Band & Tone Jamming Analysis and Detection on LoRa signals

Clément Demeslay, Roland Gautier, Anthony Fiche, Gilles Burel

Band & Tone Jamming Analysis and Detection on LoRa signals

Clément Demeslay*, *Student Member, IEEE*, Roland Gautier†, *Member, IEEE*, Anthony Fiche ‡, *Member, IEEE* and Gilles Burel§, *Senior Member, IEEE*
Univ Brest, Lab-STICC, CNRS, UMR 6285, F-29200, France
Email: *clement.demeslay@univ-brest.fr, †roland.gautier@univ-brest.fr, ‡anthony.fiche@univ-brest.fr, §gilles.burel@univ-brest.fr

***Abstract*—This paper examines the effect of Band Jamming (BJ) and Tone Jamming (TJ) on LoRa signals in a flat Additive White Gaussian Noise ($AWGN$) channel. In this scenario, LoRa proves to have good resiliency against these jamming attacks. Furthermore, a simple and lightweight BJ and TJ jammer detection scheme is derived. Theoretical and simulation results shows good detection capability, especially with Single Tone Jamming (STJ).**

***Index Terms*—LoRa, chirp modulation, Band Jamming, Tone Jamming, jammer detection.**

I. Introduction

The Internet of Things (IoT) is experiencing striking growth since the past few years enabling much more devices to communicate and allowing many scenarios to be a reality such as smart cities. The number of IoT devices is expected to rapidly grow, jumping from almost 10 to more than 21 billion [1]. Many technologies were developed in that sense relying on licensed bands (Narrow Band IoT ($NB-IoT$), Extended Coverage GSM ($EC-GSM$) and LTE-Machine ($LTE-M$)) or unlicensed bands such as SigFox, Ingenu, Weightless or Long Range (LoRa) [2]. This paper focuses on LoRa standard. LoRa has been initially developed by the French company Cycleo in 2012 and is now the property of Semtech company, the founder of LoRa Alliance. LoRa is nowadays a front runner in LP-WAN solutions and holds a lot of attention by the scientific research community. The LoRa vulnerabilities were addressed in the literature. In [3], a malicious LoRa user acts as a reactive jammer by sending random LoRa symbols to a legitimate LoRa node. The authors evaluated the jamming impact on Packet Delivery Ratio (PDR) and the frame detection probability by the jammer with real world LoRa transceivers. The authors from [4], [5] highlighted that the long Time On Air (TOA) of LoRa gives a bigger opportunity window for the jammer, especially with high modulation orders. Physical layer mitigation techniques were proposed to reduce jamming effectiveness such as frequency hopping scheme that was presented in [6]. To the best of authors knowledge, traditional jamming (mainly Band Jamming (BJ) and Tone Jamming (TJ)) impact on LoRa has not been investigated yet. Although smart jammers (*e.g.* malicious LoRa user) are more efficient, traditional jammers are still a threat for LoRa networks. Indeed, traditional jammers use usually low-cost devices and require minimal setup procedures. They can be then easily implemented and need therefore to be tackled. This paper focuses on the LoRa victim node. We propose to investigate the effect of both BJ and TJ on LoRa signals, the performance associated and a simple jamming detection scheme leveraging LoRa physical layer characteristics is derived. This gives the ability to a LoRa node to alert the presence of a jammer in the close environment. The main contributions of this paper are:

- An analysis of both BJ and TJ applied on LoRa signals that reveals the good LoRa's resiliency against these jamming attacks.
- A simple and efficient BJ and TJ detection scheme enabling more security in LoRa networks.

The remainder of the paper is organized as follows. In Section II, a brief review of LoRa physical layer is performed. Section III presents BJ and TJ models and the different jamming strategies are discussed. Section IV evaluates the impact of BJ & TJ on LoRa signals while Section V introduces the jammer detection scheme. Simulation results are presented in Section VI to assess jamming impact on Symbol Error Rate (SER) performance and jamming detection capability. Finally, Section VII concludes the paper.

II. LoRa modulation overview

A. LoRa waveforms

In the literature, LoRa waveforms are of the type of Chirp Spread Spectrum (CSS) signals. These signals rely on sine waves with Instantaneous Frequency (IF) that varies linearly with time over frequency range $f \in [-B/2, B/2]$ ($B \in \{125, 250, 500\}$ kHz) and time range $t \in [0, T]$ (T denotes the symbol period). This basic signal is called an *up-chirp* or *down-chirp* when frequency respectively increases or decreases over time. A LoRa symbol consists of SF bits ($SF \in \{7, 8, \dots, 12\}$) leading to an M-ary modulation with $M = 2^{SF} \in \{128, 256, \dots, 4096\}$. The symbol duration T is defined as $T = M/B$. This gives $T \approx \{1, 2, \dots, 32\}$ ms for $B = 125$ kHz and $SF = \{7, \dots, 12\}$. We may see that LoRa has quite long symbol duration compared to other modulation schemes such as $OFDM$ where symbols usually last only tens of μs. In the discrete-time signal model, the Nyquist sampling rate ($F_s = 1/T_s$) is used (*i.e.* $T_s = 1/B = T/M$) to reduce complexity. The signal symbol has then M samples.

Each symbol $a \in \{0, 1, \ldots, M-1\}$ is mapped to an *up-chirp* that is temporally shifted by $\tau_a = aT_s$ periods. We may notice that a temporal shift τ_a conducts to shift by $aB/M = a/(MT_s) = a/T$ the IF. The modulo operation is applied to ensure that IF remains in the interval $[-B/2, B/2]$. This behavior is the heart of CSS process. A mathematical expression of LoRa waveform sampled at $t = kT_s$ has been derived in [7] :

$$x(kT_s; a) \triangleq x_a[k] = e^{2j\pi k\left(\frac{a}{M} - \frac{1}{2} + \frac{k}{2M}\right)} \quad k = 0, 1, \ldots, M-1 \tag{1}$$

We may see that an *up-chirp* is actually a LoRa waveform with symbol index $a = 0$, written $x_0[k]$. Its conjugate $x_0^*[k]$ is then a *down-chirp*.

B. LoRa demodulation scheme

Reference [8] proposed a simple and efficient solution to demodulate LoRa signals. In Additive White Gaussian Noise ($AWGN$) channel, the demodulation process is based on the Maximum Likelihood (ML) detection scheme. The received signal is:

$$r[k] = x_a[k] + w[k] \tag{2}$$

with $w[k]$ a complex $AWGN$ with zero-mean and variance $\sigma^2 = E[|w[k]|^2]$. The Signal to Noise Ratio (SNR) is defined as $SNR = 1/\sigma^2$. ML detector aims to select index $\widehat{a}$ that maximizes the scalar product $\langle r[k], x_n[k]\rangle$ for $n = 0, 1, \ldots, M-1$ defined as:

$$\begin{aligned}\langle r[k], x_n[k]\rangle &= \sum_{k=0}^{M-1} r[k]x_n^*[k] \\ &= \sum_{k=0}^{M-1} \underbrace{(x_a[k] + w[k])x_0^*[k]}_{\tilde{r}[k]}\, e^{-j2\pi\frac{n}{M}k} \\ &= \tilde{R}[n] = \tilde{X}_a[n] + \tilde{W}[n] = M\delta[n-a] + \tilde{W}[n]\end{aligned} \tag{3}$$

with $\tilde{X}_a[k] = DFT\{x_a[k]x_0^*[k]\} = M\delta[n-a]$ and $\tilde{W}[k] = DFT\{w[k]x_0^*[k]\} \sim \mathcal{CN}(0, \sigma_w^2)$, $\sigma_w^2 = M\sigma^2$. $DFT\{.\}$ denotes the Discrete Fourier Transform (DFT) function. The demodulation stage proceeds with two simple operations:

- multiply the received signal by the *down-chirp* $x_0^*[k]$, also called dechirping,
- compute $\tilde{R}[n]$, the DFT of $\tilde{r}[k]$ and select the discrete frequency index $\widehat{a}$ that maximizes $\tilde{R}[n]$.

This way, the dechirp process merges all the signal energy in a unique frequency bin a and can be easily retrieved by taking the magnitude or square magnitude (non-coherent detection) of $\tilde{R}[n]$. The symbol detection is then:

$$\widehat{a}_{NCOH} = \arg\max_n \quad |\tilde{R}[n]|^2 \equiv \arg\max_n \quad |\tilde{R}[n]| \tag{4}$$

III. Traditional Jammer models

This section briefly reviews traditional jammer models and the main strategies that can be adopted by the jammer.

A. Band Jamming

BJ model is presented in Figure 1. It adds a jamming signal $w_J[k]$, usually an $AWGN$, in the data signal bandwidth. The jamming signal bandwidth may be restricted to a fraction of the data signal bandwidth as:

$$B_J = B \times \rho, \quad \rho \in]0; 1] \tag{5}$$

When $\rho = 1$, the jammer covers the entire useful bandwidth and is called Full Band Jamming (FBJ). For $\rho \neq 1$, the jammer is a Partial Band Jammer (PBJ). The total jamming power is fixed to $\sigma_J^2 = B \times N$ where N is the spectral density level and B the total available bandwidth, as depicted in Figure 1. ρ is the fraction of B to be covered by the jammer. As total available jamming power is fixed, reducing ρ increases therefore the spectral density level by a factor $1/\rho$.

The jammer can also tune the bandwidth position *i.e.* center frequency ν_J.

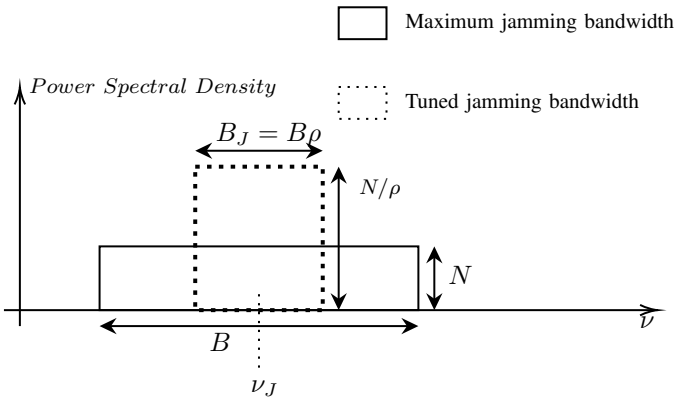

Fig. 1. Band Jamming model illustration.

B. Tone Jamming

TJ adds several sine waveforms in the useful bandwidth as depicted in Figure 2. The expression of the discrete jamming signal sampled at $t = kT_s$ is then:

$$\begin{aligned}s_{TJ}[k] &= \sum_{v=0}^{V-1} s_{TJ}^v[k] = \sum_{v=0}^{V-1} \sigma_J^v e^{2j\pi\nu_v k + j\phi_v} \\ \nu_v &= \frac{u_v}{M}, \quad u_v \in]0; M-1]\end{aligned} \tag{6}$$

With ϕ_v the initial phase of the vth tone signal and uniformly distributed over $[0; 2\pi]$. When $V = 1$ the jamming signal is Single Tone Jamming (STJ) and Multi Tone Jamming (MTJ) otherwise. From (6) the jammer can tune each sine waveform power. An optimal power strategy for the jammer is to adopt an uniform scheme [9] *i.e.* $(\sigma_J^v)^2 = \sigma_J^2/V$. This scheme is considered in this paper.

C. Jamming behaviors

In the literature, the jammer has mainly three different behaviors: the constant, reactive and random jammers. The

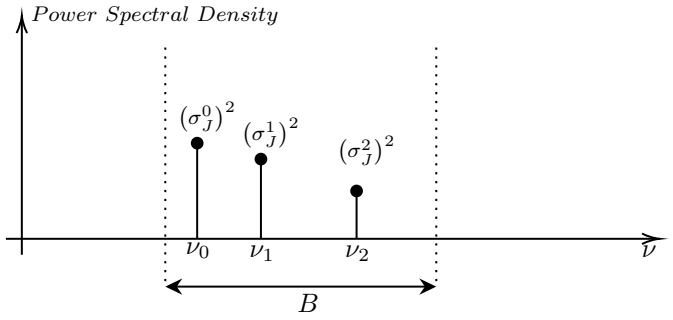

Fig. 2. Tone Jamming model illustration for $V = 3$.

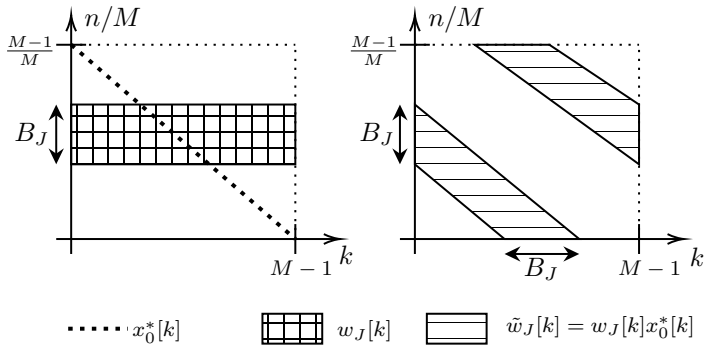

Fig. 3. Partial Band Jamming effect on LoRa DFT.

constant jammer has the maximum impact on the victim but is not energy efficient and easily detectable. This behavior is therefore usually ignored at the expense of the reactive jammer that is passive most of the time and sends a jamming signal only when detecting the target signal to be jammed. This behavior is a good energy/impact trade-off and is very likely to be found in real threats. We consider this strategy in the rest of the paper. Random jamming is less effective than reactive jamming but difficult to detect due to its random nature. Depending on the jammer behavior, the received signal at the victim LoRa node follows the next four hypotheses:

- $H_0 : r[k] = w[k]$
- $H_1 : r[k] = x_a[k] + w[k] + s[k]$
- $H_2 : r[k] = x_a[k] + w[k]$
- $H_3 : r[k] = w[k] + s[k]$

Hypotheses H_1 and H_3 are only valid for the constant jammer. The reactive jammer enables hypotheses H_0 and H_1 while random jammer enables the four hypotheses.

IV. BJ & TJ EFFECT ON LORA SIGNALS

The effect of jamming is only present for H_1. We denote the Noise Jamming Ratio (NJR) as $NJR = \sigma^2/\sigma_J^2$. The received signal at the victim LoRa node after dechirp process and DFT is:

$$\tilde{R}[n] = \tilde{X}_a[n] + \tilde{W}[n] + \tilde{S}[n] \tag{7}$$

The term $\tilde{S}[n]$ in (7) introduces interference. We focus on this term for the study of jamming. The term $\tilde{S}[n]$ is renamed as $\tilde{S}_{BJ}[n]$ for BJ and $\tilde{S}_{TJ}[n]$ for TJ.

A. BJ effect

The effect is illustrated in Figure 3. We may see that PBJ has the same effect as FBJ thanks to dechirp operation. The DFT output will have then an equivalent noise power of $\sigma_{BJ}^2 = \sigma_w^2 + M\sigma_J^2$ with limited impact on performance as it will be highlighted in Section VI.

B. TJ effect

TJ effect is illustrated similarly as BJ in Figure 4. We consider for instance integer u_v values. The dechirp and DFT operations lead to an effect equivalent as computing the DFT of a LoRa symbol with value $a = u_v$ and modulated by a *down-chirp*. The interference term is then:

$$\tilde{S}_{TJ}[n] = \sum_{v=0}^{V-1} DFT\{x_{u_v}^*[k]\} \tag{8}$$

Without loss of generality we consider $V = 1$ to evaluate (8). Developing (8) yields:

$$\tilde{S}_{STJ}[n] = \sqrt{\sigma_J^2} \sum_{k=0}^{M-1} e^{2j\pi \frac{-k^2+(M+2u_0-2n)k}{2M}} \tag{9}$$

The sum in (9) is in the form of a Generalized Quadratic Gaussian Sum ($GQGS$) resolution task. The $GQGS$ is defined as [10]:

$$G(\eta, \epsilon, \gamma) = \sum_{x=0}^{|\gamma|-1} e\left(\frac{\eta x^2 + \epsilon x}{\gamma}\right), \quad e(x) = e^{2j\pi x} \tag{10}$$

With η, ϵ and γ integers. When η odd, ϵ even and γ a power of 2, $G(\eta, \epsilon, \gamma)$ is:

$$G(\eta, \epsilon, \gamma) = e\left(-\frac{\frac{\epsilon^2}{4\eta}}{\gamma}\right) G(\eta, |\gamma|) \tag{11}$$

with $G(\eta, |\gamma|) = (1 + j^\eta)\sqrt{|\gamma|}$. By identification between (9) and (10), $\eta = -1$, $\epsilon = M + 2u_0 - 2n$ and $\gamma = 2M$ for LoRa. η is odd, ϵ is even and γ a power of 2 so (11) is valid. $G(\eta, |\gamma|)$ is then for LoRa $G(-1, 2M) = (1 - j)\sqrt{2M}$. We note that the sum in (9) has a range of $k = 0, \ldots, M-1$, contrarily to (10) that supposes to have a sum from $x = 0$ to $x = 2M - 1$. It can be normalized knowing that $\sum_{k=0}^{2M-1} e^{2j\pi \frac{\eta k^2+\epsilon k}{\gamma}} = 2\sum_{k=0}^{M-1} e^{2j\pi \frac{\eta k^2+\epsilon k}{\gamma}}$ with $e^{2j\pi \frac{\eta k^2+\epsilon k}{\gamma}} = e^{2j\pi \frac{\eta(k+M)^2+\epsilon(k+M)}{\gamma}}$, $k = 0, \ldots, M-1$. $\tilde{S}_{STJ}[n]$ is then:

$$\tilde{S}_{STJ}[n] = \sqrt{\sigma_J^2} \frac{G(-1, \epsilon_0, 2M)}{2}, \quad \epsilon_0 = M + 2u_0 - 2n \tag{12}$$

$\tilde{S}_{TJ}[n]$ is finally for any V:

$$\tilde{S}_{TJ}[n] = \sqrt{\sigma_J^2/V} \sum_{v=0}^{V-1} \frac{G(-1, \epsilon_v, 2M)}{2}, \quad \epsilon_v = M + 2u_v - 2n \tag{13}$$

When u_v is not integer, the computation of (9) is not possible with (13). The sum must be then computed numerically for each n value.

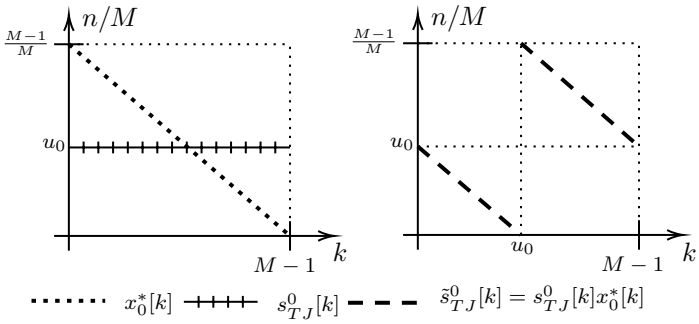

Fig. 4. Single Tone Jamming effect on LoRa DFT.

Figure 5 presents the DFT output of received LoRa signal contaminated by TJ, for $SF = 7$. This SF value is considered for the rest of the paper. The noise term $\tilde{W}[n]$ is neglected for convenience. When $V = 1$ and u_0 integer, the DFT magnitude is equal for each bin at $n \neq a$ and of value $\sqrt{M\sigma_J^2} = 16$ in this example ($\sigma_J^2 = 2$). When u_0 is not integer, the DFT experiences deformations. These deformations are maximum when $u_0 = \lfloor u_0 \rfloor + 0.5$ and has an oscillation behavior centered around $\sqrt{M\sigma_J^2}$, as showed in the figure. The oscillation is null at $n = M/2 + \lfloor u_0 \rfloor + 1$. When $V = 2$, a sine modulation wise behavior appears with frequency of approximately $|u_0 - u_1| \mod M$ and shifted circularly by $\min(u_0, u_1)$ positions. The DFT output is quite unpredictable for $V > 1$ and u_v not integer. We may see that the bin magnitude at $n = a$ depends on a. That is, certain a values depending on u_v will reduce or increase the expected magnitude of M without jamming. More precisely, we may see the following condition leading to performance improvement or degradation:

$$\text{if} \begin{cases} \Re\{\tilde{S}[a]\} > 0, & |\tilde{R}[a]| > M : \text{performance improvement} \\ \Re\{\tilde{S}[a]\} < 0, & |\tilde{R}[a]| < M : \text{performance degradation} \end{cases} \tag{14}$$

The symbols minimizing and maximizing performance are denoted a_{min} and a_{max} and are derived as:

$$\begin{aligned} a_{min} &= \arg\min_n \quad \Re\{\tilde{S}[n]\} \\ a_{max} &= \arg\max_n \quad \Re\{\tilde{S}[n]\} \end{aligned} \tag{15}$$

An example of DFT output with symbols $a = a_{max}$ and $a = a_{min}$ is showed in Figure 6, with $u_0 = 20$. In this case, $a_{max} = 67$ and $a_{min} = 3$. Moreover, the performance gain and loss are respectively $\Gamma^+ = \tilde{R}[a_{max}] - M = \sqrt{M\sigma_J^2}$ and $\Gamma^- = M - \tilde{R}[a_{min}] = \sqrt{M\sigma_J^2}$, for $V = 1$. When $V > 1$, the performance gain/loss does not hold exactly the same behavior with $\Gamma^+ > \Gamma^-$ or $\Gamma^+ < \Gamma^-$, depending on u_v values.

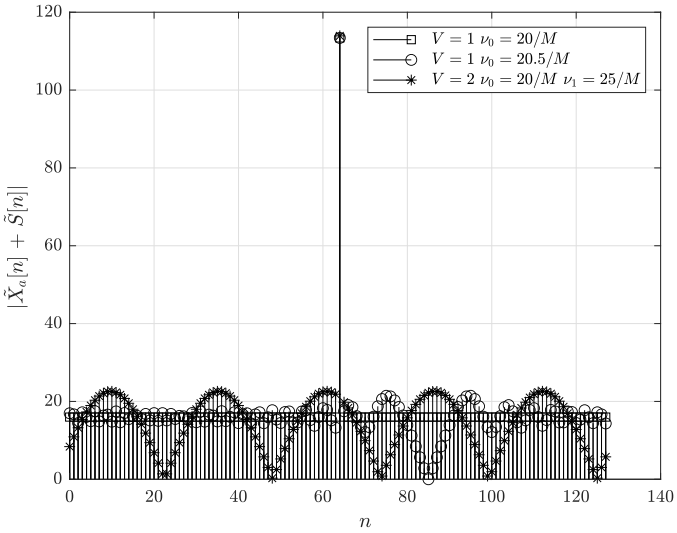

Fig. 5. DFT output of received LoRa plus TJ signal without noise for $V = \{1, 2\}$ and different sine waveform of frequencies u_v. $SF = 7$, $a = M/2$.

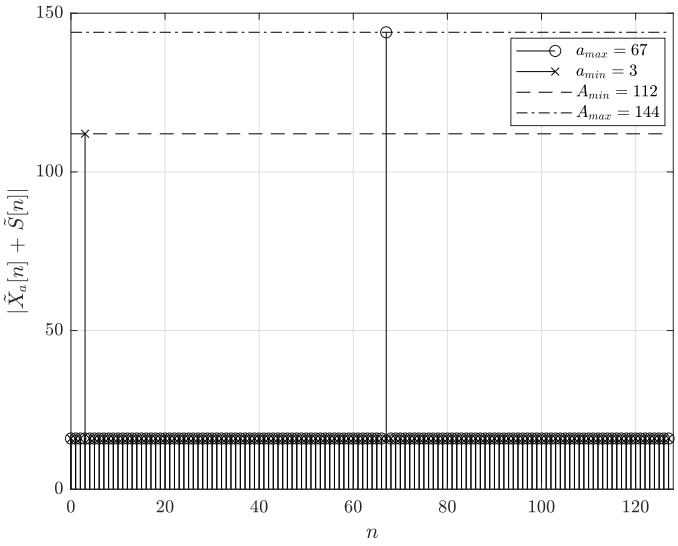

Fig. 6. DFT output of received LoRa plus TJ signal without noise for $V = 1$, $u_0 = 20$ and $SF = 7$.

V. Jammer detection scheme

A. LoRa DFT $PDFs$

The jamming detection scheme is performed in the frequency domain *i.e.* the LoRa dechirped DFT to keep simple implementation. We may recall the Probability Density Functions (PDF) of $|\tilde{R}[n]|$ for the two hypotheses H_0 and H_1 (reactive jammer), noted as $|\tilde{R}_{H_0}[n]|$, $|\tilde{R}_{H_1}^{BJ}[n]|$ and $|\tilde{R}_{H_1}^{TJ}[n]|$ for BJ and TJ, respectively. In H_0, only $AWGN$ is present. Its statistic is not changed by the dechirp process. We can easily conclude that Random Variable (RV) X_{H_0} of $|\tilde{R}_{H_0}[n]|$ follows a Rayleigh distribution $f_{X_{H_0}}(t) = Rayl(t, b_{X_{H_0}})$ with $b_{X_{H_0}} = \sqrt{M\sigma^2/2}$ the scale parameter.

The term $\tilde{S}[n]$ in H_1 leads to a Rayleigh PDF $f_{X_{H_1}^{BJ}}(t) = Rayl(t, b_{X_{H_1}^{BJ}})$ with $b_{X_{H_1}^{BJ}} = \sqrt{M(\sigma^2 + \sigma_J^2)/2}$, for BJ and $n \neq a$. TJ throws a Rician PDF to $|\tilde{R}_{H_1}^{TJ}[n]| \sim X_{H_1}^{TJ}$,

$f_{X_{H_1}^{TJ}}(t) = Rice(t, \mu_{X_{H_1}^{TJ}}, \sigma_{X_{H_1}^{TJ}})$ with non centrality parameter $\mu_{X_{H_1}^{TJ}} = \sqrt{M\sigma_J^2}$ and scale parameter $\sigma_{X_{H_1}^{TJ}} = b_{X_{H_0}}$, $n \neq a$.

B. Jammer detector

A simple solution to detect the BJ or TJ jammer is to compute the following normalized quantity test:

$$z = \sum_{l=0}^{L-1} \frac{|\tilde{R}[n_l]|}{b_{X_{H_0}}}, \quad n_l \neq a \tag{16}$$

As the jammer is reactive, the LoRa node can estimate regularly $w[k]$ variance during silence periods *i.e.* in H_0 hypothesis and leverage this information to detect the jammer. From (16), the receiver chooses randomly L frequency indexes different from $n = a$. Indeed, the PDF of $|\tilde{R}_{H_1}[a]|$ depends on a for both BJ and TJ, an information not available. To mitigate this situation, the receiver can eliminate the N_λ frequency bins that are above a certain threshold. The threshold is designed with Neyman-Pearson (NP) criterion. The False Alarm Probability (FAP) P_{fa} is fixed and the threshold is derived by:

$$\lambda = F_{Rayl}^{-1}(1 - P_{fa}; \sqrt{M\sigma^2/2}) \tag{17}$$

with $F_{Rayl}^{-1}(.;.)$ denoting the inverse Cumulative Density Function (CDF) of Rayleigh RV. We note z_{H_0} and z_{H_1} the quantity test in H_0 and H_1 hypotheses, respectively. It is worth-noting that z_{H_0} is a sum of Rayleigh RVs. The evaluation of PDF and CDF of a sum of Rayleigh RVs has been studied in the literature. The authors from [11] derived a closed-form approximation based on Small Argument Approximation (SAA) approach. Their solution is widely used but has the drawback to introduce bias as L grows. More recent studies proposed a closed-form expression but limited to small L values, $L \in \{2, \ldots, 16\}$ in [12] for example. To have more flexibility, we choose SAA technique. From [11], PDF Z_{H_0} is:

$$f_{Z_{H_0}}^{SAA}(t) = \sum_{l=0}^{L-1} X_{H_0}^l = \frac{t^{2L-1} e^{-\frac{t^2}{2b_{Z_{H_0}^{SAA}}}}}{2^{L-1}(b_{Z_{H_0}^{SAA}})^L (L-1)!^1}$$
$$b_{Z_{H_0}^{SAA}} = \frac{1}{L}[(2L-1)!^2]^{1/L} \tag{18}$$

where

$$x!^c = 1 \times (1+c) \times (1+2c) \times \ldots \times x \tag{19}$$

Its CDF is:

$$F_{Z_{H_0}}^{SAA}(t) = 1 - e^{-\frac{t^2}{2b_{Z_{H_0}^{SAA}}}} \sum_{l=0}^{L-1} \frac{\left(\frac{t^2}{2b_{Z_{H_0}^{SAA}}}\right)^l}{l!^1} \tag{20}$$

In H_1 and BJ, $z_{H_1}^{BJ}$ follows the same PDF as z_{H_0} but with different parameter $b_{Z_{H_1}^{BJ,SAA}} = \frac{1+\frac{\sigma_J^2}{\sigma^2}}{L}[(2L-1)!^2]^{1/L}$ as the noise DFT has variance σ_{BJ}^2. The associated CDF is $F_{Z_{H_1}}^{BJ,SAA}$. In TJ case, $z_{H_1}^{TJ}$ is a sum of Rician RVs. Similar research to evaluate sum of Rician RVs has been performed [13], [14] but are still limited to small L values (up to $L = 10$ in [14]) and reduced number of possible NJR values, $NJR_{dB} \in \{-7, -5, -3, -1\}$ in [13]. This limits the application to our LoRa jammer detector. We decide to use instead the approximation of the Rician distribution when $V = 1$. If $NJR_{dB} \to \infty$, $f_{Z_{H_1}}^{STJ}$ approaches $f_{Z_{H_0}}^{SAA}$ and noted $f_{Z_{H_1}}^{STJ^+}$. If $NJR_{dB} \to -\infty$, $f_{Z_{H_1}}^{STJ}$ is a normal distribution noted $f_{Z_{H_1}}^{STJ^-}$:

$$f_{Z_{H_1}}^{STJ^-}(t) = \mathcal{N}(t, \mu_{Z_{H_1}^{STJ^-}}, \sigma_{Z_{H_1}^{STJ^-}})$$
$$\mu_{Z_{H_1}^{STJ^-}} = \frac{\sqrt{M(\sigma^2/2 + \sigma_J^2)L}}{b_{X_{H_0}}}, \quad \sigma_{Z_{H_1}^{STJ^-}} = 1 \tag{21}$$

The CDF are $F_{Z_{H_1}^{STJ^-}}$ and $F_{Z_{H_1}^{STJ^+}}$. Intermediate NJR_{dB} values will lead to reasonably small bias. When $V > 1$, the PDF has not analytical expression and must be therefore numerically computed. CDF is noted $F_{Z_{H_1}}^{MTJ}$. Finally, the receiver detects the jammer with a threshold identically designed as λ with fixed FAP:

$$\lambda_{SAA} = \left(F_{Z_{H_0}}^{SAA}\right)^{-1}(1 - P_{fa}^{SAA}) \tag{22}$$

$$z \underset{H_0}{\overset{H_1}{\gtrless}} \lambda_{SAA} \tag{23}$$

An illustration for BJ case of theoretical PDFs and histograms for both H_0 and H_1 hypotheses are depicted in Figure 7.

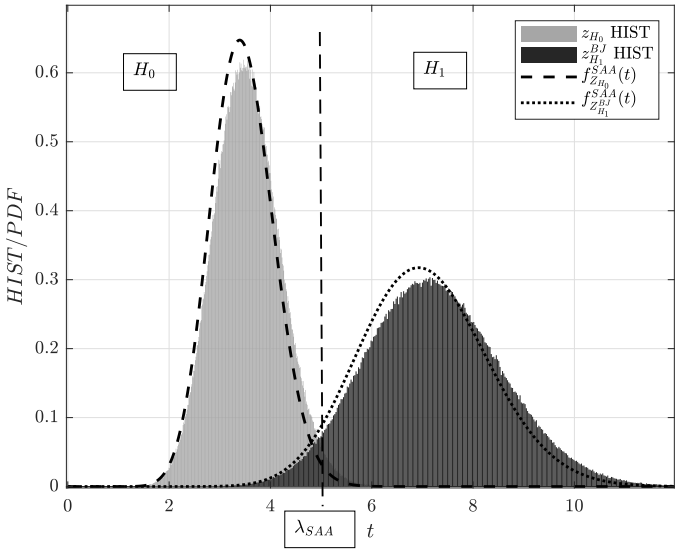

Fig. 7. Theoretical PDFs and histograms of quantities test z_{H_0} and $z_{H_1}^{BJ}$ for BJ. $NJR_{dB} = -5$, $SNR_{dB} = -5$, $L = 8$ and $\rho = 0.6$. Histograms have indexes t_h normalized such that $t = t_h/\sqrt{L}$ as stated in [12].

VI. SIMULATION RESULTS

This section provides Monte-Carlo simulation results to evaluate BJ and TJ performance impact on SER and assess the jammer detection capability. To simulate BJ, an $AWGN$ is generated and filtered according to ρ and σ_J^2 constraints.

A. PBJ and MTJ performance impact on SER

The simulations are performed with respect to Signal Jamming Ratio (SJR) $SJR = 1/\sigma_J^2$. The SNR is fixed to $SNR_{dB} = -8$.

1) PBJ performance impact on SER: Figure 8 highlights the impact of ρ on performance as mentioned in Section IV-A. $SJR_{dB} \in \{-3, 0, 3\}$ and $AWGN$ performance showed as comparison. Higher SJR_{dB} values slowly reduce performance with a SER difference of roughly 1.1×10^{-2} between $SJR_{dB} = -3$ and $SJR_{dB} = 3$. We may see in the Figure that ρ has virtually no impact on performance whatever SJR is. This confirms performance predictions made in Section IV-A, as σ_J^2 is fixed. It is obvious that BJ is not a good strategy for the jammer.

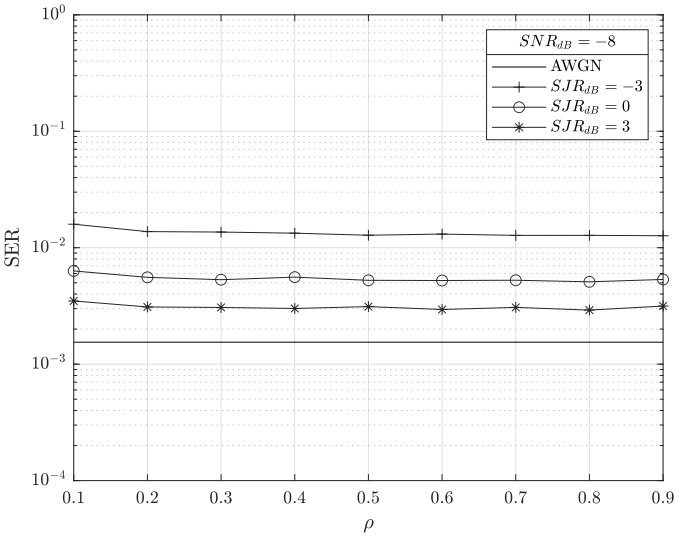

Fig. 8. PBJ SER performance depending on $\rho \in \{0.1, 0.2, \ldots, 0.9\}$ $SNR_{dB} = -8$ and $SJR_{dB} \in \{-3, 0, 3\}$.

2) MTJ performance impact on SER: For MTJ performance impact evaluation, u_v is integer and chosen uniformly in $u_v \in \{0, \ldots, M-1\}$ at each Monte-Carlo trial. Figure 9 points out two interesting performance results. First, V has no particular influence on performance when u_v is integer. This also true for u_v non integer. Indeed, the periodic DFT output behavior for u_v non integer as depicted in Figure 5 has average magnitude values around $\sqrt{M\sigma_J^2}$, the value when u_v is integer. Statistically, for a random and uniform over $[0; M-1]$, this does not influence performance. Second, a value has a huge impact on performance. The symbol minimizing performance a_{min} leads to very poor performance that reaches $AWGN$ one only from $SJR_{dB} = 20$. Interestingly, a_{max} does not improve so much performance, with only a gain of about 1.1×10^{-3} at $SJR_{dB} = -5$.

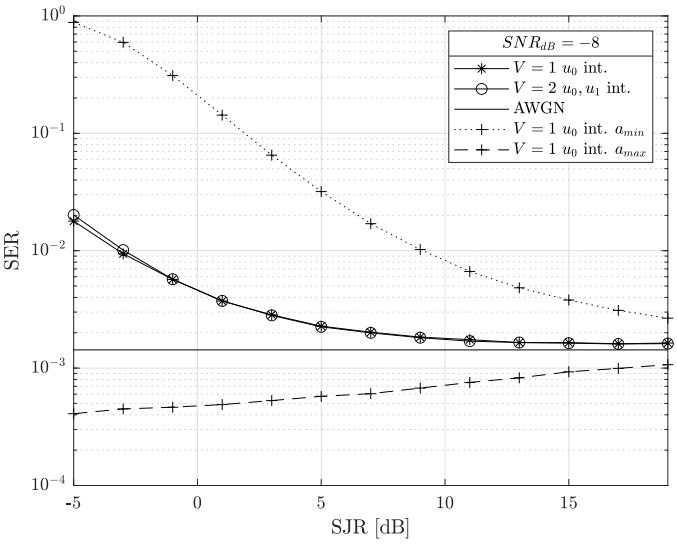

Fig. 9. MTJ SER performance as a function of SJR. $SNR_{dB} = -8$, u_v integer and considering a_{min} and a_{max} symbol values.

B. Jammer detection performance

We compare in this section jammer detection performance for several NJR_{dB} and L values. Theoretical CDFs $F_{Z_{H_0}}^{SAA}$ and $F_{Z_{H_1}}^{BJ,SAA}$ for BJ are computed using Equation (20). Depending on V, $F_{Z_{H_1}^{STJ^-}}$, $F_{Z_{H_1}^{STJ^+}}$ or $F_{Z_{H_1}^{MTJ}}$ are computed for TJ case. Note that $F_{Z_{H_1}^{MTJ}}$ is numerically computed based on its PDF with Monte-Carlo trials. λ_{SAA} is also computed numerically as [12] does not provide inverse CDF. The Miss Detection Probability (MDP) for BJ and TJ are respectively computed as:

$$P_{md}^{BJ} = \int_{-\infty}^{\lambda_{SAA}} f_{Z_{H_1}}^{BJ,SAA}(t)dt = F_{Z_{H_1}}^{BJ,SAA}(\lambda_{SAA}) \quad (24)$$

$$P_{md}^{STJ} = \int_{-\infty}^{\lambda_{SAA}} f_{Z_{H_1}}^{STJ^{+/-}}(t)dt = F_{Z_{H_1}}^{STJ^{+/-}}(\lambda_{SAA}) \quad (25)$$

$$P_{md}^{MTJ} = \int_{-\infty}^{\lambda_{SAA}} f_{Z_{H_1}}^{MTJ}(t)dt = F_{Z_{H_1}}^{MTJ}(\lambda_{SAA}) \quad (26)$$

1) Theoretical performance: Theoretical P_{md} performance as a function of L and NJR are plotted in Figures 10 and 11, respectively, for FBJ and STJ. ρ then equals 1. We may see that as L increases or NJR decreases, the P_{md} reduces. Consequently, the jammer detection performance increases. It can be easily explained by the fact that for $L = 1$, taking a single frequency bin is insufficient to make a proper decision. Ideally, $L = M - N_\lambda$ (the bin magnitude at $n = a$ is ignored). However, the theoretical/simulation bias will be more important for large L due to SAA limitation and therefore the obtained P_{md} will be slightly different, as it will be highlighted in next section. If NJR is to high, the jammer power is overlooked in the noise floor leading to impossible detection. A trade-off between P_{fa}^{SAA} and P_{md} is necessary as less false alarm will increase non detection. It can also be seen that STJ

detection outperforms FBJ detection. A P_{md} factor of about 390 at $L = 64$ and $P_{fa}^{SAA} = 10^{-3}$ is experienced in Figure 10.

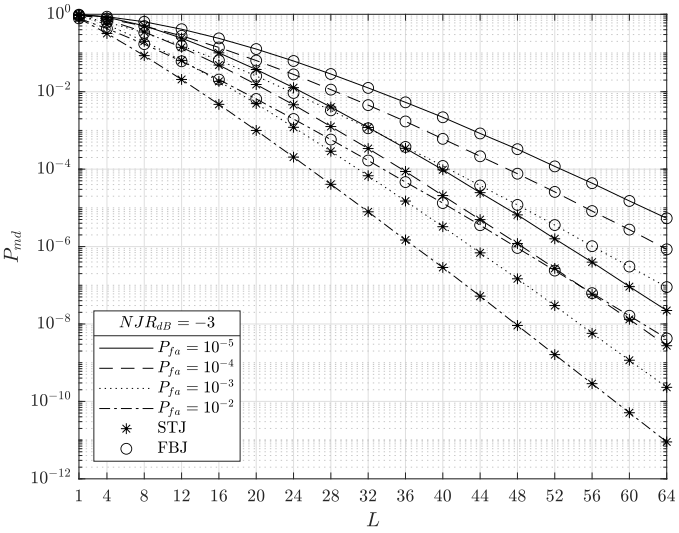

Fig. 10. Theoretical FBJ and STJ P_{md} as a function of L for different $P_{fa}^{SAA} \in \{10^{-2}, 10^{-3}, 10^{-4}, 10^{-5}\}$. $NJR_{dB} = -3$.

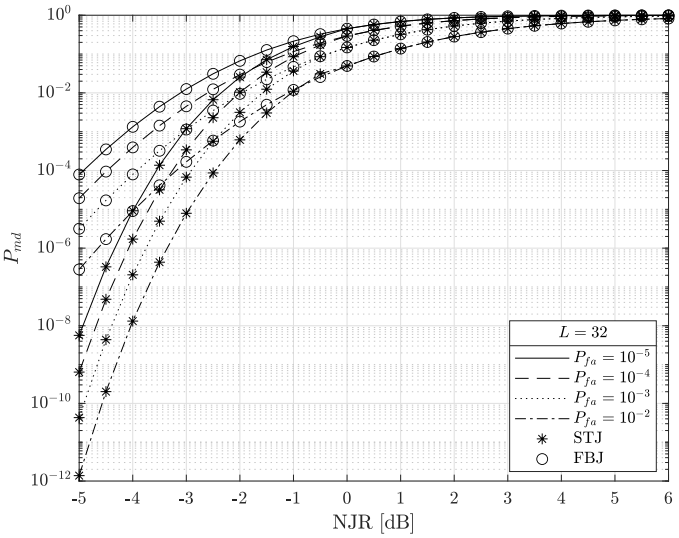

Fig. 11. Theoretical FBJ and STJ P_{md} as a function of NJR for different $P_{fa}^{SAA} \in \{10^{-2}, 10^{-3}, 10^{-4}, 10^{-5}\}$. $L = 32$.

2) Theoretical versus Simulation performance: We finally compare simulation against theoretical P_{md}. PBJ simulation are performed with $\rho = 0.6$. MTJ is evaluated for $V \in \{1, 3\}$ with ν_v values $\nu_0 = 0.711$, $\nu_1 = 0.812$ and $\nu_2 = 0.273$. From Figure 12, we may see that $L = 16$ introduces a slightly higher bias compared with $L = 4$, as expected, in favor of higher P_{md} performance.

From Figure 13, we remark that the theory/simulation bias is reduced for $V = 3$. Indeed, computing numerically $F_{Z_{H_1}^{MTJ}}$ removes CDF/histogram bias. MTJ detection experiences a performance hit with $V = 3$ but is still more efficient than PBJ. At $NJR_{dB} = -10$ and $P_{fa}^{SAA} = 10^{-5}$, BJ has a P_{md} of roughly 9×10^{-2} against 6×10^{-2} for MTJ. Higher V values does not change P_{md} performance *i.e.* $P_{md}^{v-1} \approx P_{md}^{v}$ for $V > 1$.

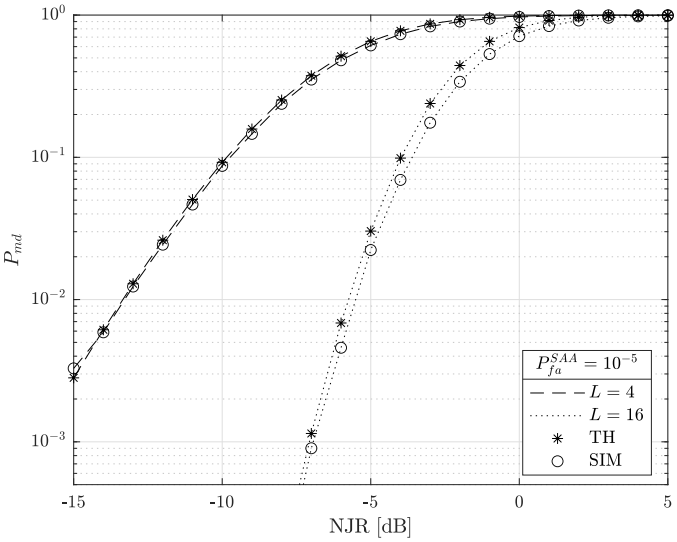

Fig. 12. Theoretical versus simulation P_{md} for PBJ as a function of NJR for different $P_{fa}^{SAA} = 10^{-5}$, $L \in \{4, 16\}$, $SNR_{dB} = 0$ and $\rho = 0.6$.

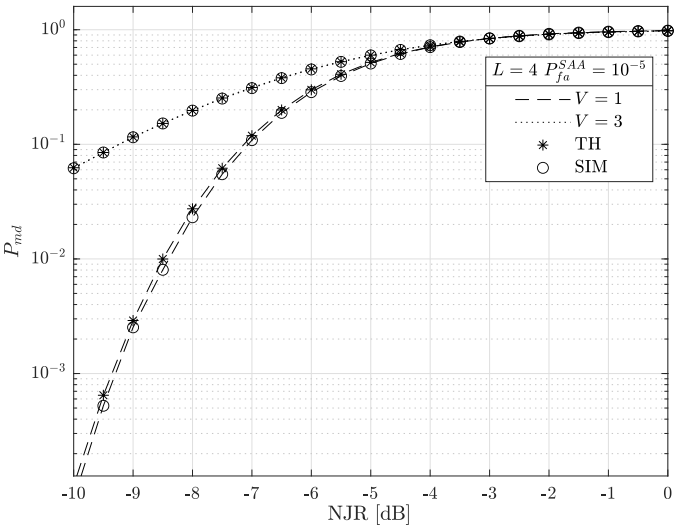

Fig. 13. Theoretical versus simulation P_{md} for STJ ($V = 1$) and MTJ ($V = 3$) as a function of NJR for different $P_{fa}^{SAA} = 10^{-5}$, $SNR_{dB} = 0$ and $L = 4$.

VII. Conclusion

In this paper, analysis of both BJ and TJ on LoRa signals was carried out. We pointed out that PBJ has virtually same effect as FBJ. It is therefore equivalent to an additional source of $AWGN$ leading then to small SER performance degradation. We also highlighted that TJ parameters V and u_v has negligible impact on SER performance. We can conclude that LoRa is quite robust to BJ and TJ. We also developed a simple scheme to detect efficiently BJ and TJ. The method leverages traditional basic LoRa processing without adding a burden on complexity. Overall, TJ detector performs better than BJ, even when considering MTJ scenario even though

MTJ detection appears to be less efficient than TJ. This work can be further extended. For example, real tests on LoRa transceivers can be performed to assess the article conclusions drawn beforehand in more realistic conditions. Furthermore, the theoretical impact of a multi-path channel on these jamming schemes can be explored. Temporal and frequency desynchronizations impact may be also investigated.

ACKNOWLEDGMENT

This work was jointly supported by the Brest Institute of Computer Science and Mathematics ($IBNM$) CyberIoT Chair of Excellence of the University of Brest, the Brittany Region and the "Pôle d'Excellence Cyber".

REFERENCES

[1] Statista. (2016, November) Internet of things (IoT) active device connections installed base worldwide from 2015 to 2025. [Online]. Available: https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/

[2] C. Goursaud and J. Gorce, "Dedicated networks for IoT: PHY / MAC state of the art and challenges," *EAI endorsed transactions on Internet of Things*, October 2015.

[3] C. Huang, C. Lin, R. Cheng, S. J. Yang, and S. Sheu, "Experimental evaluation of jamming threat in lorawan," in *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, April 2019, pp. 1–6.

[4] E. Aras, G. S. Ramachandran, P. Lawrence, and D. Hughes, "Exploring the security vulnerabilities of lora," in *2017 3rd IEEE International Conference on Cybernetics (CYBCONF)*, 2017, pp. 1–6.

[5] E. Aras, N. Small, G. Ramachandran, S. Delbruel, W. Joosen, and D. Hughes, "Selective jamming of lorawan using commodity hardware," *Proceedings of the 14th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, 2017.

[6] A. Ahmar, E. Aras, W. Joosen, and D. Hughes, "Towards more scalable and secure lpwan networks using cryptographic frequency hopping," in *2019 Wireless Days (WD)*, 2019, pp. 1–4.

[7] M. Chiani and A. Elzanaty, "On the LoRa modulation for IoT: Waveform properties and spectral analysis," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8463–8470, May 2019.

[8] L. Vangelista, "Frequency shift chirp modulation: The LoRa modulation," *IEEE Signal Processing Letters*, vol. 24, no. 12, pp. 1818–1821, December 2017.

[9] T. Li, T. Song, and Y. Liang, *Wireless Communications under Hostile Jamming: Security and Efficiency*. Springer Singapore, 2018.

[10] B. Berndt, R. Evans, and K. Williams, *Gauss and Jacobi Sums*. Wiley, 1998.

[11] M. Schwartz, W. Benett, and S. Stein, *Communication Systems and Techniques*. New York:McGraw Hill, 1966.

[12] J. Hu and N. C. Beaulieu, "Accurate simple closed-form approximations to the distributions and densities of a sum of independent rayleigh random variables," in *Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers, 2004.*, vol. 1, 2004, pp. 1092–1095 Vol.1.

[13] ——, "Accurate closed-form approximations to ricean sum distributions and densities," *IEEE Communications Letters*, vol. 9, no. 2, pp. 133–135, 2005.

[14] J. A. Lopez-Salcedo, "Simple closed-form approximation to ricean sum distributions," *IEEE Signal Processing Letters*, vol. 16, no. 3, pp. 153–155, 2009.