International Journal of Safety and Security Engineering
Vol. 15, No. 1, January, 2025, pp. 181-187
Journal homepage: http://iieta.org/journals/ijsse

Security Threat Analysis in 5G Cognitive Radio Networks: A Deep Learning Ensemble Approach

M. Minilal*, M. Meena

Department of ECE, Vels Institute of Science Technology and Advanced Studies, Chennai 600117, India

Corresponding Author Email: minilal.raj@gmail.com

https://doi.org/10.18280/ijsse.150119

Received: 16 December 2024
Revised: 2 January 2025
Accepted: 18 January 2025
Available online: 31 January 2025

Keywords:
cognitive radio network, malicious user detection, deep learning, LSTM algorithm GRU algorithm

ABSTRACT

Spectrum constraints are a significant problem in the field of communication networks. A cutting-edge wireless communication technology called cognitive radio allows devices to maximize spectrum consumption and adjust to their surroundings dynamically. Despite its promise, cognitive radio technology has several security vulnerabilities that endanger the network. Cognitive radio security is crucial to accomplish dynamic spectrum access. We can ensure that cognitive radio technology is deployed and operated securely by being aware of and responding to these security concerns. In cognitive radio, artificial intelligence is crucial in identifying malevolent users. This work employs an ensemble of long-term, and short-term, GRU approach to distinguish fraudulent users from authorized users. The suggested method for detection was implemented on data sets containing several parameters, including SNR and modulation scheme energy. The proposed algorithm shows compelling evidence of outperforming the state-of-the-art algorithms in detection.

1. INTRODUCTION

The swift development of 5G technology is driving extraordinary innovations in the telecommunication industry, resulting in remarkable enhancements to data speed, network capacities, and connectivity options. By enabling unlicensed users, cognitive radio has the potential to be a transformative technology that solves problems related to spectrum shortages. Dynamic spectrum access and spectrum awareness are crucial features of cognitive radio networks (CRN) [1]. Cognitive Radio devices provide real-time sensing and detection capabilities for available spectrum bands and can intelligently transition between various spectrum bands to enhance communication. Spectrum efficiency can be improved by maximizing capacity, decreasing congestion, and optimizing spectrum consumption.

The cognitive radio system, although offering several benefits, is not immune to malicious attacks, which can compromise its functionality and security. Critical malicious attacks are [2]:

Spectrum sensing and data falsification: malevolent nodes can alter spectrum sensing data, resulting in inaccurate choices. This is one of the leading security concerns with cognitive radio.

Primary user emulation attack: malicious nodes can impersonate primary users, leading cognitive radio devices to unnecessarily exit the channel. This technique is known as the "primary user emulation attack."

Interference and jamming: malevolent nodes can impede intelligent radio transmission.

Eves dropping and privacy: CR devices can intercept private data.

To address the complexities of identifying malicious users, this study leverages robust artificial intelligence methods [3]. Specifically, it presents a deep learning approach for detecting illegitimate users in cognitive radio networks (CRNs). Deep learning, a subset of machine learning, utilizes artificial neural networks to analyze and interpret complex data. By mimicking the human brain's structure and function, deep learning algorithms can refine their performance independently.

This research focuses on Recurrent Neural Networks (RNNs), particularly suitable for sequential data, to investigate security concerns in CRNs. The expanding use of 5G cognitive radio networks has increased their vulnerability to novel security threats, rendering traditional protection measures ineffective. The intricate technologies underlying these networks present significant challenges in detecting and mitigating malicious activities.

Conventional detection methods are inadequate against rapidly evolving and complex threats. Therefore, 5G cognitive radio networks require advanced, real-time detection mechanisms. This research proposes a pioneering, ensemble-based framework for identifying malicious users in 5G cognitive radio networks. By integrating multiple deep learning algorithms, the framework aims to enhance detection accuracy, robustness, and adaptability.

A novel ensemble model, combining Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) techniques, is proposed to identify and classify malicious users in cognitive radio networks. The model's performance is evaluated through an extensive simulation study, utilizing a proprietary database, to assess its effectiveness in detecting malicious activities.

2. RELATED WORK

In reference [4], GRU -SVM-based threat detection system for CRNs. This approach combines the strength of GRU (Gated recurrent units) and SVM (support vector machine) to effectively notice the threats in CRNs. The GRU-SVM-based system has demonstrated improved detection accuracy and reduced false alarms compared to traditional threat detection approaches. The system effectively detected various types of security threats in CRNs, including primary user emulation attacks as well as spectrum sensing and data falsification attacks. In CRN, the GRU-SVM model has an 82.45 percent testing accuracy and an 80.99 percent training accuracy in identifying hostile users.

Benazzouza et al. [5] propose a novel prediction model that combines stacking and DL techniques for malicious user detection and spectrum sensing. The authors use a dataset of CRN simulations to evaluate the proposed model. The data set includes features like signal-to-noise ratio, signal strength, and modulation type. The outcomes determine that the suggested model achieves a higher detection accuracy of 95.6 percent and a low false alarm rate (2.1) for malicious user detection. This proposed model provides an effective solution for malicious user detection and spectrum sensing in CRNs. The combination of stacking and DL techniques improves the detection accuracy and reduces false alarms.

CRN [6] are vulnerable to SSDF (spectrum sensing and data falsification) attacks, which can compromise the security and reliability of the network. For SSDF attack detection in CRNs, the authors suggest a unique hierarchical ensemble extreme learning machine (HCME-ELM) based on cats and mice. Three steps make up the suggested approach: extreme learning machine, hierarchical ensemble, and data pre-processing. The authors evaluate the proposed HCME-ELM method using a simulated CRN network. The result shows that the proposed method achieves high detection accuracy (97.5) and low false alarm rate (2.1) for SSDF attack detection. The HCME-ELM method provides an effective solution for SSDF attack detection in CRNs. The detection accuracy is increased and the false alarm rate is decreased by using the hierarchical ensemble technique using ELM as the basic classifier.

The IoT (Internet of things) and 5th generation networks are vulnerable [7] to various types of intrusions including malware, ransomware, and denial of service (Dos) attacks. These assaults are not detectable by conventional security measures like intrusion detection systems and firewalls. To identify breaches in IOT and 5G networks, the authors suggest a cognitive security framework that makes use of the DL approach. The authors evaluate the proposed framework using a dataset of network traffic data from IoT and 5G networks. The findings demonstrate that the suggested framework detects intrusions with a low false positive rate of 2.1% and a high accuracy of 95.6%.

Reference [8] presents a novel framework, Optimal Deep Learning Empowered Malicious User Detection for Spectrum Sensing (ODL-MUDSS), designed to automatically identify and classify malicious users (MUs) in Cognitive Radio Networks (CRNs). The ODL-MUDSS model leverages deep belief networks (DBNs) to detect MUs with high accuracy. To further enhance the recognition performance of DBNs, the model incorporates the sand cat swarm optimization (SCSO) algorithm, leading to improved detection results. The performance of the ODL-MUDSS technique is extensively validated through various experiments. The comprehensive evaluation results demonstrate the superiority of the ODL-MUDSS model over existing approaches, achieving exceptional performance metrics, including: Accuracy: 97.75%, Precision: 97.75%, Recall: 97.75%, F-score: 97.75%.

3. SYSTEM MODEL

The application of DL approaches has led to notable progress in the fields of sequential data modeling and natural language processing (NLP). Complex patterns and correlations in sequential data can be captured with remarkable performance by GRU (Gated Recurrent Unit) and LSTM (Long Short-Term Memory) architectures. However, individual LSTM and GRU models are not immune to limitations. LSTMs often suffer from high computational costs and vanishing gradients, whereas GRUs face challenges in capturing long-term dependencies. This study suggests a novel ensemble model that combines the advantages of GRU and LSTM architectures in a synergistic manner to overcome these constraints. In this case, we employ the ensemble model of the LSTM model as well as the GRU model to detect malicious users (Figure 1). Such algorithms are RNN types that are ideal for analyzing sequential data, such as user signals in a CRN.

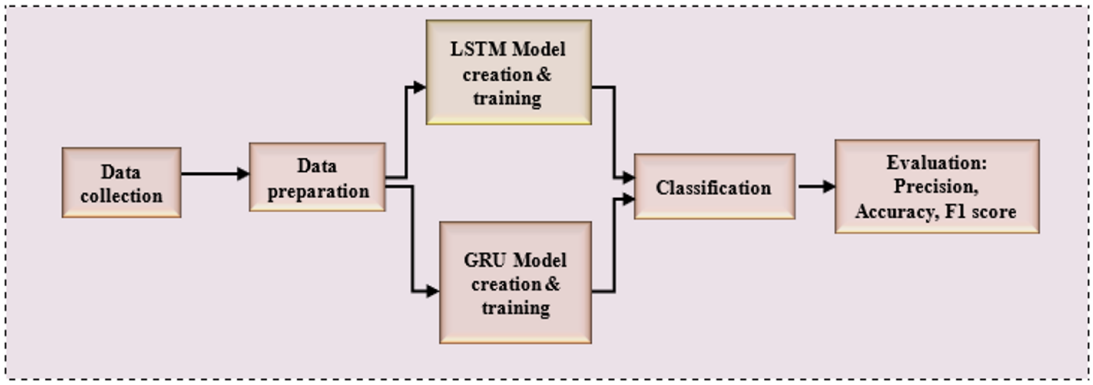

Figure 1. System model

LSTM is a widely utilized architecture [9] of RNN in DL. Using its long-term dependencies, this method is perfect for producing sequence predictions. Long-term memory, short-term memory, and recent past event data are used to make decisions. By permitting the gradient to pass through the cell state and maintaining a constant error flow that prevents the gradient from vanishing, LSTM can manage long-term dependencies. As shown in Fig. 1, the LSTM-GRU Ensemble

Model's workflow involves a three-stage process, consisting of data preprocessing, classification, and identification of malicious users. The experiments are conducted with the help of own dataset generated in the lab [10]. The different stages included in the classification process are data collection and pre-processing. Data preparation involves dividing it into training, testing sets, and validation sets.

The third stage of LSTM&GRU model creation provides for the selection of several layers and activation functions of the network. Further steps are training, classification, and evaluation. During the training process, data is input into the LSTM model, as well as the GRU model learns patterns and relationships in the data and monitors the performance metrics [11]. The classification stages model uses the trained LSTM model to classify new unseen sequences and select the class including the higher possibility as the predicted class.

3.1 LSTM and GRU architecture

LSTM cells constitute the essential parts of LSTM networks shown in Figure 2. Each cell possesses an output gate, an input gate, as well as a forget gate [12]. An LSTM layer is created when a single LSTM cell gets input from the layer above and outputs to the layer below. The LSTM architecture is made up of at least one LSTM layer. Prediction or else categorization is done using the output of the last LSTM layer. The cell state of the LSTM layer keeps the data over an extended period, and for a brief interval of time, the information is stored in a hidden state. The sigmoid [13] function and tanh layers are the activation functions. Three gates are there in each LSTM cell: output gate, input gate, as well as forget gate.

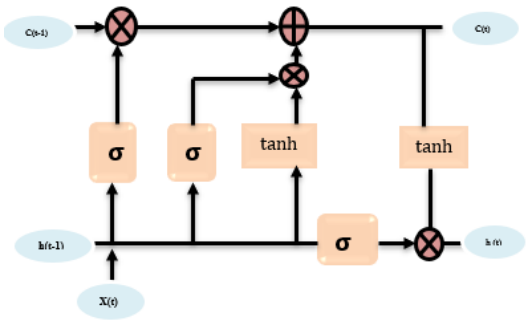

Figure 2. LSTM architecture

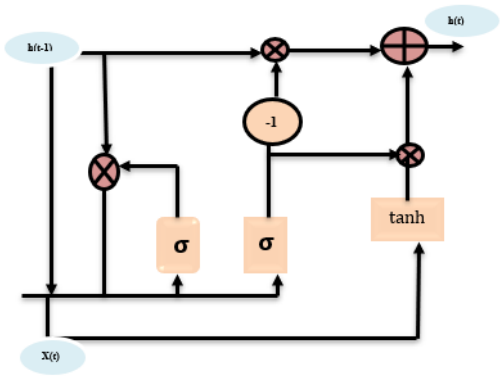

Figure 3. GRU architecture

A particular kind of RNN architecture called GRU is shown in Figure 3 made to process sequential data, including time series data, natural language processing, and speech recognition. The GRU (gated Recurrent Unit) architecture comprises four primary components: input gate, output gate, cell state, reset gate, along with hidden state, which work together to facilitate efficient and effective sequential data processing. The input gate regulates the influx of fresh information into the cell state. The present input and the prior hidden state are utilized as inputs to produce a number ranging from 0 to 1, indicating the quantity of new information to be incorporated into the cell state.

To regulate the information flow from prior hidden state to the present hidden state, the reset gate is essential. It calculates how much historical data should be eliminated by producing a value among 0 and 1 depending on the current input and the earlier hidden state. The cell state, on the other hand, serves as the GRU's internal memory, which is updated by integrating the previous cell state, input gate, and reset gate. In the GRU architecture, the hidden state constitutes output generated at each time step, resulting from the interaction between the output gate and cell state. Additionally, the output gate controls the information that flows from the hidden state to the output by using the input and prior hidden state to calculate a value between 0 and 1, which shows the magnitude of the output information.

The entry of fresh data into the cell is controlled by the input gate.

$$I_G = \sigma[w^I(F_t, Y_{t-1}) + C^I] \tag{1}$$

Output gate Manages the cell's output.

$$O_G = \sigma[w^O(F_t, Y_{t-1}) + c^o] \tag{2}$$

The forget gate controls the data that should be discarded from the prior cell state.

$$F_G = \sigma[w^F(F_t, Y_{t-1}) + c^F] \tag{3}$$

Memory cell that is given by

$$M_t = \tanH[w^M(F_t, Y_{t-1}) + c^M] \tag{4}$$

4. RESULT AND DISCUSSION

The proposed ensemble model harnesses the synergistic strengths of LSTMs and GRUs to enhance the precision and resilience of sequential data modeling. By integrating the long-term memory capabilities of LSTMs with the efficient gating mechanism of GRUs, the ensemble model can more effectively capture intricate patterns and relationships in sequential data. This section examines the LSTM&GRU ensemble approach's MU identification results. We employed our unique datasets, which were specifically designed and compiled for the experiments. The information about the dataset is outlined in Table 1. We prepared datasets of 10,000 samples. We conducted several thorough simulations to assess how well the suggested approach performed [14]. Thirty percent of the dataset is put aside for testing throughout the training phase, while the rest of the 70 percent is utilized for training. The model is trained utilizing 7000 data samples, and 3000 data samples are chosen for model testing. Table 1 demonstrates the sample dataset of characteristics, including modulation scheme, power level, frequency band,

transmission time, entropy, SNR, and energy of the signal. The data set is labeled as malicious and primary users according to the set parameters. The frequency band used for this study is 2.4GHz.

The proposed model's performance in detecting MUs is evaluated using confusion matrices, as illustrated in Figures 4 and 5. These matrices facilitate a comprehensive evaluation of the model's accuracy, pinpointing its strengths and weaknesses. In the context of binary classification, the confusion matrix results comprise four essential variables, with true positives and true negatives being vital indicators of performance [15].

The following measures are used to assess the model's performance:

True Positive (TP): Actual positive occurrences are appropriately predicted by the model as positive. Malicious users are effectively identified as such in this suggested strategy.

True Negative (TN): The actual negative instance is properly predicted by the model to be negative. Primary users are successfully identified as primary users in this model.

False Negative (FN): Primary users are mistakenly thought to be malicious.

False Positive (FP): The Malicious users are incorrectly identified as the primary users.

Table 1. Data set model

Modulation	Power Level (dBm)	Frequency Band	Transmission Time	Entropy	SNR (dB)	Energy	Class
QPSK	-53.463	2.5GHz	Regular	6.324234	8.750942	18.11682	Malicious
QAM	-71.2432	2.4GHz	Irregular	0.773697	7.748341	7.094953	Malicious
BPSK	-86.4234	2.5GHz	Regular	3.879428	14.78016	26.41114	Malicious
BPSK	-88.3579	2.1GHz	Irregular	2.733452	16.89098	28.00546	Malicious
QPSK	-68.231	1.8GHz	Regular	1.263381	8.302331	17.57211	PU
QPSK	-60.8332	1.8GHz	Regular	3.89735	9.362323	19.51454	PU
QPSK	-85.9626	2.4GHz	Regular	0.394418	12.63905	23.13752	Malicious

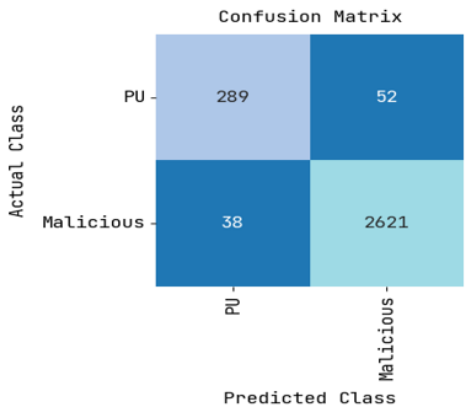

Figure 4. Confusion matrix of testing

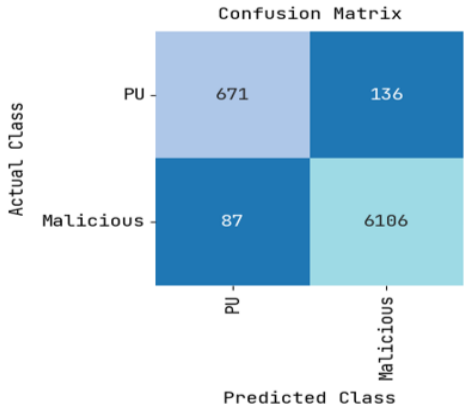

Figure 5. Confusion matrix of training

The goal of this DL models is to identify complex patterns as well as relationships within training data, enabling accurate predictions and classification decisions. Evaluating precision, accuracy, recall, as well as F-score is essential to ensure optimal model performance, as these metrics offer a comprehensive understanding of model strengths, weaknesses, and opportunities for refinement.

Accuracy: The percentage of correctly categorized nodes relative to the total number of nodes evaluated is known as accuracy. Its definition is as follows:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{5}$$

Precision is a quality metric when assessing a machine-learning model. When making positive predictions, it gauges how accurate the model is. It may be explained as:

$$\text{Precision} = \frac{TP}{TP + FP} \tag{6}$$

An ML model can be assessed as a quantity metric. It computes the overall number of successful positive predictions made out of all possible positive predictions. It is characterized as Recall.

$$\text{Recall} = \frac{TP}{TP + FN} \tag{7}$$

The balance between precision as well as recall is evaluated by the F score, that is the harmonic mean of both precision and recall. The ideal value of the F_{score} is 1.

$$F_{score} = \frac{2 * (Precision * Recall)}{(Precision + Recall)} \tag{8}$$

MCC measures the correlation between predicted and actual classes.

$$MCC = \frac{(TP * TN - FP * FN)}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}} \tag{9}$$

Table 2 demonstrates the performance matrices of the recommended model. Comparing the models using a curve-based method, such as the PR (Precision-Recall) curve, is another way to explore the various models' classifier performance. Figures 6 and 7 illustrate the suggested model's

P-R curve. The precision-recall curves focus on the trade-off between precision & recall. The PR curve uses the x-axis to show the recall value and the y-axis to show the precision value. A higher recall indicates fewer false negatives, whereas a higher accuracy value indicates fewer false positives.

Table 2. Performance calculations of training data

Performance Metrics	Training			Testing		
	PU	Malicious	Overall	PU	Malicious	Overall
Accuracy	.8135	0.986	0.9088	0.8475	0.9857	0.9166
Precision	0.8852	0.9782	0.9317	0.8838	0.9805	0.9322
Recall	0.8315	0.986	0.9088	0.8475	0.9857	0.9166
F-Score	0.8575	0.9821	0.9198	0.8653	0.9831	0.9242
MCC	0.8401	0.8401	0.8401	0.8486	0.8486	0.8486

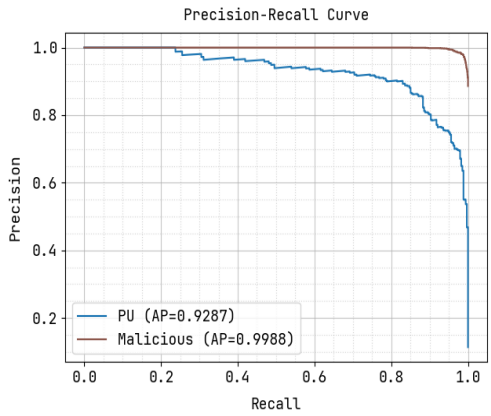

Figure 6. P-R Curve of testing model

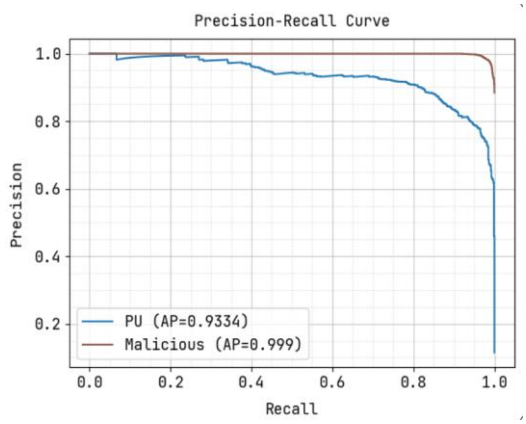

Figure 7. PR Curve of training model

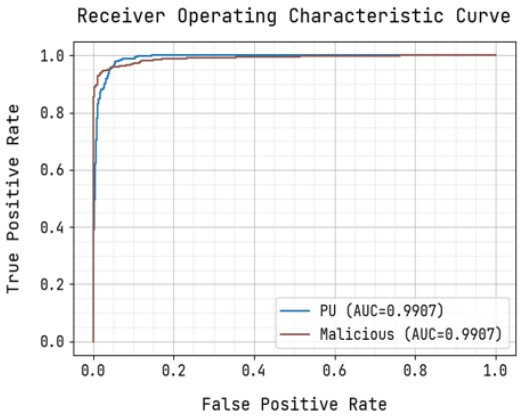

Figure 8. ROC curve of the testing model

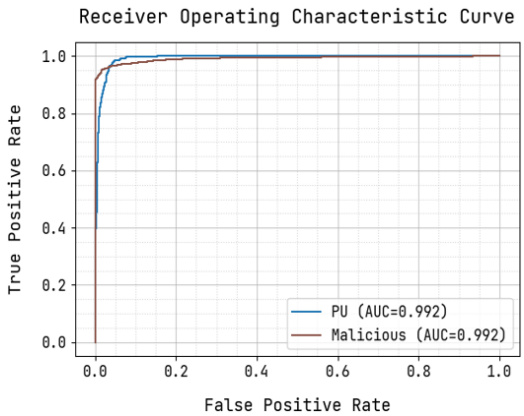

Figure 9. ROC curve of training model

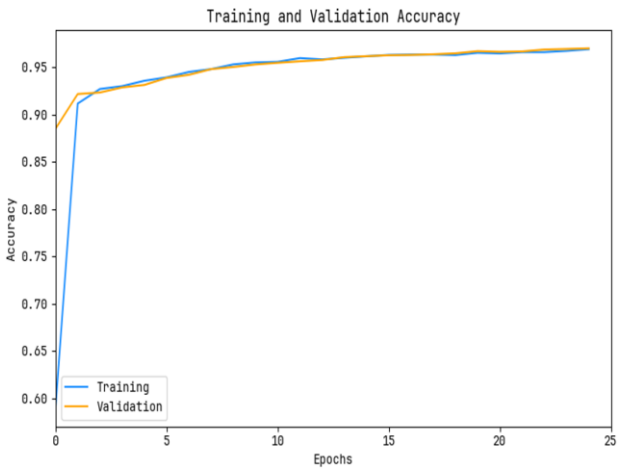

Figure 10. Training & validation accuracy

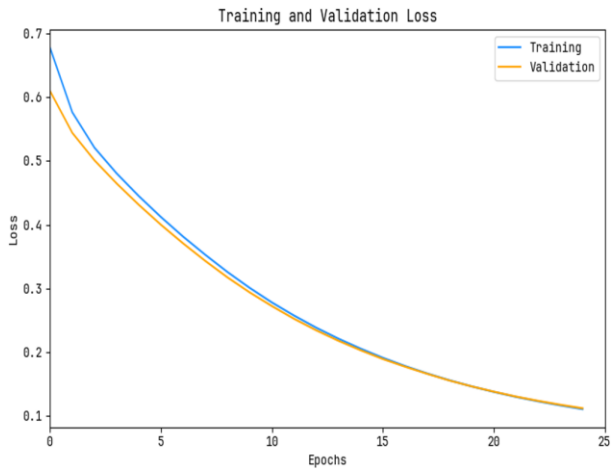

Figure 11. Training & validation loss

Table 3. Training & validation accuracy and loss

Epochs	Training Accuracy	Validation Accuracy	Training Loss	Validation Loss
1	0.5891	0.885	0.6771	0.6094
5	0.9357	0.9313	0.4449	0.4312
10	0.9551	0.953	0.301	0.2939
15	0.9616	0.9617	0.2058	0.2033
20	0.9653	0.967	0.1467	0.1467
25	0.9691	0.97	0.1111	0.1124

A steep precision-recall curve indicates a high-performance classifier. The average precision (AP) is the summary metric that measures the classifier's performance across all recall values. A higher AP indicates a better classifier. In the proposed model, the AP value of the primary user is 0.93, and for malicious users, AP=0.99 A high-quality classifier will always have an AP value greater than 0.5 or equal to 1. Therefore, the suggested model provides a superior classification.

The performance of a classifier is visually represented by the ROC curve, that contrasts the true positive rate and false positive rate across distinct thresholds [16]. This plot provides another way to visualise the performance of a classifier [17]. The percentage of real positive cases that the classifier accurately recognizes is evaluated by the true positive rate. A good classifier, requires a high TPR preferably greater than 0.9. The proposed model classifier shows a good TPR for testing and training models.

The classifier's efficacy is evaluated using the AUC metric, demonstrating a strong link between scores (0.5-1) and accuracy. Figures 8 and 9 illustrate the proposed LSTM-GRU model's exceptional performance, achieving AUC values of 0.992 (training) and 0.9907 (testing) with an 80:20 train-test split, outperforming other models. Moreover, training accuracy and validation accuracy are crucial parameters, indicating the model's reliability. The training and validation accuracy plots in Figures 10 and 11 provide insight into the model's performance. A well-performing model should achieve high accuracy in both training and validation phases, indicating good generalization and robustness [18]. By dividing the total number of training samples by the number of correct predictions, the training accuracy has been determined. To calculate validation accuracy, divide the number of correct predictions by the total number of validation samples [19]. Separate datasets are used for validation accuracy, which are not used during training. Validation accuracy is a better indicator of the model performance on real-world data. The accuracy of the training and validation sets is summarized in Table 3. As the model undergoes more training epochs, its validation accuracy consistently improves, outperforming other models and showcasing its enhanced capabilities.

Overfitting is the reason why training accuracy is usually higher than validation accuracy. For a model to perform well, both validation and training accuracy should be high, and the margin between the two should be minimal. A low training loss suggests that the model is fitting in the training data effectively. Loss of training is a measure of the proposed model's error. Usually, validation loss exceeds training loss [20]. The average loss over the validation samples on a separate validation data set is used to calculate validation loss. Table 3 demonstrates the accuracy as well as training loss along with validation data for different epochs. A comparison of the LSTM-GRU model with existing methods is presented in Figure 12. The simulation results reveal that the GRU-SVM model underperforms, whereas the GRU-LSTM model achieves enhanced performance in detecting malicious users in cognitive radio networks (CRN).

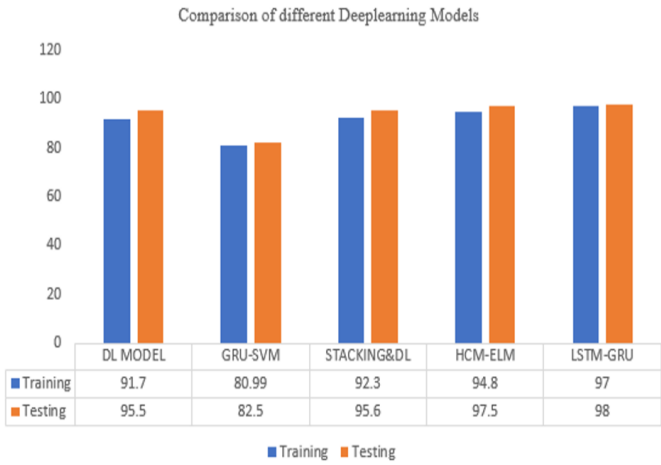

Figure 12. Comparison of different models

5. CONCLUSIONS

This study highlights the importance of artificial intelligence, particularly the LSTM-GRU ensemble model, in identifying malicious users in Cognitive Radio Networks (CRNs). The proposed model offers a triple advantage: superior accuracy, enhanced robustness, and improved efficiency. By combining the strengths of LSTMs and GRUs, the ensemble model achieves higher accuracy and demonstrates improved resilience to noisy or missing data. Additionally, the incorporation of GRU reduces computational costs, making the model more suitable for large-scale sequential data modeling tasks.

The results show that the LSTM-GRU model accurately detects malicious users with a peak accuracy of 98%. To further improve the model's performance, future studies should focus on developing more diverse and extensive datasets. This study validates the effectiveness and reliability of the LSTM-GRU model in detecting fraudulent users within CRNs.

Future research can explore the development of a hybrid approach that combines metaheuristic optimization techniques with multimodal fusion methods to enhance the accuracy and effectiveness of malicious user detection in CRNs.

REFERENCES

[1] Mitola, J., Maguire, G.Q. (1999). Cognitive radio: making software radios more personal. IEEE Personal Communications, 6(4): 13-18. https://doi.org/10.1109/98.788210

[2] Hlavacek, D., Chang, J.M. (2014). A layered approach to cognitive radio network security: A survey. Computer Networks, 75: 414-436. https://doi.org/10.1016/j.comnet.2014.10.001
[3] Bkassiny, M., Li, Y., Jayaweera, S.K. (2012). A survey on machine-learning techniques in cognitive radios. IEEE Communications Surveys & Tutorials, 15(3): 1136-1159. https://doi.org/10.1109/SURV.2012.100412.00017
[4] Clement, J.C. (2023). GRU-SVM based threat detection in cognitive radio network. Sensors, 23(3): 1326. https://doi.org/10.3390/s23031326
[5] Benazzouza, S., Ridouani, M., Salahdine, F., Hayar, A. (2022). A novel prediction model for malicious users detection and spectrum sensing based on stacking and deep learning. Sensors, 22(17): 6477. https://doi.org/10.3390/s22176477
[6] Kumar, G.P., Reddy, D.K. (2022). Hierarchical Cat and Mouse based ensemble extreme learning machine for spectrum sensing data falsification attack detection in cognitive radio network. Microprocessors and Microsystems, 90: 104523. https://doi.org/10.1016/j.micpro.2022.104523
[7] Lilhore, U.K., Dalal, S., Simaiya, S. (2024). A cognitive security framework for detecting intrusions in IoT and 5G utilizing deep learning. Computers & Security, 136: 103560. https://doi.org/10.1016/j.cose.2023.103560
[8] Khan, M.S., Khan, L., Gul, N., Amir, M., Kim, J., Kim, S.M. (2020). Support vector machine-based classification of malicious users in cognitive radio networks. Wireless Communications and Mobile Computing, 2020(1): 8846948. https://doi.org/10.1155/2020/8846948
[9] Park, J., Chang, S. (2021). A particulate matter concentration prediction model based on long short-term memory and an artificial neural network. International Journal of Environmental Research and Public Health, 18(13): 6801. https://doi.org/10.3390/ijerph18136801
[10] Kiliç, K., Sallan, J.M. (2023). Study of delay prediction in the US airport network. Aerospace, 10(4): 342. https://doi.org/10.3390/aerospace10040342
[11] Ponnusamy, V., Kottursamy, K., Karthick, T., Mukeshkrishnan, M.B., Malathi, D., Ahanger, T.A. (2020). Primary user emulation attack mitigation using neural network. Computers & Electrical Engineering, 88: 106849. https://doi.org/10.1016/j.compeleceng.2020.106849
[12] Park, J., Chang, S. (2021). A particulate matter concentration prediction model based on long short-term memory and an artificial neural network. International Journal of Environmental Research and Public Health, 18(13): 6801. https://doi.org/10.3390/ijerph18136801
[13] Selvi, S.A., Sundararajan, M. (2016). SVM based two level authentication for primary user emulation attack detection. Indian Journal of Science and Technology, 9(29): 1-8. https://doi.org/10.17485/ijst/2016/v9i29/89270
[14] Aygül, M.A., Furqan, H.M., Nazzal, M., Arslan, H. (2020). Deep learning-assisted detection of PUE and jamming attacks in cognitive radio systems. In 2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall), Victoria, BC, Canada, pp. 1-5. https://doi.org/10.1109/VTC2020-Fall49728.2020.9348579
[15] Sivagurunathan, P.T., Ramakrishnan, P., Sathishkumar, N. (2021). Recent paradigms for efficient spectrum sensing in cognitive radio networks: Issues and challenges. Journal of Physics: Conference Series, 1717(1): 012057.10.1088/1742-6596/1717/1/012057
[16] Abbas, N., Nasser, Y., Ahmad, K.E. (2015). Recent advances on artificial intelligence and learning techniques in cognitive radio networks. EURASIP Journal on Wireless Communications and Networking, 2015: 174. https://doi.org/10.1186/s13638-015-0381-7
[17] Cadena Muñoz, E., Pedraza Martinez, L.F., Ortiz Trivino, J.E. (2020). Detection of malicious primary user emulation based on a support vector machine for a mobile cognitive radio network using software-defined radio. Electronics, 9(8): 1282. https://doi.org/10.3390/electronics9081282
[18] Upadhye, A., Saravanan, P., Chandra, S.S., Gurugopinath, S. (2021). A survey on machine learning algorithms for applications in cognitive radio networks. In 2021 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), Bangalore, India, pp. 1-6. https://doi.org/10.1109/CONECCT52877.2021.9622610
[19] Tasheva, Z., Bogdanov, R. (2018). A relationship between cognitive information processing in learning theory and machine learning techniques in cognitive radios. In Society Integration Education Proceedings of the International Scientific Conference, 5: 465-474. https://doi.org/10.17770/sie2018vol1.3191
[20] Almuqren, L., Maray, M., Alotaibi, F.A., Alzahrani, A., Mahmud, A., Rizwanullah, M. (2024). Optimal deep learning empowered malicious user detection for spectrum sensing in cognitive radio networks. IEEE Access, 12: 35300-35308. https://doi.org/10.1109/ACCESS.2024.3367993