JAM-ME: Exploiting Jamming to Accomplish Drone Mission

Roberto Di Pietro, Gabriele Oligeri, Pietro Tedeschi
Hamad Bin Khalifa University, College of Science and Engineering
Division of Information and Computing Technology, Doha (Qatar)
e-mail: rdipietro@hbku.edu.qa, goligeri@hbku.edu.qa, ptedeschi@mail.hbku.edu.qa

***Abstract*—In this paper, we show, for the first time in the literature, that the common assumption that jamming is an effective way to neutralise drones, is false. In particular, we propose *JAM-ME* a solution that allows the drone to exploit an adversarial jamming signal to implement an emergency but yet effective navigation system, enabling the drone to accomplish its mission. Our contributions are manifold: first, we revise the jamming based anti-drone techniques; second, we introduce a basic model for *JAM-ME* and accompanying mathematical tool—rooted in systems control theory. Further, we show through an extensive simulation campaign that *JAM-ME* do allow a drone to accomplish its mission in a jammed area. Finally, we also discuss possible techniques to mitigate the impact of *JAM-ME* as well as its limitations, and we conclude highlighting further research directions. We believe that our contribution, other than being interesting on its own, can pave the way for further research in the highlighted directions, as well as having a compelling follow up from a practitioner point of view.**

I. Introduction

Unmanned Aerial Vehicles (UAVs), also known as drones, are remote-controlled aircraft that are becoming more and more popular due to their low cost, widespread availability, and wide range of applications—from commercial to leisure ones. Indeed, applications for drones are emerging in several fields, e.g., monitoring, surveillance, shipping, and patrolling [1], [2], [3]. Commercial drones are usually remotely controlled by users via the standard Wi-Fi bands (2.4GHz, 5GHz), and perform just a few tasks autonomously, such as tracking a target or being able to go back to the original take-off position. Unfortunately, drones can be very easily exploited to commit crimes, such as violating the privacy of people, for instance by shooting aerial pictures and videos. But drones could also be employed for more devastating criminal activities, such as to bomb critical infrastructures, e.g. airport, hospital and power plants, or even crowded places such as sport and cultural events [4], [5]. Given the above threats, in the last few years several countermeasures have been deployed to prevent the drones to reach a protected area. Some of these techniques involve the use of nets to be shot to the drone from the ground (with a gun) or even by another drone hunting for the not authorised one [6]. Recently, most important manufacturers of drones are implementing a 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 choosing a drone which is not implementing this feature.While the above countermeasures do have some degree of usefulness, one of the most effective and deployed solutions against drones is jamming. Jamming is a radio technique that involves a transmitter, i.e., the jammer, to broadcast a high power signal against the drone in order to disrupt its communications. Jamming is a very effective technique, since it allows the user to prevent the drone from either: (i) sending and receiving control commands to/from the remote controller, or (ii) receiving the Global Positioning System (GPS) coordinates—hence forcing the drone to abort its mission. Therefore, to the best of our knowledge, jamming is so far considered the most effective technique to be deployed for the protection of a target area from an approaching drone [7], [8], [9].

Contribution. In this paper, we show for the first time in the literature, that jamming might be almost useless when employed 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 a jammer jamming the whole radio spectrum, that makes jamming completely ineffective. *JAM-ME* leverages the jamming signal to compute the location of the jammer, that in turn is leveraged as a radio-beacon to compute the relative position of the drone with respect to the target. This latter will allow the drone to accomplish its mission.

Roadmap. The rest of the paper is organised as follows. Section II reports background information and related work, while Section III describes 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 our reference scenario. Finally, Section VI, provides possible mitigation techniques to *JAM-ME* and draws a few research directions, while in Section VII presents some concluding remarks.

II. Background and Related Work

In the following, we first provide a synthesis of the threats posed by an improper use of drones; later, we review the most important contributions, techniques, and solutions related to jamming and localisation this contribution is rooted on; and, finally, the last segment will address how jamming is currently employed to defeat drones.

A. Drones as Attack Vectors

Drones can be used to implement several attack strategies. As small flying entities, they can reach protected areas carrying hazardous material (e.g. explosive, virus) or can be equipped with devices (e.g. camera) that can violate privacy—in both cited cases, with very little chance of being detected. In the following, we summarise the main threats involving drones into three main families:

- *Privacy*. Drones can be easily used to take pictures and video from difficult to reach perspectives, and therefore, they can be maliciously used to collect information harming people / organisation privacy, as well as carrying out recognition activities that can be the needed prequel of a more dreadful activity.
- *Cyber-security*. Drones can be used to carry equipment, e.g., jammers, relay, radio, or any other ICT devices, to unconventional places to subsequently mount further attacks—e.g. eavesdropping, jamming, or extending adversarial ICT capabilities.
- *Critical Infrastructures*. Drone can be used against critical infrastructures facilities, such as airports, oil&gas industries, nuclear power plants, etc., for several operations, e.g., reconnaissance missions, providing support to a ground attack.
- *Safety*. Drones can be directly used for harming people safety by making them collide with people or things—think, for instance, to a drone colliding with a passenger airline commercial carrier [10]. Moreover, drones might also be used to deliver radioactive or explosives payload.

B. Related Work

Radio jamming. Jamming is used for several purposes that go beyond the malicious activities of disrupting all the target's radio communications [11]; a recent research topic exploits jamming to enforce confidentiality on wireless communications [12]: 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. Cooperative jamming is an interesting and growing topic enabling two parties to communicate without resorting to data encryption [13], [14]. Recently, cooperative jamming has been also combined with the novel technology of Multiple-Input Multiple-Output (MIMO) transducers [15]. Low power GNSS jammers could be adopted to attack the correlation process of a signal by disrupting the Position, Navigation and Timing (PNT) capabilities for a specific receiver[16]. Finally, jamming is also used in several security scenarios to prevent not-authorised communications (e.g., preventing the use of mobile-phones to inmates and defeating triggering signals during bomb neutralisation).

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, and inferring the distance to the transmitter assuming well-known propagation models [17], [18]. Other localisation techniques leverage different propagation phenomena, such as delay spread, the angle of arrival, and time of flight. Moreover, several algorithms might be adopted, e.g., trilateration, multilateration, triangulation, angulation, and lateration. Implementing the above techniques on drones is feasible for the majority of cases since such techniques depend only on information that is readily available from the radio level. One of the most reliable information, in particular in open-field scenarios, is the Received Signal Strength (RSS) and, without loss of generality, this will be the feature we are going to exploit throughout our proposed attack and scenario.

Jamming mitigation. Several techniques have been designed to mitigate malicious jammers. The majority of them resort to probabilistic algorithms and protocols to evade the jammed frequencies [19]. In [20], game theory is used 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. Finally, the solution in [21] proposes a cooperative spatial retreat algorithm that enables drones to cooperate for mitigating the action of the jammer.

C. Defeating Drones with Jamming

Commercial drones mainly use 2.4GHz and 5GHz bands. This is due to minimising interference between the controlling channel and the First Person View (FPV) streaming usually provided by the on-board camera. Moreover, both the bands allow for very small antennas (hence minimising weight and exposed components); do not interfere with the GPS bands (1574.42MHz and 1227.60MHz); and, they provide large transmission bandwidth. Other frequency bands can be used by drones to communicate with the remote controller such as 900MHz and 1.3GHz. Although being more robust to Wi-Fi noise and less influenced by obstacles, such frequencies are not so popular among the vendors due to the intrinsic interference with the GPS system and the required bigger antenna form-factor. All of the above frequencies belong to the so-called Industrial Scientific and Medical (ISM) bands, internationally reserved for supporting industrial, scientific, and medical purposes communications. Moreover, all the commercial available Software Defined Radios (SDRs) can be used to transmit over such frequencies. SDRs are radio communication equipment thatare becoming popular, giving researchers and telecommunication practitioners the freedom to implement any radio communication scheme and protocol from scratch and, 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 the most effective DoS attack that can be performed against radio links, designed aiming at preventing either the transmission or the reception of a message. The usage of a directive antenna in this scenario allows to concentrate the power budget of the jammer, on a very strict angle without interfering with other

devices in the neighbourhood. This defence strategy is usually combined with the classical assumption that the drone, having lost the communication with the remote controller and the GPS signal, switches to a firmware-coded *safety mode* that requires the drone to land, being it unable to take any further decision to progress towards the accomplishment of its mission.

III. System and Adversary Model

The key intuition behind our solution that allows a drone to push forward its mission, despite the presence of a jammer, is that jamming, like any other radio communication, can be exploited to estimate the distance to the transmitting source. While standard localisation techniques suffer from classical propagation phenomena such as multipath and low transmission power, the case of jamming is significantly different. Indeed, the jammer is strongly motivated to use as much power as possible to thwart the communication capabilities of the drone and, in particular, its access to the GPS location service.

The above scenario represents the ideal conditions for the estimation of the distance between the drone and the jammer, where the distance d can be computed as [22]:

$$d = \frac{\lambda}{(4\pi)}\sqrt{G\frac{T}{R}} \quad (1)$$

where λ is the radio frequency wavelength, T and R are the transmitted and the received power by the jammer and the drone, respectively, and finally, G sums up the transmitter-receiver antenna gains. Due to the lack of space, in this paper we only consider the *Friis* path loss model (Eq. 1) and we leave the performance evaluation in the presence of more realistic path loss models to future works. 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.

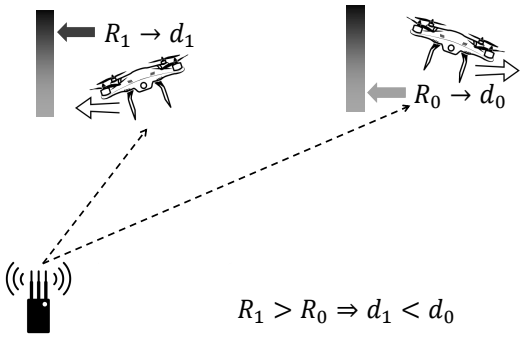

Figure 1. A drone exploiting the jamming signal for range estimation.

Moreover, we observe that the model from Eq. 1 does not take into account the noise due to multi-path fading. While we acknowledge that—in standard scenario—the distance estimation might be improved using more precise statistical description of the channel, we highlight that the scenario considered in this paper is not standard: we expect the jamming signal to be extremely powerful, and the line-of-sight component being strong respect to the other components. The above assumptions are motivated by the defence strategy: the jamming should be powerful in order to be disruptive at far distances to prevent the drone to get close to the protected area, while line-of-sight will be guaranteed by the jammer itself that is interested to maximise the radiated power (against the drone) by adopting a tracking mechanism. Figure 1 shows a toy example where the drone firstly estimates a received power R_0, and subsequently a received power $R_1 = 2 \times R_0$ (+3dB). Recalling Eq. (1), the drone can estimate to have approached the jammer by a factor $d_1/d_0 = 1/\sqrt{2}$. Assuming the firmware of the drone has been compromised by a malicious entity (or, simply, that it could be programmed), we can implement a combined navigation system that behaves as usual when the drone receives the radio commands from the remote controller, while it switches to the *JAM-ME* mode when it detects a jamming attack. While jamming detection is out of the scope of this paper, we can assume that the *JAM-ME* mode could be triggered, for instance, by the interruption of GPS data and communication links.

Jamming techniques. The jammer can deploy different strategies to disrupt the drone's communications. For instance, the jammer might deploy an *omnidirectional* or a *directive* antenna. While the former broadcasts the same jamming pattern all over a circular area, the latter concentrates the signal power on a very tight and precise target that should lie in front of the antenna. From our perspective, the more powerful is the jamming signal, the more reliable will be the *JAM-ME* navigation system.

Hardware and software assumptions. We assume our drone to be a commercial one featuring standard radio functionalities and that the drone's antenna is perfectly omnidirectional —being such an antenna the standard one available on the vast majority of the commercial models. Received Signal Strength estimation of jamming power is provided out-of-the-box by the 802.11 protocol (e.g., leveraging the drone's Wi-Fi network card). Moreover, we assume the drone's antenna to be perfectly omnidirectional, since a directive antenna would enable the drone to infer more information related to the jammer and its position. Finally, we assume that the drone standard navigation system has been reprogrammed, with a non-standard behaviour in the presence of a jammer, since commonly available drones either land or crash when they lose their radio communication capabilities.

A. Definitions and Playground Assumptions

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

- **Drone.** An Unmanned Aerial Vehicle flying from a source position to a target destination. We assume the drone not being remote controlled but pre-programmed according to a mission plan. The mission plan involves a set of waypoints to reach a pre-determined target.

- **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 jammer, being able to jam all the radio frequencies in the radio spectrum over a circle of radius $\mathcal{D}_{thr} = 479$ meters.

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

Target position awareness. The adversary (and therefore the drone) is aware of the target position, i.e., its GPS coordinates. We assume the target being 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) [23].

Unknown jammer position. We assume the jammer position to be unknown; though it should be in the close neighbourhood of the target. We observe that a jammer standing at the same position of the target guarantees maximum range protection.

No Instrumental Navigation Systems (INSs). We assume the worst-case scenario according where the drone does not resort to any additional sensors, such as magnetometers, accelerometers or the camera, to compute its current position and planning the future trajectory.

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

Table I
NOTATION SUMMARY

RSS	Received Signal Strength
$\mathcal{P}_{thr} = -30dB$	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
(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

IV. LEVERAGING JAMMING FOR DRONE NAVIGATION

In this section, we provide the architectural model of a *flight controller* being able to fly a drone close to a target in the presence of a jammer. As previously introduced in Section III, our idea mainly resorts to leverage the RSS estimated by the drone with respect to the jammer, so as to infer on the direction to take to reach the target. Figure 2 depicts the block diagram of a standard *closed loop control system* constituted by a Proportional-Integral-Derivative (PID) controller and the drone. The closed loop control system is particularly suitable for our solution since the control action from the controller $c(t)$ is dependent on feedback from the output process variable $y(t)$ [24]. We observe that, when the reference signal $r(t)$ is equal to the feedback, i.e., $y(t) = r(t)$, the error $e(t)$ becomes null, and in turn, the control variable $c(t)$ does not change—hence preserving the system status (i.e. maintaining the drone trajectory). Conversely, when the output variable $y(t)$ takes different values from the one of the reference signal $r(t)$, the error increases and, in turn, the control signal $c(t)$ compensates to make the output variable $y(t)$ returning to the original value $r(t) = y(t)$.

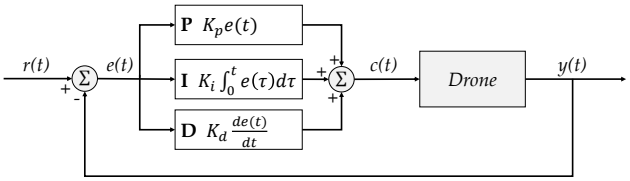

Figure 2. System architecture of the drone flight controller.

The PID controller sums up three key elements: a proportional, an integrative, and a derivative controller behaving according to Eq. 2:

$$c(t) = K_p e(t) + K_i \int_0^t e(\tau)d\tau + K_d \frac{\partial}{\partial t} e(t) \qquad (2)$$

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 is the critical gain.

V. REFERENCE SCENARIO

In this section, we consider our reference scenario as depicted in Fig. 3 constituted by a drone (triangle) willing to reach a target (cross) that, in turn, is protected by a jammer (diamond). In our reference scenario, we assume the target and the jammer are placed at the same position, i.e., the jammer wants to maximise the perimeter of the protection area around the target. Moreover, we assume that drone's navigation inside the jamming area is not affected by any drift or external forces such as the wind. We will relax this latter assumption in the next sections. We identify the following subsequent phases that the drone should execute to reach a jammer protected target.

Approaching the jamming area. During Phase 1, being outside of the jamming area, the drone performs a standard navigation trajectory by resorting to the GPS. As stated before, the drone is following a pre-determined path constituted by a set of pre-loaded way-points up to the jamming area.

Estimating the jammer position. Phase 2 starts when the drone detects the jamming signal, e.g., by monitoring the RSS [25], and inferring the presence of the jammer when the RSS is greater than a given threshold $\mathcal{P}_{thr}$, i.e., RSS $> \mathcal{P}_{thr}$. During Phase 2, the drone can still receive the GPS signal, and therefore, it can leverage such information for computing the jammer's position; as depicted in Fig. 3 (Phase 2), the drone will keep a trajectory such that the received power $P(t)$ will be constant and equal to $\mathcal{P}_{thr}$—that is, flying on the boundary

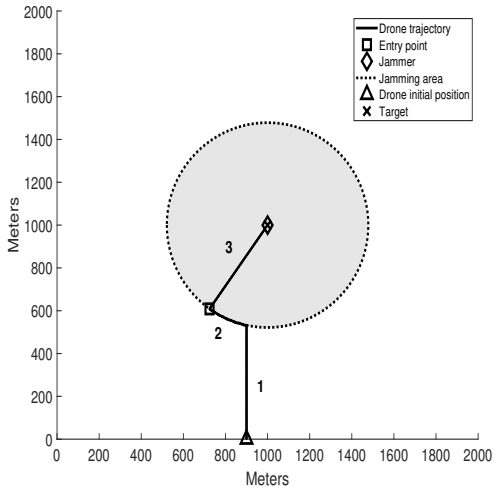

Figure 3. Reference scenario of a drone reaching a target: (i) Approaching the jamming area; (ii) Estimating the jammer position; and, finally, (iii) Approaching the Target.

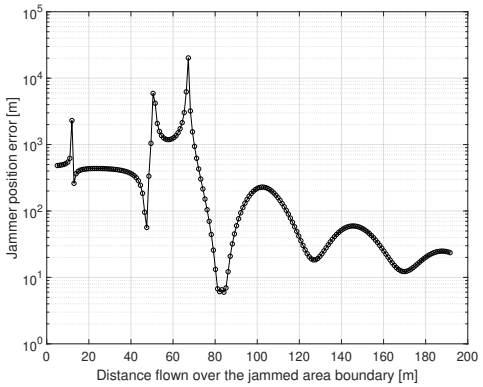

Figure 4. Jammer position error estimation as a function of the distance travelled by the drone.

of the jamming area. This can be achieved by adopting the system architecture of Fig. 3 and setting $r(t) = \mathcal{P}_{thr}$ and $K_c = 1$ (empirically estimated) for the PID controller's gain. The aforementioned behaviour is possible if we assume the drone is able to estimate the Received Signal Strength on the GPS received signal and by considering $\mathcal{P}_{thr}$ as the maximum allowed RSS from the jammer to correctly receiving the GPS signal. Without loss of generality, in this paper, we consider $\mathcal{P}_{thr} = -30dB$, but we observe that this value can vary by adopting different GPS receivers. Finally, assuming the drone has flown over the jamming area boundary, it can use the log of its past GPS positions to estimate the position of the jammer as the centre of the jamming boundary using the Pratt method [26]. Assuming no external forces (e.g., wind drift) inside the jamming area, the optimal entry point is constituted by the point on the circumference guaranteeing a minimal error on the jammer position estimation (square in Fig. 3). Figure 4 shows the error estimation of the jammer position as the drone keeps moving over the jamming area boundary. It is worth reminding that our model assumes the drone being able to perfectly receive the GPS signal both outside and at the border of the jammed area. As the intuition would suggest, we observe that the error in the position estimation of the jammer can be made arbitrarily small by making the drone fly longer over the boundary of the jamming area. Indeed, the more samples the drone can take, the smaller the cited error. We stop the estimation process when the error is less than a predefined threshold (25 meters), i.e., after the drone has flown a distance of about 190 meters.

Approaching the target. During Phase 3, the drone leaves the border of the area of jamming, and flies toward the target. It is worth noting that the drone can precisely estimate the angle of entry into the jammed area, since it knows its current position and the position of the target.

Stop criteria. In order to precisely reach the target, we consider $P(t) = P_T(t)$, where $P(t)$ is the RSS experienced by the drone, and $P_T(t)$ is the expected RSS at the target position (T_x, T_y). We observe that $P_T(t)$ can be estimated by the drone since the jammer position has been estimated (before entering the jamming area), and therefore, the distance between the jammer and the target is known to the drone.

Figure 5 depicts the Received Signal Strength by the drone as a function of the time when executing the three previously introduced phases. During Phase 1, the drone flies against the jamming area and the RSS $P(t)$ increases up to the time (530 seconds) when it reaches the jamming boundary, i.e., $P(t) = \mathcal{P}_{thr}$. Subsequently, the drone starts Phase 2, and the PID controller allows the drone to fly over the jamming boundary and to keep the RSS almost constant (from 530 to 730 seconds). Finally, the drone initiates Phase 3 by entering the jamming area and experiencing a fast-growing RSS. Figure 6 shows the RSS $P(t)$ by the drone when flying over the jamming boundary. We observe that $P(t)$ fluctuates due to the flying behaviour of the drone on the jamming boundary: during that period the drone is governed by the PID controller having as reference input $r(t) = \mathcal{P}_{thr}$. We observe that such a behaviour also affects the estimation of the jammer position (recall the oscillations in Fig. 4).

VI. Discussion and Further Directions

In this section we will discuss the proposed solution, highlighting possible countermeasures to a drone exploiting the jamming signal to navigate to a target position. Later, we will discuss the limitations this contribution is affected by, and finally we will expose some research directions.

Countermeasures. We have shown that standard jamming techniques are not effective against drones that have been reprogrammed to be robust to such a defensive solution. A solution for a *smart* jammer to re-gain effectiveness could be to modulate the jamming signal in order to prevent the

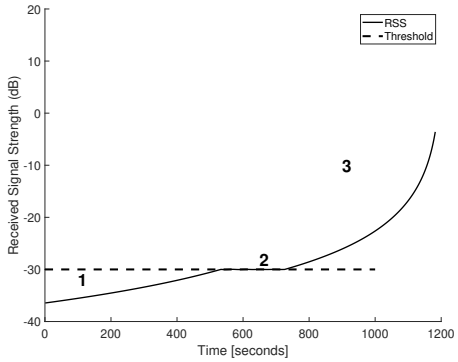

Figure 5. Received Signal Strength experienced by the drone when approaching the target (solid line), and Received Signal Strength $\mathcal{P}_{thr}$ at the jamming area boundary (dashed line).

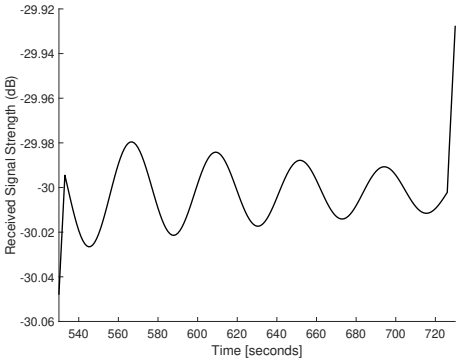

Figure 6. Received Signal Strength experienced by the drone when flying over the jammer boundary area—flight being controlled by the PID.

JAM-ME navigation system to estimate the current position of the drone and calculate the trajectory. However, we observe that a *smart* jammer randomly choosing the jamming power does not solve the problem: It would be enough for the drone to adaptively collect a certain amount of jamming samples, compute some relevant statistics, e.g., the average (computed over a sensitive number of samples), and adapt its trajectory as already introduced before. 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; and, *Adaptive jamming*—the jammer modulates the jamming power as a function of the estimated distance. The jammer can either increase or decrease the jamming power in order to mimic either a closer or a further distance to the drone, respectively. Combining the two above techniques, i.e., distance bounding and adaptive jamming, could lead to having the jammer controlling the drone's flight direction either far away or to a closer position with respect to the jammer itself. Indeed, assuming the drone computes its direction as a function of the received jamming power, the jammer can actually vary the transmitted power in order to influence the drone's trajectory. The weakness of the above solutions is that, for them to work, the jammer needs to detect the drone well in advance in order to perform the distance bounding. Although several techniques have been previously investigated to detect the presence of a drone, e.g., the sound of the propellers, movement detection, and radio fingerprinting, this is still an open challenge and a direction for the future research.

Limitations. The current solution is the result of a thorough modelling and the adoption of known results from the control theory (the PID controller), blended with the original intuition that we could leverage the very same jamming signal to help the drone navigating. The extensive simulations do support the intuition, the model, and the maths *JAM-ME* is rooted into. While preliminary results do confirm our findings, for the sake of space and completeness, we will report those findings in a future work. It is worth mentioning that we are performing active research on the wind drift issue, in order to cope with this system variable.

At the time of writing, our solution could not be adopted against a new class of low power GNSS jammers [16] or receivers that adopts Viterbi decoders [27]. Despite the above limitations, both currently under investigation, we believe that *JAM-ME* still enjoys a wide applicability range.

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 being the major ones: (i) how to mitigate external forces like wind; (ii) to provide a path loss model that takes into account the effects of Rayleigh and shadowing fading; (iii) what happens when the number of jammers increases; (iv) what if we could consider more drones, with some limited communication capabilities among them: would this help drones to reach the target in a more efficient way?; and, finally, (v) what would be the best theoretical model to describe the jammer(s)-drone(s) interaction.

VII. 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. Our solution—*JAM-ME*— 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, still reaches its assigned target. These results are supported by a thorough analytical model as well as an extensive simulation campaign. We have also discussed a few countermeasures that jammers could adopt to neutralise our solution and their shortcomings. Further, some research directions in this novel research domain have been exposed. Finally, we believe that the disruptive technique reported in this paper and its associated performance, other than showing the quality and viability of the proposed solution, also pave the way for further research in this domain.

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] S. J. (Mirror), "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, 2017, (Accessed: 2019-01-20).

[5] T. Guardian, "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, 2016, (Accessed: 2019-01-20).

[6] M. G. (Forbes), "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/, 2018, (Accessed: 2019-01-20).

[7] 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. [Online]. Available: http://doi.acm.org/10.1145/3001836

[8] 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.

[9] R. Curpen, T. Blan, I. A. Miclo, and I. Comnici, "Assessment of signal jamming efficiency against lte uavs," in *2018 International Conference on Communications (COMM)*, June 2018, pp. 367–370.

[10] 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-drone, 2019, (Accessed: 2019-01-20).

[11] C. M. (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: 2019-01-20).

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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, oct 2018. [Online]. Available: https://doi.org/10.33012/2018.15909

[17] 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.

[18] 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.

[19] 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. [Online]. Available: http://doi.acm.org/10.1145/2766498.2766515

[20] 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.

[21] 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.

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

[23] C. Koettl and B. M. T. N. Y. Times), "A closer look at the drone attack on maduro in venezuela," https://www.nytimes.com/2018/08/10/world/americas/venezuela-video-analysis.html, 2018, (Accessed: 2019-01-20).

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

[25] 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. [Online]. Available: http://doi.acm.org/10.1145/1062689.1062697

[26] V. Pratt, "Direct least-squares fitting of algebraic surfaces," *SIGGRAPH Comput. Graph.*, vol. 21, no. 4, pp. 145–152, Aug. 1987. [Online]. Available: http://doi.acm.org/10.1145/37402.37420

[27] 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. [Online]. Available: https://doi.org/10.33012/2016.14671