SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V13I7P116

Volume 13 Issue 7, 231-240, July 2026

Original Article

Reliable Data Communication using Bayes Optimal Classifier in MWSN

S. Archana[1], V. Jayapradha[2]

[1,2]*Department of Electronics and Communication Engineering, Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya, Kanchipuram, Tamil Nadu, India.*

[1]*Corresponding Author : archana.phd@yahoo.com*

Received: 16 May 2026 Revised: 11 June 2026 Accepted: 01 July 2026 Published: 29 July 2026

Abstract *- Mobile Wireless Sensor Networks (MWSNs) are extensively used in mission-critical and dynamic applications such as intelligent transportation systems, disaster management, and environmental monitoring. Though abnormal sensor node behaviour, such as malicious or selfish sensor nodes, may extremely degrade Quality of Service (QoS) in MWSNs due to sensor node mobility, energy limitations, and unpredictable climatic conditions. To enhance network reliability and QoS in MWSNs, this work introduces a Reliable Data Communication using Bayes Optimal Classifier (RCBC) in MWSN. The proposed approach uses multidimensional characteristics, including residual energy level, packet received ratio, selfishness rate, and delay, to probabilistically describe sensor node behaviour. The RCBC approach uses the bayes optimum classifier isolates normal and abnormal sensor nodes under ambiguity. By classifying recognized abnormal sensor nodes from data forwarding and routing procedures, throughput and residual energy are improved. Simulation findings expose that the proposed RCBC technique outperforms machine learning classifiers in terms of abnormal node detection accuracy, false positive and false negative ratio, making it ideal for dynamic MWSN scenarios.*

Keywords *- Mobile Wireless Sensor Networks, Abnormal node detection, Bayes Optimal Classifier, Quality of Service, Network Reliability.*

1. Introduction

The MWSNs are extensively used in mission-critical applications such as industrial automation, smart agriculture, healthcare, and environmental monitoring [1]. Sensor nodes are very susceptible to anomalous behaviours brought on by malicious assaults, node malfunctions, and energy depletion because of their open wireless channel, unsupervised operation, low energy resources, and poor computing capabilities. By increasing packet loss, latency, and energy consumption, as well as decreasing overall QoS and network longevity, the presence of abnormal nodes significantly impairs network performance [2].

Guaranteeing reliable data communication in MWSNs is challenging since mobile sensor nodes are susceptible to failures, energy diminution, environmental instabilities, and malicious attacks that can create abnormal behavior and cooperation data integrity. Several existing approaches have been introduced to enhance communication malicious sensor nodes. Conventional approaches mostly rely on threshold-based methods, trust management schemes, clustering algorithms, and machine learning approaches. However, many of these approaches hurt from restrictions such as high computational complexity, minimized detection accuracy under dynamic network situations, raised communication overhead, and insufficient handling of doubt in sensor observations. Therefore, abnormal sensor nodes may remain unobserved, leading to unreliable data transmission and degraded network performance. Hence, a significant research gap happens in evolving a lightweight and precise classification approach that can efficiently classify abnormal sensor nodes whereas handling reliable communication in resource-constrained MWSNs. Existing approaches have not adequately discovered the application of probabilistic decision-making techniques that can achieve uncertainty and recover classification accuracy with lesser computational cost.

To address this gap, this approach introduces a Reliable Data Communication approach utilizing a Bayes Optimal Classifier to separate abnormal sensor nodes in MWSNs. The proposed approach influences Bayesian probabilistic categorization to differentiate normal and abnormal node behavior based on detected network parameters. By precisely classifying and isolating abnormal nodes, the approaches improve data reliability, minimizes communication disruptions, and enhance overall network performance. Experimental outcomes illustrate that the proposed approach

reaches superior detection accuracy and communication reliability compared with conventional approaches, making it an appropriate solution for secure and efficient MWSN environments. The novelty of this work can be concise as follows:

1.1. Bayesian-Based Abnormal Node Isolation

The proposed approach applies a Bayes Optimal Classifier to classify and separate abnormal sensor nodes that have established limited attention in MWSN reliability studies.

1.2. Enhancing Reliable Data Communication

Rather than concentrating merely on anomaly detection, the proposed approach participates in abnormal node separation with communication reliability enhancement, ensuring that only normal nodes contribute to data transmission.

1.3. Low Computational Complexity

Compared with complex machine learning and deep learning approaches, the Bayes Optimal Classifier provides a lightweight probabilistic solution appropriate for resource-constrained MWSNs.

2. Related Works

Several approaches have been proposed for abnormal node detection in MWSNs. However, this approach splits up four divisions, such as Threshold-based approaches, Statistical model-based approaches, Machine learning-based approaches and Reinforcement learning-based approaches. These models are specified below.

2.1. Threshold-based Approaches

These approaches monitor parameters such as energy or packet loss, but they lack adaptability to dynamic conditions. Anomaly detection is a broadly utilized technique in MWSNs to classify anomaly events. Energy efficiency when detecting anomalies in data by applying compression of measurement data and minimizing operating time lacking compromising measurement resolution. This efficiently minimizes energy utilization. Furthermore, the deep sequential learning algorithm removes the requisite for labelled data and time-expending [3]. Abnormal nodes are detected via the Convolutional Neural Network (CNN) method [4].

2.2. Statistical Model-Based Approaches

The following reasons make statistical methods for detecting abnormal nodes: Low computational complexity is required, avoid depending on large, labelled datasets, appropriate for sensor nodes with limited resources and allow distribution and online detection. By quantifying statistical differences from typical node behaviour, these methods detect abnormalities. The Statistical Anomaly Detection Framework offers statistical frameworks that use probabilistic models to simulate typical sensor behaviour. This allows for the identification of statistically significant abnormalities in network behaviour, which may be signs of assaults, such as hostile node activity. To identify both environmental and network abnormalities, these models consider the temporal and spatial dynamics of sensors [5]. To identify anomalies like jamming and packet delay disturbances, statistical process control approaches such as the Exponential Weighted Moving Average (EWMA) have been used. The main concept is that harmful activity modifies statistical characteristics that may be monitored to trigger alerts [6]. The correlation theory-based malicious-node detection approach guards against fault data injection attacks [7].

2.3. Machine Learning-Based Approaches

Traditional security measures are often inadequate in MWSNs because of their dynamic topology, energy constraints, and ignorance of previous attacks. By facilitating adaptive, data-driven, and intelligent intrusion detection, ML-based malicious node detection has become a viable remedy. ML approaches use network data to detect malicious activity and learn patterns of normal and abnormal node behavior [8]. Most abnormal node detection methods now in use depend on Machine Learning (ML) classifiers [9] like Support Vector Machine (SVM) [10], K-Nearest Neighbors (KNN) [11], and Artificial Neural Network (ANN) [12]. Dependency on manually defined thresholds, sensitivity to noise and dynamic network conditions, high computational overhead, the need for large, labelled datasets, and suboptimal decision boundaries that fall short of minimizing overall classification error in probabilistic environments are just a few of the drawbacks of these methods.

Conventional detection techniques depend on heuristic rules or set thresholds, which are ineffective in dynamic and unpredictable environments. Although ML techniques increase flexibility, they often come with significant computational overhead and extensive training datasets [13]—malicious Node Detection Using SVM and Blockchain (MDSB) approach established on behavioral and node features. During the training module, usual and malicious node behaviors are applied to construct an optimal hyperplane, which divorces legitimate nodes from attackers. Once trained, the SVM algorithm categorizes nodes, and distinguished malicious nodes are isolated from routing and data collection processes. However, it raises the overhead, delay, energy depletion, and lacks scalability [14].

Furthermore, a lot of approaches fail to explicitly account for node behaviour uncertainty, which increases false positives and false negatives, particularly in highly dynamic and diverse MWSN settings [15]. To effectively model uncertainty, optimally fuse multiple behavioural parameters and minimise misclassification risk under

resource constraints, a robust and probabilistically optimal abnormal node detection framework is therefore desperately needed. Because Random Forest (RF) and similar ensembles can handle complicated feature interactions and nonlinear decision limits, they have shown good performance. RF classifiers have been tuned for better intrusion detection performance via metaheuristic optimization [16]. ML models enhance accuracy but need widespread training and computational resources.

2.4. Reinforcement Learning-Based Approaches

Traditional Compared to routing applications, RL for malicious node identification in MWSN is still in its infancy, but some fields demonstrate its potential: adapts over time but introduces convergence delays. Generative Adversarial Network (GAN) and Actor-Critic reinforcement learning are used in a Reinforcement Learning (RL) based intrusion detection system to identify malicious activity or intrusions automatically. By simulating assault patterns, the GAN aids the RL agent in learning the best course of action in a changing environment, hence increasing detection accuracy. This approach improves accuracy more than traditional static IDS models [17]. By monitoring node activity patterns over time, research on using RL for Wireless Sensor Network (WSN) intrusion detection demonstrates that RL agents can dynamically adapt to network behaviour and learn to differentiate between benign and malicious nodes. Through constant policy updates based on observed incentives for accurate/inaccurate classifications, RL enhances detection performance [18]—analysis of Adaptive Behaviour Using RL. The ability of RL to provide adaptive detection techniques that can react to changing harmful tactics (such as grey-hole or random dropping assaults) has been highlighted in recent research. RL agents adapt their rules in reaction to malicious efforts to avoid detection and changes in network state, rather than depending on predefined decision limits.

Contrasting static thresholding, RL is capable of self-reliantly adjusting its judgment thresholds and recording temporal node behaviour (such as loss rates and energy irregularities [19]. Adaptive RL with Dij-Huff Method (ARDM) using Dijkstra's algorithm discovers the sensor nodes with the highest energy and the best possible distance route. In addition, the Huffman coding calculates the binary hop count that provides each hop security. However, this mechanism does not detect the abnormal nodes efficiently; due to node mobility, the performance decreases [20]. Table 1 describes the summary of the literature survey.

Table 1. Summary of literature survey

Approaches	Key contributions	Limitations
Deep Sequential Learning [3]	Improved anomaly detection	High computational requirements
Convolutional Neural Network [4]	Enhanced an abnormal node detection	CNN models request important training data and energy
Correlation-based Detection [7]	Efficiently recognized malicious nodes	Performance may decrease in an extremely dynamic network
SVM, and a KNN-based abnormal state warning method [11]	Enhanced network security observing via effective anomaly categorization.	Mainly concentrated on network security instead of abnormal sensor node isolation.
Hybrid ANN with Grasshopper Optimization [12]	Improved anomaly detection accuracy	Computational complexity is relatively high
Heuristic-assisted Deep Learning [13]	Reached secure routing and malicious node detection	Deep learning needs widespread training and resources
SVM with Blockchain-based Secure Storage [14]	Enhanced malicious node detection and secured sensor data storage	Blockchain execution creates storage and communication overhead
Uncertainty propagation in node classification [15]	Conveyed uncertainty handling during node classification	Does not explicitly target abnormal node isolation
Tabu Search Optimized RF [16]	Enhanced intrusion detection accuracy via optimized learning	Raised computational complexity and overhead
Blockchain-based Secure Routing and [18]	Improved routing security and trust establishment	Blockchain increases energy consumption and delays
RL Approach [19]	Improved intrusion detection performance	Training convergence and scalability remain challenging
Adaptive RL with Dij-Huff Routing [20]	Secured optimal routing	It concentrated on routing optimization rather than abnormal node categorization.

3. Proposed System

MWSN contains a set of mobile sensor nodes arranged arbitrarily over an observing region. Sensor nodes reveal dynamic topography because of mobility and are controlled by inadequate resources like energy, bandwidth, and memory. Every sensor node can sense, collect data, and data transmission. A Base Station (BS) collects data from mobile sensor nodes either directly or via multi-hop routing. Figure 1 demonstrates an example diagram of the RCBC approach.

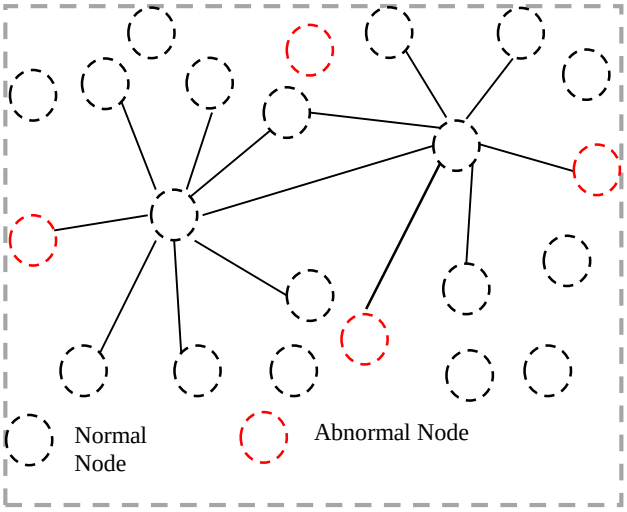

Fig. 1 Structure of the RCBC approach

It contains normal mobile sensor nodes and abnormal mobile sensor nodes. Abnormal nodes may act selfishly or maliciously. Selfish nodes act selfishly to save their resources, and malicious nodes do severe action for destroying the MWSN. Neighbor table is updated periodically based on mobile node characters such as mobile sensor node Selfishness Rate (SR), Packet Received Ratio (PRR), Packet Delay (PD), and levels of Residual Energy (RE). The fraction of mobile sensor nodes that act selfishly by rejecting relaying packets to others to preserve energy is known as the SR. PDR evaluates the consistency of the network by computing the ratio of the whole number of data packets effectively obtained at the BS to the whole number of packets created by the sensor nodes. RE represents the remaining battery energy of a mobile sensor node after detecting, processing, communicating, and obtaining operations. Mobile sensor nodes with greater RE are more stable and cooperative, where low-energy nodes tend to behave selfishly and induce route failures. RE is classified into multiple levels to help the bayes optimal classifier in identifying reliable forwarding nodes. PD represents the average time taken for a data packet to move from the sensor nodes to the BS, containing all processing, transmission, queuing, broadcast, and retransmission delays. Enhanced delay aims to mitigate misrouting, intended congestion, and buffering attacks. Lesser delay represents quicker and more efficient data transmission in MWSN.

A mobile sensor node is measured abnormally if its behavior differs considerably from normal functional patterns because of malicious intent, leading to QoS reduction. Abnormal nodes avoid data forwarding and increase the overhead and delay. The proposed system utilizes the bayes optimal classifier algorithm, which computes every mobile sensor node's Abnormality Score (ABS). The ABS value is greater than the threshold that mobile sensor nodes are separated from the route. The objective of the proposed system is to accurately categorize abnormal sensor nodes from the network, reduce categorization cost, and improve QoS metrics, for example, throughput, categorization accuracy and residual energy. Figure 2 illustrates the component diagram of the RCBC approach.

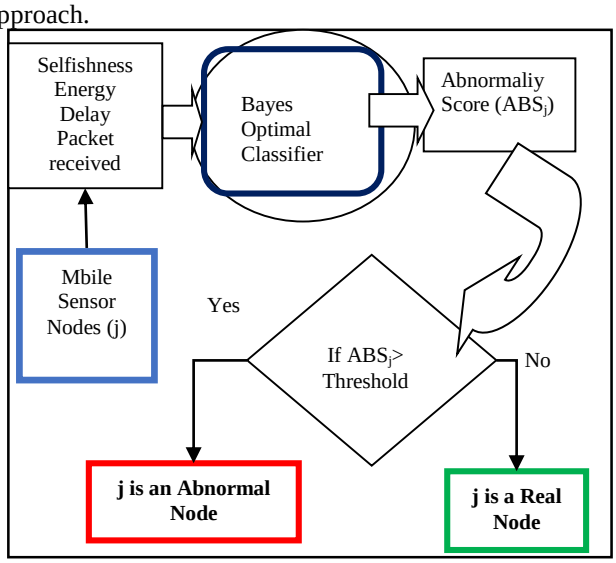

Fig. 2 Component diagram of the RCBC approach

3.1. Bayes Optimal Classifier Algorithm

The node is categorized into the class with the greatest posterior probability after the conditional probability of each class given these attributes is calculated using the Bayes Optimal Classifier. This probabilistic decision procedure offers the best theoretical benchmark for abnormal node identification while minimizing the classification error. The bayes optimal classifier can effectively differentiate between cooperative and misbehaving nodes by using SR, PRR, PD, and residual energy as input variables. In MWSN, each sensor node j is represented by a feature vector as specified in Equation (1).

$$X_j = RE, PRR, PD, SR \quad (1)$$

Here, SR indicates the Selfishness rate, RE denotes the level of remaining energy, PRR refers to the ratio of packets received, and PD denotes the delay of the packet. Every node goes to one of two categories (CA), and it is specified in Equation (2). Here, C_{RN} represents the real sensor node category, and C_{AB} indicates an abnormal sensor node category.

$$CA \in \{C_{RN}(Real)|C_{AB}(Abnormal)\} \quad (2)$$

3.1.1. Bayesian Decision Theory

By calculating the probability that a sample falls into a certain class, Bayesian decision theory is often used to categorize data into several categories. The sample is usually assigned to the class with the highest posterior probability by the decision procedure. When the data's probability distributions are known, this method yields a mathematically optimum solution. The bayes optimal classifier allots a node to the class with the highest posterior possibility is specified in Equation (3).

$$CA = \arg \max_{CA \in \{CA_{RN}, CA_{AB}\}} P(CA|X) \quad (3)$$

Where, $P(CA|X) = \frac{P(X|CA)P(CA)}{P(X)}$

Meanwhile $P(X)$ refers to a constant for all categories. Hence,

$$CA = \arg \max_{C} [P(X|CA)P(C)] \quad (4)$$

3.1.2. Probability Modeling of Sensor Node Characters

An essential first step in identifying anomalous nodes in MWSNs is probability modelling of sensor node characteristics. This method treats each sensor node's behavioral characteristics, including SR, PRR, PD, and RE level, as random variables whose statistical patterns may be examined. Assuming uncertain independence of characteristics is usually assumed for MWSN efficiency.

$$P(X|CA) = P(SR|CA)P(RE|CA)$$

$$P(PD|CA)P(PDR|CA) \quad (5)$$

$$P(x_j|CA) = \frac{1}{\sqrt{2\pi\sigma_{CA,j}^2}} exp\left(-\frac{(x_j - \mu_{Cj})^2}{2\sigma_{CA,j}^2}\right) \quad (6)$$

Here, μ_{Cj}, $\sigma_{CA,j}^2$: mean and variance of characteristic j for category CA

3.1.3. Bayes Optimal Decision Rule

A key idea in probabilistic classification, the bayes optimal decision rule determines the best course of action based on observed data. This rule assigns a data instance to the class with the greatest posterior probability after considering the likelihood of the observable characteristics as well as previous probabilities. When the actual probability distributions of the data are known, this method is seen to be the theoretically best choice as it reduces the probability of classification mistakes. The bayes optimal classifier a lot of mobile sensor nodes are categorized as abnormal nodes.

$$P(CA_{AB}|X) > P(CA_{RN}|X) \quad (7)$$

The score of an abnormality (ABS) is defined as

$$ABS_j = \frac{P(C_{AB}|x_j)}{P(C_{RN}|x_j)} \quad (8)$$

The proposed system reduces the probable categorization risk, confirming optimal detection under insecurity. The proposed system improves energy efficiency, is appropriate for resource-constrained environments, and has less computational complexity. Table 2 discusses the categorization of abnormal node behavior.

Table 2. Categorize abnormal node behavior

Characteristics	Real Node	Abnormal Node
SR	Low	High
RE	Moderate-high	Abnormally Low
PDR	High	Low
PD	Low	High

Algorithm: Bayes Optimal Abnormal Node Detection Steps

1. Initialize MWSN and arrange mobile sensor nodes
2. Gather node characters periodically
3. Update the neighbor table periodically
4. Apply the Bayes optimal decision rule
5. Categorize abnormal mobile sensor nodes using the abnormality score
6. Separate abnormal nodes from routing
7. Update QoS-aware routing paths

Repeat the categorization process.

4. Results and Discussion

The proposed mechanism is performed by applying NS-2.35. The system utilizes a network topology of 500 × 850-meter square. Here, 100 mobile sensor nodes are arranged, and the mobile sensor nodes are moving randomly. The efficiency and robustness of the RCBC approach are assessed using the University of New South Wales - Network Behavior 2015 (UNSW-NB15) dataset. This methodology integrates the advantages of Navy Bayes for classification, thus improving security and malicious node detection accuracy of MWSN. The throughput, packet lost, residual energy and delay value parameters measure the efficiency of the RCBC approach. Simulation results demonstrate that the proposed RCBC reaches greater detection accuracy, throughput, minimizes false positive rate, and network delay.

4.1. Throughput Ratio

A key performance parameter for assessing how well MWSN transfers data from sensor nodes to the receiver in the face of mobility and potential abnormal behaviour is the

Throughput Ratio. The percentage of correctly received data packets reaching the receiver in relation to the total number of packets produced by the sensor nodes is known as the throughput ratio. Figure 3 demonstrates the throughput of ARDM, MDSB and RCBC approaches with sensor node count.

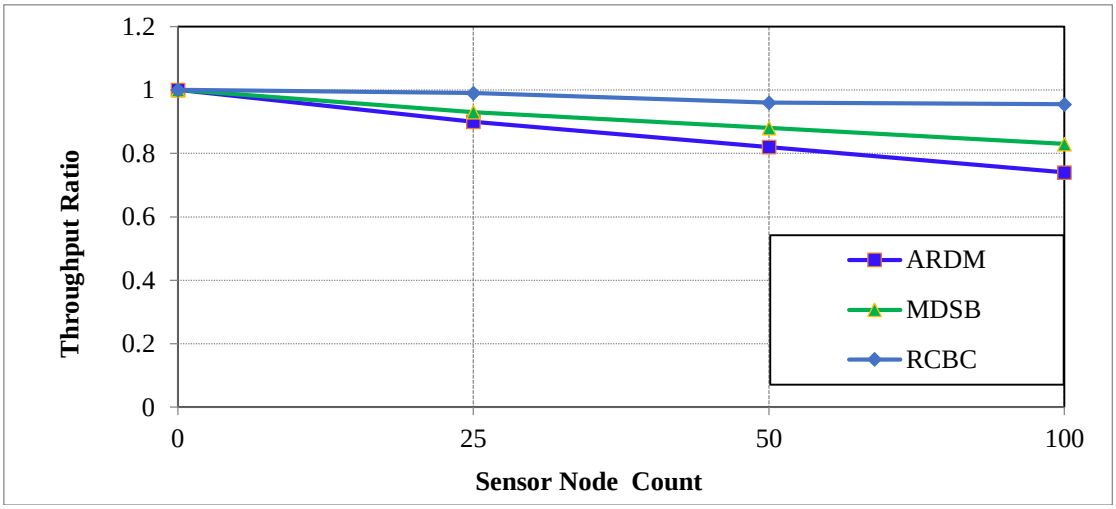

Fig. 3 Throughput of ARDM, MDSB and RCBC approaches with sensor node count

Usually, undetected abnormal nodes minimize throughput by losing or misclassifying packets. From the simulation results, the existing ARDM and MDSB approaches have lesser throughput ratio since applying the SVM algorithm performs better in a static sensor node topology. However, the proposed RCBC approach utilizes the Bayes optimal algorithm that detects abnormal nodes efficiently based on node behavior. Hence, the RCBC approach reaches the 0.955 throughput ratio than the other approaches.

4.2. Delay

Detection delay is definite as the time passed between the beginning of abnormal behavior and its efficient detection by the system. In MWSN, extreme network delay can happen due to inefficient routing, congestion, and the presence of abnormal nodes that purposefully delay packet forwarding. Figure 4 displays the delay of ARDM, MDSB and RCBC approaches with sensor node count.

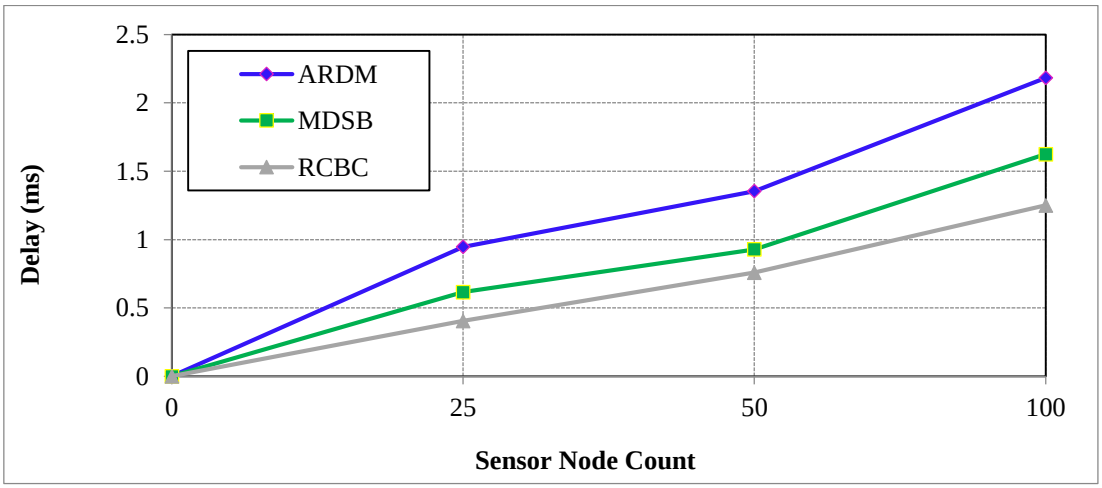

Fig. 4 Delay of ARDM, MDSB and RCBC approaches with sensor node count

The average delay of ARDM and MDSB approaches are very high when raises the sensor node count. However, the proposed RCBC approach increases the average delay value since it applies the Bayes optimal errors, which can adapt dynamically, thus increasing abnormal nodes detection efficiently. This confirms that packets are transmitted via reliable sensor nodes with efficient communication behavior. Hence, needless waiting time, losing packet, and retransmissions are minimized, which eventually decreases the network delay and enhances the quality of data transmission. The proposed RCBC approach has a 1.25 ms delay. This is the lowest value delay compared to the other approaches.

4.3. Residual Energy

Residual energy is a significant factor utilized in abnormal node detection while applying the bayes optimal classifier. The remaining battery energy of a sensor node after communication, sensing, and processing activities is known as residual energy, and it is a key performance parameter in MWSN. Normal nodes usually continue a balanced energy utilization pattern while sharing in packet forwarding operations. In contrast, abnormal sensor nodes may indicate improper energy behavior or abnormally high residual energy since they evade forwarding packets due to abnormal or inefficient operations. Figure 5 describes Residual Energy of ARDM, MDSB and RCBC approaches with sensor node count.

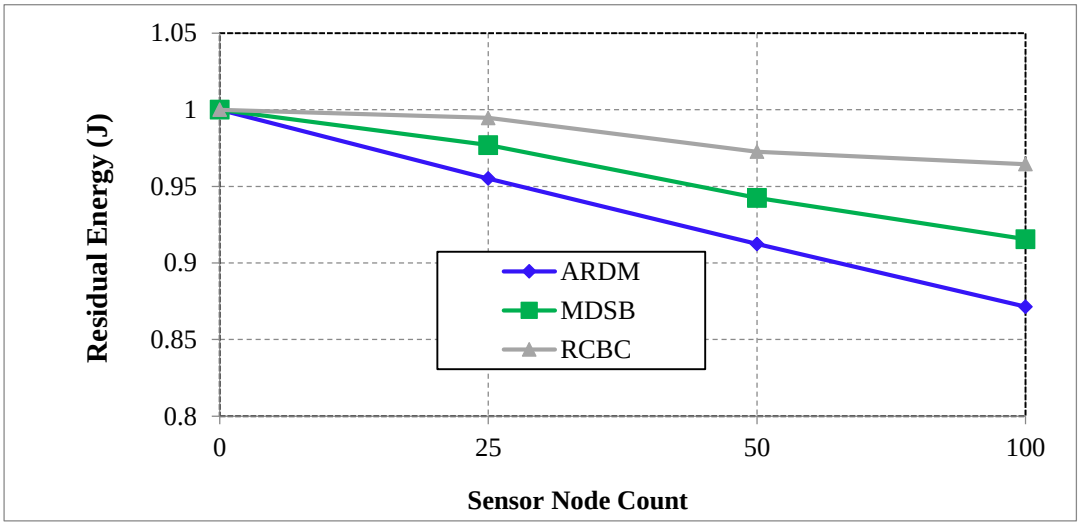

Fig. 5 Residual energy of ARDM, MDSB and RCBC approaches with sensor node count

The existing ARDM and MDSB approaches have low residual energy, which leads to network separating. The proposed system RCBC has lesser computation and energy depletion since the bayes optimal classifier executes abnormal sensor nodes detection by applying parameters like residual energy, packet delay, selfishness and PDR. By integrating residual energy into the classification process, the RCBC approach can efficiently differentiate cooperative nodes from malfunctioning ones, enabling 0.9644 joule energy-efficient routing decisions and enhancing the network lifetime.

4.4. Abnormal Node Detection Ratio

One important performance statistic for assessing how well a detection algorithm finds abnormal nodes in an MWSN is the abnormal node detection ratio. A higher abnormal node detection ratio specifies better detection capacity and enhanced network security. Figure 6 illustrates the abnormal node detection Ratio of ARDM, MDSB and RCBC approaches with sensor node count.

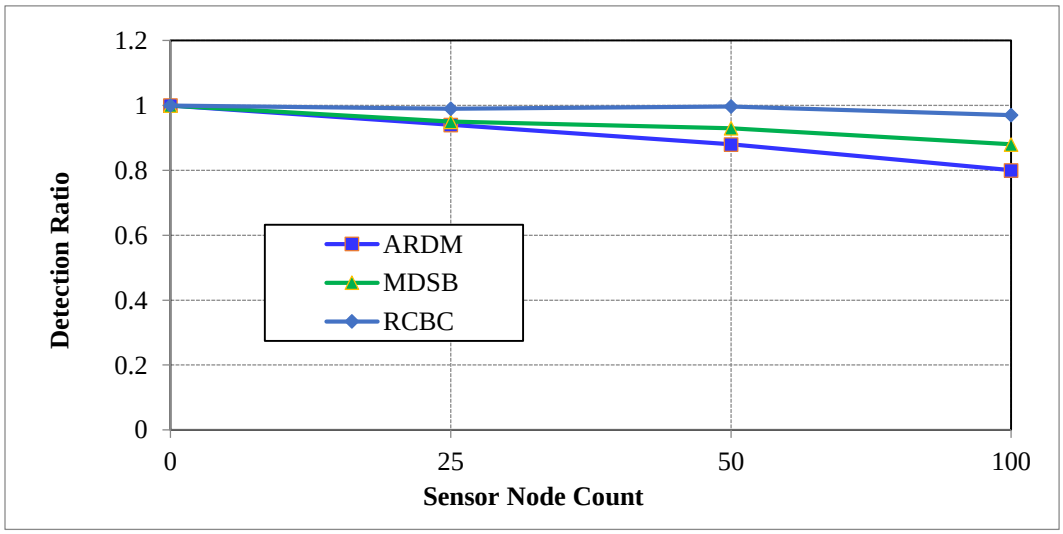

Fig. 6 Abnormal Node Detection Ratio of ARDM, MDSB and RCBC approaches with sensor node count

In MWSN, a high abnormal node detection ratio is vital since mobile sensor nodes can distribute attacks quickly, undetected nodes reduce QoS and throughput performance, and also increase energy consumption. The existing abnormal nodes detection approaches, like ARDM, MDSB does not perform well during sensor node mobility. In MWSN, the Bayes optimal algorithm-based abnormal sensor identification is more proper and operative than the SVM-based detection, as it better deals with uncertainty, mobility, inadequate training data, and energy restrictions while reaching lesser false negative ratio and 0.97 ratio abnormal node detection accuracy.

4.5. Ratio of False Negative

The percentage of abnormal nodes that the Bayes optimal classifier erroneously categorizes as normal in a MWSN is measured by the Ratio of false negatives. Figure 7 demonstrates the ratio of false negative for ARDM, MDSB and RCBC approaches with sensor node count. The existing ARDM and MDSB approaches have low residual energy, which leads to network separating. The proposed system RCBC has lesser computation and energy depletion since the bayes optimal classifier executes abnormal sensor nodes detection by applying parameters like residual energy, packet delay, selfishness and PRR.

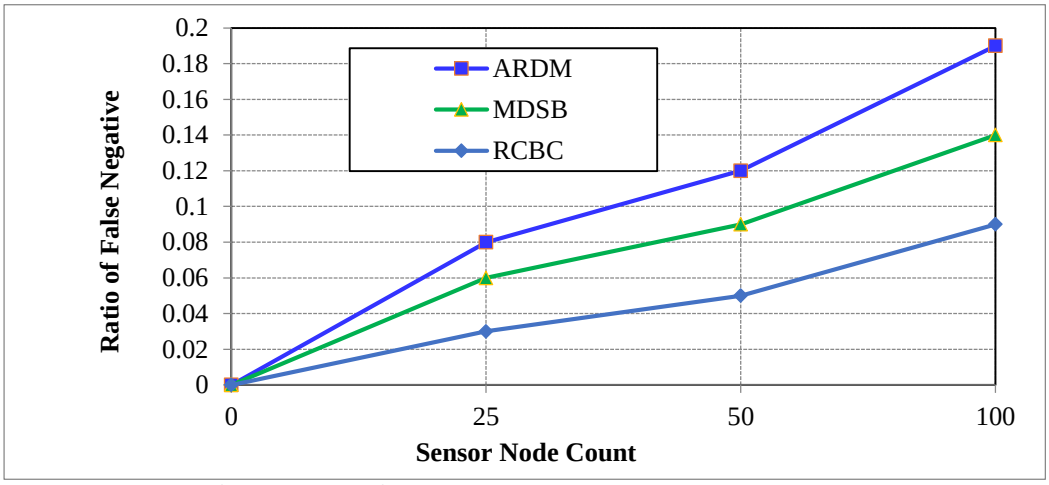

Fig. 7 Ratio of False Negative of ARDM, MDSB and RCBC approaches with sensor node count

By integrating residual energy into the classification process, the RCBC approach can efficiently differentiate cooperative nodes from malfunctioning ones, enabling energy-efficient routing decisions and enhancing the network lifetime.

Hence, the RCBC approach has a 0.09 false negative ratio compared to the other approaches.

4.6. Ratio of False Positive

Ratio of false positives computes the frequency with which the system misidentifies a real sensor node as an abnormal sensor node. Low ratio of false positive denotes better performance, and a higher ratio of false positive refers to poor performance, such as several normal node's mis-categorized as abnormal sensor nodes. Figure 8 demonstrates that the ratio of false positive for ARDM, MDSB and RCBC approaches the sensor node count.

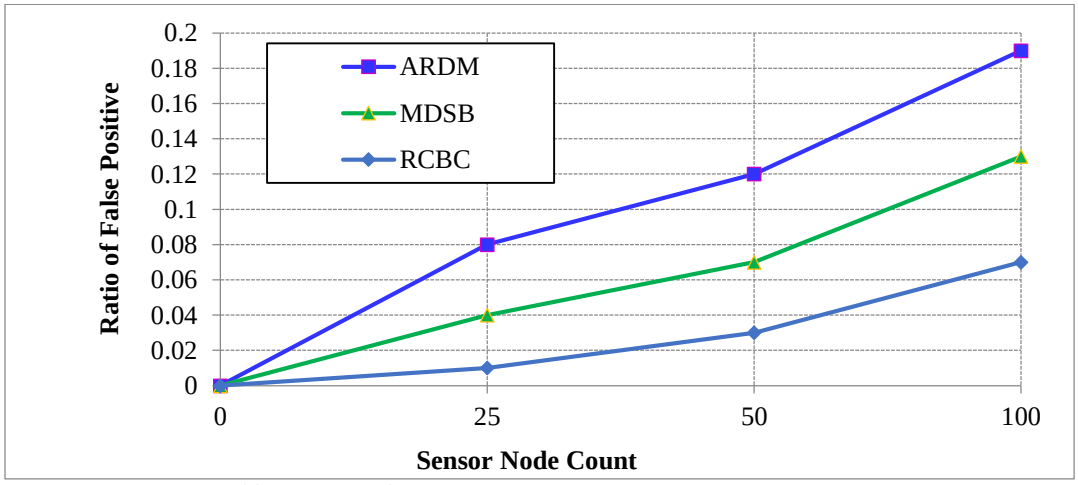

Fig. 8 Ratio of false positive of ARDM, MDSB and RCBC approaches with sensor node count

From the simulation results, the existing ARDM and MDSB mechanism creates high ratio of false positives; as a result, unnecessary separation of real sensor nodes origins depletion of energy, minimized lifetime, and degrades the QoS. However, the proposed RCBC mechanism applies to the Bayes optimization algorithm, which minimizes the false positive ratio in MWSN. An efficient bayes optimal search algorithm objective to reach a 0.07 ratio of false positives, ensuring that normal nodes are not mistakenly penalized while still exactly identifying abnormal nodes. Minimizing the ratio of false positive assistance supports stable communication, effective routing, and enhanced overall performance of the MWSN.

5. Conclusion

This paper presented a bayes optimal classifier-based abnormal node detection approach for MWSNs. If a mobile sensor node's behaviour deviates significantly from typical functioning patterns due to malicious intent, resulting in a decrease in QoS, it is considered abnormal. Malicious nodes increase costs and delay by avoiding data forwarding. The proposed RCBC approach applied the Bayes optimal classifier algorithm for detecting abnormal nodes from abnormality scores. This abnormal score is computed by the mobile sensor node PRR, selfishness rate, levels of residual energy and packet delay. The purpose of the RCBC system is to categorize abnormal sensor nodes from the network efficiently, minimize categorization cost, and enhance QoS metrics. Simulation results confirm significant improvements in throughput and residual energy. Furthermore, it minimized the network delay, false positive ratio and false negative ratio. Future research will concentrate on real-world deployment situations and hybrid Bayesian reinforcement learning algorithms. Offloading Bayesian categorization tasks to fog nodes can minimize computation overhead on mobile sensor nodes and facilitate rapid decision-making in large MWSNs.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Funding Statement

Funding information is not available

References

[1] Natalie Temene et al., "A Survey on Mobility in Wireless Sensor Networks," *Ad Hoc Networks*, vol. 125, pp. 1-30, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[2] Rahma Gantassi et al., "Enhanced Network QoS in Large Scale and High Sensor Node Density Wireless Sensor Networks Using (IR-DV-Hop) Localization Algorithm and Mobile Data Collector (MDC)," *IEEE Access*, vol. 12, pp. 37957-37973, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[3] Mustafa Matar et al., "Anomaly Detection in Coastal Wireless Sensors via Efficient Deep Sequential Learning," *IEEE Access*, vol. 11, pp. 110260-110271, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] Xingkun Xu, and Jerry Chun-Wei Lin, "Abnormal Nodes Sensing Model in Regional Wireless Networks Based on a Convolutional Neural Network," *Wireless Networks*, vol. 29, no. 7, pp. 2981-2992, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[5] Kyle DeMedeiros, Abdeltawab Hendawi, and Marco Alvarez, "A Survey of AI-Based Anomaly Detection in IoT and Sensor Networks," *Sensors*, vol. 23, no. 3, pp. 1-33, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[6] Hossein Pirayesh, and Hashing Zeng, "Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 767-809, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Yingxu Lai et al., "Identifying Malicious Nodes in Wireless Sensor Networks Based on Correlation Detection," *Computers & Security*, vol. 113, pp. 1-12, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] I. Gethzi Ahila Poornima, and B. Paramasivan, "Anomaly Detection in Wireless Sensor Network using Machine Learning Algorithm," *Computer Communications*, vol. 151, pp. 331-337, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[9] Yazeed Yasin Ghadi et al., "Machine Learning Solutions for the Security of Wireless Sensor Networks: A Review," *IEEE Access*, vol. 12, pp. 12699-12719, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[10] Liqun Hou, and Qianchi Huang, "A Smart WSNs Node with SENSOR Computing and Unsupervised One-Class SVM Classifier for Machine Fault Detection," *Measurement*, vol. 242, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[11] Xiong Luo et al., "Abnormal State Warning System of Network Security Management based on KD Tree and KNN," *Procedia Computer Science*, vol. 247, pp. 1005-1011, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[12] T. Thamaraimanalan, and S. Ramalingam, "Hybrid Artificial Neural Network-based Grasshopper Optimization Algorithm for Anomaly Detection in Wireless Body Area Networks," *IETE Journal of Research*, vol. 70, no. 4, pp. 3738-3752, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[13] Dingari Kalpana, and P. Ajitha, "A Hybrid Heuristic-Assisted Deep Learning for Secured Routing and Malicious Node Detection in Wireless Sensor Networks," Peer-to-Peer Networking and Applications, vol. 17, no. 5, pp. 2758-2780, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[14] Ajit Kumar Singh Yadav et al., "Malicious Node Detection Using SVM and Secured Data Storage Using Blockchain in WSN," *International Journal of System Assurance Engineering and Management*, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[15] Zhao Xu et al., "Uncertainty Propagation in Node Classification," *2022 IEEE International Conference on Data Mining (ICDM)*, Orlando, FL, USA, pp. 1275-1280, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] Vivek Kumar Pandey et al., "Enhancing Intrusion Detection in Wireless Sensor Networks Using a Tabu Search-Based Optimised Random Forest," *Scientific Reports*, vol. 15, no. 1, pp. 1-21, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[17] Afrah Gueriani, Hamza Kheddar, and Ahmed Cherif Mazari, "Deep Reinforcement Learning for Intrusion Detection in IoT: A Survey," *2023 2nd International Conference on Electronics, Energy and Measurement (IC2EM)*, Medea, Algeria, pp. 1-7, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[18] Saba Awan et al., "Blockchain-Based Secure Routing and Trust Management in Wireless Sensor Networks," *Sensors*, vol. 22, no. 2, pp. 1-24, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[19] K. Saimadhuri et al., "Enhance the Intrusion Detection performance of WSN using RLA," *2024 International Conference on Intelligent Computing and Sustainable Innovations in Technology (IC-SIT)*, Bhubaneswar, India, pp. 1-5, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[20] K. Sai Madhuri, and Jithendranath Mungara, "Adaptive Reinforcement learning with Dij-Huff Method to Secure Optimal Route in Smart Healthcare System," *Cardiometry*, no. 25, pp. 1131-1139, 2022. [CrossRef] [Google Scholar] [Publisher Link]