RESEARCH PAPER

AeroSense: Energy-Aware Anomaly-Driven Fault Monitoring for Wireless Sensor Networks

Mrs. G. Premalatha[1], Hariharan S[2], Kitheyon A[3]

[1]Senior Assistant Professor, Department of Electronics and Communication Engineering, IFET College of Engineering, Villupuram, India
Email: pgsmartprem@gmail.com

[2]IV/B.E/ECE, Department of Electronics and Communication Engineering, IFET College of Engineering, Villupuram, India
Email: hariharansubramanian169@gmail.com

[3]IV/B.E/ECE, Department of Electronics and Communication Engineering, IFET College of Engineering, Villupuram, India
Email: kithekethci26@gmail.com

ABSTRACT

Wireless Sensor Networks consist of large numbers of low-power sensor nodes deployed to operate autonomously over extended periods. In such deployments, sensor nodes are exposed to environmental stress, hardware degradation, and energy limitations, which often result in subtle abnormal behaviors rather than complete node failures. These behaviors may appear as irregular sensor values, persistent output patterns, gradual measurement drift, communication irregularities, or accelerated battery depletion.

Index Terms: Wireless Sensor Networks, Fault Detection, Anomaly Detection, Energy Efficiency, Lightweight Algorithms.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have become an important component of modern monitoring and automation systems because they enable physical environments to be observed in a distributed and cost-effective manner. A typical WSN is composed of a large number of small, low-power sensor nodes deployed over a geographical region to collect data such as temperature, humidity, pressure, vibration, and pollution levels. These networks are commonly applied in areas such as environmental monitoring, smart agriculture, industrial automation, healthcare applications, structural health monitoring, and disaster management.

Despite their wide range of applications, WSNs operate under strict resource constraints. Sensor nodes rely on limited-capacity batteries and are frequently deployed in locations where battery replacement or routine maintenance is difficult or impractical. Along with energy limitations, sensor nodes possess limited computational capability, restricted memory, and depend on wireless communication links that may be unreliable. These constraints make energy efficiency and operational reliability key considerations in WSN deployments. During long-term operation, sensor nodes are exposed to harsh environmental conditions, including temperature variations, humidity, dust, and electromagnetic interference. As a result, sensor nodes become vulnerable to different types of faults. Factors such as hardware degradation, sensor aging, and environmental stressors can lead to gradual performance deterioration, making early fault detection and energy-aware monitoring essential for maintaining network reliability and longevity.

How to cite this article: Premalatha G, Hariharan S, Kitheyon A. AeroSense: Energy-Aware Anomaly-Driven Fault Monitoring for Wireless Sensor Networks. Int J Drug Deliv Technol. 2026;16(52s): 1123-1130. DOI: 10.25258/ijddt.16.52s.145

Source of support: Nil.

Conflict of interest: None.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have become an important component of modern monitoring and automation systems because they enable physical environments to be observed in a distributed and cost-effective manner. A typical WSN is composed of a large number of small, low-power sensor nodes deployed over a geographical region to collect data such as temperature, humidity, pressure, vibration, and pollution levels. These networks are commonly applied in areas such as environmental monitoring, smart agriculture, industrial automation, healthcare applications, structural health monitoring, and disaster management.

Despite their wide range of applications, WSNs operate under strict resource constraints. Sensor nodes rely on limited-capacity batteries and are frequently deployed in locations where battery replacement or routine maintenance is difficult or impractical. Along with energy limitations, sensor nodes possess limited computational capability, restricted memory, and depend on wireless communication links that may be unreliable. These constraints make energy efficiency and op-erational reliability key considerations in WSN deployments. During long-term operation, sensor nodes are exposed to harsh environmental conditions, including temperature varia-tions, humidity, dust, and electromagnetic interference. As a result, sensor nodes become vulnerable to different types of faults. Factors such as hardware degradation, sensor aging, calibration inaccuracies, software defects, and communication interference can contribute to abnormal behavior. Common fault manifestations include sudden spikes in sensor readings, sensors remaining fixed at constant values, gradual drift in measurements, packet losses caused by communication fail-ures, and abnormal battery depletion.

Faults in WSNs present a serious challenge because they directly influence the quality and reliability of the collected data. Incorrect sensor readings may lead to inaccurate analysis and poor decision-making at the application layer, which can have severe consequences in safety-critical applications such as healthcare monitoring, industrial control systems, and disaster response operations. Therefore, timely and accurate detection of sensor faults is essential to ensure dependable network performance.

Traditional fault detection approaches in WSNs typically depend on centralized processing, where sensor nodes periodically transmit raw data to a central sink node for analysis. Although centralized techniques can achieve high detection accuracy, they introduce significant communication overhead, resulting in rapid battery depletion and a reduction in network lifetime. Continuous data transmission also increases network congestion and packet collisions, further degrading overall system performance.

To address these limitations, recent studies have investigated advanced fault detection methods based on machine learning and data-driven models. While these approaches can improve detection performance, they generally require large training datasets, complex computations, and frequent model updates. Such requirements make machine learning-based solutions unsuitable for resource-constrained sensor nodes, particularly in large-scale and long-term deployments.

In response to these challenges, there is an increasing demand for lightweight, distributed, and energy-aware fault monitoring solutions that can operate efficiently within WSN constraints. A practical fault detection framework should reduce communication overhead, utilize simple local processing, and detect a wide range of fault types without relying on complex models or extensive training.

Motivated by these requirements, this paper proposes *AeroSense*, an energy-aware and anomaly-driven fault monitoring framework designed specifically for Wireless Sensor Networks. AeroSense allows each sensor node to independently observe its own behavior using simple statistical analysis over a sliding window of recent sensor readings. Instead of transmitting data continuously, communication is initiated only when abnormal behavior is detected. This anomaly-driven communication strategy effectively reduces unnecessary transmissions and conserves energy.

The proposed framework is capable of identifying multiple fault types, including spike faults, stuck-at faults, gradual sensor drift, communication failures, and battery drain anomalies. Through extensive simulation-based evaluation, AeroSense demonstrates reliable fault detection with low detection delay while maintaining high energy efficiency. These properties make AeroSense suitable for long-term and large-scale WSN deployments where energy conservation and reliability are of primary importance.

The remainder of this paper is organized as follows. Section II reviews related work on fault detection in Wireless Sensor Networks. Section III presents the system model and problem formulation. Section IV describes the proposed AeroSense algorithm in detail. Section V discusses the simulation setup and performance metrics. Section VI presents and analyzes the simulation results. Finally, Section VII concludes the paper and outlines directions for future research.

II. Related Work

Fault detection and monitoring in Wireless Sensor Networks (WSNs) has attracted continuous research attention over the past two decades. This interest is mainly driven by the limited resources of sensor nodes and the importance of maintaining reliable data collection. As a result, a wide range of techniques has been proposed to detect and isolate faulty nodes while attempting to reduce energy consumption and communication overhead.

Early studies in this area mainly focused on simple statistical and threshold-based fault detection techniques. These methods typically used predefined thresholds, moving averages, and variance-based analysis to identify abnormal sensor readings. Such approaches are computationally efficient and straightforward to implement on resource-constrained sensor nodes. However, fixed threshold mechanisms are highly sensi-tive to environmental variations and measurement noise, which often leads to false alarms or missed fault detections. In ad-dition, these techniques have limited capability in identifying gradual faults such as sensor drift or intermittent anomalies that emerge over time.

To overcome the limitations of basic statistical techniques, model-based and rule-based fault detection methods were later introduced. In these approaches, the observed behavior of sensor nodes is evaluated against predefined system models or expert-defined rules. Although model-based techniques canachieve high detection accuracy under controlled conditions, they depend heavily on prior knowledge of system behavior and fault characteristics. In practical deployments where oper-ating conditions are dynamic and unpredictable, maintaining accurate models becomes challenging, thereby reducing their effectiveness.

As sensor networks began generating larger volumes of data, researchers explored data-driven and machine learning-based fault detection methods. Techniques such as clustering, classification, neural networks, and support vector machines have been applied to identify anomalies and faulty behavior in WSNs. These methods generally offer improved detection accuracy and adaptability to complex fault patterns. How-ever, machine learning-based approaches introduce consid-erable computational complexity, increased memory usage, and higher communication overhead. Model training and up-dates often require centralized processing and frequent data exchange, making these solutions unsuitable for large-scale, energy-constrained sensor networks.

To reduce dependence on centralized processing, distributed fault detection approaches were proposed. In such schemes, sensor nodes cooperate with neighboring nodes to detect faults based on spatial and temporal correlations. Although distributed approaches reduce direct communication with the sink node, they still involve inter-node communication, which increases energy consumption and can limit scalability in dense network deployments.

Another significant research direction involves trust-based and reputation-based fault detection mechanisms. These meth-ods assign trust values to sensor nodes based on their historical behavior and consistency with

neighboring nodes. Nodes with lower trust values are identified as faulty or potentially mali-cious. While trust-based techniques improve robustness against faulty and compromised nodes, maintaining trust information requires continuous monitoring and information exchange, which introduces additional overhead.

Recent research has placed greater emphasis on energy-aware and event-driven fault detection strategies. Rather than relying on periodic data reporting, event-driven methods initi-ate communication only when abnormal behavior is detected. This approach significantly reduces unnecessary transmissions and helps conserve energy. Anomaly-based reporting has been shown to be particularly effective in extending network life-time while maintaining acceptable fault detection performance. Several studies have also examined fault detection in Inter-net of Things (IoT)-based sensor networks, where scalability and energy efficiency are key requirements. Lightweight statis-tical methods combined with adaptive threshold mechanisms have been proposed to balance detection accuracy and energy consumption. Nevertheless, many of these approaches still depend on centralized analysis or require complex parameter tuning.

In contrast to the above methods, the proposed AeroSense framework adopts a fully distributed and anomaly-driven fault monitoring strategy. AeroSense performs simple statistical analysis locally at each sensor node and triggers communi-cation only when an anomaly is detected, thereby reducing communication overhead and energy consumption. Unlike ma-chine learning-based approaches, AeroSense does not require training data or complex models. Compared to fixed-threshold techniques, the use of sliding-window statistics enables more effective detection of both abrupt and gradual faults.

Overall, existing studies highlight the inherent trade-off between detection accuracy, computational complexity, and energy efficiency in WSN fault detection. The AeroSense framework is designed to address this trade-off by offering a practical, lightweight, and energy-aware solution suitable for long-term and large-scale Wireless Sensor Network deploy-ments.

III. System Model and Problem Formulation

This section outlines the system assumptions, network ar-chitecture, sensor observation model, and energy consumption model used in the proposed AeroSense framework. Its purpose is to clearly define the operating environment and preciselyhen a sensor becomes faulty, its readings deviate from the nominal observation model. Depending on the nature of the fault, these deviations can appear as abrupt changes, persistent abnormal values, or gradual variations over time. The goal of the fault detection mechanism is to identify such deviations while remaining resilient to normal measurement noise.

C. Sliding Window Statistical Model

To account for temporal changes in sensor readings, each sensor node maintains a sliding window containing the most recent W observations. This sliding window strategy enables the node to compute local statistical measures in real time without the need to store long-term historical data. The mean value of the sensor readings within the window is computed as:

$$\mu_i(t) = \frac{1}{W} \sum_{k=t-W+1}^{t} x_i(k) \quad (2)$$

The associated stan dard deviation is then calculated as:

describe the fault monitoring problem addressed in this work.

A. Network Model

The Wireless Sensor Network examined in this study is composed of a group of low-power sensor nodes deployed across a monitoring area. Each sensor node includes four essential components: a sensing unit for acquiring data, a processing unit for local computations, a wireless transceiver for communication, and a limited battery source for power supply. After deployment, the sensor nodes are assumed to remain stationary and are randomly distributed within the sensing region.

Sensor nodes periodically collect environmental data such as temperature, humidity, or pressure at fixed sampling intervals. Owing to energy limitations, nodes do not transmit sensed data continuously to the sink node. Instead, communication is carried out selectively and is triggered only when abnormal behavior is detected. A single sink node is used to gather fault reports and perform higher-level analysis.

The wireless communication channel is considered unre-liable, and packet losses may occur as a result of interfer-ence, signal fading, or network congestion. Each sensor node functions independently and carries out local fault detection without requiring coordination or information exchange with neighboring nodes.

B. Sensor Observation Model

Let $x_i(t)$ represent the sensor reading produced by node i at time instant t. Under normal operating conditions, the sensor observation is modeled as:

$$x_i(t) = \mu_i + \epsilon_i(t) \quad (1)$$

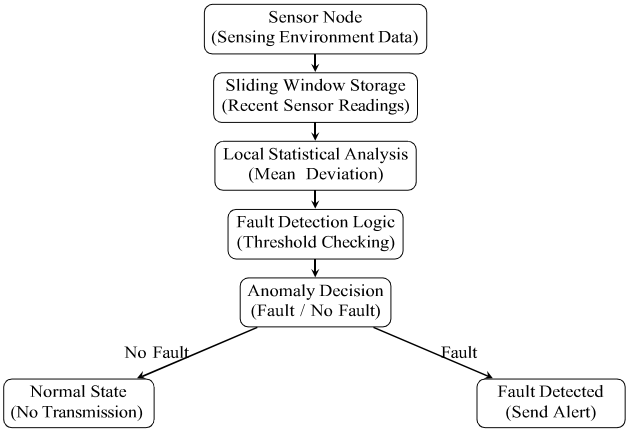
where μ_i denotes the nominal or expected value of the sensed parameter at node i, and $\epsilon_i(t)$ represents measurement noise. The noise component is assumed to have zero mean and bounded variance, accounting for random variations caused by environmental influences

and sensor imperfections. $\sigma(t) = \frac{1}{W} \sum_{k=t-W+1}^{t} (x(k) - \mu(t))^2$ (3)

Together, these statistical measures offer a concise descrip-tion of recent sensor behavior and serve as the foundation for performing local anomaly detection at each node.

D. Anomaly Detection Rule

An anomaly is identified when the difference between the current sensor reading and the estimated mean exceeds a predefined adaptive threshold. In particular, node i flags an anomaly at time t when:



$$|x_i(t) - \mu_i(t)| > \max(K\sigma_i(t), \vartheta) \quad (4)$$

where K represents a sensitivity factor that determines the effect of statistical variation, and ϑ denotes an absolute thresh-old used to limit false detections when variance is low. By combining these two threshold components, the detection rule is able to identify both sudden faults, such as spike and stuck-at conditions, as well as slowly developing faults such as sensor drift.

E. Energy Consumption Model

Energy efficiency plays a crucial role in the operation of Wireless Sensor Networks. The total energy consumed by node i during a sensing interval is modeled as:

$$E_i = E_{\text{sense}} + E_{\text{proc}} + E_{\text{tx}} + E_{\text{idle}} \quad (5)$$

where E_{sense} represents the energy required for sensing activities, E_{proc} denotes the energy consumed during local processing, E_{tx} corresponds to the energy spent on wireless data transmission, and E_{idle} accounts for the energy consumed while the node remains in an idle listening state.

In practical WSN deployments, wireless communication typically consumes much more energy than sensing or lo-cal computation. As a result, minimizing the number of transmissions becomes a key factor in extending network

lifetime. The anomaly-driven communication strategy used in AeroSense addresses this issue by restricting data transmission to instances where fault-related events are detected.

F. Problem Formulation

Based on the system model described above, the fault monitoring problem considered in this work can be stated as the design of a distributed fault detection mechanism that allows each sensor node to locally identify abnormal behavior in its sensed data while keeping energy consumption and communication overhead as low as possible.

The proposed solution is required to satisfy the following objectives:

- Accurately detect different types of faults, including spike faults, stuck-at conditions, sensor drift, communication failures, and battery drain anomalies.
- Limit false alarms caused by normal measurement noise and variations in the operating environment.
- Reduce communication overhead by avoiding periodic transmission of sensor data.
- Extend network lifetime under strict energy constraints.
- Maintain low computational and memory requirements suitable for resource-constrained sensor nodes.

The AeroSense framework is developed to meet these objectives by combining lightweight local statistical processing with an anomaly-driven communication strategy.

Fig. 1. Block diagram of the proposed System

IV. Proposed AeroSense Algorithm

This section describes the design and operating principle of the proposed AeroSense fault monitoring algorithm. The main goal of AeroSense is to allow each sensor node to independently detect abnormal behavior using lightweight local processing while reducing communication overhead and overall energy consumption.

A. Design Philosophy

The design of AeroSense is based on three key considerations: simplicity, energy efficiency, and robustness. Because sensor nodes operate with limited resources, the algorithm

avoids complex computations, model training procedures, and coordination between nodes. Instead, it depends on simple statistical analysis carried out locally at each sensor node.

A second important design aspect is the use of anomaly-driven communication. Rather than periodically transmitting sensor readings irrespective of network conditions, AeroSense initiates communication only when abnormal behavior is detected. This approach greatly reduces unnecessary data transmissions, conserves energy, and helps extend the overall network lifetime.

B. Algorithm Overview

Each sensor node continuously observes its own sensor readings over time. To capture short-term changes in sen-sor behavior, a sliding window of recent observations is maintained. At each sensing interval, the node updates its local statistical values and checks whether the current reading deviates noticeably from the expected pattern.

When this deviation exceeds a predefined adaptive thresh-old, the node identifies the event as an anomaly and generates a fault report. If no abnormal behavior is detected, the node remains silent and continues its regular sensing operation. This local decision-making approach ensures that sensor nodes operating normally do not expend energy on unnecessary communication.

C. Step-by-Step Algorithm Description

The AeroSense algorithm executes the following steps at each sensor node:

1) **Initialization:** Each sensor node sets up a sliding win-dow of size W to store recent sensor readings. Initial statistical values are calculated once a sufficient number of samples has been collected.
2) **Data Acquisition:** At every sensing interval t, the node collects a new sensor reading $x_i(t)$ from its sensing unit.
3) **Window Update:** The newly acquired reading is in-serted into the sliding window, and the oldest reading is removed to preserve the fixed window length.
4) **Statistical Computation:** Using the values stored in the sliding window, the node computes the mean $\mu_i(t)$ and the standard deviation $\sigma_i(t)$.
5) **Anomaly Evaluation:** The difference between the cur-rent reading and the estimated mean is compared with an adaptive threshold. If this condition is met, the reading is marked as abnormal.
6) **Fault Reporting:** When an anomaly is detected, the node sends a concise fault report to the sink node. If no abnormal behavior is identified, the node avoids communication to conserve energy.

D. Anomaly Detection Capability

Due to its statistical formulation, the AeroSense algorithm is capable of identifying a wide range of fault types. Sudden deviations in sensor readings lead to rapid anomaly detection, which allows spike faults and stuck-at faults to be detected quickly. Gradual changes in sensor behavior, such as drift

faults, are captured as the estimated mean evolves over time. Communication-related and battery-related faults are identified by observing abnormal transmission behavior and unusual energy depletion patterns.

E. Computational and Communication Efficiency

The computational overhead of AeroSense remains low because each sensor node performs only simple arithmetic operations on a fixed-size sliding window. The processing cost at each sensing interval is $O(W)$, and the memory requirement is restricted to storing W sensor readings.

In terms of communication, AeroSense reduces network traffic by following an event-driven reporting approach. During normal operation, sensor nodes remain silent and transmit data only when a fault is detected. This selective communication strategy results in significant energy savings when compared to conventional periodic reporting methods.

F. Algorithm Pseudocode

[H] AeroSense Local Fault Detection Algorithm [1] Initial-ize sliding window of size W each sensing instant t Sense data $x_i(t)$ Update sliding window Compute $\mu_i(t)$ and $\sigma_i(t)$
$|x_i(t) - \mu_i(t)| > \max(K\sigma_i(t), \vartheta)$ Mark anomaly Transmit fault report to sink

G. Discussion

By combining local statistical processing with anomaly-driven communication, AeroSense is able to balance fault detection performance with energy efficiency. The algorithm functions independently at each sensor node, requires only minimal computational and memory resources, and remains scalable as the network size increases. These features make AeroSense well suited for long-term Wireless Sensor Network deployments where reliability and energy conservation are essential.

V. Simulation Setup

To assess the effectiveness of the proposed AeroSense framework, a detailed simulation study is carried out using a discrete-time, software-based simulation environment. The simulation is configured to closely represent the operational behavior of a typical Wireless Sensor Network, while allowing controlled injection of different fault scenarios. This section outlines the network configuration, fault injection approach, energy modeling parameters, and the performance metrics used for evaluation.

A. Network Configuration

The simulated Wireless Sensor Network comprises 30 sen-sor nodes randomly deployed over a two-dimensional moni-toring area. After deployment, all sensor nodes are assumed to remain stationary and operate independently without mobility. A single sink node is positioned at a fixed location and is responsible for receiving fault reports from the sensor nodes. Each sensor node periodically samples an environmental parameter at uniform time intervals. The simulation is executed for a total of 1000 discrete time steps, which is sufficient adually shifting sensor readings away from their nominal values as time progresses. Communication faults are emulated by randomly dropping packets or introducing transmission delays, while battery drain faults are simulated by increasing the rate of energy depletion for selected sensor nodes.

Faults are injected into only a subset of sensor nodes to

ensure the coexistence of both faulty and normal nodes within the network. This setup enables evaluation of the algorithm's ability to correctly localize faulty nodes without producing false alarms from healthy nodes.

B. Energy Consumption Modeling

Energy consumption is explicitly modeled to evaluate the energy efficiency of the proposed framework. Each sensor node begins operation with an initial battery level of 100%. Energy is consumed during sensing operations, local data processing, wireless data transmission, and idle listening. Communication-related energy consumption is assumed to be significantly higher than that of sensing and computation, reflecting practical characteristics of sensor hardware.

The anomaly-driven communication strategy employed by AeroSense ensures that energy- intensive transmissions occur only when faults are detected. This allows the simulation to clearly demonstrate the energy savings achieved when compared to periodic reporting schemes.

C. Parameter Settings

The sliding window size is configured as $W = 10$, providing a balance between detection responsiveness and tolerance to noise. The sensitivity parameter K is set to 3, enabling effective detection of abnormal deviations while limiting false alarms. The absolute threshold ϑ is chosen based on the expected range of sensor readings. These parameters are kept constant throughout the simulation to ensure consistent evaluation.

D. Performance Metrics

The performance of AeroSense is assessed using several key metrics. Detection accuracy indicates the ability of the frame-work to correctly identify faulty behavior. Detection delay is defined as the time difference between the occurrence of a

fault and its detection by the algorithm. Energy consumption is measured as the total energy consumed by each sensor node over the simulation duration. Communication overhead is evaluated based on the number of transmissions generated during the simulation.

Together, these metrics provide a comprehensive evaluation of the trade-off between fault detection performance and energy efficiency.

E. Baseline Comparison

For comparison, AeroSense is evaluated against a conventional periodic reporting approach in which sensor nodes transmit data at every sensing interval, regardless of network conditions. This baseline is used to highlight the advantages of anomaly-driven communication in reducing unnecessary transmissions and conserving energy.

The simulation results obtained using the above configuration are discussed in the following section to demonstrate the effectiveness of the proposed AeroSense framework under various fault conditions.

VI. Results and Discussion

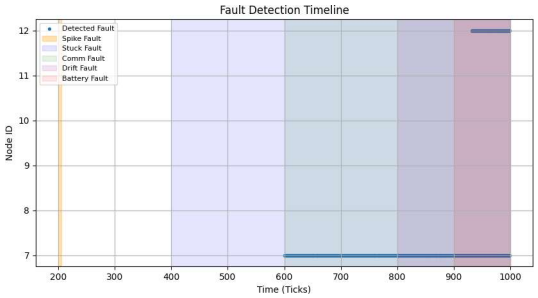


Fig. 4. Fault detection timeline across sensor nodes.

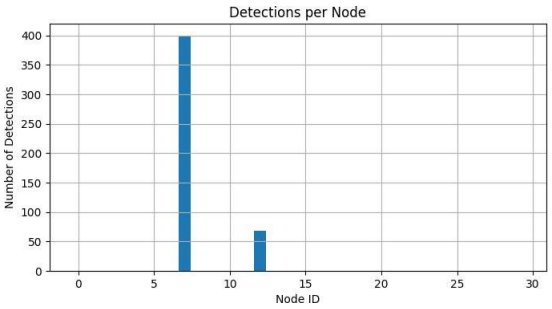
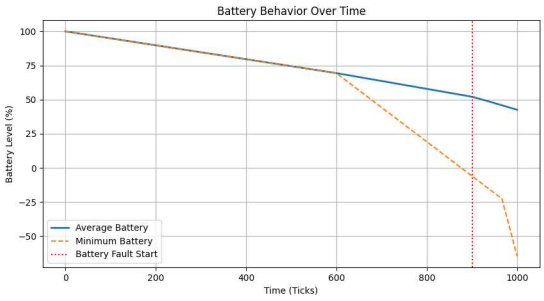


Fig. 5. Number of fault detections per node.



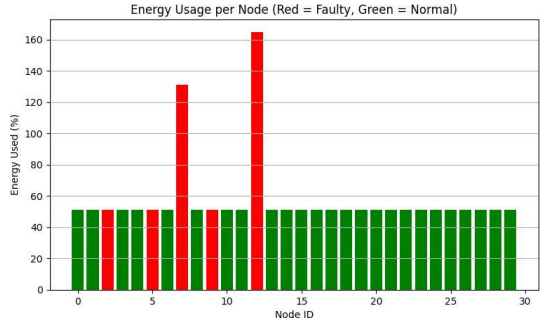


Fig. 2. Battery level variation over time showing abnormal battery drain.

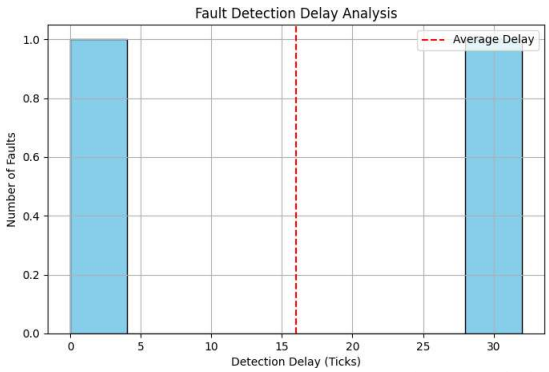


Fig. 3. Fault detection delay distribution across fault types.

Fig. 6. Energy consumption per node (faulty vs normal).

A. Figure-wise Discussion

Figures 2–6 illustrate the behavior of the network under different fault conditions when using the AeroSense frame-work. The results show that faults are detected in a timely manner while maintaining efficient energy usage. Since com-munication is triggered only by anomalous behavior, additional energy consumption is largely confined to faulty nodes, which contributes to an improvement in overall network lifetime.

B. Results Summary

Overall, the results indicate that AeroSense provides reliable fault detection with low detection delay and reduced com-munication overhead when compared to continuous reporting schemes. This confirms the effectiveness of the anomaly-driven communication strategy in balancing detection perfor-mance and energy efficiency.

VII. Comparative Analysis

When compared with traditional periodic reporting schemes, AeroSense reduces communication overhead by restricting data transmission to anomaly events rather than continuous reporting. In contrast, centralized fault detection methods rely on constant data transmission, which results in faster battery depletion and a shorter overall network lifetime.

In comparison with machine learning-based approaches, AeroSense does not depend on training datasets, frequent model updates, or complex computational processes. This makes it more appropriate for resource-constrained sen-sor nodes. The use of lightweight statistical processing in AeroSense supports scalability and simplifies deployment while still providing reliable fault detection performance.

VIII. Limitations

The evaluation is carried out under the assumption of static network conditions with predefined threshold values. Dynamic network environments and the use of adaptive threshold tuning are not addressed in this study.

IX. Conclusion and Future Work

This paper presented AeroSense, an energy-aware and anomaly-driven fault monitoring framework designed for Wireless Sensor Networks operating under strict resource constraints. The proposed approach allows each sensor node to independently observe its own behavior using lightweight sta-tistical analysis, removing the need for centralized processing or complex model training. By employing an anomaly-driven communication strategy, AeroSense reduces unnecessary data transmissions, thereby conserving energy and extending over-all network lifetime.

Simulation-based evaluation demonstrates that AeroSense is capable of accurately detecting a wide range of fault types, including spike faults, stuck-at faults, gradual sensor drift, communication failures, and abnormal battery drain. The results indicate that most faults are detected within a short time window, enabling timely response while maintain-ing low computational and communication overhead. Energy consumption analysis further shows that healthy nodes avoid excessive transmissions, leading to improved overall energy efficiency when compared to conventional periodic reporting approaches.

A key strength of the AeroSense framework is its simplicity and practical applicability. The algorithm requires minimal memory and processing resources, making it suitable for deployment on low-power sensor hardware. Unlike machine learning-based solutions, AeroSense does not depend on train-ing data or complex parameter tuning, which simplifies im-plementation and

supports scalability in large-scale network deployments.

Despite its effectiveness, the current implementation of AeroSense has certain limitations. The evaluation is performed under the assumption of static network conditions and fixed threshold parameters, which may not fully reflect the behavior of real-world deployments. In highly dynamic environmentschanges in network topology, communication conditions, and environmental factors may influence fault detection perfor-mance.

Future work will focus on improving the adaptability and robustness of the AeroSense framework. One potential direc-tion involves developing adaptive threshold mechanisms that automatically adjust sensitivity parameters based on observed network behavior. Incorporating fault severity estimation may further enhance decision-making by enabling prioritization of critical faults. Extending the framework to support mobile sensor nodes and dynamic network conditions is another direction that can broaden its applicability.

An additional future direction involves implementing and validating AeroSense on physical sensor platforms such as Arduino, ESP32, or industrial IoT nodes. Experimental de-ployment in real environments can provide valuable insights into practical challenges, including hardware variability and environmental noise. Incorporating lightweight security mech-anisms to distinguish between faulty behavior and malicious activity also represents a potential extension.

Overall, AeroSense offers a practical and energy-efficient solution for fault monitoring in Wireless Sensor Networks. Its lightweight design, low energy overhead, and reliable detection performance make it a strong candidate for long-term monitoring applications and future IoT-based sensing systems.

pp. 1346–1357.

[13] Y. Zhang, N. Meratnia, and P. Havinga, "Outlier detection techniques for wireless sensor networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 12, no. 2, pp. 159–170, Second Quarter 2010.

[14] A. Ahmed and K. Tepe, "Trust-based fault detection in wireless sensor networks," *Frontiers of Computer Science*, vol. 10, no. 4, pp. 728–741, Aug. 2016.

[15] S. Misra, M. Reisslein, and G. Xue, "A survey of energy hole problem in wireless sensor networks," *IEEE Systems Journal*, vol. 10, no. 2, pp. 681–693, Jun. 2016.

[16] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, "System architecture directions for networked sensors," in *Proc. ASPLOS*, Cambridge, MA, USA, 2000, pp. 93–104.

[17] A. Sharif, M. Raza, and M. Shafiq, "Energy-aware fault detection framework for IoT-based sensor networks," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9781–9792, Jun. 2021.

[18] Z. He, X. Xu, and S. Deng, "kNN-based fault detection in wireless sensor networks," *Computer Communications*, vol. 31, no. 10, pp. 2588–2596, Jun. 2008.

[19] T. Clouqueur, K. K. Saluja, and P. Ramanathan, "Fault tolerance in collaborative sensor networks for target detection," in *Proc. IEEE INFOCOM*, Anchorage, AK, USA, 2001, pp. 143–152.

[20] J. A. Stankovic, "Wireless sensor networks," *Computer*, vol. 41, no. 10, pp. 92–95, Oct. 2008.

APPENDIX A: SIMULATION PARAMETERS

The simulation is configured with 30 sensor nodes, a sliding window size of $W = 10$, a sensitivity parameter of $K = 3$, and an initial battery level set to 100%.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, Aug. 2002.

[2] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292–2330, Aug. 2008.

[3] K. Ro¨mer and F. Mattern, "The design space of wireless sensor net-works," *IEEE Wireless Communications*, vol. 11, no. 6, pp. 54–61, Dec. 2004.

[4] X. Luo, M. Dong, and Y. Huang, "On distributed fault detection in wireless sensor networks," *IEEE Transactions on Computers*, vol. 55, no. 1, pp. 58–70, Jan. 2006.

[5] N. Ramanathan, K. Chang, R. Kapur, L. Girod, E. Kohler, and D. Estrin, "Sympathy for the sensor network debugger," in *Proc. ACM SenSys*, San Diego, CA, USA, 2005, pp. 255–268.

[6] P. Jiang, "A new method for node fault detection in wireless sensor networks," *Sensors*, vol. 9, no. 2, pp. 1282–1294, Feb. 2009.

[7] S. Rajasegarar, C. Leckie, M. Palaniswami, and J. C. Bezdek, "Dis-tributed anomaly detection in wireless sensor networks," *IEEE Wireless Communications*, vol. 15, no. 4, pp. 34–40, Aug. 2008.

[8] C. C. Aggarwal, *Outlier Analysis*, 2nd ed., Cham, Switzerland: Springer, 2017.

[9] J. Chen, S. Kher, and A. K. Somani, "Distributed fault detection of wireless sensor networks," in *Proc. ACM DiWANS*, Los Angeles, CA, USA, 2006, pp. 65–72.

[10] H. Karl and A. Willig, *Protocols and Architectures for Wireless Sensor Networks*, New York, NY, USA: Wiley, 2005.

[11] L. Ruiz-Garcia, L. Lunadei, P. Barreiro, and J. I. Robla, "A review of wireless sensor technologies and applications in agriculture," *Sensors*, vol. 9, no. 6, pp. 4728–4750, Jun. 2009.

[12] M. Ding, D. Chen, K. Xing, and X. Cheng, "Localized fault detection in sensor networks," in *Proc. IEEE INFOCOM*, Miami, FL, USA, 2005,