Detection and Classification of Radio Frequency Jamming Attacks using Machine learning

G.S Kasturi, Ansh Jain, and Jagdeep Singh*
Division of Information Technology, Netaji Subhas Institute of Technology,
University of Delhi, New Delhi, India
{kasturi710, a.j120562, jagdeepknit}@gmail.com

Received: September 10, 2020; Accepted: December 11, 2020; Published: December 31, 2020

Abstract

Wireless networks are an important aspect of communication technologies that avoid the cost and burden of cable installation. They play a vital role in our everyday lives. However, these wireless networks have some limitations which can be exploited by malicious users to capture transmitted information or cause disruptions in communications. A Radio Frequency Jamming (RF-Jamming) attack is one such type of attack that interferes with authentic wireless signals by reducing the signal-to-noise ratio. These types of attacks pose serious threats to many applications especially the safety-critical ones such as self-driving cars. Hence, it is crucial to institute countermeasures to prevent these attacks and establish a reliable communication system. Furthermore, to take the appropriate steps for the protection against such attacks, it is important to know the type of jamming attack that a network has been exposed to. In other words, in addition to detection, the classification of these attacks is also necessary. Therefore, in this paper, we tackle this problem and propose a machine learning-based classification technique for different types of jamming attacks. We simulate the jamming scenario in wireless ad-hoc networks using the network simulator ns-3 and use the data collected from the simulation to train and evaluate different algorithms. We compare the accuracy of each algorithm and provide the results that showcase that the classification of jamming attacks can be done with very high accuracy using the Gradient Boosting Algorithm.

Keywords: Jamming Attacks Classification, Wireless Networks, NS-3, Gradient Boosting

1 Introduction

Wireless networks play an important role in communication to provide a continuous connection and uninterrupted services. These networks are the key to achieving ubiquitous computing and help in realizing limitless use cases. Due to the widespread use of this technology, the security of such networks is an issue of major concern. An attacker can use jamming techniques to exploit various vulnerabilities of the MAC (Media Access Control) layer or PHY (Physical) layer protocols. An attacker can also launch intelligent jamming strategies by exploiting higher-level semantics such as ACK packets and DATA packets in the protocol layer. A jamming attack is a type of denial-of-service attack and involves transmitting a radio signal which decreases the signal-to-noise ratio and thus disrupting a legitimate communication between a sender and a receiver. Jamming attacks can be executed in multiple ways for example through a permanent jamming signal (Constant Jammer) that blocks all packages in a network, or injecting jamming packets in a network at random intervals (Random Jammer). An important subset

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 11(4):49-62, Dec. 2020
DOI:*10.22667/JOWUA.2020.12.31.049*

*Corresponding author: Division of Information Technology, Netaji Subhas Institute of Technology, 110078, Tel: +91-9458729314

of wireless networks are the Vehicular ad hoc networks (VANETs). The significance of detecting a jamming attack is expected to increase with the growth of safety-critical use cases. For example, in VANETs, drivers can be alerted about malfunctioning equipment through jamming detection.

Due to the vast scope and importance of this task, many solutions have been proposed for tackling RF jamming in the past. [11] employs Frequency hoping techniques such as Frequency Hoping Spread spectrum (FHSS), in the physical layer to stop jamming attacks. This technique involves hopping between various frequencies, such that the actual signal is spread and has a greater resistance towards interfering signals. Although this strategy is effective, it experiences large bandwidth wastage as the bandwidth required is much larger than the actual signal to be transmitted. Other solutions that address the jamming issue [20] include Ultra Wide Band (UWB), multi-antenna, and antenna polarisation. Also, there are many solutions to tackle the attack in multi-hop networks such as re-routing the traffic from the area in which jamming occurs. As wireless networks are highly susceptible to jamming attacks, an effective strategy to ensure their detection is essential to ensure normal operation. Further, apart from the detection of an attack, it is imperative to detect the type of jamming attack to utilize suitable countermeasures. This can be achieved by the careful comparison and analysis of a wireless network under both jammed and standard situations. Various metrics from different layers can be tracked which can potentially indicate whether a jamming activity has occurred such as Packet Delivery Rate (PDR) in the application layer, Channel busy time in the MAC layer, etc.

Therefore, in this paper, we provide a machine learning-based approach that can use such metrics to detect and classify different types of jamming attacks. We use ns-3 for the simulation of the jamming network and study three types of jammers i.e. constant, reactive, and random. We collect metrics from different layers through the simulation and feed them to the machine learning algorithm. The technique proposed achieves high accuracy, incurs minimal overhead costs, and can be used on the device. This work is an extension of the paper ”Machine Learning-Based RF Jamming Classification Techniques in Wireless Ad Hoc Networks” [7]. This version demonstrates a more thorough analysis of the data collected and introduces another algorithm for comparison to provide comprehensive results. The result presented in this version showcase a higher accuracy as well, due to the change in parameters during the dataset collection.

The remaining paper is divided into the following sections. Section 2 delineates the related work and background for the task of detecting and classifying jamming attacks in wireless networks. Section 3 presents our motivation behind proposing a framework to detect and classify jamming attacks. Section 4 describes the approach used in this paper for simulation and detection. Section 5 provides the results and analysis of the experiments conducted and finally, section 6 provides the conclusion and discusses the future scope of this work.

2 Related Work

Security is one of the major concerns in wireless communication. There have been many recent studies to address this concern including [15] by Vishal et al. which addresses security in 5G mobile networks, [6] by Jeong et al. which tackles intrusive incidents through the Internet. Due to the widespread nature of wireless communication [3], jamming attacks pose a serious threat to it. There have been many studies that showcase the effects of these attacks for 802.15.4 and 802.11 [10], [2] systems, in cellular systems [5], [14] [16]. In [13] by Oscar et al., jamming attacks in vehicular networks and their detection techniques have been studied and an improved algorithm for this detection has been proposed. Z.Yu et al. in [19], has studied jamming attacks and proposed a detection scheme in wireless sensor networks for loose communication channels. In [4], the authors have analyzed different jamming attacks and provided an approach for their detection as well as classification. Also, in [1], Emekcan Aras et al. have proposed

detection mechanisms for attacks in LoRa (Long Range) networks using simple hardware to counter the various security threats in LoRa and LoRaWAN (Long Range Wide Area Network) networks delineated in their work. Sudip Misra et al. in their work [9] have used a honey pot as a pre-emptive defense mechanism against jamming attacks. A dummy communication is generated by the honeynodes at a frequency comparable to the actual frequency of communication and authentic nodes are pre-emptively alerted of imminent attacks. Therefore, the authentic nodes are able to jump to a new frequency even before the jammer starts scanning that frequency. These examples underscore the importance of correctly detecting security issues in wireless networks and the need for taking appropriate steps for preventing them.

Similarly, in the case of jamming attacks which are analyzed in this paper, it is also important to distinguish between the type of attack that can be employed by an attacker in order to determine the correct countermeasures. In [18] by Wenyuan Xu et al., four such attack models have been proposed and their effectiveness has been evaluated by measuring their effects on communication between a sender and a receiver in a wireless medium. The work in [18] addresses the limitation that no single measurement can accurately confirm the presence of a jamming signal and therefore this necessitates the development of a more sophisticated scheme for such detection. This paper, therefore, proposes two enhanced schemes that use consistency checks. The first uses signal strength as a reactive consistency check while the other one uses location information. The paper analyzes the effectiveness and feasibility of both the schemes for the detection of jamming attacks.

In the present schemes, the physical layer techniques such as spread spectrum are used as the

Figure 1: References

countermeasures used against jamming attacks. However, these countermeasures may not be effective in all situations. The most effective choice in most scenarios is to detect jamming attacks. Oscar et al. in [13] have proposed a random forest-based method for the detection in 802.11 networks and shown that it performs best compared to other methods. Zhuo Lu et al. in [8] has created a robust and efficient detection system for time-critical networks using gambling based modeling.

The implementation of jamming scenarios is a challenge in itself and many researchers have used different strategies for this simulation. Vanhoef et al. in [17] have used WIFI hardware which is easily available to mimic a jammer by changing the open-source driver. This technique is cheaper and easier as compared to USRP which was used by Nguyen et al. [12]. Universal Software Radio Peripheral (USRP) can be used to implement reactive jammer using GNURadio for WIFI and WiMAX but is expensive and complex. Emekcan Aras et al. for their work used simple hardware that comprises of Rasberry Pi, Arduino, and LoRa Wireless to implement a jammer for LoRa networks.

3 Motivation

The problem of detecting jamming attacks has been tackled by many researchers but the classification of such attacks has not been studied in-depth and has room for improvement. These attacks can cause severe damages in many applications, especially in time-critical ones such as VANETS. Therefore the classification of jamming attacks is extremely vital so that suitable countermeasures can be employed to prevent and recover from such attacks effectively and efficiently. Also, due to the low resources of communication devices, the computation complexity and memory limit are major constraints for employing detection and classification algorithms. Therefore, in this paper, we propose a technique that can classify different types of jamming attacks without incurring major time and computation overheads.

Previous work by Feng et al. [4] proposes a similar technique that uses the Random Forest algorithm but through extensive experimentation, we show that the accuracy can be improved further by employing other machine learning algorithms that have better performance than Random Forest.

We use ns-3 to simulate and collect data for jamming and normal situations. We record the Packet Delivery Ratio (PDR) and Received Signal Strength (RSS) metric from the application and physical layers respectively for training different machine learning algorithms. We analyze the results from all algorithms in detail and provide a comparison to select the technique that performs best. The work presented in this paper can be used as the foundation work for further research for tackling and preventing different types of jamming attacks.

4 System Design

The aim of this paper is the detection and classification of Radio Frequency jamming by observing the RSS and PDR values at the receiver. These attacks can be easily executed by emitting a signal that causes interference and disruption of legitimate messages across a channel, thus stopping the receiver node from securing authentic signals. The end-to-end algorithm proposed in this paper is depicted in Figure 2 and the major steps involved are:-

- Collect data through simulation of different jamming scenarios (including no jamming) in ns-3 and use the data for training ML algorithms
- Use Gradient Boosting for the classification of different types of jamming attacks.

The work done previously for the classification of jamming attacks have used various machine learning algorithms. The algorithm that achieved the best performance was found to be Random Forest.

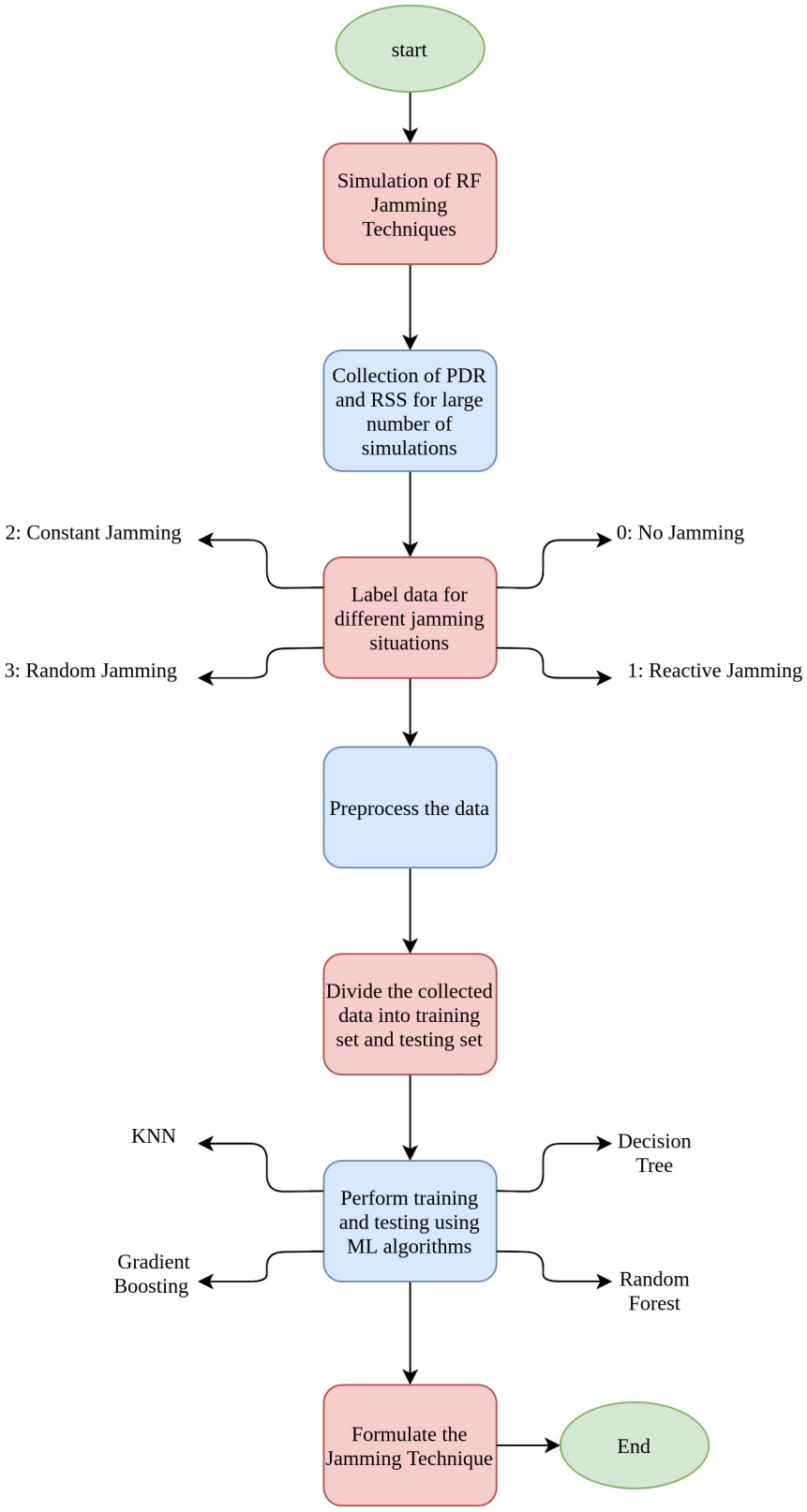


Figure 2: Proposed Algorithm

In this paper, however, we employ the Gradient Boosting Technique (GBT) and compare its results with other algorithms. We find that for detection and classification of jamming attacks, Gradient Boosting outperforms even Random Forest which was previously considered to be the best. We provide results from other algorithms (MLP, KNN, Decision Tree) as well to show comparison with GBT.

4.1 Gradient Boosting

The Gradient Boosting Technique (GBT) is an instance of a boosting algorithm which is an ensemble technique and can be used for both classification and regression tasks. Few important concepts for understanding GBT are as follows:-

- *Ensembling*: - An ensemble technique is the one in which the final predictor is formed by the collection of multiple weak predictors. For example, the prediction from many decision trees is combined either through majority voting or mean prediction values to form the final output in a Random Forest algorithm. The Ensembling hierarchy is shown in Figure 3.

- *Bagging*: - This is a type of ensemble technique in which the predictors are formed independently in parallel and the final prediction is the combination of all the predictors using a deterministic averaging technique e.g. Random Forest

- *Boosting*: - This technique is also an ensemble technique but differs from bagging as the weak predictors are formed sequentially, not independently. Each predictor learns from its predecessor and tries to correct the mistakes made by it e.g. GBT.

Hence, in GBT the predictors are formed sequentially as it is a boosting technique and therefore differs from Random Forest which is a bagging technique. The results provided in the paper show that using GBT for the classification of jamming attacks is more reliable than Random Forest. Algorithm 1 explains the algorithm for GBT, where X is the input, Y is the output and n are the number of training data points.

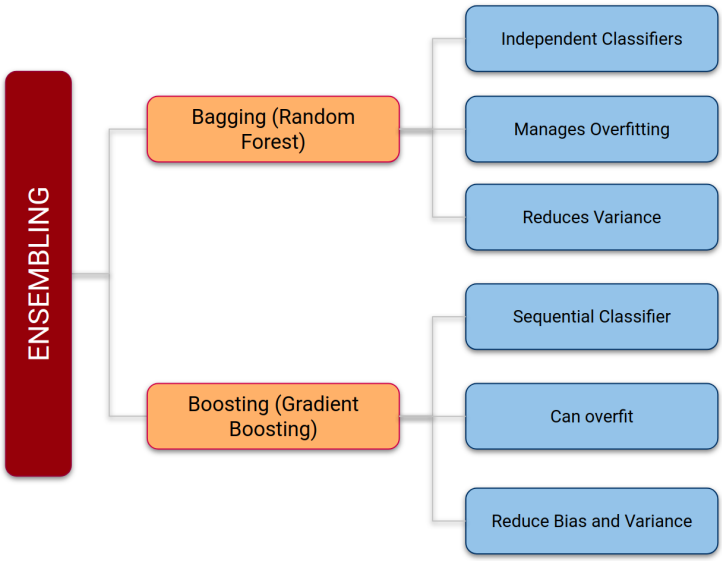


Figure 3: Ensembling Hierarchy

Algorithm 1 Gradient Boosting Algorithm

Fit estimator F^1
for i in $[1,M]//M$ weak estimators
$Loss^i = \sum_{j=1}^{n}(Y_j - F^i(X_j))^2$loss in ith iteration
calculate gradient:$-\frac{\partial L^i}{\partial X_j} = \frac{-2}{n} * (Y_j - F^i(X_j) \forall i$
Fit a weak estimator H^i on $(X, \frac{\partial L}{\partial X})$
//ρ changes the step size
Prediction: $F^m(X) = F^i(X) + \rho * H^i(X) = F^1 + \rho * \sum_{i=1}^{m} H^i(X)$

4.2 Jamming Attacks Model

Jamming attacks are a type of Denial-of-Service (DOS) attacks in which the attacker/jammer occupies the network channel where authentic nodes are communicating, thus preventing them from using the channel. The three types of jammers are:-

- *Constant Jammers*: A constant jammer continuously produces high-power noise in the form of random bits. This generation of random bits is independent of traffic in the channel or channel sensing. The jammer does not obey the MAC protocols.
- *Reactive Jammers*: A reactive jammer unlike a constant jammer uses channel sensing to become active only when there is transmitted through the channel. It corrupts few bits of the legitimate package in the transmission channel and therefore the packet received fails the checksum and is discarded by the receiver. The reactive jammer acts only when there is actual transmission in the channel.
- *Random Jammers*: A random jammer also does not follow MAC protocols and switches between sleep and jamming modes in random intervals of time. During the jamming interval, it can act as either a constant or a reactive jammer. It sleeps during random intervals irrespective of the traffic in the communication channel.

5 Evaluation

We collected the dataset using ns-3 by running simulations for multiple scenarios. The parameters such as the transmitting power and distance between the sender, receiver, and jammer nodes were varied to collect a large quantity of data. The preprocessing of data included the removal of duplicate values, handling null values, and normalization to remove the bias of algorithms towards a particular feature. The collected data was then used for the training of the proposed model and also for the analysis of different types of attacks.

The metrics used for the classification are Packet Delivery Ratio (PDR) and Received Signal Strength (RSS), which are obtained at the receiver's end. The above metrics can be observed easily through hardware that is already existing and do not require sender information unlike other metrics like noise. The PDR is calculated as the ratio of the number of packets received correctly to the total number of preambles received at the receiver node and the RSS is simply measured for each packet at the receiver. The PDR is updated in a sliding window for each successful delivery of a packet. It is considered to be zero in a sliding window if no packet is obtained at the receiver during that window. We collect the PDR and RSS values for different scenarios and label the data collected as follows:- a) No Jammer - 0, b) Constant jammer - 1, c) Reactive Jammer - 2, d) Random Jammer - 3.

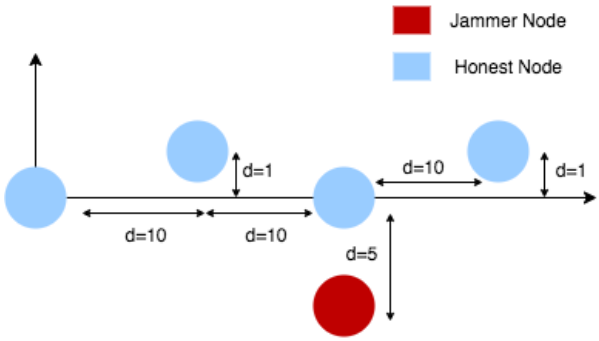


Figure 4: Configuration of Nodes

The layout used for simulation is shown in Figure 4. The position of all the nodes is a function of the variable ”d”.

- Node 0 (source) = (0.0, 0.0, 0.0)
- Node 1 = (d, 0.1 * d, 0.0));
- Node 2 = (2 *d, 0.0, 0.0);
- Node 3 (receiver) = (3 * d, 0.1 * d, 0.0);
- Node 4 (Jammer) = (2 * d, -0.5 * d, 0.0);

It has been observed by some researchers that PDR alone can be used as the metric to detect a jamming attack as during jamming attacks it is reduced significantly. But, it has been also shown that in congested networks, the value of PDR can still be very high (as high as 78%). This value, however, is reduced significantly if the link quality at the receiver is poor. Hence, using only PDR would not be sufficient to obtain good results and we require both PDR and RSS for the classification of jamming attacks. We, therefore, collect the data for both the metrics and vary different parameters during the simulation for different jamming scenarios. The PDR and RSS values are calculated in ns-3 using the wireless module utility at the receiver (i.e. Node 3). The function used is TraceConnectwithoutContext() which calls a callback function that records the PDR and RSS metrics. The callback function is called whenever the value of RSS changes. The parameters are varied as described below:-

- *Distance between the nodes:* The first parameter we vary is the distance between the nodes which is a function of the variable “d” (Figure 4. The RSS value is varied due to change in “d” and consequently, the PDR value is also changed. We observe that as the distance is increased the values of PDR and RSS are both reduced. The value of distance was varied between 7m to 13m in a linear manner. For each jamming situation(i.e. for all 3 jammers) the simulation was run for 60s and the jammer was switched on at 7s.
- *Transmission Power:* The signal strength at the sender during transmission is specified by setting the Transmission power (TX Power) metric. A reliable connection has a higher value of power and therefore a stronger signal is transmitted. On the other hand, lower transmission power will lead to a decrease in the RSS value and imply that the message will not go very far. Hence reducing the transmission power will lead to poor quality of transmission and reduced PDR. The Transmission power was varied from -20dBm to 20 dBm.

- *Number of Packets:* The number of packets was also varied which affects the congestion in the network. As congestion is increased, the PDR value decreases.

The collected data was labeled into 4 classes (No jammer, Constant Jammer, Reactive Jammer, Random Jammer). This data was normalized and shuffled and then split into training and test set. We considered two cases for the split and the best result was recorded.:-

- 60% train and 40% test
- 70% train and 30% test

The parameters for each of the classification algorithms were also changed as follow:-

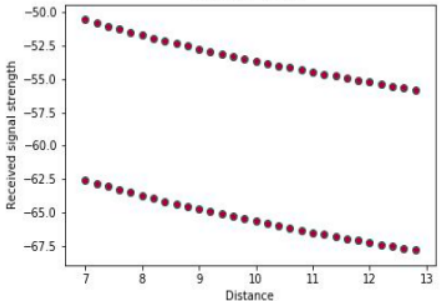
- *Multi-layer perceptron (MLP)* - The learning rate was taken as 0.001, 0.01, and 0.1, and also the number of iterations was changed from 100-300 with 50 intervals. The best result is reported in this paper.
- *Random Forest* - The number of predictors was taken as 2, 5, 10, 100, 1000, and the most accurate results were recorded.
- *K Nearest Neighbours (KNN)*- The neighbors were varied from 2 - 20 with a step of 2 and the most accurate results were recorded.
- *Decision Tree* - Only the basic case was tested and no parameters were changed.
- *Gradient Boosting* - The number of predictors was considered to be 1, 10, and 100, and also the max depth of each tree was taken to be 1, 10, 100. The learning rate was also varied from 0.1 to 1 with 0.1 as an interval.

Figure 5: Key for result analysis

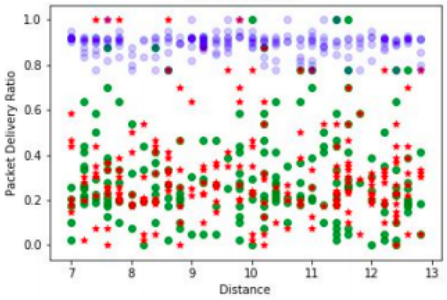
5.1 Data Analysis

We analyze the effect of increasing distance between the nodes and transmission power on the packet delivery ratio (PDR) and received signal strength (RSS) separately. For all the jamming scenarios, we vary the value of 'd' (Figure 4) from 7m to 13m, run the simulation for 60s, and collect the values of RSS and PDR at the receiver node. As per intuition (Figure 6a), as the distance between nodes increases, the received signal strength decreases for all jamming scenarios. Note that, in Figure 5, we have shown the color map for all jamming scenarios which is applicable for all subsequent graphical representations (Figure 6, Figure 7, Figure 8, Figure 9). In Figure 6a, we observe two lines where the upper line denotes the RSS when a data packet is being received by the recipient node, and the lower line represents the RSS when no data packet is being received. Figure 6b represents how PDR at recipient node changes when the distance between the nodes is increased. We observe that PDR in the case of random jamming lies in the upper range. To analyze the effect of transmission power, for all jamming scenarios, we vary power from -20dBm to 20dBm, run the simulation for 60s and collect the values of RSS and PDR at the

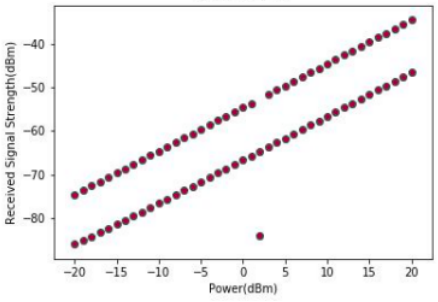
receiver node. As expected, in Figure 6c, we observe that as the transmission power increases, the RSS value at the recipient node increases. Figure 6d represents the variation of PDR with transmission power, and we again observe that PDR lies in the upper range for random jammer which proves the inefficacy of random jamming as compared to constant and reactive jamming.



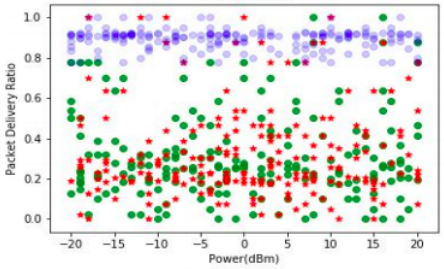
(a) RSS vs Distance



(b) PDR vs Distance



(c) RSS vs Power



(d) PDR vs Power

Figure 6: Analysis of RSS and PDR with changing distance and power

5.2 Experiments and Results

The simulation results for different scenarios are shown in Figure 7, Figure 8 and Figure 9. These graphs show that it is simple and straightforward to distinguish between jamming and no jamming situations as the RSS is increased during jamming scenarios because the received signal has the added strength of both the jamming signal and the original message. However, it is difficult to classify between different jamming attacks, as the graph for PDR vs RSS in these cases is more overlapping. Another trend that we can observe from the graphs is that for low PDR values the graph is congested whereas for higher values it is becoming more sparse in the case of the reactive and the constant jammer. Hence, these jamming techniques are more effective in blocking the original methods than random jamming for which PDR values are still comparatively higher. Also, we can observe that for no jamming situations, the value of PDR remains appreciable even with low values of RSS, the value is only dropped when RSS values decrease beyond a threshold and are almost diminishing.

We also provide accuracy for all 5 algorithms in different scenarios. Table 1 represents the accuracy in case of changing distance, table 2 represents the accuracy in case of changing power, and table 3 shows the accuracy for changing power as well as distance. In all three cases, it can be seen that Gradient Boosting performs extremely well on the classification task and surpasses the next best algorithm i.e. Random Forest by 2 - 3%. Also, the GBT algorithm achieves greater than 90% accuracy in all the cases.

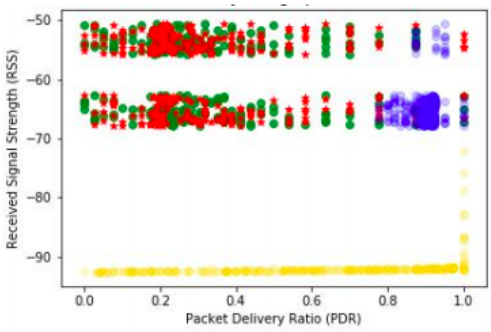


Figure 7: PDR vs RSS(for changing distance). Distance ranges from -10m to 10m and for each value of distance, simulation runs for 60s collecting PDR and RSS values for different jamming scenarios.

Machine learning Algorithm	**Accuracy**
Multi-Layer Perceptron	67.1%
KNN	71.5%
Decision Tree	87.8%
Random Forest	90.4%
Gradient Boosting (Our Model)	93.0%

Table 2: Accuracies (for changing transmission power)

Machine learning Algorithm	**Accuracy**
Multi-Layer Perceptron	68.2%
KNN	75.3%
Decision Tree	90.1%
Random Forest	93.0%
Gradient Boosting (Our Model)	94.9%

Table 1: Accuracies (for changing distance)

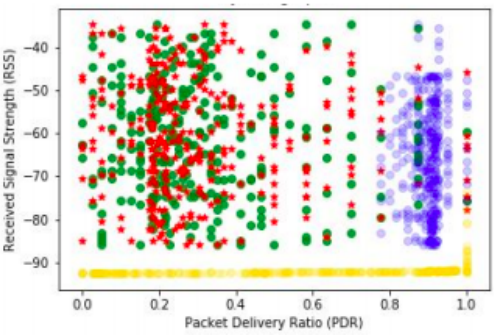


Figure 8: PDR vs RSS (for changing power) .Transmission power ranges from -20dBm to 20dBm and for each transmission power value, simulation runs for 60s collecting PDR and RSS values for different jamming scenarios.

Machine learning Algorithm	Accuracy
Multi-Layer Perceptron	67.5%
KNN	72.3%
Decision Tree	88.7%
Random Forest	92.6%
Gradient Boosting (Our Model)	94.2%

Table 3: Accuracies (for changing distance and power simultaneously)

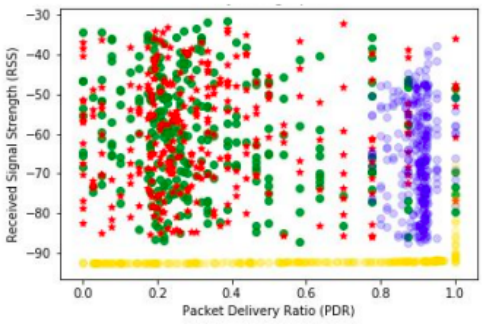


Figure 9: PDR vs RSS (for changing power and distance). Transmission power ranges from -20dBm to 20dBm and distance ranges from -10m to 10m, and for each combination of distance and power, simulation runs for 60s collecting PDR and RSS values for different jamming scenarios.

6 Conclusion

The paper proposes an RF Jamming classification using machine learning in wireless Ad-hoc networks. This classification is necessary in order to take appropriate steps to counter different types of attacks. We simulate a real-world scenario using the ns-3 simulator and use the data to train the ML algorithms. The results showcase the superiority of the gradient boosting algorithm in distinguishing between different types of attacks. We observe that although it is quite easy to distinguish between jamming and non-jamming scenarios, it is more difficult to differentiate between different jamming scenarios. The GBT overcomes this challenge to a great extent but the accuracy can be improved even further by optimizing and exploring other algorithms. Also, further research can be done for extending this topic to mobile nodes such as VANETS, and other features such as location, speed of nodes, etc. can also be considered for improving the accuracy even further. Another challenging task after classification is to devise strategies to counter each type of attack. The work done in this paper can act as the baseline for further research in this field as well.

References

[1] E. Aras, N. Small, G. S. Ramachandran, S. Delbruel, W. Joosen, and D. Hughes. Selective jamming of lorawan using commodity hardware. In *Proc. of the 14th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MobiQuitous'17), Melbourne, Victoria, Australia*, pages 363–372. ACM, November 2017.

[2] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa. Performance of ieee 802.11 under jamming. *Mobile Networks and Applications*, 18:678–696, August 2011.

[3] S. K. Dhurandher, J. Singh, I. Woungang, R. Kumar, and G. Gupta. Message trust-based secure multipath routing protocol for opportunistic networks. *International Journal of Communication Systems*, 33(8):e4364, February 2020.

[4] Z. Feng and C. Hua. Machine learning-based rf jamming detection in wireless networks. In *Proc. of the 3rd International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC'18), Shanghai, China*, pages 1–6. IEEE, December 2018.

[5] M. Hamalainen, V. Hovinen, R. Tesi, J. H. Iinatti, and M. Latva-aho. On the uwb system coexistence with gsm900, umts/wcdma, and gps. *IEEE Journal on Selected areas in Communications*, 20(9):1712–1721, December 2002.

[6] H.-D. J. Jeong, W. Hyun, J. Lim, and I. You. Anomaly teletraffic intrusion detection systems on hadoop-based platforms: A survey of some problems and solutions. In *Proc. of the 15th International Conference on Network-Based Information Systems (NBiS'12), Melbourne, Victoria, Australia*, pages 766–770. IEEE, September 2012.

[7] G. S. Kasturi, A. Jain, and J. Singh. Machine learning-based rf jamming classification techniques in wireless ad hoc networks. In *Proc. of the 3rd International Conference on Wireless, Intelligent and Distributed Environment for Communication (WIDECOM'20), Toronto, Canada*, pages 99–111. Springer, Cham, June 2020.

[8] Z. Lu, W. Wang, and C. Wang. From jammer to gambler: Modeling and detection of jamming attacks against time-critical traffic. In *Proc. of 30th IEEE International Conference on Computer Communications (INFOCOM'11), Shanghai, China*, pages 1871–1879. IEEE, April 2011.

[9] S. Misra, S. K. Dhurandher, A. Rayankula, and D. Agrawal. Using honeynodes for defense against jamming attacks in wireless infrastructure-based networks. *Computers & electrical engineering*, 36(2):367–382, March 2010.

[10] O. P. nal, A. Aguiar, and J. Gross. In vanets we trust?: Characterizing rf jamming in vehicular networks. In *Proc. of the 9th ACM International Workshop on Vehicular Inter-Networking, Systems, and Applications (VANET'12), Low Wood Bay, Lake District, UK*, page 83–92. ACM, June 2012.

[11] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein. Using channel hopping to increase 802.11 resilience to jamming attacks. In *Proc. of the 26th IEEE International Conference on Computer Communications (INFOCOM'07), Barcelona, Spain*, pages 2526–2530. IEEE, May 2007.

[12] D. Nguyen, C. Sahin, B. Shishkin, N. Kandasamy, and K. R. Dandekar. A real-time and protocol-aware reactive jamming framework built on software-defined radios. In *Proc. of the 2014 ACM workshop on Software radio implementation forum (SIGCOMM'14), Chicago, Illinois, USA*, pages 15–22. ACM, August 2014.

[13] O. Puñal, I. Aktaş, C.-J. Schnelke, G. Abidin, K. Wehrle, and J. Gross. Machine learning-based jamming detection for ieee 802.11: Design and experimental evaluation. In *Proc. of the 2014 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'14), Sydney, New South Wales, Australia*, pages 1–10. IEEE, June 2014.

[14] C. Shahriar, S. Sodagari, and T. C. Clancy. Physical-layer security challenges of dsa-enabled td-lte. In *Proc. of the 4th International Conference on Cognitive Radio and Advanced Spectrum Management (CogART'11), Barcelona, Spain*, pages 1–6. ACM, October 2011.

[15] V. Sharma, I. You, F.-Y. Leu, and M. Atiquzzaman. Secure and efficient protocol for fast handover in 5g mobile xhaul networks. *Journal of Network and Computer Applications*, 102:38–57, January 2018.

[16] F. Song, M. Zhu, Y. Zhou, I. You, and H. Zhang. Smart collaborative tracking for ubiquitous power iot in edge-cloud interplay domain. *IEEE Internet of Things Journal*, 7(7):6046–6055, December 2019.

[17] M. Vanhoef and F. Piessens. Advanced wi-fi attacks using commodity hardware. In *Proc. of the 30th Annual Computer Security Applications Conference (ACSAC'14), New Orleans, Louisiana, USA*, pages 256–265. ACM, December 2014.

[18] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In *Proc. of the 6th ACM international symposium on Mobile ad hoc networking and computing (MobiHoc'05), Urbana-Champaign, Illinois, USA*, pages 46–57. ACM, May 2005.

[19] Z. Yu and J. J. Tsai. A framework of machine learning based intrusion detection for wireless sensor networks.

In *Proc. of the 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'08), Taichung, Taiwan*, pages 272–279. IEEE, June 2008.

[20] L. Zhao, A. M. Haimovich, and H. Grebel. Performance of ultra-wideband communications in the presence of interference. In *Proc. of the IEEE International Conference on Communications. Conference Record (ICC'01), Helsinki, Finland*, pages 2948–2952. IEEE, June 2001.

Author Biography

Ansh Jain is currently working as a software engineer at Samsung RnD Institute Bangalore. He graduated from Netaji Subhas Institute of Technology in 2019, where he majored in Information Technology. Being a proficient coder, he enjoys developing creative and challenging solutions. His primary areas of research include machine learning and computer vision. He has had experience with research in the video analytics domain during his undergraduate studies (Research Internship at Indian Institute of Technology Kanpur) and work experience at Samsung (Developing Video editing solutions for consumers).

GS Kasturi is a graduate of Netaji Subhas Institute of Technology, University of Delhi, India. During her undergraduate course, she explored various applications of AI, including jamming attack detection. She also interned at the Indian Institute of Technology (Kanpur) and pursued research on Computer Vision and language. The internship molded her into a Computer Vision Enthusiast, actively exploring the domain, especially multimodal systems. Currently, she is working as a software engineer at Walmart Labs, building e-commerce solutions..

Jagdeep Singh is pursuing Ph.D. from Division of Information Technology, Netaji Subhas Institute of Technology, University of Delhi, India. His Ph.D work is based on networking area where he is exploring the routing techniques in opportunistic delay tolerant networks. He earned his M.Tech in Computer Science and Engineering from Kamla Nehru Institute of Technology, Sultanpur, India. His research interests are in machine learning, artificial intelligence, opportunistic networks, cloud computing, machine to machine communications, next-generation wireless networks. He has published his research in various reputed journals of computer science such as IET, International Journal of Communication System, Journal of Internet Technology and many more. He has also presented his research work in several national and international conferences such as IEEE ICC, IEEE GLOBECOM, IEEE INDICON, ACM ICDCN, AINA and many more.