CPU (2.4 GHz). The reliability of each edge equals 0.9. The graph reliability values obtained using the tested algorithms coincided with an accuracy of up to six decimal places. The mentioned values are also shown in Table 1.

TABLE 1. Units for magnetic properties.

Graph	FACTORING	2-CUTS	LONGCUTS	Reliability
K_4^{20}	4.3 s	<1 s	<1 s	0.993445
K_4^{25}	2 m 7s	<1 s	<1 s	0.992753
K_4^{100}	>24 h	2 s	<1 s	0.982438

The experiments clearly demonstrate the limitations of all-terminal reliability algorithms based on factorization. The reliability calculation time for real-size networks becomes unacceptably long. In the same situation, the decomposition approach also makes such a calculation quite fast, while the use of longitudinal cuts additionally speeds up the calculation.

VI. CONCLUSION

In this article, we consider the main approaches to improve LWSN reliability, such as error correction mechanisms in received packets and topology connectivity enhancement. To analyze and optimize these approaches, we have developed mathematical tools. The problem of calculating the probability of connectivity of linear wireless sensor networks with unreliable communication channels has been considered. We analyzed the influence of the parameters of the correction codes on the reliability of message de-livery to the sink through a large number of intermediate nodes. Longer messages generally allow a higher bit error threshold and offer a better error correction capability, but they require more energy. We have obtained formulas for finding a trade-off between network reliability and message transfer overhead. Please note that specific system settings may vary depending on network characteristics, application requirements, and environmental factors. A new approach to the all-terminal reliability calculation is proposed on the basis of the formula for decomposing a network in a two-vertex cut. For networks of an extensional spatial structure with many such cuts, arranged in series, we describe a method for identifying such cuts and a method for their subsequent traversal. As a result, it becomes possible to calculate the reliability of such a network with a single calculation of the reliability of its components as well as of components merged by the cutting nodes. We focus on exact algorithms since approximate methods can lead to an inadequate choice of system parameters. A corresponding numerical example is given. In the general case, the calculation of the all-terminal reliability is an NP hard problem. However, we use the properties of longitudinal graphs and find an algorithm of polynomial complexity in practically important cases. Numerical experiments show that this approach significantly speeds up the calculation of the reliability of a longitudinal graph and significantly outperforms all known similar algorithms.

REFERENCES

[1] A. Sabata and S. Brossia, "Remote monitoring of pipeline using wireless sensor network," U.S. Patent 7 526 994, May 5, 2009.

[2] Y. Deng, Z. Zhou, Z. Zhao, Y. Luo, X. Yi, J. Li, G. Hui, Y. Gao, and D. Shi, "Simulation study on ASCMP protocol in utility tunnel WSN," *IEEE Access*, vol. 7, pp. 168141–168150, 2019.

[3] A. M. Rahmani, S. Ali, M. H. Malik, E. Yousefpoor, M. S. Yousefpoor, A. Mousavi, F. Khan, and M. Hosseinzadeh, "An energy-aware and Q-learning-based area coverage for oil pipeline monitoring systems using sensors and Internet of Things," *Sci. Rep.*, vol. 12, no. 1, p. 9638, Jun. 2022.

[4] V. J. Hodge, S. O'Keefe, M. Weeks, and A. Moulds, "Wireless sensor networks for condition monitoring in the railway industry: A survey," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 3, pp. 1088–1106, Jun. 2015.

[5] S. Yoon, W. Ye, J. Heidemann, B. Littlefield, and C. Shahabi, "SWATS: Wireless sensor networks for steamflood and waterflood pipeline monitoring," *IEEE Netw.*, vol. 25, no. 1, pp. 50–56, Jan./Feb. 2011.

[6] F. Tong, L. Zheng, M. Ahmadi, M. Ni, and J. Pan, "Modeling and analyzing duty-cycling pipelined-scheduling MAC for linear sensor networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2608–2620, Apr. 2016.

[7] H.-B. Yang, "Reliability comparison between plain-based and cluster-based linear wireless sensor networks," *IEEE Sensors J.*, vol. 23, no. 6, pp. 6303–6311, Mar. 2023.

[8] A. Badi and I. Mahgoub, "ReapIoT: Reliable, energy-aware network protocol for large-scale Internet-of-Things (IoT) applications," *IEEE Internet Things J.*, vol. 8, no. 17, pp. 13582–13592, Sep. 2021.

[9] N. Tekin, H. U. Yildiz, and V. C. Gungor, "Node-level error control strategies for prolonging the lifetime of wireless sensor networks," *IEEE Sensors J.*, vol. 21, no. 13, pp. 15386–15397, Jul. 2021.

[10] M. M. Ali, S. J. Hashim, M. A. Chaudhary, G. Ferré, F. Z. Rokhani, and Z. Ahmad, "A reviewing approach to analyze the advancements of error detection and correction codes in channel coding with emphasis on LPWAN and IoT systems," *IEEE Access*, vol. 11, pp. 127077–127097, 2023.

[11] K. S. Trivedi, *Probability and Statistics With Reliability, Queuing and Computer Science Applications*, 2nd ed., New York, NY, USA: Wiley, 2016.

[12] V. Shakhov and A. Yurgenson, "Towards edge computing based monitoring for smart ports," in *Proc. 21st Int. Conf. Comput. Sci. Appl. (ICCSA)*, in Lecture Notes in Computer Science, vol. 12958, Sep. 2021, pp. 262–271.

[13] M. C. Vuran and I. F. Akyildiz, "Error control in wireless sensor networks: A cross layer analysis," *IEEE/ACM Trans. Netw.*, vol. 17, no. 4, pp. 1186–1199, Aug. 2009.

[14] C. Qiu, H. Shen, S. Soltani, K. Sapra, H. Jiang, and J. O. Hallstrom, "CEDAR: A low-latency and distributed strategy for packet recovery in wireless networks," *IEEE/ACM Trans. Netw.*, vol. 23, no. 5, pp. 1514–1527, Oct. 2015.

[15] O. Kabadurmus and A. E. Smith, "Evaluating reliability/survivability of capacitated wireless networks," *IEEE Trans. Rel.*, vol. 67, no. 1, pp. 26–40, Mar. 2018.

[16] L. Zhang, X. S. Liu, J. W. Pang, D. G. Xu, and V. C. M. Leung, "Reliability and survivability analysis of artificial cobweb network model used in the low-voltage power-line communication system," *IEEE Trans. Power Del.*, vol. 31, no. 5, pp. 1980–1988, Oct. 2016.

[17] J.-H. Park, "All-terminal reliability analysis of wireless networks of redundant radio modules," *IEEE Internet Things J.*, vol. 3, no. 2, pp. 219–230, Apr. 2016.

[18] M. O. Ball, "Complexity of network reliability computations," *Networks*, vol. 10, no. 2, pp. 153–165, Jun. 1980.

[19] P. Romero, "Universal reliability bounds for sparse networks," *IEEE Trans. Rel.*, vol. 71, no. 1, pp. 359–369, Mar. 2022.

[20] M. O. Ball, "Computational complexity of network reliability analysis: An overview," *IEEE Trans. Rel.*, vol. R-35, no. 3, pp. 230–239, Aug. 1986.

[21] J.-M. Won and F. Karray, "A greedy algorithm for faster feasibility evaluation of all-terminal-reliable networks," *IEEE Trans. Syst. Man, Cybern. B, Cybern.*, vol. 41, no. 6, pp. 1600–1611, Dec. 2011.

[22] A. Szlovencsak, I. Godor, J. Harmatos, and T. Cinkler, "Planning reliable UMTS terrestrial access networks," *IEEE Commun. Mag.*, vol. 40, no. 1, pp. 66–72, Jan. 2002.

[23] Y. Mo, L. Xing, and J. Jiang, "Modeling and analyzing linear wireless sensor networks with backbone support," *IEEE Trans. Syst. Man, Cybern., Syst.*, vol. 50, no. 10, pp. 3912–3924, Oct. 2020.

[24] F. Li and W. Liu, "An efficient algorithm for reliability evaluation of the bus network," *IEEE Access*, vol. 10, pp. 121772–121783, 2022.

[25] P. L. Shrestha, M. Hempel, H. Sharif, and H.-H. Chen, "Modeling latency and reliability of hybrid technology networking," *IEEE Sensors J.*, vol. 13, no. 10, pp. 3616–3624, Oct. 2013.

[26] Z. Zhang, F. Shao, N. Zhang, and Y. Niu, "Maximizing k-terminal network reliability in some sparse graphs," *IEEE/ACM Trans. Netw.*, vol. 29, no. 1, pp. 190–202, Feb. 2021.

[27] P. Zhu, J. Han, Y. Guo, and F. Lombardi, "Reliability and criticality analysis of communication networks by stochastic computation," *IEEE Netw.*, vol. 30, no. 6, pp. 70–76, Nov./Dec. 2016.

[28] S. Ali, A. Ashraf, S. B. Qaisar, M. K. Afridi, H. Saeed, S. Rashid, E. A. Felemban, and A. A. Sheikh, "SimpliMote: A wireless sensor network monitoring platform for oil and gas pipelines," *IEEE Syst. J.*, vol. 12, no. 1, pp. 778–789, Mar. 2018.

[29] M. Z. Hasan, F. Al-Turjman, and H. Al-Rizzo, "Analysis of cross-layer design of quality-of-service forward geographic wireless sensor network routing strategies in green Internet of Things," *IEEE Access*, vol. 6, pp. 20371–20389, 2018.

[30] C. Wang, X. Shen, H. Wang, H. Zhang, and H. Mei, "Reinforcement learning-based opportunistic routing protocol using depth information for energy-efficient underwater wireless sensor networks," *IEEE Sensors J.*, vol. 23, no. 15, pp. 17771–17783, Aug. 2023.

[31] D. Tyrovolas, A. Chrysologou, G. Chondrogiannis, S. Tegos, P.-V. Mekikis, P. Diamantoulakis, S. Ioannidis, C. Liaskos, N. Chatzidiamantis, and G. Karagiannidis, "Slotted ALOHA with code combining for IoT networks," in *Proc. IEEE Int. Medit. Conf. Commun. Netw. (MeditCom)*, Dubrovnik, Croatia, Sep. 2023, pp. 164–168.

[32] S. A. Tegos, P. D. Diamantoulakis, A. S. Lioumpas, P. G. Sarigiannidis, and G. K. Karagiannidis, "Slotted ALOHA with NOMA for the next generation IoT," *IEEE Trans. Commun.*, vol. 68, no. 10, pp. 6289–6301, Oct. 2020.

[33] V. Shakhov and I. Koo, "Graph-based technique for survivability assessment and optimization of IoT applications," *Int. J. Softw. Tools Technol. Transf.*, vol. 23, no. 1, pp. 105–114, Feb. 2021.

[34] S. N. Karam, K. Bilal, J. Shuja, L. U. Khan, M. Bilal, and M. K. Khan, "Intelligent IoT- and UAV-assisted architecture for pipeline monitoring in OGI," *IT Prof.*, vol. 26, no. 3, pp. 46–54, May 2024.

[35] I. Jawhar, N. Mohamed, J. Al-Jaroodi, and S. Zhang, "An architecture for using autonomous underwater vehicles in wireless sensor networks for underwater pipeline monitoring," *IEEE Trans. Ind. Informat.*, vol. 15, no. 3, pp. 1329–1340, Mar. 2019.

[36] N. Mohamed, I. Jawhar, J. Al-Jaroodi, and L. Zhang, "Sensor network architectures for monitoring underwater pipelines," *Sensors*, vol. 11, no. 11, pp. 10738–10764, Nov. 2011.

[37] H. Pérez-Rosés, "Sixty years of network reliability," *Math. Comput. Sci.*, vol. 12, no. 3, pp. 275–293, Sep. 2018.

[38] A. Rodionov, D. Migov, and O. Rodionova, "Improvements in the efficiency of cumulative updating of all-terminal network reliability," *IEEE Trans. Rel.*, vol. 61, no. 2, pp. 460–465, Jun. 2012.

[39] R. K. Wood, "Triconnected decomposition for computing K-terminal network reliability," *Networks*, vol. 19, no. 2, pp. 203–220, Mar. 1989.

[40] D. Migov, O. Rodionova, A. Rodionov, and H. Choo, "Network probabilistic connectivity: Using node cuts," in *Proc. Emerg. Directions Embedded Ubiquitous Comput.*, in Lecture Notes in Computer Science, vol. 4097, 2006, pp. 702–709.

[41] J. M. Burgos and F. R. Amoza, "Factorization of network reliability with perfect nodes I: Introduction and statements," *Discrete Appl. Math.*, vol. 198, pp. 82–90, Jan. 2016.

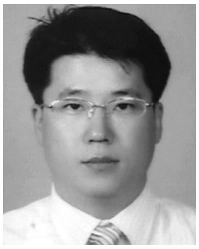
[42] S. Chakraborty, N. K. Goyal, S. Mahapatra, and S. Soh, "Minimal path-based reliability model for wireless sensor networks with multistate nodes," *IEEE Trans. Rel.*, vol. 69, no. 1, pp. 382–400, Mar. 2020.

VLADIMIR V. SHAKHOV (Member, IEEE) received the B.S. degree in mechanics and applied mathematics, the M.S. degree in mathematics, and the Ph.D. degree in computer science from Novosibirsk State University, Novosibirsk, Russia, in 1994, 1996, and 2000, respectively. He has been a Senior Researcher with the Institute of Computational Mathematics and Mathematical Geophysics, since 2000. He was a Senior Researcher with the Samsung Advanced Institute of Technology, Suwon, South Korea, and a Senior Software Developer with Intel Corporation, Novosibirsk. He visited Sungkyunkwan University, South Korea, multiple times. From 2014 to 2016, he was an Associate Professor with the Siberian State University of Telecommunications and Information Sciences. He is currently a Research Professor with the University of Ulsan, South Korea. His research interests include system performance analysis, the IoT security, and data analytics. He was the Vice Chair of the IEEE Russian Siberia Section and the Section was awarded the IEEE Gold Awards for Outstanding Section Membership Recruitment Performance.

DENIS A. MIGOV received the M.S. degree in mathematics and computer science from Novosibirsk State University, in 2003, and the Ph.D. degree in mathematics and computer science from the Institute of Computational Mathematics and Mathematical Geophysics, Siberian Branch, Russian Academy of Sciences, Novosibirsk, in 2008. He currently serves as a Senior Research Fellow at the Institute of Computational Mathematics and Mathematical Geophysics and holds the position of Associate Professor at Novosibirsk State Technical University. His research interests include graph theory, network reliability calculation, network topology optimization, wireless sensor networks, and parallel algorithms on graphs and networks.

HONGLONG CHEN (Senior Member, IEEE) received the M.E. degree in control science and engineering from Zhejiang University, Hangzhou, China, in 2008, and the Ph.D. degree in computer science from The Hong Kong Polytechnic University, Hong Kong, in 2012. He was a Postdoctoral Researcher with the School of CIDSE, Arizona State University, Tempe, AZ, USA, from 2015 to 2016. He is currently a Professor and a Ph.D. Supervisor with the College of Control Science and Engineering, China University of Petroleum (East China), Qingdao, China. He has authored or co-authored more than 100 research papers in prestigious journals and conferences, including IEEE Transactions on Information Forensics and Security, IEEE Transactions on Mobile Computing, IEEE Internet of Things Journal, IEEE Transactions on Industrial Informatics, IEEE Transactions on Wireless Communications, IEEE INFOCOM, and the International Joint Conference on Artificial Intelligence. His current research interests include the Internet of Things and cyber security. He is a Senior Member of China Computer Federation (CCF) and a member of ACM. He was the Guest Editor of IEEE Transactions on Industrial Informatics.

POLINA V. MISHCHENKO received the M.S. degree in computer science and computer engineering from Novosibirsk State Technical University, in 2012. She is currently a Senior Lecturer with the Computer Engineering Department, Novosibirsk State Technical University. Her research interests include high-performance computing technologies and information networks.



INSOO KOO (Member, IEEE) received the B.E. degree from Konkuk University, Seoul, South Korea, in 1996, and the M.S. and Ph.D. degrees from Gwangju Institute of Science and Technology (GIST), Gwangju, South Korea, in 1998 and 2002, respectively. From 2002 to 2004, he was a Research Professor with the Ultrafast Fiber-Optic Networks Research Center, GIST. He was a Visiting Scholar with the Royal Institute of Science and Technology, Sweden, for one year. In 2005, he joined the University of Ulsan, where he is currently a Full Professor. His research interests include next-generation wireless communication systems and wireless sensor networks.