Article

A Survey on Coverage and Security in Wireless Sensor Networks

Mari M. Moslehi and Habib M. Ammari *

Posted Date: 7 May 2025

doi: 10.20944/preprints202505.0438.v1

Keywords: wireless sensor networks; coverage; security challenge; deployment strategies; sensor node types

 doi:10.20944/preprints202505.0438.v1

Article

A Survey on Coverage and Security in Wireless Sensor Networks

Mari M. Moslehi [1] and Habib M. Ammari [2,*]

[1] Department of Computer Science, Sacramento State University, Sacramento, California 95819, USA
[2] Wireless Sensor and Mobile Autonomous Networks, (WiSeMAN) Research Center, School of Engineering, College of Arts and Sciences, Texas A&M International University, Laredo, Texas 78041, USA
* Correspondence: Habib.Ammari@tamiu.edu

Abstract: This survey paper focuses on area coverage and security aspects in wireless sensor networks. It attempts to address the major critical issues related to both of them, and present solutions to address them. In fact, the complete function of wireless sensor networks will only be practicable when both of these issues have been taken into consideration in real-world applications, such as environmental monitoring, precision agriculture, and surveillance, to name a few. Various strategic methods developed for deploying sensors with two-dimensional, three-dimensional, deterministic, and nondeterministic deployment analyses regarding their impact on coverage, connectivity, energy efficiency, and scalability are discussed. This survey will also investigate the deployment of homogeneous and heterogeneous sensors in wireless sensor networks, showing exactly how design criteria are influencing network deployment, operations, and security. These will highlight some major security challenges, including strong encryption, authentication mechanisms, intrusion detection, resource depletion, and node compromise attack countermeasures. The findings provide insight into improving the reliability and energy efficiency of WSNs, therefore forming a basis for further research and development into secure and efficient deployment of wireless sensor networks.

Keywords: wireless sensor networks; coverage; security challenge; deployment strategies; sensor node types

1. Introduction

A wireless sensor network (WSN) consists of wireless sensor nodes, each of which has data storage, data processing, sensing, and communication capabilities. The capabilities of these networks to monitor and collect data in different environments and on a varied basis have found intense promotion. These include but are not limited to applications, such as environmental monitoring, precision agricultural relationships, and surveillance. The developed WSNs can monitor conditions in the environment, such as temperature, humidity, and pollutant levels, which are important data for ecological research in addition to supporting disaster reduction. With precision agriculture, WSNs can further monitor moisture in the soil, climatic conditions, as well as the presence of pests, thus improving results in crop management and optimizing the use of resources with better yields. This will support monitoring of large areas for defense activities, such as border patrol and battlefield surveillance. Now, WSNs become an evolutionary paradigm for collecting and studying features of data, with advances in MEMS technology, wireless communication, and digital electronics in conjunction with their collaborative and self-organizing nature [1]. The growing interest and advancements in WSNs are increasingly significant in modern technology due to their versatile applications and continuous innovation. Initially conceived for military use, WSNs have now become integral to the Internet of Things (IoT), supporting a wide array of applications in various sectors, such as environmental monitoring, agriculture, urban development, healthcare, and industry. WSNs are adaptable because their sensor nodes can sense, process, and communicate. Some of these include research into issues,

 doi:10.20944/preprints202505.0438.v1

such as energy efficiency, data management, and communication reliability. New research trends are attracted by emerging technologies in machine and deep learning, 5G technologies, and edge computing, which improve WSN functionality. These are capable of driving research trends that have focused on performance optimization, energy sustainability, and integration with other technology domains. The interest in WSNs that has been upheld all these years, and the diversity of its different applications, make it relevant with a potential contribution to future technological landscapes [2]. Essentially, there are several challenges in WSN deployment that must be taken care of and which are related to energy efficiency, security, and coverage. The region of interest should be guaranteed to have coverage, but due to the static nature and limited sensing range of the sensor nodes, there are usually gaps in sensing, making data collection unequal in most cases. The other significant challenge lies in energy efficiency. Indeed, sensor nodes are normally powered by batteries, and their deployment in hostile or inaccessible environments makes it impractical to replace or recharge them regularly. Thus, this necessitates the prolonging of the lifetime of a network by reducing energy consumption through efficient routing and data aggregation techniques. Security is equally important, as WSNs are very vulnerable to diverse types of attacks, such as data interception or manipulation in the nodes, potentially leading to the compromise of integrity or confidentiality of the transferred information. Therefore, tight encryption and authentication protocols must be implemented to help counteract such vulnerabilities. All these challenges must be addressed to guarantee successful WSN deployment and operation, making them functional in the scenarios of various applications —from industrial automation and environmental monitoring to other fields [3]. In WSNs, the sensor nodes can be considered as the elements that can influence or drive the whole design and functionality of the network. On the other hand, based on their fabrication, sensor nodes can be broadly classified into two categories, namely homogeneous and heterogeneous. Homogeneous sensor networks are built by identical nodes with precisely identical hardware capabilities and energy resources.

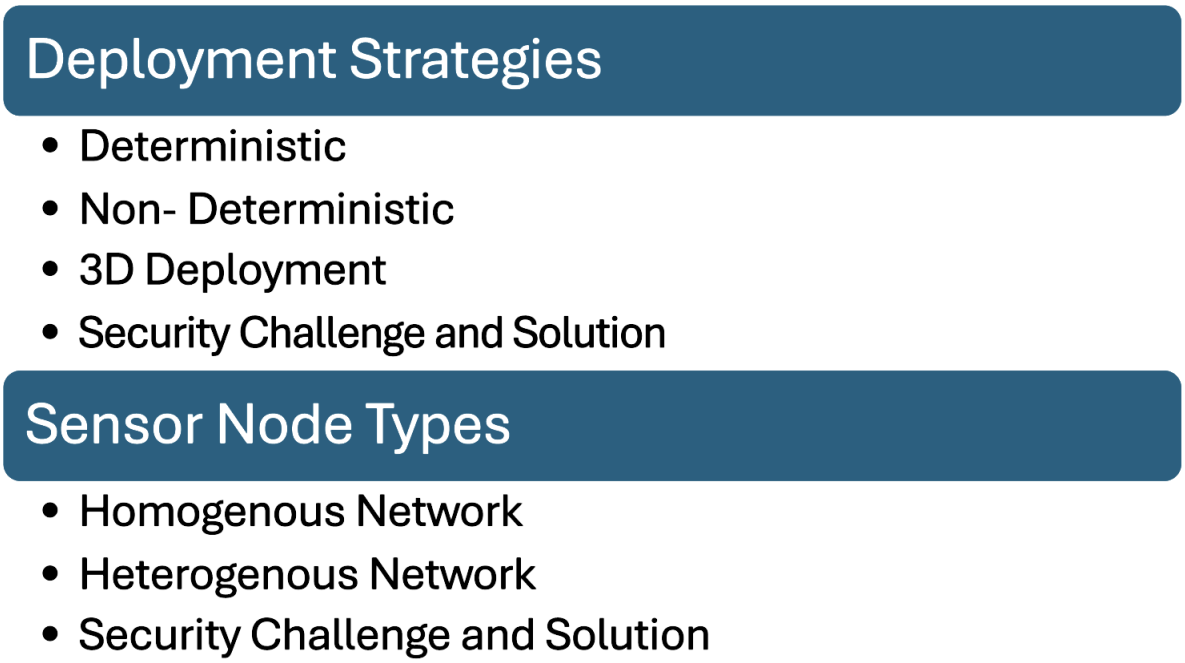

Figure 1. Classification of Deployment Strategies in Wireless Sensor Networks

This homogeneity makes the design and maintenance of the network easier and provides the same performance at all nodes. However, homogeneous networks are prone to an early exhaustion of energy in some nodes, normally those who become cluster heads more often as a result of their better energy

 doi:10.20944/preprints202505.0438.v1

status. On the other hand, heterogeneous sensor networks have different sets of nodes with disparate values of energy and capacity. These networks normally consist of a mixture of basic sensor nodes and more powerful cluster head nodes. Equipped with higher processing and communication capability, it is possible for the cluster heads to undertake heavier data loads and increase transmission distances without experiencing data exhaustion. This configuration could improve the energy efficiency of the network, thereby increasing its lifetime. However, it can be difficult to cope with diversity in types of nodes and maintain balanced energy consumption. This survey paper is therefore concluded in view of the fact that homogeneous or heterogeneous sensor nodes are chosen depending on application requirements while keeping in mind all trade-offs among energy efficiency, user-friendliness, and cost used [4]. This survey study is being written because there are various important questions in the subject that need to be explored and answered.

- In the context of cost, coverage, connectivity, energy efficiency, environment suitability, and scalability, what are the most effective deployment strategies for WSNs?
- What is the impact of homogeneous and heterogeneous sensor nodes on the design, functionality, and security of WSNs?
- Particularly in deployment, node types, and security, what are the main obstacles and potential future research directions in WSNs?

Our study is motivated by many critical inquiries in the area that need to be investigated and solved. In this survey paper, several possible deployment strategies are taken for review with respect to consideration of cost, coverage, connectivity, energy efficiency, environment suitability, and scalability for a variety of sensor node types. A clear structure of the paper is set out through two broad divisions: Deployment strategies and node types of sensors. The classification (refer to Figure 1) covers all major talks concerning design, functionality, security issues of WSNs, homogeneous and heterogeneous WSNs, and deterministic, non-deterministic, and three-dimensional (3D) deployment strategies. This attempts to individualize the basic challenges and future research directions in WSNs by critically analyzing these areas.

2. Classification of Deployment Strategies

The approaches of deployment can be factors that essentially affect the performance and efficiency of Wireless sensor networks. In this section, three main strategies are analyzed: Deterministic, non-deterministic, and 3D deployment, comparing them for various arguments, like cost of deployment, coverage, connectivity, environmental suitability, energy efficiency, and scalability.

2.1. Deployment strategies

The sensor nodes can either be deployed at the same time or put in an area of separate coverage. They can also be dropped from an aircraft, delivered by artillery shells, missiles, or rockets, or solely deployed by humans or robots. The structure of the network may change once defined due to events, such as the movement of sensor nodes, connectivity problems, their energy levels, malfunctions, and tasks [1]. Another method is the use of 3D deployment strategies in volumetric coverage environments, like underwater and industrial spaces, to increase the network's spatial monitoring capabilities [5]. Deterministic deployment strategies, where nodes are located at a predefined location, provide high coverage accuracy and network reliability, but may incur higher costs and complexity [6]. On the other hand, nondeterministic deployment, characterized by the random placement of nodes offers scalability and ease of deployment, especially in hard-to-reach or dangerous environments. However, this approach can lead to coverage and inconsistent performance [7]. In addition to these strategies, 3D deployment techniques are crucial for applications that require volumetric coverage, such as monitoring multi-level buildings, underwater environments, or industrial facilities. These methods improve spatial coverage and address difficult deployment constraints, making them crucial for

 doi:10.20944/preprints202505.0438.v1

comprehensive environmental monitoring [8]. All three of these deployment strategies differ in terms of deployment costs, coverage, connectivity, environmental suitability, energy efficiency, and scalability. The choice of deployment strategy significantly impacts the overall effectiveness of WSNs, influencing factors such as data accuracy, network robustness, and maintenance requirements [9]. Furthermore, advanced algorithms and techniques, including optimization methods and machine learning, are increasingly employed to enhance deployment efficiency and adapt to dynamic conditions within the monitored area [10]. In the following sections, we will analyze each deployment strategy: deterministic, non-deterministic, and 3D deployment, focusing on aspects such as deployment cost, coverage, connectivity, environment suitability, energy efficiency, and scalability. This analysis is therefore going to provide overall information on their impacts on the performance of wireless sensor networks. The comparative summary for the deployment strategies, as shown in Table 1, highlights important features and performance indicators. This comparison tries to give a clear knowledge of how each method performs in a variety of operational factors so as to help choose the best strategy for particular WSN applications.

Table 1. Comparison of Deployment Strategies

Aspect	**Deterministic**	**Non-Deterministic**	**3D**
Deployment Cost	Higher due to precise planning, advanced sensors, and relay nodes [11,12]	Lower initial cost due to reduced planning and simple setup [11, 20]	Significantly higher due to specialized equipment and precise positioning techniques [5,25,26]
Coverage	Full coverage using optimal patterns (e.g., triangular lattices) but susceptible to coverage holes due to placement errors and failures [13,14]	Resilient coverage due to random placement, but higher sensor density is required. Can utilize probabilistic models and mobile nodes to fill gaps [13,20,21]	Ensures coverage in complex 3D spaces using polynomial-time algorithms, distributed algorithms, and multi-objective genetic algorithms [27–29]
Connectivity	Guaranteed connectivity through strategic placement, even with obstacles [6,15]	Challenges in maintaining connectivity due to random placement; may need additional sensors or increased communication [20,23]	Maintained through truncated octahedron placement and distributed deployment algorithms [30,31]
Environment Suitability	Suitable for controlled, known environments with obstacles. Optimized placement for efficient communication [16,17]	Suitable for unknown, hostile environments where precise placement is not feasible. Adaptable and robust to changes [16,17,20]	Suitable for complex terrains like underwater and urban environments but requires line-of-sight and path-loss considerations [29,32]

 doi:10.20944/preprints202505.0438.v1

Table 1. *Cont.*

Aspect	Deterministic	Non-Deterministic	3D
Energy Efficiency	Maximized through strategic placement and optimized communication protocols. Reduced energy consumption due to minimal node movement [9,15]	Challenges due to non-uniform distribution in random deployment. Requires efficient algorithms for movement and energy management [9,20]	Achieved by minimizing active sensors while ensuring coverage, using optimal strategies and 3D-Voronoi partitioning [33,34]
Scalability	Demonstrated through optimal node placement strategies based on electrostatic field theory for efficient resource utilization and network performance [18,19]	Enhanced by exploiting spatio-temporal correlations and the ability to deploy large numbers of nodes without precise placement [20,24]	Enhanced through dynamic coordinate systems and virtual architectures for efficient data routing and management [33,35]

2.2. Deterministic Coverage

2.2.1. Deployment Cost

Deterministic deployment strategies involve placing sensors in planned locations, which allows for controlled sensor distribution and optimized energy management. This approach typically results in higher implementation costs due to the precision and design required, as well as the potential increase in hardware costs for more complex sensors and relay nodes. However, deterministic strategies can achieve longer network lifetime by ensuring optimal coverage and energy efficiency [11]. Moreover, although deterministic deployment methods provide optimal network configuration, they are often impractical and expensive for large-scale wireless sensor networks and inaccessible for harsh regions of interest [12].

2.2.2. Coverage

Optimal placement patterns, like a triangular grid, ensure effective coverage and connectivity in wireless sensor networks despite potential placement errors and sensor failures. The deterministic implementation uses optimal patterns such as a triangular grid to achieve complete coverage in the monitored area. However, this approach can lead to coverage gaps due to placement errors and sensor failures, which reduces the overall coverage quality [13]. Systematic placement of sensor nodes, especially using a triangular grid pattern, ensures complete coverage and maintains connectivity between nodes. This method is particularly effective when the communication area is equal to or greater than three times the square root of the sensing area, which optimizes then number of sensor nodes required and improves network efficiency and reliability [14].

2.2.3. Connectivity

In the deterministic use of wireless sensor networks, connectivity ensures that each sensor node can transmit its data to a base station either directly or through multiple other sensor nodes. This connectivity limit is critical to maintain data flow in the network and is typically achieved by placing sensor nodes in a way that ensures communication between them even in the presence of obstacles or different deployment patterns [6][15].

2.2.4. Environmental Suitability

This preplanned placement in deterministic deployment enables the placing of sensors at the best places, which aids communication and makes the network connectivity better, even with obstacles

 doi:10.20944/preprints202505.0438.v1

in the detection field [16]. More importantly, good planning of the node's placement is important for sustainability to the environment. This ensures optimal coverage and efficient use of resources, which is important for monitoring critical parameters such as temperature, humidity, and gas concentrations in the warehouse environment, promoting sustainable and efficient operations[17].

2.2.5. Energy Efficiency

Energy efficiency can be maximized through strategic placement and optimized communication protocols. Predefined sensor locations and controlled deployment processes reduce the need for extensive movement and relocation of nodes, thus saving energy. By optimizing the initial layout based on geometric patterns or algorithms, deterministic deployment ensures efficient use of energy resources, which improves overall network performance and longevity [9]. In addition, deterministic deployment strategies in WSNs optimize sensor placement to minimize redundant data transmission and increase network lifetime, which is critical to maintaining network coverage and connectivity constraints. This approach significantly reduces the energy consumption of sensor nodes, ensuring efficient communication paths and reducing the need for frequent reconfiguration [15].

2.2.6. Scalability

One of the aspects pointing toward the scalability of WSNs is optimal node placement strategies. Massive networks have optimal node deployments to ensure that the least node utilization can be achieved while ensuring effective coverage and connectivity. Electrostatic field theory rules govern how to excel at the best way of assigning nodes, getting stronger with the number of nodes in a network. That will ensure efficient traffic and data flow utilization in large and complex environments. With this approach, deterministic deployment is scaled in large wireless sensor networks, where efficient resource utilization and network efficiency are realized using deterministic deployment [18]. In addition to that, energy scalability can be improved by the placement of sensor nodes with deterministic deployment, which reduces redundant data transmission and ensures improvement in overall network efficiency. This method ensures the minimization of energy consumption while maintaining effective coverage and connectivity, which is essential for scalable and sustainable WSN operation [19].

2.3. Non-Deterministic Coverage

2.3.1. Deployment Cost

The strategies of non-deterministic deployment involve random placement of the sensors, and these require less preparation and set-up. Because of that, it will have lower initial deployment costs. This technology avoids the logistical constraints associated with deterministic deployment and is frequently utilized in harsh or hostile locations where manual sensor placement is impractical. To provide sufficient coverage and network lifespan, more sensors must be deployed because randomness might result in energy imbalances, coverage gaps, and inefficiencies. While there may be immediate savings, these savings may be outweighed by long-term operating expenses and the requirement for additional sensors [11]. Moreover, a WSN with randomly deployed sensor nodes performs worse than one with deterministic deployment; more sensor nodes are frequently needed, and they may need to be reallocated to fill in gaps, which raises overall costs and energy consumption [20].

2.3.2. Coverage

When we use non-deterministic, or random, deployment, which sets up sensors according to a uniform Poisson process, we can naturally account for sensor failures and placement errors. It offers a more resilient and flexible coverage, even though it typically needs a larger sensor density to provide the same coverage as deterministic deployment [13]. One of the main challenges in non-deterministic deployment is reaching optimal coverage and connection. Since nodes are dispersed at random, it

 doi:10.20944/preprints202505.0438.v1

is essential to make sure that every location within a field of interest (FoI) is covered. Commonly used methods include using mobile nodes to bridge service gaps and probabilistic coverage models [20]. Furthermore, non-deterministic deployment is applied in settings where it is impossible to precisely manage the location of sensors because of things like hostility or inaccessibility. Uneven sensor distribution and coverage gaps may result from this kind of deployment, requiring the use of extra techniques or algorithms to guarantee adequate coverage. To efficiently maintain coverage and connectivity even in uncertain circumstances, it is important to find solutions that can handle the problem of ensuring barrier coverage, where sensors are installed to monitor boundaries against infiltration [21].

2.3.3. Connectivity

In most cases, network connectivity is often ensured but with challenges when non-deterministic deployment strategies are used. The random deployment could result in a higher chance of disconnected nodes; therefore, more sensors are needed or there is more communication overhead to have the wireless sensor network connected. Good connectivity in non-deterministic deployment is desirable [22]. Fast deployment of numerous nodes without perfect placement enhances scalability and is very useful for large and complex systems [20]. It is pointed out that, for instance, in non-determined deployments, how many WSNs interconnect with each other depends on a number of nodes, the range of communication, and the topology of this network. Regarding these kinds of scenarios, research shows that the network mostly includes some isolated nodes and areas with a Giant Connected Component. By analyzing the relationship between node density and communication radius, it was found that the connection increases rapidly within a key communication radius during an interval, which provides a fully connected network. This understanding helps to achieve requisite connectivity levels with high effectiveness by tuning deployment parameter [23].

2.3.4. Environment Suitability

Non-deterministic deployment scenarios often find applications in placing sensors around unexplored land, hazardous urban zones, harsh fields, or disaster-affected areas. In general, the stochastic nature of the places where the sensors land in such a stochastic sensor placement may introduce some difficulty in maintaining proper network connectivity or providing proper coverage [16]. However, non-deterministic policies seem to work well in the harsh conditions of a warehouse deployment. Although it would be necessary to deploy more redundant nodes to achieve complete coverage, this technology is affordable and appropriate for settings where accurate placement is difficult. The network can self-organize itself and adapt in order to effectively cover this type of region [17]. Since non-deterministic systems are more flexible and resilient right from the start than deterministic, they are by themselves more reliable and can handle the. The network can adapt to its environment for any occurrence of an obstacle or alteration in the course of circumstances, since the nodes do not have fixed positions. The ability enables the network to scale since it can therefore work correctly in dynamic environments. Moreover, the random distribution of the nodes has made the net robustly resilient against the failure of nodes because, generally, there are likely to be overlapping coverage areas that will make up for the lost nodes [20].

2.3.5. Energy Efficiency

Energy efficiency is due to the nature of the environment, unexpected and frequently hostile, in non-deterministic deployment scenarios such as harsh fields or disaster zones. In case of random deployment of mobile sensor nodes, the distribution will not be uniform; therefore, this will increase energy consumption by having the nodes move a lot to get the needed coverage and connectivity. To ensure longer operational lifetimes for the sensor network under such demanding conditions, efficient methods are needed to minimize the energy consumed during the deployment phase [9]. In

 doi:10.20944/preprints202505.0438.v1

non-deterministic deployments, energy efficient algorithms also control power usage by scheduling sleep, compressing data, and optimizing routing to increase network lifetime. These tactics guarantee that overall energy usage stays within reasonable bounds even with an increase in the number of nodes [20].

2.3.6. Scalability

It effectively addresses the scalability of non-deterministic deployment in WSNs by studying the spatio-temporal correlations. In this regard, dense deployment of sensor nodes implies strongly correlated observations in both the temporal and spatial dimensions. This relation makes it possible to develop efficient, scalable communication protocols with an increasing number of sensor nodes by using non-deterministic deployment. scalable, energy-efficient, and dependable data transmission across large-scale by taking use of these correlations [24]. Furthermore, the scaling benefits of non-deterministic deployment are significant in harsh environments. These methods entail spreading sensor nodes at random throughout a FoI, which is frequently required for applications including environmental monitoring, military surveillance, and disaster monitoring. Using simulation tools like NS-3, MATLAB, OMNeT++, one can get to the scalability of non-deterministic deployment because it involves evaluation against more than one performance measure: coverage ratio, connectivity, and energy consumption per node. It gives a good idea about understanding scalability in depth and how to maximize it [20].

2.4. Three-Dimensional Deployment

2.4.1. Deployment Cost

Three-dimensional sensor node deployments require more advanced equipment and accurate positioning methods than 2D deployments, the cost of implementing WSNs in 3D environments is much higher. In complicated contexts like underwater monitoring and urban infrastructure surveillance, which need for sophisticated planning and sensor placement procedures to provide optimal coverage and connectivity [25]. In order to manage these increased costs, Nasri and Mnasri [5] stress the significance of cost-effective deployment strategies. This becomes more so in the cases of 3D terrains, where all the costs are incurred in having to partition the region of interest into easy-to-comprehend sub-regions and then calculate the optimum number and positions for the sensor nodes. The relationship of costs comes in with the difficulty of the terrain and how sophisticated algorithms are required to handle uneven topography [26].

2.4.2. Coverage

The coverage problem is making sure that sensor nodes sufficiently cover each point in a 3D sensing field. Huang and Tseng [27] introduced a polynomial-time solution that converts the problem from 3D to 2D and back to 1D space, allowing for quick coverage verification in 3D networks. Watfa and Commuri [28] presented a distributed method to select a subset of operational nodes for full coverage, reducing the number of active nodes required while maintaining thorough 3D coverage. Unaldi and Temel [29] came up with a way to use wavelet transform-based mutation operators and multi-objective genetic algorithms to get the most coverage and network connectivity in 3D environments.

2.4.3. Connectivity

In 3D WSNs installations connectivity is a must for the operation of a network. In order to guarantee connectivity when a truncated octahedron placement technique is utilized, Alam and Haas [30] suggested that the transmission range must be at least 1.7889 times the sensing range. The paper by Fu and Yang resolves this problem by integrating Digital Elevation Model (DEM) data in the construction process to build up a realistic 3D surface model. The greedy algorithm and the DEM probability coverage model are used in this paper to improve deployment strategies even more by

 doi:10.20944/preprints202505.0438.v1

taking into account the effects of signal loss and terrain obstruction. Greedy algorithm is used for optimal placement of nodes, focusing majorly on maximizing coverage but reducing deployment costs. The program will systematically pick places for deployment that would include the maximum number of grid points. The program efficiently treats the intricate data existing in real 3D environments. Results from simulations showed this strategy improved tremendously in terms of the coverage rate and cut computing costs compared to traditional algorithms. The combination of DEM data together with the implementation of such a Greedy algorithm guarantees strong connectivity of the network and effectively overcomes the challenges of 3D terrains [31].

2.4.4. Environment Suitability

To make 3D deployment suitable for WSNs, it is necessary to handle the difficulties presented by complicated topography and provide dependable communication. In their 2014 paper, Unaldi and Temel [29] explored the application of multi-objective genetic algorithms to sensor placement optimization, considering path-loss and line-of-sight factors that are crucial in harsh environment. Saad and Senouci [32] highlights the significance of considering environmental suitability when deploying 3D wireless sensor networks. The authors discuss the intricacies of real-world applications, highlighting that conventional approaches typically depend on idealized environmental conditions that may not yield practical outcomes. The authors present a Bresenham line-of-sight based coverage model that integrates the terrain's structure with actual sensor behavior to achieve a more accurate representation of coverage. This model allows for the re-formulation of the 3D deployment problem by taking into account features like as obstructions, holes, and varying elevation. These factors are essential in selecting appropriate areas for deployment. The method utilizes a multi-objective genetic algorithm that incorporates adaptive and guided genetic operators. These operators are tuned using approaches such as search space reduction and sampling-based evaluation. Extensive simulations confirm that this strategy improves coverage and saves deployment costs. Additionally, it guarantees appropriate sensor placement in locations with diverse and difficult topographies, making it ideal for realistic 3D WSN deployments. To make 3D deployment suitable for WSNs, it is necessary to handle the difficulties presented by complicated topography and provide dependable communication. Unaldi and Temel [29] explored the application of multi-objective genetic algorithms to sensor placement optimization, considering path-loss and line-of-sight factors that are crucial in harsh environment. Saad and Senouci [32] highlighted the significance of considering environmental suitability when deploying 3D wireless sensor networks. The authors address the difficulties that occur in real-world applications, stating that typically, such algorithms rely on idealistic assumptions about the environment and frequently fail to produce realistic results. In this paper, the authors introduce a Bresenham line-of-sight-based coverage model combining the terrain structure with realistic sensor behavior in modeling coverage. This model enables the reformulation of the 3D deployment problem with features such as obstructions, holes, and variations in elevation. All these factors are very important in the choice of areas to be deployed. The approach uses a multi-objective genetic algorithm with adaptive and guided genetic operators. These genetic operators are fitted through reduction of the search space and other sampling-based evaluation methods. Extensive simulations show that this strategy improves the coverage and reduces the deployment costs. Moreover, this approach ensures proper placing of sensors in sites with various and harsh topographies, making it very suitable for realistic 3D WSN deployments.

2.4.5. Energy Efficiency

In 3D wireless sensor networks, energy can be saved by using fewer active sensors while still covering the entire area. Watfa and Commuri [33] developed techniques and algorithms that switch off extra sensors and activate backup ones to fill in gaps when sensors fail. In order to minimize active nodes while maintaining comprehensive coverage, Gou et al. [34] addressed energy-efficient

 doi:10.20944/preprints202505.0438.v1

coverage in 3D heterogeneous networks using 3D-Voronoi partitioning and the K-means algorithm. This allowed the network to operate longer and showed increased sustainability and efficiency.

2.4.6. Scalability

The scalability of WSNs for 3D deployment is enhanced through dynamic coordinate systems and virtual architectures that enable efficient data routing and management of large-scale node collections while maintaining energy efficiency. Watfa and Commuri [33] highlighted the importance of these systems in managing scalability challenges. Reddy and Chandra [35] introduced the 3D-DV-CD algorithm, which integrates Coplanarity Degree (CD) into the traditional 3D-DV-Hop method to improve positioning accuracy and extend coverage by promoting unknown nodes to helper anchor nodes, addressing scalability issues effectively in 3D WSNs.

3. Security Challenge and Solutions

The deployment of WSNs faces significant challenges in security due to inherent limitations in computation power and energy, which make them very vulnerable, problems that include securing the channel or protection against unauthorized access, ensuring the integrity and confidentiality of the data. For instance, Monali et al. [36] discussed multi-tier security that should be integrated into WSNs, strong encryption and authentication mechanisms at the same time. Additionally, Obodoeze [37] discussed how the deployment in sensitive environments, like the Niger Delta oil fields, exacerbates these security issues and calls for practical architectures that address both energy consumption and security threats. Advanced solutions, such as machine learning, have thus been proposed in combating these challenges by enhancing detection with decision-making intelligence and reducing security management costs[38]. According to Saidi et al. [39], game theoretic based approaches can be successfully merged with the cryptographic techniques to handle such DoS attacks and other malicious behaviors, which would provide a comprehensive security strategy. While several security attacks are brought about by the deployment of WSNs, a multi-layer approach, in general, can offer solutions that would be sufficiently robust, facilitated with the assistance of advanced technologies like machine learning and game theory, besides conventional cryptographic methods. After this broad discussion on the general security challenges in WSN deployments, the discussion will be narrowed down to those specific security challenges related to deterministic and non-deterministic and 3D deployment. Each one of these different deployment methods opens into a separate set of vulnerabilities and attack vectors, and requires distinct security measures to ensure network integrity, confidentiality, and availability. Table 2 summarizes some of the latest research works from the years 2023 and 2024, where these security challenges were deeply discussed and many recent advances in this domain are presented.

 doi:10.20944/preprints202505.0438.v1

Table 2. Overview of Research Papers on Security Challenges in Different Deployment Types (2023-2024)

Authors	Date	Deployment Type	Security Challenge Addressed	Proposed Solution
O. Embarak, et al.[41]	2023	Deterministic	DoS (e.g., jamming, resource depletion)	ML-based IDS for DoS detection and mitigation.
A. Bassey, et al[42]	2023	Deterministic	Physical tampering, key compromise	Probabilistic key management using ECC and XOR operations.
A. Boualem, et al[43]	2023	Deterministic	Targeted, unpredictable attacks	Hybrid Fuzzy-Possibilistic model for node scheduling.
A. Khan, et al[44]	2024	Deterministic	Clone attacks, intrusion detection	Aperiodic tiling to create unpredictable sensor deployments.
Medina, F., et al[45]	2024	Deterministic	Coverage holes, network disconnection	Combine deterministic and random deployment for coverage.
H. Bian, et al[46]	2024	Deterministic	Malicious control, data leakage	Situ-Oracle framework using RNN models for secure analysis.
Elsayed et al.[47]	2024	Deterministic	Node capture, tampering, eavesdropping	TD3 with sensor fusion (NCNN) for real-time threat response.
L. Desgeorges, et al[53]	2023	Non Deterministic	Anomalies in SDN control	Dual-controller with ML-based anomaly detection.
S. Sharma, et al[52]	2023	Non Deterministic	General security threats	Dragonfly algorithm for trust-based node security.
P. Arunkumar et al[51]	2024	Non-Deterministic	General Security threats	Bat algorithm with Q-learning for secure routing.
A. Shah, et al[40]	2023	Deterministic & Non Deterministic	DoS: Denial of Sleep	ILSM combining RWM and GWO to optimize routing and energy use.
P. Sebothoma, et al[48]	2023	Deterministic & Non Deterministic	DoS: Denial of Sleep	DSD-RSA algorithm for attack prevention and energy optimization.
V. Prakash, et al[49]	2023	Deterministic & Non Deterministic	General security challenges in WSNs	Bio-inspired ACO and PSO algorithms for secure node placement.
S. Khan, et al[50]	2024	Deterministic & Non Deterministic	Black-hole, gray-hole, wormhole	ANN model to detect and mitigate routing attacks.
S. Suma Christal Mary, et al[54]	2023	3D Deployment	Intrusion, wormhole, IP spoofing	Blockchain-based routing with XOR hashing.
Y. Kim, et al[55]	2024	3D Deployment	Deployment errors	Simulate 3D terrains to improve key distribution robustness.
A. Afghantoloee, et al[56]	2024	3D Deployment	Security challenges in 3D deployment	PO-3DVOR algorithm for optimized sensor placement.
S. Hafeez[57]	2024	3D Deployment	DDoS, spoofing, message injection	Blockchain for secure UAV communication and authentication.

3.1. Deterministic Deployment Security Challenge

Security is inherently more manageable in deterministic WSN deployment due to the planned and controlled placement of the sensor nodes. This structured approach allows the implementation of a predefined protocol of security against the specific locations of nodes, which may be devised in a manner such that each node can be protected adequately from all sorts of potential threats. It

 doi:10.20944/preprints202505.0438.v1

makes the network topology predictable because of the deterministic deployment, which will go a long way in efficient network design. This would, in turn, possibly offer a very good scope for encryption mechanisms, authentication techniques, and intrusion detection systems for effective monitoring and responding to certain areas. Shah et al. also pointed out in this paper that knowledge of the exact positions of the nodes permits network designers to look ahead and mitigate potential security risks-connected with unauthorized access or data interception-through reinforcements on critical points in the network. Thirdly, deterministic deployment makes possible the establishment of more secure communication paths that are less allergic to attacks, given that, with nodes located at fixed positions, routing protocols are allowed to be optimized to ensure both safety and efficiency. The type of attack discussed in this paper is the "denial-of-sleep" attack. Since this type of attack aims at depleting the energy resources of sensor nodes by keeping them away from entering a low-power sleep state, thus exhausting fast and accelerating its failure, the proposed security model would help in sustaining WSN by mitigating such attacks via optimization of routing paths with significant improvement in energy efficiency at each node [40]. As discussed by Abu Said [41], the case of deterministic deployment regarding WSNs in the context of Industry 4.0 faces specific security problems, especially regarding the protection against Denial-of-Service attacks. It is easier for attackers to take advantage of the network predictability by searching for specific nodes as potential targets inside a deterministic setup-that is to say, sensor nodes are placed in known, fixed positions-in order to mount DoS attacks based on jamming, resource depletion, or selective forwarding. Deterministic deployment is highly structured and predictable; therefore, it is more susceptible to this kind of attack because finding and dislocating crucial nodes becomes simple for any adversary. This stresses the need for a strong intrusion detection system (IDS), built on machine learning techniques for monitoring and scrutinizing patterns in network traffic. These systems can detect and mitigate DoS attacks by incorporating learning units in space and time; hence, this provides the WSNs deployed in deterministic patterns with unparalleled security. This approach provides a scalable and resilient solution that would guarantee the integrity and availability of industrial networks against potential cyber threats. This, however, leads to huge security implications in a deterministic deployment where sensor nodes are placed at strategic, pre-determined positions within WSN, opening adversaries that might physically tamper with or target nodes to damage the network in that predictability in node positioning. The importance of robust key management systems in mitigating such risks has been highlighted in Bassey et al. [42]. The proposed model relies on a probabilistic key management approach, which introduces randomness into the generation and distribution of keys, making it more secure since attackers cannot predict or intercept communication. Moreover, elliptic curve cryptography (ECC) plays a major role in the key management process and, hence, reinforces security to such an extent that even when an attacker has compromised components of the network, he or she would have a very hard task trying to reverse-engineer the keys in use. As such, this balances the solving of inherent security challenges of deterministic deployment pertaining to both computational efficiency and robust security. Adda et al. [43] proposed the solution targeted to enhance security in deterministic deployments of WSNs leverages the predictability of node placement to realize robust strategies for coverage while mitigating security risks. This is achieved by optimizing a hybrid Fuzzy-Possibilistic model for node scheduling and state transitions to ensure that only the bare minimum number of nodes SB needs to be active at any instant of time to accomplish coverage and connectivity. It employs fuzzy logic and possibility theory to model uncertainties in node energy reserves and communication capabilities to guarantee the integrity of the network against possible security threats. The model considers the problem of finding the optimal set of nodes to activate, considering the trade-off between energy efficiency and spatial coverage. In such a way, it minimizes the likelihood for an adversary to successfully target critical nodes, enhancing network security. Besides, in its adaptability to changes in the environment, the network becomes resilient against disruptions caused by both external attacks and internal failures. Deterministic node deployment followed by grid patterns such as square, hexagonal, or triangular

 doi:10.20944/preprints202505.0438.v1

layouts. In particular, an attacker can easily exploit the predictability of the sensor placement in deterministic deployments to map out sensor positions without much ado; hence making any planned attacks-from clone and selective forwarding to others-easier to carry out. Ayaz and Gabe [44] enhanced security by including aperiodic tiling, which brings both complexity and randomness into the sensor deployment and thus increases distinctive difficulty for attackers to predict sensor positions in order to effectively compromise the network. In fact, deterministic deployment of nodes in WSNs has great importance for the subsequent security and reliability of Industrial Internet of Things (IIoT) systems under extreme conditions, such as [46] underground mining. According to Medina et al. ¸iteMedina2024, deterministic deployment involves an intentional placement of sensor nodes at fixed predefined positions within the mine, for example, at tunnel crossings and changes in slope and work faces. That would be useful, because this approach would imply having the main advantages in terms of full control of coverage and connectivity, often highly required in monitoring hazardous environments such as underground coal mines due to the presence of explosive atmospheres. The deterministic approach provides increased security since it would be less likely for coverage holes to occur, while at the same time connectivity within the sensor network is assured-even against the failure of sensor nodes. By carefully considering node placement, both the network covers optimally using a minimum number of sensors; that itself minimizes cost and actually simplifies the deployment process. Moreover, with this approach, every critical area is monitored continuously giving early warnings and hence minimizing the risk of explosive gases. This study emphasizes the integral deployment strategy while integrating the deterministic deployment with random deployment methodologies in satisfying the complex mine environments with different coverage and connectivity requirements while increasing the general safety and efficiency of the monitoring system. Because of predefined location of deterministic deployment, it would also enable thorough control over the network topology critical to mitigation against such fundamental security risks as coverage holes and network disconnections. As Bian et al. [46] discussed in their paper, in turn, pre-planning locations of sensor nodes reduces the possibility of adversaries easily identifying and accessing weak points in the network. This allows for the integration of robust security mechanisms, for which the uniform structure of the network makes encryption, authentication, and routing mechanisms easier to apply. It naturally follows that the regularity of a deterministic approach in deployment enhances WSN resilience against physical tampering and cyber-attacks, enabling a more secure and reliable network infrastructure. In this regard, deterministic deployment in WSNs requires security to be paramount, especially when nodes must be placed at pre-determined positions and most vulnerable to specially targeted attacks. Based on the algorithm proposed in the referenced work integrating Twin Delayed Deep Deterministic Policy Gradient (TD3) with Nvidia Convolutional Neural Network (NCNN), this paper proposes that it can be adapted for deterministic deployment security enhancement. By leveraging TD3 that refines decision-making in real-time, it can make dynamic adjustments against potential threats, thereby making it hard for attackers to potentially exploit known deployment patterns. On the other hand, a sensor fusion technique adopted by the combination of data from multiple sensors such as the Camera and LiDAR provides a more comprehensive environmental understanding and, hence enables the detection of anomalies and unauthorized activity that compromises the network. In this respect, this real-time adaptability combined with multi-sensor data fusion enhances deterministic deployment for security and makes such a network resilient to various attacks, even if the strategy of its deployment is known [47]. Sebothoma et al. [48] produced an algorithm called DSD-RSA that does well in structuring the nature of the network in deployments that are deterministic, with the sensor nodes being deployed according to a certain kind of plan. With the placing of nodes at exact locations, the algorithm must execute proper resource management and establish secure channels of communication. A full predictable layout allows it to use the S-MAC protocol in a manner that optimally coordinates sleep cycles on nodes to avoid unnecessary energy consumption. Furthermore, in this manuscript, AES and RSA are used so that data transmission is secure and reliable, as encryption and key management

 doi:10.20944/preprints202505.0438.v1

are performed according to the consistent topology of the network. This methodology increases the resiliency of the network against Denial of Sleep (DoSL) attacks and enhances the overall performance with reduced latency and high throughput according to a controlled deployment scenario. In the case of WSN deterministic deployment, sensor nodes are deployed at strategic locations to ensure optimal coverage and connectivity. The paper by Prakash et al. [49] discussed various bioinspired optimization techniques that could be used to further optimize the node placements at their optimal locations in a deterministic deployment, such as Particle Swarm Optimization (PSO) and Ant Colony Optimization (ACO). It aims at leveraging deterministic deployment's structured nature in optimizing network performance for the determination of the location of each node to attain maximum coverage with minimum energy consumption. The predictable node layout allows easier implementation of security protocols since the network topology is known and can be factored into the design of secure communication pathways. Deterministic deployment allows for an environment where the usage of bio-inspired techniques guarantees high levels of network security while ensuring optimality in the use of resources, subsequently ensuring that the network remains resilient against possible security threats. According to Khan et al. [50], in deterministic WSN deployment, sensor nodes are deployed according to a predefined pattern, such as grid or hexagonal configurations, sometimes driven by needs linked to the environment where sensors will be deployed. On one side, this kind of deployment surely grants the best coverage and connectivity possible; on the other side, there is some security vulnerability that an attacker can exploit. The main threats towards security include predictability in node location that may enable adversaries to strategically attack, such as physical tampering or capture, which compromises critical data, or even insert malicious nodes into the network. Deterministic deployment may also be more susceptible to routing attacks such as the sinkhole or wormhole attacks, where an adversary leverages the predictability in node deployment to compromise routing decisions. Various security mechanisms have been presented in the literature to mitigate these threats: robust authentication protocols, intrusion detection systems, and secure routing techniques have been designed to compensate for the weaknesses brought about by deterministic deployment. In fact, Artificial Neural Networks (ANNs) has been used in the improvement of anomaly detection and securing the communication paths in deterministic WSN by adapting to the predictable nature of the network topology and identifying deviations which could indicate an attack.

3.1.1. Conclusion

While deterministic deployment has many advantages, such as controlled node placement in WSNs and optimized network design, it has also unique challenges in terms of security. Predictable node locations improve efficiency in routing and energy management but make the network prone to certain types of attacks, including Denial-of-Service, physical tampering, and routing attacks. These threats arise since the mapping of topology and the selective destruction of critical nodes are pretty easy to be performed by adversaries. However, this risk can be mitigated through appropriate security protocol deployment: encryption, intrusion detection system, and key management techniques-benefiting from the structured nature of deterministic deployments. Other more resilient techniques for dealing with possible cyber threats in deterministic deployments include aperiodic tiling, bioinspired optimization, and machine learning-based intrusion detection systems. Deterministic deployment leads to higher exposure in certain types of vulnerabilities, but with the right security mechanisms in place, it can guarantee a much secure and more efficient WSNs.

The analyses done on deterministic deployment in WSNs have shown certain interesting trends during the years 2023 and 2024 that shows in Figure2 . In the year 2023, there were 3 papers solely focused on deterministic deployment, and an equal number of papers using both the deterministic and non-deterministic approaches under the method of deployment. This hence means that, within this year, the researchers were indeed looking into the advantages of both planned and hybrid deployment strategies. In deterministic deployment, sensor nodes are placed in a pre-planned structured manner;

 doi:10.20944/preprints202505.0438.v1

hence, more control over network topology is manifest, and hence, addressing several challenges-security, energy efficiency, and connectivity-can be much more easily achieved. By 2024, interest had grown for deterministic deployment, since now 4 papers focused on this topic. On the other hand, papers discussing both approaches totaled only 1 in that year, indicating perhaps that work was narrowing to more pure research on deterministic methods. This might denote the strength of the deterministic method of deployment strategy, since it develops a regular network topology that can be optimized for security protocols, intrusion detection systems, and energy conserving techniques. The increasing interest in deterministic deployment reflects the relevance of the latter to applications whose operative necessities include network reliability, efficiency, and security. In such a context, deterministic approaches can turn out to be an essential solution to increase the scalability and robustness requirements imposed by different industries on evolving sensor networks, ranging from environmental monitoring and industrial automation up to healthcare. These upwards research trends could be indicative that deterministic deployment will play a determining role in the near future regarding WSN design and implementation.

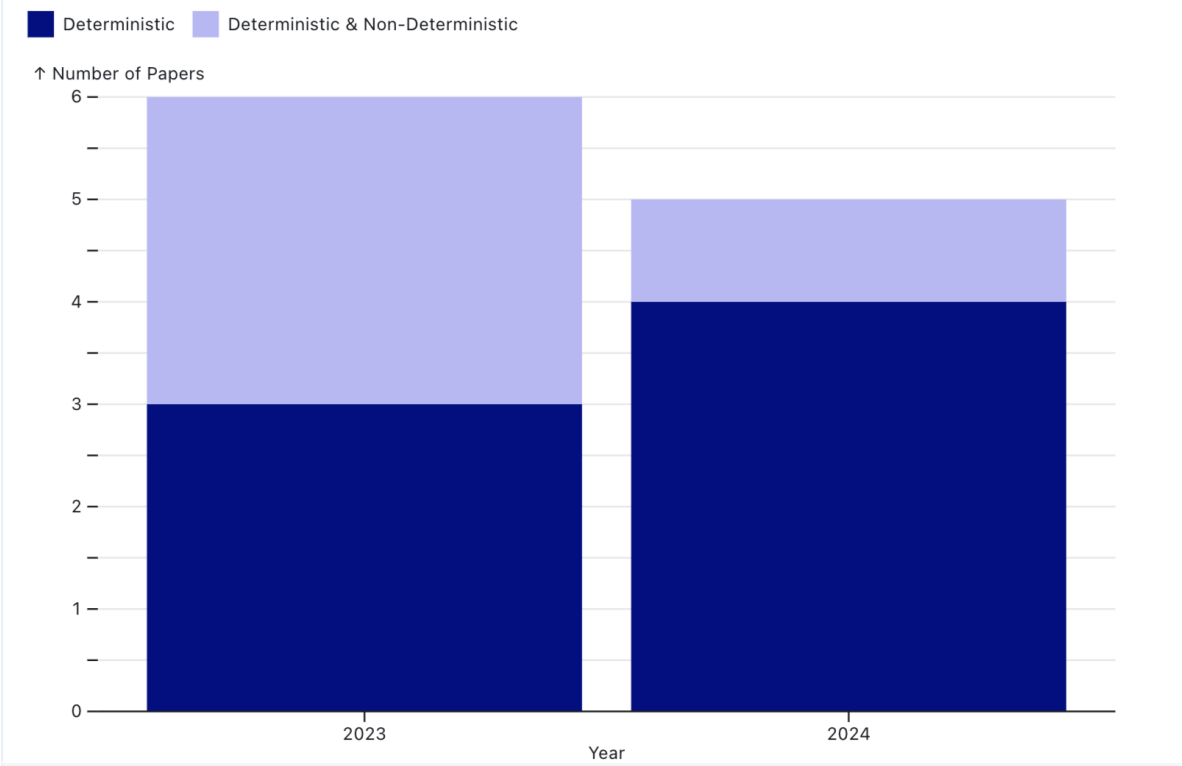

Figure 2. Number of Papers for Deterministic Deployment for 2023 and 2024

3.2. Non-Deterministic Deployment: Security Challenge

In contrast to deterministic deployment, non-deterministic node deployments are an even more challenging task for network efficiency and security because of their random manner of placing sensor nodes. Sebothoma [48] proposed that in such scenarios the algorithm DSD-RSA will adapt, showing elasticity in securing a network even when node placement cannot be accurately predicted. The algorithm seeks to conserve power with no compromise in protection against DoSL attacks using the S-MAC protocol by varying the sleep cycles according to the real-time conditions. More specially, the use of AES and RSA mechanisms for data encryption and key exchange is very essential in this aspect, which maintains data integrity and confidentiality in a dispersed and irregular topology network. This flexibility makes the DSD-RSA algorithm a competitive candidate in nondeterministic WSN security, where conventional security measures could be inflexible. The paper by Prakash et

 doi:10.20944/preprints202505.0438.v1

al. [49] addressed these challenges by employing bio-inspired approaches such as ACO and PSO, which are designed to optimize the network despite the randomness. For security, non-deterministic deployments require robust algorithms that can adapt to the irregular distribution of nodes to ensure secure data transmission and efficient energy use. The paper highlights that Swarm Intelligence techniques, particularly ACO and PSO, are effective in optimizing these networks by enhancing coverage and connectivity while simultaneously maintaining security. These algorithms dynamically adjust to the network's topology, allowing them to respond to potential security threats like data breaches or attacks that exploit the random placement of nodes. The proposed solution by Adda et al. [43] addressed intrinsic uncertainties with the node placement so as to effectively secure the network for nondeterministic deployments in WSNs. As a matter of fact, a hybrid Fuzzy-Possibility model such as that proposed in this paper is best for such an environment where the exact position and status of sensor nodes cannot be predicted. This model performs dynamic scheduling of active and passive states of nodes using a fuzzy logic-possibility theory combination to enable the network to dynamically adapt to ever-changing environmental conditions and their potential threats. In this model, a probabilistic decision-making process is used in choosing the most reliable nodes for activation that can guarantee continuous coverage while reducing any possibility of coverage holes or weak points that may be used by the attackers. Moreover, the flexibility of the model in applying uncertainty provides a robust solution for non-deterministic deployment because it can adapt to changes in network topology and maintain the network even when there will be unpredictable environmental factors. This approach does not only protect the network against potential intrusions but also prolongs its lifetime through energy consumption optimization across the network. Non-deterministic deployment means tasks are complex to manage where the placement of sensor nodes is random or semi-random. It discusses that such node placing, being highly unsure, may lead to non-uniform coverage and hence introduce some vulnerabilities, like sensing holes, into the system that can be compromised by adversaries. This is because the fixed topology of the network demands runtime adaptive security measures to dynamically alter their decisions against changes in conditions and potential threats. For instance, optimization techniques like Grey Wolf Optimization (GWO) need to be integrated for enhancing security while carrying out non-deterministic deployments, as routing paths and node movements for better management to reduce vulnerabilities will be facilitated. Adapting to node distribution according to a random process, this automatically will demand the use of robust encryption and authentication protocols that can work optimally under network topology uncertainties. The paper points out that the prime essentials in keeping the network resilient against attacks-when node position and connections are not predetermined-develop security strategies that can adapt to non-deterministic deployment uncertainties [40]. The security of non-deterministic deployment in Software-Defined Networking (SDN) is particularly challenging due to the inherent unpredictability in the control plane's decision-making process. Desgeorges et al. [53] proposed a dual-controller architecture to enhance the security of SDN by detecting anomalies in the non-deterministic decisions made by the primary controller. The architecture consists of a nominal controller responsible for network operations and an observer controller that monitors the primary controller's activities to identify any anomalies. The anomaly detection process involves evaluating the likelihood of decisions using machine learning algorithms such as Probabilistic Finite Automaton (PFA), Hidden Markov Models (HMM), and Recurrent Neural Networks (RNN). These algorithms assess both the performance and the structure of decisions, allowing for the detection of deviations from expected behavior. This approach helps in mitigating risks associated with malicious attacks that exploit the non-deterministic nature of SDN control planes, ensuring a more robust and secure network environment. Sharma et al. [52] analyzed some of the security challenges and their solutions in the case of non-deterministic deployment in WSNs. In the nondeterministic deployment method, sensor nodes are scattered all over the target area in a random way, which may lead to irregular coverage. As there is no predetermined placement of nodes, it attracts more security threats. Based on this, the authors propose the Dragonfly Algorithm, which

 doi:10.20944/preprints202505.0438.v1

will enhance the security of wireless sensor networks by emphasizing trust management among nodes. This approach evaluates node and route reliability in the network to avoid the malicious activities of fictitious data injection and node compromise, usually occurring in non-deterministic deployment. The proposed model, therefore, uses machine learning and swarm intelligence to adapt dynamically to changes in the network for better security and lifetime of the network. Arunkumar [51] proposed the Modified Bat-Q-learning algorithm, considering major challenges of secure and accurate node localizations in the nondeterministic deployments of WSNs. The modified bat algorithm applies to optimize node placements for better localization accuracy, while Q-learning introduces a state-action-reward mechanism to efficiently locate nodes as well as ensuring secure communication. This approach exploits the natural behavior of bats in optimizing and allows a faster convergence toward the optimal solutions that extend the network's lifetime. The combined usage of MBQ further provides enhanced energy efficiency along with secure routing, especially in those scenarios where random node deployment is done without any predetermination of node positions. The experimental results show that the proposed MBQ algorithm performs better compared to existing techniques on packet delivery rate, latency, energy consumption in network lifetime. Non-deterministic deployment of WSNs, where sensor nodes are spread randomly or dynamically in the target area, involves different security issues compared to deterministic deployment. Khan et al. [50] addressed that the randomness of node placement strengthens the resistance of the network to some assaults that are predictable, like those against particular nodes depending on their location. On the other hand, this type of deployment strategy brings about a more difficult network topology to handle and secure. In particular, the most vulnerable attacks against routing protocols are black-hole or gray-hole attacks, where compromised nodes advertise themselves as an optimum path attracting traffic and then discard or alter the data. Herein, the uncertainty and non-predictability of node locations in non-deterministic deployments make the application of traditional security measures challenging since network topology may change very frequently. To address these challenges, several sophisticated security schemes, based on machine learning methodologies such as ANNs, have been developed. These methods learn and adapt in the dynamic nature of a non-deterministic WSN. The protocol will be empowered with robust solutions against the detection and mitigation of routing attacks through continuous monitoring of network traffic. Additionally, it will be capable of identifying anomalous behavior that might indicate potential infringements in security.

3.2.1. Conclusion

The deployment of a WSN in a non-deterministic manner may lead to many serious security issues, since it is not predictable exactly where these nodes would lie after their deployment. The randomness in deployment will make the network prone to several vulnerabilities, such as coverage gaps resulting in an increase in feasibility for several types of attacks like DoS, black-hole, and grey-hole. However, innovative solutions using bio-inspired optimization algorithms such as ACO and PSO, and the application of robust protocols of encryption help attenuate these challenges by dynamical adaptation to the irregular topology of the network. Other advanced techniques involve intrusion detection systems based on machine learning and hybrid models, among them Fuzzy-Possibilistic, approaches that amplify the security with efficiency in non-deterministic deployments. The solutions make sure that WSNs can work in environments that are hard to predict. They do this by using a mix of flexible and adaptive security strategies. This makes the network last longer without interruptions by protecting the data integrity and privacy.

The research on non-deterministic deployment in WSNs presents a remarkable turn of the tide of interest from 2023 onwards. This year, there are 3 papers strictly devoted to non-deterministic deployment; the other 3 papers address both the deterministic and non-deterministic strategies that shows in Figure 3. Non-deterministic deployment features the random or probabilistic distribution of nodes. It is usually preferred because of its flexibility, especially in dynamic environments, where pre-

 doi:10.20944/preprints202505.0438.v1

planned deployment cannot be made effectively or involves too much cost. Considering that in 2023, an increasing amount of research is being done, one can say that the deployment strategy will adapt to completely unpredictable scenarios by offering solutions for ad-hoc networks, large-scale environmental monitoring, or disaster recovery situations. However, the research focus on non-deterministic deployment appears diluted in 2024. There was only one paper solely focused on nondeterministic deployment, and similarly only one examining the combination of deterministic and nondeterministic approaches. This fall may mean that researchers are developing a taste for more regularized methods of deployment or perhaps maturation of research in the nondeterministic techniques whereby major challenges like coverage, energy efficiency, and security have already been adequately addressed. With a lower number of papers, non-deterministic deployment retains importance in scenarios where flexibility and adaptability are needed-for example, when node placement for environmental parameter monitoring is neither feasible nor effective. Ongoing investigations, though at a lower pace, on hybrid deployment methods that combine deterministic with non-deterministic approaches would hint at the fact that non-deterministic strategies are still considered complementary to the more controlled ones for the purpose of ensuring maximum coverage while reducing vulnerabilities. Non-deterministic deployment is most likely to remain relevant as the WSN technology evolves, in areas that require rapid deployment and dynamic adaptability.

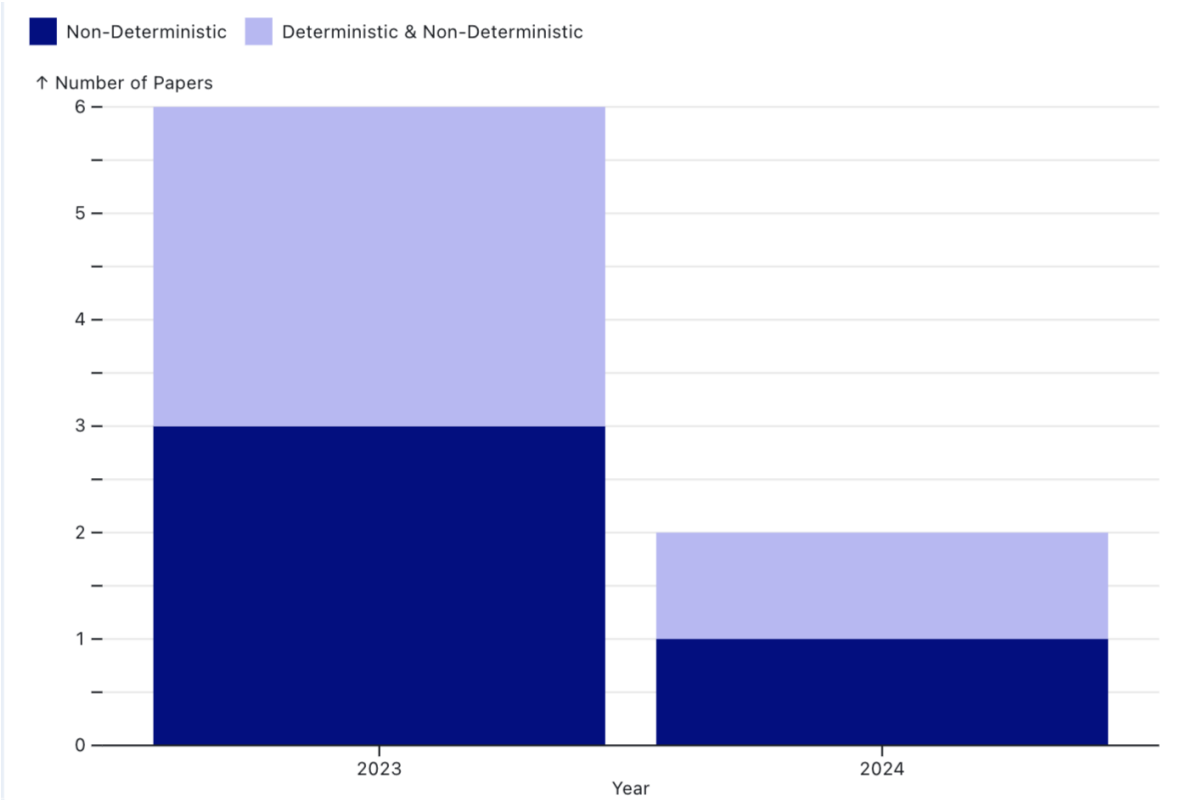

Figure 3. Number of Papers for Non-Deterministic Deployment for 2023 and 2024

3.3. 3D Deployment Security Challenge

Mary et al. [54] addressed the security challenges of 3D deployment in WSNs, proposing an innovative framework using blockchain technology to secure data routing across the network. The network manages its complex 3D topology by using Voronoi cell architecture with dynamic and uncertainty principle-based secured selection of mobile cluster heads. These cluster heads provide stability to the network and establish secure communication between sensor nodes and the base station. Due to the use of a lightweight XOR-based hash function, data packets are securely routed and encrypted in such a way that it makes the sensor network resistant to several types of attacks,

 doi:10.20944/preprints202505.0438.v1

even those against its own 3D structure. The use of blockchain enhances security through the tamper-proof record of all exchanges of data to prevent unauthorized access and maintain network integrity operating in a 3D environment. This approach enhances the overall security of the network and provides the highest energy-efficient consumption, hence prolonging its life. Kim et al. [55] proposed a new approach to enhance the security set in 3D deployment environments of WSN by addressing one of the most impactful factors of deployment errors on location-based pairwise key predistribution protocols. For evaluating the occurrence of deployment errors due to real-world terrains-like hills and mountains with physical factors like gravity and air resistance, the authors propose a detailed simulation framework. This study analyzes the performance of some important key predistribution protocols under these conditions and identifies some critical environmental factors which can minimize deployment errors and subsequently improve network connectivity and security. It highlights that solution schemes in the deployment phase must consider 3D terrain features and other external physical factors for key predistribution to be resilient against potential security threats in non-deterministic large-scale WSN deployments. The PO-3DVOR algorithm enhances the security of 3D deployment through a purpose-oriented weighted coverage (PWC) estimation, which considers sensor visibility, environmental obstacles, and legibility of the space to make an optimal sensor placement for a security threat in an area where coverage is most critical. The deployed network is further made secure by the algorithm through a movement strategy inspired by adjusting sensor positions in relation to their proximity to obstacles and the need for coverage in low-legibility areas. The effectiveness of this algorithm in adapting to complex 3D environments-with its focus on maximizing coverage-thereby assures it of enhancing security for multitype sensor networks [56]. In her thesis, entitled "Blockchain-based Secure Unmanned Aerial Vehicles (UAV) in Network Design and Optimization," Hafeez [57], proposed a blockchain-based solution to improve the security of 3D Deployments of UAVs through blockchain for the solution of natural vulnerabilities within the UAV Networks. Currently, she has presented a framework known as BETA-UAV in her thesis, which utilizes the cryptography and immutability features of blockchain for securing communication and data transmission in UAV networks. This is particularly effective in 3D deployment, since the complexity and openness of such an environment make the network more vulnerable against some sort of attacks, mainly Distributed Denial-of-Service (DDoS), spoofing, and eavesdropping. The implemented blockchain within the BETA-UAV further ensures that all transactions and communications within the UAV network are securely recorded in a tamperproof ledger, enabling secure authentication and integrity of data, making it resilient to cyber threats. Thus, this can critically enhance the security and reliability for 3D UAV operations.

3.3.1. Conclusion

Eventually, 3D deployment in WSNs opens very special security issues due to the complexity of the environment. However, novel solutions reside in blockchain technology, key predistribution protocols, and advanced algorithms that befit the mitigation of these risks. Mary et al. [54] suggested a blockchain-based system that protects data routing from tampering with simple XOR-based hash functions and built-in security through Voronoi cell architecture. Kim et al. [55] talked about how important it is to think about physical factors like terrain in 3D environments. This makes sure that key predistribution protocols are resilient against mistakes that could happen during deployment. The PO-3DVOR algorithm develops the heuristics of sensor placement further, considering changes due to obstacles in the environment. Simultaneously, blockchain-based solutions, such as BETA-UAV, provide robust security to UAVs in their deployments within 3D spaces. All these techniques ensure secure communication of data with integrity and resilience against cyber threats at all levels, thereby enhancing the security and dependability of 3D WSN deployments. Research on 3D deployment in WSNs shows an increasing trend of interest in the advanced deployment strategy from 2023 to 2024 that shows in Figure 4. While in the year 2023, only one paper reported 3D deployment, hence, it was

 doi:10.20944/preprints202505.0438.v1

relatively in the infancy stage. In 2024, however, it has risen to 3 papers, indicating clear attention and recognition of advantages by researchers towards 3D deployment in WSNs. In this respect, 3D deployment of sensor nodes in a three-dimensional space rather than on the traditional 2D plane can bring a wide advantage when coverage and connectivity come at stake in very lengthy scenarios beyond flat surface environments. This kind of deployment finds great relevance for scenarios such as multi-story building monitoring, underwater networks, aerial systems, and complex industrial or geological environments where the traditional 2D methods might fall short. This can be evidenced by the increased trend of research outputs, ranging from 2023 to 2024. In fact, 3D deployment is presenting a feasible solution that can enhance coverage and network performance in difficult environments. It deploys all the spatial dimensions in the efficient deployment of sensors, which improves connectivity and affords more flexibility in handling node coverage challenges, communication reliability, and energy efficiency. As WSNs are being extended to more sophisticated application scenarios, three-dimensional deployment is at the point of view of a researcher while optimizing network design for real-world, three-dimensional environments.

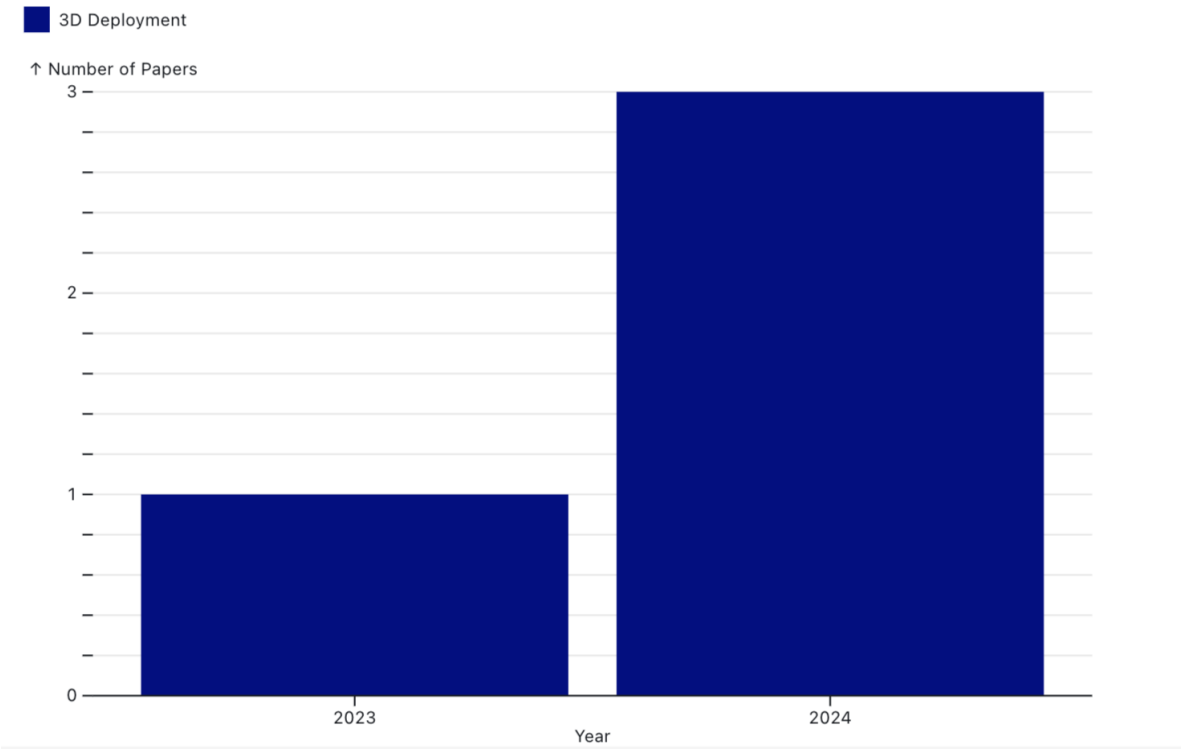

Figure 4. Number of Papers on 3D Deployment for 2023 and 2024

4. Sensor Node Types

Knowing the various types of sensor nodes in WSNs is important for understanding how and why they might be deployed and operated. The basic elements of WSNs, called sensor nodes, are by nature very different and have specific functions and capabilities within the network [1]. Sensor nodes differ by several orders of magnitude concerning their power consumption, computational capacity, and communication range. Generally, they are designed to perform specific tasks such as sensing, data processing, and communication [58]. As defined by Mhatre and Rosenberg [4], homogeneous sensor nodes have the same configuration in hardware and software, thus ensuring predictable performance across the network as well as ease of design and management. Heterogeneous sensor nodes, on the other hand, consist of some advanced and some normal nodes with a wide range of resources—a better microprocessor and more memory. This allows them to offload processing duties that would otherwise wear down the network, increasing its longevity and reliability [69]. Both homogeneous

 doi:10.20944/preprints202505.0438.v1

or heterogeneous, these sensor nodes must be strategically deployed in order to optimize network coverage, connectivity, and energy efficiency. This will allow different applications, like military surveillance and environmental monitoring, to have their unique needs met [70]. Recognizing these differences facilitates the design of reliable and effective WSNs that are suited to a range of operational needs [72]. A detailed look at the differences between homogeneous and heterogeneous networks is shown in Table 3. The table also explains the standards used to group different kinds of sensor nodes in WSNs.

Table 3. Comparison of Homogeneous and Heterogeneous Networks

Aspect	Homogeneous Network	Heterogeneous Network
Definition	Nodes have the same function and are interchangeable	There are two or more classes of nodes categorized by both function and utility
Connectivity	Optimized by equal node degrees, long girths, and short path-sums, ensuring efficient and stable communication	Enhances connectivity with low-power nodes within a macro cell network, reducing dead zones
Energy Efficiency	Limited by uniform energy consumption across all nodes, leading to early power depletion in some nodes	Utilizes nodes with varying energy levels, extending network lifespan and reducing energy consumption by 40%
Node Composition	Nodes with identical hardware and software configurations, ensuring uniform performance. Identifying key nodes is crucial for network stability, using diverse evaluation methods	Includes normal nodes (resource-constrained) and heterogeneous nodes (enhanced resources), improving reliability
Node Deployment	Identical nodes deployed deterministically or randomly to ensure adequate coverage and connectivity	Strategic placement of stationary and mobile nodes to optimize coverage and network lifetime

4.1. Homogeneous Networks

Homogeneous networks have nodes that perform the same function within them. Each user is interchangeable with the next, in terms of the basic tasks they carry out. For example, every phone in a landline network serves essentially the same purpose as every other, and most people buy telephones for similar purposes. Broadly speaking, the networks used for telecommunications are often homogeneous [59].

4.1.1. Communication

Homogeneous networks do have inherent structural features that maximize communication within them. To explain this in greater detail, homogeneous networks are intended to provide maximal synchronization and robustness against attacks by maximizing node degrees, girths, and short path sums. Improved synchronizing capabilities and robustness show that this kind of structural uniformity does allow effective and stable communication across a network. Because of these characteristics, homogeneous networks are especially useful for applications like brain-network research and information transmission in social networks that require for dependable and persistent communication routes [60].

4.1.2. Energy Efficiency

Homogeneous network often suffers from the problem that all nodes have uniform energy consumption in order to improve energy efficiency, making farthest nodes from the Base Station die

 doi:10.20944/preprints202505.0438.v1

prematurely. Thus, the energy efficiency is of concern in this case due to the uniform capabilities of all the sensor nodes with limited battery capacity. Among these techniques, arguably the most popular method applied to enhance energy efficiency is the Low Energy Adaptive Clustering Hierarchy (LEACH) protocol. In effect, LEACH basically organizes sensor nodes into clusters and selects a cluster head with the help of a probabilistic approach; later, this cluster head collects the data and transmits it to the base station. Although there are advantages of a homogeneous system in LEACH, it still has inefficiencies with respect to energy use. This is because every node consumes energy at an equal rate, resulting in a uniform depletion of energy resources throughout the network. Therefore, it is crucial to develop energy-efficient protocols that limit energy usage and extend the lifespan of homogeneous network in order to ensure their effectiveness [66]. Vipan and Ankit [68] proposed a new method of making homogeneous networks more energy efficient. They suggested the selection of a cluster head most suitable for them by using the Artificial Hummingbird Algorithm in its place. Started with the perception of various aspects like residual energy, intra-cluster distance, and balanced cluster formation, MAHA-EECHS can effectively extend the total lifespan of the network by reducing average energy consumption. It has been noticed that the MATLAB simulations showed MAHA-EECHS performance superior to the current algorithms in terms of energy efficiency and life span of the first node in the network.

4.1.3. Node Composition

In a homogeneous network, all nodes usually make up the node composition with the same hardware and software configurations. Having nodes that are identical in sensing, processing, and communication means that it can work at constant performance. The consistency that comes with this makes the designing, managing, and optimizing of a network easier since one is able to predictively control the behavior of nodes and usage of resources. Homogeneous networks ensure consistency in data gathering and processing, which is particularly useful in applications like surveillance and environmental monitoring [61].

4.1.4. Classification of Critical Nodes

Understanding and controlling the stability and functionality of networks means finding their critical nodes in homogeneous networks. Important nodes are very powerful; removing an important node could harm the network. There are a variety of ways to consider these critical nodes, but this can be categorized into five aspects: node operations, node feature vectors, node neighbors, node-to-node paths, and multiple indications. All proposed methods have a special advantage and peculiar challenges. Central nodes in homogeneous networks can be used in a variety of ways, such as epidemic management, rumor mitigation, strategic marketing, and basic protein discovery. The protection of these critical nodes enhances the reliability and overall stability of the network [62].

4.1.5. Node Deployment

The deployment of nodes in homogeneous networks is very important to achieve full coverage and connectivity in WSN. All the sensor nodes in these networks have the same functionality/characteristics and are deployed in such a way as to optimize both area coverage and network performance. The deployment tactics may be either deterministic or random, depending on the application and the environmental requirements. On the other hand, random deployment scatters nodes in the area of interest in an unbiased manner, causing most of the time, voids created in the network and a possible imbalance of the number of nodes. For instance, deterministic deployment can be done by arranging nodes either in a regular grid or a triangular lattice, while not varying from a given configuration. The idea behind efficient deployment is that the number of nodes should be kept to a minimum subject to constant sensing of full coverage and connectivity, thereby optimizing energy consumption and hence increasing the lifetime of the network. Determining their placements

 doi:10.20944/preprints202505.0438.v1

in such a way that no region is left uncovered at any time and the network works at all times requires much more sophisticated methods for efficient deployment, including force-based and grid-based procedures [63].

4.2. Heterogeneous Networks

A heterogeneous network comprises two or more classes of nodes, which are categorized based on the utility and function. The nodes perform different functions as opposed to homogeneous networks. One good case is the Honeybook marketplace network whose event planners, photographers, and florists reveal different behaviors. Similarly, the eBay's network serves buyers and merchants for fundamentally different purposes. The network's adaptability and robustness are improved by this diversity; however, it also introduces complication in optimization and management [59].

4.2.1. Communication

A heterogeneous network (HetNet) is a traditional macro cell network that has different kinds of low-power nodes (LPNs) dispersed within it. These LPNs, like micro base stations, pico eNBs, home eNBs, and distributed antenna systems, improve connectivity by reducing dead zones and traffic hotspots through targeted coverage. This deployment method guarantees a network that is both efficient and robust, thereby addressing the exponential increase in mobile data traffic demands [64]. Singh and Chand [65] presented a multilevel heterogeneous network model to improve communication efficiency in WSNs. In this model, multiple levels of node heterogeneity are allowed; each level corresponds to different energy capacities of the sensor nodes. It is possible to make the HEED (Hybrid Energy-Efficient Distributed) clustering protocol work with a multilevel structure, which makes communication better in this mixed network. In the process of making a clustering decision, it puts into consideration node residual energy, node density, average energy, and distance to the base station. By this, it ensures that the cluster head is picked on the basis of all these factors, hence efficiency and reliability in communications. The approach not only balances the dissipation of energy across a network, thus avoiding energy holes, but also greatly extends the lifetime of a network by reducing the energy dissipation rate with increasing heterogeneity. Another way this model achieves effectiveness is through the use of fuzzy logic in refining the choice of cluster heads for improved data aggregation and transmission efficiency.

4.2.2. Energy Efficiency

In comparison to homogeneous systems, heterogeneous network significantly extend the network's overall lifespan and reduce energy consumption by about 40% by utilizing nodes with varying energy levels and capabilities, such as advanced nodes with higher initial energy. The research authored by Saravanakumar and Susila [66] demonstrates a noteworthy enhancement in the energy efficiency of heterogeneous WSNs as compared to homogeneous systems. The authors suggest an improved iteration of the Low Energy Adaptive Clustering Hierarchy (LEACH) protocol, referred to as LEACH-Heterogeneous. This strategy involves the inclusion of nodes with different starting energy levels, where a certain proportion of nodes (10% in this investigation) have higher initial energy relative to the rest of the nodes. The simulation findings indicate that the use of this mixed architecture can enhance energy efficiency by up to 40% and prolong the lifespan of the network. The LEACH-Heterogeneous protocol enhances energy efficiency by dynamically forming and re-forming clusters based on the remaining energy of nodes. This strategy efficiently minimizes energy usage and extends the lifespan of the network by optimizing the utilization of high-energy nodes. This results in a more even distribution of energy and a decrease in overall energy consumption. Purkar and Deshpande [67] proposed an energy-efficient, cluster-based protocol for heterogeneous WSNs; it is called EECPEP-HWSN. This new approach has been proposed to enhance the energy efficiency, stability, and network lifetime of HWSNs themselves by using three levels of sensor nodes: normal, advanced,

 doi:10.20944/preprints202505.0438.v1

and super nodes. During the cluster head selection process, parameters such as initial energy, hop count, and residual energy of the nodes are considered in real-time. This makes sure that only the most appropriate nodes are elected to become cluster heads, balancing load across a network and significantly reducing energy consumption, which prolongs the lifespan of a network with improved throughput. Compared to traditional protocols like LEACH, DEEC, and SEP, EECPEP-HWSN has high improvements considering energy efficiency and network performance, thus remaining a robust solution for HWSNs that have an energy constraint.

4.2.3. Node Composition

The more expensive and powerful heterogeneous nodes process all tasks, including data filtering, fusion, and transportation. Heterogeneous nodes have advanced processing resources, higher energy capacity, and communication features such as high-bandwidth, long-range transceivers. Heterogeneous nodes greatly enhance the performance of the network, extending the lifetime of the network, improving the reliability of data transfer, and reducing latency. These nodes frequently serve as mediators that gather data from regular nodes and transport it efficiently to the sink, hence reducing energy consumption and prolonging the operational lifespan of the network. Maximizing the benefits and maintaining robust and efficient network performance requires strategically deploying these diverse nodes, which have been optimized for different network parameters [69].

4.2.4. Node Deployment

A heterogeneous network in WSNs is composed of sensor nodes of diverse sorts, each with distinct capabilities, energy levels, and functionality. Heterogeneous networks utilize a combination of sensor nodes to enhance performance and cost-effectiveness, in contrast to homogeneous networks where all nodes are identical. These nodes can include of energy-efficient sensors for simple data gathering and highly capable nodes for data analysis and communication. The deployment of these nodes considers aspects such as energy consumption, coverage area, communication range, and application-specific needs. For example, strategically positioning high-power nodes can guarantee reliable data transmission over long distances, while dispersing low-power nodes can efficiently cover large areas. The variable composition of nodes in the network allows for improved adaptation to various surroundings and application requirements, thereby boosting the overall functionality and lifespan of the WSN. In addition, the use of movable nodes such as Unmanned Aerial Vehicles (UAVs) or robots provides flexibility by enabling the nodes to shift their positions dynamically. This ensures that optimal coverage and connectivity are maintained even when environmental circumstances vary [70]. Halder and Dasbit [71] presented a scheme in which both Sensor Nodes (SNs) and Relay Nodes (RNs) are deployed in a predetermined manner with the view of ensuring uniform distribution of energy across the network. Unlike in homogeneous networks, where every node performs the same task, heterogeneous networks deploy nodes with different roles: some sensing, others relaying data. This differentiation enables the network to balance energy consumption better since RNs are concerned with the more power-consuming operation of data transmission. Deploying RNs in areas of the site that have a greater quantity of data traffic reduces the "energy hole" problem facing nodes nearer the sink, which outspend their energy due to higher relay loads. The proposed deployment strategy not only increases the lifetime but also ensures coverage and connectivity, thus overall keeping the network operational for a longer duration. Simulation results show that this approach performs far better than traditional homogeneous deployment strategies, therefore proving the fact that heterogeneous node deployment indeed performs better in improving the overall performance of WSNs.

4.2.5. Classification of Critical Nodes

Aspects of heterogeneous wireless sensor networks (HWSNs) include the range of sensor nodes that are used, each with unique functionality, power supply, and capacities. One of these features is

 doi:10.20944/preprints202505.0438.v1

sensor diversity, which improves network monitoring by allowing different sensors to gather different kinds of data, such as motion, temperature, and humidity. Deployment plans take into account several elements, including energy efficiency, coverage, and connection, to satisfy specific requirements. Since most sensors have a certain amount of battery life, energy management is essential to extending the lifespan of the network. Adapting to changes in sensor node status, such as nodes going into sleep mode or needing to be recharged, is part of the network dynamics component. Furthermore, the network design can be layered, combining multiple levels including physical, data link, and network layers to suit diverse applications and quality of service (QoS) requirements, or hierarchical, with clusters overseen by cluster heads. These elements work together to enhance HWSNs' performance, adaptability, and dependability, which qualifies them for a range of uses including security, healthcare, and environmental monitoring [72].

4.3. Security Challenge and Solutions

The security challenges governed by the very nature of this technology have to be surmounted by WSNs through the fast deployment and growth into different applications. These threats on security of different types are faced by these networks owing to their very nature: decentralized and bound by resource constraints [73]. All these types of networks pose distinct security challenges: homogeneous networks, where sensor nodes are similar; heterogeneous networks, where the nodes have various capabilities; and highly cluster-based homogeneous networks demand higher security to be guarded against a possible intrusion through the communication protocol [74]. On the other hand, the use of high-end sensor nodes increases the quality of privacy and the efficiency of message distribution in heterogeneous networks [75]. Secure routing in WSNs is a must to protect them from malicious attacks and resource-constrained environments [76]. Moreover, effective key management schemes that take into account the position data of sensor nodes have been proposed to reduce security risks in those environments [77]. These security challenges must be dealt with using innovative solutions so as to not only ensure reliability but also functionality of homogeneous and heterogeneous networks. This survey was done by taking into consideration imperative research papers from 2023 and 2024. An imperative area taken into consideration when compiling the survey was the identification of critical security challenges, types of attacks, and proposed solutions. Table 4 and Table 5 below in this section illustrate some security challenges and homogeneous as well as heterogeneous network solutions.

4.4. Homogeneous Network Security Challenge

In the past few years, homogeneous security in WSNs has received increased research, especially in the publications of 2023 and 2024. All papers nearly cover most of the security categories that are of importance to the protection of WSNs. Advanced machine learning techniques and hybrid models emphasize intrusion detection to identify and mitigate a wide variety of cyber attacks, including DoS and gray hole attacks. Resource optimization strategies are probed to avoid resource depletion attacks, ensuring efficient energy management and the longevity of the network lifespan. Novel algorithms and protocols that enhance detection and response capabilities are utilized in mitigating malicious node attacks, including Sybil attacks, black holes, and false data injections. Elliptic curve cryptography and improved techniques of encryption strengthen key management against brute-force attackers and compromise. This can also include the integration of traditional cryptographic algorithms with Quantum Key Distribution to fight quantum threats and challenges that quantum computing will pose in the near future. All these studies, at last, collectively underscore the need for an integrated strategy to ensure comprehensive and resilient security in a homogeneous network. The various security categories explored in greater detail in the next sections are: Intrusion Detection, Resource Optimization, Malicious Node Attack, Key Management, and Quantum Threats.The critical areas with regards to the homogeneous network environments where security measures are necessary are shown in Figure 5. Each of these categories represents a significant part of network security that must be

 doi:10.20944/preprints202505.0438.v1

covered to maintain the integrity, confidentiality, and availability of the network. Table 4 summarizes a wide range of research papers published in 2023 and 2024. The papers present various security challenges in homogeneous networks; this includes details about the authors, date of publication, addressed security challenge, and proposed solutions. This classification, in homogeneous networks, further helps realize how various techniques and approaches contribute towards mitigating these security concerns.

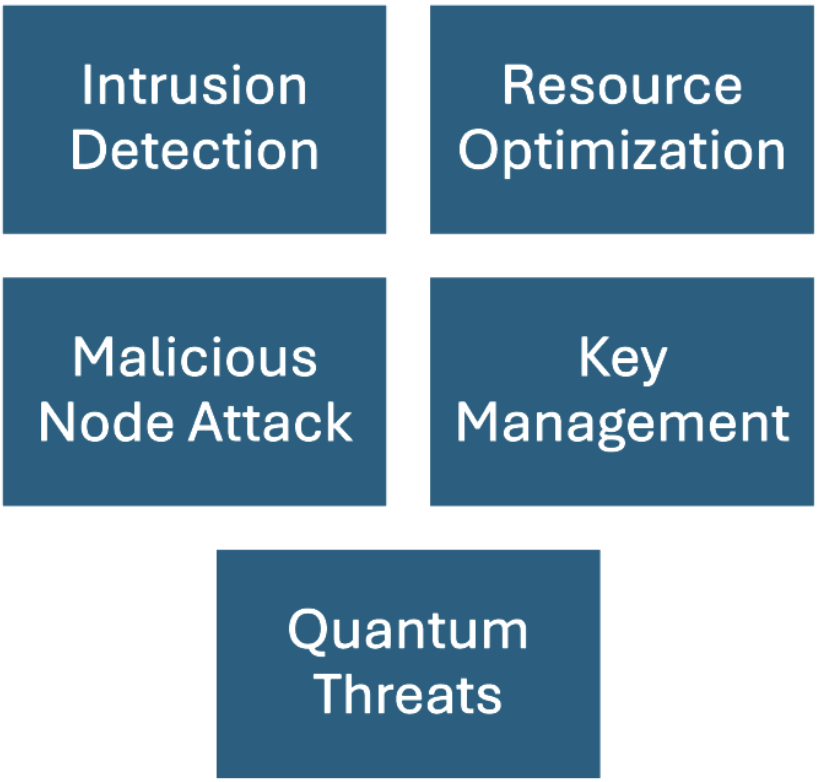

Figure 5. Security Challenge in Heterogeneous Network

4.4.1. Intrusion Detection

Intrusion Detection is a very important feature that provides security to WSNs in homogeneous network environments in which all nodes share similar features and vulnerabilities. The need for monitoring system traffic for possible hazards and suspicious activities includes Denial of Service (DoS) and requires the implementation of Intrusion Detection Systems (IDS). These attacks can be in the form of flooding, gray hole, black hole, and Time Division Multiple Access (TDMA) into the network and each may cause serious threat to the integrity of data and performance of the network. Effective IDS can help reduce such threats by appropriately detecting and responding to the intrusions. Many research papers have been published that intend to enhance systems for intrusion detection in WSNs. Sharma and Bhardwaj [84] dealt with an effective way to protect the WSNs deployed in agricultural scenarios from the various cyber attacks. It focuses on distributed denial-of-service (DoS) attacks, which cover flooding, gray hole, black hole, and TDMA attacks. The proposed framework using machine learning techniques like decision tree classifiers, Gaussian Naïve Bayes, and random forest classifiers provides the detection and mitigation of these attacks by enhancing the security and resilience of WSNs in terms of prudent agriculture monitoring and assured integrity of the data. Sedhuramalingam and Kumar [87] enhanced intrusion detection in WSNs using a hybrid model. Their proposed model, HGFSO-DLIDS, is a hybrid of deep learning techniques like Deep Convolutional Neural Networks (DCNN) and Bidirectional Long Short-Term Memory (BiLSTM), with Felis Margarita

 doi:10.20944/preprints202505.0438.v1

Swarm Optimization (FMSO) and Grampus Optimization Algorithm (GOA). The reason these methods are combined is for enhancing the performance of IDS by hyperparameter optimization and deep learning to achieve accurate classification. This will lead to high accuracy in detection and fewer false alarms compared to traditional approaches [88]. Most of the works discussed in Sahaya and Jasvant [89] dealt with several types of attacks against WSNs, such as routing attacks including sinkhole and selective forwarding, node capture, and physical attacks. Through the use of Mutual Information (MI) analysis, they proposed a method for detecting such intrusions by identifying critical nodes and anomalies within the network so that the overall security and robustness of WSNs are enhanced against malevolent activities, leaving them with stronger protection against an extensive variety of threats.

Table 4. Overview of Research Papers on Security Challenges in Homogeneous Networks (2023-2024)

Authors	**Date**	**Security Challenge Addressed**	**Proposed Solution**
Z. Teng, et al.[91]	2023	Malicious Node Attack	TS-BRS reputation model using time series analysis
Z. Ahmad Mir, et al.[92]	2023	Malicious Node Attack	Gray Wolf Optimization (GWO) for resource allocation and node placement
L. Tan, et al.[79]	2023	Key Management	Elliptic curve cryptography with AVL search tree and LEACH model
S. Urooj, et al.[80]	2023	Key Management	ECC with AES and clustering through LEACH protocol
Alghamdi, et al.[81]	2023	Key Management	SPAR-SSO protocol using connection quality estimation and power-aware routing
L. H. Alhasnawy, et al.[83]	2023	Quantum Threats	BB84 protocol with AES algorithm for quantum key distribution
G. Mehta, et al.[93]	2023	Malicious Node Attack	Improved LEACH protocol for detection and mitigation
Y. Zhang, et al.[90]	2023	Resource Optimization	WSN technology with AI for home safety monitoring
I. Sharma, et al.[84]	2024	Intrusion Detection	Machine learning framework with decision tree, Gaussian Naïve Bayes, and random forest
C. Puttaswamy, et al.[94]	2024	Malicious Node Attack	Fuzzy logic for cluster head selection and hybrid RSA and AES encryption

 doi:10.20944/preprints202505.0438.v1

Table 4. *Cont.*

Authors	Date	Security Challenge Addressed	Proposed Solution
M. A. Vieira, et al.[95]	2024	Malicious Node Attack	ARC-LEACH protocol with anomaly report cycling
K. Sedhuramalingam, et al.[87]	2024	Intrusion Detection	Hybrid GFSO model with DCNN and BiLSTM
J. Dr. LohithJ, et al.[88]	2024	Intrusion Detection	Quad LEACH protocol with integrated security agents
M. Sahaya, et al.[89]	2024	Intrusion Detection	Mutual information analysis for detecting critical nodes and anomalies
Venčkauskas, et al.[98]	2024	Key Management	Encrypted tunnels, periodic key exchanges, and sender's message authentication code
S. Khan, et al.[99]	2024	Malicious Node Attack	ANN-based detection with CICIDS2017 dataset
P. Vennam, et al.[96]	2024	Malicious Node Attack	SS-ChOA for secure Cluster Head selection and routing
M. Shanmathi, et al.[97]	2024	Malicious Node Attack	CNN-FL for node categorization and NGO-optimized routing strategy

4.4.2. Resource Optimization

In homogeneous networks, where nodes have similar capabilities and resources, resource optimization forms a very important part of the assurance of the longevity and efficiency of WSNs. Accordingly, optimization of the usage of resources, in particular energy, in a WSN context is required to help preserve network functionality and hence prolong operational life. Resource optimization is the procedure of eliminating unnecessary transmissions and efficiently handling computational loads to maximize network efficiency and minimize energy consumption. Zhang and Jing [90] explored the potential of AI, combined with WSN technology, in improving the efficiency of home safety monitoring systems. Although the paper does not explicitly describe different types of attacks, it IS emphasized that resource optimization in WSNs is very essential. For example, energy drain represents a particular form of attack designed to drain the battery life of sensor nodes by ensuring that they don't stop sending data. Such an attack could rapidly drain the resources of a network, causing system crashes and reducing the reliability of home safety monitoring. Resource optimization is important in this context for the effective use of sensors to ensure sustained performance and high reliability with regard to home-safety monitoring. The primary goal is to achieve efficient usage of resources and energy by utilizing AI technologies so that the network's capacity for monitoring residential environments efficiently is enhanced. This approach avoids any potential risks through strategies aimed at reducing unnecessary data transmission and balancing computational demand across the network. Ultimately, this enhances overall security and ensures better performance of WSNs in home safety applications.

 doi:10.20944/preprints202505.0438.v1

4.4.3. Malicious Node Attack

Malicious node attacks are one of the most serious issues threatening the integrity and reliability of WSNs, in which the misbehaving nodes inject false data, utilize excessive resources, or exhibit random behavior to undermine network operations. A number of mechanisms have been introduced to help counter these threats and improve security. Zhijun Teng et al. [91] focused on just one kind of problem: Malicious node attacks, more specifically called 'false data injection'. This method entails the injection of fake information by compromised nodes to disrupt network operations and reduce performance. The study seeks to maintain the accuracy and reliability of data transmission within the network by identifying and isolating malicious nodes with a Bayesian reputation evaluation model. Mir and Yadav [92] addressed resource depletion attacks, which are a subset of malicious node attacks. The goal of these attacks is to deplete the resources of network nodes, resulting in network disruption. The authors suggest that Gray Wolf Optimization (GWO) be implemented to improve security management by optimizing resource allocation, node placement, and data transmission efficiency, therefore effectively mitigating the effects of malicious attacks [93]. Puttaswamy and Shivaprasad [94] reviewed a variety of malicious node attacks, such as spoofing, Sybil attacks, selective forwarding, and replay attacks. The authors implement an advanced cluster head selection mechanism that is integrated with a hybrid and lightweight encryption technique to mitigate these threats, thereby guaranteeing energy-efficient, secure, and dependable data transmission in WSNs. Vieira and Liu [95] focused on black hole attacks in which malicious nodes discard all data packets destined for the base station. This work proposed ARC-LEACH (Anomaly Report Cycling LEACH), a new enhancement of the LEACH protocol. This protocol detects a black hole attack using rotating cluster heads and sending blacklist messages from the base station to isolate and neutralize malicious nodes. Khan and Khan [50] employed artificial neural networks (ANNs) to identify routing attacks, including black hole, gray hole, and wormhole attacks. The potential of ANN-based techniques to improve the security of WSNs is demonstrated by the proposed method, which employs feed-forward ANNs to model the dynamic behavior of WSNs and identify these threats with high accuracy. The ADLFAHA algorithm, which is introduced by Vennam and Mouleeswaran [96], addressed both black hole and Denial of Service (DoS) attacks. The network resilience and reliable data transmission are enhanced by this method, which emphasizes secure Cluster Head (SCH) selection and secure routing to prevent malicious nodes from intercepting or overwhelming network traffic. Finally, Shanmathi and Sonker [97] addressed malware node attacks, which involve manipulating compromised nodes, eavesdropping, or denying service to data packets. They suggested using a Neuro Genetic Optimizer (NGO) with a Convolutional Neural Network with Fuzzy Logic (CNN-FL) to classify nodes and optimize routing paths. This approach has the potential to substantially enhance packet delivery ratio, reduce latency, and minimize energy consumption. These studies, taken as a whole, bring into relief the ingenuity of approaches and varied strategies being worked on to secure WSNs against malicious nodes and ensure efficient functioning of network operations on the one hand and robust security on the other.

4.4.4. Key Management

One is aware that effective key management strategies will enable data integrity, confidentiality, and prevention from unauthorized access. Some methodologies have been explored with regard to the challenges in the process of key management due to compromise attacks, side-channel attacks, and brute-force attacks. Tan and Zheng [79] addressed compromise attacks in the context of WSNs. Such attacks may further result in the compromise of nodes, disruption of data integrity, fraudulent data insertion, or monitoring of data, thus wasting network resources. Such threats impart a need to present an effective key management system that is equipped with elliptic curve cryptography, having an AVL search tree and a LEACH model as mitigates. This combination greatly improves security by reducing computational overhead, energy consumption, and memory usage, thus providing an effective way to protect against compromise attacks. Urooj and Lata [80] dealt with the issues of

 doi:10.20944/preprints202505.0438.v1

side-channel attacks and brute-force attacks over the key management framework. The authors suggest a hybrid cryptography algorithm that combines Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) to improve the energy efficiency and security of WSNs. By utilizing the capabilities of both ECC and AES, this method guarantees secure and efficient data encryption, providing robust protection against these types of attacks. Alghamdi and Al Shahrani [81] defined side-channel attacks as exploits that glean information from the physical implementation of a system and not through vulnerabilities of the algorithms. This can involve monitoring power consumption variations, electromagnetic emissions, or even change in timing. Brute-force attacks are computationally intensive and time-consuming, particularly as key lengths increase, as they involve the systematic testing of all potential keys or passwords until the correct one is identified. Venčauskas et al. [98] engaged with highly important issues of communication security in-vehicle wireless sensor networks, which mitigation strategies emphasize resisting brute-force attacks through efficient key management. In this sense, the proposed framework incorporates improved key management, whereby periodic cryptography key exchanges minimize the window of opportunity where an attacker can use any single key and frequently change keys. This also includes a secure generation of new session keys, followed by encryption for distribution across the network to ensure key exchange in confidentiality and integrity. Within the framework lies a Message Authentication Code (MAC) that confirms communication authenticity, adding an extra layer of security against unauthorized access. It enhances the overall security of the in-vehicle wireless sensor network, since it corrects these key management problems, hence defending against brute-force attacks and other key-related vulnerabilities. The following studies, however, make it clear that diverse strategies and innovative approaches are being worked out for the key management in WSNs to ensure efficient network operation with robust security in the presence of various types of attacks.

4.4.5. Quantum Threats

As quantum computers further develop, the potential for solving complex mathematical problems underlying many current cryptographic algorithms will compromise the confidentiality and integrity of data in these networks. For this reason, emerging threats have to result in new cryptographic techniques resilient to quantum computational capabilities. Another work on the topic of quantum threats in WSNs [83] proposes a hybrid security solution that integrates the Advanced Encryption Standard (AES) and algorithm with Quantum Key Distribution (QKD). On top of that, QKD makes use of quantum mechanics principles to generate secure cryptographic keys. AES is utilized for data encryption in the network. This implies, according to quantum properties, such as the no-cloning theorem and the principle of quantum superposition, with the BB84 protocol, the key distribution process of will be able to recognize someone trying to listen in. The solution incorporates QKD into AES and hence improves the total security of any WSN against possible quantum attacks. QKD is resilient key distribution, secure in the presence of quantum computers. QKD generates encryption keys that are employed to encrypt data with AES, guaranteeing that the encryption keys will remain secure even if adversaries possess quantum computational capabilities. With this mixed method, the network is protected against both future quantum threats and current computational attacks. It offers a complete way to protect WSNs in a threat landscape that is always changing.

4.4.6. Conclusion

In summary, the research conducted on homogeneous security WSNs between 2023 and 2024 encompasses a wide range of security categories. Eight papers contributed different effective detection and mitigation techniques against various threats, among them Sybil attacks, black holes, and false data injection. Most of the researches were focused on Malicious Node Attacks. The other important area was intrusion detection, where four papers elaborated on the use of hybrid systems and novel machine learning models in detecting and forestalling such attacks as DoS and gray hole. Four papers also

 doi:10.20944/preprints202505.0438.v1

extensively dealt with key management, featuring robust cryptographic solutions against brute-force attacks and compromise. One paper each discussed resource optimization and quantum threats. The strategies on the efficient use of resources in fighting against depletion attacks and quantum key distribution to counter potential quantum computing threats were highlighted. Last but not least, the integrity of science research was protected from publication and peer review integrity attacks through setting up robust peer-review procedures and post-publication review mechanisms. These various studies highlight the multi-dimensional approach required in order to achieve full security in homogeneous WSNs. The categories and the number of papers which cover each security concern are represented in Figure 6.

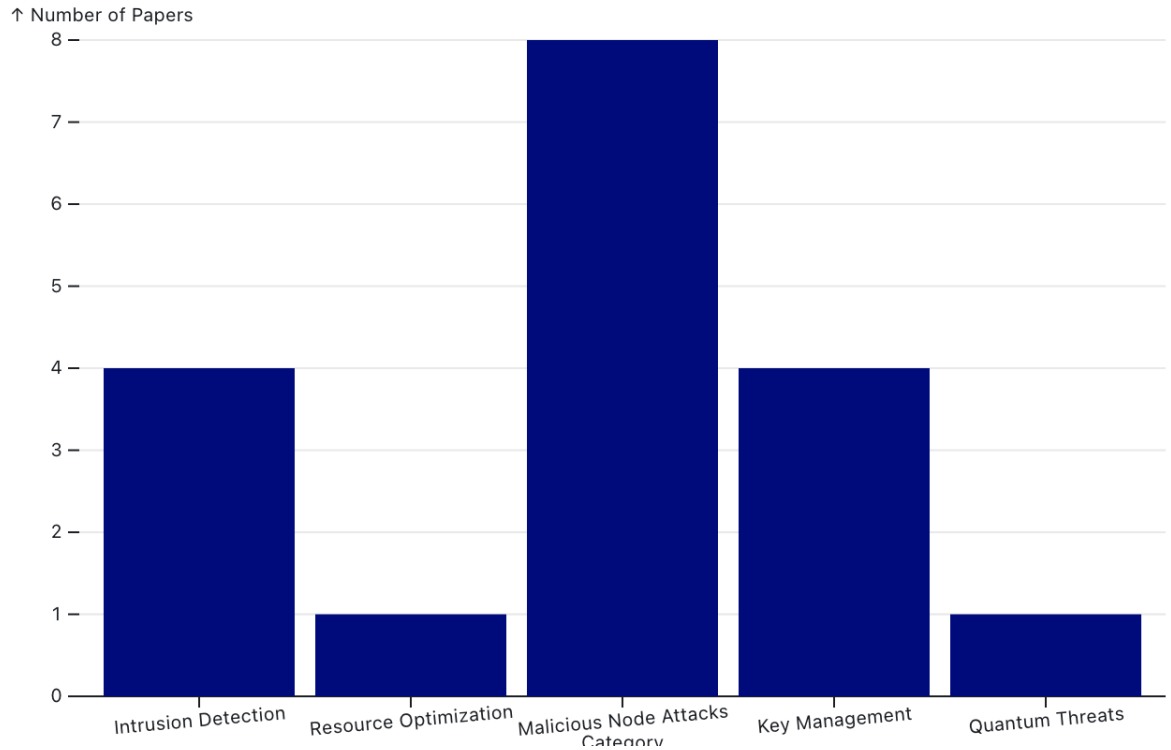

Figure 6. Frequency of Categories Research Papers

4.5. Heterogeneous Network: Security Challenges

The heterogeneous networks, which combine many varieties of sensor nodes with enormous differences in capabilities, are vulnerable to quite different security issues and opportunities. Sophisticated algorithms are needed to optimize the interactions between various node types for handling the network efficiently. The communication should be secure by including full encryption and authentication procedures to avoid vulnerabilities as much as possible. Protection against sophisticated attacks, thus, calls for advanced security measures, hence the need for intrusion prevention and anomaly detection. In the case of a unified security framework enables a defense strategy scalable for heterogeneous networks since customization of this architecture is done in accordance with their heterogeneous nature. Security should go hand in hand with energy efficacy, ensuring the network's longevity and effectiveness in real-world applications. The critical areas in homogeneous network environments where security measures are essential are illustrated in Figure 7. Network management, privacy and data protection, communication security, advanced Security techniques, security Framework and energy efficiency are the main challenges identified. The integrity, confidentiality, and availability of the network must be preserved by addressing each of these categories, which each represent a substantial aspect of network security. Table 5 represents a collection of various research works published in the years 2023 and 2024. The papers target different security challenges that occur

 doi:10.20944/preprints202505.0438.v1

in heterogeneous networks, along with their authors, publication date, addressed security challenge, and proposed solution. The classification makes it easier to identify how various techniques and approaches keep on contributing towards mitigating the above-mentioned different security issues occurring within independent homogeneous networks.

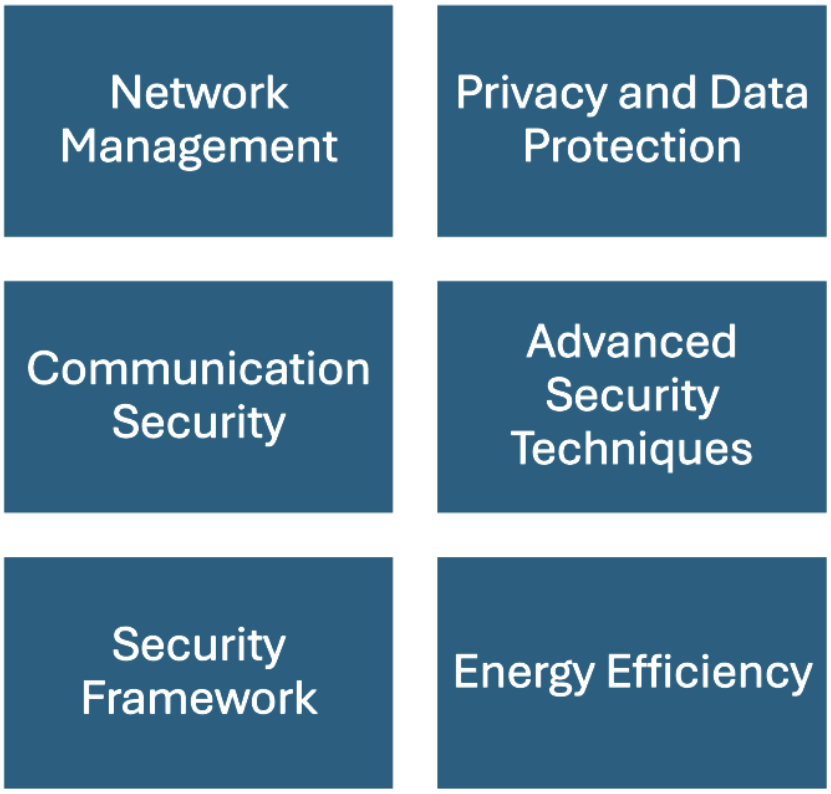

Figure 7. Security Challenge in Homogeneous Network

Table 5. Overview of Research Papers on Security Challenges in Homogeneous Networks (2023-2024)

Authors	Date	Security Challenge Addressed	Proposed Solution
Jing Li, et al.[101]	2023	Network Management	Rule-based reasoning using description logic for predicting network security situations
Lianwei Qu, et al.[102]	2023	Privacy and Data Protection	HNPP model with differential privacy and random perturbations for secure network publishing
Y. Hu, et al.[103]	2023	Privacy and Data Protection	Distributed Weighted Classification Method for network slicing in Space-Air-Ground integrated networks

 doi:10.20944/preprints202505.0438.v1

Z. Han, et al.[104]	2023	Communication Security	Game theory-based optimization for channel access attack defense in UAV-aided networks
V. Bouček, M. Husák[105]	2023	Network Management	Graph-based tool for recommending similar devices to analyze cyber attack impact
Xabier, et al.[106]	2023	Network Management	Federated Learning with unsupervised device clustering for network anomaly detection
Junkai Yi, Lin Guo[107]	2023	Network Management	AHP-based evaluation with XGBoost for network security assessment in IIoT
J. Zhang, et al.[108]	2024	Advanced Security Threats	Attention sharing mechanism for domain adaptation in IoT intrusion detection
Changkui Yin, et al.[109]	2024	Privacy and Data Protection	STLLM-ECS framework with edge computing for secure PM2.5 level forecasting
D. Bhanu, et al.[110]	2024	Energy Efficiency	OECS-RA for optimal cluster head and secure-hop selection in WSNs
W. Wang, et al.[112]	2024	Network Management	VHetNet-enabled AFL framework with CA2C algorithm for anomaly detection in IoT
Wenbo Zhang, et al.[108]	2024	Advanced Security Technique	vBiLSTM and KGC-N model for network security knowledge graph completion
T. Quinn, et al.[114]	2024	Security Framework	PoC trust management for routing in software-defined wireless networks
W. Yu, et al.[115]	2024	Security Framework	DevSecOps and AIOps for continuous security monitoring in substation networks
J. Li, et al.[116]	2024	Privacy and Data Protection	DL-based caching framework with differential privacy for IoT network caching
Q. Zhang, et al.[117]	2024	Communication Security	AHTST strategy with Lyapunov optimization for secure heterogeneous traffic transmission

 doi:10.20944/preprints202505.0438.v1

4.5.1. Network Management

Li and Huang [101] focused on security management challenges in an IoT context within power systems. As noted by these authors, network environments become easily susceptible to intrusion assaults or Trojan horse viruses, which gets further aggravated by the dynamic nature and expansion of IoT devices. They propose a rule-based reasoning approach that exploits multi-source knowledge to improve the management of security. The model is designed for a much more effective prediction of network security situations, which can be achieved by incorporating description logic-based language into it and designing the reasoning rules implemented in order to complement the semantic representation of security data. Compared to conventional methods, such as the entropy method, this innovative approach provides practical guidance for network security management that is significantly more effective. Consequently, the paper makes a valuable contribution to the field by providing a strong framework for security administration in the constantly changing environment of IoT networks. Boucek and Husak [105] presented a prototype tool that would enhance network security management by recommending similar devices close to a compromised machine. It calculates the similarity score and recommends the devices likely to be targeted after an initial exploitation, using contemporary graph-based technologies to efficiently store and query network data. This is particularly useful for detecting and containing very fast-spreading malware, such as ransomware, which uses a variety of attack vectors including social engineering. It can identify at-risk devices automatically; this greatly aids in vulnerability management, impact assessment, early warning, and digital forensics. In that sense, it lays the efficient groundwork for proactive network security management. The proposed system provides practical guidance for securing network environments, considerably reduces the workload of security operators, and speeds up incident response times. In the context of anomaly detection, Xabier and Jose [106] presented a clustered federated learning architecture for network anomaly detection over large-scale heterogeneous IoT networks. Federated learning is used in the architecture to build unsupervised models that can discover unknown network anomalies, which may portend security breaches. Going ahead to decentralize model training across nodes eliminates the need for central data aggregation, thus ensuring data privacy, and solves the challenge of big and heterogeneous IoT networks. The federated learning approach clusters IoT devices with similarities in order to allow more efficient and speedy detection. This will ensure that network management systems detect strange behavior of the network within a very short time, so fixing is quick. The architecture improves the general resilience and security level for IoT networks, letting real-time threat detection execute immediately after that; it empowers strong, scalable network management. Yi and Lin [107] focused on the solving of network security problems to enhance situational awareness in Industrial Internet of Things (IIoT). They identified a wide variety of cyber-attacks, including DDoS, DoS, backdoor, injection, MitM, password, ransomware, scanning, and XSS, which exert jeopardies in terms of stability, confidentiality, integrity, and availability concerning IIoT systems. They put forward a New Network Security Situation Assessment (NSSA) model based on the Analytic Hierarchy Process (AHP) and Extreme Gradient Boosting (XGBoost) to counter these threats. In the proposed model, considering the unique security requirements of the IIoT system, the security situation is assessed quantitatively. It uses the balanced data sampling technique, AUOS, to handle the challenge of imbalance attack traffic data; therefore, ensuring an accurate detection and classification of attacks. It provides a rich situational awareness framework that lets security analysts have complete views, assessment, and understanding of the security posture of IIoT networks in real-time, and hence it enables proactive and informed decision-making protection of the industrial operation. This will be achieved via these methodologies.

4.5.2. Privacy and Data Protection

The main purpose of Qu and Wang's work [102] is to solve the problem of privacy leakage in the process of publishing heterogeneous network data. The main problem is the leakage of private

 doi:10.20944/preprints202505.0438.v1

data brought on by background knowledge attacks. In such an attack, sensitive data is inferred through prior knowledge provided. In this proposal, it would consist of the transformation into homogeneous networks equivalent to heterogeneous networks and the application of differential privacy techniques with random disruptions. This approach has a good balance between data usability and privacy, as it ensures protection of sensitive information during data transmission and publication. Experimental analysis across real datasets has shown quite clearly that this framework is efficient, both in preserving privacy and ensuring data utility together with high original edge retention and clustering precision rates. Hu and Shi [103] studied edge computing to reduce privacy leakage during data transmission in a heterogeneous network. Data leakage, as the primary attack type, is addressed during the centralized process of training. This happens with the transfer of large volumes of data from sensors to a central cloud. In order to mitigate this issue, they suggest the Spatio-Temporal Large Language Model with Edge Computing Servers (STLLM-ECS) framework, which partitions the network into subgraphs, which allows localized data processing and reducing the possibility of privacy violations. This approach improves security by minimizing the necessity for extensive data transmission across potentially vulnerable networks and retaining data in immediate access to its source. In another contribution, Yin et al. [109] identified data leakage during transmission as a major security concern. This kind of attack is due to the transfers of large datasets from the sensors to some central cloud, hence increasing the risk of interception and access by entities with malicious intentions. They proposed a secure transmission framework using Edge Computing Servers for the same. Locally processing and training data at the edge reduces the need for extensive data transmission. This method effectively mitigates the risk of data leakage and improves data security, guaranteeing that sensitive information remains safe during forecasting operations. This decentralized processing not only enhances the efficacy and accuracy of PM2.5 predictions by leveraging local computational resources and reducing latency, but also secures data. Li and Feng [116] focused on privacy leakage during model training and transmission in heterogeneous networks. They emphasized two kinds of attacks: White-box, under which attackers could acquire the model's parameters, and black-box attacks, whereby attackers repeatedly query to extract sensitive information. Their proposal is for a framework with differential privacy techniques to mitigate such threats. These techniques introduce disturbance to data, thereby guaranteeing the privacy and security of user information. Furthermore, a boosting incorporated method improves the caching model's robustness and accuracy. This method effectively balances the necessity for privacy protection with the preservation of high performance in heterogeneous IoT network caching.

4.5.3. Communication Security

Han et al. [104] focused on the Channel Access Attacks (CAA) problem in 6G networks, paying special emphasis to UAV-aided heterogeneous networks. Such attacks will greatly degrade the performance of a network due to the jamming of a channel or flooding it with useless data packets, hence causing a disruption in communication. The authors propose a smart optimization framework using methods from game theory, such as potential games, Stackelberg games, and coalition games, in resource-management tasks concerning the efficient handling of such concerns. In the paper, the proposed mechanism improves communication security by optimizing channel access, power control, and link selection to guarantee reliability and good performance of the network under attack. The proposed strategies improve the overall security and effectiveness of the network by ensuring optimum AoI, productivity, and latency. It improves the resilience of the network against CAAs. In another study [117], the problem being addressed is eavesdropping attacks in a wireless multiuser uplink heterogeneous network. This network consists of Age-of-Information (AoI)-oriented and throughput-oriented users. Unscheduled users may potentially act as eavesdroppers. The authors have implemented a security scheme in the physical layer to address this problem; it works by creating noise and using Time-Division Multiple Access (TDMA) to protect the secret keys during

 doi:10.20944/preprints202505.0438.v1

transmission. A few countermeasures are made to protect a channel access attack and achieve no break into communication channels. They incorporate encryption, secure access protocols such as physical layer security techniques, and other techniques to ensure that data remains confidential and secure from surveillance and other malicious activities. The adaptive strategies in this paper have the potential for greatly reducing AoI while attaining a high rate of secrecy as a strong defense against attacks aimed at accessing the channel.

4.5.4. Advanced Security Techniques

Zhang and Li [108] used advanced security techniques with AI and machine learning to protect IoT networks from sophisticated cyber-attacks. The authors consider the challenges of the diverse and dispersed character of IoT devices, which frequently adhere to distinct data distributions. Specifically, the framework domain adaptation approach and an attention-sharing mechanism make the intrusion detection model fit various IoT environments. This forms a ground for detecting and mitigating many other types of attacks related to backdoor intrusions and password breaches. The methodology assures that data from different IoT devices can be projected in a unified space so as to enhance accuracy and reduce biases in predicting threats. Results from experiments showed that the framework was better than traditional methods because it could adapt to different network environments and keep security strong in a wide range of IoT situations. The integration of AI and machine learning is a demonstration of the advancement in security techniques created specifically for the dynamic and evolving landscape of IoT networks. Zhang and Wenbo [113] also made contributions to the field by further addressing the issue of incomplete and fragmented cybersecurity knowledge graphs. In contexts of cybersecurity, it is a result of deficiencies that exist in current text encoding models resulting in inadequate reasoning capability. It would hence propose a solution incorporating a Knowledge Graph Completion model (KGC-N) together with advanced AI techniques for processing and encoding textual data. This is achieved by combining word2vec and BiLSTM models. This model enhances the accuracy and efficiency of knowledge graph completion by utilizing graph attention networks to enhance the fusion of neighborhood features. These methods are a component of sophisticated security measures that utilize AI and machine learning to enhance comprehension and mitigation of cyber threats by offering a more comprehensive and precise representation of cybersecurity knowledge. Those studies altogether underline the fact that AI and machine learning play a very important role in enhancing cybersecurity measures. These works offer robust frameworks efficient in threat detection and mitigation, as they meet the distinct challenges of IoT environments with modern methods of data processing. Using cutting-edge methods such as domain adaptation and knowledge graph completion shows how AI-driven methods can protect the safety and integrity of complicated network systems from new cyber threats.

4.5.5. Security Framework

Yu and Qian [115] provided countermeasures against cybersecurity threats that significantly impact the stability of substation networks, further decentralizing the discipline. Such attacks have strong potentials for operational failures and outages by disrupting critical infrastructural setup. In light of it, the authors propose a framework combining DevSecOps with AIOps to mitigate such risks. This framework includes orchestrated response mechanisms, automated threat detection, and continuous security monitoring. The framework makes substation networks safer by incorporating security into development processes and using AI for real-time operations. It does this by ensuring strong governance and proactive defense against sophisticated cyber threats. In a recent study, Quinn and Shah [114] focused on the homogeneous security of WSNs. This work has been useful in giving insight as to why WSNs are vulnerable to different security threats. Great emphasis is placed on the prevalence of Malicious Node Attacks by the various papers that propose different innovative strategies to detect and mitigate such threats as Sybil attacks, black holes, false data injection, etc. Such systems

 doi:10.20944/preprints202505.0438.v1

emphasize the success rate of intrusion detection systems that could have sophisticated machine learning models in detecting and preventing DoS and gray hole attacks. In this research, a very critical element of key management is being presented in which cryptographic solutions against brute-force attacks or compromise are proposed. The research investigates strategies for resource optimization to prevent resource depletion assaults and guarantee the effective use of network resources. Quantum Key Distribution (QKD) is implemented to safeguard against potential quantum computation capabilities.

4.5.6. Energy Efficiency

Bhanu and Santhosh [110] focused on solving the dual challenges of energy efficiency and security in Heterogeneous Wireless Sensor Networks (H-WSNs). The various attacks considered here are mainly based on node capture, where the malicious entities compromise the sensor nodes to disturb the functionality of the network. In such threats, the proposed OECS-RA algorithm improves the resiliency of the network by optimizing its energy consumption through efficient clustering and routing mechanisms. It efficiently defends against different types of attacks, including denial-of-service and wormhole attacks, through their secure-hop selection scheme in protecting data transmission. The algorithm's energy-efficient clustering and strong security measures in the network enable improved throughput, dependable communication, and extended lifetime. Thus, this method can have applications, particularly in real-time fields like medicine and transportation, also business where energy efficiency is combined with issues of a high level of security.

4.5.7. Conclusion

The variety of topics covered in these different themes—including network management, privacy and data protection, communication security, advanced security techniques, security frameworks, and energy efficiency come together to provide a comprehensive overview of present-day developments and challenges in the cybersecurity domain. Some of the novel approaches at work include federated learning, multi-sensor data fusion, and rule-based reasoning for improving resiliency and efficiency in network management against novel cyber threats. The goals of research into privacy and data protection are to avoid possible leakage of privacy and ensure secure transmission of data through differential privacy, edge computing, and other deep learning-based frameworks. Security communication research investigates strategies for defense against eavesdropping and channel access assaults through game theory for resource optimization and the approaches of physical-layer security. Advanced security techniques leverage domain adaptation and knowledge graph completion, applied to mitigate IoT challenges. Enhanced by AI-based machine learning, threat detection is improved. Security frameworks deal with solutions holistically, emphasizing governance and interoperability; they encompass a wide array of respective mechanisms for security. Energy efficiency research in recent times has focused on the optimization of energy consumption and enhancement of security in heterogeneous WSN through algorithms that integrate energy-efficient clustering with robust security. Therefore, these studies also put an emphasis on the fact that interdisciplinary approaches and innovation are continuous for the improvement of security, efficiency, and resilience of modern networked systems. The categories and the number of papers covering each security concern are depicted in Figure 5.

 doi:10.20944/preprints202505.0438.v1

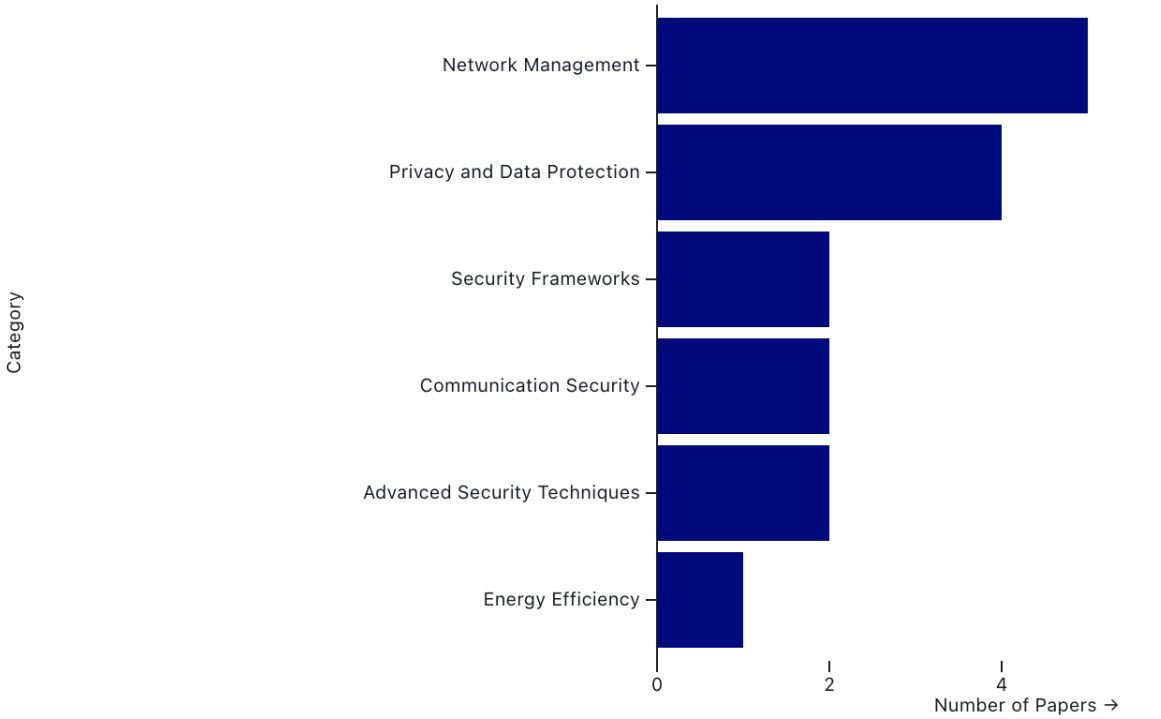

Figure 8. Frequency of Categories Research Papers

5. Conclusion

There are several challenges and problems associated with the WSN deployment process, which are mainly related to energy efficiency, security, and coverage effectiveness. These issues need to be addressed for better functionality and reliability in WSNs regarding applications such as environmental monitoring, precision agriculture, and surveillance for effective performance. In view of defending against these vulnerabilities, there is an acute need for robust protocols for encryption and authentication. Further research and innovations in WSN capabilities once again stress their importance in modern data collection and analysis. This offers a lot of insight and solutions to enhance understanding in the classification of sensor nodes and the deployment strategies for WSNs towards more efficient and resilient network design in the future.

Acknowledgments: This work has been partially supported by an NSF funded proposal (Award Number: 2244594) for an NSF REU Site, titled "REU Site: Gluing Computer Science and Convex Geometry: Research Experiences for Undergraduates from Community Colleges" whose PI is Dr. Ammari.

References

1. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless sensor networks: a survey," Computer Networks, Volume 38, Issue 4, 2002, Pages 393-422, ISSN 1389-1286, https://doi.org/10.1016/S1389–1286(01)00302-4.
2. Kandris D, Anastasiadis E. Advanced Wireless Sensor Networks: Applications, Challenges and Research Trends. Electronics. 2024; 13(12):2268. https://doi.org/10.3390
3. Salman, Dheyab & Ibrahim, & Mahdi, Abdullah & Yas, Qahtan. (2021). Challenges and Issues for Wireless Sensor Networks: A Survey. 6. 1-19.
4. V. Mhatre and C. Rosenberg, "Homogeneous vs heterogeneous clustered sensor networks: a comparative study," 2004 IEEE International Conference on Communications (IEEE Cat. No.04CH37577), Paris, France, 2004, pp. 3646-3651 Vol.6, doi: 10.1109/ICC.2004.1313223.

 doi:10.20944/preprints202505.0438.v1

5. Nasri, Nejah and Mnasri, Sami and Val, Thierry 3D Node Deployment Strategies Prediction in Wireless Sensors Network. (2019) International Journal of Electronics, 1. 1-30. ISSN 0020-7217
6. You-Chiun Wang, Chun-Chi Hu, and Yu-Chee Tseng, "Efficient deployment algorithms for ensuring coverage and connectivity of wireless sensor networks," First International Conference on Wireless Internet (WICON'05), Budapest, Hungary, 2005, pp. 114-121, doi: 10.1109/WICON.2005.13.
7. Wei Li and C. G. Cassandras, "A minimum-power wireless sensor network self-deployment scheme," IEEE Wireless Communications and Networking Conference, 2005, New Orleans, LA, USA, 2005, pp. 1897-1902 Vol. 3, doi: 10.1109/WCNC.2005.1424801.
8. T. Andersen and S. Tirthapura, "Wireless sensor deployment for 3D coverage with constraints," 2009 Sixth International Conference on Networked Sensing Systems (INSS), Pittsburgh, PA, USA, 2009, pp. 1-4, doi: 10.1109/INSS.2009.5409946.
9. Nojeong Heo and P. K. Varshney, "Energy-efficient deployment of Intelligent Mobile sensor networks," in IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, vol. 35, no. 1, pp. 78-92, Jan. 2005, doi: 10.1109/TSMCA.2004.838486 .
10. Y. Zou and Krishnendu Chakrabarty, "Sensor deployment and target localization based on virtual forces," IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428), San Francisco, CA, USA, 2003, pp. 1293-1303 vol.2, doi: 10.1109/INFCOM.2003 .
11. Z. Cheng, M. Perillo and W. B. Heinzelman, "General Network Lifetime and Cost Models for Evaluating Sensor Network Deployment Strategies," in IEEE Transactions on Mobile Computing, vol. 7, no. 4, pp. 484-497, April 2008, doi: 10.1109/TMC.2007.70784.
12. Soumya J Bhat, Santhosh K V, "A localization and deployment model for wireless sensor networks using arithmetic optimization algorithm," 2023.
13. P. Balister and S. Kumar, "Random vs. Deterministic Deployment of Sensors in the Presence of Failures and Placement Errors," IEEE INFOCOM 2009, Rio de Janeiro, Brazil, 2009, pp. 2896-2900, doi: 10.1109/INFCOM.2009.5062254.
14. Ines Khoufi, Pascale Minet, Anis Laouiti, Saoucene Mahfoudh. "Survey of Deployment Algorithms in Wireless Sensor Networks: Coverage and Connectivity Issues and Challenges." International Journal of Autonomous and Adaptive Communications Systems, 2017, 10 (4), pp.341-390. doi: 10.1504/IJAACS.2017.10009671.
15. Sourour Elloumi, Olivier Hudry, Estel Marie, Agathe Martin, Agnès Plateau, et al., "Optimization of wireless sensor networks deployment with coverage and connectivity constraints," Annals of Operations Research, vol. 298, no. 1-2, pp. 183-206, 2021. DOI: 10.1007/s10479-018-2943-7.
16. Guiling Wang, Guohong Cao, and T. La Porta, "Movement-assisted sensor deployment," IEEE INFOCOM 2004, Hong Kong, China, 2004, pp. 2469-2479 vol.4, doi: 10.1109/INFCOM.2004.1354668.
17. Mao, J., Jiang, X. & Zhang, X., "Analysis of node deployment in wireless sensor networks in warehouse environment monitoring systems," J Wireless Com Network 2019, 288 (2019). DOI: 10.1186/s13638-019-1615-x.
18. S. Toumpis and L. Tassiulas, "Optimal deployment of large wireless sensor networks," in IEEE Transactions on Information Theory, vol. 52, no. 7, pp. 2935-2953, July 2006, doi: 10.1109/TIT.2006.876256.
19. Saadallah, N. R., & Alabady, S. A. (2024). An Energy Efficient and Scalable WSN with Enhanced Data Aggregation Accuracy. Journal of Telecommunications and Information Technology, 2(2), 48–57. https://doi.org/10.26636/jtit.2024.2.1510
20. Rahul Priyadarshi, Bharat Gupta, and Amulya Anurag, "Deployment techniques in wireless sensor networks: a survey, classification, challenges, and future research issues," 2020.
21. Boualem, Adda et al. "Linear and Non-Linear Barrier Coverage in Deterministic and Uncertain environment in WSNs: A New Classification." ArXiv abs/2306.12355 (2023): n. pag.
22. H. P. Gupta, S. V. Rao and V. Tamarapalli, "Analysis of Stochastic k-Coverage and Connectivity in Sensor Networks With Boundary Deployment," in IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 4, pp. 1861-1871, Aug. 2015, doi: 10.1109/TITS.2014.2379699.

23. P. Geng, A. Yang and Y. Liu, "Research on Connectivity and Coverage of WSNs Based on Complex Network Characteristics," 2023 12th International Conference of Information and Communication Technology (ICTech), Wuhan, China, 2023, pp. 484-488, doi: 10.1109/ICTech58362.2023.00096.
24. Mehmet C. Vuran, Özgür B. Akan, Ian F. Akyildiz, Spatio-temporal correlation: theory and applications for wireless sensor networks, Computer Networks, Volume 45, Issue 3, 2004, Pages 245-259, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2004.03.007.
25. Niculescu, D. (2003). Positioning in ad hoc sensor networks. IEEE Network, 18(4), 24-29.
26. Zafer, M., Senouci, M.R. and Aissani, M. (2021) 'Efficient deployment approach of wireless sensor networks on 3D terrains', Int. J. Data Mining, Modelling and Management, Vol. 13, Nos. 1/2, pp.114–136.
27. Chi-Fu Huang, Yu-Chee Tseng and Li-Chu Lo, "The coverage problem in three-dimensional wireless sensor networks," IEEE Global Telecommunications Conference, 2004. GLOBECOM '04., Dallas, TX, USA, 2004, pp. 3182-3186 Vol.5, doi: 10.1109/GLOCOM.2004.1378938.
28. M. K. Watfa and S. Commuri, "The 3-Dimensional Wireless Sensor Network Coverage Problem," 2006 IEEE International Conference on Networking, Sensing and Control, Ft. Lauderdale, FL, USA, 2006, pp. 856-861, doi: 10.1109/ICNSC.2006.1673259.
29. Unaldi, N. and Temel, S., 2014, October. Wireless sensor deployment method on 3D environments to maximize quality of coverage and quality of network connectivity. In Proceedings of the World Congress Engineering and Computer science (Vol. 2, pp. 2078-0966).
30. S. M. Nazrul Alam and Zygmunt J. Haas. 2006. Coverage and connectivity in three-dimensional networks. In Proceedings of the 12th annual international conference on Mobile computing and networking (MobiCom '06). Association for Computing Machinery, New York, NY, USA, 346–357. https://doi.org/10.1145/1161089.1161128
31. Fu, W.; Yang, Y.; Hong, G.; Hou, J. WSN Deployment Strategy for Real 3D Terrain Coverage Based on Greedy Algorithm with DEM Probability Coverage Model. Electronics 2021, 10, 2028. 10.3390/electronics10162028
32. A. Saad, M. R. Senouci and O. Benyattou, "Toward a Realistic Approach for the Deployment of 3D Wireless Sensor Networks," in IEEE Transactions on Mobile Computing, vol. 21, no. 4, pp. 1508-1519, 1 April 2022, doi: 10.1109/TMC.2020.3024939.
33. Mohamed K. Watfa and Sesh Commuri. 2008. An energy efficient and self-healing 3-dimensional sensor cover. Int. J. Ad Hoc Ubiquitous Comput. 3, 1 (December 2007), 33–47. https://doi.org/10.1504/IJAHUC.2008.016193.
34. Gou, P.; Guo, B.; Guo, M.; Mao, S. VKECE-3D: Energy-Efficient Coverage Enhancement in Three-Dimensional Heterogeneous Wireless Sensor Networks Based on 3D-Voronoi and K- Means Algorithm. Sensors 2023, 23, 573. https://doi.org/10.3390/s23020573
35. Reddy, M.R., Chandra, M.L.R. "An Improved 3D-DV-Hop Localization Algorithm to Improve Accuracy for 3D Wireless Sensor Networks." SN COMPUT. SCI. 5, 245 (2024). https://doi.org/10.1007/s42979-023-02557-8.
36. Rajput, Monali & Ghawte, Usama. (2017). Security Challenges in Wireless Sensor Networks. International Journal of Computer Applications. 168. 24-28. 10.5120/ijca2017914414.
37. Obodoeze, Engr. Dr. Fidelis. (2012). Wireless Sensor Network in Niger Delta Oil and Gas Field Monitoring: The Security Challenges and Countermeasures. International Journal of Distributed and Parallel systems. 3. 65-77. 10.5121/ijdps.2012.3606.
38. Ahmad R, Wazirali R, Abu-Ain T. Machine Learning for Wireless Sensor Networks Security: An Overview of Challenges and Issues. Sensors. 2022; 22(13):4730. https://doi.org/10.3390/s22134730
39. Saidi, H., Gretete, D., Addaim, A. (2020). Game Theory for Wireless Sensor Network Security. In: Yang, XS., Sherratt, S., Dey, N., Joshi, A. (eds) Fourth International Congress on Information and Communication Technology. Advances in Intelligent Systems and Computing, vol 1041. Springer, Singapore.
40. Shah, Ansar & Aljubayri, Mohammed & Khan, Muhammad & Alqahtani, Jarallah & Mscs, Mahmood & Sulaiman, Adel & Shaikh, Asadullah. (2023). ILSM: Incorporated Lightweight Security Model for Improving QOS in WSN. Computer Systems Science and Engineering. 46. 2471-2488. 10.32604/csse.2023.034951.
41. H., O. Abu, R. "Securing Wireless Sensor Networks Against DoS attacks in Industrial 4.0," Journal of Intelligent Systems and Internet of Things, vol. , no. , pp. 66-74, 2023. DOI: https://doi.org/10.54216/JISIoT.080106

 doi:10.20944/preprints202505.0438.v1

42. Bassey, Aniebiet & Johnson, Enyenihi & Umoh, Gabriel. (2023). Secret Key Management in Wireless Sensor Network Based on Probabilistic Technique. Journal of Engineering Research and Reports. 25. 162-170. 10.9734/jerr/2023/v25i121049.
43. Adda Boualem, Cyril de Runz, Marwane Ayaida, Herman Akdag. A fuzzy/possibility approach for area coverage in wireless sensor networks. Soft Computing, 2023, 27, pp.9367-9382. ff10.1007/s00500- 023-08406-3ff. ffhal-04108659f
44. Khan, A.; Macias-Villegas, G.; Ammari, H. M. Aperiodic Tiling for Enhancing Security in Wireless Sensor Networks. Preprints 2024, 2024081495. https://doi.org/10.20944/preprints202408.1495.v1
45. Medina F, Ruiz H, Espíndola J, Avendaño E. Deploying IIoT Systems for Long-Term Planning in Underground Mining: A Focus on the Monitoring of Explosive Atmospheres. Applied Sciences. 2024; 14(3):1116. https://doi.org/10.3390/app14031116
46. Bian H, Zhang W, Chang CK. Situ-Oracle: A Learning-Based Situation Analysis Framework for Blockchain-Based IoT Systems. Blockchains. 2024; 2(2):173-194. https://doi.org/10.3390/blockchains2020009
47. Elsayed, Mahmoud Ayman Mohamed. Navigating the Rules: Integrating TD3 and Sensor Fusion for TrafficAware Autonomous Vehicle Path Planning. 2024. American University in Cairo, Master's Thesis. AUC Knowledge Fountain. https://fount.aucegypt.edu/etds/2369
48. P. Sebothoma and T. E. Mathonsi, "An Enhanced Security Algorithm for Wireless Sensor Networks," 2023 International Conference on Electrical, Computer and Energy Technologies (ICECET), Cape Town, South Africa, 2023, pp. 1-6, doi: 10.1109/ICECET58911.2023.10389443.
49. V. Prakash, A. R. Mishra and S. Pandey, "A Perspective View of Bio-Inspire Approaches Employing in Wireless Sensor Networks," 2023 International Conference on IoT, Communication and Automation Technology (ICICAT), Gorakhpur, India, 2023, pp. 1-8, doi: 10.1109/ICICAT57735.2023.10263645.
50. Khan S, Khan MA, Alnazzawi N. Artificial Neural Network-Based Mechanism to Detect Security Threats in Wireless Sensor Networks. Sensors. 2024; 24(5):1641. https://doi.org/10.3390/s24051641
51. Arunkumar, P., & Savitha, K. K. (2024). Secure and Accurate Node Localisation and Route Optimization for Wireless Sensor Network (WSN). African Journal of Bio Sciences, 6(8), 435-449. https://doi.org/10.48047/AFJBS.6.8.2024.435-449
52. Sharma, S., Kaur, A., Gupta, D. et al. Dragon fly algorithm based approach for escalating the security among the nodes in wireless sensor network based system. SN Appl. Sci. 5, 376 (2023). https://doi.org/10.1007/s42452-023-05614-2
53. Loïc Desgeorges, Jean-Philippe Georges, Thierry Divoux, Detection of anomalies of a non-deterministic software-defined networking control, Computers & Security, Volume 129, 2023, 103228, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2023.103228.
54. S. Suma Christal Mary, S. Jothi Shri, E. Thenmozhi, K. Murugeswari, "Data Security in Wireless Sensor Networks using an Efficient Cryptographic Technique to Protect Against Intrusion," SSRG International Journal of Electronics and Communication Engineering, vol. 10, no. 4, pp. 41-50, 2023. Crossref, https://doi.org/10.14445/23488549/IJECE-V10I4P105
55. Kim, Y., Lim, E., & Kwon, T. (2024). On the Impact of Deployment Errors in Location-Based Key Predistribution Protocols for Wireless Sensor Networks. IEEE Access. DOI: 10.1109/ACCESS.2024.3372653
56. A. Afghantoloee and M. Abolfazl Mostafavi, "A Purpose-Oriented 3-D Voronoi Algorithm for Deployment of a Multitype Sensor Network in Complex 3-D Indoor Environments in Support of the Mobility of People With Motor Disabilities," in IEEE Transactions on Instrumentation and Measurement, vol. 73, pp. 1-13, 2024, Art no. 2519713, doi: 10.1109/TIM.2024.3398087.
57. S. Hafeez, "Blockchain-based Secure Unmanned Aerial Vehicles (UAV) in Network Design and Optimization," Ph.D. dissertation, School of Engineering, College of Science and Engineering, Univ. of Glasgow, Glasgow, U.K., 2024. doi: 10.5525/gla.thesis.84460. Available: https://theses.gla.ac.uk/id/eprint/84460.
58. Mainwaring, Alan & Polastre, Joseph & Szewczyk, Robert & Culler, David & Anderson, John. (2002). Wireless Sensor Networks for Habitat Monitoring. Proceedings of the ACM International Workshop on Wireless Sensor Networks and Applications. 10.1145/570738.570751.
59. Guides Publishing.(2023). The Network Effects Bible. Retrieved July 10, 2024, from the-network-effects-bible/121732
60. Shi D, Lü L, Chen G. Totally homogeneous networks. Natl Sci Rev. 2019 Oct;6(5):962- 969. doi: 10.1093/nsr/nwz050. Epub 2019 Apr 9. PMID: 34691957; PMCID: PMC8291615.

 doi:10.20944/preprints202505.0438.v1

61. [51]Liang, Junbin et al. “A Survey of Coverage Problems in Wireless Sensor Networks.” (2014).
62. Y. Jiang, L. Liu and J. Shu, "Overview of Key Node Evaluation in Complex Networks," 2023 3rd International Conference on Intelligent Communications and Computing (ICC), Nanchang, China, 2023, pp. 354-358, doi: 10.1109/ICC59986.2023.10421031.
63. M. Farsi, M. A. Elhosseini, M. Badawy, H. Arafat Ali and H. Zain Eldin, "Deployment Techniques in Wireless Sensor Networks, Coverage and Connectivity: A Survey," in IEEE Access, vol. 7, pp. 28940-28954, 2019, doi: 10.1109/ACCESS.2019.2902072.
64. A. Chatap and S. Sirsikar, "Review on various routing protocols for heterogeneous wireless sensor network," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2017, pp. 440-444, doi: 10.1109/I- SMAC.2017.8058388.
65. Singh, Samayveer & Chand, Satish & Kumar, Bijendra. (2017). Multilevel heterogeneous network model for wireless sensor networks. Telecommunication Systems. 64. 10.1007/s11235-016-0174-2.
66. Saravanakumar, R., Susila, S. G., & Raja, J. (2011). Energy efficient homogeneous and heterogeneous system for wireless sensor networks. International Journal of Computer Applications, 17(4), 33-38. doi:10.5120/2207-2805
67. Purkar, Santosh V., Deshpande, R. S., Energy Efficient Clustering Protocol to Enhance Performance of Heterogeneous Wireless Sensor Network: EECPEP-HWSN, Journal of Computer Networks and Communications, 2018, 2078627, 12 pages, 2018. https://doi.org/10.1155/2018/2078627
68. V. Kusla, G. S. Brar, V. K. Garg, A. Bansal and R. Kaushal, "Meta-heuristic Artificial Humming Bird Algorithm Based Energy Efficient Cluster Head Selection (MAHA-EECHS) in Wireless Sensor Networks," 2023 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, 2023, pp. 1-6, doi: 10.1109/ESCI56872.2023.10100064.
69. L. Yu, N. Wang, W. Zhang and C. Zheng, "Deploying a Heterogeneous Wireless Sensor Network," 2007 International Conference on Wireless Communications, Networking and Mobile Computing, Shanghai, China, 2007, pp. 2588-2591, doi: 10.1109/WICOM.2007.644.
70. Elfouly, F.H.; Ramadan, R.A.; Khedr, A.Y.; Yadav, K.; Azar, A.T.; Abdelhamed, M.A. Efficient Node Deployment of Large-Scale Heterogeneous Wireless Sensor Networks. Appl. Sci. 2021, 11, 10924. https://doi.org/10.3390/app112210924
71. Halder, Subir & Dasbit, Sipra. (2014). Enhancement of wireless sensor network lifetime by deploying heterogeneous nodes. Journal of Network and Computer Applications. 38. 106–124. 10.1016/j.jnca.2013.03.008.
72. Elif Bozkaya, Mumtaz Karatas, Levent Eriskin, Chapter 1 - Heterogeneous wireless sensor networks: Deployment strategies and coverage models, Editor(s): Kiran Ahuja, Anand Nayyar, Kavita Sharma, Comprehensive Guide to Heterogeneous Networks, Academic Press, 2023, Pages 1-32, ISBN 9780323905275, doi: https://doi.org/10.1016/B978-0-323-90527-5.00009-5.
73. Singh, Anuj Kumar and Patro, B.D.K, A Novel Security Protocol for Wireless Sensor Networks Based on Elliptic Curve Signcryption (November 8, 2019). International Journal of Computer Networks & Communications (IJCNC) Vol.11, No.5, September 2019, Available at SSRN: https://ssrn.com/abstract=3483512
74. Ferreira, Adrián & de Melo, Marco Aurélio & Oliveira, Leonardo & Habib, Eduardo & Wong, Hao & Loureiro, Antonio. (2005). On the Security of Cluster-Based Communication Protocols for Wireless Sensor Networks. 449-458. 10.1007/978-3-540-31956-6_53.
75. Y. Li, D. Yong and J. Ma, "Secure Message Distribution Scheme with Configurable Privacy for Heterogeneous Wireless Sensor Networks," 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, Shanghai, China, 2008, pp. 10-15, doi: 10.1109/EUC.2008.70.
76. Junyao He and Feng Xu 2020 J. Phys.: Conf. Ser. 1486 022052
77. Prasan Kumar Sahoo, Jonathan Jen-Rong Chen and Ping-Tai Sun, "Efficient security mechanisms for the distributed wireless sensor networks," Third International Conference on Information Technology and Applications (ICITA'05), Sydney, NSW, Australia, 2005, pp. 541-546 vol.2, doi: 10.1109/ICITA.2005.124.
78. A. AlBusaidi and F. H. Mohideen, "Analysis of Wireless Sensor Network Security Models: A Salient Approach for Deeper Inspection Using Deep Neural Networks," 2023 International Conference on Emerging Techniques in Computational Intelligence (ICETCI), Hyderabad,

India, 2023, pp. 276-282,
doi: 10.1109/ICETCI58599.2023.10330927.

79. Tan, L., Zheng, Q., & Chen, J. (2023). Providing an effective key management scheme to increase transaction security of homogeneous mobile wireless sensor networks. No DOI provided.
80. Urooj, S., Lata, S., Ahmad, S., Mehfuz, S., & Kalathil, S. (2023). Cryptographic Data Security for Reliable Wireless Sensor Network. No DOI provided.
81. Alghamdi, A., Al Shahrani, A. M., Alyami, S., Khan, I., Sri, P. S. G. A., Dutta, P., Rizwan, A., & Venkatareddy, P. (2023). Security and energy efficient cyber-physical systems using predictive modeling approaches in wireless sensor network. No DOI provided.
82. Kandasamy, M., Anto, S., Baranitharan, K., Rastogi, R., Satwik, G., & Sampathkumar, A. (2023). Smart Grid Security Based on Blockchain with Industrial Fault Detection Using Wireless Sensor Network and Deep Learning Techniques. Hindawi. doi: 10.1155/2023/3806121. PDF.
83. Alhasnawy, L. H., & Al-Mashanji, A. (2023). Improving Wireless Sensor Network Security Using Quantum Key Distribution. Baghdad Science Journal. doi:10.21123/bsj.2023.7460. PDF.
84. Sharma, I., Bhardwaj, A., & Kaushik, K. (2024). Enhancing agricultural wireless sensor network security through integrated machine learning approaches. Wiley Online Library. doi:10.1002/spy2.437.
85. Singh, T., & Vaid, R. (2024). Preserving Security in Terms of Authentication on Blockchain-Based Wireless Sensor Network (WSN). Journal of Sensor Networks.
86. Venkat, B., Kumar, V., Gopakumar, G., Subham, D., & Murali, K. (2024). Improved Security of Network Clock Synchronization in Wireless Sensor Networks. Journal of Network Security.
87. Sedhuramalingam, K., & Kumar, N. S. (2024). A Hybrid Rider Optimization with Deep Learning Driven Intrusion Detection Framework in Wireless Sensor Network. Journal of Intrusion Detection Systems.
88. LohithJ, J., Shreya, & Priya, H. (2024). Enhancing Wireless Sensor Network Longevity and Security: A Quad-LEACH Approach. Journal of Wireless Sensor Networks.
89. Sahaya, M., Jasvant, S. A., Sathees, R. S., Jeya, V., & Anitha, R. R. (2024). Enhancing Wireless Sensor Network Security Through Mutual Information Analysis for Intrusion Detection and Resilience. Journal of Engineering Science, 14(3), 2532-2546. doi:10.52783/jes.2532. PDF.
90. Zhang, Y., Jing, R., Ji, X., & Hu, N. (2023). Application of wireless sensor network technology based on artificial intelligence in security monitoring system. De Gruyter. doi:10.1515/comp-2022-0280. PDF.
91. Teng, Zhijun & Zhu, Sian & Li, Mingzhe & Yu, Libo & Gu, Jinliang & Guo, Liwen. (2023). Wireless sensor network security defense strategy based on Bayesian reputation evaluation model. IET Communications. 18. n/a-n/a. 10.1049/cmu2.12700.
92. Mir, Z. A., & Yadav, S. (2023). Leveraging Gray Wolf Optimization for enhanced security management in wireless sensor networks. Tuijin Jishu/Journal of Propulsion Technology, 44(4), 6295. No DOI provided.
93. Mehta, G., Bhuvneshwari, & Singh, A. (2023). Improved Wireless Sensor Network Security Through Node Leach Technique. IEEE Xplore. doi:10.1109/INOCON57975.2023.10100985.
94. Puttaswamy, C., & Shivaprasad, N. P. K. (2024). Enhancing wireless sensor network security with optimized cluster head selection and hybrid public-key encryption. International Journal of Electrical and Computer Engineering, 14(3), 2976-2987. doi: 10.11591/ijece.v14i3.pp2976-2987.
95. Vieira, M. A., & Liu, H. (2024). Defense against Black Hole Attacks in Wireless Sensor Network with Anomaly Report Cycling. Journal of Cyber-Physical Systems.
96. Vennam, P., & Mouleeswaran, S. K. (2024). Spiral Shape - Chimp Optimization Algorithm for Secure Cluster-Based Routing in Wireless Sensor Network. Journal of Network and Computer Applications.
97. Shanmathi, M., Sonker, A., Hussain, Z., Ashraf, M., Singh, M., & Syamala, M. (2024). Enhancing wireless sensor network security and efficiency with CNN-FL and NGO optimization. Measurement: Sensors, 24(101057). doi:10.1016/j.measen.2024.101057.
98. Venčkauskas, A., Taparauskas, M., Grigaliūnas, Š., & Brūzgienė, R. (2024). Enhancing Communication Security in In-Vehicle Wireless Sensor Network. Automotive Cybersecurity Journal.
99. Khan S, Khan MA, Alnazzawi N. Artificial Neural Network-Based Mechanism to Detect Security Threats in Wireless Sensor Networks. Sensors. 2024; 24(5):1641. https://doi.org/10.3390/s24051641

 doi:10.20944/preprints202505.0438.v1

100. Idris, I. A., & Issahku, F. Y. (2024). Advancing Wireless Sensor Network Security through the Implementation of Homomorphic Encryption for Secure and Private Image Processing. International Journal for Research in Applied Science and Engineering Technology. doi:10.22214/ijraset.2024.58180.
101. Jing Li, Xingjie Huang, Chan Wang, Jinmeng Zhao, Beibei Su, and Zhijie Shang "Design of heterogeneous network security device management platform based on multi-source data", Proc. SPIE 12702, International Conference on Intelligent Systems, Communications, and Computer Networks (ISCCN 2023), 127021F (16 June 2023); https://doi.org/10.1117/12.2680013
102. Lianwei Qu, Yong Wang, Jing Yang, and Meng Zhao. 2023. A heterogeneous network structure publishing security framework based on cloud-edge collaboration. Comput. Netw. 234, C (Oct 2023). https://doi.org/10.1016/j.comnet.2023.109947
103. Y. Hu, N. Shi, L. Lu and C. Wang, "Space-Air-Ground Integrated Heterogeneous Network Slicing with Native Intelligence,"
2023 IEEE/CIC International Conference on Communications in China (ICCC Workshops), Dalian, China, 2023, pp. 1-6,
doi: 10.1109/ICCCWorkshops57813.2023.10233779.
104. Z. Han et al., "Smart Optimization Solution for Channel Access Attack Defense Under UAV-Aided Heterogeneous Network," in IEEE Internet of Things Journal, vol. 10, no. 21, pp. 18890-18897, 1 Nov.1, 2023, doi: 10.1109/JIOT.2023.3281942.
105. Bouček, Vladimír & Husák, Martin. (2023). Recommending Similar Devices in Close Proximity for Network Security Management. 481-484. 10.1109/WiMob58348.2023.10187729.
106. Xabier Sáez-de-Cámara, Jose Luis Flores, Cristóbal Arellano, Aitor Urbieta, Urko Zurutuza, Clustered federated learning architecture for network anomaly detection in large scale heterogeneous IoT networks, Computers & Security, Volume 131, 2023, 103299, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2023.103299.
107. Yi, Junkai, and Lin Guo. 2023. "AHP-Based Network Security Situation Assessment for Industrial Internet of Things" Electronics 12, no. 16: 3458. https://doi.org/10.3390/electronics12163458.
108. Zhang J, Li Y, Zhang L. Heterogeneous network intrusion detection via domain adaptation in IoT environment. Internet Technology Letters. 2024;e531. doi: 10.1002/itl2.531
109. Yin, Changkui, Yingchi Mao, Zhenyuan He, Meng Chen, Xiaoming He, and Yi Rong. 2024.
"Edge Computing-Enabled Secure Forecasting Nationwide Industry PM2.5 with LLM in the Heterogeneous Network"
Electronics 13, no. 13: 2581.
doi: 10.3390/electronics13132581.
110. Bhanu, D.. Santhosh, R.. Heterogeneous Wireless Sensor Network Design with Optimal Energy Conservation and Security through Efficient Routing Algorithm. Journal of Journal of Cybersecurity and Information Management 13, no. 2 (2024): 140-154. DOI: https://doi.org/10.54216/JCIM.130211
111. Z. Wu, P. Xu and H. Fan, "Network Security Situation Assessment Method Based Eigenvector Centrality," 2024 International Wireless Communications and Mobile Computing (IWCMC), Ayia Napa, Cyprus, 2024, pp. 103-108,
doi: 10.1109/IWCMC61514.2024.10592357.
112. W. Wang, O. Abbasi, H. Yanikomeroglu, C. Liang, L. Tang and Q. Chen, "A Vertical Heterogeneous Network (VHetNet)-Enabled Asynchronous Federated Learning-Based Anomaly Detection Framework for Ubiquitous IoT," in *IEEE Open Journal of the Communications Society*, vol. 5, pp. 332-348, 2024, doi: 10.1109/OJCOMS.2023.3342008. https://doi.org/10.1109/OJCOMS.2023.3342008
113. Zhang, Wenbo, Mengxuan Wang, Guangjie Han, Yongxin Feng, and Xiaobo Tan. 2024. "A Knowledge Graph Completion Algorithm Based on the Fusion of Neighborhood Features and vBiLSTM Encoding for Network Security" Electronics 13, no. 9: 1661. https://doi.org/10.3390/electronics13091661
114. T. Quinn, S. D. Ali Shah, F. Bouhafs and F. Den Hartog, "Towards trust-based routing for data plane security in heterogeneous Software-Defined Wireless Networks," 2024 IEEE 10th International Conference on Network Softwarization (NetSoft), Saint Louis, MO, USA, 2024, pp. 37-42, doi: 10.1109/NetSoft60951.2024.10588898.
115. W. Yu, J. Qian, R. Xu, C. Jin, H. Fang and X. Shi, "Improving Substation Network Security with DevSecOps and AIOps," 2024 IEEE 10th Conference on Big Data Security on Cloud (BigDataSecurity), NYC, NY, USA, 2024, pp. 113-118, doi: 10.1109/BigDataSecurity62737.2024.00027.

 doi:10.20944/preprints202505.0438.v1

116. J. Li, M. Feng and S. Li, "A Deep Learning Cache Framework for Privacy Security on Heterogeneous IoT Networks," in IEEE Access, vol. 12, pp. 93261-93269, 2024, doi: 10.1109/ACCESS.2024.3422487.
117. Q. Zhang et al., "Optimal Age of Information and Throughput Scheduling in Heterogeneous Traffic Wireless Physical-Layer Security Communications," in IEEE Internet of Things Journal, vol. 11, no. 13, pp. 23644-23660, 1 July1, 2024, doi: 10.1109/JIOT.2024.3386765.