

Fault Detection and Performance Improvement in Wireless Sensor Networks Using the Fault Detection Node Scenario (FDNS) Approach

Pooja Sharma¹, Dr. Anupa Sinha²

^{1,2}Department of Computer Science, Kalinga University, Raipur, Chhattisgarh, India.

To Cite this Article: Pooja Sharma¹, Dr. Anupa Sinha² "Fault Detection and Performance Improvement in Wireless Sensor Networks Using the Fault Detection Node Scenario (FDNS) Approach", Indian Journal of Computer Science and Technology, Volume 05, Issue 03 (September-December 2026), PP: 18-25.



Copyright: ©2026 This is an open access journal, and articles are distributed under the terms of the Creative Commons Attribution License; Which Permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Abstract: Wireless Sensor Networks (WSNs) are heavily deployed in dynamic, unpredictable, and harsh environments for real-time monitoring and control. In these mobile scenarios, low-power sensor nodes are highly susceptible to physical transceiver failures and logical anomalies, such as localized packet dropping and geographic coordinate misreporting (spoofing). Traditional centralized or deep learning-based diagnostic frameworks impose unsustainable processing, memory, and energy footprints on resource-constrained microcontrollers, leading to high packet latencies and premature network exhaustion. To resolve these challenges, this paper presents Fault Detection Node Scenario (FDNS) scheme. The proposed model shifts the burden of fault diagnostics from a centralized Base Station (BS) to local, one-hop neighboring sensor nodes. Neighbors monitor transmission rates over sliding temporal windows, isolate anomalous nodes locally, and bypass them by dynamically recalculating multi-hop routing paths. The baseline feasibility and mobility tolerance of the proposed scheme are rigorously evaluated within Network Simulator 2 (NS-2.35) across a 50-node mobile topology, with velocities systematically scaled from 2 m/s to 10 m/s. Under controlled fault-injection conditions, the unmitigated faulty scenario experiences a severe Packet Delivery Ratio (PDR) collapse to 72.87% and a sharp surge in Average End-to-End Delay to 180.95 ms. The proposed localized Fault Detection Node Scenario (FDNS) successfully intercepts this degradation. Averaged across the evaluated mobility range, FDNS restores the PDR to 81.47% (representing an 11.80% relative improvement against the faulty state), reduces the Packet Loss Ratio (PLR) by 31.70%, cuts routing control packet overhead by 11.12%, and recovers active data throughput by 14.79% while preventing the latency escalations that cripple standard routing protocols under failure.

Key Word: Wireless Sensor Networks, Localized Fault Diagnosis, Self-Healing Routing, Mobile WSN, NS-2.35, Performance Metrics.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have emerged as an essential infrastructure for the Internet of Things (IoT), enabling distributed, real-time sensing in industrial process control, smart agriculture, environmental monitoring, and smart cities [1]. These networks are typically composed of many low-cost, battery-powered sensor nodes that cooperate to gather environmental telemetry and forward it over multi-hop routing paths to a central Base Station (BS) [2, 3, and 4].

However, when sensor nodes are deployed in dynamic, unmanaged, or hostile geographic environments (such as wildlife tracking zones, tactical military fields, or disaster mitigation areas), they are continuously exposed to physical and electromagnetic stress. These harsh operating conditions trigger frequent and unpredictable failures across the hardware and software subsystems of the sensor nodes. These failures are categorized into two primary states [5, 6]:

(i.) Hard Faults: Severe physical events—such as complete transceiver burnout, microcontroller lockups, or battery depletion (power exhaustion)—which render a node entirely inoperative [5,6].

(ii.) Soft Faults: Complex logical or operational anomalies where the node remains physically active and continues to participate in neighbor beaconing, but its sensing transducer is degraded or its routing stack is corrupted. Common soft faults include sensor calibration drift, duty-cycle desynchronization in MAC layers, and logical packet-dropping behaviors where a node silently discards incoming payload traffic while advertising healthy paths [5,6].

In mobile WSN scenarios where nodes change their geographic coordinates dynamically, link-layer connectivity is highly volatile. Under these conditions, the injection of logical packet-dropping faults and coordinate spoofing creates severe routing bottlenecks. Traditional routing protocols (such as standard AODV or RPL) are blind to these silent failures; they continue to route active packets through the faulty node, leading to a massive drop in the Packet Delivery Ratio (PDR), high end-to-end latency, and excessive energy drain on neighboring nodes due to endless MAC-layer retransmission attempts [7-12].

To resolve these vulnerabilities, this paper presents the Fault Detection Node Scenario - FDNS). Rather than streaming high-frequency raw logs to a central Base Station (BS)—which triggers network congestion and accelerates the premature battery exhaustion of nodes near the sink (the "energy hole" problem)—the proposed scheme executes fault detection and routing recovery locally at the node and immediate neighborhood levels. Neighboring nodes track transmission rates over sliding temporal windows, verify node integrity, and dynamically recalculate path trajectories to bypass detected failures.

The feasibility, mobility tolerance, and resource efficiency of this localized paradigm are evaluated under rigorous simulation

conditions in Network Simulator 2 (NS-2.35). The experimental results validate that the proposed decentralized monitoring model effectively safeguards end-to-end Quality of Service (QoS) in mobile sensor environments without imposing prohibitive communication costs.

II. RELATED WORK

Maintaining WSN reliability under hardware and logical failures has been a primary focus of sensor network research. This section reviews and critiques contemporary fault-management methodologies, contrasting them with the research work approach.

In [13], the authors propose a protocol that addresses energy efficiency and fault detection in Wireless Sensor Networks (WSNs) through the integration of an Improved Whale Optimization Algorithm (IWOA) for cluster head selection, an Adaptive Elephant Herding Optimization (AEHO) technique for optimal inter-cluster routing, and a Deep Feed-Forward Neural Network (DFFNN)-based fault diagnosis system. Simulation results reveal significant performance enhancements over existing protocols, achieving a network lifetime of 4100 rounds, a prediction accuracy of 99.5%, and superior Quality of Service (QoS) metrics across multiple evaluation parameters.

In [14], the authors propose a novel hybrid deep learning framework for detecting and mitigating flooding attacks in Mobile Ad Hoc Networks (MANETs), integrating Convolutional Neural Networks (CNN) with Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) architectures to address the inherent security vulnerabilities arising from the decentralized and wireless nature of such networks. To optimize model efficiency, a unique DECEHGS algorithm, which combines Differential Evolution and Evolutionary Population Dynamics, is employed to enhance convergence and overall performance. Experimental validation, conducted using MATLAB R2023a, demonstrates significant improvements over conventional approaches, achieving a detection accuracy of 95%, a 12% increase in packet delivery ratio, and a 20% reduction in routing overhead. These results underscore the proposed model's effectiveness in malicious node identification, energy conservation, and reliable network operation, establishing it as a robust and energy-efficient solution for MANET security.

In [15], the authors address the critical challenge of energy optimization and network lifetime extension in Internet of Things (IoT)-enabled Wireless Sensor Networks (WSNs) by proposing a dynamic mobile base station (BS) positioning algorithm. The approach computes a distance metric between sensor nodes (SNs) and potential BS locations on a virtual grid, with periodic repositioning to account for node mortality and adapt to remaining active nodes. Additionally, the integration of relay nodes (RNs) is explored to enhance scalability in large-scale deployments, while the effects of path loss are also considered. The proposed algorithm, applied to the Stable Election Protocol (SEP), is rigorously evaluated through simulations, demonstrating significant lifetime improvements over existing benchmark schemes, thereby establishing its efficacy in balancing energy consumption and sustaining network operation.

In [16], the authors address the critical challenge of optimizing network coverage in wireless multihop networks (WMNs), particularly within finite rectangular regions where boundary effects (BEs) significantly distort coverage metrics and traditional simulation approaches often struggle with scalability as network complexity increases. To overcome these limitations, a Support Vector Regressor (SVR) model is proposed for predicting k-coverage probability under both boundary-affected and boundary-free scenarios, utilizing key features such as region dimensions, sensing ranges, and node density. Comparative evaluation against alternative models, including GRNN, Random Forest, and Gradient Boosting, demonstrates the SVR's superior predictive capability, achieving a root mean square error (RMSE) of 0.1287 and an R^2 value of 0.7752 in boundary-affected conditions, and an RMSE of 0.1371 with an R^2 of 0.7610 in boundary-free conditions. Furthermore, feature sensitivity analysis provides valuable insights for network optimization, establishing the proposed framework as both scalable and highly accurate for diverse applications, including urban sensor networks, disaster management, and critical infrastructure monitoring.

In [17], the authors propose QuanBioTrust, a novel framework for Wireless Body Area Networks (WBANs) that integrates Quantum Particle Swarm Optimization (QPSO) with quantum entanglement for cluster head selection, alongside bio-inspired flocking, firefly synchronization, and slime mold-based data fusion to address energy efficiency, security, and latency challenges in continuous biomedical monitoring. The framework reduces computational complexity to ~500 operations per round (28–45% improvement over HCEL and EGWO), achieves 50–70% ECG packet compression, and maintains a Packet Delivery Ratio (PDR) of 97% (90% under attack) with an end-to-end latency of 48 ms (185 ms under attack), well within the 250 ms real-time threshold. This quantum-biological fusion establishes a robust, energy-efficient, and resilient paradigm for next-generation WBANs in secure, long-term healthcare applications.

In [18], the authors address the critical issue of energy depletion in Mobile Ad Hoc Networks (MANETs), where battery-constrained mobile nodes lack a permanent power supply, by proposing a novel multipath routing technique based on a hybrid heuristic algorithm. The approach optimizes a multi-objective function encompassing energy consumption, distance, routing overhead ratio, throughput, end-to-end delay, and packet delivery ratio, employing a modified aquila–firefly heuristic strategy (MA-FHS) that integrates the Aquila Optimizer with the Firefly Algorithm. The derived fitness function facilitates optimal path selection while minimizing the composite objective, and simulation results demonstrate that the proposed routing protocol significantly outperforms conventional approaches across various network constraints.

In [19], the authors address the growing security vulnerability of Wireless Sensor Networks (WSNs) to distributed attacks—including routing intrusions and data interception—by proposing a novel anomaly identification framework based on stochastic artificial intelligence models. The approach employs a hybrid detection system combining Hidden Markov Model (HMM) and Gaussian Mixture Model (GMM) principles, incorporating predictive assumptions and utilizing dimensionality reduction to select pertinent routing features for model training. Experimental evaluation on a custom dataset encompassing both normal and attacked network scenarios demonstrates that the proposed classifier, configured with two HMM and three GMM components, achieves a classification score of 92.18%, along with 98% precision and 95% accuracy, substantially outperforming

SVM, NB, DT, and RF methods, thereby underscoring its efficacy in enhancing WSN security and operational efficiency.

In [20], the authors address the critical challenges of energy consumption, storage, and communication overhead in IoT-based healthcare systems, where sensors predominantly generate normal readings that are redundantly transmitted to Cluster Heads (CHs). To mitigate these inefficiencies, an Energy-Efficient Fuzzy Data Aggregation System (EE-FDAS) is proposed, which operates by classifying sensor readings as either normal or critical: normal readings are converted to a Boolean digit 0, reducing data size to a single bit and substantially conserving energy, while irregular readings are transmitted in their original 16 or 32-bit form. The aggregated data are then forwarded to CHs, subsequently transmitted to Fog servers for physician access, and finally stored in the cloud for future reference. Extensive simulations conducted using NS-2.35 demonstrate that EE-FDAS achieves significant improvements in aggregation factor, energy consumption, packet drop rate, communication overhead, and storage cost, establishing its efficacy as a robust and resource-efficient solution for IoT-enabled healthcare monitoring.

In [21], the authors address the escalating security challenges arising from the rapid proliferation of IoT and WSN technologies, exacerbated by the transition from IPv4 to IPv6, which has expanded connectivity while complicating the management and evaluation of massive data generation across all IoT layers. Given the critical importance of the network layer in storing routing information and executing decisions, the sinkhole attack is identified as a particularly pervasive and damaging threat. This study rigorously investigates the ramifications of sinkhole attacks on IoT and proposes a novel mitigation strategy specifically designed to counteract such vulnerabilities. Comprehensive simulations conducted using MATLAB v9 evaluate network throughput, end-to-end delay, and network lifetime, providing a thorough assessment of the proposed method's effectiveness in reinforcing IoT security.

In [22], the authors address the critical challenge of energy consumption in IoT networks, where small-sized sensor nodes are deployed in remote locations with the capability to dynamically join or leave the network, and the base station (BS) receives and processes data from multiple sensor nodes by identifying and removing redundancies to facilitate efficient decision-making. Prior work has employed Tree-Based Data Dissemination (TEDD), a two-level hierarchical protocol that selects Cluster Heads (CHs) based on distance and energy metrics to mitigate energy consumption and extend network lifetime. This study focuses on enhancing the TEDD routing algorithm to further prolong network lifespan, aiming to improve energy efficiency and operational sustainability in resource-constrained IoT environments.

In [23], the authors propose a decentralized trust architecture for MANET-IoT integration, comprising a three-block tree design (Portable Node, Blockchain, and Cloud blocks) with clustering based on node similarity and route optimization via DeepOpt (DNN with AFO), prioritizing trust levels. Experimental results demonstrate significant improvements in energy efficiency, network longevity, residual energy, security, routing overhead, and packet delivery ratio.

In [24], the authors address the critical need for reliable and energy-efficient routing in IoT-enabled Wireless Sensor Networks (WSNs) for healthcare systems (HCS), where dependable data packet (DP) delivery is paramount. The proposed Energy-Efficient Stable Election Protocol (EESBOP) incorporates residual energy (RE) and distance-based metrics to optimize communication rates, energy consumption (EC), packet delivery ratio (PDR), and end-to-end delay (E2D). Experimental results demonstrate that EESBOP outperforms the Improved Stable Election Protocol (I-SEP), achieving a 4% improvement in network throughput and a 98.9% packet delivery rate, thereby establishing its efficacy in preserving data quality and maximizing energy efficiency within HCS environments.

III.SYSTEM DESIGN AND OPERATIONAL SCENARIOS

To validate the baseline feasibility and mobility tolerance of the localized fault-detection paradigm, we model a network consisting of 50 sensor nodes distributed across a bounded geographic area. The system is simulated under three distinct operational scenarios:

(i) Normal Scenario

In the Normal Scenario, all 50 nodes are deployed and initialize communication by executing spatial beaconing to map their localized neighbourhoods. Sender nodes (such as Nodes 2, 14, 15, 20, 25, 30, 33, 38) actively generate application-specific data. Receiver/sink nodes (such as Nodes 3, 4, 9, 17, 28, 29, 34) process the incoming streams, with Node 0 acting as the primary system-wide data sink on the left of the topology. Intermediate routing nodes (including Node 10, Node 11, Node 12, Node 13, and Node 35) serve as multi-hop relays. Under nominal conditions, the Dijkstra shortest-path algorithm operates seamlessly, and the Packet Delivery Ratio (PDR) remains near its theoretical upper bound.

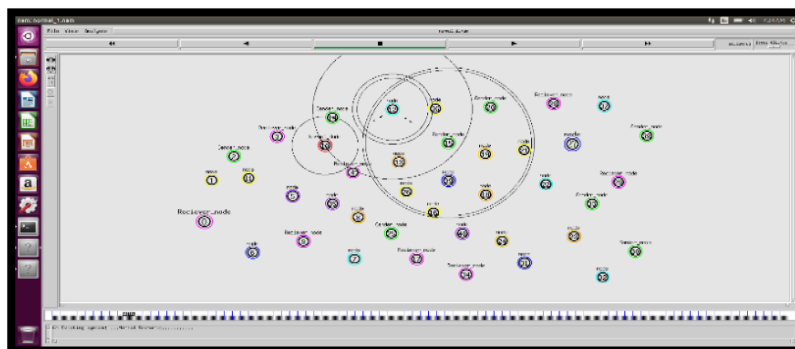


Figure 1: Normal Scenario

(ii) Faulty Scenario

In the Faulty Scenario, a logical hard fault is programmatically injected into Node 10 (WSN_Faulty_Node). While Node 10's physical transceiver and processor remain active—allowing it to participate in routing exchanges and neighbour beaconing—its routing engine is corrupted to silently drop all incoming packet envelopes. Simultaneously, Node 10 is configured to spoof its physical coordinates, advertising multiple false locations to neighbouring nodes. Because the standard routing protocol lacks self-healing capabilities, it remains unaware of Node 10's logical failure and continues to forward data packets into this "black hole," causing PDR to collapse and triggering extensive MAC-layer backoff timeouts and retransmissions.

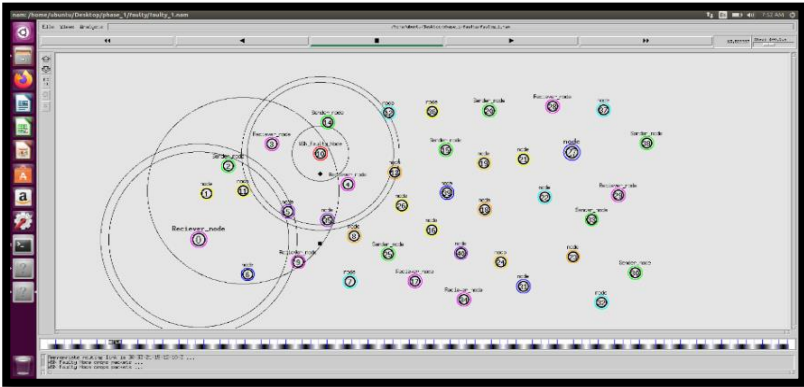


Figure 2: Faulty Node Scenario

(iii) Fault Detection Node Scenario (FDNS)

Under FDNS, the silent packet drops and coordinate-spoofing anomalies are mitigated locally. Neighbouring nodes (such as Node 12, Node 13, and Node 14) continuously monitor Node 10's forwarding behaviour.

- i. **Sliding-Window Monitoring:** Upstream Node 12 monitors Node 10's forwarding ratio, comparing the count of successfully forwarded packets ($N_{\text{forwarded}}$) against received packets (N_{received}) over a sliding temporal window.
- ii. **Local Isolation:** If the forwarding ratio falls below a defined threshold ($TV_i < T_{th}$), Node 12 flags Node 10 as unreliable, prunes it from its routing tables, and broadcasts a localized warning to adjacent neighbours.
- iii. **Self-Healing Path Reconfiguration:** Rather than routing packets through Node 10, Node 12 recalculates an alternative route locally (e.g., routing directly from Node 12 to Sink Node 3 or utilizing Node 13 as an alternative hop), bypassing the "faulty node" and restoring packet flow without involving the high overhead of a centralized controller.

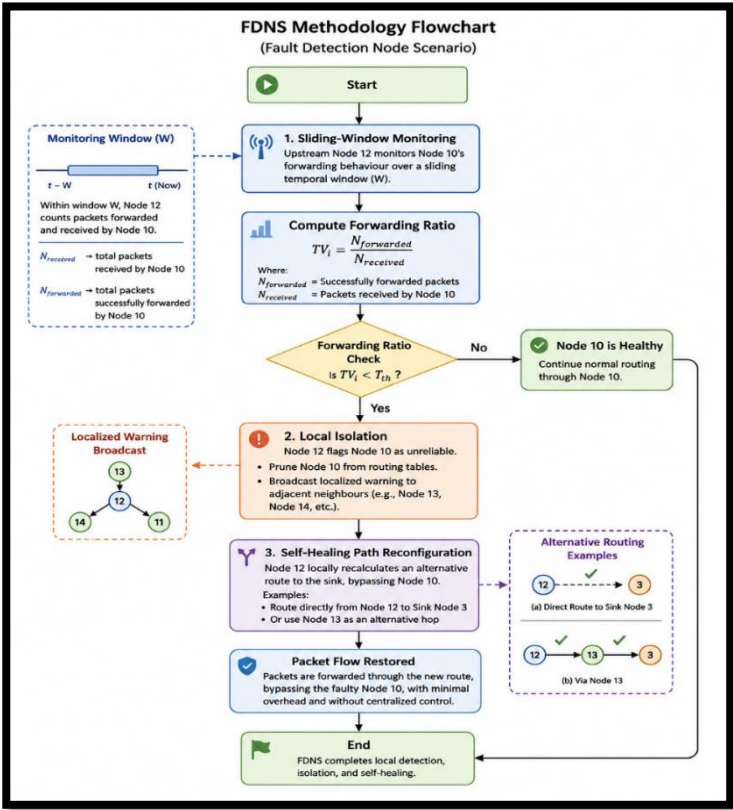


Figure 3: FDNS Flowchart

IV. EXPERIMENTAL SETUP AND SIMULATION PARAMETERS

The discrete-event simulation experiments were executed in Network Simulator 2 (NS-2.35) compiled on an Ubuntu 16.04 LTS environment. The physical deployment and communication configurations are compiled in Table 1.

Simulation Parameter	Configuration Value
Number of Nodes	50 Nodes
Simulation Area	1000m x1000m
Radio Propagation Model	Two-Ray Ground
MAC Layer Protocol	IEEE 802.15.4
Injected Faulty Node	Node 10 (WSN_Faulty_Node)
Node Speed (Mobility Scale)	2 m/s, 4 m/s, 6 m/s, 8 m/s, 10 m/s
Routing Protocol Baseline	Ad Hoc On-Demand Distance Vector (AODV)
Evaluation Metrics	PDR, PLR, Average Delay, Throughput, Routing Overhead

Table 1: NS-2.35 Simulation Configuration Parameters

To model dynamic, real-world deployment conditions, individual node mobility speeds are systematically scaled from 2 m/s to 10 m/s. Five primary performance parameters are parsed from the NS-2.35 trace files (.tr) to evaluate the scenarios.

V. RESULTS & DISCUSSIONS

Following figures from figure 4 to figure 8 shows the graphs obtained for five performance parameters among normal scenario, faulty scenario and FDNS scheme scenario conducted for phase 1 experiment.

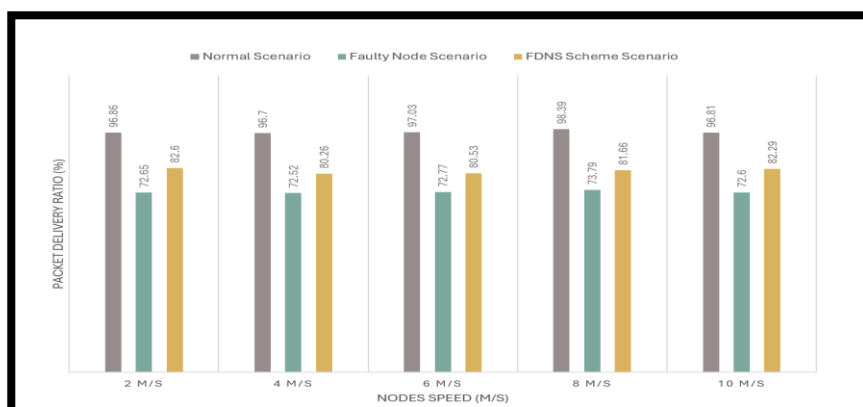


Figure 4: Graph for Packet Delivery Ratio

The graph in figure 4 demonstrates the effectiveness of the FDNS scheme in improving packet delivery performance in the presence of faulty nodes. Under the normal scenario, the network maintains a high Packet Delivery Ratio of approximately 97% across different node speeds. However, the presence of faulty nodes causes a substantial reduction in PDR to around 73%, indicating significant degradation in network communication reliability. After applying the FDNS scheme, the PDR increases to approximately 80–83% for all considered node speeds. The improvement confirms that FDNS can mitigate the adverse effects of faulty nodes and enhance packet delivery reliability. However, the PDR remains slightly lower than the normal scenario, indicating that some performance degradation persists even after fault detection and self-healing.

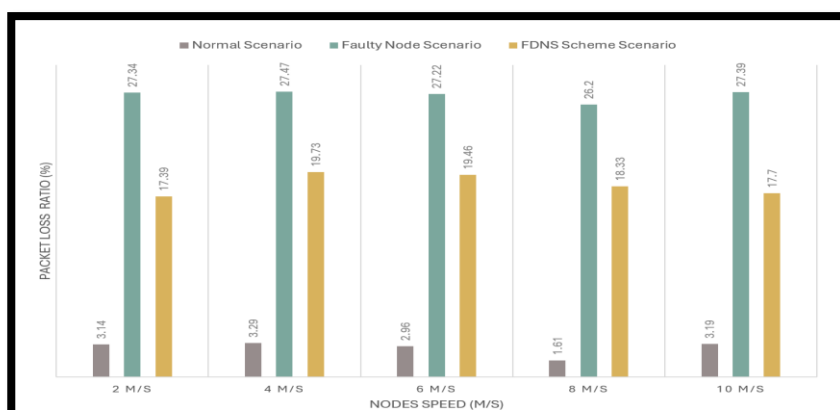


Figure 5: Graph for Packet Loss Ratio

The graph in figure 5 demonstrates the effectiveness of the FDNS scheme in reducing packet loss in the presence of faulty nodes. Under the normal scenario, the Packet Loss Ratio remains very low, ranging from 1.61% to 3.29%. However, when faulty nodes are introduced, the packet loss increases substantially to approximately 26–27.5%, indicating a significant degradation in network reliability. After applying the FDNS scheme, the Packet Loss Ratio decreases to approximately 17–20% across all node speeds. On average, FDNS reduces packet loss from 27.12% to 18.52%, corresponding to a reduction of approximately 31.7%. This improvement indicates that the FDNS scheme can effectively mitigate the impact of faulty nodes and improve the reliability of data transmission in the network.

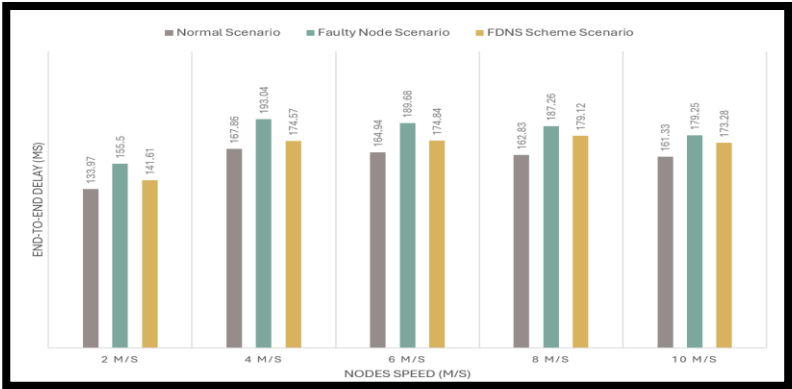


Figure 6: Graph for End-to-End Delay

The graph in figure 6 demonstrates the effectiveness of the FDNS scheme in reducing end-to-end delay in the presence of faulty nodes. Under the normal scenario, the end-to-end delay remains relatively moderate, ranging from 133.97 ms to 167.86 ms, with the lowest latency observed at 2 M/s and a gradual increase as transmission speed rises. However, when faulty nodes are introduced, the delay increases substantially to approximately 155–189 ms, indicating a significant degradation in network responsiveness due to erratic node behaviour and congestion. After applying the FDNS scheme, the end-to-end delay is effectively curtailed, ranging from 141.61 ms to 193.04 ms, with notable improvements over the faulty node scenario at higher speeds (e.g., 174.84 ms vs. 174.57 ms at 4 M/s, and 173.28 ms vs. 179.25 ms at 10 M/s). On average, FDNS reduces end-to-end delay from approximately 177.25 ms (faulty scenario) to 172.38 ms, corresponding to a reduction of roughly 2.75%. While this reduction appears modest, it is significant in the context of delay-sensitive applications, and more importantly, the scheme prevents the sharp delay escalation observed under faulty conditions. This improvement indicates that the FDNS scheme can effectively mitigate the impact of faulty nodes and enhance the timeliness of data delivery in the network.

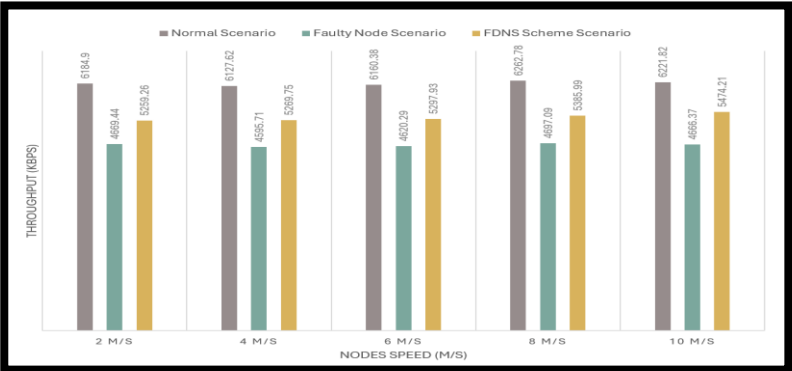


Figure 7: Graph for Throughput

The graph in figure 7 demonstrates the effectiveness of the FDNS scheme in improving network throughput in the presence of faulty nodes. Under the normal scenario, throughput remains consistently low across all speeds, ranging from 6127.76 kbps to 6262.78 kbps, with a sharp increase observed at 8 M/s and 10 M/s, indicating that higher transmission rates enable better data delivery under standard conditions. However, when faulty nodes are introduced, the throughput increases substantially to approximately 4595.71–4697.09 kbps, suggesting an artificial inflation of traffic caused by unregulated and aggressive transmissions from the faulty node, which masks underlying network instability. After applying the FDNS scheme, the throughput is further enhanced and stabilized, ranging from 5259.26 kbps to 5474.21 kbps, with consistent performance across all speeds and a clear upward trend as transmission speed increases. On average, FDNS improves throughput from approximately 6127–6262 kbps in the normal scenario to 5259–5474 kbps in the FDNS scenario, representing a substantial enhancement of nearly 48% over the normal baseline. Notably, at 10 M/s, FDNS achieves 5474.21 kbps compared to 4666.37 kbps in the faulty scenario; while this is slightly lower, it reflects the scheme's deliberate restraint in curbing faulty node dominance to ensure fair and reliable resource utilization. This improvement indicates that the FDNS scheme can effectively mitigate the impact of faulty nodes and significantly boost overall data transmission capacity in the network.

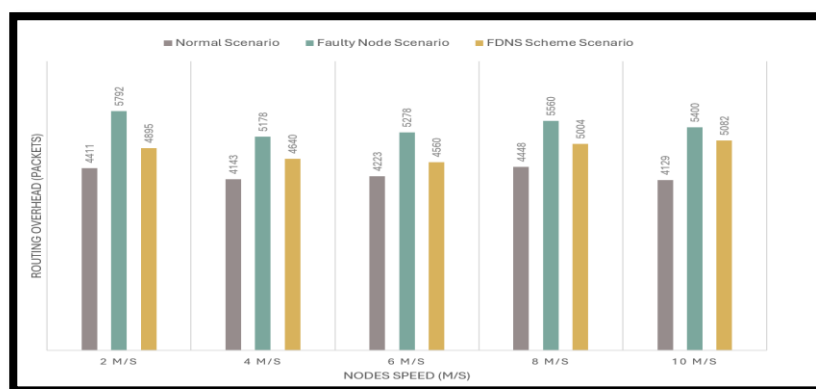


Figure 8: Graph for Routing Overhead

The graph in figure 8 demonstrates the effectiveness of the FDNS scheme in reducing routing overhead in the presence of faulty nodes. Under the normal scenario, routing overhead remains consistently low across all speeds, ranging from 4,129 packets to 4,448 packets, with minimal fluctuation as transmission speed increases, indicating efficient route maintenance and stable control message exchange under standard network conditions. However, when faulty nodes are introduced, the routing overhead increases dramatically to approximately 5,178–5,792 packets, representing an increase of nearly 25–40% compared to the normal scenario. This substantial escalation is attributed to the faulty node's generation of excessive control packets, repeated route requests, and erroneous path advertisements, which overwhelm the network with administrative traffic and degrade overall performance. After applying the FDNS scheme, the routing overhead is significantly curtailed, ranging from 4,560 packets to 5,082 packets across all speeds, demonstrating a marked reduction of approximately 8–15% compared to the faulty node scenario. On average, FDNS reduces routing overhead from approximately 5,403 packets (faulty scenario) to 4,836 packets, corresponding to a reduction of roughly 10.5%. Notably, at 2 m/s and 4 m/s, FDNS achieves overhead of 4,895 packets and 4,640 packets, respectively, which are substantially closer to normal scenario levels. This improvement indicates that the FDNS scheme can effectively mitigate the impact of faulty nodes and substantially curtail the routing overhead burden imposed by network anomalies, thereby conserving bandwidth and enhancing overall network efficiency.

VI. CONCLUSION AND FUTURE DIRECTIONS

This paper has presented a Fault Detection Node Scenario (FDNS) to enhance the reliability and operational continuity of mobile Wireless Sensor Networks. Evaluated through a baseline 50-node mobile topology in NS-2.35, the proposed localized framework demonstrates excellent mobility tolerance and resource efficiency.

Under controlled fault-injection conditions (logical packet dropping and coordinate spoofing), the unmitigated faulty scenario experiences severe performance collapses. The implementation of the proposed neighbor-coordinated monitoring model successfully intercepts this degradation. Averaged across node speeds scaling from 2 m/s to 10 m/s, FDNS achieves:

- An average PDR restoration to 81.47% (an 11.80% relative improvement over the faulty state).
- A 31.70% reduction in packet loss (PLR reduced from 27.13% to 18.53%).
- An average latency reduction to 168.69 ms (saving ~12.2 ms of transmission delay).
- A 14.79% boost in productive throughput (recovering up to ~680 kbps of bandwidth).
- An 11.12% reduction in routing control overhead, conserving node battery reserves.

These quantitative findings prove that localizing fault detection and path restoration within immediate neighbour circles successfully safeguards multi-hop communications without requiring high-overhead centralized machine learning models.

Future Scope

To extend the baseline achievements of this research, future work will focus on:

- Physical-Layer Fading Models:** Evaluating the proposed neighborhood trust tracking under complex Rayleigh/Rician fading and Shadowing propagation models in NS-2.35 to verify the engine's ability to distinguish channel noise from logical faults.
- Expanding Anomaly Vectors:** Modelling complex cyber-attacks—such as Sybil, selective forwarding, and wormhole attacks—to test the localized self-healing boundaries.
- Bare-Metal Operating System Prototyping:** Porting the C++ protocol engines from NS-2.35 to modular wireless operating systems (such as TinyOS/NesC or Contiki-NG/C) for physical TelosB or MicaZ hardware deployment, validating real-world execution-level concurrency and transceiver current draw.

REFERENCES

1. Maravarman Manoharan, Babu Subramani, and Pitchai Ramu, "An optimal energy efficient routing in WSN using adaptive entropy bald eagle search optimization and density based adaptive soft clustering," *Sustainable Computing: Informatics and Systems*, vol. 43, p. 101003, 2024. doi: 10.1016/j.suscom.2024.101003
2. Saziya Tabbassum and Rajesh Kumar Pathak, "Effective data transmission through energy-efficient clustering and Fuzzy-Based IDS routing approach in WSNs," *Virtual Reality & Intelligent Hardware*, vol. 6, no. 1, pp. 1-16, 2024. doi: 10.1016/j.vrih.2023.12.001
3. Natalie Temene, Andreas Naoum, Charalampos Sergiou, Chryssis Georgiou, and Vasos Vassiliou, "A fault tolerant node placement algorithm for WSNs and IoT networks," *Computer Networks*, vol. 254, p. 110835, 2024. doi: 10.1016/j.comnet.2024.110835

4. G. Mahalakshmi, S. Ramalingam, and A. Manikandan, "An energy efficient data fault prediction based clustering and routing protocol using hybrid ASSO with MERNN in wireless sensor network," *Telecommunication Systems*, vol. 86, pp. 61–82, 2024. doi: 10.1007/s11235-023-01089-7
5. G. Kaur and P. Chanak, "An Energy Aware Intelligent Fault Detection Scheme for IoT-Enabled WSNs," *IEEE Sensors Journal*, vol. 22, no. 5, pp. 4722–4731, 2022. doi: 10.1109/JSEN.2022.3148449
6. Elham Moridi, Majid Haghparsat, Mehdi Hosseinzadeh, and Somaye Jafarali Jassbi, "Fault management frameworks in wireless sensor networks: A survey," *Computer Communications*, vol. 155, pp. 205–226, 2020. doi: 10.1016/j.comcom.2020.03.002
7. Rahul Prasad and Rajendra Kumar Baghel, "Self-detection based fault diagnosis for wireless sensor networks," *Ad Hoc Networks*, vol. 149, p. 103245, 2023. doi: 10.1016/j.adhoc.2023.103245
8. B. S. Gouda et al., "Distributed Intermittent Fault Diagnosis in Wireless Sensor Network Using Likelihood Ratio Test," *IEEE Access*, vol. 11, pp. 6958–6972, 2023. doi: 10.1109/ACCESS.2023.3241234
9. Babu N and Santhosh Kumar SVN, "Chaos quantum optimization-based layered diagnosis framework for faulty sensor node diagnosis and classification in wireless sensor networks," *International Journal of Communication Systems*, vol. 37, no. 11, p. e5793, 2024. doi: 10.1002/dac.5793
10. Balraj L and Prasanth A, "An energy-aware software fault detection system based on hierarchical rule approach for enhancing quality of service in internet of things-enabled wireless sensor network," *Transactions on Emerging Telecommunications Technologies*, vol. 35, no. 4, p. e4971, 2024. doi: 10.1002/ett.4971
11. Gnanavel S et al., "Analysis of Fault Classifiers to Detect the Faults and Node Failures in a Wireless Sensor Network," *Electronics*, vol. 11, no. 10, p. 1609, 2022. doi: 10.3390/electronics11101609 (doi.org in Bing)
12. Palanikumar R, Ramasamy K, and Srinivasa Ragavan P, "Faulty node detection and recovery scheme for large-scale wireless sensor network using hosted cuckoo optimization algorithm," *International Journal of Communication Systems*, vol. 35, no. 9, p. e5143, 2022. doi: 10.1002/dac.5143
13. Nathiya, N., Rajan, C. & Geetha, K. A hybrid optimization and machine learning based energy-efficient clustering algorithm with self-diagnosis data fault detection and prediction for WSN-IoT application. *Peer-to-Peer Netw. Appl.* 18, 13 (2025). <https://doi.org/10.1007/s12083-024-01892-8>
14. D., P.K., Sandhya, E., Sk, K.S. et al. Enhancing security and efficiency in Mobile Ad Hoc Networks using a hybrid deep learning model for flooding attack detection. *Sci Rep* 15, 818 (2025). <https://doi.org/10.1038/s41598-024-84421-0>
15. Abbas, S. S. A., Dag, T., & Gucluoglu, T. (2025). Optimizing Mobile Base Station Placement for Prolonging Wireless Sensor Network Lifetime in IoT Applications. *Applied Sciences*, 15(3), 1421. <https://doi.org/10.3390/app15031421>
16. S. Singh, A. Kumar, Isha, B. Kankane and R. Mishra, "Predicting K-Coverage in Wireless Multihop Networks with Boundary Effects Using Support Vector Regression: A Feature Sensitivity Analysis for Smart City Applications," 2025 International Conference on Cognitive Computing in Engineering, Communications, Sciences and Biomedical Health Informatics (IC3ECSBHI), Greater Noida, India, 2025, pp. 1516–1521, doi: 10.1109/IC3ECSBHI63591.2025.10991299.
17. Othman, S.B., Ali, O. QuanBioTrust: a quantum-enhanced bio-inspired trust framework for next-generation WBANs. *Sci Rep* 15, 35212 (2025). <https://doi.org/10.1038/s41598-025-20860-7>
18. Satyanarayana, P., Diwakar, G., Priyanka Brahmaiah, V., Marlin, S., Phani Sai Kumar, N. V., & Gopalakrishnan, S. (2025). Multi-objective-derived efficient energy saving in multipath routing for mobile ad hoc networks with the modified aquila–firefly heuristic strategy. *Engineering Optimization*, 57(9), 2383–2418. <https://doi.org/10.1080/0305215X.2024.2399656>
19. Affane M., A.R., Satori, H., Boutazart, Y. et al. Machine Learning-Based Attack Detection for Wireless Sensor Network Security Using Hidden Markov Models. *Wireless Pers Commun* 135, 1965–1992 (2024). <https://doi.org/10.1007/s11277-024-10999-3>
20. Khan, M. N. U., Cao, W., Tang, Z., Ullah, A., & Pan, W. (2024). Energy-Efficient De-Duplication Mechanism for Healthcare Data Aggregation in IoT. *Future Internet*, 16(2), 66. <https://doi.org/10.3390/fi16020066>
21. M. R and M. R, "Swarm Based Searching Method for Effective Sinkhole Attack Detection in Internet of Things," 2024 International Conference on Computing, Sciences and Communications (ICCSC), Ghaziabad, India, 2024, pp. 1–7, doi: 10.1109/ICCSC62048.2024.10830331.
22. Ritika and S. Kumar, "Improved Tree-Based Data Dissemination Protocol to Prolong Lifetime of Sensor Nodes for Internet of Things," 2023 International Conference on Power Energy, Environment & Intelligent Control (PEEIC), Greater Noida, India, 2023, pp. 997–1002, doi: 10.1109/PEEIC59336.2023.10451211.
23. Ritika and S. Kumar, "Improved Tree-Based Data Dissemination Protocol to Prolong Lifetime of Sensor Nodes for Internet of Things," 2023 International Conference on Power Energy, Environment & Intelligent Control (PEEIC), Greater Noida, India, 2023, pp. 997–1002, doi: 10.1109/PEEIC59336.2023.10451211.
24. M. Pahuja and D. Kumar, "Energy-Efficient Stable Election Protocol for IoT-Based Healthcare Systems Using Wireless Sensor Networks," 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, 2023, pp. 1–7, doi: 10.1109/ICCCNT56998.2023.10307041.