Detecting Jamming Attacks in Wireless Communication Using Machine Learning Models

Paradesi Subba Rao, Nooka Varsha Reddy, Shaik Suhani, Kasetty Susmitha,
Lalam Jhansi and Pinjari Aneefa
Department of Computer Science and Engineering, Santhiram Engineering College, Nandyal-518501, Andhra Pradesh, India

Keywords: Jamming Detection, Machine Learning, RSSI, SNR, BER, Packet Loss Rate, Conventional, Software-Defined Radio, Threshold.

Abstract: Attacks from indiscriminate jammers could prevent communications by disrupting wireless networks. In conventional jamming detection systems, software-defined radios or fixed-threshold signal evaluation algorithms are incorporated in an attempt to solve the problem. These methods do not cope well with sophisticated and adaptive jamming techniques due to inflexibility, excessive resource expenditure, and high rates of false alarms. Fixed-threshold techniques cannot be adjusted adaptively, while methods based on SDR necessitate high volumes of both processing power and costly radio frequency hardware. Machine learning algorithms based jamming detection systems take features such as RSSI, SNR, BER, and packet loss rate as detection model metrics. The proposed solution enhances the robustness and security of wireless communication systems by providing fast, adaptable and hardware-independent response to jamming inquiries.

1 INTRODUCTION

First of all, 5G, the Internet of Things, self-operation systems and defense operations depend on this technology of wireless communication. However, such networks are vulnerable to interference attacks, where a malicious person disrupts communication to block transmission. These attacks can cause serious security issues, loss of data and disruption of networks, thus requiring effective detection techniques.

More traditional jamming detection techniques use Software-Defined Radios (SDRs), or fixed-thresholds. Even with existing threshold-based approaches monitoring network metrics (e.g., RSSI, SNR, BER, packet loss rates), there are many false positive events due to these disturbances. Nonetheless, while the SDR-based method yields accurate and precise results, the practical implementation is limited by high computational requirements and expensive hardware. In order to cover these limitations, in this paper we propose a machine learning-based jamming detection system. The approach increases detection accuracy and eliminates the need for additional devices.

Using Random Forest, Support Vector Machines (SVM), Neural Networks, the proposed system characterizes network states as normal or jammed in real-time. Because the model continuously monitors the actions in the network, it is highly scalable, effective, and affordable, helping to discover new kinds of jamming techniques and ensuring that wireless networks work in a secure manner. The optimal solution is applicable to various wireless communication situations, ranging from 5G networks, IoT ecosystems, and military defence applications to critical infrastructure for its convenience, effectiveness, and cost implications.

2 LITERATURE REVIEW

2.1 Machine Learning

Machine learning considers learning as a computer science activity or task. In contrast to traditional

Rao, P. S., Reddy, N. V., Suhani, S., Susmitha, K., Jhansi, L. and Aneefa, P.
Detecting Jamming Attacks in Wireless Communication Using Machine Learning Models.
DOI: 10.5220/0013891700004919

In *Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies (ICRDICCT'25 2025) - Volume 3*, pages 63-66
ISBN: 978-989-758-777-1

programming, ML does not restrict itself to the program specifying a sequence of steps. In this way, "gathers" means that it learns to predict by analyzing data and identifying patterns. In supervised (the models are trained on labeled data), unsupervised (the data themselves are exploited to learn patterns, etc. without a priori assigned labels), and reinforcement (learning the decision-making process from trial-by-trial experience) ML it is also feasible to partition the ML in various sub-classes. Speech recognition, fraud detection, recommender systems, and predictive analytics are among these. Computing lies in the large, databases being updated and scored continuously as a stream of new data comes in, an important feature of businesses in the fields of cybersecurity, health, and automation.

2.2 How Machine Learning Is Used in Detecting in Jamming Attacks

Jamming attack detection over wireless communications is claimed to be one of the most difficult problems, as the attacker uses an adaptive interference recovery that is more complex than the standard assumptions to detect ordinary jammers. These types of attacks introduce radio frequency interference into the input channel to compromise or stop communication. This results in a loss or stopping of communication services, which in turn causes network and service disruptions.

Machine learning (ML) offers a highly effective method, as it can track network activities, learn from the past, and identify malicious activities that indicate jamming. The algorithms, based on machine learning, can be trained to identify the attack signatures in the network parameters, e.g., Received Signal Strength Indicator (RSSI), Signal-to-Noise Ratio (SNR), Bit Error Rate (BER), and Packet Loss Rate. Jamming-type attacks usually cause substantial packet loss, an increase in BER, and a sudden decrease in RSSI, all of which the ML models are trained to associate with jamming.

3 METHODOLOGY

This section describes the methodology used to identify jamming attacks; in particular, section 3.1 describes the project architecture (figure 1), section 3.2 describes the dataset information, section 3.3 describes the feature extraction approach.

3.1 Architecture

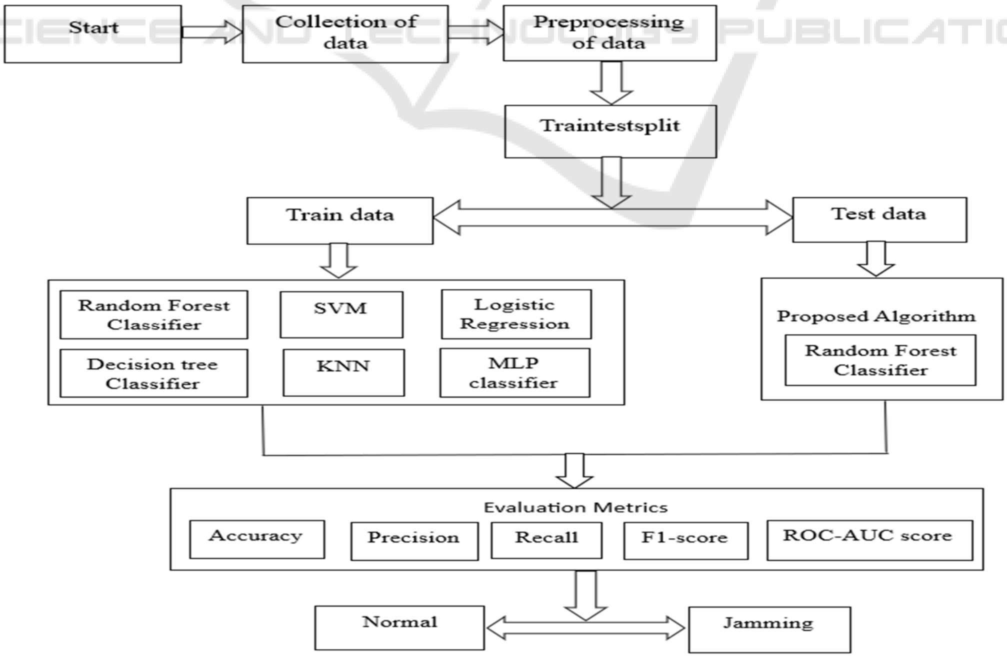

Figure 1: System Architecture.

3.1 Dataset Information

RSSI-Measures the strength of incoming signal in dBm (decibel-milliwatts), lower value represents weaker signals.
SNR - The measurement of the ratio of signal power to noise power in decibels. Higher values indicate better signal quality.
BER - Describes the percent of bits that were routed incorrectly due to some form of destruction. Greater number of errors means higher figure of BER.
Packet Loss Rate (%) - Percentage of packets that did not reach their destination, indicative of disturb at the network.
Label - Defines the state of network set to be Jamming (1) or Normal (0).

3.2 Feature Extraction

F1: RSSI analyses normal operations that are characterized by higher RSSI values, whereas lower values signal jamming activity.
F2: SNR analyses Elevated SNR signifies positive network conditions, while lower SNR denotes potential jamming.
F3: BER Analysis the interference is likely with high BER values, while low BER values indicate stable communications.
F4: Packet loss rate Normal operations are characterized by lower packet loss, whereas higher packet loss indicates jamming activity.
F5: Jamming attack classification during training the model, classify network states into 'normal' (0) or 'jamming' (1) for use in the model.

4 IMPLEMENTATION AND RESULTS

In this section the implementation details are mentioned to detect the jamming attacks. 4.1 Section contains the model selection and 4.2 section contains the results of the implements.

4.1 Model Selection

Model 1: Random Forest
Random Forest is a strong machine learning model which predicts results by averaging a few decision trees. Since every individual tree inspects other segments of the data, the final model improves on their accuracy and strength. The combined power helps it to address various parameters like RSSI, SNR, BER, and Packet Loss Rate making it more useful for jamming threat identification.

Model-2: Support Vector Machine
In SVM we train the data of this type of model which differentiate between the data which experiences interference in the network and that which works normal. Under the condition that there are clean features that can significantly separate normal signals from jamming attacks, performance of the technique is at its best. While SVM is relatively slow on large datasets, it is an invaluable approach when working with high-dimensional data.

Model-3: K-Nearest-Neighbour
KNN estimates network states based on neighbouring data points. If most of the closest points have been marked as normal based on network conditions, the new point is assigned normal; if the area is congested, the new point is considered jammed.

Model-4: Decision Tree Classifier
A Decision Tree Classifier is a simple and interpretable machine learning method for classification problems. Its decision rules create a tree-like structure, where the data is partitioned into branches based on certain features.

Model-5: Logistic Regression
The Logistic Regression model was a basic model which looked at what the probability was that the network was working correctly versus congested. Simple to use, efficient in operation, but less effective than other models like Random Forest or Neural Networks in terms of complex jamming attack pattern handling.

Model-6: Multi-Layer Perceptron
The MLP is just yet another neural network that is aimed at classifying and identifying through patterns. The architecture includes one input layer, one or more hidden layers, and one final output layer. As the computational weight of each neuron, it carries its calculations through a function that takes the incoming messages and sorts through them to filter and enhance the respective elements, such as through use of Rectified Linear Units (ReLU) or a Sigmoid Functions. Therefore, since MLP is adaptive to learn from RSSI, SNR, BER, and Packet Loss Rate, one of the useful tools for learning adaptively from the data of the inherent complex patterns of these metrics is the detection of jamming attacks.

4.2 Results

ROC-AUC curve as shown in figure 2 is a pictorial representation of the true positive rate versus the false positive rate.

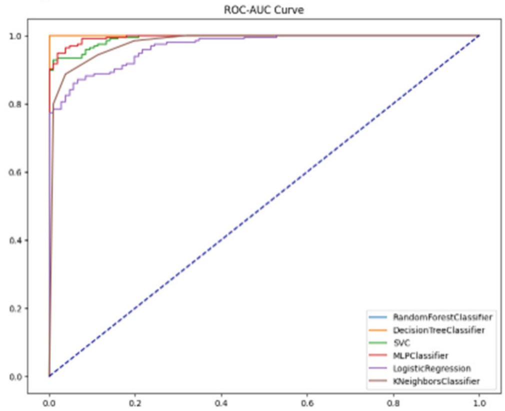

Figure 2: ROC-AUC Scores of Test Data.

5 CONCLUSIONS

In our paper we provide a solution for jamming attacks using machine learning models. Out of the models tested, the Random Forest Classifier proved to be the best performer with a test accuracy of 97% and a ROC-AUC score of 99.01%. The performance metrics demonstrate how well our method works to differentiate between normal network traffic and jamming attacks, which would significantly increase the security of wireless networks.

REFERENCES

Chaitanya, V. Lakshmi, and G. Vijaya Bhaskar. "Apriori vs Genetic algorithms for Identifying Frequent Item Sets." International journal of Innovative Research &Development 3.6 (2014): 249-254.

Chaitanya, V. Lakshmi. "Machine Learning Based Predictive Model for Data Fusion Based Intruder Alert System." journal of algebraic statistics 13.2 (2022): 2477-2483

Chaitanya, V. Lakshmi, et al. "Identification of traffic sign boards and voice assistance system for driving." AIP Conference Proceedings. Vol. 3028. No. 1. AIP Publishing, 2024

Devi, M. Sharmila, et al. "Machine Learning Based Classification and Clustering Analysis of Efficiency of Exercise against Covid-19 Infection." Journal of Algebraic Statistics 13.3 (2022): 112-117.

Devi, M. Sharmila, et al. "Extracting and Analyzing Features in Natural Language Processing for Deep Learning with English Language." Journal of Research Publication and Reviews 4.4 (2023): 497-502.

Mahammad, Farooq Sunar, Karthik Balasubramanian, and T. Sudhakar Babu. "A comprehensive research on video imaging techniques." All Open Access, Bronze (2019).

Mahammad, Farooq Sunar, and V. Madhu Viswanatham. "Performance analysis of data compression algorithms for heterogeneous architecture through parallel approach." The Journal of Supercomputing 76.4 (2020): 2275-2288.

Mahammad, Farooq Sunar, et al. "Key distribution scheme for preventing key reinstallation attack in wireless networks." AIP Conference Proceedings. Vol. 3028. No. 1. AIP Publishing, 2024.

Mandalapu, Sharmila Devi, et al. "Rainfall prediction using machine learning." AIP Conference Proceedings . Vol. 3028. No. 1. AIP Publishing, 2024.

Mr.M.Amareswara Kumar, “Baby care warning system based on IoT and GSM to prevent leaving a child in a parked car” in International Conference on Emerging Trends in Electronics and Communication Engineering - 2023, API Proceedings July-2024

Mr.M.Amareswara Kumar, “Effective Feature Engineering Technique for Heart Disease Prediction with Machine Learning” in International Journal of Engineering & Science Research, Volume 14, Issue 2, April-2024 with ISSN 2277-2685.

Paradesi SubbaRao,”Morphed Image Detection using Structural Similarity Index Measure”M6 Volume 48 Issue 4 (December 2024),https://powertechjournal.com

Paradesi Subba Rao, ”Detecting malicious Twitter bots using machine learning” AIP Conf. Proc. 3028, 020073 (2024),https://doi.org/10.1063/5.0212693

Parumanchala Bhaskar, et al. "Machine Learning Based Predictive Model for Closed Loop Air Filtering System." Journal of Algebraic Statistics 13.3 (2022): 416-423.

Parumanchala Bhaskar, et al. "Incorporating Deep Learning Techniques to Estimate the Damage of Cars During the Accidents" AIP Conference Proceedings. Vol. 3028. No. 1. AIP Publishing, 2024.

Parumanchala Bhaskar, et al “Cloud Computing Network in Remote Sensing-Based Climate Detection Using Machine Learning Algorithms” remote sensing in earth systems sciences (springer).

Suman, Jami Venkata, et al. "Leveraging natural language processing in conversational AI agents to improve healthcare security." Conversational Artificial Intelligence (2024): 699-711.

Sunar, Mahammad Farooq, and V. Madhu Viswanatham. "A fast approach to encrypt and decrypt video streams for secure channel transmission." World Review of Science, Technology and Sustainable Development 14.1 (2018): 11-28.