Automating Unmanned Aerial Vehicle (UAV) Classification and Detection through Signal and Image Recognition

ENS Anirudh Murali, USN

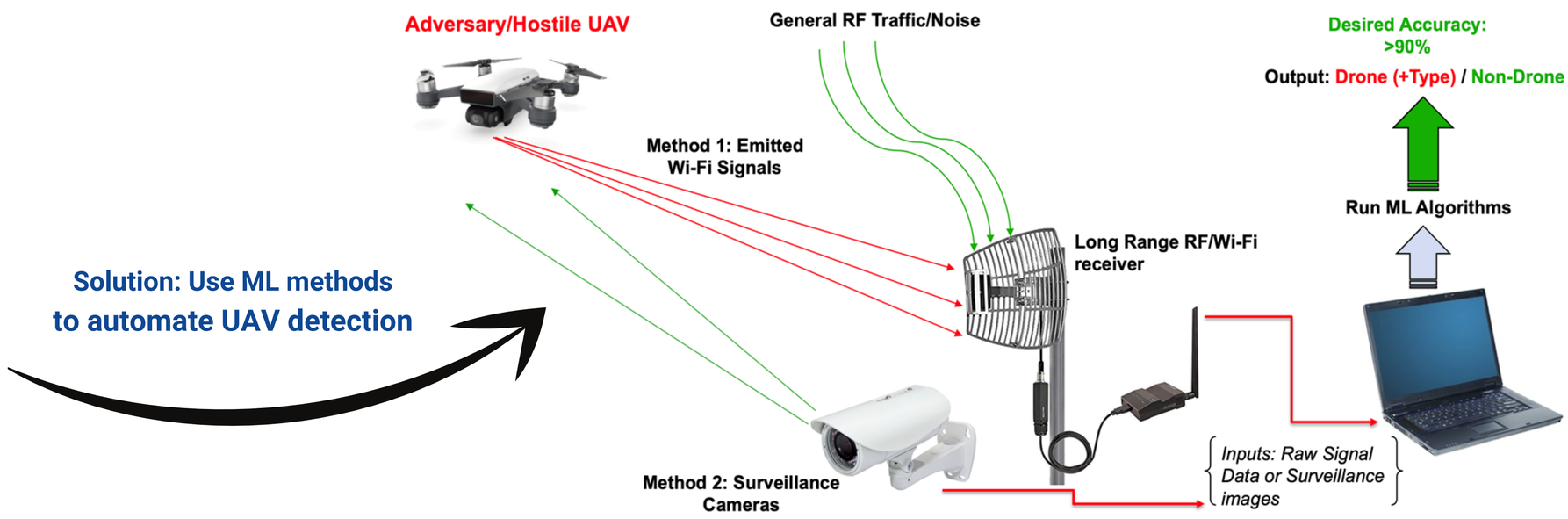
Company Advisors: Dr. Sean Duffy, Dr. Elizabeth Godoy, Dr. Jeff McHarg

Faculty Advisor: Jordan Levine

Motivation

- Unmanned Aerial Vehicles (UAV) are increasingly utilized in both military and civilian settings.
- Increased drone use leads to significant security concerns
- Manual detection through traditional RADAR systems is inefficient and difficult

Problem Statement



Timeline

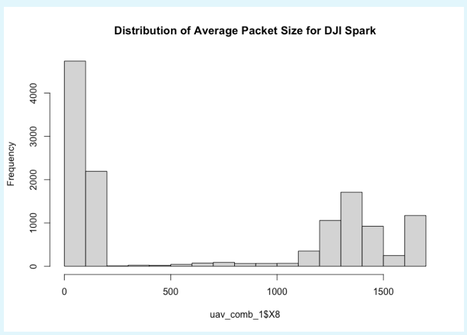
Wi-Fi Data Sourcing → Exploratory Analysis → Clustering Analysis → Wi-Fi Binary Modeling → Wi-Fi Multiclass Modeling → Sensitivity Analysis → Build Image Database → Image Neural Network Modeling → Develop Implementation Scenarios

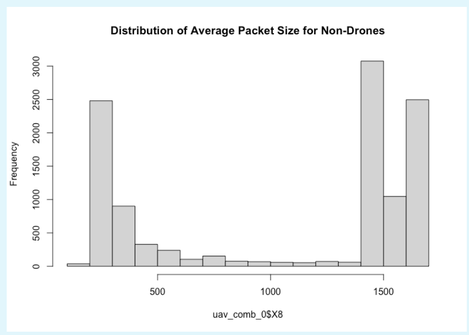
Detection Method 1: Wi-fi Based

Data description

- 6 datasets covering 3 Civilian UAV variants (DJI Spark, Parrot Bebop, DBPower UDI)
- Raw data features are Wi-fi Packet Size (bytes) and Packet Interarrival Time (ms)
- **Feature Engineering:** We generate 18 statistical measures derived from the raw data to expand the feature space
- Mix of UAV signals and general network traffic from laptops, smartphones, internet streaming, etc

Exploratory Analysis + Clustering





A univariate analysis of raw Wi-fi Packet size reveals clear distinctions between UAV(left) and General Traffic(right). This indicates that our data is well suited for a machine learning approach.

Cluster #	1	2	3	4	5	6	7	8	9	10
UAV	3	0	704	3	0	0	6063	1448	3837	801
Non-UAV	2523	3673	560	1657	670	12	421	740	627	371

Cluster assignments generated from our K-means clustering algorithm. Clusters 7,8, and 9 contain **88.2% of UAV data points**, while clusters 1, 2, 4, and 5 contain **75.5% of General Traffic**. Clustering results indicate that we can confidently categorize unlabeled data in the future

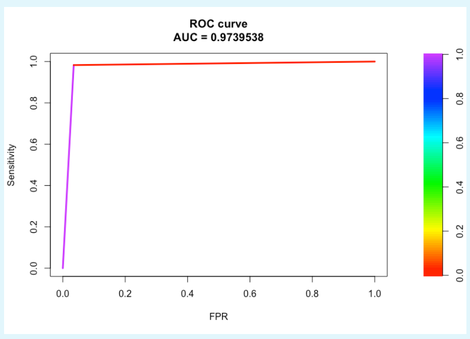
Classification Modeling

Binary

We begin with a simpler binary classification problem to distinguish between a single UAV variant and general network traffic. Both Logistic Regression and ensemble methods perform admirably, with XGBoost providing the best overall results.

Modeling Results

Model	AUC	Accuracy	False Positive Rate	False Negative Rate
Logistic Regression	0.91	92.1%	2.4%	2.5%
Random Forest	0.94	97.9%	2.9%	1.9%
XGBoost	**0.973**	**98.8%**	**1.16%**	**1.2%**

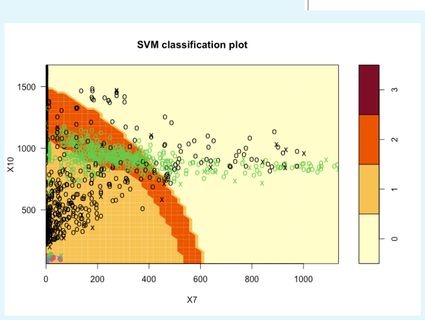


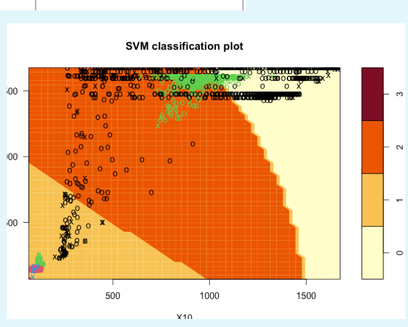
Multiclass

In real-world settings, there will likely be multiple different types of drones operating concurrently. As such, we not only want to distinguish whether a certain signal is from a UAV, but also classify exactly what type of UAV is being detected. By combining the binary classification datasets, we develop a multiclass problem with four distinct classes (3 UAVs + General Traffic). We model this scenario utilizing a Multiclass Support Vector Machine.

Modeling Results

Type	*Prediction Accuracy*
Overall	**93.173%**
DJI Spark	94.25%
Parrot Bebop	92.11%
DBPower UDI	93.02%



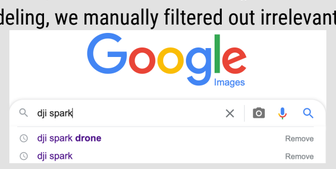


Detection Method 2: Image Based

Using the same 3 drones as the Wi-fi dataset, we build an image database in order to train image recognition neural networks. The primary goal of this modeling is to enable automated UAV detection via modern surveillance camera systems.

Database Construction

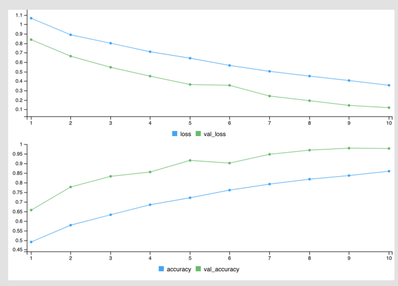
To construct the image recognition database, we coded an image scraper which takes a Google Image keyword search as an input, and accordingly downloads a specified number of images. Our final database consists of ~30,000 images (10,000 per UAV type). Prior to modeling, we manually filtered out irrelevant images to ensure a high-quality dataset.



Neural Network Modeling

After constructing the database, we pre-process all images by scaling them to identical sizes and specifying the desired color palette.

We then train a Sequential Convolutional Neural Network (SCNN).
Our best performing model achieves a prediction accuracy of **84.5%**.
Visualized below is the improvement in model validation performance per training iteration

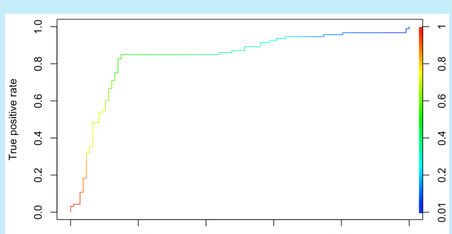


Wi-fi Sensitivity Analysis

To explore the effects of data noise (a key element in practical model implementation), we conduct a thorough sensitivity analysis on both the binary and multiclass models. We perturb data points using random draws from Uniform and Normal distributions. The parameter for these distributions are based on the mean and standard deviation of individual features.

As expected, model performance drops when data is perturbed, however the results below indicate that despite perturbation, our models still perform admirably. Due to the high potential for noise in the data-collection process, we believe these results can accurately reflect the range of performance that will be seen in the real world.

Binary Results



Perturbed data **AUC = 0.82**, as compared to 0.97 for non-perturbed data

Multiclass Results

Model	Accuracy
Non-Perturbed	93.175%
Uniform Dist.	89.37%
Normal Dist.	90.42%
Normal Dist. w/50% perturbation	91.89%

We see that accuracy drops by 2-4% in the multiclass scenario

Implementation Scenarios

Civilian Implementation

In the civilian sector, our models can be implemented by the Federal Aviation Administration (FAA) in order to improve safety and security in areas surrounding airports.

We also envision local/federal law enforcement agencies implementing these models to better manage security and privacy concerns associated with increased UAV use.

Military Implementation

In military settings there are various potential applications of our research. Using our models, military bases both domestic and abroad can capitalize on their signal and video surveillance systems to enable early detection and warning of incoming adversary UAVs. Our models can also be implemented on Naval vessels, which have traditionally relied on RADAR systems for aerial detection.