Mesopotamian journal of Cybersecurity
Vol.5, No.3, **pp**. 1199–1217
DOI: https://doi.org/10.58496/MJCS/2025/064; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Research Article

A Proposed Algorithm For Avoiding Jammer In Structure-Free Wireless Sensor Networks

Zainab Shaker Matar Al-Husseini[1,2,*], Hussain K. Chaiel [3], Amel Meddeb [4], Ahmed Fakhfakh[1]

[1] *Laboratory of Signals, Systems, Artificial Intelligence and Networks (SM@RTS), Digital Research Center of Sfax, University of Sfax, Sfax, Tunisia*

[2] *University of Diyala, College of sciences, Computer Sciences Department*

[3] *College of Engineering, University of Sumer, Rifae, Iraq*

[4] *National School of Electronic and telecommunication of Sfax, University of Sfax ,Sfax,Tunisia*

ARTICLEINFO

Article History

Received 20 Jun 2025
Revised 14 Aug 2025
Accepted 17 Sep 2025
Published 20 Oct 2025

Keywords

Denial-of-Service (DoS) attacks.

structure-free .

jamming.

wireless sensor networks (WSNs).

signal-to-jamming ratio (SJR) and attack.

ABSTRACT

Wireless Sensor Networks (WSNs) have emerged as a transformative technology with applications in critical and often inaccessible environments, including military and security domains. These networks comprise cooperative sensor nodes that gather and relay data to a base station. However, their inherent resource constraints—particularly the non-rechargeable nature of energy—pose a major challenge to network longevity and reliability. Conventional fixed-path transmission protocols exacerbate this issue, as energy-depleted or jammed nodes can disrupt communication, leading to partial or complete data loss. The primary objective of this study is to design and evaluate a structure-free transmission protocol that dynamically adapts data routing in order to optimize energy utilization and enhance resilience against jamming attacks. To achieve this, our study examines the impact of four distinct jammer types—Constant, Deceptive, Random, and Reactive—on key performance indicators, including energy consumption, signal-to-jamming ratio, and data rate. Simulation results reveal that jamming increases the number of transmission levels by up to 55%, with Deceptive Jammers generating the fewest and Constant Jammers the most. Energy consumption rises by as much as 62% under jamming, with Random Jammers causing the highest drain. Moreover, data rates increase by approximately 37% in the presence of jamming. These findings highlight the proposed protocol's effectiveness in mitigating jamming effects while preserving network energy, offering a robust solution for WSNs deployed in hostile or high-risk environments.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) represent a transformative advancement in sensing and communication technologies, enabling large-scale, real-time monitoring of physical phenomena in diverse and often challenging environments. Comprising spatially distributed, resource-constrained sensor nodes, WSNs have found applications in environmental monitoring, industrial automation, military operations, and security systems [1]-[4]. These sensor nodes typically integrate sensing, processing, communication, and power units, with the latter being the most critical resource due to its non-rechargeable nature [5]-[9]. The depletion of a node's energy directly impacts the network's longevity and reliability [10]-[12]. Figure 1 illustrates the architecture of WSNs.

*Corresponding author. myyusnani@gmail.com

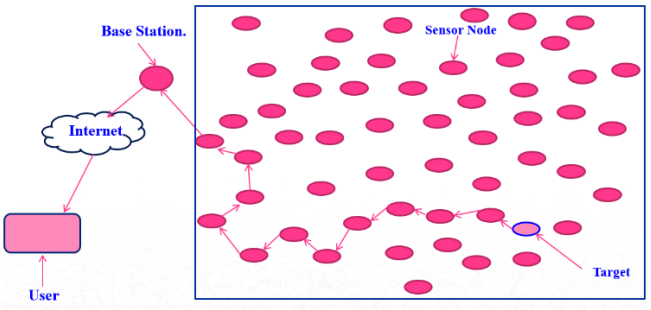

Fig .1. illustrates the architecture of WSNs..

Traditionally, WSN data transmission protocols have been structure-based, relying on fixed routing paths [13]-[18]. While straightforward, this approach introduces vulnerabilities: if an intermediate node is energy-depleted or subjected to malicious interference, communication along the path may be disrupted. Among the most severe threats is jamming, a form of denial-of-service (DoS) attack in which adversaries deliberately emit interference signals to degrade or block data transmission [19]-[22]. Jamming can be classified into several types—Constant, Deceptive, Random, and Reactive—each posing unique challenges to network performance and energy efficiency.

To address these limitations, this study proposes a structure-free transmission protocol designed to adapt routing paths dynamically, ensuring robust data delivery even in the presence of various jamming attacks. The primary objective of this study is to design, implement, and evaluate an adaptive, structure-free communication protocol that enhances energy efficiency, mitigates the adverse effects of four different jamming types, and ensures resilient data transmission in structure-free WSNs. Furthermore, the study investigates the protocol's impact on energy consumption, signal-to-jamming ratio, and data transmission under hostile conditions, providing insights into improving the reliability and longevity of WSN deployments.

The remainder of this paper is organized as follows: Section 2 introduces jamming and its types, Section 3 reviews related literature, Section 4 details the proposed protocol, Section 5 presents the studied scenarios, Section 6 provides the experimental results, and Section 7 concludes the study.

2. Jammer

After briefly introducing the background of jamming, this section explores the concept in depth. In the early 1900s, military radiotelegraphs were the primary targets of the first known jamming attempts. Russia and Germany were the pioneers in this regard. It was mostly co-channel characters that made up the jamming signals. The usage of ground radio during World War II is when the practice of jamming communications during warfare first emerged [23]-[28]. Jamming in wireless networks denotes intentional disruption of active communications by diminishing the signal-to-noise ratio at receivers by the transmission of interfering signals. Jamming and standard network interference are essentially distinct due to their intrinsic properties. Jamming is the purposeful deployment of wireless signals to disrupt communication, while interference denotes unintended disturbances that occur without conscious aim [29]. The principal determinant of jamming attack efficacy is the signal-to-noise ratio (SNR), mathematically defined as SNR = P_signal/P_noise, where P denotes average power. Jamming effectiveness is considered substantial when the signal-to-noise ratio SNR < 1[23]- [28], [30].

Unauthorized nodes that have infiltrated the wireless sensor network can conduct the jamming operation. These nodes demonstrate energy inefficiency, leading to a more rapid loss of energy compared to legal nodes [30], [31]. Deliberately placing the jamming nodes at an optimal distance from the genuine nodes can accomplish this. The classifications of jamming attacks in wireless sensor networks may be specified as follows[32]:-

A. Constant Jammer

The system generates a continuous flow of random bits that does not conform to the carrier sense multiple access (CSMA) protocol. Per the Carrier Sense Multiple Access (CSMA) protocol, a legal node must assess the condition of the wireless channel before commencing transmission. A frame may only be sent when the medium has been idle for a period equal to the DCF Interframe Space (DIFS). If the channel is found to be occupied during the Distributed Interframe Space (DIFS) time, the station must postpone its transmission. The continuous disruption caused by a relentless jammer obstructs authorized nodes from initiating communication, since it thoroughly saturates the wireless channel. This attack strategy exhibits considerable energy inefficiency and a substantial probability of detection. It is distinguished by its direct execution, making it exceptionally approachable. The adverse effect on network communications is substantial, culminating in a total failure of communication capability for all users [33]-[35].

B. Deceptive Jammer

The transmission technique entails the continuous emission of standard packets, rather than the stochastic bit release typical of a constant jammer. The jammer affects neighboring nodes by creating a false impression of a valid signal, compelling them to stay in a receptive state until it stops functioning or becomes inactive. Identifying a deceptive jammer is more complex than recognizing a continuous jammer since it sends authentic packets instead of random ones. The deceptive jammer, akin to the continuous jammer, demonstrates energy inefficiency owing to its perpetual gearbox; yet, it provides considerable installation convenience [33]-[36].

C. Random Jammer

The transfer of random bits or standard packets into networks happens sporadically. This gadget is specifically designed for energy saving, unlike the technologies above. The system experiences a cyclical transition between two separate states: a quiescent phase and a jamming period. The subject experiences a hibernating period, then by an active phase marked by jamming, before reverting to a dormant state. We can categories the lengths of the sleep and jam intervals as either preset or stochastic ones. A trade-off arises between jamming efficacy and energy saving, since the gadget cannot perform jamming tasks during its allocated sleep time. We can recalibrate the balance between efficiency and effectiveness by adjusting the ratios of sleep duration and leisure activities, like jamming [33]-[36].

D. Reactive Jammer

The reactive jammer exclusively triggers the jamming process upon the detection of network activity on a specific channel. Consequently, a reactive jammer is designed to obstruct the transmission of a message. Both small and large transmissions may be disrupted. The energy efficacy of a reactive jammer is lower than that of a random jammer as a result of the continuous network monitoring requirement. In practical scenarios, the inherent difficulty of precisely determining the packet delivery ratio (PDR) presents a greater challenge when detecting a reactive jammer than a proactive jammer[35]-[38].

2.1 Jammers' impact on wireless sensor networks

We elucidated in the preceding paragraphs that wireless sensor networks include a collection of wireless sensor nodes. These sensor nodes collaborate to monitor or send information between nodes. The existence of jamming devices in proximity to these sensor nodes might significantly impair the sent signal, resulting in its total obstruction. As a result, jamming devices halt or deactivate the entire network. These jamming devices then transmit signals. Figure 2 illustrates the impact of jamming devices on the network. The image clearly depicts a cluster of sensor nodes. These sensor nodes transmit data across nodes, ultimately reaching the base station. However, if it finds jamming devices, it might block them or prevent some nodes nearby from sending their data because of the signals from the jamming devices, as explained earlier.

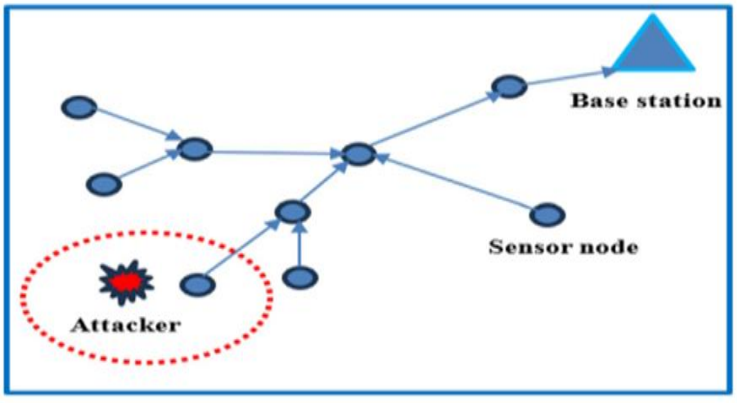

Fig .2. depicts the effect of a jammer on communication completeness in WSNs.

3. PREVIOUS WORKS

This section provides a thorough understanding of wireless sensor networks, including jamming and many forms of jamming devices. This section is a compilation of prior works on this subject. The operational guidelines for jamming in wireless sensor networks differ. Some concentrate on identifying jamming nodes inside the area, others on ascertaining the optimal transmission channel for information among jamming nodes, while some are oriented towards anti-jamming strategies and many other methodologies. Table 1 below presents a selection of prior works together with an indication of the direction of effort.

TABLE I. PREVIOUS STUDIES ON THE CONCEPT OF JAMMING IN WIRELESS SENSOR NETWORKS, CLASSIFIED BY THE STUDY'S EMPHASIS

Title	Direction	Addressed Problem	Technique/Approach	Ref.
"Deep Predictive Coding Neural Network for RF Anomaly Detection in Wireless Networks"	Interference detection	Jamming and RF spectrum interference	Neural network for predictive coding in spectrum anomaly detection	[39]
"Novel Hybrid Intrusion Detection System for Clustered Wireless Sensor Network"	Network intrusion detection	Jamming and intrusions in clustered WSNs	Hybrid anomaly and misuse detection using SVM	[40]
"A Statistical Approach to Detect Jamming Attacks in Wireless Sensor Networks"	A Statistical Method for Identifying Jamming Attacks in WSN	A Statistical Method for Identifying Jamming Attacks in WSN	A method for using statistics to identify jamming hazards in wireless sensor networks	[41]
"Jamming Detection Mechanisms for Wireless Sensor Networks"	Jamming Detection Mechanisms for WSN	Jamming Detection Mechanisms for WSN	Identifying jamming devices inside wireless sensor networks	[42]
"A Novel Jammer Detection Framework for Cluster-Based Wireless Sensor Networks"	Innovative Framework for Jammer Identification in Clustered WSN	Framework for detecting jammers in cluster-based wireless sensor networks	Innovative Framework for Jammer Detection in Cluster-Based Wireless Sensor Networks	[43]
"Tracking a Jammer in Wireless Sensor Networks Using Extended Kalman Filter"	Jammer Localization	Challenges in precisely monitoring mobile jammers in WSNs	Employs signal-to-noise ratios and the Extended Kalman Filter to ascertain jammer locations and identify boundary nodes for efficient tracking	[44]
"A Novel Location Pinpointed Anti-Jammer with Knowledge Estimated Localize"	Jammer Detection and Localization	Inefficiencies in the identification and localization of jammers in mobile wireless sensor networks	Introducing KNOWEL, which integrates energy detection and adaptive filtering to precisely identify and localize jammers, hence improving safe data transmission.	[45]
"A Fast Anti-Jamming Algorithm Based on Imitation Learning for WSN"	Machine Learning-Based Anti-Jamming	Challenges in acclimatizing to fluctuating jamming conditions	Proposes a rapid anti-jamming solution using imitation learning and recurrent neural networks, allowing WSN nodes to assimilate expert trajectories and optimize spectrum choices	[46]
"Jammed Node Detection and Routing in a Multihop Wireless Sensor Network Using Hybrid Techniques"	Hybrid Detection and Routing	Challenges in identifying jammed nodes and sustaining routing in multihop WSN	Proposes a hybrid approach that integrates fuzzy logic with ant colony optimization for the identification of jammed nodes and the facilitation of efficient routing	[47]
"Stackelberg Game Approaches for Anti-jamming Defence in Wireless Networks"	Game Theory-Based Anti-Jamming	Strategic engagements between assailants and protectors in WSN	Proposes anti-jamming communication solutions using Stackelberg game models to enhance defense mechanisms in hostile environments	[48]
"A Novel Jamming Attacks Detection Approach Based on Machine Learning for Wireless Communication"	Machine Learning	Conventional techniques are ineffective against sophisticated jammers	The study evaluates machine learning methods for jamming detection, such as random forests, support vector machines, and neural networks	[49]
"An Adaptive Anti-Jamming System in Hyper Ledger-Based Wireless Sensor Networks"	Anti-jamming security	Jamming attacks in blockchain-integrated WSNs	Adaptive system leveraging Hyperledger blockchain for secure communication	[50]
"Defeating Proactive Jammers Using Deep Reinforcement Learning for Resource-Constrained IoT Networks"	Anti-jamming communication	Proactive jamming in IoT networks	Deep Q-Network (DQN) variants tailored for low-power devices	[51]
"Jammer Location-Aware Method in Wireless Sensor Networks Based on Fibonacci Branch Search"	Jammer localization	Accurate localization of jammers in WSNs	Fibonacci Branch Search (FBS) algorithm for efficient jammer localization	[52]
"Game-Theoretic Learning Anti-Jamming Approaches in Wireless Networks"	Anti-jamming strategy	Developing intelligent anti-jamming strategies	Game-theoretic learning frameworks including Stackelberg and Markov games	[53]

This study delivers a novel and practical advancement for Wireless Sensor Networks (WSNs) by introducing a structure-free transmission protocol specifically designed to overcome the long-standing limitations of fixed-path routing that persist even in the most recent research. Unlike existing studies that predominantly focus on either jammer localization or jammer detection, our approach provides a comprehensive and integrated solution by combining three key contributions: dynamic structure-free routing, which eliminates dependency on fixed transmission paths and mitigates communication failures caused by energy-depleted nodes or targeted jamming; jamming-resilient operation, which effectively counters four distinct types of jammers (Constant, Deceptive, Random, and Reactive) by dynamically selecting secure and resource-efficient transmission nodes; and an energy-aware design, which conducts the first detailed analysis of WSN energy consumption under multiple jamming scenarios, highlighting quantifiable differences in resource depletion and emphasizing energy as the network's most valuable and vulnerable asset. By unifying these contributions into a single protocol, this work moves beyond incremental improvements and provides a robust, field-relevant solution to enhance the resilience, efficiency, and operational lifetime of WSN deployments in critical and hostile environments. In summary, while the majority of previous studies (Table 1) have focused primarily on jammer detection, localization, or isolated anti-jamming strategies, they have often overlooked the combined challenges of energy efficiency and resilience against multiple jamming types. In contrast, the present work introduces a unified structure-free protocol that simultaneously addresses dynamic routing, energy-aware operation, and robustness against four distinct jamming models, thereby filling a critical research gap and distinguishing itself from prior literature.

4. PROPOSED SYSTEM

This section introduces our innovative architecture designed to implement a dynamic (non-stationary) data transmission mechanism that overcomes the inherent limitations of structure-based approaches in Wireless Sensor Networks (WSNs). The proposed design not only enables efficient and flexible data delivery in structure-free environments but also integrates advanced strategies to detect, circumvent, and mitigate the impact of jamming attacks. Furthermore, the architecture explicitly addresses energy efficiency, analyzing power consumption patterns under the influence of different types of jammers—an aspect often overlooked in prior studies.

Figure 3 illustrates the conceptual framework of the proposed system. Initially, we describe the methodology for constructing a logical and adaptive network topology capable of maintaining operational continuity despite the presence of jammers. Subsequently, we detail a selective node qualification process that identifies optimal sensor nodes for data transmission, based on both resource availability and signal-to-jamming ratio (SJR) requirements for reliable event reporting. Finally, we outline the multi-hop relay selection strategy, which dynamically determines additional sensor nodes to ensure secure, uninterrupted data transfer even in hostile, jammer-rich environments.

This integrated approach distinguishes our work from existing research by simultaneously addressing transmission adaptability, anti-jamming resilience, and energy optimization within a unified protocol.

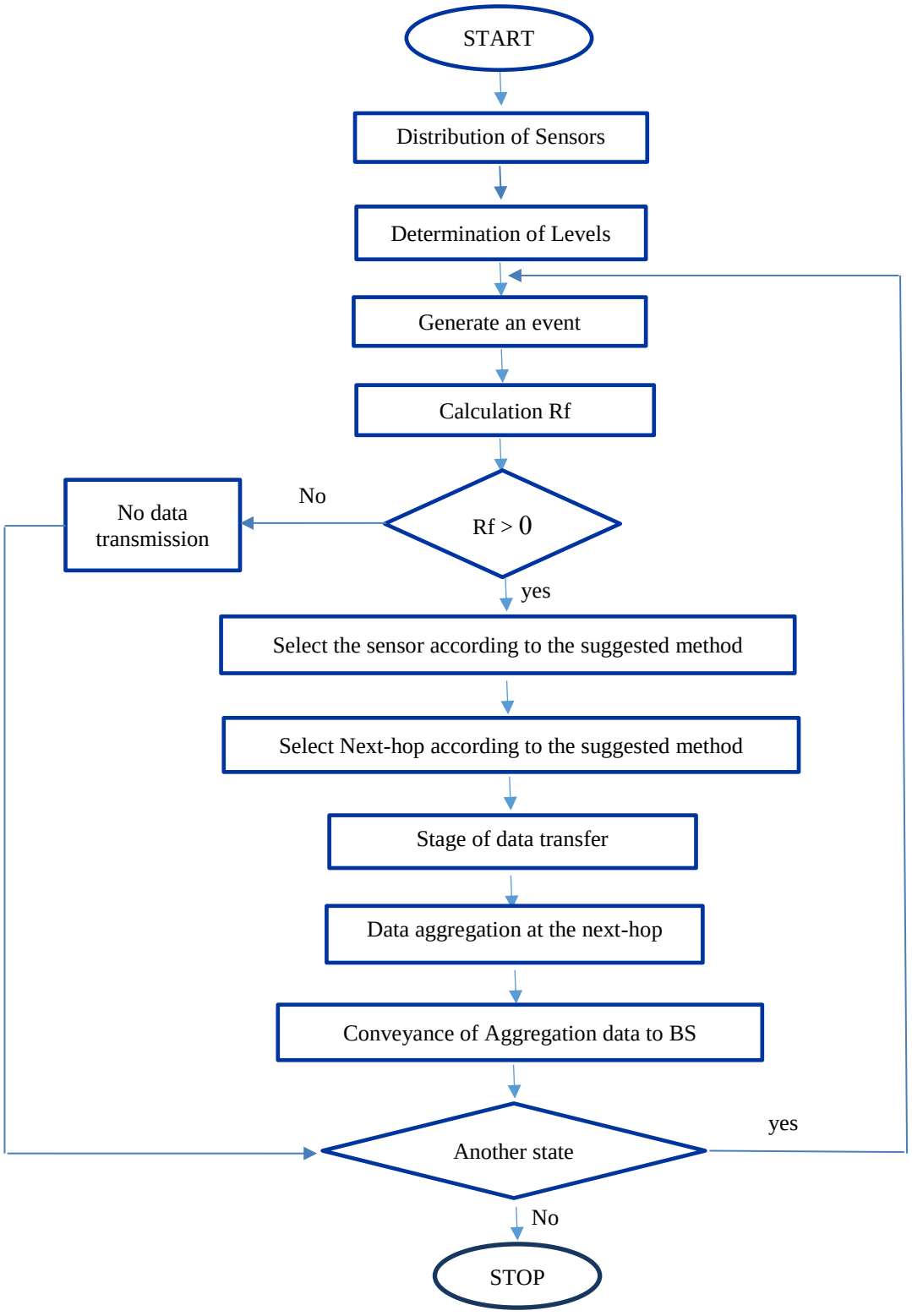

Fig .3. The block diagram of the suggested algorithm.

4.1 Topology Construction of Structure-Free Networks

Topology management mitigates issues that may emerge from the extensive number of nodes and their dense arrangement. Topology control preserves connection while using little power. During the setup or building phase of the network architecture, it is essential to ascertain the position of each sensor within its control region, the positions of neighboring nodes, and the base station (BS).

Each sensor node has a unique identification. Upon deployment of the sensor node, the base station (BS) initiates the phase for constructing the network topology. The research area assumes that there are jamming nodes, which makes setting up the network more complicated because these jamming nodes will be sending signals at the same time. Consequently, the signal-to-jamming ratio (SJR) primarily determines the construction or configuration of this topology.

The base station transmits a message, irrespective of its content. All nodes within the examined region may receive this message, contingent upon the Signal-to-Jamming Ratio (SJR) at these nodes being higher than or equal to one. This indicates that the signal from the base station may be accurately received; these nodes are classified as level one. Nodes with a Signal-to-Jamming Ratio (SJR) below one are classified as dead nodes, since they are significantly impacted by jamming nodes in the vicinity. Sensor nodes that successfully receive the message from the base station then retransmit it throughout the monitored region. Nodes capable of receiving the message, provided that their Signal-to-Jamming Ratio (SJR) is greater than or equal to one, are classified as Level 2 nodes. Nodes with a Signal-to-Jamming Ratio (SJR) below one are considered inactive or missing in our setup because they are heavily affected by interference from nearby nodes. Consequently, the transmission from one node to another develops the topology incrementally. The initial construction of this topology occurs only once. The following graphic (figure 4) illustrates this.

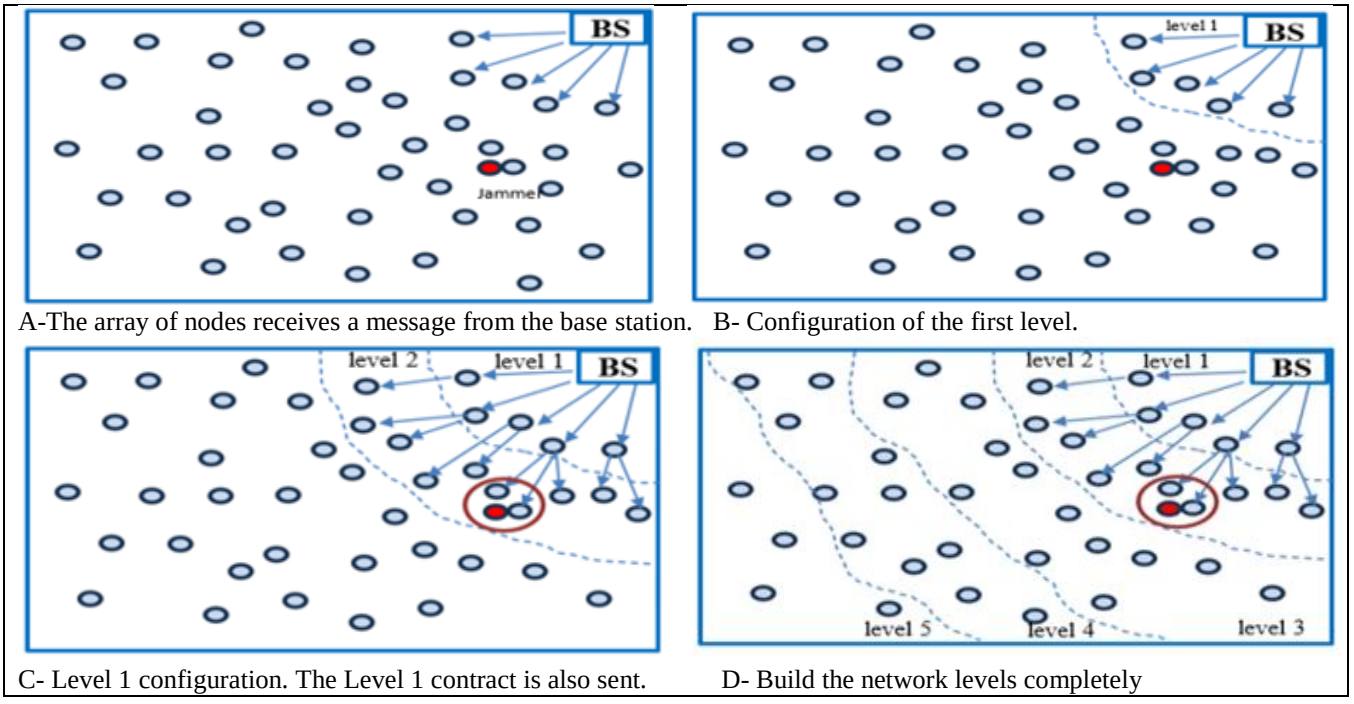

Fig .4. illustrates the logical topology designs of a sensing field equipped with jammers.

The figure 4 demonstrates the integrated construction or formation of the network topology. However, the presence of jamming nodes has blocked some sensor nodes from receiving signals or signals from other nodes. Therefore, they are considered dead or non-existent nodes, as indicated in the figure by the red circle. Since they cannot receive a signal, consequent to the signal obtained from the jamming nodes, the signal received from the jamming nodes exceeds the signal from the sensor nodes.

Without jamming nodes, a network can generate a maximum of three levels. With jamming nodes, the number of levels becomes five or six, and so on. In other words, the presence of jamming nodes increases the number of levels generated in a network. This behavior is what we observed during the simulation, and what will also be explained in the results presented later. In summary, we can state that jamming nodes placed in a specific area impact two stages: the first stage involves

constructing the network topology, and the second stage pertains to the reception and transmission of data within that network.

4.2 Monitoring of the events

Following deployment, the sensor nodes are randomly distributed across the designated area, with their quantity and specifications summarized in Table 2. Subsequently, the network topology—subject to interference effects—is established and configured, as detailed in Section 4.1.

We then present the methodology for monitoring diverse events occurring in locations that are either difficult or nearly impossible to access through conventional means, leveraging the capabilities of Wireless Sensor Networks (WSNs). In recent years, there has been growing interest in employing WSNs for the rapid and accurate monitoring of critical scenarios, such as supervising nuclear reactors or detecting faults in high-value equipment. WSNs are particularly well-suited for these applications, enabling the deployment of sensors in strategic locations to observe activities and relay the collected data via multi-hop transmissions to a base station for appropriate response.

Recent studies indicate that integrating multimedia sensors within a WSN enhances the system's ability to monitor multiple event types simultaneously, improving the precision of event characterization as more data is acquired. When an event occurs within the monitored region, the Relational Factor (Rf) for each affected sensor node is computed, as described in Section 4.2.1. The sensor node with the lowest topological level and an Rf greater than zero is identified as the primary node of interest. Furthermore, the Signal-to-Jammer Ratio (SJR) for this node must be ≥ 1, ensuring reliable data transmission to a neighboring sensor node.

The selected node—having met these criteria—is considered the most likely to have accurately detected the event. It then selects an adjacent node within communication range for data forwarding. This process continues iteratively, with each node selecting the next relay, until the data ultimately reaches the base station. A detailed description of the relay node selection procedure is provided in Section 4.3.

4.2.1. Calculation of the Relational Factor (Rf)

When a specific event occurs within the monitoring range of the deployed sensors, the Relational Factor (Rf) for each sensor node located within the event's sensing range is computed using the following equation:

$$Rf = (SL - d\ Event\_sensor) / d\ Event\_sensor \quad \textbf{(1)}$$

Where:

- **SL** represents the sensitivity level of the sensor node.
- **d_{Event_sensor}** denotes the distance between the event location and the sensor node.

A sensor node is selected as a candidate for data forwarding if it satisfies the following conditions:

1. **Signal-to-Jammer Ratio (SJR) ≥ 1**, indicating that the node is not significantly affected by jamming devices to the extent that it cannot transmit the sensed data.
2. **Rf > 0**, meaning the node has successfully detected data from the specific event.
3. Possesses the **lowest topology level**, thereby minimizing the transmission path length and reducing energy consumption.

Once a qualifying node is identified, it selects another node within its communication range for data forwarding. This process is repeated in a multi-hop manner passing data from one node to the next until the information ultimately reaches the base station. The detailed procedure for selecting the subsequent sensor node is provided in **Section 4.3**.

4.3 Selection of Subsequent Node

Each sensor node selects the next node to transmit information to according to a cost function. This cost function is formulated based on the next hop node's remaining energy, available buffer capacity, and signal-to-Jamming ratio (SJR). Each sensor node identifies the neighboring sensor holding group and selects one of these neighbors for data redirection according to a consistent cost function. Every node possesses a distinct sensor information table. The information includes the node's ID, available buffer (Buffst), signal-to-jamming ratio (SJR), and residual energy (E resd).

When a certain node detects data or gets a data packet from the upper-level nodes, it transmits it to a lower-level node, continuing this process until it reaches the base station (BS). The node computes the cost function for all subsequent elements. The lower-level node j (Nj) designates the subsequent jump node i (Ni) with the highest value of the cost function (CF max). The Signal-to-Jamming Ratio (SJR) of the subsequent node must be at least 1 to guarantee accurate data reception and transmission. A particular sensor node may qualify to receive data or information, provided that its power and storage capacity are substantial. However, its Signal-to-Jamming Ratio (SJR) is less than one, which means the node cannot effectively receive or send data because of interference from jamming devices in the area being studied.

Consequently, the Signal-to-Jamming Ratio (SJR) of the candidate node must be higher than or equal to one. The cost function is determined by.

$$\mathbf{CF}\ max = \boldsymbol{max}\ (i \in N)\ \{\alpha(\frac{\text{available energy .i}}{\text{initial energy}} + \frac{\text{available buffer.i}}{\text{initial buffer}} + \text{SJR})\ \} \quad (2)$$

Where N represents a set of neighbors of Nj

α denotes the inverse, with the distance between the designated coordinates of the transmitting and receiving nodes calculated as follows: -

$$\alpha = 1/\sqrt{(xt - xr)^2 + (yt - yr)^2} \quad (3)$$

Available energy. i: The next hop node's remaining energy.

Available buffer. i: The next hop node's available buffer capacity.

SJR: The Signal-to-Jamming Ratio of the subsequent node.

TABLE II. SIMULATION PARAMETERS.

sensor field area	500 *500 m2
Quantity of sensor nodes	400
Packet size	60 bytes
Length of buffer	65 packets
Preliminary node energy	70 J
Data transmission capacity	200 Kb/s
Detection length	50 m
Radio coverage	40 m
E elec	50 nanojoules per bit
E sense	0.083 watts
E agg	5nJ/bit/signal
E amg	10 pJ/bit/m2
Number of run attempts per 35 minutes	25 run
Total run time	35 minute
Total jamming power	100watt/MHz
Sensing length of jammer	50 m
Radio range of jammer	40 m
Saving time for random jammer	25%

5. FACTORS STUDIED

5.1 Distribution of sensors

The deployment process commences with the distribution of sensor nodes across the designated simulation area, measuring 500 × 500 m². For this study, a random deployment strategy is employed, reflecting realistic scenarios in which wireless sensor networks are utilized in hazardous, remote, or otherwise inaccessible environments. Such conditions often preclude manual placement, making random deployment the most viable and safe alternative. This strategy not only enhances the practicality of the network setup but also aligns with the research objective of evaluating network performance under real-world constraints. Figure 5 presents the resulting spatial distribution of the randomly deployed sensor nodes within the simulated environment.

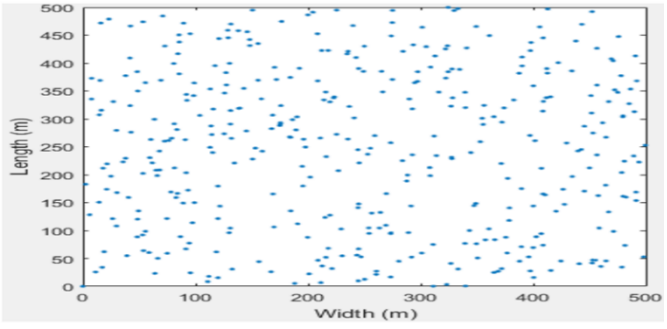

Fig .5. . Randomly distribute sensor nodes throughout the studied area.

5.2 Levels Determination

As established in Section 4.1, the formation of hierarchical levels within the network topology plays a critical role in the proposed data transmission mechanism. These levels facilitate systematic and energy-efficient data transfer, ensuring that information flows progressively from higher to lower levels until the Base Station (BS) is reached. For instance, when a Level 5 sensor node detects an event, it transmits the corresponding data to a designated Level 4 node. This process continues sequentially through lower levels, Level 3, Level 2, and Level 1, until the data reaches Level 0, where the BS resides. Such a structured approach minimizes transmission distance at each step, reducing energy consumption and improving network longevity. Figure 6 illustrates the level-based network topology in the absence of jamming devices.

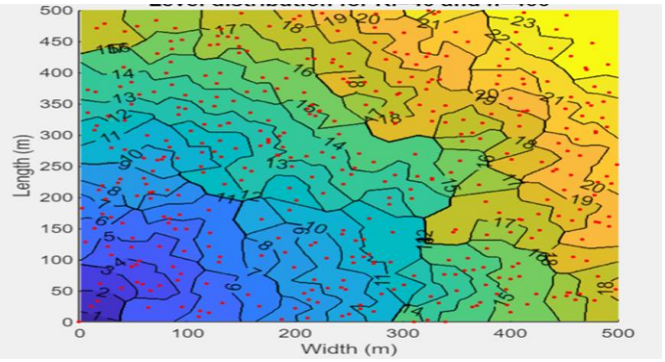

Fig .6. Level configuration in structure-free WSNs

5.3 Jammer Distribution

A set of jammer nodes was randomly distributed throughout the studied area. To study the subject fully, the jammer nodes were distributed in varying numbers—one, two, or three. We obtained the results below during the simulation.

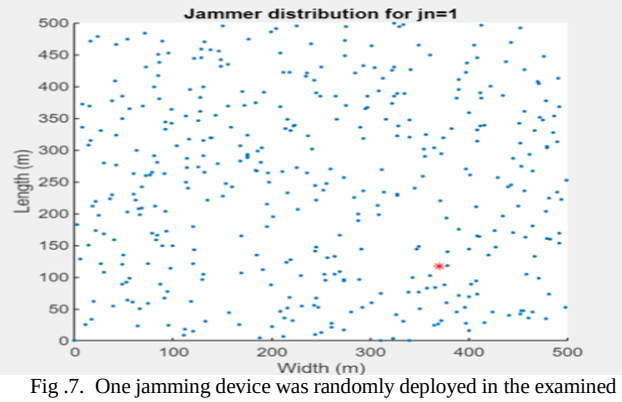

Fig .7. One jamming device was randomly deployed in the examined region..

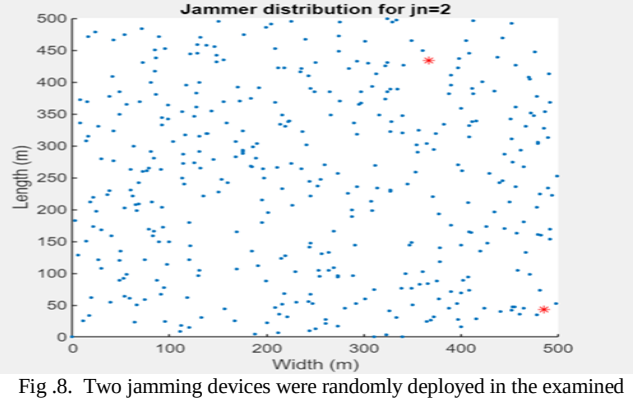

Fig .8. Two jamming devices were randomly deployed in the examined region.

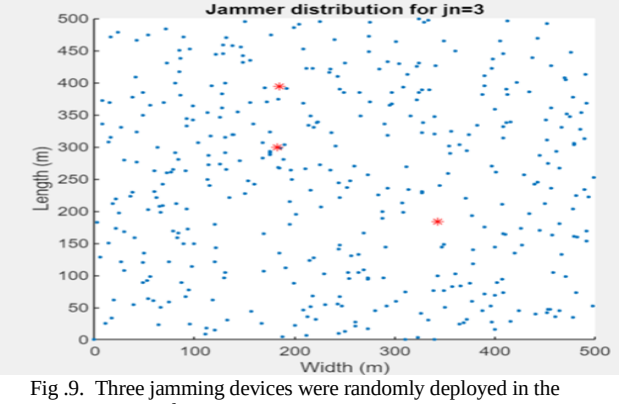

Fig .9. Three jamming devices were randomly deployed in the examined region.

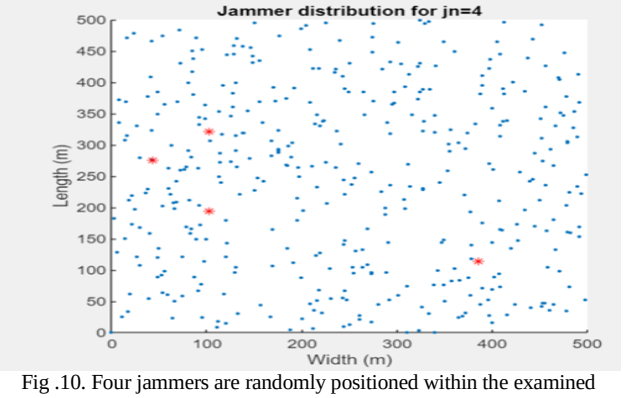

Fig .10. Four jammers are randomly positioned within the examined region.

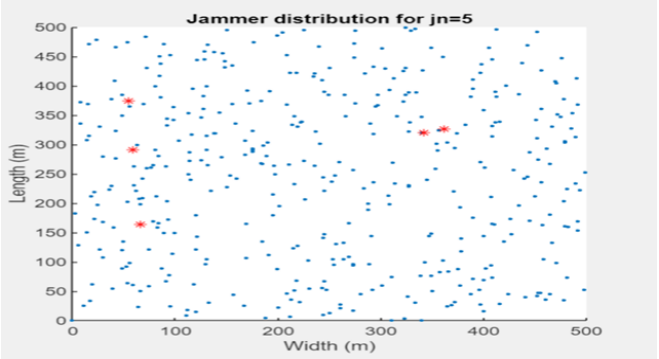

Fig .11. Five jamming devices randomly positioned inside the examined region.

5.4 Level Formation Under the Influence of Jamming Devices

As described in Section 4.1, the process for constructing hierarchical levels within the network topology was introduced, and Section 5.2 illustrated the formation of these levels in the absence of jamming nodes in the studied area. In this section, we investigate how the presence of jamming nodes disrupts this critical and foundational stage of the proposed protocol. Jamming interference results in the creation of coverage voids within the monitored area, which in turn fragments the network and necessitates the formation of additional hierarchical levels. This not only increases the overall transmission path length but also escalates energy consumption, thereby reducing the efficiency and reliability of data delivery. The figures provided below depict scenarios involving different types of jamming nodes, beginning with the case of a single jammer. Furthermore, we will present below the resulting levels formed under the influence of the four studied types of jamming devices.

A. Constant Jammer

This type emits a random signal over the wireless channel, ensuring that the bandwidth always remains busy. This signal hinders wireless nodes' ability to transmit data.

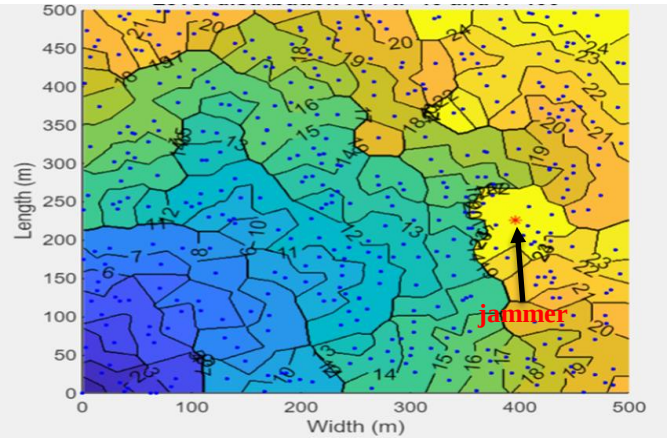

Fig .12. Deploy one Constant Jammer node randomly throughout the studied area.

Figure 12 illustrates the studied area following the deployment of a single constant jamming node. It can be observed that the number of hierarchical levels has increased compared to Figure 6, which depicts the topology without any jamming. Additionally, an unmonitored region effectively a coverage gap has emerged within the studied area. This gap is a direct consequence of the constant jammer's interference, whereby the sensor nodes located within its range are adversely affected by the continuous emission of jamming signals, rendering them incapable of participating in effective data transmission.

B. Deceptive Jammer

This jamming emits an uninterrupted stream of radio bits inside the communication channel. The legitimate receiving node is specific that consistent communication has transpired. This jamming is more effective than the continuous type and harder for the wireless network to find, but it uses more energy. The figure below (Figure 13) shows the studied area after deploying a single Deceptive jammer. We notice that the location of this jammer was randomly located in the location

shown in the figure above (Figure 13). Consequently, the end of the studied area became like a gap. In other words, the jammer nodes started to affect an area that was not visible.

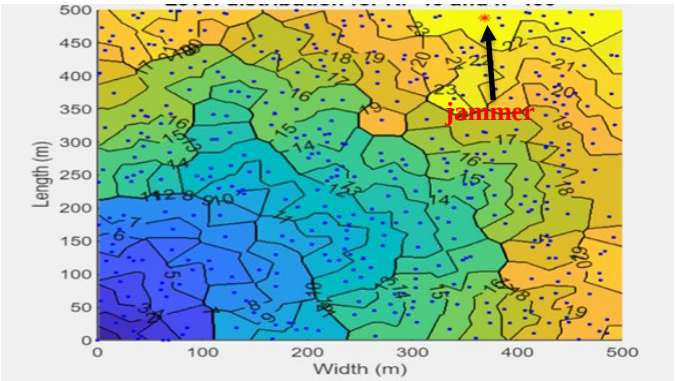

Fig .13. Deploy a single Deceptive Jammer node randomly throughout the studied area.

C. Random Jammer

This type of jammer is operational for a specific duration, after which it ceases transmission for some time to conserve energy. Consequently, the energy consumption necessary is lower than that of the constant and second varieties.

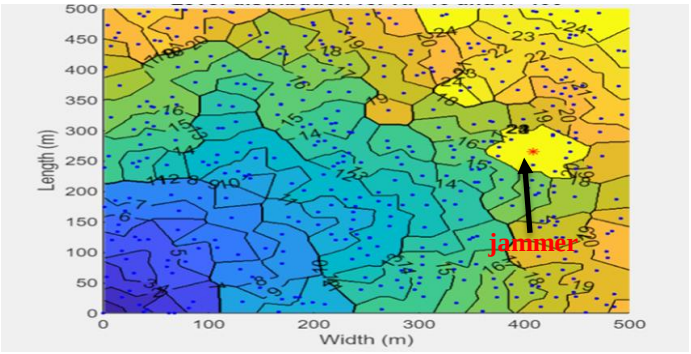

Fig .14. Deploy a single Random Jammer node randomly throughout the studied area.

Figure 14 presents the studied area after deploying a single random jamming node. The number of hierarchical levels has increased compared to Figure 6, which represents the topology without jamming nodes. Moreover, a coverage gap—or unmonitored region—has emerged within the study area. This gap results from the interference exerted by the random jammer on nearby sensor nodes through the emission of jamming signals. As previously outlined in our discussion of jammer types, this category operates intermittently, alternating between active and inactive states. The timing of these operational periods is nondeterministic, thereby introducing a degree of unpredictability into the network's performance.

D. Reactive Jammer

Upon monitoring the wireless transmission channel's activities, this sort of jammer emits a random signal to disrupt the original signal.

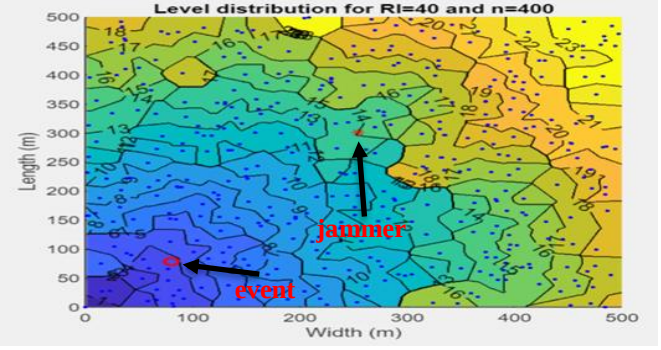

Fig .15. Deploy one Reactive Jammer node randomly throughout the studied area.

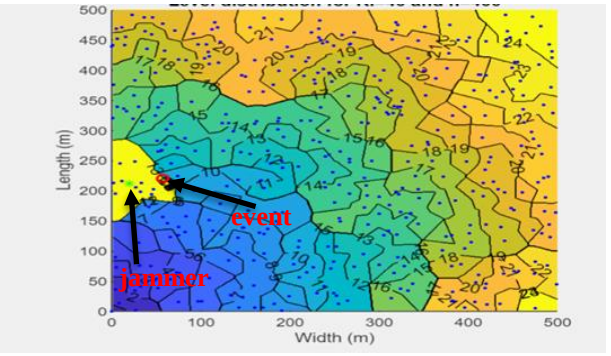

Fig .16. Deploy one Reactive Jammer node randomly throughout the studied area.

Figure 15 illustrates the deployment of a single reactive jammer node. In this scenario, no event occurred in proximity to the jammer node; hence, its operation, as previously described, produced no observable impact. Specifically, there was neither an increase in the number of hierarchical levels nor the formation of coverage gaps within the studied area. To effectively demonstrate the operational mechanism of this jammer type, the simulation was executed approximately fifteen times until a reactive jammer node was positioned near the event. Under these conditions, observable changes emerged in the network topology, including an increase in the number of levels and the appearance of a coverage gap, as depicted in Figure 16.

5.5 The path followed by transmission

This section illustrates the transmission path from a sensor node that has detected a specific event to subsequent sensor nodes, continuing until the data reaches the Base Station. The accompanying figures compare the conventional transmission path with the path established by the proposed protocol, highlighting the differences in routing efficiency and resilience. The visual representations below provide a clear demonstration of these transmission patterns.

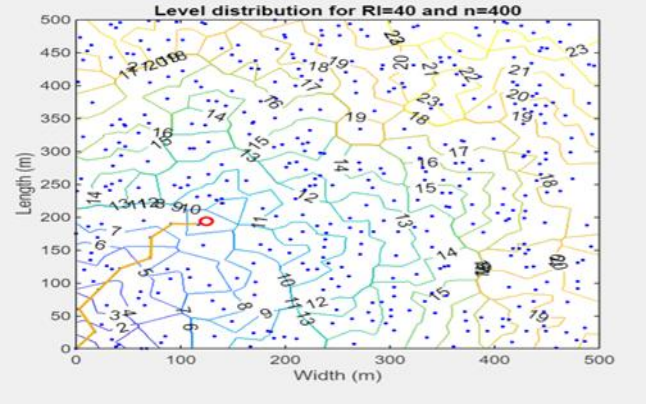

Fig .17. The traditional path of a single event generated through the studied area.

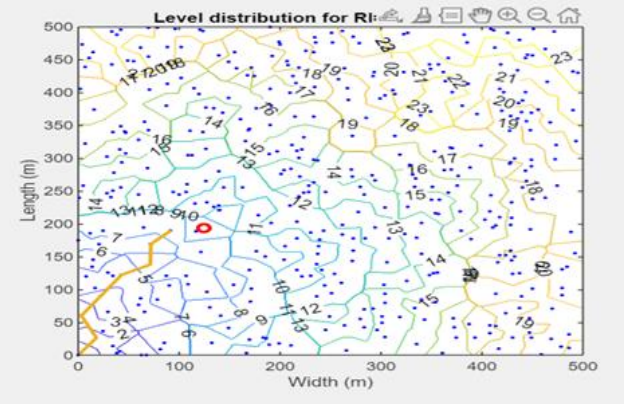

Fig .18. The path followed by the proposed method for a single event generated through the studied area.

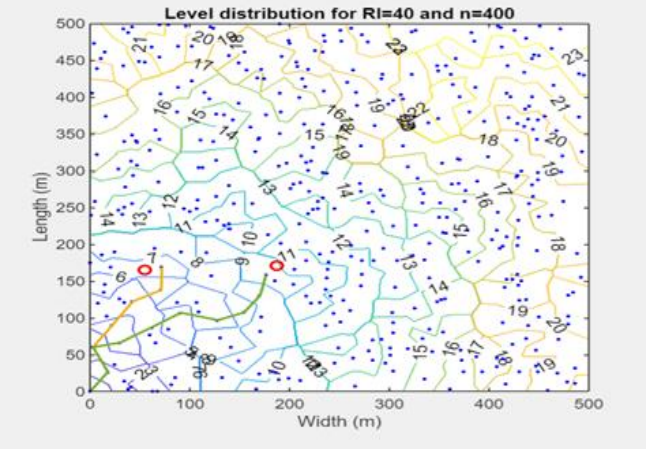

Fig .19. The traditional path of two events generated through the studied area

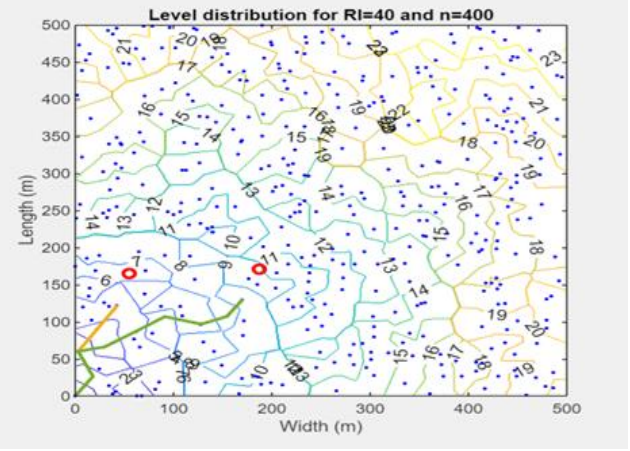

Fig .20. The suggested technique delineates the trajectory for the two generated occurrences inside the examined region.

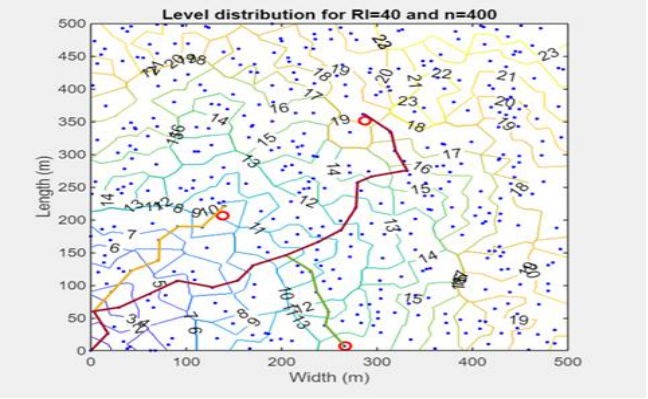

Fig .21. illustrates the trajectory of the Traditional method, showing three occurrences produced within the examined region.

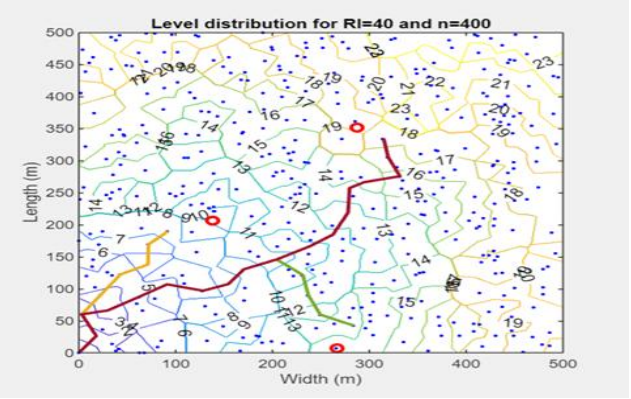

Fig .22. The path followed by the proposed method for three events generated within the studied area.

The figures above compare data transmission paths for one, two, or three detected events using the traditional deterministic approach and the proposed topology-free protocol. In the traditional approach, routing follows long paths, thus consuming more energy.

In contrast, the proposed topology-free protocol dynamically selects the next routing node based on the remaining energy, signal-to-Jamming ratio (SJR), and proximity to the destination. This adaptive capability shortens the overall transmission path, reduces the number of hops, minimizes end-to-end delay, and reduces energy consumption, improving efficiency and extending the network lifetime. Furthermore, it maintains reliable data transmission even in the presence of jamming nodes or environmental changes, which is critical for mission-critical wireless sensor network (WSN) applications.

6. SIMULATION RESULTS

The following section presents the simulation results obtained for the proposed protocol. As previously described, it employs a changeable (non-stationary) transmission mechanism to overcome the limitations of fixed-path transmission. The protocol is designed to be jammer-resistant, and its performance was evaluated against four different types of jamming devices.

6.1 Relationship between Number of Jammer Nodes and Number of Levels Formed

The simulation results show a direct relationship between the number of jammer nodes deployed in the network and the number of levels formed within the topology. As the number of jammer nodes increases, the number of levels also increases, reflecting the disruptions introduced by jamming signals that force data to traverse longer and more complex paths. This effect contributes to higher energy consumption and may also create unmonitored regions within the coverage area.

These findings, illustrated in Figure 23, demonstrate the significant influence of jamming activity on both the structural integrity and operational efficiency of wireless sensor networks.

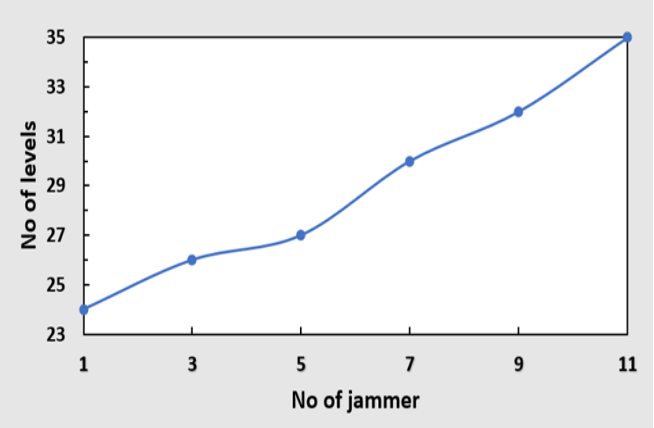

Fig .23. The correlation between the quantity of jammers and the number of levels established in structure-free wireless sensor networks (WSNs).

6.2 Relationship between Signal-to-Jamming Ratio (SJR) and Number of Levels Formed

The results indicate a clear relationship between the signal-to-jamming ratio (SJR) and the number of levels established in the network. As the SJR increases, the number of levels also rises, although the rate of this increase varies among the four jammer types studied—Constant, Deceptive, Random, and Reactive.

Among them, the Constant jammer produced the highest number of levels, signifying the strongest structural disruption, while the Deceptive jammer resulted in the lowest number. The Random and Reactive jammers displayed intermediate effects.

This comparison, shown in Figure 24, highlights the distinct operational patterns of different jammer types and their corresponding impacts on routing complexity, energy consumption, and network coverage.

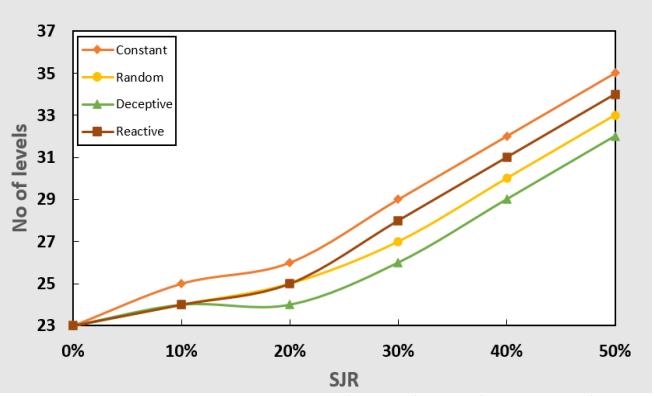

Fig .24. Relationship between signal-to- jamming ratio (SJR) and number of levels formed for structure-free wireless sensor networks with different types of jammers.

6.3 Relationship between Signal-to-Jamming Ratio (SJR) and Level Formation Time

The experimental analysis reveals that higher SJR values are associated with longer times required to form levels within the proposed protocol. This pattern is observed across all jammer types, though the extent of the effect differs.

The Constant jammer showed the shortest formation times, indicating relatively lower temporal disruption, while the Random jammer produced the longest times, reflecting its unpredictability and stronger influence on dynamic routing. The Deceptive and Reactive jammers resulted in intermediate formation times.

As illustrated in Figure 25, these observations emphasize how jammer type and SJR jointly affect the temporal efficiency of level formation, providing key insights into protocol performance under varying interference conditions.

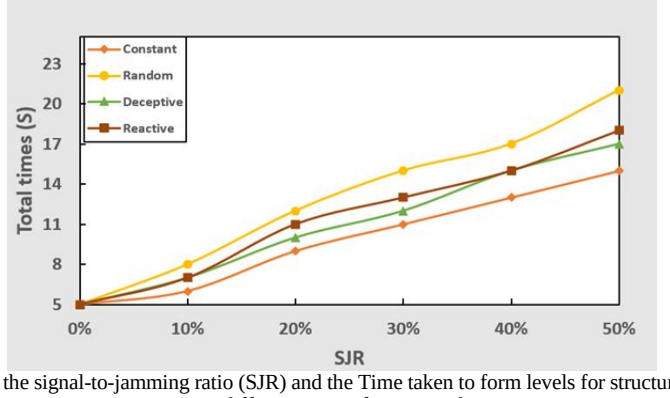

Fig .25. The relationship between the signal-to-jamming ratio (SJR) and the Time taken to form levels for structure-free WSNs with the presence of different types of jamming devices.

6.4 Event Period and Energy Consumption

Another key parameter used to evaluate the performance of the proposed system is the relationship between the event period and total energy consumption, examined under both jamming and non-jamming conditions. The results indicate that shorter event periods lead to higher overall energy consumption. This outcome arises because, within the fixed operational time of 35 minutes (as set in the simulation parameters), shorter event durations allow for more events to occur, thereby

increasing the total energy required. Conversely, longer event periods result in fewer events, leading to lower cumulative energy usage.

The analysis also shows that the presence of jamming nodes amplifies total energy consumption compared to scenarios without interference. Among the four jammer types, the Constant jammer resulted in the lowest additional energy consumption, while the Random jammer produced the highest, reflecting its irregular and unpredictable interference patterns.

These findings, illustrated in **Figure 26**, highlight how both event periodicity and jammer characteristics influence network energy efficiency and event-handling performance.

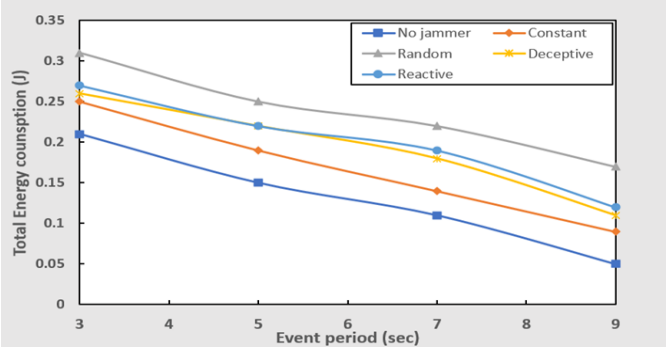

Fig .26. Power consumption and event duration of structure-free WSNs with the presence of different types of jammers.

6.5 Data Rate and Energy Consumption

An additional performance metric assessed in this study is the relationship between data transmission rate and total energy consumption. The results show that higher transmission rates lead to increased overall energy usage, as the greater number of packets sent during the event period requires more power for both transmission and processing. For example, transmitting at 400 bits per second consumes more energy than at 200 bits per second, due to the larger data volume handled within the same timeframe. The energy consumption values shown in Figure 27 reflect the cumulative energy expenditure of all events and sensor nodes along the communication path in each simulation scenario.

A comparison of scenarios with and without jamming further indicates that the presence of jamming nodes significantly elevates energy consumption. However, the degree of increase differs depending on the jammer type. Among the four studied devices, the Constant jammer produced the lowest additional consumption, while the Deceptive and Reactive jammers yielded similar intermediate values. The Random jammer consistently resulted in the highest energy consumption, attributable to its irregular and unpredictable interference behavior.

These findings, summarized in Figure 27, highlight the combined influence of transmission rate and jammer characteristics on the overall energy efficiency of wireless sensor networks.

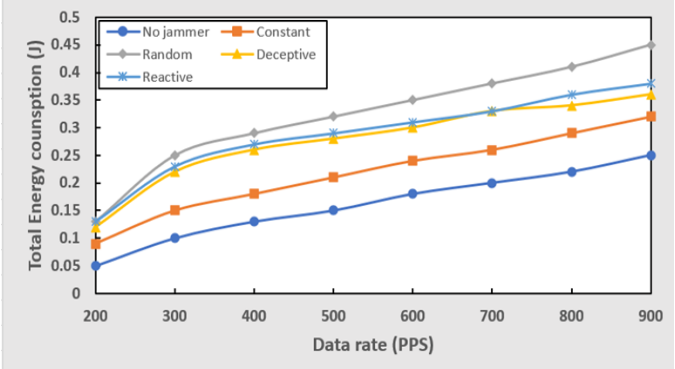

Fig .27. Different types of jammers affect power consumption and data rates in structure-free wireless sensor networks.

7. CONCLUSION

This study addressed the challenge of jamming in structure-free wireless sensor networks (WSNs) by proposing a dynamic, energy-aware transmission protocol capable of adapting to diverse jamming scenarios. Unlike conventional fixed-path routing, the proposed approach avoids structural rigidity by dynamically selecting transmission paths according to residual energy, signal-to-jamming ratio (SJR), and proximity to the destination node.

The simulation analysis yielded several key findings. First, the presence of jammer nodes significantly altered network topology by increasing the number of hierarchical levels, which led to longer communication paths, higher energy consumption, and potential coverage gaps. Second, the signal-to-jamming ratio strongly influenced both the number of levels and the time required for their formation, with each jammer type exhibiting distinct interference characteristics. Third, event duration and data transmission rate directly impacted total energy consumption, with random jammers consistently producing the highest energy overhead.

Collectively, these findings demonstrate the resilience and adaptability of the proposed protocol. By integrating jammer-resilient routing with energy-aware decision-making, the protocol effectively reduces delays, balances resource utilization, and prolongs network lifetime, even under severe interference from Constant, Deceptive, Random, and Reactive jammers. In summary, this work makes two primary contributions: (i) it delivers the first integrated assessment of energy efficiency, structural dynamics, and resilience under multiple jamming types, and (ii) it introduces a practical structure-free anti-jamming protocol that enhances both reliability and operational sustainability. These contributions provide a strong foundation for deploying WSNs in mission-critical applications such as disaster recovery, environmental monitoring, and military surveillance, where secure and efficient communication is essential.

Conflicts of Interest

The authors declare no conflicts of interest.

Funding

The authors acknowledge that the research was carried out at their own expense and without any financial funding from a private or governmental institution.

Acknowledgment

The author is grateful to the institution for their collaboration and provision of necessary facilities that contributed to the successful completion of this research.

References

[1] B. Krishnamachari, Networking Wireless Sensors. Cambridge, U.K.: Cambridge Univ. Press, 2005.
[2] R. Priyadarshi, “Energy-efficient routing in wireless sensor networks: A meta-heuristic and artificial intelligence-based approach: A comprehensive review,” Arch. Comput. Methods Eng., vol. 31, no. 4, pp. 2877–2915, Jan. 2024, doi: 10.1007/s11831-023-10039-6 .
[3] D. W. Wajgi and J. V. Tembhurne, “Localization in wireless sensor networks and wireless multimedia sensor networks using clustering techniques,” Multimedia Tools Appl., vol. 83, no. 3, pp. 6829–6879, Jun. 2023, doi: 10.1007/s11042-023-15956-z .
[4] I. Stojmenovic, Handbook of Sensor Networks. Hoboken, NJ, USA: Wiley, 2005.
[5] A. I. Al-Sulaifanie, B. K. Al-Sulaifanie, and S. Biswas, “Recent trends in clustering algorithms for wireless sensor networks: A comprehensive review,” Comput. Commun., vol. 191, pp. 395–424, Jul. 2022, doi: 10.1016/j.comcom.2022.05.006 .
[6] M. M. Afsar and M.-H. Tayarani-N, “Clustering in sensor networks: A literature survey,” J. Netw. Comput. Appl., vol. 46, pp. 198–226, Nov. 2014, doi: 10.1016/j.jnca.2014.09.005 .
[7] S. A. Hussein et al., “Integrating law, cybersecurity, and AI: Deep learning for securing iris-based biometric systems,” Mesopotamian J. Cybersecurity, vol. 5, no. 2, pp. 319–336, 2025, doi: 10.58496/MJCS/2025/020 .
[8] H. K. Chaiel, Z. S. M. Al-Husseini, and K. I. Arif, “Energy enhancement techniques for structure-free wireless sensor network with encrypted data,” Int. J. Sens. Wireless Commun. Control, vol. 10, no. 3, pp. 402–412, Jun. 2019.
[9] X. Sun, S. Yan, B. Wang, L. Xia, Q. Liu, and H. Zhang, “Air temperature error correction based on solar radiation in an economical meteorological wireless sensor network,” Sensors, vol. 15, no. 8, pp. 18114–18139, Jul. 2015, doi: 10.3390/s150818114 .

[10] M. Albdair, Z. R. Mohsin, A. Saihood, A. M. Hamad, and A. Sahi, "Secured multi-objective optimisation-based protocol for reliable data transmission in underwater wireless sensor networks," Mesopotamian J. Cybersecurity, vol. 5, no. 1, pp. 216–239, Mar. 2025, doi: 10.58496/MJCS/2025/015 .
[11] S. P. Singh and S. C. Sharma, "A survey on cluster based routing protocols in wireless sensor networks," Procedia Comput. Sci., vol. 45, pp. 687–695, 2015, doi: 10.1016/j.procs.2015.03.133 .
[12] N. A. Pantazis, S. A. Nikolidakis, and D. D. Vergados, "Energy-efficient routing protocols in wireless sensor networks: A survey," IEEE Commun. Surv. Tuts., vol. 15, no. 2, pp. 551–591, Second Quart. 2013, doi: 10.1109/SURV.2012.062612.00084 .
[13] S. Ramesh et al., "Optimization of LEACH protocol in wireless sensor network using machine learning," Comput. Intell. Neurosci., vol. 2022, Art. no. 5393251, Aug. 2022, doi: 10.1155/2022/5393251 .
[14] I. F. Jaleel, R. S. Ali, and G. A. Abed, "Improvement of Internet of Things (IoT) interference based on pre-coding techniques over 5G networks," Mesopotamian J. Cybersecurity, vol. 5, no. 1, pp. 11–22, Jan. 2025, doi: 10.58496/MJCS/2025/002 .
[15] C.-M. Chao and T.-Y. Hsiao, "Design of structure-free and energy-balanced data aggregation in wireless sensor networks," J. Netw. Comput. Appl., vol. 37, no. 1, pp. 229–239, Jan. 2014, doi: 10.1016/j.jnca.2013.02.013.
[16] C.-M. Chao and T.-Y. Hsiao, "Design of structure-free and energy-balanced data aggregation in wireless sensor networks," in Proc. IEEE Int. Conf. High Perform. Comput. Commun., 2009, pp. 222–229, doi: 10.1109/HPCC.2009.63 .
[17] M. H. Yeganeh, H. Yousefi, N. Alinaghipour, and A. Movaghar, "RDAG: A structure-free real-time data aggregation protocol for wireless sensor networks," in Proc. IEEE 17th Int. Conf. Embedded Real-Time Comput. Syst. Appl. (RTCSA), vol. 1, Aug. 2011, pp. 51–60, doi: 10.1109/RTCSA.2011.70 .
[18] S. A. S. Naem and S. M. Hameed, "Digital watermarking techniques, challenges, and applications: A review," Mesopotamian J. Cybersecurity, vol. 5, no. 2, pp. 453–476, 2025, doi: 10.58496/MJCS/2025/028 .
[19] Q. Wang and T. Zhang, "A survey on security in wireless sensor networks," Kristianstad Univ. Res. Portal, pp. 293–320, 2025. [Online]. Available: https://researchportal.hkr.se/en/publications/a-survey-on-security-in-wireless-sensor-networks
[20] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," IEEE Commun. Surv. Tuts., vol. 11, no. 4, pp. 42–56, Fourth Quart. 2009, doi: 10.1109/SURV.2009.090404 .
[21] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," Computer, vol. 35, no. 10, pp. 54–62, Oct. 2002, doi: 10.1109/MC.2002.1039518 .
[22] Y. W. Law, L. van Hoesel, J. Doumen, P. H. Hartel, and P. J. M. Havinga, "Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols," in Proc. 3rd ACM Workshop Secur. Ad Hoc Sensor Netw., Nov. 2005, pp. 1–10, doi: 10.1145/1102219.1102234 .
[23] A. Mpitziopoulos, D. Gavalas, G. Pantziou, and C. Konstantopoulos, "Defending wireless sensor networks from jamming attacks," in Proc. IEEE 18th Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC), Sep. 2007, pp. 1–5, doi: 10.1109/PIMRC.2007.4394775 .
[24] C. W. Commander, P. M. Pardalos, V. Ryabchenko, S. Uryasev, and G. Zrazhevsky, "The wireless network jamming problem," J. Comb. Optim., vol. 14, no. 4, pp. 481–498, Dec. 2007, doi: 10.1007/s10878-007-9071-7 .
[25] S. M. Shareef and R. F. Hassan, "Improved blockchain technique based on modified SLIM algorithm for cyber security," Mesopotamian J. Cybersecurity, vol. 5, no. 1, pp. 147–164, Feb. 2025, doi: 10.58496/MJCS/2025/010 .
[26] J. Fan, T. Liang, T. Wang, and J. Liu, "Identification and localization of the jammer in wireless sensor networks," Comput. J., vol. 62, no. 10, pp. 1515–1527, Oct. 2019, doi: 10.1093/comjnl/bxz055 .
[27] K. Dhivyasri, "Wireless sensor network jammer attack: A detailed review," Int. J. Res. Appl. Sci. Eng. Technol., vol. 8, no. 8, pp. 233–238, Aug. 2020, doi: 10.22214/ijraset.2020.30844 .
[28] A. Cortés-Leal, C. Del-Valle-Soto, C. Cardenas, L. J. Valdivia, and J. A. Del Puerto-Flores, "Performance metric analysis for a jamming detection mechanism under collaborative and cooperative schemes in industrial wireless sensor networks," Sensors, vol. 22, no. 1, p. 178, Dec. 2021, doi: 10.3390/s22010178 .
[29] Z. S. M. Al-Husseini, H. K. Chaiel, A. Meddeb, and A. Fakhfakh, "A detailed review of wireless sensor network, jammer, the types, location, detection and countermeasures of jammers," Serv.-Oriented Comput. Appl., vol. 18, no. 3, pp. 225–247, Apr. 2024, doi: 10.1007/s11761-024-00396-w .
[30] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in Proc. 6th ACM Int. Symp. Mobile Ad Hoc Netw. Comput. (MobiHoc), 2005, pp. 46–57, doi: 10.1145/1062689.1062697 .
[31] M. Cheng, Y. Ling, and W. B. Wu, "Time series analysis for jamming attack detection in wireless networks," in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2017, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/document/8254000

[32] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attacks and network defense policies in wireless sensor networks," in Proc. IEEE INFOCOM, May 2007, pp. 1307–1315, doi: 10.1109/INFCOM.2007.155 .
[33] A. W. Wood, J. A. Stankovic, and G. Zhou, "DEEJAM: Defeating energy-efficient jamming in IEEE 802.15.4-based wireless networks," in Proc. IEEE SECON, Jun. 2007, pp. 60–69, doi: 10.1109/SAHCN.2007.4292818 .
[34] S. Vadlamani, B. Eksioglu, H. Medal, and A. Nandi, "Jamming attacks on wireless networks: A taxonomic survey," Int. J. Prod. Econ., vol. 172, pp. 76–94, Feb. 2016, doi: 10.1016/j.ijpe.2015.11.008 .
[35] K. Grover, A. Lim, and Q. Yang, "Jamming and anti-jamming techniques in wireless networks: A survey," Int. J. Ad Hoc Ubiquitous Comput., vol. 17, no. 4, pp. 197–215, 2014, doi: 10.1504/IJAHUC.2014.066419 .
[36] K. Panyim, T. Hayajneh, P. Krishnamurthy, and D. Tipper, "On limited-range strategic/random jamming attacks in wireless ad hoc networks," in Proc. IEEE 34th Conf. Local Comput. Netw. (LCN), Zurich, Switzerland, Oct. 2009, pp. 922–929, doi: 10.1109/LCN.2009.5355041 .
[37] N. Z. Khalaf et al., "Development of real-time threat detection systems with AI-driven cybersecurity in critical infrastructure," Mesopotamian J. Cybersecurity, vol. 5, no. 2, pp. 501–513, 2025, doi: 10.58496/MJCS/2025/031 .
[38] D. Mihaylova, "An overview of methods of reducing the effect of jamming attacks at the physical layer of wireless networks," in Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 283, 2019, pp. 271–284, doi: 10.1007/978-3-030-23976-3_24 .
[39] N. Tandiya, A. Jauhar, V. Marojevic, and J. H. Reed, "Deep predictive coding neural network for RF anomaly detection in wireless networks," in Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops), May 2018, pp. 1–6, doi: 10.1109/ICCW.2018.8403654 .
[40] H. Sedjelmaci and M. Feham, "Novel hybrid intrusion detection system for clustered wireless sensor network," Int. J. Netw. Secur. Appl., vol. 3, no. 4, pp. 1–14, Jul. 2011, doi: 10.5121/IJNSA.2011.3401 .
[41] O. Osanaiye, A. Alfa, and G. Hancke, "A statistical approach to detect jamming attacks in wireless sensor networks," Sensors, vol. 18, no. 6, p. 1691, May 2018, doi: 10.3390/s18061691 .
[42] M. Çakıroğlu and A. T. Özcerit, "Jamming detection mechanisms for wireless sensor networks," in Proc. 3rd Int. ICST Conf. Scalable Inf. Syst. (InfoScale), Jan. 2008, pp. 1–8, doi: 10.4108/ICST.INFO SCALE2008.3484 .
[43] P. Ganeshkumar, K. P. Vijayakumar, and M. Anandaraj, "A novel jammer detection framework for cluster-based wireless sensor networks," EURASIP J. Wireless Commun. Netw., vol. 2016, Art. no. 29, Feb. 2016, doi: 10.1186/s13638-016-0528-1 .
[44] W. Aldosari and M. Zohdy, "Tracking a jammer in wireless sensor networks and selecting boundary nodes by estimating signal-to-noise ratios and using an extended Kalman filter," J. Sens. Actuator Netw., vol. 7, no. 4, p. 48, Nov. 2018, doi: 10.3390/jsan7040048 .
[45] S. Muthu Mariappan and S. Selvakumar, "A novel location pinpointed anti-jammer with knowledge estimated localizer for secured data transmission in mobile wireless sensor network," Wireless Pers. Commun., vol. 118, no. 4, pp. 2073–2094, Jun. 2021, doi: 10.1007/s11277-020-07885-z .
[46] W. Zhou, Z. Zhou, Y. Niu, Q. Zhou, and H. Ding, "A fast anti-jamming algorithm based on imitation learning for WSN," Sensors, vol. 23, no. 22, p. 9240, Nov. 2023, doi: 10.3390/s23229240 .
[47] M. Meenalochani and S. Sudha, "Jammed node detection and routing in a multihop wireless sensor network using hybrid techniques," Wireless Pers. Commun., vol. 104, no. 2, pp. 663–675, Jan. 2019, doi: 10.1007/s11277-018-6042-5 .
[48] L. Jia, Y. Xu, Y. Sun, S. Feng, and A. Anpalagan, "Stackelberg game approaches for anti-jamming defence in wireless networks," IEEE Wireless Commun., vol. 25, no. 6, pp. 120–128, Dec. 2018, doi: 10.1109/MWC.2017.1700363 .
[49] Y. Arjoune, F. Salahdine, M. S. Islam, E. Ghribi, and N. Kaabouch, "A novel jamming attacks detection approach based on machine learning for wireless communication," in Proc. Int. Conf. Inf. Netw. (ICOIN), Jan. 2020, pp. 459–464, doi: 10.1109/ICOIN48656.2020.9016462 .
[50] B. Mbarek, M. Ge, and T. Pitner, "An adaptive anti-jamming system in Hyperledger-based wireless sensor networks," Wireless Netw., vol. 28, no. 2, pp. 691–703, Feb. 2022, doi: 10.1007/s11276-022-02886-1 .
[51] A. S. Ali, S. Naser, and S. Muhaidat, "Defeating proactive jammers using deep reinforcement learning for resource-constrained IoT networks," in Proc. IEEE 34th Annu. Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC), Sep. 2023, pp. 1–6, doi: 10.1109/PIMRC56721.2023.10293793 .
[52] F. Yang, N. Shu, C. Hu, J. Huang, and Z. Niu, "Jammer location-aware method in wireless sensor networks based on Fibonacci branch search," J. Sens., vol. 2023, Art. no. 2261730, May 2023, doi: 10.1155/2023/2261730.
[53] L. Jia et al., "Game-theoretic learning anti-jamming approaches in wireless networks," IEEE Commun. Mag., vol. 60, no. 5, pp. 60–66, May 2022, doi: 10.1109/MCOM.001.00496 .