IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Leveraging Jamming to Help Drones Complete Their Mission

PIETRO TEDESCHI, GABRIELE OLIGERI, AND ROBERTO DI PIETRO

Hamad Bin Khalifa University, College of Science and Engineering, Information and Computing Technology Division, Doha, Qatar (e-mail: ptedeschi@mail.hbku.edu.qa, {goligeri, rdipietro}@hbku.edu.qa)

Corresponding Author: Pietro Tedeschi (e-mail: ptedeschi@mail.hbku.edu.qa).

The publication of this article was funded by the Qatar National Library (QNL), Doha, Qatar and awards NPRP11S-0109-180242, UREP23-065-1-014, and NPRP X-063-1-014 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.

ABSTRACT We propose *JAM-ME*, an autonomous jamming-assisted navigation system that allows a drone to accomplish its mission even in the presence of an anti-drone jamming protection system. In this contribution, we review the current state-of-the-art highlighting how current solutions to respond to drones are completely ineffective against *JAM-ME*. In particular, we introduce our solution and its theoretical framework, and later we relax a few constraints of the baseline model (adding wind drift, and allowing the target to be randomly placed within the jammed area). Moreover, we run extensive simulations that do support our findings: even under the combined action of jamming and wind drift, the drone can reach a target randomly deployed in the jamming area—any other drone, under the same conditions, would have simply failed. As per the overhead, under very conservative assumptions, *JAM-ME* experiences an average overhead of 70%; however, note that such overhead can be reduced by at least a tenfold factor in practical settings—discussed in the paper. Finally, we highlight the intrinsic limitations of our solution, potential countermeasures, and new jamming strategies that can pave the way to further research.

INDEX TERMS UAV security, jamming, Global Positioning System, passive homing systems

I. INTRODUCTION

UNMANNED Aerial Vehicles, also known as drones, are becoming popular enabling technology for several applications including monitoring, surveillance and shipping [1], [2], [3], [4]. In particular, commercial drones are becoming more and more autonomous by shifting from pure remote-controlled devices exploiting the WiFi bands (2.4GHz - 5GHz) to portable and independent flying devices featuring obstacle sensing, palm launch, gesture control and tracking capabilities. Unfortunately, these new features can be easily exploited to commit several types of crimes spanning from privacy violation, e.g., shooting aerial photos, bomb critical infrastructures, or even crowded places [5], [6], [7]. As such, drones could represent—like no other technology before—, an imminent threat to people safety. Given the above-introduced issues, in the last few years, several countermeasures have been deployed to prevent the drones to reach a protected area. Some of these techniques include to destroy the drone with guns; however, while these techniques can be considered in war zones, they cannot be clearly adopted in everyday civil scenarios. Other techniques involve the use of nets to be shot to the drone from the ground (with a gun) or even by drones hunting for the not authorised ones [8]. All these solutions have drawbacks though: the former requires a relatively short distance between the drone and the operator of the gun, while the latter might not be effective if the drone implements strong evasion techniques. Driven by the increasing hype associated with drones' threat, the vast majority of manufacturers are hard-coding no-fly-zone functionality in the firmware of the drone itself. This should increase flight safety and prevent accidental flights in restricted areas. Unfortunately, experienced hackers can overcome this solution by reprogramming the drone firmware or even choosing a drone which is not implementing this feature—only a few manufacturers are compliant with the described feature.

The state of the art on detecting either the presence of a drone or its manoeuvres is provided by solutions adopting machine learning techniques [9], deep neural networks [10], audio analysis [11], [12], ambient radio frequency signals (emitted from UAVs), radars, acoustic sensors, and computer vision [13]. One emerging technique to respond to drone

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2963105, IEEE Access

threat is *jamming*. A jammer can broadcast a powerful signal with the aim of disrupting all the communications in the neighborhood by preventing the receivers to correctly receive and retrieve the messages from the radio spectrum as they have been transmitted from the source. Jamming is particularly suitable against drones since it allows to disrupt both the remote controller and the Global Positioning System (GPS) navigation of the drone. Indeed, jamming can affect the link between the remote controller and the drone preventing the reception of the messages at either the drone or the remote controller. Moreover, jamming can be used to disrupt the reception of the GPS information at the drone, and therefore, preventing the positioning and navigation functionalities (i.e., forcing the drone to enter in safe-mode, landing or flying back to its home position) of it [14], [15], [16]. To date, jamming the GPS is considered one of the most compelling techniques to protect particular targets, areas, infrastructures, and to prevent unauthorized flights from drones.

Contribution. In this paper, we prove that jamming might be almost useless when deployed to mitigate drone threats. In particular, we introduce a simple yet effective navigation algorithm (*JAM-ME*) based only on the exploitation of the RSS of the RF signals emitted by the jammer, that makes jamming completely ineffective [17]. *JAM-ME* is a jamming-based navigation technique that leverages the jamming signal to estimate the jammer location, that in turn is leveraged as a radio-beacon to compute the relative position of the drone concerning the target. We provide a thorough model for *JAM-ME*, and we show evidence that, in the above-cited harsh conditions and further assuming a very conservative setting (drone speed of just $1m/s$), the drone can still accomplish its mission: reaching an assigned target randomly located within the jammed area—even in presence of wind-drift. Further, we run an extensive simulation campaign, showing the quality and viability of our solution. Indeed, the incurred overhead (that is, the extra-time to reach the target) is estimated at about 70% under the very stringent, conservative conditions considered in this paper—conditions where no drone, to date, could operate—; the same overhead could be reduced to a mere 7% (a tenfold decrease) under normal operating conditions. We conducted an extensive simulation campaign using MATLAB©2019a, while the source code of *JAM-ME* has been released as open-source [18], to allow further research on this topic. The simulator of our model could allow practitioners and academia to verify our claims and to compare their own solutions with *JAM-ME*, eventually using our source code as a ready-to-use basis for their software development.

Roadmap. In section II we report background information and related work in the area, introducing major security, privacy, and safety concerns posed by drones, and we discuss on the effectiveness of jamming to defeat drones. In section III we describe the scenario assumed throughout this work. In section IV we present the core idea behind the jamming-based drone navigation system, while in Section V we show the performance of our solution in a baseline scenario (no wind drift and target at the same position of the jammer). In sections VI and VII we show the performance of our solution when wind intensity can randomly change, and when the target is randomly deployed within the jammed area. Finally, in section VIII, we discuss possible mitigation techniques to *JAM-ME*, while in Section IX we report some concluding remarks.

II. BACKGROUND AND RELATED WORK

In the following section, we provide some insights about drones as attack vectors, and we review the most important contributions related to jamming as potential response to drone threat.

A. DRONES AS ATTACK VECTORS

Attacks delivered by drones are becoming more and more difficult to detect and avoid. Drones are becoming smaller with increase capacity of carrying payloads, and therefore, the perfect attack vector to reach unauthorized areas carrying hazardous materials such as explosives and viruses.

In the following, we summarise the main cybersecurity threats involving drones into two main families:

- *Privacy*. Modern drones feature autonomous reconnaissance functionalities combined with video-photography capabilities. Moreover, by becoming more and more silent, they can fly over the target at high altitude and being virtually undetected when taking high-resolution pictures and videos of the target itself.
- *Safety & Critical Infrastructures*. A critical infrastructure is a system or part of it, essential for the health, economic and social well-being of citizens. A damage or destruction would have a significant impact in a country, due to the impossibility of guaranteeing such functions. Nowadays, with the digital transformation and Industry 4.0, the practice of protecting critical infrastructures/facilities is a tough task. Critical infrastructures are increasingly vulnerable to cyber-attacks such as the disruption of online services with malware (e.g. Stuxnet) aimed to undermine the security of the country. Drones can be used against critical infrastructures facilities, such as airports, oil&gas industries, nuclear power plants, water treatment facilities, ports, telecommunication networks, etc., fulfilling several types of missions, e.g., reconnaissance missions, or providing support to a ground attack. Indeed, drones are becoming more and more suitable to carry heavy payloads including jammers, relays, and radio equipment to location difficult to reach and control. From the safety perspective, drones can be adopted to directly threat people safety by carrying explosives or radioactive materials[19], or colliding with airplanes during the take-off and landing procedures [20].

B. RELATED WORK

In this section we present several contributions in the literature related to radio jamming techniques, jammer localisation, and jamming mitigation solutions.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2963105, IEEE Access

1) Radio Jamming

Jamming is used for several purposes that go beyond the malicious activities of disrupting all the target's radio communications [21]. Indeed, a recent research topic exploits jamming to enforce confidentiality on wireless communications [22]: the transmitter and the receiver exchange messages while a cooperating third party jams the transmissions such that only the receiver will be able to detect and retrieve the message transmitted by the sender. The adopted solution is a physical-layer technique that aims to improve the secrecy capacity of the channel. Cooperative jamming is an interesting and growing topic enabling two parties to communicate without resorting to data encryption [23], [24]. The authors propose the adoption of a friendly jammer aimed to jam the channel between the source and the eavesdropper. Recently, cooperative jamming has been also combined with the novel technology of Multiple-Input Multiple-Output (MIMO) transducers [25]. This enables the receiver, which is in turn provided with a jammer, to disrupt the communications of the transmitter at all the locations but not at its receiving antenna. Finally, jamming is also used in several security scenarios to prevent not-authorised communications; a few examples are: preventing the use of mobile-phones to inmates and defeating triggering signals during bomb neutralisation.

2) Jammer Localisation

Jammer localisation solutions are attracting attention for both military and civilian application domains. Different techniques have been deployed to estimate the position of a radio receiver by exploiting radio signals propagation. One of the most adopted techniques involves the estimation of the Received Signal Strength (RSS) by the receiver side, and inferring the distance to the transmitter assuming well-known propagation models [26], [27]. In details, authors in [26] propose a solution to localise the jammer leveraging the trilateration technique. To achieve this goal they take into account the RSSI measurements and adopt a radio propagation model to compute the respective distances between the jammer and the node(s). Further, authors in [27] leverages the Time-of-Arrival (ToA), Angle-of-Arrival (AoA), and the RSS to compute the distances (between the jammer and the node(s)) and retrieve the jammer position in a wireless cooperative network. Other solutions (for omnidirectional and directive jammer localization) such as Centroid Localisation (CL), Virtual Force Iteration Localization (VFIL) and Adaptive Jammer Localisation Algorithm (AJLA) can be used to locate the jammer position [28]. The CL is an algorithm that computes the geometric center of the jammer, by averaging the estimated distances between the jammed nodes and the jammer; the VFIL is an improvement of the CL algorithm that aims to estimate the transmission range of the jammer and finally provide the region where the jammer could be located; the AJLA is an optimized algorithm that adopts CL or VFIL if the detected antenna is omnidirectional, while it adopts the Improved Gravitational Search Algorithm (IGSA) when the detected antenna is directional. The majority of the localisation techniques that have been proposed focus on indoor environments, and they address the issue of not consistent RSS estimations due to the lack of line-of-sight, moving people/objects, and strong multipath effects affecting the indoor environments. Outdoor localisation is actually an easier scenario due to the presence, for the majority of the time, of a clear and strong link between the transmitter and the receiver [29]. Other localisation techniques leverage different propagation phenomena, such as delay spread and time of flight.

Depending on the scenario and the number of transmitting entities, several techniques can be adopted to locate the transmitting source, e.g., trilateration, multilateration, triangulation, angulation, and lateration. Radio source localization is a well-known topic in the literature, in particular, when it comes to locating the transmitting source by exploiting only RSS, i.e., by mapping the received power to the distance to the transmitting source.

A solution to localize multiple jammers, with the analysis of the variation in the front-end signal power, recorded by the Unmanned Aerial Vehicles (UAVs) on-board GPS receivers in the network is pointed out in [30]. The authors leveraged a Gaussian Mixture Probability Hypothesis Density Filter over a graph framework, and the Levenberg-Marquardt (LM) algorithm as a minimizer. The proposed algorithm: Simultaneous Localization of Multiple Jammers and Receivers (SLMR) detects the presence of a jamming signal, computes the number of jammers and the distances between the UAVs and the relative transmission powers. Finally, after the data collection, the LM minimiser is adopted to compute the jammer position.

3) Jamming Mitigation

Guaranteeing reliable communications in the presence of jammers is a challenging task that has been undertaken by several researchers by resorting to different solutions, e.g., exploiting probabilistic protocols and algorithms to evade the jammed frequencies [31]. The authors proposed an anti-jamming protocol that guarantees to N nodes in a network to receive a broadcast message even with the presence of a powerful jammer. The adopted technique consists to broadcast a message as a series of unicast communications by choosing a random frequency. The solution consists to (i) deploy the network with n pre-shared keys k_{ij} between the nodes i and j, (ii) select two potential candidates nodes i, j, (iii) select the communication frequency f according the equation $f = H(k_{ij}|t)(modF)$, where t is the current time-slot, F is the cardinality of the set of the available frequencies and H is a one-way hashing function. The authors in [32] adopted the game theory to mitigate jamming attacks and minimise the damaging effect on the frequency-hopping spread-spectrum for satellite communication, by leveraging the two-player asymmetric zero-sum game framework. In detail, [32] assumes the channel capacity of the victim under jamming as the payoff of the game, while the victim and the attacker are modelled as entities that are able to spread

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2963105, IEEE Access

signals on a specified frequency. Further, the authors in [33] adopt the energy harvesting as a counter-jamming technique, since a part of the harmful interference can be harvested to increase the transmit power. The interaction between a pair of legitimate nodes and a malicious jammer is formulated as a zero-sum game. A novel technique based on frequency-hopping spread spectrum has been deployed in [34] to counteract the jamming attacks against Communication-Based Train Control (CBTC). In [35], the authors present a novel technique that optimizes the flight path for a UAV by estimating the UAV heading angle. Indeed, they provide a particular beamforming weight design for a UAV relay network that maximizes the Signal-to-Interference-plus-Noise Ratio (SINR) instead of the SNR (under the jamming attack) at the receiver. Furthermore, they provide a method to estimate the unknown jamming related parameters (gain, SINR) which are required for the optimization problem. In [36], cooperative jamming is exploited to secure the communications among UAVs, even in the presence of an eavesdropper. An idle UAV is employed as a friendly jammer, which can transmit jamming signals to confuse the eavesdroppers.

Finally, the solution in [37] proposes a cooperative spatial retreat algorithm that enables drones to cooperate for mitigating the action of the jammer. Implementing jamming mitigation techniques on-board of drones is not practical for several reasons: firstly, the majority of the solutions are not suitable for command-and-control scenarios due to their intrinsic latency, which in turn are dependent on their probabilistic nature. Semi-autonomous solutions might be practical: the drone might receive only partial instructions to be executed while for the majority of the time being autonomous. Under such an assumption, the solution provided by [38] enables peer to peer communications in the presence of a jammer that disrupts all the radio communications and that is still able to jam a large fraction of the empty radio spectrum.

Finally, authors in [39], introduced a jamming-based navigation solution to be used as a backup navigation system when radio-jamming prevents the reception of GPS signals: a multi-antenna communication system is adopted for estimating the angle of arrival of the ground home transmitter. While authors address the issue of jamming navigation under GPS jamming, their solution exploits beam-forming to locate the jamming source. Further, their approach requires a special hardware setup (multiple-antennas) to be deployed on the drone. Conversely, our solution does not require any special hardware, while only resorting to the received signal strength estimation of the jamming signal.

All the previously introduced solutions exploit jamming against wireless network devices and drones in the standard way; that is, assuming that once the drone is not able to communicate with the remote controller, it will abort its mission. This paper highlights how a drone can exploit the jamming for accomplishing its mission, and therefore, making radio-jamming useless to the aim of drone defence and response. Hence, calling for further research in this field.

C. DEFEATING DRONES WITH JAMMING

Commercial drones resort to various communication frequencies spanning between the lower 900 - 1.3GHz band to the higher WiFi frequencies (2.4GHz and 5GHz bands). WiFi frequencies are usually preferred by vendors since they provide more bandwidth, in particular, for video streaming, and for guaranteeing less interference with the GPS bands (1575.42MHz and 1227.60MHz). Moreover, the WiFi frequencies band turn out to be more robust to multipath fading caused by the presence of obstacles, and therefore, guaranteeing a better link quality between the remote controller and the drone. All the commercial available Software Defined Radios (SDRs) can be used to transmit over the aforementioned frequencies. SDRs are radio communication equipment whose components are implemented employing software embedded systems, such as Field-Programmable Gate Array (FPGA). SDRs are becoming nowadays more and more powerful and popular, giving researchers and telecommunication practitioners the freedom to implement any radio communication scheme and protocol from scratch—and, incidentally, providing a powerful tool to control/interfere with drones.

One of the most popular trends is to exploit the flexibility of SDRs to implement Denial of Service (DoS) attacks (jamming) to the radio communication link between the drone and its remote controller. Jamming is indeed the most effective DoS attacks that can be performed against radio links. Hence, over the years, several techniques have been designed aiming at preventing either the transmission or the reception of a message. Usually, the best strategy consists of transmitting a high-power synthetically generated noise to the targeted receiver, which in turn will no more be able to retrieve the transmitted signal due to the low Signal-to-Noise Ratio (SNR).

A directive antenna can be particularly useful in the previous scenario, allowing the jammer to concentrate its power budget on a very restricted area (main lobe of the directive antenna), and therefore, avoiding to waste jamming power. The previous assumption works when assuming the drone comes with a firmware-coded safety mode that forces the drone to land when it loses both the GPS signal and the link with the remote controller.

Several works have suggested disrupting device-to-device communications by resorting to jammers. For instance, by preventing both positioning and navigation with the disruption of the GPS link [40]. Furthermore, a jammer can prevent the usage of the Industrial Scientific and Medical (ISM) band for data communication, or inhibit the Wi-Fi communications adopted for both telemetry and wireless video transmission [41]. Multerer *et al.* [42] build an anti-drone system which consists of a 3D Frequency Modulated Continuous Wave (FMCW) Multiple Input Multiple Output (MIMO) radar and a directional jammer. Moreover, Shi *et al.* [15] developed an anti-drone system which combines multiple passive surveillance technologies to realize drone detection, localization, and radio frequency jamming. Pärlin *et al.* [43] investigated

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2963105, IEEE Access

the threat model to neutralize remotely controlled Unmanned Aerial Vehicle by RF jamming.

Only a few countermeasures are possible to mitigate jamming. Some of them include the re-programming of the drone's firmware to fly autonomously even when under jamming attacks. More in general, in the absence of any radio information, the drone might continue its path trying to get outside of the jamming region. Moreover, a drone, having inferred the presence of a jammer—for instance, due to the loss of all communications links and GPS signal—might increase its flight height, again to escape the action of the jammer. All of the above techniques eventually might enable the drone to re-gain the communication link between itself and the remote controller. However, they do not allow the drone to navigate autonomously in the presence of the jammer and to accomplish its mission.

III. SYSTEM AND ADVERSARY MODEL

The idea behind our solution is to exploit the jamming signal to locate the jammer, and subsequently, to exploit its position to compute the relative distance to the drone, and eventually, to set-up a jamming-assisted navigation system. Jamming, like any other signal transmission, is characterized by a transmission power and a path loss, that in turn, if properly modelled, they can be exploited to compute the distance to the transmitting source. Contrary to any other signal source, the jammer is motivated to maximize the received signal strength, e.g., using a directive antenna or a high transmission power, and therefore, the receiver (drone) is always under the best conditions to perform the aforementioned estimations.

The above scenario represents the ideal conditions for the estimation of the distance between the drone and the jammer, where the distance d [44] can be computed with the following equation:

$$d = \frac{\lambda}{4\pi}\sqrt{G\frac{P_t}{P_r}} \tag{1}$$

where λ is the radio frequency wavelength, P_t and P_r are the transmitted and the received power by the jammer and the drone, respectively, and finally, G is the product of the transmitter-receiver antenna gains in Line of Sight (LoS). Equation 1 is particularly suitable for LoS scenarios and it has been proven to provide excellent performance for the ground-to-air link [45], [39], such that one experienced by a remote controller and a drone. It is worth noticing that, although the transmitted power and the transmitter's antenna gain might be unknown to the drone, the *important* information for localisation (and navigation) purposes is the variation of the received power when the drone moves closer-to/further from the jammer. Finally, we highlight that deterministic path loss models (such that one adopted in this work) has been proved in the literature to be suitable for several suburban and rural environments [46], i.e., open field areas with no obstructions. Conversely, we did not take into account multi-path fading since the adopted model has been proved to be a good approximation for the channel attenuation of the drone-to-controller link [12], [30], [35], [39], [43].

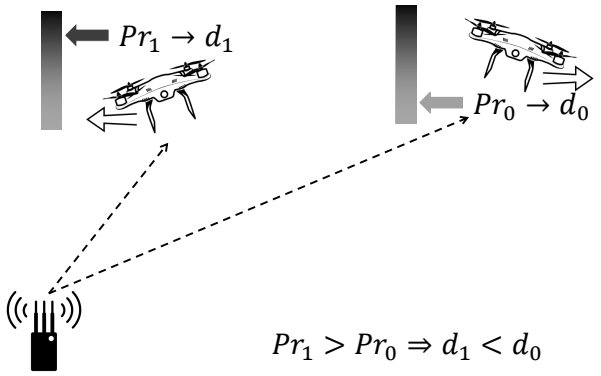

Figure 1. A drone exploiting the jamming signal for range estimation.

Figure 1 shows a toy example where the drone is flying over a no-fly-zone to reach a pre-determined target (close to the jammer). After detecting the presence of the jammer, it firstly estimates the received power Pr_0 from the unknown signal source (jammer), and then, it derives the distance d_0. After moving towards the signal source, the drone estimates a higher received signal strength compared to the case when the drone is more distant from the jammer. As a numerical example, let us assume $Pr_1 = 2 \times Pr_0$ therefore, the drone will measure an increment in the received signal strength of $+3$dBm. Recalling Eq. (1), the drone can estimate to have moved closer to the jammer by a factor of $d_1/d_0 = 1/\sqrt{2}$. As it will be clear in the following, it is possible to precisely estimate the distance to the jammer even without receiving any information from the GPS. Indeed, as mentioned before, the drone can estimate its initial distance to the jammer (d_0) from a position where the GPS is not jammed, assuming the position of the jammer is known (target), and the jamming transmission power (P_t) is unknown. Subsequently, when the drone moves closer to the jammer, it will lose the GPS signal, but it will be able to infer its distance to the jammer ($d_1/d_0 = 1/\sqrt{2}$) from the variation of the received signal strength, i.e., $+3$dBm in the previous example. Our intuition, that has to lead us to implement a backup navigation system exploiting the jamming signal source, relies on the aforementioned relationship.

A. DEFINITIONS AND PLAYGROUND ASSUMPTIONS

In the remainder of this paper, we consider the following entities:

- **Drone.** An Unmanned Aerial Vehicle (UAV) flying from a source position to a target destination. We assume the drone has been pre-programmed according to a mission plan and not radio-controlled; indeed, our jamming scenario makes the remote control of the drone useless. The mission plan involves a set of intermediate way-points and a final destination target.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2963105, IEEE Access

- **Adversary.** We assume the adversary is able to reprogram the drone and being able to change the mission plan parameters and all the flight control systems.
- **Target.** The destination point that the drone has to reach.
- **Jammer.** The radio device used to protect the target neighbourhood. We assume a very powerful, omnidirectional and isotropic jammer, being able to jam all the radio frequencies in the radio spectrum over a circle of radius $\mathcal{D}_{thr}$ meters. Recalling the free space model (Eq. 2), the maximum jamming distance $\mathcal{D}_{thr}$ yields:

$$P_r = P_t + G_t + G_r + 20\log_{10}(\frac{c}{4\pi f \mathcal{D}_{thr}}), \quad \mathcal{D}_{thr} = \frac{1}{\frac{4\pi f}{c}10^{(\frac{P_r - P_t}{20})}} \tag{2}$$

  where $P_r = -30$dBm is receiving threshold of the drone, $P_t = 20$dBm is the jammer transmission power, $G_t = G_r = 0$ are the (isotropic) antennas' gains [47], and finally, $f = 1575.42$MHz is the GPS frequency. We highlight that different P_r and P_t do not affect our analysis while changing the performance of the jammer. Indeed, our analysis is rooted on the general idea of jamming-based navigation, and therefore, the more powerful is the jammer the more reliable will be the reference point for our navigation system. Finally, we observe that under the realistic aforementioned assumption, $\mathcal{D}_{thr} = 479$ meters.

Further, we assume the firmware of the drone has been reprogrammed in such a way that, the drone behaves as usual, when the link between the remote controller and the drone is not affected by the jammer, while it switches to *JAM-ME* mode when both the signals from the GPS and the remote controller cannot be received.

Jamming techniques. Different jamming techniques and equipment can be deployed to prevent the drone to communicate with the remote controller. A preliminary consideration should be devoted to the antenna that can be either *omnidirectional* or *directive*. While the former spreads the radiating power in all the directions, the latter focuses the jamming energy budget in only one direction, i.e., main antenna lobe. Moreover, while the omnidirectional antenna suffers less jamming power concerning the directive one (the transmitted power is indeed spread uniformly in the circle around it), it does not require to track the drone. Indeed, in order to be effective, the directive antenna has to precisely aim at the drone all the time. From our perspective, the more powerful is the jamming signal, the more reliable will be the *JAM-ME* navigation system. Finally, we assume the jamming signal power as constant all over the time, and an isotropic/omnidirectional antenna. Indeed, constant-power jammers, e.g., *constant jammer, deceptive jammer, spot jammer*, are a common assumption in the literature. Moreover, we observe that a power-modulated jamming transmitter might not be effective to achieve maximum area coverage, therefore allowing enemy communications at closer distances. Indeed, the drone might exploit the periods characterized by low-power jamming transmission to receive both positioning and navigation information, and therefore, getting closer to the target.

Hardware and software assumptions. Without loss of generality, we assume our drone to be a commercial one featuring standard radio functionalities. Received Signal Strength estimation is provided out-of-the-box by the 802.11 protocol (Wi-Fi). Therefore, the estimation of the received jamming power, as well as any other transmission, might be provided by assuming a mini SDR mounted on a drone (e.g. HackRF, LimeSDR) that acquires the RSS value and sends it to the drone as input for the computation. Moreover, we assume the drone's antenna to be isotropic and omnidirectional; we stress that this is a conservative assumption since a directive antenna would enable the drone to infer more information related to the jammer and its position. Indeed, a directive antenna characterized by different radiation patterns, might let the drone get closer to the jammer by exploiting the (side) lobes with minimum gain.

Drone sensing assumptions. We assume a drone featuring no sensors. Standard navigation techniques might resort to vision (limited to scenarios with good weather conditions, e.g. without fog, rains, artificial lights—during the night), acoustic and physical sensing, e.g., accelerometer, magnetometer and barometer readings. In this work, we assume the conservative stance of a pure RF-based navigation (jamming-driven), while being aware that sensors can significantly improve the performance of the navigation.

Finally, we assume that the drone standard navigation system has been reprogrammed. Indeed, we assume a non-standard behaviour of the drone in the presence of a jammer, since commonly available drones either land or crash when they lose their radio communication capabilities. There are plenty of examples in the literature related to firmware hacking, e.g., Maldrone and Node Copter, but we can also assume that our drone has been assembled from scratch and programmed using one of the available open-source platform, e.g., Dronecode [48], ArduPilot [49].

In order to prove the feasibility of drone navigation under jamming conditions, we consider the following challenging scenario configuration.

Scenario Configuration. We consider a jammer protecting an area against drones as depicted by Fig. 2. The drone is programmed to fly over the area and reaching the target. On the one hand, the jammer protects a certain perimeter (jammed area represented by the grey circle within the dashed black circumference) and the respective target located in the area. The jammer prevents the reception of the GPS signals, and therefore, the navigation of any UAV. On the other hand, the adversary might re-program the firmware of the drone according to our algorithm (*JAM-ME*) to feature a jamming-based navigation system. By adopting this solution, the attacker will be able to fly over the jamming area, and reach the target.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2963105, IEEE Access

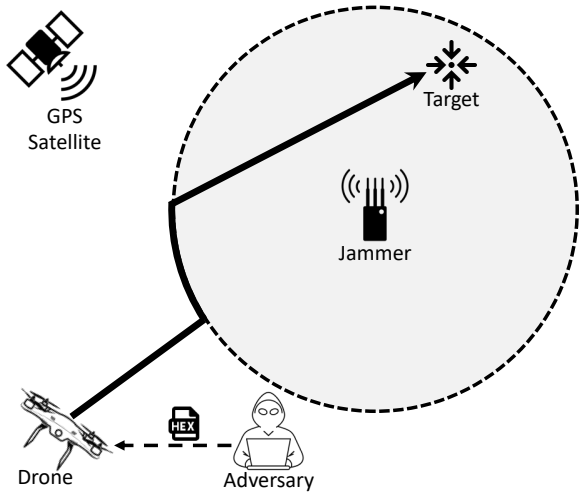

Figure 2. **Scenario Configuration.**

Target position awareness. We assume the target GPS position been well known to the adversary, and therefore, to the drone. The target might be constituted by a static object such as a critical infrastructure, i.e., airport, hospital, oil, and gas refinery, or a static person (e.g. a VIP attending a public event) [50].

Unknown jammer position. We assume the jammer been deployed in the proximity of the target, although its position been unknown. We observe that a jammer standing at the same position of the target guarantees maximum range protection while a jammer placed to a different position might expose one side of the target. Regardless of these considerations, we will show that our solution is agnostic concerning the relative position of the jammer.

Unknown drift forces inside the jamming area. We consider a scenario where the drone might be affected by unknown wind drift. We consider a drift force constituted by both a random direction and a random strength. Nevertheless, no drift is considered outside the jamming area, since the drone, being able to receive the GPS signal, can autonomously compensate and correct its position accordingly. That is, even if the drift force is there, it does not affect the drones navigation capabilities since this last one can compensate the drift generated effects.

No Instrumental Navigation Systems (INSs). We assume the worst-case scenario according to which the drone does not resort to any navigation system based on sensors that might allow to compute its current position and planning the future trajectory.

Simulator parameters. Table 1 wraps up the notation used throughout this paper and it introduces some of the parameters adopted in the simulator.

IV. LEVERAGING JAMMING FOR DRONE NAVIGATION

This section introduces the architectural model of the *flight controller* exploiting the received signal strength of a jammer to fly close to a predetermined target. Figure 3 shows the

Table 1. Notation summary

RSS	Received Signal Strength
$\mathcal{P}_{thr} = -30dBm$	Received Signal Strength at the jamming area boundary
$\mathcal{D}_{thr} = 479m$	Distance between the jammer and the jamming area boundary
$P(t)$	Received Signal Strength by the drone
$V_D = 1m/s$	Reference speed of the drone
α_w	Wind angle
(T_x, T_y)	Target position
(ep_x, ep_y)	Entry point in the jamming area
$P_T(t)$	Expected Received Signal Strength at the target position

block diagram of a *closed loop control system* constituted by a Proportional-Integral-Derivative (PID) controller and a drone. The control action $c(t)$ from the controller is provided as input to the drone system, which in turn, will generate the output process variable $y(t)$ that will be piggyback as input to the controller as the difference from a reference signal. Firstly, we highlight that when $y(t) = r(t)$, the error $e(t)$ becomes null, and in turn, the control variable $c(t)$ does not change, and therefore, the drone preserves its current status, i.e., maintaining its current trajectory. When the output $y(t)$ is not null, the error increases and, in turn, the control signal compensates the status of the drone to recover to $y(t) = r(t)$. It is worth noting that in this context, the PID controller variables are mapped as follows:

1) the reference variable $r(t)$ corresponds to the received signal strength. We consider a conversion factor $\eta = 1 \cdot \frac{m}{Watt*s}$ to make it dimensionally consistent with the other entities in the PID controller;
2) the error variable $e(t)$ maps the difference between the current received and the expected power signal strength;
3) the output variable $y(t)$ matches with movement/speed compensation that the drone needs to take into account to adjust its trajectory.

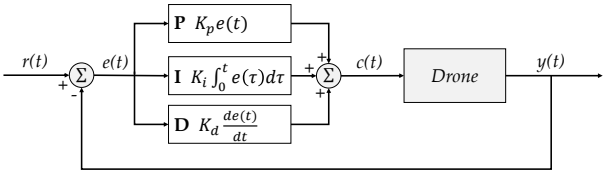

Figure 3. **System architecture of the drone flight controller.**

The PID controller sums up three key elements: a proportional, an integrative, and a derivative controller behaving according to Eq. 3:

$$c(t) = K_p e(t) + K_i \int_0^t e(\tau)d\tau + K_d \frac{\partial}{\partial t} e(t) \qquad (3)$$

where K_p, K_i, and K_d are the proportional, integral, and derivative gains, respectively. Finally, we adopt the Ziegler-Nichols method to tune the above parameters, i.e., $K_p = 0.6K_c$, $K_i = 2K_p$, and $K_d = K_p/8$, where K_c (empirically estimated) is the critical gain [51].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2963105, IEEE Access

V. BASELINE SCENARIO

In this section, we consider a baseline scenario as reported in Fig. 4 constituted by a drone (triangle) willing to accomplish a mission by reaching a target (cross) protected by a jammer (diamond). In this case, we assume that the target and the jammer share the same coordinates and the jammer transmits the jamming signals at its maximum power level to achieve the maximum area coverage around the target. Further, we stress that in this scenario the navigation of the drone is not affected by any drift or external forces such as the wind. We will relax this assumption in the latter sections.

In order to reach the target protected by the jammer, the drone should accomplish the following phases.

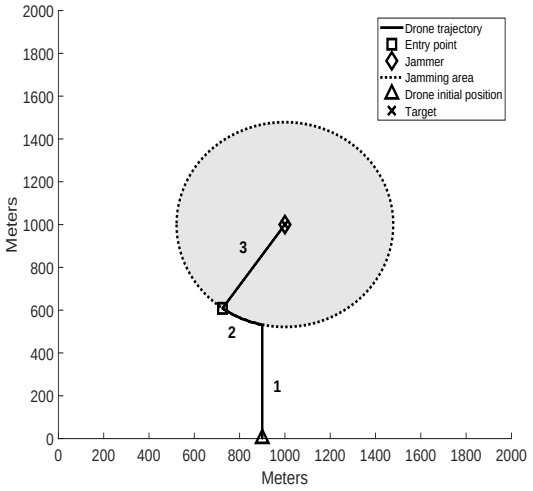

Figure 4. Baseline scenario of a drone reaching a target: (i) Approaching the jamming area; (ii) Estimating the jammer position and, finally, (iii) Approaching the Target.

Approaching the jamming area. In Phase 1, when the drone is outside the jamming area (dotted circle), it leverages its standard navigation positioning system (e.g. GPS) to follow the path to the destination. As specified before, the drone is programmed to follow a trajectory (solid line) that consists of a set of pre-loaded way-points up to the target (located in the jamming area).

Estimating the jammer position. Phase 2 starts when the drone detects the jamming signal, e.g., by monitoring the RSS [52], and inferring the presence of the jammer when the RSS is greater than a given threshold $\mathcal{P}_{thr}$, i.e., RSS $> \mathcal{P}_{thr}$. A simple and effective way to estimate $\mathcal{P}_{thr}$ can be obtained by continuously measuring the GPS link, and when such a link gets corrupted due to the jammer, the drone moves back up to the position where the GPS link is working properly. Therefore, during this phase, the drone is still able to receive the signal from the GPS satellites—being far away from the jammer, it is able to estimate the power of the jamming signal, while this latter one is not strong enough to jam the GPS signal yet. In order to compute the position of the jammer, as shown in Fig. 4 (Phase 2), the drone will follow a path coincident with the boundary of the jamming area, such that the received signal power $P(t)$ is constant and equal to $\mathcal{P}_{thr}$. We assume that the drone can estimate the Received Signal Strength on the GPS received signal by considering $\mathcal{P}_{thr}$ as the RSS upper limit to receive the GPS signal without any interference due to the jammer. In order to estimate the jammer position and follow a path coincident with the boundary of the jamming area, the drone will adopt a PID controller as depicted in Fig. 3 by setting the reference variable $r(t) = \mathcal{P}_{thr}$ and the critical controller's gain $K_c = 1$ (empirically estimated). Feedback signal $y(t)$ is compared with the reference signal/variable $r(t)$ and the difference between $r(t)$ and $y(t)$ is the error value $e(t)$ provided to the PID controller. According to the proportional, integral and derivative control terms, the controller minimizes the error related to the drone's trajectory to estimate the jammer position. Minimising the error with the PID controller, the drone will follow a path coincident with the boundary of the jamming area by keeping the received jamming power constant. In general, in this contribution, we considered a power receiving threshold $\mathcal{P}_{thr} = -30dBm$. During our experiments, we noted that this threshold value could be different if we take into account several GPS receivers—left for future work. As a final step for this phase (the drone flying over the border of the jammed area), the collected position data from the GPS sensor can be used to estimate the jammer's position as the centre of the jamming area boundary, by adopting the Pratt method [53].

Assuming no drifting forces in the jamming area (e.g. no wind), the drone will choose the optimal entry point (square in Fig. 4) on the jamming area boundary by minimizing the error on the jammer position estimation. The error estimation of the jammer position is depicted in Fig. 5, according to the movement of the drone over the jamming area boundary.

The error associated with the position estimation of the jammer can be made arbitrarily small by delaying Phase 2, i.e., by making the drone flying longer on the boundary of the jamming area. Indeed, the jamming position error can be minimized by acquiring more samples on the border associated with the received signal strength of the jammer itself. Without loss of generality, we decide to stop the process of estimating the jamming position when the error associated with the position itself is less than a predefined threshold (25 meters). Assuming the previously introduced system parameters, this translates in the drone flying a distance, over the border of the jammed area, of about 190 meters.

Approaching the target. The drone flies towards the target during Phase 3. We observe that the direction to the target is well-know to the drone since it knows its current position (at the jamming border) and it knows the position of the target. While in this section the target and the jammer have the same position, we will relax this assumption in Section VII.

Stop criteria. We assume the drone will stop flying towards the target when $P(t) = P_T(t)$ where $P(t)$ is the RSS

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2963105, IEEE Access

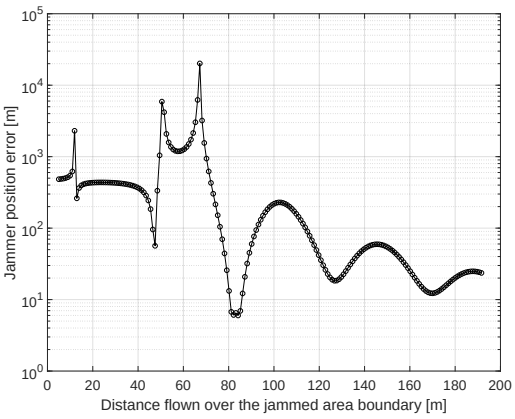

Figure 5. Jammer position error estimation as a function of the distance travelled by the drone.

measured by the drone, and $P_T(t)$ is the expected RSS at the target position (T_x, T_y). We highlight that $P_T(t)$ can be pre-computed by the drone before entering the jamming area since the position of the target is assumed to be well-known to the drone.

We observed that a stop criteria that takes into account the distance travelled by the drone instead of signal strength, i.e., the drone computes the distance to the target with dead reckoning techniques using sensors such as accelerometers, and stops after having covered that distance, is not fair with our assumptions. Indeed, we want to stress that (i) we are assuming a drone featuring no sensors, and (ii) in the presence of wind, this stop criteria does not allow to reach the target.

Figure 6 shows the Received Signal Strength as a function of the time when the drone approaches the target accomplishing the three phases previously described. During Phase 1 the drone flies straight to the target up to the point where $P(t) = \mathcal{P}_{thr}$, i.e., the RSS by the drone is equal to the threshold to infer on the presence of a jammer. We stress that even at this location, the drone is still able to receive the GPS signal. Indeed, as previously discussed, if this is not happening, the threshold $\mathcal{P}_{thr}$ can be made arbitrarily small to guarantee the correct reception of the GPS signal. Now, assuming the drone is receiving both the jamming and the GPS signal, it can fly around the jammer (the jamming boundary) by keeping a constant distance to it, and therefore, guaranteeing the jamming signal is not disrupting the GPS one (in Figure 7, is depicted the fluctuating RSS experienced by the drone when is flying around the jammer). The aforementioned task is accomplished during Phase 2 exploiting PID controller where $r(t) = \mathcal{P}_{thr}$. Moreover, during this phase, the drone estimates the position of the jammer, and when such an estimation is precise enough (as shown in Fig. 5), it decides to enter the jamming area (losing the GPS assisted navigation) and flying being assisted only by the jamming signal. In this phase called Phase 3, since the drone is moving towards the target(jammer), it will measure a RSS value that will be increased as it approaches the source of the jamming signal.

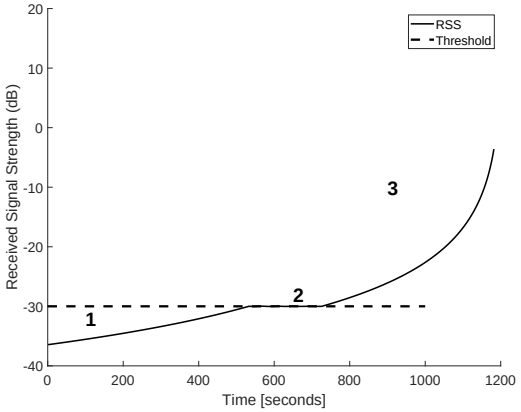

Figure 6. Received Signal Strength experienced by the drone when approaching the target (solid line), and Received Signal Strength $\mathcal{P}_{thr}$ at the jamming area boundary (dashed line).

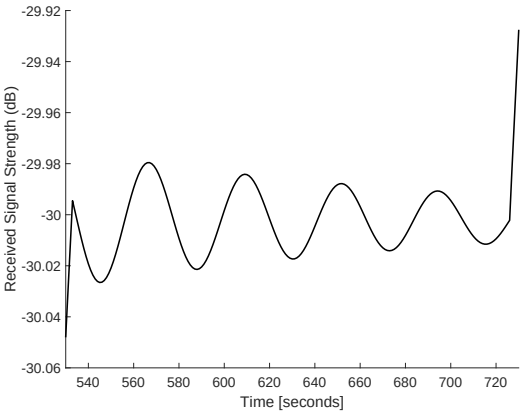

Figure 7. Received Signal Strength experienced by the drone when flying over the jammer boundary area—flight being controlled by the PID.

Algorithm 1 provides the pseudo-code of our solution.

- **Phase 1.** During Phase 1, the drone follows the pre-programmed way-points' sequence up to the location where the received signal strength overcomes a pre-defined threshold P_{thr}; indeed, we assume that the threshold P_{thr} is consistent with a position such that the drone still receives the GPS signals. The way-points are (x, y) coordinates pre-loaded in the drone's memory, and can be recovered by calling the function *load_waypoints()*, while the *gps_get_location()* will be adopted to get the current GPS drone's position (x_D, y_D).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2963105, IEEE Access

Data: initialize parameters;
Result: drone path;

```
// Phase 1
// Fly to the target
while (RSS < P_thr) do
    waypoints = load_waypoints();
    (x_D, y_D) ← gps_get_location();
end
// Phase 2
P ← P_thr;
K_c ← 1;
h ← 1;
detour();
while jam_pos_error <= thr do
    e ← RSS − P_thr;
    PID_controller(e, K_c, h);
    D_thr, (x_J, y_J) ← jammer_pos_estimation();
    h ← h + 1
end
PT(t) ← estimate_rx_power_on_target(x_T, y_T);
// Phases 3 and 4
α_w ← atan2(T_y − y_D, T_x − x_D);
(ep_x, ep_y) ← (T_x, T_y) + D_thr * cos(α_w) + D_thr * sin(α_w);
reach_entry_point(ep_x, ep_y);
h ← 1;
while RSS < PT(t) do
    e ← RSS − P_thr;
    u ← PID_controller(e, K_c, h);
    x_D ← (pos(end) + u) * cos(α_w);
    y_D ← (pos(end) + u) * sin(α_w);
    h ← h + 1
end
```

Algorithm 1: Pseudo-code of our proposed solution.

- **Phase 2.** When $P_{thr} \geq RSS$ Phase 2 starts. During this phase, the drone will perform a maneuver (either to the left or the right) by calling the function *detour()* and following a path such that $P == P_{thr}$. The later is possible by exploiting the PID controller receiving as input: (i) the error $e \leftarrow RSS - P_{thr}$ between the actual received signal strength (RSS) and the threshold P_{thr}; (ii) the critical gain K_c; and, finally, (iii) the iteration counter h. The controller will keep the drone on the circumference with center the jammer (x_J, y_J) by minimizing the aforementioned error, and therefore, computing the distance to the jammer D_{thr} by resorting to the function *jammer_pos_estimation()* by using the *Pratt* method [53]). Finally, the drone will estimate the received power $PT(t)$ on the target by calling the function *estimate_rx_power_on_target*(x_T, y_T), i.e., by resorting to the mathematical model of Eq. 2).
- **Phases 3 and 4.** The drone computes the entrance angle α_w and the entry point coordinates (ep_x, ep_y) and it will reach them according to the function *reach_entry_point*$(ep_x,\ ep_y)$. Subsequently, the drone will navigate across the jammed area to reach the target with coordinates (x_T, y_T), until $RSS < PT(t)$. The PID will control the drone navigation by compensating its position at every iteration h, as discussed in the previous phase. Finally, the drone current position (x_D, y_D) is update by combining the old position $pos(end)$ and the control variable u. At the end of this phase, the drone will reach the target position (x_T, y_T).

VI. DRONE NAVIGATION IN THE PRESENCE OF WIND DRIFT

In this section, we consider a wind drift with a direction that is incidental with the drone direction of an angle randomly chosen between 0 and 2π. We stress that the influence of the wind might be significant since the drone cannot resort to any useful navigation information. Indeed, in our case scenario, the wind can either slow down up to the standstill state or double the speed of the drone towards the target. The aforementioned behaviour combined with the lack of positioning and navigation information makes reaching the target a very challenging task that we solved by controlling the drone speed and position according to the Received Signal Strength from the jammer.

As for the intensity of the wind drift, it can dynamically vary between zero and the speed of the drone, in both directions; that is the drone will experience, during its movement towards the target, both upwind (frontal wind, contrasting the drone) and downwind (rear wind, speeding-up the drone). That is, while we do not pose any restriction on the intensity the wind, we assume that the direction of the wind will not change once the drone enters the jammed area, or that it will change just slightly.

We believe such an assumption is reasonable since the distance from the target is generally just few hundred meters (that will be covered by the drone in few minutes), and therefore the direction of the wind within the jammed area could be consistent with the wind direction detected just before entering such an area. Moreover, the drone could also rely on statistical data reporting on the dominant wind. Finally, it is worth noting that having a drone moving at $1m/s$ $(3.6Km/h)$ is a very conservative case; higher speed would require the drone to fly in the jammed area for a shorter period of time, and therefore the assumption that the wind direction does not change could hold with much higher assurance.

Approaching a target in the presence of wind drift is a particularly challenging task. Indeed, while the wind drift affects both the x and the y components of the navigation, the only available information inside the jamming area is the RSS—this latter one being a function of the radial distance to the jammer. We propose to solve this problem by accurately choosing the entry point on the circumference. Indeed, by choosing the entry point over the line passing through the jammer/target and parallel to the wind direction, we reduce the problem to one only degree of freedom (the wind intensity). Figure 8 shows the result of a simulation according to our scenario: as for the previous case, the drone first flies to the border of the jamming area (Phase 1) by following the pre-loaded way-points sequence; once the cited border has been reached, the drone estimates the jammer position by flying over the border (Phase 2, up to the asterisk in Fig. 8); it computes the entry point as a function of the target/jammer position and the wind direction (Phase 3); and, finally, it flies

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2963105, IEEE Access

towards the target (Phase 4). We remind that, in this case, the jammer (diamond in Fig. 8) and the target (cross in Fig. 8) are spatially coincident—in the next section we will treat the case where the target is not coincident with the jammer.

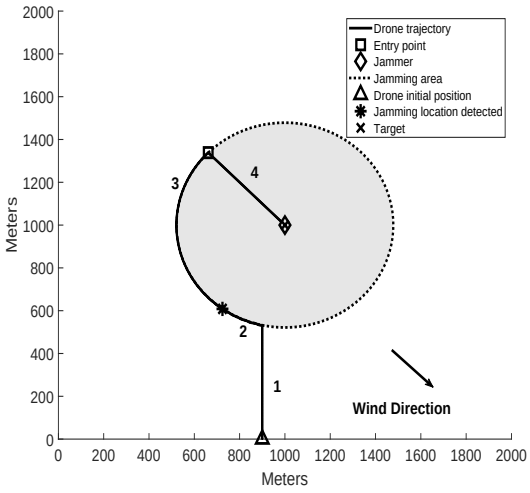

Figure 8. Scenario of a drone reaching a target in the presence of a wind drift: (i) Approaching the jamming area; (ii) Estimating the jammer position; (iii) Reaching the Entry Point; and, finally, (iv) Approaching the Target.

According to our assumptions, the drone estimates the wind direction outside of the jamming area, and then, it leverages this information to compute the entry point. As above discussed, we assume the wind direction to be constant; conversely, we consider the wind having a randomly varying intensity—assuming over time also upwind or downwind directions—that will be compensated by the PID controller by using a critical gain K_c equal to $K_c = 0.6$ (empirically estimated). We estimated the critical gain K_c through a trial-and-error procedure. In particular, we conducted several simulation experiments to estimate the optimal value of K_c for the PID controller to achieve a fast control with satisfactory stability. Therefore, recalling from Table 1 the target position as (T_x, T_y), the radius of the jamming areas as $\mathcal{D}_{thr}$, and finally, the wind angle as α_w, the entry point ep can be computed as depicted by Eq. 4:

$$(ep_x, ep_y) = (T_x, T_y) + \mathcal{D}_{thr} * cos(\alpha_w) + \mathcal{D}_{thr} * sin(\alpha_w) \quad (4)$$

After the drone has reached the entry point, it aims at the target. While in this section the target is coincident with the jammer, in next section we will release this assumption. We recall that the drone can precisely compute the direction between the entry point (ep_x, ep_y) and the target (T_x, T_y) since it knows the coordinates of both of them.

Dealing with unknown wind intensity. We consider the system design previously introduced by Fig. 3, and we adopt the PID controller to guarantee a constant speed for the drone.

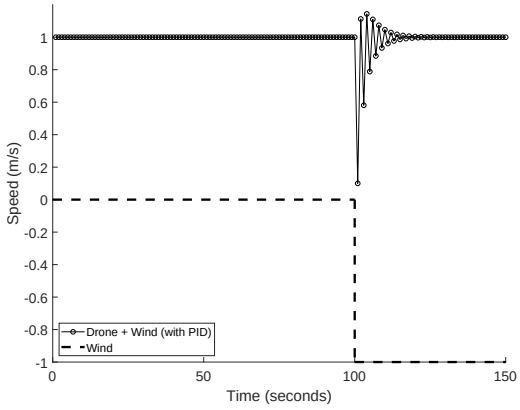

Figure 9. Wind drift mitigation by adopting the PID controller: dashed-line represents the wind speed (upwind $1m/s$), while line with circle-dots shows the drone's speed considering the action of the PID controller.

Therefore, we adopt a certain predefined speed (V_D) as the reference signal $r(t)$, while the system output turns out to be the current speed of the drone $v_D(t)$. Concerning the computation of the drone speed inside the jamming area, we resort to Eq. 5:

$$v_D(t) = \eta \frac{\partial}{\partial t} P(t) \quad (5)$$

where $\eta = 1 \cdot m/(Watt * s)$ is a conversion factor. Indeed, we recall that the received signal power is strictly related to the distance to the jammer by Eq. 1, and in turn, to the speed, by assuming the speed as the differentiate of the travelled distance.

Figure 9 depicts the drone's speed (line with circle-dots) as a function of the time when subject to a step change wind strength (dashed line). Firstly, we observe that wind intensity is exactly the same as the drone ($1m/s$ upwind - worst case), and it has been modelled as a step happening at $t = 100$ seconds. The wind might stop the drone (having the same upwind intensity) if no other instrumental navigation systems are taken into account—as it is the case in this work.

We observe that the adoption of a PID controller, configured with a reference signal equal to $V_D = 1m/s$ estimating the drone's speed as a function of the Received Signal Strength, as introduced by Eq. 5, can overcome the upwind force, and therefore, it helps the drone to keep a constant speed towards the target.

To provide a better comprehension of the effects of the wind on the drone's ability to accomplish its mission, we considered different upwind intensities spanning between 0.1 and $0.9m/s$. Figure 10 shows the local minimum for each considered case. Note that at time 99 (x-axis) the drone is not experiencing any wind; the wind starts blowing (upwind) at time 100. We observe that in all the cases the PID controller is able to recover from the upwind step and to guarantee

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2963105, IEEE Access

a subsequent constant speed of $1m/s$. As expected, the stronger the wind, the more it takes to regain the original speed. However, after just 7 seconds, in all the considered cases, the original speed ($1m/s$) has been recovered.

Finally, it is worth noting that having a drone moving at $1m/s$ ($3.6Km/h$) is a very conservative case, other than for what highlighted at the beginning of this section, having a higher speed would also translate in the drone to cruise faster the jammed area, and hence reaching the target in a shorter time. For instance, a speed of just $40Km/h$ (compared to the $3.6Km/h$ assumed in this paper) could translate in reducing the incurred overhead (extra-time to reach the target in the presence of an external force, e.g., wind) of more than 90%, as it will be detailed at the end of Section VII.

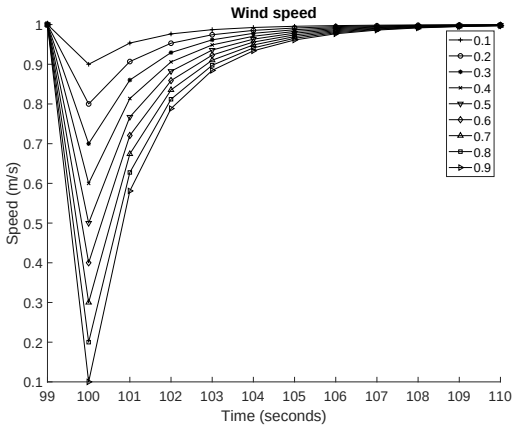

Figure 10. Resulting drone speed for different upwind speeds - spanning from 0.1 to $0.9m/s$: solid lines represent the local minimum associated with the drone governed by the PID controller.

VII. APPROACHING A RANDOMLY DEPLOYED TARGET

In this section, we consider the general case of a target within the jamming area, but placed in a different position concerning the jammer. This is motivated by either logistic assumptions, i.e., the jammer cannot be placed close to the target, or in an attempt to implement a simple countermeasure, being the target aware of the *JAM-ME* feature of the drone—it will be shown that this countermeasure is ineffective.

Figure 11 depicts the trajectory of a drone (triangle) willing to reach a target (cross). As for the previous cases, the drone is approaching the jamming area by following a path of way-points (Phase 1), it is aware of the target position, but it does not know the jammer position and the wind strength that it might encounter when flying inside the jamming area.

As for the previous case (Fig. 8), the drone is required to estimate the position of the jammer flying over the jamming area border (Phase 2, up to the asterisk in Fig. 11) and, subsequently, to estimate the point of entrance (square) in the jamming area (Phase 3) so as to reach the target (Phase 4). The entry point is critical when the target is not superimposed on the jammer. Indeed, the entry point should lay on the line

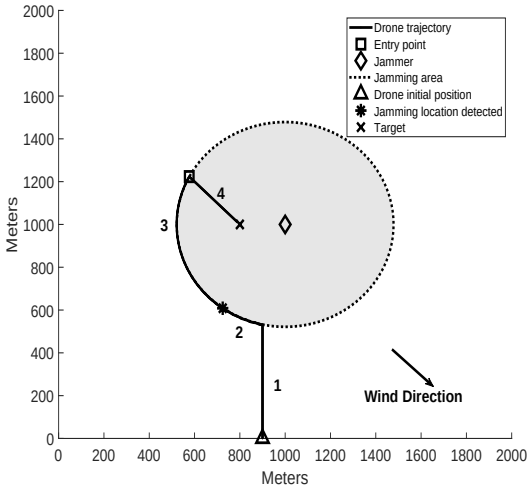

Figure 11. Scenario of a drone reaching a target (not coincident with the jammer) in the presence of a wind drift: (i) Approaching the jamming area; (ii) Estimating the jammer position; (iii) Reaching the Entry Point; and, finally, (iv) Approaching the Target.

parallel to the wind and passing by the target. This latter requirement guarantees that the drone will fly in the same absolute direction of the wind (either upwind or downwind), and therefore, its trajectory will not be affected, while the intensity of the wind could dynamically change—this latter phenomenon being compensated by the drone via the PID controller.

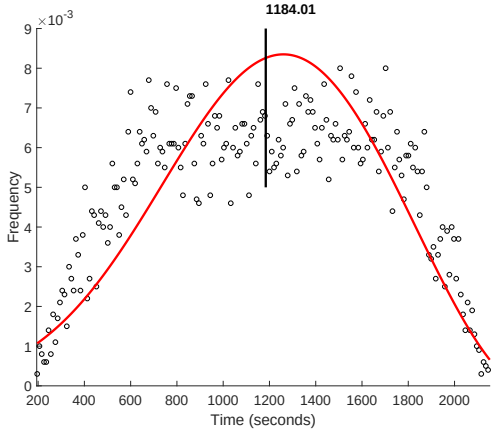

Figure 12. Time to reach a randomly deployed target assuming a speed of $1m/s$ and an upwind speed equal to the drone's speed.

Figure 12 shows the time to reach a randomly deployed target inside the jamming area assuming a drone's speed of $1m/s$ and an upwind of the same intensity (worst case scenario). We consider a total of $10,000$ simulations where we do not consider the time to approach the jamming area (Phase 1 in Fig. 11). Therefore, we conceive only the time to

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2963105, IEEE Access

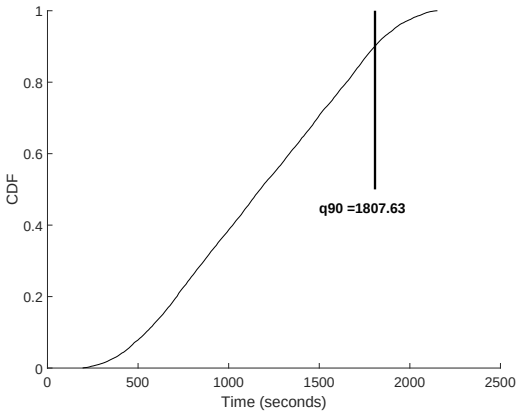

Figure 13. Cumulative Distribution Function (CDF) associated with the time to reach a random distributed target: solid vertical line shows the quantile 90 being equal to $1,807.63$ seconds.

estimate the jamming position, reaching the entry point, and approaching the target. The solid red line in Fig. 11 shows the best-fit probability distribution according to the Maximum Likelihood Estimate (MLE) being the Generalised Extreme Value (GEV). Let μ the location parameter, σ the scale parameter, and $k \neq 0$ the shape parameter, the probability density function for the GEV distribution is:

$$y = f(x|k,\mu,\sigma) = \frac{1}{\sigma} e^{\left(-\left(1+k\frac{(x-\mu)}{\sigma}\right)^{-\frac{1}{k}}\right)} \left(1+k\frac{(x-\mu)}{\sigma}\right)^{-1-\frac{1}{k}} \tag{6}$$

where $k = -0.38$, $\sigma = 486.05$, and $\mu = 1042.17$.

We observe an average time of $1,184.01$ seconds for the drone to reach the target (in each simulation, the target has been placed in a random position inside the jamming area), while Fig. 13 shows the cumulative distribution function associated to the same data and a quantile 90 equal to $1,807.63$ seconds, i.e., the probability that the drone reaches a randomly deployed target in less than $1,807.63$ seconds is 0.9.

Moreover, we consider the distance between the drone's initial position and the target, and we compare it with the actual path flown by the drone when governed by the PID as depicted by Fig. 14. We estimated an average distance between the drone initial position and the target as equal to $1,024.08$ meters (average shortest in Fig. 14), while the average flown trip turns out to be $1,756.49$ meters (average flown in Fig. 14), being equal to an overhead (extra-time to reach a target that is not deployed in the same position of the jammer) of about 70%. We stress that the aforementioned distances take into account all the phases to reach the target: Phase 1: approaching the jamming area (about 532 meters); Phase 2: estimating the jamming position (about 194 meters); Phase 3: reaching the entry point (about 753 meters); and, finally, Phase 4: approaching the target (about 282 meters). Note that the distribution of the cloud of points in Fig. 14 is not uniform, though showing a certain degree of symmetry. For instance, we assume that the drone wants to reach a target, where the distance between the drone and the target itself is $1300m$ (see the x-axis). Since the target is positioned in the jammed area and there are external forces (e.g. the wind) that generated an overhead on *JAM-ME*, the drone mission will incur into an overhead. In the cited example, the drone will reach the target through $2000m$ (see the y-axis), instead of the estimated $1300m$ (see the x-axis).

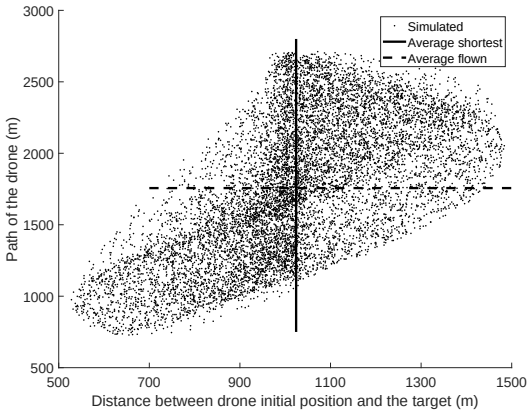

Figure 14. Comparison between the actual drone path (y-axis) and the shortest one (x-axis).

As a final consideration, it is worth noting that in this paper we have embraced a very conservative case: a drone speed of just $1m/s$ (a low-end commercial drone, such as the 3DR-Solo, can reach $89Km/h$, that is $24.72m/s$). Indeed, if the drone could move at a higher speed, the benefits would be striking. For instance, at a real—yet conservative—speed of just $40Km/h$ ($11.12m/s$), that is less than 45% of the max speed of the 3DR-Solo, the drone could spend (compared with a cruise speed of $1m/s$) less than one-tenth of the time required by Phase 2 and Phase 3 —flying over the jamming border to locate the jammer, and then moving to the entry point. In the example reported in this section, this translates in having Phase 2 and Phase 3 completed (on average) in less than 86 second (i.e. flying a distance of $194 + 753$ meters at $11.12m/s$) instead of 947 seconds (947 meters flown at $1m/s$); that is, a more than 90% overhead (extra-time required by the drone to reach a target that is not deployed at the same position of the jammer) reduction. Moreover, as already noticed, a higher speed would also dramatically reduce the time spent in the jamming area, and hence reducing the possibility to experience a change in the wind direction. For instance, once the drone is directing towards the target while in the jamming area (Phase 4), the time to cover a distance of roughly 500 meters, would be less than 50 seconds.

VIII. DISCUSSION AND FURTHER DIRECTIONS

In this section we will discuss the proposed solution, highlighting possible countermeasures to a drone navigating ex-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2963105, IEEE Access

ploiting the jamming signal. Later, we will discuss the limitations this contribution is affected by, and finally we will expose some research directions.

Countermeasures. We demonstrated that the standard techniques to jam a radio signal are not effective against drones that adopt the proposed countermeasure. A viable option to prevent the *JAM-ME* navigation system to estimate the current position of the drone and compute the trajectory, consists to modulate the radio jamming signal (e.g. change randomly the power transmission).

Power-modulated Jammer. The proposed RF-based navigation system requires a constant jamming signal. As previously discussed, power-modulated jamming, although being theoretically possible, has never been investigated before. Moreover, modulating the jamming power implies the reduction of the jamming coverage enabling, although for very short periods, enemy communications, and therefore, being not effective to the general goal of disrupting the communications. Further, it is worth noticing that while a power-modulated jammer might be more difficult to detect, varying the transmission power might allow a few packets to be still exchanged between the drone and the remote controller, in particular during the periods of low power jamming.

Another smart strategy that a jammer could adopt is to perform the two following concurrent tasks:

- *Distance bounding*: The jammer estimates the distance to the drone using already available techniques, e.g., the time between the transmission and the reception of the transmitted and the reflected jamming signal by the drone (radar).
- *Adaptive jamming*: Let P_T the power transmission and d_e the estimated distance. The jammer adjusts and controls its transmission power as a function $P_T(d_e)$. In details, the jammer can modulate the power transmission by increasing or decreasing it, to mimic a dummy distance (i.e. closer or further to the drone).

Adaptive jamming and distance bounding might be combined to control the flight direction of the drone. Indeed, the jammer might vary the jamming power to affect the decision of the drone. The above solution requires the detection of the drone well in advance to perform the distance bounding. Moreover, the aforementioned technique requires the jammer to feature a precise distance estimation technique involving more hardware software, e.g., radar.

Limitations. The current proposal is the result of well-known solutions from control theory combined with our intuition of approaching a target (jamming the neighborhood to protect itself from drones) by exploiting a jamming-assisted navigation system. Although the extensive simulations do support our intuition (the source code of our simulator *JAM-ME* [18] has been released as open-source, to further boost industry and academia toward the development of robust and secure critical navigation systems), we do recognise three limitations in this work: (i) a full validation of the model is possible only via real experiments. As of the time of writing, we have in our lab a testbed set completed with jammer and drones (3DR-Solo). While preliminary results do confirm our findings, we will report those findings in a future work; and, (ii) the assumption on the wind-direction stability, (iii) the Proof of Concept to demonstrate the feasibility of our solution. Despite this latter one has been thoroughly discussed in Section VI, it is worth mentioning that we are performing active research on this issue, to cope with this system variable.

Despite the above limitations, both currently under investigation, we believe that *JAM-ME* still enjoys a wide applicability range. At the time of writing, our solution could not be adopted against a new class of low power GNSS jammers [54] or receivers that adopts Viterbi decoders [55]. Despite the above limitations, both currently under investigation, we believe that *JAM-ME* still enjoys a wide applicability range.

Civil applications. Jamming assisted navigation might be considered as a backup system when standard navigation systems either fail or are corrupted. As an application scenario, we can consider a drone carrying medical equipment in a hostile area while an attacker is jamming the area. The drone could exploit the jammer as a radio-beacon to reach the target position, and provide the medical supplies. Other scenarios might include aerial crop surveys, search and rescue, inspection of power lines and pipelines, reconnaissance operations, surveillance, and waste management [56].

Research directions. The solution presented in this paper is, to the best of our knowledge, the first one that leverages the very same jamming activity to restore navigation functionalities. As such, we do recognise that there are still plenty of research questions that call for further investigations. In the following we list what we believe is the major ones: (i) how to tame the power-modulated jammer countermeasure; (ii) how to accommodate a changing direction wind; (iii) investigate on what happens when the number of jammers increases, with respect to the considered scenarios; (iv) what if we could consider more drones, with some limited communication capabilities among them: would this help drones to reach the target more efficiently?; and, finally, (v) what would be the best theoretical model to describe the jammer(s)-drone(s) interaction—for instance following the same line of reasoning as the game-theoretical model adopting the Bayesian Stackelberg game, used to formulate the competitive interactions between drone and jammer as in [57].

IX. CONCLUSION

In this paper, we have shown that jamming being the most effective way to neutralise the threat posed by a drone, despite being a commonly accepted assumption, is false. Indeed, we have devised a solution (*JAM-ME*) that, even when all the radio spectrum is jammed, provides a set of minimal, yet effective, navigation functionalities by exploiting just the very same jamming signal.

In particular, a drone adopting our completely passive solution, even in a very conservative scenario—moving in a jammed area, with active wind drift, the target being randomly deployed in the jammed area, and a drone speed

of $1m/s$—, still reaches its assigned target. *JAM-ME* is also efficient: it introduces a delay in reaching the target of about 70% when compared against a standard direct cruise—but note that a drone not equipped with *JAM-ME*, would have simply failed reaching its target. Moreover, as discussed in the paper, such overhead can be dramatically reduced (by 90% and more) just increasing the drone speed.

Further, we also introduce some countermeasures that could be deployed—and their limitations—to neutralise *JAM-ME*. Finally, we outline future and open research directions for the development of reliable solutions adopting this disruptive technology.

X. ACKNOWLEDGEMENTS

The authors would like to thank the anonymous reviewers for their suggestions, that helped to improve the quality of the manuscript.

The publication of this article was funded by the Qatar National Library (QNL), Doha, Qatar and awards NPRP11S-0109-180242, UREP23-065-1-014, and NPRP X-063-1-014 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 or the QNL.

References

[1] F. Flammini, C. Pragliola, and G. Smarra, "Railway infrastructure monitoring by drones," in 2016 International Conference on Electrical Systems for Aircraft, Railway, Ship Propulsion and Road Vehicles International Transportation Electrification Conference (ESARS-ITEC). IEEE, Nov 2016, pp. 1–6.

[2] S. Chandrasekharan, K. Gomez, A. Al-Hourani, S. Kandeepan, T. Rasheed, L. Goratti, L. Reynaud, D. Grace, I. Bucaille, T. Wirth, and S. Allsopp, "Designing and implementing future aerial communication networks," IEEE Communications Magazine, vol. 54, no. 5, pp. 26–34, May 2016.

[3] M. Erdelj, E. Natalizio, K. R. Chowdhury, and I. F. Akyildiz, "Help from the Sky: Leveraging UAVs for Disaster Management," IEEE Pervasive Computing, vol. 16, no. 1, pp. 24–32, Jan 2017.

[4] M. Mozaffari, W. Saad, M. Bennis, Y. Nam, and M. Debbah, "A Tutorial on UAVs for Wireless Networks: Applications, Challenges, and Open Problems," IEEE Communications Surveys Tutorials, vol. 21, no. 3, pp. 2334–2360, 2019.

[5] Stephen Jones (Mirror). (2017) Drone crashes into boeing 737 jet plane coming into land at mozambique airport. http://www.mirror.co.uk/news/world-news/drone-crashes-boeing-737-jet-9574073. (Accessed: 2019-09-14).

[6] The Guardian. (2016) Crew members injured as plane avoids near collision with suspected drone. https://www.theguardian.com/world/2016/nov/14/toronto-airport-drone-incident-injuries-canada. (Accessed: 2019-09-14).

[7] BBC. (2019) Saudi arabia oil facilities ablaze after drone strikes. https://www.bbc.com/news/world-middle-east-49699429. (Accessed: 2019-09-14).

[8] Michael Goldstein (Forbes). (2018) After gatwick, will 2019 bring a drone-airliner disaster? https://www.forbes.com/sites/michaelgoldstein/2018/12/22/will-2019-bring-a-drone-airliner-disaster/. (Accessed: 2019-09-14).

[9] S. Sciancalepore, O. A. Ibrahim, G. Oligeri, and R. Di Pietro, "Picking a Needle in a Haystack: Detecting Drones via Network Traffic Analysis," arXiv preprint arXiv:1901.03535, 2019.

[10] C. Aker and S. Kalkan, "Using deep networks for drone detection," in 2017 14th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), Aug 2017, pp. 1–6.

[11] J. Busset, F. Perrodin, P. Wellig, B. Ott, K. Heutschi, T. Rühl, and T. Nussbaumer, "Detection and tracking of drones using advanced acoustic cameras," in Proc. SPIE 9647, Unmanned/Unattended Sensors and Sensor Networks XI; and Advanced Free-Space Optical Communication Techniques and Applications, vol. 9647, 2015.

[12] J. Kim, C. Park, J. Ahn, Y. Ko, J. Park, and J. C. Gallagher, "Real-time UAV sound detection and analysis system," in 2017 IEEE Sensors Applications Symposium (SAS), March 2017, pp. 1–5.

[13] I. Guvenc, F. Koohifar, S. Singh, M. L. Sichitiu, and D. Matolak, "Detection, Tracking, and Interdiction for Amateur Drones," IEEE Communications Magazine, vol. 56, no. 4, pp. 75–81, April 2018.

[14] R. Altawy and A. M. Youssef, "Security, Privacy, and Safety Aspects of Civilian Drones: A Survey," ACM Trans. Cyber-Phys. Syst., vol. 1, no. 2, pp. 7:1–7:25, Nov. 2016.

[15] X. Shi, C. Yang, W. Xie, C. Liang, Z. Shi, and J. Chen, "Anti-Drone System with Multiple Surveillance Technologies: Architecture, Implementation, and Challenges," IEEE Communications Magazine, vol. 56, no. 4, pp. 68–74, April 2018.

[16] R. Curpen, T. Bălan, I. A. Micloş, and I. Comănici, "Assessment of Signal Jamming Efficiency Against LTE UAVs," in 2018 International Conference on Communications (COMM), June 2018, pp. 367–370.

[17] R. Di Pietro, G. Oligeri, and P. Tedeschi, "JAM-ME: Exploiting Jamming to Accomplish Drone Mission," in 2019 IEEE Conference on Communications and Network Security (CNS), June 2019, pp. 1–9.

[18] Cybersecurity Research and Innovation Lab (CRI-LAB), "Open-source code of the implementation of JAM-ME protocol," https://github.com/pietrotedeschi/jamme, 2019, (Accessed: 2019-09-14).

[19] Michael S. Schmidt and Eric Schmitt (The New York Times). (2016) Pentagon confronts a new threat from isis: Exploding drones. https://www.nytimes.com/2016/10/12/world/middleeast/iraq-drones-isis.html. (Accessed: 2019-09-14).

[20] C. Forrest, "17 drone disasters that show why the faa hates drones," https://www.techrepublic.com/article/12-drone-disasters-that-show-why-the-faa-hates-drones/, 2019, (Accessed: 2019-09-14).

[21] Chris Matyszczyk (CNET), "Truck driver has gps jammer accidentally jams Newark airport," https://www.cnet.com/news/truck-driver-has-gps-jammer-accidentally-jams-newark-airport, 2013, (Accessed: 2019-09-14).

[22] L. Lv, J. Chen, L. Yang, and Y. Kuo, "Improving physical layer security in untrusted relay networks: cooperative jamming and power allocation," IET Communications, vol. 11, no. 3, pp. 393–399, 2017.

[23] H. Xing, K.-K. Wong, A. Nallanathan, and R. Zhang, "Wireless Powered Cooperative Jamming for Secrecy Multi-AF Relaying Networks," IEEE Transactions on Wireless Communications, vol. 15, no. 12, pp. 7971–7984, Dec 2016.

[24] L. Tang and Q. Li, "Wireless Power Transfer and Cooperative Jamming for Secrecy Throughput Maximization," IEEE Wireless Communications Letters, vol. 5, no. 5, pp. 556–559, Oct 2016.

[25] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A Comprehensive Survey on Cooperative Relaying and Jamming Strategies for Physical Layer Security," IEEE Communications Surveys Tutorials, pp. 1–1, 2018.

[26] P. Barsocchi, S. Lenzi, S. Chessa, and G. Giunta, "A Novel Approach to Indoor RSSI Localization by Automatic Calibration of the Wireless Propagation Model," in VTC Spring 2009 - IEEE 69th Vehicular Technology Conference. IEEE, April 2009, pp. 1–5.

[27] N. Patwari, J. N. Ash, S. Kyperountas, A. O. Hero, R. L. Moses, and N. Correal, "Locating the nodes: cooperative localization in wireless sensor networks," IEEE Signal Processing Magazine, vol. 22, no. 4, pp. 54–69, July 2005.

[28] T. Wang, X. Wei, J. Fan, and T. Liang, "Adaptive jammer localization in wireless networks," Computer Networks, vol. 141, pp. 17 – 30, 2018.

[29] Q. D. Vo and P. De, "A Survey of Fingerprint-Based Outdoor Localization," IEEE Communications Surveys Tutorials, vol. 18, no. 1, pp. 491–506, Firstquarter 2016.

[30] S. Bhamidipati and G. X. Gao, "Locating Multiple GPS Jammers Using Networked UAVs," IEEE Internet of Things Journal, pp. 1–1, 2019.

[31] R. Di Pietro and G. Oligeri, "Freedom of Speech: Thwarting Jammers via a Probabilistic Approach," in Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks, ser. WiSec '15. New York, NY, USA: ACM, 2015, pp. 4:1–4:6.

[32] Q. Wang, T. Nguyen, P. Khanh, and H. Kwon, "Mitigating Jamming Attack: A Game-Theoretic Perspective," IEEE Transactions on Vehicular Technology, vol. 67, no. 7, pp. 6063–6074, July 2018.

[33] G. Rezgui, E. V. Belmega, and A. Chorti, "Mitigating Jamming Attacks Using Energy Harvesting," IEEE Wireless Communications Letters, vol. 8, no. 1, pp. 297–300, Feb 2019.

[34] S. Lakshminarayana, J. S. Karachiwala, S.-Y. Chang, G. Revadigar, S. L. S. Kumar, D. K. Yau, and Y.-C. Hu, "Signal Jamming Attacks Against Communication-Based Train Control: Attack Impact and Countermeasure," in Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks, ser. WiSec '18. New York, NY, USA: ACM, 2018, pp. 160–171.

[35] M. Mah, H. Lim, and A. W. Tan, "UAV Relay Flight Path Planning in the Presence of Jamming Signal," IEEE Access, vol. 7, pp. 40 913–40 924, 2019.

[36] Y. Li, R. Zhang, J. Zhang, S. Gao, and L. Yang, "Cooperative Jamming for Secure UAV Communications with Partial Eavesdropper Information," IEEE Access, pp. 1–1, 2019.

[37] J.-H. Kang and K.-J. Park, "Spatial retreat of net-drones under communication failure," in 2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN). IEEE, July 2016, pp. 89–91.

[38] R. Di Pietro and G. Oligeri, "Silence is Golden: Exploiting Jamming and Radio Silence to Communicate," ACM Trans. Inf. Syst. Secur., vol. 17, no. 3, pp. 9:1–9:24, Mar. 2015.

[39] B. Van den Bergh and S. Pollin, "Keeping UAVs Under Control During GPS Jamming," IEEE Systems Journal, vol. 13, no. 2, pp. 2010–2021, June 2019.

[40] G. Oligeri, S. Sciancalepore, O. Ibrahim, and R. Di Pietro, "Drive Me Not: GPS Spoofing Detection via Cellular Network," in Proceedings of the 12th ACM Conference on Security & Privacy in Wireless and Mobile Networks, ser. WiSec '19, 2019.

[41] B. Nassi, A. Shabtai, R. Masuoka, and Y. Elovici, "SoK-Security and Privacy in the Age of Drones: Threats, Challenges, Solution Mechanisms, and Scientific Gaps," arXiv preprint arXiv:1903.05155, 2019.

[42] T. Multerer, A. Ganis, U. Prechtel, E. Miralles, A. Meusling, J. Mietzner, M. Vossiek, M. Loghi, and V. Ziegler, "Low-cost jamming system against small drones using a 3D MIMO radar based tracking," in 2017 European Radar Conference (EURAD), Oct 2017, pp. 299–302.

[43] K. Pärlin, M. M. Alam, and Y. Le Moullec, "Jamming of UAV remote control systems using software defined radio," in 2018 International Conference on Military Communications and Information Systems (ICMCIS), May 2018, pp. 1–6.

[44] T. Rappaport, Wireless Communications: Principles and Practice, 2nd ed. Upper Saddle River, NJ, USA: Prentice Hall PTR, 2001.

[45] B. V. Der Bergh, A. Chiumento, and S. Pollin, "LTE in the sky: trading off propagation benefits with interference costs for aerial nodes," IEEE Communications Magazine, vol. 54, no. 5, pp. 44–50, May 2016.

[46] A. A. Khuwaja, Y. Chen, N. Zhao, M. Alouini, and P. Dobbins, "A Survey of Channel Modeling for UAV Communications," IEEE Communications Surveys Tutorials, vol. 20, no. 4, pp. 2804–2821, Fourthquarter 2018.

[47] Fahlstrom, Paul and Gleason, Thomas, Introduction to UAV systems. John Wiley & Sons, 2012.

[48] Dronecode - The Open Source UAV Platform, https://www.dronecode.org/, 2019.

[49] ArduPilot Open Source Autopilot, http://www.ardupilot.org/, 2019.

[50] Christoph Koettl and Barbara Marcolini (The New York Times). (2018) A closer look at the drone attack on maduro in venezuela. https://www.nytimes.com/2018/08/10/world/americas/venezuela-video-analysis.html. (Accessed: 2019-09-14).

[51] K. Ogata, Modern Control Engineering, 5th ed. Upper Saddle River, New Jersey, USA: Prentice Hall PTR, 2010.

[52] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," in Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing, ser. MobiHoc '05. New York, NY, USA: ACM, 2005, pp. 46–57.

[53] V. Pratt, "Direct Least-squares Fitting of Algebraic Surfaces," SIGGRAPH Comput. Graph., vol. 21, no. 4, pp. 145–152, Aug. 1987.

[54] G. Caparra, S. Ceccato, F. Formaggio, N. Laurenti, and S. Tomasin, "Low power selective denial of service attacks against GNSS," in Proceedings of the 31st International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2018). Institute of Navigation. Institute of Navigation, Oct 2018.

[55] J. T. Curran, "A Modified Viterbi Decoder for Joint Data-Recovery and Cycle-Slip Correction," in Proceedings of the 29th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2016). Institute of Navigation, Nov 2016.

[56] R. L. Finn and D. Wright, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications," Computer Law & Security Review, vol. 28, no. 2, pp. 184 – 194, 2012.

[57] Y. Xu, G. Ren, J. Chen, Y. Luo, L. Jia, X. Liu, Y. Yang, and Y. Xu, "A One-Leader Multi-Follower Bayesian-Stackelberg Game for Anti-Jamming Transmission in UAV Communication Networks," IEEE Access, vol. 6, pp. 21 697–21 709, 2018.