AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Rferred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(2026)

DYNAMIC ROLE-BASED SECURITY FRAMEWORK WITH HYBRID VOTING CLASSIFIERS FOR SENSOR NETWORK PROTECTION

Edhigani Revathi[1], A. Nagarani[2], Rekha Gangula[3*], G Bhanu Prakash[1], Dasari Prashanth[1], Kudikala Hari Priya[1]

[1]UG Student, [2]Assistant Professor, [3]Associate Professor and Head, [1,2,3]Department of Computer Science and Engineering (AI&ML)

[1,2,3]Vaagdevi Engineering College, Bollikunta, Warangal, 506005, Telangana, India

*Correspondence: Rekha Gangula (gangularekha@gmail.com)

Abstract

Wireless Sensor Networks (WSNs) play a crucial role in modern communication systems by enabling efficient data collection and monitoring across applications such as environmental sensing, healthcare, military surveillance, and smart cities. However, the open communication architecture and limited security mechanisms of WSNs make them highly vulnerable to routing attacks, including flooding, TDMA manipulation, gray hole, and black hole attacks. These threats disrupt network communication, increase energy consumption, and reduce overall system reliability and lifespan. Traditional intrusion detection systems in WSNs rely on rule-based and signature-based techniques that detect known attack patterns. While effective for predefined threats, these methods struggle to identify novel and complex attacks in dynamic network environments. To address these limitations, this study proposes a machine learning–based routing attack detection framework that analyzes network communication parameters to identify malicious behavior. The framework incorporates baseline classifiers such as Decision Tree Classifier (DTC), Ridge Classifier (RC), and Linear Discriminant Analysis (LDA) to evaluate detection performance. Additionally, a novel hybrid model, termed Deep Reservoir Routing Defense (DRRD), is introduced by integrating Echo State Network (ESN) with Decision Tree Cost Complexity Pruning (DTCCP). The ESN performs reservoir-based feature transformation to capture dynamic communication patterns, while DTCCP ensures accurate classification based on transformed features. To enhance model performance, preprocessing techniques including label encoding, missing value handling, and SMOTE-based data balancing are applied. Experimental results demonstrate that the proposed DRRD model significantly outperforms traditional methods in detection accuracy, offering a scalable and efficient solution for securing WSN environments.

Keywords: intrusion detection, machine learning, routing attacks, wireless sensor networks, decision tree cost complexity pruning

1. Introduction

Wireless Sensor Networks (WSNs) [1] have become a fundamental technology in modern cyber-physical systems, supporting real-time monitoring, environmental sensing, and intelligent decision-making across various domains such as environmental monitoring, healthcare, industrial automation, and smart cities. These networks consist of spatially distributed sensor nodes with capabilities for sensing [2], processing, and wireless communication, enabling large-scale and autonomous data collection and transmission. The origins of sensor networks date back to the Cold War, particularly with the deployment of acoustic arrays in the Sound Surveillance System (SOSUS) for detecting Soviet submarines. Over time, advancements in microelectronics [3], low-power communication, and embedded systems have significantly accelerated the adoption of WSNs, making them vital in both civilian and military applications. Numerous studies have explored different aspects of WSN deployment. Despite their advantages, the deployment of sensor nodes remains one of the most

challenging aspects in WSN design as shown in Figure 1. Sensor nodes vary in terms of energy resources, processing power, communication range, and sensing capabilities.

While this diversity allows for application-specific adaptability, it also increases the complexity of deployment strategies. Additionally, deployment requirements differ widely depending on the application, with some focusing on complete area coverage, while others prioritize connectivity [4], fault tolerance, energy efficiency, or real-time performance. Therefore, deployment must balance multiple objectives such as maximizing coverage, extending network lifetime, minimizing cost, and ensuring robustness against environmental changes. Although several surveys have addressed WSN deployment, many concentrate on specific aspects such as coverage strategies, energy-efficient routing, or algorithmic techniques. For instance, some studies focus solely on node placement optimization without considering overall architecture [5] and sensing models, while others emphasize clustering methods or mobile node positioning with limited applicability. These isolated approaches do not offer a comprehensive understanding of the design space that combines architecture, objectives, sensing models, and deployment strategies.

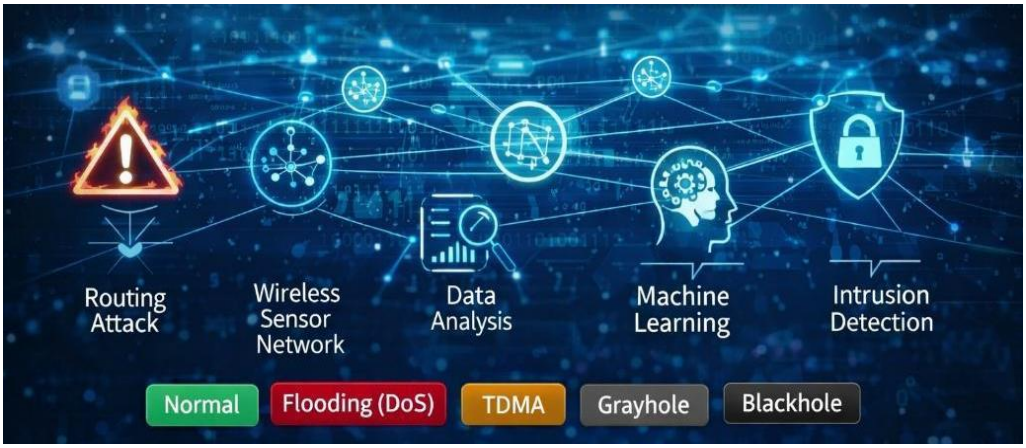

Figure 1: Various Types of WSN Attacks.

Research Motivation: Modern industries increasingly rely on WSN to collect and analyse operational data in real time. Companies involved in smart manufacturing, logistics monitoring, agriculture technology, environmental monitoring, and smart cities depend on sensor networks to ensure continuous data collection and system monitoring. For example, industrial companies use sensor networks to monitor machinery conditions, while agricultural companies rely on sensor nodes to analyse soil moisture, crop health, and environmental factors. These systems generate large volumes of network communication data, and analysing this data becomes crucial for maintaining system reliability. Cybersecurity firms, cloud service providers, and IoT solution companies continuously analyse network traffic data to detect abnormal activities and potential attacks.

2. Literature Survey

Masdari et al. [6] addressed privacy concerns in IoT data processing and demonstrated that secure SVM training can be performed efficiently without relying on a trusted third party. Verma et al. [7] reviewed the security of RPL-based 6LoWPAN networks by presenting IoT architecture, identifying RPL threats, and discussing defense mechanisms along with evaluation metrics. Tahsien et al. [8] surveyed machine learning-based solutions for IoT security, providing classifications of cyber-attacks based on behavior, targeted layers, and impact, while also highlighting challenges in applying ML techniques.

Avila et al. [9] conducted a systematic literature review on RPL security, analyzing 53 studies covering mitigation strategies, authentication mechanisms, cryptographic solutions, and secure routing

techniques. However, the study lacked detailed critical evaluation of individual approaches. Faraj et al. [10] presented a survey on machine learning-based intrusion detection systems for IoT, focusing on system design, taxonomy, and implementation challenges, while also identifying open research issues. Khraisat et al. [11] reviewed various IDS strategies in IoT environments, discussing deployment methods, validation techniques, datasets, and comparisons between machine learning and deep learning approaches.

Pasikhani et al. [12] provided a comprehensive systematic literature review of IDS in RPL-based 6LoWPAN networks, covering 103 studies and presenting detailed taxonomy, statistical analysis, and evaluation metrics, along with identified research gaps and future directions. Sharma et al. [13] proposed a framework for simulating RPL attacks and generating a multi-class dataset with 58 features for supervised machine learning models. Müller et al. [14] introduced a distributed anomaly detection approach for single mote attacks in RPL networks, targeting HF, VN, and BH attacks by deploying pre-trained models within network nodes. Canbalaban et al. [15] developed a cross-layer intrusion detection system using neural networks to detect multiple attacks, including VN, WP, and HF, by combining routing-layer and link-layer features.

Qureshi et al. [16] proposed a secure framework for attack detection in smart city and Industrial IoT environments, involving feature reduction using genetic programming followed by attack detection. Kumar et al. [17] proposed a Decision Tree-based IDS to prevent intra and inter-network Denial-of-Service (DoS) attacks, specifically analyzing the behavior and impact of HF and VN attacks. Osman et al. [18] proposed a lightweight machine learning-based approach, ML-LGBM, for detecting VN attacks in RPL-based IoT networks, which includes dataset generation, feature extraction, classification using Light Gradient Boosting Machine, and model optimization.

Rekha Gangula et al. [19] proposed a hybrid optimization framework combining Bottlenose Dolphin Optimization and Artificial Fish Swarm Algorithm for IoT intrusion detection. The hybrid model optimized feature selection and classifier performance. The approach achieved improved detection rates with reduced complexity. Rekha Gangula et al. [20] proposed a stacked Bidirectional Long Short-Term Memory (BiLSTM) with elastic regression classifier optimized using Aquila Optimizer. The model captured temporal dependencies in network traffic. The optimization process enhanced classification precision. Rekha Gangula et al. [21] proposed a Distributed Denial-of-Service (DDoS) detection model using Gated Recurrent Unit (GRU) with Binary Whale Optimization Algorithm. The model learned sequential attack patterns effectively. The optimization improved detection speed and accuracy. Rekha Gangula et al. [22] proposed enhanced deep learning networks for advanced intrusion detection and prevention systems. The framework integrated deep feature extraction with intelligent classification. The system improved detection capability in Industry 6.0 environments.

3. Proposed System

The proposed system presents a machine learning–based framework for detecting routing attacks in wireless sensor networks. Initially, the network traffic dataset is collected in CSV format and undergoes a data processing stage that includes label encoding, handling missing values, and normalization. To address class imbalance, the SMOTE technique is applied, after which the dataset is divided into training and testing sets. The system incorporates multiple baseline machine learning models, including Decision Tree Classifier, Ridge Classifier, and Linear Discriminant Analysis (LDA), to perform classification and comparison. In addition to these models, a hybrid approach is introduced where feature scaling is performed, followed by feature extraction using the Echo State Network (ESN). The extracted reservoir features are then passed to the DTCCP classifier for final classification. The prediction module processes unseen test data through preprocessing and ESN-based feature extraction,

and the trained hybrid model predicts routing attack types such as Normal, Flooding, TDMA, Grayhole, and Blackhole as illustrated in Figure 2.

Step 1: Dataset Uploading: The system begins with loading the network traffic dataset in CSV format. The administrator selects the dataset through a Tkinter-based file dialog interface. The dataset is then read using the panda's library and stored for further processing.

Step 2: Data Processing: In this stage, the dataset undergoes preprocessing which includes label encoding of categorical features, handling missing values, and normalization. This ensures that the data is in a suitable format for machine learning models.

Step 3: Exploratory Data Analysis (EDA): Exploratory data analysis is performed to understand the dataset characteristics. Various visualizations such as attack distribution plots, correlation heatmaps, boxplots, scatter plots, histograms, and bar plots are generated to analyze relationships between features and attack categories.

Step 4: Dataset Balancing using SMOTE: To handle class imbalance, SMOTE is applied to generate synthetic samples for minority classes. This ensures that all attack categories are equally represented during model training.

Step 5: Train-Test Data Splitting: The balanced dataset is split into training and testing sets using stratified sampling. This maintains consistent class distribution across both datasets.

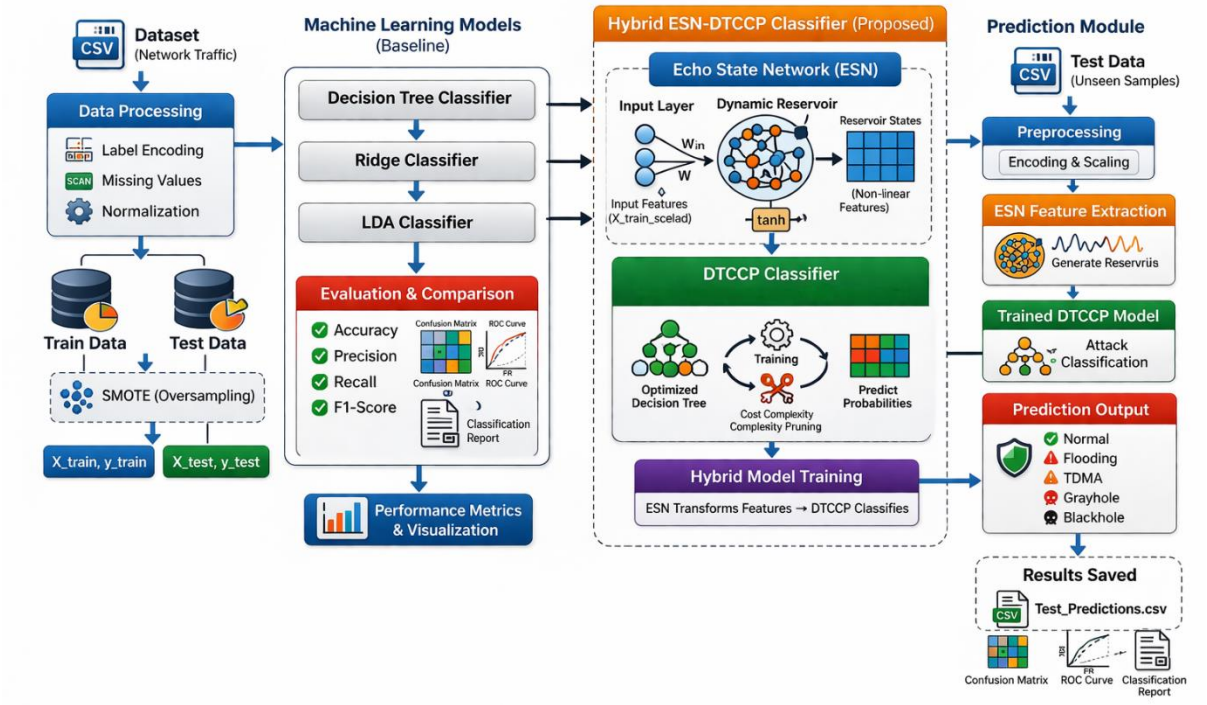

Figure 2: Proposed system architecture.

Step 6: Machine Learning Model Training: The system trains multiple baseline classifiers, including Decision Tree Classifier, Ridge Classifier, and LDA. These models learn patterns from the training data to detect routing attacks and are used for performance comparison.

Step 7: Hybrid Model Development (ESN-DTCCP): The proposed hybrid model integrates ESN and DTCCP classifier. Initially, the input features are scaled and passed through the ESN, which generates reservoir states representing transformed features. These features are then provided to the DTCCP classifier, which performs classification using an optimized decision tree approach.

Step 8: Model Evaluation and Performance Analysis: The trained models are evaluated using metrics such as accuracy, precision, recall, and F1-score. Additional evaluation includes confusion matrix visualization, ROC curve analysis, and classification reports to measure performance across different attack categories.

Step 9: Prediction Module: In the final stage, unseen test data is processed through preprocessing and ESN-based feature extraction. The trained hybrid model predicts attack types including Normal, Flooding, TDMA, Grayhole, and Blackhole. The results are displayed through the Tkinter interface and saved in CSV format for further analysis.

3.1 Proposed DRRD Model

The proposed DRRD model is a hybrid machine learning framework designed to detect routing attacks in wireless sensor networks by combining the feature extraction capability of ESN with the classification capability of DTCCP. The ESN component captures complex patterns in the network traffic by transforming the input features into dynamic reservoir states, while the DTCCP classifier analyzes these enriched features to identify routing attacks. By integrating reservoir-based feature representation with efficient classification, the DRRD model improves the detection of attacks such as Normal, Flooding, TDMA, Grayhole, and Blackhole as shown in Figure 3.

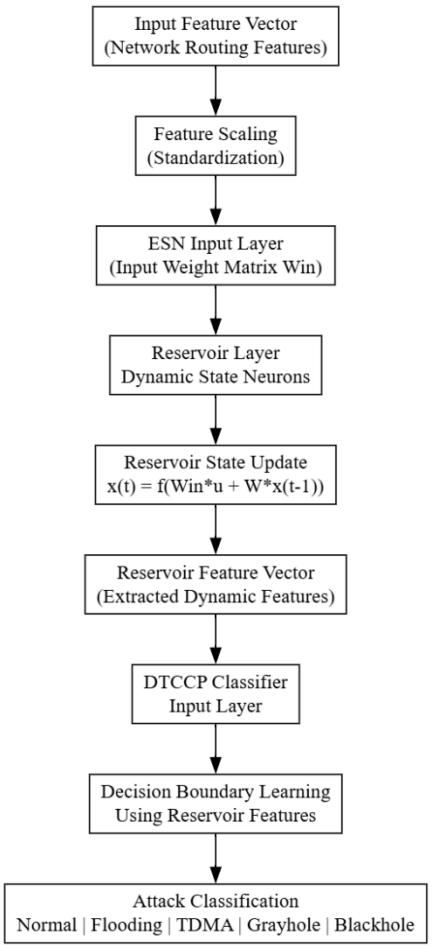

Figure 3: Internal workflow of DRRD Model

Step 1. Input Feature Vector Processing: The DRRD model receives the input feature vector representing network routing behavior parameters. Each vector contains multiple attributes describing communication patterns in the wireless sensor network. These input features are provided to the ESN component for advanced representation learning.

Step 2. Input Weight Projection in ESN: Inside the ESN, the input features are multiplied with randomly initialized input weights. This projection maps the original feature vector into the reservoir space. The transformation increases the representational capacity of the features for better pattern extraction.

Step 3. Reservoir State Activation: The projected inputs activate neurons within the ESN reservoir layer. Each neuron updates its internal state based on the input signal and the reservoir connections. This process generates nonlinear dynamic responses that capture hidden relationships among network routing features.

Step 4. Reservoir Feature Generation: After the reservoir activation process, the ESN produces a reservoir state vector. This vector represents the transformed feature space that contains richer information about network traffic patterns. These reservoir features highlight differences between normal traffic and routing attacks.

Step 5. Feature Transfer to DTCCP: The generated reservoir feature vectors are then forwarded to the DTCCP classifier. These features act as high-level representations of the input data. The classifier uses them to learn the boundaries between different routing attack categories.

Step 6. Decision Learning in DTCCP: During training, the DTCCP classifier analyzes the reservoir features along with their corresponding attack labels. It learns how different patterns in the reservoir states correspond to specific routing attacks. This step builds an effective classification model.

Step 7. Attack Classification: During prediction, the incoming network feature vector is first transformed by the ESN reservoir. The generated reservoir states are then evaluated by the DTCCP classifier. Based on the learned decision boundaries, the model predicts the appropriate routing attack class.

Step 8. Probability-Based Decision Output: The DTCCP classifier also estimates probability scores for each possible attack class. These scores represent the likelihood of each attack type. The class with the highest probability is selected as the final predicted output of the DRRD model.

4. Results and Discussion\

Fig. 4 shows the confusion matrix generated for the RC. The matrix indicates a significant improvement in classification performance compared to the DT model. Most of the samples belonging to each attack category are correctly classified along the diagonal elements of the matrix. The RC demonstrates strong performance in detecting Flooding and Grayhole attacks. However, a moderate number of TDMA samples are misclassified as Normal or Blackhole attacks. Despite these minor errors, the model maintains high overall accuracy. The confusion matrix demonstrates that the RC can effectively learn patterns from the dataset. This results in more reliable routing attack detection performance.

Fig. 5 illustrates the confusion matrix obtained from the LDA classifier. The matrix shows that LDA achieves strong classification performance across most attack categories. A large number of samples are correctly classified along the diagonal elements of the matrix. The classifier successfully detects Normal, Flooding, Grayhole, and Blackhole attacks with high accuracy. However, some TDMA samples are misclassified as Normal due to similarities in feature patterns. This indicates partial overlap between certain routing behavior characteristics. Even with this limitation, LDA achieves high overall classification accuracy. The confusion matrix demonstrates the effectiveness of LDA in separating different attack classes.

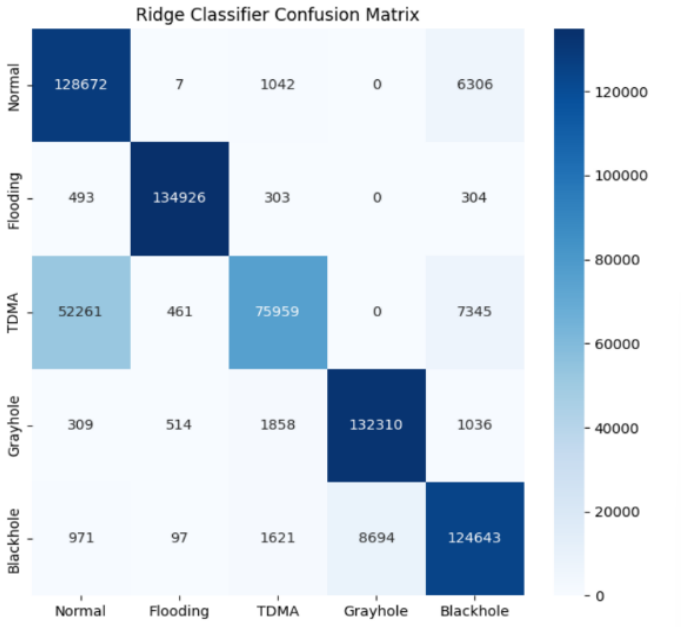

Figure 4: Confusion matrix obtained using RC

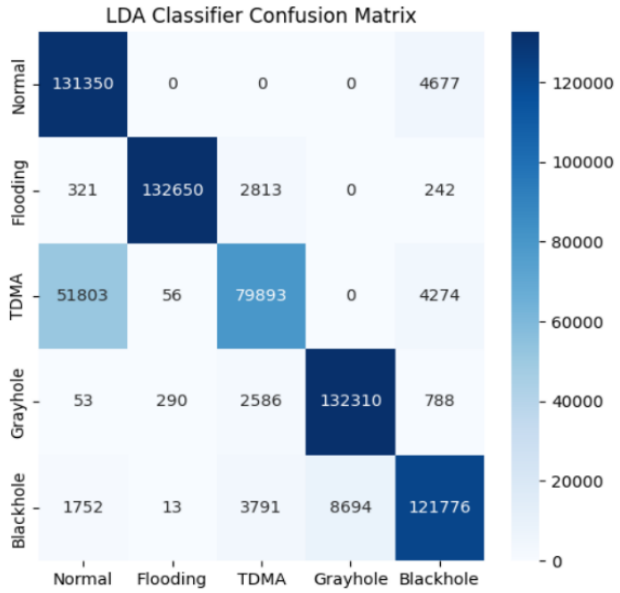

Figure 5: Illustration of confusion matrix using LDA

Fig. 6 presents the confusion matrix for the proposed ESN–DTCCP hybrid classifier. The matrix clearly shows that almost all samples are correctly classified across all attack categories. The diagonal elements contain the majority of values, indicating correct classification results. Only a very small number of misclassifications are observed in the matrix. This demonstrates the superior performance of the hybrid model compared to traditional classifiers. The ESN component captures complex routing patterns within the dataset. The DTCCP classifier then accurately categorizes these patterns into appropriate attack classes. This combined approach results in extremely high routing attack detection accuracy.

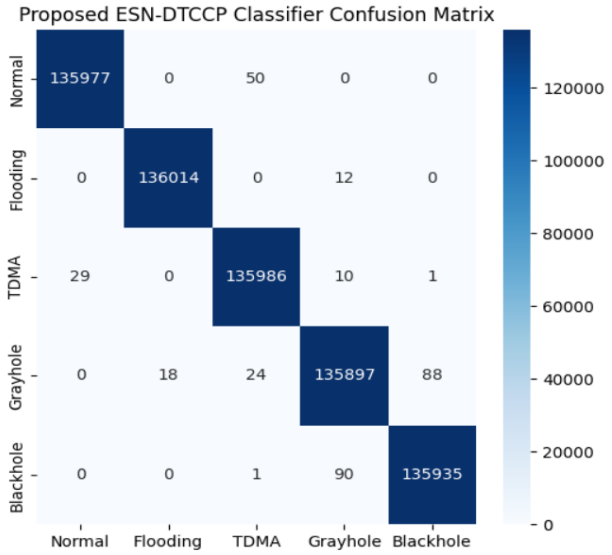

Fig. 6: illustration of confusion matrix using DRRD Model

Table 1 presents the performance comparison of different machine learning algorithms used for routing attack detection. The algorithms compared include DT, RC, LDA, and the proposed DRRD model. The comparison is based on evaluation metrics such as Accuracy, Precision, Recall, and F1-score. The DT classifier shows the lowest performance with an accuracy of 39.99%, indicating poor classification capability. RC and LDA achieve significantly better results with accuracies of 87.71% and 87.92% respectively. These models demonstrate good performance but still show limitations in certain attack categories. The proposed DRRD achieves the highest performance with an accuracy of 99.95%. The results indicate that the proposed hybrid model provides superior detection capability compared to traditional machine learning algorithms.

Table 1: Performance Comparison of Routing Attack Detection Algorithms

Algorithm	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-Score (%)**
DT Classifier	39.99	24.98	39.99	27.99
RC model	87.71	89.35	87.71	87.19
LDA Classifier	87.92	89.31	87.92	87.56
Proposed DRRD Model	99.95	99.95	99.95	99.95

5. Conclusion

The research presents a machine learning–based approach for detecting routing attacks in WSN using multiple classification algorithms. The system was designed to analyse network communication features such as cluster head selection, data transmission, routing distance, and energy consumption to identify different attack categories including Normal, Flooding, TDMA, Grayhole, and Blackhole. Several machine learning algorithms including DT, RC, and LDA were implemented and evaluated to analyse their effectiveness in routing attack detection. Experimental results demonstrate that the DT classifier shows relatively low performance with an accuracy of 39.99%, indicating its limited ability to correctly classify multiple attack categories. The RC and LDA algorithms significantly improve detection capability by achieving accuracies of 87.71% and 87.92%. The proposed DRRD model

achieves the best performance among all evaluated classifiers with an accuracy of 99.95%, along with very high precision, recall, and F1-score values. This improvement is achieved through the integration of ESN for dynamic feature representation and DTCCP classification for accurate attack detection. The hybrid approach effectively captures complex routing behaviour patterns and significantly improves classification performance. The system can be further improved by integrating deep learning techniques to enhance routing attack detection accuracy in large-scale WSN. Future research can also focus on implementing real-time network monitoring and deploying the system in real-world sensor network environments for practical security applications.

REFERENCES

[1]. C. Lin, Z. Shang, W. Du, J. Ren, L. Wang, and G. Wu, "CoDoC: A novel attack for wireless rechargeable sensor networks through denial of charge," in Proc. IEEE INFOCOM, Apr. 2019, pp. 856–864, doi: 10.1109/INFOCOM.2019.8737403.

[2]. H. Belkhiri, A. Messai, A.-L. Beylot, and F. Haider, "Denial of service attack detection in wireless sensor networks and software defined wireless sensor networks: A brief review," in Proc. Int. Conf. Big Data Internet Things. Cham, Switzerland : Springer, 2022, pp. 100–115, doi: 10.1007/978-3-031-07969-6_8.

[3]. R. Roman and J. Lopez, "Integrating wireless sensor networks and the internet: A security analysis," Internet Res., vol. 19, no. 2, pp. 246–259, Apr. 2009, doi: 10.1108/10662240910952373.

[4]. C. Duru, A. Aniedu, O. T. Innocent, and A. E. Eo, "Modeling of wireless sensor networks jamming attack strategies," Amer. Sci. Res. J. Eng., Technol., Sci., vol. 67, no. 1, pp. 48–65, 2020.

[5]. A. A. Rezaee and F. Pasandideh, "A fuzzy congestion control protocol based on active queue management in wireless sensor networks with medical applications," Wireless Pers. Commun., vol. 98, no. 1, pp. 815–842, Jan. 2018.

[6]. M. Masdari, "Energy efficient clustering and congestion control in WSNs with mobile sinks," Wireless Pers. Commun., vol. 111, no. 1, pp. 611–642, Mar. 2020.

[7]. Verma, A.; Ranga, V. Security of RPL Based 6LoWPAN Networks in the Internet of Things: A Review. IEEE Sen. J. 2020, 20, 5666–5690.

[8]. Reddy, S. K. R. (2021). Strengthening the Security of Loyalty Reward Systems: An In-Depth Analysis of Emerging Cyber Threats and Protection Mechanisms. Journal of Computational Analysis and Applications, 29(6).

[9]. Purmani, S. S. R. (2024). Aligning IT investment decisions with overall business strategy from an enterprise program management perspective, focusing on the integration of IT leadership in strategic decision-making processes. International Journal of Communication Networks and Information Security, 16(5), 1213–1219.

[10]. Faraj, O.; Megías, D.; Ahmad, A.M.; Garcia-Alfaro, J. Taxonomy and challenges in machine learning-based approaches to detect attacks in the internet of things. In Proceedings of the 15th International Conference on Availability, Reliability and Security, Virtual Event, Ireland, 25–28 August 2020; pp. 1–10.

[11]. Khraisat, A.; Alazab, A. A critical review of intrusion detection systems in the internet of things: Techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. Cybersecurity 2021, 4, 18.

[12]. Kalae, U. K. (2025). Optimizing cost-effective cloud data pipeline orchestration across multiple cloud providers. Journal of Information Systems Engineering and Management, 10(63s), e726–e741.

[13]. Sharma, M.; Elmiligi, H.; Gebali, F.; Verma, A. Simulating Attacks for RPL and Generating Multi-class Dataset for Supervised Machine Learning. In Proceedings of the 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 17–19 October 2019; pp. 20–26.

[14]. Müller, N.; Debus, P.; Kowatsch, D.; Böttinger, K. Distributed Anomaly Detection of Single Mote Attacks in RPL Networks. In Proceedings of the 16th International Joint Conference on e-Business and Telecommunications, Prague, Czech Republic, 26–28 July 2019; Volume 2, pp. 378–385.

[15]. Canbalaban, E.; Sen, S. A Cross-Layer Intrusion Detection System for RPL-Based Internet of Things. In International Conference on Ad-Hoc Networks and Wireless; Springer: Bari, Italy, 2020; Volume 12338, pp. 214–227.

[16]. Qureshi, K.N.; Rana, S.S.; Ahmed, A.; Jeon, G. A novel and secure attacks detection framework for smart cities industrial internet of things. Sustain. Cities Soc. 2020, 61, 102343.

[17]. Kumar, V.; Kumar, V.; Sinha, D.; Das, A.K. Simulation Analysis of DDoS Attack in the IoT Environment. In Advances in Intelligent Systems and Computing; Springer: Cham, Switzerland, 2020; Volume 1122, pp. 77–87.

[18]. Osman, M.; He, J.; Mokbal, F.M.M.; Zhu, N.; Qureshi, S. ML-LGBM: A Machine Learning Model Based on Light Gradient Boosting Machine for the Detection of Version Number Attacks in RPL-Based Networks. IEEE Access 2021, 9, 83654–83665.

[19]. Rekha Gangula,Murali Mohan Vutukuru,M.Ranjeeth kumar “Hybridization of Bottlenose Dolphin Optimization and Artificial Fish Swarm Algorithm with Efficient Classifier for Detecting the Network Intrusion in Internet of Things (IoT)”. International Journal of Intelligent Systems and Applications in Engineering. IJISAE, 2024, 12(6s), 220–232

[20]. Rekha Gangula,Murali Mohan Vutukuru,M.Ranjeeth kumar ” Network Intrusion Detection Method Using Stacked BILSTM Elastic Regression Classifier with Aquila Optimizer Algorithm for Internet of Things (IoT)." International Journal on Recent and Innovation Trends in Computing and Communication 11: 118-131.International Journal of Recent Technology and Engineering “Usage of Machine Learning algorithms in DataMining” in May 2019.

[21]. Rekha Gangula,Murali Mohan Vutukuru,M.Ranjeeth kumar “A Comprehense study of DDoS Attack Detecting algorithm using GRU-BWFA classifier “.Measurement:Sensors Volume 24, December 2022, 100570. https://doi.org/10.1016/j.measen.2022.100570

[22]. Rekha Gangula, Suma Patra, Nata Sheker Reddy Miriyala” Enhanced deep learning networks for advanced intrusion detection and prevention systems” Industry 6.0 Technology, Practices, Challenges, and Applications. ISBN: 9781003517993 https://doi.org/10.1201/9781003517993.