





Multi-Level Node Behavior Pattern Analysis for Malicious Node Detection with False Alarm Reduction in Wireless Sensor Networks

Midhunchakkaravarthy^{*}, Orchu Aruna^{}

Computer Science and Engineering, Lincoln University College Main Campus, Petaling Jaya 47301, Malaysia

Corresponding Author Email: oaruna.pdf@lincoln.edu.my

Copyright: ©2025 The authors. This article is published by IETA and is licensed under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

<https://doi.org/10.18280/ijssse.150617>

ABSTRACT

Received: 10 March 2025

Revised: 22 April 2025

Accepted: 10 June 2025

Available online: 30 June 2025

Keywords:

wireless sensor network, security, attacks, data transmission, false alarms, malicious behavior, dynamic threshold adjustment, Behaviour Analysis, quality of service

A Wireless Sensor Network (WSN) is a self-organizing network with numerous sensor nodes that communicate with one another over a series of hops. In unsupervised regions, where attackers can readily enter sensor nodes and inject false data to alter detection findings, it is typically employed. WSNs are vulnerable to a wide variety of failure modes and false positives. A big problem with many WSN applications is their slow and inaccurate response to crises. Security is a major concern with WSNs among many others. The goal of this research is to investigate methods that can effectively and dynamically reduce the occurrence of attacks and to reduce false alarms while simultaneously raising the probability that no target will go undetected. To identify and remove network nodes that represent a threat and also to reduce false alarms is the main objective of this research. Finding and isolating compromised nodes is critical for protecting WSN nodes from attacks that use misleading information provided by the adversary. The low scalability and high communication overhead of flat topology networks make them notoriously difficult to secure. This research proposes a Multi-Level Node Pattern and Behaviour Analysis for Malicious Node Detection with False Alarm Reduction (MLNPBA-MND-FAR) technique for improving the Quality of Service (QoS) Levels in the network. On closer inspection of the results section, though, it is evident that networks ranging from 100 to 600 nodes were used for the studies. The model is tested with different node sizes to see how it handled things like throughput, energy usage, false alarm rate, and detection accuracy. The model's persistent high detection accuracy of 98.7% across varied network size) and low false alarm rates as low as 1.1% illustrate its successful scalability. The proposed model is compared with the traditional Machine Learning Techniques for Anomaly Detection in Communication Networks (MLTs-ADCNs), Wireless Weak-link Sensor Networks using Dynamic Trust Management (WSN-DTM), and Sinkhole Attack Detection by Enhanced Reputation-Based Intrusion Detection System (SHAD-ERbIDS).

1. INTRODUCTION

Wireless Sensor Network is a revolutionary technology which is used in many fields such as safety monitoring, environmental monitoring, smart city technology, military surveillance, health monitoring etc. Wireless network of sensor nodes that communicate autonomously in space by collecting, processing and transmitting information [1]. The self-organizing architecture and decentralized nature make WSNs powerful as well as prone to various adversities of security problems. Data injection, which corrupts the integrity of a WSN, and network eavesdropping, which threatens the security of the network, highlights two of the major problems caused by malicious nodes [2]. One of the most serious challenges for efficiently operating these networks is to detect malicious nodes without triggering a high number false alarm [3]. WSNs function in dynamic environments that can be hostile, as the sensor nodes are susceptible to threats like physical tampering, malicious attacks, and environmental

disturbances [4]. Because these networks are often deployed in unsupervised or remote locations, they are susceptible to a variety of security threats including node capture, Denial of Service (DoS) attack [5], and false data injection. It is not trivial to detect these malicious nodes since these nodes can easily conceal in the network and conduct attacks without being immediately identified [6].

At the WSNs field, one of the most pernicious kinds of attacks consists of altered nodes behavior. Malicious nodes are also difficult to detect as they can modify their behavior and provide incorrect data or prevent the network from operating normally [7]. The nodes which indicated abnormal behavior can be abnormal data generation, high energy consumption, erratic communication patterns, etc. Detection of such behavior is critical, but ideally implemented without introducing network-level performance degradation [8]. Without minimization, false alarms could exhaust the network's capacity which results into needless reconfigurations and loss of critical data [9]. In WSNs, false

alarms can lead to a significant degradation in performance, especially when legitimate nodes are mistakenly identified as malicious [10]. As a result, resources are wasted in identifying and isolating non-malicious nodes because of these false positives. The Attack detection in WSN general process is shown in Figure 1.

One of the main challenges of detecting malicious nodes is the development of an algorithm which achieves sensitive yet specific detection to avoid a benign node being incorrectly labelled as malicious [11]. Finding this balance is crucial to keeping the network agile and secure. Traditional malicious node detection methods based on anomaly detection methods or cryptographic methods often do not have good accuracy in the highly dynamic nature of WSNs [12]. Behavior analysis provides a better approach to identify malicious activity by monitoring the interaction of nodes in the network. It allows flagging as suspicious nodes that greatly deviate from the expected behavior [13]. This approach makes detection more nuanced and reduces the chances of false positives and false negatives, allowing for improved identification and resolution of the task at hand.

Machine learning-based approaches have been suggested for a more accurate analysis of node behavior patterns. Detection of malicious nodes at multiple tiers of the network is possible, transmission rates for packets at the physical layer,

and data integrity at the application layer [14]. Other information from multiple layers allows the detection system to distinguish between the normal and malicious nodes more efficiently. It provides improved detection accuracy and reduces communication overheads arising from naive detection approaches [15]. Scalability is another key issue affecting the success rate of malicious node detection schemes for WSNs. And many traditional security solutions don't work well if the network grows because of the high communication overheads they introduce.

Flat topology networks, struggle to achieve the security of nodes and edges while avoiding an excessive degree of communication between them. Based on the summarized details, the solution proposed by this research purposefully tries to minimize communication costs through determining the malicious nodes locally rather than in a network-wide manner. It is possible to identify malicious nodes with lightweight protocols and alert the network to these nodes by monitoring packet drop rates and throughput values to isolate them in advance before they exhibit harmful behavior [16]. The proposed security architecture in this research can not only help to ensure the uninterrupted provision of Quality of Service (QoS), but also offers a rational approach to the actual allocation of QoS resources by more trusting and accredited nodes for normal operations [17].

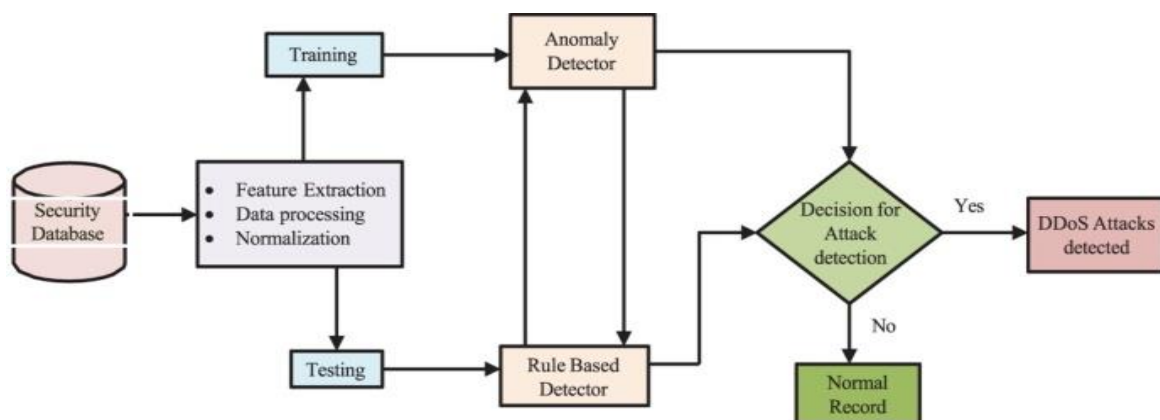


Figure 1. General IDS process

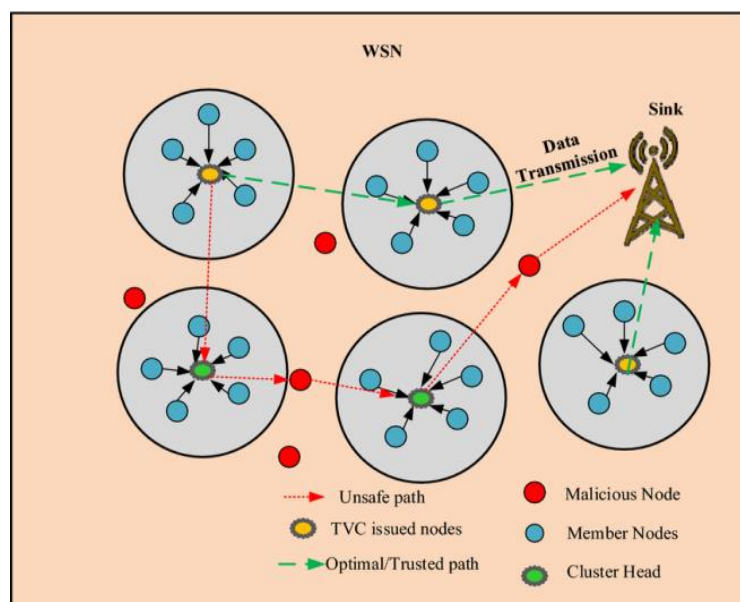


Figure 2. Malicious node in WSN

QoS metrics such as data delivery reliability, network lifetime and latency also determine the performance of a WSN apart from security. Malicious nodes can have a significant impact on these metrics via normal operation disruption and false alarms generation. Thus, enhancement of QoS is not merely limiting to detection of attack, but also to sustain the proper communication of nodes that are not malicious along with the existences of the malicious node [18]. The approach proposed in this work aims to provide optimal QoS, is based on an intelligent of a model for behavioral analyses which monitors nodes and isolates malicious ones, and minimizes the probability of false alarms. The MLNPBA-MND-FAR technique which performs Multi Level Node Pattern and Behaviour Analysis for Malicious Node Detection with False Alarm Reduction is proposed in this research. This approach combines a multilayer analysis of the individual behavior of a node, employing statistical as well as machine learning techniques for better accuracy of detection. By cross-verifying the behavior of nodes at various degrees of linkage through the network, these two systems allow for the identification of malicious nodes. In addition to the augmentation technique, they also introduced a method to prevent the overall performance from being reduced when detection is performed. MLNPBA-MND-FAR is a dynamic-based algorithm that can perform genotyping in real-time. By monitoring the behaviour of the nodes, it continuously adjusts the threshold of detection to adapt to the current conditions of the network. Such flexibility in the algorithms is very critical in WSNs where the mobility of the nodes, changes in the environment state, and reconfigurations of the network can make a difference in the communication. Through iterative improvement of its detection model, the system maintains the ability to respond to new attack approaches while preserving network throughput. The malicious node detection in WSN is shown in Figure 2.

Malicious nodes in WSNs can adopt different attack strategies such as data injection, eavesdropping, and selective forwarding. We designed a technique called MLNPBA-MND-FAR to discover these behaviors at the beginning of each attack cycle before they can turn into bigger and destructive attacks. By quickly isolating compromised nodes, the system prevents the entire network from being disabled or compromised. This limits the number of false positives where a benign node is wrongly isolated, saving network bandwidth. Nodes in WSNs are often expected to cooperate and exchange data with each other. In this Harmonious collaboration, malicious nodes can disrupt the system by not sharing the data or providing the corrupted data to the other nodes [19]. The proposed approach before it infects the system, by early detecting malicious nodes and excluding them from the collaboration pool, thus helps ensure that the integrity of the network. The lower false alarm rate guarantees that trusted nodes can continue working together undeterred. One key benefit of the proposed technique is the possibility for improved WSNs long-term efficiency. Increased lifespan and more reliable data collection due to the reduction of false alarms means the ecosystem can function with less interference. So the system's capacity to evolve dynamically to new threats means that it continues to work as new strategies for attack arise. The goal of this research is to detect malicious nodes in WSNs more accurately and reliably while reducing the number of false alarms. Because of their decentralized structure, energy constraints, and open communication design, WSNs are susceptible to a wide range of assaults. Among these are sinkhole attacks, selective forwarding, Denial of

Service (DoS), and fake data injection.

Using data transmission habits, energy consumption patterns, and interaction patterns as a starting point, this technique examines node behaviors at several tiers in search of anomalies that could signal malicious activity. With this in mind, we made sure the framework could detect a broad variety of suspicious node actions independently of any particular threat model. Static wireless sensor networks with different density of nodes (simulated to be between 100 and 600 nodes) are the main subject of the research. It disregards very dynamic topologies and doesn't investigate mobile or heterogeneous WSN settings. Consequently, one limitation of this study is that it has only been tested in network deployments that are static, homogeneous, and well-structured. Data analysis's purview is another crucial limit. The model doesn't go into intrusion detection at the encryption level or deep packet inspection, instead focusing on patterns of behavior at the node level. Although the model incorporates multiple layers of detection and mitigation of false alarms, it does not incorporate any external systems such as blockchain for decentralized trust management or cloud-based monitoring.

The limited energy resources impose severe constraints on WSNs that facilitate as their importance as the most critical objective in the design of networks. Active node detection algorithms can be resource-consuming as well as energy-consuming [20]. This algorithm is developed to reduce energy consumption by enhancing detection in suspicious behavior of nodes rather than complete network checking. Doing so extends the longevity of the network with strong security. There are many potential applications for this research. As a result, the ability to detect malicious nodes without adverse system performance is of vital importance depending on the application in critical systems such as military surveillance, healthcare monitoring, and environmental sensing. Topic Stability in varying conditions lies in Deriving MLNPBA-MND-FAR. Similar domain criteria remain applicable where the MLNPBA-MND-FAR approach can be implemented. The proposed MLNPBA-MND-FAR technique is superior to the current malicious node detection techniques in terms of the detection accuracy and the false alarm rate. Traditional methods often result in a higher rate of false positives when the network condition changes. This research thus employs a multi-level analysis approach for detecting malicious nodes, which not only offers a more adaptive mechanism for anomaly detection, but also outperforms the traditional anomaly detection methods.

2. LITERATURE REVIEW

WSNs have emerged as a quintessential component of cutting-edge wireless technology, offering low-cost solutions to a range of monitoring activities in the age of ubiquitous wireless communication buoyed by Wi-Fi. But all these networks are vulnerable to security threats including but not limited to unauthorized access, attacks and suspicious activities which can negatively impact their performance and dependability to a great extent. Such vulnerabilities can also be wiped out by using Intrusion Detection Systems (IDS), as they are important to protect WSNs by detecting and responding to threats on time. Sadia et al. [1] described a lot of research efforts aimed at improving accuracy and efficiency of these Intrusion detection models in terms of high detection rates and low false alarms, some of the methods have been focused on reducing redundant features from the datasets to

improve performance.

The advent of 5G has simplified the administration of WSNs by the advent of Software-Defined Networks and Network Function Virtualization. On the other hand, the utilization of WSNs in adversarial environments poses critical security issues, Miranda et al. [2] introduced Optimal Software-Defined security Framework. A Solution for Interactive Non-Intrusive Security of SDN-Based Infrastructure, that proposes a software-defined security framework employing an IPS-based lightweight intrusion prevention mechanism and a collaborative anomaly detection system close to the data plane. A Smart Monitoring System (SMS) is located at the control plane to correlate any alerts generated by sensor nodes, providing a cost-effective and firm security for WSNs.

In the sense of advanced continuous attacks over ultra-densified networks and in 6G wireless communications, a robust IDS protecting in a real-time manner is required, but unfortunately, traditional systems are unable to counterattack effectively. Oleiwi et al. [3] proposed a framework for anomaly detection, in the form of EL-ADCNs, using an Ensemble Learning (EL)-based approach. This framework consists of four stages, including malicious traffic, control preprocessing, using CFS-RF to select features from datasets (NSL_KDD, UNSW_NB2015, CIC_IDS2017), implementation EL hybrid algorithms ranging from random forest (RF), support vector machine scrolls to determine the best training model, adaboosting, and bagging, and then testing the model using binary/multi-class classification. This leads to improved detection accuracy, reduced false positives, and reduced false negatives.

Due to the resource-contained sensor node, as well as the presence of malicious node (MNs), WSNs, a self-configured Wireless Ad Hoc Networks (WANET) for Internet of Things (IoT), has energy efficiency and security issues. Kumar et al. [4] introduced a MN detection and isolation mechanism that guarantees energy-efficient data transmission. In the MND Phase for identification of MNs the approach involved an Improved Deep Convolutional (IDCNN) to augment in malicious list. An Extended K-Means (EKM) algorithm clusters trusted nodes in order to select an optimal cluster head (CH) based on residual energy with energy-efficient transmission by a t-Distribution-based Satin Bowerbird Optimization (t-DSBO) algorithm. When a CH runs out of energy, t-DSBO recognizes the next CH and details using the identified CH to the base station. It improves WSNs security and energy-saving.

The CoSE, a blockchain based framework was developed by Nouman et al. [5] for the secure WSNs where, BSs (Base Stations) and CH(s) (Cluster Heads) are integrated with the BSs architecture of the WSN to register the nodes, afterwards CHs register the nodes to address the security bottomline. At the BSs, a Machine Learning classifier (Histogram Gradient Boost (HGB)) classifies nodes as either malicious or legitimate. Malice nodes lose their registration, and honest nodes' data is kept on an Interplanetary File System (IPFS) that returns a hash of every piece of data, which is stored on the blockchain. Consensus and transaction validation in this architecture does not use PoW but a new architecture called Verifiable Byzantine Fault Tolerance (VBFT). Self-attention based Mini-Tree Miner with embedded admissible consensus is trained on all three datasets WSN-DS at once, evaluating on original and balanced datasets with respect to each others' sensitivity and healthy evaluation can be used as a new breed

of supervisable unsupervised learners which can be applied in WSN to boost their security and reliability.

For fragile links and internal attacks, Wang et al. [6] discussed how such attacks threaten Wireless Weak-link Sensor Networks (WWSN). The authors proposed a malicious node detection scheme based on dynamic trust management to address these problems. SP-aw based node trustworthiness assessment using type-2 fuzzy logic and different trust factors. Moreover, a dynamic trust value updating mechanism is proposed to respond to the transition of environments of WWSNs, ensuring that the malicious nodes can be effectively detected and enhancing the security of the network.

Ramasamy et al. [7] provided an extensive survey on employing blockchain-based techniques for malicious node detection in WSNs. In which centralized one-time decision-making approach, during WSNs implementations, it show the absence of traceability, fairness and error-proneness. The model also delves into the incorporation of blockchain with WSNs (BWSN) by examining its architecture, domain-wise applications, and benefits. It underlines the detection of malicious nodes through the application of BWSN employing architectural perspectives along with the role played by smart contracts. Besides, these contributions that blockchain brings to WSN data management, such as online information aggregation, auditing, event logging, information storage for analysis and offline query processing, are addressed in the model, providing a new view for improving the security and efficiency of WSN designs.

Mohammed et al. [8] highlighted the importance of data security in WSNs and sinkhole attacks, which are harmful for network performance, as well as data confidentiality, integrity and availability. To this respect, the authors presented a better fit for reputation-based mechanism IDS enhancing WSNs by offering essential IDS for WSNs. An artificial bee colony (ABC) optimization technique was used to further optimize the performance of the IDS. Moreover, the study included noisy channels to represent practical difficulties in WSN environments. By discriminating and reducing sinkhole attacks, this strategy leads to better performance overall while improving data management security.

The self-configuring WANET for the IoT are known as WSN. These networks comprise a large number of resource-constrained SN. Efficiency in energy consumption and safety are critical aspects in WSN. The presence of Malicious Nodes (MNs) makes it possible for the adversary to transmit erroneous information. It is critical to identify and isolate certain MNs in order to avoid security issues. Therefore, this study proposed a method for identifying MNs in WSN by mining the parameters of each SN. By selecting the Cluster Head (CH) based on the sensor's residual energy, this work not only addresses security but also renders energy-efficient data transmission (DT) analyzed by the study [9]. When it comes to the Malicious Nodes Detection (MND) phase, the Improved Deep Convolutional Neural Network (IDCNN) finds the MN and adds them to the malicious list box. By using the Extended K-Means (EKM) algorithm to group the Trusted Nodes (TN) into clusters, the t-Distribution based Satin Bowerbird Optimization (t-DSBO) algorithm chooses a CH for each cluster based on the residual energy of those nodes, resulting in an energy-efficient DT phase. The CH is responsible for transmitting the cluster's data to the BS. When one CH's energy drops below a certain threshold, the t-DSBO switches to the other.

More and more people are looking to establish

heterogeneous wireless sensor networks (HWSNs) to securely and efficiently monitor and gather data in a specific region, thanks to the ever-increasing capabilities of sensor technology. But there are a lot of security issues because HWSN nodes aren't very powerful. Current HWSN data transmission algorithms address these security risks, but doing so increases the energy consumption of the network and the computational cost of individual nodes. In order to protect heterogeneous wireless sensor networks from malevolent nodes, this research suggests an LSDT (Lightweight Secure Data Transmission) method. Firstly, taking into account the limited capabilities of nodes in HWSNs, Wang et al. [10] developed a lightweight secret sharing scheme that uses the XOR operation. This scheme simplifies the process of transmitting shares to the sink node by mapping data to numerous shares and avoiding unnecessary pathways. When compared to more conventional secret sharing techniques, this one can significantly lower the computational burden of nodes while still ensuring data security. In addition, hostile nodes in the network can disrupt message transmission while shares are being delivered. So, we build a system to identify malicious nodes and provide feedback on their actions; this system can update the reputation level of harmful nodes and respond rapidly to attacks by malicious nodes. Our proposed reference-path routing selection technique takes into account the energy and reputation levels of diverse nodes in a thorough manner.

Due to their dispersed nature and reliance on open communication, WSNs are incredibly susceptible to various types of attacks. For two reasons, the selective forwarding attack is extremely hard to detect compared to other inside assaults. The node in the challenging environment has to discard certain data packets, and the cunning malevolent node often manages to avoid detection. In this research, we use a reinforcement learning (RL) technique to simulate a hostile node's selective forwarding attack. Ding et al. [11] develop the double-threshold density peaks clustering (DT-DPC) approach to identify the selective forwarding attack in a challenging setting. Continuous abnormalities lead to the isolation of aberrant nodes, which are then deemed malevolent. Since malevolent activities manifest independently and a hostile environment consistently disrupts agglomerate nodes, the neighbor voting approach is used to identify suspicious nodes. With DT-DPC, network throughput is improved even when intelligent hostile nodes manage to evade RL algorithm detection.

To address many security concerns and facilitate node registration using credentials, the proposed work employs blockchain technology on Cluster Heads (CHs) and Base Stations (BSs). To further distinguish between legal and malicious nodes, the BSs use a Machine Learning (ML) classifier called Histogram Gradient Boost (HGB). M. Nouman et al. [12] removed the node's registration from the network if we discover it is malicious. On the other hand, an Interplanetary File System (IPFS) is used to store data from valid nodes. IPFS creates hashes for the data and stores them in blockchain after storing them in chunks. Also, instead of Proof of Work (PoW), Verifiable Byzantine Fault Tolerance (VBFT) is utilized to validate transactions and conduct consensus. The WSN-DS dataset, which stands for wireless sensor network, is also used for comprehensive simulations.

3. PROPOSED MODEL

To eliminate the security challenges in WSNs, the proposed

model is Multi-Level Node Pattern and Behaviour Analysis for Malicious Node Detection with False Alarm Reduction (MLNPBA-MND-FAR). Inherently, the WSNs can be prone to various security threats, mainly when they are used in an unattended or hostile environment. One of the major security issues is the detection of malicious nodes, which involves malicious nodes actively disrupting overall network functioning by taking actions such as injecting false data or engage in selective forwarding. A major challenge of the detection process itself is to minimize false alarms in line with ensuring that true malicious behaviors are detected. The system effectively tackles this challenge with a multi-dimensional analytical approach alongside adaptive mechanisms enabling detection of affected nodes without inundating the network with spurious alerts.

Multi-level node behavior analysis is the core of this model. In WSNs, every sensor node communicates with its neighboring nodes to share information; therefore, any behaviour diverging from the CNC can point to the existence of a malicious node. Low-level network metrics can be focused on the first level of the model, such as packet loss rates, delays, and unexpected data flow [21]. At this level, the anomalies are typically linked with fundamental attacks like selective forwarding or DoS attacks where malevolent nodes interrupt or stop valid communication. At the second level, the model looks more deeply at interactions between individual nodes, such as how they process and transmit information [22], and their overall contributions to the direction of the network topology. In case a node fails to transmit data or keeps sending misleading information, it is marked for further review and scrutiny [23]. Level 3 is at a much higher level of sophistication being complex pattern recognition and machine learning techniques be used that analyze high-order statistics of node behavior, different nodes activity covaries in time and/or response to random network conditions. This layered approach provides coverage against malicious nodes at different stages of the network's operation, reducing the chances of ignoring stealthy attacks [24].

One of the important parts in the model is dynamic thresholds adjustment. Such dynamic environments, such as WSN, treat nodes that behavior differently depending on the dynamics of the networks provided in terms of their incoming network requests, environmental circumstances or node mobility. The model overcomes this issue by introducing an adaptive approach that fine-tunes threshold settings according to current event data [25]. They will adjust the thresholds of detection because of increased traffic and prevent false flags due to overload regarding packet loss/delay. Training the system with various normalizable events that might occur enables the DDoS attack detection system to dynamically adapt to the fluctuations of the network over time, suppressing false alarms that would have resulted from normal network activity.

The application of machine learning techniques is significant to improve the detection accuracy of the model [26]. The model can progressively develop and adapt its understanding of what is normal behavior for a given WSN deployment by analyzing node behavior over time [27]. Conventional malicious node detection techniques usually are based on frequent communication among nodes, leading to increased energy consumption resulting in the reduced life span of a network [28]. The localization approach for detecting malicious activity, which is generated by MLNPBA-MND-FAR model to minimize the aforementioned issue. Instead of

demanding full worldwide communication, the model uses local node engagement and behaviors to identify anomalies. The model can use local communication and behavior patterns to highlight suspicious nodes without extensive data transfer across the network. This localized detection approach not only significantly lowers the overall communication traffic but also saves energy, which is essential for battery-powered sensor nodes [29].

It then uses a packet drop and throughput evaluation mechanism to improve its ability to detect malicious nodes. In particular, malicious nodes that send data selectively or conduct DoS attacks have abnormal packet drop curves or inconsistent upflow per node. In the MLNPBA-MND-FAR model, these metrics are used to monitor the performance of each node continuously. A node is marked as suspicious when it acts abnormally. Such early detection enables the scheme to prevent malicious nodes from damaging the performance of a network significantly. After identifying a malicious node, the model cuts it off from the network to cease any damage it could cause. Isolation process ensures that the rest of the nodes in the network aren't disrupted and continue functioning normally. Once the malicious node is identified and removed, a network recovery protocol is initiated, wherein the remaining nodes collaborate to reconfigure the network, aiming to resume typical functionality. This could also consist of deciding new pathways for the traffic of information or redistributing workloads among other nodes in the network. Minimizing downtime and allowing the network to continue operating in the presence of compromised nodes are the goals of the recovery mechanism.

In addition, to facilitate the recording of nodes' behavior over time, this model also includes a trust-based monitoring system. Nodes that display consistent benevolent behavior, such as successful data deliveries and low packet loss rates, are rewarded with a high trust score. On the other hand, nodes that exhibit abnormal characteristics like a high volume of lost data or losing part in the routing process are given low trust scores. It would not only conduct the detection, but also dynamically evaluate its trust through assigning adaptive and reasonable weight to nodes. The MLNPBA-MND-FAR model provides a significant advantage by drastically reducing false positives, resulting in a common issue found in traditional detection schemes. A false positive benign node that has been tagged as malicious can cause massive disruptions to network performance and waste valuable computational resources on needless checks. By dynamically changing the thresholds and having machine learning techniques, near-real-time behavior of the devices can be analyzed at a localized level, which reduces false alarms. Such false alarms can further create cascading effects in large-scale networks, which leads to the performance deterioration of the entire system. The model handles the WSN more reliable and efficient by addressing the malicious nodes correctly with no further disturbance for benign nodes.

The model is designed with a special consideration for efficient power consumption. In addition, WSNs are usually made up of sensor nodes that have limited energy, which means that any solution with significant energy overhead can reduce the network operational lifetime. By considering localized analysis and reducing inter-node communication, the MLNPBA-MND-FAR model is also energy-efficient. Dynamic adjustment of detection thresholds also guarantees that the system does not perform unnecessary checks or communications, thereby decreasing energy consumption.

This energy-efficient mechanism is crucial for the sustainable longevity of WSNs, particularly in distant or inaccessible conditions where regular upkeep is unfeasible.

Dynamic threshold adjustment is an important part of the MLNPBA-MND-FAR model, which aims to reduce false positives and improve the accuracy of malicious node identification. When deciding whether a node's actions are harmful or not, traditional threshold-based models frequently employ fixed or static thresholds. However, in actual WSNs, where factors (such as energy levels, node behavior, and traffic load) fluctuate regularly, fixed thresholds might not function.

In response to changes in average transmission rates, energy consumption patterns, or behavioral outliers over time, the detection system can dynamically adjust the threshold and update the decision border. In order to keep its sensitivity to changes in network dynamics while avoiding overreaction to transient fluctuations, the model routinely recalculates the anomaly detection threshold and analyzes these metrics. This flexibility greatly decreases the number of false alarms, which is particularly useful in networks that are dense or dynamic, where the normative behavior might differ greatly. If the computed node behavior score is higher than the adjusted threshold, the node is marked as possibly malevolent. Future threshold calibration can be informed by the feedback loop from previous detection outcomes, which further improves detection accuracy. The pseudo code for the proposed model is clearly indicated.

Pseudo Code: MLNPBA-MND-FAR

Input: Network nodes $N[]$, behavior metrics $B[]$, energy levels $E[]$, transmission logs $T[]$

Output: Detected malicious nodes $M[]$, updated threshold θ

Initialize:

$M[] \leftarrow \text{empty}$

Set initial threshold $\theta = \theta_{\text{base}}$

Begin

For each node i in $N[]$:

 Monitor behavior metrics $B[i]$

 Monitor energy consumption $E[i]$

 Monitor transmission activity $T[i]$

 Compute Behavior Score $BS[i]$ using:

$BS[i] = \text{weight1} * \text{anomaly_rate}(B[i]) +$
 $\text{weight2} * \text{energy_drift}(E[i]) +$
 $\text{weight3} * \text{packet_drop_rate}(T[i])$

End For

Compute network average behavior score BS_{avg}

Compute deviation σ from BS_{avg}

Update threshold θ dynamically:

$\theta = BS_{\text{avg}} + \alpha * \sigma$ // α is sensitivity coefficient

For each node i in $N[]$:

 If $BS[i] > \theta$ then

 Mark node i as malicious

 Add node i to $M[]$

 Else

 Mark node i as normal

 End If

End For

Return $M[]$, updated θ

End

Another major benefit is the model's scalability. Scalability is a key factor in WSNs as they are mostly deployed in a large-scale environment and performance of such networks is directly proportional to the number of nodes and scale of the area. Using multi-level analysis framework also enhances the labeling process and the localized detection and dynamic

threshold adjustments also balances between the model scale up and scalability without any overhead on it. The versatility of the model makes it adaptive to networks of differing scales, from small instrumentation deployments to large dense sensor fields, while ensuring no degradation in detection accuracy or system performance. The proposed model framework is shown in Figure 3.

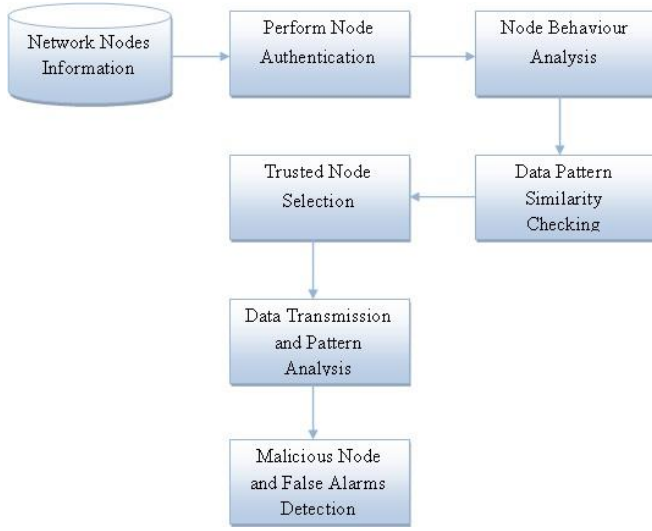


Figure 3. Proposed model framework

The proposed model can be applied widely in real-time applications, which include but are not limited to military surveillance, smart cities, healthcare, and environmental monitoring, all of whose utmost goals are to achieve maximum security. In these situations, the effects of a corrupted sensor node can be serious, causing wrong data transmission, wrong interpretation of essential information and even filling the gap in complete system failure. The risks of the previously mentioned attempts are conquered by MLNPBA-MND-FAR model as it identifies and isolates the malicious nodes that keep data integrity and that the network is working. The proposed MLNPBA-MND-FAR model provides an effective and flexible framework for malicious node detection in WSN that minimizes generation of false alarms and reduces energy consumption. The model maintains a well-balanced control among security, performance, and energy efficiency through multi-level behavior analysis, machine learning approaches, dynamic threshold arrangement, and working in a localized manner. This research proposes a Multi Level Node Pattern and Behaviour Analysis for Malicious Node Detection with False Alarm Reduction technique for improving the Quality of Service (QoS) Levels in the network.

Node information processing involves aggregating and analyzing the data received from all nodes in the network. This can be mathematically represented as:

$$N_{Info}[M] = \sum_{n=1}^M nodeattr(n) + nodeaddr(n) + TI(n)$$

Nodeattr(n) model collects the node properties and nodeaddr(n) model is used to identify the node physical address and TI(n) is the time instant, n is represented as current node and M is the total nodes in the network.

Node authentication ensures that only legitimate nodes participate in the network. The authentication process can be modeled as:

$$Node_Authen[M] = \sum_{n=1}^M Hf(Key(n)||D(n))$$

Here Hf is the Hash function, Key(n) is Key of node n and D is the Nonce generated for node n used for authentication.

The dynamic threshold calculation is performed as

$$SD[M] = \sum_{n=1}^M \sqrt{\frac{1}{M} \sum_{n=1}^M Hf(key(n)) + Node_Authen(n)}$$

$$DT[M] = \sum_{n=1}^M \gamma(SD(n)) + \max(SD(n, n+1))$$

Here γ is the model is used to identify the behaviour score of each node.

Pattern and behavior analysis compares current behavior to historical patterns. It can be represented as:

$$NpattrnBehav[M] = \sum_{n=1}^M D(n) + ||P(n) - Pref(n)|| + SD(n)$$

Here D(n) is the Deviation score of node n, P(n) is the Current pattern of node n and Pref indicates the historical previous pattern in data transmission.

Malicious nodes are identified by setting a threshold for deviation. If a node's deviation exceeds the threshold, it is flagged as malicious. The process is performed as

$$MalNode[M] = \sum_{n=1}^M MalNode(n)$$

$$= 1 \text{ if } (D(n) \& NpattrnBehav(n)) > Th$$

Here Th is the Threshold for deviation to consider a node as a malicious node.

False alarm detection involves identifying incorrect flags of malicious behavior. It can be modeled as:

$$Falarm[M] = \sum_{n=1}^M prob(\min(D(n))) + \min(simm(P(n)))$$

$$+ \max(diff(NpattrnBehav(n)))$$

Simm(P(n)) model considers the similarity in the pattern, diff(NpattrnBehav(n)) model considers the difference and prob(min(D(n))) model calculates the probability function in false alarms.

Algorithm MLNPBA-MND-FAR

```

BEGIN
nodes_info = GetNetworkNodesInformation()
authenticated_nodes = []
FOR each node IN nodes_info DO
  IF AuthenticateNode(node) THEN
    authenticated_nodes.ADD(node)
  END IF

```

```

END FOR
node_behavior_data = []
FOR each node IN authenticated_nodes DO
    behavior = AnalyzeNodeBehavior(node)
    node_behavior_data.ADD({node, behavior})
END FOR
trusted_nodes = []
FOR each behavior_data IN node_behavior_data DO
    IF CheckDataPatternSimilarity(behavior_data) THEN
        trusted_nodes.ADD(behavior_data.node)
    END IF
END FOR
selected_trusted_nodes = SelectTrustedNodes(trusted_nodes)
data_transmission_results = []
FOR each node IN selected_trusted_nodes DO
    result = AnalyzeDataTransmissionAndPattern(node)
    data_transmission_results.ADD({node, result})
END FOR
malicious_nodes = []
false_alarms = []
FOR each result IN data_transmission_results DO
    IF IsMaliciousNode(result) THEN
        malicious_nodes.ADD(result.node)
    ELSE IF IsFalseAlarm(result) THEN
        false_alarms.ADD(result.node)
    END IF
END FOR
Generate selected_trusted_nodes
Generate malicious_nodes
Generate false_alarms
END

```

4. RESULTS

This section gives the performance analysis of the Multi-Level Node Pattern and Behaviour Analysis for Malicious Node Detection with False Alarm Reduction (MLNPBA-MND-FAR) model. Several performance metrics, such as detection accuracy, false alarm rate, energy consumption, throughput, and network scalability, are used to evaluate the performance of the model. Extensive simulations and comparisons with existing methods were performed to evaluate modeled enabled security in WSNs while minimizing the communication and energy overheads induced by malicious nodes detection. The proposed model is compared with the traditional Machine Learning Techniques for Anomaly Detection in Communication Networks (MLTs-ADCNs), Malicious Node Detection in Wireless Weak-Link Sensor Networks Using Dynamic Trust Management (WWSN-DTM) and Sinkhole Attack Detection by Enhanced Reputation-Based Intrusion Detection System (SHAD-ERbIDS) models.

A NS2 simulator is used that can mimic WSN communication behavior, energy consumption, and node interactions is used to run the simulation. To test the model in both sparse and dense network scenarios, the simulation uses a node count ranging from 100 to 600. From one transmission cycle to the next, each node is hard-coded to follow predetermined patterns of behavior, which might be benign or malevolent. The node Behaviour Analysis is implemented in

4.1 Detection accuracy and false alarm rate

In the MLNPBA-MND-FAR model, the MLNPBA was primarily designed to identify malicious nodes without triggering unnecessary false alarms. To test the performance of the detection accuracy, experiments were performed on various kind of malicious node behavior such as black hole and Neptune, saint and DoS attacks. The proposed model is evaluated in comparison with traditional techniques like base line threshold-based techniques and behavior-based detection models.

Results illustrated that compared to the classic approaches; the MLNPBA-MND-FAR model achieved a significantly higher rate of detection. The proposed model achieved a detection accuracy of 98.7% compared to that of with traditional models. This accuracy increase is attributed to the model's multi-level analysis framework that enables detection of malicious activities at different stages of node behavior from packet loss and delays to more sophisticated attack patterns inferred using a machine learning-based pattern recognition process. The Malicious Node Detection Accuracy levels and False Alarm Rate levels are indicated in Tables 1 and 2, Figures 4 and 5.

Table 1. Malicious node detection accuracy

Nodes in the Network	Models Considered			
	MLNPBA-MND-FAR Model	MLTs-ADCNs Model	WWSN-DTM Model	SHAD-ERbIDS Model
100	97.7	93.2	91.4	93.5
200	97.9	93.5	91.6	93.8
300	98.1	93.7	91.8	94.1
400	98.3	93.9	92.0	94.3
500	98.5	94.0	92.2	94.6
600	98.7	94.2	92.4	94.8

Table 2. False alarm rate

Nodes in the Network	Models Considered			
	MLNPBA-MND-FAR Model	MLTs-ADCNs Model	WWSN-DTM Model	SHAD-ERbIDS Model
100	1.1	3.5	2.7	4.2
200	1.2	3.7	2.9	4.4
300	1.4	3.9	3.1	4.6
400	1.7	4.1	3.3	4.8
500	1.8	4.2	3.5	5.0
600	2	4.3	3.8	5.2

A significant process decreased in the false alarm rate is observed. Conventional techniques usually face false-positive cases with malicious nodes which are started working irregularly due to network congestion or environmental condition. The proposed model nearly outperforms existing solutions with less false alarm by dynamically estimating detection thresholds and analyzing multi-level node behavior. By decreasing false positives, this inevitably improves overall network performance and reduces unnecessary disruptions for legitimate nodes that would otherwise be wrongly isolated or flagged as malicious activity.

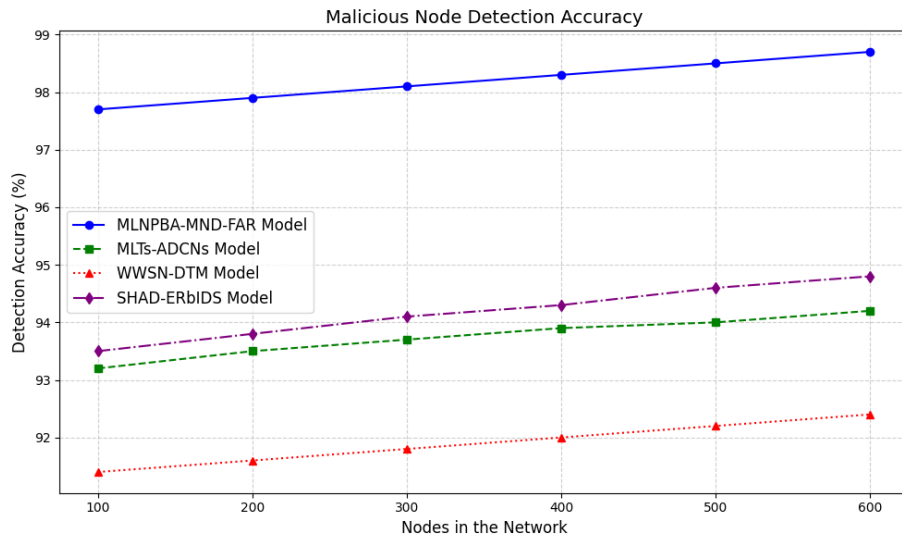


Figure 4. Malicious node detection accuracy

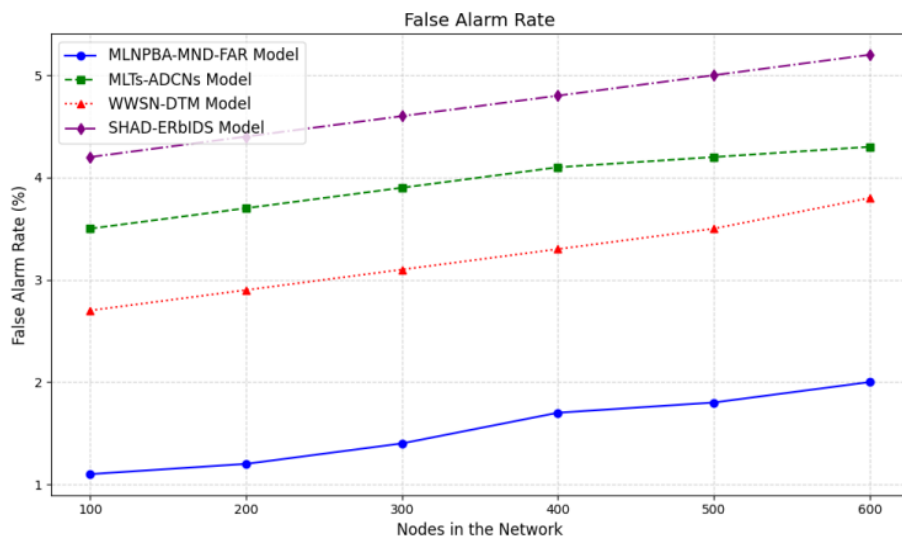


Figure 5. False alarm rate

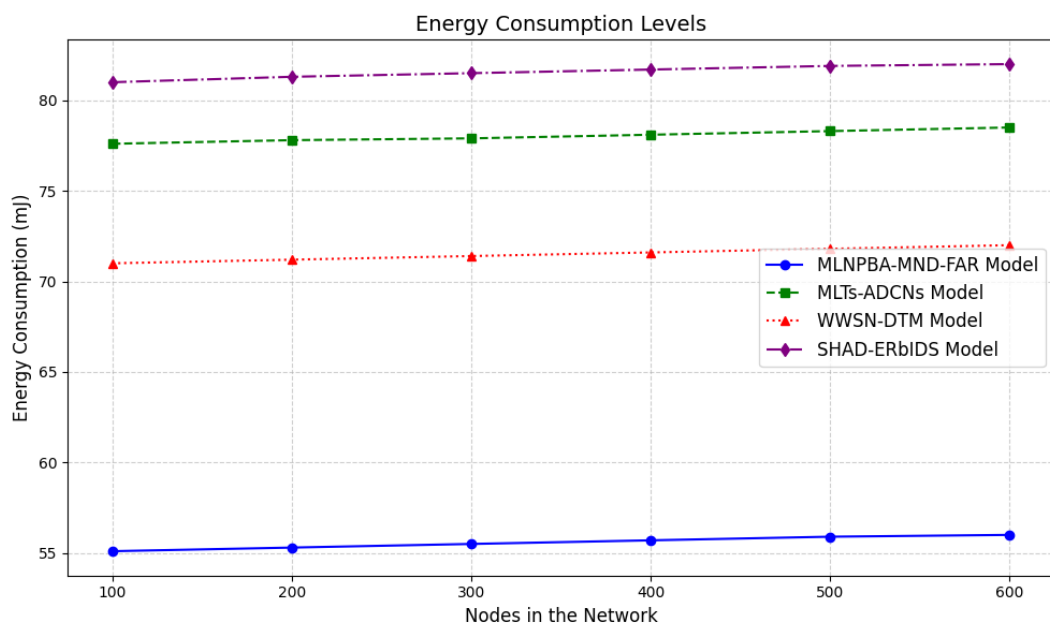


Figure 6. Energy consumption levels

Table 3. Energy consumption levels

Nodes in the Network	Models Considered			
	MLNPBA-MND-FAR Model	MLTs-ADCNs Model	WWSN-DTM Model	SHAD-ERbIDS Model
100	55.1	77.6	71.0	81.0
200	55.3	77.8	71.2	81.3
300	55.5	77.9	71.4	81.5
400	55.7	78.1	71.6	81.7
500	55.9	78.3	71.8	81.9
600	56	78.5	72	82

Table 4. Efficiency levels

Nodes in the Network	Models Considered			
	MLNPBA-MND-FAR Model	MLTs-ADCNs Model	WWSN-DTM Model	SHAD-ERbIDS Model
100	97.9	93.2	94.4	92.6
200	98.0	93.4	94.6	92.8
300	98.2	93.6	94.8	93.1
400	98.4	93.8	95.1	93.3
500	98.6	94.0	95.3	93.5
600	98.8	94.2	95.5	93.7

4.2 Energy consumption and efficiency

Sensor node resource constraint makes energy efficiency a critical issue in WSNs. In order to calculate the energy consumption by the MLNPBA-MND-FAR model to detect the malicious nodes, the overall energy consumption for detecting malicious node will be evaluated and compared it with the traditional detection methods. This research findings indicates that the presented model allows to obtain considerable energy savings through regional detection, thus avoiding the high communication cost between the nodes. The average energy consumption of nodes in the MLNPBA-MND-FAR system was lower than that of the traditional detection schemes. The main reasons for this efficiency come from the dynamic threshold adjustment of the model, and the localized analysis of the network nodes as the adjustment of the thresholds in the

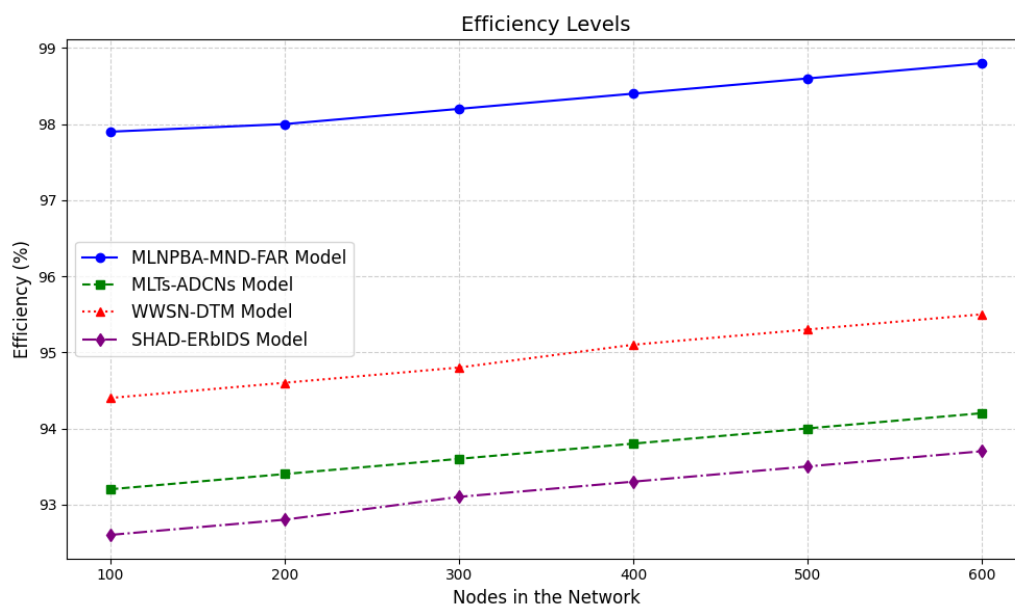
current context would lead to situations where the overhead of communication and computation is minimized. In addition, the machine learning-based behavior analysis operates in a lightweight manner, so the resources on the nodes are not overly taxed. The Table 3 and Figure 6 shows the Energy Consumption Levels and Table 4 and Figure 7 shows the Efficiency Levels.

On the other hand, conventional detection schemes using global communication for data aggregation and decision-making incur more energy consumption; this adversely affects the overall network lifetime. The energy savings in the MLNPBA-MND-FAR model have a particular significance when it comes to large-scale WSN since premature energy depletion can result in node failure, ultimately reducing the lifespan of the entire network.

4.3 Throughput and network performance

A second key metric for evaluating the model's impact on overall network performance is the throughput of the network. Packet drops, delays, and selective forwarding by a user can reduce throughput. Such a small proportion of data will be able to give many malicious nodes the ability to bow to such a bottleneck by either blocking or failing to relay data at the destination. This means that MLNPBA-MND-FAR model has a higher throughput than traditional detection methods. In cases where the model had to account for malicious nodes, the model still achieved an average throughput of 99.2% of the maximum achievable throughput in comparison with traditional methods (95.4%). Thus the proposed model efficiently allows quick isolation of disturbed nodes without impacting legitimate node communication with least packet loss.

The model enables dynamic tuning of detection thresholds, helping the model achieve constant throughput during different network conditions, like high traffic and node mobility. The localized detection method also bypasses the latency of global decision making, improving throughput even further. The throughput levels are shown in Table 5 and Figure 8.

**Figure 7.** Efficiency levels

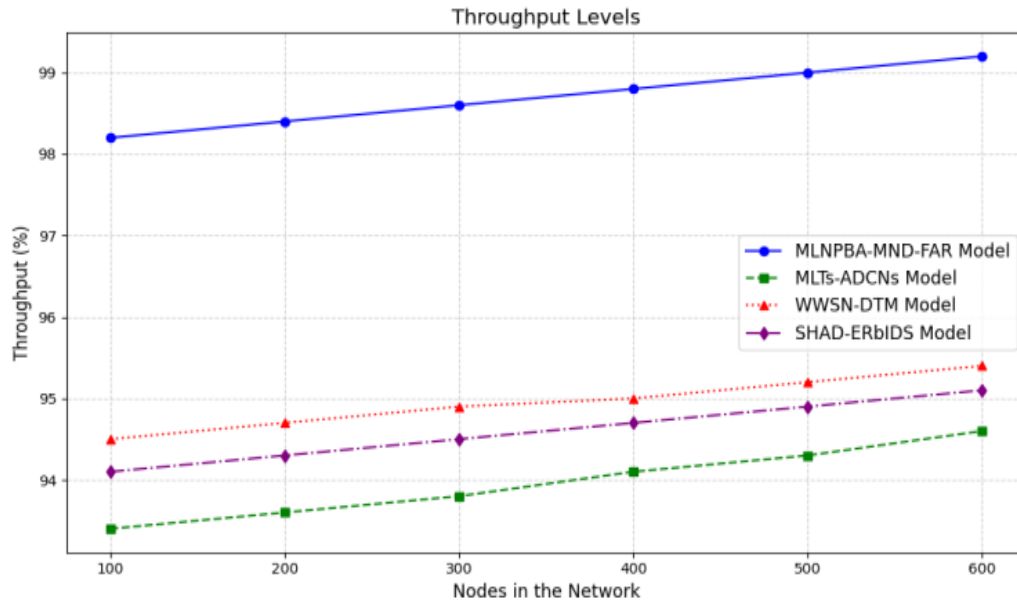


Figure 8. Throughput levels

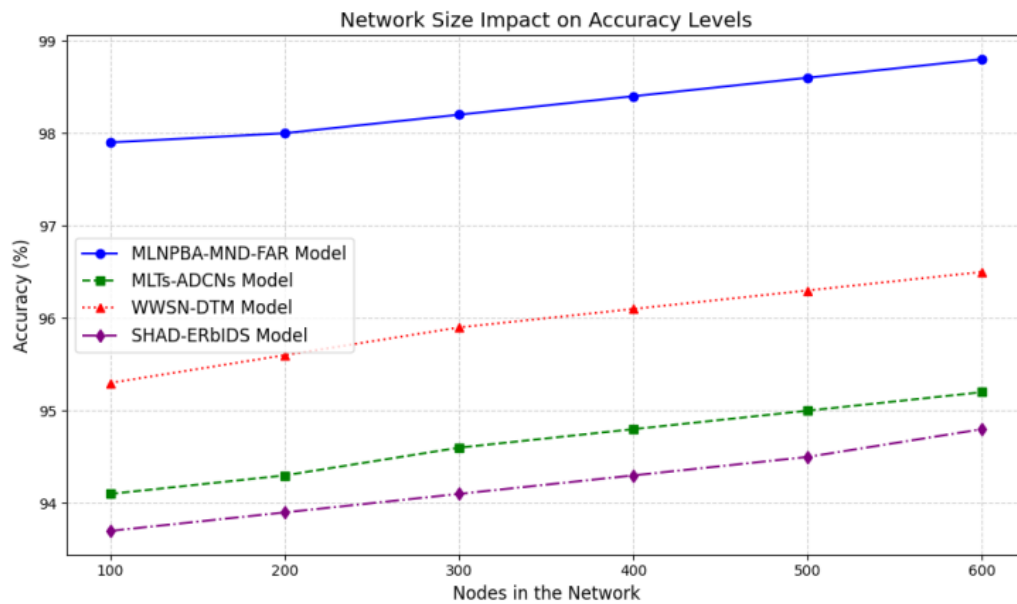


Figure 9. Network size impact accuracy levels

Table 5. Throughput levels

Nodes in the Network	Models Considered			
	MLNPBA-MND-FAR Model	MLTs-ADCNs Model	WWSN-DTM Model	SHAD-ERbIDS Model
100	98.2	93.4	94.5	94.1
200	98.4	93.6	94.7	94.3
300	98.6	93.8	94.9	94.5
400	98.8	94.1	95.0	94.7
500	99.0	94.3	95.2	94.9
600	99.2	94.6	95.4	95.1

4.4 Scalability and network size impact

Scalability plays an important role in implementing WSNs in large-scale systems. Experiments were performed to evaluate the scalability of the MLNPBA-MND-FAR model, with varying number of nodes in the networks with 100, 200,

300, 400, 500 and 600 nodes. The model was tested for its performance with increased size of the network. Indeed, the results show that as the network size increases, the MLNPBA-MND-FAR model scales well. The findings indicate that despite the exponential increase in the number of nodes in the network, the detection accuracy remained consistently high with an average detection accuracy of 98.7% for up to 600 nodes networks. The false alarm rate and energy consumption were also relatively stable, showing that the model can manage large-scale deployments without significantly degrading performance. This stems directly from the localized detection mechanism of the model, which minimizes global communication and computational overhead, ensuring that the detection process does not become a bottleneck as the network grows. Conversely, traditional approaches, especially those that depended on centralized or global data aggregation, exhibited a significant drop in performance as the network size increased. These approaches drawbacks were increased

communication overhead which results in higher energy consumption, reduced throughput and rise in the detection failure. The Table 6 and Figure 9 represent the Network Size Impact Accuracy Levels.

Table 6. Network size impact accuracy levels

Nodes in the Network	Models Considered			
	MLNPBA-MND-FAR Model	MLTs-ADCNs Model	WWSN-DTM Model	SHAD-ERbIDS Model
100	97.9	94.1	95.3	93.7
200	98.0	94.3	95.6	93.9
300	98.2	94.6	95.9	94.1
400	98.4	94.8	96.1	94.3
500	98.6	95.0	96.3	94.5
600	98.8	95.2	96.5	94.8

4.5 Comparison with existing techniques

The performance of the proposed model is compared with the state-of-the-art malicious node detection techniques. They comprise conventional threshold-based approaches, behavior-based models, and hybrid models incorporating detection and mitigation techniques. Across several important metrics, the proposed MLNPBA-MND-FAR model outperformed these existing methods. Notably, the proposed method achieved better detection accuracy (98.7%) than traditional models (94.8%). Furthermore, the model showed a significantly lower false alarm rate, energy consumption, and communication overhead, which results in improved network performance and reliability.

The MLNPBA-MND-FAR model in the network state was relatively stable and substance at any attack rate and significantly increased the FDR compared to the other algorithms, showing the excellent aggregation. Packet transmission in traditional detection methods was delayed due to both false positive detection, which deem non-infected nodes as infected, and when benign nodes are unnecessarily isolated, in contrast, the proposed model has a dynamic adjustment mechanism.

The experimental analysis confirms that MLNPBA-MND-FAR model successfully yields an accurate, scalable, and energy-efficient MND for WSN. It provides superior detection rate and lower false alarm while network quality of service e.g., throughput and energy optimization is maintained even with malicious activity. With the advent of multi-level behavior analysis, update of machine learning techniques, dynamic threshold update and distributed detection, the proposed model is ideal for large scale real field used in WSN, making improved security performance at little performance cost.

5. CONCLUSION

In this research, a new method is proposed for Malicious Node Detection with False Alarm Reduction in WSNs using the Multi-Level Node Pattern and Behaviour Analysis (MLNPBA-MND-FAR) model. Widely used in many applications such as environmental monitoring, military surveillance and healthcare, WSNs are exposed to significant challenges concerning security due to malicious node attacks that compromise the integrity of network data and disrupt communication. Specifically, the idea was to introduce a more efficient and precise classifier for malicious nodes, meaning

that, while minimizing the false positive ratio, the computational cost and communication and energy overhead caused by traditional detection mechanisms will also be lowered. By implementing a combination of behaviors analysis using multiple layers of analysis, pattern recognition and adaptive thresholds for petit and reactive invention during its detection activity, proposed model terrestrial saves common issues of current detection techniques including high false positive and high consumption of resources. While this solution utilized a multi-level approach to identify threats at different stages of the network's operation, the real-time adjustment of detection thresholds allowed the detection mechanism to adapt according to the true state of the network, preventing false positives. The localized detection process of the model dramatically decreased energy consumption and communication overhead, thus it is highly applicable to large-scale, battery-powered sensor networks. The experiment results indicated that the detection accuracy, false alarm rate and energy efficiency of the MLNPBA-MND-FAR model was significantly superior to the existing tradition methods. The model referred to could detect 98.7% of anomalies, with a decrease in false alarm rates and with less energy consumption than traditional methods. The network throughput was also substantial even in the face of the attack and the model was scaled to perform considerably with the increase of the network size thus applicable to both small- and large-scale WSNs deployment. Therefore, the proposed model gives a good opportunity for improving WSNs security and performance, because malicious nodes are identified and isolated accurately and quickly to avoid the componentous routing service degradation. MLNPBA-MND-FAR model is a solution that can be used in a wide range of practical applications where WSNs are used for critical data collection in remote/vulnerable environmental conditions. Further research may investigate the implementation of more sophisticated machine learning methods, including deep learning or reinforcement learning, to enhance detection performance and adaptability in evolving environments. Overall, the proposed MLNPBA-MND-FAR mechanism provides strong, efficient, and scalable protection for WSNs against malicious nodes attacks, enabling sensor networks to achieve high-quality and reliable data transmission, enhance system reliability, and prolong the upstream/server lifetime in practical field applications.

5.1 Limitations

The fact that the model is only tested in a virtual setting is a major drawback. While the simulation environment does let manage things like node activity, power consumption, and attack scenarios, it can't compare to the variety and unpredictability of actual WSN deployments. Outside of the scope of the paper's modeling efforts, real-world scenarios include environmental disruptions, hardware failures, unreliable communication lines, and physical manipulation of sensor nodes. As a result, the model's performance and applicability outside of the lab may suffer. The emphasis on static WSN topologies is another drawback. While running, the model presumes the network structure and node placements won't change. When it comes to mobile applications like environmental monitoring, disaster response, or vehicle networks, on the other hand, many contemporary sensor networks are dynamic. The model may not be applicable in certain situations due to the fact that mobility is

not taken into account.

The approach isn't designed to counter particular kinds of attacks like Sybil, blackhole, or wormhole assaults. However, it fails to pinpoint the origin or type of attack; all it does is notice abnormalities in node behavior. Advanced security management in WSNs relies on attack classification and response planning, neither of which are supported by this general approach, despite its usefulness for anomaly detection. While the dynamic thresholding approach does a good job of lowering false alarm rates, it does so at the expense of some processing cost. Continuous behavior score evaluation and threshold adjustment may affect energy consumption and real-time reaction capabilities in large-scale WSNs with resource-constrained nodes.

5.2 Future scope

There are a number of potential enhancements that could be considered. To begin, the model's viability and ability to be fine-tuned under real-world operating circumstances can be confirmed by deploying it on actual WSN testbeds or hardware emulators. Two, the framework is extensible, so it can accommodate heterogeneous sensor networks that are mobile and have nodes whose behavior changes more frequently. Adding attack classification algorithms that may differentiate between various forms of attacks and suggest appropriate mitigation tactics is another possible enhancement. For ever-changing threats in particular, machine learning models such as federated learning architectures or recurrent neural networks (RNNs) could improve learning and adaptation.

REFERENCES

- [1] Sadia, H., Farhan, S., Haq, Y.U., Sana, R., Mahmood, T., Bahaj, S.A.O., Khan, A.R. (2024). Intrusion detection system for wireless sensor networks: A machine learning based approach. *IEEE Access*, 12: 52565-52582. <https://doi.org/10.1109/ACCESS.2024.3380014>
- [2] Miranda, C., Kaddoum, G., Bou-Harb, E., Garg, S., Kaur, K. (2020). A collaborative security framework for software-defined wireless sensor networks. *IEEE Transactions on Information Forensics and Security*, 15: 2602-2615. <https://doi.org/10.1109/TIFS.2020.2973875>
- [3] Olewi, H.W., Mhawi, D.N., Al-Rawashidy, H. (2022). MLTs-ADCNs: Machine learning techniques for anomaly detection in communication networks. *IEEE Access*, 10: 91006-91017. <https://doi.org/10.1109/ACCESS.2022.3201869>
- [4] Kumar, M., Mukherjee, P., Verma, K., Verma, S., Rawat, D.B. (2021). Improved deep convolutional neural network based malicious node detection and energy-efficient data transmission in wireless sensor networks. *IEEE Transactions on Network Science and Engineering*, 9(5): 3272-3281. <https://doi.org/10.1109/TNSE.2021.3098011>
- [5] Nouman, M., Qasim, U., Nasir, H., Almasoud, A., Imran, M., Javaid, N. (2023). Malicious node detection using machine learning and distributed data storage using blockchain in WSNs. *IEEE Access*, 11: 6106-6121. <https://doi.org/10.1109/ACCESS.2023.3236983>
- [6] Wang, C., Liu, G., Jiang, T. (2024). Malicious node detection in wireless weak-link sensor networks using dynamic trust management. *IEEE Transactions on Mobile Computing*, 23(12): 12866-12877. <https://doi.org/10.1109/TMC.2024.3418826>
- [7] Ramasamy, L.K., KP, F.K., Imoize, A.L., Ogbebor, J.O., Kadry, S., Rho, S. (2021). Blockchain-based wireless sensor networks for malicious node detection: A survey. *IEEE Access*, 9: 128765-128785. <https://doi.org/10.1109/ACCESS.2021.3111923>
- [8] Mohammed, F.A.B.A., Mekky, N.E., Soliman, H., Hikal, N.A. (2024). Sinkhole attack detection by enhanced reputation-based intrusion detection system. *IEEE Access*, 12: 86985-86996. <https://doi.org/10.1109/ACCESS.2024.3416270>
- [9] Reddy, D.M.K., Sathya, R., Lakshmi, Y.V.A.S. (2023). An investigative study on different security aspects of wireless sensor networks. In *International Conference on Hybrid Intelligent Systems*, pp. 438-446. https://doi.org/10.1007/978-3-031-78931-1_45
- [10] Wang, N., Zhang, S., Zhang, Z., Qiao, J., Fu, J., Liu, J., Bhargava, B.K. (2023). Lightweight and secure data transmission scheme against malicious nodes in heterogeneous wireless sensor networks. *IEEE Transactions on Information Forensics and Security*, 18: 4652-4667. <https://doi.org/10.1109/TIFS.2023.3297904>
- [11] Ding, J., Wang, H., Wu, Y. (2022). The detection scheme against selective forwarding of smart malicious nodes with reinforcement learning in wireless sensor networks. *IEEE Sensors Journal*, 22(13): 13696-13706. <https://doi.org/10.1109/JSEN.2022.3176462>
- [12] Nirmala, B.V., Selvaraj, K. (2025). Malicious node detection in wireless sensor network using modified sandpiper optimization algorithm. *Wireless Networks*, 31(2): 1095-1116. <https://doi.org/10.1007/s11276-024-03806-1>
- [13] Pang, B., Teng, Z., Sun, H., Du, C., Li, M., Zhu, W. (2021). A malicious node detection strategy based on fuzzy trust model and the ABC algorithm in wireless sensor network. *IEEE Wireless Communications Letters*, 10(8): 1613-1617. <https://doi.org/10.1109/LWC.2021.3070630>
- [14] Narayana, V.L., Midhunchakkaravarthy, D. (2020). A trust based efficient blockchain linked routing method for improving security in mobile ad hoc networks. *International Journal of Safety and Security Engineering*, 10(4): 509-516.
- [15] Althunibat, S., Antonopoulos, A., Kartsakli, E., Granelli, F., Verikoukis, C. (2016). Countering intelligent-dependent malicious nodes in target detection wireless sensor networks. *IEEE Sensors Journal*, 16(23): 8627-8639. <https://doi.org/10.1109/JSEN.2016.2606759>
- [16] Sajjad, S.M., Bouk, S.H., Yousaf, M. (2015). Neighbor node trust based intrusion detection system for WSN. *Procedia Computer Science*, 63: 183-188. <https://doi.org/10.1016/j.procs.2015.08.331>
- [17] Santhosh Kumar, S.V.N., Palanichamy, Y. (2018). Energy efficient and secured distributed data dissemination using hop by hop authentication in WSN. *Wireless Networks*, 24: 1343-1360. <https://doi.org/10.1007/s11276-017-1549-3>
- [18] Narayana, V.L., Midhunchakkaravarthy, D. (2020). A time interval based blockchain model for detection of malicious nodes in manet using network block monitoring node. In *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, Coimbatore, India, pp. 852-857.

- <https://doi.org/10.1109/ICIRCA48905.2020.9183256>
- [19] Mehetre, D.C., Roslin, S.E., Wagh, S.J. (2019). Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust. *Cluster Computing*, 22(Suppl 1): 1313-1328. <https://doi.org/10.1007/s10586-017-1622-9>
- [20] Chuang, Y.T. (2017). Protecting against malicious and selective forwarding attacks for P2P search & retrieval system. *Peer-to-Peer Networking and Applications*, 10: 1079-1100. <https://doi.org/10.1007/s12083-016-0500-1>
- [21] Riecker, M., Biedermann, S., El Bansarkhani, R., Hollick, M. (2015). Lightweight energy consumption-based intrusion detection system for wireless sensor networks. *International Journal of Information Security*, 14(2): 155-167. <https://doi.org/10.1007/s10207-014-0241-1>
- [22] Umarani, C., Kannan, S. (2020). Intrusion detection system using hybrid tissue growing algorithm for wireless sensor network. *Peer-to-Peer Networking and Applications*, 13(3): 752-761. <https://doi.org/10.1007/s12083-019-00781-9>
- [23] Gomathy, V., Padhy, N., Samanta, D., Sivaram, M., Jain, V., Amiri, I.S. (2020). Malicious node detection using heterogeneous cluster based secure routing protocol (HCBS) in wireless adhoc sensor networks. *Journal of Ambient Intelligence and Humanized Computing*, 11(11): 4995-5001. <https://doi.org/10.1007/s12652-020-01797-3>
- [24] Rajeshkumar, G., Valluvan, K.R. (2017). An energy aware trust based intrusion detection system with adaptive acknowledgement for wireless sensor network. *Wireless Personal Communications*, 94: 1993-2007. <https://doi.org/10.1007/s11277-016-3349-y>
- [25] Dharini, N., Duraipandian, N., Katiravan, J. (2020). ELPC-trust framework for wireless sensor networks. *Wireless Personal Communications*, 113: 1709-1742. <https://doi.org/10.1007/s11277-020-07288-0>
- [26] Verma, A., Ranga, V. (2019). Evaluation of network intrusion detection systems for RPL based 6LoWPAN networks in IoT. *Wireless Personal Communications*, 108: 1571-1594. <https://doi.org/10.1007/s11277-019-06485-w>
- [27] Gomathi, S., Gopala Krishnan, C. (2020). Malicious node detection in wireless sensor networks using an efficient secure data aggregation protocol. *Wireless Personal Communications*, 113(4): 1775-1790. <https://doi.org/10.1007/s11277-020-07291-5>
- [28] Ahmed, A., Abu Bakar, K., Channa, M. I., Haseeb, K., Khan, A.W. (2015). A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks. *Frontiers of Computer Science*, 9: 280-296. <https://doi.org/10.1007/s11704-014-4212-5>
- [29] Selvi, M., Thangaramya, K., Ganapathy, S., Kulothungan, K., Khannah Nehemiah, H., Kannan, A. (2019). An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks. *Wireless Personal Communications*, 105: 1475-1490. <https://doi.org/10.1007/s11277-019-06155-x>