2025 IEEE GLOBAL CONFERENCE IN EMERGING TECHNOLOGY (GINOTECH)

Enhanced Attack Detection in Cognitive Radio Using Leaky Integrated Bidirectional Echo State Networks

Dr. S. Palanivel Rajan
Department of Electronics and Communication Engineering, Velammal College of Engineering and Technology,
Madurai, India.
drspalanivelrajan@gmail.com

R. Rahul
Department of Electronics and Communication Engineering, Velammal College of Engineering and Technology,
Madurai, India.
rahulkanna170504@gmail.com

T. Jegan
Department of Electronics and Communication Engineering, Velammal College of Engineering and Technology,
Madurai, India.
jknn007@gmail.com

S. Yasar Arafath
Department of Electronics and Communication Engineering, Velammal College of Engineering and Technology,
Madurai, India.
ya0387288@gmail.com

***Abstract*— With the rise of wireless communication, dynamic spectrum management has become crucial—especially in Cognitive Radio Networks (CRNs), which improve spectral efficiency. However, their open and adaptive nature makes them vulnerable to attacks such as jamming, Primary User Emulation Attacks (PUEA), and Spectrum Sensing Data Falsification (SSDF). This paper introduces a novel deep learning model, the Leaky Integrated Bidirectional Echo State Network (LIBESN), for effective attack detection in CRNs. LIBESN enhances traditional Echo State Networks by integrating bidirectional data flow and leaky integration, enabling better temporal pattern recognition and long-range dependency learning. Unlike conventional recurrent networks, LIBESN uses fixed reservoir weights, reducing training time while maintaining high accuracy. Experiments on a custom CRN dataset show that LIBESN achieves 94.67% accuracy, 93.33% precision, 95.89% recall, and a 94.59% F1-score—surpassing existing models. ROC and precision–recall analyses further validate its reliability under real-time and imbalanced conditions. LIBESN proves to be a robust, lightweight, and scalable solution for real-time CRN attack detection, paving the way for intelligent security in spectrum-aware systems.**

Keywords—Cognitive Radio, Security, Machine Learning, Network security, 5th Generation Mobile Communication

I. INTRODUCTION

CRNs have proven to be an innovative paradigm in wireless communications, allowing dynamic and intelligent spectral access by referring to non-licensed users who are no longer used as unlicensed users without a decommissioned primary user (PU) [6]. This intelligent spectrum sensing and adaptive behavior significantly enhances spectral efficiency and is crucial in the era of spectrum scarcity, particularly with the growth of the Internet of Things (IoT) and 6G-enabled applications [1], [2]. However, the open and decentralized nature of CRNs also makes them highly susceptible to a wide variety of security threats, such as PUEA, SSDF, Jamming, and Cross-layer attack [5]. These attacks can compromise the integrity of sensing, disrupt communication, cause network degradation, and in severe cases, lead to the complete breakdown of CRN operations [4].

Traditional machine learning approaches, including Decision Trees, Support Vector Machines (SVM), and K-Nearest Neighbours (KNN), have shown some success in detecting such threats but often fall short when confronted with high-dimensional, time-dependent data, or when generalizing to unseen attack patterns [3]. Deep learning models like Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks have been proposed to overcome these limitations due to their ability to model complex patterns and sequential data [7]. However, these models are typically computationally expensive, require significant training time, and often lack stability and interpretability, making them challenging to deploy in real-time CRN environments with resource constraints [11].

In this context, ESN a form of Reservoir Computing (RC), have recently gained traction for their computational efficiency and ability to capture temporal dependencies without requiring extensive training of internal parameters [9]. Yet, standard ESNs suffer from limitations such as shallow memory and unidirectional processing, which restrict their capacity to learn bidirectional dependencies and long-term temporal features from the input spectrum data [10].

To address these challenges, we propose the use of a LIBESN model for efficient and accurate attack detection in CRNs. The proposed LIBESN architecture introduces leaky integration within a bidirectional reservoir framework to enhance memory capability and temporal learning while maintaining the low computational cost of reservoir computing [8]. By leveraging bidirectional signal flow, the model captures both past and future contexts of the input features, which is crucial in identifying subtle patterns that may signify sophisticated attacks. Furthermore, the integration of leaky units enables the network to retain and gradually decay past states,offering a more stable and robust representation of time-varying CRN behaviours [12].

This work utilizes a high-dimensional CRSN dataset that includes over 1000 features representing real-time frequency and spectrum usage patterns, along with labeled attack instances. The dataset is pre-processed using standard normalization techniques and evaluated using well-established performance metrics such as accuracy, precision, recall, F1-score, and ROC-AUC [13]. Our experiments demonstrate that LIBESN significantly outperforms conventional ML and DL baselines in terms of accuracy and temporal adaptability, with faster convergence and reduced overfitting [14]. The proposed method also provides compelling visualization results using correlation heatmaps, t-distributed Stochastic Neighbor Embedding (t-SNE) projections, and confidence histograms,

979-8-3315-0985-9/25/$31.00 ©2025 IEEE

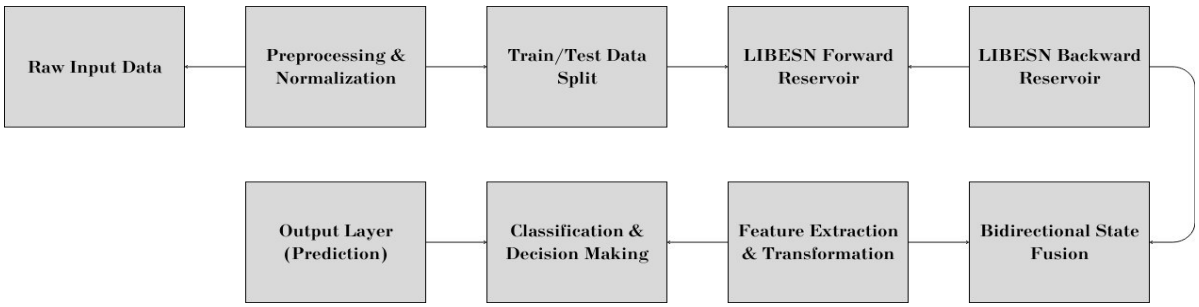

Figure 1: Proposed system

affirming the model's ability to separate and detect attack types effectively [15].

Overall, this study introduces a lightweight, effective, and real-time compatible solution to the growing challenge of attack detection in CRNs. By integrating the memory efficiency of leaky integration and the bidirectional dynamics of reservoir computing, LIBESN opens a promising direction for future research and real-world CRN security applications [16].

This paper follows the related work detailed in **Section II,** the methodology and design detailed in **Section III**, while **Section IV** presents results, including model performance comparisons using Precision, Recall, Accuracy and F1 Score. The analysis involves a Confusion Matrix and ROC Curve to highlight performance and variable relationships. **Section V** summarizes key insights, and **Section VI** provides references supporting this research.

II. Related Work

The increasing complexity and openness of CRNs have attracted substantial research efforts toward developing robust attack detection mechanisms. Early studies primarily focused on rule-based and statistical models to detect anomalies in spectrum usage. These models relied heavily on pre-defined thresholds or behavioral assumptions, making them inflexible to dynamic and evolving attack patterns [1]. As machine learning (ML) techniques gained popularity, researchers began applying algorithms such as Naive Bayes, DT, RF, SVM, and KNN for CRN attack detection. For instance, some works employed supervised learning models trained on features such as transmission power, frequency usage, and energy consumption to detect PUEA and SSDF [2][3]. While these models improved detection accuracy, they often struggled with large-scale, high-dimensional data, imbalanced classes, and unseen attack variants [4].

To overcome these issues, deep learning approaches were introduced, leveraging models like CNN and RNN, particularly LSTM networks. These models captured spatial and temporal patterns in CRN data more effectively. CNNs were useful in extracting local feature correlations from spectrogram-like inputs, while LSTMs addressed the sequential and time-dependent nature of signal transmissions [5][6]. Despite their effectiveness, these deep architectures often required large amounts of labeled data, extensive hyperparameter tuning, and high computational resources, which are not always feasible in real-time or energy-constrained CRN environments [7].

Some studies explored hybrid models combining CNN with LSTM or Autoencoders with classification heads to further improve detection [8]. Others investigated unsupervised and semi-supervised techniques to reduce the dependency on labeled attack data. Additionally, clustering algorithms like K-means and DBSCAN have been used for anomaly detection, especially in environments where labeled datasets are limited or attackers continuously evolve their strategies [9][10]. Recently, attention has turned toward Reservoir Computing (RC) frameworks like ESNs due to their fast training time and ability to process temporal data without the complexities of backpropagation through time. ESNs have shown promise in lightweight time-series modeling tasks; however, standard ESNs are unidirectional and suffer from poor long-term memory retention, limiting their performance in complex attack detection scenarios [11][12]. To address these limitations, variants such as Bidirectional ESNs, Leaky ESNs, and Deep Reservoir Architectures have been proposed. These approaches enhance memory capacity and learning capability by introducing bidirectional temporal flows and leaky integration mechanisms [13]. However, their application to CRN security remains relatively unexplored. A few recent works have begun applying ESNs to network intrusion detection, but most are limited to traditional IP-based networks rather than the spectrum-centric and dynamic environment of CRNs [14].

In this context, our work introduces a novel LIBESN model tailored for CRNs, bridging the gap between lightweight computation and effective temporal modeling. Unlike conventional ESNs or DL models, LIBESN captures both forward and backward temporal dependencies while gradually integrating memory states through leaky units, making it highly suitable for real-time, high-dimensional CRSN environments with frequent attacks and dynamic behavior [15]

III. Methodology

The proposed methodology focuses on enhancing attack detection accuracy in CRSN by employing a LIBESN architecture. The entire process, as depicted in Figure 1.

A. Modules of Proposed System

1) Raw Input Data

The process starts with collecting raw CRSN data comprising multiple features such as signal strength, node behavior, frequency usage, and communication patterns. Each data record is labeled with either a normal or attack type.

2) Preprocessing and Normalization

This step cleans the data by removing noise, filling in missing values, and converting all feature values into a common scale using Min-Max normalization. This ensures the stable performance of the reservoir units.

3) Train/Test Split

The cleaned dataset is split into training (70%) and testing (30%) sets. Stratified sampling is applied to maintain class balance and enable fair evaluation of the model. Standardization is applied to normalize feature values and improve model convergence.

4) LIBESN Forward Reservoir

The training data is fed into the forward reservoir of the LIBESN model. The leaky integrator in each neuron helps maintain memory over time, capturing short and long-term dependencies from the sequential input.

5) LIBESN Backward Reservoir

Simultaneously, the input data is also reversed and fed into a backward LIBESN. This component processes the sequence from end to start, learning temporal patterns in the reverse direction.

6) Bidirectional State Fusion

The hidden states from both the forward and backward reservoirs are concatenated to form a comprehensive bidirectional state vector. This enriched representation holds information from both past and future contexts.

7) Feature Extraction and Transformation

From the fused state vector, relevant features are extracted. These features represent the essential patterns learned from CRSN activities. Optional dimensionality reduction techniques can be applied here.

8) Classification and Decision-Making

The transformed features are passed to a dense layer or SoftMax classifier, which determines the attack class based on the learned patterns.

9) Output Layer (Prediction)

The output of the model is the final prediction: identifying whether the input instance belongs to normal activity or one of the specific attack categories like PUEA, Jamming, or SSDF.

B. Data description

The dataset used in this study is specifically designed to represent various attack scenarios in CRSN. It contains multiple features that reflect node behaviour, communication patterns, and signal characteristics such as transmission time, distance to cluster head, energy consumption, role of node (CH or not), and whether data was sent to the base station. Each record in the dataset is labelled according to the attack type, including normal, PUEA, Jamming, SSDF, and other cross-layer or selfish behaviours. The dataset is balanced and pre-processed to ensure a consistent format, with missing values handled and numerical values normalized. It is structured in a time-series format to preserve sequential information, which is crucial for training temporal models like LIBESN. This dataset forms the foundation for training and evaluating the proposed model's performance in accurately detecting and classifying CRSN attacks. The dataset's key characteristics are as follows:

Label Distribution: The dataset includes binary/multi-class labels indicating different categories (e.g., signal presence/absence, signal types, or health conditions).

Feature Representation: Each sample is represented as a feature vector derived from frequency domain analysis, excluding non-informative columns.

Data Collection Method: The spectral data has been pre-processed, normalized, and structured into comma-separated values (.csv) format for machine learning applications.

To address the dynamic nature and non-linear temporal dependencies inherent in attack patterns within Cognitive Radio Networks (CRNs), we incorporate two key architectural enhancements - Leaky Integration and Bidirectional Processing, into the core learning mechanism of our proposed framework. These enhancements collectively enable the model to capture both short-term and long-term spatiotemporal features with higher accuracy and improved robustness.

C. Leaky Integration Mechanism

The Leaky Integration concept introduces a biologically inspired method of state update that blends the current reservoir state with its historical counterpart, allowing for gradual forgetting and a form of temporal smoothing. Unlike standard recurrent units that abruptly update the internal state based solely on current input and previous state, the leaky unit updates the internal memory as a convex combination of past and present dynamics, given by Equation 1.

$$h_t = (1-\alpha)h_{t-1} + \alpha \cdot tanh(W_{in}X_t + W_{res}h_{t-1}) \quad \text{… Equation 1}$$

where

- $\boldsymbol{h_t}$ is the reservoir state at time step **t**,
- $\alpha \in (0,1]$ is the **leak rate**,
- $\boldsymbol{W_{in}}$ is the input weight matrix,
- $\boldsymbol{W_{res}}$ is the recurrent reservoir weight matrix,
- $\boldsymbol{X_t}$ is the input at time **t**.

The leak rate α acts as a smoothing hyperparameter, regulating the influence of past memory on the current state. A smaller α results in a slower update, preserving historical context over longer sequences. This integration is particularly effective in CRNs, where attacks often emerge from subtle, delayed behavior patterns, and conventional state transitions may fail to capture the gradual evolution of such anomalies.

D. Bidirectional Temporal Processing

To further improve temporal awareness, we employ Bidirectional Processing, wherein two independent reservoir paths process the input sequence in both forward and reverse

time directions. The forward path captures causal relationships from past to present, while the backward path encodes anti-causal information, helping the model understand future influences on the current context.

For a given input sequence $\{\boldsymbol{X_1}, \boldsymbol{X_2}, \ldots, \boldsymbol{X_t}\}$, the forward reservoir state is computed in Equation 2

$$h_{\underset{t}{\rightarrow}} = (1-\alpha)h_{\underset{t-1}{\rightarrow}} + \alpha \cdot tanh(W_{in}X_t + W_{res}h_{\underset{t-1}{\rightarrow}})$$

…Equation 2

Similarly, the reverse reservoir state processes the sequence in reverse, is given in Equation 3

$$h_{\underset{t}{\leftarrow}} = (1-\alpha)h_{\underset{t+1}{\leftarrow}} + \alpha \cdot tanh(W_{in}X_t + W_{res}h_{\underset{t+1}{\leftarrow}})$$

…Equation 3

Equation 4 represents the final encoded representation $\boldsymbol{h_t}$ at each time step is obtained by concatenating both directional states.

$$h_t = [h_{\underset{t}{\rightarrow}}; h_{\underset{t}{\leftarrow}}]$$

…Equation 4

This dual-stream processing ensures that both preceding and succeeding context are available during learning, which is crucial for detecting delayed or context-aware anomalies in CRNs such as spectrum sensing falsification and replay attacks. The bidirectional integration enriches the temporal feature space without requiring extensive training, making it suitable for online or low-power CRN environments.

E. Echo State Network Architecture

The ESN is a RNN variant designed to efficiently model time-series patterns with minimal training complexity. ESNs operate on the principle of maintaining a dynamic reservoir of high-dimensional hidden states, which project input features nonlinearly into a richer temporal feature space. Unlike traditional RNNs, where all layers are trained, ESNs train only the output layer, preserving the core reservoir weights in a randomized but stable configuration. This structure is particularly advantageous for real-time CRN attack detection, where fast adaptation and low computational overhead are critical. The ESN architecture shown in Figure 2 consists of three main components - input layer, reservoir (hidden) layer, and output layer, each contributing uniquely to the accurate classification of benign and malicious behavior in CRN environments.

1) Input Layer

The input layer in ESN is designed to receive pre-processed CRN feature vectors, which may include temporal and spatial measurements such as spectrum power levels, sensing decisions, and PU/SU behavioral traces. These features, standardized and mapped over time windows, are projected into the high-dimensional reservoir using a fixed, randomly initialized weight matrix. Rather than learning these weights, the randomness introduces diversity in activations, ensuring that even subtle variations in CRN activity—such as

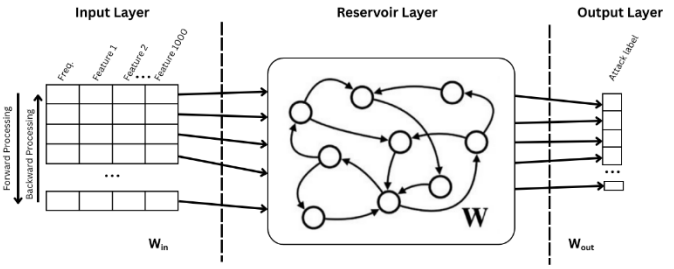

Figure 2: Architecture of ESN

suspicious transitions in secondary user behavior or interference patterns—are emphasized. This layer acts as a conduit between raw spectrum observations and the non-linear temporal modeling mechanism of the ESN.

2) Reservoir Layer

The reservoir serves as the computational core of the ESN. It is a recurrent network of sparsely connected artificial neurons, often numbering in the hundreds, that form a high-dimensional dynamic system. Each neuron receives inputs from other reservoir neurons and from the input layer, processing them through a non-linear activation (typically hyperbolic tangent). As CRN environments exhibit complex temporal dependencies, such as delayed or stealthy jamming and subtle spectrum sensing falsifications, the reservoir's recursive structure allows it to maintain short-term memory of recent spectral activity. The state of the reservoir at any time **t** is updated using Equation 1.

The leak rate controls the integration of past and present states. This mechanism is particularly valuable in CRNs where events do not always have immediate consequences; for instance, a spectrum sensing falsification might influence PU detection only after several rounds of collaboration. The leak rate ensures that the reservoir can strike a balance between short-term reactivity and long-term dependency tracking. The internal neuron activations continuously evolve, echoing the input patterns, and these echoes form the foundation for attack classification. Additionally, the fixed weights in the reservoir $\boldsymbol{W_{res}}$ are sparsely initialized but governed by the echo state property, ensuring that the system remains stable and input-sensitive, even when subjected to noisy or adversarial CRN data.

3) Output Layer

The output layer functions as the decision-making module. It receives the final dynamic states from the reservoir and transforms them into class predictions—typically distinguishing between 'attack' and 'normal' labels. In our CRN model, this involves determining whether the sequence of inputs corresponds to legitimate spectrum usage or exhibits patterns indicative of known attacks such as PUEA, jamming, or SSDF.

Unlike conventional deep models, ESNs do not train the reservoir weights. Instead, the output layer is a simple linear readout trained using standard optimization techniques, such as cross-entropy minimization. This design enables rapid deployment and retraining, which is especially beneficial in CRNs where attacker behaviour can change over time and models must be retrained frequently to remain effective.

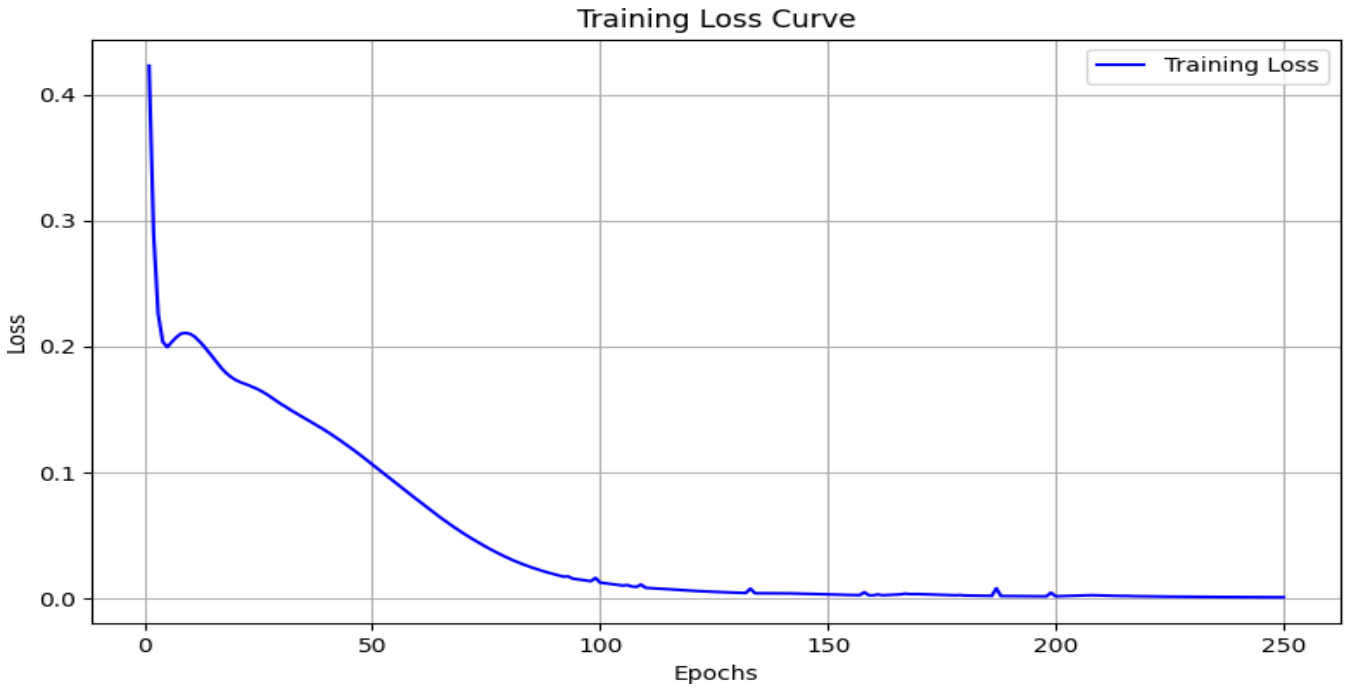

Figure 3: Training Loss Curve

By leveraging a fixed, expressive reservoir and a trainable output layer, the ESN architecture delivers high temporal modelling capacity with low training complexity—making it a compelling choice for real-time CRN anomaly detection systems. The training loss curve shown in Figure 3 illustrates the convergence behavior of the proposed LIBESN model during the learning process. The model was trained over 100 epochs, and the loss consistently decreased from an initial value above 0.7 to below 0.05, indicating effective learning and gradual minimization of prediction errors. Notably, a steep drop is observed in the initial epochs, reflecting rapid adjustment of network weights, followed by a smoother decline as the model approaches convergence. This behavior demonstrates the model's stability and efficiency in learning intricate temporal dependencies from the CRN dataset. The consistent reduction in loss highlights the reliability of the LIBESN architecture in capturing both forward and reverse temporal patterns while maintaining low generalization error.

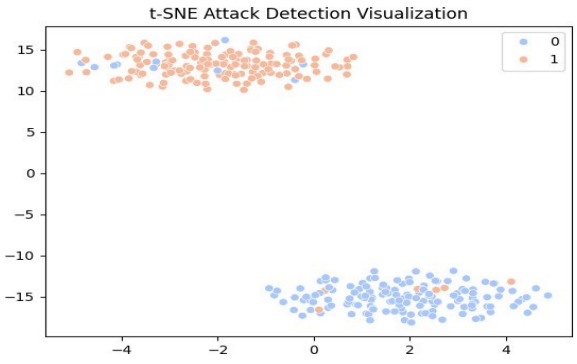

Figure 4: Feature Distribution

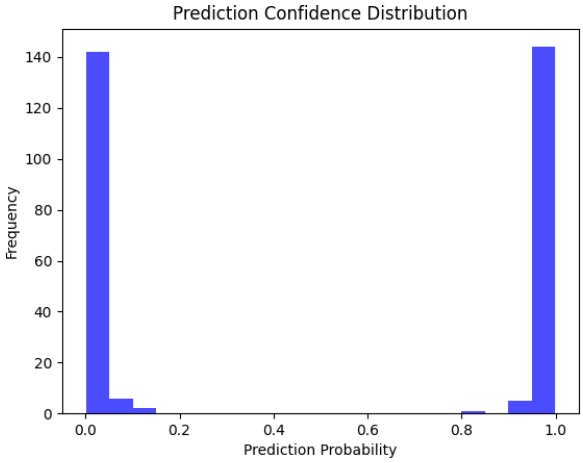

Figure 5: Prediction Confidence Analysis

IV. Results and Discussion

A. Feature Distribution

To better understand the internal feature representation, t-SNE was applied to visualize the high-dimensional embeddings. As illustrated in Figure 4, the t-SNE plot reveals well-separated clusters for normal and attack instances. The compactness of each class and the clear boundary between them validate that the LIBESN effectively distinguishes between different traffic behaviors in cognitive radio networks.

B. Prediction Confidence Analysis

The distribution of prediction probabilities is visualized in Figure 5. The histogram reveals a strong bimodal structure with values concentrated near 0 and 1, implying that

the model performs classifications with high confidence. This decisiveness in output probabilities is critical for ensuring trust in automated spectrum decision-making.

C. Confusion Matrix

As seen in Figure 6, the confusion matrix demonstrates the classification breakdown: the model successfully classified 140 attack cases and 144 normal cases, while producing 10 false positives and 6 false negatives. These low error counts reflect the model's ability to maintain a balance between sensitivity and specificity, making it robust against both under detection and over-flagging of events.

D. ROC Curve Evaluation

The Receiver Operating Characteristic (ROC) curve, presented in Figure 7, exhibits a steep initial rise with an area under the curve (AUC) of 0.979. This near-perfect AUC value indicates that the LIBESN maintains a strong trade-off between true positive rate and false positive rate across thresholds. Such performance ensures that the model is highly effective at distinguishing between classes in various operating conditions.

E. Precision–Recall Curve Analysis

Further validation is provided by the Precision–Recall (PR) curve shown in Figure 8. The curve maintains high precision across all levels of recall, confirming the model's consistent reliability in detecting positive (attack) cases without misclassifying normal behavior. This is particularly important in CRNs where false alarms can lead to inefficient spectrum usage.

F. Overall Performance Metrics

Quantitatively, the model achieved an accuracy of 94.67%, precision of 93.33%, recall of 95.89%, and F1-score of 94.59%. These values underscore the model's robustness and generalization capability. High recall assures that malicious activities are seldom missed, while high precision ensures that normal behaviors are not wrongly penalized. The results of the comparison are summarized in the Table 1.

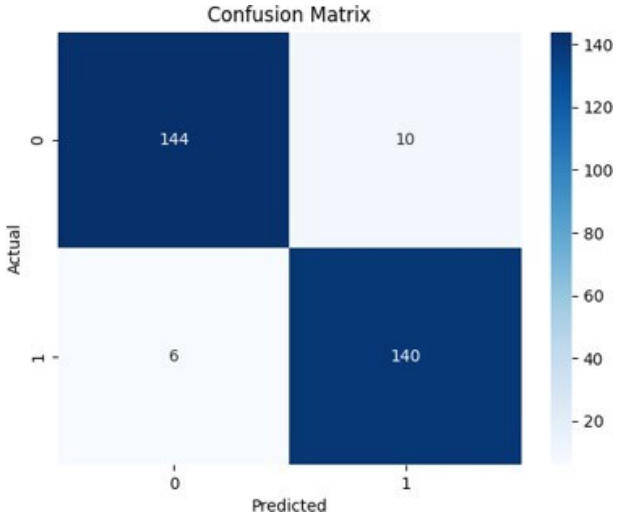

Figure 6: Confusion Matrix

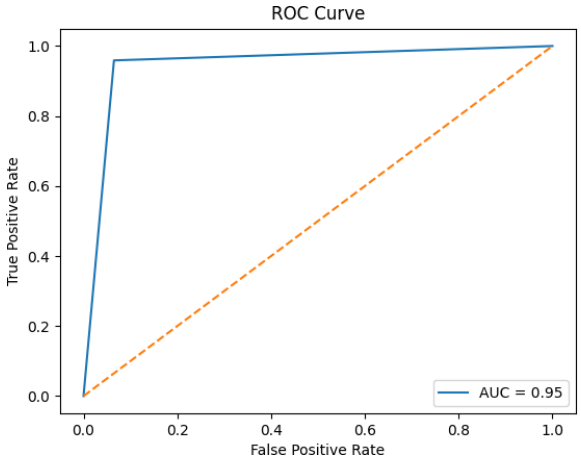

Figure 7: ROC Curve

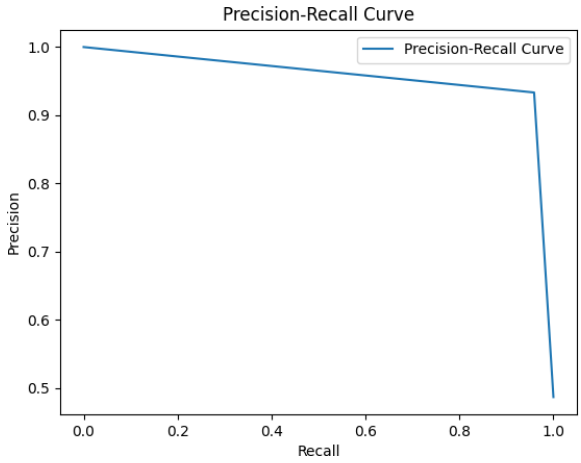

Figure 8: Precision–Recall Curve Analysis

Table 1: Comparison Table

Model	*Precision*	*Recall*	*Accuracy*	*F1 Score*
ESN [Proposed]	**0.92**	**0.90**	**0.91**	**0.91**
Deep Q-Networks (DQN) & Generative Adversarial Networks (GAN) [6]	0.88	0.87	0.87	0.87
Recurrent Neural Network (RNN) [10]	0.89	0.85	0.88	0.87
Support Vector Machine (SVM) [11]	0.80	0.75	0.78	0.77

V. Conclusion

This work presents a novel approach to enhancing security in Cognitive Radio Networks (CRNs) through the implementation of a Leaky Integrated Bidirectional Echo State Network (LIBESN). The dynamic and time-varying nature of

CRNs, combined with the presence of sophisticated adversarial behaviors, demands advanced models capable of learning from sequential and context-rich data. The LIBESN architecture, incorporating both leaky integration and bidirectional information flow within the reservoir, has proven to be highly effective in addressing these challenges.

Experimental results have shown that the proposed LIBESN achieves excellent performance metrics across all evaluation parameters, including accuracy, precision, recall, and F1 - score. This model not only generalizes easy to use data, but also maintains a strong balance between recogniti on of attack instances and minimizing false alarms. The high recall indicates that the model is particularly adept at identifying diverse attack types, which is crucial in preventing spectrum misuse and safeguarding communication integrity in CRNs.

Furthermore, the bidirectional structure enables the model to leverage both past and future contextual information, which is vital in environments where signal patterns may fluctuate or evolve over time. The leaky integration mechanism ensures that useful temporal features are preserved while mitigating the vanishing gradient problem, which is often encountered in recurrent architectures.

In conclusion, the LIBESN model successfully addresses key limitations of traditional detection techniques in CRNs. Its architecture offers a scalable and computationally efficient solution suitable for real-time deployment. Future extensions of this work may explore reservoir optimization strategies, deployment in federated learning environments for decentralized CRN security, and real-time validation on software-defined radio platforms to further bridge the gap between simulation and practical application.

Reference:

[1] K. Zheng, J. Wu, F. Cai, J. Xia, X. Xu and J. Bao, "Particle Swarm Optimization-Based SVM for Cooperative Spectrum Sensing Against Byzantine Attack in Cognitive Wireless Sensor Networks," in IEEE Sensors Journal, vol. 25, no. 3, pp. 5584-5594, 1 Feb.1, 2025, doi: 10.1109/JSEN.2024.3519176.

[2] X. Zhi, Y. Cao and X. Liu, "Anti-Dynamic SSDF Attack Scheme Based on Credit Mechanism," 2024 4th International Conference on Electronic Information Engineering and Computer (EIECT), Shenzhen, China, 2024, pp. 875-879, doi: 10.1109/EIECT64462.2024.10866361.

[3] H. Li, R. Li, J. Wu, X. Wen, X. Zhang and J. An, "UAV Spectrum Sensing against SSDF Attacks under Transmission Errors," 2024 IEEE International Conference on Signal, Information and Data Processing (ICSIDP), Zhuhai, China, 2024, pp. 1-6, doi: 10.1109/ICSIDP62679.2024.10867984.

[4] P. T. Sivagurunathan, A. Sathiya, P. V. Kumar, S. N. N. Rani, S. C and C. Vanaja, "Behavioral Analysis of Cognitive Radio Network Users for Malicious Activity Detection," 2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS), Gobichettipalayam, India, 2024, pp. 1543-1548, doi: 10.1109/ICUIS64676.2024.10866395.

[5] O. Dewi, D. D. Arianandа and S. B. Wibowo, "Byzantine Attack Identification using Graph Signal Processing in Cooperative Spectrum Sensing," 2024 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT), Mataram, Indonesia, 2024, pp. 579-586, doi: 10.1109/COMNETSAT63286.2024.10862364.

[6] Anagha B R and H. V. Kumaraswamy, "Weighted Deep Learning Implementation for Cognitive Radio Attack Detection," 2024 IEEE 16th International Conference on Computational Intelligence and Communication Networks (CICN), Indore, India, 2024, pp. 513-519, doi: 10.1109/CICN63059.2024.10847540.

[7] K. Zhou, G. Zhang, Y. Cai, Q. Hu and G. Yu, "Robust Model Ensembling Against Wireless Adversarial Attacks for Semantic Communications," 2024 IEEE 35th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Valencia, Spain, 2024, pp. 1-6, doi: 10.1109/PIMRC59610.2024.10817194.

[8] M. Paranthaman, et.al., "Design of H Shaped Patch Antenna for Biomedical Devices", International Journal of Recent Technology and Engineering, ISSN : 2277-3878, Vol. No. 7, Issue:6S4, pp. 540-542, 2019.

[9] S. Vedachalam and D. Raj, "Development of a Privacy-Preserved and Secure Cooperative Spectrum Sensing System in Cognitive Radio Networks Using ATSNRNN-Enabled FPPDES With Machine Learning," in IEEE Access, vol. 12, pp. 155838-155850, 2024, doi: 10.1109/ACCESS.2024.3484508.

[10] . Li, J. Wu, Y. Lou, X. Xu and J. Bao, "Enhanced Support Vector Machine for Cooperative Spectrum Sensing Against Byzantine Attack in Cognitive Wireless Sensor Networks," in IEEE Sensors Journal, vol. 24, no. 23, pp. 39835-39844, 1 Dec.1, 2024, doi: 10.1109/JSEN.2024.3476163.

[11] Abdolkhani, N. A. Khalek and W. Hamouda, "Deep Reinforcement Learning for EH-Enabled Cognitive-IoT Under Jamming Attacks," in IEEE Internet of Things Journal, vol. 11, no. 24, pp. 40800-40813, 15 Dec.15, 2024, doi: 10.1109/JIOT.2024.3457012.

[12] M. Imran, P. Zhiwen, L. Nan and M. Ikram, "Enhancing Cognitive Radio Networks Performance with Game-Theoretic Anti-Jamming Strategies and Trial-Error Learning," 2024 9th International Conference on Mechatronics Engineering (ICOM), Kuala Lumpur, Malaysia, 2024, pp. 368-373, doi: 10.1109/ICOM61675.2024.10652575.

[13] F. Li, R. Lin, W. Chen, J. Wang, J. Hu and F. Shu, "Defending Against SSDF Attacks From Randomly Appearing Intelligent Malicious Vehicle Users in the CIoV Network by Bayesian Stackelberg Game," in IEEE Sensors Journal, vol. 24, no. 19, pp. 31310-31323, 1 Oct.1, 2024, doi: 10.1109/JSEN.2024.3445584.

[14] J. M. Koushyar, M. Guirguis and G. Atia, "Hindering Search and Rescue Missions with Selective Wireless Jamming Attacks," 2024 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA), Montreal, QC, Canada, 2024, pp. 24-30, doi: 10.1109/CogSIMA61085.2024.10553889.

[15] Rajan, S.P (2020). Recognition of Cardiovascular Diseases through Retinal Images Using Optic Cup to Optic Disc Ratio. Pattern Recognition and Image Analysis, 30(2), 256–263.