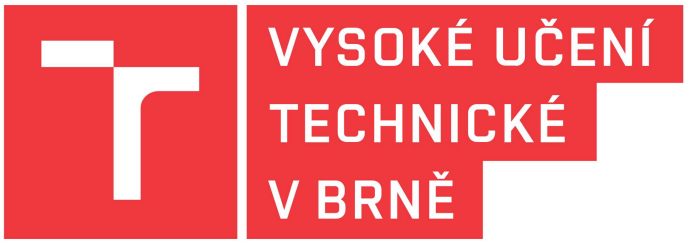
Adrian DORFMULLER
Mikael DOS SANTOS



Machine Learning Project

Classification of 5G Base Stations

Our GITHUB Link : https://github.com/urboyadrian/MLF_Project

1. Introduction

With the growth of mobile communication technologies, particularly 5G, there has been an increase in cybersecurity concerns targeting these systems. One of the significant threats is the deployment of rogue base stations, known as False Base Stations (FBS), which mimic legitimate network nodes and attempt to capture sensitive user data.

This project aims to implement and evaluate a machine learning-based model to identify whether a base station is legitimate or fraudulent using 4G LTE channel frequency response data. The objective is not only to achieve high classification accuracy but also to understand the model performance through various visual diagnostics.

2. Problem Description

The classification task consists of identifying base stations as:

- **Class 0**: Legitimate base station (gNodeB from T-Mobile)
- **Class 1**: Fraudulent base station at Position 1
- **Class 2**: Fraudulent base station at Position 2

Dataset

- Format: .npy files, each representing a 2D matrix of shape (72, 48)
- label_train.csv: Contains training labels and sample IDs
- test_format.csv: Contains IDs for test predictions

The dataset is highly imbalanced, with a majority of samples in Class 0.

3. Methodology

To begin, we ensured that all training data and labels were correctly aligned. This involved reading the label_train.csv file, which contains the mapping between sample IDs and their respective class labels, and matching each ID with its corresponding .npy file in the training folder. Each .npy file consists of a 2D matrix representing the LTE channel frequency response with dimensions (72, 48). These matrices were flattened into 1D vectors, resulting in 3456 features per sample. This transformation was necessary to adapt the data format for compatibility with traditional machine learning algorithms, such as Random Forests. Once the data was flattened, we applied standardization using the StandardScaler from Scikit-learn. This step ensured that the features had a mean of zero and a standard deviation of one, which helps improve the convergence and stability of many machine learning models.

For the classification task, we opted for a Random Forest Classifier. This choice was motivated by the model's inherent ability to handle high-dimensional feature spaces, as well as its robustness against overfitting, particularly useful when dealing with noisy or imbalanced datasets. Random Forests operate as an ensemble of decision trees, each trained on a different subset of the data, and aggregate their predictions through majority voting. This architecture allows the model to learn complex decision boundaries without requiring extensive feature engineering. Additionally, Random Forests are relatively fast to train and evaluate, making them ideal for initial experimentation and baselining.

To properly assess the performance of our model, we relied on several well-established evaluation metrics. While overall accuracy provides a general sense of performance, it can be misleading in the presence of class imbalance, as seen in our dataset. Therefore, we complemented accuracy with more informative metrics such as precision, recall, and the F1-score for each class. Precision quantifies how many of the predicted positives were actually correct, while recall measures how many of the actual positives were correctly identified by the model. The F1-score, which is the harmonic mean of precision and recall, provides a balanced measure that accounts for both false positives and false negatives. These metrics allow us to more thoroughly evaluate the model's effectiveness across all classes, particularly for the minority classes that represent fraudulent base stations.

4. Results and Visual Analysis

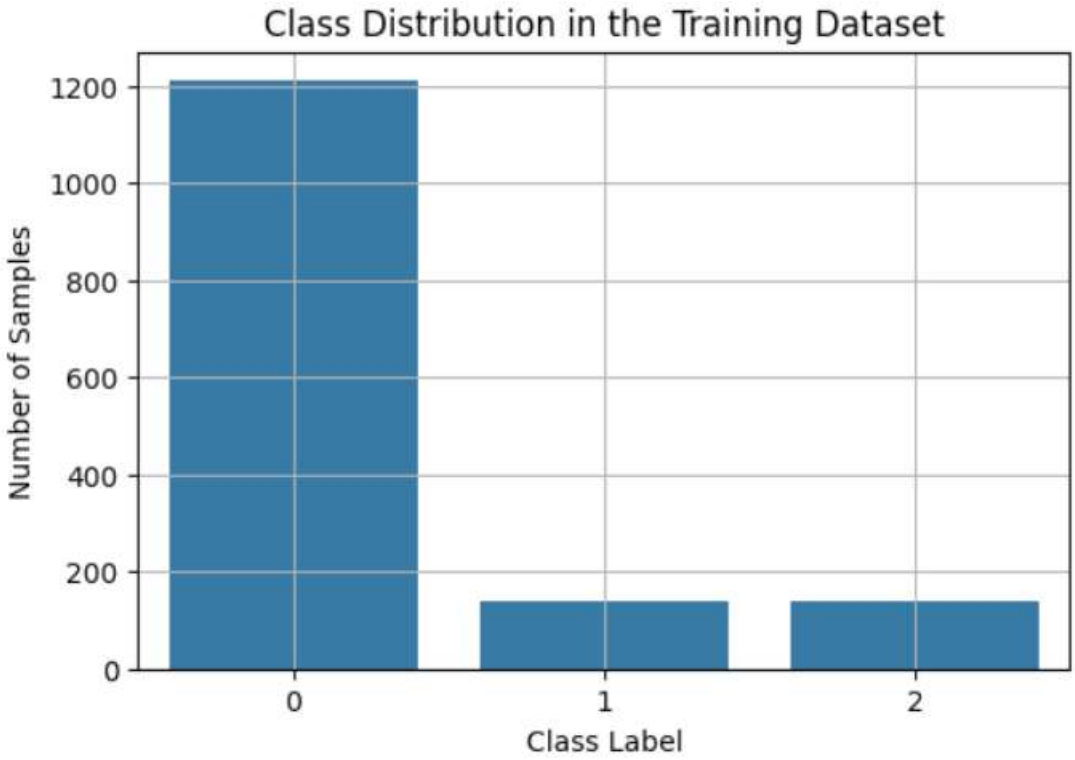


Figure 1: Class Distribution in the Training Dataset

This figure shows the class distribution within the training dataset. It clearly reveals a significant class imbalance, with Class 0 (legitimate base stations) vastly outnumbering Classes 1 and 2 (fraudulent base stations). This imbalance necessitates careful evaluation using metrics beyond overall accuracy.

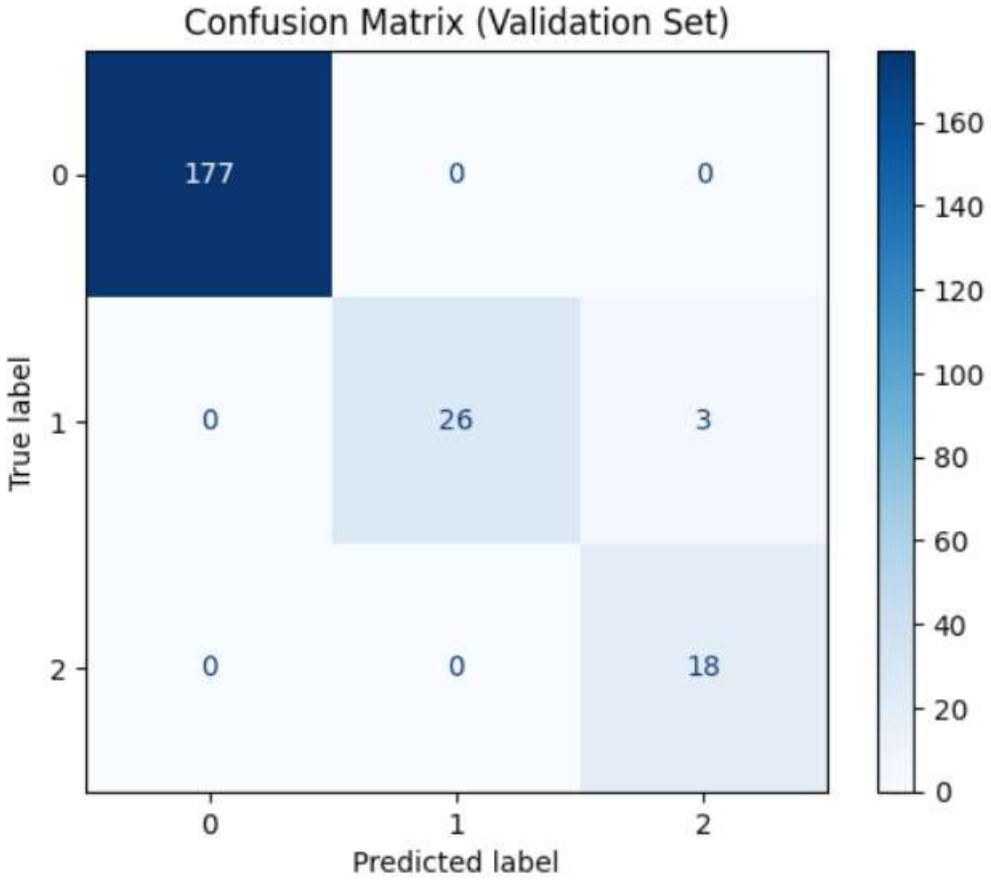


Figure 2: Confusion Matrix on Validation Set

The confusion matrix provides insight into the classification performance of our model. The model achieved perfect classification for Class 0, with all 177 samples correctly identified. For Class 1, 26 out of 29 samples were correctly classified, with 3 misclassified as Class 2. Class 2 was predicted perfectly with no false positives. These results show the model's strong discriminative capability between legitimate and fraudulent base stations.

Classification Report (Validation Set):

	precision	recall	f1-score	support
0	1.00	1.00	1.00	177
1	1.00	0.90	0.95	29
2	0.86	1.00	0.92	18
accuracy			0.99	224
macro avg	0.95	0.97	0.96	224
weighted avg	0.99	0.99	0.99	224

Figure 3: Classification Report

This report summarizes the precision, recall, and F1-score for each class. The model achieved perfect scores for Class 0, high scores for Class 1 (precision 1.00, recall 0.90), and strong performance for Class 2 (precision 0.86, recall 1.00). The macro-average F1-score is 0.96, and the overall accuracy is 99%.

These metrics confirm that the model performs exceptionally well across all classes despite the imbalance, with minimal confusion between the classes.

Figure 4: Final Kaggle Submission Score

Our final Kaggle submission achieved a **Public Score of 0.96666**, indicating strong generalization on unseen test data. The consistency between validation accuracy (99%) and the Kaggle score supports the robustness and reliability of our trained model.

5. Conclusion

In this project, we addressed the critical issue of detecting fraudulent 5G base stations, a major concern in the field of mobile network security. By leveraging supervised machine learning techniques and 4G LTE channel frequency response data, we designed and trained a robust classification model capable of distinguishing between legitimate and rogue base stations. Our approach focused on clear data preprocessing, reliable feature extraction by flattening channel response matrices, and the implementation of a Random Forest classifier, which proved to be highly effective for our problem.

The results demonstrated excellent classification performance, with a validation accuracy of 99% and a public Kaggle score of 0.96666. These results indicate that our model generalizes well and maintains high precision and recall across all three classes, especially crucial given the class imbalance in the dataset. The analysis of the confusion matrix confirmed the model's reliability, particularly in detecting legitimate base stations without being confused by fraudulent signals.

Beyond technical performance, our methodology highlights the importance of clean data alignment, the use of appropriate evaluation metrics, and the value of visual analytics for interpreting model behavior. These aspects contributed significantly to the success of our model and provided clear evidence of its robustness.

Overall, this project shows that machine learning can play a vital role in securing next-generation mobile networks by detecting potential intrusions through pattern recognition in signal data. The insights and results gained from this work provide a strong foundation for future exploration and real-world applications.

Key success factors include:

- Clean and aligned preprocessing between .npy files and labels
- A simple yet powerful Random Forest model avoiding overfitting
- Visual diagnostics confirming the reliability of predictions