Threat Sync: A Collaborative Insider Threat and Malicious Domain Detection Framework Using Shared Intelligence

Rishitha Parankusham[1], T. Srilekha[2*]

[1]PG Student, [2]Assistant Professor, [1,2]Department of Computer Science and Engineering
[1,2]Vaagdevi Engineering College, Warangal, 506005, Telangana, India.
[1]rishithaparankusham@gmail.com, [2]srilekha.522@gmail.com
*Correspondence: T. Srilekha(srilekha.522@gmail.com)

ABSTRACT

Wireless Sensor Networks (WSNs) have emerged as a fundamental technology for enabling intelligent sensing, monitoring, and communication across a wide range of applications, including environmental monitoring, healthcare systems, industrial automation, military surveillance, and smart city infrastructures. Conventional routing attack detection mechanisms primarily rely on rule-based techniques or traditional machine learning approaches. Although these methods provide acceptable performance in controlled environments, they often struggle to capture complex communication patterns, adapt to dynamic network conditions, and offer transparent explanations for their predictions. To address these limitations, this research proposes an interpretable hybrid framework that integrates Recurrent Processing Networks (RPN) with Fast Interpretable Greedy-Tree Sums (FIGS) for intelligent routing attack detection and reliability estimation in Wireless Sensor Networks. The proposed framework adopts the 1 Classification and 2 Regression Tree (1CA2RT) methodology, where a single classification task is performed for Node Status prediction, while two regression tasks are utilized to estimate Reputation Score and Dynamic Trust Score. Initially, the WSN dataset undergoes comprehensive preprocessing, including data cleaning, feature selection, normalization, feature scaling, and exploratory data analysis to enhance data quality and improve model effectiveness. Subsequently, the extracted features are processed through the proposed RPN-FIGS framework to perform accurate classification and regression tasks. For performance evaluation, established machine learning algorithms such as K-Nearest Neighbors (KNN), Passive-Aggressive (PA), and Gradient Boosting (GB) are implemented as benchmark models for comparative analysis. Experimental results demonstrate that the proposed framework provides improved attack detection capability, reliable trust estimation, enhanced interpretability, and superior scalability. Consequently, the proposed RPN-FIGS model offers an effective and transparent solution for strengthening network security, improving communication reliability, and supporting intelligent decision-making in modern WSN environments.

Key words: Fast Interpretable Greedy-Tree Sums (FIGS), Recurrent Processing Networks (RPN), routing attack detection, trust estimation, Wireless Sensor Networks (WSNs).

1. INTRODUCTION

WSNs have emerged as a fundamental technology for modern intelligent systems, enabling continuous monitoring, automated control, and data-driven decision-making across a wide range of applications, including environmental monitoring, healthcare, industrial automation, military surveillance, and smart city infrastructures [1]. Despite these technological advancements, the deployment and management of sensor nodes remain major challenges in WSN design due to the heterogeneous and resource-constrained nature of the network. Sensor nodes differ in terms of energy availability, sensing capabilities, computational resources, transmission range [2], and communication power, making uniform deployment strategies difficult to

Doi:10.48047/ijiee.2026.16.2.52

implement effectively [3]. Furthermore, application-specific requirements often demand the simultaneous optimization of multiple performance objectives, including sensing coverage, network connectivity, energy efficiency, fault tolerance, communication reliability, and real-time data delivery [4].

These objectives frequently conflict with one another, requiring careful trade-offs during network planning and operation. For example, maximizing sensing coverage may increase energy consumption, while prioritizing energy conservation can adversely affect network responsiveness and communication quality.

.

Figure 1 illustrates a security threat scenario in an Internet of Things (IoT)-enabled WSN, where multiple sensor nodes communicate with a base station and IoT server through a sensor field connected to the IoT cloud. A malicious node, highlighted in red, infiltrates the network and positions itself along the communication path between legitimate sensor nodes and the target destination. The attacker attempts to compromise network operations by injecting false data, manipulating routing information, intercepting transmitted packets, or launching denial-of-service attacks

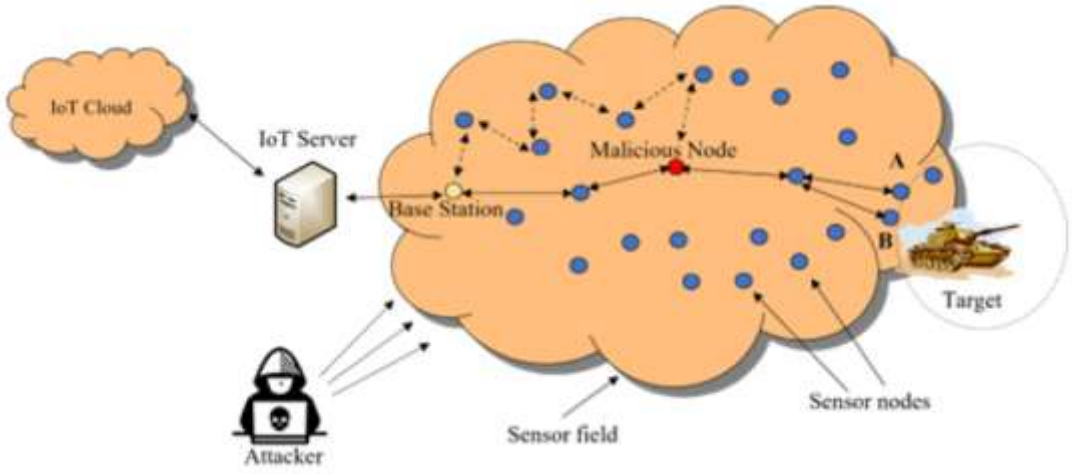

Figure 1. Malicious Node Attack Scenario in an IoT-Based Wireless Sensor Network

1.2 Research Objectives

- To implement 1CA2RT by applying one classification model for Node Status prediction and two regression models for Reputation Score and Dynamic Trust Score estimation.
- To develop the hybrid approach such as RPN-FIGS by combining deep learning feature extraction with interpretable classification.
- To compare the performance of the 1CA2RT models and evaluate the effectiveness of the proposed RPN-FIGS using standard classification and regression performance metrics for intelligent routing attack detection and reliability estimation in WSNs.

2. LITERATURE SURVEY

Haque et al. [6] proposed a smart wireless sensor network framework incorporating both physical and virtual sensors for forest fire evolution prediction. The methodology generated virtual sensors using polynomial regression models to augment the sensing coverage without deploying additional hardware. The collected data from physical and virtual sensors were combined into a supervector representation. A Multi-Layer Perceptron (MLP) neural network was trained to classify various fire scenarios, including early warning stages such as smoke and lightning events. Experimental evaluation demonstrated improved prediction accuracy and scalability for large forest monitoring environments. The prediction performance varies depending on the number and placement of virtual sensors, leading to inconsistent improvements across different fire scenarios. Kilius et al. [7] developed a time delay

Doi:10.48047/ijiee.2026.16.2.52

characterization framework for distributed wireless sensor network measurement applications. The methodology analyzed low-cost WSN topologies and measured communication delays under different operating conditions. Quantitative jitter analysis was conducted to examine the impact of modulation schemes and data transmission rates. Experimental probability density functions were utilized to evaluate synchronization error propagation across network layers. A controlled propagation delay jitter synchronization mechanism was further proposed to enhance timing accuracy in distributed sensing systems. The framework primarily focuses on synchronization performance and does not address network security or fault tolerance issues.

Ma et al. [8] introduced an innovative reliability evaluation algorithm for linear wireless sensor networks. The methodology modeled network reliability using node connectivity and communication link characteristics. A reliability assessment mechanism was designed to estimate network survivability under different failure conditions. Mathematical analysis was employed to evaluate end-to-end communication reliability across linear sensor deployments. The proposed algorithm provided an efficient means of predicting network performance and maintenance requirements. The reliability model assumes predefined network conditions, which may not accurately reflect highly dynamic deployment environments. Narayana et al. [9] proposed an energy-efficient and secure routing strategy for opportunistic data transmission in wireless sensor networks. The methodology utilized intelligent route selection based on node energy levels and communication trust metrics. Secure forwarding paths were established to prevent malicious data interception and packet loss. Opportunistic transmission techniques were incorporated to improve network throughput and reduce energy consumption. Extensive simulations were conducted to validate routing efficiency and security performance. Frequent route discovery and trust evaluation processes increase computational overhead in large-scale networks.

Hasan et al. [10] developed the SEER-PM protocol for secure and energy-efficient routing in pipeline monitoring wireless sensor networks. The methodology integrated security-aware route establishment with residual energy-based node selection. Data forwarding decisions considered both communication reliability and energy conservation. Attack mitigation mechanisms were incorporated to protect sensitive monitoring information. Performance evaluations demonstrated enhanced network lifetime and secure data delivery. The protocol performance may degrade when deployed in highly dynamic network topologies with frequent node failures. Sudheer et al. [11] introduced a blockchain-based randomized trusted node routing model for wireless sensor networks. The methodology employed blockchain technology to maintain immutable trust records among sensor nodes. Randomized node selection was utilized to minimize routing predictability and enhance security. Trust values were continuously updated based on node behavior and transaction history. The framework improved secure communication while reducing the risk of routing attacks. Blockchain operations introduce additional storage and processing requirements for resource-constrained sensor nodes.

Niranjana et al. [12] proposed the QAR-GGNN framework for QoS-aware secure routing using a min-cost strategy-based Gated Graph Neural Network. The methodology modeled network topology as a graph and employed GGNNs to learn routing patterns. Quality of Service parameters such as delay, bandwidth, and energy consumption were incorporated into route optimization. The min-cost strategy ensured efficient path selection while maintaining network security. Experimental results showed improved routing performance and reliability. Graph neural network training requires substantial computational resources and large datasets. Kuchanapally et al. [13] developed IRAB-NET, an interpretable hybrid

Doi:10.48047/ijiee.2026.16.2.52

boosting framework for intelligent routing attack detection and reliability estimation in WSNs. The methodology combined ensemble boosting techniques with explainable machine learning models. Routing behavior features were extracted to identify malicious activities and reliability degradation. Interpretability mechanisms provided insights into attack detection decisions. The framework simultaneously estimated network reliability and security status. The hybrid boosting structure increases model complexity and training time.

Agnihotri et al. [14] proposed a deep learning-based detection and recovery mechanism for mitigating selective forwarding attacks in event-driven wireless sensor networks. The methodology utilized deep neural networks to identify abnormal packet forwarding behavior. Suspicious nodes were detected through traffic pattern analysis and behavioral monitoring. Recovery procedures rerouted packets through alternative secure paths. Simulation studies demonstrated effective attack mitigation and network recovery. Deep learning models require extensive training data for maintaining detection accuracy. Juwaied et al. [15] introduced an intelligence-driven leader selection framework for PEGASIS-based wireless sensor networks. The methodology applied machine learning techniques to analyze node characteristics such as residual energy, communication quality, and trustworthiness. Data-driven leader selection improved cluster coordination and routing efficiency. Security factors were incorporated to prevent malicious node participation. The framework enhanced sustainability and secure data aggregation. Leader selection performance depends heavily on the quality of collected network statistics.

3. PROPOSED SYSTEM

The proposed methodology establishes a systematic framework for intelligent routing attack detection and reliability estimation in WSNs using a data-driven machine learning approach. The methodology begins with WSN data collection, followed by data preprocessing and feature engineering to prepare high-quality data for analysis. The processed dataset is then utilized to perform one classification task and two regression tasks based on the 1CA2RT methodology. Existing machine learning models, including KNN, PA, and GB, are employed for comparative analysis alongside the proposed RPN-FIGS. The framework supports accurate identification of routing attacks while simultaneously estimating Reputation Score and Dynamic Trust Score to evaluate the reliability of sensor nodes. Comprehensive performance evaluation and visualization are integrated into a Django-based web application, enabling interactive analysis, prediction, and monitoring. The entire workflow is designed to provide secure, scalable, interpretable, and efficient decision support for WSN environments, as shown in Figure 2.

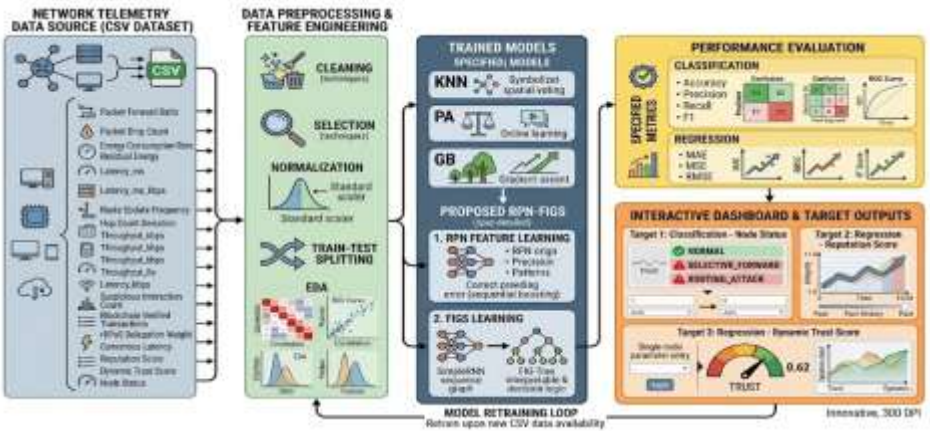

Figure 2: Proposed system architecture for insider threat and malicious domain detection framework using shared intelligence.

Doi:10.48047/ijiee.2026.16.2.52

User Interface (Web Browser): Users interact with the system through a browser-based graphical interface developed using the Django framework. The interface provides user registration, authentication, dataset exploration, exploratory data analysis, model execution, performance comparison, and single-node prediction functionalities. Users can provide communication parameters of sensor nodes and obtain prediction results through an interactive dashboard.

Django Web Server (views.py): The Django backend receives user requests and routes them to the appropriate processing modules. It manages user authentication, dataset loading, feature processing, model execution, prediction requests, visualization generation, and result presentation. The server coordinates communication between the user interface, machine learning modules, trained models, and the SQLite database.

Database (SQLite): SQLite serves as the backend database for storing application-related information. It maintains user registration details, login credentials, prediction history, and other system records. The database communicates efficiently with the Django application to support secure data management.

Raw Data (CSV Dataset): The WSN dataset serves as the primary input for intelligent routing attack detection and reliability estimation. The dataset contains communication, routing, energy, blockchain, trust, and network performance-related attributes collected from sensor nodes. Important attributes include Packet Forward Ratio, Packet Drop Count, Energy Consumption Rate, Residual Energy, Latency, Route Update Frequency, Hop Count Deviation, Throughput, Suspicious Interaction Count, Blockchain Verified Transactions, rDPoS Delegation Weight, Consensus Latency, Reputation Score, Dynamic Trust Score, and Node Status.

3.1 Proposed RPN-FIGS

The RPN-FIGS framework serves as the intelligent analytical component by integrating recurrent feature representation with an interpretable boosting-based prediction mechanism.

1. RPN (Recurrent Parameter/Feature Network)

- The RPN component learns sequential relationships among routing, communication, trust, and network behaviour features.
- It captures hidden feature representations that describe communication patterns among sensor nodes.
- The learned representations improve feature understanding for routing behaviour analysis and reliability estimation.

2. FIGS-Based Learning (Fast Interpretable Greedy Trees)

- The extracted feature representations are utilized by the FIGS model for intelligent prediction.
- FIGS performs one classification task for Node Status prediction and two regression tasks for Reputation Score and Dynamic Trust Score estimation.
- The interpretable tree-based learning strategy enhances prediction accuracy while maintaining model transparency and explainability.

Performance Evaluation: The framework evaluates all existing models and the proposed RPN-FIGS using standard classification and regression evaluation metrics. Classification performance is measured using Accuracy, Precision, Recall, F1-Score, Confusion Matrix, and ROC Curve. Regression performance is evaluated using MAE, MSE, RMSE, and R^2 Score. Comparative analysis identifies the most effective model for routing attack detection and reliability estimation.

Prediction Results & Target Outputs

- The trained models generate predictions for three distinct targets:
- **Target 1 (Classification):** Node Status
- **Target 2 (Regression):** Reputation Score
- **Target 3 (Regression):** Dynamic Trust Score
- Prediction results are displayed through the Django interface together with graphical visualizations and comparative performance reports.

Doi:10.48047/ijiee.2026.16.2.52

- The framework supports real-time prediction and intelligent analysis of WSN communication behaviour.

4. RESULTS AND DISCUSSIONS

The implementation of the intelligent routing attack detection and reliability estimation framework follows a systematic sequence of predefined and inbuilt Python functions that collectively support data preprocessing, machine learning, deep learning, performance evaluation, and web-based prediction. The execution begins with user authentication and dataset loading, followed by feature preprocessing and exploratory data analysis. The processed dataset is then utilized to implement one classification task and two regression tasks using existing machine learning models together with the proposed hybrid framework. Finally, the trained models are evaluated and deployed through a Django-based web interface for real-time prediction and visualization

.

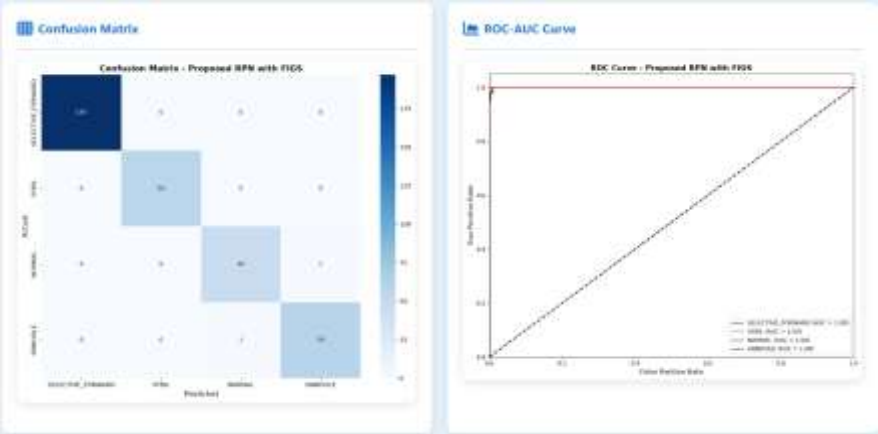

Figure 3: Confusion Matrix and ROC-AUC Curve Obtained for classification models RPN-FIGS

Figure 3 illustrates the confusion matrix and ROC-AUC curve for the proposed RPN-FIGS model, demonstrating superior classification performance. The confusion matrix shows perfect classification for selective forwarding (197) and Sybil nodes (56), with only 1 misclassification observed in normal and sinkhole classes. Normal nodes achieve 46 correct predictions with 1 minor error, while sinkhole nodes achieve 59 correct predictions with 1 misclassification. The ROC-AUC curve indicates perfect performance with AUC values of 1.00 for all classes, reflecting complete separability. These results confirm the effectiveness of the proposed model in accurately identifying routing attacks.

Figure 4 illustrates the scatter plot for the proposed RPN-FIGS model, demonstrating highly accurate prediction performance. The data points are tightly clustered along the ideal prediction line across the entire range of values from 0.0 to 1.0. Minimal deviation is observed, indicating very low prediction error and strong generalization capability. The clustering is especially dense in the higher reputation range (0.8–1.0), showing precise predictions. This aligns with its superior performance metrics, including MAE of 0.056 and R^2 score of 0.9391

.

Doi:10.48047/ijiee.2026.16.2.52

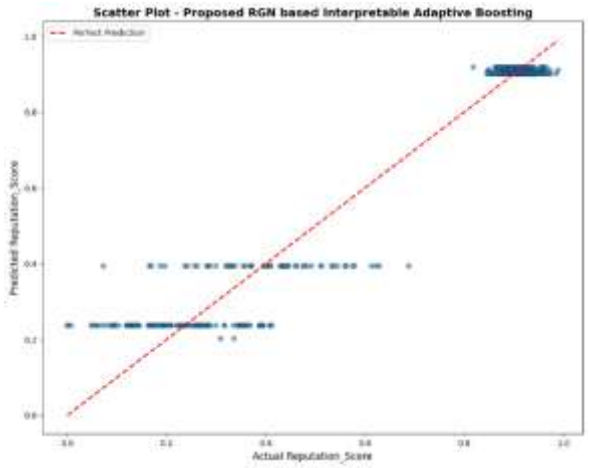

Figure 4: Scatter Plots Obtained for Reputation Regression models RPN-FIGS

Figure 5 illustrates the scatter plot for the proposed RPN-FIGS model, demonstrating superior prediction accuracy for trust values. The data points are tightly clustered along the ideal prediction line across the full range of values from 0.0 to 1.0. Minimal deviation is observed, indicating very low prediction error and strong generalization capability. The clustering is especially dense in the higher trust region (0.8–1.0), showing precise predictions. This aligns with its performance metrics, including MAE of 0.0524 and R^2 score of 0.9514.

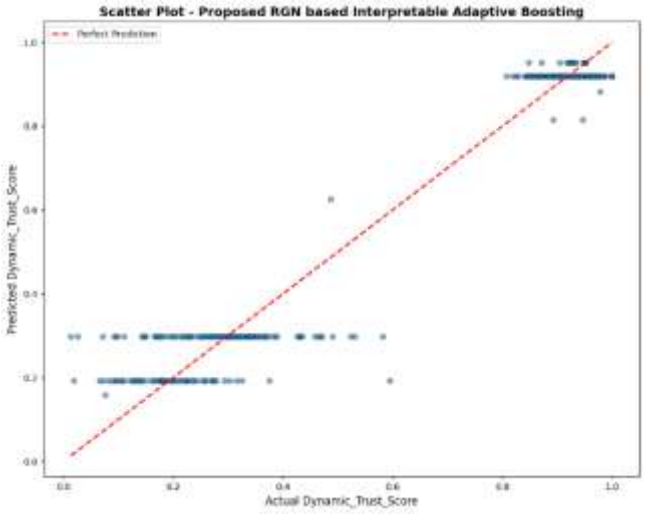

Figure 5: Scatter Plots Obtained for Trust Regression models RPN-FIGS

Figure 6 illustrates the single prediction results obtained on test data using multiple classification models along with the proposed RGN-based approach. The table presents predictions for 10 instances across KNN, PA, AB and RPN-FIGS models, considering target classes such as NORMAL, SYBIL, SINKHOLE, and SELECTIVE FORWARD. It shows that most predictions are consistent across models, particularly for NORMAL and SINKHOLE classes, while minor variations are observed in certain instances where AdaBoost differs from others. The RGN model demonstrates stable classification performance by aligning closely with majority predictions while also providing numerical outputs for reputation and trust scores. The reputation values range approximately from 0.2361 to 0.9119, and trust values range from 0.1937 to 0.9199, indicating clear separation between

Doi:10.48047/ijiee.2026.16.2.52

benign and malicious nodes. Higher scores are consistently associated with NORMAL nodes, while lower scores correspond to SYBIL, SINKHOLE, and SELECTIVE FORWARD classes.

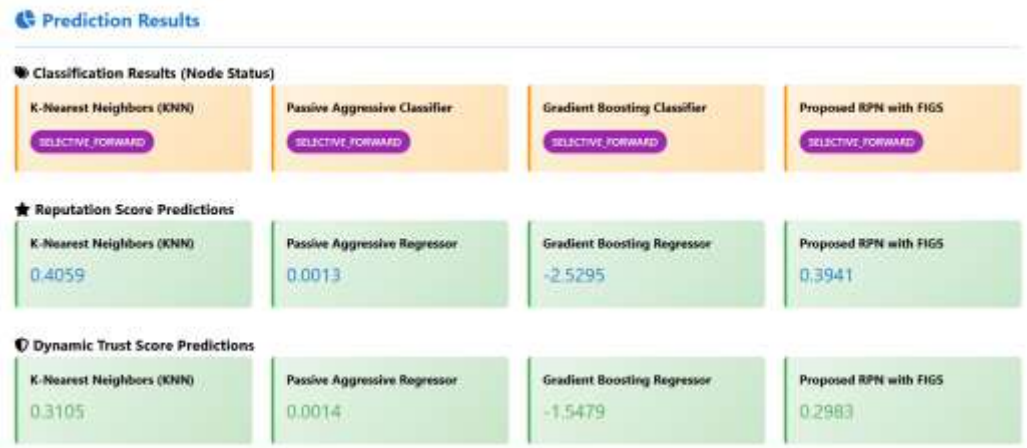

Figure 6: Prediction on test data

Comparative Analysis

Table 1 presents a comparative performance analysis of different classification models based on accuracy, precision, recall, and F1-score. The proposed RPN-FIGS model achieves the highest performance across all metrics with a consistent value of 99.44%, indicating superior classification capability. KNN also demonstrates strong performance with values above 98%, making it a reliable baseline model. The PA model shows moderately high results, with precision slightly higher than accuracy and recall, indicating balanced but slightly varied predictions. In contrast, the GB model exhibits significantly lower performance, with all metrics falling below 77%, highlighting its limitations in this task. The consistency between precision, recall, and F1-score for RPN-FIGS indicates stable and well-generalized predictions.

Table 1: Classification Performance Metrics Comparison for Node status

Model	Accuracy (%)	Precision (%)	Recalling (%)	F1-Score (%)
KNN	98.61	98.63	98.61	98.62
PA	95.83	96.67	95.83	95.91
GB	76.67	72.35	76.67	73.60
Proposed RPN-FIGS	99.44	99.44	99.44	99.44

Table 2 presents the performance metrics for reputation score prediction across different regression models. The proposed RPN-FIGS achieves the lowest error values with MAE of 0.0560, MSE of 0.0064, and RMSE of 0.0802, indicating highly accurate predictions. It also attains the highest R^2 score of 0.9391, showing strong model fit and reliability. KNN performs well with relatively low error values and a high R^2 of 0.8703, making it the second-best model. In contrast, PA shows higher error values and a negative R^2 score (-3.7190), indicating poor generalization. GB performs the worst with extremely high errors and a significantly

Doi:10.48047/ijiee.2026.16.2.52

negative R^2 (-29.5113), reflecting severe prediction instability.

Table 2: Regression Performance Metrics for Reputation Score Target.

Model	MAE	MSE	RMSE	R^2 Score
KNN	0.0783	0.0137	0.1170	0.8703
PA	0.6267	0.4982	0.7058	-3.7190
GB	1.4889	3.2209	1.7947	-29.5113
Proposed RPN-FIGS	0.0560	0.0064	0.0802	0.9391

Table 3: Regression Performance Metrics for Trust Score Target.

Model	MAE	MSE	RMSE	R^2 Score
KNN	0.0714	0.0094	0.0971	0.9179
PA	0.6172	0.4957	0.7040	-3.3167
GB	2.9267	8.5828	2.9296	-73.7459
Proposed RPN-FIGS	0.0524	0.0056	0.0747	0.9514

Table 3 presents the performance metrics for trust score prediction using different regression models. The proposed RPN-FIGS again achieves superior performance with the lowest MAE (0.0524), MSE (0.0056), and RMSE (0.0747), along with the highest R^2 score of 0.9514. KNN also shows strong performance with low error values and a high R^2 of 0.9179, indicating reliable predictions. PA demonstrates poor performance with higher error values and a negative R^2 score (-3.3167), suggesting weak model fitting. GB shows extremely poor results with very high error values and a highly negative R^2 (-73.7459), indicating failure to capture the data pattern. The consistency of RPN-FIGS across both tables highlights its robustness and effectiveness in predicting trust and reputation scores.

5. CONCLUSION AND FUTURE SCOPE

The research presents an intelligent and interpretable framework for routing attack detection and reliability estimation in WSNs by combining recurrent feature learning with an explainable tree-based prediction approach. The proposed RPN-FIGS framework effectively captures complex communication patterns and generates reliable predictions for one classification task and two regression tasks under the 1CA2RT methodology. Experimental evaluation demonstrates that the proposed framework consistently outperforms the existing KNN, PA, and GB models in terms of prediction accuracy and regression performance. For classification, the framework achieves an accuracy of 99.44%, providing highly reliable identification of normal and malicious sensor nodes. In the regression tasks, it records the lowest prediction errors with MAE values of 0.0560 for Reputation Score and 0.0524 for Dynamic Trust Score, while obtaining R^2 scores of 0.9391 and 0.9514, respectively. The framework also incorporates comprehensive data preprocessing, exploratory data analysis, and visualization modules that improve understanding of communication behavior and model performance.

Doi:10.48047/ijiee.2026.16.2.52

REFERNCES

[1] Sarkar NI, Gul S. Deploying WSNs in Multi-Story Buildings toward Internet of Things-Based Intelligent Environments: An Empirical Study. Sensors. 2024; 24(11):3415. https://doi.org/10.3390/s24113415.

[2] Sankaranarayanan S, Vijayakumar R, Swaminathan S, Almarri B, Lorenz P, Rodrigues JJPC. Node Localization Method in WSNs Using Combined Crow Search and the Weighted Centroid Method. Sensors. 2024; 24(15):4791. https://doi.org/10.3390/s24154791.

[3] Ullah A, Khan FS, Mohy-ud-din Z, Hassany N, Gul JZ, Khan M, Kim WY, Park YC, Rehman MM. A Hybrid Approach for Energy Consumption and Improvement in Sensor Network Lifespan in WSNs. Sensors. 2024; 24(5):1353. https://doi.org/10.3390/s24051353.

[4] Mushtaq MU, Venter H, Singh A, Owais M. Advances in Energy Harvesting for Sustainable WSNs: Challenges and Opportunities. Hardware. 2025; 3(1):1. https://doi.org/10.3390/hardware3010001.

[5] Agarwal H, Singh AP, Singh A, Kumar A, Agrawal PK, Saranya S. Comparing New Wireless Sensor Network Protocols through Simulation and Data Analysis. Engineering Proceedings. 2024; 62(1):21. https://doi.org/10.3390/engproc2024062021.

[6] Haque A, Soliman H. Smart WSNs with Virtual Sensors for Forest Fire Evolution Prediction Using Machine Learning. Electronics. 2025; 14(2):223. https://doi.org/10.3390/electronics14020223.

[7] Kilius Š, Gailius D, Knyva M, Balčiūnas G, Meškuotienė A, Dobilienė J, Joneliūnas S, Kuzas P. Time Delay Characterization in WSNs for Distributed Measurement Applications. Journal of Sensor and Actuator Networks. 2024; 13(3):31. https://doi.org/10.3390/jsan13030031.

[8] Ma T, Guo H, Li X. An Innovative Linear Wireless Sensor Network Reliability Evaluation Algorithm. Sensors. 2025; 25(1):285. https://doi.org/10.3390/s25010285.

[9] Narayana, Potu, K. Keerthi, Osamah Ibrahim Khalaf, Premkumar Chithaluru, Manoj A. Patil, Sridevi Tumula, Dharmana Jayaram, and Mhd Saeed Sharif. "Energy-efficient and secure routing strategy for opportunistic data transmission in WSNs." Journal of Cyber Security Technology 10, no. 1 (2026): 1-36.

[10] Hasan, Rasha, Rafe Alasem, Ahmed Akl Mahmoud, Yazeed Alsarhan, and Mahmud Mansour. "SEER-PM: A Secure and Energy-Efficient Routing Protocol for Pipeline Monitoring Wireless Sensor Networks." Algorithms 19, no. 6 (2026): 493.

[11] Sudheer, Bandlamudi Naga, and Kamepalli Sujatha. "Blockchain based randomized trusted node routing model in wireless sensor network." Discover Computing 29, no. 1 (2026): 385.

[12] Niranjana, M. Ishwarya, and N. Kumareshan. "QAR-GGNN: QoS Aware Secure Routing in WSN via Mincost Strategy based Gated Graph Neural Network." International Journal of Computational Intelligence Systems (2026).

[13] Kuchanapally, Bhaskar Babu, Mogulaji Vyshnavi, Kusuma Pranitha, and Katakam Sai Shiva. "IRAB-NET: An Interpretable Hybrid Boosting Framework for Intelligent Routing Attack Detection and Reliability Estimation in WSNs." American Journal of Management and IOT Medical Computing 5, no. 2 (2026): 306-315.

[14] Agnihotri, Atul Kumar, and Vishal Awasthi. "Deep learning-based detection and recovery mechanism for mitigating selective forwarding attacks in event-driven wireless sensor network." Peer-to-Peer Networking and Applications 19, no. 2 (2026): 56.

[15] Juwaied, Abdulla, and Andrzej Romanowski. "Intelligence-Driven Leader Selection in PEGASIS: A Data-Driven Machine Learning Framework for Sustainable and Secure Wireless Sensor Networks." Electronics 15, no. 8 (2026): 1686.

Doi:10.48047/ijiee.2026.16.2.52