Drone Detection and Mitigation using RF Frequency

Jordan Smith, Tuan Le and Gabriel Fedelin-Natividad
Advisor: Dr. Tamer Omar

Cal Poly Pomona

Project Overview

This project aims to create a drone detection, classification and mitigation system utilizing machine learning algorithms. Machine learning is used to classify different drone models. Based on the classification, a specific replay attack signal is transmitted to force the detected drone to land.

Hardware and Software

Fig.1 Hack Rf One and Universal Radio Hacker

The **HackRF One** and **Universal Radio Hacker (URH)** are two important tools used in this project. The HackRF One is used to receive and transmit RF signals for the detection and mitigation components. URH is used to interface with the HackRF, and through the URH Command Line Interface we can run everything in Jupyter Notebook.

Dataset

Fig.2 DJI Mavic Air, Bokigibi and Roku F11 Pro drones

The dataset we used consists of multiple different drone signals for different operations such as: idling, moving up or down, turning left or right, or powering on or off. The **Mel-Frequency Cepstral Coefficients (MFCC)**, features of these signals are then extracted and stored in .npy files to allow for faster system execution. Landing signals are also included in the dataset, which will be transmitted after detection to force the drone to land.

System Architecture

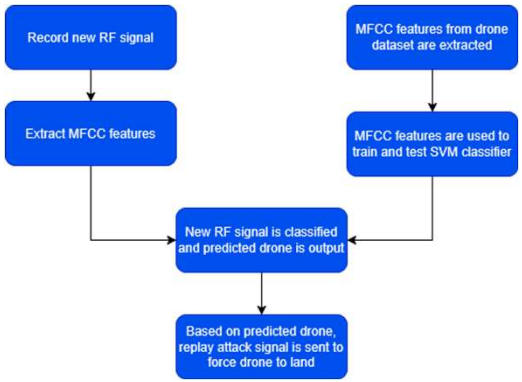

Fig.3 System Architecture Flow chart

This system is designed to identify and mitigate drones based on their **radio frequency (RF)** signals. It begins by capturing a new RF signal from a nearby drone, from which MFCCs are extracted as distinguishing features. These features are then fed into a Support Vector Machine (SVM) classifier that has been pre-trained using MFCC features from a dataset of known drones. Once the classifier predicts the identity of the drone, a corresponding replay attack signal is transmitted to manipulate the drone's behavior, forcing it to land.

PCA Results

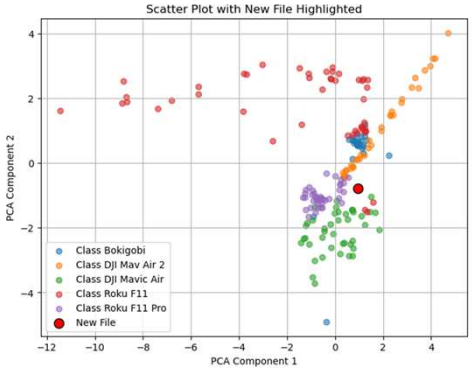

Fig.4 PCA plot of MFCC features and new file

This **PCA Scatter Plot** shows a reduced two-dimensional view of our drone RF signals, with each color representing a different drone model. The distinct separation of clusters suggests clear differences between drone types. A newly recorded sample, highlighted in red, appears near the cluster of its likely class, indicating an effective classification.

Confusion Matrix

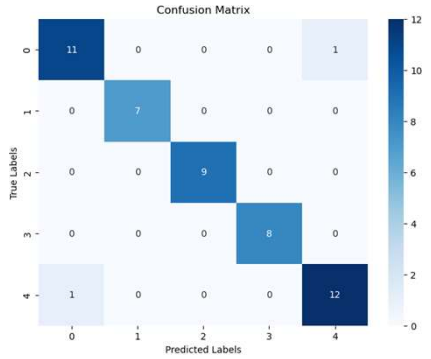

Fig.5 Confusion matrix for SVM classifier

The **Confusion Matrix** above shows the performance of the SVM classifier in identifying drone classes based MFCC features. Each row represents the actual drone class, while each column represents the predicted class. The strong diagonal dominance indicates high classification accuracy, with most signals being correctly identified. Misclassifications are minimal, occurring only between Class 0 and Class 4, suggesting a slight similarity in their RF patterns. Overall, the model demonstrates robust performance with accurate drone identification across all five classes.

Future Work

Improvements could be made in the features that are extracted from the RF signals and used in machine learning. Time-Domain, Frequency-Domain or Time-Frequency features could all be extracted and used instead of or together with the MFCC features to achieve superior classification results. Additional improvements should also be made in the replay attack system, as many drones have rolling code systems that would prevent our current implementation of replaying command signals from working.