Fall 2021

RF Fingerprinting Unmanned Aerial Vehicles

Norah Ondus
Embry-Riddle Aeronautical University, ondusn@my.erau.edu

RF Fingerprinting Unmanned Aerial Vehicles

by

Norah Ondus

A thesis submitted in partial fulfillment of the requirements for the degree of
Master of Science in Cybersecurity Engineering
at Embry-Riddle Aeronautical University

Department of Electrical Engineering and Computer Science
Embry-Riddle Aeronautical University
Daytona Beach, Florida

NOV2021

RF Fingerprinting Unmanned Aerial Vehicles

by Norah Ondus

This thesis was prepared under the direction of the candidate's Thesis Committee Chair, Dr. Laxima Niure Kandel, and has been approved by the members of the thesis committee. It was submitted to the Department of Electrical Engineering and Computer Science in partial fulfillment of the requirements for the Degree of Master of Science in Cybersecurity Engineering.

_____
Laxima Niure Kandel, Ph.D.
Committee Chair

_____
Dr. Houbing Song, Ph.D.
Committee Member

_____
Dr. Omar Ochoa, Ph.D.
Committee Member

_____ _____
Babiceanu, Radu F, Ph.D. Date
Chair, Electrical Engineering and Computer Science

_____ _____
James W. Gregory, Ph.D. Date
Dean, College of Engineering

_____ _____
Christopher Grant, Ph.D. Date
Associate Provost of Academic Support

Acknowledgments

I am deeply grateful to ALLAH, and I would like to express my sincere gratitude to my family for their support and my advisor, Professor. Laxima Niure Kandel, for providing me with the guidance and counsel I need for writing my thesis. I also thank Dr. Houbing Song and Dr. Omar Ochoa for their willingness to serve on my committee and for all the support.

Table of Contents

List of Figures

Abstract

As unmanned aerial vehicles (UAVs) continue to become more readily available, their use in civil, military, and commercial applications is growing significantly. From aerial surveillance to search-and-rescue to package delivery the use cases of UAVs are accelerating. This accelerating popularity gives rise to numerous attack possibilities for example impersonation attacks in drone-based delivery, in a UAV swarm, etc. In order to ensure drone security, in this project we propose an authentication system based on RF fingerprinting. Specifically, we extract and use the device-specific hardware impairments embedded in the transmitted RF signal to separate the identity of each UAV. To achieve this goal, AlexNet with the data augmentation technique was employed.

Chapter 1

Introduction

Unmanned Aerial Vehicles (UAV) or Unmanned Aircraft Systems (UAS) commonly known as drones fly without a human pilot and are controlled remotely by a remote controller. Some drones can even fly autonomously. The complete system includes the controller and communication system in conjunction with sensors and GPS. UAVs have payloads that are lighter than a person, which allows them to be much smaller. Weaponized military UAVs are lighter than crewed counterparts with equivalent weapons while carrying large payloads. Because civilian UAVs lack life critical components, they may be made of lighter but less durable materials and forms, and their electronic control systems can be less thoroughly tested [1]. The design of quadcopter is now common for small UAVs. However, it is rarely utilized for crewed aircraft. UAVs can be classified based on their weight, altitude, degree of autonomy, and composite criteria.

Lately, UAVs are widely being used for different military, commercial and civilian applications. They are highly effective while minimizing the overall cost and risks. Unmanned aerial systems (UAS) are being developed for a variety of reasons, one of which is being economical. Smaller vehicles may thus provide a significant advantage in terms of stealth applications for various defense and security purposes. They are more likely to make less noise and blend in with their surroundings when appropriately suited to their surroundings using the well-known method of camouflage. Miniaturization allows for the

employment of less powerful propulsion systems that would be impossible to utilize in a crewed aircraft, such as small electric motors, sensors, and battery packs. The main use of UAVs in the military is for recognition and surveillance missions. Another benefit of miniaturizing UAVs is that they may fit into extremely narrow spaces such as ventilation pipes, tunnels, pipelines, collapsed structures, and sewer pipes. Ground vehicles are more prone to become trapped in such confined areas than flying aircraft. Drones and internet of things (IoT) technologies have produced new business applications. Drones combined with on-ground IoT sensor networks may assist agricultural firms in monitoring land and crops, energy companies in surveying power lines and operating equipment, and insurance companies in monitoring claims and policies [2]. The most important commercial use of UAVs is in the agriculture field. Due to resource depletion, farmlands are reduced, and with the short supply of agricultural labor, there is an urgent need for more convenient and smarter agricultural solutions than traditional methods as global demand for food production grows exponentially [1]. Agricultural drones have been utilized in different farmlands to assist in the development of sustainable agriculture. With the ongoing Covid-19 pandemic situation, UAVs are conveniently used for delivering goods.

However, the increasing application space has also led to increased threats and security breaches some of which are discussed by the authors in [3]. The detection and identification of UAVs in important for the military and public security. The low flying height and small radar cross-section of UAVs are the two biggest obstacles to the detection of the UAVs. Surveillance radar concepts against UAVs are often based on mechanical rotating antenna concepts that are mounted on high observation locations such as the tops of buildings or steeples. In a city with numerous high buildings, the situation becomes worse, especially

when towering structures block the line of sight. Various companies and research organizations are using Class 1 UAVs to combat the danger [4]. In a high-dynamic environment, these concepts are much time taking, and based on the exhibiting effects, they are too expensive to deploy on a large scale.

Since UAVs are limited in computational and energy resources, RF fingerprinting methods for the secure detection/authentication of UAVs are gaining traction from the research community. RF fingerprinting is a physical layer (PHY) method that helps in detecting transmitter-generated features (noises) at the receiver side [5]. Because of random hardware noise and dynamic multipath reflection in interior situations, achieving decimeter-level accuracy with commodity technology is difficult. When we convert our analog signal to a digital signal using DAC, some sort of noise is added to the signal. Noise affects the phase of the signal. We can further use this phase offset as a fingerprint of the UAV. RF fingerprinting with deep neural networks has shown tremendous potential for the detection of static UAVs but there is not much work has been done for flying UAVs. Moreover, the UAVs hovering introduces complex variations between the transmitter and the receiver, which should be taken into the account for solving the problem. Different machine learning (ML) algorithms were also introduced to learn the hardware features of the UAVs in order to detect them. In this work, we are applying a customized Alexnet neural network for the UAV classification. Alexnet uses multiple convolutional filters with different sizes to fully extract the features from the input signals. Due to the dense convolutional approach of the model, Alexnet proves itself very promising in high accuracy hovering UAV classification. The trained model was tested in different scenarios which included testing on same bursts as in training data as well as testing on unseen bursts which

did not appear in training data. One vs all approach was applied while training. Results show that the proposed model can achieve an identification accuracy of 85%.

Chapter 2

Literature Review

Physical layer security techniques have been widely investigated for WiFi devices [6-8]. In [6], the author presented a study in which their team evaluated the performance of 802.11n in a practical environment, Performance of the module which uses spatial diversity, spatial multiplexing, and channel characteristics were observed under different testing scenarios. In their testing scenario, they used 3x3 MIMO (Multiple-Input Multiple-Output) along with RF equipment to measure the received signal values. According to the author, increasing the number of antennas to three resulted in improved MIMO gain up to 2.2x. Furthermore, they reported that spatial diversity also improved the overall MIMO gain. They compared 2x3 configuration with 3x3 and 2x3 outperformed the other one. 2x3 configuration runs faster on more than three-quarters of the links. Modern NIC report CSI information that has embedded hardware noise along with the channel gains. This CSI is exploited by many researchers for security. In [7], a novel CFO-based WiFi device fingerprinting mechanism along with CFO estimation using CSI was proposed. The authors proposed a solution to overcome the long-standing threats such as network freeloading and rogue APs. The author proposed a readily deployable solution based on Channel State Information (CSI) and Carrier Frequency Offsets (CFO). This solution does not require any changes on access points and network infrastructure. The proposed solution predicts the CFO of wireless devices from their CSI only. Since CFO is purely based on oscillator drifting and it changes continuously, it is embedded in the transmitted signal and added to the received phase of the signal. Therefore, CFO cannot be manipulated very easily. They

performed a variety of experiments and tests on 23 phones and 34 access points. The author reported that their proposed solution can detect attacks with 93% accuracy. Over the last decade, many studies have proven themselves for the precise indoor WiFi device location for emergency applications. These WiFi devices have the benefit of being low cost and minimal complexity. There is a lot of interest and research for exploiting WiFi technology like the 802.11n standard for indoor localization. In this paper, the authors [8], provide a brief literature review of the recent WiFi localization devices, mainly targeting their pros and cons, technical details, and future work. Due to the fewer number of antennas, WiFi devices suffer from non-trivial phase noise. This can be minimized by using spatial smoothing, which helps in decreasing the correlation by averaging the signal from incoming antennas. Other techniques include using wired communication to cancel the errors, channel reciprocity, use of large distance to remove antenna coupling, and complex conjugate method to cancel the errors. All above WiFi-based research demonstrates that physical layer security is a promising security tool and is particularly useful for resource-constrained cyber-physical systems such as UAVs.

UAVs are widely employed in military and civilian industries due to their tiny size, low cost, and high versatility. They face cyber dangers in addition to the broad applications of UAVs and the tremendous growth of information technologies. False spoofing is a common cyber-attack among them. If this attack hits UAVs, it could cause property damage as well as the disclosure of private information or confidential documents. The author here [9], proposed Double Shortcuts Zero-Bias Residual Network. is a UAV anomalous data detection system with a modest store capacity and low time complexity. It is created by merging residual blocks with double shortcuts and a fully linked Zero-Bias

(ZB) layer for anomaly detection. The detection accuracy of the Double Shortcuts ZB-ResNet model is enhanced by roughly two percentage points when compared to the experimental findings of the upgraded Convolutional Neural Networks with ZB layer. In paper [10], the author presents a framework for sequential and time-dependent abnormalities detection. Regarding classification borders and abnormalities, the author investigated the latent space features of zero-bias neural networks. Then, they showed how to convert zero-bias DNN classifiers into performance-assured binary abnormality detectors using a unique technique. Finally, they present a sequential Quickest Detection (QD) technique that uses the converted abnormality detector to offer the theoretically ensured lowest abnormal event detection delay under false alarm limits. They test the framework's usefulness in aircraft communication systems and simulation utilizing real huge signal recordings.

Thus, recently UAV security using physical layer is gaining importance and a wide variety of UAV detection and classification methods have been proposed [11–13]. In [11], the author overviewed the trajectory design, communication protocols, resource allocation, cooperative UAVs and their wireless communication. They proposed MIMO and millimeter wave UAV system for improved communication security and better system spectral efficiency. They did a comprehensive analysis on NOMA(Non-Orthogonal Multiple Access), Beamforming, and mmWave techniques which enhances the performance of physical layer security. UAVs integration to the future 5G wireless cellular network will bring a lot of benefits for UAVs and the telecommunication industry. UAVs can be used as new mobile aerial platforms in the cellular network to provide

communication services for ground users, or will serve as aerial users for the ground base stations. Aerial wireless networks however are more prone to jamming or eavesdropping by malicious ground nodes and also impersonation attacks by malicious UAVs in the aerial wireless network [12]. The authors in [12] analyzed Ground-to-Air and Air-to-Ground UAV networks and proposed different solutions with their own pros and cons to address the above mentioned challenges with aerial wireless networks. The techniques proposed include 3D beamforming, UAV coordination, utilizing UAV mobility. 3D beamforming requires a large antenna at UAV; UAV coordination requires signaling overhead while leveraging UAV mobility which adds to more energy propulsion and consumption. In another research work [13], the authors analyzed physical layer security of Air-to-Ground UAV and derived an expression for Secrecy Outage Probability (SOP) for analyzing the security of a network numerically. This work considers the security of a Network Flying Platform (NFP) which communicates with the ground nodes in the presence of single or multiple eavesdroppers. SOP expressions are used to analyze the level of security in the case of standard and beamforming wireless communication networks for single or multiple eavesdroppers. The beamforming communication network proved to be more effective to counter eavesdropping but the overhead cost for beamforming must be considered. In [14], the authors leverage phase differences between multiple RF chains within the same receiver. The relative difference between the different RF transmitter oscillators over a MIMO (Multi-Input Multi-Output) network was used as a distinguishing feature or fingerprint. The authors showed through experiments that phase difference remains stable over time and frequency thus it can be used as a distinguishing trait. This requires hardware to measure phase difference and was done under specific conditions. This approach

introduced in the paper showed promise in case of wired networks achieving accuracy of 97% in identifying the transmitter network interface cards (NICs), but the accuracy reduced in the case of wireless transmissions and under mobile conditions. Neural Networks have also shown promising results in RF fingerprinting. The authors in [15] used Convolutional Neural Network (CNN) for identifying and verifying wireless transmitters. A CNN architecture VGG16 was modified for fingerprinting wireless transmitters. The model was trained on 5 wireless transmitters, and they achieved an accuracy of 99.7%. The data used for the training purposes was synthetic, so it requires further improvements for real-world application.

Unmanned aircraft systems (UAS) are gaining popularity worldwide, especially in the United States. UAS are well used for safety concerns and enable more successful scientific research. However, UAS poses a threat due to increased reliance on computer and communication-based technology, jeopardizing the national security, safety, and privacy of the public [16]. A counter-UAS (C-UAS) system is capable of disabling, interrupting, or seizing control of an unmanned aircraft or UAS legally and safely. In recent years, import researches have been done on C-UAS, based on acoustic, passive, vision, radar, or data fusion; and state of the art mitigation technologies. A typical system would have two subsystems: one for detection to detect, stalk, and identify the UAS, while also having a minimal footprint and supporting automated functions and location services. The second subsystem is mitigation for legal and safe control of UAS, with little collateral damage and minimum cost. The need for a detection and mitigation system is explained by discussing the different safety, security, and public threats. Therefore, it is to be believed that an integrated system capable of identifying and mitigating UAS will be critical to their safe

integration into the airspace system. The development of aviation revolutionized the way we explore the globe [17]. Planes present us with the excess of new options for completing tough jobs. Unmanned aerial vehicle (UAV) drones have grown in popularity as a way to reduce the risk to human pilots while completing difficult operations. The cost and difficulty of building highly agile UAVs have both decreased considerably. Different privacy, public safety, and security issues have arisen as a result of the simplicity with which drones may be flown. To solve this problem, the dual approach: detection and eviction are proposed. Using the SDR receivers, the system initially searches the channels often utilized by uninvited drones in the surveillance region. We can identify the uninvited drone's telemetry control and video streaming channel using pattern recognition algorithms. A piece of warning information is communicated into its analog video streaming channel to depart the drone from the observation region. The other solution will be to disable the drone's telemetry channel and activate its return strategy. The next step is to decode the UAV's telemetry channel's baseband symbols using a raw SDR classifier. If the decoding operation is regarded as successful the landing commands are put into the UAV's control channel. Some of the challenges of the proposed approach are the relevance of acoustic detection on high SIR, sensitivity to Gaussian noise. The SVM-based classifier is sensitive to bit error rate.

UAVs are also used for indoor applications like asset tracking and surveillance and require accurate location/position estimation. Global positioning system (GPS) is either unavailable or has weak received signal strength and hence cannot be used for indoor applications. To properly land in indoor aprons, GPS is required for coordination. Therefore, we need some non-GPS-based solutions to succeed in dealing with these

problems. Vision-based solutions are being used to overcome the problem, but they don't perform well due to the poor illumination and relative positioning instead of global positions. To cater to this problem, WiGig Beam Fingerprinting based positioning system was proposed by the author [18]. WiGig devices are assumed to be low powered and off-the-shelf devices for short distance communications. In the proposed approach, location fingerprint is estimated by the beam patterns of low power WiGig. To eliminate the possibility of error, a weighted K-nearest neighbor algorithm is used in the positioning process. In other experiments, the position localization errors at the 90th percentile are less than 1m. The authors in [19] used a machine learning method which focuses on the transmission delay and packet size of encrypted Wi-fi traffic for UAV detection and operation mode identification. Features are extracted using only the size of packet and inter-arrival packet delay. Packet size and inter-arrival packet delay vary from vendor to vendor due to vendor-specific implementation of UAV command control and video streaming protocols. Operation mode which can be standby, hovering, or flying, etc. also affects the relevant features. The machine learning model was optimized for feature selection as well as prediction within one model using one objective function. Experimental results showed that the proposed methods could detect and identify tested UAVs within 0.15-0.35s with a maximum accuracy of 95.2%. The UAV detection range is within the range of 70m and 40m in the line-of-sight (LoS) and non-line-of-sight (NLoS) scenarios respectively. Another proposed framework AirID [20], uses Deep Convolutional Neural Network to identify UAVs based on I/Q samples transmitted by different UAV transmitters. Software Defined Radios (SDR) mounted on UAVs were used to transmit signals to the ground receiver. CNN model was trained on this data to detect and identify

UAVs. Impairment(fingerprints) were added to the data post-training to test the robustness of the model. Real world experiments were performed in a 100 sq ft area and the model achieved an accuracy of 98% for the classification of UAVs. Another work in [21], provided a framework to perform UAV detection and Classification by splitting the raw signals into frames and then converting them into wavelet domain. This reduced bias of the signal and the size of data to be processed. Features selected from the energy-time domain and Naïve Bayes approach were used for the detection of UAVs. K-nearest neighbor (KNN) was used to classify the UAV while achieving an accuracy of 96%. These tests were performed on synthetic data generated by Monte Carlo simulations. In another work [22], the authors performed the detection and classification of UAVs in the presence of Wi-fi and Bluetooth interference. A multistage detector was used to detect UAV controller signal from background noise and interference signals. After detecting the UAV controller signal, it is classified using k-nearest neighbor (KNN) model. Neighborhood Component Analysis (NCA) was used to reduce the irrelevant features from data. Tests were performed at 25 SNR to achieve an accuracy of 98.13%.

In this work [23], the authors proposed the WiFi-based approach using statistical fingerprinting analysis for the detection of aerial devices. Different features related to UAV controller and video transmission are extracted from the WiFi network. All traffic flows are captured by the WiFi channels. The acquired data are then pre-processed and sent to global traffic capture to extract the key features of the UAV. The performance of the proposed solution is tested in different cases and reported with an average precision greater than 96 %. Thus, the identification and detection of illegal drones have become a huge challenge for researchers. In this paper [24], the authors proposed a hierarchical learning-

based approach for the detection and identification of UAVs. The detection system consists of a UAV controller and two receivers to record the signal strength from the UAV. The first receiver records the lower band RF signals, and the second receiver records the high band RF signals. The collected RF signals are processed using the LabVIEW software. The generated dataset is used to train the proposed method for detection and identification. The data is pre-processed again before the hierarchical learning approach. The filtering process is used to eliminate the noises, conflicts and to reduce the data size. Total four classifiers are used, the first classifier looks into the presence of UAV, the second classifier helps to detect the type of UAV, and the last two classifiers are used to define the modes of Bebop and AR. The reported classification accuracy of this approach is nearly 99%. The use of unmanned aerial vehicles (UAVs) in the urban setting has grown which increases the security risk and difficulty in managing airspace resources. To resolve these issues, the positioning of UAVs technology is used. Although the time of arrival (TOA)-based location technology is extensively utilized because of its great precision, its effectiveness in an urban setting may be hampered by severe multipath and (NLOS)non-line-of-sight propagation. The authors in [25], proposed a two-stage machine learning detecting method and used ray tracing simulation to build the multipath fingerprinting dataset. Ray tracing simulation provides the channel impulse response of the site and all the reflection and scattering points of the paths. The coarse positioning with the random forest is proposed to increase the distance between the labels. It helps in locating the UAV region. The next stage is the fine positioning in the neural network, where networks are trained to predict the precise position of the UAVs. They demonstrate through simulation that the method placement error is less than 16 m for 90 % of cases.

Moreover, for extracting communication channel characteristics of UAVs, the author [26], proposed empirical mode decomposition (EMD) and ensemble empirical mode decomposition (EEMD) methods. To train machine learning model for RF pattern recognition, intrinsic mode functions (IMF) are used as features. The author used EMD and EEMD signal decomposition for micro UAS classification and detection. Since each intrinsic mode function has its own frequency domain components which are used for communication between UAV and its remote controller. The pattern formed by these IMF is used to classify different UAVs with quite a good accuracy. The introduction of EMD and EEMD results in a denoising effect which improved overall classification accuracy. In the paper [27], the author proposed a time domain based multiple UAV classification-based model. In the proposed algorithm, transient signal and video signal are converted to time domain using short time Fourier transform. To remove unwanted and redundant dimension features, Principal Component Analysis (PCA) technique is used to reduce the dimension of given data. Support Vector Machine (SVM) and K-Nearest Neighbor algorithms (KNN) are trained on this rectified data. Author reported 98% accuracy for the SVM model. The Internet of Things (IoT) is quickly becoming an integral part of daily life, enabling a wide range of new services and applications. The prevalence of rogue IoT devices, on the other hand, has exposed the IoT to untold dangers with grave implications. Detecting rogue IoT devices and identifying authentic ones is the first step in safeguarding the IoT. The authors divide IoT device detection and identification into four categories in their paper [28]: device-specific pattern recognition, Deep Learning enabled device identification, unsupervised device identification, and anomalous device detection. From the standpoint of machine learning, the author analyzed existing non-cryptographic IoT device

identification technologies and identified several major emerging themes, including continuous learning, abnormality detection, and deep unsupervised learning. The rise of relatively inexpensive unmanned aerial vehicles has resulted from the advancement of new technologies. Concerns about privacy, public safety, and security have been raised as a result of these UAVs. Inadequate control over UAVs that reach critical locations is one concern posed by unauthorized UAV operation. An acoustic technique can be used to detect the presence of a UAV in one approach. In paper [29], the authors have recognized that and suggested some techniques to cater to these issues. To identify the appearance and estimate the position of unknown UAVs, a wireless distributed acoustic sensor network can be deployed. Furthermore, a software-defined radio (SDR) can apply machine learning techniques to recognize and decode the unauthorized UAV's telemetry protocols. Acoustic techniques may have a restricted detection range and may not be able to give spatial localization of a detected UAV, especially in three dimensions. In paper [30], the author proposed an approach using the UAV position. In this approach, UAVs may be required to send their positions via a standardized protocol or beacon, such as the Automated Dependent Surveillance Broadcast (ADS-B). However, such an approach is not without its drawbacks. Deep Learning (DL) is widely used in the Internet of Things (IoT). Applying deep neural networks to IoT devices results in a new generation of apps capable of complicated sensing and recognition tasks, allowing humans to interact with their physical surroundings in new ways [31-33]. Non-cryptographic Device Identification (NDI) is one of the DL-based IoT applications. Various Incremental Learning algorithms are used in the NDI system. The major drawback of IL algorithms is their extensive storage requirement which is not suitable for IoT devices, and their performance degrades when historical data

is not available. To address the issues, different suggestions have been proposed. First, a new metric, Degree of Conflict for quantifying the topological maturity of DNN models is introduced. Then, to explain the catastrophic forgetting in DNN models, a novel perspective on causation the “Conflict of fingerprints” is presented. The enhanced IL scheme, Channel Separation Enabled Incremental Learning (CSIL) is designed for the wireless identification system. The proposed framework is evaluated with real data **“**Automatic Dependent Surveillance-Broadcast”. The result accurately identifies the IoT devices and can be generalized to the medical domain such as virus detection.

Chapter 3

Methodology

3.1 Dataset Gathering:

The UAV dataset was gathered from [1]. For the data generation, atotal of 7 UAVs were used in experiments. To avoid any signal disturbance and interface, UAV experiments were done in an RF anechoic chamber. For the testing, DJI M100 drones were used as transmitter. In the receiving end, high-performance USRP X310 boards were used. In the dataset, 4 pairs of distances were used. UAVs flew at 6,9,12,15 ft distance from the receiver. Different experiments were done at these specific distances. In the experiment, 2 sec data of each UAV was recorded with a pause of 10 sec respectively. This process was repeated 3 times to avoid any noise and outlier value. That 10s pause interval is used as the separation between intervals. In 2s data, there are 140 signals which were sent to the receiver from the transmitter. These 140 signals are labeled as a Burst. Single UAV sends 4 bursts in a single communication. Visual representation is shown in Figure1. There are almost 13000 experiments data in total. Raw signals are saved in binary format in the IQ form. Each experiment has its own metadata file which contains details about the experiment [34].

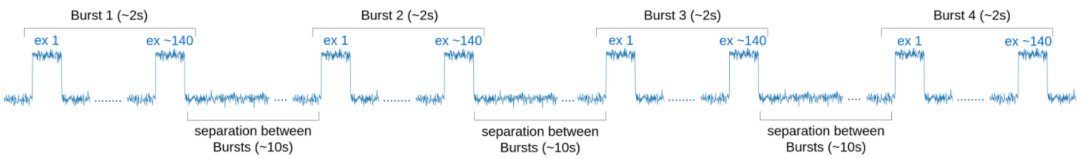


Figure 1. I/Q samples collected from a set of UAVs at a certain distance [34]

3.2 Dataset Preprocessing:

Dataset is split into training, validation, and test sets depending on different strategies which will be explained in a later section. Next, we calculate the mean μ and standard deviation σ for the whole dataset in a preprocessing step. This mean and standard deviation are used to normalize the training and test batches. Neural Network is trained on the slices of examples which are non-overlapping portions of examples and contain consecutive raw I/Q samples. Data batches were prepared with a slice size of 200 using the *Data Generator* class of *Keras* library. During training, random set of examples are loaded in memory and random slices are extracted from these examples which results in shuffling of training set without loading all of it into memory. This provides more variation of the training set to be observed by the model, resulting in a more robust model. Slices equal to "batch size" are selected from different examples to form a batch with I/Q samples separated into two channels forming a tensor with dimension (batch size, 200, 2). This tensor is then normalized using mean μ and standard deviation σ calculated previously as shown below before feeding the data into the model for training:

$$X_{normalized} = \frac{X-\mu}{\sigma} \qquad [35]$$

Before training the model, data examples were partitioned based on the distance of UAVs from receiver. For each partition, 7 separate datasets were created where each dataset was designed to identify a specific UAV from the rest. This partition of data caused an imbalance in training data which means that there was a large difference in positive examples as compared to negative examples. This imbalance results in the overfitting of

the model on more abundant examples. To overcome this problem, slices from an equal number of positive and negative examples were sampled for each batch during training.

3.3 Neural Network Training, Validation & Testing

For the neural net, modified 1D AlexNet with ~1.1 million parameters were used as shown in Fig. 2. The modified version of AlexNet1D consists of 5 blocks of 1D Convolution layers stacked together. Each block consists of three layers which include a 1D convolutional layer with 128 filters and size 7 followed by another 1D convolutional layer with 128 filters and size 5. A MaxPooling layer is attached at the end of each block. These blocks are followed by 2 Fully Connected (FC) layers with layer sizes of 256 and 128 respectively. The final layer FC layer consists of a single neuron for binary classification.

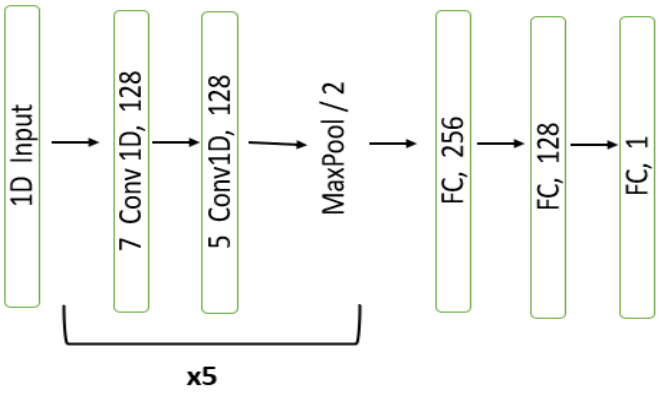


Figure 2. Neural Network Architecture for AlexNet 1D with ~1.1M parameters

The neural network was trained to identify one UAV from the rest. So, binary cross-entropy loss was used to train the model with Adam optimizer. A learning rate of 0.0001 was used for training. After each epoch, the neural network was tested on the validation set. After training, the model was tested on a test set. Equal slices were sampled from positive and negative examples for the test set to get balanced accuracy same as during training. Each

slice was normalized with previously recorded mean and standard deviation before being fed into the model.

The model was trained for two scenarios.

Scenario 1 - Training on all bursts and testing on all bursts: In this scenario, the dataset was first shuffled and then split into sequences of 60%, 20%, and 20% for training, validation, and test for each distance, UAV, and each burst. The data was shuffled to allow neural the network to go through the data in multiple variations every epoch so that it can be trained more robustly against noise. The data is split into train and validation to monitor if the model is overfitting during training.

Scenario 2 - Training on 1,2, 3 bursts and testing on 4th burst: For this case, the model was trained on bursts 1,2,3 with 90% for the training set and 10% for the validation set. After training, the model was tested on burst 4. This scenario was performed to measure the effects on accuracy in case there is an unseen burst in test data that did not appear during training.

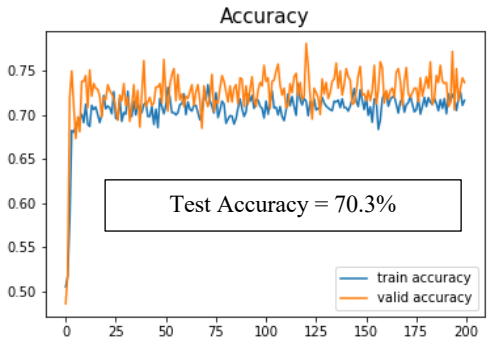
Chapter 4

Evaluation and Results

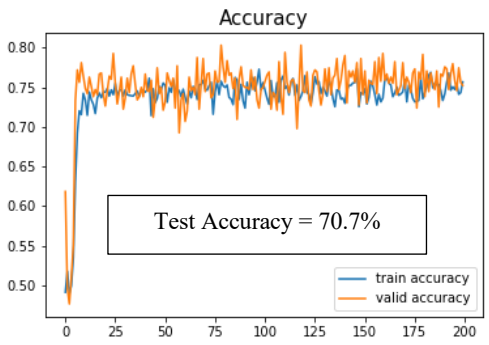
We have gathered from 7 different UAVs at 4 different distances. After the data gathering, processing was done on the raw collected dataset. Different bursts of the signal were created using a single raw signal. 1D Alexnet was trained with two scenarios. In 1st scenario, all the burst data was divided into two parts. One data part was used for training the model while the other was used for testing. In 2nd scenario, the first 3 bursts were used for training while the last burst was used only for testing. Following are the results for Alexnet1D trained on all bursts and tested on all bursts.

Results Scenario 1 (4 burst of data was shuffled, then divided into training, validation, and testing):

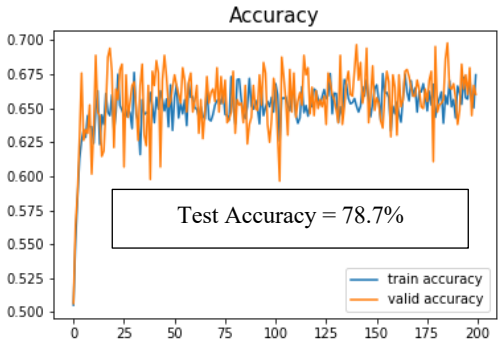
Scenario 1 & distance 6 ft



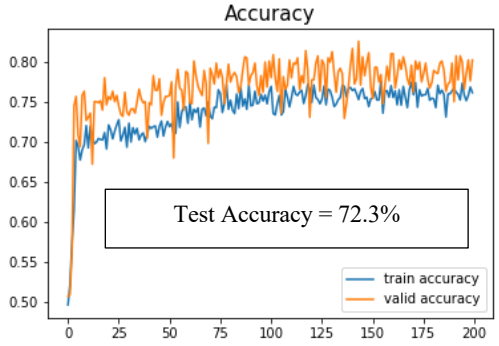
(a) UAV 1



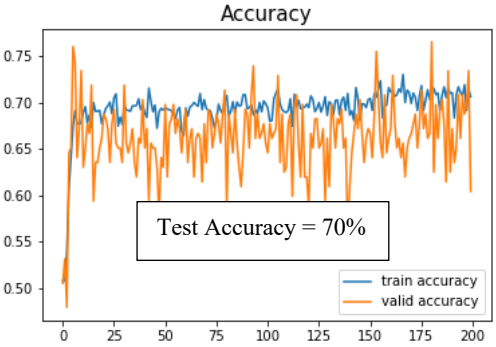
(b) UAV 2



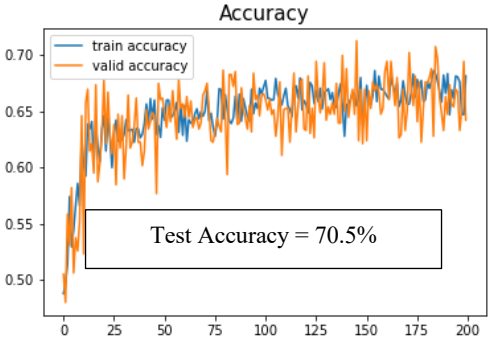
(c) UAV 3



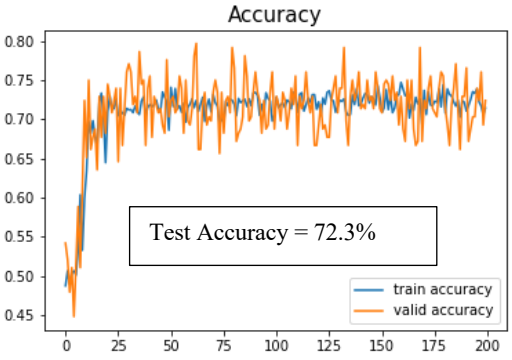
(d) UAV 4



(e) UAV 5



(f) UAV 6



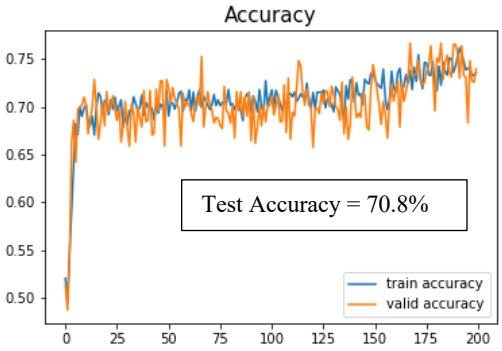
(g) UAV 7

Figure 3. UAV Identification Accuracy for Distance 6 ft and scenario 1.

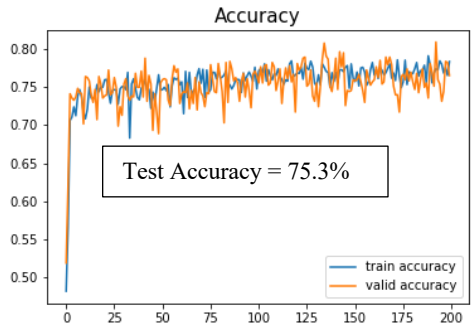
The above results show that the accuracy of the model on test data at 6ft distance remains above 70% consistently as the bursts 1, 2, 3 and 4 appear in train as well as test data. Since the data is shuffled the variation caused by the channel is shuffled and hence the training,

validation and testing are equally impacted. Because of this, we can see that the training and testing accuracies are similar. Also, for the shorter distance of 6 ft the signal to noise ration (SNR) is higher yielding larger test accuracy.

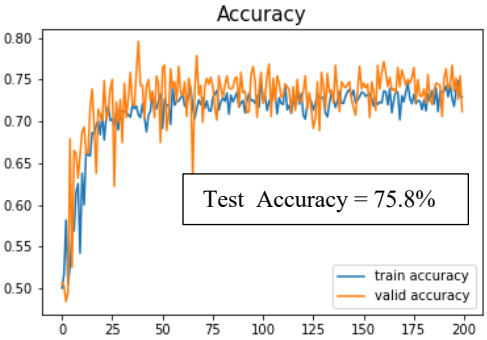
Scenario 1 & distance 9ft



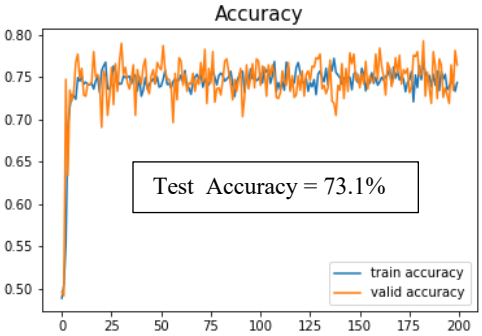
(a) UAV 1



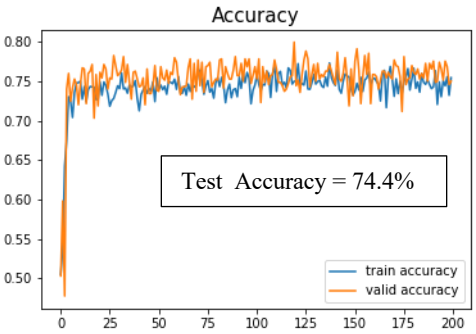
(b) UAV 2



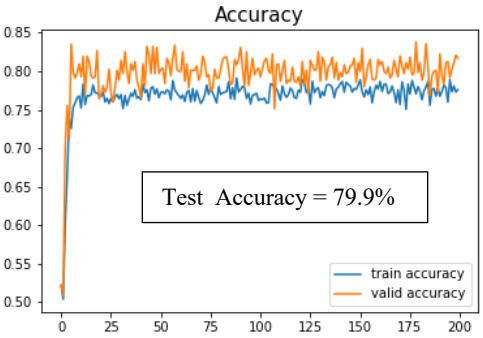
(c) UAV 3



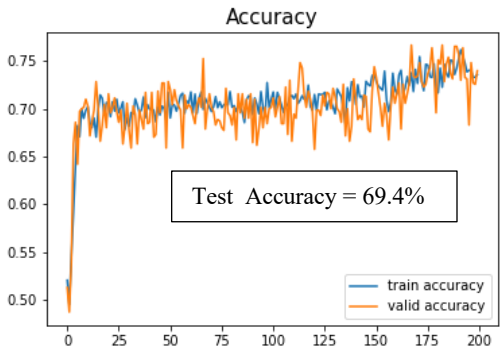
(d) UAV 4



(e) UAV 5



(f) UAV 6

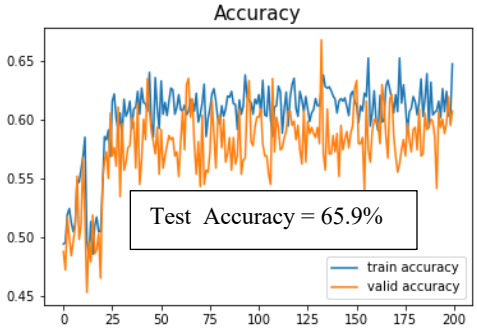


(g) UAV 7

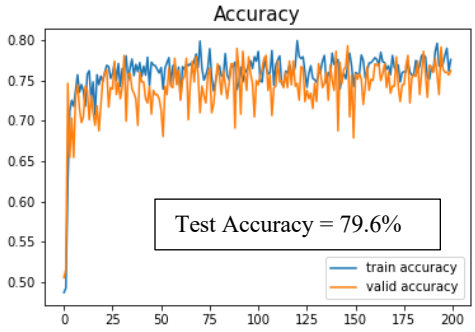
Figure 4. UAV Identification Accuracy for Distance 9 ft and scenario 1.

We can see from Figure 4. that the accuracy remains high for all UAVs when the distance increases from 6ft to 9ft. Again, the reason is high SNR and well shuffled data across training validation and testing.

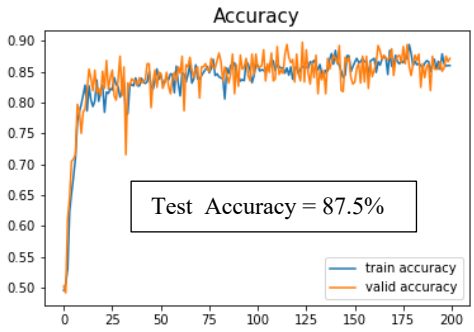
Scenario 1 & distance 12 ft



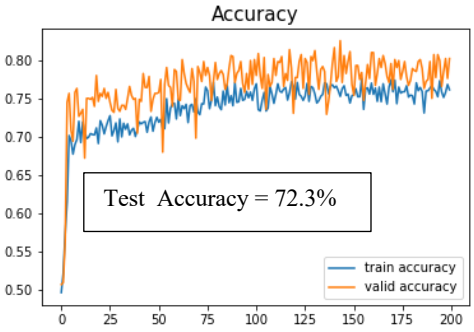
(a) UAV 1



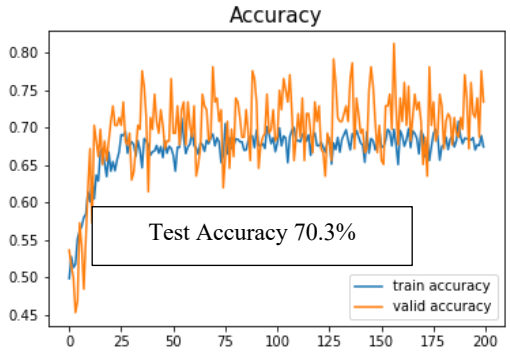
(b) UAV 2



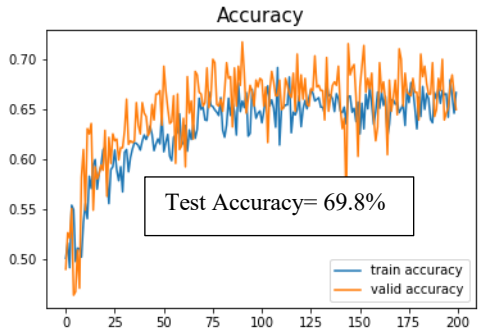
(c) UAV 3



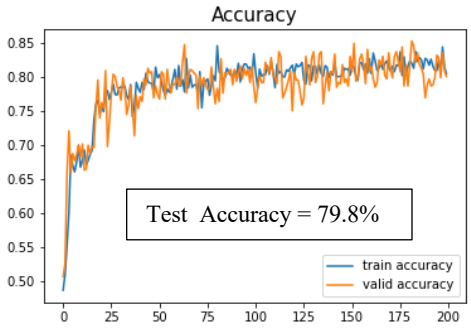
(d) UAV 4



(e) UAV 5



(f) UAV 6

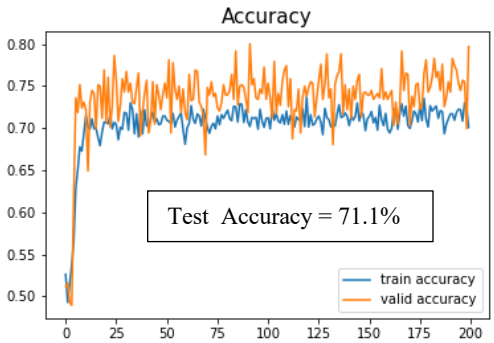


(g) UAV 7

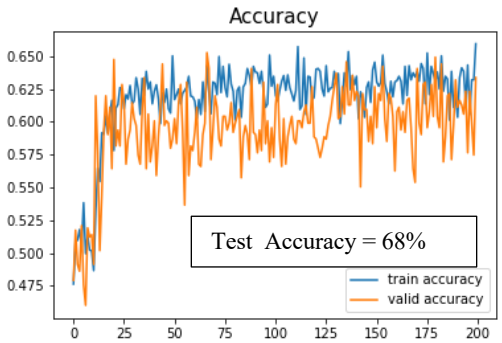
Figure 5. UAV Identification Accuracy for Distance 12 ft and scenario 1.

The results in Figure 5. demonstrates that when the distance between the transmitter and receiver is increased to 12 ft, the accuracy remains high (around 79%, see Figure 5) for most of the UAVs when we train on all bursts.

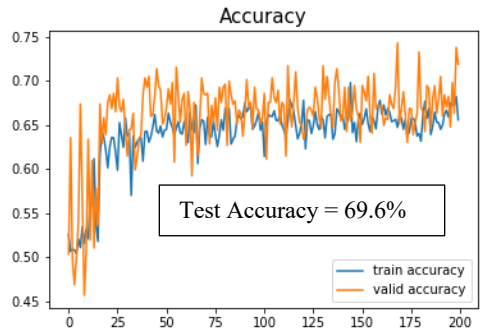
Scenario 1 & distance 15 ft



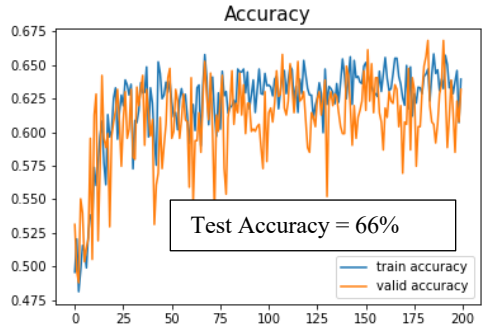
(a) UAV 1



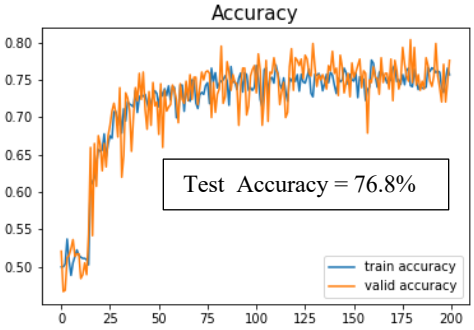
(b) UAV 2



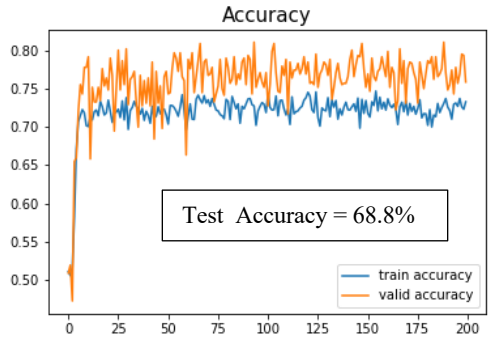
(c) UAV 3



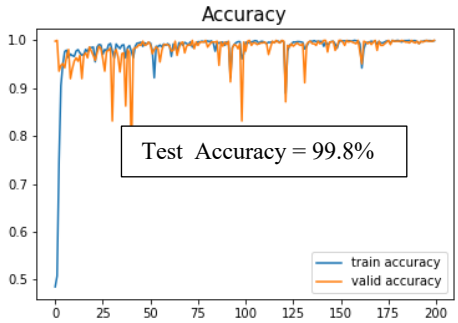
(d) UAV 4



(e) UAV 5



(f) UAV 6



(g) UAV 7

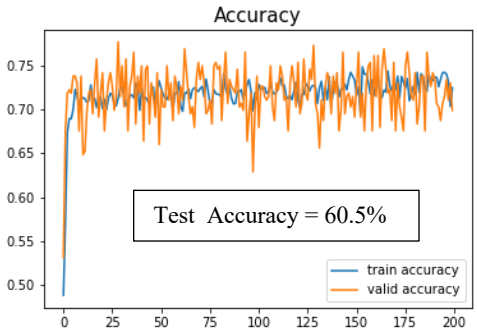
Figure 6. UAV Identification Accuracy for Distance 15 ft and scenario 1.

When the distance was increased to 15ft, as can be seen in Figure 6., the accuracy for UAV UAV7 was quite high as compared to other cases. This happens because there is only 1 example in the dataset for UAV7 at distance 15ft. Because of which, the model overfits on negative examples. The neural network predicts all examples as negative, and it results in high accuracy because nearly all the examples in the test set are negative resulting in high

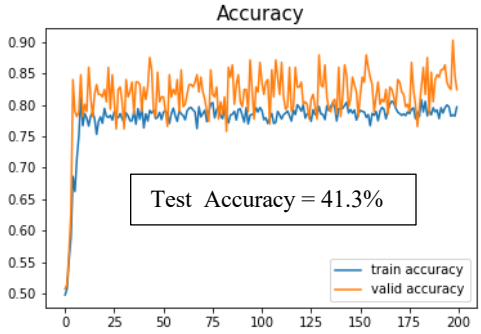
test accuracy. For all different UAV distances, the learning rate of 0.001 was used to allow the model to converge faster.

Results Scenario 2 (3 burst of data was shuffled, then divided into training, validation and 4th burst was used for testing):

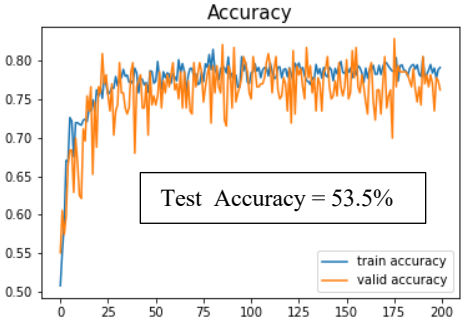
Scenario 2 & distance 6 ft



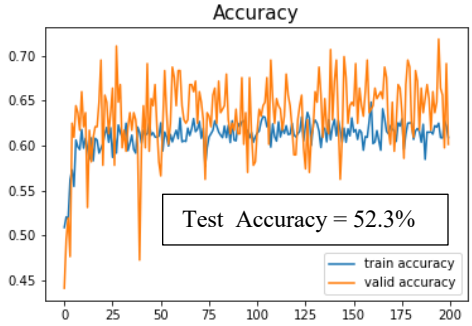
(a) UAV 1



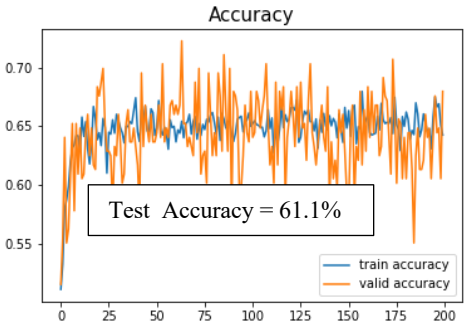
(b) UAV 2

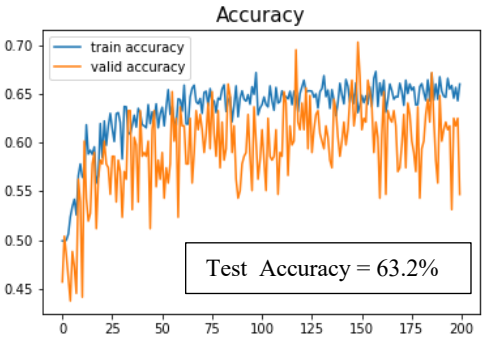


(c) UAV 3

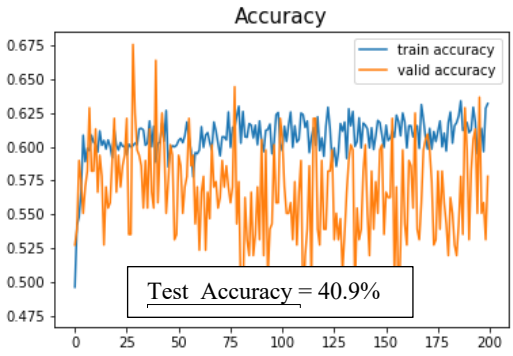


(d) UAV 4





(e) UAV 5 (f) UAV 6

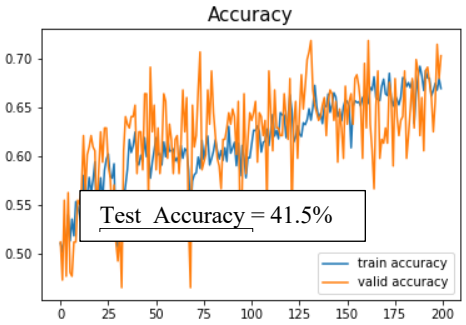


(g) UAV 7

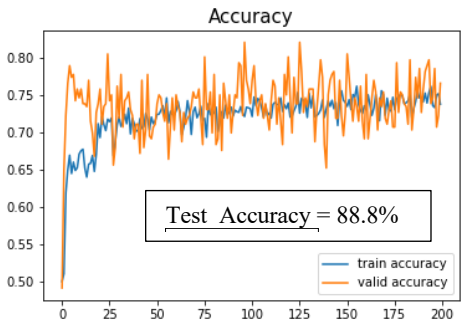
Figure 7. UAV Identification Accuracy for Distance 6 ft and scenario 2.

As the results in Figure 7. demonstrate, for the second scenario and distance 6ft, we trained on 1, 2, 3 burst and tested on new burst 4. This resulted in lower accuracy (around 50% or below) as compared to scenario 1. This difference is since the channel noise during the training and testing are different. The wireless channel is very dynamic and the assumption that the channel data is coherent during the training and testing is invalid.

Scenario 2 & distance 9 ft



(a) UAV 1



(b) UAV 2

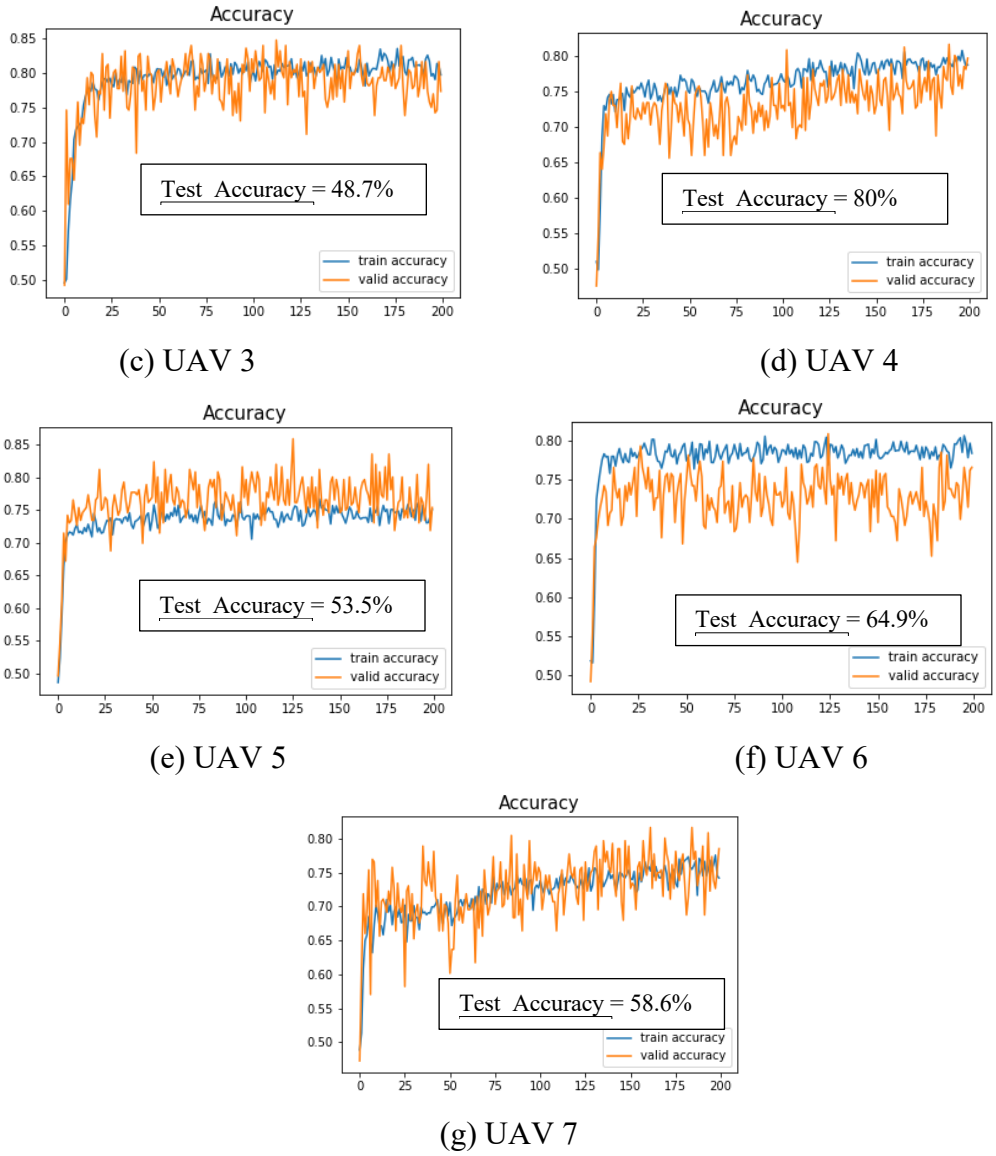
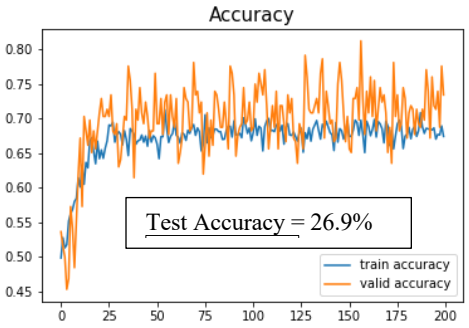


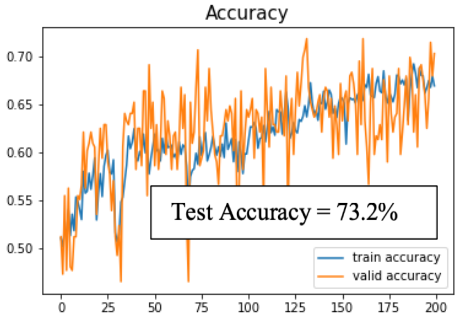
Figure 8. UAV Identification Accuracy for Distance 9 ft and scenario 2.

Like distance of 6 ft, the accuracy for distance of 9 ft for scenario 2 is low as seen in Figure 8. Again, training on 1, 2, 3 burst resulted in accuracy of 50 % for most of the UAVs. The reason being when we test on unseen burst i.e., on new samples the channel will have dramatically changed as compared to samples used for the training of the model.

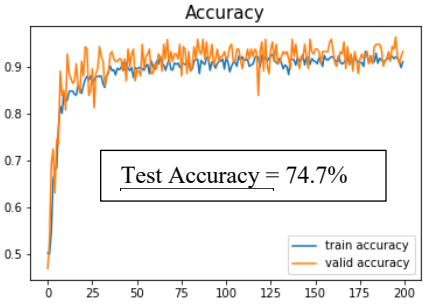
Scenario 2 & distance 12 ft



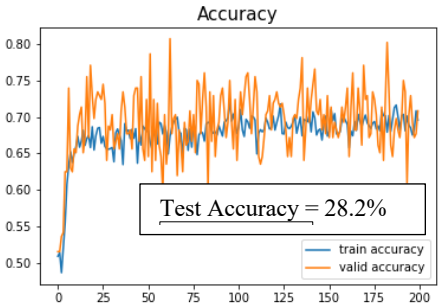
(a) UAV 1



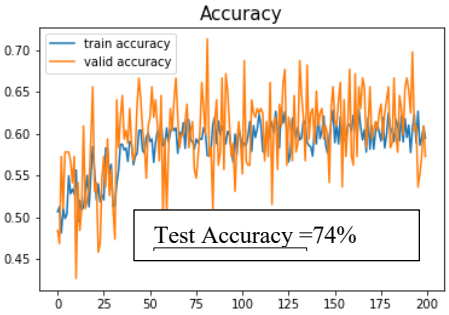
(b) UAV 2



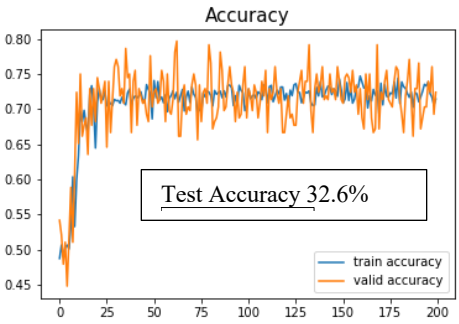
(c) UAV 3



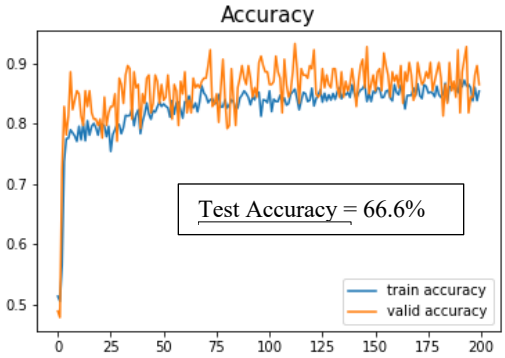
(d) UAV 4



(e) UAV 5



(f) UAV 6

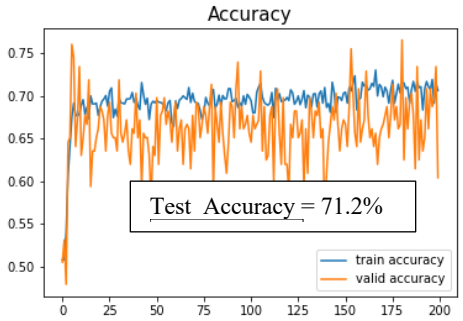


(g) UAV 7

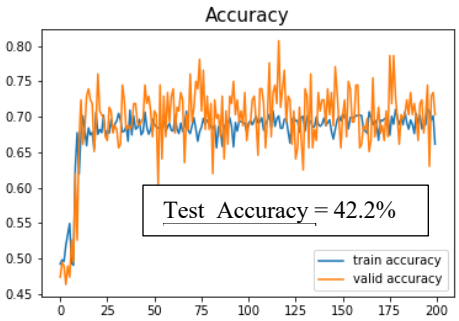
Figure 9. UAV Identification Accuracy for Distance 12 ft and scenario 2.

When the distance was increased to 12 ft, we can see from Figure 9 the accuracy declined. The identification accuracy decreased to around 30% or below for UAV1, UAV4, and UAV7 and was higher about 70% for the other UAVs.

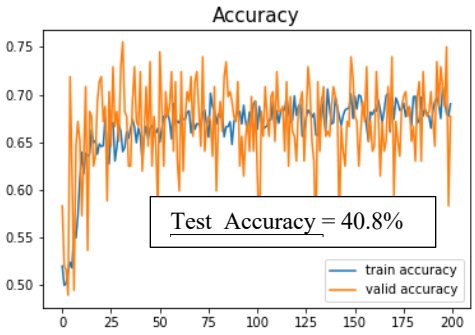
Scenario 2 & distance 15 ft



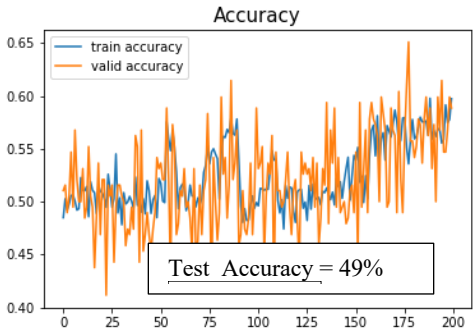
(a) UAV 1



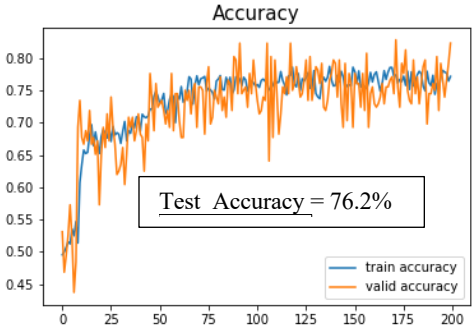
(b) UAV 2



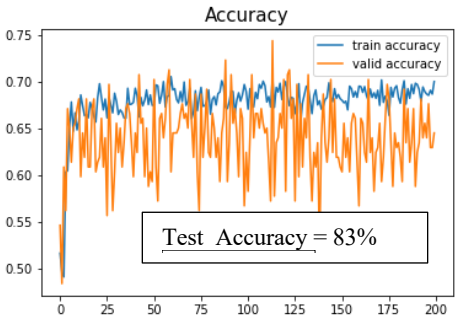
(c) UAV 3



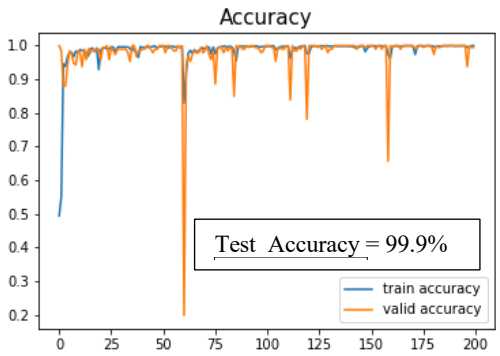
(d) UAV 4



(e) UAV 5



(f) UAV 6



(g) UAV 7

Figure 10. UAV Identification Accuracy for Distance 15 ft and scenario 2.

We see similar results when the distance was increased to 15 feet for scenario 2. As illustrated in the above Figure 10. for distance 15 ft and UAV 7 the accuracy was high about 99.8%. This was surprising and after further investigating, we found that the UAV7 at distance 15 ft had only one example which led to the overfitting on negative examples.

Chapter 5

Conclusion and Future Work

5.1 Conclusion

In this research work, we capture the complex fingerprints of RF communication modules within UAVs using the customized deep learning model AlexNet. These captured fingerprints are then used as a source to classify and identify hovering UAVs. UAVs were classified in a one-vs-all manner as a binary classification problem. We modified AlexNet to process 1d I/Q samples from the UAV transmitter communication module. The fingerprints were extracted for 7 UAVs at distances 6 ft, 9 ft, 12 ft, and 15 ft to capture the strength, variance, and dynamics of multipath and the constant hovering of the UAVs. AlexNet was trained based on 2 scenarios. First, the models were trained and tested on all bursts. Second, the models were trained on bursts 1, 2, 3 and tested on burst 4. Our results showed that the models trained on all bursts maintain average accuracy of above 70% for most UAVs and distances. However, training on 1, 2, 3 bursts and testing on burst 4 resulted in lower accuracy (around 50% or below) as compared to the former case. Moreover, for improve our results we trained models with higher number epochs and various learning rates. On other hand, for not improved results dataset for specific UAV was insufficient to train the model since the unbalanced dataset cause overfitting.

5.2 Future Work

In this work we employed deep learning for drone detection for hovering UAVs. We used AlexNet to extract the hardware noise features. The large accuracy difference between the two training scenarios clearly indicate that the network trained on previously collected dataset performs poorly on the test data set making the extracted fingerprints invalid. The main reason behind is the continuously changing wireless environment and constant hovering of the UAVs. This is a fundamental difficulty and is an open research problem for moving UAVs. We observe following directions for improvements:

- We will employ multi-classifier deep network models to improve the test accuracy on unseen bursts. Data Augmentation technique will be employed to make the model more robust against constantly changing environment.
- Detection of more drones: our current work detected 7 UAVs, however, in practice a swarm of drones will have even larger number of UAVs.
- Large varieties of experiments will be carried out in diverse environment settings and the validity and robustness of the fingerprints will be evaluated.
- Lastly, impact of wind, temperature, hardware weathering and speed of drones and the interference signals on the fingerprint extraction will be researched.

References

[1] "Unmanned Aerial Vehicle. "Wikipedia. Wikimedia Foundation, October 2021. https://en.wikipedia.org/wiki/Unmanned_aerial_vehicle#:~:text=An%20unmanned%20aerial%20vehicle%20(UAV,of%20communications%20with%20the%20UAV.

[2] Namuduri, Kamesh; Chaumette, Serge; Kim, Jae H.; Sterbenz, James P. G., "UAV Networks and Communications || Introduction to UAV Systems," pp. 1–25, 2017.

[3] X. Sun, D. W. K. Ng, Z. Ding, Y. Xu and Z. Zhong, "Physical Layer Security in UAV Systems: Challenges and Opportunities," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 40-47, October 2019.

[4] D. Nußler, A. Shoykhetbrod, S. Gutgemann, A. Kuter, B. Welp, N. Pohl, and C. Krebs, "Detection of unmanned aerial vehicles (UAV) in urban environments," Emerging *Imaging and Sensing Technologies for Security and Defence III. International Society for Optics and Photonics*, vol. 10799, pp. 166 – 176, 2018.

[5] Soltani, N., Reus-Muns, G., Salehi, B., Dy, J., Ioannidis, S., & Chowdhury, K., "RF Fingerprinting Unmanned Aerial Vehicles with Non-Standard Transmitter Waveforms*," IEEE Transactions on Vehicular Technology,* vol. 69, no. 12, pp. 15518–15531, 2020.

[6] Halperin, D. et al. "Two Antennas are Better than One: A Measurement Study of 802. 11 n." (2009).

[7] J. Hua, H. Sun, Z. Shen, Z. Qian and S. Zhong, "Accurate and Efficient Wireless Device Fingerprinting Using Channel State Information," IEEE INFOCOM 2018 - IEEE Conference on Computer Communications, 2018, pp. 1700-1708, doi: 10.1109/INFOCOM.2018.8485917.

[8] L. N. Kandel and S. Yu, "Indoor Localization Using Commodity Wi-Fi APs: Techniques and Challenges," 2019 International Conference on Computing, Networking and Communications (ICNC), 2019, pp. 526-530, doi: 10.1109/ICCNC.2019.8685501.

[9] Z. Wang, Z. Yu, Y. Liu and H. Song, "Abnormal Data Detection of Unmanned Aerial Vehicles Based on Double Shortcuts ZB-ResNet," 2021 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), Xi'an, China, 2021, pp. 1-6.doi: 10.1109/ICSPCC52875.2021.9564996

[10] Y. Liu, J. Wang, J. Li, S. Niu, L. Wu and H. Song, "Zero-bias Deep Learning Enabled Quickest Abnormal Event Detection in IoT," in IEEE Internet of Things Journal.doi: 10.1109/JIOT.2021.3126819.

[11] X. Sun, D. W. K. Ng, Z. Ding, Y. Xu and Z. Zhong, “Physical Layer Security in UAV Systems: Challenges and Opportunities” in IEEE Wireless Communications, vol. 26, no. 5, pp. 40-47, October 2019, doi:10.1109/MWC.001.1900028.

[12] Qingqing Wu, Weidong Mei, & Rui Zhang. (2019). Safeguarding Wireless Network with UAVs: APhysical Layer Security Perspective.

[13] Omri, A., & Hasna, M. O. (2018). Physical Layer Security Analysis of UAV based Communication Networks. 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall). https://doi.org/10.1109/vtcfall.2018.8690950

[14] L. N. Kandel, Z. Zhang and S. Yu, “Exploiting CSI-MIMO for Accurate and Efficient Device Identification”2019 IEEE Global Communications Conference (GLOBECOM), 2019, pp. 1-6, doi:10.1109/GLOBECOM38437.2019.9014191.

[15] Halperin, D., Hu, W., Sheth, A., & Wetherall, D. (2010). A RF Fingerprint Recognition Method Based on Deeply Convolutional Neural Network. ACM SIGCOMM Computer Communication Review, 40(1), 19–25. https://doi.org/10.1145/1672308.1672313.

[16] J. Wang, Y. Liu and H. Song, "Counter-Unmanned Aircraft System(s) (C-UAS): State of the Art, Challenges, and Future Trends," in IEEE Aerospace and Electronic Systems Magazine, vol. 36, no. 3, pp. 4-29, 1 March 2021.doi: 10.1109/MAES.2020.3015537

[17] X. Yue, Y. Liu, J. Wang, H. Song and H. Cao, "Software Defined Radio and Wireless Acoustic Networking for Amateur Drone Surveillance," in IEEE Communications Magazine, vol. 56, no. 4, pp. 90-97, April 2018.doi: 10.1109/MCOM.2018.1700423

[18] P. -Y. Hong, C. -Y. Li, H. -R. Chang, Y. Hsueh and K. Wang, "WBF-PS: WiGig Beam Fingerprinting for UAV Positioning System in GPS-denied Environments," IEEE INFOCOM 2020 - IEEE Conference on Computer Communications, 2020, pp. 1778-1787, doi: 10.1109/INFOCOM41043.2020.9155468.

[19] Alipour-Fanid, M. Dabaghchian, N. Wang, P. Wang, L. Zhao and K. Zeng, "Machine Learning-Based Delay-Aware UAV Detection and Operation Mode Identification Over Encrypted Wi-Fi Traffic," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2346-2360, 2020, doi: 10.1109/TIFS.2019.2959899.

[20] S. Mohanti, N. Soltani, K. Sankhe, D. Jaisinghani, M. Di Felice and K. Chowdhury, "AirID: Injecting a Custom RF Fingerprint for Enhanced UAV Identification using Deep Learning," GLOBECOM 2020 - 2020 IEEE Global Communications Conference, 2020, pp. 1-6, doi: 10.1109/GLOBECOM42002.2020.9322561.

[21] M. Ezuma, F. Erden, C. K. Anjinappa, O. Ozdemir and I. Guvenc, "Micro-UAV Detection and Classification from RF Fingerprints Using Machine Learning Techniques," 2019 IEEE Aerospace Conference, 2019, pp. 1-13, doi: 10.1109/AERO.2019.8741970.

[22] M. Ezuma, F. Erden, C. Kumar Anjinappa, O. Ozdemir and I. Guvenc, "Detection and Classification of UAVs Using RF Fingerprints in the Presence of Wi-Fi and Bluetooth Interference," in IEEE Open Journal of the Communications Society, vol. 1, pp. 60-76, 2020, doi: 10.1109/OJCOMS.2019.2955889.

[23] Bisio, C. Garibotto, F. Lavagetto, A. Sciarrone and S. Zappatore, "Unauthorized Amateur UAV Detection Based on WiFi Statistical Fingerprint Analysis," in IEEE Communications Magazine, vol. 56, no. 4, pp. 106-111, April 2018, doi: 10.1109/MCOM.2018.1700340.

[24] Nemer I, Sheltami T, Ahmad I, Yasar AU-H, Abdeen MAR. RF-Based UAV Detection and Identification Using Hierarchical Learning Approach. *Sensors*. 2021; 21(6):1947. https://doi.org/10.3390/s21061947

[25] J. Tan and H. Zhao, "UAV Localization with Multipath Fingerprints and Machine Learning in Urban NLOS Scenario," 2020 IEEE 6th International Conference on Computer and Communications (ICCC), 2020, pp. 1494-1499, doi: 10.1109/ICCC51575.2020.9345143.

[26] C. Xu, F. He, B. Chen, Y. Jiang and H. Song, "Adaptive RF Fingerprint Decomposition in Micro UAV Detection based on Machine Learning," ICASSP 2021 - 2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)

[27] C. Xu, B. Chen, Y. Liu, F. He and H. Song, "RF Fingerprint Measurement For Detecting Multiple Amateur Drones Based on STFT and Feature Reduction," 2020 Integrated Communications Navigation and Surveillance Conference (ICNS), Herndon, VA, USA, 2020, pp. 4G1-1-4G1-7.

[28] Y. Liu, J. Wang, J. Li, S. Niu and H. Song, "Machine Learning for the Detection and Identification of Internet of Things (IoT) Devices: A Survey," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2021.3099028.

[29] Houbing Song, Yongxin Liu, Jian Wang, "UAS Detection and Negation," US Patent US 2021/0197967 A1, Jul. 1, 2021. Available: https://patents.google.com/patent/US20210197967A1/.

[30] Houbing Song, Yongxin Liu, Jian Wang, "UAS Detection and Negation," WO Patent WO2020236328A2, Nov. 26, 2020. Available: https://patents.google.com/patent/WO2020236328A2.

[31] Y. Liu, J. Wang, J. Li, S. Niu and H. Song, "Class-Incremental Learning for Wireless Device Identification in IoT," in IEEE Internet of Things Journal.

[32] L. N. Kandel and S. Yu, "VWAN: Virtual WiFi ANtennas for Increased Indoor Localization Accuracy," 2019 IEEE International Conference on Industrial Internet (ICII), 2019, pp. 258-267, doi: 10.1109/ICII.2019.00052.

[33] L. N. Kandel, Z. Zhang and S. Yu, "Poster: Using Commodity WiFi Devices For Object Sensing And Imaging," 2019 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), 2019, pp. 1-2, doi: 10.1109/DySPAN.2019.8935637.

[34] "Hovering Uavs RF Fingerprinting Datasets." *GENESYS*, https://genesys-lab.org/hovering-uavs.

[35] N. Soltani, G. Reus-Muns, B. Salehi, J. Dy, S. Ioannidis and K. Chowdhury, "RF Fingerprinting Unmanned Aerial Vehicles With Non-Standard Transmitter Waveforms," in *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 15518-15531, Dec. 2020, doi: 10.1109/TVT.2020.3042128.