International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue INSPIRE'25, pp 176-179, April-2025
https://doi.org/10.47001/IRJIET/2025.INSPIRE29
International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25)

Detecting Jamming Attacks Using Machine Learning Models

[1]Paradesi Subba Rao, [2]Nooka Varsha Reddy, [3]Shaik Suhani, [4]Kasetty Susmitha, [5]Lalam Jhansi, [6]Pinjari Aneefa

[1]Assistant Professor, Department of Computer Science and Engineering, Santhiram Engineering College, India
[2,3,4,5,6]Student, Department of Computer Science and Engineering, Santhiram Engineering College, India
E-mail: subbarao.cse@srecnandyal.edu.in

***Abstract* - A wireless network is the target of jamming attacks, which cause an undesired denial of service. Despite its robustness due to the utilisation of millimetre wave bands, 5G is susceptible to these attacks. Random jamming has the ability to disrupt wireless networks and stop conversations. Traditional jamming detection systems and solutions try to use fixed-threshold signal evaluation techniques or software-defined radios. Because of their relatively rigid behaviour, high false alarm frequency, and resource-intensive detections, traditional tactics frequently lose their effectiveness when faced with clever or adaptable threats. Fixed-threshold approaches are free from the need to integrate expensive radio frequency hardware and vast amounts of processing, whilst SDR-based implementations can only be fixed threshold mechanisms. RSSI, SNR, BER, and packet loss rate are considered as the detection model metrics in machine learning-based jamming detection systems. By responding to the jamming enquiries quickly, flexibly, and in a hardware- independent manner.**

Keywords: Traditional Jamming, Threshold value, Software defined radio, RSSI, SNR, BER, Packet loss rate

I. INTRODUCTION

5G is expected to be replaced in the near future by the wireless phone network of the previous generation, which is expected to grow in size and lower latency. As a result, it is projected that billions of wireless devices will be online. Including the current network, 5G is also susceptible to cyber security threats including jamming and issues with GPS operation. This leads to cognitive radio transmission, which exposes these networks to novel attacks such as user simulation or primary assaults in the spectral record. It is crucial to do research on how 5G technology affects cyber security. In an attempt to lower the SNR of authorized users, Discore interfered with communication by sending wireless signals that exceed a communication channel.

Reactive, deceptive, random, and continual jammers are the four general categories of jamming attacks. High-performance noise transmission that continually obstructs attacks. After then, there is a clear strategy that is spread from channel to channel and keeps going throughout time. There are occasional issues that don't adhere to a certain channel-switching scheme. Illegal packets on wireless channels are used by fraudulent jammers.

Responsive destruction targets just communication channels and regularly checks the frequency channel status. Another way to classify interference is as intelligent or normal. There isn't the usual interruption.

Since the continuously delivered signals all play simultaneously, normal jammers are unable to identify them. The signal broadcast patterns of actual users may be swiftly learned, recognized, and ascertained by intelligent jammers. To further damage the real transmission, they can next use their offensive strategies or change the transmission power.

There are several approaches to jamming detection. The two primary categories of these methods are machine learning and non-machine learning. Among the parameters and methods utilized in non-machine learning approaches include sewer surfing, fuzzy logic, game theory, timing channels, thresholds, and area mapping of crowded zones. A time series model was employed in another study to track connection circumstances and evaluate the state of communication networks by contrasting them with previous data.

For instance, a technique based on artificial neural networks may be able to do periodic signal spectral analysis in addition to more general spectrum reconstruction. This technique separates jamming signals from narrowband communications using a combination of modulation and signal quality assessment. On the other hand, a recognition framework using machine learning with support vector machine, adaptive boosting and optimization techniques. Using metrics such as the raw number of packets (or frames), busy channel ratios, packets ratios, and maximum idle periods, they were able to identify jamming attempts based on the jamming patterns. Most of these approaches require extensive resources and only provide temporary relief. While detecting a connection failure is possible, determining the cause of the

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue INSPIRE'25, pp 176-179, April-2025
https://doi.org/10.47001/IRJIET/2025.INSPIRE29
International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25)

service disruption is often difficult. Moreover, these methods can have a comparatively higher false alarm rate.

II. METHODOLOGY

In this research, the identification of jamming assaults is treated as a classification problem in which the algorithm has to distinguish between two possible outcomes: either the link is disrupted by a jammer or it is disrupted for some other reason.

The justification for using machine learning concepts to this problem is that they are successful in solving complex problems quickly and with the least amount of resources. Carefully choosing pertinent characteristics is essential to creating a successful machine learning model. Several characteristics have been used in this study to identify the presence of jamming assaults. One characteristic alone is not enough to identify the presence of a jamming assault. Furthermore, it might be difficult to establish analytical connections between these metrics and the state of the link. In order to detect jamming attacks, machine learning is used to find a direct connection between these four measures.

2.1 Jamming attack model

Jamming attacks target wireless networks' cross-layer as well as physical layer. Jamming signals, which stop a transmitter and a receiver channel from communicating, are necessary under these attacks. When the jamming signals keep the channel busy for an extended period of time, it creates a denial of service. It should be clear that training and validating classification models need robust methods. Even though selection curve characteristics are sometimes disregarded, they are crucial to detection approaches in machine learning. This makes the need for effective and rapid detection techniques that can more precisely detect jamming activities critical.

2.2 Feature selection

The parameters of faulty packet ratio, clear channel, packet delivery ratio, and received signal strength evaluation are used to identify jamming assaults. These four characteristics were chosen since any communication system card with a network interface has diagnostic capabilities that allow these metrics to be estimated. The faulty packet ratio and the ability to identify jamming attempts are two important characteristics to practice.

It is the proportion of incorrect packages received. By examining the frame check sequence of the arriving packets at the medium access control level, the receivers determine this faulty packet ratio. The bad packet ratio rises when the channel is attacked, but it is very low while the connection is in good transmission condition.

Every time the receiver successfully gets the right packet, it returns the acknowledgment packet to the transmitter. The package. The delivery ratio is quite high when the connection state is good. is extremely precious, and if the link is attacked, its worth decreases dramatically. The Clean Path Analysis can be used to quantify the amount of channel discovered and the efficiency of its ability to be occupied. If the channel value for this parameter increases, jamming attacks take place. The received signal strength, or RSS, gauges the power surrounding the receiver. It is high if there is no assault, but it falls if the channel is attacked in any way.

2.3 Machine Learning Algorithms

1. Random Forest

Random Forest is a multi-level classifier that consists of many decision trees. This is done by having the test data evaluated by the trees in question based on their feature attributes. It consists of split nodes and leaves. Each decision node is a function for classified test data and the branches represent values which can be predicted by that node. Using multiple trees reduces the overfitting risk. This mechanism is responsible for balancing the distribution of data and improves the performance of the complete model. For random forest classifier the core settings define how many trees are created, tree-related characteristics are (the least rankings, splitting criteria, etc. The Random Forest is a predictor and aggregates the predictions of the individual trees.

2. Support Vector Machine

The Support Vector Machine constructs a hyperplane for separating two categories of data. The kernel selected determines the line that separates these classes. This framework allows us to use different kernels, such as linear or radial basis functions.

3. Neural Network

Neural networks are computational models based on human and animal brains but allowing machines to learn from data they consume. [It shows] an impressive ability to learn and solve different problems in various areas such as image processing, signal processing, and communications. A neural network is composed of an input layer, one or more hidden layers, and an output layer. Multiple layers consists of one or multiple neurons. Neurons have an activation function and multiple connections to various neurons from layers that flow out. The neural network training process adjusts this weight to find the perfect weight, which minimizes the error of the

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue INSPIRE'25, pp 176-179, April-2025
https://doi.org/10.47001/IRJIET/2025.INSPIRE29
International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25)

predicted function as compared to the actual data set configuration that was targeted. There are two concepts on which every neural network rests: feedforward and backpropagation. Feedforward is the simplest type of artificial neural network., where information only travels from the input layer to the output layer via the hidden layers, in one direction.

III. RESULTS AND DISCUSSIONS

Four different parameters were used as features for detection of jamming attacks to verify the machine learning model. Under both a targeted link and secure link scenario, data was collected via a realistic environment simulation for each of these parameters. Finally, using cross-validation methods, the data logs were split into n segments to train and evaluate the model. To utilize an n-times cross-validation approach, the data was divided into n samples of approximately equal size.

We evaluate the performance of these models on the data set and in this research, we try out algorithms for a range of folds.

IV. CONCLUSION

5G technology is designed with millimeter wave bands not to be disrupted by attacks. But it works on frequency bands lower than 6 GHz causing it vulnerable to interference. Smart jamming detection systems are a must have for countering these threats. We have analyzed current methods of improved identification in this paper. For jamming attack detection purpose, we explored and tested different machine learning models. We are extracting features and selected properties, compiling large data sets used to train, validate and test random forests, support vector machines and neural network algorithms. A cross-validation approach will be employed and a learning curve will be presented to evaluate the performance of these models with respect to a series of defined metrics. The results show that it is possible to detect jamming using Random Forest technology.

REFERENCES

[1] Paradesi Subba Rao; Farooq Sunar Mahammad; Parumanchala Bhaskar; M. Shabarish; S. V. Kishore; T. Varun Kumar; B. Chandra Sekhar; S. M. Mansoor. "Detecting malicious Twitter bots using machine learning." https://doi.org/10.1063/5.0212693.

[2] "Morphed Image Detection using Structural Similarity Index Measure", Kiran Kumar G1, Manjula Prabakaran2, Paradesi SubbaRao3, Harini K4, Madhan Mohan R5, Sai Nithin M6 Volume 48 Issue 4 (December 2024) https://powertechjournal.com.

[3] 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.

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

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

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

[7] 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.

[8] 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.

[9] 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.

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

[11] 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.

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

[13] 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.

[14] 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.

[15] Parumanchala Bhaskar, et al "Cloud Computing Network in Remote Sensing-Based Climate Detection

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue INSPIRE'25, pp 176-179, April-2025
https://doi.org/10.47001/IRJIET/2025.INSPIRE29
International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25)

Using Machine Learning Algorithms" remote sensing in earth systems sciences (springer).

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

Citation of this Article:

Paradesi Subba Rao, Nooka Varsha Reddy, Shaik Suhani, Kasetty Susmitha, Lalam Jhansi, & Pinjari Aneefa. (2025). Detecting Jamming Attacks Using Machine Learning Models. In proceeding of International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25), published by *IRJIET*, Volume 9, Special Issue of INSPIRE'25, pp 176-179. Article DOI https://doi.org/10.47001/IRJIET/2025.INSPIRE29

****

