Comprehensive Analysis of Efficiency and Security Challenges in Sensor Network Routing

Nadiia Dovzhenko[1,2], Oleg Barabash[1], Nataliia Ausheva[1], Yevhen Ivanichenko[2], and Sergiy Obushnyi[2]

[1] *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute,"* 37 *Peremogy* ave.*, Kyiv, 03056, Ukraine*
[2] *Borys Grinchenko Kyiv University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine*

Abstract

The use of new wireless technologies not only enhances the economic development of countries worldwide but also improves the quality of life for ordinary citizens. This improvement is particularly noticeable in the realm of wireless IoT/IIoT technologies. Sensor networks have also reached a stage of rapid development. Today, there is no doubt about the advantages of utilizing hundreds of sensors. The widespread connection of sensors allows us to address a wide range of issues, from monitoring the environment (forest fires, assessing climate shifts, soil pollution, and carbon dioxide levels) to enhancing law enforcement by strengthening protection against potential terrorist threats. It also helps improve traffic management and road congestion in urban areas, as well as healthcare and more. Simultaneously, the use of sensors addresses a series of issues related to information security. Today, data confidentiality and security are pivotal concerns in the context of IoT and sensor networks. To ensure an adequate level of protection for sensor network ecosystems, it is essential not only to analyze risks but also to influence the development and enhancement of approaches.

Keywords

Network, sensor, nodes, protection, security, attacks, functional stability, flooding, method, routing.

1. Introduction

The use of new wireless technologies not only enhances the economic development of countries worldwide but also improves the quality of life for ordinary citizens. This improvement is particularly noticeable in the realm of wireless IoT/IIoT technologies. Sensor networks have also reached a stage of rapid development [1].

Today, there is no doubt about the advantages of utilizing hundreds of sensors. The widespread connection of sensors allows us to address a wide range of issues, from monitoring the environment (forest fires, assessing climate shifts, soil pollution, and carbon dioxide levels) to enhancing law enforcement by strengthening protection against potential terrorist threats. It also helps improve traffic management and road congestion in urban areas, as well as healthcare and more [2–3].

Simultaneously, the use of sensors addresses a series of issues related to information security. Today, data confidentiality and security are pivotal concerns in the context of IoT and sensor networks. To ensure an adequate level of protection for sensor network ecosystems, it is essential not only to analyze risks but also to influence the development and enhancement of approaches [4].

CPITS-2023-II: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2023, Kyiv, Ukraine
EMAIL: nadezhdadovzhenko@gmail.com (N. Dovzhenko); bar64@ukr.net (O. Barabash); nataauscheva@gmail.com (N. Ausheva); y.ivanichenko@kubg.edu.ua (Y. Ivanichenko); s.obushnyi@kubg.edu.ua (S. Obushnyi)
ORCID: 0000-0003-4164-0066 (N. Dovzhenko); 0000-0003-1715-0761 (O. Barabash); 0000-0003-0816-2971 (N. Ausheva); 0000-0002-6408-443X (Y. Ivanichenko); 0000-0001-6936-955X (S. Obushnyi)

2. Main Part

Traditionally, components of sensor networks have been considered for implementation in high-performance radiation and nuclear threat detection systems, such as sensors for reconnaissance and surveillance systems, radio communication control systems, medical applications, seismic monitoring, and more. Sensor network nodes can monitor events in the surrounding environment, even in places where human presence is dangerous or unlikely, while also exchanging information with neighboring nodes.

Often, these nodes perform certain standard computations based on the acquired information. This has been brought about by the convergence of networks, wireless communications, and the rapid advancement of information technologies. Special attention should also be given to the hardware of sensors, the decreasing costs of processors, sensor miniaturization, and the low power requirements of radio module components. All of these processes and features have placed sensor networks on the cusp of a potential development era [5].

However, the question of safeguarding sensitive, confidential data exchanged between sensor network nodes is becoming increasingly critical.

Sensor network nodes collect and initially process data arrays. The next step is to transmit the data to control nodes, main hubs, or a server using wired or wireless connections. At this stage, the primary task for a sensor network component is to select an optimal route for transmitting processed data.

When it comes to sensors sensitive to the data they receive (e.g., streaming audio/video in UAV applications), the choice of data transmission route becomes critical in terms of network connectivity. Specific criteria need to be considered. For instance, previously chosen optimal routes may be inefficient for streaming audio/video or might become overloaded when participating in data transfer among other nodes.

Connectivity is closely related to the concepts of resilience and fault tolerance for both individual components and the entire sensor network. It refers to the network's ability to adapt to new changes, configurations, and scaling. Therefore, there is a need not only to predict the traffic transmitted between sensor network nodes but also to address routing issues. This aspect is often of interest to malicious actors as it is one of the vulnerable points [6].

For sensor networks that operate based on self-organizing algorithms, there are significant information security risks. These risks can be realized through various means, such as Denial of Service (DoS) attacks targeting the disruption of legitimate routing algorithms and information transmission.

DoS attacks pose a serious threat to sensor network components, primarily targeting the communication channel with malicious traffic. These attacks can be categorized into two types: attacks disrupting routing algorithms and attacks aimed at exhausting the resources of network nodes.

The first type of attack results in the routing protocol behaving incorrectly, failing to perform its functions, and negatively impacting neighboring nodes. This impact is challenging to assess until there are collisions or substantial data loss. It may go unnoticed until the wireless segment of the network stops responding to requests.

The second type of attack is based on a different principle. It involves gradually increasing the consumption of resources, both at individual nodes and within the entire network segment. This can also lead to a rapid increase in bandwidth and negatively affect the energy potential of the nodes.

Examples of such attacks include:

- *Hello Flood Attack*. In this attack, a node starts broadcasting broadcast requests (or any similar essential information) with a certain power level, notifying all surrounding nodes of its presence. According to the concept of a sensor network, other neighboring nodes begin to participate in relaying messages, including adding a new node that transmits a powerful signal. The connectivity algorithm triggers, and once the new node starts receiving data packets from neighboring nodes, the transmission stops. Nodes continue transmitting packets with service information, inquiring about the success of the transmission. However, the network segment essentially becomes dysfunctional.

- *Falsification, Modification, or Illegitimate Message Duplication*. The main idea is to introduce altered messages into a specific network segment by a rogue node, disrupting the routing process and eventually rendering the entire network segment inoperative.
- *Routing Loop Attack.* Routing loops are a well-known concept in networks. However, the appearance of this attack in wireless networks is problematic as it not only leads to data loss but also disconnects entire network segments. A malicious node creates a situation where the internal resources of the sensor begin to deplete, and data packets are no longer transmitted to neighboring nodes as required by the routing algorithm. Instead, they are transmitted among multiple adjacent nodes, rapidly impacting bandwidth and critically affecting the network's resilience and fault tolerance.
- *Wormhole Attack.* In this attack, a malicious node intercepts packets at any point in a network segment and redirects them to another rogue node located in a different network segment. Packet transmission occurs through several nodes, causing their gradual congestion. Additionally, the transmission process is organized bidirectionally. Therefore, all nodes participating in transmission will perceive malicious nodes as neighbors, expending their resources on illegitimate traffic, which affects the network's reliability and resilience.
- *Detour Attack*. A malicious node attempts to reroute legitimate traffic packets between legitimate nodes along a specific route, often an unoptimized path through the most unfavorable segments of the network, leading to increased packet hops and causing data loss and delays due to increased processing time. The malicious node may also add virtual nodes to the primary route, making the verified, optimal route redundant.

These attacks pose significant challenges in terms of ensuring the security and stability of sensor networks.

To detect anomalies among nodes in a sensor network that would lead to the localization of not only harmful traffic but also malicious nodes, it's essential to identify a set of indicators that receive significant attention. These indicators include packet transmission delay, overhead costs of routing algorithms, and the network's lifetime [7].

Packet Transmission Delay. The delay in packet transmission depends on time delays, the number of hops between nodes, and the actual length of the path between the sender and receiver. By significantly reducing the delay in packet transmission between nodes, the overall end-to-end delay is also reduced, decreasing the likelihood of implementing malicious nodes or traffic.

While traditional packet transmission approaches in networks choose an optimal route, possibly minimizing delay, it is worthwhile to reduce the transmission delay by sending packets to the first available node among neighbors. This improves the overall routing metric and is calculated using the formula:

$$S_{ij} = \frac{p_j}{p_i + \cdots + p_{n_i}} \tag{1}$$

where i is node, n_i is sender, ω_i is sender's frequency, ω_j is receiver node's frequency.

Essentially, after the activation of a sender node with a certain standard frequency, it has equal rights (probability) to choose a neighboring node to establish a communication session.

This ensures that the set of possible neighboring elements for connection is strictly regulated to plan routes more carefully and avoid packet wandering, reducing the performance impact due to redirection delays.

Too few alternative neighboring nodes can lead to shorter paths and an increase in redirection delays (deterministic routing), resulting in security gaps and vulnerabilities [8].

Overhead Costs of Routing Algorithms. In conventional networks, the costs associated with routing usually don't affect the network's resilience and fault tolerance, making it less of a problem. However, when calculating the number of nodes in a wireless sensor network, connectivity, and optimal route algorithms, the issue of overhead costs becomes more significant. As nodes form a certain routing structure, considerations about the energy efficiency of network components [9], the bandwidth between them [10], and the features of further amortization during scaling are projected from the design stage.

Unfortunately, it's challenging to predict all real-world conditions and negative factors in practice. Even if nodes physically do not change their location, the topology continuously changes due to variations in connection quality, connections, sensor influence, and interference.

If a specific network segment undergoes regular changes due to these characteristics, network components require constant updates of routing algorithms.

Overhead costs include memory bytes for storing received or initial data processing and defining the node's wakeup frequency. With slow route updates or disregarding these features, nodes and their nearest neighbors can eventually come under the scrutiny of malicious actors or hackers, and their routes will be compromised.

Network Lifetime. This metric is defined as the time for the complete energy consumption cycle of the first network node.

It is considered an important metric for real-time deployment and essentially depends on the battery capacity of the nodes and the average energy consumption of a node that will consume resources primarily.

To achieve this, it is beneficial to reduce the level of maximum energy consumption among all sensor network nodes by partially transitioning them to sleep mode and active mode accordingly [11].

Nodes within the receiver's range can transmit messages without any delay, thus saving energy resources.

To maintain a stable and high level of energy efficiency in wireless sensor networks, it's necessary to consider an approach in which time intervals can be avoided or replaced during continuous updates of data about neighboring nodes, as required by routing protocols [12].

For instance, to choose the best route for sending packets to nodes, an updated list of routing metrics for neighboring components is essential.

This approach is referred to as the node's working cycle and is calculated as follows:

$$OC = \frac{T}{a} \qquad (2)$$

where T is duration, a is node's activity period.

The activity period can be calculated by inverting the activity frequency c:

$$a = 1/c. \qquad (3)$$

$$OC = \delta c. \qquad (4)$$

For example, assuming a node is active for 5 ms every 200 ms (T = 5 ms, a = 200 ms, c = 5 Hz), this results in a working cycle OC = 0.025 (Fig. 1, Table 1).

Table 1

Node Operating Cycle (OC) Values under Variations in Duration from 0 to 100 ms

T	10	30	50	70	80	90	100
OC	0,05	0,15	0,25	0,35	0,4	0,45	0,5

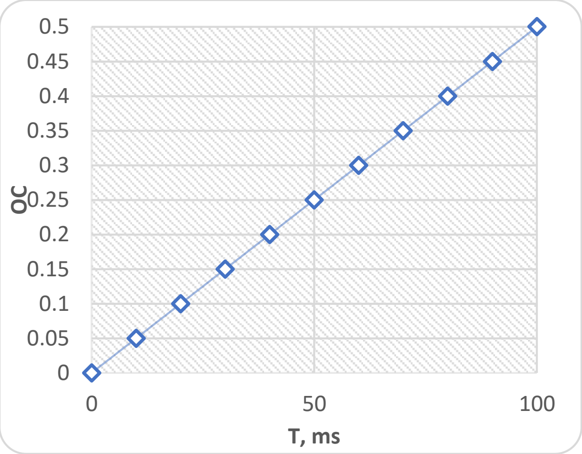

Figure 1: Node Operating Cycle (OC) Values under Variations in Duration from 0 to 100 ms

Having such a working cycle means that the node is active for 2.5% of the time.

Comparing it to a node that is active for 100 ms every second (T = 100 ms, a = 1000 ms, c = 1 Hz, OC = 0.1), the first node's lifetime is four times longer than the latter's, even though it is active five times more often (Fig. 2).

As this example demonstrates, energy efficiency is a delicate balance between a and the duration T.

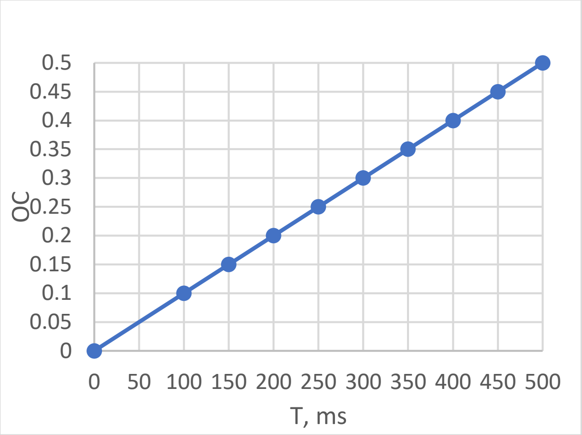

Figure 2: Node Operating Cycle (OC) Values under Variations in Duration from 0 to 500 ms

As this example demonstrates, energy efficiency is a delicate balance between a and the duration T.

Another approach that needs consideration is assessing the interaction duration between nodes. The expected value $H[K]$ of unique uniform random variables N (neighbors), given by a beta random variable with parameters $\alpha = 1$ and $\beta = N$, is defined as:

$$K \sim L\,(1, N). \tag{5}$$

$$H[K] = \frac{1}{1+N}. \tag{6}$$

Considering the wakeup period W and the number of neighbors N, the expected duration of the interaction phase can be calculated as follows:

$$H[s] = \frac{W}{1+N}. \tag{7}$$

The modeling of the amplification factor M in comparison to unicast transmission is calculated as:

$$M = \frac{H[s]}{H[K]} = \frac{W}{1+N}\frac{2}{W} = \frac{2}{1+N}. \tag{8}$$

Taking into account that the interaction time in unicast transmission $H[K]$ equals $W/2$, with the presence of 100 nodes in a network segment, the expected interaction and packet transmission time will be 50 times less than when using unicast transmission between neighboring nodes.

The results of the calculations using this approach with varying numbers of nodes ranging from 0 to 100 are shown in Fig. 3.

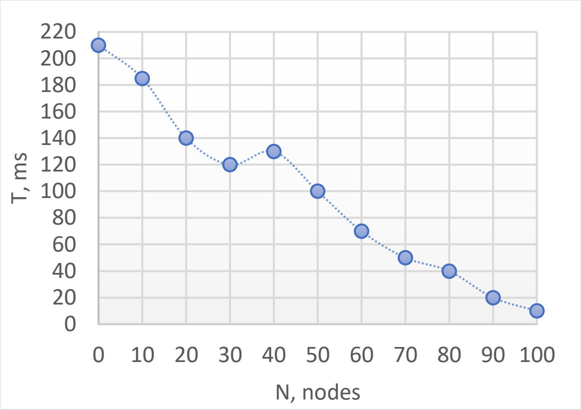

Figure 3: Results of calculations using the proposed approach with varying numbers of nodes ranging from 0 to 100 nodes

These calculations are approximate as they do not consider possible collisions, which could delay the detection of the first node.

In the event of anomalies occurring, the value of T will rapidly fluctuate, allowing not only the adjustment of data packet transmission but also the localization of negative factors or the actions of a malicious actor.

References

[1] N. Dovzhenko, et al., Method of Sensor Network Functioning under the Redistribution Condition of Requests between Nodes, in: Cybersecurity Providing in Information and Telecommunication Systems vol. 3421 (2023) 278–283.

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

[3] M. TajDini, et al., Wireless Sensors for Brain Activity—A Survey, Electronics 9(12), iss. 2092 (2020) 1–26. doi:10.3390/electronics9122092.

[4] S. Dovgiy, O. Kopiika, O. Kozlov, Architectures for the Information Systems, Network Resources and Network Services, Cybersecurity Providing in Information and Telecommunication Systems II vol.3187 (2021) 293–301.

[5] A. Bondarchuk, et al., The Research of Problems of the Information Algorithm Functioning in the Presence of Preserved Nodes in Wireless Sensor Networks, Cybersecur. Educ. Sci. Tech. 4(4) (2019) 54–61. doi: 10.28925/2663-4023.2019.4.5461.

[6] N. Dovzhenko, R. Kyrychok, Z. Brzhevska, The Construction of the Data Routing System for Wireless Sensor Nework on the Basis of Flooding Concept, Modern Inf. Secur. 4(36) (2018) 17–21. doi: 10.31673/2409-7292.2018.041216.

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

[8] P. Kasirajan, C. Larsen, S. Jagannathan, A New Data Aggregation Scheme Via Adaptive Compression for Wireless Sensor Networks, ACM Transactions on Sensor Networks (TOSN) 9(1) (2012). 1–26. doi: 10.1145/2379799.2379804.

[9] 100 V. Buriachok, V. Sokolov, P. Skladannyi, Security Rating Metrics for Distributed Wireless Systems, in: Workshop of the 8th International Conference on "Mathematics. Information Technologies. Education": Modern Machine Learning Technologies and Data Science, vol. 2386 (2019) 222–233.

[10] 101 Z. Hu, et al., Bandwidth Research of Wireless IoT Switches, in: IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (2020). doi: 10.1109/tcset49122.2020.2354922.

[11] L. Berkman, et al., The Intelligent Control System for Infocommunication Networks, Int. J. Emerg. Trends Eng. Res. 8(5) (2020) 1920–1925. doi: 10.30534/ijeter/2020/73852020.

[12] L. Globa, et al., Approach to Uniform Platform Development for the Ecology Digital Environment of Ukraine, Prog. Adv. Inf. Commun. Technol. Syst. (2022) 83–100.