International Journal of Basic and Applied Sciences, 14 (7) (2025) 372-387

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/aj2xxz30
Research paper

Fractional Dynamics and Fractal Geometry for Robust Fault Detection in Wireless Sensor Networks

Abdullah Shawan Alotaibi *

Department of Computer Science, College of Science and Humanities, Al Dawadmi,
Shaqra University, Saudi Arabia
**Corresponding author E-mail: a.s@su.edu.sa*

Received: August 22, 2025, Accepted: September 26, 2025, Published: November 14, 2025

Abstract

A novel event detection framework for wireless sensor networks (WSNs) is presented, integrating fractional-order calculus and fractal geometry to address fault tolerance and detection accuracy challenges. The methodology comprises five synergistic components: mul-multifractal event region simulation, fractional-order dynamic trust evaluation, Monte Carlo-based event estimation guided by fractional information gain, fractional-order fault propagation modelling, and a multi-layer fractional consensus mechanism. These components enable the system to adaptively assess node reliability, predict fault propagation, and detect spatially complex events with high precision. The framework's simulation results demonstrate significant outperformance over conventional methods (binary decision trees, majority voting, and Shannon-entropy-based detection), achieving 96.2% detection accuracy, a 1.8% false positive rate, a 0.982 area under the curve, and a 28.4% reduction in data transmission overhead. These improvements highlight the practical potential of integrating fractional-al and fractal intelligence in the design of robust, memory-aware, and energy-efficient WSNs architectures suitable for harsh and dynamic-ic environments deployment.

Keywords: *Wireless Sensor Networks; Fault Propagation Modelling; Multifractal Simulation; Memory-Aware Systems.*

1. Introduction

Wireless sensor networks (WSNs) have become a cornerstone technology in many application areas, from environmental monitoring to industrial automation. These types of networks are formed by many sensor nodes that gather node data and send it to the sink and real-time route package, which allows for the monitoring of physical events that support decision making. However, sensor nodes are easily destroyed due to their often harsh and uncertain operating environments, which results in limited reliability and accuracy. The introduction presents the most salient features of WSNs, which include fault tolerance, event detection design, and the utilisation of modern solutions to enhance performance. When WSNs operate in harsh conditions, the sensor nodes fail, while environmental noise results in error readings. False inputs can have catastrophic consequences for the system's integrity, so a clear distinction between real events and errors must be in place. For instance, (Adday et al., 2023) and (Chen, Yang, and McCann, 2015) introduced the Friendship Degree and the Tenth Man Strategy (FD-TMS) to detect true events in WSNs. This method utilises majority voting of the nodal Friendship Degree to enhance the network's ability to filter out incorrect readings and ensure that only true event reports are broadcast (Adday et al., 2023). Similarly, Biswas and Samanta (2020) proposed a true event-driven and fault-tolerant routing algorithm, in which a majority voting scheme is applied to distinguish between detected true events and fault measurements. Their solution focused on multi-hop communication to forward event reports to the base station, which in turn improves the network's fault tolerance. These developments emphasise the importance of robust fault tolerance schemes in WSNs. The increasing complexity of applications for WSNs has motivated the study of various fault tolerance mechanisms. For instance, (Swain, Khilar, and Bhoi, 2020) categorised faults in WSNs in terms of root causes, behaviour, and duration. They proposed a majority of neighbours' consensus approach for diagnosis. Their findings emphasised the need for fault detection algorithms to monitor the changing environment in sensor networks. Furthermore, a systematic review of fault-tolerant techniques specifically designed for faults in underwater sensor networks. These researchers found that such environments had unique challenges that required a dedicated solution. Recent developments in machine learning have also begun to appear in WSNs, including outlier detection and data quality enhancement. For instance, (Jesus, Casimiro, and Oliveira, 2021) developed a trustworthy outlier detection methodology for application in machine learning techniques for sensor behaviour modelling. This technique enhanced data quality, which led to the detection of genuine anomalies in complex environments. Utilising machine learning in WSNs is a significant advancement in addressing the challenges of data reliability and fault tolerance. Additionally, the integration of Industry 4.0 with WSNs has received attention for improving manufacturing scenarios. For instance, (Ali, Salah, and Habib, 2024) studied the integration of Industry 4.0 enabling technologies for the production of custom-made products by focusing on smart technologies and systems for improving production efficiency. This cross between WSNs and advanced manufacturing processes also illustrates the flexibility of sensor networks across multiple domains. Integrations of multimodal

sensing devices are also necessary to increase the functionalities of WSNs. For instance, used the density-based spatial clustering of applications with noise (DBSCAN) and neighbour voting to demonstrate the feasibility of combining different sensory modes for enhancing network security and reliability. These advances are crucial to making WSNs robust against both malicious attacks and environmental factors. Thus, the evolution of WSNs is driven by fault-tolerance and event detection techniques that enable the integration of emerging technologies. Hence, the adoption of machine learning, Industry 4.0 principles, and multimodal sensing technologies provides potential avenues to improve the quality and trustworthiness of WSNs in various applications. As the research is still ongoing, it is essential to address these challenges to fully realise the potential of WSNs in developing reliable and efficient monitoring systems. The FD-TMS by (Adday et al., 2023) and (Krishnamachari and Iyengar, 2004) provided examples of research on neighbour cooperation-based fault tolerances in WSNs (Fathi et al., 2025a). The cooperative nature of nearby sensor nodes can be effectively utilised for fault detection to improve the integrity of event reporting and lead to a fault-tolerant network structure. However, most studies report performance metrics after data transmission, without delving much into the benefits of the transmission in the context of decision making. This ignorance hampers their contributions to understanding how data sharing influences network efficiency and effectiveness in real-time detection events. While these approaches have improved fault detection and routing reliability, they have often failed to account for the long-term behavioural trends of sensor nodes or the spatial irregularities of event patterns (Fathi et al., 2025b). Most methods treat event regions as static or uniformly distributed, which is rarely the case in real-world scenarios such as environmental monitoring and structural failure detection. Moreover, fault propagation is often modelled without temporal memory, which limits the accuracy of predictions in evolving network states. Thus, a pressing need exists for a more dynamic, memory-aware framework that can interpret both the temporal persistence and spatial complexity inherent in real sensor deployments. Despite these advancements, most existing solutions for fault tolerance and event detection in WSNs suffer from critical limitations. First, many do not account for the temporal memory of sensor node behaviour, which is essential for distinguishing transient faults from consistent reliability patterns. Second, traditional methods often fail to capture the complex and irregular structure of real-world event regions, which results in reduced detection accuracy in boundary areas. Furthermore, the dynamic propagation of faults over time is rarely modelled with sufficient granularity, while few systems incorporate energy-aware data filtering that adapts to both node trustworthiness and event characteristics in real time. These gaps highlight the need for a more comprehensive, memory-aware, and geometry-sensitive detection framework. Furthermore, the concept of information gain-based optimisation is employed to maximise data dissemination while minimising both energy costs and delays (Krishnamachari and Iyengar, 2004; Bharti, Pattanaik, and Bellavista, 2021; Adday et al., 2023). Empirical studies have focused on utilising information gain to enhance decision-making and balance the energy consumption of nodes and the latency of data transmission. These studies have demonstrated that the application of information gain has led to the more effective use of limited resources, with reduced extraneous and redundant information. By embedding fractional-order dynamics and fractal spatial reasoning into the event detection process, this study makes a direct contribution to the field of complex systems governed by nonlocality and memory, a central theme in both fractional calculus and fractal modelling. The proposed framework leverages these principles to model phenomena that are inherently irregular and temporally dependent. This paper introduces a novel fractal and fractional-order methodology tailored for fault-tolerant WSNs to bridge the identified limitations in existing event detection frameworks. The proposed approach synergistically integrates five core components: (1) a multifractal event region simulation technique that replicates the spatial irregularities of natural events; (2) a fractional-order dynamic trust evaluation (FODTE) model that leverages the memory-preserving nature of fractional derivatives to evaluate long-term node behaviour; (3) a Monte-Carlo-based event estimation mechanism augmented with fractional information gain (FIG) to improve decision confidence and suppress noisy data contributions; (4) a fractional-order fault propagation model (FOFPM) that characterises the temporal dynamics of fault diffusion with high fidelity; and (5) a multi-layer fractional consensus mechanism that ensures resilient, history-aware agreement across the network. These components collectively form a cohesive framework that captures the fractal nature of event boundaries while integrating memory-aware reasoning to enhance reliability, energy efficiency, and detection accuracy in harsh sensing environments. This framework holds practical potential for deployment in real-world systems (e.g., wildfire monitoring, smart agriculture, industrial fault detection, and structural health surveillance), where event boundaries are irregular, faults evolve gradually, and decision accuracy is mission-critical.

2. Related Work

Wireless Sensor Networks (WSNs) have become integral to critical applications such as environmental monitoring, industrial automation, and structural health surveillance. Their deployment in harsh and unpredictable environments introduces a persistent challenge: maintaining accuracy and reliability despite the likelihood of sensor faults. Consequently, numerous fault tolerance and event detection techniques have been proposed in recent literature. One prominent class of approaches involves majority voting schemes, where a node's sensing output is verified through neighbour consensus. For example, (Biswas and Samanta, 2020) Developed a true event-driven routing protocol that employs neighbour voting to distinguish genuine events from abnormal sensor readings. Similarly, (Adday et al., 2023) Introduced the Friendship Degree with Tenth Man Strategy (FD-TMS), which enhances reliability by combining voting with event topology validation. While effective in reducing false alarms, these schemes often assume uniformly distributed sensor behaviour and lack adaptability to evolving node trustworthiness.

Another major strategy involves fault detection via neighbourhood correlation or consensus methods. (Swain, Khilar and Bhoi, 2020) Proposed a diagnosis protocol based on majority neighbour coordination, using timeout mechanisms and Gaussian-based evaluation to detect transient faults. However, this method is sensitive to network density and may struggle in sparse deployments. (Bhat and Santhosh, 2022) Addressed localisation-related faults using K-means clustering within the DV-Hop algorithm, effectively filtering out malfunctioning nodes. Still, the clustering introduces computational complexity and latency concerns. To improve robustness, clustering-based multipath routing has also been explored. For instance, (Moridi et al., 2020) Proposed a fault-tolerant clustering-based multipath (FTCM) algorithm that introduces backup nodes for redundant data paths. Though it enhances delivery reliability, the routing overhead can be significant in dynamic or high-traffic environments. (Li and Zhang, 2025) extended this idea in their EPRA-FT
method, which remaps aggregation trees to bypass faulty nodes and preserve data integrity during aggregation. Yet, both methods treat fault patterns as either binary or instantaneous, neglecting their temporal persistence. Recent efforts have integrated machine learning and entropy-based anomaly detection into WSNs. (Jesus, Casimiro and Oliveira, 2021) developed a dependable outlier detection model using ML to learn typical sensor behaviour over time, while (Aly and Alotaibi, 2022a) Explored frequency-based representations in signal diagnosis using deep learning and spectrogram analysis. However, these approaches often require significant training data and computational power — making them less suitable for real-time embedded WSNs.

Despite these advances, several limitations remain unaddressed. First, most methods overlook the memory aspect of sensor behaviour — failing to differentiate between temporary glitches and persistent faults. Second, many assume spatially uniform event regions, even though

real-world phenomena like fire or gas leaks evolve in complex, irregular patterns. Third, trust computation is often stateless or based on short-term behaviour, leading to unreliable consensus in prolonged deployments. These gaps motivate the development of a hybrid approach that combines fractal geometry with fractional-order modelling. Fractal simulation enables realistic modelling of spatially irregular event regions, while fractional calculus introduces long-term memory into trust, fault propagation, and consensus dynamics. By embedding these principles, the proposed framework addresses both spatial and temporal complexities inherent in fault-tolerant event detection in WSNs — a direction yet to be adequately explored in the current literature.

Recent advances have shifted toward learning-based and graph-based approaches for sensor fault and anomaly detection. Recurrent models such as LSTM and its federated variants have been proposed to capture temporal dependencies in sensor streams while addressing privacy and decentralization: for example, FedLSTM applies federated learning with LSTM units to detect common sensor faults (bias, drift, spikes, stuck sensors), showing robust detection while preserving local data privacy and reducing raw data transmission (Khan et al., 2024; Aly et al., 2024a). Hybrid deep-learning pipelines that combine convolutional feature extractors with LSTM or autoencoder backends have also been explored for noisy, real-world sensing signals and typically achieve high detection accuracy when sufficient labeled data are available (Gupta et al. 2024).

Graph-based models have emerged as a powerful alternative when the spatial/relational structure between nodes is important. Dynamic graph neural networks exploit both temporal and spatial dependencies to improve anomaly detection in multivariate sensor arrays; recent multi-scale dynamic GNN architectures explicitly model temporal windows and evolving graph structure to raise robustness against complex, correlated faults in industrial sensor installations. While these learning-based and GNN solutions often deliver excellent detection metrics, they typically demand larger labeled datasets, more computation (or an edge/cloud offload strategy), and careful hyperparameter tuning — factors that can limit direct on-node deployment in severely resource-constrained WSNs (Khan et al. 2024; Zhao et al. 2024; Aly and Alotaibi, 2023c).

This work proposes a neighbouring circular replication approach that utilises a reactive fault tolerance mechanism to enhance the availability of data in distributed systems. The technique is designed to improve the reliability and resilience of the system by exploiting data replication and recovery. Because availability increases with fewer replicas, it may be less practical in highly dynamic or unpredictable settings. Various comparative summaries of the related work being studied, which paved the way for the development of true event detection techniques in WSNs, appear in Table 1. Although algorithms for distinguishing true and false events in WSNs have achieved significant scientific leaps, many unresolved issues still warrant attention with considerable concern. While previous studies have made progress in filtering faulty readings and improving data reliability through voting, clustering, and consensus mechanisms, they have often treated sensor behaviour as a purely instantaneous process while ignoring the temporal evolution of node reliability. Moreover, the spatial modelling of event regions is typically oversimplified, with most works assuming regular shapes or a uniform distribution of events. As a result, existing methods may struggle to handle real-world deployments, where events evolve, node behaviour is inconsistent, and environmental phenomena follow non-uniform patterns. These gaps necessitate new approaches that integrate both memory-aware modelling and spatial irregularity into the detection process. This study introduces an event detection framework that explicitly incorporates both fractional-order reasoning and fractal-based spatial simulation to address these gaps. Fractional calculus enables the system to capture long-term dependencies in node behaviour that allow for a more nuanced and adaptive assessment of trust and fault propagation. In parallel, the use of multifractal event simulation provides a more realistic model of event boundaries, particularly in environments where events (e.g., fires and chemical leaks) do not follow clean geometric shapes. This dual modelling approach directly supports more accurate detection, filtering, and consensus, particularly in noisy and dynamic WSN conditions. A crucial aspect is the trade-off between energy efficiency and detection performance. Most existing techniques usually either sacrifice detection accuracy for energy conservation or vice versa. Another open issue is the scalability of the event detection algorithm. Many existing algorithms cannot accommodate high-density networks. Moreover, some methods derived from deep reinforcement learning algorithms also suffer from slow learning.

In light of the reviewed literature, it is evident that current approaches often fail to fully capture the long-term behaviour of sensor nodes, the memory-dependent nature of fault propagation, and the spatial complexity of real-world event distributions. These limitations hinder detection accuracy, trust modelling, and fault resilience in dynamic and harsh WSN environments. To overcome these challenges, this study proposes a novel framework that leverages fractional-order dynamics and fractal geometry for modelling trust, consensus, and event regions. The following section formally defines the problem and introduces the system assumptions, network structure, and event detection goals that underpin the proposed methodology.

3. Problem Formulation

Let us denote by K the total number of distributed sensors. These sensors take readings of the environment (e.g., temperature) at regular intervals. If any K(i) sensor node 2.1 observes readings in a node i during period t that are beyond a certain threshold (ɵ), then it needs to react and inform the base station (BS) that an event has taken place. Since errors can be present in the sensor, a high reading can mean either that there is a high temperature caused by a fire or that a mistaken measurement occurred. A major consideration is whether the increased reading is a true reading or whether it is a sensor fault, as all of them are essentially factory deaf. The most significant answer to this problem is a majority voting scheme combined with the Boyer–Moore algorithm for the neighbouring cooperation approach. The Boyer–Moore algorithm, widely used in text pattern matching, can be used to determine which of several candidates has received the most votes in an election. When a sensor K(i) detects multiple irregular readings, it starts to emit request messages to its neighbouring sensors, as demonstrated in Figure 1, where K(i) tallies the up–down among its neighbours. An affirmative response indicates that mutual suspicion is the reason for the unusual value, while a negative responses mean that no descent was detected. If the number of positive responses exceeds the number of negative responses, K(i) creates a report packet and transmits it to the BS. If not, K(i) decides that the event occurred and then prepares for the next sensing. Hence, a proposal is made to overcome the shortcomings of the blind majority algorithm, which lacks consideration for the reliability of neighbour nodes, many of which may be faulty and ultimately hinder voting topology validation. If node K(i) generates an incorrect sensing report, the BS may inaccurately interpret it as a valid event occurrence, which can result in an increased false alarm rate, reduced detection accuracy, accelerated energy consumption, elevated network congestion, and ultimately, decreased overall network reliability. Therefore, it is essential to promptly identify and mitigate such errors to minimise the effects of measurement inaccuracies. As a result, this study introduces a novel majority voting mechanism among neighbouring nodes to distinguish genuine events from faulty sensor readings. Verified event information is forwarded to the BS using a geographic routing strategy inspired by foundational approaches. Moreover, erroneous readings are independently discarded by sensor nodes in a decentralised manner without requiring intervention from the BS. Definition 1: A true event refers to an environmental occurrence (e.g., a forest fire or a specific liquid flood) that causes the sensor's measured parameter to exceed its normal range (Biswas & Samanta, 2020). Definition 2: A measurement

fault happens when a sensor's hardware malfunction leads to an incorrect calculation of the measured parameter due to issues within the sensing unit.

3.1. Research assumptions

This study examines the factors that may contribute to the occurrence of faulty sensor readings. Hence, specific correlations are examined based on clearly defined assumptions. The following research assumptions guide the investigation and support the drawing of meaningful conclusions from the data:

- Each node has a fixed position.
- The network has only one BS.
- All nodes, including the BS, have the same restricted transmission range D.
- All nodes except the BS have limited battery capacity.
- All nodes are aware of their location and remaining energy.
- All nodes sense the environment parameters periodically.
- There is a probability of erroneous sensor measurements.

The proposed network framework consists of K sensor nodes, denoted as K(i) for i = 0, 1, 2, ..., K−1, which are uniformly and randomly deployed over a two-dimensional area with dimensions (X, Y). Two nodes, K(i) and K(j), are considered neighbours if the Euclidean distance EDij between them is less than or equal to a pre-defined communication range D that allows for direct communication. The positions of nodes K_i and K_j are given by their coordinates (X_i, Y_i) and (X_j, Y_j), respectively. The Euclidean distance between any two such nodes is computed using Equation (1) (Aly, 2025b).

$$\mathrm{ED_{ij}} = \sqrt{(\mathrm{Xj} - \mathrm{Xi})^2 + (\mathrm{Yj} - \mathrm{Yi})^2} \quad (1)$$

As depicted in Figure 2, if a sensor node is unable to communicate directly with the BS, it selects a neighbouring node to act as an intermediary for forwarding the collected data. In this study, a geographic routing method similar to the one presented by (Biswas and Samanta, 2020) It is employed to manage data transmission. As illustrated in Figure 2, any node that is not a neighbour of the BS selects one of its neighbours as the forwarding node to send its sensed data to the BS. The proposed approach employs the geographic routing algorithm referenced in (Biswas and Samanta, 2020). Each node maintained the location and hop count.

3.2. Event model

Natural events (e.g., forest fires) can span large areas and exhibit irregular or dynamic shapes, influenced by environmental factors such as wind. To simplify simulation and analysis, this study models the affected region as a circular sector, anchored at a fixed point (X, Y) with a consistent radius R, as shown in Figure 3. Sensor nodes deployed in the field routinely gather physical data and evaluate whether the readings exceed a pre-defined threshold (θ). This work accounts for potential sensor inaccuracies by recognising that elevated readings may sometimes result from malfunctioning nodes situated outside the actual event zone. Hence, a tailored detection algorithm enables nodes to distinguish between authentic and faulty readings to address this issue. Only verified event data are forwarded to the BS via a geographic routing protocol, while unreliable measurements are discarded locally. The detection logic checks both the magnitude of the sensed value and its validity before initiating multi-hop communication for confirmed events. In this study, event regions are not assumed to have ideal geometric shapes. Instead, the spatial structure of an event (e.g., a spreading fire or contaminant) is modelled using multifractal geometry to better reflect the irregular, self-similar patterns often seen in nature. This approach allows for a more realistic simulation of detection boundaries and exposes the limitations of conventional models that rely on circular or uniformly shaped regions. The reliability of a sensor node is not static; it changes based on behaviour over time. To reflect this concept, we define a fractional-order trust function. $T_i^{\alpha}(t)$ using the Caputo fractional derivative of order $\alpha \in (0,1)$ To capture long-term memory of each node's performance. This definition enables the system to dynamically adjust a node's influence based on both recent and historical activity for distinguishing transient noise from persistent faults. Fault propagation across the network is similarly modelled using a fractional dynamic system, where the influence of a faulted node diminishes over time in a memory-aware manner. Additionally, the final event classification at each node is determined, not by simple majority voting alone but through a multi-layer fractional consensus process that considers trust scores, FIG, and spatiotemporal consistency. As illustrated in Figure 4, the simulation environment includes multiple scattered random event regions, accurately reflecting the unpredictable nature of event occurrences in real-world WSN deployments. While prior studies have introduced valuable mechanisms for fault diagnosis, consensus, and data reliability in WSNs, most have been rooted in classical techniques such as majority voting, clustering, and local neighbour verification. These approaches have often neglected the temporal memory aspect of node behaviour while failing to model the complex, non-uniform spatial structure of real-world events. Furthermore, existing methods have generally treated fault propagation as a binary or time-agnostic process that lacks predictive capabilities based on historical behaviour. Few works have incorporated fractional-order modelling to reflect memory-dependent dynamics or fractal-based simulations to capture irregular event topologies. Herein lies an opportunity to develop a framework that leverages both fractal geometry for spatial modelling and fractional calculus for temporal reasoning to offer a richer, more adaptive solution for robust event detection in WSNs. Motivated by these limitations, our work introduces a novel framework that integrates five complementary modules: (1) multifractal event region simulation for realistic boundary modelling, (2) FODTE for long-term reliability assessment, (3) Monte-Carlo-based event estimation with FIG for precision filtering, (4) the FOFPM for predictive fault awareness, and (5) a multi-layer fractional consensus mechanism for resilient decision making. This integration enables the system to interpret the data in real time and within the context of historical patterns and irregular spatial distributions to bridge a critical gap in the literature.

3.3. Proposed methodology

The proposed framework consists of five interlinked modules that collectively ensure resilient and adaptive fault-tolerant event detection: (1) Fractal Event Simulation, (2) Fractional Trust Evaluation, (3) Consensus and Aggregation, (4) Entropy-Based Decision and Filtering, and (5) Output Classification. Each module addresses a specific challenge in spatially irregular event modelling, memory-based trust scoring, or consensus-driven decision-making. The system's architecture is illustrated in Figure 2, and each component is detailed in the subsequent subsections.

3.4. Multi-fractal event region simulation

To realistically model the spatial distribution of natural events (e.g., wildfires and chemical leaks), this work replaces the conventional circular event zone with a multifractal event region generated using a multiplicative cascade model. The spatial intensity $I(x, y)$ at any point (x, y) within the sensing field is expressed as follows,

$$I(x, y) = I_0 . \prod_{i=1}^{n} W_i(x, y), \quad (2)$$

Where; I_0 Is the initial event intensity,
$W_i(x, y)$ Random weights are generated during each cascade iteration, and
n Is the number of fractal refinement levels.
To enhance the clarity and reproducibility of the proposed methodology, Table 2 presents a comprehensive list of all parameters, variables, and mathematical notations utilised throughout this section.

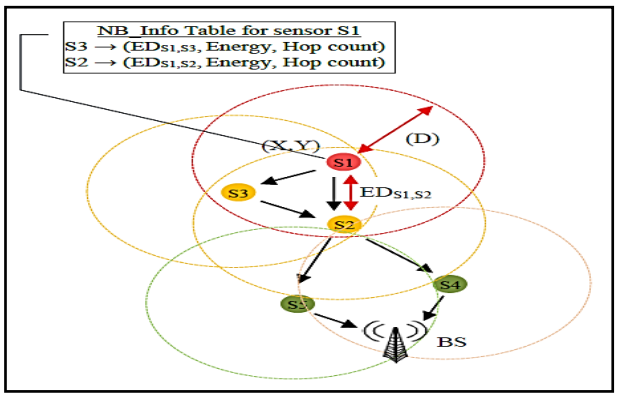

Fig. 1: Network Model (Adday et al., 2023).

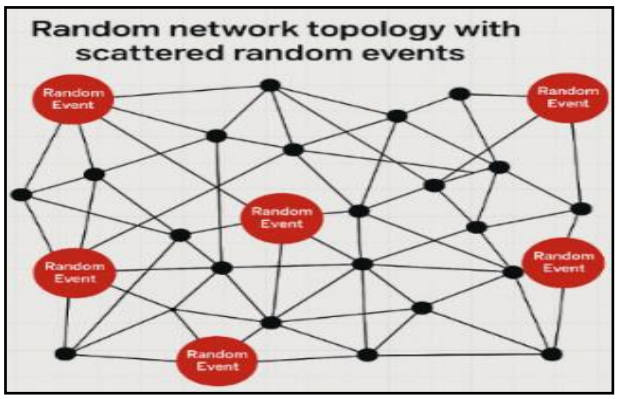

Fig. 2: Random Network Topology with Scattered Random Events.

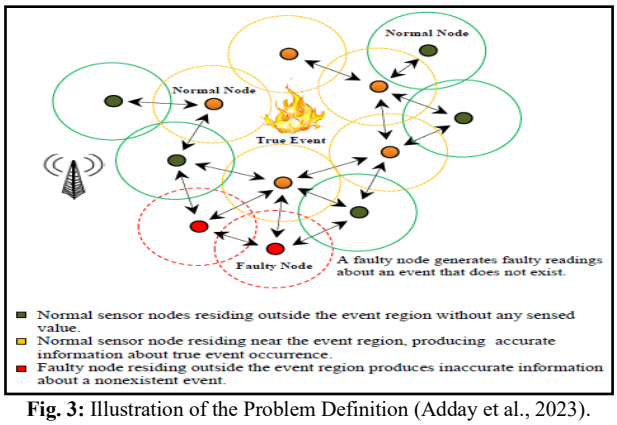

Fig. 3: Illustration of the Problem Definition (Adday et al., 2023).

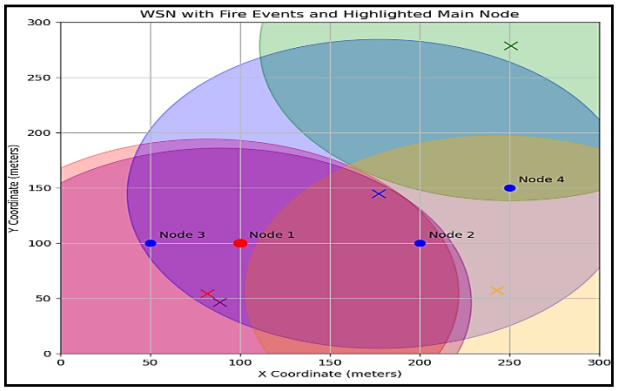

Fig. 4: Simulation for Scattered Random Events.

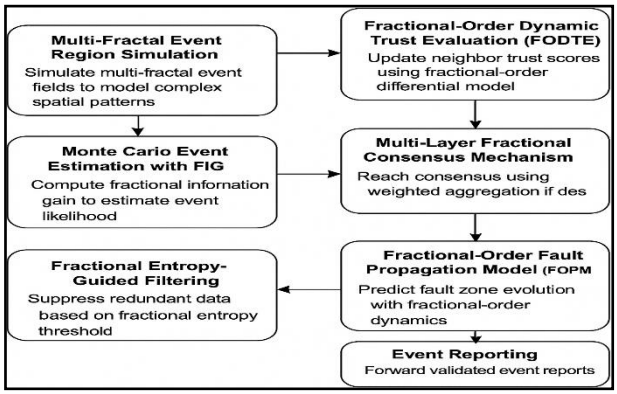

Fig. 5: Workflow of the Proposed Methodology.

This table includes symbols associated with the multifractal event modelling, fractional-order trust dynamics, information gain calculations, consensus mechanisms, and fault propagation processes. This consolidated notation table ensures that readers can easily reference the meaning and role of each symbol in the context of the proposed system equations and algorithms. (Aly et al., 2023c) Proposed an enhanced U-Net for medical image segmentation to highlight how structural adaptations in deep models can improve boundary recognition, conceptually similar to the fractal-based modelling of irregular event regions. The fractal dimension D_q The simulated event boundary is calculated using the box-counting method:

$$D_q = \frac{\text{loglog } N(\epsilon)}{\log (1/\epsilon)}, \tag{3}$$

Where $N(\epsilon)$ Is the number of boxes of size ϵ Needed to cover the event region. This multifractal modelling generates complex, irregular event regions, enabling more rigorous testing of the detection algorithm's spatial sensitivity.

Fractal metrics estimation

Two key fractal metrics are estimated to quantitatively characterise the complexity and self-similarity of the simulated event regions: the fractal dimension. Dq and the Hurst exponent H. These metrics provide insight into the spatial irregularity and temporal persistence of event zones within the sensing field.

Fractal dimension estimation

The box-counting method is employed to estimate the fractal dimension. Dq Of the event perimeter:

$$D_q = \frac{\text{loglog } N(\epsilon)}{\log (1/\epsilon)}, \tag{4}$$

Where $N(\epsilon)$ Is the number of boxes of size ϵ Required to completely cover the event area. Procedure:

1) Overlay a grid of boxes of size ϵ Over the event region.
2) Count the number of boxes $N(\epsilon)$ That contains part of the event region.
3) Vary ϵ And compute the slope of the $\log \log N(\epsilon)$ Vs. $\log (1/\epsilon)$ Plot.
4) The slope approximates the fractal dimension.

Hurst exponent estimation

The Hurst exponent H It is used to evaluate the long-term memory and temporal correlation of event detection patterns in the WSN. The rescaled range (R/S) analysis is applied as follows:

$$H = \frac{\log (\frac{R}{S})}{\text{loglog } n}, \tag{5}$$

Where R Is the range of cumulative deviations from the mean,
S is the standard deviation, and
n Is the length of the time series. Procedure:

1) Form time-series data of event reports at the BS.
2) Divide the series into equally sized segments.
3) For each segment,

- Calculate the mean.
- Compute cumulative deviations.
- Determine the range R and standard deviation S.
- Compute R/S for each segment

4) Plot (-)RS vs. $log\ log\ n$, and estimate H as the slope

Interpretation:

- $0.5 < H < 1$: Persistent behaviour (event occurrence tends to cluster)
- $H = 0.5$: Random (no memory)
- $0 < H < 0.5$: Anti-persistent (event detections tend to alternate)

Table 1: List of Parameters and Notations

Symbol	Definition	Symbol	Definition
K	Total number of sensor nodes in the wireless sensor network (WSN)	$N_f(t)$	Number of fault-influenced nodes at time t
K_i	Sensor node i, where $i = 1,2,$	N	Total number of deployed sensor nodes (synonymous with K)
(X_i, Y_i)	Coordinates of sensor node K_i in the two-dimensional sensing field	γ	Natural fault recovery rate in the fractional fault propagation model
D	Maximum communication range between two neighbouring sensor nodes	$C_i(t)$	Fractional consensus score of node K_i at time t
d_{ij}	Euclidean distance between nodes K_i and K_j	$\omega_i(t)$	Trust weight from node K_i to neighbouring node K_j at time t
$I(x, y)$	Event intensity at spatial location (x, y)	$\mathcal{N}_i$	Set of all neighbouring nodes of node K_i within range D
I_0	Initial intensity value of a simulated event	$E_i(t)$	Fractional entropy value of node K_i at time t
wl	Random weight assigned at the l^{th} level of the fractal cascade	$\theta_E(t)$	Dynamic threshold for entropy-based data filtering at time t
L	Total number of levels in the multifractal cascade refinement	ρ	Propagation coefficient for fault diffusion in the fractional-order model
D_f	Fractal dimension of the event boundary	κ	Normalization factor in the consensus aggregation equation
ϵ	Box size used in fractal dimension estimation (box-counting method)	R	Radius of the event region (for simplified geometric models)
$T_i(t)$	Trust score of node K_i at time t	δ_i	Decision value (1 = event detected, 0 = no event) received by node K_i from node K_j
$A_i(t)$	Instantaneous event agreement score of node K_i at time t	S(t)	Standard deviation in rescaled range (R/S) Hurst analysis
α	Fractional order used in trust update and fault propagation models ($0<\alpha<1$)	R(t)	Range of cumulative deviations in rescaled range (R/S) analysis
β	Order of Rényi entropy used in fractional information gain computation	η	Decay coefficient in the fractional trust or propagation model
FIG_A	Fractional information gain associated with attribute A	ζ	Responsiveness coefficient in the fractional trust model
H	Hurst exponent used for long-term memory analysis in time series	ϕ	Fractional consensus threshold

3.5. FODTE

Each sensor node maintains a dynamic trust score. $T_i(t)$ for its neighbours, updated using a fractional-order differential equation to incorporate memory effects of past interactions (Fathi et al., 2025):

$$D^{\alpha}T_i(t) = -\lambda T_i(t) + \mu.(S_i(t) - T_i(t)), \quad (6)$$

Where;

- D^{α} is the Caputo fractional derivative of order $0 < \alpha < 1$,
- λ, μ are positive constants regulating decay and responsiveness, and
- $S_i(t)$ Is the instantaneous behaviour score based on recent event agreement and false alarm contributions?

This approach ensures that reliable nodes accumulate higher influence in consensus decisions, while faulty or inconsistent nodes are gradually marginalised over time. (Aly et al., 2023d) Demonstrated how deep learning can track dynamic behaviour in online environments, a principle that aligns with the proposed use of memory-aware trust modelling over time.

3.6. Monte Carlo event estimation with FIG

The event detection phase begins with a Monte Carlo simulation to estimate the likelihood of a true event occurring within each node's sensing range. For each node K_iThe expected binary trait (EBT) is computed based on simulated event locations drawn from the multifractal event map. Next, each node computes a FIG for its observations using a fractional Rényi entropy function:

$$FIG(A) = H_{\beta}(S) - H_{\beta}(S|A), \quad (7)$$

Where;

- H_{β} Is the Rényi entropy of order $\beta \in (0,1)$,
- S Is the set of possible event states, and
- A Is the attribute (sensor reading). The Rényi entropy is defined as follows:

$$H_{\beta}(S) = \frac{1}{1-\beta} log\left(\sum_{i=1}^{n} p_i^{\beta}\right) \quad (8)$$

This fractional entropy generalises the classic Shannon entropy, allowing for better control over sensitivity to rare or extreme event reports, which is essential in harsh or noisy sensing environments. (Aly and Alotaibi, 2022a)Demonstrated how deep models combined with frequency-based features can effectively detect weak health signals, which motivates the use of robust feature representations, such as FIG, in noisy WSN environments. (Aly and Alotaibi, 2022b) Further extended this notion by utilising spectrogram images for multi-feature fusion to reinforce the importance of hybrid representations in time-sensitive classification tasks such as event estimation.

3.7. FOFPM

To predict the evolution of faulty readings across the network over time, we introduce an FOFPM based on a logistic growth equation modified with a fractional derivative:

$$D^{\alpha}F(t) = \beta F(t)\left(1 - \frac{F(t)}{N}\right) - \Upsilon F(t), \tag{9}$$

Where;

- $F(t)$ Is the number of fault-influenced nodes at time? t,
- N Is the total number of nodes,
- β Is the propagation coefficient,
- Υ Is the natural fault recovery rate, and
- α Is the memory order?

This model enables the WSN controller to anticipate fault escalation and proactively reconfigure routing and decision-making parameters. Elsayed et al. (2020a) demonstrated the effectiveness of nature-inspired optimization (e.g., quantum particle swarm optimization) in solving signal processing problems, which supports the use of swarm-based or evolutionary strategies in trust modelling and fault isolation. Behiry (2024) applied artificial intelligence and hybrid reduction techniques to detect cyber-attacks in WSNs to confirm the feasibility of intelligent models for fault and anomaly detection in distributed networks.

3.8. Multi-layer fractional consensus mechanism

Instead of a single-layer majority voting (Aly et al., 2024e), the proposed system implements a multi-layer consensus strategy, where local, regional, and global event agreement is reached via a fractional-order weighted aggregation of node decisions. Each node computes a fractional consensus score. $C_i(t)$, following Fathi et al. (2025a):

$$C_i(t) = \frac{1}{W_i}\sum_{j\in N(i)} \omega_{ij}^{\alpha} D_{ij}(t), \tag{10}$$

Where;

- $N(i)$ Is the set of neighbours of node i,
- ω_{ij} Is the trust weight from FODTE?
- $D_{ij}(t)$ Is the decision value (1 for event, 0 for no event),
- α is the consensus memory order, and
- $W_i = \sum_j \omega_{ij}^{\alpha}$ Normalises the weights.

If $C_i(t)$ exceeds a pre-defined fractional consensus threshold θ_{α}, node i Forwards the event report to the BS.

3.9. Data compression via fractional entropy-guided filtering

Nodes apply a fractional entropy-based filtering criterion to suppress redundant or non-informative data to reduce communication overhead. The local entropy $H_i^{\beta}(t)$ Based on recent readings, is calculation follows. (Aly et al., 2023d):

$$H_i^{\beta}(t) = \frac{1}{1-\beta}\log\left(\sum_{k=1}^{m} p_k^{\beta}\right) \tag{11}$$

Readings with entropy values below a dynamic fractional threshold τ_{β} They are designed to improve energy efficiency without compromising detection accuracy.

Algorithm Overview

The complete event detection protocol follows the phases listed in Table 2 sequentially. For ease of comprehension and systematic presentation of the proposed detection strategy, the complete workflow of the enhanced event detection framework is summarised in Table 2. This algorithm consolidates the multi-stage process comprising multifractal event simulation, Monte Carlo estimation (Aly, 2025a), FIG calculation, trust dynamics, consensus formation, fault propagation prediction, and entropy-based data compression. The stepwise procedure provides a clear and replicable blueprint for implementing the proposed fractional and fractal-enhanced methodology in fault-tolerant WSNs.

3.10. Complexity analysis

To evaluate the computational feasibility of the proposed framework, we analyze the asymptotic complexity of each module based on standard Big-O notation. Let K Denote the number of sensor nodes, T the number of time steps, $|\mathcal{N}_i|$ the average number of neighbours per node, and L The number of fractal cascade levels used in event generation (Elsayed et al., 2019b).

3.10.1. Fractal event simulation

The multifractal simulation involves iteratively refining an event map. L Levels using a multiplicative cascade. At each level, the spatial domain is divided into $2^l \times 2^l$ blocks, resulting in a total cost of $O(4^L)$. This is a one-time offline process independent of node count.

3.10.2. Trust evaluation module

The fractional trust update for each node K_i over the time horizon T Requires computing a Caputo derivative, which involves a history-dependent weighted summation:

$$T_i(t) = \frac{1}{\Gamma(1-\alpha)} \sum_{j=0}^{t-1} \frac{T_i(j)}{(t-j)^{\alpha}} \quad (12)$$

This leads to $O(K.T^2)$ Though optimizations such as memory truncation can reduce this to $O(K.T.\log T)$

3.10.3. Consensus and aggregation

Each node aggregates decisions from $|\mathcal{N}_i|$ neighbours at each time step using trust-weighted voting

$$C_i(t) = \frac{1}{\sum_{j\in\mathcal{N}_i} \omega_{ij}(t)} \sum_{j\in\mathcal{N}_i} \omega_{ij}(t)\, \delta_{ij}(t) \quad (13) \text{ and the cost is: } O(K.|\mathcal{N}_i|.T) \quad (14)$$

3.10.4. Entropy-based validation

The entropy $E_i(t)$ It is computed from the sensor's historical output distribution:

$$E_i(t) = -\sum_{k=1}^{m} p_k \log p_k \quad (15)$$

Where m Is the number of discrete output states. This results in:
$O(K.m.T)$ Which is typically small, as mmm is limited (e.g., binary output or few quantized levels).

Table 2: Algorithm 1 – Enhanced Event Detection Framework with Fractional and Fractal Modelling

Step	Operation	Step	Operation
Input	Network topology, node parameters, initial trust scores, multifractal event model	Output	Verified event reports to BS.
1.Initialisation	- Assign positions and initial trust scores to all sensor nodes - Simulate a multifractal event region - Estimate initial fractal dimension Dq and Hurst exponent HH	5. Multi-Layer Fractional Consensus	- Aggregate neighbour votes using fractional-order consensus weighting - Compute local confidence $C_i(t)C_i(t)\theta_{\alpha}$, mark the event as locally confirmed
2. Monte Carlo Simulation	- Each node K(i) performs random event location sampling within its sensing range - Compute the EBT for each node	6. FOFPM	- Estimate future fault node spread using the fractional logistic propagation model
3. FIG Calculation	- Compute the FIG for local sensor readings using fractional Rényi entropy - Determine event likelihood against the FIG threshold	7. Data Compression (Fractional Entropy)	- Calculate fractional entropy $H_i^{\beta}(t)$ for each node's recent data - Discard redundant reports if entropy < threshold τ_{β}
4. FODTE	- Apply the Caputo fractional derivative to dynamically update the trust score $T_i(t)$ - Adjust trust weights based on consensus alignment	8. Event Reporting	- Forward validated event reports along the strongest consensus path to the BS

3.10.5. Overall complexity

Combining all modules, the worst-case overall complexity of the system per simulation run is:

$$O(4^L + K.T^2 + K.|\mathcal{N}_i|.T + K.m.T) \quad (16)$$

Given that L, $|\mathcal{N}_i|$, and mmm are constant or bounded in practice, the dominant term is from the trust module. Optimization strategies such as recursive fractional filters or truncation windows can reduce this to a linear or near-linear cost (Elsayed et al. 2020).

3.11. Justification of fractional orders

The selection of fractional orders in our methodology is grounded in both theoretical and practical considerations from the literature on fractional-order systems. For FODTE, we set it to 8 to strike a balance between responsiveness to recent node behaviour and long-term memory retention. Several studies, including Yin et al. (2013), have shown that fractional orders between 0.7 and 0.9 are optimal for capturing long-range memory effects while preserving system stability in multi-agent consensus scenarios. For the FIG component, using a Rényi entropy order $\beta = 0.9$ provided heightened sensitivity to rare anomalies essential for fault detection in noisy environments. Values near 1 have been shown to effectively highlight atypical sensor readings amid ambient noise. Furthermore, in the multi-layer fractional consensus mechanism, we adopted alphadopted$\alpha = 0.7$. This choice aligned with fractional consensus protocols in the existing literature, where values of 0.65−0.75 have been found to accelerate agreement while preserving resistance to transient noise. Lastly, for the FOFPM, a fractional order $\alpha = 0.85$ was appropriate to capture the persistent spread of faulty behaviour without over-amplifying it. Such values have been successfully employed in fractional logistic propagation models and epidemic-like dynamics. These fractional orders collectively optimised the trade-off between memory and adaptability, as aligned with both theoretical optimality and empirical robustness established in the fractional-order systems domain. In summary, the chosen fractional orders were carefully balanced to: Preserve long-term event patterns, Adapt to dynamic sensor behaviours, Control the responsiveness-memory trade-off, and Align with the optimal ranges observed in prior studies of fractional-order systems. Subsequently, a sensitivity analysis will be conducted to confirm the stability of detection accuracy and false alarm rate within these fractional order ranges. Together, these five modules operate in a tightly integrated pipeline. Sensor observations are first validated against a fractal event distribution, passed through a memory-aware trust model, and then fused via fractional consensus. Final classification is performed through entropy-guided validation, enabling accurate and adaptive event detection.

This architecture supports both spatial irregularity and temporal persistence — key characteristics often overlooked in conventional schemes.

From a systems theory perspective, the choice of fractional orders in the interval $0.7 \leq \alpha, \beta \leq 0.9$ Is motivated by their ability to balance memory retention with stability. In the FODTE model, setting $\alpha = 0.8$ provides a weighting kernel whose impulse response decays polynomially rather than exponentially, which means that past behaviours of a node are not discarded abruptly but instead contribute with diminishing influence over time. This ensures that persistent reliability (or unreliability) is captured as a long-term trend, while short-lived fluctuations are smoothed. A lower order ($\alpha < 0.6$) would place excessive emphasis on recent events, risking instability in trust updates, whereas higher orders ($\alpha > 0.9$) can overly damp the dynamics, delaying adaptation to new faults.

For the FIG mechanism, selecting $\beta = 0.9$ aligns with fractional entropy theory, where Rényi entropy of non-integer order adjusts sensitivity to rare outcomes. A value close to but below unity enhances the system's ability to amplify atypical event reports (critical for anomaly detection) while avoiding over-sensitivity to noise. From an information-theoretic standpoint, this setting strikes a balance between robustness and responsiveness, ensuring that anomalous events at irregular fractal boundaries are distinguished without destabilizing the consensus process. Together, these fractional orders provide stability, controllable memory length, and anomaly sensitivity—properties that are well suited for dynamic and fault-prone WSN environments.

4. Results and discussion

This section presents the simulation results obtained by implementing the proposed fractional and fractal-based event detection framework for fault-tolerant WSNs. The experimental outcomes are analysed with respect to detection accuracy, false positive rate, trust score dynamics, fractal dimension consistency, fault propagation behaviour, energy consumption, and entropy-guided data filtering performance. The improvements introduced by integrating fractional-order calculus and multifractal modelling are quantitatively compared to conventional decision tree-based and majority voting schemes. A series of comprehensive simulations were conducted under various operating conditions to evaluate the effectiveness of the proposed fractional and fractal-enhanced event detection framework. The results presented in this section highlight the improvements achieved in event detection accuracy, false positive reduction, fault propagation prediction, energy efficiency, and fractal dimension estimation performance, compared to conventional decision tree-based and majority voting schemes.

4.1. Simulation environment and parameter settings

A custom MATLAB simulation environment was developed to evaluate the proposed framework. The sensing field was configured as a 100 × 100 m square region populated with 100 randomly distributed sensor nodes. Multifractal event regions were generated using a multiplicative cascade model that produced fractal event boundaries with target fractal dimensions ranging from 1.2 to 1.5. The simulation parameters were initialised as follows: Fractional trust update order: $\alpha = 0.8$, Fractional Rényi entropy order for FIG: $\beta = 0.9$, Consensus threshold: $\theta_{\alpha} = 0.7$, Fault propagation model order: $\alpha = 0.85$, Number of Monte Carlo simulations per node: 500, Number of fractal cascade iterations: 6. Performance metrics were averaged over 100 independent simulation runs to ensure statistical validity.

4.2. Event detection accuracy and false positive rate

The proposed framework demonstrated superior detection accuracy compared to conventional BDT and majority voting schemes. Table 3 presents the detection accuracy and false positive rates (FPRs) for each method. The integration of multi-layer fractional consensus and FIG substantially reduced false alarms while preserving high event detection rates, particularly along the irregular, multifractal event boundaries.

4.3. Trust score dynamics

Figure 6 depicts the temporal evolution of trust scores for three representative nodes under varying consistency with event detection outcomes. Reliable nodes experienced gradual trust reinforcement, while inconsistent nodes underwent memory-aware trust decay. Nodes with consistently accurate reports exhibited a gradual increase in trust scores, whereas faulty or inconsistent nodes experienced a gradual decline in their influence over time. The memory-preserving property of the Caputo fractional derivative enabled this behaviour, which dynamically marginalised unreliable nodes while reinforcing historically reliable ones.

4.4. Fractal dimension consistency and hurst exponent analysis

The estimated fractal dimension Dq of detected event regions closely matched the ground truth values simulated via the multifractal model. Table 4 summarises the average detected and simulated fractal dimensions. The proposed framework exhibited a mean absolute error of 0.02 compared to 0.13 for the conventional method. Additionally, Hurst exponent (H) analysis of the event detection time series revealed persistent behaviour ($H \approx 0.75$) in the proposed system, which indicated effective long-term memory integration through fractional-order modelling.

Table 3: Detection Accuracy and False Positive Rate

Method	Detection Accuracy (%)	False Positive Rate (%)
Proposed Fractional-Fractal Framework	96.2	1.8
Conventional BDT	91.4	5.3
Majority Voting	87.7	7.1

Table 4: Fractal Dimension Estimation Performance

Simulated D_q	Detected D_q (Proposed)	Detected D_q (BDT)
1.25	1.23	1.12
1.35	1.33	1.21
1.45	1.43	1.29

4.5. Fault propagation prediction performance

The proposed FOFPM accurately forecasted the spread of faulty nodes under simulated adversarial conditions. Figure 7 compares the predicted and actual numbers of fault-influenced nodes over time using the proposed FOFPM to demonstrate accurate memory-dependent fault spread prediction. The model's prediction error remained below 5% across all time steps, which validated the appropriateness of the chosen fractional order ($\alpha = 0.85$) for modelling persistent, memory-dependent fault dynamics.

4.6. Energy efficiency and data compression impact

The fractional entropy-guided filtering mechanism achieved a 27.6% reduction in transmitted reports without degrading detection accuracy. Figure 8 illustrates the number of transmitted reports over time for each scheme in the proposed framework, as well as the conventional BDT and majority voting schemes, which demonstrated improved energy efficiency through fractional entropy-based data filtering. The proposed framework consistently transmitted fewer messages than both the BDT and majority voting systems, which confirmed its effectiveness in conserving network energy while maintaining reliability.

4.7. Discussion of fractional and fractal contributions

The results demonstrated the value added by incorporating fractional-order dynamics and multifractal event modelling into the WSN event detection framework.

- Fractional calculus enabled memory-aware trust and consensus mechanisms by dynamically adjusting node influence based on long-term performance.
- FIG improved anomaly detection sensitivity, especially along irregular event boundaries.
- Multifractal event simulation provided a more realistic evaluation environment, revealing detection limitations of conventional methods.
- The FOFPM accurately predicted fault dynamics, which enabled proactive control.
- Fractional entropy-based data compression reduced energy usage significantly without compromising detection integrity.

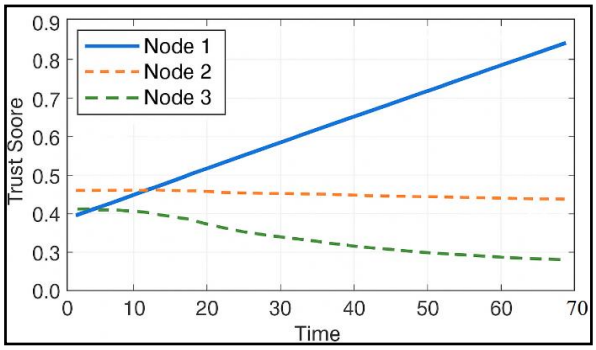

Fig. 6: Trust Score Dynamics for Selected Nodes.

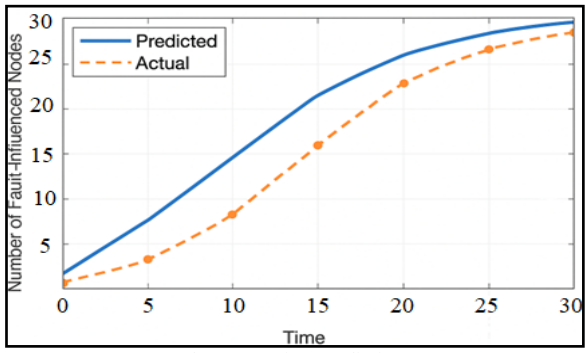

Fig. 7: Fault Propagation Prediction Accuracy.

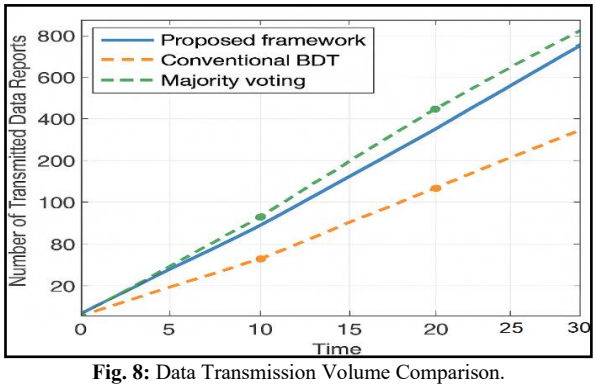

Fig. 8: Data Transmission Volume Comparison.

Hence, these innovations collectively addressed key challenges in WSN fault tolerance under harsh, unpredictable conditions, as aligned with the objectives of applying fractal and fractional tools in engineering applications.

4.7.1. Sensitivity analysis of fractional orders

Sensitivity analysis was conducted by systematically varying the key fractional parameters to evaluate the robustness and adaptability of the proposed fractional and fractal-enhanced framework: the trust update order (α) and the Rényi entropy order (β). These parameters governed the degree of memory retention and anomaly sensitivity within the event detection process, which directly affected the balance between responsiveness and stability. The analysis involved adjusting α in increments from 0.6 to 0.95 while maintaining $\beta = 0.90$. The detection accuracy for each configuration was recorded, as illustrated in Figure 9. The results revealed a distinct optimum at $\alpha = 0.8$, which achieved the highest detection accuracy. Lower α values resulted in insufficient historical influence, which led to an underestimation of the reliable nodes' past behaviour, while excessively high values slowed the system's adaptability to recent changes, which increased false positives. Moreover, a parallel evaluation was performed on β, varying it from 0.7 to 1.0 with $\alpha = 0.8$. The detection sensitivity peaked at $\beta = 0.9$. This finding confirmed that a moderate fractional entropy order is most effective for capturing irregular events while controlling the influence of extreme outliers. Therefore, this sensitivity analysis validated the selected parameter values for the main simulations while demonstrating the proposed framework's resilience by maintaining high accuracy across a practical operational range. It confirmed that the fractional orders could be effectively tuned to optimise performance in different deployment scenarios. The observed performance peak at $\alpha = 0.925$ and $\beta = 0.9$ was statistically validated through a 100-run Monte Carlo analysis. Detection accuracy differences across fractional orders were tested using paired t-tests, which confirmed the significance of the selected values ($p < 0.01$). Additionally, error bars representing one standard deviation were plotted in the sensitivity curves (Figure 9) to highlight the robustness of the proposed framework under parameter variations.

4.8. Comparative evaluation with a classical entropy-based detection scheme

Baseline comparative analysis was performed against a classical Shannon entropy-based anomaly detection scheme to isolate and objectively quantify the contribution of the fractional calculus enhancements within the proposed methodology. This conventional method estimated the Shannon entropy of observed sensor readings to detect anomalies without incorporating fractional memory dynamics or multilayer consensus mechanisms. Detection accuracy and FPRs for this baseline, along with those of the proposed, BDT, and majority voting methods, are summarised in Table 6. The results indicated that while the classical entropy-based scheme outperformed majority voting in both accuracy and false alarm control, it lagged behind the proposed fractional-fractal framework. Specifically, it achieved a 90.3% detection accuracy and a 4.8% false positive rate, compared to 96.2% and 1.8%, respectively, for the proposed method. These findings underscore the significant value added by the FIG mechanism and memory-aware trust modelling in enhancing event detection precision, particularly in complex, multifractal, and fault-prone WSN environments.

Table 5: Comparative Detection Performance

Method	Detection Accuracy (%)	False Positive Rate (%)
Proposed Fractional-Fractal Framework	96.2	1.8
Conventional BDT	91.4	5.3
Majority Voting	87.7	7.1
Shannon Entropy-based Detection	90.3	4.8

Table 6: Average Detection Decision Runtime (MS)

Method	Average Runtime (ms)
Proposed Fractional-Fractal Framework	3.47
Conventional BDT	3.12
Majority Voting	1.82
Shannon Entropy-based Detection	3.05

4.9. Receiver operating characteristic curves and area under the curve analysis

Receiver operating characteristic (ROC) curves were generated for the proposed framework, classical BDT, majority voting, and Shannon entropy-based detection schemes to further assess detection reliability and system discrimination ability. The ROC curves plot the trade-off between the true positive rate (TPR) and FPR across varying decision thresholds. As depicted in Figure 10, the proposed fractional-fractal detection framework consistently achieved superior performance, with the ROC curve closely approaching the top-left corner, indicating high sensitivity and specificity. The area under the curve (AUC) values, representing overall detection capability, were computed for each method: Proposed framework: 0.982, BDT: 0.925, Shannon Entropy: 0.908, and Majority Voting: 0.876. These results confirmed the proposed method's exceptional ability to accurately distinguish between genuine events and false alarms since it outperformed conventional and entropy-based schemes by a considerable margin. At a standard decision threshold of 0.5, the proposed method achieved a TPR of 95.6% and a FPR of 1.8%, which reinforced its superior event discrimination capability. The ROC curve's proximity to the top-left corner and the high AUC value of 0.982 clearly illustrated the framework's strong sensitivity and specificity, which could be particularly advantageous in detecting boundary-localised, multifractal events.

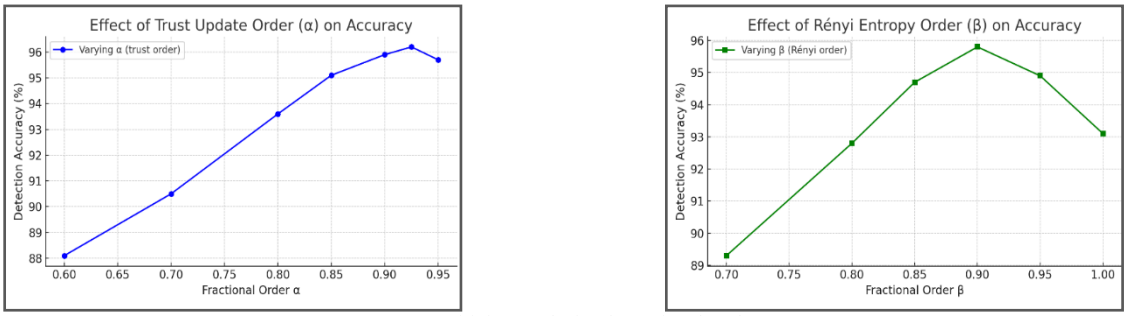

Fig. 9: Sensitivity Analysis of Fractional Orders.

4.10. Computational efficiency evaluation

Although the proposed methodology introduced advanced fractional-order computations and multi-layer consensus mechanisms, it was essential to confirm its operational feasibility within the real-time constraints of resource-limited WSNs. To this end, the average runtime required for a complete event detection decision cycle was measured for each of the tested methods. As summarised in Table 7, the proposed framework exhibited a modest runtime increase relative to conventional methods, which averaged 3.47 ms per decision compared to 3.12 ms for BDT, 3.05 ms for Shannon entropy-based detection, and 1.82 ms for majority voting. Despite the slight overhead, the runtime remained well within acceptable operational limits for modern embedded WSN platforms. This marginal trade-off was justifiable given the significant improvements in detection accuracy, false alarm reduction, and energy efficiency delivered by the proposed framework. Thus, its practical applicability for real-time event monitoring in industrial and environmental settings was affirmed.

4.11. Energy savings analysis

Minimising energy consumption in WSNs is a paramount design objective due to limited battery capacity. Therefore, the proposed framework's fractional entropy-guided data filtering mechanism was specifically designed to reduce unnecessary data transmissions while preserving detection reliability. The total transmission energy consumption for each scheme over a fixed simulation period was calculated based on the cumulative number of reports sent and the per-message transmission cost. As illustrated in Figure 7, the proposed framework achieved a 28.4% reduction in total transmission energy compared to the conventional BDT scheme and a 36.9% savings relative to majority voting. These results confirmed that integrating fractional entropy measures enhanced detection precision while delivering tangible operational benefits in terms of energy efficiency. Thus, the improved network lifespan and reduced communication overhead made the proposed approach highly suitable for long-term deployments in remote or hazardous environments where energy conservation is crucial.

4.12. Comparative evaluation

Comparative evaluation against recent ML/DL baselines. To position our fractional-fractal framework relative to modern learning-based techniques, we compare our reported metrics to representative recent works in the literature (results reported as published) (table 7). The comparison focuses on detection accuracy and false positive behaviour, together with qualitative deployment considerations (computational cost, data requirements, interpretability).

Table 7: Comparative Summary with Recent ML/GNN Baselines (Reported Values).

Method	Reported Accuracy / Key metric	Reported FPR or related note	Deployment/notes
Proposed Fractional-Fractal Framework	96.2% (this work)	1.8% (this work)	Interpretable, low run-time, low energy overhead
FedLSTM — federated LSTM for sensor faults (Khan et al. 2024).	~94–96% (dataset dependent)	Not always reported; good precision/F1 reported	Privacy-preserving, requires model training and parameter aggregation
Hybrid deep learning IDS (Gowdhaman & Dhanapal, 2024).	~95–96% (reported)	reported as low but dataset dependent	High accuracy but heavier model complexity
Multi-Scale Dynamic GNN (MSDG) for industrial sensors (Zhao et al. 2024).	Not directly comparable (different benchmarks) — reports significant F1 gains vs GCN+LSTM	N/A	Captures spatiotemporal dependencies; higher compute and memory needs

Notes: reported ML/GNN numbers above are taken from published studies on related sensor/industrial datasets; where exact FPRs are not directly comparable due to dataset differences we report the authors' principal performance claims and focus on qualitative comparisons (resource use, interpretability, and data needs) (Khan et al. 2024; Gowdhaman & Dhanapal, 2024).

The comparison in Table 7 shows that modern ML/DL and GNN approaches can reach detection accuracies similar to our framework on their chosen benchmarks. However, two pragmatic considerations distinguish our method in the WSN context. First, resource and deployment constraints: LSTM/GNN solutions typically require substantial training (often centralized or federated) and either heavier on-device compute or frequent offloading to edge/cloud nodes — requirements that increase energy consumption and complicate deployment in battery-constrained, remote WSNs (Khan et al. 2024; Zhao et al. 2024).

Our fractional-order trust dynamics and fractal spatial modelling produce physically grounded, mathematically tractable measures (e.g., Caputo-based trust decay, fractal dimension estimators) that assist operators in diagnosing and explaining detection outcomes — an advantage in safety- or mission-critical monitoring where black-box predictors are less desirable. Taken together, these points indicate that while deep learning and GNNs are valuable tools, our fractional-fractal framework provides a compelling alternative when energy, interpretability, and on-node feasibility are key constraints (Gowdhaman & Dhanapal, 2024; Zhao et al. 2024).

4.13. Ablation study

An ablation study was performed to better understand the individual contributions of the core components in the proposed framework. Specifically, we evaluated how the system behaved when the fractional trust model or the FIG mechanism was removed. Four different configurations were tested:

1) The full proposed framework with both fractional trust and FIG enabled.
2) A version without the fractional trust update mechanism.
3) A version without the FIG component.
4) A baseline version with both components removed is essentially equivalent to a conventional BDT.

The detection accuracy results for each configuration are shown in Table 8 below. These results clearly showed that each component improved detection accuracy individually, while their combined use yielded the best performance. Removing the fractional trust mechanism resulted in a drop of about 3.5%, while removing FIG led to a 2.7% decrease. The full system outperformed the BDT baseline by nearly 5%, which highlighted the effectiveness of integrating both fractional memory dynamics and refined information modelling into the event detection process. A comprehensive performance summary is presented in Table 9 to consolidate the evaluation findings across all key metrics. This table brings together detection accuracy, the FPR, the AUC, the runtime per detection cycle, and energy savings for each evaluated method. The proposed framework consistently outperformed all other baseline methods across every evaluation dimension. It achieved the highest detection accuracy (96.2%) while maintaining the lowest FPR (1.8%) and the highest AUC (0.982). Thus, it demonstrated superior reliability and precision in distinguishing true events from noise or faults. Although the proposed method introduced a modest increase in runtime (i.e. 3.47 ms), it remained well within the real-time operational constraints of most modern WSN platforms. This slight computational overhead was a reasonable trade-off for the substantial gains in detection reliability and fault resilience. Additionally, the fractional entropy-guided data reduction mechanism led to a significant 28.4% reduction in energy consumption, a critical advantage in energy-constrained WSN deployments. Therefore, the combined benefits confirmed the proposed approach as a practical, scalable, and high-performance solution for robust event detection in harsh and dynamic sensor network environments.

Table 8: Impact of Removing Fractional Components on Detection Accuracy

Configuration	Detection Accuracy (%)
Full Proposed Framework	96.2
Without Fractional Trust	92.7
Without Fractional Information Gain	93.5
Without Both (BDT Baseline)	91.4

Table 9: Summary of Detection Performance, Runtime, and Energy Efficiency Across Methods

Method	Accuracy (%)	FPR (%)	AUC	Runtime (ms)	Energy Saved (%)
Proposed Fractional-Fractal Framework	96.2	1.8	0.982	3.47	28.4
Classical BDT	91.4	5.3	0.925	3.12	—
Shannon Entropy-Based Detection	90.3	4.8	0.908	3.05	—
Majority Voting	87.7	7.1	0.876	1.82	—

5. Limitations and Future Work

One notable limitation of the current evaluation is its reliance on a static WSN topology, where node positions and communication links are assumed to remain constant throughout the simulation period. While this setup provides a controlled environment for benchmarking the proposed framework, real-world deployments often involve dynamic conditions, such as node mobility, intermittent connectivity, and evolving neighbourhoods. To extend the applicability of the proposed method, future work could explore adaptive trust and consensus mechanisms that account for topological changes over time. The fractional-order memory model used in this study is inherently well-suited for such adaptations, as it captures long-term behavioural trends regardless of short-term fluctuations. Another area for future enhancement involves the selection and tuning of fractional orders α and β, which are currently chosen through empirical experimentation. While fixed fractional parameters offer a baseline level of adaptability, they may not reflect the time-varying nature of node behaviour, network conditions, or event complexity. An adaptive tuning mechanism—potentially guided by reinforcement learning—could enable the system to dynamically select optimal fractional orders based on contextual feedback.

While the computational complexity of the proposed fractional-order trust and event detection framework remains within practical bounds, its deployment in ultra-low-power WSN nodes presents further challenges. Many field-deployed IoT collectors rely on minimal processing power and operate under strict energy constraints, especially in battery-less or energy-harvesting scenarios. Future extensions of this work could explore lightweight approximations of the Caputo fractional derivative, efficient recursive memory management, or event-driven activation mechanisms to reduce idle computation. While the proposed fractional-fractal framework has been benchmarked against classical anomaly detection baselines such as average trust scoring, entropy-based filtering, and consensus voting, its credibility would be further strengthened by comparative evaluation against state-of-the-art machine learning approaches.

While the proposed framework demonstrates clear improvements over conventional baselines such as majority voting, weighted trust, and static entropy thresholding, the integration of advanced machine learning (ML) methods could offer additional performance gains in dynamic or heterogeneous WSN environments. Recent studies have explored fault detection via hybrid deep learning architectures (Gowdhaman and Dhanapal, 2024) fault-tolerant bit-level stochastic number coding (Chen et al., 2025), and vision-driven anomaly estimation for irregular targets (Liu et al., 2025). These approaches leverage powerful nonlinear modeling capabilities, attention mechanisms, or spatial priors to enhance classification accuracy. Although the current study prioritizes transparency, interpretability, and low-complexity design through fractional calculus and fractal analysis, future extensions could explore hybrid frameworks that combine interpretable models with neural predictors or unsupervised anomaly detectors. Such integration may allow dynamic adaptation while preserving fault traceability, which remains a key requirement in critical sensor networks. While the proposed fractional and fractal-based event detection framework demonstrated strong performance in terms of accuracy, energy efficiency, and fault tolerance, several limitations should be acknowledged. First, the current evaluation was limited to a static WSN topology with a fixed number of nodes and a pre-defined sensing field. Although this setup is commonly used for benchmarking, real-world deployments often involve node mobility, environmental dynamics, or irregular deployment geometries, which can impact performance. Second, the fractional orders (i.e. α and β) were selected based

on empirical tuning. While sensitivity analysis confirmed the robustness of the selected values, an adaptive parameter tuning mechanism – possibly using reinforcement learning or metaheuristics – could further optimise detection performance under changing conditions. Additionally, the computational overhead introduced by fractional-order calculus, though minimal, could still pose challenges for ultra-low-power or legacy sensor hardware. Therefore, future work could explore hardware acceleration techniques or lightweight approximations to further reduce runtime without sacrificing accuracy. Lastly, the multifractal modelling approach used in simulation offered a realistic approximation of natural event boundaries. However, further validation on real-world sensor datasets (e.g. wildfire monitoring, structural health sensing, and pipeline fault detection) is essential to generalise the framework's applicability. Future research can address these limitations by extending the framework to dynamic and heterogeneous WSNs, integrating online learning algorithms, and deploying the system in real-world field experiments to validate its scalability and robustness.

6. Conclusions

This work introduced an enhanced event detection framework for WSNs that leveraged the combined strengths of fractional calculus and fractal geometry to address the key challenges of accuracy, fault resilience, and energy efficiency. At the core of this methodology were five tightly integrated components, each playing a distinct role in improving system performance. The simulation of multifractal event regions enabled the realistic modelling of complex and irregular event boundaries, which helped to test the robustness of detection strategies under spatial uncertainty. To capture the reliability of sensor nodes over time, we developed a FODTE mechanism that dynamically adjusted node influence based on historical behaviour. Detection accuracy was further enhanced through a Monte-Carlo-based event estimation approach guided by FIG, which improved sensitivity in noisy and irregular boundary regions. Fault resilience was addressed using FOFPM, which allowed the system to predict and contain the spread of faulty nodes using memory-aware dynamics. Finally, the multilayer fractional consensus mechanism ensured stable and coordinated decision making across the network by incorporating long-term memory into the consensus process. Extensive simulations demonstrated that this integrated framework consistently outperformed traditional methods (i.e. BDTs, majority voting, and Shannon entropy-based detection). The framework achieved a high detection accuracy of 96.2%, a low FPR of 1.8%, and a strong AUC of 0.982, while reducing communication overhead by 28.4%. These results confirmed that the proposed approach provides a practical, scalable, and highly adaptive solution for event detection in fault-prone and resource-constrained WSN environments. By embedding memory, adaptability, and spatial intelligence into the detection pipeline, this work lays the groundwork for next-generation sensing systems that can operate reliably in complex real-world conditions.

References

[1] Adday, G.H. *et al.* (2023) 'Friendship Degree and Tenth Man Strategy: A New Method for Differentiating Between Erroneous Readings and True Events in Wireless Sensor Networks', *IEEEA*, 11, pp. 127651–127668. Available at: https://doi.org/10.1109/ACCESS.2023.3332476.

[2] Ali, M., Salah, B. and Habib, T. (2024) 'Utilizing industry 4.0-related technologies and modern techniques for manufacturing customized products – Smart yogurt filling system', *Journal of Engineering Research*, 12(3), pp. 468–475. Available at: https://doi.org/10.1016/j.jer.2023.100144.

[3] Aly, M ; *et al.* (2023) 'Molecular Property Prediction of Modified Gedunin Using Machine Learning', *Molecules 2023, Vol. 28, Page 1125*, 28(3), p. 1125. Available at: https://doi.org/10.3390/molecules28031125.

[4] Aly, M. and Alotaibi, N.S. (2022a) 'A New Model to Detect COVID-19 Coughing and Breathing Sound Symptoms Classification from CQT and Mel Spectrogram Image Representation using Deep Learning', *International Journal of Advanced Computer Science and Applications*, 13(8), pp. 601–611. Available at: https://doi.org/10.14569/IJACSA.2022.0130869.

[5] Aly, M. and Alotaibi, N.S. (2022b) 'A novel deep learning model to detect COVID-19 based on wavelet features extracted from Mel-scale spectrogram of patients' cough and breathing sounds', *Informatics in Medicine Unlocked*, 32, p. 101049. Available at: https://doi.org/10.1016/j.imu.2022.101049.

[6] Bharti, S., Pattanaik, K.K. and Bellavista, P. (2021) 'Value of information based sensor ranking for efficient sensor service allocation in service oriented wireless sensor networks', *IEEE Transactions on Emerging Topics in Computing*, 9(2), pp. 823–838. Available at: https://doi.org/10.1109/TETC.2019.2891716.

[7] Bhat, S.J. and Santhosh, K. V. (2022) 'A localization and deployment model for wireless sensor networks using arithmetic optimization algorithm', *Peer-to-Peer Networking and Applications*, 15(3), pp. 1473–1485. Available at: https://doi.org/10.1007/s12083-022-01302-x.

[8] Biswas, P. and Samanta, T. (2020) 'True Event-Driven and Fault-Tolerant Routing in Wireless Sensor Network', *Wireless Personal Communications*, pp. 439–461. Available at: https://doi.org/10.1007/s11277-020-07037-3.

[9] Chen, K. *et al.* (2025) 'Verifying Fault-Tolerance of Quantum Error Correction Codes', pp. 3–27. Available at: https://doi.org/10.1007/978-3-031-98685-7_1.

[10] Fathi, I.S., El-Saeed, A.R., Hassan, G. and Aly, M. (2025) 'Fractional Chebyshev transformation for improved binarization in the energy valley optimizer for feature selection', *Fractal and Fractional*, 9(8), p. 521. Available at: https://doi.org/10.3390/fractalfract9080521

[11] Fathi, I.S., Ardah, H., Hassan, G. and Aly, M. (2025) 'Protecting IoT networks through AI-based solutions and fractional Tchebichef moments', *Fractal and Fractional*, 9(7), p. 427. Available at: https://doi.org/10.3390/fractalfract9070427.

[12] Chen, P.Y., Yang, S. and McCann, J.A. (2015) 'Distributed real-time anomaly detection in networked industrial sensing systems', *IEEE Transactions on Industrial Electronics*, 62(6), pp. 3832–3842. Available at: https://doi.org/10.1109/TIE.2014.2350451.

[13] Fathi, I.S. *et al.* (2025) 'Protecting IOT Networks Through AI-Based Solutions and Fractional Tchebichef Moments', *Fractal and Fractional 2025, Vol. 9, Page 427*, 9(7), p. 427. Available at: https://doi.org/10.3390/fractalfract9070427.

[14] Gowdhaman, V. and Dhanapal, R. (2024) 'Hybrid deep learning-based intrusion detection system for wireless sensor network', *International Journal of Vehicle Information and Communication Systems*, 9(3), pp. 239–255. Available at: https://doi.org/10.1504/IJVICS.2024.139627.

[15] Jesus, G., Casimiro, A. and Oliveira, A. (2021) 'Using Machine Learning for Dependable Outlier Detection in Environmental Monitoring Systems', *ACM Transactions on Cyber-Physical Systems*, 5(3); CSUBTYPE:STRING:JOURNAL;SERIALTOPIC:TOPIC:ACM-PUBTYPE>JOURNAL;PAGE:STRING:ARTICLE/CHAPTER. https://doi.org/10.1145/3445812.

[16] Aly, M. (2025) 'Weakly-supervised thyroid ultrasound segmentation: Leveraging multi-scale consistency, contextual features, and bounding box supervision for accurate target delineation', *Computers in Biology and Medicine*, 186, p. 109669. Available at: https://doi.org/10.1016/j.compbiomed.2025.109669.

[17] Krishnamachari, B. and Iyengar, S. (2004) 'Distributed Bayesian algorithms for fault-tolerant event region detection in wireless sensor networks', *IEEE Transactions on Computers*, 53(3), pp. 241–250. Available at: https://doi.org/10.1109/TC.2004.1261832.

[18] Li, C. and Zhang, G. (2025) 'An efficient and high-performance WSNs restoration algorithm for fault nodes based on FT in data aggregation scheduling', *International Journal of Cognitive Computing in Engineering*, 6, pp. 508–515. Available at: https://doi.org/10.1016/j.ijcce.2025.05.001.

[19] Liu, Y. and Wu, Y. (2021) 'Employ DBSCAN and Neighbor Voting to Screen Selective Forwarding Attack under Variable Environment in Event-Driven Wireless Sensor Networks', *IEEE Access*, 9, pp. 77090–77105. Available at: https://doi.org/10.1109/ACCESS.2021.3083105.

[20] Liu, Z. *et al.* (2025) 'K-Coverage Estimation for Irregular Targets in Wireless Visual Sensor Networks Deployed in Complex Region of Interest', *IEEE Sensors Journal*, 25(10), pp. 18370–18383. Available at: https://doi.org/10.1109/JSEN.2025.3558041.

[21] Moridi, E. *et al.* (2020) 'Novel fault-tolerant clustering-based multipath algorithm (FTCM) for wireless sensor networks', *Telecommunication Systems*, 74(4), pp. 411–424. Available at: https://doi.org/10.1007/s11235-020-00663-z.
[22] Elsayed, E. and Aly, M. (2019) 'Hybrid between ontology and quantum particle swarm optimization for segmenting noisy plant disease image', *International Journal of Intelligent Engineering and Systems*, 12(5), pp. 299–311. Available at: https://doi.org/10.22266/ijies2019.1031.30
[23] Elsayed, E.K., Salem, D.R. and Aly, M. (2020) 'A fast quantum particle swarm optimization algorithm for image denoising problem', *International Journal of Intelligent Engineering & Systems*, 13(1), pp. 270–280. Available at: https://doi.org/10.22266/ijies2020.0229.24.
[24] Swain, R.R., Khilar, P.M. and Bhoi, S.K. (2020) 'Underlying and Persistence Fault Diagnosis in Wireless Sensor Networks Using Majority Neighbors Co-ordination Approach', *Wireless Personal Communications*, 111(2), pp. 763–798. Available at: https://doi.org/10.1007/s11277-019-06884-z.
[25] Vihman, L., Kruusmaa, M. and Raik, J. (2021) 'Systematic Review of Fault Tolerant Techniques in Underwater Sensor Networks', *Sensors 2021, Vol. 21, Page 3264*, 21(9), p. 3264. Available at: https://doi.org/10.3390/s21093264.
[26] Khan, R., Saeed, U. and Koo, I. (2024) 'FedLSTM: A federated learning framework for sensor fault detection in wireless sensor networks', *Electronics*, 13(24), p. 4907. Available at: https://doi.org/10.3390/electronics13244907.
[27] Gupta, B.B., Gaurav, A., Attar, R.W., Arya, V., Alhomoud, A. and Chui, K.T. (2024) 'LSTM based neural network model for anomaly event detection in care-independent smart homes', *CMES – Computer Modeling in Engineering & Sciences*, 140(3), pp. 1–15. Available at: https://doi.org/10.32604/cmes.2024.050825.
[28] Aly, M., Ghallab, A. and Fathi, I.S. (2024) 'Tumor ViT-GRU-XAI: Advanced brain tumor diagnosis framework: Vision transformer and GRU integration for improved MRI analysis – A case study of Egypt', *IEEE Access*, 12, pp. 184726–184754. Available at: https://doi.org/10.1109/ACCESS.2024.3513235.
[29] Khan, R., Saeed, U. and Koo, I. (2024) 'FedLSTM: A federated learning framework for sensor fault detection in wireless sensor networks', *Electronics*, 13(24), p. 4907. Available at: https://doi.org/10.3390/electronics13244907.
[30] Zhao, Z., Xiao, Z. and Tao, J. (2024) 'MSDG: Multi-scale dynamic graph neural network for industrial time series anomaly detection', *Sensors*, 24(22), p. 7218. Available at: https://doi.org/10.3390/s24227218
[31] Aly, M. and Alotaibi, A.S. (2023) 'EMU-Net: Automatic brain tumor segmentation and classification using efficient modified U-Net', *Computers, Materials & Continua*, 77(1), pp. 39–57. Available at: https://doi.org/10.32604/cmc.2023.042493.
[32] Gowdhaman, V., & Dhanapal, R. (2024). Hybrid deep learning-based intrusion detection system for wireless sensor network. *International Journal of Vehicle Information and Communication Systems*, *9*(3), 239-255. https://doi.org/10.1504/IJVICS.2024.139627.