Received 9 October 2019; revised 6 November 2019; accepted 7 November 2019.
Date of publication 14 November 2019; date of current version 1 January 2020.

Digital Object Identifier 10.1109/OJCOMS.2019.2955889

Detection and Classification of UAVs Using RF Fingerprints in the Presence of Wi-Fi and Bluetooth Interference

MARTINS EZUMA , FATIH ERDEN, CHETHAN KUMAR ANJINAPPA , OZGUR OZDEMIR (Member, IEEE), AND ISMAIL GUVENC (Senior Member, IEEE)

Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, NC 27606, USA

CORRESPONDING AUTHOR: M. EZUMA (e-mail: mcezuma@ncsu.edu)

This work was supported in part by the National Aeronautics and Space Administration (NASA) through the Federal Award under Grant NNX17AJ94A. This paper was presented in part at the IEEE Aerospace Conference, Big Sky, Montana, March 2019 [1]. *(Martins Ezuma, Fatih Erden, and Chethan Kumar Anjinappa contributed equally to this work.)*

ABSTRACT This paper investigates the problem of detection and classification of unmanned aerial vehicles (UAVs) in the presence of wireless interference signals using a passive radio frequency (RF) surveillance system. The system uses a multistage detector to distinguish signals transmitted by a UAV controller from the background noise and interference signals. First, RF signals from any source are detected using a Markov models-based naïve Bayes decision mechanism. When the receiver operates at a signal-to-noise ratio (SNR) of 10 dB, and the threshold, which defines the states of the models, is set at a level 3.5 times the standard deviation of the preprocessed noise data, a detection accuracy of 99.8% with a false alarm rate of 2.8% is achieved. Second, signals from Wi-Fi and Bluetooth emitters, if present, are detected based on the bandwidth and modulation features of the detected RF signal. Once the input signal is identified as a UAV controller signal, it is classified using machine learning (ML) techniques. Fifteen statistical features extracted from the energy transients of the UAV controller signals are fed to neighborhood component analysis (NCA), and the three most significant features are selected. The performance of the NCA and five different ML classifiers are studied for 15 different types of UAV controllers. A classification accuracy of 98.13% is achieved by k-nearest neighbor classifier at 25 dB SNR. Classification performance is also investigated at different SNR levels and for a set of 17 UAV controllers which includes two pairs from the same UAV controller models.

INDEX TERMS Interference, machine learning, Markov models, RF fingerprinting, unmanned aerial vehicles (UAVs), UAV detection and classification.

I. INTRODUCTION

UNMANNED aerial vehicles (UAVs), or drones, are becoming ubiquitous in modern society. The recent popularity of UAVs is mainly due to the advancement in micro-electro-mechanical systems-based precision sensors, such as inertial motion units and gyroscopes, which are used for guidance, navigation, and control of UAVs. Consequently, UAVs have become relatively cheap and affordable. They are finding new applications in areas such as surveillance, smart policing, search and rescue missions, infrastructure inspections, package delivery, and precision agriculture [2]. Judging by the current trend in UAV applications, it is expected that UAVs will become an integral part of modern society. However, there are security and privacy issues associated with the ubiquity of UAVs.

In recent times, UAVs have been used in ways that introduce a threat to public safety [3]. There have been several instances where hobby drones have been used to transport illegal drugs across prison walls. In addition, drones have carried out espionage attacks which pose serious risk to public safety. Recently, drones operated by dissidents have flown into sensitive national infrastructures like nuclear reactors and airports [4]. Moreover, drones are becoming tools for cyberattack and terrorism. For instance, Wi-Fi sniffing UAVs can eavesdrop on smartphone users and steal sensitive data without being detected [5], [6].

Considering the security and privacy issues associated with UAVs, accurate detection and classification of these vehicles are vital to public safety and national security. One promising technique for UAV detection is based on the analysis of radio frequency (RF) signals from UAV controllers. In [7], drone pilots are identified by analyzing RF signals captured from the drone controllers. The pilots' behavioral biometrics can be identified from the captured signals using machine learning (ML) techniques. The ML algorithms are trained using the RF signals when the controller is handled by the legitimate owner of the device. That way, it is possible to identify different drones and their pilots. However, while the behavioral biometrics of drone pilot is an important information for drone detection, an adversary could be anyone whose behavior metrics we have no prior knowledge of. Therefore, in order to accurately detect and identify an adversary drone, one should focus on identifying the intrinsic signature of the drone controller itself. These intrinsic signatures can be extracted from the RF signals transmitted by the UAV controllers and referred to as the *RF fingerprints* of the controllers.

Since the communication signals of most commercial and hobby grade UAVs are transmitted in the same frequency band as Wi-Fi and Bluetooth transmissions, it becomes challenging to detect and identify RF signals from the UAV controllers in the presence of these interferers. Moreover, surveillance and electronic warfare systems should be able to differentiate UAVs from different manufacturers. For instance, the identity of a UAV can provide useful information about the payload, operational range, control signal characteristics (e.g., for jamming such signals), and the threat capability of the associated UAV. Accurate identification of UAVs is also important in digital forensic analysis of aerial threats.

In this work, we propose a multistage UAV detection and an ML-based classification system for identifying 17 different UAV controllers in the presence of wireless interference, i.e., Wi-Fi and Bluetooth devices. The multistage UAV detection system consists of two detectors. The first detector employs a two-state Markov model based naïve Bayes algorithm in deciding if the captured data contains RF signals or not. Once an RF signal is detected, the second stage detector decides if the signal comes from a UAV controller or an interference source. Given that the detected RF signal is from an interference source, the source class is identified as Wi-Fi or Bluetooth. On the other hand, if the detected signal is from a UAV controller, the signal is transferred to the ML-based classification system to determine the make and model of the UAV controller. In an earlier work [1], the authors proposed a system for detecting and classifying 14 different UAV controllers. The system design assumes the absence of interference signals. However, this assumption is not always correct. The contributions of the current work are summarized as follows.

1) The paper investigates the problem of detecting and classifying signals from UAV controllers in the presence of co-channel wireless interference. We consider interference from Wi-Fi and Bluetooth sources and describe a methodology to detect the UAVs. The interference detection ensures the proposed UAV detection system is robust against false alarms and missed target detection. In addition, in [1], we used two fixed thresholds, positioned at $\pm 3\sigma$, to transform the captured signal into three-state Markov models, where σ is the standard deviation of the noise signal in the environment. However, in the current work, we use a single threshold to transform the captured signal into two-state Markov models, which reduces overall complexity. We also define a procedure to determine the optimum threshold value based on the available training data. It turns out that better detection accuracy can be achieved when a single but properly selected threshold is used to generate the Markov models. At an SNR of 10 dB, the current work achieves a detection accuracy of 99.8% using a threshold that is 3.5 times the standard deviation. However, in [1], the detection accuracy is 84% under the same SNR condition. Besides, in the current study, we evaluate the detection performance for different thresholds based on the false alarm rate (FAR).
2) We introduce the concept of *energy transient* for the extraction of RF-based features and show how effective it is for the classification of the UAV controller signals. The energy transient is computed using the representation of the RF signals in energy-time-frequency domain. From the energy transient, 15 statistical features are extracted for the UAV classification. The performance of five different ML algorithms are compared using the proposed RF fingerprinting technique. In addition, we investigate the neighborhood component analysis (NCA) as a practical algorithm for feature selection in the classification problem. The classification results using the three most significant features, selected by the NCA, are compared with those when all the 15 RF features are used. We also evaluate the classification performance at different signal-to-noise ratios (SNRs). For an SNR of 25 dB, the results show that the k-nearest neighbor (kNN) and random forest (RandF) machine learning algorithms are the best performing classifiers, achieving accuracy of 98.13% and 97.73%, respectively, when the three most significant RF-based features are used for the classification of 15 UAV controllers. In comparison, the kNN classifier achieves an accuracy of 96.3% when used to classify 14 UAV controllers [1]. Furthermore, in the current work, for the case of 15 UAV controllers, DA and NN classifiers achieve an average accuracy of 94.43% and 96.13%, respectively. However, in [1], DA and NN achieve an average accuracy of 88.15% and 58.49%, respectively, when used to classify 14 UAV controllers.

3) We study the confusion that results when attempting to classify UAV controllers of the same make and model. This is important in digital forensic analysis and detecting decoys in surveillance systems. To investigate this confusion, we included two pairs of identical UAV controllers to a pool of 13 different UAV controllers. That is, we capture control signals from 17 UAV controllers and evaluate the ability of the proposed classification system at different SNRs. For an SNR of 25 dB, kNN and RandF achieve accuracy of 95.53% and 95.18%, respectively, when the three most significant RF features are used. To the best of our knowledge, past studies on UAV classification using RF techniques considers only a limited number of different make and model UAV controllers, often less than 10 [8], [9].

The remainder of the paper is organized as follows: Section II provides a brief overview of the related work. Section III describes the multistage detection system, and Section IV introduces the methodology to detect Wi-Fi and Bluetooth interference signals. Feature extraction and the RF fingerprinting-based UAV classification system are explained in Section V. The experimental setup and data capture technique is described in Section VI while the detection and classification results are presented in Section VII. The paper is concluded in Section VIII.

II. RELATED WORK

UAV detection and classification through RF signals can be grouped into two major headings: RF physical layer features-based and RF medium access control (MAC) layer features-based techniques. In general, these techniques use an RF sensing device to capture the RF communication signal between a UAV and its controller.

A. RF PHYSICAL LAYER FEATURES-BASED TECHNIQUES

Most of the techniques classified within this category rely on the physical layer characteristics of the RF transmission from a UAV to its controller (or vice versa), such as the amplitude envelope or the spectrum of the RF signal. These techniques are sometimes referred to as RF fingerprinting techniques because they utilize the unique characteristics of the RF signals for the detection and classification of the UAVs. Experimental investigations show that most of the commercial UAVs have unique RF signatures which is due to the circuitry design and modulation techniques employed. Therefore, RF fingerprints extracted from the UAV or its remote controller signals can be used as a basis for the detection and classification of the UAVs.

In [10], RF fingerprints of the UAV's wireless control signals are extracted by computing the amplitude envelope of the signal. The dimensionality of the processed signal is reduced by performing principal component analysis (PCA), and the lower-dimensional data is fed into an auxiliary classifier Wasserstein generative adversarial networks (AC-WGANs). The AC-WGANs achieves an overall classification rate of 95% when four different types of UAVs are considered.

In [11], drones are detected by analyzing the RF background activities along with the RF signals emitted when the drones are operated in different modes. Afterward, RF spectrum of the drone signal is computed using the discrete Fourier transform (DFT). The drone classification system is designed by training a deep neural network with the RF spectrum data of different drones. The system shows an accuracy of 99.7% when two drones are classified, 84.5% with four drones, and 46.8% with ten drones.

In [12], an industry integrated counter-drone solution is described. The solution is based on a network of distributed RF sensors. In this system, RF signals from different UAV controllers are detected using an energy detector. Afterward, the signals of interest are classified using RF spectral shape correlation features. Besides, distributed RF sensors make it possible to localize the UAV controller using time difference of arrival (TDoA) or multilateration techniques. However, this industrial solution is quite expensive.

B. RF MAC LAYER FEATURES-BASED TECHNIQUES

There are many UAVs that use Wi-Fi protocol for video streaming and control. The techniques categorized under this heading use MAC layer features, such as packet statistics, for detection and classification of the Wi-Fi controlled UAVs. These techniques are sometimes referred to as Wi-Fi fingerprinting techniques. Thus, the RF detection system consists primarily of a Wi-Fi packet-sniffing device, which can intercept the Wi-Fi data traffic between a UAV and its remote controller. In [9], unauthorized Wi-Fi controlled UAVs are detected by a patrolling drone using a set of Wi-Fi statistical features. The extracted features include MAC addresses, root-mean-square (RMS) of the Wi-Fi packet length, packet duration, average packet inter-arrival time, among others. These features are used to train different ML algorithms which perform the UAV classification task. In [9], the random tree and random forest classifiers achieve the best performance as measured by the true positive and false positive rates.

In [13], drone presence is detected by eavesdropping on Wi-Fi channels between the drone and its controller. The system detects drones by analyzing the impact of their unique vibration and body shifting motions on the Wi-Fi signals transmitted by the drone. The system achieves accuracy above 90% at 50 meters.

In general, a major concern with the Wi-Fi fingerprinting techniques is the privacy. This is because the same Wi-Fi detection system can spoof Wi-Fi traffic data from a smartphone user or a private Wi-Fi network. In addition, only a limited number of commercial drones employ Wi-Fi links for video streaming and control. Most commercial drones use proprietary communication links.

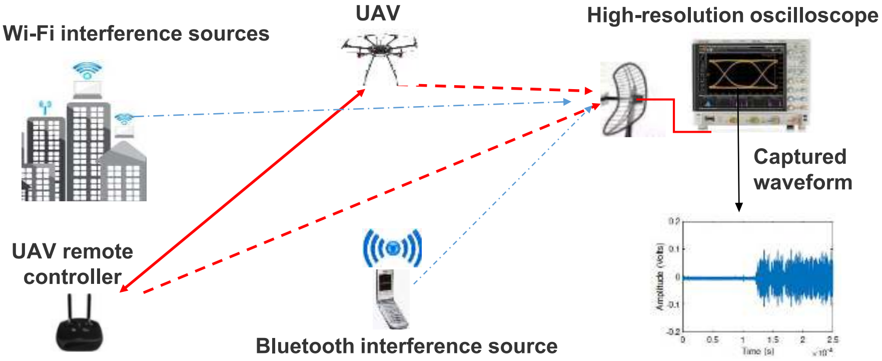


FIGURE 1. The scenario of the RF-based UAV detection system. The passive RF surveillance system listens for the signal transmitted between the controller and the UAV. The environment contains signals from Wi-Fi and Bluetooth interference devices which operate in the same frequency band with the UAV and its remote controller.

Besides RF and Wi-Fi fingerprinting techniques, several other techniques have been investigated for UAV detection, including radar-based techniques, acoustic techniques, and computer vision techniques [14]. However, as discussed in [14], traditional radar systems are not so effective in detecting UAVs with small radar cross sections, and acoustic and computer vision-based techniques are greatly impaired by ambient environmental conditions. In contrast, RF techniques are not limited by these problems. We start by describing the design of the multistage detector of our proposed RF-based system.

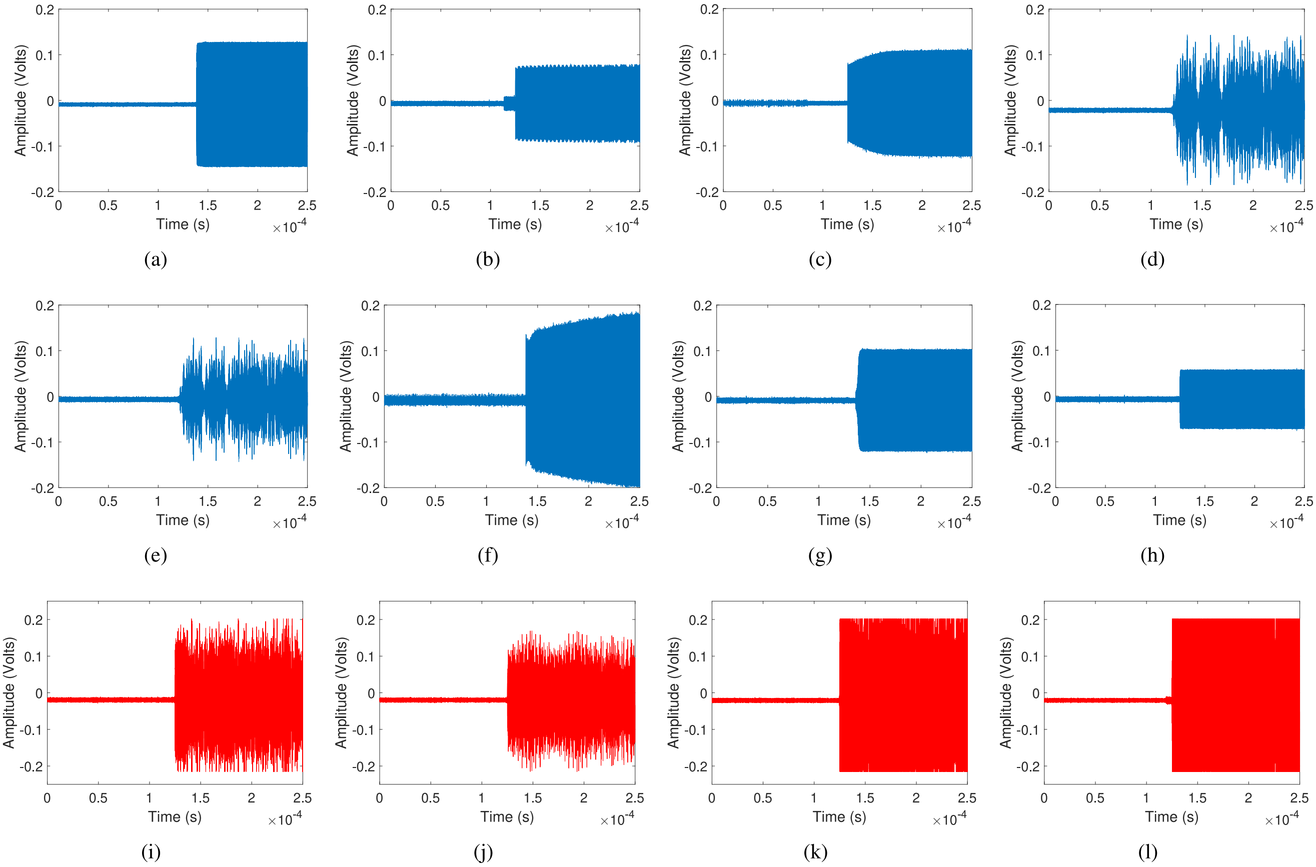
III. MULTISTAGE UAV SIGNAL DETECTION

We consider the scenario shown in Fig. 1, where a passive RF surveillance system listens for the control signals transmitted between a UAV and its remote controller. The main hardware components of the surveillance system are 2.4 GHz RF antenna and a high-frequency oscilloscope, which is capable of sampling the captured data at 20 GSa/s. Instead of an oscilloscope, a standard software-defined radio like the universal software radio peripheral (USRP) can also be used for data capture. In order to avoid aliasing, the data capture device should be able to sample the captured data above the Nyquist rate. In this study, since we are interested in capturing RF data in the 2.4 GHz band, the data capture device should be able to sample at a rate of at least 5 MSa/s. Besides, if the RF surveillance system is passive as described in Fig. 1, then it increases the stealth attribute of the detection system. This implies, the system shown in Fig. 1 can detect an adversary UAV while itself remaining undetected by the UAV. This stealth attribute is vital in electronic warfare environments where low probability of intercept (LPI) emitters are very valuable. Furthermore, the passive RF detection system has an advantage over a radar system in terms of the maximum detection range. This is because why a radar would have to transmit pulses and listen for the backscattering (echo) from the target, the passive RF detector only needs to listen for the signals from the target.

Since most commercial UAVs operate in the 2.4 GHz band, the passive RF surveillance system is designed to operate in this frequency band. However, this also corresponds to the operational band of Wi-Fi and mobile Bluetooth devices. Therefore, in real wireless environment, signals from these wireless sources will act as interference to the detection of the UAV control signals. Also, in such real environment, the presence of noise may further reduce the chance of correctly detecting the UAV signals when present.

Given the scenario in Fig. 1, the passive RF surveillance system has to decide if the captured data comes from a UAV controller, an interference source, or background noise. In the case where the captured data comes from a UAV controller, the detection system should be able to correctly classify the UAV controller. However, if the detected signal is from an interference source, the detection system should be able to correctly identify the source, i.e., a Wi-Fi or a Bluetooth device. Therefore, the detection problem is a multi-hypothesis problem. For such problems, it is well known that computational complexity increases as the number of hypothesis increases. Consequently, the multi-hypothesis detection problem can be simplified by using a multistage sequential detector. In this system, each detection stage is a simple binary hypothesis test which is much easier to solve.

Fig. 2 illustrates sample RF signals captured from eight different UAV controllers and four different UAVs (on flight). The figure shows each signal has different characteristics, which can be exploited for identifying the source UAV controller. The flowchart in Fig. 3 provides a high-level graphical description of the entire system. The first step in detecting and identifying a UAV controller is data capture. Usually, the captured raw signal has a large size and is often very noisy. Therefore, before detection and classification, the signals are first pre-processed using multiresolution analysis. Next, the processed signals are transferred to the multistage detection system, which consists of two stages. In the first stage, the detector employs naïve Bayesian hypothesis test in deciding if the captured signal is an RF signal or noise. If the decision is positive, the second stage detector is activated to decide if the captured RF signal comes from an interference source or a UAV controller. This detector uses bandwidth analysis



(a) (b) (c) (d)

(e) (f) (g) (h)

(i) (j) (k) (l)

FIGURE 2. RF signals captured from eight different UAV controllers and four different UAVs while on flight: (a) Graupner MC-32, (b) Spektrum DX6e, (c) Futaba T8FG, (d) DJI Phantom 4 Pro, (e) DJI Inspire 1 Pro, (f) JR X9303, (g) Jeti Duplex DC-16, (h) FlySky FS-T6, (i) DJI Matrice 600 UAV, (j) DJI Phantom 4 Pro UAV, (k) DJI Inspire 1 Pro UAV, (l) DJI Mavic Pro.

and modulation-based features for interference detection. If the detected RF signal is not from a Wi-Fi or Bluetooth interference source, it is presumed to be a signal transmitted by a UAV controller. Consequently, the detected signal is transferred to an ML-based classification system for accurate identification of the UAV controller.

A. PRE-PROCESSING STEP: MULTIRESOLUTION ANALYSIS

Captured RF data are pre-processed by means of wavelet-based multiresolution analysis. It has been established that multiresolution decomposition using discrete wavelet transform (DWT) like the Haar wavelet transform is effective for analyzing the information content of signals and images [15].

In this work, multiresolution decomposition of the captured RF data are carried out using the two-level Haar transform as shown in Fig. 4. Using this transform, the raw input signal is decomposed into subbands, and important time-frequency information can be extracted at different resolution levels [16]. In the first level, the input RF data are split into low- and high-frequency components by means of the half band low-pass ($h[n]$) and high-pass ($g[n]$) filters, respectively. This process is followed by a dyadic decimation, or downsampling, of the filter outputs to produce the approximate coefficients, $a_1[n]$, and detail coefficients, $d_1[n]$. In the second level, $a_1[n]$ coefficients are further decomposed in a similar manner, and the generated $d_2[n]$ coefficients are taken as the final output ($y_{\mathrm{T}}[n]$). Then, $y_{\mathrm{T}}[n]$ is input to the multistage detection system. Moving from left to right in Fig. 4, we get coarser representation of the captured RF data. The output RF data will have fewer samples due to the successive downsampling of the input RF data. This reduces the computational complexity of the overall process. Multiresolution analysis is also useful in detecting weak signals in the presence of background noise and removing the bias in the signals, leading to a higher detection accuracy, which is required in applications like UAV threat detection.

Fig. 5 shows the effect of the Haar wavelet decomposition on a sample signal captured from the controller of the DJI Phantom 4 Pro UAV. It is clear from the figure that the wavelet transform removes the bias in the signal alignment and reduces the data size. It will be shown in Section V, the transformation also preserves the characteristics of the original waveform. After the pre-processing step, the data is transferred to the first stage of the detection system, where we decide if the captured data is an RF signal or noise.

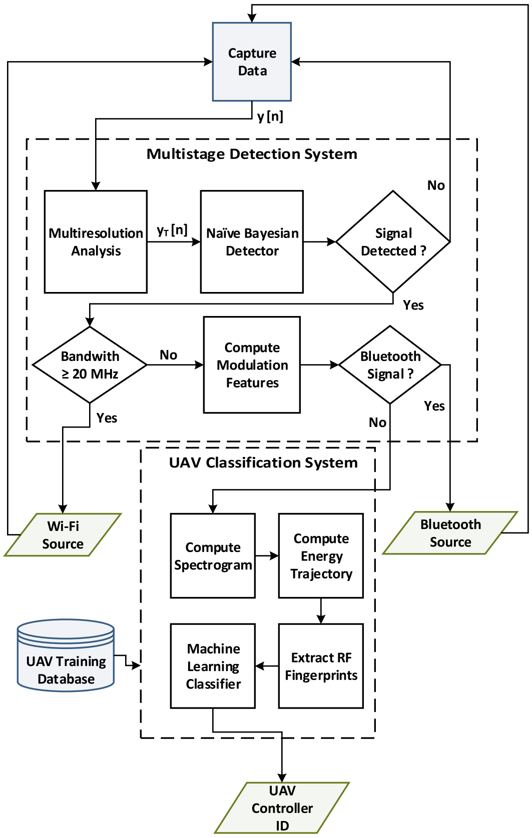


FIGURE 3. The system flowchart providing a graphical description of information processing and flow of data through the system.

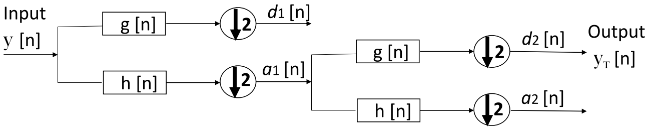
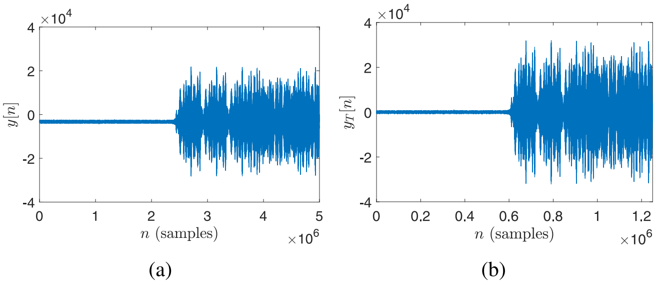


FIGURE 4. The two-level discrete Haar wavelet transform for pre-processing of the captured raw data.



(a)

(b)

FIGURE 5. (a) The sampled raw data *y*[*n*] captured from the remote controller of a DJI Phantom 4 Pro UAV using an oscilloscope with a sampling rate of 20 GSa/s, and (b) the transformed data $y_T[n]$ obtained at the output of the two-level Haar wavelet filter. Due to successive downsampling, $y_T[n]$ has about 3.8 × 10^6 fewer data samples than *y*[*n*].

B. NAÏVE BAYES DECISION MECHANISM FOR RF SIGNAL DETECTION

In this stage, we first model the pre-processed RF data, $y_T[n]$, using two-state Markov models for "RF signal" and "noise" classes. This allows us to compute the likelihood that the captured data come from either the signal or noise class. According to the Bayesian decision theory, the optimum detector is the one that maximizes the posterior probability. Mathematically, let $C \in \{0, 1\}$ be an index denoting the class of the pre-processed RF data $y_T[n]$, where $C = 1$ when the captured raw signal $y[n]$ is an RF signal, and $C = 0$ otherwise. Let $S_{y_T} = [S_{y_T}(1), S_{y_T}(2), \dots, S_{y_T}(N)]^\top$ be the state vector representation of the given test data $y_T[n]$ containing N samples, with $S_{y_T}(i) \in \{S_1, S_2\}$, $i = 1, 2, \dots, N$, and S_1 and S_2 being the two states in the Markov models. Then, the posterior probability of the RF signal class given S_{y_T} is

$$P\big(C = 1|S_{y_T}\big) = \frac{P\big(S_{y_T}|C = 1\big)P(C = 1)}{P\big(S_{y_T}\big)}, \tag{1}$$

where $P(S_{y_T}|C = 1)$ is the likelihood function conditioned on $C = 1$, $P(C = 1)$ is the prior probability of the RF signal class, and $P(S_{y_T})$ is the evidence. A similar expression holds for the posterior probability $P(C = 0|S_{y_T})$. In practice, since the evidence is not a function of C, it can be ignored. Therefore, we are only interested in maximizing the numerator in (1). That is,

$$\widehat{C} = \arg\max_{C} P\big(S_{y_T}|C\big)P(C). \tag{2}$$

We decide that the captured signal belongs to an RF signal (i.e., $C = 1$), if

$$P\big(S_{y_T}|C = 1\big)P(C = 1) \geq P\big(S_{y_T}|C = 0\big)P(C = 0). \tag{3}$$

For the detection experiment, we collected an equal number of RF and noise signals. Therefore, it is rational to assume the prior probabilities of the RF signal and noise classes are equal, then the decision rule in (3) reduces to

$$P\big(S_{y_T}|C = 1\big) \geq P\big(S_{y_T}|C = 0\big). \tag{4}$$

Therefore, for a given test data, we need to compute and compare the likelihood probabilities $P(S_{y_T}|C = \{0, 1\})$. First, in order to compute the likelihood probability for the RF signal and noise classes, we use large amount of training data captured from multiple UAV controllers, Wi-Fi routers, mobile Bluetooth emitters, and background noise. This training data set is stored in a database as shown in Fig. 3. Since the captured RF data (after sampling) is a discrete time-varying waveform, we can model it as a stochastic sequence of states/events. The likelihood probability of such a state sequence can be computed based on the transitions between the states of the generated Markov models.

A two-state Markov model for a given signal $y_T[n]$ can be generated by mapping each sample in the signal to one of the two states (S_1 and S_2). The samples whose absolute amplitudes are less than or equal to a predetermined threshold δ are considered as in state S_1, while the samples with absolute amplitude greater than δ are considered as in state S_2. Mathematically, the state transformation is performed as follows:

$$S_{y_T}(n) = \begin{cases} S_1, & |y_T[n]| \leq \delta \\ S_2, & |y_T[n]| > \delta. \end{cases} \tag{5}$$

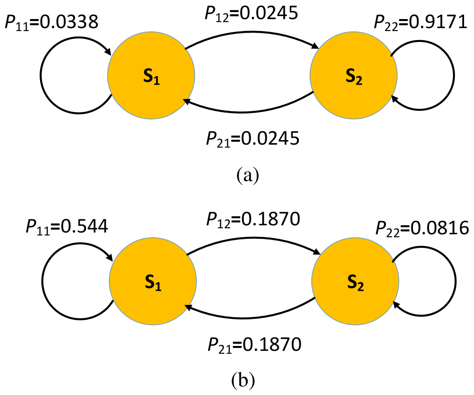


FIGURE 6. Two-state Markov model and associated state transition probabilities using $\delta = 3.5\sigma$ for (a) the RF signal class, and (b) the noise class.

Based on the above rule, it is straightforward to transform $y_T[n]$ into the state vector, S_{y_T}. Once S_{y_T} is obtained, the probability of a transition between any two states is calculated. Note that the state vector is generated based on the amplitude of the signal samples in the wavelet domain. The choice of δ in (5) depends on the operating SNR of the system and will be discussed in Section VII-A. The transition count matrix, $\boldsymbol{T}_N$, and the transition probability matrix, $\boldsymbol{T}_P$, are defined as follows:

$$\boldsymbol{T}_N = \begin{bmatrix} N_{11} & N_{12} \\ N_{21} & N_{22} \end{bmatrix}, \boldsymbol{T}_P = \begin{bmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{bmatrix} = \frac{\boldsymbol{T}_N}{\sum_{i,j} N_{ij}}, \quad (6)$$

respectively, where N_{ij} is the number of transitions from state S_i to S_j among all samples of $y_T[n]$, and $p_{ij} = P(S_i \rightarrow S_j)$ is the probability of a transition from state S_i to S_j. The matrix $\boldsymbol{T}_P$ is obtained by normalizing the $\boldsymbol{T}_N$ matrix with the total number of samples in the signal. It is expected that the transition probabilities generated for the signal class (UAV, Wi-Fi, and Bluetooth) and the noise class will be significantly different at modest SNR levels. Also, the choice of δ in (5) dictates the transition probabilities for both the signal and noise class. In Section VII-A, the threshold δ is expressed in terms of the estimated standard deviation (σ) of the preprocessed noise data captured from the environment. Moreover, during the experiments, data is captured within a short time window (0.25 ms), thus we assume the environmental noise is stationary during this interval.

Fig. 6 shows the two-state Markov models for the RF signal and noise classes obtained from the training data using $\delta = 3.5\sigma$. From Fig. 6(a), we see that for the signal class, p_{22} is significantly higher than p_{11}, p_{12}, and p_{21}. On the other hand, from Fig. 6(b), we see that for the noise class, p_{11} is significantly higher than the other transition probabilities. Based on these observations, the differences between the state transition probabilities of each class can be utilized to determine the class of a captured test signal.

Consequently, the likelihood of the test signal being an RF signal can be calculated as follows:

$$\begin{aligned} P\big(S_{y_T}|C=1\big) &= \prod_{n=1}^{N-1} p\big(S_{y_T}(n) \rightarrow S_{y_T}(n+1)|C=1\big) \\ &= \prod_{i,j=\{1,2\}} \boldsymbol{T}_{P_{C=1}}^{\boldsymbol{T}_N(i,j)}(i,j) \\ &= \prod_{i,j=\{1,2\}} p_{ij;C=1}^{N_{ij}}. \end{aligned} \quad (7)$$

The product of the conditional transition probabilities in the above equation gives the likelihood of obtaining the state vector S_{y_T} given the hypothesis $C = 1$ is true. The log-likelihood of the above expression is:

$$\log\big(P\big(S_{y_T}|C=1\big)\big) = \sum_{i,j=\{1,2\}} N_{ij} \log\big(p_{ij;C=1}\big). \quad (8)$$

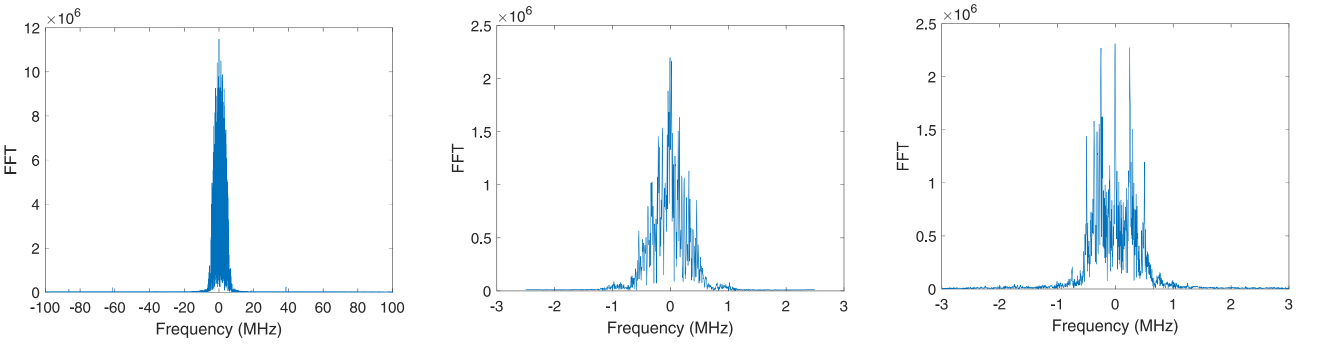
Similarly, the log-likelihood of the signal coming from a noise class is calculated by

$$\log\big(P\big(S_{y_T}|C=0\big)\big) = \sum_{i,j=\{1,2\}} N_{ij} \log\big(p_{ij;C=0}\big). \quad (9)$$

The decision will be favored to $C = 1$, if $\log(P(S_{y_T}|C = 1)) \geq \log(P(S_{y_T}|C = 0))$; otherwise, $C = 0$. We discuss the detection results in Section VII-A. If the captured test signal belongs to the RF signal class, then the second stage detector is invoked to identify UAV controller-type signals. Otherwise, the system continues sensing the environment for the presence of signals as shown in Fig. 3.

IV. DETECTION OF WI-FI AND BLUETOOTH INTERFERENCE

In recent times, there has been interest in detecting Wi-Fi and Bluetooth signals [17]. In [18], a new technique is proposed for classifying Wi-Fi and Bluetooth interference signals in the 2.4 GHz band. The technique uses the Hidden Markov Model (HMM) to model sequences or periodicity in the captured signal. The expectation-maximization (EM) algorithm is used to learn the parameters of the HMM models. The proposed system achieved accuracy above 88%. The major drawback is the fact that the EM algorithm often converges to a local maximum. Therefore, the EM algorithm might fail in computing a consistent estimate of the parameters of the model. Besides, in the context of RF-based UAV detection in urban environments, where the Wi-Fi and Bluetooth signals are considered as interference, there has been minimal research efforts. Fortunately, these interference signals are well standardized and can be identified by using the knowledge of their specifications. Table 1 provides a brief summary of the specifications for Wi-Fi and Bluetooth transmissions. It is obvious that the signal bandwidth and the modulation type are two important features for identifying the Wi-Fi and Bluetooth signals. The second stage detector exploits these features for detecting these interference sources.



(a) (b) (c)

FIGURE 7. Bandwidth analysis of (a) Wi-Fi signal, (b) Bluetooth signal from Motorola e5 cruise, and (c) Spektrum DX5e UAV controller signal.

TABLE 1. Specifications of the Wi-Fi and Bluetooth standards.

Standard	Bluetooth (IEEE 802.15.1 WPAN)	Wi-Fi (IEEE 802.11 WLAN)
Center frequency (GHz)	2.4	2.4/ 5
Bandwidth (MHz)	1	20/ 40/ 80/ 160
PHY modulation [20], [21]	GFSK/FSK/DPSK	DSSS/ OFDM
Range (m)	variable	>50
Data rate (Mbps)	2	variable

The first step in deciding if the detected signal is a wireless interference or not is to perform bandwidth analysis. This is because Wi-Fi signals can be easily identified by their bandwidth. According to Table 1, Bluetooth 2.0 signals have a bandwidth of 1 or 2 MHz, Wi-Fi signals have a bandwidth of 20 MHz (or more) while all the UAV controller signals in our database have bandwidth less than 10 MHz. Therefore, if the detected RF signal has a bandwidth equal or greater than 20 MHz, it is classified as a Wi-Fi signal. Bandwidth analysis is performed by taking the Fourier transform of the resampled signal. Fig. 7 shows the result of the bandwidth analysis of a typical Wi-Fi, a Bluetooth (from Motorola e5 cruise), and a UAV (Spektrum DX5e) controller signal.

If the detected signal has a bandwidth less than 20 MHz, it is assumed to be transmitted either from a Bluetooth interference source or a valid UAV controller. Since most mobile Bluetooth devices employ Gaussian frequency shift keying GFSK/FSK modulation, it is reasonable to detect and discriminate these devices by means of modulation features. In this study, two GFSK/FSK modulation features, namely, frequency deviation and symbol duration, will be used to discriminate Bluetooth signals. Frequency deviation is a measure of the maximum difference between the peak frequency in the GFSK/FSK signal and the center frequency. On the other hand, symbol duration is the minimum time interval in the observed Bluetooth waveform or pulse. Therefore, using a GFSK/FSK demodulator, these features can be extracted and used as the basis for Bluetooth signal detection.

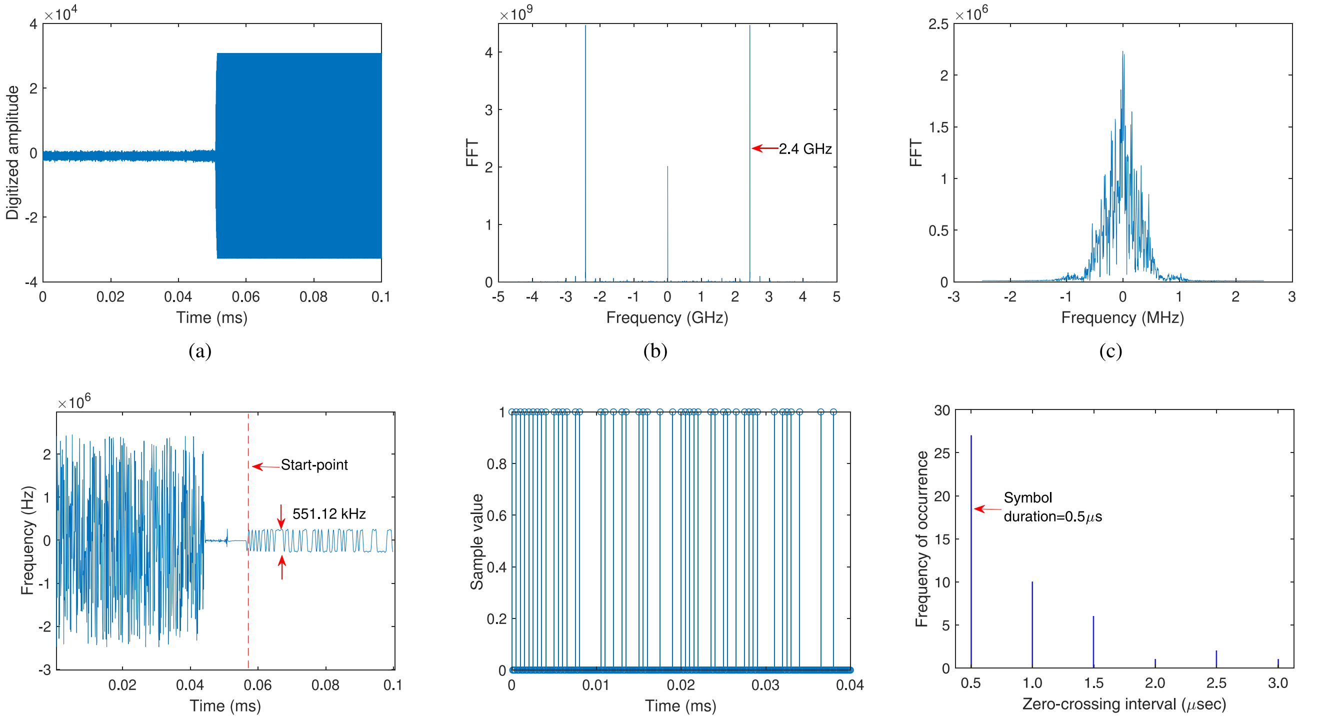
We consider a zero-crossing GFSK/FSK demodulator. It is known that the Bluetooth GFSK/FSK signal is transmitted in burst consisting of M data bits $d_m \in \{-1, +1\}$, each bit having a period T_b and average energy per bit E_b [19]. A general model for such a signal is given as:

$$s(t) = \sqrt{\frac{2E_b}{T_b}}.\cos(2\pi f_o t + \varphi(t, \alpha) + \varphi_o) + n(t), \quad (10)$$

where $\varphi(t, \alpha)$ is a phase modulating function, φ_o is an arbitrary phase constant, f_o is the operational frequency, and $n(t)$ is the channel noise component. The zero-crossing demodulator considered herein for Bluetooth interference detection is able to detect the time instants at which the signal $s(t)$ is equal to zero and has a positive slope, i.e., the zero-crossings. When a Bluetooth device transmits at the basic rate using the standard GFSK/FSK modulation, one symbol represents one bit. Therefore, the time interval between consecutive zero-crossings is a measure of the symbol duration of the Bluetooth signal.

Fig. 8 shows the results of the zero-crossing demodulation of a Bluetooth signal from Motorola e5 cruise. The captured Bluetooth signal and its fast Fourier transform (FFT) are shown in Fig. 8(a) and Fig. 8(b), respectively. From Fig. 8(b), we see that the transmit frequency of the Bluetooth device is 2.4 GHz. Afterward, the signal is shifted and resampled by 1/2000. The FFT of the resampled signal is shown in Fig. 8(c). This figure shows that the bandwidth of the Bluetooth signal is around 2 MHz, which is far less than 20 MHz. Next, the resampled signal is demodulated by taking the derivative of its phase angle, and the start point of the demodulated signal is estimated using the Higuchi algorithm [22]. The Higuchi algorithm detects the start point of the signal by measuring the fractal dimensions of the signal. Once the start point is detected, the frequency deviation is estimated as one half the peak-to-peak frequency of the demodulated signal. Fig. 8(d) shows a plot of the demodulated signal and the estimated start point which is obtained using the Higuchi algorithm. From the figure, the peak to peak frequency of the demodulated signal is estimated as 551.12 kHz, and therefore, the frequency deviation is 275.56 kHz.

In order to estimate the symbol duration, the demodulated signal is converted to a binary signal by using the mean as a threshold. Fig. 8(e) shows the binary signal,



(a) (b) (c)

(d) (e) (f)

FIGURE 8. Extraction of the modulation features of a Bluetooth interference signal from Motorola e5 cruise mobile device using zero-crossing demodulation technique: (a) Raw signal, (b) FFT of the raw signal, (c) FFT of the shifted and resampled signal (by 1/2000), (d) the demodulated signal showing a peak-to-peak frequency of 551.12 kHz, (e) binary signal, and (f) histogram of the time-interval between consecutive zero-crossings in the modulated signal.

where binary one represents a positive frequency deviation, and a binary zero represents a negative frequency deviation. Then, we compute the derivative of the binary signals to locate the zero-crossings. To ensure we accurately compute the symbol duration, we compute the histogram of the time intervals between consecutive zero-crossings. This is necessary because channel distortions will cause some deviation in these intervals. Fig. 8(f) shows the histogram of the time intervals between consecutive zero-crossings for the Bluetooth signal. The estimated symbol duration is 0.5 μs. To validate the joint discriminating ability of these modulation features, Bluetooth signals from six mobile phones and signals from nine UAV controllers are collected. The mobile phones are Iphone 7, Iphone XR, LG X charge, Motorola G Play, Motorola e5 cruise, and Samsung Galaxy Note 9. The UAV controllers considered are Jeti Duplex DC-16, Spektrum DX5e, Spektrum DX6e, Spektrum DX6i, Spektrum JR X9303, FlySky FS-T6, Graupner MC-32, HK-T6A, and Turnigy 9X. The UAV signals are frequency modulated as well. Therefore, all the collected signals are demodulated using the zero-crossing technique. Fig. 9 shows the feature space of the demodulated Bluetooth and UAV controller signals. The figure shows a clear clustering of the Bluetooth signals from different mobile phones. All the Bluetooth signals have a symbol duration of 0.5μs and a frequency deviation of less than 350 kHz. Therefore, the frequency deviation and symbol duration can be used as features in a simple maximum likelihood classifier for identifying Bluetooth interference signals. If the detected signal is not from a Bluetooth interference source, it is presumed to be an emission from a UAV controller and transferred to the UAV classification system.

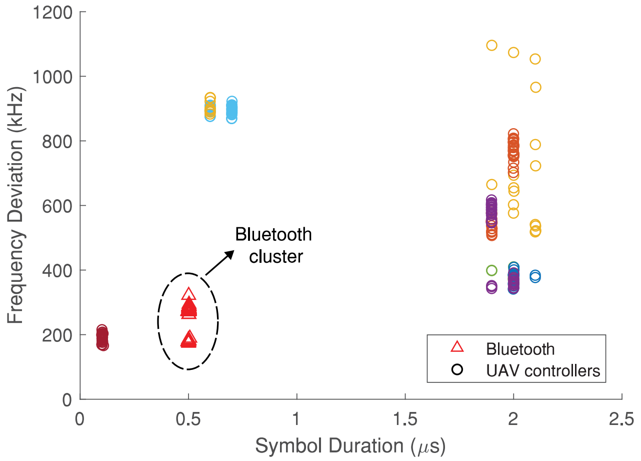


FIGURE 9. Feature space showing the symbol duration and frequency deviation of the signals from several mobile Bluetooth devices and UAV controllers. Each UAV controller is represented by a circular marker of a unique color.

V. UAV CLASSIFICATION USING RF FINGERPRINTS

The input to the ML classifiers are the RF-based features extracted from the energy-time-frequency domain representation of the UAV controller signals. For this representation,

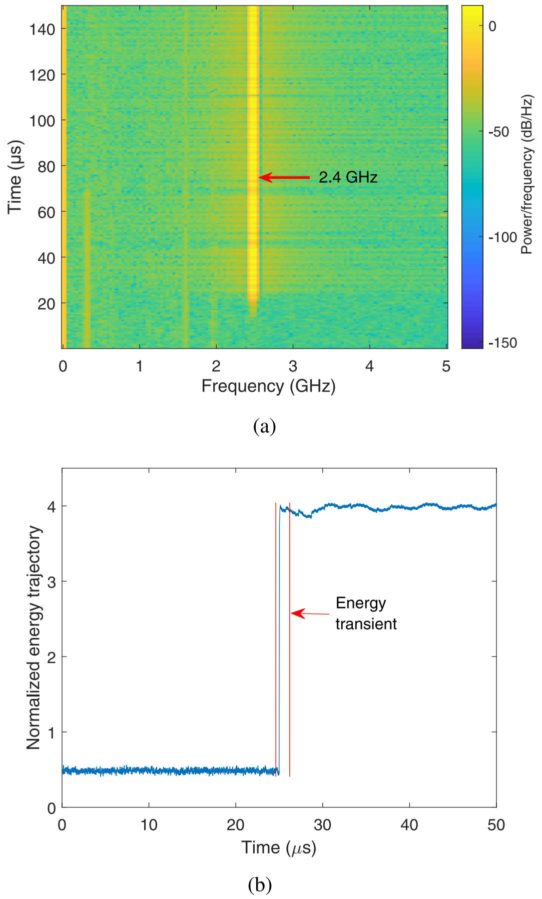


FIGURE 10. (a) The spectrogram and, (b) the energy trajectory of the UAV controller signal shown in Fig. 5.

we use the spectrogram method. The spectrogram of any signal is computed using the squared magnitude of the discrete time short-time Fourier transform (STFT)

$$\text{Spectrogram}(m, \omega) = \left| \sum_{k=-\infty}^{\infty} y_{\mathrm{T}}[k] \mathrm{w}[k-m] e^{-j\omega k} \right|^2, \quad (11)$$

where $y_{\mathrm{T}}[n]$ is the pre-processed signal captured by the surveillance system, m is discrete time, ω is the frequency, and w[n] is a sliding window function that acts as a filter. The spectrogram analysis of the captured RF signals can reveal the transmit frequency of the signal as well as the frequency hopping patterns. Fig. 10(a) shows the spectrogram of the signal captured from the remote controller of the DJI Phantom 4 Pro UAV (the signal in Fig. 5). In computing the spectrogram, the signal is divided into segments of length 128 with an overlap of 120 samples between adjoining segments. Then, a Hamming window is used, followed by a 256-point DFT. The spectrogram shows that the transmit frequency of the signal is 2.4 GHz.

The spectrogram displays the energy distribution of the signal along the time-frequency axis. Therefore, the energy trajectory can be computed from the spectrogram by taking the maximum energy values along the time-axis. From this distribution, we estimate the energy transient by searching for the most abrupt change in the mean or variance of the normalized energy trajectory. The term *transient* is defined as a sudden change in the waveform of the signal which could be due to modulation in amplitude, frequency or phase. A transient contains unique information of the signal and can be exploited in classification tasks. Accurate detection of the start point of time-domain transients is critical and highly dependent on the environmental noise level. If the SNR is considerably low, transient start point may not be detected properly and this may result in extracting features that do not represent the signal. Due to this problem, we propose to use energy transient by using an analogy between the transients in the time-domain and energy-time-frequency domain. For the RF signal in Fig. 5, the normalized energy trajectory and the corresponding energy transient are shown in Fig. 10(b).

TABLE 2. Statistical features.

Features	Formula	Measures
Mean (μ)	$\frac{1}{N}\sum_{i=1}^{N} x_i$	Central tendency
Absolute mean ($\bar{x}$)	$\frac{1}{N}\sum_{i=1}^{N} \lvert x_i \rvert$	Central tendency
Standard deviation(σ_T)	$\left[\frac{1}{N-1}\sum_{i=1}^{N}(x_i-\bar{x})^2\right]^{\frac{1}{2}}$	Dispersion
Skewness (γ)	$\frac{\sum_{i=1}^{N}(x_i-\bar{x})^3}{(N-1)\sigma_T^3}$	Asymmetry/shape descriptor
Entropy (H)	$-\sum_{i=1}^{N} x_i \log_2 x_i$	Uncertainty
Root mean square (x_{rms})	$\left[\frac{1}{N}\sum_{i=1}^{N} x_i^2\right]^{\frac{1}{2}}$	Magnitude/Average power
Root (x_{r})	$\left[\frac{1}{N}\sum_{i=1}^{N} \lvert x_i \rvert^{\frac{1}{2}}\right]^2$	Magnitude
Kurtosis (k)	$\frac{\sum_{i=1}^{N}(x_i-\bar{x})^4}{(N-1)\sigma_T^4}$	Tail/shape descriptor
Variance	$\frac{1}{N}\sum_{i=1}^{N}(x_i-\mu)^2$	Dispersion
Peak value (x_{pv})	$\max(\mathrm{x_i})$	Amplitude
Peak to peak (x_{ppv})	$\max(\mathrm{x_i}) - \min(\mathrm{x_i})$	Waveform amplitude
Shape factor(x_{sf})	$\frac{x_{\mathrm{rms}}}{\bar{x}}$	Shape descriptor
Crest factor	$\frac{x_{\mathrm{max}}}{x_{\mathrm{rms}}}$	Peak extremity
Impulse factor	$\frac{x_{\mathrm{max}}}{\bar{x}}$	Impulse
Clearance factor	$\frac{x_{\mathrm{max}}}{x_{\mathrm{r}}}$	Spikiness

Once the energy transient is detected, RF fingerprints (a set of 15 statistical features) are extracted. Each feature is a physical descriptor of the energy transients and can provide valuable information for ML-based classification of the signals captured from different UAV controllers. Table 2 gives the list of the extracted features used in this study. The features extracted from 17 UAV controllers are used to train five different ML algorithms: kNN, RandF, discriminant analysis (DA), support vector machine (SVM), and neural networks (NN). Since some of the features may be correlated, therefore redundant, we also perform feature selection to reduce the computational cost of the classification algorithm.

A. FEATURE SELECTION USING NCA

The NCA algorithm is a nearest neighbor-based feature weighting algorithm, which learns a feature weighting vector by maximizing a leave-one-out classification accuracy using a gradient based optimizer. It is a non-parametric, embedded, and supervised learning method for feature selection. NCA learns the weighting vector/matrix by which the primary data

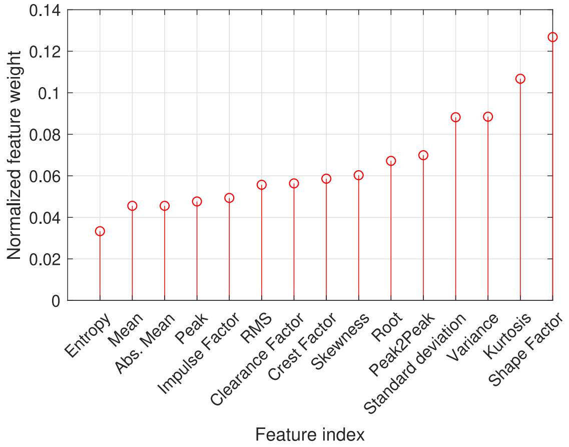


FIGURE 11. NCA ranking of all the 15 RF fingerprints extracted from 17 UAV controllers.

are transformed into a lower-dimensional space [23]. In this lower-dimensional space, the features are ranked according to a weight metric, with the more important features receiving higher weight values.

Given a set of training samples representing the different UAV controllers, $U = \{(\boldsymbol{x_1}, Y_1), \ldots, (\boldsymbol{x_i}, Y_i), \ldots, (\boldsymbol{x_n}, Y_n)\}$, where $\boldsymbol{x_i}$ is a p-dimensional feature vector extracted from the energy transient, $Y_i \in \{1, 2, \ldots, C\}$ are the corresponding class labels, and C is the number of classes. Then the NCA learns the feature weighting vector $\mathbf{w}$ by maximizing a regularized objective function $f(\mathbf{w})$ with respect to the weight of each features. The regularized objective function is defined as:

$$f(\mathbf{w}) = \frac{1}{n}\sum_{i=1}^{n}\left[\sum_{j=1, i\neq j}^{n} p_{ij}Y_{ij} - \lambda\sum_{r=1}^{p} w_r^2\right], \quad \text{where}$$

$$p_{ij} = \begin{cases} \frac{k(d_{\mathbf{w}}(\boldsymbol{x}_i, \boldsymbol{x}_j))}{\sum_{j=1, i\neq j}^{n} k(d_{\mathbf{w}}(\boldsymbol{x}_i, \boldsymbol{x}_j))} & \text{if } i \neq j \\ 0, & \text{if } i = j \end{cases},$$

$$Y_{ij} = \begin{cases} 1, & \text{if } Y_i = Y_j \\ 0, & \text{otherwise,} \end{cases} \tag{12}$$

n is the number of samples in the feature set, λ is the regularization term, w_r is a weight associated with the rth feature, and p_{ij} is the probability with which each point $\boldsymbol{x}_i$ selects another point $\boldsymbol{x}_j$ as its reference neighbor and inherits the class label of the latter [24]. The parameter Y_{ij} is an indicator function, $d_{\mathbf{w}}(\boldsymbol{x}_i, \boldsymbol{x}_j) = \sum_{r=1}^{p} w_r^2 |x_{ir} - x_{jr}|$ is a weighted distance function between $\boldsymbol{x}_i$ and $\boldsymbol{x}_j$, and $k(a) = \exp(\frac{a}{\sigma})$ is some kernel function. Thus, NCA is a kernel-based feature selection algorithm that selects the most descriptive and informative features by optimizing (12) using gradient update techniques.

Fig. 11 shows the results of the NCA ranking of 15 features extracted from the 17 UAV controllers. The experimental setup and structure of the captured data are described in Section VI. In Fig. 11, we see that NCA ranks the RF fingerprints according to their weight values. It turns out that the shape factor is the most discriminative feature in the feature set. The next significant feature is the kurtosis which describes the tailedness of the energy trajectory curve. Next are variance and standard deviation. On the other hand, entropy, which measures the uncertainty in the data set, is the least significant feature. Based on these results, the ML algorithms can safely discard the less important features and still achieve good (even better) classification performance. This is because discarding the less significant features reduces the chance of overfitting. In addition, for large-scale classification problems, there can be huge computational saving in training and testing the classifiers with fewer number of features.

TABLE 3. UAV catalogue.

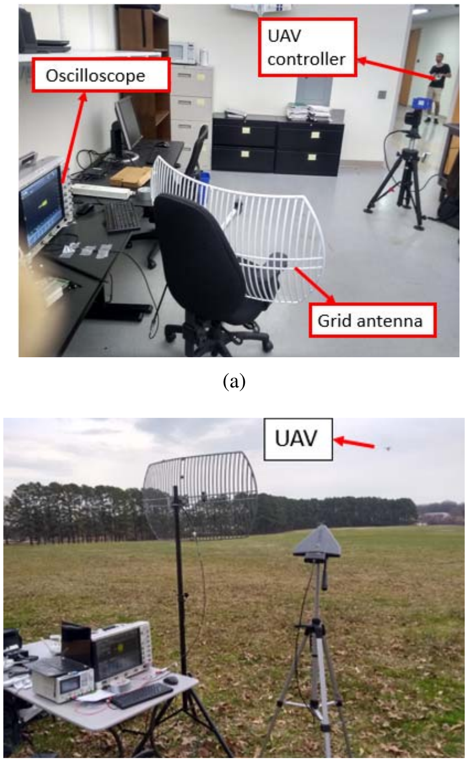
Make	Model	Make	Model
DJI	Inspire 1 Pro Matrice 100 Matrice 600[1] Phantom 4 Pro[1] Phantom 3	Spektrum	DX5e DX6e DX6i JR X9303
Futaba	T8FG	Graupner	MC-32
HobbyKing	HK-T6A	FlySky	FS-T6
Turnigy	9X	Jeti Duplex	DC-16

VI. EXPERIMENTAL SETUP AND DATA CAPTURE

During the experiments, RF signals are captured from 17 UAV controllers, six mobile Bluetooth devices (smart phones), and a Wi-Fi router. Table 3 gives the catalogue of the UAV controllers from eight different manufacturers. All the UAV controllers transmit control signals in the 2.4 GHz frequency band. In particular, a pair of UAV controllers from DJI Matrice 600 and DJI Phantom 4 Pro models are used while only one of the other controller type is used. This is important for forensic and security analysis to investigate the confusion that would arise when a target recognition system attempt to distinguish between UAV controllers of the same make and model. For the remaining part of the study we will refer to the pair of DJI Matrice 600 as DJI M600 Mpact and DJI M600 Ngat. Similarly, the pair of Phantom 4 Pro controllers will be referred to as DJI Phantom 4 Pro Mpact and DJI Phantom 4 Pro Ngat.

Fig. 12 shows the indoor and outdoor experimental scenarios. In each case, the RF passive surveillance system detects signals transmitted by the UAV controllers and the interference sources. Due to space limitations, only the results of the indoor experiments will be reported. The experimental RF passive surveillance system consists of a 6 GHz bandwidth Keysight MSOS604A oscilloscope with a maximum sampling frequency of 20 GSa/s, 2 dBi omnidirectional antenna (for short distance detection), and 24 dBi Wi-Fi grid antenna (for longer distance detection). The antennas operate in the 2.4 GHz frequency band. Furthermore, to ensure only signals in the 2.4 GHz band are captured, the output of the

[1] A pair of these controllers is used in this study. For all other controllers, only one of each type is considered.



(a)

(b)

FIGURE 12. (a) Indoor and (b) outdoor experimental scenarios for UAV signal detection.

receiving antenna is passed through a 2.4 GHz bandpass filter. The addition of a 2.4 GHz bandpass filter also removes out of band interference signals. Therefore, only Wi-Fi and Bluetooth interference signals are considered in this study. Moreover, the detection range of the RF surveillance system can be further improved by using a combination of high-gain receive antennas and low-noise power amplifiers (LNAs).

The receiver antenna continuously senses the environment for the presence of RF signals. During both the training and test phases, data capture is performed in real-time followed by breaking into windows of a specific duration. Afterward, the captured data are automatically saved in MATLAB extension format (.mat) in a cloud database for post-processing. We note that, for accurate detection of the RF signals, the window length should be small enough so that the transitions that characterize the RF signals are not dominated by those of the noise signals. On the other hand, for the classification process, the window length should be kept large enough such that the energy transient can be extracted properly. Based on these considerations, the window length is set to 0.25 ms. For each controller, 100 RF signals, each of which contains 5000k samples (spanning a period of 0.25 ms), are collected. During the experiment, the data was partitioned with the ratio $p = 0.2$. We used 80% for training (training (60%) + cross-validation (20%)) and 20% for testing. We set aside the test data and performed cross-validation to train the machine learning models. The cross validation avoids over-fitting and helps to remove the bias in the training phase. To be specific, we used k-fold cross-validation (with $k = 5$), where data is divided into k subsets, where each time, one of the k subsets is used as the validation/test set and the remaining $k-1$ subsets are used for training the model. The error is averaged over all k trials to get the total effectiveness of the model. The final test error was recorded by averaging the test error for different Monte-Carlo simulations.

VII. RESULTS

A. DETECTION RESULTS

Detection performance of the proposed system is assessed for different SNRs and threshold choices, and the results are presented in Fig. 13. The selected thresholds are functions of the standard deviation (σ) of the preprocessed noise data and the FAR specification. The value of σ is estimated after performing multiresolution analysis (wavelet preprocessing) of a concatenation of several noise data captured from the environment. On the other hand, FAR, also known as the probability of false detection, is the percentage of false alarms per the number of non-events.

Fig. 13 shows that at very low SNR, such as −10 dB, the detection accuracy is generally very low irrespective of the threshold. As a result, in case of low-level signals (where signals completely buried in the noise), the probability of missed detection increases. Besides, for a given SNR, it is observed that the set threshold also affects the performance of the detection system. For instance, when the system operates at an SNR of 2 dB, a threshold of $\delta = 0.1\sigma$ will achieve a detection accuracy of above 99%. However, the threshold $\delta = 0.1\sigma$ yields to a FAR of 100%. Therefore, a very low threshold value will result in a high percentage of misclassification of the noise data as signals. Furthermore, for the given SNR of 2 dB, an increase in the threshold value to $\delta = 1.1\sigma$ will reduce the detection accuracy and FAR to 96.6% and 14.8%, respectively. Further increase in the threshold to $\delta = 2.5\sigma$ will greatly reduce the detection accuracy and FAR to 40.4% and 3.2%, respectively. Therefore, the optimum threshold depends on the operating condition and the requirements on the FAR. Besides, the input impedance of the oscilloscope places a fundamental limit on the sensitivity of the passive detection system used in this study.

In addition, Fig. 13 shows that better detection performance (with low FAR) can be achieved if the detector operates at higher SNRs (above 8 dB) and threshold $\delta \in [2.5\sigma, 4.1\sigma]$. For instance, when the receiver operates at an SNR of 10 dB with a threshold $\delta = 3.5\sigma$, the detection accuracy becomes 99.8% and, FAR drops to 2.8%. Although a continuous increase in the threshold will further reduce the FAR, it will not always guarantee a better detection accuracy, especially when the receiver operates at SNRs of less than 18 dB. This is because the dissimilarity between the transition matrices of the RF signal and noise classes reduces as δ increases beyond some optimum value. Therefore, there is a high chance of detection error as δ increases indefinitely.

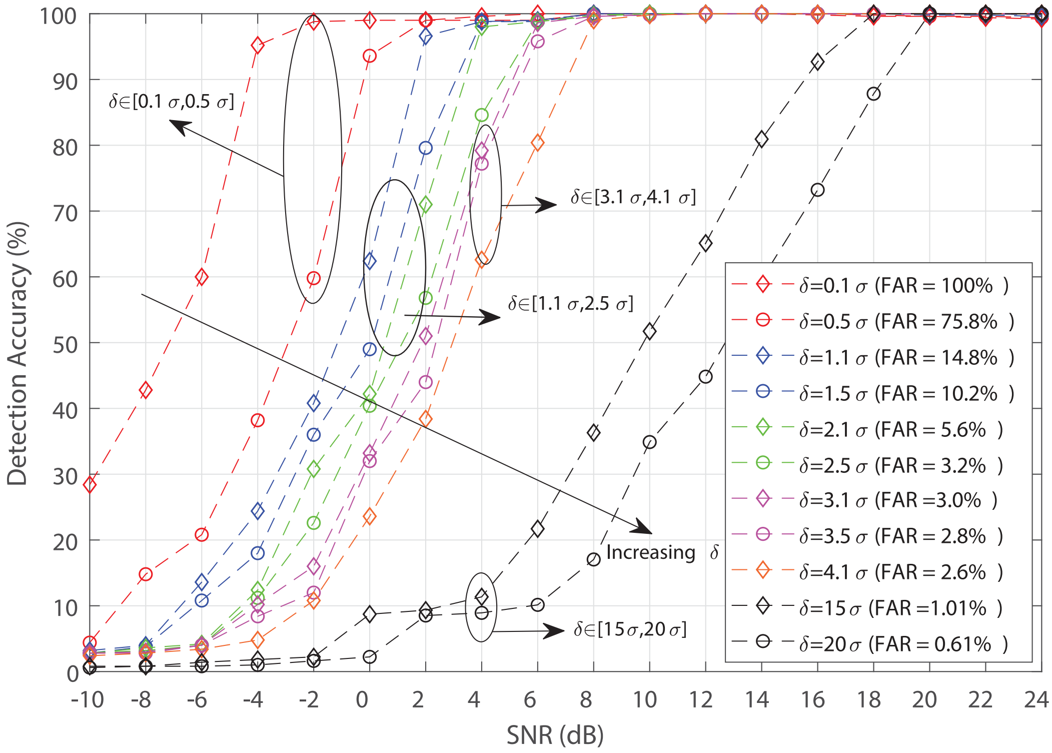


FIGURE 13. The signal detection accuracy of the Markov model-based naïve Bayesian detector versus SNR for different values of δ.

Once a signal has been detected, the bandwidth and the modulation-based features are estimated as described in Section IV. This information is used to decide if the signal comes from a UAV controller or any of the known interference sources (Wi-Fi and Bluetooth sources). Given that the detected signal comes from a UAV controller, it is sent to the ML-based classification system for accurate identification. Classification results are discussed next.

B. UAV CLASSIFICATION RESULTS

For the classification problem, 15 statistical features given in Table 2 are extracted. Feature selection is performed using the NCA algorithm as described in Section V-A.

To validate the result efficiency of the NCA and the ML classifiers, 10 Monte Carlo simulations are run on the test dataset. On one hand, all the 15 features are used for the UAV controller classification problem. On the other hand, only three most significant features are used according to the NCA weight ranking shown in Fig. 11. These are the shape factor, kurtosis and variance. The classification experiments are run separately for the case of 15 and 17 UAV controllers. Here, the number of controllers represents the number of classes considered. In the case of 15 controllers, all the controllers are of a different model. However, in the case of 17 controllers, a pair of DJI Matrice 600 (labeled as DJI Matrice 600 Mpact and DJI Matrice 600 Ngat) and a pair DJI Phantom 4 Pro controllers (labeled as DJI Phantom 4 Pro Mpact and DJI Phantom 4 Pro Ngat) are considered in addition to 13 different models.

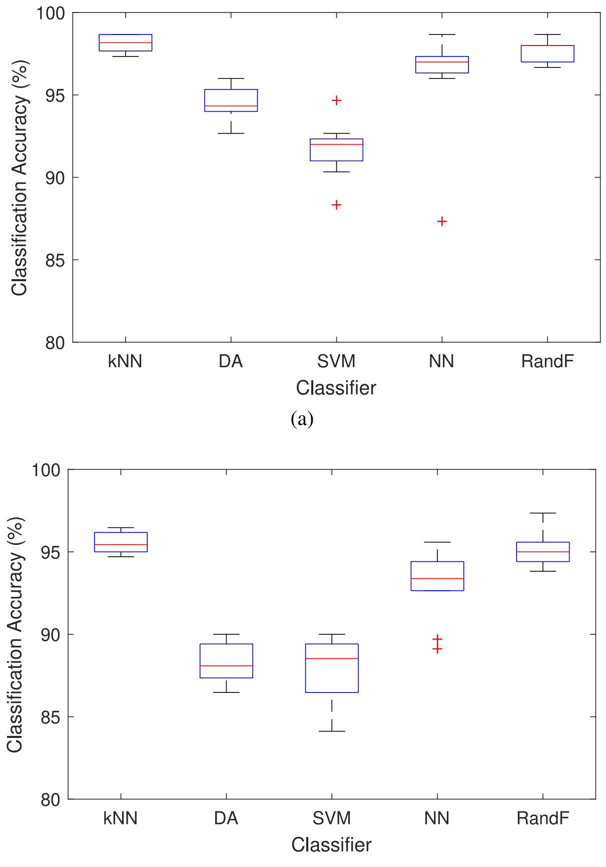
We used the Bayesian optimization method to obtain the best hyper-parameters for our machine learning models. Bayesian optimization has become a successful tool for hyperparameter optimization of machine learning algorithms, such as support vector machines or deep neural networks. The algorithm internally maintains a Gaussian process model of the objective function and uses objective function evaluations to train this model. More details can be found in [25], [26]. Some of the critical hyper-parameters for the machine learning models (for the 17 controller case) after the Bayesian hyperparameter optimization are listed below:

- kNN: Number of neighbors = 10, Distance metric = mahalanobis
- DA: Type = Linear, Delta = 0.15146, Gamma = 0.00016419
- SVM: Coding: onevsone, Lambda = 3.9941e-08, Learner = Logistic
- NN: Double layer: Number of hidden nodes (Layer 1) = 45, Number of hidden nodes (Layer 2) = 15, Learning rate = 0.30103, Activation functions = radbas
- RandF: Bagged Ensemble with 60 bagged decision trees

Table 4 provides the classification accuracy of all five ML algorithms. With the exception of the kNN and NN classifiers, the table shows that the classification accuracy is only slightly higher when all the features are used as compared to when only the three selected features are used. Table 4 shows that it takes each ML classifier between 18-142 s to classify the set of test signals extracted from all 17 UAV controllers. The time taken is lesser when we use

TABLE 4. Performance of the ML classification algorithms at 25 dB SNR. 100 sample signals from each UAV controller is captured with 80% used for training and 20% for testing (partition ratio = 0.2). The selected RF fingerprints are: Shape factor, kurtosis, and variance.

# of controllers	Classifier	Accuracy (%)[2]		Computational Time (s)[2]	
		All Feat.	Selected Feat.	All Feat.	Selected Feat.
15	kNN	97.30	98.13	24.85	24.57
	DA	96.30	94.43	19.42	18.58
	SVM	96.47	91.67	119.22	111.02
	NN	96.73	96.13	38.73	38.14
	RandF	98.53	97.73	21.37	20.89
17	kNN	95.62	95.53	26.16	25.13
	DA	92.77	88.12	19.36	18.90
	SVM	93.82	87.88	139.94	141.68
	NN	92.88	93.03	46.04	43.33
	RandF	96.32	95.18	24.71	24.84



(a)

(b)

FIGURE 14. Box plot analysis of the classification accuracy of the ML classifiers using the three selected features (shape factor, kurtosis, and variance) with (a) 15 controllers, and (b) 17 controllers.

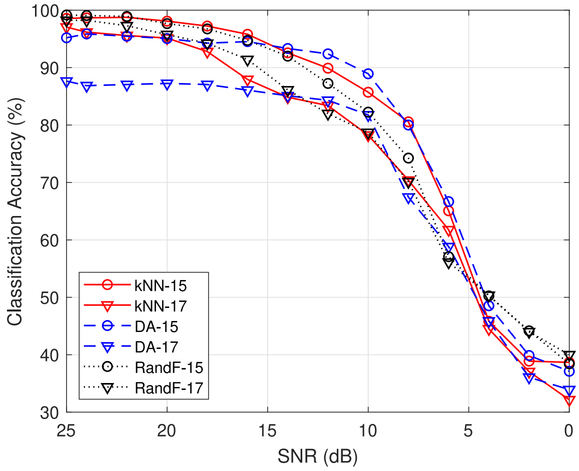
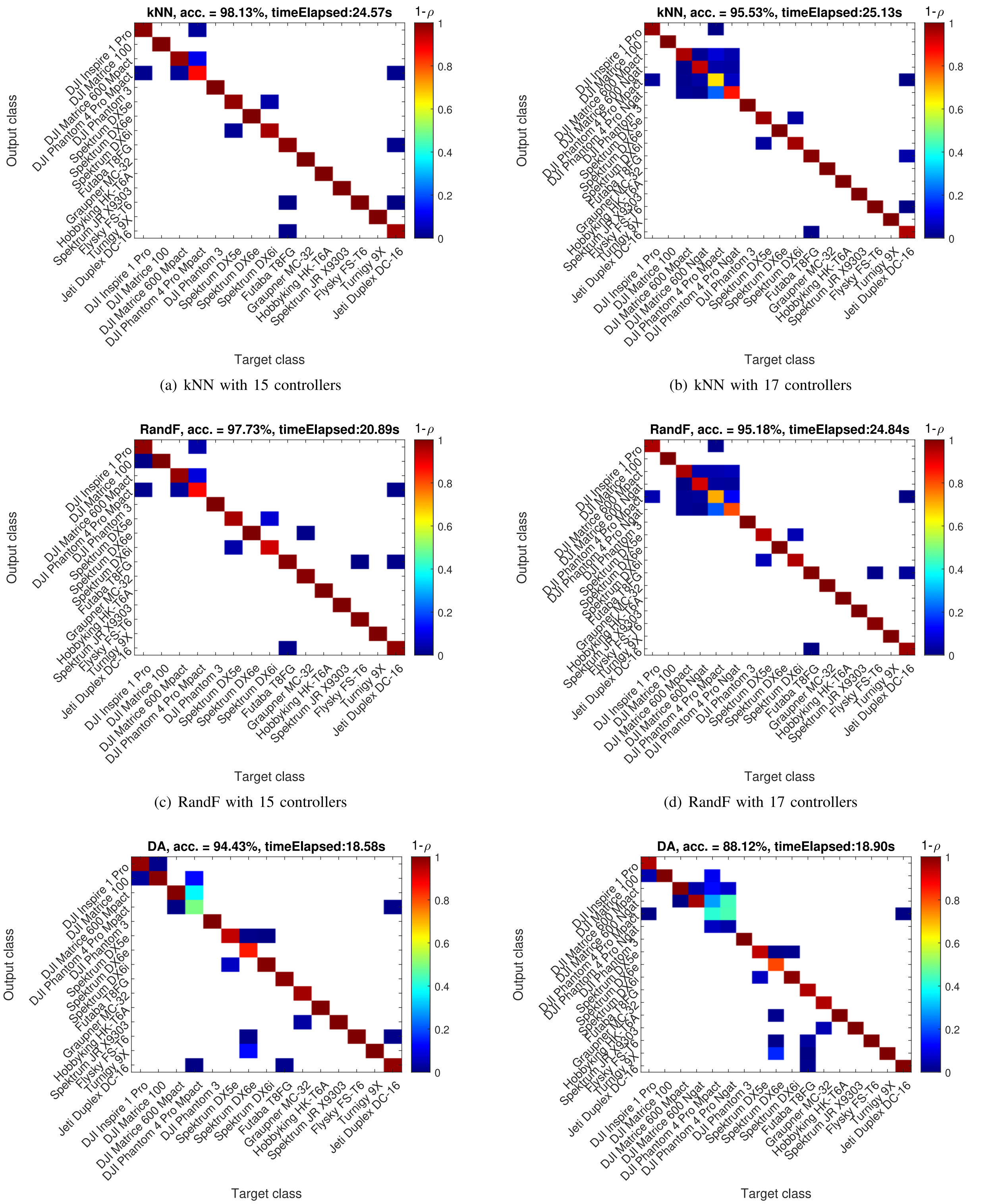


FIGURE 15. Classification accuracy versus SNR for kNN, RandF and DA classifiers using the three selected RF fingerprints (shape factor, kurtosis, and variance) as features for training and testing the ML classifiers.

only the selected features obtained from the NCA algorithm. The savings in time, though little, will scale greatly as the number of UAVs (to be classified) increases. This time saving may be critical in aerial surveillance systems, where the response time to effectively neutralizing a threat is very small. The outdoor experimental test shows that it takes less than 0.5 s to detect and identify the RF signals from a single UAV controller which is 200 m away. This timing is significantly small because most commercial and hobby grade UAVs travel at a very slow speed. For instance, the maximum speed of DJI Phantom 3 UAV is about 16 m/s. This means the proposed passive detection system can detect this UAV hundred of miles away before it gets into harm's way. Moreover, the complexity of the proposed system lies only in the training phase. It took several hours to train the system using thousands of signals captured from all 17 controllers at different SNR. Once trained, the system has a good performance to complexity ratio. Moreover, training is performed only once. In the test phase, only the relevant features are used for classification. Hence, the results in Table 4 validate the decision to perform feature selection using the NCA algorithm.

Table 4 shows the RandF classifier yields the highest classification accuracy when all the features are used. For the case of 15 and 17 controllers, RandF achieves an accuracy of 98.53% and 96.32%, respectively. Therefore, when all the features are used, RandF is the best performing classifier. It is followed by the kNN classifier, which achieves an accuracy of 97.30% and 95.62% with 15 and 17 controllers, respectively. The DA classifier is the least optimal when all the features are utilized. On the other hand, when only the three selected features are used, the kNN classifier performs

[2] Both the accuracy and total computation time are the average of the 10 Monte Carlo simulations.



(a) kNN with 15 controllers

(b) kNN with 17 controllers

(c) RandF with 15 controllers

(d) RandF with 17 controllers

(e) DA with 15 controllers

(f) DA with 17 controllers

FIGURE 16. Confusion matrices of kNN, RandF and DA classifiers using the three selected RF fingerprints (shape factor, kurtosis, and variance). In the confusion matrices, the colorbar is used to specify the degree of confusion in terms of the confusion probability ρ. Moving down the colorbar, the degree of confusion increases with increasing value of ρ.

the best with an accuracy of 98.13% and 95.53% for 15 and 17 controllers, respectively. It is followed by the RandF classifier which an accuracy of 97.73% and 95.18% with 15 and 17 controllers, respectively. When only the three most significant features are used, the least optimal classifier is SVM. We also note that the DA classifier has the shortest computational time whereas the SVM classifier has the longest computational time. The DA classifier computes and decomposes the class covariance matrices. Fortunately, MATLAB has optimized subroutines/functions for matrix computation and decomposition. As a result, DA is very fast and efficiently implemented in MATLAB. However, SVM is slow because it has several key parameters that need to be optimized to achieve the best classification performance. SVM hyperparameter optimization searches for different kernel functions (Sigmoid, linear, RBF, etc). This process is time-consuming.

Table 4 provides only the average classification accuracy results. A more detailed summary can be obtained from a box plot analysis shown in Fig. 14. Each box plot gives a summary of the performance of a classifier in terms of the minimum, first quartile, median (red horizontal line), third quartile, and the maximum accuracy values over 10 Monte Carlo simulations. Comparing the box plots in Fig. 14(a) and Fig. 14(b), we see that the box plot metrics for each classifier are lower in the case of 17 controllers as compared to the case of 15 controllers. This will be further investigated with the help of the confusion matrix. In addition, the box plots reveal the presence of outliers in the performance of the SVM and NN classifiers. These outliers suggest that for a given test signal, SVM and NN classifiers could produce accuracy values well below the average values reported in Table 4. This observation raises the concern about the reliability of these classifiers for the UAV controller classification problem.

The SNR of the detected signal is an important factor that influences the accuracy of the classifiers. Fig. 15 shows the accuracy versus SNR for the kNN, RandF and DA classifiers. For signals with SNR in the interval between 15 and 25 dB, the kNN is slightly better than the RandF for the case of 15 controllers. In the same SNR region, the RandF performs best for the case of 17 controllers. In this SNR range, the DA classifier has the worst performance. On the other hand, for SNR between 4 and 15 dB, the performance of the DA classifier improves significantly, outperforming the kNN and RandF classifiers when 15 controllers are considered. This is an interesting observation since DA is known to have the shortest computational time. However, for SNR between 0 to 4 dB, the RandF classifier has the best performance. In general, the accuracy of all the classifiers increases with SNR. Therefore, to ensure accurate identification of the UAV controller, it is best to operate the receiver at SNR above 15 dB, in which case, kNN and RandF are the optimal classifiers for the datasets. Fig. 15 also shows that for all SNR, the accuracy plot is slightly lower when 17 controllers are considered as compared to the case of 15 controllers.

The confusion matrix gives an idea of what a classifier is getting right and the type of errors it makes. Fig. 16 shows the confusion matrices of the classifiers: kNN, RandF and DA for the case of 15 and 17 remote controllers. On the vertical axis of each confusion matrix is the output class or the prediction of the classifier while the horizontal is the target class or true label. From the confusion matrices in Fig. 16, we observe that in the case of 17 controllers, the degree of confusion around the DJI controllers is relatively higher as compared to the case of 15 controllers. This is because in the former, we intentionally included two pairs of identical DJI controllers (DJI Matrice 600 MPact, DJI Matrice 600 Ngat, DJI Phantom 4 Pro Mpact, and DJI Phantom 4 Pro Ngat). Consequently, there are some confusions among these four controllers leading to a slight reduction in the classification accuracy in the case of 17 controllers. However, the kNN and RandF classifiers still achieves an average accuracy of 95.53% and 95.18%, respectively. Therefore, these classifiers are robust in identifying UAV controllers of the same make and model. On the other hand, the DA classifier is characterized by several more confusions among different controllers which reduces its average accuracy to 88.12% in the case of 17 remote controllers. Thus, while the kNN and RandF seem to be the best classifiers, the DA classifier still performs well for the given dataset.

VIII. CONCLUSION

In this paper, the problem of detecting and classifying RF signals from different UAV controllers is investigated. The detection system is designed to operate in the presence of wireless interference from Wi-Fi and Bluetooth sources. These interference signals are detected using a multistage detector, which estimates the bandwidth and modulation features of the detected RF signals. Once the signal from a UAV controller is detected, it is identified using RF fingerprints along with the ML-based classification techniques. Reducing the number of required features with the help of NCA, the study shows that it is possible to achieve an accuracy of 98.13% in classifying 15 different controllers using only three features in a kNN classifier. It is also shown that the proposed system can even classify the same make and model UAV controllers without much compromising the overall accuracy. In addition, the detection and classification performance of the proposed system is tested for a range of SNR levels. In each task, the system is shown to be safe for SNR levels of above 10 dB. Future studies will present the detection of UAVs directly from the UAV signals in outdoor scenarios and consider the potential of sensor fusion for improved UAV detection.

REFERENCES

[1] M. Ezuma, F. Erden, C. K. Anjinappa, O. Ozdemir, and I. Guvenc, "Micro-UAV detection and classification from RF fingerprints using machine learning techniques," in *Proc. IEEE Aerosp. Conf.*, Big Sky, MT, USA, Mar. 2019.

[2] H. Shakhatreh *et al.*, "Unmanned aerial vehicles (UAVs): A survey on civil applications and key research challenges," *IEEE Access*, vol. 7, pp. 48572–48634, 2019.

[3] I. Güvenç, O. Ozdemir, Y. Yapici, H. Mehrpouyan, and D. Matolak, "Detection, localization, and tracking of unauthorized UAS and jammers," in *Proc. IEEE/AIAA Digit. Avionics Syst. Conf. (DASC)*, St. Petersburg, FL, USA, Sep. 2017, pp. 1–10.

[4] A. Solodov, A. Williams, S. Al Hanaei, and B. Goddard, "Analyzing the threat of unmanned aerial vehicles (UAV) to nuclear facilities," *Security J.*, vol. 31, no. 1, pp. 305–324, Feb. 2018.

[5] A. A. A. Alajmi, A. Vulpe, and O. Fratu, "UAVs for Wi-Fi receiver mapping and packet sniffing with antenna radiation pattern diversity," *Wireless Pers. Commun.*, vol. 92, no. 1, pp. 297–313, Jan. 2017.

[6] B. Nassi, A. Shabtai, R. Masuoka, and Y. Elovici. *Sok-Security and Privacy in the Age of Drones: Threats, Challenges, Solution Mechanisms, and Scientific Gaps*. [Online]. Available: https://arxiv.org/pdf/1605.07079.pdf

[7] A. Shoufan, H. M. Al-Angari, M. F. A. Sheikh, and E. Damiani, "Drone pilot identification by classifying radio-control signals," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 10, pp. 2439–2447, Oct. 2018.

[8] Z. Shi, M. Huang, C. Zhao, L. Huang, X. Du, and Y. Zhao, "Detection of LSSUAV using hash fingerprint based SVDD," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Paris, France, May 2017, pp. 1–5.

[9] I. Bisio, C. Garibotto, F. Lavagetto, A. Sciarrone, and S. Zappatore, "Unauthorized amateur UAV detection based on WiFi statistical fingerprint analysis," *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 106–111, Apr. 2018.

[10] C. Zhao, C. Chen, Z. Cai, M. Shi, X. Du, and M. Guizani, "Classification of small UAVs based on auxiliary classifier Wasserstein GANs," in *Proc. IEEE Glob. Telecommun. Conf. (GLOBECOM)*, Abu Dhabi, UAE, Dec. 2018, pp. 206–212.

[11] M. F. Al-Sa'd, A. Al-Ali, A. Mohamed, T. Khattab, and A. Erbad, "RF-based drone detection and identification using deep learning approaches: An initiative towards a large open source drone database," *Future Gener. Comput. Syst.*, vol. 100, pp. 86–97, Nov. 2019.

[12] *RF Techniques for Detection, Classification and Location of Commercial Drone Controllers*, KeySight Technol., Santa Rosa, CA, USA, 2017. [Online]. Available: https://tekmarkgroup.com/eshop/image/catalog/Application/AEROSPACE/Paper-5_Techniques-for-Detection-Location-of-Commercial-Drone-Controllers_2017-Malaysia-AD-Symposium.pdf

[13] P. Nguyen, H. Truong, M. Ravindranathan, A. Nguyen, R. Han, and T. Vu, "Matthan: Drone presence detection by identifying physical signatures in the drone's RF communication," in *Proc. ACM Int. Conf. Mobile Syst. Appl. Services (ACM MobiSys)*, Niagara Falls, NY, USA, Jun. 2017, pp. 211–224.

[14] I. Guvenc, F. Koohifar, S. Singh, M. L. Sichitiu, and D. Matolak, "Detection, tracking, and interdiction for amateur drones," *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 75–81, Apr. 2018.

[15] S. G. Mallat, "A theory for multiresolution signal decomposition: The wavelet representation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 11, no. 7, pp. 674–693, Jul. 1989.

[16] A. Bultan and R. A. Haddad, "System identification with denoising," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, vol. 1. Istanbul, Turkey, Jun. 2000, pp. 576–579.

[17] S. Rayanchu, A. Patro, and S. Banerjee, "Airshark: Detecting non-WiFi RF devices using commodity WiFi hardware," in *Proc. ACM Internet Meas. Conf. (ACM IMC)*, Berlin, Germany, Nov. 2011, pp. 137–154.

[18] Z. Weng, P. Orlik, and K. J. Kim, "Classification of wireless interference on 2.4 GHz spectrum," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Istanbul, Turkey, 2014, pp. 786–791.

[19] T. Scholand and P. Jung, "Bluetooth receiver with zero-crossing zero-forcing demodulation," *IET Electron. Lett.*, vol. 39, no. 17, pp. 1275–1277, Aug. 2003.

[20] *Introduction to Bluetooth Device Testing: From Theory to Transmitter and Receiver Measurements*, Nat. Instrum., Austin, TX, USA, Sep. 2016. [Online]. Available: http://download.ni.com/evaluation/rf/intro_to_bluetooth_test.pdf

[21] *Wi-Fi: Overview of the 802.11 Physical Layer and Transmitter Measurements*, Tektronix, Beaverton, OR, USA, Oct. 2017. [Online]. Available: https://www.tek.com/document/primer/wi-fi-overview-80211-physical-layer-and-transmitter-measurements

[22] R. Esteller, G. Vachtsevanos, J. Echauz, and B. Litt, "A comparison of waveform fractal dimension algorithms," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 48, no. 2, pp. 177–183, Feb. 2001.

[23] J. Goldberger, G. E. Hinton, S. T. Roweis, and R. R. Salakhutdinov, "Neighbourhood components analysis," in *Proc. NeurIPS*, Vancouver, BC, Canada, Dec. 2004, pp. 513–520.

[24] W. Yang, K. Wang, and W. Zuo, "Neighborhood component feature selection for high-dimensional data," *J. Comput.*, vol. 7, no. 1, pp. 161–168, Jan. 2012.

[25] J. Snoek, H. Larochelle, and R. P. Adams, "Practical Bayesian optimization of machine learning algorithms," in *Proc. Adv. Neural Inf. Process. Syst.*, 2012, pp. 2951–2959.

[26] A. Klein, S. Falkner, S. Bartels, P. Hennig, and F. Hutter. *Fast Bayesian Optimization of Machine Learning Hyperparameters on Large Datasets*. [Online]. Available: https://arxiv.org/pdf/1605.07079.pdf

MARTINS EZUMA received the B.S. degree in physics from the Federal University of Technology, Owerri, Nigeria, in 2010, the first M.S. degree in information and communication engineering from Chosun University, Gwangju, South Korea, in 2015, and the second M.S. degree in electrical engineering from the New Jersey Institute of Technology in 2016. He is currently pursuing the Ph.D. degree in electrical and computer engineering with North Carolina State University. His research interest include signal processing, UAV detection, radar, electronic warfare, 5G channel sounding, and pattern recognition.

FATIH ERDEN received the B.S. and M.S. degrees in electrical and electronics engineering from Bilkent University, Ankara, Turkey, in 2007 and 2009, respectively, and the Ph.D. degree in electrical and electronics engineering from Hacettepe University, Ankara, Turkey, in 2015.

From 2015 to 2016, he was an Assistant Professor with the Department of Electrical and Electronics Engineering, Atilim University, Ankara. From 2016 to 2018, he was a Post-Doctoral Researcher with Signal Processing Group, Bilkent University, Ankara. He is currently working as a Research Associate with the Department of Electrical and Computer Engineering, North Carolina State University. His research interests include signal and image processing, time-series analysis, infrared sensors, ambient-assisted living, mmWave communications, and UAV detection and navigation.

CHETHAN KUMAR ANJINAPPA received the B.E. degree in electronics and communication engineering from the Sri Jayachamarajendra College of Engineering, Mysuru, India, in 2012, and the M.E. degree in signal processing from the Indian Institute of Science (IISc), Bengaluru, India, in 2016. He is currently pursuing the Ph.D. degree in electrical engineering with North Carolina State University. He worked as a Project Associate with Signal Processing for Communications Laboratory, IISc from 2016 to 2017. His research interest include 5G and mmWave communication, V2X communication, sparse signal processing, and machine learning.

OZGUR OZDEMIR received the B.S. degree in electrical and electronics engineering from Bogazici University, Istanbul, Turkey, in 1999, and the M.S. and Ph.D. degrees in electrical engineering from the University of Texas at Dallas, Richardson, TX, USA, in 2002 and 2007, respectively. He joined a Visiting Research Scholar with the Department of Electrical and Computer Engineering, NCSU. He has been an Assistant Professor with the Department of Electrical and Electronics Engineering, Fatih University, Turkey, and a Post-Doctoral Scholar with Qatar University, Doha, Qatar. His research interest include opportunistic approaches in wireless systems, experimental multiple-antenna systems, digital compensation of radio-frequency impairments, wireless multi-carrier communications, and software defined radios.

ISMAIL GUVENC worked as a Research Engineer with DOCOMO Innovations, Inc., Palo Alto, CA, USA from 2006 to 2012, and as an Assistant Professor with Florida International University, Miami, FL, USA, from 2012 to 2016. He has been an Associate Professor with North Carolina State University since August 2016. His recent research interests include 5G and mmWave wireless networks, UAV communications, and heterogeneous networks. He is a recipient of the 2016 FIU College of Engineering Faculty Research Award, the 2015 NSF CAREER Award, the 2014 Ralph E. Powe Junior Faculty Award, and the 2006 USF Outstanding Dissertation Award.