2021 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)

Modelling a Communication Channel under Jamming: Experimental Model and Applications

Pietro Tedeschi*, Savio Sciancalepore†, Roberto Di Pietro*
*Division of Information and Computing Technology (ICT)
College of Science and Engineering (CSE), Hamad Bin Khalifa University (HBKU), Doha, Qatar
{ptedeschi, rdipietro}@hbku.edu.qa
†Eindhoven University of Technology, Eindhoven, Netherlands
s.sciancalepore@tue.nl

***Abstract*—Traditional studies on jamming effectiveness and propagation over the wireless channel assume ideal theoretical models, such as Friis and Rician. However, the cited models have been hardly validated by on-field assessments in real jamming scenarios. To the best of our knowledge, we are the first ones to fill the highlighted gap. In particular, our objective is to provide a realistic jamming propagation model, taking into account heterogeneous operating frequencies and technologies. Our findings, supported by an extensive experimental campaign on outdoor jamming propagation, show that independently from the communication frequency the jamming power received at a given distance from the jamming source (fast fading) can be best modelled through a *t-locationScale* distribution, while the power of the received jamming decades with the increase of the distance from the jamming source (slow fading) following a *power law*. As reference applications of the derived experimental model, we describe and demonstrate its usage in two different use-cases, i.e., jamming source localization and dead-reckoning navigation, showing that our model outperforms traditional and state-of-the-art propagation models when dealing with real jamming scenarios. All the acquired data have been released as open-source, to foster experimental research activities on jamming propagation models and their applications.**

***Index Terms*—Jamming, Channel Propagation Model, Jamming Localization, Dead Reckoning Navigation.**

I. Introduction

Jamming is currently one of the most popular and effective techniques adopted to prevent communications in a given area of interest [1], [2]. By injecting noise at high power on one or more wireless channels, it is possible to disrupt regular wireless communications on the target frequencies to disable the communication infrastructure of the competing entities in the area [3]. With the technological progress in manufacturing and embedding technologies characterizing the last decade, jamming devices have gained in disruption range and effectiveness [4]. Jamming techniques are used both in offensive and defensive applications. For instance, the army increasingly uses jamming when conducting operations on lands and sea, to disable key communication technologies on the target, such as the Global Positioning System (GPS) and the regular wireless communications capabilities [5]. At the same time, jamming represents one of the key strategies to protect against privacy invasion attacks carried out by remotely-piloted drones or to allow communications only via pre-defined escape mechanisms (e.g., friendly jamming) [6].

Although jamming being a popular technology, the fine-grained effects of the injection of jamming signals on the behaviour of a generic wireless communication channel are still mostly unclear. Despite the existence of related studies concerning traditional wireless communication channels (e.g., [7], [8], [9], [10]), the validity and general applicability of such studies to jammed channels are mostly unexplored. Specifically, as emerged from the literature study summarized in Section II, the recent literature misses an accurate description of the propagation model of a jamming signal at different frequencies, its behaviour and effectiveness at increasing distance from the emission point, as well as its capability to resist against side-channels attacks, e.g., aimed at identifying its location and using it against the deploying entity. In addition, none of the studies available in the literature provided real, shared data allowing to model outdoor jamming propagation.

The knowledge and modelling of the above-described phenomena could have several applications. For instance, by analyzing the received power at different locations, a mobile entity could gain information on the jammer's deployment site (i.e., jammer localization). The receiving device could also correlate such measurements with the last known self-location, to implement secondary self-localization approaches. Moreover, in areas where the GPS is denied, similar techniques could be used to navigate in a jammed area (i.e., dead reckoning navigation) or unveil sensitive information about the location of a protected target. Furthermore, the entity deploying the jammer can use such models to plan in advance the area to be disrupted by the intentional interference and to identify weak spots beforehand.

Contributions. We aim to fill the above-highlighted knowledge gap by providing methods and techniques to model a communication channel subject to jamming attacks. In particular, our methodology is rooted on an extensive experimental campaign, carried out by acquiring real outdoor jamming signals on three different reference channels (500.00 MHz, 1,575.42 MHz, and 2,437.00 MHz). Based on such data, we analyzed the resulting status of the channel at increasing distance from the jamming source. Our results show that, independently from the channel frequency, the received jamming power at a given distance from the emitting source consistently

978-0-7381-2646-3/21/$31.00 ©2021 IEEE
DOI 10.1109/ISPA-BDCloud-SocialCom-SustainCom52081.2021.00210

exhibits the same statistical behaviour, that can be best modelled through a *t-locationScale* distribution. At the same time, independently from the frequency, the emitted jamming power decades at increasing distance from the source, following a *power-law* distribution (i.e., quicker than commonly-assumed experimental models, based on the square law). To show the effectiveness and applicability of our results, we applied our findings to two reference use-cases, i.e., jamming source localization and jammer-aided navigation. We demonstrate that a mobile entity (e.g., an Unmanned Aerial Vehicle (UAV)), able to identify ongoing jamming, can use our model to determine the deployment location of the jamming with errors as small as ≈ 27 cm. Moreover, using our model, the mobile entity can stealthily navigate the jammed area to reach the jammer or any target deployed in the area, with accuracy and performance depending on the match of our model with real operating conditions, the time spent in channel acquisition, and real-time constraints.

We released the data acquired from the wireless communication channel during our experimental campaign as open-source, allowing researchers and practitioners from both Academia and Industry to verify our findings and to leverage them to further validate their proposed models—for instance, the effectiveness of their anti-jamming methods on real outdoor jammed channel conditions [11].

Roadmap. The rest of this manuscript is organized as follows. Section II summarizes the related work, Section III illustrates the assumed scenario, Section IV describes the methodology we used to model the jammed channel, Section V depicts our findings from three reference case studies, Section VI presents two reference applications of our model, i.e., for jammer localization and dead reckoning navigation in a jammed area, respectively, Section VII compares our findings with the current literature, and finally, Section VIII tightens conclusions and draws future research directions.

II. Related Work

This section analyses the scientific contributions closest to our work, explaining similarities and differences with our approach. Overall, we divide the discussion based on the subject topic, i.e., channel modelling, jammer localization, and dead-reckoning navigation.

Channel Modelling. The authors in [7] provided a detailed tutorial on the modelling of a generic wireless communication channel. The authors focused on the most common radio propagation models available in the literature, by providing empirical results in different scenarios and a set of recommendations to model an RF communication channel properly. Despite being inspiring for this work, the cited contribution did not provide any reference to the modelling of a jammed communication channel (see Section VII for more details). A few other works specifically tackled communication channels experienced by drones. For instance, the authors in [12] provided a tutorial on UAV-aided wireless communications, describing the existing radio propagation models most suitable for UAV applications. Although the *t-locationScale* distribution is mentioned, there are no further details, and not even findings based on real data in jamming scenarios. Other studies on UAV-aided communication channels focused on suburban scenarios ([13]) and UWB communications ([14]), but they do not take jamming into account. Note that some contributions, such as [15], studied the effectiveness of radio jamming attacks based on packet reception profiles, and also released data. However, such data do not allow to model the behavior of the radio propagation channel during a jamming attack, and neither to characterize its variations on different frequencies.

Jammer Localization. A few studies have tackled jammer localization. The authors in [16] proposed a lightweight and distributed algorithm leveraging the gradient descent technique on the Packet Delivery Ratio (PDR) for jammer localization. The authors in [17] exploited the Received Signal Strength (RSS) to localize a jammer, by increasing the transmission power gradually up to the jamming power, so to estimate the jammer position. Other contributions, such as [18], proposed collaborative solutions based on the Time-of-Arrival (ToA) and Angle-of-Arrival (AoA), combined with the RSS. By estimating the distance between the receiving nodes and the jammer, they localize the jamming source. Other solutions such as [19] use various techniques such as Centroid Localisation (CL), Virtual Force Iteration Localization (VFIL), and Adaptive Jammer Localisation Algorithm (AJLA). However, neither the cited contributions use real data, nor test the effectiveness of their solutions based on real data.

Dead Reckoning Navigation. Dead-Reckoning navigation systems estimate the current position of a mobile device by using previously-determined locations and additional cyber-physical information, such as speed, wind, and other reference sources, not meant explicitly for navigation purposes. In this context, the authors in [20] introduced a dead reckoning system for outdoor localization using crowd-sourcing (e.g. via road landmarks, sensors, radio anchors) to reset location inaccuracies in GPS-denied environments. In [21], the authors proposed a system exploiting jamming signals to support the navigation of an autonomous vehicle. Their scheme first localizes the jamming source and then uses the jammer as a radio-beacon to reach the destination. Another example is the proposal by the authors in [22], introducing a data-based dead reckoning navigation system for ships allowing position estimates during a Global Navigation Satellite System (GNSS) outage. Note that none of these proposals used real data, but only simulated data based on idealized propagation models or assumptions. Finally, note that some previous "closed-source" military products, such as the AGM-88 HARM [23] used during the cold war, already included strategies to autonomously detect/localize enemy radars, e.g., to destroy them. However, being the cited products and their further releases protected by intellectual property rights, we cannot know the details about the underlying technology.

III. Scenario and Assumptions

The scenario of this manuscript is depicted in Figure 1.

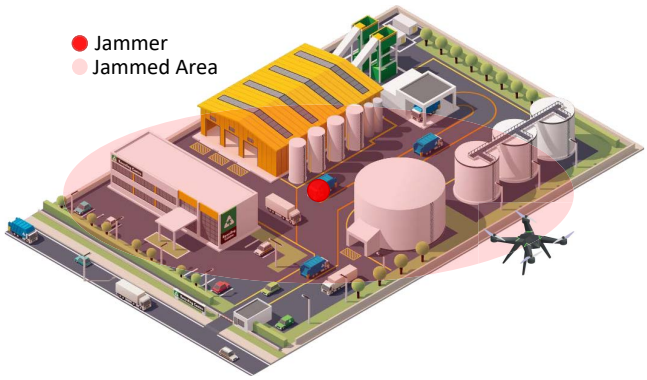

Figure 1: Scenario assumed in this work. A jammer emits noise on a bandwidth $\left[f_0 - \frac{B}{2}, f_0 + \frac{B}{2}\right]$. A mobile entity (e.g., an UAV) detects the jamming and performs several channel acquisitions rounds in different locations, so to model the channel and infer information about the jammer.

We assume that a jammer device (referred to simply as a *jammer*) is placed statically in a specific location. It emits a high-power signal on a particular bandwidth $\left[f_0 - \frac{B}{2}, f_0 + \frac{B}{2}\right]$, with f_0 central jamming frequency, to block all contemporary wireless communications on this frequency/channel. Without loss of generality, we assume that the signal emitted by the jammer is Additive White Gaussian Noise (AWGN), constantly injected on the communication channel—we refer to the jammer operating under this condition as a *constant jammer*. Note that this is not a limitation of our approach, and it does not compromise the general applicability of our results to scenarios where the jamming is intermittent. Indeed, provided that the jamming is detected, it is enough to restrict the analysis to the RSS values above a given threshold to apply our method also when the jamming is intermittent. Moreover, we assume that the jammer features an omnidirectional antenna, so that the emitted interference can propagate wirelessly with an angle of 360 degrees around its deployment location. This assumption is also realistic, as the jammer is usually interested in blocking communications across all directions. The jammer is also placed at the highest location, to spread its effect to the maximum distance.

At the same time, we assume that the receiving device is equipped with a general-purpose RF receiver, able to extract from the channel the RSS samples over a specific bandwidth B around the main communication channel f_0 (i.e., the frequency range is $\left[f_0 - \frac{B}{2}, f_0 + \frac{B}{2}\right]$). We also assume that the receiving device is mobile, being able to acquire the *status* of the selected communication channel at different locations and to correlate such measurements. For instance, the receiving device can be an UAV or a drone, equipped with a tiny Software Defined Radio (SDR) such as a MyriadRF LimeSDR [24]. We also assume a Line of Sight (LoS) link between the jammer and the receiver. This assumption is also reasonable, as a jammer is usually placed at the highest possible location, to maximize its disruptive effect on the surrounding environment. Conversely, Non-Line of Sight (NLOS) propagation conditions limit the range and effectiveness of a jammer, being a sub-optimal deployment.

Finally, we summarize the notation used in this paper in Table I.

Table I: Notation used throughout the paper.

Notation	Description
f_0	Channel central frequency.
B	Acquired bandwidth around f_0.
P_J	Jamming power.
$\mathcal{P}_r(d,t)$	RSS at time t and distance d from the jammer.
d	Distance from the transmitter.
$\Theta(d)$	Deterministic component of RSS at distance d.
$\Psi(p)$	Long-term/slow fading at position p.
$\varphi(t)$	Short-term/fast fading at the time t.
s_r	Sample rate of the receiving device.
s_t	Sample rate of the transmitter device.
D	Vector of the distances used for channel modeling.
d_n	Generic *n-th* element of the distance vector D.
K	FFT input and output window size.
τ	Acquisition time of the RSS samples.
M	Number of observed FFT windows per acquisition.
λ	RSS Threshold for jamming detection.
rss_n	Generic *n-th* element of real experimental data.
$\hat{rss}_n$	Generic *n-th* element of the reconstructed data.
e_n	Residuals (estimates of the errors).
$\hat{L}$	Maximum value of the likelihood function.
δ	Number of parameters for the AIC tool.
μ	Mean Value of the acquired samples.
σ	Variance of the acquired samples.
Λ_f	Set of distributions used for channel modeling.
a, b, c	Coefficients of the power-relationship model.
$\beta\left(\Lambda_f\right)$	Resulting channel model.
$\mathcal{P}_\omega$	RSS expected at the boundary of the jammed area.
$\mathcal{P}_E$	RSS expected on the jammer location.

IV. Modelling Communication Channels under Jamming

This section describes the method we used to model a generic communication channel under jamming attacks. Without loss of generality, let us assume that a jammer is placed in a given area of interest. It emits noise uniformly-at-random on the frequency f_0, with the maximum available power P_J.

In line with the analysis reported by the authors in [7] for a generic communication channel, we can express the RSS $\mathcal{P}_r(d,t)$ at distance d from the jamming location, at the time t, as shown in Eq. 1.

$$\mathcal{P}_r(d,t) = \Theta(d) + \Psi(d) + \varphi(t)[dBm], \tag{1}$$

where $\Theta(d)$ is the deterministic component of the received power at distance d, usually modeled through a path-loss radio propagation model, $\Psi(d)$ denotes the space-dependent component, namely *long-term/slow fading* or *shadowing*, generated by the scattering and reflections of the radio signal due to obstacles, and $\varphi(t)$ describes the time-dependent component of the received signal at the time t, namely *short-term/fast fading*.

The jammed channel characterization aims to set up a general model that can be used to characterize the behaviour

of the RSS of the jamming across both time and space. Our technique consists of the following phases.

- *Data Acquisition.* In this phase, the receiver acquires RSS samples at several locations at a distance d_n from the jammer, for a time τ.
- *Fast Fading Model Generation.* The receiver analyzes all the samples received at a given location (distance d_n from the jammer), to obtain information about the time-related evolution of the distribution of the RSS samples, i.e., $\varphi(t)$.
- *Slow Fading Model Generation.* The receiver analyzes the change in the distribution of the RSS at different distances, to obtain information on the space-related evolution of the distribution of the RSS samples, i.e., $\Psi(d)$.

Note that our model does not explicitly derive the deterministic component $\Theta(d)$. However, its modelling is implicit in the definition of the components $\varphi(t)$ and $\Psi(d)$.

Data Acquisition. This phase consists of the acquisition of a set of RSS samples, in the bandwidth $\left[f_0 - \frac{B}{2}, f_0 + \frac{B}{2}\right]$ around the reference channel frequency f_0, for a time τ, and for a set of distances $D = \{d_1, d_2, \ldots, d_n\}$ from the jamming source. Note that, starting from the raw I/Q samples acquired with a sample rate s_r, the receiving device performs a Fast Fourier Transform (FFT) operation with a window size K, to obtain estimates of the RSS on the reference bandwidth. As a result, for each channel with central frequency f_0 and distance d_n from the jamming source, this phase outputs an $M \times K$ matrix, where M are the total number of observed windows and K is the FFT size. Such samples are then processed to obtain information about the fast fading and slow fading components, as described below.

Fast Fading Model Generation. In this phase, for a given channel with central frequency f_0, we consider only the RSS samples acquired at a given distance d_n from the jamming source. From the previous phase, we recall that we have in input a matrix with size $M \times K$, where M are the total number of observed windows, and K is the FFT size. To focus the analysis on the signal of interest only, we set up a threshold λ and, for each row of the matrix, we selected only the RSS samples exceeding such a threshold. Then, we computed the *mean* of the remaining RSS values, obtaining a single RSS value summarizing all the measurements of the signal of interest around f_0.

Overall, the output of the previous operation is a set of M RSS values, summarizing the time-domain evolution of the RSS on the frequency f_0 at a distance d_n from the emitting source. Due to the fast fading effects, these values are statistically distributed and not static. Therefore, we obtain the empirical statistical distribution of these values through a histogram modelling each value's appearance ratio in the set of M RSS values. The statistical distribution of these weights is then compared to a set of well-known distributions, to find the statistical distribution (and related parameters) that best fits the experimental data. To find the parameters of each distribution that are closer to our data, we used the Maximum Likelihood (ML) method [25]. In particular, we find the parameters of the statistical model that minimize the residuals e_n, as in Eq. 2.

$$e_n = \left(rss_n - \hat{rss}_n\right), \tag{2}$$

where rss_n denotes the real (discrete) experimental data, $\hat{rss}_n$ refers to the reconstructed values using the specific statistical distribution, and e_n identifies the residuals. Note that the tools available to fit statistical distributions to experimental data require strictly positive values. Therefore, it might be necessary to convert the RSS into strictly-positive values, i.e., to switch RSS from $[dBm]$ to $[mW]$.

Finally, to cross-compare the best-fit statistical distributions, we used the Akaike Information Criterion (AIC) tool, as in Eq. 3.

$$AIC = 2 \cdot \delta - 2 \ln\left(\hat{L}\right), \tag{3}$$

where $\hat{L}$ is the maximum value of the likelihood function for the model, and δ represents the number of parameters for the corresponding distributions. The lower the AIC, the better the specific distribution fits the experimental data. Therefore, the statistical distribution (and related parameters) that exhibits the lower AIC is selected as the reference statistical distribution of the fast fading component of the jamming signal.

The final output of this phase is a set of statistical distributions, valid for each frequency f_0 and distance d_n from the jamming source, together with the related parameters (e.g., the mean value $\mu_{f,n}$ and the variance $\sigma_{f,n}$).

Slow Fading Model Generation. In this phase, we cross-correlate the statistical distributions (and related parameters) for different locations at a distance d_n from the emitting source, for the same reference channel frequency f_0. Recall that the output of the previous phase is a set of statistical distributions, characterized by parameters such as the mean $\mu_{f,n}$ of the samples acquired on the channel with frequency f, at a distance d_n from the jamming source. We consider all the mean values of such distributions, stacked in a vector $\Lambda_f = \left[\mu_{f,1}, \mu_{f,2}, \ldots, \mu_{f,n}, \ldots, \mu_{f,N}\right]$, and we apply a regression technique based on the Nonlinear Least Squares (NLS) criterion. The result is the non-linear model that best fits the available values by minimizing the related residuals, as described in Eq. 4.

$$\beta\left(\Lambda_f\right) = \min_{a,b,c}\left(a \cdot \Lambda_f^b + c - \Lambda_f\right), \tag{4}$$

where the values a, b, c are the coefficients of the power-relationship, while $\beta\left(\Lambda_f\right)$ is the resulting model. Note that we considered the best-fit model as the one characterized by the combination of the lowest Root Mean Square Error (RMSE), lowest Sum of Squared Errors (SSE), and higher R-squared metric. Algorithm 1 summarizes the above-described procedure through pseudo-code.

We highlight that building the model of a jammer in a real-time adversarial jamming situation is not possible, as it would require knowledge of the position of the jammer. The technique we just described is intended to provide a general model of a jammed communication channel, that could be

Input: RSS samples;
Result: Propagation model $\beta\left(\Lambda_f\right)$;

Select f_0;
for $n \leftarrow d_1$ **to** d_N **do**
    // Data Acquisition
    while *($t < \tau$)* **do**
        samples(n) = *acquire_samples()*;
        $y(n) \leftarrow$ *FFT$_K$(samples(i))*;
    end
    // Fast Fading Model Generation
    $m(f_0, n) \leftarrow$ *extract_mean*($y(n)$);
    setup_fitting_options();
    $distrib(f_0, n) \leftarrow$ *estimate_distribution*($m(f_0, n)$);
end
// Slow Fading Model Generation
for $n \leftarrow d_1$ **to** d_N **do**
    $\mu_{distrib}(f_0, n) \leftarrow$ *extract_mean_from_distribution*($distrib(f_0, n)$);
end
setup_fitting_options();
$[xData, yData] \leftarrow$ *prepare_Curve_Data(d,* $\mu_{distrib}(f_0, n)$*)*;
$\beta\left(\Lambda_f\right) \leftarrow$ *best_fit*($xData, yData$);

Algorithm 1: Pseudo-code of the jammed channel modeling.

stored in the memory of any device. As demonstrated in Section VI, when jamming is detected, the general model can be used at run-time by a mobile receiving device for several applications (see Section VI).

V. Experimental Case Studies

In this section, we illustrate our experimental setup and we provide reference case studies for three different frequencies. Specifically, Section V-A outlines the setup of the acquisition campaign, while Section V-B, Section V-C, and Section V-D describe our findings when $f_0 = 500.00$ MHz, $f_0 = 1,542.00$ MHz, and $f_0 = 2,437.000$ MHz, respectively.

A. Experimental Setup

Figure 2 shows the system setup adopted for our measurements.

The device adopted as the jammer is an USRP Ettus Research X310 SDR [26], featuring a UBX160 daughterboard [27]. This device can emit wireless signals at the peak power of 20 dBm, in the range $[0 - 6]$ GHz, with a maximum instantaneous bandwidth of 120 MHz. On the receiving side, we used a MyriadRF LimeSDR, a tiny SDR able to transmit and receive RF signals in the range $[0 - 3]$ GHz, with a maximum instantaneous bandwidth of 20 MHz. Its limited weight, i.e., $\approx$ 49 grams only, also allows for easy and practical integration with commercial drones. In the experiments, we used antennas that best fit the selected frequency range. For instance, for the case study #1 on $f_0 = 500$ MHz, we used both

Figure 2: Experimental setup used for the measurements.

at the transmission and the reception side an antenna *ANT500*, provided by Great Scott Gadgets, optimized for RF operations in the frequency range $[0 - 1]$ GHz. We set the antennas gains to the maximum available value for the transmitter and the receiver to have the maximum effectiveness in the radiation (TX side) and conversion (RX side) of the signal's power. Note that the deployment strategy allowed us to assume that there is LoS between the transmitter and the receiver in all the experiments. Moreover, the nodes were deployed at the same height—hence restricting our scenario to the 2-D case deployment.

To drive the behaviour of the SDRs, we used the GNURadio Development Toolkit [28], running over two general-purpose laptops (Dell XPS15 9560, equipped with 32GB of RAM and 8 Intel Core i7700HQ processors running at 2.80 GHz) running the OS Linux Ubuntu 20.04 LTS. Then, we transferred all the data acquired on the receiving device to the application software Matlab (version 2020b) for the following processing.

As reference case studies, we selected three different values of f_0, i.e., $f_0 = 500.00$ MHz, $f_0 = 1,575.42$ MHz, and $f_0 = 2,437.00$ MHz. In addition, we set an FFT size of $K = 1,024$ samples and sample rates of $s_t = 2$ MHz on the transmitter and $s_r = 5$ MHz on the receiver. Finally, we acquired the RSS samples for a time $\tau = 10$ minutes, at distances $D = \{0.5, 1, 1.5, 2, 3.5, 5, 10, 15, 20\}$ meters from the jamming source. We selected the maximum measurement distance of 20 meters to not break local regulations on emission levels. However, note that such a limitation does not impact on the global validity and applicability of our research, as we are interested in the propagation model of jamming signals, and not on its range effectiveness/limitations.

The configuration used for the experiments is summarized in Table II.

B. Case Study #1: 500.00 MHz (TETRA)

In this case study, we focus on the frequency $f_0 = 500$ MHz, used by several avionic and military technologies,

Table II: Setup of the experiments.

Notation	Value
f_0	$[500.00, 1,575.42, 2,437.00]$ MHz
τ	10 minutes
D	$\{0.5, 1, 1.5, 2, 3.5, 5, 10, 15, 20\}$ meters
s_t	2 MHz
s_r	5 MHz
B	5 MHz
K	$1,024$ samples

such as TETRA [29]. In our experimentation, both the transmitter and the receiver used *ANT500* antennas provided by Great Scott Gadgets [30]. These antennas are designed for operations in the frequency range $[75 - 1,000]$ MHz, with an omnidirectional radiation pattern.

We recorded RSS samples at the receiver at 9 locations, at distances $\{0.5, 1, 1.5, 2, 3.5, 5, 10, 15, 20\}$ meters from the jamming source, and we set up the receiver to take all the RSS samples in the range $[497.5 - 502.5]$ MHz. Then, we applied the fast fading model generation procedure described in Section IV to find the statistical distribution that best fits the experimental data. To this aim, we used the Matlab tool *allfitdist* [31], a ready-to-use Matlab library that automatizes the fitting process by testing a wide range of statistical distributions and selecting the best fitting distribution using the lowest AIC as a metric, as described in Section IV. We found out that, independently from the distance from the jamming source, the statistical distribution characterized by the minimum AIC on the experimental data is the *t-locationScale* distribution (a parameterized t-Student distribution), characterized by the Probability Distribution Function (PDF) shown in Eq. 5:

$$p(x|\mu,\sigma,\nu) = \frac{\Gamma\left(\frac{\nu+1}{2}\right)}{\sigma\sqrt{\nu\pi}\,\Gamma\left(\frac{\nu}{2}\right)}\left[\frac{\nu + \left(\frac{x-\mu}{\sigma}\right)^2}{\nu}\right]^{-\left(\frac{\nu+1}{2}\right)}, \quad (5)$$

where $\Gamma(\circ)$ is the gamma function, $-\infty < \mu < +\infty$ is the location parameter, $\sigma > 0$ is the scale parameter, and $\nu > 0$ is the shape parameter. Note that the values of μ, σ, and ν at specific locations are different, as they depend on the distance from the jamming source and the effect of the channel. Figure 3 shows the *t-locationScale* distributions that best fit the gathered experimental data on the frequency $f_0 = 500$ MHz, across the tested locations.

Following the *Slow Fading Model Generation* process described in Section IV, we applied the non-linear regression techniques based on the NLS criterion, and we found the power-law model that best fits the mean values of all the distributions, described in Eq. 6 and shown in Figure 4.

$$\left(a \cdot \Lambda_f^b + c - \Lambda_f\right) = \left(-7.205 \cdot \Lambda_f^{0.5154} - 56.04\right). \quad (6)$$

C. Case study #2: $1,575.42$ MHz (GPS)

In this case study, both the transmitter and the receiver used the *ANT500* antennas, similarly to the case study #1. Despite these antennas are designed for optimal operations in the frequency range $[75 - 1,000]$ MHz, they demonstrated

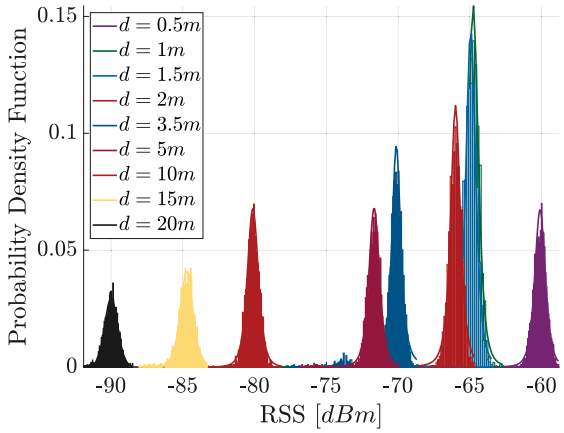

Figure 3: Fast Fading model generation at $f_0 = 500$ MHz. Each PDF represents the distribution that best fits the experimental data. For each location, the best-fit distribution is a *t-locationScale*.

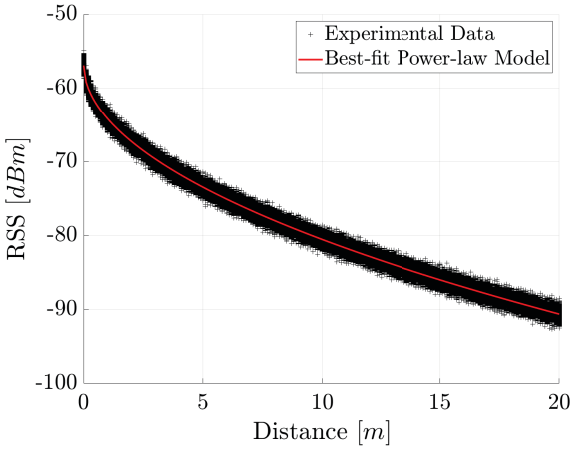

Figure 4: Slow Fading Model Generation at $f_0 = 500$ MHz. The red line corresponds to the power-law model that best fits the experimental data (black crosses).

acceptable behavior also on this frequency, as demonstrated by recent successful GPS spoofing attacks (e.g., the one in [32]) and large-scale reverse engineering attacks (e.g., the one in [33]) realized through these antennas on the GPS ($f_0 = 1,575.42$ MHz) and IRIDIUM ($1,626.27$ MHz) communication channels, respectively.

We set up the receiver to take all the RSS samples in the range $[1,572.92 - 1,577.92]$ MHz and, similarly to the case study #1, we recorded RSS samples at the receiver at 9 locations, at distances $\{0.5, 1, 1.5, 2, 3.5, 5, 10, 15, 20\}$ meters from the jamming source.

Then, by using the Matlab tool *allfitdist* previously de-

scribed, we applied the fast fading model generation procedure described in Section IV to find the statistical distribution that best fits the experimental data. Our result is very similar to the Case Study #1. Indeed, as shown in Figure 5, we found out that, independently from the distance from the jamming source, the statistical distribution characterized by the minimum AIC on the experimental data is the *t-locationScale* statistical distribution (recall Eq. 5 in Section V-B).

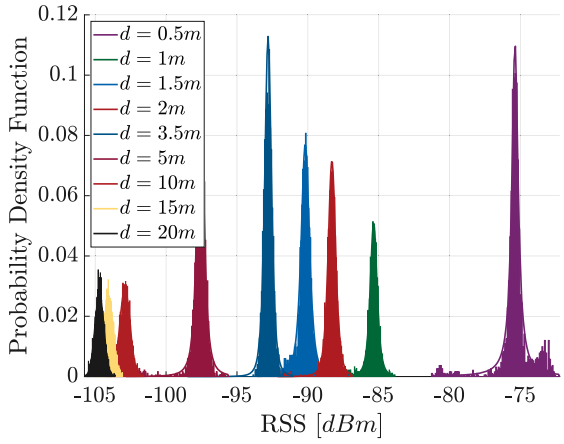

Figure 5: Fast Fading Model Generation at $f_0 = 1,575.42$ MHz. Each shape represents the distribution that best fits the experimental data. For each location, the best-fit distribution is a *t-locationScale*.

Then, in accordance with the *Slow Fading Model Generation* process described in Section IV, we applied the non-linear regression techniques based on the NLS criterion, to find the power-law model that best fits the mean values of all the distributions, described in Eq. 7 and shown in Figure 6.

$$\left(a \cdot \Lambda_f^b + c - \Lambda_f\right) = \left(41.92 \cdot \Lambda_f^{-0.2461} - 124.6\right). \quad (7)$$

D. Case study #3: 2,437.00 MHz (Wi-Fi)

Differently from the previously described scenarios, in this case study both the transmitter and the receiver used the *VERT2450* Dual-band omnidirectional vertical antennas, provided by Ettus Research [34]. These antennas are optimized to operate in the frequency ranges $[2,400.00 - 2,480.00]$ MHz and $[4,900.00 - 5,800.00]$ MHz, with an omnidirectional radiation pattern, at 3 dBi gain.

Since this case study aims to evaluate the jamming propagation model on Wi-Fi typical frequencies, we selected the most *uncongested* channel, i.e., the channel 6, with centre frequency $f_0 = 2,437.00$ MHz. In line with the previous setup, we configured the receiver to take all the RSS samples in the range $[2,434.5 - 2,439.5]$ MHz and we recorded RSS samples at the receiver at 9 locations,

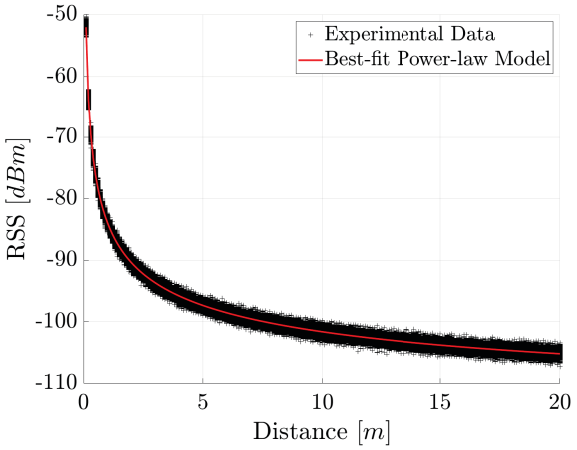

Figure 6: Slow Fading Model Generation at $f_0 = 1,575.42$ MHz. The red line corresponds to the power-law model that best fits the experimental data (black crosses).

at distances $\{0.5, 1, 1.5, 2, 3.5, 5, 10, 15, 20\}$ meters from the jamming source.

Then, by using the Matlab tool *allfitdist* previously described, we applied the fast fading model generation procedure described in Section IV to find the statistical distribution that best fits the experimental data.

Our result is very similar to the case studies previously discussed. Indeed, as shown in Figure 7, we found out that, independently from the distance from the jamming source, the statistical distribution characterized by the minimum AIC on the experimental data is the *t-locationScale* distribution (recall Eq. 5 in Section V-B).

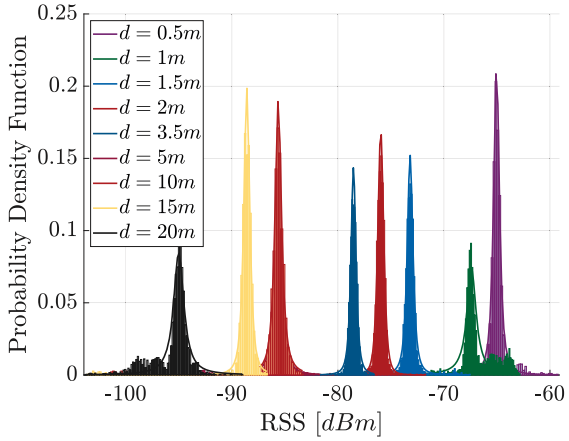

Figure 7: Fast Fading Model Generation at $f_0 = 2,437.00$ MHz. Each shape represents the distribution that best fits the experimental data. For each location, the best-fit distribution is a *t-locationScale*.

Then, in accordance with the *Slow Fading Model Generation* process described in Section IV, we applied the non-linear regression technique based on the NLS criterion, to find the power-law model that best fits the mean values of all the distributions, described in Eq. 8 and shown in Figure 8.

$$\left(a \cdot \Lambda_f^b + c - \Lambda_f\right) = \cdot \left(331.9 \cdot \Lambda_f^{-0.02382} - 403.1\right). \quad (8)$$

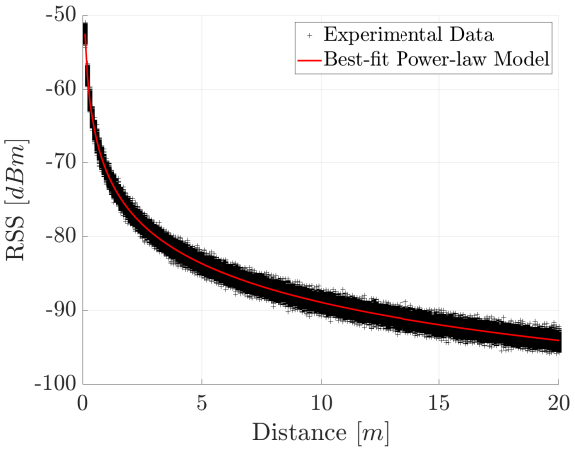

Figure 8: Slow Fading Model Generation at $f_0 = 2,437.00$ MHz. The red line corresponds to the power-law model that best fits the experimental data (black crosses).

Summary. The main finding of our experimental campaign is that, independently from the distance from the jamming source and the frequency, the RSS samples of the jamming signal received at a specific location over a given time frame follow the same statistical distribution, i.e., a *t-locationScale*. When comparing the best-fit distributions on the same frequency over different locations at increasing distance from the jamming source, the mean value of the distributions decreases due to the strong dependency of the received jamming power from the space travelled. The mathematical law that best fits this behaviour is a power law, characterized by coefficients (a, b and c) depending on the specific operating frequency. Note that a power-law with such coefficients decays (with distance) quicker than commonly-assumed models (e.g., the *square law*), further demonstrating that signal propagation in real outdoor scenarios is severely affected by distortion phenomena that decrease its area coverage.

VI. Use-Cases

In this section, we demonstrate the applicability and utility of the results presented in Section V, through reference use-cases. Specifically, Section VI-A applies the results previously introduced for jammer localization, while Section VI-B shows how mobile entities, such as drones, can leverage the model previously introduced to navigate in an area under jamming through a *dead reckoning navigation system*. Note that these use-cases are only two of the many possible applications of the before-introduced model, and they do not limit the applicability of our results to further applications (e.g., jamming detection and self-localization, to name a few).

A. Use-case #1: Jammer Localization

We consider the scenario depicted in Figure 9, constituted by a drone (reported as a triangle) moving with a speed of 10 m/s (36 Km/h), willing to identify the location of a jammer (reported as a diamond). We assume that the jammer aims to

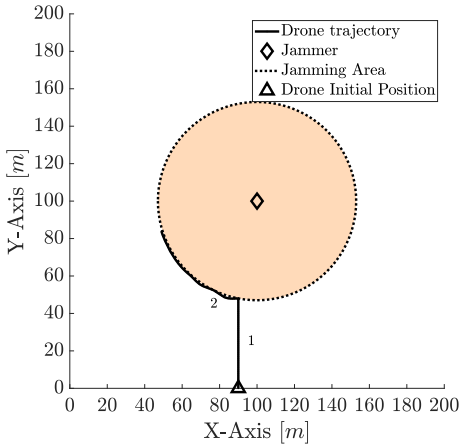

Figure 9: Jammer localization use-case. A drone (triangle) aims to localize a jammer (diamond) active in given area of interest (orange circle), by moving on the bounds of the jammed area (black dots).

deny the reception of GPS signals in a given area of interest, e.g., to protect a sensitive target from being approached by GPS-aided devices. Therefore, we reasonably assume that the jammer emits jamming signals constantly on the frequency $f_0 = 1,575.42$ mHz at its maximum power level (20 dBm), to maximize area coverage.

When the drone is located outside the jammed area, it leverages a GNSS technology (e.g., the GPS) to follow the path towards its intended destination. At a given time, the drone detects to be subject to a jamming attack. The drone can detect jamming through different techniques. For instance, the drone can identify the lack of GPS reception. Alternatively, it can evaluate the instantaneous RSS and detect that the mean value of the power received on the GPS communication channel exceeds a given threshold $\mathcal{P}_\omega$ ($\mathcal{P}_\omega = -97.8$ dBm for the GPS, based on [35]). At this time, the drone returns to the last *stable* position by using an inertial navigation system and activates a jammer localization procedure based on the channel model presented in Section IV.

In line with the proposal in [21], we model the jammer localization system through a closed loop control system, where the drone adopts a Proportional-Integral-Derivative (PID) controller to compensate the error on the power estimation, as

depicted in Figure 10. We denote $r(t)$ as the real-time input of the PID (coincidental with $rss(t)$), $c(t)$ as the control signal generated by the PID controller, $y(t)$ as the output variable, and $e(t) = y(t) - r(t)$ as the steady-state error. To make $r(t)$ dimensionally consistent with the other parameters in the PID, we assume a conversion factor $\kappa = 1 \cdot \frac{m}{Watt*s}$. The behaviour

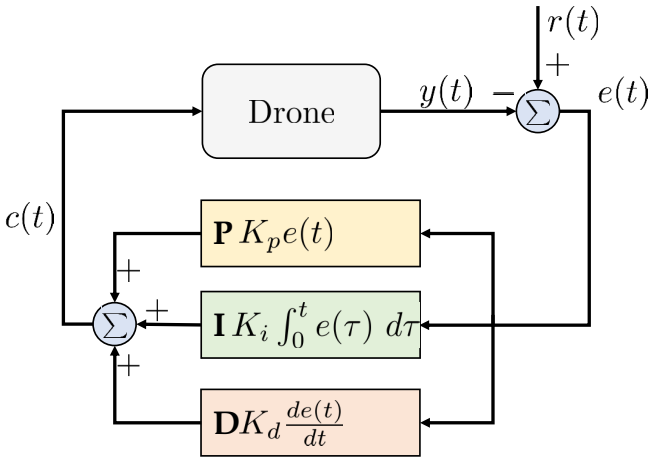

Figure 10: PID Controller used for jammer localization. The drone applies the PID to find the locations where it experiences a constant received jamming power $\mathcal{P}_\omega$.

of the PID is modelled through Eq. 9.

$$c(t) = K_p \cdot e(t) + K_i \cdot \int_0^t e(\tau)d\tau + K_d \frac{\partial}{\partial t} e(t) \qquad (9)$$

being K_p, K_i, and K_d the proportional, integral, and derivative gains of the PID, respectively, tuned with the the Ziegler-Nichols method [36], and $K_c = 1$ being the critical gain factor, empirically estimated.

Note that the drone aims to identify the jammer's location as the centre of any *ideal* circumference, where a receiver experiences a constant profile of the received jamming power. Given that the drone should be able to move towards a specific point in space where it expects constant received power, we selected such circumference as the one where $r(t) = \mathcal{P}_\omega$, so to be able to still receive GPS signal.

To estimate the power received by the jammer at a given location, the drone uses the experimental model described in Section IV, and in particular, the one with the parameters defined for the GPS technology, described in V-C. Using such a model and the PID logic described in Figure 10, the drone obtains the control signal $c(t)$, that instructs it on the new position where to move to experience $r(t) = \mathcal{P}_\omega$. Therefore, using the GPS (still receivable based on the condition $r(t) = \mathcal{P}_\omega$), the drone moves to such a location, acquires the signal $r(t)$, and computes the error $e(t) = y(t) - r(t)$. Such error is used as the input to generate a new estimation, and the process repeats as explained above.

At each step, the drone acquires new GPS coordinates of points experiencing the same signal power $\mathcal{P}_\omega$, and it constructs an increasing arc of the circumference describing the bounds of the jammed area. Then, the drone uses the Pratt's algorithm to estimate the jammer position (x_J, y_J) starting from a set of coordinates of one of its arc [37]. Specifically, the Pratt's algorithm fits a circle to a set of data points on a plane, and it returns the circle centre and the radius. Let us define as $posJ_i = (x_{J_i}, y_{J_i})$ the estimated jammer position through the Pratt's algorithm at the step i of the algorithm. The whole process stops when the standard deviation of the last ten estimated jammer positions is less than a pre-selected convergence threshold $\beta = 0.01$.

To verify the effectiveness of the described strategy, we set up $1,000$ simulations with different channel conditions, and we evaluated the jammer position estimation error while varying the number of acquired FFT windows (M). We summarize the results of the experiments in Figure 11.

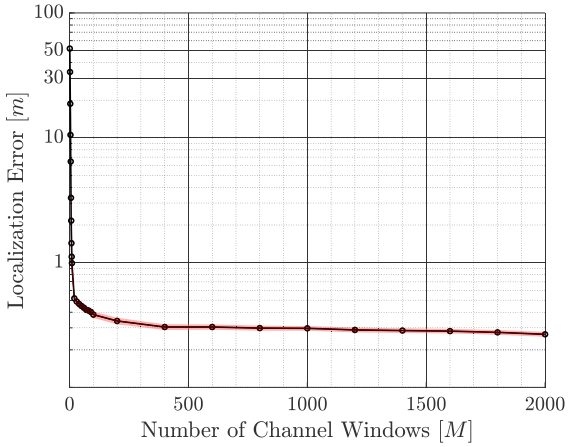

Figure 11: Jammer position estimation error as a function of the number of channel windows (radio samples) M acquired by the drone at each channel acquisition.

The results show that the jammer localization error significantly decreases by increasing the consecutive number of FFT acquired from the (jammed) communication channel (M). Indeed, the higher the number of channel windows considered at each step, the more precise the wireless channel estimate, and the higher the precision in the jammer location estimation. Considering only $2,000$ FFT channel windows (i.e., acquiring the channel for ≈ 0.41 seconds at each step), the above-described algorithm localizes the jammer with a precision of ≈ 0.29 meters, by requiring on average only 72 steps by the drone. Overall, these results enhance the findings in the reference paper [21], where the authors localized the jamming source using simulations carried out through a simplified propagation model based on the ideal Friis free-space loss model (Section VII will provide more details on this aspect).

B. Use-case #2: Navigating a Jammed Area

The model described in Section IV can also be used to allow a mobile entity (e.g., a drone) to navigate autonomously in the

jammed area, as proposed in [38].

In line with Section VI-A, we assumed a constant jammer, emitting the highest possible power on the GPS frequency ($f_0 = 1,575.42$ MHz). As depicted in Figure 12, the approach described by the authors in [38] first detects the jamming (1), then localizes the jammer through a method similar to the one depicted in Section VI-A (2), and then uses the jamming signal to navigate towards its location, by following a direction that maximizes the received jamming power (3). We hereby focus only on step (3), which includes applying the experimental jamming propagation model.

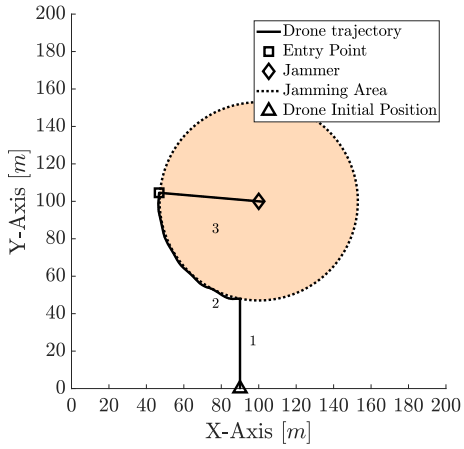

Figure 12: Dead reckoning Navigation. The drone (triangle) enters the jammed area (orange circle) and navigates from the entry point (square) to the jammer location (diamond) using the jamming signal as a reference.

The navigation procedure requires that, after localizing the jammer, the drone continues acquiring RSS samples from the channel, to obtain *estimates of its relative distance to the jammer*. Note that, although the transmitted power and the jammer's antenna gain are likely unknown to the drone, the *important* information for navigation purposes is the variation of the received power when the drone moves closer-to/further from the jammer. Specifically, before entering the jammed area, the drone uses our model to estimate the power that should be received at a distance $d = 0$ m from the jammer, namely $\mathcal{P}_E$. By knowing the drone's location and the jammer estimated position, the drone can compute its relative distance from the jammer. Moreover, it can use the power received at its location to calculate the received power level that it should experience on the jammer location, by inverting the model in Eq. 7.

Then, the drone navigates across the jammed area by using a PID controller following the logic in Figure 10 (Section VI-A). However, differently from the previous use-case, where the PID instructed the drone to move on the interference with constant RSS, now the PID compensates the drone's position error at each step to move towards the direction that maximizes the RSS. The process stops when the drone experiences an average RSS equal (or higher) than $\mathcal{P}_E$, i.e., the RSS expected on the jammer location.

In our experiments, in line with the experimental campaign, we set up a jamming power of 20 dbm, guaranteeing a jammed area of $d_t \approx 53.43m$. On the receiver side, we set the drone speed to 10 m/s, and we configured the PID with the same parameters reported in Section VI-A. We assumed that the receiver analyzes the communication channel by applying the FFT over $K = 1,024$ samples, and a sample rate of $s_r = 5$ MHz (the time to acquire N samples can be obtained as $t = N \cdot \frac{1}{s_r} \cdot K$). Then, we ran $1,000$ simulations where we applied the described navigation procedure to navigate towards the jamming source, using the devised experimental model. The results of the assessment are summarized in Table III. To evaluate the performance of the navigation scheme, we assumed that the *mission* of the drone is to reach the jammer location, and we reported the average distance (with the 95 % confidence interval) between the jammer location and the location where the navigation stops ($rss(t) > \mathcal{P}_E$).

Table III: Jammed Area Navigation Performance. We assume that the *mission* of the drone is to reach the jammer location, and we report the distance between the jammer location and the location where the navigation stops.

Acquired Channel Windows [M]	**Time to Acquire Windows [s]**	**Avg. Distance from Target [m]**
200	0.04	38.20 ± 1.09
400	0.08	19.97 ± 1.37
600	0.12	12.70 ± 1.21
800	0.16	6.13 ± 0.89
1000	0.21	3.22 ± 0.59
1200	0.25	2.44 ± 0.47
1400	0.29	1.99 ± 0.37
1600	0.33	1.48 ± 0.22
1800	0.37	1.37 ± 0.14
2000	0.41	1.28 ± 0.06

Note that the higher the number of FFT windows acquired from the (jammed) communication channel, the more accurate the channel model, and the more effective the navigation. Acquiring only 200 FFT windows per location, the navigation algorithm stops prematurely at a distance that, on average, is ≈ 38 meters from the jammer location. The accuracy of the system improves by acquiring more channel windows, and thus, by sampling the channel for more time (see the second column in Table III). Sampling $2,000$ FFT windows (in ≈ 0.41 s), we stop at a location that is on average ≈ 1.28 m from the jammer location, achieving the planned task.

VII. Comparison

We now discuss the relationship of our findings with the current literature on communication channel modelling. Currently available studies on the modelling of a generic communication channel, such as the one in [7], identified that a generic outdoor communication channel could be modelled through an *extremeValue* statistical distribution. At the same time, previous studies on jammer localization such as the

ones in [21] and [38] assumed the ideal Friis equation to approximate channel conditions.

To evaluate the mismatch of such models when applied to real data, we selected a reference scenario, and we compared the performance of the three models. Specifically, as in Section VI, we selected the GPS channel ($f_0 = 1,575.42$ MHz). We assumed mostly the same scenario and parameters considered for the analyses in Section VI. The only main difference is that the PID controller is tested in three different scenarios, where in each scenario it uses one of the three models (*t-locationScale*, *extremeValue*, Friis equation) to keep the receiver on the circumference with constant receiving power $\mathcal{P}_\omega$ (use-case #1), and to navigate towards the location with the higher expected RSS $\mathcal{P}_E$ (use-case #2).

Note that, to apply the model presented in [7] to our data, we considered the same modelling technique discussed in Section IV, and we found the parameters of the *extremeValue* distribution that best model our real data. Table IV reports the average error achieved by each of the three models in estimating the radius of the jammed area and in navigating towards the location of the jammer, by assuming the reference number of $M = 2,000$ acquired channel windows per step.

Table IV: Jamming radius estimation error and on-target navigation error when assuming that the jammed channel is modelled with Friis, *t-locationScale*, and *extremeValue* models ($M = 2,000$), respectively.

Channel Model	Friis	*extremeValue*	*t-locationScale*
Avg. Jamming Radius Error $[m]$	$117,496.57$	0.86	0.01
Avg. Distance From Jammer $[m]$	$1,958 \pm 15.85$	1.88 ± 0.48	1.29 ± 0.06

First, we note that the Friis model assumed by the authors in [21] leads to significant errors when applied to real data, making such model unsuitable for real jammer localization applications. Moreover, we note that the error derived by assuming an *extremeValue*-modelled channel (rather than a *t-locationScale*-distributed one) provides slightly worse performance—0.86 m of error over a jamming radius of ≈ 53.43 m and, ≈ 1.88 m of error for the navigation use-case. On the one hand, these findings highlight that the *t-locationScale* is the correct distribution when dealing with jammed channels. On the other hand, the mismatch between the two models is limited. This finding implicates that modelling a jammed channel as a regular communication channel (following an *extremeValue* distribution, as recommended by [7]) introduces a slight error, translating, in turn, into slightly degraded performance (more time to localize the jammer, larger navigation time, increased energy consumption).

VIII. Conclusion and Future Work

In this paper, we presented an experimental model for a communication channel subject to jamming. Our methodology is rooted on an extensive experimental campaign, where we gathered real jamming data for three communication frequencies representative of valuable services (Tetra, GPS, and Wi-Fi) over several distances at various locations. Processing the collected data, we found the best statistical distributions modelling both fast fading and slow fading effects on the identified channels when subject to jamming. Our investigation revealed that, independently from the selected frequency, fast fading on a jammed communication channel can be best modelled through a *t-locationScale* distribution. In contrast, the slow fading exhibits a behaviour that is best modelled through a power law. Among the many possible applications, we discussed two use-cases of the presented model, i.e., jamming localization and dead-reckoning navigation. We showed that, using our model, a mobile receiving device (e.g., a drone) can localize a jammer with a precision of $\approx$ 29 cm, and that it can reach the jamming source with an accuracy of ≈ 1.28 meters. We also compared our new model with statistical models available from the literature, showing the superior performances of our proposal. Finally, the data of our experimental campaign have been released as open-source [11], to allow Academia and Industry to validate and refine our results, as well as apply our findings to new use-cases. In the future, we plan to extend our measurement campaign with data acquired through an SDR carried out by a drone, so to collect the data for an entire 3-D plane at low granularity.

Acknowledgments

The authors would like to thank the anonymous reviewers, that helped improving the quality of the paper. This publication was partially supported by awards NPRP-S-11-0109-180242 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.

References

[1] Y. Huo, Y. Tian, L. Ma, X. Cheng, and T. Jing, "Jamming strategies for physical layer security," *IEEE Wireless Communications*, vol. 25, no. 1, pp. 148–153, 2018.

[2] Z. Zhang, J. Wu, J. Deng, and M. Qiu, "Jamming ack attack to wireless networks and a mitigation approach," in *IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference*, 2008, pp. 1–5.

[3] Z. Chi, Y. Li, X. Liu, W. Wang, Y. Yao, T. Zhu, and Y. Zhang, "Countering Cross-Technology Jamming Attack," in *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 99–110.

[4] S. Sciancalepore and R. Di Pietro, "Bittransfer: Mitigating Reactive Jamming in Electronic Warfare Scenarios," *IEEE Access*, vol. 7, pp. 156 175–156 190, 2019.

[5] R. A. Poisel, *Introduction to Communication Electronic Warfare Systems*. USA: Artech House, Inc., 2002.

[6] C. Zhong, J. Yao, and J. Xu, "Secure UAV Communication With Cooperative Jamming and Trajectory Control," *IEEE Communications Letters*, vol. 23, no. 2, pp. 286–289, 2019.

[7] A. Zanella, "Best Practice in RSS Measurements and Ranging," *IEEE Communications Surveys Tutorials*, vol. 18, no. 4, pp. 2662–2686, 2016.

[8] C. You and R. Zhang, "3D Trajectory Optimization in Rician Fading for UAV-Enabled Data Harvesting," *IEEE Transactions on Wireless Communications*, vol. 18, no. 6, pp. 3192–3207, June 2019.

[9] Y. Zeng, X. Xu, and R. Zhang, "Trajectory Design for Completion Time Minimization in UAV-Enabled Multicasting," *IEEE Transactions on Wireless Communications*, vol. 17, no. 4, pp. 2233–2246, April 2018.

[10] L. Yang, J. Chen, M. O. Hasna, and H. Yang, "Outage Performance of UAV-Assisted Relaying Systems With RF Energy Harvesting," *IEEE Communications Letters*, vol. 22, no. 12, pp. 2471–2474, Dec 2018.

[11] Cybersecurity Research and Innovation Lab (CRI-LAB), "Modelling a Communication Channel under Jamming: Experimental Model and Applications - Open-Source Dataset," https://github.com/pietrotedeschi/jamming_channel_dataset/, 2021.

[12] E. Vinogradov and S. Pollin, "Tutorial: Wireless Communications with Unmanned Aerial Vehicles," in *2019 53rd IEEE International Conference on Communications (ICC)*. Unpublished, 2019.

[13] X. Cai, A. Gonzalez-Plaza, D. Alonso, L. Zhang, C. B. Rodríguez, A. P. Yuste, and X. Yin, "Low altitude UAV propagation channel modelling," in *2017 11th European Conference on Antennas and Propagation (EUCAP)*, 2017, pp. 1443–1447.

[14] W. Khawaja, I. Guvenc, and D. Matolak, "UWB Channel Sounding and Modeling for UAV Air-to-Ground Propagation Channels," in *2016 IEEE Global Communications Conference (GLOBECOM)*, 2016, pp. 1–7.

[15] O. Punal, C. Pereira, A. Aguiar, and J. Gross, "Experimental Characterization and Modeling of RF Jamming Attacks on VANETs," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 2, pp. 524–540, 2015.

[16] K. Pelechrinis, I. Koutsopoulos, I. Broustis, and S. V. Krishnamurthy, "Lightweight Jammer Localization in Wireless Networks: System Design and Implementation," in *GLOBECOM 2009 - 2009 IEEE Global Telecommunications Conference*, Nov 2009, pp. 1–6.

[17] Y. S. Kim, F. Mokaya, E. Chen, and P. Tague, "All your jammers belong to us — Localization of wireless sensors under jamming attack," in *2012 IEEE International Conference on Communications (ICC)*, June 2012, pp. 949–954.

[18] Z. Niu, H. Li, X. Zhou, and J. Huang, "Overview of Jammer Localization in Wireless Sensor Networks," in *IEEE 9th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*, vol. 9, 2020, pp. 9–13.

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

[20] H. Aly, A. Basalamah, and M. Youssef, "Accurate and Energy-Efficient GPS-Less Outdoor Localization," *ACM Trans. Spatial Algorithms Syst.*, vol. 3, no. 2, Jul. 2017.

[21] P. Tedeschi, G. Oligeri, and R. Di Pietro, "Leveraging Jamming to Help Drones Complete Their Mission," *IEEE Access*, vol. 8, pp. 5049–5064, 2020.

[22] R. Skulstad, G. Li, T. I. Fossen, B. Vik, and H. Zhang, "Dead Reckoning of Dynamically Positioned Ships: Using an Efficient Recurrent Neural Network," *IEEE Robotics & Automation Magazine*, vol. 26, no. 3, pp. 39–51, 2019.

[23] Federation of American Scientist (FAS) - Military Analysis Network, "AGM-88 HARM," https://fas.org/man/dod-101/sys/smart/agm-88.htm, 2000, (Accessed: 2021-05-30).

[24] R. Akeela and B. Dezfouli, "Software-defined Radios: Architecture, state-of-the-art, and challenges," *Comp. Commun.*, vol. 128, pp. 106–125, 2018.

[25] F. Ricciato, S. Sciancalepore, F. Gringoli, N. Facchi, and G. Boggia, "Position and Velocity Estimation of a Non-Cooperative Source From Asynchronous Packet Arrival Time Measurements," *IEEE Transactions on Mobile Computing*, vol. 17, no. 9, pp. 2166–2179, 2018.

[26] Ettus Research, "UBX160 Daughterboard," https://www.ettus.com/product/details/UBX160, 2021, (Accessed: 2021-05-30).

[27] ——, "USRP X310," https://www.ettus.com/all-products/x310-kit/, 2021, (Accessed: 2021-05-30).

[28] E. Blossom, "GNU Radio: Tools for Exploring the Radio Frequency Spectrum," *Linux Journal*, vol. 2004, no. 122, 2004.

[29] ETSI, "Terrestrial Trunked Radio (TETRA)," https://www.etsi.org/deliver/etsi_ts/100300_100399/10039215/01.04.01_60/ts_10039215v010401p.pdf, 2010, (Accessed: 2021-05-30).

[30] Gadgets, Great Scott, "ANT500 Antenna," *Available: https://greatscottgadgets.com/ant500/*, 2021.

[31] M. Sheppard, "Allfitdist-Fit all valid parametric probability distributions to data: MATLAB Central," 2012.

[32] G. Oligeri, S. Sciancalepore, O. A. Ibrahim, and R. Di Pietro, "Drive Me Not: GPS Spoofing Detection via Cellular Network: (Architectures, Models, and Experiments)," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, 2019, p. 12–22.

[33] G. Oligeri, S. Sciancalepore, and R. Di Pietro, "GNSS spoofing detection via opportunistic IRIDIUM signals," in *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2020, pp. 42–52.

[34] Ettus Research, "VERT2450 Antenna," *Available: https://www.ettus.com/all-products/vert2450/*, 2021.

[35] NXP Semiconductors, "GPS, LNA, Sensitivity, Jamming, Cohabitation, TTFF," https://www.nxp.com/docs/en/brochure/75016740.pdf, 2020, (Accessed: 2021-05-30).

[36] K. J. Åström and T. Hägglund, *PID controllers: Theory, Design, and Tuning*. Instrument society of America Research Triangle Park, NC, 1995, vol. 2.

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

[38] 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)*, 2019, pp. 1–9.