Enhancing Sensor Network Efficiency Through Optimized Flooding Mechanism

Nadiia Dovzhenko[1, 2], Oleg Barabash[1], Andrii Musienko[1], Yevhen Ivanichenko[2], and Iryna Krasheninnik[3]

[1] *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", 37 Peremogy ave., Kyiv, 03056, Ukraine*

[2] *Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine*

[3] *Bogdan Khmelnitsky Melitopol State Pedagogical University, 59 Naukove Mistechko str., Zaporizhzhia, 69000, Ukraine*

Abstract

Sensor networks play a crucial role in modern technologies, especially with the widespread implementation of the Internet of Things, where they are used for collecting data from the physical world and transmitting it for analysis and further processing. Therefore, data security in sensor networks is a key aspect, as it affects confidentiality, integrity, and availability of information. Sensor networks employ various encryption and authentication methods to protect the transmitted and processed data. Additionally, the issue of securing the sensors and devices themselves from unauthorized access and attacks, such as Denial of Service, is becoming increasingly prominent. Naturally, security standards and protocols, specifically adapted for sensor networks and IoT, are being developed and implemented to minimize security risks. The development of machine learning and artificial intelligence technologies is also gaining popularity, as it enhances threat detection mechanisms and anomalies in network traffic, thereby more effectively protecting sensor networks. In the context of resource management and energy consumption, it is also important to consider security aspects, as attacks on sensor networks can lead to unjustified resource expenditure and, consequently, a reduction in the lifespan of devices and sensors.

Keywords

Network, sensor, nodes, efficiency, flooding, anomalies, IoT, network traffic, routing, protection, security

1. Introduction

Sensor networks today are one of the most promising technologies, having found widespread application in areas such as the creation of "smart" cities, industrial automation systems, environmental monitoring, healthcare, and many others [1].

The basis of their popularity lies in the use of relatively inexpensive components—sensor nodes, which are combined in large numbers into wireless networks [2, 3]. This allows for efficient data collection and exchange about various physical and environmental conditions that these sensors track and monitor.

Integration with next-generation networks, such as 5G and the Internet of Things (IoT), significantly expands the application possibilities of sensor networks, enhancing their efficiency and opening access to a wide range of services.

Advancements in computing and communication technologies have enabled the integration of sensing functions and the

CPITS-2024: Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2024, Kyiv, Ukraine
EMAIL: nadezhdadovzhenko@gmail.com (N. Dovzhenko); bar64@ukr.net (O. Barabash); mysienkoandrey@gmail.com (A. Musienko); y.ivanichenko@kubg.edu.ua (Y. Ivanichenko); irina_kr@mdpu.org.ua (I. Krasheninnik)
ORCID: 0000-0003-4164-0066 (N. Dovzhenko); 0000-0003-1715-0761 (O. Barabash); 0000-0002-1849-6716 (A. Musienko); 0000-0002-6408-443X (Y. Ivanichenko); 0000-0001-6689-3209 (I. Krasheninnik)

development of wireless communication interfaces. The use of microprocessors in miniature devices allows for the processing of large volumes of data in various environments.

Incorporating numerous nodes into sensor networks boosts their functionality but may compromise the overall network reliability, owing to a higher probability of failures in individual nodes.

Additionally, the distance limitations for wireless information transmission can restrict the network's range and efficiency in distributed applications. To mitigate the risks associated with node failures and ensure network reliability, connectivity strategies and approaches, redundancy, and routing in the network are applied. This enhances its resilience to failures, ensuring service continuity and connectivity between nodes even in the event of isolation of individual network elements [4].

Owing to the close integration between smart sensors and sensor nodes, sensor networks acquire unique characteristics that require a meticulous approach to their design and implementation.

The main advantage of such an approach is the ability to use energy efficiently and improve the quality of monitoring through data processing directly on sensor nodes with the help of intelligent algorithms.

The main criteria describing sensor networks include the following:

- The sensor network must be wireless; this minimizes environmental interference and simplifies deployment in various locations;
- The sensor network consists of thousands of sensors (network nodes) with any coverage area and performs any tasks assigned to it; scalability is critical for adapting to different applications and territory sizes;
- Sensors within the network must self-organize into a wireless network capable of transmitting arbitrary information between any two sensors in the network, with the necessary transmission speed; technologies such as mesh networks allow sensors to dynamically reorganize to optimize communication paths;
- Sensor nodes must consume a minimal amount of energy, as they operate over a significant period; the use of energy-efficient communication protocols and energy management algorithms is key to extending the life of the network;
- Sensor nodes must respond promptly, be unobtrusive, convenient to use, and low-cost. The integration of technologies such as microelectromechanical systems allows the creation of miniature, highly efficient sensor nodes at an affordable price.

Today, many sensor networks are limited in terms of coverage area and the number of tasks they can perform. They are capable of transmitting only certain types of information with limited bandwidth.

However, the continuous development of technologies and innovations allows for the expansion of sensor network capabilities, particularly through the improvement of data encoding and transmission systems, making them more flexible and efficient in various application conditions.

2. Features of Effective Resource Management

Effective resource management and security in modern sensor networks require a comprehensive approach that includes not only the development of the latest protection mechanisms and traffic management but also a focus on optimizing energy consumption and resource utilization. This is because sensor networks typically consist of a large number of devices located in diverse conditions, requiring adaptability and high efficiency in management to ensure their long-term operation.

For example, in sensor networks, there are often identical scenarios of abnormal use of signaling and bandwidth, which can lead to inefficient use of energy and network resources.

- Abnormal use of signaling. If the wireless network’s idle mode timer is set to ten seconds, establishing a session involves additional signaling and sending a single packet every 11 seconds.
- This results in sending 330 packets or about 13 KB of data during one operating period, necessitating at least 54 minutes of the mobile device’s battery life and airtime for sending 330 signaling events.

- Abnormal use of airtime. For example, when a node transmits data for five seconds, it leads to the continuous active use of network resources. In this case, approximately 720 packets or 28.8 KB are transmitted over one hour, requiring 60 minutes of battery life and only sending one signal message.
- Anomalous bandwidth usage demonstrates the significant resource requirements for downloading large files, such as videos larger than 1 GB, which necessitates at least 1.5 hours of continuous high-frequency communication sessions at a speed of 1.5 Mbps.

The mentioned scenarios confirm the need for developing and implementing effective traffic and resource management mechanisms, as well as security methods, including encryption and authentication algorithms, protection algorithms against anomaly detection from DoS attacks, and other threats [5–7].

Additionally, significant attention must be paid to the development of standards and protocols to ensure equipment compatibility, which simplifies the integration of new technologies and the scaling of existing networks.

This also includes the development of comprehensive security systems that protect data from unauthorized access and cyber-attacks, using advanced methods of encryption, authentication, and anomaly detection.

In conclusion, effective resource management and security assurance in sensor networks require an integrated approach that combines the latest data management technologies, energy optimization, cybersecurity, and artificial intelligence. Such an approach will ensure high reliability, efficiency, and security of sensor networks, adapted to complex and dynamic application conditions [8].

3. Connectivity in Sensor Networks

When designing the sensor network infrastructure, it is necessary to highlight the issue of connectivity. After all, establishing connectivity between the constituent elements of the network is crucial for several reasons.

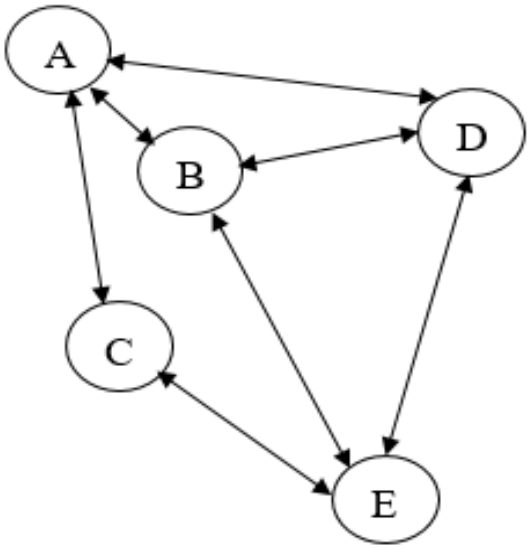

Figure 1: An example of the connectivity of nodes in a sensor network

First of all, there is efficient use of energy resources. This is because components, which often have limited energy resources, are used in sensor networks. Therefore, rational and effective connectivity can significantly minimize energy consumption by optimizing data transmission routes [9].

Second, there is less attention paid to issues of scalability. Clear and logical connectivity positively affects the incorporation of new approaches to expand the constituent components of the sensor network without significant changes to the existing infrastructure

Thirdly, it's notable that the reliability of data transmission increases with rational connectivity of network components. Connectivity between nodes facilitates reliable data transmission from sensors to the central data collection and processing node, which is especially important in critical applications such as medical, military, or security systems [10].

Fourthly, there is minimization of data loss. Reliable connectivity reduces the risk of data loss during transmission between nodes, ensuring more accurate and dependable collection and priority processing of data for further retransmission within the network.

Factors such as coverage, flexibility, mobility, and response speed of sensor network nodes are also crucial. Thus, ensuring effective connectivity is fundamental to the successful operation of sensor networks [11].

4. Optimization of the Flooding Mechanism

Flooding is a basic message propagation mechanism in sensor networks that, despite its simplicity, can be optimized to reduce redundancy and enhance efficiency.

One of the key disadvantages of flooding is a significant number of redundant messages, which can quickly exhaust the energy resources of nodes, especially in conditions of restriction or economy.

Therefore, it is advisable to optimize the flooding process using a forwarding tree, which allows for limiting the number of transmissions by selectively sending messages through a structured approach [12].

The flooding protocol in sensor networks operates by having each node, upon receiving a message, transmit it to all its neighbors, except the source node. A node only uses information about its nearest neighbors for transmission.

To improve efficiency and reduce redundancy, a "forwarding tree" structure is used to optimize message distribution by selectively transmitting authentication codes not to all neighbors, but only to selected nodes, which helps reduce the total number of transmissions.

The creation of a "forwarding tree" begins with an initiator that designates each of its neighbors as the root of a subtree of depth k.

For each such root, the initiator transmits the authentication codes required by all nodes in those subtrees. Further expansion of the tree occurs by including nodes that meet two criteria: they are k hops away from the current root and are reachable from any node at the last level in the current forwarding tree.

To illustrate the practicality of the suggested method, envision a sensor network comprising 100 nodes, with each node connected to an average of 10 immediate neighbors [13].

Employing conventional flooding for message dissemination throughout this network would necessitate each node to broadcast the message 10 times, cumulatively resulting in around 1000 transmissions, excluding additional redundancies.

However, through the application of a forwarding tree with a depth of $k = 2$, it's possible to markedly decrease the transmission count.

Should each initiating node relay messages solely to its direct neighbors, and subsequently, these neighbors transmit only to nodes in the subsequent layer, the total transmissions could be curtailed to approximately 200–300, contingent on the network's structural configuration and the nodes' positioning.

An increase in the tree depth, k, further diminishes the requisite number of transmissions.

In Fig. 2, the number of transmissions for different numbers of nodes (10, 50, 100) is compared between traditional flooding and optimized flooding using a forwarding tree at $k = 2$.

It is evident that as the number of nodes in the sensor network increases, the number of necessary transmissions with traditional flooding rises linearly and at a much faster rate than with optimized flooding.

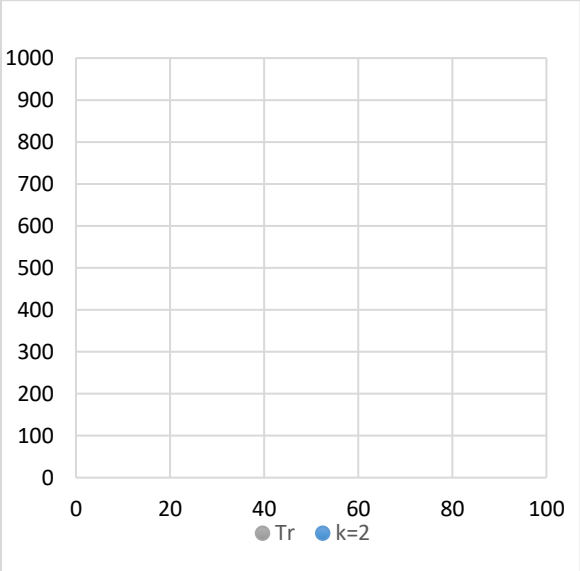

Figure 2: Comparison of traditional flooding and optimized flooding using a forwarding tree at $k = 2$

Optimized flooding demonstrates significantly better efficiency by reducing the total number of transmissions, especially in larger networks [14].

In Fig. 3, the number of transmissions across different node counts (10, 50, 100) is compared between traditional flooding and optimized flooding utilizing a forwarding tree at various tree depths ($k = 2, k = 3, and\ k = 5$).

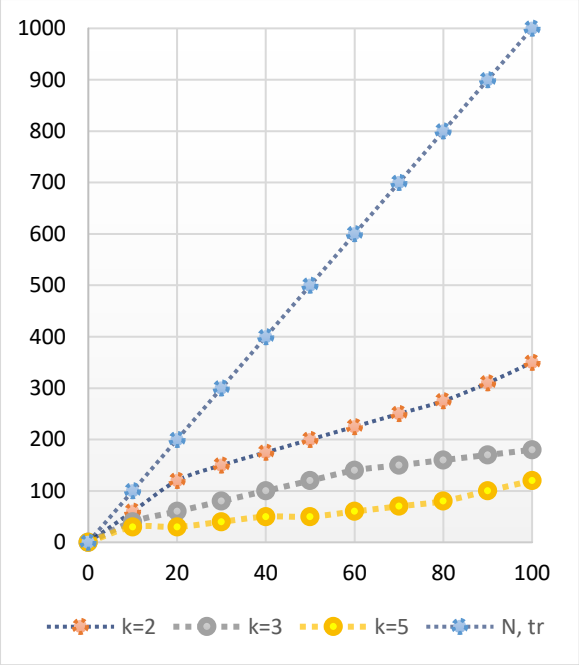

Figure 3: Comparison of traditional flooding and optimized flooding using forwarding tree for $k = 2, k = 3$ *and* $k = 5$

As k increases, the figure illustrates how deeper forwarding trees can further reduce the total number of transmissions, thereby conserving the energy of the nodes [15]. This highlights the significance of optimizing message propagation in sensor networks to enhance efficiency and conserve energy [16].

Traditionally, flooding is calculated as follows:

$$E_{total} = T * P, \quad (1)$$

where E_{total} is the total energy consumption of one node, T is the number of transmission cycles, P is the number of messages transmitted in one cycle.

In the traditional flooding scenario, each node conventionally transmits 10 messages per cycle, and each node exhausts its energy after 100 cycles (assuming all energy is spent on transmission only).

Optimized flooding is calculated as follows:

$$E_{opt} = T * P_k, \quad (2)$$

where E_{opt} is the total energy consumption of one node with optimized flooding, P_k is the number of messages transmitted in one cycle when condition k changes.

In the scenario with optimized flooding for $k = 2$, each node will exhaust its energy in 200 cycles; for $k = 3$—for 333 cycles; for $k = 5$—for 500 cycles. This means that for 100 transmission cycles, nodes will be able to stay active much longer in scenarios with optimized flooding, especially at larger values of k.

5. Conclusions

The optimization of the flooding mechanism involves the implementation of strategies that reduce the number of redundant messages caused by the traditional flooding method. This is achieved by carefully selecting the nodes that participate in data transmission to minimize the energy consumption of each node and increase the overall efficiency of the network.

This approach allows for an increase in the lifetime of the sensor network and improves the quality of service by reducing the time of message delivery and increasing the reliability of data transmission.

It is also worth noting that the optimization of the flooding mechanism in sensor networks not only reduces energy consumption and increases the efficiency of data distribution but also contributes to increasing their security. Fewer transmissions reduce the risk of interception and unauthorized access to data and make Denial-of-Service (DoS) attacks more difficult because fewer active nodes need to be attacked. Thus, optimized flooding helps create a more attack-resistant sensor network structure.

References

[1] H. Hulak, et al., Dynamic Model of Guarantee Capacity and Cyber Security Management in the Critical Automated System, in: 2nd International Conference on Conflict Management in Global Information Networks, vol. 3530 (2023) 102–111.

[2] V. Sokolov, P. Skladannyi, H. Hulak, Stability Verification of Self-Organized Wireless Networks with Block Encryption, in: 5th International Workshop on Computer Modeling and Intelligent Systems, vol. 3137 (2022) 227–237.

[3] V. Buriachok, et al., Invasion Detection Model using Two-Stage Criterion of Detection of Network Anomalies, in: Workshop on Cybersecurity Providing in

Information and Telecommunication Systems, vol. 2746 (2020) 23–32.
[4] N. Dovzhenko, et al., Comprehensive Analysis of Efficiency and Security Challenges in Sensor Network Routing, in: Cybersecurity Providing in Information and Telecommunication Systems II Vol. 3550 (2023) 275–280.
[5] V. Sokolov, P. Skladannyi, N. Korshun, ZigBee Network Resistance to Jamming Attacks, in: IEEE 6th International Conference on Information and Telecommunication Technologies and Radio Electronics (2023) 161–165. doi: 10.1109/UkrMiCo61577.2023.10380360.
[6] V. Sokolov, P. Skladannyi, A. Platonenko, Jump-Stay Jamming Attack on Wi-Fi Systems, in: IEEE 18th International Conference on Computer Science and Information Technologies (2023) 1–5. doi: 10.1109/CSIT61576.2023.10324031.
[7] V. Sokolov, P. Skladannyi, V. Astapenya, Bluetooth Low-Energy Beacon Resistance to Jamming Attack, in: IEEE 13th International Conference on Electronics and Information Technologies (2023) 270–274. doi: 10.1109/ELIT61488.2023.10310815.
[8] 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.
[9] S. Dovgiy, O. Kopiika, O. Kozlov, Architectures for the Information Systems, Network Resources and Network Services, in: Cybersecurity Providing in Information and Telecommunication Systems II Vol. 3187 (2021) 293–301.
[10] Z. Hu, et al., Analytical Assessment of Security Level of Distributed and Scalable Computer Systems, Int. J. Intell. Syst. Appl 8(12) (2016) 57–64.
[11] V. Mukhin, et al., Method of Restoring Parameters of Information Objects in a Unified Information Space Based on Computer Networks, Int. J. Comput. Netw. Inf. Secur. 12(2) (2020) 11–21.
[12] O. Barabash, et al., Development of a Hybrid Network Traffic Load Management Mechanism Using Smart Components. IEEE 7th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC) (2023) 38–41.
[13] V. Mashkov, O. Barabash, Self-Checking of Modular Systems under Random Performance of Elementary Checks, Engineering Simulation 12 (1995) 433–445.
[14] L. Globa, et al., Approach to Uniform Platform Development for the Ecology Digital Environment of Ukraine, Progress in Advanced Information and Communication Technology and Systems, LNNS 548 (2022) 83–100. doi: 10.1007/978-3-031-16368-5_4.
[15] Y. Melnyk Yurii, et al., The Process of Network Flows Distribution based on Traffic Engineering Method, International Journal of Advanced Trends in Computer Science and engineering 8(6) (2019) 3036–304. doi: 10.30534/ijatcse/2019/60862019.
[16] O. Barabash, et al., Distribution of Values of Cantor Type Fractal Functions with Specified Restrictions, Contemporary Approaches and Methods in Fundamental Mathematics and Mechanics (2021) 433–455. doi: 10.1007/978-3-030-50302-4_21.