Unauthorized Amateur UAV Detection Based on WiFi Statistical Fingerprint Analysis

Igor Bisio, Chiara Garibotto, Fabio Lavagetto, Andrea Sciarrone, and Sandro Zappatore

After a survey of the existing solutions, the authors propose a WiFi-based approach aimed at detecting nearby aerial or terrestrial devices by performing statistical fingerprint analysis on wireless traffic. This novel detection technique, tested in a variety of real-life scenarios, proved able to efficiently detect and identify intruder drones in all the considered experimental setups.

Abstract

Amateur drones are enjoying great popularity in recent years due to the wide commercial diffusion of small, rather low-cost devices. More and more user-friendly, easy-to-pilot aerial and terrestrial drones are available off the shelf, and people can even remotely pilot them using their smartphones. This situation brings up the problem of keeping unauthorized drones away from private or sensitive areas, where they can represent a personal or public threat. With this motivation, after a survey of the existing solutions, we propose a WiFi-based approach aimed at detecting nearby aerial or terrestrial devices by performing statistical fingerprint analysis on wireless traffic. This novel detection technique, tested in a variety of real-life scenarios, proved able to efficiently detect and identify intruder drones in all the considered experimental setups, making it a promising unmanned aerial vehicle detection approach in the framework of amateur drone surveillance.

Introduction

Drones have been enjoying great popularity in recent years thanks to their lower costs and smaller size. This kind of unmanned aerial vehicle (UAV) is generally called a *miniature drone* or *mini-drone*, and such UAVs are usually easy to pilot, even through WiFi smartphones and tablets.

Enabled by technological advances, the availability of open source software, and hardware miniaturization, amateur drones have recently found various key applications. The widespread diffusion of smart objects interconnected and managed remotely via the Internet in such a way as to make them intelligent, programmable, and more capable of interacting with human beings as well as of unmanned vehicles will likely take a major role in the connected smart cities of the future [1, 2]. However, the pervasive use of drones also leads to technical and societal concerns and issues that need to be addressed, related to security, privacy, and public safety. In the coming years, a technology able to monitor and identify drones, and keep them away from sensitive areas will become fundamental.

For this reason, research efforts must be put into the design and development of proper techniques able to detect the presence of remotely piloted devices, such as flying or terrestrial drones. The urge of a system able to detect and distinguish possible threats leads to the research of proper methods and technologies suitable for different real-life situations and working conditions. We can think of various possible practical solutions for a system able to identify drone threats. For example, consider a *guardian* entity, whose task is to monitor a sensitive area and keep it safe from unauthorized devices. This guardian can be employed in many configurations, each suitable for different applications and scenarios. Unauthorized UAV sensing systems could be implemented on different types of devices and located as depicted in Fig. 1:

- *Fixed ground system*, continuously monitoring the nearby area (like a security camera)
- *Fixed aerial system*, always scanning the surrounding flying zone (like a radar or sonar system)
- *Patrolling drone*, actively moving throughout the sensitive area in search of possible threats (like a police patrol)

Finding a solution suitable to be employed in all these scenarios requires a system that must comply with some basic characteristics:

- It must be lightweight to be easily embeddable, for example, on a small UAV.
- It shall not be sensitive to the interference produced by the guardian itself.
- It must have low power requirements and high autonomy.

Different techniques have been developed that are able to efficiently perform the drone detection task, but many of them are not suited for all the previously described real-life surveillance scenarios. Moreover, some techniques are subject to relevant drawbacks. An insightful discussion on the most commonly employed UAV identification approaches is provided later.

In addition to the need for complying to the requirements dictated by the previously mentioned surveillance scenarios, the main motivation that has led our research lies in the fact that nowadays a particular interest arises in the detection of not only large military UAVs, but also smaller amateur drones. This is due to the widespread diffusion of remotely driven commercial devices able to carry a payload and having video streaming capabilities. A large part of low-cost miniature drones is usually controlled via device-to-device (D2D) communication to directly route data traffic between spatially close objects providing energy efficiency, high throughput, low delay, as well as spectrum efficiency [3]. A list of commercially available drones relying on WiFi communication is provided in Table 1.

Digital Object Identifier:
10.1109/MCOM.2018.1700340

The authors are with the University of Genoa, Italy; Igor Bisio is also with the Peoples' Friendship University of Russia.

Most of these drones also include the so-called first person view (FPV) mode, which allows the owner to pilot the UAV remotely by using the video stream of a real-time camera that provides the first-person perspective of the drone itself. This type of streaming, together with the control signals, has particular characteristics that allow UAV detection through traffic analysis.

This article, after a survey of the existing techniques, proposes a novel WiFi statistical fingerprint-based drone detection method that exploits the inherent characteristics of drone control and FPV transmissions in order to sense the presence of a remotely piloted vehicle in the nearby WiFi coverage area. This technique takes into account the particular features of the WiFi traffic produced by drones and their controllers, and uses machine learning algorithms to detect the presence of such devices in the considered surveillance area.

The remainder of this article is structured as follows. We present an overview of existing drone detection methods; we describe the proposed fingerprint-based approach, and show the results obtained during the experimental tests. Finally, in the last section conclusions are drawn, and the envisaged future work is briefly described.

Overview of Drone Detection Methods

A UAV is a promising carriage for data gathering since it has sufficient as well as efficient resources in terms of both time and energy [4]. The great diffusion of UAVs in recent years has led to many concerns and issues on delicate topics, such as security and privacy. For this reason, a number of solutions are present in the literature to search and detect the presence of drones in a nearby area. The reliable detection of drones, however, is a challenging task due to the presence of many objects in the air, such as birds, clouds, and airplanes. To this aim, a variety of methods have been proposed [5]. In the following, a brief survey of the main existing drone detection techniques is presented. A summary of the described methods is available in Table 2.

Video-Based Detection

This class of techniques is based on the use of camera sensors able to identify a moving object against the background of the sky [6]. Commercial cameras can reach an operative range of about 350 ft, which leads to a quite reasonable surveillance area. The main issue related to this type of detection method is that, in the case of small UAVs such as quad-copters, it is very difficult to distinguish drones from birds or other possible flying objects. Cameras are usually equipped with sensors and/or motion detection for attempting to distinguish the automatic and mechanical movements of drones from the more natural behavior of birds. However, these approaches usually fail in the case of gliding birds [5]. Cameras are also very sensitive to lighting conditions, and they can identify objects only when the target is in line of sight.

Sound-Based Detection

These approaches consist of using microphones in order to capture ambient sounds. Most of the microphones have a working range of about 25–30 ft. The rationale behind this kind of technique is that UAVs usually produce a typical hissing high-frequency sound around 40 kHz due to their brushless direct current motors. In [7] the authors propose an audio classification system for drone detection based on data mining techniques. They employ hidden Markov models (HMMs) in order to perform phoneme analysis and identify drones by their emitted audio sounds. The approach works well in quiet environments, but it usually fails in urban areas or noisy conditions. Another drawback of audio-based detection is that audio sensors cannot be mounted onboard a patrol UAV for surveillance purposes since they would also capture the patrol UAV sound as well.

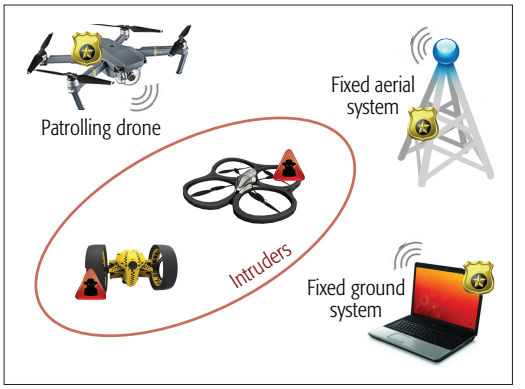

Figure 1. Practical real-life approaches to drone surveillance.

Drone model	Brand	Frequency (GHz)	Weight (g)	Price ($)
AR.Drone	Parrot	2.4	420	320
Bebop 2	Parrot	2.4	500	580
Disco FPV	Parrot	2.4	750	1390
Jumping Race	Parrot	2.4, 5	205	170
Mambo	Parrot	2.4	100	130
Swing	Parrot	2.4	295	150
Typhoon H	Yuneec	5	1950	1280
H501A X4 Air Pro	Hubsan	2.4	1300	230
H507A X4 Star Pro	Hubsan	2.4	162	99
X8SW	Syma	2.4	1500	155
X8SC	Syma	2.4	1500	150
X5UW	Syma	2.4	127	75
U818A Discovery	UdiRc	2.4	132	100
U29W	UdiRc	2.4	100	60
U845 Voyager	UdiRc	2.4	98.5	70
U36W	UdiRc	2.4	23	25
U28W	UdiRc	2.4	53	75
U31W	UdiRc	2.4	85	100

Table 1. A list of off-the-shelf amateur WiFi drones.

Radar-Based Detection

This class of methods exploits the electromagnetic principle of backscattering. The traditional radar approach is useful for detecting large aircraft, but it fails with small-sized quad-copters. Indeed, using

The partitioned flows are analyzed, and specific features are extracted so that each traffic flow is completely defined by the corresponding feature vector, which we call the fingerprint. The main features used to identify the relevant traffic are related to the duration and behavior of the traffic flow, and the distribution of the corresponding packets.

Detection approach	Target principle	Onboard deployment	Characteristics and drawbacks
Video-based	Image object and motion detection	✓	Hard to distinguish drones from other flying objects Range < 350 ft Needs line of sight
Sound-based	Hissing high frequency around 40 kHz	×	Fails in noisy urban areas Cannot be mounted onboard drones Range 25–30 ft
Radar-based	Backscattering of electromagnetic waves Doppler and micro-Doppler effect	✓	Fails to detect small quad-copters
Temperature	Hot gases produced by engines	×	Fails if drones have electric motors High cost and low reliability Range < 350 ft
Radio frequency	Control and video transmission over RF	✓	Difficult when altitude is high Depends on transmit power and receiver sensitivity Range < 1400 ft
WiFi-based	Piloting and video using WiFi protocol	✓	Available for WiFi drones only WiFi working range

Table 2. Summary of existing drone detection methods.

the radar cross-section (RCS) as a feature for drone identification is not quite suitable to detect small UAVs, which are objects providing a rather small RCS [8]. Moreover, it is often difficult to distinguish mechanical devices from other biological flying objects, such as birds or insects. Another difficulty is introduced by the fact that most commercial amateur drones are made of plastic material, which may have dielectric properties close to air, thus resulting in little reflection back to the transmitter. For this reason, modified types of radar sensors have been developed that exploit the energy backscattered from rotating parts like propellers and rotors by analyzing micro-Doppler signatures. The authors in [9] use these characteristic features and their spectral correlation functions (SCFs) for a radar sensor aimed at automatically detecting and classifying micro unmanned aerial systems (UASs). The proposed approach employs a deep belief network (DBN) to classify the signature patterns: the experimental results demonstrate that the system may achieve high accuracy values. The radar-based detection technique can be implemented in a rather portable format, and it is therefore suitable for also being employed onboard surveillance drones (e.g., as in [10]).

Temperature-Based Detection

Thermal drone detection is based on the idea that some drones, such as fixed-wing UAVs, employ turbo-fan and turbo-gases as a propulsion system. These engines produce hot gases from the exhaust, which facilitate temperature-based detection [11]. However, a large number of commercial drones are electric quad-copter vehicles, which do not radiate enough heat to be detected by this method. The range of effectiveness of this technique is about 350 ft, the implementation costs are very high, and the drone identification rate is limited, which usually leads to employing this type of sensor as an add-on to other main UAV detection systems. An important drawback of this technique is that it cannot be mounted onboard drones, as the temperature of the drone itself would interfere with the sensor measurements.

Radio-Frequency-Based Detection

The RF-based method relies on the fact that drones communicate with the ground control station through RF transmissions. The most commonly employed frequency bands are around 2.4 and 5 GHz, the same bands used by WiFi devices. Moreover, UAVs equipped with cameras usually transmit video to their control unit on the same wireless channel. In [12], the authors present an algorithm for detecting Universal Mobile Telecommunications System (UMTS), LTE, and drone communication signals in adverse environments. Morphological filtering in the frequency domain is used to separate the desired signal from perturbations, thus allowing reliable detection. RF detection has a very long effective range, covering over 1400 ft. A minor issue of this technique is that target detection rate strongly depends on transmitter power and receiver sensitivity.

WiFi-Based Detection

WiFi-based detection methods rely on the fact that a large majority of commercial low-cost amateur drones are controlled and/or transmit video streaming on WiFi bands. In the literature similar approaches are not very commonly used to identify UAVs, whereas they are sometimes employed by drones themselves to locate other types of nearby devices [13]. The main idea is to exploit a wireless packet sniffer in order to capture packet flows (or portion of flows) belonging to drone transmission. However, these techniques are usually based on a priori knowledge of the type of remotely piloted vehicle, such as the vendor organizationally unique identifier (OUI) used to identify the sender/receiver of specific packets [14]. The drone detection method proposed in this article belongs to this class of techniques; however, it differs from the existing literature since it analyzes the statistical fingerprint of traffic flows in order to identify the drones. Thus, this method does not require a priori knowledge of UAVs to successfully identify a nearby target drone. In the following, we describe our novel WiFi statistical fingerprint-based drone detection method.

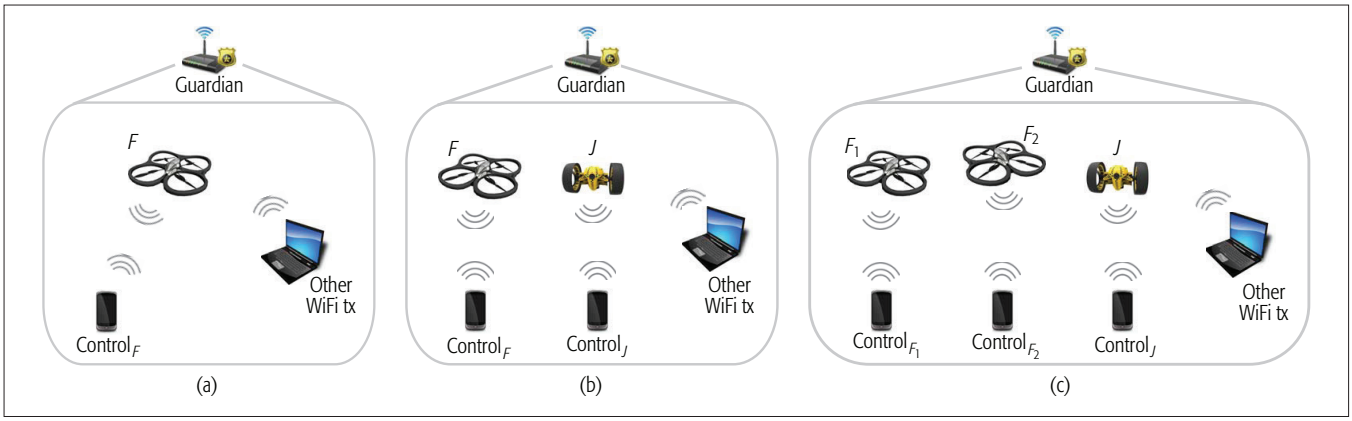

Figure 2. Scheme of the considered scenarios: a) single flying drone; b) flying and terrestrial drones; c) multiple flying and terrestrial drones.

The WiFi-based detection method is also well suited for portable systems that can be mounted onboard patrolling drones due to its minimal hardware requirements.

WiFi-Based Drone Detection System

This article proposes a drone detection method based on several features extracted from WiFi network traffic flows related to drone control and video transmissions. The final goal is to detect the possible presence of an unauthorized UAV in a given surveillance area. A network packet sniffer *Wireshark* onboard a guardian captures all traffic flows on WiFi channels; the acquired data are dumped in a *pcap* file. It can be locally processed (i.e., onboard the guardian) or sent to a remote station to extract a set of specific features from the global traffic capture, as described in the following.

We consider as a flow any wireless stream of network packets identified by the couple {Source MAC Address, Destination MAC Address} (MAC: medium access control). Packets in which source and destination addresses are swapped are considered as belonging to the same flow. The captured traffic is processed and partitioned based on a predefined time *window*, which determines the time interval at which detection is performed. This enables the system to provide real-time drone detection, instead of being forced to wait for the end of the transmission to identify the nature of the considered flows. The partitioned flows are analyzed, and specific features are extracted so that each traffic flow is completely defined by the corresponding feature vector, which we call the *fingerprint*. The main features used to identify the relevant traffic are related to the duration and behavior of the traffic flow, and the distribution of the corresponding packets.

In order to obtain effective drone detection, we selected the following features to determine the statistical fingerprint relative to a single flow:

- Total number of packets (Tot_pack)
- Total duration of the flow (Duration)
- Average packet length (Mean_len)
- Root mean square (RMS) of packet length (Len_rms)
- Average packets inter-arrival time (Mean_delta)
- RMS of packets inter-arrival time (Delta_rms)
- Number of embedded packets (Embedded_pack)
- Number of packets with specific DS status flags (Mode1, Mode2, Mode3, Mode4)

We define *embedded packets* as those packets whose source/destination addresses coincide with the transmitter/receiver address, and we consider it as an indication of a possible embedded WiFi network card.

After the feature extraction phase, the actual identification of drone-specific patterns is performed by means of consolidated machine learning techniques that allow recognizing different classes. The specific algorithms and scenarios considered in this article are described.

Experimental Campaign

This section describes the results obtained when evaluating our proposed method in experimental tests. In all the considered scenarios, the surveillance entity (the guardian) we employed is a laptop running Mac OS, with the Wireshark sniffer in monitor mode installed onboard. The laptop implements, onboard, our proposed WiFi-based drone detection algorithm, which uses the aforementioned statistical analysis on wireless traffic to identify the presence of unauthorized drones in the surrounding area.

The devices employed during our tests are a Parrot AR.Drone 2.0 UAV, an older model of flying Parrot AR.Drone, and a Parrot Jumping Race Max terrestrial drone. The UAVs are two typical amateur FPV electric quad-copters weighting about 400 g, equipped with a high definition 720p camera and a flying range of 50 m, which can be controlled over WiFi at 2.4 GHz by a remote Android or iOS device. The second type of device is a two-wheel terrestrial drone, also capable of jumping, which can be piloted via WiFi at both 2.4 and 5 GHz by a remote mobile device. This drone weights about 200 g and is equipped with a VGA camera for FPV drive control. The devices used to remotely pilot the drones are two Samsung Galaxy Tab 2 tablets for the UAVs and a Xiaomi Redmi 4 Pro smartphone for the terrestrial drone control.

All the experimental tests were conducted in a working environment, which also includes other devices sharing the same WiFi channel. Examples of such ongoing traffic flows are video streaming, audio streaming, video conference calls, web browsing, FTP downloading, and so on.

For the recognition phase, we employed the well-known software tool Weka [15], which

The results have shown that our approach is able to efficiently detect the presence of unauthorized drones in all the considered conditions with an average precision greater than 96 percent.

Classifier	Scenario	UAV class true positive (%)	UAV class precision (%)	UAVs classified as terrestrial drones (%)	UAVs classified as background traffic (%)
Random tree	*Training*	95.5	100	4.5	0
	Sc-1	89.9	100	10.1	0
	Sc-2	93.3	100	4.4	2.2
	Sc-3	87	100	11.3	1.4
Random forest	*Training*	95.5	100	4.5	0
	Sc-1	87.4	100	12.4	0
	Sc-2	93.3	100	4.4	2.2
	Sc-3	84.5	100	14.1	1.4
SMO	*Training*	95.5	100	0.0	4.5
	Sc-1	63	69.4	33.6	3.4
	Sc-2	91.1	100	2.2	6.7
	Sc-3	60	100	59.2	5.6
Logit Boost	*Training*	95.5	100	4.5	0
	Sc-1	82.4	74.8	17.6	0
	Sc-2	93.3	100	4.4	2.2
	Sc-3	83	100	15.5	1.4

Table 3. Comparison of performance results related to UAV detection using different classifiers.

provides an implementation of many efficient machine learning classifiers. In this evaluation, we consider some different classifiers to establish the best performance. In particular, the employed classifiers are:

- **Random tree:** This is a decision tree classifier that considers randomly chosen attributes at each node. It performs no pruning.
- **Random forest:** This is a classifier that consists of a forest of random trees.
- **SMO:** This is a sequential minimal optimization algorithm for training a support vector machine with a polynomial kernel.
- **Logit Boost:** This is a machine learning approach that performs additive logistic regression.

The model related to each classifier has been constructed by using a large set of flow data obtained by applying a 5 *s* partitioning window to a long WiFi recording. The capture was related to a scenario where one UAV, one terrestrial drone, and a number of background TCP/IP traffic sources were present. It is worth noting that these sources generated both audio/video streams and variable length data exchanges. Each model was trained to recognize three different device classes (UAV, terrestrial drone, and background traffic), and it was self-validated by using an 80 percent percentage split. In this first iteration of the performance evaluation, we selected as classification parameters the default configuration available in Weka. Then the thus constructed models were used to classify the traffic flows related to the scenarios described below.

Sc-1: Single Flying Drone: The scenario depicted in Fig. 2a includes a single flying AR.Drone controlled by an Android tablet. The traffic produced by this UAV shares the same channel used by flows related to YouTube and live web radio streaming, together with background WLAN traffic coming from working devices in the nearby area.

Sc-2: Flying and Terrestrial Drones: This experimental setup, shown in Fig. 2b, is quite similar to the previous one. However, in this scenario a terrestrial Jumping Race Max controlled by an Android smartphone is also moving in the area. As before, the testing environment is disturbed by different types of transmissions and multimedia streaming traffic produced by various nearby working devices.

Sc-3: Multiple Flying and Terrestrial Drones: This scenario consists of two flying AR.Drones, plus a terrestrial Jumping Race Max violating the same no-access area. Background interfering flows coming from other devices are also considered in this experimental test. The corresponding general scheme is illustrated in Fig. 2c.

Table 3 reports the results achieved by employing different machine learning approaches. In all the considered scenarios the UAV(s), terrestrial drone, and WLAN traffic took place on the same channel of 2.4 GHz WiFi band. However, the detection algorithm could easily be modified so that the guardian can cyclically scan the different available WiFi channels. The percentage of drone flows is about 1 percent of the total number of flows. The first column of the table specifies the employed classifier; the second column reports the testing scenarios; the third shows the true positive (TP) percentage relative to the UAV class, defined as the number of UAV flows correctly classified as UAV traffic; the fourth column reports the UAV class precision, defined as the ratio between true positives and the sum of true and false positive UAV classification; the fifth and sixth ones refer to the percentage of UAVs erroneously classified as terrestrial drones and as normal background flows, respectively.

Almost all classification approaches allow the achievement of comparable results for the precision level of the flying drone class; only the SMO classifier shows slightly lower performance. Indeed, the UAV class precision is always above 70 percent for all the considered scenarios. It should be noted that in the case of error, all the considered algorithms tend to misclassify UAVs as terrestrial drones. In this sense, the class relative to terrestrial drones may be considered as a warning of the possible presence of undesired UAVs. Rarely, the classifiers confuse the traffic produced by a UAV as background traffic generated by other authorized devices transmitting

in the considered WLAN. The only exception is given by the SMO classifier, which is more prone to misclassifying drones as background traffic than the other machine learning approaches. Our experiments highlight that the highest recognition performance can be obtained when employing decision tree learning methods. We also analyzed the case where the acquired WiFi capture is partitioned with a window of 10 s. The obtained results are quite similar to the ones related to the case shown in Table 3; however, the true positive rate is slightly lower, which is due to the smaller number of flows available for describing the UAV traffic, thus reducing the accuracy of the trained model. Another related aspect to consider is that classifiers are significantly affected by the length of the WiFi capture used as the training set: a long WiFi capture strongly tends to stabilize the behavior of all the considered classifiers.

Conclusions and Future Work

This article has tackled the emerging problem of drone detection for the surveillance of sensitive areas. We have reviewed the main approaches discussed in the literature and have also outlined the main constraints that characterize the enablement of sensitive area surveillance against the presence of low-cost amateur UAVs. We have proposed an effective UAV detection approach based on WiFi statistical fingerprint analysis, which allows easy identification of the presence of unauthorized drones in a nearby area by monitoring the data traffic on a wireless channel. The usefulness of this method is motivated by the increasing amount of commercial amateur drones using WiFi as control and FPV video streaming protocol. We have tested the performance of our method in different scenarios, also in the presence of interfering wireless traffic due to nearby devices. The results have shown that our approach is able to efficiently detect the presence of unauthorized drones in all the considered conditions with an average precision greater than 96 percent. Furthermore, the experiments have revealed that classifiers exhibit significant sensitivity to the length of the WiFi capture used as the training dataset. Therefore, the achieved results suggest that our approach could be a promising technique in the framework of drone surveillance, and it would be worth further research efforts and improvements. To this aim, a deeper analysis and proper tuning of the parameters driving the machine learning algorithms will be fundamental. Moreover, extending the research to a larger set of traffic data derived from different UAV types would strengthen the classification model and further improve the accuracy of amateur drone detection.

Acknowledgement

This publication was financially supported by the Ministry of Education and Science of the Russian Federation (Agreement number 02.a03.21.0008).

References

[1] E. Vattapparamban *et al.*, "Drones for Smart Cities: Issues in Cybersecurity, Privacy, and Public Safety," *2016 Int'l. Wireless Commun. and Mobile Computing Conf.*, Sept. 2016, pp. 216–21.

[2] J. Liu and W. Sun, "Smart Attacks against Intelligent Wearables in People-Centric Internet of Things," *IEEE Commun. Mag.*, vol. 54, no. 12, Dec. 2016, pp. 44–49.

[3] J. Liu *et al.*, "Device-to-Device Communication in LTE-Advanced Networks: A Survey," *IEEE Commun. Surveys & Tutorials*, vol. 17, no. 4, 2015, pp. 1923–40.

[4] M. Dong *et al.*, "UAV-Assisted Data Gathering in Wireless Sensor Networks," *J. Supercomputing*, vol. 70, no. 3, Dec. 2014, pp. 1142–55; http://dx.doi.org/10.1007/s11227-014-1161-6, accessed Aug. 28, 2017.

[5] S. R. Ganti and Y. Kim, "Implementation of Detection and Tracking Mechanism for Small UAS," *2016 Int'l. Conf. Unmanned Aircraft Systems*, June 2016, pp. 1254–60.

[6] M. A. Ma'sum *et al.*, "Simulation of Intelligent Unmanned Aerial Vehicle (UAV) for Military Surveillance," *2013 Int'l. Conf. Advanced Computer Science and Inf. Systems*, Sept. 2013, pp. 161–66.

[7] M. Nijim and N. Mantrawadi, "Drone Classification and Identification System by Phenome Analysis Using Data Mining Techniques," *2016 IEEE Symp. Technologies for Homeland Security*, May 2016, pp. 1–5.

[8] M. Ritchie *et al.*, "Micro-Drone RCS Analysis," *2015 IEEE Radar Conf.*, Oct. 2015, pp. 452–56.

[9] G. J. Mendis *et al.*, "Deep Learning Based Doppler Radar for Micro UAS Detection and Classification," *MILCOM 2016*, Nov. 2016, pp. 924–29.

[10] A. Moses, M. J. Rutherford, and K. P. Valavanis, "Radar-Based Detection and Identification for Miniature Air Vehicles," *2011 IEEE Int'l. Conf. Control Applications*, Sept. 2011, pp. 933–40.

[11] R. Stolkin *et al.*, "Bayesian Fusion of Thermal and Visible Spectra Camera Data for Mean Shift Tracking with Rapid Background Adaptation," *2012 IEEE Sensors*, Oct. 2012, pp. 1–4.

[12] M. Witschi *et al.*, "Detection of Modern Communication Signals Using Frequency Domain Morphological Filtering," *2016 24th Euro. Signal Processing Conf.*, Aug 2016, pp. 1413–17.

[13] Z. Liu *et al.*, "Rise of Mini-Drones: Applications and Issues," *Proc. 2015 ACM Wksp. Privacy-Aware Mobile Computing*, ser. PAMCO '15, 2015, pp. 7–12; http://doi.acm.org/10.1145/2757302.2757303, accessed Aug. 28, 2017.

[14] S. Kamkar, "Skyjack: Autonomous Drone Hacking w/ Raspberry Pi, aircrack & Javascript"; http://www.samy.pl/skyjack/, accessed Aug. 28, 2017.

[15] M. Hall *et al.*, "The weka Data Mining Software: An Update," *SIGKDD Explor. Newsl.*, vol. 11, no. 1, Nov. 2009, pp. 10–18; http:.ust 28, 2017.

Biographies

Igor Bisio (igor.bisio@unige.it) is an assistant professor and member of the research staff of the Telecommunication Research Group and, in particular, of the Digital Signal Processing (DSP) and the Satellite Communications and Networking (SCNL) Laboratories in the DITEN Department of the University of Genoa. His research concerns signal processing over the Internet of Things, context and location awareness, adaptive coding, safety and e-health applications, and satellite communication systems.

Chiara Garibotto is currently working as a Ph.D. student at the Digital Signal Processing Laboratory in the DITEN Department of the University of Genoa. Her main research activities concern signal processing applied to speaker recognition, context awareness, and multiple observations, especially in the framework of smart spaces, the Internet of Things, and intelligent transportation systems.

Fabio Lavagetto is full professor in telecommunications at the University of Genoa. Since 2016 he has been a member of the Board of Directors of the University of Genoa. Since 1995, he has been the head of research of the Digital Signal Processing (DSP) Laboratory in the DITEN Department of the University of Genoa, with responsibility for numerous national and international research projects and contracts.

Andrea Sciarrone is currently a postdoctoral research fellow and member of research staff of the Telecommunication Research Group and, in particular, the DSP Laboratory in the DITEN Department of the University of Genoa. His research concerns signal processing over the Internet of Things, context and location awareness, and safety and e-health applications.

Sandro Zappatore is an associate professor of telecommunications at the University of Genoa. His interests are in the areas of signal processing, especially audio and video coding, and computer networks. His current research is devoted to multimedia network applications, with special interest in grid-based platforms for the control of remote laboratories, wireless sensor networks, and network security.

A deeper analysis and proper tuning of the parameters driving the machine learning algorithms will be fundamental. Moreover, extending the research to a larger set of traffic data derived from different UAV types would strengthen the classification model and further improve the accuracy of amateur drone detection.