

Jamming Attack Identification in Cognitive Radio Networks: An Adversarial Behavior Perspective

Chhaya C. Athavale¹ and K.P. Patil²

¹Research Scholar, Electronics and Telecommunication Department, Sinhgad Academy of Engineering, Pune, India
Email: chhayaathavale@gmail.com

²Sinhgad Academy of Engineering, Pune, India
Email: kppatil1@gmail.com

Abstract— Cognitive Radio Networks (CRNs) enable opportunistic spectrum utilization, but their performance is compromised by adversarial users that exploit vulnerabilities in spectrum sensing and management. Two major adversary categories are selfish and malicious users. Selfish users misreport sensing results or occupy channels for personal gain, often due to malfunctioning sensors or spectrum hoarding strategies. Malicious users, by contrast, deliberately disrupt CRNs through targeted attacks, including Primary User Emulation Attacks (PUEA), Spectrum Sensing Data Falsification (SSDF), and jamming. These attacks degrade detection probability, increase interference with licensed users, and reduce network throughput. Although prior research has extensively examined jamming detection, the classification and distinction between selfish and malicious adversaries remain insufficiently addressed. This work analyzes adversarial behavior in CRNs, focusing on differentiating selfish misuse from intentional malicious disruption. By characterizing attack patterns, evaluating their impact on sensing performance, and identifying classification gaps, this study provides a foundation for developing robust adversary detection frameworks. The ultimate objective is to strengthen CRN resilience against heterogeneous threats and ensure reliable spectrum access.

Keywords— Cognitive radio networks, security provisions, attacks, malicious behaviour, jamming attack.

I. INTRODUCTION

The term Cognitive Radio (CR) refers to wireless technologies that are linked with networks that possess computationally intellectual radio properties and related computer-to-computer communications. It is used for determining the requirement of the user communications based on the function of user context and delivering wireless services and radio resources. As a result, cognitive radio approaches are only available for the effective and efficient use of the spectrum [1]. This method is efficient for gaining access to the spectrum since it can analyze the series to learn about the environment of the classes and then decide what to do by changing the operational parameters. To access the spectrum, a network user must first identify licensed users, commonly known as Primary Users (PUs). The radio frequency (RF) environment in the area must also be sensed in the absence of a PU to establish the usable spectrum. Spectrum sensing is the term used to describe this crucial procedure. Spectrum sensing tries to give PUs interference-free access by restricting its interference with PUs and changing it to the open band.

In addition, secondary users must effectively identify and make use of the spectrum gaps [2]. As a result, both primary radio networks and cognitive radio networks depend on the detection performance in spectrum sensing [3]. The spectrum scarcity problem has been raised due to the result of the increased deployment of wireless networks brought on by the enhanced utilization of wireless devices. However, the spectrum designated by the license holders is not well used [4].

The goal of the rapidly expanding field in the wireless network research is to connect almost every aspect of life with a network that has significantly higher speed, extremely low latency, and widespread connectivity.

The different layers of CRN are considered for analyzing the threats in CRN, which will include the details based on traditional wireless security issues and CRN security issues, layer-wise attacks and security provision, and adversary's behavior to find malicious behavior and jamming attack.[5]

Jamming attacks are viewed as an important threat that can compromise fully connected networks and cause disruptions. They can be carried out on the intelligent sensing layer. Furthermore, jamming has the potential to stop wireless nodes from collecting data from other sources. Attacks known as denial of service (jamming) cause wireless radio communications to be disrupted by superimposing a signal with a much higher noise power over legal signals in order to lower the Signal to Noise Ratio using a jammer. It is challenging to identify jamming attacks while a wireless network is operating normally because interference from the surroundings or jamming can disrupt the communication between the base station and other users. In order to identify and classify type of jammer, a jamming detection technique requires the deployment of at least one node which combines many strategies [4]. This node samples the adversary's broadcast. In [5], researchers are motivated by the emerging TinyML movement, which enables on-device deep learning and machine learning to facilitate the integration of intelligence on devices with limited power resources. A developing area of artificial intelligence called TinyML offers machine learning solutions that are more localized, low-powered, and reduce power consumption and network traffic while giving end users high availability [5]. To identify jamming attacks, deep learning techniques can be applied to the deployed nodes. The availability of low-cost, user-friendly jamming techniques has made jamming a major research priority and continues to do so. In order to achieve this, studies on anti-jamming strategies have been carried out on a variety of networks, including Wireless Networks, Vehicular Ad Hoc Networks (VANET) [7], and Wireless Sensor Networks (WSN) [6]. Jamming attacks come in several forms. Researchers concentrate on two kinds of jammers: periodic and constant. The process of continually introducing noise (AWGN) into the channel is known as constant jamming, and it interferes with communication for an undetermined period of time. In contrast, periodic jamming involves injecting the AWGN into the channel on a regular basis—that is, jamming for three seconds and sleeping for three seconds. The majority of edge devices are solely used for measurements or data collecting, making jamming detection a difficult task. Because of this, it is more difficult to identify and stop these kinds of attacks. Among the anti-jamming methods are jamming detection and localization [8]. There are several ways to identify jamming attacks, including techniques based on machine learning. The identification of various jamming attack types in wireless networks by deep learning algorithms and machine learning algorithms has been the subject of much research. Machine learning techniques include tree-based classifiers, support vector machines [9-13], and gradient boosting [13] are some of the detection approaches used in some of the present work. Furthermore, only a small number of contributions [14, 15] discussed the application of deep learning techniques. Packet Delivery Ratio (PDR) [15], RSS [16], or a mix of both are [17-18] the metrics that are commonly utilized.

The work of this paper is organized as follows: Section II describes the related work which is relevant to this work presented here. Section III Discuss the proposed system architecture.

Section IV covers the results and discussion part of this paper. Section V end up with the conclusion of this work.

II. RELATED WORK

The IoT (TinyML)-based approach used in the jamming identification and categorization techniques detailed in [5] is based on a deep learning model that is implemented on a Raspberry Pi. The regular channel state and two other types of jammers—constant and periodic—are included in this trained deep learning model. A Software Defined Radio, which is connected to the Raspberry Pi, keeps an eye on the Wi-Fi channel and gathers signal data in the form of received signal strength (RSS). A deep learning model implemented on TinyML then determines whether a jamming attack is occurring and what kind of attack it is. The researchers made this dataset available as open source. The database released by researcher is utilized in this progress, which consist of 1230 signals [5] for each type of jamming and normal channel. The researcher constructed CNN model with multi-layer 1D and trained in order to categorize the various kinds of jamming attacks. The researcher exhibited a

TinyML-based Internet of Things (IoT) jamming identification and categorization system and employed HackRF to model two distinct types of jamming attacks: constant and periodic. The suggested implementation includes a HackRF and a Raspberry Pi IoT device; the Raspberry Pi detects the channel and logs RSS data. With the use of recorded RSS data, the Raspberry Pi's deep learning model was trained to identify and categorize the many types of jamming attacks that are carried out in the network. The model was able to identify a jamming type with an accuracy of 86.3%.

III. PROPOSED SYSTEM ARCHITECTURE

As the objective of this paper is to analyze an adversary in Cognitive Radio Network and differentiate between the malicious and selfish users. The database released is utilized in this paper, which consist of 1230 signals [5] for each type of jamming, constant jamming, random or periodic jamming and normal channel. The RSS and the signal structure associated with the gathered data for each form of jammer and normal channel is shown. In Figure1 RSS readings associated Normal Channel is plotted, RSS readings associated Constant Jammer plot is given in Figure 2, Figure 3 explains RSS readings associated for Random Jammer and In Figure 4 RSS readings associated with all types of jammers and normal channel plot is given. CNN model is constructed and trained in order to categorize the kinds of jamming attacks as constant or random jammer and in this work the accuracy of 95% is achieved. Deep Neural Network is modeled and trained in order to classify the jamming attack as constant or random jammer using same dataset and the accuracy of 96% is achieved.

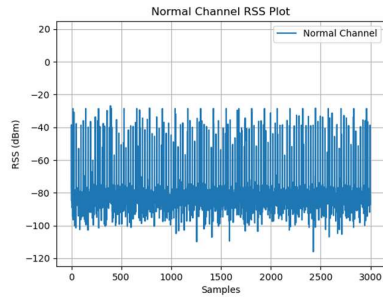


Figure 1. RSS readings associated Normal Channel

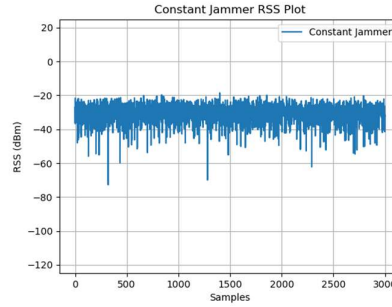


Figure 2. RSS readings associated Constant Jammer

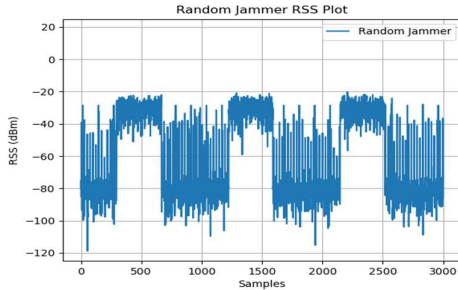


Figure 3. RSS readings associated Random Jammer

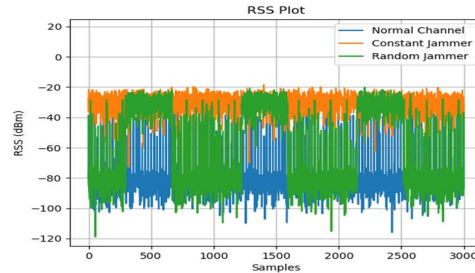


Figure 4. RSS readings associated all types of Jammer

A. Deep Learning Approach

The CNN model with multi-layer 1D is constructed and trained in order to categorize the kinds of jamming attacks as constant or periodic or random jammer. The database released is utilized in this work, which consist of 1230 signals [5] for each type of jamming and channel. For the data preprocessing from 410 signals per jamming type, 310 signals are used for training and 100 signals for testing are used. In training set total 930 signals and for testing 300 signals are considered and given labels using one hot encoding. The training and validation set of data are separated for the validation of the data training set, which provides the model's performance for each epoch. The Adam optimizer is used which helps in reducing loss function by tuning the parameters. In this model Rectified Linear Units is used as activation function, Categorical cross-entropy as a loss function and at output layer SoftMax function used. Next, the model's performance is described in terms of testing, validation, and training.

IV. RESULTS AND DISCUSSION

A. Model Training for CNN

The performance of the CNN model is described in the form of testing, validation, and training process. Figure 5 shows training accuracy of CNN model with number of epochs. Accuracy increases with the number of epochs. In each epochs internal parameters of the model get updated by minimizing the error and results in maximizing accuracy of the model. In Figure 5 we can observed the training and validation accuracy. Figure 6 illustrates the relation between loss and the number of the epochs. The CNN Model's confusion matrix for the data classification is shown in Figure 7. It illustrates, the prediction of constant jamming is 100%, for normal channel 94% and prediction of random or periodic jamming is 90%.

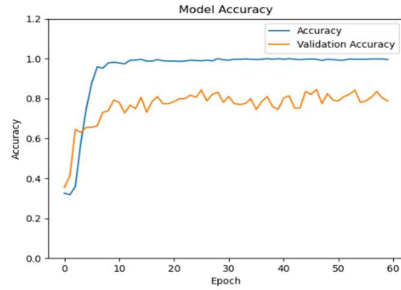


Figure 5: Accuracy varies with the epochs

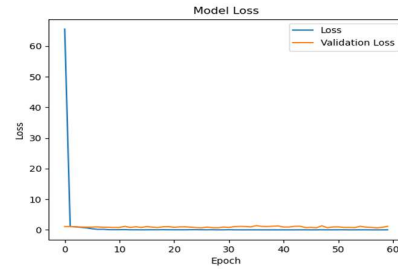


Figure 6: Relation between Loss and the epochs

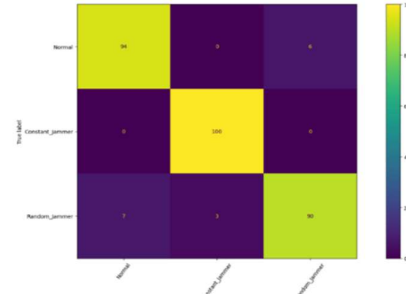


Figure 7: CNN Model's Confusion Matrix for Data Classification

B. Model Training for DNN

The performance of the DNN model is described in the form of testing, validation, and training process. Figure 8 gives the training accuracy and validation accuracy of DNN model with number of epochs. It increases with the number of epochs. In each epochs internal parameters of the model get updated by minimizing the error and results in maximizing accuracy of the model. Figure 9 shows the relation between loss function and the number of the epochs. Figure 10 shows DNN Model's Confusion Matrix for Data Classification. It illustrates, the prediction of constant jamming is 90%, for normal channel 97% and prediction of random or periodic jamming is 100%.

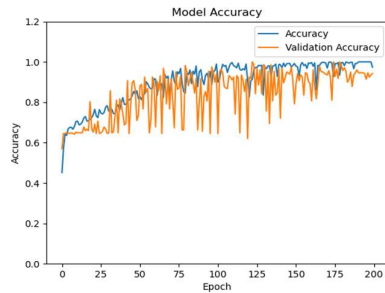


Figure 8: Accuracy varies with the epochs

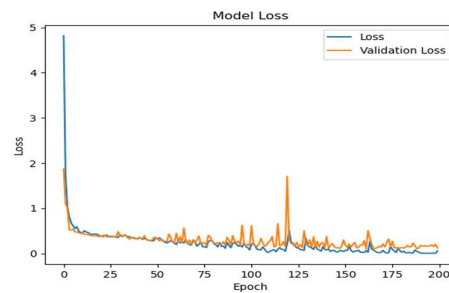


Figure 9: Relation between Loss and the epochs

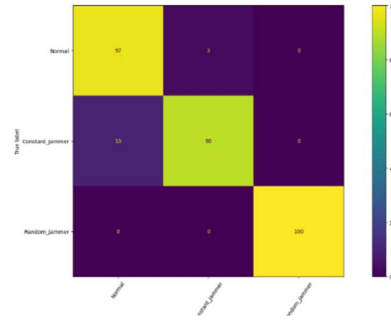


Figure 10: DNN Model's Confusion Matrix for Data Classification

Table 1 gives evolution metrics for the CNN and DNN model where we can observe that an accuracy of the jamming classification is 95% and 96% respectively.

TABLE I: MODEL EVALUATION METRICS

Model	Parameters	Normal	Constant jammer	Random jammer	Accuracy
CNN	Precision	0.93	0.97	0.94	0.95
	Recall	0.94	1.00	0.90	
	F1 score	0.94	0.99	0.92	
DNN	Precision	0.91	0.97	1.00	0.96
	Recall	0.97	0.90	1.00	
	F1 score	0.94	0.93	1.00	

V. CONCLUSION

This work shows the study of the implementation of an edge AI-based technique to identify jamming in IoT wireless networks where researcher [5] explained the classification of two types of jamming attacks: constant and periodic and they got jamming type detection accuracy of 86.3%. The researcher proposed implementation including hardware and software module which senses the channel and records the received signal strength of the signal i.e. RSS. They made this dataset available as open to all. By referring this data set, this work shows the implementation of CNN, and DNN model and achieved an accuracy to classify adversaries as constant jamming, periodic or random jamming and normal channel with the accuracy of 95% and 96% respectively.

REFERENCES

- [1] F. Salahdine, and N. Kaabouch, "Security threats, detection, and countermeasures for physical layer in cognitive radio networks: A survey", *Physical Communication*, vol. 39, pp.101001, 2020.
- [2] Z. Sun, Z. Xu, M.Z. Hammad, X. Ning, Q. Wang, and L. Guo, "Defending against massive SSDF attacks from a novel perspective of honest secondary users", *IEEE Communications Letters*, vol. 23, no. 10, pp.1696-1699, 2019.
- [3] N. Marriwala, H. Punj, S. Panda, I. Kaur, and D. Rathore, "An authentication-based approach for prevention of spectrum sensing data falsification attacks in cognitive radio network", *Wireless Personal Communications*, pp.1-27, 2022.
- [4] W.N. Singh, and N. Marchang, "Security Vulnerability in Spectrum Allocation in Cognitive Radio Network", In *International Conference on Advanced Computing Networking and Informatics: ICANI-2018*, pp. 215-224, Springer Singapore, 2019.
- [5] C.C.Athavale and K.P.Patil "Analysis of Various Attacks In Cognitive Radio Network and Security Provisions "International Conference on Cognitive Robotics and Intelligent Systems (ICC - ROBINS)2024.
- [6] Hossein Pirayesh and Huacheng Zeng. 2022. Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials* 2022.
- [7] Partha Pratim Ray. 2021. A review on TinyML: State-of-the-art and prospects. *Journal of King Saud University-Computer and Information Sciences* 2021.
- [8] Satish Vadlamani, Burak Eksioglu, Hugh Medal, and Apurba Nandi. 2016. Jamming attacks on wireless networks: A taxonomic survey. *International Journal of Production Economics* 172 (2016), 76–94.
- [9] Mohammed Saeed Al-Kahtani. 2012. Survey on security attacks in vehicular adhoc networks (VANETs). In *2012 6th international conference on signal processing and communication systems*. IEEE, 1–9.
- [10] Kanika Grover, Alvin Lim, and Qing Yang. 2014. Jamming and anti-jamming techniques in wireless networks: a survey. *International Journal of Ad Hoc and Ubiquitous Computing* 17, 4 (2014), 197–215.

- [11] Youness Arjoune, Fatima Salahdine, Md Shoriful Islam, Elias Ghribi, and Naima Kaabouch. 2020. A novel jamming attacks detection approach based on machine learning for wireless communication. In 2020 International Conference on Information Networking (ICOIN). IEEE, 459–464.
- [12] Ericsson. n.d. Ushering in A Better-Connected Future. Retrieved April 2022 from <https://www.ericsson.com/en/about-us/company-facts/ericssonworldwide/india/authored-articles/ushering-in-a-better-connected-future>.
- [13] Zhutian Feng and Cunqing Hua. 2018. Machine learning-based RF jamming detection in wireless networks. In 2018 third international conference on security of smart cities, industrial control system and communications (SSIC). IEEE, 1–6.
- [14] E Jayabalan and R Pugazendi. 2021. Deep learning model-based detection of jamming attacks in low-power and lossy wireless networks. *Soft Computing* (2021), 1–22.
- [15] GS Kasturi, Ansh Jain, and Jagdeep Singh. 2020. Detection and Classification of Radio Frequency Jamming Attacks using Machine learning. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.* 11, 4 (2020), 49–62.
- [16] Khaled B Letaief, Yuanming Shi, Jianmin Lu, and Jianhua Lu. 2021. Edge Artificial Intelligence for 6G: Vision, Enabling Technologies, and Applications. *IEEE Journal on Selected Areas in Communications* 40, 1 (2021), 5–36.
- [17] M Premkumar and TVP Sundararajan. 2020. DLDM: Deep learning-based defense mechanism for denial-of-service attacks in wireless sensor networks. *Microprocessors and Microsystems* 79 (2020), 103278.
- [18] Bikalpa Upadhyaya, Sumei Sun, and Biplab Sikdar. 2019. Machine learning based jamming detection in wireless IoT networks. In 2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS). IEEE, 1–5.