

Research Article

# Compromise Between Topology Connection, Load Balance and Wireless Sensor Networks' Anomalies (WSN)

Serhii Perepelitsyn<sup>\*</sup> , Andriy Perepelitsyn 

Green Optimum LLC, Kyiv, Ukraine

## Abstract

The article addresses the challenge of ensuring a compromise between topological connectivity, load balancing, and anomaly detection in Wireless Sensor Networks (WSN). It analyzes current methods and approaches for optimizing the performance of sensor networks under dynamic conditions. The goal of this work is to analyze the interrelationship between these compromise aspects and propose an optimal approach for their integration. The article proposes a combined approach, which enables an optimal trade-off between these characteristics and enhances network interaction efficiency. To ensure the efficient operation of wireless sensor networks (WSN), it is essential to balance three key factors: topological connectivity and stable connectivity, even load distribution and security. Anomaly detection in wireless sensor networks (WSN) is critically important for ensuring their security and reliability. Modern anomaly detection methods include statistical analysis and machine learning techniques. Statistical traffic analysis enables the identification of deviations from normal network behavior, which may indicate anomalies existence. This approach is based on collecting and analyzing network traffic data, such as transmitted data volume, packet frequency, and other parameters. Deviations from established norms can signal potential issues or attacks. Further research in this domain should focus on the development of intelligent algorithms capable of adapting to real-time network changes. The integration of artificial intelligence and machine learning in WSN systems opens new opportunities for improving their efficiency and resilience to environmental changes.

## Keywords

Wireless Sensor Networks, Topological Connectivity, Load Balancing, Anomalies Detection, Artificial Intelligence, Neural Networks

## 1. Introduction

Wireless Sensor Networks (WSN) are a critical component of modern communication systems and are used for data collection and transmission across various domains, such as environmental monitoring, industrial automation, and military applications. One of the key challenges in deploying such networks is maintaining topological connectivity, which ensures stable data transmission between nodes. A reliable topological structure enables the

network to operate even under challenging conditions and in the event of node failures. To maintain topological connectivity, the power transmitters algorithms are employed, they allow dynamic regulation of the nodes' energy consumption, as well as self-organizing routing protocols that automatically update routes in response to changes within the network. Hardware optimization techniques allow to achieve the best results in sen-

<sup>\*</sup>Corresponding author: [sergpsa@inbox.lv](mailto:sergpsa@inbox.lv) (Serhii Perepelitsyn)

**Received:** 24 March 2025; **Accepted:** 6 May 2025; **Published:** 22 May 2025



Copyright: © The Author(s), 2025. Published by Science Publishing Group. This is an **Open Access** article, distributed under the terms of the Creative Commons Attribution 4.0 License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

sor radio networks that process video, audio, and other complex data [1].

Additionally, mobile nodes can help improve coverage and avoid data transmission issues. To prevent the overload of individual nodes, load balancing methods are used. Adaptive routing allows selecting less congested nodes for traffic transmission, while clustering techniques, such as the LEACH and HEED algorithms, aid in grouping nodes into clusters that evenly distribute the load [2]. Moreover, dynamic role distribution within the network allows modification of node functions based on the current network state. Various approaches are employed for anomaly detection within the network. Statistical methods analyze network behavior and detect deviations in node operations. Machine learning techniques, including Gaussian Mixture Model (GMM) algorithms, neural networks, and Random Forest, are also used to detect anomaly nodes based on previous data.

Simpler approaches are also commonly used, such as threshold control, where the system registers anomalies in exceeding critical metrics. Network intrusion detection systems are typically deployed at the perimeter of the network or in relatively important segments of the network to monitor various data packets. A bottleneck that impacts network performance is the processing speed of the network security device [3, 4]. A manual [5] proposes a method for distributing self-similar traffic among the sensors of the intrusion detection system.

## 2. Modern Methods Analysis

Modern approaches to optimizing the performance of wireless sensor networks in dynamic environments aim to ensure stable connectivity, balanced load distribution, and anomaly detection. The most effective solutions integrate multiple optimization methods simultaneously. Multi-agent systems enable autonomous nodes to make real-time decisions regarding the optimization of their parameters. Additionally, the incorporation of the Internet of Things (IoT) and cloud computing allows the network to process large volumes of data and adapt to changes in real time. These methods and approaches enhance the stability, energy efficiency, and security of wireless sensor networks, even in the presence of dynamic topology changes, uneven load distribution, and potential threats.

This study examines various approaches to optimizing the performance of wireless sensor networks (WSN) and proposes methods for integrating topological connectivity, load balancing, and anomaly detection to maximize network efficiency.

### 2.1. Methods to Ensure Topological Connectivity

Various methods for maintaining topological connectivity are employed to ensure the stable operation of wireless sensor networks (WSN). One such method is transmitters power control, which enables dynamic adjustment of node coverage radius based on network conditions. This approach minimizes

energy consumption and reduces interference between neighboring nodes. Another effective approach involves self-recovery algorithms, which can automatically adapt to network changes, monitor node status, and reconfigure routing in response to node failures or in case new sensors were added.

The implementation of these methods relies on specialized software modules. For example, the Dynamic Power Control Module is responsible for adjusting signal transmission levels based on network load and node positioning. This helps reduce energy consumption while maintaining network connectivity. Another critical component is the Topology Recovery Module, which analyzes network connections and automatically adjusts routing in response to structural changes within the network.

Further details on these methods can be found in the following scientific publications [1, 2, 6-13].

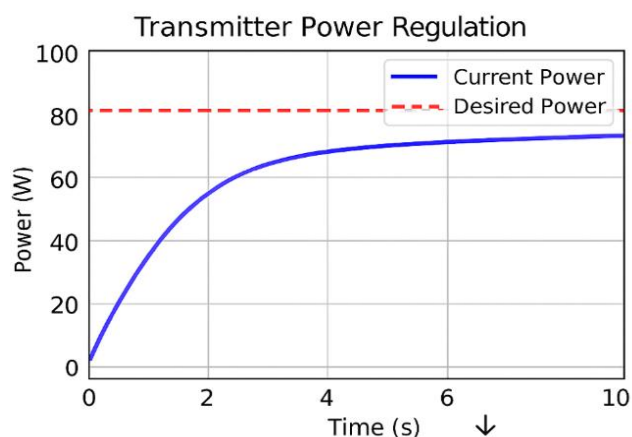


Figure 1. Transmitter's power regulation graph.

An example of code in the multi-paradigm, high-level programming language Python (transmitter power control) is provided in Appendix.

The graph illustrates how the transmitter power (blue line) changes over time when using a PID controller:

- 1) Initially, the transmitter power is set at 5 W (initial power level).
- 2) The PID controller applies corrections to the current power to bring it closer to the desired power level (100 W).
- 3) Over time, the transmitter power stabilizes at the desired level.
- 4) The red dashed line on the graph represents the desired power level (100 W) that the transmitter aims to achieve.
- 5) Thanks to the controller, the system reaches a stable state while minimizing errors.
- 6) This process demonstrates
- 7) system stabilization through corrections applied by the PID controller.

The plot should show a smooth transition from the initial

power (50 W) to the desired power (100 W), with the power output stabilizing after some time. This is a typical behavior for a system controlled by a PID regulator.

## 2.2. Methods of Load Balancing

Load balancing in wireless sensor networks (WSN) is a critically important task, as overloading individual nodes can lead to rapid energy discharge and network failure. To ensure an even distribution of workload, adaptive routing algorithms are employed, allowing real-time adjustments to data transmission routes. This helps prevent congestion at specific nodes by redirecting traffic flows through less loaded routes. Another approach involves resource allocation methods that optimize the utilization of the network's energy and computational resources. These methods prevent scenarios where some nodes operate at their maximum capacity while others remain underutilized. The implementation of these mechanisms relies on specialized software modules. For example, the Routing Optimization Module analyzes node load and adjusts data transmission routes, ensuring a more even distribution of traffic. This is particularly crucial for networks with high traffic dynamics, such as military or industrial WSNs. Another key component is the Traffic Balancing Module, which monitors the volume of data passing through each node and distributes it across different routes. This helps prevent network bottlenecks and extends the lifespan of battery-powered nodes. There are numerous scientific studies dedicated to this topic.

One such study is presented in a master's thesis, where an adaptive clustering algorithm for WSNs with mobile nodes was developed. This algorithm enhances the network's lifespan and ensures operational stability, which is crucial for dynamic application conditions [14].

Another study explores optimization methods for routing in WSNs. The research analyzes the implementation of routing algorithms that include the specific requirements of sensor networks, such as limited energy resources and the need for reliable data transmission [15].

## 2.3. Anomaly Detection Methods

Anomaly detection in wireless sensor networks (WSN) is critically important for ensuring their security and reliability. Modern anomaly detection methods include statistical analysis and machine learning techniques. Statistical traffic analysis enables the identification of deviations from normal network behavior, which may indicate anomalies existence. This approach is based on collecting and analyzing network traffic data, such as transmitted data volume, packet frequency, and other parameters. Deviations from established norms can signal potential issues or attacks.

Machine learning and artificial intelligence are widely used for recognizing patterns of anomalous behavior. In particular, convolutional neural networks (CNN) and recurrent neural

networks (RNN) can be utilized to analyze network traffic and detect anomalies. Research has shown that CNNs combined with long short-term memory (LSTM) layers exhibit high effectiveness in detecting network anomalies.

The most optimal approach for network anomaly detection is the convolutional neural network with long short-term memory (CNN-LSTM). It is significantly faster than a recurrent neural network (RNN) and more reliable than standalone LSTM layers. Besides, it's convenient in application which opens wide array of opportunities to detect network anomalies. [16].

Software modules for anomaly detection.

The Statistical Anomaly Detection Module assists in identifying irregularities in the operation of a wireless sensor network (WSN). It collects node performance data, analyzes it, and determines whether any unusual changes indicate potential faults or attacks. How does it work? First, the module collects data from sensor nodes, including traffic levels, signal strength, and other key parameters. It then calculates average values and establishes thresholds for normal network behavior. If new data exceeds these thresholds, the system flags it as an anomaly. This approach enables early detection of potential issues. For example, if a node suddenly starts transmitting an unusually high volume of data, it could indicate an attack or a malfunction. In such cases, the module can send alerts to administrators or modify network operations to prevent failures. Similar methods are widely applied in numerous studies [17].

The AI-based Threat Detection Module utilizes machine learning algorithms to identify suspicious activity within wireless sensor networks (WSNs). This module analyzes sensor data to determine whether potential threats or malfunctions exist within the network.

How does it work? First, the module gathers network operation data, such as signal levels, traffic volume, and energy consumption, etc. These data points are then cleaned and analyzed to establish patterns of normal operation. Based on this information, the module learns to distinguish between typical and anomalous behavior. If deviations from the norm arise, the system can identify them as potential attacks or network issues. The primary advantage of this approach is the ability to automatically and rapidly detect threats before they cause harm. The system continuously improves by learning from new data, allowing it to adapt to network changes. Research on this topic can be found in works such as [17, 18]. Implementing an AI-based Threat Detection Module enhances the security and reliability of wireless sensor networks, ensuring timely identification and mitigation of potential threats.

An example of code with visualization of results using the multiparadigm high-level programming language Python (anomaly detection using GMM) can be found in Appendix.

*GMM anomaly detection code explanation*

The Gaussian Mixture Model (GMM) is one of the effective approaches for detecting anomalies in data. In this example, we apply GMM to analyze a one-dimensional dataset

containing the following values: [1, 2, 2.1, 5, 6, 8, 100]. The last value (100) is a clear anomaly.

#### 1. Creating the GMM Model

GMM is used to represent data as a mixture of multiple normal distributions (in our case, two). The model attempts to find the best representation of the data using these distributions.

2. *Computing the Probability of Belonging to Clusters.* For each data point, the model calculates the logarithmic probability score, indicating how well the value fits the identified normal distributions.

3. *Identifying Anomalous Points.* An anomaly threshold is set at the 10th percentile of the log-probability scores. If a value falls below this threshold, it is classified as an anomaly.

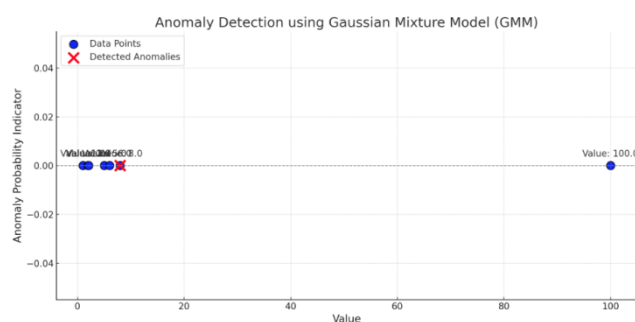
#### 4. Visualization of Results.

1) Blue circles (o) represent normal data points.

2) Red crosses (x) mark detected anomalies.

3) The visualization includes labeled data points, a horizontal reference line ( $y=0$ ), and a grid for better clarity.

Thus, the model successfully identifies 100 as an anomaly since it significantly deviates from the rest of the dataset.



**Figure 2.** Result Visualization Graph.

#### Explanation of the Visualization Graph

- 1) Blue dots on the graph represent the original data points.
- 2) Red "x" marks indicate detected anomalies.
- 3) GMM analyzes the data distribution and identifies points with a low probability of belonging to the main clusters.

### 3. Trade-off Between Parameters and Methods

To ensure the efficient operation of wireless sensor net-

works (WSN), it is essential to balance three key factors: topological connectivity and stable connectivity, even load distribution and security.

One way to achieve this is by adjusting transmitter power levels. If a node transmits with excessive power, it consumes more energy and may cause interference. Conversely, if the power is too low, connections may be lost. Therefore, continuous signal level adjustment is necessary to maintain reliable communication while reducing energy consumption. Another method is intelligent routing. Data in the network can be transmitted through multiple nodes. If some nodes become overloaded, the entire system may slow down. Modern algorithms adapt to network changes and automatically select the most efficient data transmission paths. It is also crucial to detect anomalies, or unusual network events. For instance, if a node suddenly starts transmitting an excessive amount of data or unexpectedly stops working, it could indicate a failure or even a cyberattack. To detect such issues quickly, specialized algorithms analyze network data and identify suspicious activities. All these functionalities can be implemented using specialized software. The system can operate as a single integrated solution or consist of multiple independent modules that communicate via APIs. This modular approach enhances flexibility and allows customization based on specific needs. Summary of methods. To achieve an optimal trade-off, various tools and techniques can be applied depending on the required accuracy, computational resources, and network type. Clustering Methods help divide sensor nodes into groups. K-Means partitions nodes into clusters but assumes they have a circular shape. Fuzzy C-Means allows nodes to belong to multiple clusters simultaneously with a certain probability. Gaussian Mixture Models (GMM) create more flexible groupings, particularly in heterogeneous networks.

Energy-Efficient Routing reduces power consumption by selecting paths based on node energy levels. Energy-Aware Routing chooses the most energy-efficient path. LEACH dynamically changes cluster leaders to conserve energy and PEGASIS enables nodes to transmit data through their nearest neighbors, minimizing energy use.

Intelligent Approaches leverage deep neural networks (DNNs) for traffic load and optimal traffic routing prediction. Q-Learning & Deep Reinforcement Learning are used for optimal energy-balancing strategies. Genetic Algorithms search for the most efficient routing paths in the network.

**Table 1.** Comparison of methods.

Method	Influence on Topological Connectivity	Load Balancing	Anomaly Detection
LEACH	High (Stable Network)	Moderate (Dynamic Cluster Heads)	Low (Not Focusing on Anomalies)

Method	Influence on Topological Connectivity	Load Balancing	Anomaly Detection
<i>GMM</i>	Moderate (Changes of Clusterization)	High (Probability Distribution)	Moderate (Anomalies can Mix)
<i>Q-Learning Routing</i>	High (Adaptive Route)	High (Dynamic Balancing)	Low (No Imbedded Anomaly Detection)
<i>Isolation Forest</i>	Neutral	Neutral	High (Detection of Local Anomalies)
Autoencoders	Neutral	Neutral	High (Complex Anomalies)

## 4. Results

The optimal solution depends on the use case scenario.

- 1) If the priority is connectivity, LEACH, EAR, and Q-Learning should be used.
- 2) If the priority is load balancing, GMM and Reinforcement Learning will be most effective.
- 3) If the priority is anomaly detection, the best results are achieved with Isolation Forest and Autoencoders.

Hybrid methods (e.g., GMM + Q-Learning + Autoencoders) can provide a balance between the three aspects of the compromise—topological connectivity, load balancing, and anomaly detection in wireless sensor networks (WSN).

Further research in this area should focus on the development of intelligent algorithms capable of adapting to network changes in real time. These algorithms should combine energy consumption optimization, efficient routing, and distributed anomaly detection methods. Integrating artificial intelligence and machine learning into WSN systems opens up new opportunities for improving their efficiency and resilience to environmental changes.

## 5. Discussion

The optimal operation of wireless sensor networks (WSNs) is only possible if there is a proper balance between three key aspects: topological connectivity, even load distribution, and effective anomaly detection. Each of these factors directly impacts the network's performance and reliability.

- 1) Topological connectivity is critically important for uninterrupted data transmission between nodes. Loss of connectivity can lead to data loss and disrupt the operation of the entire network. The use of dynamic transmission power control algorithms enables adaptive maintenance of connectivity while simultaneously reducing energy consumption.
- 2) Even load distribution ensures the efficient operation of the network by preventing overload on individual nodes. This is particularly important in large networks, where resources are limited, and excessive load on certain nodes can lead to their rapid failure. The hybrid routing

methods application helps to dynamically balance the load, reducing the risk of overload and extending the network's lifespan.

- 3) Anomaly detection plays a crucial role in ensuring the security and reliability of WSNs. Distributed anomaly detection algorithms enable the identification of both internal network failures (e.g., node malfunctions) and external threats (e.g., cyberattacks). The use of machine learning methods significantly enhances the accuracy of detecting suspicious activities while minimizing resource consumption.

## 6. Conclusions

Integrating various methods, such as GMM + Q-Learning + Autoencoders, into a single platform ensures a balance between the three aspects of the trade-off—topological connectivity, load balancing, and anomaly detection in wireless sensor networks (WSN).

Thus, the future development of WSNs will focus on creating self-organizing, adaptive, and energy-efficient networks capable of effectively operating in dynamic conditions, ensuring stable connectivity, even load distribution, and high security.

## Abbreviations

WSN	Wireless Sensor Networks
GMM	Gaussian Mixture Model
IoT	Internet of Things
CNN	Convolutional Neural Networks
LSTM	Long Short-Term memory

## Acknowledgments

The authors express their gratitude to Dmitry Kucherov, Department of Computerized Control Systems, National Aviation University, for support in preparing and writing the article.



## Author Contributions

Author input according to SciencePG requirements and accepted CrediT taxonomy.

**Serhii Perepelitsyn:** Concept, Resources, Formal Analysis, Supervision, Investment attraction, Methodology, Scripting – Original Draft, Project Administration

**Andriy Perepelitsyn:** Data Curation, Software, Validation, Investigation, Visualization

## Funding

This study is not supported by any external funding

## Data Availability Statement

Datasets that support the results of this study are provided in Appendix.

## Conflicts of Interest

The authors declare no conflicts of interests.

## Appendix

```
import matplotlib.pyplot as plt

# PID Regulator class
class PowerRegulator:
    def __init__(self, desired_power, kp, ki, kd):
        self.desired_power = desired_power
        self.kp = kp
        self.ki = ki
        self.kd = kd
        self.previous_error = 0
        self.integral = 0

    def calculate_error(self, current_power):
        return self.desired_power - current_power

    def regulate(self, current_power, dt):
        error = self.calculate_error(current_power)
        self.integral += error * dt
        derivative = (error - self.previous_error) / dt
        adjustment = self.kp * error + self.ki * self.integral + self.kd * derivative
        self.previous_error = error
        return adjustment

# Simulation setup
desired_power = 100
current_power = 50
kp, ki, kd = 0.1, 0.01, 0.05
regulator = PowerRegulator(desired_power, kp, ki, kd)

time_values = []
power_values = []

for step in range(100):
    dt = 0.1
    adjustment = regulator.regulate(current_power, dt)
    current_power += adjustment
    power_values.append(current_power)
    time_values.append(step * dt)

# Plotting
plt.plot(time_values, power_values, label='Current Power')
plt.axhline(y=desired_power, color='r', linestyle='--', label='Desired Power')
plt.title('Transmitter Power Regulation Over Time')
plt.xlabel('Time (s)')
plt.ylabel('Power (W)')
plt.legend()
plt.grid(True)

# Save plot to file
plt.savefig('transmitter_power_plot.png', dpi=300)
plt.show()

# Console output explanation in English
print("""
Explanation:
- The plot shows how the transmitter power (blue line) changes over time using a PID controller.
- Initially, the transmitter starts at 50 W.
- The PID controller continuously adjusts the output to reach and stabilize around the desired 100 W.
- The red dashed line indicates the target power level.
- This demonstrates how feedback control enables smooth and accurate power regulation in dynamic systems.
The plot has been saved as 'transmitter_power_plot.png'.
""")
```

**Figure A1.** An example of code in the multiparadigm high-level programming language Python (transmitter power control).

```

# Повторне імпортування бібліотек після скидання стану
import numpy as np
import matplotlib.pyplot as plt
from sklearn.mixture import GaussianMixture

# Генерація тестових даних
X = np.array([[1], [2], [2.1], [5], [6], [8], [100]]) # Остання точка - аномалія

# Побудова GMM-моделі
model = GaussianMixture(n_components=2, random_state=42)
model.fit(X)

# Визначення ймовірності аномалій
scores = model.score_samples(X)
threshold = np.percentile(scores, 10)
anomalies = X[scores < threshold]

# Візуалізація результатів
plt.figure(figsize=(10, 5))
plt.scatter(X, np.zeros_like(X), label='Дані', color='blue', marker='o', s=100)
plt.scatter(anomalies, np.zeros_like(anomalies), label='Аномалії', color='red', marker='x', s=150)

# Додавання підписів до точок
for i, txt in enumerate(X.flatten()):
    plt.annotate(txt, (X[i], 0), textcoords="offset points", xytext=(0,10), ha='center', fontsize=12)

plt.axhline(y=0, color='gray', linestyle='--', linewidth=1) # Додаткові деталі
plt.xlabel('Значення', fontsize=14)
plt.ylabel('Ймовірність аномалії', fontsize=14)
plt.title('Виявлення аномалій за допомогою GMM', fontsize=16)
plt.legend(fontsize=12)
plt.grid(True, linestyle='--', alpha=0.6)
plt.show()

```

**Figure A2.** An example of code with visualization of results in the multiparadigm high-level programming language Python (anomaly detection using GMM).

## References

- [1] О. С. Шкіль, С. О. Костюк, І. В. Філіппенко. Методи енергозбереження в сенсорних мережах. *Радиоелектроника и информатика* — 2019 р. // О. S. Shkil, S. O. Kostyuk, I. V. Philippenko. *Methods of energy saving in sensor networks*. *Radio Electronics and Informatics* — 2019. [https://doi.org/10.30837/1563-0064.3\(86\).2019.214976](https://doi.org/10.30837/1563-0064.3(86).2019.214976)
- [2] Валуїський, С. В., Кисіль, А. І. Методи кластеризації в безпроводових сенсорних мережах наступного покоління. *Збірник матеріалів Міжнародної науково-технічної конференції «Перспективи телекомунікацій»*, 286–288.- 2024 р. // Valuyskyi S. V., Kysyl A. I. *Clustering methods in wireless sensor networks of next generation*. *Proceedings of the International Scientific and Technical Conference "Perspectives of Telecommunications"*
- [3] S. Noel and S. Jajodia, "Optimal IDS Sensor Placement and Alert Prioritization Using Attack Graphs," *Journal of Network and Systems Management*, 16(3), pp. 259-275, 2008. <https://doi.org/10.1007/s10922-008-9109-x>
- [4] H. Chen, J. A. Clark, S. Shaikh, H. Chivers and P. Nobles, "Optimising IDS Sensor Placement," Conference: ARES 2010, Fifth International Conference on Availability, Reliability and Security, Krakow. 15-18 February 2010 p. <https://doi.org/10.1109/ARES.2010.92>
- [5] Т. А. Радівілова, "Метод розподілу самоподібного навантаження в мережній системі виявлення вторгнень," *Проблеми телекомунікацій*, No2(21), с. 42-51, 2017 р. // T. A. Radivilova, "Method of Self-Similar Load Distribution in Network Intrusion Detection Systems," *Telecommunications Issues*.
- [6] Перепелицин С. О., Терещенко Я. В., Шевченко А. М., Лоза В. М., Терещенко В. М. *Тактичні сенсорні радіомережі - мультисенсорна детекція та локалізація рухомих об'єктів*. /журнал "Наукоємні технології" "вид-во НАУ,- №4 2023 р. // Perepelitsyn S. O., Tereschenko Y. V., Shevchenko A. M., Loza V. M., Tereschenko V. M. "Tactical sensor radio networks – multisensory detection and localization of movable objects", *Magazine "Science-intensive technologies"* Publisher Ukrainian National Academy of Science. <https://doi.org/10.18372/2310-5461.60.18265>

- [7] Перепеліцин С. О. Система захисту від загроз удару БПЛА із використанням блоків нейромережевого аналізу / Наукоємні Технології.–К. НАУ. – №1(45), 2020 р., с. 19–27. // Perepelitsyn S. O. “UAV attacks threat prevention system with neural network analysis systems”, Magazine “Science-intensive technologies” Publisher Ukrainian National Academy of Science.  
<https://doi.org/10.18372/2310-5461.45.14579>
- [8] Перепеліцин С. О. Аналіз можливості застосування хмарних обчислень у військових бездротових мережах управління тактичного рівня. – Сучасна спеціальна техніка. – К. № 2 (61), 2020 р., с. 47–58. //Perepelitsyn S. O. “Cloud computation analysis opportunities in military wireless tactical networks” – Modern Special Technics.  
[https://doi.org/10.36486/mst2411–3816.2020.2\(61\)5](https://doi.org/10.36486/mst2411–3816.2020.2(61)5)
- [9] Слюсар В. І., Перепеліцин С. О. Аналіз топології багаторангових мереж на основі торцевого добутку матриць / Міжнародна науково-технічна конференція «Радіотехнічні поля, сигнали, апарати та системи». – К. КПІ ім. Ігоря Сікорського, Київ, Україна, 16–22.11. 2020 р., с. 114-116. // Slusar V. I., Perepelitsyn S. O., “Analysis of the Topology of Multilevel Networks Based on the Tensor Product of Matrices”.  
<https://ela.kpi.ua/handle/123456789/50419>
- [10] Слюсар В. І., Перепеліцин С. О., Писаренко Р. В. Вплив топології на конфігурацію рухомих мультирангових мереж./ XII Міжнародна науково - практична конференція “Advancing in research and education”, Ля-Рошель, Франція, 07–10.12. 2020 р., с. 558-563. // Slusar V. I., Perepelitsyn S. O., Pysarenko R. V., “Topology influence on configuration of movable multilevel networks”, XII international conference “Advancing in research and education”, la Rochelle, France.  
<https://doi.org/10.13140/RG.2.2.28589.92643>
- [11] Перепеліцин С. О., Лесько О. В. Використання технології надширокопasmових сигналів та самоналагоджуваної мережі в управлінні БПЛА військового призначення / Вісник інженерної академії України. К. НАУ. – № 4, 2019 р., с. 28–34. // Perepelitsyn S. O., Lesko O. V. “Using ultra-wideband signal technology and self-tuning network in the control of military UAVs”, Bulletin of the Engineering Academy of Ukraine.  
<https://drive.google.com/file/d/1113FITRFJwJMWw2Pffo9DpGXpwrHE/view?pli=1>
- [12] П. В. Галкін. Аналіз моделей та оптимізації збору інформації в бездротових сенсорних мережах. Восточно-Европейський журнал передових технологій ISSN 1729-3774. - (71) 2014 р.. // Galkin P. V., “Wireless sensor networks model analysis and data gathering optimization”, East-European Magazine of advanced technologies.  
<https://doi.org/10.15587/1729-4061.2014.28008>
- [13] Кучеров Д. П., Пошивайло О. М., Мирошниченко І. В., Перепеліцин С. О.. Налаштування під-регулятора генетичним алгоритмом за багатокритеріальною цільовою функцією для керування нестійким об’єктом./ журнал "Проблеми управління і інформатизації", вид-во НАУ,- №4 2023 р.. // Kuchеров D. P., Poshyvailo O. M., Myroshnychenko I. V., Perepelitsyn S. O. “Tuning of a Subcontroller Using a Genetic Algorithm with a Multicriteria Objective Function for Controlling an Unstable Object. Journal "Problems of Control and Informatization".  
<https://jrn1.nau.edu.ua/index.php/PIU/article/view/18239/25513>
- [14] О. І. Лисенко, О. О Штойко. Розвиток методів маршрутизації в мобільних сенсорних мережах на основі використання адаптивного алгоритму кластеризації. Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського». - 2021 р.. // Lysenko O. I., Shtoyko O. O., Development of Routing Methods in Mobile Sensor Networks Based on the Use of an Adaptive Clustering Algorithm. National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute".  
<https://ela.kpi.ua/server/api/core/bitstreams/81d35da9-4103-4d36-8208-3d3484ccd0fb/content>
- [15] О. І. Лисенко, М. А. Скулиш. Розвиток алгоритмів маршрутизації у мобільних сенсорних мережах. Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» - 2021 р..// Lysenko O. I., Skulish M. A. Development of Routing Algorithms in Mobile Sensor Networks. National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute".
- [16] Гайдур Г. І., Гахов С. О., Бригинець А. А.. Виявлення мережевих аномалій з використанням алгоритмів нейронних мереж. Телекомунікаційні та інформаційні технології. 1 (78) — 2023 pp.. // Haidur H. I., Gahov S. O., Bryhinets A. A., Detection of Network Anomalies Using Neural Network Algorithms. Telecommunications and Information Technologies.  
<https://doi.org/10.31673/2412-4338.2023.010416>
- [17] Р. В. Дячок. Методи та засоби інтелектуалізації інформаційно-вимірювальних систем з мультисенсорною конфігурацією. Національний університет «Львівська політехніка». Дисертація. Львів - 2023 pp.. // Dyachok R. V. “Methods and Tools for the Intellectualization of Information and Measurement Systems with a Multisensory Configuration”, National University "Lviv Polytechnic". Dissertation. Lviv.
- [18] Б. Л. Луцевський. Алгоритми машинного навчання для виявлення та прогнозування атак на мережеву інфраструктуру. Західноукраїнський національний університет Факультет комп’ютерних інформаційних технологій. Тернопіль - 2023 р..// Lushevskiy B. L., Machine Learning Algorithms for Detecting and Predicting Attacks on Network Infrastructure. West Ukrainian National University, Faculty of Computer Information Technologies. Ternopil - 2023 p.