4-2019

Uncover the Power of Multipath : Detecting NLOS Drones Using Low-Cost WiFi Devices

Ashok Vardhan Raja

Follow this and additional works at: https://commons.erau.edu/edt

Part of the Aerospace Engineering Commons

Scholarly Commons Citation
Raja, Ashok Vardhan, "Uncover the Power of Multipath : Detecting NLOS Drones Using Low-Cost WiFi Devices" (2019).
Dissertations and Theses. 441.
https://commons.erau.edu/edt/441

This Thesis - Open Access is brought to you for free and open access by Scholarly Commons. It has been accepted for inclusion in Dissertations and Theses by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu, wolfe309@erau.edu.
UNCOVER THE POWER OF MULTIPATH: DETECTING NLOS DRONES USING LOW-COST WiFi DEVICES

by
Ashok Vardhan Raja

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, Computer, Software, and Systems Engineering
Embry-Riddle Aeronautical University
Daytona Beach, Florida
April 2019
UNCOVER THE POWER OF MULTIPATH: DETECTING NLOS DRONES USING LOW-COST WIFI DEVICES

by Ashok Vardhan Raja

This thesis was prepared under the direction of the candidate’s Thesis Committee Chair, Dr. Jiawei Yuan, and has been approved by the members of the thesis committee. It was submitted to the Department of Electrical, Computer, Software, and Systems Engineering in partial fulfillment of the requirements for the degree of Master of Science in Cybersecurity Engineering.

Jiawei Yuan, Ph.D.
Committee Chair

Remzi Seker, Ph.D.
Committee Member

Radu F. Babiceanu, Ph.D.
Committee Member

Timothy A. Wilson, Sc.D.
Chair, Electrical, Computer, Software, and Systems Engineering

Maj Mirmirani, Ph.D.
Dean, College of Engineering

Lon Moeller, J.D
Senior Vice President for Academic Affairs and Provost

4/22/19 Date
Acknowledgements

I would like to thank my thesis advisor Dr. Yuan and my committee members Dr. Seker and Dr. Babiceanu of the Department of Electrical, Computer, Software and Systems Engineering for supporting me. Dr. Yuan, is the best advisor I could have asked for. He was always available whenever I had any questions. He made sure my thesis was going in a positive direction. I thank God for making me choose him as my advisor. Secondly, I would like to thank my family for helping me achieve my dreams. I would also like to thank Mr. Yifan Tian for being my mentor while working on my thesis research. And finally, I would like to thank my friends at Embry-Riddle for all the support they have provided me.
Abstract

In recent years, consumer UAV technology has seen considerable advances. Consumer UAVs have become an ideal vector for privacy invasions due to their affordability, size, maneuverability, and their ability to stream live high-quality video. There is considerable proliferation of drones in both civil and military domains. Hence it is critical to detect invading unmanned aerial vehicles (UAVs) or drones in a timely manner for both security and safeguarding privacy. Currently available solutions like active radar, video or acoustic sensors are very expensive (especially for individuals) and have considerable constraints (e.g., requiring visual line of sight).

Recent research on drone detection with passive RF signals provides an opportunity for low-cost deployment of drone detectors on commodity wireless devices. The state of the arts in this direction mainly focus on detecting drones using line-of-sight (LOS) RF signals which are less noisy as compared to their non-LOS (NLOS) counterparts. To the best of our knowledge, there is no existing cost-effective solution for the general public to enable non-LOS (NLOS) detection for drone privacy invasion, which is the most common condition and it still remains an open challenge.

This thesis research provides a low-cost UAV detection system for privacy invasion caused by customer drone. Our model supports NLOS detection with low-cost hardware under $50, and hence it is affordable for the general public to deploy in their house, apartments, and office. Our work utilizes inherent drone motions (i.e., body shifting and vibrations) as unique signatures for drone detection. Firstly, we validated the relationship between drone motions and RF signal under the NLOS condition using extensive experiments. This is motivated by the fact that under NLOS conditions slight changes to the position or motion of a drone could lead to dramatic change in multi-path components in received RF signals. The NLOS condition “amplifies” the RF signatures introduced by drone motions.

We designed a deep learning model to capture the complex features from NLOS RF signals. In particular, we designed and trained a long short-term memory (LSTM) neural network [15, 27], a generative model which can effectively extract features of inputs for NLOS drone detection. Moreover, without knowing the presence of drones, our system starts with classifying any detected RF signals into LOS signals and NLOS signals before the NLOS drone learner is used. Classification of LOS and NLOS sig-
signals is feasible because they exhibit different combined features such as strength, variance, and distribution due to their differences in multipath effects. We used the supervised support vector machine (S-SVM) [17] as the learning model, which is effective for binary classification.

This design is validated via extensive experiments using commodity drones in residential areas with other Wi-Fi enabled mobile devices.

Index Terms—Drone, UAV, Deep Learning, RF Signal, Line of-Sight
# Contents

Acknowledgements i  
Abstract iii  
Table of Contents v  
List of Figures vi  
List of Tables vii  
List of Abbreviations viii  
1 Introduction 1  
2 Literature Review 3  
  2.1 Radar Detection ................................................................. 3  
  2.2 Video-Based and Audio-Based Drone Detection .............................. 4  
  2.3 Detecting using Thermal Imaging .............................................. 4  
  2.4 Detecting using Acoustic Cameras ............................................ 5  
  2.5 RF Based Detection .............................................................. 5  
3 System Model 7  
4 Design Methodology 8  
  4.1 Drone Unique Flying Patterns .................................................. 8  
  4.2 Proof of Drone Motion changing RSS values .................................. 9  
  4.3 LOS and NLOS Differentiation .................................................. 11  
  4.4 NLOS-Based Drone Detection .................................................. 13  
  4.5 LOS Based Detection ............................................................. 16  
5 Experiments 18  
  5.1 Experiment Setup ................................................................. 18  
  5.2 Evaluation .............................................................................. 20  
    5.2.1 Setting the batch size and vector size ................................... 20  
    5.2.2 Same house training and testing scenario ............................... 21
5.2.3 Transfer trained scenarios ............................ 21
  5.2.3.1 Case A - Person A training vs Person B testing ... 22
  5.2.3.2 Case B - Person C training vs Person B testing ... 22
  5.2.3.3 Case C - Person A and Person C training vs Person
       B testing ........................................... 23
  5.2.4 Advantages of using multiple house for training ....... 23

6 Conclusions and Future Research ........................ 25
  6.1 Conclusions ............................................ 25
  6.2 Future Research ........................................ 26

Bibliography .............................................. 26
List of Figures

3.1 Representation of our setup .................................................. 7
4.1 NLOS Condition PI Placed Indoors – Drone Motion and RSS Relation 10
4.2 NLOS Condition PI Placed Indoors – Drone Motion and RSS Relation 11
4.3 Flowchart of our system ......................................................... 12
4.4 LOS vs NLOS classification using S-SVM ................................. 13
4.6 Implementation of LSTM(Long Short-Term Memory) [15] .............. 15
4.7 Flowchart for NLOS Based Drone Detection and Classification ...... 16
5.1 The bird view of the residential area ....................................... 18
5.2 Flying patterns of the drone ..................................................... 19
List of Tables

5.1 Training time during Batch Size 64 and Vector Size 64. . . . . . . . . 20
5.2 Training time during Batch Size 128 and Vector Size 126. . . . . . . . 20
5.3 Training time during Batch Size 256 and Vector Size 256. . . . . . . . 20
5.4 Same House Training and Testing Scenario. . . . . . . . . . . . . . . 21
5.5 Different House Training and Testing Scenario . . . . . . . . . . . . . 22
5.6 Different House Training and Testing Scenario . . . . . . . . . . . . . 22
5.7 Different Combined House Training and Testing Scenario. . . . . . . . 23
## List of Abbreviations

<table>
<thead>
<tr>
<th>C</th>
<th>CNN: Convolutional Neural Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>FAA: Federal Aviation Administration</td>
</tr>
<tr>
<td></td>
<td>FPV: First Person View</td>
</tr>
<tr>
<td>G</td>
<td>GWS: Ground Wireless Sensors</td>
</tr>
<tr>
<td>L</td>
<td>LOS: Line of Sight</td>
</tr>
<tr>
<td></td>
<td>LSTM: Long Short-Term Memory</td>
</tr>
<tr>
<td>N</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NLOS: Non-Line of Sight</td>
</tr>
<tr>
<td>R</td>
<td>RF: Radio Frequency</td>
</tr>
<tr>
<td></td>
<td>RNN: Recurrent Neural Network</td>
</tr>
<tr>
<td></td>
<td>RSS: Radio Signal Strength</td>
</tr>
<tr>
<td>S</td>
<td>S-SVM: Supervised Support Vector Machines</td>
</tr>
<tr>
<td>U</td>
<td>UAV: Unmanned Aerial Vehicle</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

Over the last couple of years, the commercial and military sector in the United States and globally has seen an astounding increase in Unmanned Aerial Vehicles (UAVs). This includes drones, and drone platforms. This in turn has increased the interest in drone detection technologies. [1, 37]. The recent report from the United States Federal Aviation Administration (FAA) tells us that it is almost becoming difficult to count the number of drones and its application in the marketplace especially in small UAVs sector [1]. By 2020 it is estimated that there would be at least 3.17 million UAVs [23]. This proliferation of UAVs brings advantages and disadvantages associated with it. The advantages are that the increase in number of UAVs will add more competition to the marketplace which will make it more affordable for general public. Not to forget the wide range of applicability in various commercial sectors including agriculture, medical industry, accident reporting, detecting natural disaster, etc. UAVs are becoming something more than a tool that assists human efforts and efficiencies in many ways.

The biggest threat UAVs possess is that it can be easily misused by people for all the wrong reasons which can negate the benefits it brings in (or) an accidental crash into a neighbors compound while flying a drone (Note, when we say by accident, it means not on purpose) can cause privacy issues if the drone has video camera and it was recording its flight [32]. In 2015, we witnessed a hobbyist crash a two feet drone on the White House grounds which raised questions about the president’s security [43]. Another incident of misuse was when we saw one of the busiest airports in London being shut down for nearly 36 hours when they detected unauthorized drone use [6]. Data and data processing is an integral part of drone and drone development applications. These data include but not limited to personal identifiable information, military data, personal health information, etc. Ultimately these data if misused could be detrimental to individual’s privacy, nation’s security and the smooth functioning of commercial sector.

Detection is the key to develop good preemptive measures [18, 19, 20, 44, 46]. This will lead the development of drone technologies in the right direction and monitor the
A variety of UAV detection approaches have been proposed for military and commercial security systems. One of the approaches that have been proposed in the commercial and military sector is detecting UAVs using Active Radar technique. This technique is used to detect wide range of regular aircrafts and large UAVs, but they are incompetent in detecting small LOS and NLOS which may radiate similar radioactive signals such as birds. Also, this technique are very complex and expensive almost making it unaffordable for general public who use small UAVs.

Other approaches include Acoustic Sensors, video-based solution and passive RF signal-based drone detection. The problem with Acoustic Sensors and Video Based Solutions is that they are limited by distance and visual line of sight. Sometimes these approaches are even constrained by weather conditions making it ineffective. Bimbach et al in his recent studies have proposed a motion introduced RF signals detection system to which relies highly on analyzing flying patterns using statistical features of passive RF signal (i.e. RSS). The issue with passive RF based detection systems is that they take advantage of RSS variations and assume existences of LOS. In this paper we argue the contrary i.e. Bimbach’s approach are not always helpful for drone detection in NLOS cases.

Introduced in this thesis, is a low-cost UAV detection system for privacy invasion caused by customer drone. Our model supports NLOS detection with low-cost hardware under $50, and hence it is affordable for the general public to deploy in their house, apartments, and office. To be specific, we first explored and validated the relationship between drone motions (i.e., shifting, vibration, acceleration, position changing) and RF signal under the NLOS condition using extensive experiments. This is motivated by the fact that under NLOS conditions slight changes to the position or motion of a drone could lead to dramatic change in multi-path components in received RF signals. By this, the NLOS condition “amplifies” the RF signatures introduced by drone motions. We then designed a deep learning model to capture the complex features from NLOS RF signals. In particular, we designed and trained a long short-term memory (LSTM) neural network [15, 27], a generative model which can effectively extract features of inputs for NLOS drone detection. Moreover, without knowing the presence of drones, our system starts with classifying any detected RF signals into LOS signals and NLOS signals before the NLOS drone learner is used. Classification of LOS and NLOS signals is feasible because they exhibit different combined features such as strength, variance, and distribution due to their differences in multipath effects. We used the supervised support vector machine (S-SVM) [17] as the learning model, which is effective for binary classification.

We validated our design via extensive experiments using commodity drones in residential areas with other mobile devices including GoPro camera and smartphones presented. We use Raspberry PI 3 Model B with a commodity USB WiFi module Edimax N150 as the wireless drone detector.
Chapter 2

Literature Review

A collection of contemporary literature was studied to understand the current developments in the field of UAV detection. The following sections summarize the relevant information researched and gives an up-to-date perception of work done in UAV detection. UAVs have become very popular [31, 33]. In the recent past considerable regulations in flight control have been put in place. But, despite these flight control regulations, the popularity of Unmanned Aerial Vehicles (UAVs) have grown astronomically [33]. UAVs are increasingly being used for civilian applications, military applications, and for personal use [33]. This rapid increase has introduced a serious threat to privacy of the individual, public security, and military security [33]. Hence there is an urgent need to detect drones in a reliable and faster manner [31].

Detecting drones has become a staple of military and aircraft control for a long time. According to the underlying sensing modalities, existing drone detection systems can be classified into four major categories - Radar, Passive Radio Frequency (RF), Audio and Video based approaches. Radar systems use active detection strategy that transmits radio waves first, and then determines the presence and location of objects by analyzing their reflections. Traditional radar systems have been demonstrated for effective aircraft detection; however, the miniaturized size of drones makes them extremely difficult to detect because of their small reflection areas. The drone invasion at the White House in 2015 is an example of incompetence of radar systems in face of small drones [43]. While recent efforts on radar systems have shown their improved accuracy in detecting drones [3, 21, 45], the high costs (tens of thousands of dollars) prevent them from pervasive deployment by the general public. On the other hand, drones are also increasingly using radar vision for detecting and avoiding obstacles [21].

2.1 Radar Detection

Radar technology is being improvised to improve its scanning range. Phased-array radars can emit radio waves in predetermined patterns, and in predetermined direc-
tion. By using phased-array radars we can scan the entire field of view [21]. There is a growing interest in using a distributed FMCW Radar system, which works on fiber-optic links for detecting small drones [45]. This k-band radar systems have very high sensitivity, linearity and flatness. They can detect low-radar cross section targets much easily. They can also measure the range and velocity of these targets [45]. Similarly, non-coherent radars are also increasingly being used for detection of low observable objects [3].

2.2 Video-Based and Audio-Based Drone Detection

Video-based drone detection also becomes increasingly popular with the recent advances in computer vision [12, 31, 33, 42]. These approaches apply machine learning on surveillance camera data to extract the appearance and motion cues of drones. Challenges to this approach exist mainly on its reliance on environment conditions (e.g., high line-of-sight visibility). How to distinguish between small drones and other flying objects at distance [9] also remains an open challenge. Alternative types of cameras such as thermal and near-infrared cameras are also considered to mitigate the constraints of conventional surveillance cameras under low-or zero-light conditions [30, 47]. However, these devices are also limited to line-of-sight regions, let alone their high costs. Lian Du et al had studied the small UAV detection in videos from a single moving camera [31]. They had used motion estimation methods, low-rank based model, and CNN-SVM approach. J Li had studied a new approach to detect drones from a single camera mounted on a different UAV [33]. Similarly, A Rozantstev had studied the detection of drones using single moving camera [42].

Audio-based drone detection techniques [11, 13, 16] employ acoustic sensors to collect suspicious audio data from drones. These collected audio data are compared with drone acoustic signatures stored in a pre-established database. The accuracy of audio-based detection is greatly affected by the background noise of the environment, such as city traffic in the urban areas and other noises at nearby frequencies. In addition, these techniques are also of high cost and not suitable for pervasive deployment.

2.3 Detecting using Thermal Imaging

There are other innovative methods that are being studied for the rapid detection of drones. Sanjay K Boddhu, and Matt McCartney had studied a collaborative smartphone sensing platform for the smart detection of hostile drones [9]. Infrared systems [47] have increased the capability to detect drones many fold. Thermal imaging sensors have made it possible to detect drones day and night, detect unlimited number of target. They can ensure detection over long-range, and wide area surrounding [47]. Similarly, Vumii’s family of long range surveillance cameras combine advanced
video channels, thermal camera systems, continuous zoom optics and high resolution
 imagers to detect and track hostile threats at a distance of more than 20 Km [30].

2.4 Detecting using Acoustic Cameras

Several researchers are studying the application of Acoustic cameras in drone detections [11, 13]. Case, Zelnio and Rigling studied the utility of Low-cost acoustic array for the detection and tracking of UAVs [13]. Jol Busset and Florian Perrodin studied detection of drones using advanced acoustic cameras [11]. Commercially available models have successfully employed acoustic cameras for drone detections [16]. For example, Drone Shield Base Processor system collects audio data and compares it with the acoustic signatures that are preloaded in the systems database [16]. Despite, the above limitations, there is burgeoning efforts and products in the commercial market place. Currently they rely heavily on acoustic sensors and Infra-Red techniques [4, 16, 30, 47]. For example, Antidrone [4] uses DroneShield user interfaces in their drone detections systems, which assures high accuracy of UAV acoustic detection. It uses both audio and visual interface to provide necessary system data and alerts. To increase the user comfort the interface can be accessed from both web browsers and mobile device portals [4].

2.5 RF Based Detection

The above mentioned detection system is really expensive and cannot be afforded by common people. Currently there is considerable interest in passive RF-based drone detection techniques. The passive RF-based technique detects drones by analyzing various RF characteristics [8, 38, 39]. Nguyen et al had studied the detection of drones by utilizing the packet frequency of detected RF signals [38, 39]. This technique has an inherent drawback as the RF signals could be polluted by similar frequency outputs in the busy urban environment. For example, VOIP traffic can interfere and can lead to false alarms in this method. Birnbach had worked on a protocol to use the received signal strengths (RSS) to create a pattern from the drone invasion events [8]. Drones can then be detected by matching the newly detected RF signals to match this pattern [8]. The biggest handicap for Birnbach’s method is that it can only detect drones flying towards the detection system. Also, the RSS measurement can only work better in the line-of-sight (LOS) condition. As we are aware, LOS conditions are difficult to achieve in all circumstances in the urban environment [8]. Other authors are working on software-defined radio (SDR) to distinguish drone signals from other mobile wireless sources [24]. The SDR devices are currently available off-the-shelf, and the detection system can be easily set up. Unfortunately, they are expensive and can cost hundreds to thousands of dollars. Hence, they are not suitable for mass deployment by the general public [24]. Currently most of the state-of-art RF based approaches work best only in the LOS conditions. There is still considerable chal-
challenge in establishing RF based drone detection systems which can be successful in non-line-of-sight (NLOS) conditions.

There is an increased interest in leveraging Machine learning and Deep learning techniques in the field of drone detection [7, 12, 26, 35, 41, 49]. In Machine learning techniques, the problem of Drone detection is resolved into a simple equation of finding a small rectangle that encloses the drone in a video sequence [12]. Aker and Kalkan had studied a model in which they used an end-to-end object detection model based on convolutional neural networks [12]. They developed an algorithm by combining back ground subtracted real images to for creating an extensive artificial data set for training the network [8]. Several machine learning algorithms and platforms are being integrated into drone detection research [35, 49]. Supervised machine learning algorithms are also becoming increasingly popular. For example, K-nearest neighbors (KNN) algorithm is an innovative emerging option [41]. KNN is easy to implement and can perform complex classification tasks. KNN is a non-parametric learning system and does not have any assumptions about the underlying data [41]. This is especially useful in problems like signal data from drones as they do not follow uniform distribution or linear separability [41]. Similarly, data augmentation techniques [40] are also useful in improving machine learning models. In this technique data points, especially images, are increased in the data set. This leads to increasing number of rows and objects augmenting the machine learning process [40]. These sophisticated machine learning techniques have the exciting possibilities in drone detection systems.

Furthermore, recently, Recurrent Neural networks (RNN) and Long short-term memory networks (LSTMs) have revolutionized the machine learning algorithms [15]. Recurrent neural networks with loops allow the information to persist and allows the machine to think like humans. The don’t have to think from the scratch each time [15]. LSTMs are special kind of RNN networks which can overcome long term dependency problem and remember long term. Both RNN and LSTMs in turn have exciting possibilities for the drone detection systems.
Chapter 3

System Model

This thesis aims at real-time drone detection using NLOS RF signals. We will be using one or more ground wireless sensors (GWS) to collect RF signals to detect the presence of invading drones. We have used low-cost devices such as Raspberry Pi which will have GWS sensors, making it affordable for easy deployment. To support this structure the system will need constant wireless communications with the ground control station or console via omnidirectional antennas for wireless communication frequencies. GWS sensors in these devices are used to measure received wireless signal strength (RSS) of trespassing drones based on wireless communication frequencies. This was the same assumption that was used in RF-based drone detection proposal. However, there is a computability issues between invading drone and GWS sensors. Therefore, the accuracy of GWS sensors using wireless channels will not be useful for drone detection especially when the circumstances of invasion are random and unpredictable. This is the case most of the time. Therefore, the GWS do not always have LOS wireless links to the drone as shown in Fig. 1.

Figure 3.1: Representation of our setup

We propose that by placing at least one GWS sensor it will be easy to determine the existence of NLOS links. When the drones are proximately close the RSS signals are significantly stronger than the noise threshold. Otherwise, RF signals are not useful for drone detection.
Chapter 4

Design Methodology

We plan to have 2 Raspberry Pi devices, to monitor for UAV invasion. One device
will be in LOS with the UAV and the other device will be in NLOS with the UAV. We
will capture the signal strength to further analyze if the signals are from a drone or
some other devices. We then require a consumer UAV to successfully finish research.

4.1 Drone Unique Flying Patterns

Existing research shows us that the motion of drones follows their own aerodynamic
principles through their flying control mechanism. Take quad-motor drones - one of
the most popular drone models – for example, the motion of drones is controlled by
adjusting rotation of the four propellers [10, 28, 50]. In order to achieve equilibrium
while flying the four factors comes into play

- Forces
- Directions
- Moments
- Rotation speed

An appropriate combination is required to maintain the drone in motion which is
achieved by drone’s flying control system [5, 10, 25, 34, 36]. A drone may be in
equilibrium in its unique way due to the following reasons:

- Controller’s reaction to non-deterministic factors such as environmental changes
  (e.g., wind), errors within the drone’s control loops and vibrations caused by
  propellers
- Flying control algorithms used by the drone given a rich body of available
  control algorithms
• The input from human controllers in case of drones controlled by people (which is popular for amateur drones)

This tells us, drone flights would exhibit unique patterns due to drone body shifting, propeller and motor vibration, drone control system [22] and finally the user who is controlling the drone. Drone body shifting occurs when drone tries to balance its body under due to gust of winds during its flight [14, 48]. It usually takes several iterations for a drone’s control system to converge to a balance state. Such a converging process is unique to individual drones due to its unique physical and mechanical features [29]. A sequence of such body shiftings [51] happen when drone changes its flight status (e.g., speed, direction) or fights against environmental changes (e.g., winds) and can serve as the unique signature for the drone’s movement. In addition to body shiftings, vibration of drone motor and propellers can cause slight movements of drone body as studied in. Such vibration (in terms of frequency and magnitude) is highly correlated with the drone’s mechanical properties, and hence produces another unique signature of drone motion. Also, the interaction between a drone’s control system and human inputs may cause unique patterns of drone motions.

For example, a human controller may create “jitters” off drone movements due to imperfect estimation of drone’s state (e.g., its speed and acceleration) and some of the human controller is not experienced in flying drones. So, they experiment with various controller buttons to create equilibrium in order for the drone to fly. These “jitters” in turn may cause additional drone body shiftings (due to body adjustment) and vibration (due to accelerations). The drone’s motion patterns can affect the RF signals received at receivers. In particular, slight spatial location change of drone (i.e., its RF transmitter) would result in significant shift in phase of received RF signals. However, for non-cooperative drones such phase shifts cannot be measured because of unknown transmitting signals. In this case, we observe received signal strength (RSS) which is also closely related to the relative distance between the RF transmitter and the receiver. Different from phase information, the RSS measurement is the strength of the superposition of RF signals and noise, and is less sensitive to slight motions. This is particularly true in free space or LOS situations in which RF path loss is proportional to the logarithm of the distance between the transmitter and the receiver. In NLOS situations, the slight changes of transmitter locations may result in more severe change in RSS at receivers. This is because slight changes in transmitter location may result in different multi-paths of RF propagation. This provides an opportunity for UAV detection under NLOS scenarios.

### 4.2 Proof of Drone Motion changing RSS values

In this section we want to prove our hypothesis - The wireless signal transmitted out by drones will be affected by their motions and these changes are measurable. In other words, drone motion or vibration causes the change in RSS values. When we
place the raspberry Pi indoors we have two cases.

- Pi is in NLOS with the drone
- Pi is in LOS with the drone

We first validated our hypothesis for NLOS condition. In Figure 4.1, we take a start of the peak and an end of the peak to create a zone and observe the results in that time period. We notice that a sudden change in drone’s motion or when you cause a sudden vibration we can see the change in RSS measurements. We take another peak and create a zone and observe the relation between drone motion and the RSS values in that time period.

Next, we validated our hypothesis in LOS condition. When the drone is in LOS with the Pi, we take a start of the peak and an end of the peak to create a zone and

![Figure 4.1: NLOS Condition PI Placed Indoors – Drone Motion and RSS Relation](image)

CHAPTER 4. DESIGN METHODOLOGY 10
and observe the results in that time period as shown in Figure 4.2. We notice that a sudden change in drone’s motion or when you cause a sudden vibration we can see the change in RSS measurements. Hence we are able to prove that the drone motion or vibration is directly proportional to the change in RSS values.

![Drone Vibration](image)

**Figure 4.2: NLOS Condition PI Placed Indoors – Drone Motion and RSS Relation**

### 4.3 LOS and NLOS Differentiation

When the transmitter and the receiver are at NLOS locations, the RF signal propagation is usually subject to distortion due to the blockage and obstacles in the transmission path. This introduces noise to the signal as compared to their LOS counterparts. RSS measurements at LOS GWS’ and NLOS ones are expected to have different features such as strength, variance, and distribution. Such significant differences discourage us from conducting drone detection directly using mixed LOS and NLOS RSS measurements. Instead, we propose to first differentiate LOS signals from NLOS signals upon the detection of any RF signals and then apply drone detection on NLOS RSS measurements. The flow chart of our system is shown in Fig. 4.3.
The main idea of our RSS differentiation scheme is to explore statistical features from collected RSS measurements, and then employ learning approaches to classify LOS and NLOS signals. Specifically, we extract the following features from RSS samples \([r_{i1}; r_{i2};...,r_{ij}]\) for the \(i\)th time window – mean values, average log values, standard deviation, kurtosis, and skewness. In particular, the mean value is used since LOS usually has stronger RSS measurement compared with NLOS for GWS at similar distances to the UAV. Standard deviation is used to measure the variance for RSS samples. Since NLOS signals usually contain more multipath noises, their standard deviations are expected to be larger than LOS signals. This is intuitively true for both drone transmitters or RF transmitters on the ground. The average log value converts the RSS into logarithmic space, because the RSS has a linear relationship with the logarithmic distance. Kurtosis and skewness measure the peaks and asymmetry of the RSS probability distribution respectively.
Figure 4.4: LOS vs NLOS classification using S-SVM

To build the LOS/NLOS classifier, we use the supervised support vector machine (S-SVM) as the learning model [17], which is effective for separating low dimensional feature vectors in two groups. To verify our conjecture, we conducted preliminary experiments and collected 5,000 sets of drone RSS samples for LOS and NLOS conditions in residential areas, each set has around 10 RSS measurements. For each set of RSS samples, aforementioned five features are then extracted and a label (LOS or NLOS) is assigned. These 5,000 feature vectors are then trained with the S-SVM algorithm to obtain the LOS/NLOS classifier. To evaluate the effectiveness of our classifier, we further collected 250 LOS and 250 NLOS test sets to validate the accuracy of our model. As shown in Fig.4, our learning-based identification solution can effectively distinguish LOS and NLOS signals, where the likelihood score measures how likely an input sets shall be LOS \((score \geq 0)\) or NLOS \((score < 0)\). The results show that our solution achieves accuracy rates of 98.4% and 96% for LOS and NLOS signals respectively, over the testing dataset we collected. With the NLOS or LOS signals identified, our system continues to determine whether the RF signals are from a drone. To this end, we propose to extract unique features pertaining to drone flight behaviors, e.g., the motion of drone etc. These features are then processed with deep learning approaches to confirm the presence of a drone. Due to the difference between LOS and NLOS signals, we design a deep learning model for drone detection using NLOS and discuss issues with drone detection with LOS signals.

4.4 NLOS-Based Drone Detection

In NLOS, cases the factors such as multipaths and distortions from any encountered obstacles have huge impact in the measurement of RSS values. NLOS RF signals
are difficult to deal with using signal processing methods, mainly because of the complexity with the wireless channels that NLOS links have to propagate through. Consequently, the aggregated multipath and signal distortion effects form noise-like Gaussian distributions. The small change in the transmitter state (e.g., location, orientation, speed) can lead to significant changes in received signals at the receiver’s side. While such phenomena produces negative impacts in conventional wireless applications, it introduces opportunities in drone detection. This is because that the impact of RF signals from inherent drone motions such as body shifting and vibrations would be “amplified” over the NLOS links. In LOS locations, however, the change of RF signals (i.e., RSS) is less significant because RF signal propagation over LOS links is less sensitive to minor motions of the transmitter.

We use LSTM to learn the features of these signatures from RSS measurements. LSTM is Long Short-Term Memory Network is a RNN created by Hochreiter & Schmidhuber in 1997 [15]. LSTM retains selective information while training the dataset. LSTM algorithm has an inbuilt sigmoid function [15]. This retaining process is done by a sigmoid function which decides how much information to retain and how much information to let go during the training process. The sigmoid curve is shown below.

![Figure 4.5: Sigmoid Function in LSTM](image)

Basically, if the output of the sigmoid function is 0 then no information is retained and if the output is 1, all the information is retained. The below figure represents the overall general algorithm of LSTM.
In our design, we take the RSS measurements and normalize the dataset. Let $X$ be the normalized data and process them so that the vector size is 126. We set the batch size to 128 and the epoch value to 100. The reason why we selected these values is because this combination yields higher accuracy during testing. Detailed evaluation is given in Chapter 5. To validate the effectiveness of our design, we conduct preliminary experiments to collect NLOS RSS data from drones and other mobile sources, including GoPro camera and smartphones, for training and exploring fingerprints. We take LSTM algorithm and train the vectorized RSS measurements and classify them into 0s and 1s. 0 represents non-drone’s RSS measurements and 1 represents drone’s RSS measurements. The below flowchart represents the process in NLOS-Based Drone Detection.

Figure 4.6: Implementation of LSTM(Long Short-Term Memory) [15]
4.5 LOS Based Detection

When the drone is at LOS locations, its RF signal propagation largely follows the free-space path-loss model [24], in which the RSS is expected to be dominated by the direct path component. A popular free-space pass-loss model [24] for drones is given as follows where $t$ represents the time slot of current transmission:

$$PL(t) = 20\log_{10}dt + 20\log_{10}f - 27.55$$

(4.1)
where $dt$ is the current distance between drone and the detector, and $f$ is the transmission frequency. As indicated by Eq, the RSS (in dBm) changes linearly to the logarithm of the distance $dt$, i.e., the change of $1/10$ $dt$ in distance results in around 1 dB change in RSS. For example, when the transmitter and the receiver are 10m away, 1 dB change in RSS requires 1m change in $dt$; the same RSS change only needs 0.1m change in $dt$ when the distance $dt$ is 1m. For drone detection, however, the drone is less likely to be too close to the detector. For drone motions such as body shifting and vibration, the change of drone locations due to these motions is expected to be within few centimeters for popular small-sized drones. RSS variations caused by such motions can be negligible considering various noises added to measured RSS. To detect such minor RSS variations, existing work [39] employs high-grain directional antenna, which is effective in eliminating noises such as multipath. Meanwhile, high-quality RSS measurement module is needed to minimize hardware and measurement errors. For this purpose, [39] uses a USRP to measure the received RF signal. These advanced devices, however, significantly add to the total cost of the drone detector. Moreover, deploying directional antenna for drone detection is impractical unless an array directional antennas are deployed to cover 360 degree space. This is because approaching direction of an invading drone is usually a prior unknown. Another work [8] detects drone by comparing short term and long-term variations of RSS with a noise threshold. Instead of using the slight body motions such as shifting and vibration, this work assumes the existence of a fixed flying pattern of an invading drone, i.e., the drone will strictly follow three phases-approach, surveillance, escape - to fulfill its tasks. It also requires that the invading drone to be in very close proximity (few meters) to the detector during surveillance and be always within direct LOS angle to the drone detector during the drone detection period. While these assumptions may hold in some scenarios, they are by no means true for general applications wherein the drone may not have to approach the target very closely to carry out its tasks. What is more, using a predetermined fixed noise threshold for drone identification can be problematic given the dynamic property of the noise. In general, however, accurately detecting drones in LOS locations using RSS is challenging. This is particularly true for low-cost wireless devices with which severe noises existing during RSS measurements.
Chapter 5

Experiments

5.1 Experiment Setup

In this section, we evaluate our design in terms of effectiveness and efficiency. To evaluate the performance of our system, we conducted experiments using a self-built drone and a popular model drone DJI SPARK. We also included other consumer wireless devices including GoPro camera and smartphones to evaluate the accuracy of the drone detection system. We use Raspberry PI 3 Model B+, which costs less than $50 at the time of performing the experiment, as drone detection system. We conducted extensive experiments in a residential area/apartment complex to evaluate real-world scenarios as shown in the figure below.

![The bird view of the residential area](image)

Figure 5.1: The bird view of the residential area

The residence house that hosted the Raspberry Pi had concrete walls. During our experiments, we placed the Raspberry Pi at two locations inside the residence house to
create LOS and NLOS situations for every test case. Different from existing work [39], our Raspberry Pi is equipped with a commodity USB Wi-Fi module Edimax N150. The drone used its built-in commodity WiFi module for communications. Both Wi-Fi modules are omni-directional and operate at 2.4GHz. No pre-configuration or calibration is needed. The flying patterns and the Raspberry Pi placement are shown in the figure below.

![Flying patterns of the drone](image)

Figure 5.2: Flying patterns of the drone

Four different flying patterns were evaluated to simulate real-world scenarios. These patterns were flying in Straight lines (which include back and forth flying), zig-zag lines, curve lines, going in a circle. For each drone flying pattern we simultaneously collected RSS measurements of non-drone Wi-Fi devices including one GoPro camera during the model training phase. During the drone’s flight, the non-drone device was carried by a person walking along the same path of the drone but at ground altitude. This is to assure that non-drone RSS’ are always present wherever the drone is. The drone was flying 5m above the ground. For each test case, we let the drone fly from far away toward the target house, then pass the house until its RSS cannot be measured. During the testing phase, we changed to different drone and different non-drone devices and collected their RSS measurements. This training and testing process are repeated for different GWS (i.e., Raspberry Pi) location and drone flying pattern combinations. The RSS values were collected at the rate of 20 samples per second.
5.2 Evaluation

5.2.1 Setting the batch size and vector size

We used LSTM to train RSS measurements (just the NLOS samples). After the model is trained, we used new samples to test the accuracy. The epoch value is set as 100, the stride is set as 9 and we set the batch size and vector size to be 64 initially. The accuracy and training time we got in training 27,392 RSS measurements and testing 6,912 RSS measurements is as below

Table 5.1: Training time during Batch Size 64 and Vector Size 64.

<table>
<thead>
<tr>
<th>Total Accuracy (%)</th>
<th>Training Data</th>
<th>Testing Data</th>
<th>Training Time (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>93.5</td>
<td>428</td>
<td>108</td>
<td>8.72</td>
</tr>
</tbody>
</table>

Then, we set the batch size to be 128 and vector size to be 126. The accuracy and the training time we got in training 50,526 RSS measurements and testing 12,726 is as below

Table 5.2: Training time during Batch Size 128 and Vector Size 126.

<table>
<thead>
<tr>
<th>Total Accuracy (%)</th>
<th>Training Data</th>
<th>Testing Data</th>
<th>Training Time (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>97.02</td>
<td>401</td>
<td>101</td>
<td>12.75</td>
</tr>
</tbody>
</table>

Then, we set the batch size to be 256 and vector size to be 256. The accuracy and the training time we got in training 87,808 RSS measurements and testing 22,016 is as below

Table 5.3: Training time during Batch Size 256 and Vector Size 256.

<table>
<thead>
<tr>
<th>Total Accuracy (%)</th>
<th>Training Data</th>
<th>Testing Data</th>
<th>Training Time (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>97.67</td>
<td>343</td>
<td>86</td>
<td>23.73</td>
</tr>
</tbody>
</table>
We can notice that as the batch size and vector size increase the accuracy is higher. But the downside is the training time of data is also increasing. To balance out the accuracy we set our batch size to be 128 and vector size to be 126 throughout our experiments.

5.2.2 Same house training and testing scenario

To evaluate the necessity of differentiating the drone RSS values from a Non-Drone RSS values in NLOS cases, we used LSTM to train 50,526 RSS measurements (just the NLOS samples). After the model is trained, we used around 12,726 new samples to test the accuracy of the model. The experimental results for same house training and testing scenario along with the accuracy are as below. For our testing samples we had 7,308 drone samples and 5,418 non-drone samples.

<table>
<thead>
<tr>
<th>Total Accuracy (%)</th>
<th>Stride</th>
<th>Training Data</th>
<th>Testing Data</th>
<th>True negative</th>
<th>False positive</th>
</tr>
</thead>
<tbody>
<tr>
<td>97.02</td>
<td>9</td>
<td>401</td>
<td>101</td>
<td>0</td>
<td>13.9</td>
</tr>
</tbody>
</table>

In our data validation for the same house training and testing scenarios, the accuracy is 97.02% which is a higher accuracy for detecting a drone and a non-drone samples from the RSS measurements. The training time is 12.75 s. The higher accuracy and our training time show us that our LSTM algorithm is successful for differentiating the RSS samples in NLOS cases.

5.2.3 Transfer trained scenarios

In the above scenario we observed that the accuracy to differentiate between a drone and Non-Drone in the NLOS RSS signals is 97.02%. In order to generalize the model we divide the further experiments into 3 parts. We used three different houses to validate our results. Here we trained the model using Person A’s apartment data and test the model with Person B apartment data. Similarly, we do the same thing with Person C’s data as training and Person B’s data to test our result. We then compare the results with a combined training model Person A and C’s data and test with Person B’s data.
5.2.3.1 Case A - Person A training vs Person B testing

To evaluate the generalized model of differentiating the drone RSS values from a Non-Drone RSS values in NLOS cases, we used different house training and testing scenarios. We used LSTM to train 63,252 RSS measurements (just the NLOS samples) from Person A’s data. After the model was trained, we used around 60,102 new samples to test the accuracy of the model from Person B’s Data. The experimental results for same house training and testing scenario along with the accuracy are as below. We set 126 as the vector size and 128 as the batch size.

Table 5.5: Different House Training and Testing Scenario.

<table>
<thead>
<tr>
<th>Total Accuracy (%)</th>
<th>Training Data</th>
<th>Testing Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>66.45</td>
<td>502</td>
<td>477</td>
</tr>
</tbody>
</table>

In our data validation for the different house training and testing scenarios, the accuracy is 66.45%. Such a low accuracy is mainly because of the NLOS samples from two different apartment have distinct statistical features due to the different multipaths included and the surrounding environment is different.

5.2.3.2 Case B - Person C training vs Person B testing

To evaluate the generalized model of differentiating the drone RSS values from a Non-Drone RSS values in NLOS cases, we first used the same house training and testing scenarios. We used LSTM to train 289,044 RSS measurements (just the NLOS samples) from Person C’s data. After the model is trained, we used around 60,102 new samples to test the accuracy of the model from Person B’s data. The experimental results for same house training and testing scenario along with the accuracy are as below. We set 126 as the vector size and 128 as the batch size.

Table 5.6: Different House Training and Testing Scenario.

<table>
<thead>
<tr>
<th>Total Accuracy (%)</th>
<th>Training Data</th>
<th>Testing Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.88</td>
<td>2294</td>
<td>477</td>
</tr>
</tbody>
</table>

In our data validation for the different house training and testing scenarios, the accuracy is 14.88%. Such a low accuracy is mainly because of the NLOS samples
from two different apartment have distinct statistical features due to the different multipaths included and the surrounding environment is different. From the above two cases we see that we get low accuracy when we transfer train the model. A comprehensive model trained from both types of RSS measurements is not able to capture the features of each of them. To improve this, we combined the training model Person A and Person C’s data and tested it with Person B’s data. Basically, we followed the idea of Data Augmentation as data augmentation covers the missing features when collecting RSS values to avoid statistical difference during our testing process.

5.2.3.3 Case C - Person A and Person C training vs Person B testing

To evaluate the generalized model of differentiating the drone RSS values from a Non-Drone RSS values in NLOS cases, we first used the same house training and testing scenarios. We used LSTM to train 125,496 RSS measurements (just the NLOS samples) from Person A and Person C’s data. After the model is trained, we used around 60,102 new samples to test the accuracy of the model from Person B’s data. The experimental results for same house training and testing scenario along with the accuracy are as below. We set 126 as the vector size and 128 as the batch size.

Table 5.7: Different Combined House Training and Testing Scenario.

<table>
<thead>
<tr>
<th>Total Accuracy (%)</th>
<th>Training Data</th>
<th>Testing Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>83.64</td>
<td>996</td>
<td>477</td>
</tr>
</tbody>
</table>

In our data validation for the different house training and testing scenarios, the accuracy is 83.64%. The accuracy is reasonable in the combined training model because when we combined the model, we covered the missing features when we changed the surrounding. So, when we tested it gave us a higher accuracy. Also, Person C’s (494 records) data is reduced to avoid data overfitting and to match Person A’s (502 records) data.

5.2.4 Advantages of using multiple house for training

Every house has different blueprint and the surroundings are different. When we do transfer training or generalize our model to detect drone RSS values, we might not cover all the features and this yield lower accuracy. In order to cover all the features for training we need to combine multiple models for training and as a result we get higher accuracy. This tells us that our model trained using LSTM detects the drone
and non-drone signals in NLOS scenarios reasonably accurate compared with other training models. Transfer learning proves that this model is applicable in different scenarios.
Chapter 6

Conclusions and Future Research

6.1 Conclusions

In this work, we developed a method to detect privacy-invasion attacks by drones based on their flying patterns, communication with their respective controller. This method is an RSS-based drone detection approach using low-cost COTS devices which is dramatically different from recent researches. Our approach does not require drones to be at LOS locations, nor does it mandate any manually introduced fly pattern though we do take advantage of inherent flying patterns of drones that are implicitly caused by their unique control and mechanical systems.

To this end, we employ deep learning to capture collective features, in received RF signals. Without knowing the presence of drones, we start with classifying any detected RF signals (i.e., their RSS measurements) into LOS signals and/or NLOS signals using S-SVM, and then using LSTM model to detect drone on NLOS signals respectively.

Our experimental results show that our work is able to detect drones in NLOS locations at a rate over 97% in the same house training and testing scenario. When transfer learning is applied then we are able to detect drone at a rate over 83%. This is in sharp contrast with the state-of-the-art passive RF-based drone detection techniques which almost disfunction in NLOS scenarios. For LOS scenario, we confirm its incompetency in drone detection through analytical study and a set of experiments.
6.2 Future Research

In this work we empirically employ deep learning for drone detection for NLOS situations. We employed LSTM, a generative model, to extract features with RSS measurements. Different from existing work which are mainly based on signal processing, our learning-based solution is able to extract sophisticated features from RSS and allow us to accurately detect drones in NLOS locations using commodity wireless interfaces. This significantly alleviates the requirements for drone detection systems as imposed by existing signal processing-based solutions. Interestingly, our experiments show a set of counter-intuition results in terms of drone detection accuracy as compared to these signal processing-based solutions. Specifically, we found that NLOS RSS measurements are more effective than LOS RSS for drone detection. With the nearly perfect NLOS drone detection accuracy, it will be interesting to explore the boundary of the accuracy for LOS drone detection as well as a more reliable drone detection mechanism in general. Specifically, we observe the following directions for such improvements:

- Collaborative sensors: in our current design, each GWS work independently to detect drones. It would be interesting to deploy a network of collaborating GWS'. With our LOS and NLOS differentiation algorithm, each GWS is able to know whether it is at LOS location to the suspicious target (i.e., drone). Given the high drone detection rate in NLOS locations, our design can be extended to select only NLOS GWS' for collaborative drone detection. Fusing algorithms such as majority voting can be utilized to obtain the final detection result. Interestingly, once drone is detected the system can work in the opposite way to localize the drone by selecting only LOS GWS' because LOS locations are superior in wireless localization than NLOS locations.

- Detection of multiple drones: our current work focuses on detecting a single drone. However, in practice, it is possible to have multiple drones or a swarm of drones simultaneously invading a zone. One challenge for multi-drone detection is the interference of the drone communications which may lead to temporal sparse RSS measurements and prevent the recovery of temporal features with drones.

Finally, we also plan to use cloud-based platform in a residential neighborhood with the help of local law enforcements. The user can upload their model to the cloud and check the presence of drone signals. We are also thinking about the cloud rejecting the user model, if the model sent by the user is a malicious file.
Bibliography


[22] Juan Escareno, S Salazar-Cruz, and R Lozano. “Embedded control of a four-rotor UAV”. In: July 2006, 6 pp. DOI: 10.1109/ACC.2006.1657333.


BIBLIOGRAPHY 28


BIBLIOGRAPHY 29


