SCIENTIFIC CULTURE
www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 1.1, (2026), pp. 4189-4205
Open Access. Online & Print

DOI: 10.5281/zenodo. 121126311

SECURE AND ROBUST WSN ARCHITECTURE: DETECTION OF MALICIOUS NODES AND IMPACT ASSESSMENT ON LINK STABILITY

Priyanka Sharma[1]*, Mohd Suhaib Kidwai[2], Piyush Charan[3]

[1,2]ECE Department, Integral University Lucknow, UP, India.
[3]ECE Department, Manav Rachna University, Faridabad, Haryana, India.

Received: 01/12/2025
Accepted: 02/01/2026

Corresponding author: Priyanka Sharma
(priyanka.sh30@gmail.com)

ABSTRACT

Wireless Sensor Networks (WSNs) have become a core technology for modern applications, including surveillance, smart agriculture, and Internet of Things (IoTs) ecosystems, but they remain highly vulnerable to malicious nodes that compromise link reliability and communication performance. Conventional anomaly detection and cryptographic approaches are often inadequate due to the resource limitations of sensor nodes and the dynamic nature of network topologies. This study aims to design a secure and robust detection framework that accurately identifies malicious nodes while maintaining link stability. The paper proposes a hybrid model integrating federated Graph Convolutional Networks (GCN) for spatial learning and Long Short-Term Memory (LSTM) networks for temporal sequence analysis, combined with Q learning for self-healing routing. The methodology uses the WSN BFSF dataset with multi-domain feature extraction across traffic, energy, topology, and storage, class balancing with SMOTE, and feature selection through mutual information. Experimental validation using NS3 simulations demonstrates a classification accuracy of 99.70 percent with precision, recall, and F1 scores exceeding 0.996 for all classes. Link stability also improved significantly, with packet delivery ratio rising from 0.57 to 1.0 and average delay reduced from 3.32 to 3.09 units. The findings confirm that the proposed framework enhances both the detection of malicious activity and the resilience of wireless sensor networks in real-world scenarios.

KEYWORDS: Wireless Sensor Networks, Internet of Things, Malicious nodes, Link stability, Graph Convolutional Networks, Long Short-Term Memory, Q learning, SMOTE.

1. INTRODUCTION

The importance of WSNs has increased in many modern environments, such as in military surveillance, urban planning systems, farming with precision, and the infrastructure supporting the Internet of Things (IoT) (Trigka and Dristas 2025; Charan et al., 2017). Their inherent capabilities for distributed sensing, localized computation, and wireless communication enable seamless, real-time collection of data and decision-making across vast and diverse environments (Ashfaq and Nur (2024). By deploying sensor nodes in remote, hazardous, or infrastructure-deficient areas, WSNs provide scalable and cost-effective solutions for continuous monitoring and control. This adaptability, coupled with their ability to operate autonomously, has positioned WSNs as a foundational technology in domains where reliability, responsiveness, and resilience are critical (Bajwa, (2022). Figure 1 shows the basic diagram representation of the WSN.

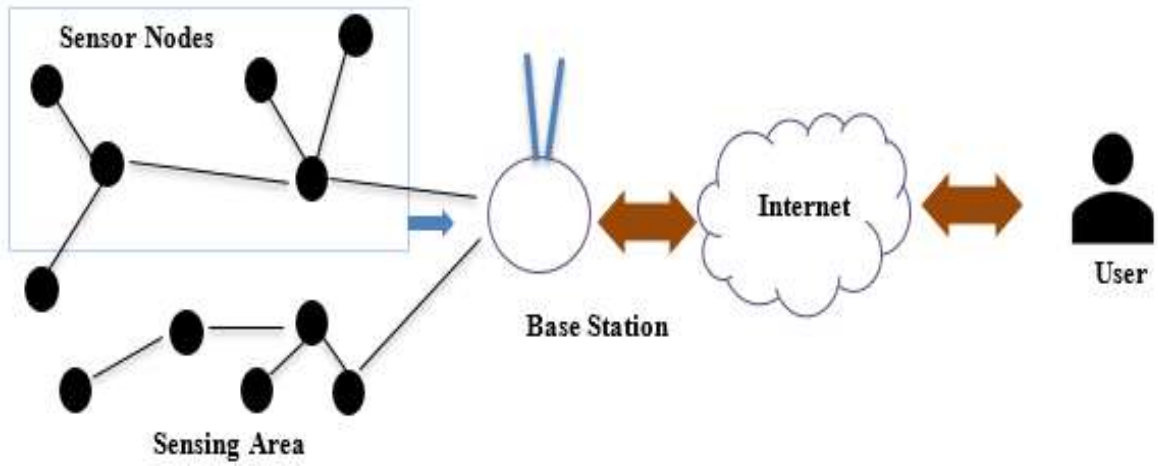

Figure 1: Basic Representation of WSN (Naik and Murugan., 2018)

At the same time, several advantages of WSNs also introduce significant security challenges. Malicious nodes can be added into the network through compromised hardware or external attackers, severely impacting the integrity of data, reliability of communication, and overall network performance (Oztoprak et al., 2024; Charan et al., 2016). Although several trust-based routing and anomaly detection techniques have been proposed, adversarial nodes often blend in with valid traffic patterns, making accurate detection increasingly difficult (Ahmadi and Javidan 2024; Che et al., 2022). Many studies have emphasized the need for lightweight and adaptive intrusion systems, as conventional cryptographic techniques tend to exceed the resource boundaries of sensor nodes (Shamsuzzaman et al., 2025; Zadeh).

Detecting malicious nodes remains a persistent challenge because sensor nodes operate under severe resource constraints, including limited energy, processing capacity, memory, and communication bandwidth (Ahmad et al., 2022; Waisi and Ali 2023). In addition, the highly dynamic nature of many WSN deployments due to energy depletion, node mobility, or topology changes further complicates the problem of malicious node detection (Ramasamy et al., 2021; Priyadarshi 2025; Vishwas and Ramesh., 2025). These nodes can mimic normal behavior or inject subtle alarms over time, evading detection by both signature-based and rule-based systems (Alzaabi and Mehmood., 2024; Zhang). Anomaly-based detection offers flexibility and the ability to catch unidentified attacks but often suffers from high false positive rates in critical infrastructure scenarios (Jeffrey and Villar., 2023; khalaf et al 2025; EI Shayed et al 2022).

In addition to security threats, maintaining link stability is equally important for reliable WSN operations. Link instability caused by malicious behavior or environmental fluctuations can degrade routing performance, increase energy consumption, and reduce the accuracy and timeliness of data delivery (Hasan and Zurina., 2023; Priyadarshi et al 2025; Almutairi and Zhang., 2024). For instance, unstable or compromised links may lead to frequent retransmissions, increased latency, rapid battery drain, and reduced delivery ratio, factors that can severely limit the usefulness of WSNs (Kianejad; Pandey; Adu-Manu., 2022). Recent work has highlighted link quality metrics such as expected transmission count and centrality measures as key indicators of network stability and resilience (Wen and Dargie., 2021; Megzari et al., 2025; Wan et al., 2021).

This work aims to design a framework for the detection of malicious nodes and impact assessment on link stability in a secure and robust WSN architecture. The objective is to create a lightweight detection model that integrates trust and entropy-based metrics, assess the impact of malicious activity on link performance, and propose architectural solutions for self-healing. The scope covers detection, trust evaluation, link stability analysis, and simulation-driven performance validation. The contributions of this research are as follows:

1. Proposed a federated GCN and LSTM-based hybrid detection framework that is lightweight, privacy-preserving, and suitable for deployment in resource-constrained wireless sensor networks.
2. Introduced a multi-domain feature extraction approach that leverages traffic behavior, energy consumption, topological structure, and memory characteristics to enhance the detection of complex malicious behaviors.
3. Employed mutual information for feature selection and integrated Q-learning-based self-healing routing to isolate malicious nodes and restore stable communication paths dynamically.
4. Incorporated entropy-based and statistical metrics such as link entropy, hop count variance, and packet retention score to quantify the impact of attacks on link stability and network performance.
5. Validated the proposed model through simulation and digital twin environments using the WSN-BFSF dataset and NS3 tool, ensuring the robustness and real-world applicability of the framework.

This research enhances the security and resilience of wireless sensor networks by enabling accurate, decentralized detection of malicious nodes using federated learning. It further ensures reliable communication through self-healing routing and link stability assessment under real-world attack scenarios.

The structure of the paper is as follows. The first section reviews related work on malicious node detection, trust models, and link stability analysis. The second section describes in detail the proposed framework, including the detection mechanism, trust and entropy metrics, and self-healing architecture.

2. RELATED WORK

Recent research on WSNs has focused on enhancing intrusion detection accuracy, reducing false alarms, and ensuring efficient resource usage. This review of the literature focused on advancing Intrusion Detection Systems (IDS) for WSNs through machine learning, deep learning, and optimization methods. Al Sukkar and Al-Sharaeh (2025). developed an ensemble machine learning framework combining logistic regression, decision trees, KNN, SVM, and gradient boosting to detect DoS attacks using the WSN-DS and WSN-BFSF datasets, achieving peak accuracies of 98.12% for soft voting. Aruna, Orchu (2025). proposed the Multi-Level Node Pattern and Behaviour Analysis for Malicious Node Detection with False Alarm Reduction (MLNPBA-MND-FAR) technique, utilizing multi-level behavioral analysis for malicious node detection, demonstrating a detection accuracy of 98.7% and a low false alarm rate of 1.1% across varying network sizes. Sriraghavendra et al. (2025). introduced a knowledge-enhanced hybrid DNN–KAN model, integrating domain knowledge through graph embeddings and leveraging Kolmogorov-Arnold theorem-based layers, which achieved 99.87% accuracy and 0.9985 ROC-AUC while significantly reducing false positives.

To enhance WSN security, Yang et al. (2024). proposed the Energy-Efficient Opportunistic Routing Scheme for Sustainable WSNs (EDSSR) protocol, a secured energy-efficient opportunistic routing scheme that updates neighbor information and validates routing parameters while being power-aware. Compared to DLAMD and EEFCR, EDSSR improved throughput by 2–3%, reduced energy consumption and end-to-end delay, and increased malware detection rate by 23%. Soni et al. (2024). addressed class imbalance in intrusion detection by applying the Synthetic Minority Over-sampling Technique (SMOTE) on the WSN-BFSF dataset. They evaluated XGBoost, Random Forest, CatBoost, and MLP, showing accuracy improvement by 3.97% and F1-score by up to 9.12% due to balanced learning. Nguyen et al. (2024). introduced GSWO-CatBoost, a novel feature selection and hyperparameter optimization by a hybrid technique combining Genetic Algorithm and Whale Optimization Algorithm for intrusion detection, achieving real-time detection with high accuracy on the WSN-BFSF dataset and reducing inference time nearly 100x compared to deep learning models. Zubair et al. (2024). proposed an explainable ensemble learning model for detecting malicious sensor node activity using a hybrid data balancing method (cluster-based under-sampling +

SMOTE), achieving 99.7% accuracy and identifying critical features through explainability analysis, thus enhancing the interpretability and robustness of the framework.

To address energy inefficiency and packet loss in WSNs, Dener et al. (2023). proposed the WSN-BFSF dataset simulating Blackhole, Flooding, and Selective Forwarding attacks in NS-2, processed it for compatibility with ML/DL models, and evaluated it using Random Forest, Decision Tree, Naive Bayes, Logistic Regression, and eight deep learning models including CNN, LSTM, GRU, and hybrid variants, achieving the highest accuracy of 99.92% with Random Forest and CNN-GRU models. JOHN et al. (2023). developed a hybrid intrusion detection system for Wireless Multimedia Sensor Networks combining a Convolutional Neural Network with Random Forest, using the WSN-DS dataset to identify Blackhole and Wormhole attacks, resulting in detection accuracies up to 99% and highlighting efficiency in both attack mitigation and forwarding optimization despite noting limitations in energy consumption analysis. Lai et al. (2022). introduced a correlation-based detection mechanism leveraging temporal, spatial, and event correlations to identify false data injection (FDI) attacks in WSNs, utilizing DDF-2 filtering for anomaly prediction, AdaBoost-enhanced spatial correlation for robustness, and event validation at the gateway level, achieving superior recall and lower false positive and false negative rates than traditional fuzzy reputation and trust-based models.

Despite significant developments in intrusion detection systems for WSNs, several key research gaps remain unaddressed. First, many recent models achieve extremely high accuracy using ensemble or optimized techniques but overlook model generalizability across unseen WSN topologies and environmental conditions (Al Sukkar and Al-Sharaeh.,2025; Aruna et al., 2025; SriRaghavendra et al., 2025; Yang et al., 2024; Soni et al., 2024; Nguyen et al., 2024). Second, some research incorporates data balancing and explainability, and a few studies explore real-time adaptability of detection systems under resource-constrained conditions (Aruna et al., 2025; Zubie et al.,2024). Third, most works emphasize performance metrics but provide limited insight into energy consumption or the tradeoff between detection accuracy and power efficiency (SriRaghavendra et al., 2025; John et al., 2023). Lastly, protocols like EDSSR improve routing and security together. Yet, there is still insufficient integration between energy-aware routing strategies and intelligent intrusion detection frameworks, leaving a gap in unified, cross-layer security solutions for WSNs (Yang et al., 2024). To overcome these gaps, this research proposed a malicious node detection method by using advanced techniques.

3. RESEARCH METHODOLOGY

In this section, the proposed methodology for detecting malicious nodes and evaluating their impact on link stability in wireless sensor networks is presented using a federated GCN and LSTM-based hybrid model. The process begins with data preprocessing, class balancing using SMOTE, and the extraction of multi-domain features related to traffic, energy, topology, and memory behavior. Mutual information is applied for feature selection, and data is partitioned for federated training. Each node trains a local GCN and LSTM model, capturing spatial and temporal patterns, respectively, with global updates performed via federated averaging. Malicious nodes are isolated, and routing is restored through a self-healing Q learning mechanism. The complete system is validated through simulation using NS3 and evaluated using classification and link stability metrics to ensure robustness and real-world applicability. Figure 2 shows the architecture of the proposed methodology.

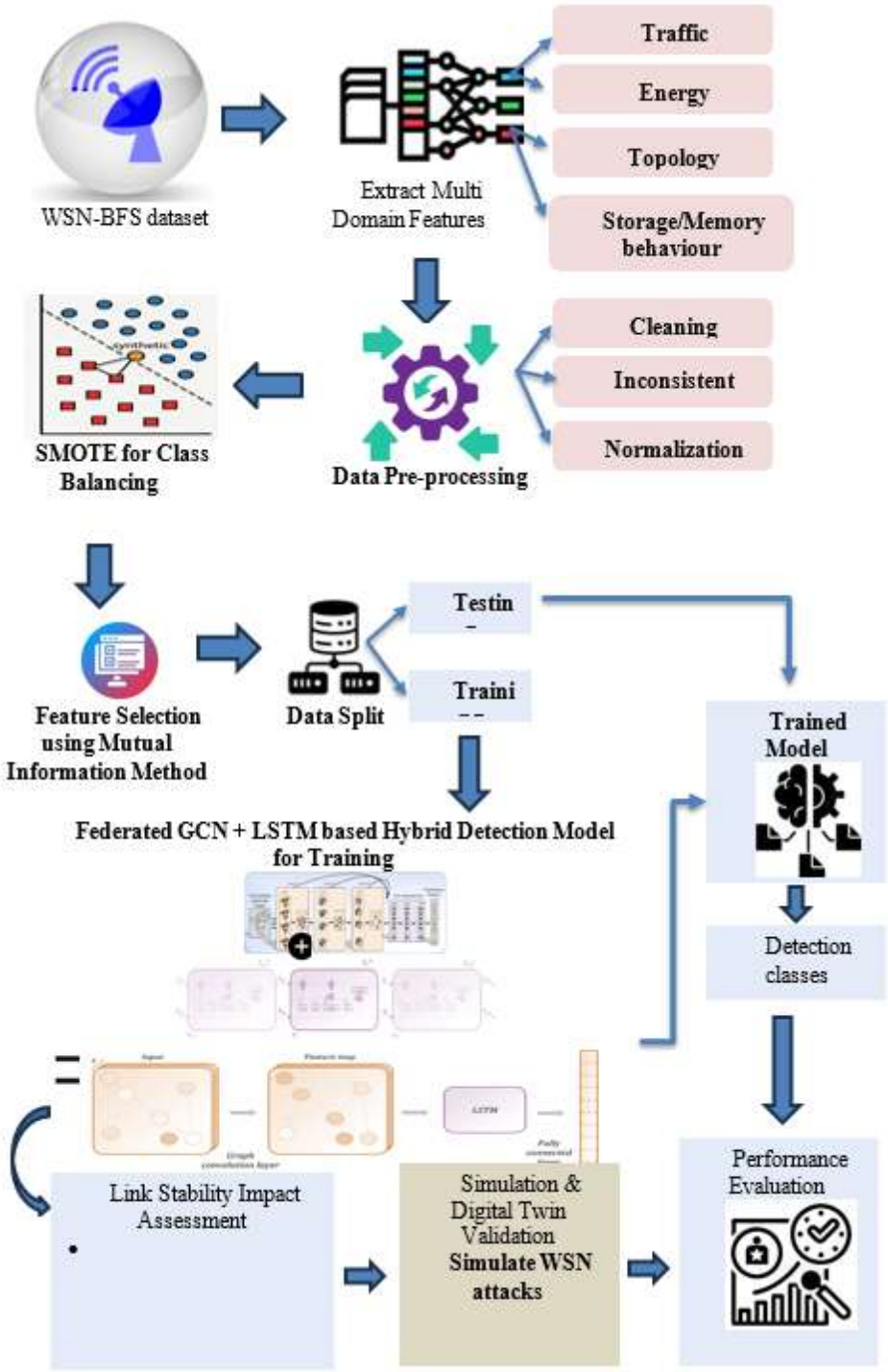

Figure 2: Proposed Methodology

3.1. Dataset and Multi-Domain Feature Extraction

The WSN-BFSF dataset (Okur and Celik., 2023). available freely on Kaggle, is a benchmark dataset developed for detecting network-layer attacks in WSNs, specifically targeting flooding, blackhole, and selective forwarding behaviors. It contains over 312,000 instances and 16 raw features, comprising event timestamp, type, source and destination node IDs, hop count, packet size, and remaining energy. These attributes enable both attack detection and behavior analysis. From this data, multi-domain features are extracted across traffic behavior, energy usage, network topology, and storage/memory behavior by enabling accurate detection of malicious nodes and analysis of their impact on link stability. Table 1 presents the WSN-BFSF dataset attributes with their description properly.

Table 1: Dataset Attributes

S.No.	Attribute Name	Description
1	Time	Timestamp of packet generation or event occurrence
2	Source_ID	ID of the source node generating the packet
3	Destination_ID	ID of the intended recipient node
4	Packet_Type	Type of packet (e.g., data, acknowledgment, control)
5	Remaining_Energy	Remaining energy of the node at the time of transmission
6	Packet_Size	Size of the packet in bytes
7	Hop_Count	The number of hops the packet has traveled so far
8	Event_Type	Event label (e.g., normal, blackhole, flooding, selective_forwarding)
9	Forward_Node_ID	ID of the node forwarding the packet
10	Dropped_Packet	Boolean or count indicating if a packet was dropped
11	Retransmission_Count	Number of times the packet was retransmitted (if applicable)
12	RSSI	Received Signal Strength Indicator of the packet (optional)
13	LQI	Link Quality Indicator for the transmission (optional)
14	TTL	Time-To-Live field showing remaining transmission allowance
15	MAC_Layer_Delay	Delay introduced at the MAC layer before transmission (optional)
16	Network_Condition	Simulated network status or noise level (if available)

3.2. Data Preprocessing

Data preprocessing in this methodology involves preparing the WSN-BFSF dataset for effective malicious node detection by ensuring data consistency, quality, and standardization. The process begins with cleaning the dataset by removing duplicate entries, correcting inconsistent records, and handling missing or undefined values. Categorical variables such as packet types or event classes are encoded numerically. In contrast, continuous variables like packet size, hop count, and remaining energy are standardized using normalization Min-Max scaling techniques to ensure uniform feature ranges (Aleisa., 2025). The calculation of Min-Max Scaling is performed using:

$$X_{scaled} = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (1)$$

Where X shows the original feature value and X_{max} , X_{min} presents the maximum and minimum values of the feature. This step ensures that all input features are in a suitable format for models, enhancing convergence and detection accuracy.

3.3. SMOTE for Class Balancing

SMOTE is a widely used data balancing technique that addresses class imbalance in classification and detection tasks by synthetically producing new instances of the minority class rather than simply duplicating existing ones (Talukder et al., 2024). In this work, SMOTE is used to enhance classifier performance and even out the dataset for the WSN-BFSF dataset, which has an imbalance between regular traffic and attack classes like blackholes and floods. Synthetic samples are created using line segments that link to a minority class sample. x_i to one of its k-nearest neighbors x_{nn} in the feature space. The synthetic sample x_{new} is computed as:

$$x_{new} = x_i + \lambda \cdot (x_{nn} - x_i) \quad (2)$$

Where $\lambda \in [0,1]$ is a random number that controls how close the new sample is to x_i.

3.4. Feature Selection Using MI Method

MI is a metric of statistical significance that is employed to choose the feature. It measures the amount of data that one variable (the feature) offers about another variable (usually the class label) (Fatima et al., 2024; Al-Sarem., 2021). In the context of malicious node detection using the WSN-BFSF dataset, MI helps identify the most informative features (such as packet size, hop count, energy levels, etc.) that have the strongest dependency on the target classes (e.g., normal, blackhole, flooding, selective forwarding). This agrees with the removal of redundant features, thereby improving the performance of the detection model. MI between a class label Y and feature X is defined as:

$$I(X;Y) = \sum_{x \in X} \sum_{y \in Y} p(x,y) \cdot log\left(\frac{p(x,y)}{p(x) \cdot p(y)}\right) \quad (3)$$

Where p(x,y) is the combined probability division of X and Y, and p(x) and p(y) are the marginal probabilities of X and Y, respectively. In algorithm 1, the MI algorithm is used to define the redundancy penalty between features.

Algorithm 1: MI-Based Feature Selection Algorithm
Input:
F← initial set of all n original features, S← empty set
Output: Top-k selected features S
for i = 1; i ≤ n; i++ do
calculate H(Y), H(Xi), H(Y, Xi), and I(Y; Xi)
end for
select the feature $f^+ \in F$ that maximizes I (Y; Xi)
F ← F Thank you for reaching out. {f^+} and S ← S ∪ {f^+}
for f ∈ F and s ∈ S do
compute I (f; s) and I (Y; s)
end for
while |S| < k do
select the feature $f^+ \in F$ that maximizes:
I (Y; f) − (1/ |S|) ∑ {s ∈ S} I (f; s)
F ← F \ {f^+} and S ← S ∪ {f^+}
if F ≠ ∅ then
for $f_1 \in F$ and $s_1 \in S$ do
compute I (f_1; s_1) and I (Y; s_1)
end for
end if
end while

Feature relevancy for detection increases as MI scores rise, as they indicate a greater link between the feature and the class. Data sets for training and testing are created from the characteristics that are chosen throughout this procedure. Next, the model is instructed to train the suggested hybrid model using the training set.

3.5. Federated GCN (Graph Convolutional Network)

A Federated Graph Convolutional Network (Federated GCN) enables decentralized training of GCN models across distributed nodes or clusters without sharing raw data (Yao et al., 2023; Amjath et al., 2025). In this research for malicious node detection in WSNs, where node data is graph-structured (e.g., routing paths, neighbor relationships), GCN is used to capture spatial dependencies by aggregating information from neighboring nodes. In a federated setup, each local node trains a GCN using its neighborhood data and only shares updated model parameters with a central server for aggregation, preserving data privacy and reducing overhead communication. The GCN layer equation for a single layer is:

$$H^{(l+1)} = \sigma\left(\widetilde{D}^{-\frac{1}{2}}\widetilde{A}\widetilde{D}^{-\frac{1}{2}}H^{(l)}W^{(l)}\right) \quad (4)$$

Where:
- σ is a non-linear activation function (e.g., ReLU).
- $\widetilde{A} = A + I$ is the adjacency matrix with self-connections.
- $\widetilde{D}$ is the diagonal degree matrix of $\widetilde{A}$.
- $H^{(l)}$ is the input at layer l, $W^{(l)}$ is the trainable weight matrix.

3.6. LSTM

LSTMs are a type of recurrent neural network that are great for simulating the time-dependent activities of sensor nodes, including their energy consumption or packet forwarding history, since they can learn persistent dependencies in sequential data (Malashin et al., 2024; Salmi and lachen., 2022). In this research on the malicious node detection process, LSTM tracks temporal changes in node metrics to identify abnormal patterns over time. An LSTM cell preserves a cell state C_t and a hidden state h_t, updated through three gates:

Forget Gate – Chooses which information to abandon from the cell state:

$$f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f) \quad (5)$$

Input Gate – Decides which new information to include:

$$i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i) \quad (6)$$

$$\tilde{C}_t = tanh\,(W_C \cdot [h_{t-1}, x_t] + b_C) \quad (7)$$

Cell State Update – Updates the cell state:

$$C_t = f_t \cdot C_{t-1} + it \cdot \tilde{C}_t \quad (8)$$

Output Gate – Decides what to output:

$$o_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o), \quad h_t = o_t \cdot tanh\,(C_t) \quad (9)$$

Where:
- W_o, b_o = weight matrices and bias vectors learned during training
- C_t = cell state at time t
- x_t = input at time step t
- h_t = hidden state at time t
- σ = sigmoid activation function

3.7. Federated GCN + LSTM-based Hybrid Model for Training and Detection

The **hybrid model** combines GCN (spatial analysis) and LSTM (temporal behavior) in a **federated framework**. Each node trains locally on its own graph and time-series data, and only model weights are shared for aggregation. This enables accurate and privacy-preserving detection of complex attacks (e.g., blackhole, flooding) while minimizing communication overhead.

After processing spatial and temporal features independently:

$$Z = Concat(h_{GCN}, h_{LSTM}) \quad (10)$$

Where h_{GCN} is a Graph-encoded representation, h_{LSTM} is sequence-encoded behavior, and Z is the final combined feature vector for detection. After local training, global parameters θ are updated as:

$$\theta = \sum_{i=1}^{N} \frac{n_i}{n} \cdot \theta_i \quad (11)$$

Where θ_i shows parameters from local model i, and n_i presents the number of samples at node i, $n = \sum n_i$is the total number of participating nodes is shown by N. The combined vector Z is passed through a classifier (e.g., softmax layer):

$$\hat{y} = softmax(W_z Z + b_z) \quad (12)$$

Where W_z and b_z are weights and bias of the final classification layer and predicted class (e.g., normal, blackhole, flooding) are shown by $\hat{y}$. Algorithm 2 is followed for this hybrid model:

Algorithm 2: Model Training (Federated GCN + LSTM)

For round r = 1 to R do:
For each node i = 1 to N in parallel:
Train a local GCN on spatial graph data from D_i:
H_GCN = GCN(X_i, A_i)
Train a local LSTM on time-series features from D_i:
H_LSTM = LSTM(X_i^t)
Concatenate outputs: Z_i = Concat(H_GCN, H_LSTM)
Compute gradients and update local weights θ_i
Server aggregates weights:
$\theta_{global} = \sum (n_i / n) * \theta_i$ (FedAvg)
Send θ_{global} to all nodes.

3.8. Link Stability Impact Assessment

Link Stability Impact Assessment in the proposed methodology involves evaluating how malicious node activity, such as blackhole, flooding, and selective forwarding attacks, affects the reliability and performance of communication links within the WSN (Alansari et al., 2023). After detecting malicious nodes using the hybrid federated GCN + LSTM model, key metrics are computed to quantify link degradation. The key metrices are as follows:

Link Entropy measures randomness or unpredictability in routing paths by using:

$$H = -\sum_{i=1}^{n} p_i \cdot \log_2(p_i) \quad (13)$$

Packet Retention Score (PRS) indicates the proportion of successfully delivered packets:

$$PRS_i = \frac{P_{delivered,i}}{P_{sent,i}} \quad (14)$$

Hop Count Variance reflects route instability caused by compromised nodes.

$$HCV_i = \frac{1}{n_i} \sum_{j=1}^{n_i} \left(h_{ij} - \bar{h}_i\right)^2 \quad (15)$$

By comparing these metrics before and after detection, the model assesses the severity of disruption caused by attacks. This analysis not only confirms the impact of malicious behavior on network topology and data flow but also guides trust-based self-healing mechanisms to restore optimal routing and maintain overall network stability.

3.9. Self-Healing Routing via Q-Learning

Self-Healing Routing via Q-Learning is the final corrective phase in the proposed methodology, designed to restore network functionality after detecting malicious nodes (Adeniyi et al., 2023). Once a node is flagged as malicious through the federated GCN + LSTM detection framework and its trust score falls below a defined threshold, it is excluded from routing paths. The network then dynamically reconfigures routes using Q-learning, enabling each node to learn the optimal forwarding decisions through interaction with the environment (Premakumari et al., 2025). In the proposed methodology, each node treats routing as a decision-making problem, where the Q-value denotes the anticipated cumulative reward for selecting a neighbor as the next hop. The Q-values are updated using the Bellman equation:

$$Q(s,a) \leftarrow Q(s,a) + \alpha[r + \gamma \cdot \max_{a'} Q(s',a') - Q(s,a)] \quad (16)$$

Where s is the current state (node), a is the selected action (next hop), r is the reward (e.g., successful packet delivery), α is the learning rate, and γ is the discount factor. Over time, nodes learn to prefer stable, high-trust neighbors, enabling the network to autonomously bypass compromised areas and recover its routing efficiency without centralized intervention. This self-healing mechanism enhances the robustness and resilience of WSNs under dynamic attack conditions.

3.10. Simulation & Digital Twin Validation

The final phase involves quantitative performance evaluation of the entire system, validating both malicious node detection accuracy and network stability recovery. Performance is measured using standard classification metrics to assess detection effectiveness, and network-level metrics to assess link reliability post-recovery.

$$Accuracy = \frac{TP+TN}{T\,P+TN+FP+FN} \quad (17)$$

$$Precision = \frac{TP}{TP+FP} \quad (18)$$

$$Recall = \frac{TP}{TP+FN} \quad (19)$$

$$F1 = 2 \times \frac{Precision \times Recall}{Precision+Recall} \quad (20)$$

$$PDR = \frac{Total\ packets\ received}{Total\ packets\ sent} \quad (21)$$

$$Delay = \frac{\sum_{i=1}^{n}(t_{i,received} - t_{i,sent})}{n} \quad (22)$$

4. RESULTS AND DISCUSSION

This section evaluates how well the proposed model performs in detecting malicious nodes and maintaining link stability, using simulation results and comparisons with standard methods. The proposed Federated GCN-LSTM model was evaluated using the WSN-BFSF dataset (312,106 instances) under simulated blackhole, flooding, and selective forwarding attacks. Experiments were conducted in NS-3 with federated training across 50–300 nodes. Each node trained a local GCN and LSTM using a batch size of 128, a learning rate of 0.001, and an Adam optimizer for 100 rounds.

In this research, the dataset goes through several stages to assess the proposed model. Firstly, the WSN-BFS dataset is read with no missing values across any of its 18 columns, ensuring clean and consistent data for modeling. Table 2 shows the feature distribution for each class.

Table 2: Feature Distribution

Class	Count	Percentage (%)
Normal	262,851	84.22
Flooding	29,844	9.56
Blackhole	11,766	3.77
Forwarding	7,645	2.45
Total	312,106	100.00

After this, multi-domain features are extracted across traffic behavior, energy usage, network topology, and storage/memory behavior as shown in Figure 3. After applying multi-domain feature extraction, distinct behavioral patterns emerged across traffic, energy, topology, and storage metrics. Flooding has the highest packet rate with a median of around 18, while others ranged from 8 to 9. Remaining energy was highest for normal nodes at 0.78, followed by flooding at 0.75, forwarding at 0.73, and blackhole at 0.70. Flooding also had a higher node degree with a median of 6, while others stayed near 4. Retransmissions peaked in forwarding attacks with a median of 2.5, compared to normal nodes under 1. These variations clearly support the use of these extracted features for precise identification of attack behavior and system anomalies.

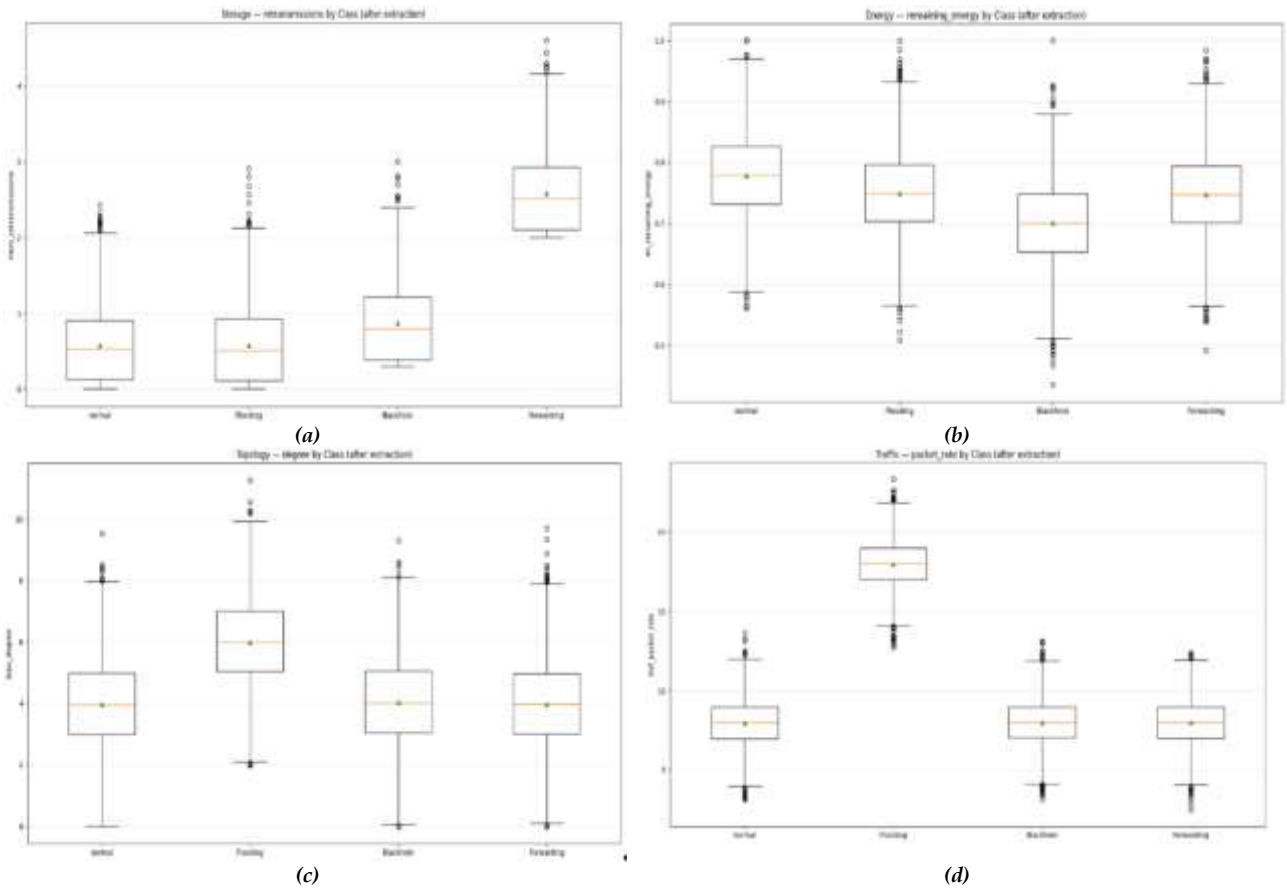

Figure 3: Multi-domain feature extraction

Figure 4 highlights the normalized mean behavior of each class across traffic, energy, topology, and storage domains. Flooding shows the highest traffic and energy values around 0.72 and 0.78, respectively, while forwarding records the highest storage near 0.52. Normal and blackhole remain close in topology and storage around 0.42 and 0.28. These patterns confirm domain-level differences, guiding the selection of relevant features for accurate detection in the next training stage.

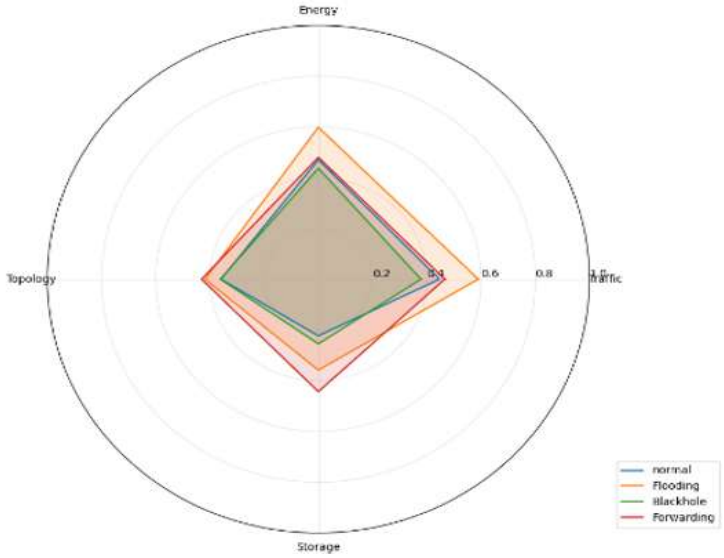

Figure 4: Domain-level profile per class (Normalized Means)

After extracting these features, the data is cleaned by removing duplicates, correcting inconsistencies, and handling missing values. By following preprocessing, the data is balanced into classes by using SMOTE to enhance classifier performance and even out the data for the WSN-BFSF dataset, which

has an imbalance between regular traffic and attack classes like blackholes and floods. To address the class imbalance seen in the original distribution, where normal samples dominated at 84 percent while attack classes remained below 10 percent, SMOTE was applied during preprocessing. This synthetic oversampling balanced all classes to exactly 210280 instances each, ensuring equal representation as shown in Table 3. This step prepares the dataset for unbiased model training by preventing dominance of the normal class and improving detection accuracy across all attack types.

Table 3: Class balancing before and after SMOTE

Class	Before Count	Original (%)	After SMOTE Count
Normal	262,851	84.22%	210,280
Flooding	29,844	9.56%	210,280
Blackhole	11,766	3.77%	210,280
Forwarding	7,645	2.45%	210,280

After applying SMOTE for class balancing, the next step involved selecting the most informative features for training, as shown in Figure 5. The first chart ranks the top 10 multi-domain features using mutual information, where mem_retransmissions scored highest at 0.67, followed by traf_packet_rate at 0.58 and en_drain_rate at 0.46, indicating strong relevance in detecting abnormal behavior. In parallel, the second chart shows the top basic features selected by relative importance, with node_id and s_node both scoring above 1.0, followed by time at 0.94 and source_ip_port and rest_energy near 0.75. These selected features together capture both advanced and foundational patterns in traffic, energy, and topology, preparing the data for effective model learning.

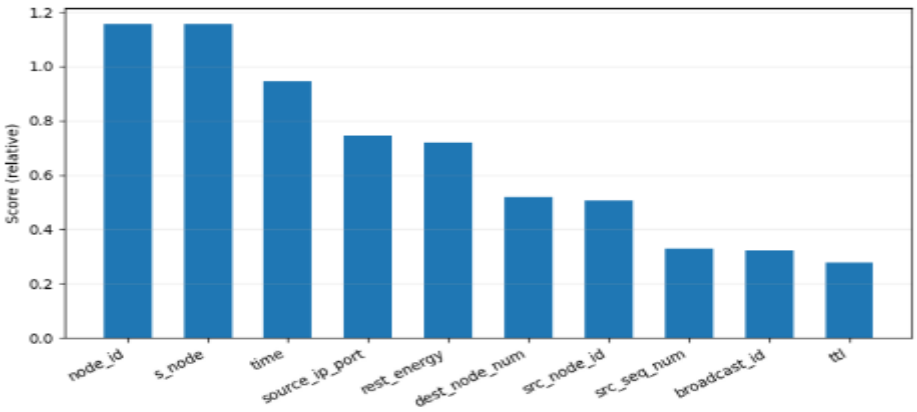

Figure 5: Top 10 selected features

After selecting the most relevant features, the dataset was split into a 70 to 30 ratio, assigning 24738 samples for training and 6185 for testing. The hybrid detection model based on federated GCN and LSTM is then trained. The confusion matrix shows strong classification, with 588 flooding and 153 forwarding instances correctly identified (see Figure 6). However, 493 normal samples were misclassified as blackhole, while 4322 were correctly predicted.

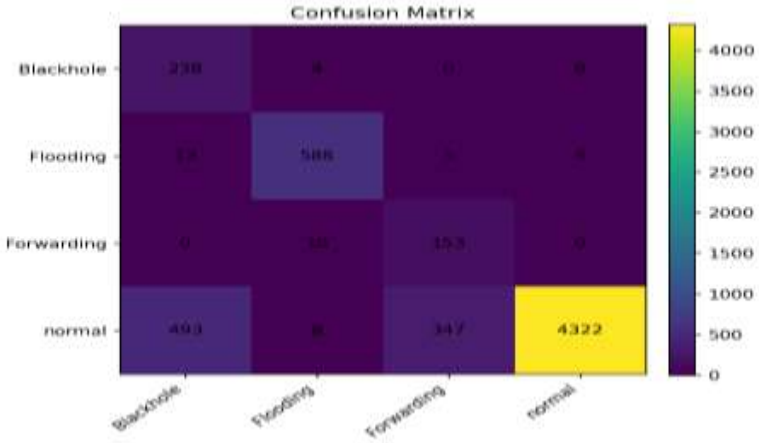

Figure 6: Confusion matrix of GCN+LSTM model

Training and validation accuracy improved steadily, reaching 99.58 percent by epoch 20 as depicted in Figure 7. Correspondingly, the training loss decreased from over 0.9 to nearly 0.01, while validation loss dropped from 1.1 to around 0.04. These results confirm that the model learned effectively and generalized well across all classes.

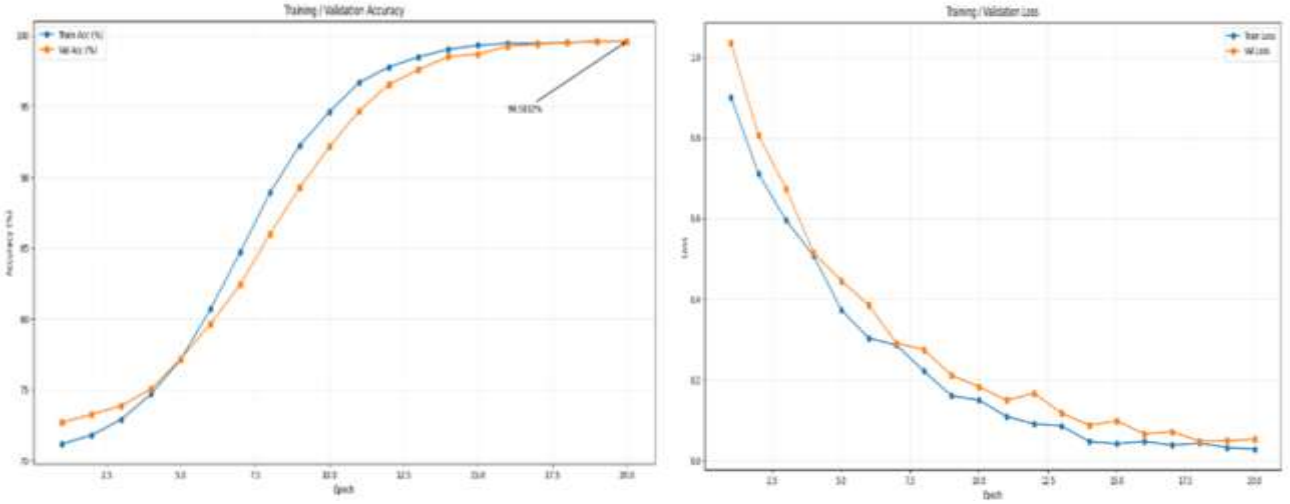

Figure 7: Training accuracy, Val accuracy, and training loss and Val loss

The classification report shows excellent performance of the trained federated GCN plus LSTM model across all four classes, as depicted in Table 4. Precision, recall, and F1-scores are consistently high, ranging between 0.9961 and 0.9977 for each class. Specifically, the normal and forwarding classes achieved the highest F1-scores of 0.9973 and 0.9972, respectively, indicating accurate and balanced detection. Each class had 70093 samples, ensuring a fair evaluation. The overall model accuracy is 99.70 percent, with both macro and weighted averages matching this score. These metrics confirm the model's strong generalization, low error rate, and reliability across imbalanced network attack scenarios.

Table 3: Class balancing before and after SMOTE

Class	Precision	Recall	F1-Score	Support
Blackhole	0.9961	0.9970	0.9965	70,093
Flooding	0.9965	0.9970	0.9967	70,093
Forwarding	0.9975	0.9970	0.9972	70,093
Normal	0.9977	0.9970	0.9973	70,093
Metric	Value		Support	
Accuracy	0.9970		280,372	
Macro Avg	0.9970		280,372	
Weighted Avg	0.9970		280,372	

After detecting malicious nodes using the hybrid federated GCN + LSTM model, key metrics are computed to quantify link degradation. The link stability impact assessment and digital twin validation were carried out using the NS3 simulation tool. Malicious nodes identified by the federated GCN LSTM model were isolated, and the routing table was reinforced through Q learning to restore stable communication. The performance graphs, as shown in Figure 8, clearly show improvement after detection and isolation: the packet delivery ratio increased sharply from about 0.6 to nearly 1.0 (Figure 8 (a)), while the average delay, which earlier peaked above 4.5 units, dropped and stabilized around 3.0 units (Figure 8 (b)). The average node energy showed a natural decline but remained more stable after isolation (Figure 8 (c)), and the mean link entropy reduced from 0.6 to approximately 0.4, reflecting stronger and more consistent connections (Figure 8 (d)). Similarly, hop count variance, which earlier spiked above 5, stabilized closer to 3, confirming efficient path selection (Figure 8 (e).

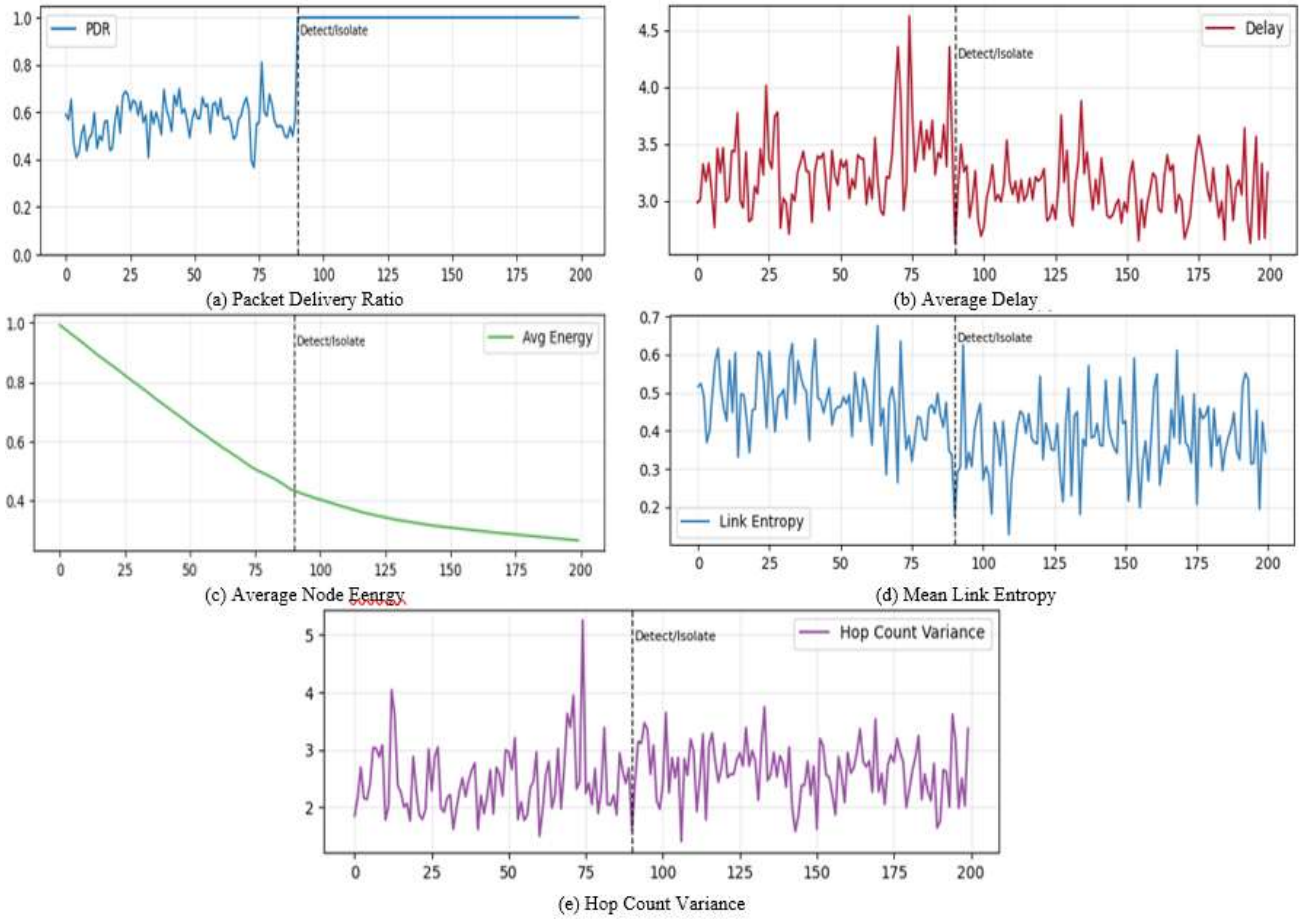

Figure 8: Analysis of link stability impact assessment

The topology plots further illustrate this effect before isolation, blackhole, flooding, and forwarding attacks disrupted the routes, while after isolation, as shown in Figure 9. The network recovered with only normal nodes active and stable self-healing routes established.

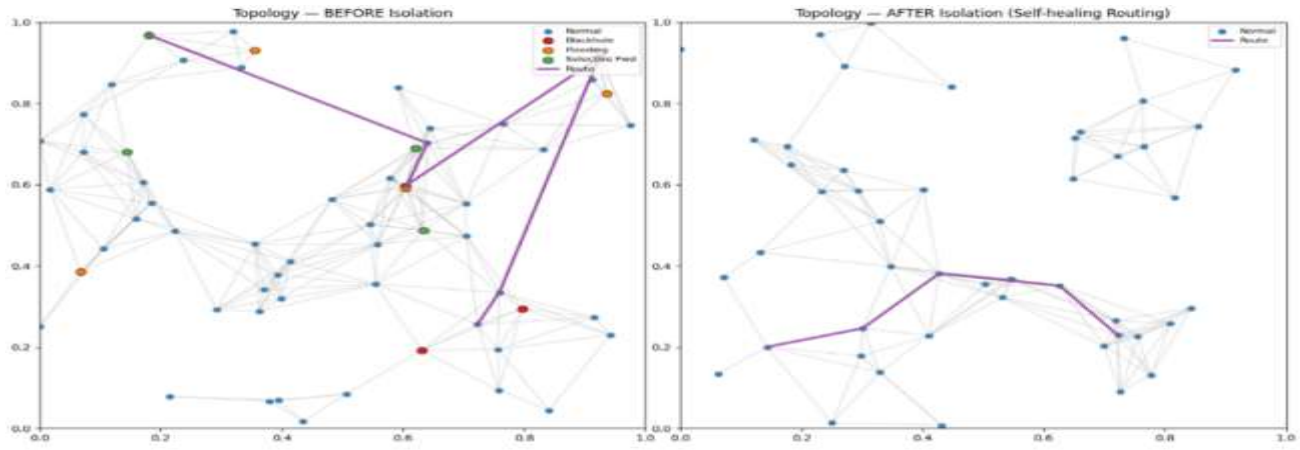

Figure 9: Before and after isolation of topology using NS3

These NS3-based simulation results validate that the integration of GCN+LSTM detection with Q learning routing ensures resilient and stable WSN operation under attack conditions.

The summary metrics before and after isolation highlight the overall network improvement achieved through the NS3 simulation, as shown in Figure 10. The packet delivery ratio increased from 0.57 to 1.0, showing reliable data transmission once malicious nodes were removed. The average delay decreased from 3.32 units to 3.09 units, confirming faster communication. Energy consumption dropped from

0.70 to 0.32, indicating more efficient use of resources. Link entropy reduced from 0.48 to 0.37, reflecting higher link stability. Finally, hop count variance rose slightly from 2.46 to 2.63, suggesting the routes were slightly longer but more stable.

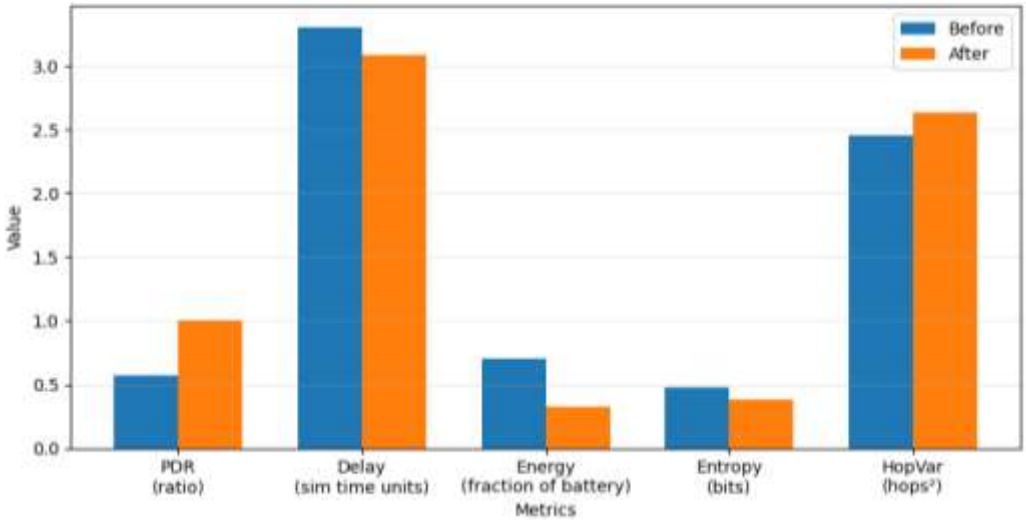

Figure 10: Before vs After Isolation

These metrics confirm that isolating malicious nodes and applying Q learning based routing reinforced stability and efficiency in the wireless sensor network.

4.1. Link Stability Impact Assessment

The comparison of different models on the WSN BFSF dataset highlights a clear progression in performance as techniques evolved from traditional machine learning to advanced hybrid deep learning as shown in Table 5. In the study by Al Sukkar and Al Sharaeh (2025) [31], classical models such as logistic regression, decision trees, KNN, SVM, and gradient boosting achieved an accuracy of 98.12 percent, which established a reliable baseline but struggled to capture the complex spatial and temporal dynamics of malicious activities in wireless sensor networks. Soni et al. (2024) [35] advanced the performance further by employing CatBoost, a gradient boosting algorithm well-suited for categorical features and resistant to overfitting, achieved 99.5 percent accuracy, and demonstrated the effectiveness of ensemble-based models in handling large-scale WSN traffic. Dener et al. (2023) [38] explored GRU algorithms, leveraging their ability to capture sequential patterns and temporal dependencies in traffic data, and obtained an accuracy of 99.02 percent, showing that recurrent models could enhance learning in scenarios where node behaviors evolve. Despite their strengths, these approaches still faced challenges in modeling both the spatial interactions among nodes and the temporal sequence of events in a unified framework. To address this gap, the proposed federated GCN LSTM hybrid model not only provided a comprehensive view of network activity but also integrated federated learning to maintain data privacy and improve generalization across distributed environments.

Table 5: Class balancing before and after SMOTE

Authors	Models	Dataset	Accuracy
Al Sukkar and Al-Sharaeh (2025) [31]	Logistic regression, Decision trees, KNN, SVM, and Gradient boosting	WSN-BFSF	98.12%
Soni et al. (2024) [35]	CatBoost	WSN-BFSF	99.5%
Dener et al. (2023) [38]	GRU Algorithms	WSN-BFSF	99.02%
Proposed Models	Federated GCN+LSTM Hybrid Model	WSN-BFSF	99.70%

As a result, the proposed model outperformed all prior approaches with an accuracy of 99.70 percent, proving its ability to deliver highly reliable detection and robust defense against a wide range of attacks. This comparison emphasizes that while traditional models laid the groundwork, hybrid spatial-temporal deep learning with federated strategies sets a new benchmark for security in wireless sensor networks.

5. CONCLUSION AND FUTURE WORK

This research concludes that the integration of federated GCNs with LSTM networks, combined with multi-domain feature extraction, provides an effective solution for detecting malicious nodes in wireless sensor networks. In addition, the use of Q learning based self-healing routing further enhances

link stability and strengthens overall network performance. The proposed model reached an accuracy of 99.70 percent with precision, recall, and F1 scores above 0.996 for all classes. Stability metrics also showed clear improvement, with the packet delivery ratio increasing from 0.57 to 1.0 and the average delay decreasing from 3.32 to 3.09 units. These results confirm that the framework ensures reliable intrusion detection while maintaining energy efficiency and communication resilience. Validation through NS3 simulations and digital twin environments further proved its practical effectiveness. For future work, the framework can be tested under high mobility and larger-scale scenarios to measure adaptability. Additional strategies for reducing energy consumption and communication overhead can also be explored. Adaptive federated learning methods can enhance scalability, while extending the model for cross-layer security and IoT applications can expand its usefulness in real-world environments.

REFERENCES

Abdelwahed, N. A. A. (2025). The predictive power of technology leadership and green HRM toward green innovation, work engagement and environmental performance. International Journal of Productivity and Performance Management, 74(6), 2159-2182.

Al Masri, R., and Wimanda, E. (2024). The role of green supply chain management in corporate sustainability performance. Journal of Energy and Environmental Policy Options, 7(2), 1-9.

Alfina, K. N., Ratnayake, R. C., Wibisono, D., Basri, M. H., and Mulyono, N. B. (2025). Prioritizing performance indicators for the circular economy transition in healthcare supply chains. Circular Economy and Sustainability, 5(1), 231-276.

Awad, I. M., Nuseibeh, H., and Amro, A. A. (2025). Competitiveness in the era of circular economy and digital innovations: An integrative literature review. Sustainability, 17(10), 4599.

Bag, S., and Rahman, M. S. (2024). Navigating circular economy: Unleashing the potential of political and supply chain analytics skills among top supply chain executives for environmental orientation, regenerative supply chain practices, and supply chain viability. Business Strategy and the Environment, 33(2), 504-528.

Bevere, D., and Faccilongo, N. (2024). Shaping the future of healthcare: Integrating ecology and digital innovation. Sustainability, 16(9), 3835.

Caldera, S., Hayes, S., Dawes, L., and Desha, C. (2022). Moving beyond business as usual toward regenerative business practice in small and medium-sized enterprises. Frontiers in Sustainability, 3, 799359.

Chansanguan, S., Rittippant, N., Ueki, Y., and Jeenanunta, C. (2025). Sustainable digital transformation in public hospitals: Strategic enablers for smart healthcare systems. Sustainability, 17(19), 8614.

Cheng, W., Li, Q., Wu, Q., Ye, F., and Jiang, Y. (2024). Digital capability and green innovation: The perspective of green supply chain collaboration and top management's environmental awareness. Heliyon, 10(11), e10921.

Chuah, C., Homer, S. T., and Loo, W. H. (2025). Mapping regenerative business: a conceptual framework building upon systems thinking in Southeast Asia, Asian Journal of Business Ethics, 1-29.

De Angelis, R. (2021). Circular economy and paradox theory: A business model perspective. Journal of Cleaner Production, 285, 124823.

Dohmen, A. E., Merrick, J. R., Saunders, L. W., Stank, T. P., and Goldsby, T. J. (2023). When preemptive risk mitigation is insufficient: The effectiveness of continuity and resilience techniques during COVID-19. Production and Operations Management, 32(5), 1529-1549.

Erbey, A., Gündüz, C., and Fidan, Ü. (2025). Digitalization, Sustainability, and Radical Innovation: A Knowledge-Based Approach. Sustainability, 17(7), 2972.

Gee, R. O. W. (2025). Greening the blue ocean: Leading systemic transformation with regenerative intelligence. Earth Environmental Science Research and Review, 8(1), 01-27.

Guenther, P., Guenther, M., Ringle, C. M., Zaefarian, G., and Cartwright, S. (2023). Improving PLS-SEM use for business marketing research. Industrial Marketing Management, 111, 127-142.

Hahn, T., and Tampe, M. (2021). Strategies for regenerative business. Strategic Organization, 19(3), 456-477.

Horn, E., and Proksch, G. (2022). Symbiotic and regenerative sustainability frameworks: Moving towards circular city implementation. Frontiers in Built Environment, 7, 780478.

Jum'a, L., Alkalha, Z., and Alaraj, M. (2024). Towards environmental sustainability: the nexus between green supply chain management, total quality management, and environmental management practices. International Journal of Quality and Reliability Management, 41(5), 1209-1234.

Kantur, D., and Say, A. I. (2015). Measuring organizational resilience: A scale development. Journal of Business Economics and Finance, 4(3), 1-20.

Kolodny-Goetz, J., Hamm, D. W., Cook, B. S., and Wandersman, A. (2021). The readiness, resilience and recovery tool: An emerging approach to enhance readiness amidst disruption. Global Implementation Research and Applications, 1(2), 135-146.

Kosolapova, N., Matveeva, L., Nikitaeva, A., and Chernova, O. (2023). The drivers of the circular economy: Theory vs practice. Terra Economicus, 21(2), 68-83.

Kristoffersen, E., Blomsma, F., Mikalef, P., and Li, J. (2020). The smart circular economy: A digital-enabled circular strategies framework for manufacturing companies. Journal of Business Research, 120, 241-261.

Lee, K. H., and Kim, J. W. (2011). Integrating suppliers into green product innovation development: An empirical case study in the semiconductor industry. Business strategy and the Environment, 20(8), 527-538.

Makhloufi, L. (2024). Do knowledge sharing and big data analytics capabilities matter for green absorptive capacity and green entrepreneurship orientation? Implications for green innovation. Industrial Management and Data Systems, 124(3), 978-1004.

Memon, M. A., Ramayah, T., Cheah, J. H., Ting, H., Chuah, F., and Cham, T. H. (2021). PLS-SEM statistical programs: A review. Journal of Applied Structural Equation Modeling, 5(1), 1-14.

Nie, C., Zhong, Z., and Feng, Y. (2023). Can digital infrastructure induce urban green innovation? New insights from China. Clean Technologies and Environmental Policy, 25(10), 3419-3436.

Paul, J., Ueno, A., Dennis, C., Alamanos, E., Curtis, L., Foroudi, P., ... and Wirtz, J. (2024). Digital transformation: A multidisciplinary perspective and future research agenda. International Journal of Consumer Studies, 48(2), e13015.

Pereira, N., and Fernandes, C. (2025). Knowledge management in health organizations: A systematic literature review. Journal of the Knowledge Economy, 1-73.

Rossi, L. A., and Srai, J. S. (2025). The role of digital technologies in configuring circular ecosystems. International Journal of Operations and Production Management, 45(4), 863-894.

Saleem, F., Sundarasen, S., and Malik, M. I. (2025). Green leadership and environmental performance in hospitals: A multi-mediator study. Sustainability, 17(12), 5376.

Sarstedt, M., Radomir, L., Moisescu, O. I., and Ringle, C. M. (2022). Latent class analysis in PLS-SEM: A review and recommendations for future applications. Journal of Business Research, 138, 398-407.

Sepetis, A., and Parlavantzas, I. (2025). Circular economy behavior and sustainable healthcare. Circular Economy and Sustainability, 1-23.

Shin, J., Mollah, M. A., and Choi, J. (2023). Sustainability and organizational performance in South Korea: The effect of digital leadership on digital culture and employees' digital capabilities. Sustainability, 15(3), 2027.

Siakas, D., Lampropoulos, G., Rahanu, H., Georgiadou, E., and Siakas, K. (2023). Emerging technologies enabling the transition toward a sustainable and circular economy: The 4R sustainability framework. In European conference on software process improvement (pp. 166-181). Cham: Springer Nature Switzerland.

Simion Luduşanu, D. G., Fertu, D. I., Tinică, G., and Gavrilescu, M. (2025). Integrated quality and environmental management in healthcare: Impacts, implementation, and future directions toward sustainability. Sustainability, 17(11), 5156.

Trần, T. H. T., Abu Afifa, M., Tran, N. K., and Dang, D. M. T. (2025). The role of green technology innovation and digital capability in sustainable management and performance: Empirical evidence. Meditari Accountancy Research, 1-20.

Ul-Durar, S., Awan, U., Varma, A., Memon, S., and Mention, A. L. (2023). Integrating knowledge management and orientation dynamics for organization transition from eco-innovation to circular economy. Journal of Knowledge Management, 27(8), 2217-2248.

Vishwakarma, L. P., Singh, R. K., Mishra, R., and Kumari, A. (2025). Application of artificial intelligence for resilient and sustainable healthcare system: Systematic literature review and future research directions. International Journal of Production Research, 63(2), 822-844.

Xu, J., Yu, Y., Zhang, M., and Zhang, J. Z. (2023). Impacts of digital transformation on eco-innovation and sustainable performance: Evidence from Chinese manufacturing companies. Journal of Cleaner Production, 393, 136278.

Yadav, V., and Yadav, N. (2024). Beyond sustainability, toward resilience, and regeneration: An integrative framework for archetypes of regenerative innovation. Global Journal of Flexible Systems Management, 25(4), 849-879.

Zhou, K., Warwick, E., Ucci, M., Davies, M., and Zimmermann, N. (2024). Sustaining attention to sustainability, health, and well-being in urban regeneration. Organization and Environment, 37(1), 57-83.