A Novel Hybrid Framework for Realistic UAV Detection using a Mixed RF Signal Database

Nassima Merabtine, Valeria Loscri, Djamel Djenouri, Shahid Latif

A Novel Hybrid Framework for Realistic UAV Detection using a Mixed RF Signal Database

Nassima Merabtine
FUN Team, Inria Lille
Villeneuve d'Ascq, France
nassimane@gmail.com

Valeria Loscri
FUN Team, Inria Lille
Villeneuve d'Ascq, France
valeria.loscri@inria.fr

Djamel Djenouri
Univesity of the West of England
Bristol, United Kingdom
Djamel.Djenouri@uwe.ac.uk

Shahid Latif
Univesity of the West of England
Bristol, United Kingdom
Shahid.Latif@uwe.ac.uk

***Abstract*—Advances in Unmanned Aerial Vehicles (UAVs) empower a plethora of applications but also raise significant security and privacy challenges. Effective UAVs detection systems are crucial for mitigating these risks. This paper deals with this problem and tackles the challenges associated with real-world testing and the limitations of existing simulation methodologies for validating and evaluating UAVs detection protocols. A novel, realistic, and extensible framework is introduced, which includes a MATLAB-based surveillance system, a Python-based detection module utilizing Stacked Denoising Autoencoder (SDAE) and Local Outlier Factor (LOF) algorithms, and a hybrid database of both real and synthetic wireless RF signals. The synthetic wireless dataset is generated by the proposed surveillance system module. The alignment between the synthetic and real data is validated with an average Mean Squared Error (MSE) of less than 0.25. The detection module proves highly effective, achieving 96% accuracy in correctly classifying Wi-Fi signals and 88% accuracy in identifying UAV signals as anomalies (outliers). This innovative approach facilitates ongoing research and development in UAV detection, with the extensibility to incorporate new RF signal types and UAV models.**

***Index Terms*—Anomaly Detection, drone detection, UAVs, Machine Learning, Cyber Critical Infrastructures.**

I. Introduction

Unmanned Aerial Vehicles (UAVs), commonly known as drones, have seen unprecedented growth in recent years due to their wide-ranging applications, from recreational activities to critical industrial operations. While the benefits of UAVs are undeniable, their widespread civilian use has raised significant concerns regarding security, privacy, and safety. A common misuse of drones involves illegal monitoring and surveillance aimed at acquiring private information from sensitive zones. Effective drone detection systems play a critical role in mitigating this risk and safeguarding public safety, critical infrastructure, and personal privacy. Numerous drone detection protocols have been proposed over recent years, spanning diverse categories, including imaging, radar, acoustic signals, Radio Frequency (RF), and hybrid detection solutions. Each technology comes with its merits and challenges. RF-based detection offers several advantages, including the ability to identify drones in both Line-of-Sight (LoS) and Non-Line-of-Sight (NLoS) conditions, low cost, non-intrusiveness, and privacy preservation in indoor spaces. Additionally, RF signals can be utilized for further analysis, facilitating the geo-localization and tracking of UAVs. Most recently proposed RF-based drone detection protocols leverage advanced Machine Learning (ML) and Deep Learning (DL) algorithms that are able to capture the rich information present in complex RF signals and thus enhance the detection accuracy.

There are two approaches for validating and evaluating RF-based UAV detection protocols: i) collecting data and conducting real experiments using drones, ii) performing simulations. While the first approach is the most realistic, it presents significant challenges. Outdoor drone testing is complex and financially costly due to the risks of mishandling and crashes. Furthermore, flying drones in urban environments typically requires flight authorizations from authorities in most countries. For these reasons, works considering real testing perform their experiments either in indoor environments [1], or in rural settings [2]. Indoor and rural testing are not realistic since critical infrastructures are located outdoors and in predominantly urban areas where numerous RF sources operate in the same frequency bands as commercial drones (2.4 GHz and 5 GHz), such as Wi-Fi, Bluetooth, and mobile cellular networks. Moreover, studies in this category are often limited by the number and types of UAVs used and the considered RF sources, providing no insight into out-of-distribution UAV RF signals from different drone models [3]. Conversely, many existing works, such as [4], validate their proposed solutions through simulations based *exclusively* on pre-established UAV RF signal databases. These databases, however, lack the diversity of signal patterns and scenarios as mentioned before.

In this context, the aim of this work is to address the challenges of complex real-world testing and the limitations of existing simulation methodologies and tools for drone detection by laying the cornerstone of a ***hybrid*** and ***extensible*** realistic simulation-based testing framework to foster research in this area. The proposed framework comprises three main components: a surveillance system module developed in MATLAB, a detection module developed in Python, and a hybrid database that mixes realistic and synthetic datasets. The contributions of this work can be summarized as follows:

- The framework can reproduce an urban environment via the surveillance system module, which allows for the creation of different types of wireless nodes, such

as Wi-Fi (802.11b/g/n/ac), Bluetooth, etc. A multitude of scenarios can be created by adjusting many parameters, such as node positions, signal strength, mobility models, and more. The efficiency of this module has been tested, and 300 different real Wi-Fi signals have been faithfully reproduced by the module with an average Pearson Correlation of 0.75 and an average MSE lower than 0.25. The detection module is based on a Stacked Denoising Autoencoder (SDAE) and Local Outlier Factor (LOF) algorithms. Results show the ability of this module to distinguish UAV signals as anomalies with an accuracy of 88%. To the best of our knowledge, this is the first attempt to create a realistic simulation framework for detecting UAVs.

- The framework uses a mixed database incorporating both real and synthetic Wi-Fi signals and real RF UAV signals. We have established a synthetic database with several types of Wi-Fi signals, i.e., 802.11n^{TM} (Wi-Fi 4 HT and non-HT), 802.11ac^{TM} (Wi-Fi 5), 802.11ax^{TM} (Wi-Fi 6 and 6E), over different distances from the reception RF systems simulating the critical infrastructure. To the best of our knowledge, only Wi-Fi 4 has been considered in the context of drone detection in existing RF signal drone databases. The concordance between synthetic and realistic Wi-Fi signals has been proven, as previously mentioned.
- The standout feature of this framework is its extensibility. Primarily, the framework can be continuously refined and expanded to emulate urban environments. This can be done by incorporating new models of RF signals into the surveillance module, such as Bluetooth, Zigbee, Microwave Ovens, Wireless Video Transmitters, RFID Systems, etc., all of which can be accurately emulated in MATLAB. The number of wireless nodes, along with their spatial parameters, packet size, throughput, and noise, can also be adjusted. Moreover, the RF signals database can be further enriched by including additional existing or newly proposed drone databases. This can be achieved by developing a module capable of handling the heterogeneity of data formats contained in various RF signal databases. This is critical because the efficacy of ML and DL-based detection protocols depends on the quality and diversity of the data used.

The rest of the paper is organized as follows: Section II reviews the related literature and demonstrates the original contributions of this work. Section III presents the proposed simulation framework. Section V discusses the obtained results IV. The conclusion of this paper and some interesting insights on future works are given in Section V.

II. Related Works

ML and DL-based algorithms have been largely explored for RF drone detection in the literature, such as KNN [5], [6], DNN [7], [8], and CNN [9]. Signal processing techniques, including DFT, STFT, and WPT are commonly utilized to extract pertinent features from RF signals [1]. Some recent studies advocate for the direct utilization of raw RF signals as input to enhance detection accuracy [10]. Identification and classification of drones have also been considered in recent works, e.g., [11]–[13], but this is beyond the scope of this paper and limits the detection. A comprehensive review of drone detection methodologies is also out of the scope of this paper, but this is available in the current literature, e.g., [14].

As the performance of ML and DL-based UAV detection protocols is intricately linked to the underlying RF signals database employed, we conducted an exhaustive review of existing databases containing RF signals from drones, which are summarized in Table I. These disparities encompass critical factors such as the environment of experimentation (indoors or outdoors), the variety and number of drones utilized, and the types of signals captured (uplink and/or downlink). It has been observed that all existing databases, except [15], focus on the 2.4 GHz frequency band. Furthermore, some databases such as [1], [16], [17] fail to account for other RF sources in the environment, representing a significant limitation in evaluating database realism.

In a broader context, existing drone detection solutions predominantly rely on either constructing their own RF drone databases (only 7 works in the literature undertake this approach) or leveraging pre-established ones. However, only four works have conducted outdoor experiments, all within rural settings. Nevertheless, the realism of indoor and rural testing scenarios is questionable, given that critical infrastructures are primarily located outdoors in urban environments characterized by high wireless traffic. Moreover, each database's scope is restricted concerning the number and types of UAVs and other RF sources considered, thereby limiting the breadth of testing and the credibility of drone detection solutions validated through these databases. This constraint impedes insights into a solution's ability to detect drone models not encompassed in the database or its capacity to differentiate between drones and other RF signals that are absent from the dataset.

To bridge this gap, the principal objective of this work is to develop a realistic and extensible simulation framework. This framework is based on a real RF drone database and augmented with synthetic RF signals modeling various urban scenarios. This enables comprehensive testing of drone detection solutions in distinguishing drone signals amidst the multitude of other RF sources present in urban environments. The proposed framework is detailed in the next section.

III. Proposed Framework

The proposed framework is composed of four main components: i) the surveillance system module, ii) the synthetic RF signals database, iii) the real RF signal databases, and iv) the anomaly detection module. The overall architecture of the framework is illustrated in Fig. 1. As demonstrated

TABLE I
SUMMARY OF EXISTING RF SIGNAL DATABASES.

Ref	Year	Environment	Number and type of drones	Signals type	Frequency band	Other RF sources
[16]	2018	Indoor/Outdoor	1 drone: Phantom4 Pro	uplink and downlink	2.4 GHz	/
[17]	2018	Outdoor	1 drone: DJI Phantom3	downlink	2.4 GHz	/
[18]	2019	Outdoor	1 drone: Mavic Air	downlink	2.4 GHz	Wi-Fi
[19]	2019	Indoor	14 drone controllers: various models e.g., DJI Inspire, Phantom 4Pro, Phantom 3)	uplink	2.4 GHz	Wi-Fi, Bluetooth, and microwave ovens
[1]	2019	Indoor	3 drones: Bebop, AR, Phantom	downlink	2.4 GHz	/
[15]	2022	Indoor	3 drones: Bebop, AR, Phantom	downlink	2.4 GHz and 5 GHz	Wi-Fi
[2]	2022	Outdoor	6 drones: DJI (Phantom 4, Inspire, Matrice 600, Mavic Pro 1), Beebeerun (mini quadcopter), 3DR (Iris FS-TH9x)	uplink and downlink	2.4 GHz	Wi-Fi and Bluetooth

in this figure, the synthetic database is generated by the surveillance system module. Both the synthetic and real databases are used by the detection module. The four components are described hereafter.

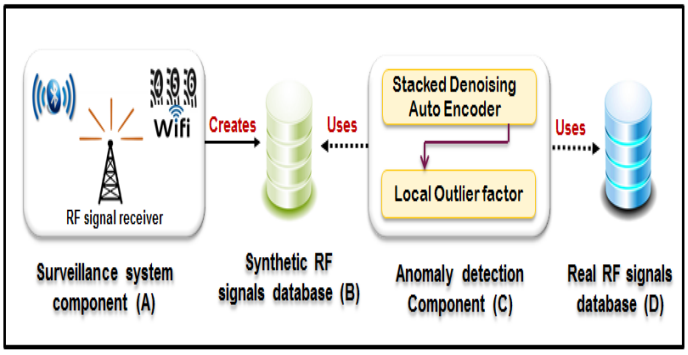

Fig. 1. The overall architecture of the proposed drone detection simulation framework.

A. Surveillance system module

The WLAN toolbox in MATLAB was used to develop this module, which offers the advantage of configuring the node protocol stack layers from the physical to the application layer and analyzing their interactions. Using this toolbox, we created three WiFi nodes: station "1", which communicates with its AP (station "2"), and station "3", which serves as the monitoring node that recovers the signals exchanged between the first station and the AP. Figure 2 shows a simplified view of the class diagram used to implement this monitoring scenario. In the “Application level” class, the scenario is implemented by specifying the simulation duration, the number of nodes, their positions, etc. This class is then called the "hWirelessNetworkSimulator" class, which simulates the wireless network for the fixed simulation time by invoking the "hWLANNode" class. The latter creates objects corresponding to each instantiated WLAN node, comprising three layers application, MAC, and physical. The “hWLANNode” class primarily interacts with the “hPHYTx” and “hPHYRx” classes, which are the physical layer interfaces responsible for sending and receiving signals, respectively. The hPHYTx class supports MAC layer request processing, transmission power management (Tx power), and waveform creation (PPDU), among other functions. The last operation is carried out using the "WlanWaveformGenerator" class, which creates signals in the form of IQ. This framework is extremely versatile and enables, as we will demonstrate in the next section, the generation of various scenarios by considering different types of WiFi devices, different packet sizes, and varying positions and distances of the nodes.

B. Synthetic RF signals database

Based on the surveillance system module presented in the previous subsection, we conducted several simulations to create a new synthetic RF signals database representing various urban scenarios. Each simulation lasted 100 ms and considered different types of WiFi sources. The impact of the distance between station 2 and station 3 (the monitoring node) was evaluated by considering distances ranging from 5 to 40 meters. Simulation parameters used to create the synthetic database are presented in Table II. As described in the previous section, the signals are recovered in the form of IQ data. Signals are sampled and consisting of five million points each. They are then segmented into slices of 1024 points each. This preprocessing is done to ensure the interoperability of our synthetic database with the real RF database considered in our framework, which will be presented in the next subsection.

C. Real RF signal database

To enhance the ’realism’ aspect of the proposed framework, a realistic RF signal database has been integrated. We chose the cardRF database proposed in [2] based on our study explained in Section II of this paper. This choice was motivated by various factors, including the diversity

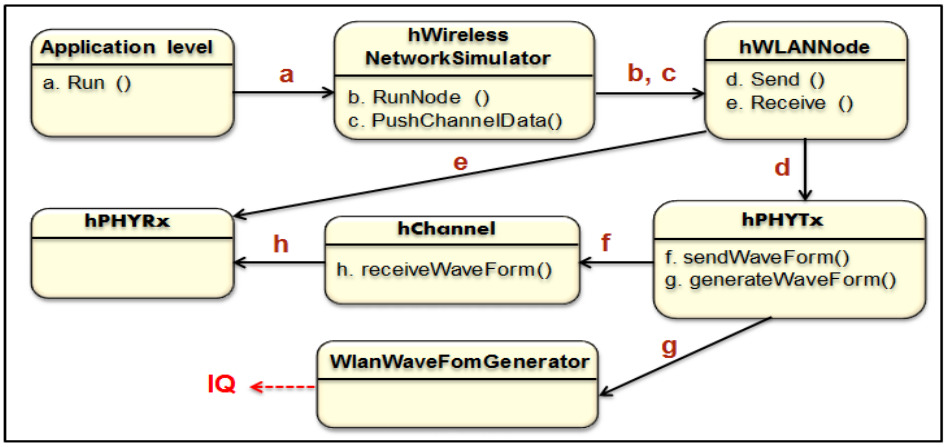

Fig. 2. A simplified diagram of the surveillance system module implemented in Matlab.

TABLE II
SOME OF THE PARAMETERS USED TO GENERATE THE RF SYNTHETIC DATABASE.

Parameter	Values
Number of nodes	3
Simulation duration	100 milliseconds
WiFi type	802.11ax^{TM} WiFi 6 and 6E, 802.11ac^{TM} WiFi 5, 802.11n^{TM} WiFi 4 HT and Non-HT
Distance	5, 10, 20, 30, 40 m
Transmission channel	36
Data Rate	100000 Kbps
Packet Size	1500

and number of drones used and the consideration of other RF signals. The signal sources included in this database are summarized in Table III.

TABLE III
LIST OF DEVICES CONSIDERED TO CONSTRUCT THE CARDRF DATABASE [2]

Signal Source	Type of Device	Type of Model/Technology
DRONE	**DJI**	**Phantom 4, Inspire, Matrice 6000, Mavic Pro 1**
DRONE	**Beebeerun**	**FPV RC drone**
DRONE	**3DR**	**Ins FS-TH9x**
Bluetooth	**Apple**	**iPhone 6S, 7s, iPad 3**
Bluetooth	**FitBit**	**Charge3 smartwatch**
Bluetooth	**Motorola**	**E5 Cruise**
WiFi	**Cisco**	**Linksys E3200**
WiFi	**TP-link**	**TL-WR940N**

D. Detection module

Existing simulators fail to accurately model the physical layer of drones, unlike WiFi and Bluetooth that are well-modeled in MATLAB. The detection module addresses this critical gap by considering the drone signals as anomalies. It involves training the anomaly detection algorithm on WiFi and Bluetooth signals and then identifying drone signals as "anomalous" or "aberrant," indicating potential risks. This process unfolds in two primary steps: first, using Stacked Denoising Autoencoders (SDAE) to compress wireless data to facilitate the efficient handling of numerous signals. Second, employing the Local Outlier Factor (LOF) method to distinguish legitimate sources (Bluetooth or WiFi) from illegitimate ones, specifically, drone signals. SDAE and LOF have been chosen for their proven effectiveness in data compression and detecting local outliers. To implement this approach, we utilized the code provided by [2]. A brief presentation of the SDAE and the LOF algorithms is given below:

1) Stacked Denoising Autoencoder - SDAE: Effective compression of wireless data before employing ML algorithms is pivotal for optimizing signal processing and analysis. In this work, we rely on an SDAE algorithm which is chosen for its robustness in noisy and nonlinear environments. The SDAE comprises three fundamental stages: encoding, coding, and decoding. It focuses on extracting key features efficiently. The sample size was reduced from 1024 to 32 points, as detailed in [2].

2) Local Outlier Factor (LOF): This is a highly effective method for identifying outliers in a dataset by measuring their distance from neighboring points [2]. It operates through four main phases:

- Estimation of k-th nearest neighbor distances
- Calculation of reachability distances based on the k-distance
- Computation of Local Reachability Density (LRD) using reachability distances
- Estimation of LOF based on LRD values

A critical aspect of LOF involves selecting appropriate hyperparameters, particularly the number of nearest neighbors and the choice of distance metric. We used the same parameters as in [2].

IV. Performance Evaluation

In this section, the proposed framework is evaluated from two key perspectives: i) the concordance between the synthetic Wi-Fi signals (generated by our surveillance system) and real ones to validate the realism of the synthetic data, ii) the precision of the LOF algorithm.

A. Data concordance

We reproduced 300 different real Wi-Fi signals from the cardRF database [2]. To evaluate and compare these signals, we calculated several comparison criteria divided into two main categories. The first category, signal characteristics, includes parameters such as frequency, phase, and signal type. The second category, statistical metrics, comprises various measures including the mean, variance, Pearson correlation, Mean Squared Error (MSE), and Root Mean Squared Error (RMSE).

The average results of 300 pairs of signals (real, synthetic) are presented in Table IV. As noticed from this table, the comparison of the average results between the real and synthetic signals reveals a strong similarity between the synthetic and real signals. The frequency of the synthetic signal (2402343750 Hz) closely matches the real signal (2402408854.1667 Hz), with nearly identical amplitudes (1 vs. 1.0005) and exact phase values. Although the mean values show a reduction in bias for the synthetic signal (-0.038865 vs. $6.8704e^{-06}$) and the variance differs. The Pearson Correlation of 0.74238 indicates a strong positive linear relationship, and the MSE below 0.25 highlights the synthetic signal's overall accuracy in approximating the real signal.

TABLE IV
Comparison of Real and Synthetic Signal Properties

Property	**Real signal**	**Synthetic signal**
Frequency	2402408854.1667	2402343750
Amplitude	1	1.0005
Phase	0.36179	0.36179
Mean	-0.038865	6.8704e-06
Variance	0.33841	0.46157
Pearson Correlation	0.74238	
MSE	0.23088	
RMSE	0.47808	

Additionally, Table IV presents the time-domain representation (amplitude vs. time plot) comparing synthetic and real signals. For this comparison, a pair of signals was randomly selected, and the resulting graph illustrates the similarity between the two signals over time.

B. Detection performance

The accuracy and effectiveness of the LOF algorithm in detecting anomalous signals are evaluated in this part, with a focus on its capability to distinguish between legitimate WiFi sources and UAV signals. For this, we combined the real and simulated databases presented above to construct a mixed database, which was subsequently split into 80% for training and 20% for testing. The training test is composed

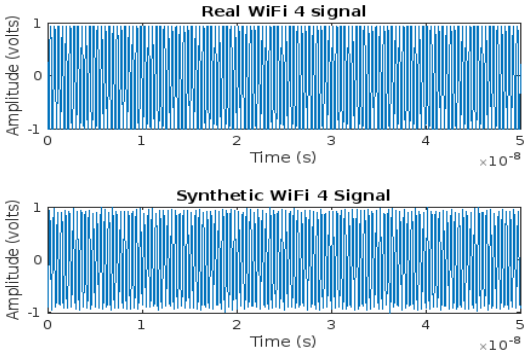

Fig. 3. Comparison between real and synthetic WiFi signals.

of 50% of real WiFi signals and 50% of synthetic ones. The 20% test set contains 50% WiFi signals and 50% drone signals. The WiFi signals are composed of 50% real WiFi signals and 50% WiFi signals generated by the MATLAB simulator. All drone signals are real. After training the LOF on mixed WiFi signals, we achieved very satisfactory results. We calculated various evaluation metrics, namely accuracy, precision, recall, and F1 score, using the formulas below:

$$Accuracy = \frac{T_P + T_N}{T_P + T_N + F_P + F_N} \tag{1}$$

$$Precision = \frac{T_P}{T_P + F_P} \tag{2}$$

$$Recall = \frac{T_P}{T_P + F_N} \tag{3}$$

$$F_1 score = 2\frac{PrecisionRecall}{Precision + Recall} \tag{4}$$

Considering the WiFi class as the target, the detection module was able to detect 96% of WiFi signals (both real and simulated) as WiFi. Furthermore, when the non-WiFi class (drone in our case) was set as the target, the algorithm correctly classified approximately 88% of drone signals. The confusion matrices presented in tables V, VI, along with table VII, provide more detailed insights into these results. In Table V, the confusion matrix with WiFi devices as the target, the model correctly classified 3168 WiFi signals and misclassified 505 drone signals as WiFi (false positives). The misclassifications can be attributed to the similarity between certain WiFi and drone signal characteristics, particularly in the synthetic WiFi data Table VII further summarizes key performance metrics, including accuracy, precision, recall, and F1 score, providing comprehensive insights into the module's robust performance across different signal classes.

V. Conclusions and Future Works

In response to the increasing prevalence of UAVs and their significant security and privacy challenges, this paper introduces an innovative simulation-based testing framework. It combines real-world and simulated data and uses

TABLE V
CONFUSION MATRIX - WIFI DEVICES AS TARGET

Prediction/Reality	WiFi	Non-WiFi
WiFi	3168	249
Non-WiFi	505	2913

TABLE VI
CONFUSION MATRIX - NON WIFI DEVICES AS TARGET

Prediction/Reality	WiFi	Non-WiFi
WiFi	2913	505
Non-WiFi	249	3168

a LOF algorithm to detect UAV signals as anomalies. Results demonstrate high performance, with the detection module achieving 96% accuracy in recognizing Wi-Fi signals and 88% accuracy in identifying UAV signals as anomalies. This framework not only addresses the limitations of current real testing and simulation approaches but also supports ongoing research and development in UAV detection systems. Future efforts will focus on expanding the framework's capabilities to incorporate diverse recent RF signals and drone models and implementing more complex and realistic scenarios. Testing more effective detection algorithms and integrating other existing real RF drone datasets are also promising avenues. Additionally, integrating a geolocation algorithm to pinpoint detected "anomalous" signals represents another compelling direction for future research.

ACKNOWLEDGMENT

This work has been partially supported by the ASTRID-ANR DEPOSIA project and the Horizon Europe MLsysOps project. It has also been supported in part by the EU CHIST-ERA project (Grant EP/Y036301/1 from EPSRC, UK) and in part by the AGYA Academy (Grant 01DL20003 from BMBF, Germany).

TABLE VII
SOME PERFORMANCE METRICS FOR THE LOF-BASED DETECTION MODULE

Class Target	Accuracy	Precision	Recall	F1 Score
WiFi	0.96	0.92	0.86	0.88
Non-WiFi	0.88	0.85	0.92	0.88

REFERENCES

[1] Abdulla Al-Ali Amr Mohamed Tamer Khattab MHD Saria Allahham, Mohammad F. Al-Sa'd and Aiman Erbad. Dronerf dataset: A dataset of drones for rf-based detection, classification and identification. *Data in Brief*, 26:104313, 2019.

[2] Olusiji Medaiyese, Martins Ezuma, Adrian Lauf, and Ayodeji Adeniran. Hierarchical learning framework for uav detection and identification. *IEEE Journal of Radio Frequency Identification*, 6:176–188, 01 2022.

[3] Yufan Chen, Lei Zhu, Yuchen Jiao, Changhua Yao, Kaixin Cheng, and Yuantao Gu. An extreme value theory-based approach for reliable drone rf signal identification. *IEEE Transactions on Cognitive Communications and Networking*, 10(2):454–469, 2024.

[4] Rabiye Kılıç, Nida Kumbasar, Emin Oral, and Ibrahim Ozbek. Drone classification using rf signal based spectral features. *Engineering Science and Technology, an International Journal*, 28, 07 2021.

[5] Mhd Al-lahham, Tamer Khattab, and Amr Mohamed. Deep learning for rf-based drone detection and identification: A multi-channel 1-d convolutional neural networks approach. pages 112–117, 02 2020.

[6] Sara Al-Emadi and Felwa Al-Senaid. Drone detection approach based on radio-frequency using convolutional neural network. 12 2020.

[7] Karel Pärlin, Taneli Riihonen, Gaspar Karm, and Matias Turunen. Jamming and classification of drones using full-duplex radios and deep learning. In *2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications*, pages 1–5, 2020.

[8] Enyinna Rexcharles, Mustapha Deji Dere Donatus, Happiness Donatus Ifeyinwa, Osichinaka Chiedu Ubadike, Bashir Abdulrazaq Muhammad, and F. Ohemu Monday. Development of an optimised neural network model for rf based uav detection and identification. In *Dutse Journal of Pure and Applied Sciences*, volume 8, 2023.

[9] Boban Sazdić-Jotić, Ivan Pokrajac, Jovan Bajcetic, Boban Bondzulic, and Danilo Obradovic. Single and multiple drones detection and identification using rf based deep learning algorithm. *Expert Systems with Applications*, 187:115928, 09 2022.

[10] Sanjoy Basak, Sreeraj Rajendran, S. Pollin, and Bart Scheers. Drone classification from rf fingerprints using deep residual nets. pages 548–555, 01 2021.

[11] Domenico Lofù, Pietro Tedeschi, Tommaso Di Noia, and Eugenio Di Sciascio. URANUS: radio frequency tracking, classification and identification of unmanned aircraft vehicles. *IEEE Open Journal of Vehicular Technology*, 4, 2023.

[12] Minjing Li, Donglai Hao, Jiaming Wang, Shuozhe Wang, Zijian Zhong, and Zhiwen Zhao. Intelligent identification and classification of small UAV remote control signals based on improved yolov5-7.0. *IEEE Access*, 12:41688–41703, 2024.

[13] Sanjoy Basak, Sreeraj Rajendran, Sofie Pollin, and Bart Scheers. Combined rf-based drone detection and classification. *IEEE Trans. Cogn. Commun. Netw.*, 8(1):111–120, 2022.

[14] Nader Al-lQubaydhi, Abdulrahman Alenezi, Turki Alanazi, Abdulrahman Senyor, Naif Alanezi, Bandar Alotaibi, Munif Alotaibi, Abdul Razaque, and Salim Hariri. Deep learning for unmanned aerial vehicles detection: A review. *Computer Science Review*, 51:100614, 2024.

[15] Boban Sazdić-Jotić, Ivan Pokrajac, Jovan Bajcetic, Boban Bondzulic, and Danilo Obradovic. Single and multiple drones detection and identification using rf based deep learning algorithm. *Expert Systems with Applications*, 187:115928, 09 2022.

[16] Hao Zhang, Conghui Cao, Lingwei Xu, and T. Aaron Gulliver. A uav detection algorithm based on an artificial neural network. *IEEE Access*, PP:1–1, 05 2018.

[17] Samith Abeywickrama, Lahiru Jayasinghe, Hua Fu, Subashini Nissanka, and Chau Yuen. Rf-based direction finding of uavs using dnn. In *2018 IEEE International Conference on Communication Systems (ICCS)*, pages 157–161, 2018.

[18] Yan Teoh and Chee Kiat Seow. Rf and network signature-based machine learning on detection of wireless controlled drone. pages 408–417, 06 2019.

[19] Martins Ezuma, Fatih Erden, Chethan Anjinappa, Ozgur Ozdemir, and Ismail Guvenc. Micro-uav detection and classification from rf fingerprints using machine learning techniques. pages 1–13, 03 2019.