GMR-23

Jamming Signal Detection Using Extreme Gradient Boosting (XGBoost) Algorithm

Abstract

- Radar jamming involves sending intentionally disruptive radio waves toward the target radar, which might over-saturate its receiver so it can't receive anything or deceive it into interpreting false information.
- Machine learning (ML) techniques increased the capability to automatically learn the experience without being explicitly programmed. Machine learning models usually require a large, labeled sample to perform.
- Building a robust jamming detection model will be challenging due to the wide variability of jamming signals and less available labeled samples.
- In this project, we developed an eXtreme Gradient Boosting (XGBoost) algorithms for radar jamming signal classification and achieved superior performance compared with Random forest and Support Vector Machine (SVM) considering the unique environment and challenges in RADAR/SDR signals.

Introduction

- In communication systems, jamming interference can cause degradation in the quality of transmitted signals, leading to increased noise levels, distortion, and loss of signal strength.
- Jamming is a big threat to radar system survival. Radar jamming can have catastrophic effects in various scenarios which lead to serious repercussions. When it interferes with vital infrastructure, commercial shipping lanes, or transportation networks, radar jamming can have a significant negative economic impact. The devastating consequences of radar jamming highlight the necessity of putting strong countermeasures in place because it can result in enormous financial losses.
- Therefore, technology to prevent jamming is required. By deploying anti-jamming systems, organizations can prevent such attacks, thereby safeguarding the confidentiality of data and preventing unauthorized parties from intercepting or tampering with communications.
- The classification of radar jamming signals is the first step toward anti-jamming. A complete anti-jamming detection process includes radar jamming signal classification, anti-jamming strategy selection, and anti-jamming performance evaluation.
- Machine learning models automatically identify important information and extract knowledge from data to make decisions. By detecting and classifying jamming signals, a more effective anti-jamming system can be created.
- We have used a large dataset to train, validate, and test machine learning models. In this study, we developed a robust Machine learning model which can classify signals even when there are less samples.
- To find radar jamming signals, the initial stage is to classify the signals. In order to classify, we are using Machine learning methods like Random Forest, Support Vector Machine (SVM) and XGBoost algorithms.

Dataset

The dataset is generated by measuring a received Wi-Fi (2.4/5GHz) signal and saving to a CSV file the following features:

- frequency
- noise
- Maximum Magnitude(max_magnitude)
- Total gain(total_gain_dB)
- Base power(base_pwr_dB)
- Received Signal Strength Indicator(rssi)
- Relative power(relpwr_dB)
- Avaerage power(avgpwr_dB)

Both jamming and non-jamming data are measured. The jammer is a HackRF One using JamRF that transmits at distances of 20, 40, 60 cm from the receiver and at powers of 0, 5, 10 dBm. The test is done in three different environments: an RF isolation chamber, laboratory, and office. During the test, each Wi-Fi channel is jammed sequentially.

Experimental Setup

Data Pre-processing:

- The time series data for each channel is then transformed into a single row with 7 by 7 features by applying seven descriptive statistics: minimum, maximum, mean, standard deviation, 75th percentile, 50th percentile, and 25th percentile making a total of 49 features.
- Set a target column for identifying jamming data as 1 and non-jamming data as 0.

Training and Testing:

- Employed CMIM feature selection algorithm, which can approximate the conditional multivariate mutual information of each candidate attribute with respect to the whole set of labels.

•For handling imbalanced data, we use SMOTE algorithm.

•We split the training and testing data into 70/30.

Machine Learning Methods:

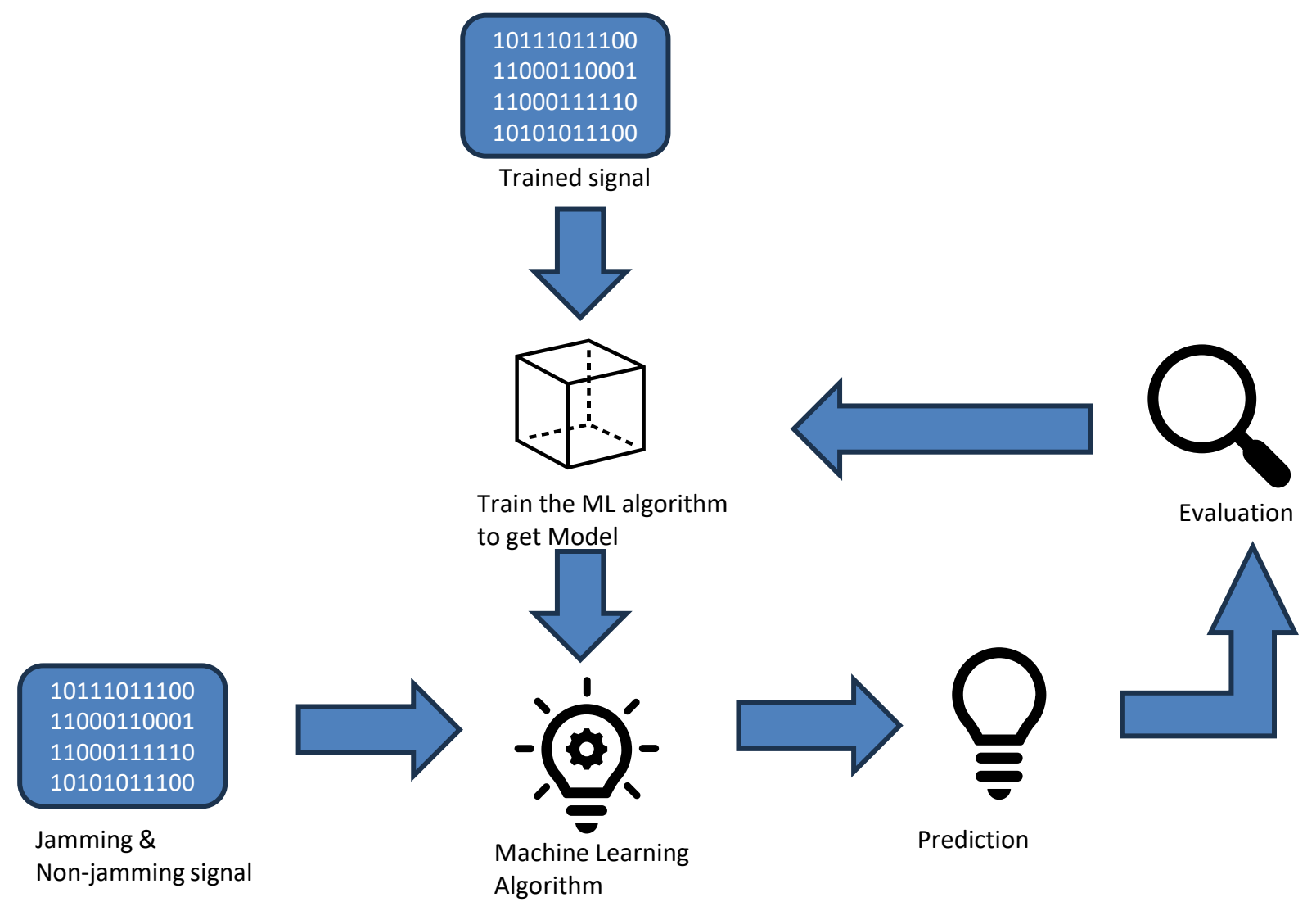

Fig. : Representing how a machine learning model works

- We have implemented the machine learning methods like Random forest, Support Vector Machine(SVM) and eXtreme Gradient Boosting(XGBoost) algorithms for comparison.

Results

The performance of the three distinct ML classifiers for jamming detection is compared.

Table 1: Performance comparison of ML algorithms

Classifiers	Accuracy
Random Forest(RF)	91%
Support Vector Machine(SVM)	84%
eXtreme Gradient Boosting	92%

To access classification model we use confusion matrix. The True positives (occur when the model accurately predicts a positive data point) have more values in XGBoost confusion matrix when compared to other classifiers. False positives (occur when the model predicts a positive data point incorrectly) have less values in XGBoost confusion matrix than others.

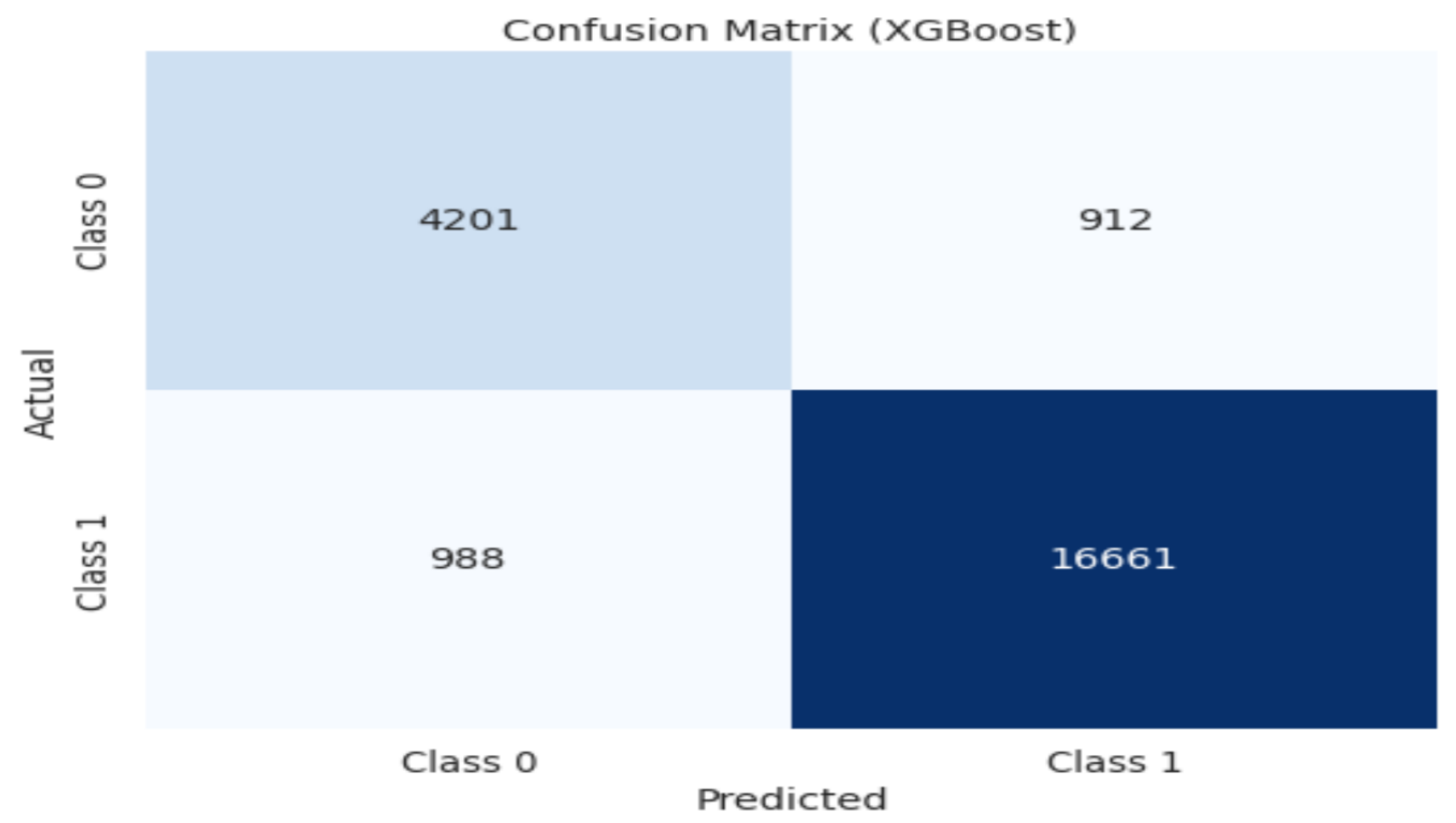

Fig.3 : Confusion Matrix of XGBoost Algorithm

Conclusions

In this study, we focused on the design decisions and challenges of implementing a machine learning model in a practical system. In addition, this article is supported by a set of measured data that can be used for jamming and interference detection. There is lack of radar signal to support the findings of this study. Our machine learning model is strong enough to identify signals. The results demonstrate that the XGBoost classifier can detect jamming attacks with a high level of accuracy and at a low cost. We applied XGBoost algorithm for jamming prediction for a radar signal. The prediction accuracy of the XGBoost model was higher on average than that of the other Machine learning models like Random forest and Support Vector Machine.

Future Work

We aim to encourage future research in two different paths. On the one hand, the presented data can inspire the creation of jamming and non-jamming data. Secondly, using anti-jamming techniques based on Deep learning model with transfer learning techniques. Image processing and object detection is one area which has seen significant performance improvements using CNNs. Our practical insights can assist the community in developing new RF jamming dataset generating testbeds and interfaces as required for future applications.

Contact Information

Kazi Aminul Islam kislam4@kennesaw.edu

Sumit Chakravarty schakra2@kennesaw.edu

Keerthana Adamana kadamana@students.kennesaw.edu

Christian Sao csao@students.kennesaw.edu

Acknowledgment

We would like to thank our professors, Sumit Chakravarty and Kazi Aminul Islam for guidance and motivation provided to us time to time. I would like to thank Department of Computer Science and Software Engineering to provide me this opportunity.

References

- Zhihong Ouyang , Lei Xue , and Feng Ding, "Research on the Influence of Track Jamming on Radar Data Processing", 2020.
- O. Punal, C. Pereira, A. Aguiar, and J. Gross, "CRAWDAD dataset uportorwthaachen/vanetjamming2012 (v. 2014-05-12),"
  Downloaded from https://crawdad.org/uportorwthaachen/vanetjamming2012/20140512 , May 2014.
- Abubakar S. Ali, Govind Singh, Willian T. Lunardi, Lina Bariah, Michael Baddeley, Martin Andreoni Lopez, JeanPierre Giacalone and Sami Muhaidat, "RF Jamming Dataset: A Wireless Spectral Scan Approach for Malicious Interference Detection", 10 2023.
- T. Chen and C. Guestrin, "Xgboost: A scalable tree boosting system," 08 2016, pp. 785–794

KENNESAW STATE UNIVERSITY
COLLEGE OF COMPUTING AND SOFTWARE ENGINEERING

Author(s) : Keerthana Adamana, Christian Sao

Advisors(s) : Kazi Aminul Islam, Sumit Chakravarty