Accepted Manuscript

RF-based drone detection and identification using deep learning approaches: An initiative towards a large open source drone database

Mohammad F. Al-Sa'd, Abdulla Al-Ali, Amr Mohamed,
Tamer Khattab, Aiman Erbad

PII: S0167-739X(18)33076-0
DOI: https://doi.org/10.1016/j.future.2019.05.007
Reference: FUTURE 4943

To appear in: *Future Generation Computer Systems*

Received date : 10 December 2018
Revised date : 12 April 2019
Accepted date : 1 May 2019

Please cite this article as: M.F. Al-Sa'd, A. Al-Ali, A. Mohamed et al., RF-based drone detection and identification using deep learning approaches: An initiative towards a large open source drone database, *Future Generation Computer Systems* (2019), https://doi.org/10.1016/j.future.2019.05.007

RF-based drone detection and identification using deep learning approaches: an initiative towards a large open source drone database

Mohammad F. Al-Sa'd[a,b,1], Abdulla Al-Ali[a], Amr Mohamed[a,*], Tamer Khattab[c], Aiman Erbad[a]

[a]*Qatar University, Department of Computer Science and Engineering, Doha, Qatar*
[b]*Laboratory of Signal Processing, Tampere University of Technology, Tampere, Finland*
[c]*Qatar University, Department of Electrical Engineering, Doha, Qatar*

Abstract

The omnipresence of unmanned aerial vehicles, or drones, among civilians can lead to technical, security, and public safety issues that need to be addressed, regulated and prevented. Security agencies are in continuous search for technologies and intelligent systems that are capable of detecting drones. Unfortunately, breakthroughs in relevant technologies are hindered by the lack of open source databases for drone's Radio Frequency (RF) signals, which are remotely sensed and stored to enable developing the most effective way for detecting and identifying these drones. This paper presents a stepping stone initiative towards the goal of building a database for the RF signals of various drones under different flight modes. We systematically collect, analyze, and record raw RF signals of different drones under different flight modes such as: off, on and connected, hovering, flying, and video recording. In addition, we design intelligent algorithms to detect and identify intruding drones using the developed RF database. Three deep neural networks (DNN) are used to detect the presence of a drone, the presence of a drone and its type, and lastly, the presence of a drone, its type, and flight mode. Performance of each DNN is validated through a 10-fold cross-validation process and evaluated using various metrics. Classification results show a general decline in performance when increasing the number of classes. Averaged accuracy has decreased from 99.7% for the first DNN (2-classes), to 84.5% for the second DNN (4-classes), and lastly, to 46.8% for the third DNN (10-classes). Nevertheless, results of the designed methods confirm the feasibility of the developed drone RF database to be used for detection and identification. The developed drone RF database along with our implementations are made publicly available for students and researchers alike.

Keywords: UAV detection, drone identification, deep learning, neural networks, machine learning.

1. Introduction

Commercial unmanned aerial vehicles, or drones, are gaining great popularity over the recent years, thanks to their lower cost, smaller size, lighter weight, higher capabilities, and advancements in batteries and motors. This has rendered drones viable for various applications, such as traffic monitoring [1, 2], weather observation [3], disaster management [4], spraying of agricultural chemicals [5], inspection of infrastructures [6], and fire detection and protection [7]. Drones are remotely controlled using wireless technologies such as Bluetooth, 4G and WiFi; hence, by using off-the-shelf upgrades, drones have become a modular solution. The ubiquitous utility of drones can lead to technical, security, and public safety issues that need to be addressed, regulated and prevented, e.g. spying, transfer of illegal or dangerous goods, disturbing electricity and telephone lines, and assault [8]. Therefore, regulating entities need technologies that are capable of detecting and identifying drones without prior assumption on their type or flight mode.

Conventional methods for detecting and identifying intruding drones, e.g. radars, vision and acoustics, are not solely reliable as they can be easily restrained [9, 10]. Radio frequency (RF) sensing combined with deep learning approaches promised a solution; however, it was hindered by the lack of databases for the RF signals of drones [11]. In this paper, we (1) build a novel open source database for the RF signals of various drones under different flight modes, and (2) test the developed database in a drone detection and identification system designed using deep neural networks. This work is a stepping stone towards a larger database built by a community of researchers to encompass the RF signals of many other drones.

The rest of the paper is organized as follows: Section 2 is an overview of related work. We present in Section 3 the system model and describe our methodologies to build and test the database. In Section 4, we present and discuss results of the drone detection and identification system, and finally, we conclude in Section 5.

2. Related Work

In this Section, we review current anti-drone systems and discuss the need for open source drone databases. Moreover, we review state-of-the-art methods used to detect and identify

*Corresponding author.
Email address: amrm@qu.edu.qa (Amr Mohamed)
[1]This work was done while Mohammad F. Al-Sa'd was with the Computer Science and Engineering Department, Qatar University, Doha, Qatar.

intruding drones and discuss their applicability in real-life scenarios. Finally, we review the role of deep learning techniques in anti-drone systems and discuss their feasibility to test the developed RF database.

Anti-drone systems: several commercial and military anti-drone systems have been discussed in the literature. A comprehensive overview of various systems and their deployed technologies is presented in [8]. Challenges and open research issues have been discussed in which "Database Build-Up"; the need to build up an increasing database of drone signatures, was emphasized upon. In [10], state-of-the-art studies on drone surveillance have been surveyed and several anti-drone systems have been discussed. Moreover, various ways to detect, track, and interdict intruding drones have been reviewed in [11]. The authors have concluded that accurate detection and tracking requires a comprehensive database of drone's signatures, hence our work comes as a stepping stone towards this goal.

Drone detection methods: various methods to detect and identify intruding drones have been discussed in the literature such as: radars [12], video surveillance [13], acoustic sensors [14], WiFi sniffing [15] and RF sensing [16]. In [17], a light weight, X-Band radar system was designed to detect drones using their Doppler signatures. Furthermore, a radar sensor was proposed in [18] to automatically detect and classify three distinct drones in a laboratory setting. Moreover, in [19], a drone detection method was introduced by exploiting 5G millimetre-wave deployments as radars. In [20, 21], computer vision object detection methods were used to detect drones in the vicinity of birds. In addition, a system to detect and identify drones from surveillance videos was developed in [9, 22]. In [23], acoustic drone detection and identification was performed using support vector machines. In addition, the same methodology was deployed in [24] to classify drones by their emitted sounds. Furthermore, in [25, 26], drone detection and tracking was performed using acoustic cameras and by direction of arrival (DOA) estimation in [27]. Moreover, in [28, 29], drone sound identification was performed using correlation analysis. In [15, 30], WiFi sniffing based drone detection was performed by statistically analyzing WiFi traffic for drone signatures. In addition, WiFi-based drone detection and disarming was conducted successfully in [31, 32]. Moreover, an energy efficient system capable of detecting and disabling video feeds of WiFi-based drones was presented in [33]. In [16], a passive cost-effective RF sensing drone detection system was designed. In addition, drone detection based on RF sensing was proposed in [34]. Preliminary investigation of active/passive RF approaches for the detection of drones was presented in [35]. Furthermore, in [36, 37], RF-based drone localization methods were developed by DOA estimation and surveillance drones.

Applicability of drone detection and identification methods depends on requirements mandated by real-life scenarios. That being said, we observe that methods other than RF sensing, cannot be solely reliable to detect or identify intruding drones. On one hand, radar, vision, and acoustic based methods can be restrained in various ways such as: using stealth technology, changing the drone physical shape and rotors, using low noise rotors, and by emitting natural sounds, e.g. bird chirps, or white noise [9]. In addition, such methods require expensive equipment, e.g. high quality video cameras, that is not designed to detect drones [9]. Moreover, WiFi-based methods are inherently limited as they cannot detect drones operated by other wireless technologies e.g. 4G, and they require knowledge of the drone's WiFi parameters, e.g. protocol and channel number. On the other hand, we found that RF sensing based methods for drone detection and identification are adequate to be used in real-life scenarios [37]. Such methods are independent of the wireless technology utilized by the drone, e.g. Bluetooth, 4G or WiFi, and are immune to physical alterations and differences among drones. However, current methods are still not fully automated nor robust due to the lack of large labelled databases for the drones RF signals. This has motivated us to build an open source database for the RF signals of various drones under different flight modes.

Drone detection techniques: intelligent detection and identification techniques have emerged vastly by the rise of data driven algorithms, such as neural networks. Deep neural networks (DNN) have shown surpassing results in various cognitive tasks such as speech recognition [38, 39], object detection and identification [40], signal compression [41], and others in all fields of science [42]. In [18], a deep belief network was utilized to classify the spectral correlation functions of three drones. Moreover, a convolutional neural network (CNN) was used to detect the presence of drones from CCTV videos in [43], from surveillance images in [44], from Doppler signatures in [45], and from audio Spectrograms in [46]. In addition, the utility of CNNs as object detectors for reconnaissance and surveillance using drones was proposed in [47]. Furthermore, reinforcement learning was used in [48] to detect temperature anomalies in drone's motors. DNNs versatility in solving optimization problems was demonstrated in other fields. For instance, in [49], it was used to detect known and unknown DDoS attacks; in [50], to detect and identify supply side fraud in programmatic exchanges; in [51] to control the water level in a four-tank system; in [52, 53] to solve various numerical problems; and finally, in [54], to solve person search and re-identification problems. This has motivated us to utilize DNNs for the design of a drone detection and identification system using the developed RF database.

3. Methodology

In this Section, we present the system model that is used to build up the drone RF database and to test its feasibility in a drone detection and identification system. First, we discuss the subsystems and components of the model and summarize their requirements and roles. After that, we elaborate on the discussion for each component and present the experimental setup to build the drone RF database. Finally, we design a drone detection and identification system using DNNs to test the feasibility of the developed RF database in real-life applications.

3.1. System Model

Figure 1 demonstrates our system model that can be divided into two subsystems; RF database development and drone de-

tection and identification, see subsystems A and B in Figure 1 respectively. The RF database development subsystem is comprised of the following three components:

- Drones under analysis: various drones that vary in size, capability, price, and technology. Flight modes are controlled by RF signals coming from and to the flight control module. See elements 1-3 in Figure 1. The main requirement for this component is to use many different drones to produce a large descriptive database for the drone's RF signals.
- Flight control module: a mobile phone or a flight controller that sends and receives RF commands to and from the drones under analysis to change their flight mode. Controlling drones via mobile phones requires installing mobile applications that can be downloaded from various stores. See elements 4-6 in Figure 1.
- RF sensing module: an RF receiver that intercepts the drone's communications with the flight control module. The receiver is connected to a laptop, via cable, that runs a program responsible for fetching, processing and storing the sensed RF data in a database. The requirement for this component is to capture all unlicensed RF bands that drones operate on without any prior assumption on its flight mode. See elements 7-10 in Figure 1.

The drone detection and identification subsystem is comprised of the following two components:

- Signal transformation: it transforms the archived complex RF signals to reveal latent information that can be learned for efficient detection and identification. See element 11 in Figure 1.
- Multi-class classification: it classifies the transformed RF signals using deep neural networks to detect and identify intruding drones. See elements 12-13 in Figure 1. The requirement for this component is to be computationally light for real-time deployment and operation.

3.2. RF database development

3.2.1. Drones under analysis

Different drones can manifest in different RF signals; which in return, can be exploited by intelligent systems for detection and identification. The following is an initial list of the drones used to build our database:

- Parrot Bebop, shown in Figure 2a.
- Parrot AR Drone, demonstrated in Figure 2b.
- DJI Phantom, illustrated in Figure 2c.

These drones are commonly used in research and civilian applications as they vary in size, price, capability and technology [55, 56]. Table 1 lists the drones main specifications. In this work, we are limited by having only three drones; however, the developed open source database is meant to be expanded by researchers and students using other types of drones.

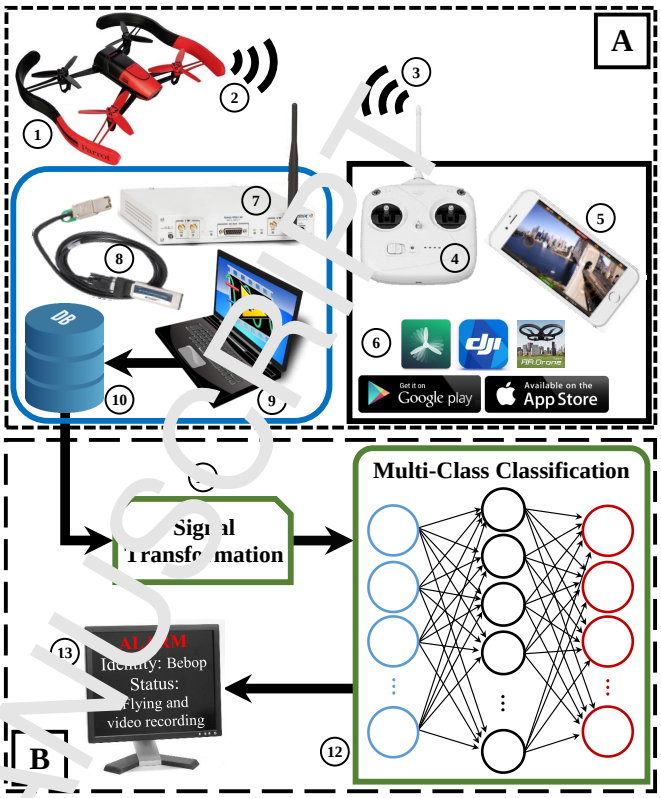


Figure 1: System model comprised of the following subsystems: (A) RF database development and (B) drone detection and identification. The system elements are as follows: (1) drones under analysis, (2) RF signal transmitted from the drone to the flight module, (3) RF signal transmitted from the flight module to the drone, (4) flight controller, (5) mobile phone acting as a flight controller, (6) mobile applications used to control various drones, (7) NI-USRP 2943R RF receiver to intercept the drone RF communications, (8) PCIe cable connecting the RF receiver with a laptop, (9) laptop acting as a processing unit for the intercepted RF data, (10) archived RF signals of various drones under different flight modes, (11) signal transformation to reveal latent information on the archived RF data, (12) multi-class classifier designed using DNNs, and (13) the system output showing the identity and flight mode of an intruding drone.

3.2.2. Flight control module

It consists of flight controllers, or mobile phones, that send and receive RF commands to and from the drones under analysis to alter their flight mode, see Figure 3. Controlling the drones by a mobile phone requires mobile applications that are specifically developed for each drone. "FreeFlight Pro", "AR.FreeFlight", and "DJI Go" are free mobile applications developed to control the Bebop, AR, and Phantom drones, respectively. Other applications can be used; however, in this work, we utilized the official application of each drone.

3.2.3. RF sensing module

It consists of RF receivers, to intercept the drone RF communications with the flight control module, connected to laptops that are responsible for fetching, processing and storing the recorded RF signals in a database. In this work, we assumed that all drones use WiFi operated at 2.4 GHz. Hence, there are some minimal assumptions. Nevertheless, one can determine the drone operating frequency using various methods such as passive frequency scanning.

Drone	Parrot Bebop	Parrot AR Drone	DJI Phantom 3
Dimensions (cm)	38×33×3.6	61×61×12.7	52×49×29
Weight (g)	400	420	1216
Battery capacity (mAh)	1200	1000	4480
Max. range (m)	250	50	1000
Connectivity	WiFi (2.4 GHz and 5 GHz)	WiFi (2.4 GHz)	WiFi (2.4 GHz - 2.483 GHz) + RF (5.725 GHz - 5.825 GHz)

Table 1: Specifications of the drones under analysis. For more details, one can read the full specifications in [57, 58, 59].

(a) Parrot Bebop drone [57].

(b) Parrot AR 2.0 elite edition drone [58].

(c) DJI Phantom 3 standard drone [59].

Figure 2: Three drones used to build the drone RF database.

(a) Drone controller for the DJI Phantom 3 drone [59].

(b) FS-TH9X general radio controller for multicopters [60].

Figure 3: Various drone radio controllers.

First, raw RF samples are acquired using two National Instruments USRP-2943 (NI-USRP) software defined radio reconfigurable devices, shown in Figure 4a. Table 2 lists the NI-USRP RF receivers specifications. Since each RF receiver has a maximum instantaneous bandwidth of 40 MHz, both receivers must be operated simultaneously to at least capture a technology spectrum such as WiFi (i.e., 80 MHz[2]) where the first receiver captures the lower half of the frequency band, and the second, records the the upper half. After that, captured RF data is transferred from the NI-USRP receivers to two standard laptops via Peripheral Component Interconnect Express (PCIe) interface kits, as shown in Figure 4b. Finally, data fetching, processing and storing are performed by programs we designed in LabVIEW Communications System Design Suite [61]. The programs are designed in a standard LabVIEW manner using front panel and block diagram environments. As demonstrated in Figure 5, by using the front panel, one can alter the captured band; lower half or upper half of the RF spectrum, carrier frequency, IQ rate, number of samples per segment, gain, and activate a specific channel of the NI-USRP receiver. In addition, one can select different flight modes and experiments to build a comprehensive database. One can download the developed LabVIEW programs from our database website in [62].

(a) NI USRP-2943R RF receiver [63].

(b) PCIe interface kit [64].

Figure 4: Elements of the RF module to intercept the drones RF signals.

3.2.4. *RF database*

RF-based drone detection and identification applications require a comprehensive database of RF signals to be used for training and testing. The database must contain RF background activities; when drones are absent, and RF drone activities; when drones are present, to be used for drone detection. In addition, it must encompass the RF signals of different drones

[2]The true bandwidth of 2.4 GHz WiFi is 94 MHz plus 3 MHz as guard bands at the beginning and end. However for simplicity, we will not capture the last channel, channel 14, and the first and last 1 MHz of the remaining spectrum as they contain negligible information. Note that to acquire the entire WiFi spectrum using a single receiver, different USRP with a larger bandwidth is needed.

Number of channels	2
Frequency range	1.2 GHz to 6 GHz
Frequency step	< 1 KHz
Grain range	0 dB to 37.5 dB
Maximum instantaneous bandwidth	40 MHz
Maximum I/Q sample rate	200 MS/s
ADC resolution	14 bit

Table 2: Specifications of the USRP-2943 40 MHz RF receivers [63].

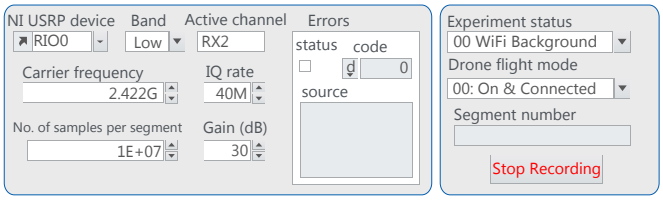


Figure 5: Front panel of the LabVIEW programs installed on the laptops to capture the drones RF communications. The "Band" option is selected as "Low" for the first laptop and "High" for the second laptop. This can be used to recreate the developed LabVIEW programs from scratch; however, one can simply download them from our database website in [62]

.

operating under different flight modes to be used for drone identification purposes and to determine the flight mode of intruding drones.

3.2.4.1. Experimental setup.

Figure 6 illustrates the experimental setup for the RF database development subsystem, subsystem A in Figure 1, to be used for populating the database with the required RF signatures. To conduct any experiment using this setup, one must perform the following tasks carefully and sequentially. If you are recording RF background activities, perform tasks 4-7.

1. Turn on the drone under analysis and connect to it using a mobile phone or a flight controller.
2. In case the utility of a mobile phone or a controller, start the mobile application to control the drone and to change its flight mode.
3. Check the drone connectivity and operation by performing simple takeoff, hovering, and landing tests.
4. Turn on the RF receivers to intercept all RF activities and to transfer those to the laptops via the PCIe connectors.
5. Open the LabVIEW programs, installed on the laptops, and select appropriate parameters depending on your experiment and requirements.
6. Start the LabVIEW programs to fetch, process and store RF data segments.
7. Stop the LabVIEW programs when you are done with the experiment.
8. For a different flight mode, go back to step 6, and for different drones go back to step 1.

3.2.4.2. Experiments.

The RF drone database is populated with the required signatures by conducting experiments organized in a tree manner

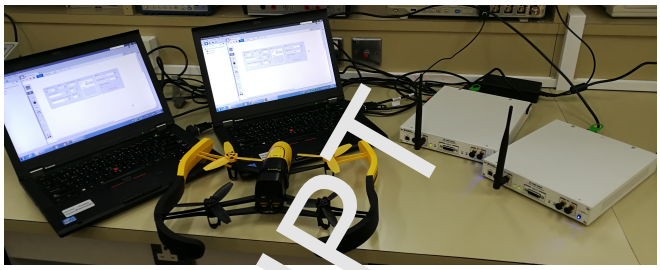


Figure 6: Experimental setup for the RF database development subsystem, subsystem A in Figure 1, using the Bebop drone. The Bebop drone is shown on the middle, the NI-USRP RF receivers are shown on the right and are connected to the laptops, shown on the left, via the PCIe connectors.

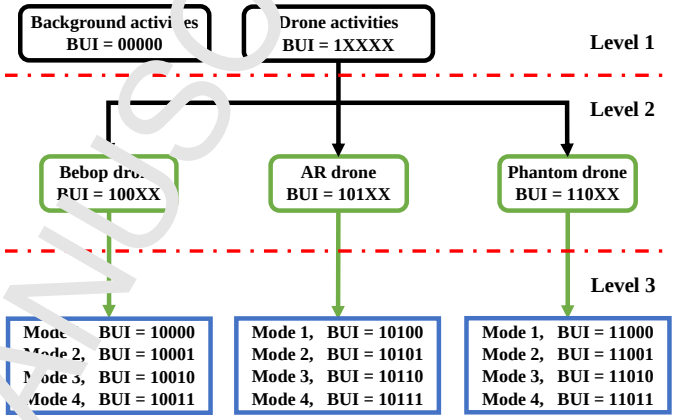


Figure 7: Experiments to record drones RF signatures organized in a tree manner consisting of three levels. The horizontal dashed red lines define the levels. BUI is a Binary Unique Identifier for each component to be used in labelling. Note that the BUI for background activities is always filled with zeros.

with three levels as demonstrated in Figure 7. The first level consists of the following branches to train and assess the drone detection system:

- Drones are off; RF background activities are recorded.
- Drones are on; drones RF activities are recorded.

The second level includes experiments that are conducted on the three drones under analysis: Bebop, AR, and the Phantom drones, to train and assess the drone identification system. Finally, the third level expands its predecessor by explicitly controlling the flight mode of each drone under analysis to assess the identification system ability in determining the flight mode of intruding drones.

- On and connected to the controller.
- Hovering automatically with no physical intervention nor control commands from the controller. Hovering altitude is determined by the drone manufacturer (approximately one meter).
- Flying without video recording. Note that the drone must not hit any obstacles in this experiment to avoid warning signals.

- Flying with video recording. Note that the drone must not hit any obstacles in this experiment to avoid warning signals.

The former experiments are conducted by following the steps summarized in Section 3.2.4.1.

3.2.4.3. Labelling.
A Binary Unique Identifier (BUI) is used to label the RF database entries according to the conducted experiment, drone type, and its specific flight mode, see Figure 7. The BUI is comprised of two binary numbers concatenated such that: BUI = [msBUI, lsBUI]. msBUI is the most significant part of the BUI representing the experiment and drone type, levels one and two, while lsBUI is the least significant part of the BUI representing the drone flight mode, third level. The BUI length L is determined using the total number of experiments E, the total number of drones D, and the total number of flight modes F as follows:

$$L = \lceil \log_2(E) \rceil + \lceil \log_2(D) \rceil + \lceil \log_2(F) \rceil , \tag{1}$$

where $\lceil . \rceil$ is the ceiling operator and in this work, $E = 2$, $D = 3$ and $F = 4$; therefore, $L = 5$. Extending the developed database using other experiments, drones, or flight modes can be easily done by increasing E, D, or F, respectively. One can always add zeros to the left of the BUI parts to extend the database labelling. For instance, if the current database is extended using $E = 4$, $D = 5$ and $F = 9$, a previously developed BUI = 10111, will become 010010011.

3.2.4.4. Database format.
Captured RF signals are stored as segments, to avoid memory overflows, using a standard comma-separated values (csv) format. This makes the drone RF database easy to load and interpret on any preferred software. Metadata for each segment in the database is included within its filename. It contains the segment BUI, followed by the selected RF frequency band; to determine if it is the first or second half of the RF spectrum, and its segment number. For instance, the third segment of the second half of the RF spectrum with BUI = 11010, phantom drone with flight mode number 3, will have the following file name: "11010H_3.csv".

3.3. Drone detection and identification

The developed drone RF database is used to train and test deep neural networks to assess the database feasibility to be used for drone detection and identification.

3.3.1. Signal transformation

It is performed to reveal latent information on the archived RF signals that can be learned for efficient detection and identification (see component 4 in Figure 1). First, since we are using two NI-USRP RF receivers that are not operated in MIMO mode[3], we compute the discrete Fourier transform (DFT) of each recorded segment coming from both receivers as follows:

$$y_i^{(L)}(m) = \left\| \sum_{n=1}^{N} x_i^{(L)}(n) \exp\left(\frac{-j2\pi m(n-1)}{N} \right) \right\| , \tag{2}$$

$$y_i^{(H)}(m) = \left\| \sum_{n=1}^{N} x_i^{(H)}(n) \exp\left(\frac{-j2\pi m(n-1)}{N} \right) \right\| , \tag{3}$$

where $x_i^{(L)}$ is the i^{th} RF segment coming from the first RF receiver that captures the lower half of the RF spectrum, $x_i^{(H)}$ is the i^{th} RF segment coming from the second RF receiver that captures the upper half of the RF spectrum, $y_i^{(L)}$ and $y_i^{(H)}$ are the spectra of the i^{th} segments coming from the first and second RF receivers respectively, n and m are the time and frequency domain indices, N is the total number of time samples in the RF segment i, and $\|.\|$ is the magnitude operator used to compute the power spectrum. Note that, $y_i^{(L)}$ and $y_i^{(H)}$ solely hold the positive spectra of $x_i^{(L)}$ and $x_i^{(H)}$ to ensure non-redundant and concise spectral projections. After that we concatenate the transformed signals of both receivers to build the entire RF spectrum i.e.:

$$y_i = \left[y_i^{(L)}, \; c\, y_i^{(H)} \right] , \tag{4}$$

$$c = \frac{\sum_{q=0}^{Q} y_i^{(L)}(M-q)}{\sum_{q=0}^{Q} y_i^{(H)}(q)} , \tag{5}$$

where c is a normalization factor calculated as the ratio between the last Q samples of the lower spectra, $y_i^{(L)}$, and the first Q samples of the upper spectra, $y_i^{(H)}$, and M is the total number of frequency bins in y_i. The normalization factor c, ensures spectral continuity between the two half's of the RF spectrum as they were captured using different devices; hence, a spectral bias is inevitable. Note that Q must be relatively small to successfully stitch the two spectra and large enough to average out any random fluctuations, e.g. $Q = 10$ for $M = 2048$.

3.3.2. Multi-class classification

Detection and identification of intruding drones is performed by a multi-class classifier designed using deep neural networks (DNN). The system must be able to detect drones and to differentiate between the RF spectra of various drones under different flight modes. A DNN consists of an input layer, hidden layers, and an output layer as shown in Figure 8. One can formulate the input-output relationship of a DNN using the following expressions [65]:

$$z_i^{(l)} = f^{(l)} \left(W^{(l)} z_i^{(l-1)} + b^{(l)} \right) , \tag{6}$$

$$W^{(l)} = \begin{bmatrix} w_{11}^{(l)} & w_{12}^{(l)} & \cdots & w_{1H^{(l-1)}}^{(l)} \\ w_{21}^{(l)} & w_{22}^{(l)} & \cdots & w_{2H^{(l-1)}}^{(l)} \\ \vdots & \vdots & \ddots & \vdots \\ w_{H^{(l)}1}^{(l)} & w_{H^{(l)}2}^{(l)} & \cdots & w_{H^{(l)}H^{(l-1)}}^{(l)} \end{bmatrix} , \tag{7}$$

where $z_i^{(l-1)}$ is the output of layer $l-1$ and the input to layer l; $z_i^{(l)}$ is the output of layer l and the input to layer $l+1$; $z_i^{(0)} = y_i$

[3] Utilizing two NI-USRP receivers in Multiple Inputs Multiple Outputs (MIMO) mode ensures time domain synchrony between the two acquired signal; thus, time domain summation can be performed. However, in this work, this is not the case as receivers are operated independently.

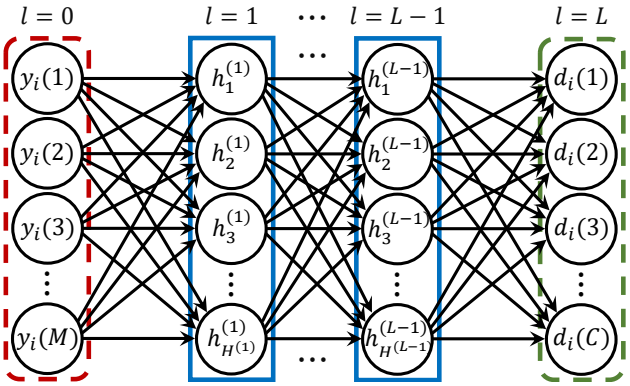


Figure 8: Deep neural network with $L-1$ hidden layers. The input layer, on the left, is outlined with a dashed rounded red rectangle; the hidden layers, on the middle, are identified by blue solid rectangles; and lastly, the output layer, on the right, is determined by a dashed rounded green rectangle.

is the spectrum of the RF segment i; $z_i^{(L)} = d_i$ is the classification vector for the RF segment i; $W^{(l)}$ is the weight matrix of layer l; $w_{pq}^{(l)}$ is the weight between the p^{th} neuron of layer l and the q^{th} neuron of layer $l-1$; $b^{(l)} = \left[b_1^{(l)}, b_2^{(l)}, \cdots, b_{H^{(l)}}^{(l)}\right]^T$ is the bias vector of layer l; $f^{(l)}$ is the activation function of layer l; $l = 1, 2, \cdots, L$; $L-1$ is the total number of hidden layers; $H^{(l)}$ is the total number of neurons in layer l; $H^{(0)} = M$; $H^{(L)} = C$; and C is the number of classes in the classification vector, d_i [65]. Note that f can be any linear or non-linear function; however, the rectified linear unit (ReLU) and the sigmoid functions, expressed in Eq. (8) and Eq. (9) respectively, are typical selections that have shown promising results [66].

$$f(x) = \begin{cases} x & x > 0 \\ 0 & x \leq 0 \end{cases}. \tag{8}$$

$$f(x) = \frac{1}{1 + e^{-x}}. \tag{9}$$

The weights and biases of the DNN are determined through a supervised learning process that minimizes the classification error [67]. The minimization is performed by a gradient descent algorithm where the gradient is computed through back-propagation [65, 67]. The classification error of the system is modelled by the mean square error such that:

$$L\left(d_i, \hat{d}_i\right) = \frac{1}{C} \sum_{c=1}^{C} \left(d_i(c) - \hat{d}_i(c)\right)^2, \tag{10}$$

where $\hat{d}_i$ and d_i are the estimated and true classification vectors of the RF segment i, respectively, and $C = DF$ is the total number of classes, see Section 3.2.4.

In this work, three DNNs are trained and tested using the developed RF database to perform the following tasks: detect the presence of a drone, detect the presence of a drone and identify its type, and lastly, detect the presence of a drone, identify its type, and determine its flight mode.

3.3.3. Cross-validation

Estimating the performance of the RF-based drone detection and identification system is conducted using stratified K-fold cross-validation; an iterative process that repeats for K times to produce performance estimates with low bias and low variance regardless of the size difference between classes [68]. First, the drone RF database is randomly segmented into K disjoint folds with balanced number of instances of each class in each fold [68]. After that, on an arbitrary iteration k, fold k is used as testing data for the DNNs while the rest of the RF database is used for training. This process is repeated K times such that the DNNs are tested using the entire RF database [69]. Finally, performance of the system is estimated by the average performance of all iterations resulting from the K-fold cross-validation procedure [68].

3.3.4. Performance evaluation

Average performance of the RF-based drone detection and identification system is presented using accuracy, precision, recall, error, false discovery rate (FDR), false negative rate (FNR) and F1 scores via confusion matrices. These performance metrics are defined as follows:

$$\text{accuracy} = \frac{TP + TN}{TP + TN + FP + FN}, \tag{11}$$

$$\text{precision} = \frac{TP}{TP + FP}, \tag{12}$$

$$\text{recall} = \frac{TP}{TP + FN}, \tag{13}$$

$$\text{error} = 1 - \text{accuracy}, \tag{14}$$

$$\text{FDR} = 1 - \text{precision}, \tag{15}$$

$$\text{FNR} = 1 - \text{recall}, \tag{16}$$

$$\text{F1 score} = 2\left(\frac{\text{precision} \times \text{recall}}{\text{precision} + \text{recall}}\right), \tag{17}$$

where TP, TN, FP and FN are true positives, true negatives, false positives, and false negatives, respectively.

Figure 9 shows an example confusion matrix for a 3-class classification problem where the rows and columns of the inner 3x3 matrix correspond to the predicted and true classes respectively. The diagonal cells, highlighted in green, represent correctly classified segments, while off-diagonal cells, highlighted in red, depict incorrectly classified segments. The number of segments and the percentage of the total number of segments are shown in each cell in bold. The gray column on the far right illustrates the precision in green, and FDR of the system in red. Furthermore, the gray row at the bottom demonstrates the recall in green, and FNR of the system in red. In addition, the blue cell in the bottom right of the plot shows the overall accuracy in green, and error in red. Moreover, the yellow column and row on the far left and top show the F1 scores for predicting each class in green and its complementary in red, (1 – F1 score), for completeness. Finally, the orange cell in the upper left of the plot shows the averaged F1 score for all classes in green and its complementary in red.

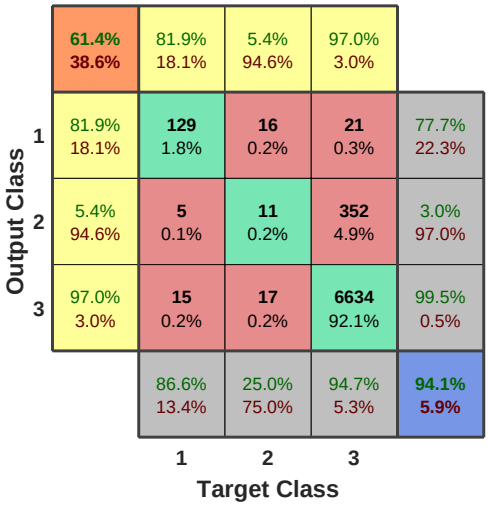


Figure 9: An example of a confusion matrix computed to evaluate the performance of a 3-class classifier. The gray right column shows precision and FDR, the gray bottom row demonstrates recall and FNR, the yellow upper row and left column show the F1 score for predicting each class, the blue cell in the bottom right of the plot shows the overall accuracy and error, and finally, the orange cell in the upper left of the plot depicts the classifier averaged F1 score.

4. Results and Discussions

In this Section, we first present the experimental settings and preprocessing utilized in this work to develop the drone RF database and the RF-based drone detection and identification system. After that, we present snippets from the developed RF database and analyze its spectral information for different drones under different flight modes. Finally, we present and discuss results of the RF-based drone detection and identification system.

4.1. Settings and preprocessing

The LabVIEW programs, installed on both laptops are operated with settings and parameters that are summarized in Table 3. We recorded 10.25 seconds of RF background activities and approximately 5.25 seconds of RF drone communications for each flight mode. This has produced a drone RF database with over 40 GB of data encompassing various RF signatures. In addition, we further segmented our database by a factor of 100 to increase the number of segments for better learning and to ensure an instantaneous representation of the RF signal ($N = 10^5$).

Settings and parameters	Laptop 1	Laptop 2
NI-USRP device	RIO0	RIO0
Active channel	RX2	RX2
RF band	L	H
Carrier frequency (MHz)	2422	2462
IQ rate (MHz)	40	40
Number of samples per segment	10^7	10^7
Gain (dB)	30	30

Table 3: LabVIEW selected settings and parameters to record the drones RF communications to populate the developed database.

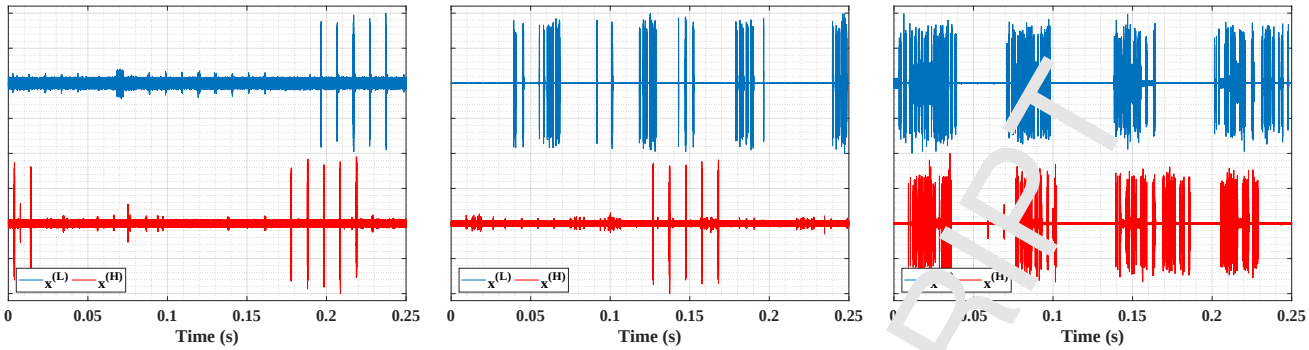
Signal transformation of each archived RF segment is performed using MATLAB FFT function with 2048 frequency bins ($M = 2048$). The full RF spectrum is constructed from its two half's, $y_i^{(L)}$ and $y_i^{(H)}$, using Eq. (7) with 10 returning points to ensure spectral continuity ($Q = 10$). This results in 46,489,600 RF samples to be used in the drone detection and identification system. Note that, the FFT is performed on zero-mean signals that are computed by the de-trending process to remove zero-frequency components.

Three DNNs are designed in Python by Keras to perform the following tasks: detect the presence of a drone, detect the presence of a drone and identify its type, and lastly, detect the presence of a drone, identify its type, and determine its flight mode. Each DNN is trained by an Adam optimizer to minimize the classification mean square error, see Eq. (10), using the following parameters: 3 hidden fully-connected layers ($L-1 = 3$), 256, 128 and 64 total number of neurons at the first, second and third hidden layers respectively ($H^{(1)} = 256, H^{(2)} = 128, H^{(3)} = 64$), total number of epochs is 200, batch size is 10, and lastly, f is the ReLU function for the hidden layers, see Eq. (8), and the sigmoid function for the output layer, see Eq. (9). The classification performance of each network is validated using a stratified 10-fold cross-validation process ($K = 10$) and evaluated using confusion matrices, see Sections 3.3.3 and 3.3.4. One must note that, better classification results can be achieved using different multi-class classifiers, deeper neural networks, and/or different hyper parameters; however, in this work, we are only testing the RF database feasibility to be used for drone detection and identification. Therefore, achieving highest performance is beyond the scope of this paper.

4.2. Analysis of the drone RF database

Table 4 illustrates the total number of segments and samples for the recordings in the developed drone RF database at each experiment level. One can note a class imbalance problem due to the different sample sizes for different classes, hence we will be using stratified cross-validation to assess the drone detection and identification system. Figure 10 shows snippets of raw recordings from the developed RF database. One can observe that drone RF communications can be fully captured using one RF receiver ($x^{(H)}$ amplitude is lower than $x^{(L)}$ in Figure 10b). Nevertheless, one cannot make such assumption as drones can automatically or intentionally change their operating channel and the utilized wireless technology.

Raw RF segments are transformed by DFT to reveal latent information that can be learned for efficient detection and identification. Figure 11 demonstrates spectral and statistical analysis of the acquired RF data. Subfigures (a-c) show the average spectra of the RF signals that are supplied to the first, second and third DNNs respectively. In addition, subfigures (d-f) illustrate the the statistical distribution of the average spectra in subfigures (a-c) using boxplots. One can note that by using Figure 11a, detecting the presence of a drone can be performed effectively by the first DNN as the two spectra show obvious differences that can be verified by the boxplots in Figure 11d. Furthermore, in Figure 11b, one can observe the alikeness among the Bebop and AR RF signals and their different



(a) RF background activities. (b) Bebop drone flying and video recording. (c) Phantom drone on and connected.

Figure 10: Snippets from the developed drone RF database. $x^{(L)}$ and $x^{(H)}$ are plotted in blue and red respectively with normalized amplitudes from -1 to 1. Figure 10a shows segment number 5 of the acquired RF background activities, Figure 10b shows segment number 10 of the acquired Bebop RF signals when flying and video recording, and lastly, Figure 10c shows segment number 7 of the acquired Phantom RF signals when on and connected.

Level	Class	Segments	Samples	Ratio (%)
1	Drone	186	$3{,}720\times10^6$	81.94%
	No Drone	41	820×10^6	18.06%
2	Bebop	84	$1{,}680\times10^6$	37.00%
	AR	81	$1{,}620\times10^6$	35.68%
	Phantom	21	420×10^6	9.25%
	No Drone	41	820×10^6	18.06%
3	Bebop mode 1	21	420×10^6	9.25%
	Bebop mode 2	21	420×10^6	9.25%
	Bebop mode 3	21	420×10^6	9.25%
	Bebop mode 4	21	420×10^6	9.25%
	AR mode 1	21	420×10^6	9.25%
	AR mode 2	21	420×10^6	9.25%
	AR mode 3	21	420×10^6	9.25%
	AR mode 4	18	360×10^6	7.94%
	Phantom mode 1	21	420×10^6	9.25%
	No Drone	41	820×10^6	18.06%

Table 4: Details of the developed drone RF database showing the number of raw samples and segments for each class at each experimental level. Note that the total number of samples is divided equally between the recordings coming from the first and second RF receivers ($x^{(L)}$ and $x^{(H)}$). For more details, see Figure 7 and Section 3.2.4.2.

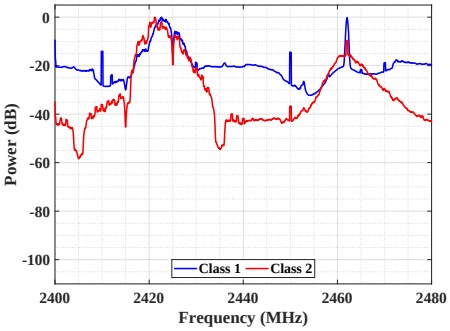
morphology when compared to the Phantom drone or RF background activities. Such similarities can hinder the second DNN from accurately differentiating these drones as confirmed by the boxplots in Figure 11e. Lastly, by using Figure 11c, the previous observation can be formally stated as follows: Bebop and AR drones have similar RF communications since they produce similar spectra for different flight modes. This is logical, as both drones are manufactured by the same company, Parrot. Therefore, detecting the flight modes of these two drones present difficulties for any intelligent system, see Figure 11f for statistical verification.

4.3. Drone detection and identification

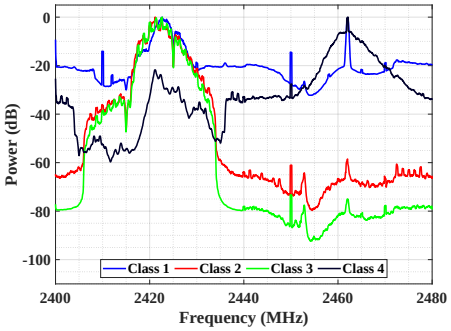
Performance evaluation of the three developed DNNs is shown in Figure 12 using confusion matrices. See Section 3.3.4 for more details on how to interpret a confusion matrix. First, Figure 12a shows the classification performance of the first DNN which detects the presence of a drone. Results demonstrate an average accuracy of 99.7%, average error of 0.3%, and average F1 score of 99.5%. Moreover, Figure 12b depicts the classification performance of the second DNN which detects the presence of a drone and identifies its type. Results demonstrate an average accuracy of 84.5%, average error of 15.5%, and average F1 score of 78.8%. Finally, Figure 12c illustrates the classification performance of the third DNN which detects the presence of a drone, identifies its type, and determines its flight mode. Results demonstrate an average accuracy of 46.8%, average error of 53.2%, and average F1 score of 43%. Generally, one can observe a decline in performance when increasing the number of classes. This can be explained by the similarities of RF communications of the Bebop and AR drones, see Figure 11. The recall when detecting background and Phantom RF signatures remained high for the second and third DNNs, 96.1% and 97.4% (see Eq. (13) and the right columns of the confusion matrices in Figure 12). However, detecting the Bebop and AR drones or identifying their flight modes is almost random. The former observations are aligned with the analysis presented in Section 4.2. Nevertheless, results of the developed system still demonstrate the feasibility of the developed drone RF database to be used for detection and identification.

5. Conclusions

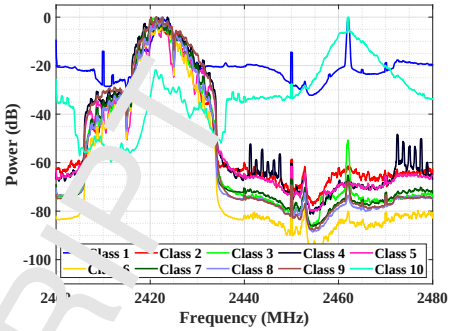
As drones are becoming more popular among civilians, regulating entities demand intelligent systems that are capable of detecting and identifying intruding drones. However, the design of such systems is hindered by the lack of large labelled open source databases. This work is a contribution towards this goal by developing a database of drones Radio Frequency (RF) communications that can be further extended by researchers and students. The developed database encompasses RF signals of various drones under different flight modes; therefore, it can be used to test and validate intelligent algorithms, and can be adopted to design drone detection and identification systems.



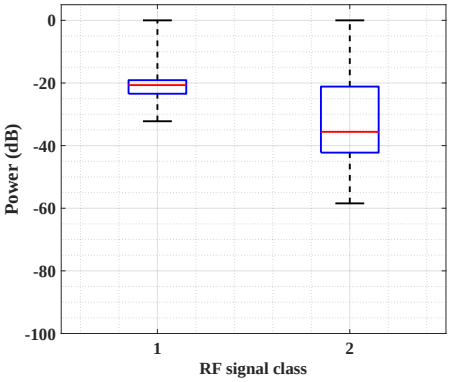
(a) Average spectra of the RF background activities (class 1) along with the RF signals of all the drones under analysis (class 2).



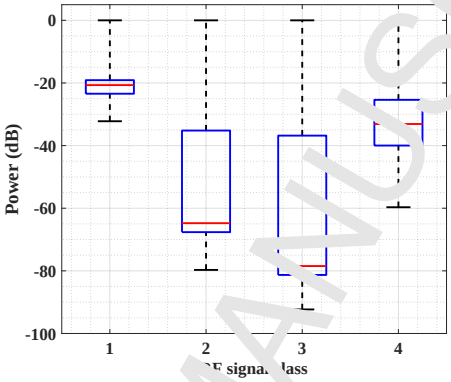
(b) Average spectra of the RF background activities (class 1) along with the RF signals of the three drones under analysis (classes 2-4).



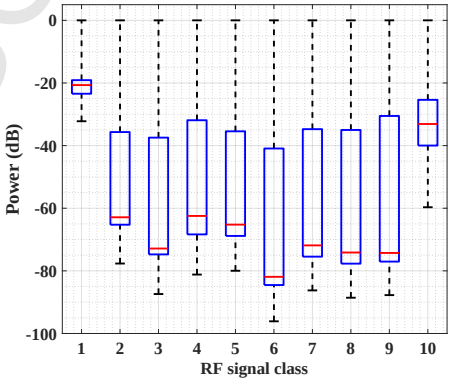
(c) Average spectra of the RF background activities (class 1) along with the RF signals of each drone under different flight mode (classes 2-10).



(d) Boxplot of the average spectra shown in Figure 11a showing the distribution of data.



(e) Boxplot of the average spectra shown in Figure 11b showing the distribution of data.



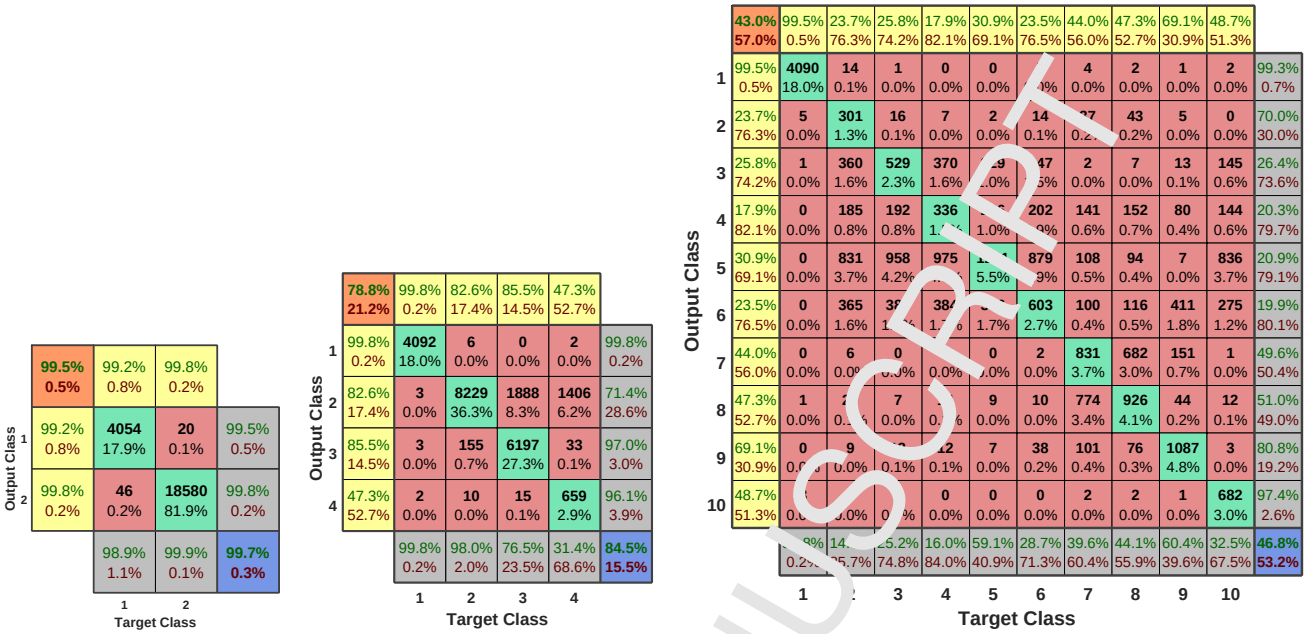
(f) Boxplot of the average spectra shown in Figure 11c showing the distribution of data.

Figure 11: Spectral and statistical analysis of the acquired RF signals to be supplied for three drone detection and identification DNNs. Figures (a-c) show the average power spectra of the acquired RF signals while Figures (d-f) show the boxplot of the computed spectra. Note that amplitudes of the average spectra are normalized to discard biases in the analysis and that they are smoothed using a 10-point moving average filter to ease visual interpretations. In Figure 11a, class 1 is for RF background activities and class 2 is for the drones RF communications (to be supplied to the first DNN). In Figure 11b, class 1 is for RF background activities and classes 2-4 are for the Bebop, AR and Phantom drones (to be supplied to the second DNN). In Figure 11c, class 1 is for RF background activities, classes 2-5 are for the Bebop 4 different flight modes, classes 6-9 are for the AR 4 different flight modes, and lastly, class 10 is for the Phantom single flight mode (to be supplied to the third DNN).

We have collected, analyzed, and recorded raw RF signals of different drones under different flight modes such as: off, on and connected, hovering, flying, and video recording. After that, to test the feasibility of the developed database, we used deep neural networks (DNNs) to detect and identify intruding drones and to determine their flight mode. We designed, validated, and evaluated three DNNs to perform the following tasks: detect the presence of a drone, detect the presence of a drone and identify its type, and lastly detect the presence of a drone, identify its type, and determine its flight mode.

Results of the developed systems showed a general decline in performance when increasing the number of classes. Average accuracy has decreased from 99.7% for the first DNN (2-classes), to 84.5% for the second DNN (4-classes), and lastly, to 46.8% for the third DNN (10-classes). This decrease was shown to be caused by similarities observed on some drones RF spectra as they were manufactured by the same company, e.g. the Bebop and AR drones. This introduces a challenging obstacle that can be mitigated using deeper neural networks or by other advanced classification algorithms. Nevertheless, results of the developed drone detection and identification system demonstrate the feasibility of the developed database to be used for testing and validating intelligent algorithms and to design advanced drone detection and identification systems. The developed drone RF database is open source and can be found in [62] along with all the implementations required to reproduce the results of this work.

In the future, one can extract features from the developed drone RF database to be used for detection and compare their results with the outcomes of our system. In addition, the developed database can be used to train and test different detectors and network architectures to systematically converge to the best detection and identification system. Furthermore, fusing the developed database with other drone detection modalities such as camera images and videos, radar echoes, and acoustic recordings, can ameliorate the performance of the detection and identification system by exploiting the strengths of each modality. The developed database can be extended by researchers and students alike in various ways such as: (1) investigating other classification algorithms, (2) expanding the developed database



(a) Average confusion matrix of the first DNN (detecting the presence of a drone).

(b) Average confusion matrix of the second DNN (detecting the presence of a drone and identifying its type).

(c) Average confusion matrix of the third DNN (detecting the presence of a drone, identifying its type, and determining its flight mode).

Figure 12: Average classification performance for the three designed DNNs using confusion matrices. In Figure 12a, class 1 is for RF background activities and class 2 is for the drones RF communications. In Figure 12b, class 1 is for RF background activities and classes 2-4 are for the Bebop, AR and Phantom drones. In Figure 12c, class 1 is for RF background activities, classes 2-5 are for the Bebop 4 different flight modes, classes 6-9 are for the AR 4 different flight modes, and lastly, class 10 is for the Phantom single flight mode.

by augmentation, e.g. adding channel fading or noise, (3) perform the same experiments using other drones, (4) study the effects of RF interference and noise when detecting and identifying drones, (5) conduct experiments for indoor and outdoor flying, (6) vary the drone speed and distance from the RF receiver, and many others.

Acknowledgements

This publication was supported by Qatar university Internal Grant No. QUCP-CENG-2018/2019 1. The work of Aiman Erbad is supported by grant number NPRP 7-1469-1-273. The findings achieved herein are solely the responsibility of the authors.

References

[1] J. Y. J. Chow, Dynamic UAV-based traffic monitoring under uncertainty as a stochastic arc-inventory routing policy, International Journal of Transportation Science and Technology 5 (3) (2016) 167 – 185, unmanned Aerial Vehicles and Remote Sensing. doi:10.1016/j.ijtst.2016.11.002.

[2] F. Mohammed, A. Idries, N. Mohamed, J. Al-Jaroodi, I. Jawhar, UAVs for smart cities: Opportunities and challenges, in: 2014 International Conference on Unmanned Aircraft Systems (ICUAS), 2014, pp. 267–273. doi:10.1109/ICUAS.2014.6842265.

[3] V. V. Klemas, Coastal and Environmental Remote Sensing from Unmanned Aerial Vehicles: An Overview, Journal of Coastal Research (2018) 1260–1267doi:10.2112/jcoastres-d-15-00005.1.

[4] M. Erdelj, E. Natalizio, K. R. Chowdhury, I. F. Akyildiz, Help from the Sky: Leveraging UAVs for Disaster Management, IEEE Pervasive Computing 16 (1) (2017) 24–32. doi:10.1109/MPRV.2017.11.

[5] Y. Huang, S. J. Thomson, W. C. Hoffmann, Y. Lan, B. K. Fritz, Development and prospect of unmanned aerial vehicle technologies for agricultural production management, International Journal of Agricultural and Biological Engineering 6 (3) (2013) 1–10. doi:10.3965/j.ijabe.20130603.001.

[6] Y. Ham, K. K. Han, J. J. Lin, M. Golparvar-Fard, Visual monitoring of civil infrastructure systems via camera-equipped Unmanned Aerial Vehicles (UAVs): a review of related works, Visualization in Engineering 4 (1) (2016) 1. doi:10.1186/s40327-015-0029-z.

[7] H. Cruz, M. Eckert, J. Meneses, J.-F. Martínez, Efficient forest fire detection index for application in unmanned aerial systems (UASs), Sensors 16 (6) (2016) 893. doi:10.3390/s16060893.

[8] X. Shi, C. Yang, W. Xie, C. Liang, Z. Shi, J. Chen, Anti-Drone System with Multiple Surveillance Technologies: Architecture, Implementation, and Challenges, IEEE Communications Magazine 56 (4) (2018) 68–74. doi:10.1109/MCOM.2018.1700430.

[9] S. R. Ganti, Y. Kim, Implementation of detection and tracking mechanism for small UAS, in: 2016 International Conference on Unmanned Aircraft Systems (ICUAS), 2016, pp. 1254–1260. doi:10.1109/ICUAS.2016.7502513.

[10] G. Ding, Q. Wu, L. Zhang, Y. Lin, T. A. Tsiftsis, Y. Yao, An Amateur Drone Surveillance System Based on the Cognitive Internet of Things, IEEE Communications Magazine 56 (1) (2018) 29–35. doi:10.1109/MCOM.2017.1700452.

[11] İ. Güvenç, F. Koohifar, S. Singh, M. L. Sichitiu, D. Matolak, Detection, Tracking, and Interdiction for Amateur Drones, IEEE Communications Magazine 56 (4) (2018) 75–81. doi:10.1109/MCOM.2018.1700455.

[12] G. C. Birch, J. C. Griffin, M. K. Erdman, UAS Detection Classification and Neutralization: Market Survey 2015, Tech. Rep. SAND2015-6365 606150, Sandia National Laboratories, United States (2015). doi:10.2172/1222445.

[13] R. L. Sturdivant, E. K. P. Chong, Systems Engineering Baseline Concept

of a Multispectral Drone Detection Solution for Airports, IEEE Access 5 (2017) 7123–7138. doi:10.1109/ACCESS.2017.2697979.

[14] İ. Güvenç, O. Ozdemir, Y. Yapici, H. Mehrpouyan, D. Matolak, Detection, localization, and tracking of unauthorized UAS and Jammers, in: 2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC), 2017, pp. 1–10. doi:10.1109/DASC.2017.8102043.

[15] I. Bisio, C. Garibotto, F. Lavagetto, A. Sciarrone, S. Zappatore, Blind Detection: Advanced Techniques for WiFi-Based Drone Surveillance, IEEE Transactions on Vehicular Technology 68 (1) (2019) 938–946. doi:10.1109/TVT.2018.2884767.

[16] P. Nguyen, H. Truong, M. Ravindranathan, A. Nguyen, R. Han, T. Vu, Cost-Effective and Passive RF-Based Drone Presence Detection and Characterization, GetMobile: Mobile Comp. and Comm. 21 (4) (2018) 30–34. doi:10.1145/3191789.3191800.

[17] A. Moses, M. J. Rutherford, K. P. Valavanis, Radar-based detection and identification for miniature air vehicles, in: 2011 IEEE International Conference on Control Applications (CCA), 2011, pp. 933–940. doi:10.1109/CCA.2011.6044363.

[18] G. J. Mendis, T. Randeny, J. Wei, A. Madanayake, Deep learning based doppler radar for micro UAS detection and classification, in: MILCOM 2016 - 2016 IEEE Military Communications Conference, 2016, pp. 924–929. doi:10.1109/MILCOM.2016.7795448.

[19] D. Solomitckii, M. Gapeyenko, V. Semkin, S. Andreev, Y. Koucheryavy, Technologies for Efficient Amateur Drone Detection in 5G Millimeter-Wave Cellular Infrastructure, IEEE Communications Magazine 56 (1) (2018) 43–50. doi:10.1109/MCOM.2017.1700450.

[20] M. Saqib, S. D. Khan, N. Sharma, M. Blumenstein, A study on detecting drones using deep convolutional neural networks, in: 2017 14th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), 2017, pp. 1–5. doi:10.1109/AVSS.2017.8078541.

[21] E. Unlu, E. Zenou, N. Riviere, Using Shape Descriptors for UAV Detection, Electronic Imaging 2018 (9) (2018) 128–1–128–5. doi:10.2352/ISSN.2470-1173.2018.09.SRV-128.

[22] M. Wu, W. Xie, X. Shi, P. Shao, Z. Shi, Real-Time Drone Detection Using Deep Learning Approach, in: L. Meng, Y. Zhang (Eds.), Machine Learning and Intelligent Communications, Springer International Publishing, Cham, 2018, pp. 22–32.

[23] A. Bernardini, F. Mangiatordi, E. Pallotti, L. Capodiferro, Drone detection by acoustic signature identification, Electronic Imaging 2017 (10) (2017) 60–64. doi:10.2352/ISSN.2470-1173.2017.10.IMAWM-168.

[24] M. Nijim, N. Mantrawadi, Drone classification and identification system by phenome analysis using data mining techniques, in: 2016 IEEE Symposium on Technologies for Homeland Security (HST), 2016, pp. 1–5. doi:10.1109/THS.2016.7568949.

[25] X. Chang, C. Yang, J. Wu, X. Shi, Z. Shi, A surveillance system for Drone Localization and Tracking Using Acoustic Arrays, in: 2018 IEEE 10th Sensor Array and Multichannel Signal Processing Workshop (SAM), 2018, pp. 573–577. doi:10.1109/SAM.2018.8448409.

[26] J. Busset, F. Perrodin, P. Wellig, B. Ott, K. Heutschi, T. Rhl, T. Nussbaumer, Detection and tracking of drones using advanced acoustic cameras, Proc.SPIE Unmanned/Unattended Sensors and Sensor Networks XI; and Advanced Free-Space Optical Communication Techniques and Applications 9647 (2015) 9647 – 9647 – 8. doi:10.1117/12.2194309.

[27] C. Yang, Z. Wu, X. Chang, X. Shi, J. Wo, Z. Shi, DOA Estimation Using Amateur Drones Harmonic Acoustic Signals, in: 2018 IEEE 10th Sensor Array and Multichannel Signal Processing Workshop (SAM), 2018, pp. 587–591. doi:10.1109/SAM.2018.8448797.

[28] J. Mezei, A. Molnár, Drone sound detection by correlation, in: 2016 IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI), 2016, pp. 509–518. doi:10.1109/SACI.2016.7507430.

[29] J. Mezei, V. Fiaska, A. Molnar, Drone sound detection, in: 2015 16th IEEE International Symposium on Computational Intelligence and Informatics (CINTI), 2015, pp. 333–338. doi:10.1109/CINTI.2015.7382945.

[30] I. Bisio, C. Garibotto, F. Lavagetto, A. Sciarrone, S. Zappatore, Unauthorized Amateur UAV Detection Based on WiFi Statistical Fingerprint Analysis, IEEE Communications Magazine 56 (4) (2018) 106–111. doi:10.1109/MCOM.2018.1700340.

[31] M. Peacock, M. N. Johnstone, Towards detection and control of civilian unmanned aerial vehicles, Proceedings of the 14th Australian Information Warfare Conference.doi:10.4225/75/57a847dfbefb5.

[32] L. Val Terrón, Design, development and assessment of techniques for neutralizing drones, Ph.D. thesis, Galician Research and Development Center in Advanced Telecommunications (2017).
URL http://castor.det.uvigo.es:8080/xmlui/bitstream/handle/123456789/96/TFM%20Lucas%20Val%20Terron.pdf?sequence=1

[33] A. Sun, W. Gong, R. Shea, J. Liu, X. S. Liu, Q. Wang, Drone privacy shield: A WiFi based defense, in: 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 2017, pp. 1–5. doi:10.1109/PIMRC.2017.8292780.

[34] H. Zhang, C. Cao, L. Xu, T. A. Gulliver, A UAV Detection Algorithm Based on an Artificial Neural Network, IEEE Access 6 (2018) 24720–24728. doi:10.1109/ACCESS.2018.2831911.

[35] P. Nguyen, M. Ravindranatha, A. Nguyen, R. Han, T. Vu, Investigating Cost-effective RF-based Detection of Drones, in: Proceedings of the 2nd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use, DroNet'16, ACM, New York, NY, USA, 2016, pp. 17–22. doi:10.1145/2935620.2935632.

[36] S. Abeywickrama, L. Jayasinghe, H. Fu, C. Yuen, RF-Based Direction Finding of UAVs Using DNN, arXiv preprint arXiv:1712.01154.

[37] M. M. Azari, H. Sallouha, A. Chiumento, S. Rajendran, E. Vinogradov, S. Pollin, Key Technologies and System Trade-offs for Detection and Localization of Amateur Drones, IEEE Communications Magazine 56 (1) (2018) 51–57. doi:10.1109/MCOM.2017.1700442.

[38] W. Chan, N. Jaitly, Q. Le, O. Vinyals, Listen, attend and spell: A neural network for large vocabulary conversational speech recognition, in: 2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2016, pp. 4960–4964. doi:10.1109/ICASSP.2016.7472621.

[39] A. Graves, A. Mohamed, G. Hinton, Speech recognition with deep recurrent neural networks, in: 2013 IEEE International Conference on Acoustics, Speech and Signal Processing, 2013, pp. 6645–6649. doi:10.1109/ICASSP.2013.6638947.

[40] K. Kang, H. Li, J. Yan, X. Zeng, B. Yang, T. Xiao, C. Zhang, Z. Wang, R. Wang, X. Wang, W. Ouyang, T-CNN: Tubelets with Convolutional Neural Networks for Object Detection from Videos, IEEE Transactions on Circuits and Systems for Video Technology (2018) 1–1doi:10.1109/TCSVT.2017.2736553.

[41] A. B. said, M. F. Al-Sa'd, M. Tlili, A. A. Abdellatif, A. Mohamed, T. Elfouly, K. Harras, M. D. O'Connor, A Deep Learning Approach for Vital Signs Compression and Energy Efficient Delivery in mhealth Systems, IEEE Access 6 (2018) 33727–33739. doi:10.1109/ACCESS.2018.2844308.

[42] Y. LeCun, Y. Bengio, G. Hinton, Deep learning, Nature 521 (2015) 436. doi:10.1038/nature14539.

[43] N. Shijith, P. Poornachandran, V. G. Sujadevi, M. M. Dharmana, Breach detection and mitigation of UAVs using deep neural network, in: 2017 Recent Developments in Control, Automation Power Engineering (RDCAPE), 2017, pp. 360–365. doi:10.1109/RDCAPE.2017.8358297.

[44] C. Aker, S. Kalkan, Using deep networks for drone detection, 2017 14th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)doi:10.1109/avss.2017.8078539.

[45] B. K. Kim, H. Kang, S. Park, Drone Classification Using Convolutional Neural Networks With Merged Doppler Images, IEEE Geoscience and Remote Sensing Letters 14 (1) (2017) 38–42. doi:10.1109/LGRS.2016.2624820.

[46] H. C. Vemula, Multiple Drone Detection and Acoustic Scene Classification with Deep Learning, Ph.D. thesis, Wright State University, Wright State University (2018).
URL http://rave.ohiolink.edu/etdc/view?acc_num=wright1547384408540764

[47] J. Lee, J. Wang, D. Crandall, S. Šabanović, G. Fox, Real-Time, Cloud-Based Object Detection for Unmanned Aerial Vehicles, in: 2017 First IEEE International Conference on Robotic Computing (IRC), 2017, pp. 36–43. doi:10.1109/IRC.2017.77.

[48] H. Lu, Y. Li, S. Mu, D. Wang, H. Kim, S. Serikawa, Motor Anomaly Detection for Unmanned Aerial Vehicles Using Reinforcement Learning, IEEE Internet of Things Journal 5 (4) (2018) 2315–2322. doi:10.1109/JIOT.2017.2737479.

[49] A. Saied, R. E. Overill, T. Radzik, Detection of known and unknown DDoS attacks using Artificial Neural Networks, Neurocomputing 172 (2016) 385 – 393. doi:10.1016/j.neucom.2015.04.101.

[50] A. Badhe, Using neural networks to detect supply side fraud in programmatic exchanges, Neural Networks & Machine Learning 1 (1) (2017) 1.
URL http://neuraldatasets.org/index.php/neuralnetworks/article/view/1

[51] J. Wang, K. Shi, Q. Huang, S. Zhong, D. Zhang, Stochastic switched sampled-data control for synchronization of delayed chaotic neural networks with packet dropout, Applied Mathematics and Computation 335 (2018) 211 – 230. doi:10.1016/j.amc.2018.04.038.

[52] K. Shi, J. Wang, S. Zhong, X. Zhang, Y. Liu, J. Cheng, New reliable nonuniform sampling control for uncertain chaotic neural networks under Markov switching topologies, Applied Mathematics and Computation 347 (2019) 169 – 193. doi:10.1016/j.amc.2018.11.011.

[53] K. Shi, Y. Tang, S. Zhong, C. Yin, X. Huang, W. Wang, Nonfragile asynchronous control for uncertain chaotic Lurie network systems with Bernoulli stochastic process, International Journal of Robust and Nonlinear Control 28 (5) (2018) 1693–1714. doi:10.1002/rnc.3980.

[54] T. Xiao, S. Li, B. Wang, L. Lin, X. Wang, Joint detection and identification feature learning for person search, in: Computer Vision and Pattern Recognition (CVPR), 2017 IEEE Conference on, IEEE, 2017, pp. 3376–3385.

[55] E. Vattapparamban, İ. Güvenç, A. İ. Yurekli, K. Akkaya, S. Uluağaç, Drones for smart cities: Issues in cybersecurity, privacy, and public safety, in: 2016 International Wireless Communications and Mobile Computing Conference (IWCMC), 2016, pp. 216–221. doi:10.1109/IWCMC.2016.7577060.

[56] D. Skorupka, A. Duchaczek, A. Waniewska, M. Kowacka, Optimization of the choice of unmanned aerial vehicles used to monitor the implementation of selected construction projects, AIP Conference Proceedings 1863 (1) (2017) 230013. doi:10.1063/1.4992398.

[57] photopoint, Online (2018). [link].
URL https://www.photopoint.ee/en/drones/363208-parrot-bebop-drone-1-red?ship_to=QA

[58] Amazon, Online (2018). [link].
URL https://www.amazon.com/Parrot-AR-Drone-2-0-Elite-Quadcopter/dp/B00FS7SU7K

[59] DJI, Online (2018). [link].
URL https://www.dji.com/phantom-3-standard

[60] ETech, FS-TH9X 2.4GHz 9CH Transmitter, Online (2018).
URL https://www.etechpk.net/shop/multicopter-accesories/fs-th9x-2-4ghz-9ch-transmitter/

[61] N. Instruments, LabVIEW Communications System Design Suite, Online (2018).
URL https://www.ni.com/en-lb/shop/select/labview-communications-system-design-suite

[62] M. F. Al-Sa'd, A. Al-Ali, A. Mohamed, T. Khattab, A. Erbad, Drones acquired RF database along with the utilized software, Online (2019).
URL https://al-sad.github.io/DroneRF

[63] N. Instruments, USRP Software Defined Radio Reconfigurable Device, Online (2018).
URL https://www.ni.com/en-lb/support/model.usrp-2943.html

[64] E. Research, ExpressCard PCIe Interface Kit (Laptop), Online (2018).
URL https://www.ettus.com/product/details/ECARD-KIT

[65] X. He, S. Xu, Artificial Neural Networks, Springer Berlin Heidelberg, Berlin, Heidelberg, 2010, Ch. 2, pp. 20–42. doi:10.1007/978-3-540-73762-9_2

[66] M. Dorofki, A. H. Elshafie, O. Jaafar, O. A. Karim, S. Mastura, Comparison of artificial neural network transfer functions abilities to simulate extreme runoff data, International Proceedings of Chemical, Biological and Environmental Engineering 33 (2012) 39–44.

[67] L. Bottou, Large-scale Machine Learning with Stochastic Gradient Descent, in: Y. Lechevallier, G. Saporta (Eds.), Proceedings of COMPSTAT'2010, Physica-Verlag HD, Heidelberg, 2010, pp. 177–186.
URL https://link.springer.com/chapter/10.1007/978-3-7908-2604-3_16#citeas

[68] X. Zeng, T. R. Martinez, Distribution-balanced stratified cross-validation for accuracy estimation, Journal of Experimental & Theoretical Artificial Intelligence 12 (1) (2000) 1–12. doi:10.1080/095281300146272.

[69] T.-T. Wong, Performance evaluation of classification algorithms by k-fold and leave-one-out cross validation, Pattern Recognition 48 (9) (2015) 2839 – 2846. doi:10.1016/j.patcog.2015.03.009.

Mohammad Fathi Al-Sa'd
received his B.Sc. and M.Sc. degrees in Electrical Engineering from Qatar University, Qatar, in 2012 and 2016 respectively. He specialized in signal processing and graduated with honors under professor Boualem Boashash supervision. He worked as a Research Assistant at Qatar University, and currently he is a Researcher and a Doctor of Science student at Laboratory of Signal Processing, Tampere University of Technology, Finland. He has served as a technical reviewer for several journals, including Biomedical Signal Processing and Control. His research interests include EEG analysis and processing, time-frequency array processing, information flow and theory, modelling and optimization and machine learning.

Abdullah Al-Ali
obtained his master's degree in software design engineering and PhD degree in Computer Engineering from Northeastern University in Boston, MA, USA in 2008 and 2014, respectively. He is an active researcher in Cognitive Radios for smart cities and vehicular ad-hoc networks (VANETs). He has published several peer-reviewed papers in journals and conferences. Dr. Abdulla is currently head of the Technology Innovation and Engineering Education (TIEE), at the College of Engineering in Qatar University.

Amr Mohamed
received his M.S. and Ph.D. in electrical and computer engineering from the University of British Columbia, Vancouver, Canada, in 2001, and 2006 respectively. His research interests include wireless networking, edge computing, and security for IoT applications. Dr. Amr Mohamed has co-authored over 160 refereed journal and conference papers, patents, textbook, and book chapters in reputed international journals, and conferences. He is serving as a technical editor in two international journals and has been part of the organizing committee of many international conferences as a symposia co-chair e.g. IEEE Globecom'16.

Tamer Khattab
received the B.Sc. and M.Sc. degrees from Cairo University, Giza, Egypt, and the Ph.D. degree from The University of British Columbia, Vancouver, BC, Canada, in 2007. From 1994 to 1999, he was with IBM wtc, Giza, Egypt. From 2000 to 2003, he was with Nokia Networks, Burnaby, BC, Canada. He joined Qatar University in 2007, where he is currently an Associate Professor of Electrical Engineering. He is also a senior member of the technical staff with Qatar Mobility Innovation Center. His research interests cover physical layer security techniques, information theoretic aspects of communication systems, and radar and RF sensing techniques.

Aiman Erbad
is an Assistant Professor at the Computer Science and Engineering (CSE) Department and the Director of Research Planning and Development at Qatar University. Dr. Erbad obtained a PhD in Computer Science from the University of British Columbia (Canada), and a Master of Computer Science in Embedded Systems and Robotics from the University of Essex (UK). Dr. Erbad received the Platinum award from H.H. The Emir Sheikh Tamim bin Hamad Al Thani at the Education Excellence Day 2013 (PhD category). Dr. Erbad research interests span cloud computing, multimedia systems and networking, and his research is published in reputed international conferences and journals.

1) RF-based drone detection is one of the most effective methods for drone detection.
2) Collect, analyze, and record RF signals of different drones under different flight statuses.
3) Design of three deep learning networks to detect and identify intruding drones.
4) The developed RF database along with our implementations are publicly available.