Context-Aware Drone Detection

Gabriele Oligeri
Division of Information and Computing Technology, College of Science and Engineering, Hamad Bin Khalifa University, Qatar Foundation, Doha, Qatar.

Savio Sciancalepore
Eindhoven University of Technology (TU/e), Eindhoven, The Netherlands.

ABSTRACT

Current commercial and research solutions for drones' detection do not make any assumption on the scenario deployment, as well as the unique mobility pattern associated with the drone's trajectory. Indeed, drones' trajectory is different from the one of people moving at the ground level, being independent of roads layout and obstacles on their path: drones fly directly towards their target, minimizing the travel time and the possibility of being detected.

Grounding on this intuition, we propose CADD, a solution enabling drone detection via context-related information. CADD leverages a sensing infrastructure to locate and track all the devices in the area to be protected, and it distinguishes the trajectory of a drone as an anomaly with respect to a ground-truth of *allowed* trajectories—the ones generated by the devices at the ground level, belonging to vehicles and users within them. We evaluated the performance of CADD over a real dataset of moving vehicles (taxi) in both urban and rural scenarios, resulting in an overall accuracy of 0.91 and 0.84, for the rural and the urban scenario, respectively.

The performances of CADD confirm the effectiveness of our solution and show its promising potential for context-related drone detection.

CCS CONCEPTS

• **Security and privacy → Mobile and wireless security**; *Domain-specific security and privacy architectures*; • **Networks → Cyber-physical networks**.

KEYWORDS

Unmanned Aerial Vehicles; Drone Detection; Context-Aware Intrusion Detection; Localization; Anomaly Detection.

ACM Reference Format:
Gabriele Oligeri and Savio Sciancalepore. 2022. Context-Aware Drone Detection. In *Proceedings of the 8th ACM Cyber-Physical System Security Workshop (CPSS '22), May 30, 2022, Nagasaki, Japan.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3494107.3522777

1 INTRODUCTION

In the last decade, Unmanned Aerial Vehicles (UAVs), as known as drones, have gained increasing popularity both in the Industry and Academia [9, 16]. Indeed, thanks to their mobility and enhanced flexibility, drones are increasingly used in a large variety of application domains, including transportation and delivery systems, health, telecommunications services, agriculture, surveillance, and military domains, to name a few [5, 23]. Such an increasing trend is confirmed by recent market studies, indicating that the global commercial drone market is projected to reach the size of around 58.4 billion U.S. dollars in 2026, growing at a compound annual growth rate of over 16 % between 2021 and 2026 [33].

Although enabling rapid and flexible service development, drones can also be used by malicious actors to disrupt critical operations and jeopardize people safety [3, 12, 35, 37]. News about incidents involving drones are even more frequent in the media, and Critical Infrastructures (CIs) such as airports, oil and gas production plants, as well as crowded mass events, are the preferred targets for disrupting drone-based attacks [6, 11, 26]. The aforementioned incidents call for efficient drones detection solutions, able to detect in advance the drones' presence in protected areas, thus mitigating threats coming from the aerial domain.

At the time of this writing, several research-oriented and industry-based solutions for drone detection are available, and also commercialized on the market (see Section 8 for a comprehensive overview). Such solutions rely on several features and metrics to perform drone detection, e.g., including radar, visual, audio, RF emanations, and traffic-based strategies. Also, several projects on drone detection have been funded by the European Union within the H2020 program, such as *SafeShore* [27] and *Aladdin* [2], to name a few.

However, such solutions typically have limitations due to the specific context where they are deployed. For instance, visual-based detection methods are limited by the range and resolution of the camera, audio-based techniques do not work in busy contexts (e.g., cities), and RF-based strategies can be severely affected by packet losses and interference phenomena. In addition, none of the above-cited techniques takes into account the features of the underlying scenario and the unique mobility properties of the drones—all features and functionalities that make them the preferred tool of attackers. Indeed, while moving towards a target, drone's trajectory can be considered almost independent of roads' layout, buildings, and obstacles on the path, thus drastically reducing the time to approach the target, while maximizing the damage. Our intuition is that, leveraging such a unique mobility pattern, it could be possible to come up with a context-aware drone detection solution, which compares the mobility pattern of users (vehicles, pedestrians, bikers) with the one of drones to detect them.

Although such an intuition might appear straightforward, drones detection using only context-related information presents many challenges: (i) first, any location information broadcasted by transmitting entities cannot be trusted, thus requiring the deployment of a reliable and robust wireless localization strategy; (ii) second, several additional digital sources might use the WiFi communication technology to emit wireless messages, including mobile phones used by pedestrians and cars drivers, thus requiring the deployment

CPSS '22, May 30, 2022, Nagasaki, Japan.

of a solution able to discriminate each source based on context-related information; and, finally, (iii) the layout of the roads and buildings might affect the accuracy of the localization algorithm and the capability to discriminate drones, thus requiring specific fine-tuning of the detection strategy.

Contribution. In this paper, we make the first step towards a Context-Aware Drone Detection (CADD) strategy. Our solution, namely CADD, can discriminate a drone flying over a No-Fly Zone (NFZ) from other moving entities in the area (vehicles, pedestrians, bikers), based on trajectory patterns extracted from GPS locations, independently of the speed and the height of flight. CADD leverages a distributed sensing infrastructure to compute the position of the emitting entity—via the Recursive Least Square (RLS) algorithm–and perform the tracking of the mobile target. Moreover, CADD can be deployed at no cost when drones broadcast radio messages, in line with the recent RemoteID regulation promulgated by the FAA [13]. We extensively tested the performance of CADD via simulations performed on a real dataset, both in an urban and in a rural scenario. Our results show that CADD can detect an unauthorized drone with outstanding accuracy, i.e., 0.91 and 0.84 in a rural and in an urban scenario, respectively. At the same time, to avoid detection, the drone should follow a path that matches the layout of roads and buildings in the playground, then becoming easily detectable through additional available techniques (e.g., visual).

Roadmap. The rest of the paper is organized as follows. Section 2 discusses the drone's detection problem introducing the main concepts adopted throughout this paper, Section 3 introduces the scenario and the adversary model considered in our work, while Section 4 provides a quick overview of our solution. Section 5 details on the adopted techniques to compute the location and tracking of the drone, Section 6 presents the performance associated with CADD, while Section 7 highlights various features and limitations of our solution. Section 8 summarizes the most important related work, and finally, Section 9 tightens conclusions and draws future research activities.

2 PROBLEM STATEMENT

We tackle the problem of detecting the presence of a drone flying over a No-Fly Zone. We consider the following architectural elements:

- **No-Fly-Zone (NFZ)**. This is the area we want to protect from the drone flight. We assume the No-Fly Zone cannot be physically isolated, since people should freely move inside and across of it. A typical example is an event involving VIPs in a crowded and open area.
- **Drone**. We assume an UAV featuring a radio transducer, thus transmitting radio messages during its flight, in line with the recent RemoteID regulation promulgated by the FAA [13],[36]. This might be the case of a radio-controlled drone, i.e., a Remotely Piloted Aircraft System (RPAS), requiring to communicate with the controller or a First-Person View (FPV) system. In the case of autonomous aerial vehicles (non-RPAS), we can assume that the drone features a camera, thus transmitting the associated video stream to the user.
- **Sensors network**. The No-Fly Zone is monitored by a network of N interconnected sensors $\{n_0, \ldots, n_i, \ldots, n_{N-1}\}$, which have the capability of eavesdropping on the radio packets of all the devices in the (No-Fly Zone) area. Note that this is not a limiting assumption, as the vast majority of NFZs already use sensors to detect invasions of their private areas. At the same time, we highlight that capturing such wireless signals only requires a probe, listening to the wireless channel, being relatively cheap and easy to deploy.
- **Data Processing Server**. It is a central server unit, interconnected with the sensor network, used to collect the data generated by each sensor and to process them, to detect the presence of any anomaly (drone) in the No-Fly Zone.

Without loss of generality, we assume that all the entities involved in the playground use the WiFi communication system to deliver wireless messages. On the one hand, we remark that such an assumption is in line with the actual drones deployments, as the RemoteID regulation is already imposing drones to deliver wireless messages using the WiFi technology. On the other hand, we highlight that this assumption makes the drone detection task even more difficult, due to the likely presence of many other devices sharing and using the same communication technology. Nevertheless, if the drone resorts to an ad-hoc communication system characterized by a special frequency and modulation, we only require the sensing infrastructure to monitor the radio spectrum, including the frequencies adopted by the drone. Indeed, our solution only requires estimating the Received Signal Strength (RSS) at specific locations (sensing nodes), without considering the content of the messages, which might also be encrypted.

For each device in the area, the sensor network will: (i) estimate the RSS associated with the signals coming from the device; (ii) perform a rough localization of the device; and (iii) evaluate if the device trajectory represents an anomaly compared to a previously generated ground-truth. Our intuition is that drones' trajectories are significantly different from any other users' category (pedestrians, cyclists, and drivers), thus making the drone trajectory unique when compared to all the possible trajectories previously collected in the No-Fly Zone. For instance, a drone usually flights directly to the target or it hovers around it, (almost) independently of the objects and man-made constructions at the ground. In turn, the aforementioned elements represent an obstacle for the users moving at the ground—thus being forced to go through different trajectories, as depicted in the toy representation of Figure 1.

Adversary Model. We assume an adversary $\mathcal{E}$, being able to radio-control a drone, and interested to fly the drone over a NFZ in order to reach a target. The aims of $\mathcal{E}$ could be manifold, e.g., crash the drone into a target, threatening people safety, or violating a restricted area, to take photos or audio/video recordings of the area itself. Moreover, we do not take any specific assumptions on how $\mathcal{E}$ controls the drone: it can be either through a Remote Controller connected wirelessly to the drone, or via the Internet (if the drone is equipped with a SIM card) or pre-programmed (if the drone is fully autonomous). Conversely, our key assumption is that the drone features a radio transducer and it keeps broadcasting radio messages for the whole flight. Modern drones generate radio traffic for several purposes, including the delivery of video-streaming through

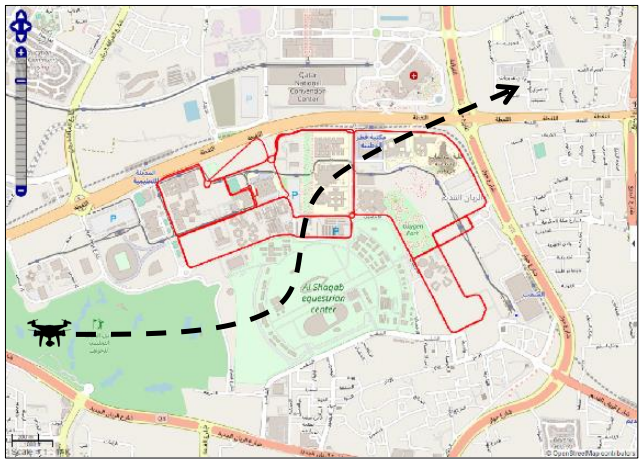

Figure 1: Context-aware drone detection: the trajectory performed by the drone can be easily detected as an anomaly respect to the set of allowed trajectories (ground truth) in the Non-Fly-Zone (NFZ).

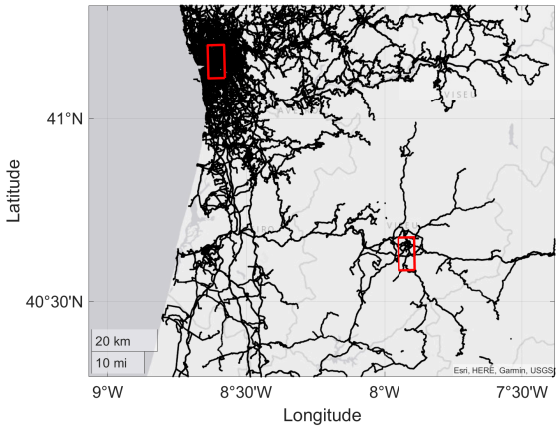

Figure 2: Dataset from [17]: GPS coordinates of taxi vehicles in the city of Porto (Portugal). Red rectangles refer to the two sub-scenario considered in this paper, i.e., urban and rural areas.

the FPV channel [18], of telemetry data to the controllers via the MAVLink protocol [14] or the broadcast of periodic identification data [13].

Evasion techniques. A smart adversary might flight the drone according to a not-suspicious trajectory, i.e., a trajectory typical of another entity such as either a street (vehicle) or a cycle path (cyclist). Although we recognize this limitation, we highlight that the deployment of our solution significantly reduces the possible attack trajectories, exposing the drone even further. Indeed, to be undetectable (to our solution), the drone might fly all over just a limited amount of paths, that might be under strict human control, thus being even more exposed and easier to detect. More details will be provided in Section 7.

3 SCENARIO AND ASSUMPTIONS

The reference playground considered throughout this paper refers to the dataset provided by [17], including the GPS coordinates of a total number of 441 taxi vehicles running in the city of Porto, Portugal, as depicted in Figure 2. It is worth noting that, although taxis might not transmit their own signals, their drivers are likely to have mobile phones inside the vehicles, emitting WiFi beacons, and thus, using the same communication channels used by drones to communicate. Moreover, the roads travelled by taxi drivers are the same travelled by the owners of private cars. Therefore, on the one hand, the adopted dataset is representative of any vehicle movement in the analyzed area. On the other hand, telling apart messages emitted by vehicles and drones is not straightforward.

In particular, we refer to two sub-areas within the original map (red rectangles in Figure 2), characterized by different densities of GPS coordinates, thus considering a different number of roads in the scenario. We denote the densest area as the *urban scenario*, while the other (less dense) area is referred to as the *rural scenario*.

Figure 3 shows the considered rural area (bottom right red rectangle in Figure 2), comprising of 4, 135 GPS coordinates and an area

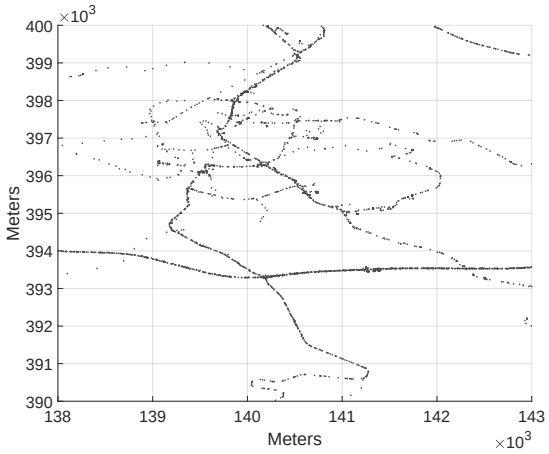

Figure 3: Rural area. It includes 4, 135 **GPS coordinates over an area of** 50 km^2**.**

of 50 km^2. Figure 4 refers to the urban area (down-town, top left red rectangle in Fig 2), comprising of 31, 556, 754 GPS coordinates and an area of 50 km^2 (same as the rural one).

Without loss of generality, in this contribution, we do not consider pedestrians and cyclists, which might be considered for future works. Indeed, this work represents a preliminary attempt in the direction of detecting drones by measuring how their trajectories differ from the ones of users and their associated devices (context-aware detection). We assume any area (potential No-Fly Zone) as characterized by a set of trajectories that are travelled day-in-day-out by the users, thus generating a ground-truth for the *allowed trajectories*, i.e., the set of grey dots in Figure 3 and Figure 4. A

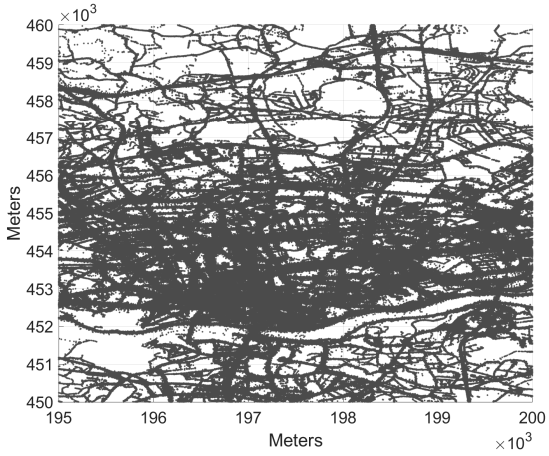

Figure 4: Urban area. It includes 31, 556, 754 **GPS coordinates over an area of** 50 km^2**.**

drone flying through the No-Fly Zone is likely to have either a straight path to reach its target or a trajectory suitable to recon the area. Such behaviour is an anomaly compared to the previously generated ground truth.

Finally, for the sake of enhanced readability, Table 1 reports the main notation used throughout the rest of the paper, along with a short description.

4 OUR SOLUTION IN A NUTSHELL

In this section, we briefly introduce CADD, our proposed solution to detect drones based on context-related information.

Definition 1. We define *Moving Target* ($\mathcal{D}$) a moving object in the No-Fly Zone. $\mathcal{D}$ can be either a vehicle or a drone, while our goal is to correctly identify it as a function of its behaviour (trajectory). ■

Our solution combines an *offline phase*, which aims at generating the ground-truth knowledge, with an *online phase*, where the actual detection of the drone is performed through the conceived solution.

- **Offline Phase.** This phase is optional and should be executed offline, before the deployment of the detection system, with the assumption that the No-Fly Zone is in a clear state, i.e., with no drones flying around. This phase aims to collect a dataset of GPS positions that reflects the road layout of the No-Fly Zone. Such coordinates can be collected either on purpose by driving around all the possible paths of the No-Fly Zone and logging the coordinates, or by resorting to already existing datasets (as we are doing in this work).
- **Online Phase.** During the online phase, each sensor in the sensor network estimates the distance to $\mathcal{D}$ and provides this information to a central server. In turn, the server estimates the location of $\mathcal{D}$ from the received distances (via multi-lateration) and it tracks $\mathcal{D}$'s movements in the No-Fly Zone. Finally, our algorithm compares $\mathcal{D}$'s trajectory with the ground-truth generated during the off-line phase, and it provides the likelihood that the mobile object is actually a drone (true positive) or a vehicle (true negative).

In the following, we provide the details of the Online Phase, since we assume our ground-truth to be constituted by the GPS coordinates provided by [17]. We simulate the presence of either a vehicle (taxi) or a drone (random trajectory in the playground) and we run our detection algorithm to infer the identity of the moving target.

5 MOBILE TARGET LOCALIZATION AND TRACKING

As mentioned before, drone's detection requires preliminary localization and tracking of the mobile target ($\mathcal{D}$). Without loss of generality, we assume the localization process requires a sensing network able to receive periodic messages (beacons) transmitted by $\mathcal{D}$. As will be more clear in the following, our localization solution only requires the deployment of several sensors throughout the NFZ, and the logging of the RSS of any received signal, emerging as a lightweight, low-cost, and easy-to-deploy strategy.

We consider $N = 500$ sensors deployed in the area, i.e., 50 sensors per squared kilometre. Moreover, we consider the log-distance path loss model, as modelled by the authors in [30], to simulate the received signal strength at the receiver side, as depicted by Eq. 1.

$$P_{rx}(d_i)[dBm] = P_{tx} - P_L(d_0) - 10 \cdot \alpha \log_{10}\left(\frac{d_i}{d_0}\right) - \chi(\sigma), \tag{1}$$

where d_i is the distance (unknown) between the sensor n_i and $\mathcal{D}$, P_{tx} is the transmission power of $\mathcal{D}$, $P_L(d_0 = 1) = 0\ dBm$ is the path loss at the reference distance $d_0 = 1$, $\alpha = 3.5$ is the path loss exponent, and finally, $\chi(\sigma)$ is a log-normal random variable with mean 0 and standard deviation $\sigma = 3$. All the previous parameters have been chosen according to the considered scenarios, i.e., urban and rural environments [25]. Finally, we consider a receiving threshold of $\gamma_{rx} = -80$ dBm and a transmitting power P_{tx} of 20 dBm, compliant with the WiFi standard. We highlight that the configuration of all the previous parameters does not affect the effectiveness of our solution, but they might reduce the performance—although we already considered worst-case conditions ($\alpha = 3.5$ and $\sigma = 3$) for the previously introduced scenarios.

We define as *path loss* $PL(d_i) = P_{tx} - P_{rx}(d_i) - P_L(d_0)$ the signal attenuation experienced by node n_i when receiving a wireless message transmitted by a source located at distance d_i from $\mathcal{D}$. Each sensor n_i can now estimate the distance $\widetilde{d_i}$ to $\mathcal{D}$ by resorting to Eq. 2.

$$\widetilde{d_i} = d_0 \cdot 10^{\frac{PL(d_i)}{10^{\alpha}}}. \tag{2}$$

As previously mentioned, we assume that not all the sensors in the sensor network can receive the transmitted signals, due to the limited transmission range of the wireless communication technology. Therefore, we assumed that a signal can be received by sensor n_i at distance d_i if and only if the received signal power is higher (or equal) than the sensitivity, i.e., $P_{rx}(d_i) \geq \gamma_{rx}$ dBm.

Different localization techniques can be adopted to obtain an estimation of $\mathcal{D}$'s position starting from the distances $\widetilde{d_i}$. Without loss of generality, in this paper, we consider the RLS algorithm, although many others are available from the literature [10].

Table 1: Notation summary.

Notation	Description
ϵ	Adversary.
$\mathcal{D}$	Moving target.
N	Sensors deployed in the area.
$P_{rx}(d_i)$	Received signal strength at the receiver i at a distance d_i from the source.
P_{tx}	Transmission power of the mobile target.
$PL(d_i)$	Path loss (signal attenuation) experienced by the sensor i at a distance d_i from the emitting source.
$P_L(d_0)$	Path loss at the reference distance $d_0 = 1$.
α	Path loss exponent.
$\chi(\sigma)$	Log-normal random variable with mean 0 and standard deviation σ.
γ_{rx}	Sensitivity (receiving threshold) of the receiver.
$\widetilde{d}_i$	Estimated distance of the sensor i from the emitting source ($\mathcal{D}$).
$(\overline{x}, \overline{y})$	Approximated position of $\mathcal{D}$ from the RLS algorithm.
$\epsilon(\widetilde{d}_{i,j})$	Cumulative error of the RLS location estimation algorithm.
$\overline{d}_i$	Distance between the current estimated position of $\mathcal{D}$ and the sensor n_i.
U_0	Initial position of $\mathcal{D}$ in the RLS algorithm.
U_k	Estimated position of $\mathcal{D}$ at round k by the RLS algorithm.
E_k	Estimated distance error associated with $\mathcal{D}$ at step k in the RLS algorithm.
J	Jacobian matrix associated with $\overline{d}_i - \widetilde{d}_i$.
$d_\eta(t)$	Distance between the position of the $\mathcal{D}$ at time t and the centroid of the closest η available GPS coordinates.
$P(d_\eta(t) < x)$	Probability that the distance between the location of the drone at time t and the centroid of the closest η available GPS coordinates is less than x.

RLS is an iterative algorithm that searches for the (approximated) position $(\overline{x}, \overline{y})$ of $\mathcal{D}$, which minimizes the cumulative error $\epsilon(\widetilde{d}_i)$, defined as in Eq. 3.

$$\epsilon(\widetilde{d}_i) = \sum_{i=0}^{N-1} \left(\overline{d}_i - \widetilde{d}_i\right)^2, \tag{3}$$

where $\overline{d}_i$ is the distance between the current estimated position of $\mathcal{D}$, i.e., $[\overline{x}, \overline{y}]$, and the sensor n_i. The RLS algorithm starts from an initial position $U_0 \equiv [\overline{x}(0), \overline{y}(0)]$ and then, for each round k, it follows the steps depicted by Eq. 4.

$$\begin{aligned} U_k &= [\overline{x}(k), \overline{y}(k)] \\ E_k &= -(J_i^T J_i^{-1}) J^T \left(\overline{d}_i - \widetilde{d}_i\right)\Big|_{U_k} \\ U_{k+1} &= U_k + E_k, \end{aligned} \tag{4}$$

where J_i is the Jacobian matrix associated with $\overline{d}_i - \widetilde{d}_i$ and $(\circ)^T$ refers to the transpose matrix. The algorithm stops when the step size $\|E_k\|$ is less than a pre-defined threshold, and we assume $[\overline{x}(k), \overline{y}(k)]$ as the position of $\mathcal{D}$.

As a toy example, we consider the drone trajectory (solid green line) in Figure 5, flying all over the previously introduced rural area (recall Figure 3). Red circles represent a random deployment of sensors, while bold red circles are the ones able to receive the messages from the drone ($P_{rx} \geq \gamma_{rx} dBm$). At each round, the RLS algorithm estimates the position of the drone by combining the estimated distances $\widetilde{d}_i$ and it generates a pair of estimated coordinates $[\overline{x}(t), \overline{y}(t)]$, (represented as blue dots in Figure 5 and the associated magnification). Finally, we consider a linear interpolation of the estimated positions of the drone (solid blue line in the magnification of Figure 5) as the final estimated trajectory associated with the drone.

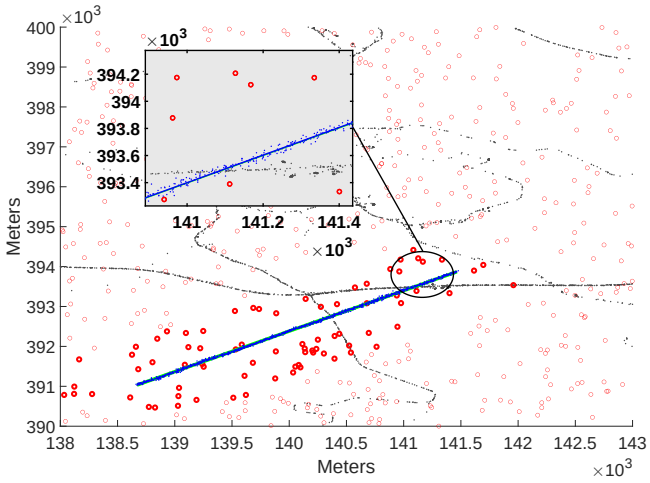

Figure 5: Estimation of the trajectory of the drone. A subset of the available sensors (bolded red cicles) receive signals from the drone (green trajectory), and collaboratively estimate its trajectory (blue dots). The trajectory (solid blue line) is estimated as a linear interpolation of the blue dots.

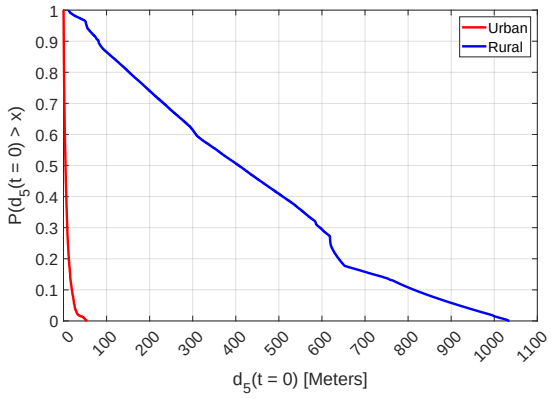

Figure 6: Inverse cumulative distribution function of the distance between the drone position at $t = 0$ (take-off time) and the closest clique of 5 GPS positions in the rural scenario (ground truth), i.e., $P(d_5(0) > x)$. The distance between the take-off point and the closest clique is (on-average) much larger for the rural scenario respect to the urban one.

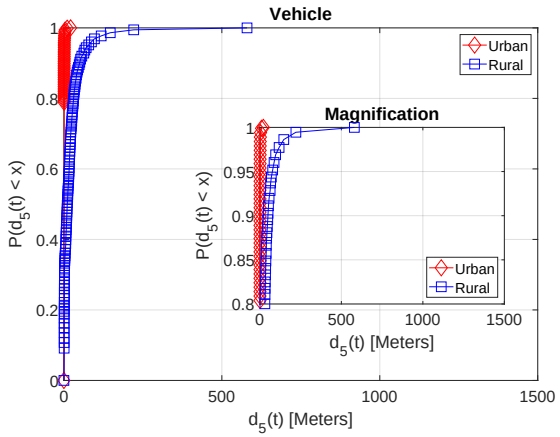

Figure 7: Cumulative distribution function associated with the distance ($d_5(t)$) between a vehicle (taxi) and the closest clique of 5 GPS coordinates: the distance is much smaller in the urban environment given the higher density of roads.

6 DETECTION OF DRONES

In this section, we introduce some metrics that will lay the foundation for the subsequent analysis.

Definition 2. We define $d_\eta(t)$ as the distance between the position of $\mathcal{D}$ at time t and the centroid of the closest η GPS coordinates collected during the *Offline Phase*. In the following, we consider the vehicles (taxis) moving on the roads as our ground truth. ■

We consider a random deployment of a drone in both rural and urban scenarios (recall Figure 3 and Figure 4, respectively) and we compute the associated $d_5(t = 0)$, i.e., the distance between the drone (at the take-off time, $t = 0$) and the centroid of the closest $\eta = 5$ GPS coordinates collected from the vehicles (more details on this choice will be provided later on in this section). Figure 6 shows the inverse cumulative distribution function associated with $d_5(t = 0)$, i.e., the probability that the drone position is at the distance $d_5(t = 0)$ greater than a considered x reference distance, i.e., $d_5(0) > x$. Our investigation highlights how the two scenarios are very different each from the other. Indeed, in the urban scenario (solid red line), it holds that $P(d_5(0) > 0.6m) \approx 0.9$, meaning that when a drone starts its flight ($t = 0$) from a random position, its distance is likely (with $P > 0.9$) to be larger than 0.6 meters from the closest clique ($\eta = 5$) of GPS coordinates (ground truth). Conversely, when we consider the rural scenario (solid blue line), the distance between the drone and the closest clique goes up to approximately 80 meters $P(d_5(0) > 80m) \approx 0.9$. Indeed, as intuition would suggest, rural scenarios are characterized by reduced density of roads; thus, the distance between the drone and the closest GPS coordinates associated with moving vehicles (ground truth) is much larger.

We would like to highlight that the clique size $\eta = 5$ has been empirically chosen as a trade-off: big η might involve distant coordinates in rural areas where the density is low, while small η (like either 1 or 2) might be affected by outliers, i.e., spurious GPS measurements. Our analysis showed that the selection of $\eta = 5$ guarantees an acceptable trade-off between coordinates density and spurious locations.

In the following, we consider the two cases of a vehicle and a drone moving in both the considered scenarios (rural and urban). We start our analysis by considering a vehicle (taxi) driving a random path taken from the dataset. To provide a fair evaluation, the GPS coordinates constituting the selected path have been removed when considering the selection of the closest clique. Figure 7 shows the cumulative distribution function associated with the distance to the closest clique of $\eta = 5$ coordinates, assuming a taxi is driving a random path constituted by a set of random coordinates taken from the dataset. The distance to the closest clique is small for both the urban and the rural scenarios, i.e., $P(d_5(t) < 0.75) \approx 0.9$ and $P(d_5(t) < 50) \approx 0.9$, respectively. As expected, taxi trajectories are very similar to each other, and therefore, a taxi (or any other vehicle) driving a random path can always find a close match to an already trajectory in the database (ground-truth). Moreover, we observe that $d_5(t)$ is much smaller in the urban scenario with respect to the rural one: this confirms our previous result, i.e., higher densities of GPS coordinates (like in an urban scenario) better fit new trajectories that follow the same path.

We now consider a random drone trajectory, and for each estimated location of the drone, we compute the distance to the closest clique of GPS coordinates ($\eta = 5$). Figure 8 shows the cumulative distribution function associated with the distance $d_5(t)$ to the closest clique of $\eta = 5$ GPS coordinates. The results confirm that the urban scenario is characterized by a significantly

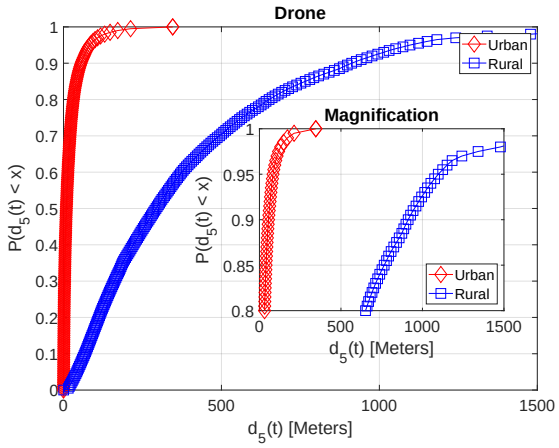

Figure 8: Cumulative distribution function associated with the distance ($d_5(t)$) between the drone ($\mathcal{D}$ (mt)) and the closest clique of 5 GPS coordinates: the distance is much smaller in the urban environment given the higher density of roads.

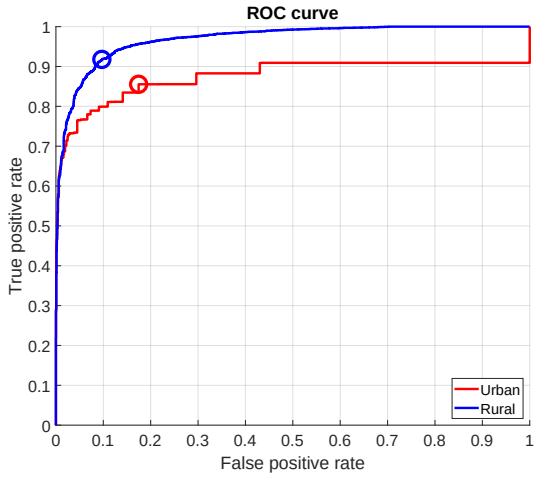

Figure 9: Receiver Operating Characteristics (ROC) curve associated with the detection performance of our solution. Circles represent the optimal operating points.

smaller distance $P(d_5(t) < 100) \approx 0.9$ compared to the rural one $P(d_5(t) < 1000) \approx 0.9$.

Moreover, the comparison of Figure 7 with Figure 8 confirms our main intuition, i.e., a random drone trajectory features (on average) larger distances compared to a vehicle driving a random path matching the GPS coordinates of other vehicles (ground truth).

Finally, Figure 9 shows the Receiver Operating Characteristics (ROC) curve associated with the performance of our detection solution. Figure 9 shows the true positive rate as a function of the false positive rate by varying the decision threshold for both the urban and rural scenarios. The ROC curve has been computed by considering different thresholds and comparing the distances $d_5(t)$ with the considered thresholds. We start our considerations by highlighting a typical parameter associated with the ROC analysis, i.e., the Area Under the Curve (AUC). The closer AUC is to 1, the better are the performance of the classification algorithm. AUC sums up to about 0.88 and 0.97 for the urban and rural scenarios, respectively. This confirms the fact that our solution performs better in the rural scenario due to less density of the GPS coordinates, thus allowing a more effective detection of the anomalies. The red and blue circles represent the optimal operating points for the urban and rural scenarios, respectively. In particular, the optimal operating point in the rural environment is $FP \approx 0.1$ and $TP \approx 0.92$, while for the urban environment is $FP \approx 0.17$ and $TP \approx 0.85$. The above configuration is achieved by adopting $d_5(t) \approx 51.3$ for the rural scenario and $d_5(t) \approx 1.5$ meters for the urban scenario.

The (balanced) accuracy of our detection solution can be computed as $\frac{1+TP-FP}{2}$ summing up to 0.84 and 0.91 for the urban and the rural scenario, respectively.

7 FEATURES AND LIMITATIONS

We hereby summarize the most important features and limitations of our solution for context-aware drone detection.

Speed. Our approach is independent of the time dimension, i.e., the speed of the drone. A naïve solution might infer the presence of a drone by considering when the speed exceeds a predefined threshold, thus being inconsistent with the context. However, in our scenario, we assume that the drone flies at a speed that is comparable to the one of the vehicles in the No-Fly Zone. We observe that such behaviour is consistent with a drone that does not want to be detected, thus deploying all the possible countermeasures.

Flight altitude. Our approach is also independent of the flight altitude. Similarly to the discussion we just had with respect to the speed of the flight, a naïve solution might infer the presence of a drone by considering when the estimated height of the transmitting source exceeds a predefined threshold, thus being inconsistent with the context. On the one hand, we highlight that, as already acknowledged by several works in the literature, identifying the height of a moving emitter using a sensor network deployed on the ground is particularly challenging, as the deployment is often unbalanced with respect to the height dimension. Thus, obtaining (or verifying) the height of a transmitting source might be hard. On the other hand, being independent of the altitude, our approach is robust also when the drone moves at a height that is comparable to one of the vehicles in the context, on purpose to avoid detection. Thus, moving at the ground instead of flying high would be an ineffective countermeasure for the drone.

Road-following flight. An interesting countermeasure to be deployed by the drone to avoid detection might be to reach the target by following the roads, thus becoming undetectable to our technique. This approach might expose much more the drone to visual detection, while it makes the number of possible trajectories to reach the target only a few, thus allowing fine-grained surveillance of the area around the target that might prevent the drone to get close to its target. In this sense, the utility and effectiveness of our solution are maximized when coupled with additional detection systems, such as the ones described in Section 8.

Radio silence. If the drone implements radio silence (no communications), it becomes undetectable to our solution. Radio silence involves a completely autonomous drone (self-navigation) that follows a pre-loaded path. We acknowledge that this configuration is not taken into account by our solution; nevertheless, the vast majority of configurations involves either a user controlling the drone with a remote controller or a drone (even autonomous) streaming the video of its path to a remote user. In both the previous cases, the wireless messages generated by the drone can be used to detect its presence with our solution.

Compatibility with latest FAA regulations. Our solution can still be adopted even when the adversary deploys a drone compliant with the latest *RemoteID* regulations promulgated by the US-based Federal Avionics Administration (FAA). In brief, the *RemoteID* rule forces all UAVs operators to transmit periodic broadcast messages reporting their identity and location, among the others. Such a rule just became effective in April 2021, and UAV operators have time to comply with it until September 2022 [13]. When a drone compliant with the RemoteID rule flies over the NFZ, its location can be estimated by the sensor network, and it can be immediately used for comparison with the ground truth. Moreover, if the drone broadcasts its GPS position, a reduced number of sensors might be deployed (the sensing infrastructure might even become useless), while our solution can just perform the detection task. Note that, to be compliant with the previous regulations, we assume the positions broadcast by the drone as genuine and not being spoofed [21, 22, 24]—this one being a strict requirement of our solution. However, note that CADD can be immediately used also to cross-check the location emitted by the drones in the RemoteID messages, to verify its consistency and to immediately identify potentially malicious drones, cheating with location reports. We plan to investigate this scenario as part of our future works.

8 RELATED WORK

Many contributions in the last years focused on amateur drones detection.

One of the most popular methods to detect drones is via sound analysis. In this context, the authors in [4] adopted Machine Learning (ML) techniques to classify various environmental sounds, such as airplanes, birds, and thunderstorms, and to compare the sound of amateur drones with the previously-mentioned natural ones. Similar findings were achieved also by the authors in [1], which used Deep Learning (DL) algorithms for the same scope. Audio traces have also been used in conjunction with cameras, such as in [15], to jointly process information from multiple sensing sources. In the systems described above, the specialized cameras and microphones arrays required to build up the detection system require a significant budget, and they are also characterized by limited detection ranges.

Radar systems are another technology that is used to achieve drones recognition. For instance, the authors in [31] proposed a K-band radar system based on fibre optic links, characterized by high sensitivity, linearity, and flatness to detect low-radar cross-section targets and measure their range and velocity. The system can detect small UAVs at a maximum distance of 500 meters, but requires the deployment of dedicated equipment. Similar issues can be found also in the work by the authors in [34], which were able to detect drones looking at the micro-Doppler signature in ground-based surveillance radar. However, radar techniques have issues especially in urban scenarios, where lots of possible targets might create noise and interference.

Other approaches worked on the physical layer, and specifically, on the RF signals emitted by amateur drones. This is the case of the contribution by the authors in [20], that identified physical features of the amateur drones in the emitted RF signals, such as body vibration and body shifting, being able also to discriminate them from other Wi-Fi emitting sources. However, methods like this latter one require Software-Defined Radios (SDRs) specifically deployed for the purpose. In the same context, the authors in [7] developed statistical models based on physical-layer measures, such as the RSS, to detect the presence of amateur drones. However, the performances of this latter approach decrease at distance from the target, while being also affected by low tolerance to Non-Line-of-Sight (NLoS). Other contributions, such as [8], worked on the packets emitted by amateur drones, looking at their statistical distribution. They conducted experimental analyses in several real-life use-cases, demonstrating the capability to discriminate the presence of the drone, as well as to identify the presence of video-streaming traffic.

Another approach is based on encrypted traffic analysis and classification, used by the authors in [28] and [29], to name a few. The authors distinguished drones' fingerprints by looking at the packets interarrival times and size, and they were able to discriminate also their movement patterns. Similar techniques were used by the authors in [32] to identify the pilot of the drone, by looking at the statistical distribution of the commands issued to the drone by the pilot. Such solutions, however, might suffer from evasion attacks and heavily depends on the reliability of the wireless communication links.

Other contributions focused on privacy issues and invasions caused by drones. For instance, the authors in [19] built up a method to identify if a specific point of interest is video-streamed by a drone, by detecting a watermark in the video streaming caused by the periodic physical stimulus on a target/victim.

Compared to the above-discussed approaches, our solution emerges as a lightweight, low-cost, and easy-to-deploy approach. Our solution can also mitigate interference and overcome limited range issues typical of the competing solutions, and it exploits the context where the NFZ is located to force the drones to follow roads and pedestrian paths, to enable easier detection, e.g., via visual surveillance.

9 CONCLUSION

In this paper, we proposed CADD, a novel solution for context-aware drone detection. CADD leverages two components: (i) a network of wireless sensors distributed in the No-Fly Zone to estimate their distance to the drone from the received signal strength associated with each radio message received from the drone, and (ii) a central server, where the data (estimated distances between each sensor and the drone) is processed to estimate the position of the drone and track its trajectory.

CADD features several properties: (i) it only relies on passive wireless eavesdropping; (ii) it is independent from both the speed and the height of the drone; and (iii) it can be coupled with already existing regulations and solutions for drone detection, such as RemoteID, enhancing further their effectiveness.

Our results, obtained via simulations performed over a real dataset, shows that CADD can infer on the presence of a drone both in an urban (crowded) and rural (less densely populated) scenario, with a True Positive Rate of 0.92 and 0.85, respectively, and a False Positive Rate of 0.1 and 0.17, respectively.

Our future work include: (i) the extension of the performance evaluation of CADD in additional scenarios, characterized by specific geographical and propagation features, (ii) additional investigations on the possibility to extend CADD with algorithms based on ML and DL, to improve drone detection in the wild, and finally, (iii) the adoption of CADD for the verification of the consistency of RemoteID location reports emitted by drones.

ACKNOWLEDGMENT

This publication was partially supported by awards NPRP12S-0125-190013 from the QNRF-Qatar National Research Fund, a member of The Qatar Foundation. The information and views set out in this publication are those of the authors and do not necessarily reflect the official opinion of the QNRF. This work has been partially supported also by the INTERSECT project, Grant No. NWA.1162.18.301, funded by Netherlands Organisation for Scientific Research (NWO). The findings reported herein are solely responsibility of the authors.

REFERENCES

[1] S. Al-Emadi, A. Al-Ali, A. Mohammad, and A. Al-Ali. 2019. Audio Based Drone Detection and Identification using Deep Learning. In *15th International Wireless Communications Mobile Computing Conference (IWCMC)*. 459–464. https://doi.org/10.1109/IWCMC.2019.8766732

[2] Aladdin Consortium. 2021. Aladdin — Advanced hoListic Adverse Drone Detection, Identification & Neutralization. http://aladdin.eu. (Accessed: 2021-10-22.

[3] R. Altawy and A. Youssef. 2016. Security, privacy, and safety aspects of civilian drones: A survey. *ACM Transactions on Cyber-Physical Systems* 1, 2 (2016), 1–25.

[4] M. Z. Anwar, Z. Kaleem, and A. Jamalipour. 2019. Machine Learning Inspired Sound-Based Amateur Drone Detection for Public Safety Applications. *IEEE Transactions on Vehicular Technology* 68, 3 (2019), 2526–2534. https://doi.org/10.1109/TVT.2019.2893615

[5] B. Alzahrani, et al. 2020. UAV assistance paradigm: State-of-the-art in applications and challenges. *Journ. of Netw. and Comput. Applicat.* (2020), 102706.

[6] BBC. 2019. Gatwick Airport: Drone attack grounds flights. http://www.bbc.co.uk/news/uk-england-sussex-4662375. (Accessed: 2021-10-22.

[7] S. Birnbach, R. Baker, and I. Martinovic. 2017. Wi-fly?: Detecting privacy invasion attacks by consumer drones. (2017).

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

[9] P. Boccadoro, D. Striccoli, and L. Grieco. 2021. An extensive survey on the Internet of Drones. *Ad Hoc Networks* 122 (2021), 102600.

[10] L. Caceres Najarro, I. Song, and K. Kim. 2021. Fundamental Limitations and State-of-the-art Solutions for Target Node Localization in WSNs. (2021).

[11] DeDrone. 2021. Worldwide Drone Incidents. Available Online: hhttps://www.dedrone.com/resources/incidents/all.

[12] R. Di Pietro, G. Oligeri, and P. Tedeschi. 2019. JAM-ME: Exploiting Jamming to Accomplish Drone Mission. In *2019 IEEE Conference on Communications and Network Security (CNS)*. 1–9. https://doi.org/10.1109/CNS.2019.8802717

[13] FAA. 2021. UAS Remote Identification Overview. Available Online: https://www.faa.gov/uas/getting_started/remote_id/.

[14] A. Koubâa, A. Allouch, M. Alajlan, Y. Javed, A. Belghith, and M. Khalgui. 2019. Micro Air Vehicle Link (MAVlink) in a Nutshell: A Survey. *IEEE Access* 7 (2019), 87658–87680.

[15] H. Liu, Z. Wei, Y. Chen, J. Pan, L. Lin, and Y. Ren. 2017. Drone Detection Based on an Audio-Assisted Camera Array. In *IEEE Third International Conference on Multimedia Big Data (BigMM)*. 402–406. https://doi.org/10.1109/BigMM.2017.57

[16] M. Mozaffari, et al. 2019. A Tutorial on UAVs for Wireless Networks: Applications, Challenges, and Open Problems. *IEEE Communications Surveys & Tutorials* 21, 3 (2019).

[17] L. Moreira-Matias, J. Gama, M. Ferreira, J. Mendes-Moreira, and L. Damas. 2013. Predicting Taxi–Passenger Demand Using Streaming Data. *IEEE Transactions on Intelligent Transportation Systems* 14, 3 (2013), 1393–1402. https://doi.org/10.1109/TITS.2013.2262376

[18] B. Nassi, R. Ben-Netanel, A. Shamir, and Y. Elovici. 2018. Game of drones-detecting streamed POI from encrypted FPV channel. *arXiv preprint arXiv:1801.03074* (2018).

[19] B. Nassi, R. Ben-Netanel, A. Shamir, and Y. Elovici. 2019. Drones' Cryptanalysis - Smashing Cryptography with a Flicker. In *2019 IEEE Symposium on Security and Privacy (SP)*. 1397–1414. https://doi.org/10.1109/SP.2019.00051

[20] P. Nguyen, H. Truong, M. Ravindranathan, A. Nguyen, R. Han, and T. Vu. 2017. Matthan: Drone Presence Detection by Identifying Physical Signatures in the Drone's RF Communication. In *Proc. of the Annual Int. Conf. on Mobile Systems, Applications, and Services (MobiSys '17)*. 211–224.

[21] G. Oligeri, S. Sciancalepore, and R. Di Pietro. 2020. GNSS Spoofing Detection via Opportunistic IRIDIUM Signals *(WiSec '20)*. Association for Computing Machinery, New York, NY, USA, 42–52. https://doi.org/10.1145/3395351.3399350

[22] G. Oligeri, S. Sciancalepore, O. Ibrahim, and R. Di Pietro. 2019. Drive Me Not: GPS Spoofing Detection via Cellular Network: (Architectures, Models, and Experiments) *(WiSec '19)*. Association for Computing Machinery, New York, NY, USA, 12–22. https://doi.org/10.1145/3317549.3319719

[23] A. Otto, N. Agatz, J. Campbell, B. Golden, and E. Pesch. 2018. Optimization approaches for civil applications of unmanned aerial vehicles (UAVs) or aerial drones: A survey. *Networks* 72, 4 (2018), 411–458.

[24] S. Raponi, S. Sciancalepore, G. Oligeri, and R. Di Pietro. 2021. Road Traffic Poisoning of Navigation Apps: Threats and Countermeasures. *IEEE Security Privacy* (2021), 2–11. https://doi.org/10.1109/MSEC.2021.3110307

[25] T. Rappaport. 2001. *Wireless Communications: Principles and Practice* (2nd ed.). Prentice Hall PTR, USA.

[26] Reuters. 2021. Saudi-led coalition says it intercepts armed drone fired at Abha airport. https://www.reuters.com/world/middle-east/saudi-led-coalition-says-intercepts-armed-drone-fired-abha-airport-2021-05-10/. (Accessed: 2021-10-22.

[27] SafeShore Consortium. 2021. SafeShore — Increasing Border Security. http://safeshore.eu. (Accessed: 2021-10-22.

[28] S. Sciancalepore, O. Ibrahim, G. Oligeri, and R. Di Pietro. 2019. Detecting drones status via encrypted traffic analysis. In *Proceedings of the ACM Workshop on Wireless Security and Machine Learning*. 67–72.

[29] S. Sciancalepore, O. Ibrahim, G. Oligeri, and R. Di Pietro. 2020. PiNcH: An effective, efficient, and robust solution to drone detection via network traffic analysis. *Computer Networks* 168 (2020), 107044.

[30] J. Seybold. 2005. *Introduction to RF propagation*. John Wiley & Sons.

[31] D. Shin, D. Jung, D. Kim, J. Ham, and S. Park. 2017. A Distributed FMCW Radar System Based on Fiber-Optic Links for Small Drone Detection. *IEEE Transactions on Instrumentation and Measurement* 66, 2 (2017), 340–347. https://doi.org/10.1109/TIM.2016.2626038

[32] A. Shoufan, H. M. Al-Angari, M. F. A. Sheikh, and E. Damiani. 2018. Drone Pilot Identification by Classifying Radio-Control Signals. *IEEE Transactions on Information Forensics and Security* 13, 10 (Oct 2018), 2439–2447.

[33] Statista. 2021. Estimated size of the global commercial drone market in 2021 with a forecast for 2026. https://www.statista.com/statistics/878018/global-commercial-drone-market-size/. Accessed: 2021-10-22.

[34] H. Sun, B. Oh, X. Guo, and Z. Lin. 2019. Improving the Doppler Resolution of Ground-Based Surveillance Radar for Drone Detection. *IEEE Trans. Aerospace Electron. Systems* 55, 6 (2019), 3667–3673. https://doi.org/10.1109/TAES.2019.2895585

[35] P. Tedeschi, G. Oligeri, and R. Di Pietro. 2020. Leveraging Jamming to Help Drones Complete Their Mission. *IEEE Access* 8 (2020), 5049–5064. https://doi.org/10.1109/ACCESS.2019.2963105

[36] P. Tedeschi, S. Sciancalepore, and R. Di Pietro. 2021. ARID: Anonymous Remote IDentification of Unmanned Aerial Vehicles. In *Annual Computer Security Applications Conference*. 207–218.

[37] T. Wall. 2016. Ordinary emergency: Drones, police, and geographies of legal terror. *Antipode* 48, 4 (2016), 1122–1139.