IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 20, 2018, accepted May 27, 2018, date of publication June 11, 2018, date of current version July 6, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2845839

Exploiting the Reciprocal Channel for Discrete Jamming to Secure Wireless Communications Against Multiple-Antenna Eavesdropper

GUSTAVO ANJOS[1,2], DANIEL CASTANHEIRA[1,2], ADÃO SILVA[1,2], ATÍLIO GAMEIRO[1,2], MARCO GOMES[2,3], (Member, IEEE), AND JOÃO P. VILELA[4]

[1]Department of Electronics, Telecommunications and Informatics, University of Aveiro, 3810-193 Aveiro, Portugal
[2]Instituto de Telecomunicações, 1049-001 Lisboa, Portugal
[3]Department of Electrical and Computer Engineering, University of Coimbra, 3030-290 Coimbra, Portugal
[4]CISUC, Department of Informatics Engineering, University of Coimbra, 3030-290 Coimbra, Portugal

Corresponding author: Gustavo Anjos (gustavoanjos@ua.pt)

This work was supported through project SWING2 (PTDC/EEITEL/3684/2014), funded by Fundos Europeus Estruturais e de Investimento through Programa Operacional Competitividade e Internacionalização-COMPETE 2020 and by National Funds from FCT-Fundos Europeus Estruturais e de Investimento, through Project POCI-01-0145-FEDER-016753.

ABSTRACT The purpose of this paper is to advance the current state of physical layer security through the design and analysis of a discrete jamming scheme that exploits the reciprocal characteristic of the wireless channel with the aim to create equivocation to a passive multiple-antenna eavesdropper. Closed form solutions of the secrecy capacity for different configurations of the jamming component were obtained and successfully compare with the simulation results. Furthermore, the secrecy level provided by the developed scheme is analyzed taking into account the number of bits extracted from the channel. The asymptotic study of the proposed secrecy technique allowed to conclude that in the high-power regime, full secrecy is obtained even considering that the eavesdropper is equipped with an unlimited number of antennas.

INDEX TERMS Physical layer security, secrecy capacity, jamming, channel reciprocity.

I. INTRODUCTION

The flexibility to exchange data between humans without the need to establish a physical connection in the access was one of the main reasons that led to the proliferation of wireless networks observed today. While in the past this interconnection was performed only among humans, the emerging concept of the Internet of Things (IoT) aims to put billions of objects exchanging data together in an autonomous way. Considering that the access connection of most part of these objects will be done through the wireless channel, the IoT paradigm promises to place the densification of wireless terminals at unprecedented levels. The large amount of objects equipped with wireless transceivers challenges the security level of wireless networks in the sense that any regular object can act as a source of eavesdropping. The technological evolution described above reinforces the need for a continuous improvement of the wireless networks security through the design of efficient secrecy schemes.

Since the appearance of initial wireless standards, protection against eavesdropping attacks has been supported by higher layer cryptographic protocols [1]. Although the widespread integration of these protocols in wireless communications, information secrecy is only achieved in the case of insufficient computational processing capacity at the eavesdropper [2].

In order to overcome the vulnerabilities associated with the use of standalone cryptographic protocols [3], [4], exploitation of the random characteristics of the physical wireless channel have been object of intensive research in order to find new schemes that improve the secrecy performance of future wireless standards. The achievement of information secrecy at the physical layer is the result of forcing a channel advantage in relation to the eavesdropper; therefore, contrarily to what happens with higher layer cryptographic protocols, physical layer security does not rely on the underlying assumption that the eavesdropper has limited computational resources [5].

In 1949, Claude Shannon defined some of the theoretical basis applied today in the design of secure communication channels. Shannon [6] stated that to achieve perfect secrecy would be required to use an independent secure key with at least the same size and entropy of the information source.

In his work, Shannon assumed that the secure key was the only information not shared between the legitimate receiver and the eavesdropper. Therefore, from the perspective of wireless communications, the channel model used in [6] does not reflects the features of a real wireless channel, making the statement above somehow pessimistic for this type of systems. A few years later, Csiszár and Korner [7] considered a more realistic scenario assuming different discrete memoryless channels for the legitimate receiver and eavesdropper. Under this assumption, Csiszár and Korner [7] made a theoretical analysis regarding the secrecy level of such a system. While Csiszár and Korner [7] considered a discrete memoryless wiretap channel, the work in [8] introduced by the first time the Gaussian wiretap channel, defining at the same time the respective secrecy capacity. Using some of the theoretical foundations established in these early works, new practical secrecy schemes have been developed with the purpose of providing information secrecy in practical communication scenarios. In recent literature it is possible to identify two major research domains in the design of physical layer secrecy schemes: the coding and the signal level domain. In the coding domain, the main objective is to design error-correction codes that also implement some level of secrecy in a wiretap channel [9]–[12]. In the case of signaling, techniques involving specific precoding designs, power allocation schemes, and cooperative jamming based on interference alignment (IA) [13], [14] and artificial noise injection have been defined in [15]–[20].

The secure degrees-of-freedom (DoF) of the wiretap channel were obtained in [21] considering the help of several cooperative jammers employing a single antenna. In this work the authors assume that the eavesdropper channel-state-information (CSI) is not available at the legitimate nodes and demonstrate that positive secure DoF are obtained by forcing the alignment of the jamming signals at the legitimate receiver. However, the need of having at least one jammer limits the implementation of the scheme proposed in [21] to scenarios with terminals available to cooperate. Xie and Ulukus [22] extend the work of [21] and derive the secure DoF of different network structures, with the difference that this time, IA is applied assuming that eavesdropper channel knowledge is available at the transmitters. Despite the necessity of having jammers available to cooperate, the scheme in [22] is also limited in the sense that does not take into account the presence of passive eavesdroppers. To remove this drawback, Goel and Negi [23] show that by combining information data with artificial noise, a positive secrecy capacity is achieved when the noise signal is transmitted in the null-space direction of the legitimate receiver. The main limitation of the scheme suggested in [23] is related to the fact that positive secrecy is reached only when the total number of antennas at the legitimate transmitter is larger than the number of antennas at the eavesdropper. For example, if we consider a massive MIMO eavesdropper, i.e. with a large number of antennas, the previous condition may not be respected. The problem of pilot contamination attacks in TDD multi-cell multiuser massive MIMO systems is focused in [24]. To address the secrecy capacity reduction caused by contaminated channel estimations, the work in [24] explores the excess degrees of freedom of a maximum ratio transmission (MRT) based massive MIMO system in order to generate artificial noise (AN) using random shaping matrix precoding as well as null-space (NS) based precoding. Taking into account the large computational complexity required to calculate the NS of large channel matrices, Zhu *et al.* [24] verified that the use of random shaping matrices for AN precoding could offer a good solution in terms of performance/complexity tradeoff.

Another important research path considered in the design of physical layer secrecy schemes explores the reciprocal characteristic of the wireless channel to establish a secure random key shared among the legitimate parties. In [25] and [26], the potential of received-signal-strength (RSS) and channel phase estimations for key generation is analyzed. While Ren *et al.* [25] and Wang *et al.* [26] focus on methods to extract secret keys, other schemes use those keys to increase the level of randomness in the transmitted data symbols [27], [28]. Anjos *et al.* [27] suggested a secrecy scheme that uses the reciprocal channel phase to randomly select discrete jamming signals at the legitimate nodes. In a preliminary secrecy evaluation, information data and discrete jamming signals are randomly combined in order to generate equivocation at the eavesdropper. In the second part of the work, the design of an efficient combining algorithm was proposed to improve the secrecy level of the initial random combining technique. The main drawback of the work in [27] is related to the fact that no general closed formulations for the secrecy capacity are provided, with the performance assessment limited to simulation results without making any theoretical analysis of the asymptotical behavior. Instead of using the reciprocal channel phase to define jamming signals Chen *et al.* [28] suggest to apply continuous random phase rotations in the transmitted data symbols. However, the method proposed in [28] only works when PSK signals are considered, being the proposed scheme insecure when QAM constellations are used.

In this paper, we propose to enhance the secrecy level of wireless networks through the design and analysis of a discrete jamming scheme that uses the randomness of the reciprocal wireless channel to force interference at a passive multiple-antenna eavesdropper. The exploration of the reciprocity feature of the channel allows the legitimate receiver to have enough information to cancel the jamming component; therefore, equivocation is only verified at the eavesdropper side. In summary, the main contributions of the present work are described in the following points:

a) Design of a discrete jamming scheme that exploits the reciprocal wireless channel with the aim of create equivocation at a passive eavesdropper;
b) Considering different configurations in the design of the jamming component, closed form solutions for the

secrecy capacity are derived and successfully compared with simulation results.

c) Through an asymptotical mathematical analysis, we prove that in the high power regime, full secrecy capacity is reached independently of the number of antennas at the eavesdropper;

d) The secrecy level provided by the different configurations of the jamming component is also analyzed taking into account the number of bits extracted from the channel.

Contrarily to the modular operation applied in [6], in this work the secret key extracted from the reciprocal legitimate channel is combined with the information source using integer addition. The physical practicality of integer addition extends the relevance of the presented work to scenarios where the secret key must be combined with the information source in a superposition physical process.

The remainder of the paper is organized as follows: Section II defines the general system model and the secrecy metrics used in the evaluation of the considered jamming technique. The secrecy scheme proposed in this manuscript is formulated in section III. A detailed mathematical analysis of the secrecy capacity of the suggested technique is provided in section IV. Section V presents the numerical and theoretical results used to assess the merit of the developed work. Finally, the main conclusions are outlined in section VI.

Notations: Boldface capital letters denote matrices and boldface lowercase letters denote column vectors. The norm of vector $\mathbf{a}$ is given by $\|\mathbf{a}\|$, being the cardinality of a random variable X defined as $|X|$. The probability mass function of the random variable X is defined as $p(X)$. The symbol $\Gamma(n)$ is the gamma function defined as $\Gamma(n) = (n-1)!$, while $\lfloor n \rfloor$ defines the highest integer lower than n. The set of all binary numbers of size n is defined as $\mathbb{B}^n$. The maximum value between 0 and n is defined as $[n]^+$.

II. SYSTEM MODEL AND EVALUATION METRICS

This section presents the system setup as well as the evaluation metrics used to assess the performance of the proposed secrecy scheme.

A. SYSTEM MODEL

In Fig. 1 is depicted the general model considered for the jamming scheme focused in this work. The following nodes compose the system: 'A' is the legitimate transmitter (Alice); 'B' is the legitimate receiver (Bob); and 'E' is the eavesdropper (Eve). We assume that 'A' and 'B' are single antenna terminals, being 'E' a multiple antenna node with N_E elements. In Fig. 1, signal d defines information data that 'A' pretends to exchange with 'B', $u(\theta_{BA})$ represents the jamming component used to protect information from 'E', h_{BA} and $\mathbf{h}_{EA}$ are the channel coefficients modeled by complex Gaussian random variables with zero mean and unitary variance, and finally n_B, $\mathbf{n}_E$ represents zero mean complex Gaussian noise with variance σ_B^2 and σ_E^2.

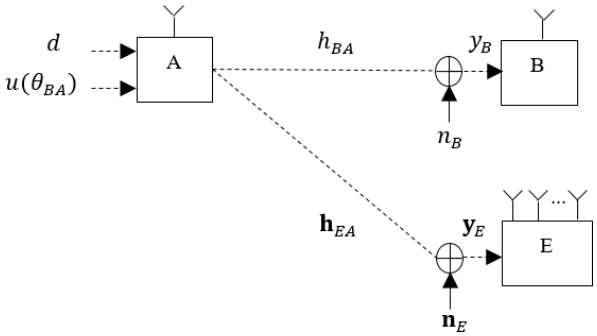


FIGURE 1. General system model.

Defining the transmitted signal at node 'A' by x_A, the received signals at 'B' and 'E' are formulated in (1) and (2) respectively,

$$y_B = h_{BA}x_A + n_B, \tag{1}$$

$$\mathbf{y}_E = \mathbf{h}_{EA}x_A + \mathbf{n}_E. \tag{2}$$

Furthermore, we consider TDD channel reciprocity and perfect channel estimations at 'A' and 'B', which are acquired through a bidirectional training process. Although we assume perfect channel estimations, in practice there are always some noise in the training channels that limits the amount of information that can be extracted. In the analytical derivations of the secrecy capacity we didn't considered the impact of practical channel estimation constraints. Additionally, we assume that 'E' is a passive terminal, and is not collocated with 'B', i.e., independence between h_{BA} and $\mathbf{h}_{EA}$ is verified. The assumption of a passive eavesdropper means that this node listens the communication and does not cause any intentional interference in the communication channel, making his presence and location uncertain to the legitimate transmitter. The transmitted power is constrained to $E[\|x_A\|^2] \leq P$. Ideal RF up- and down-conversion is also considered, with all the baseband processing applied to an independent flat fading channel realization.

B. EVALUATION METRIC

The secrecy metric used to assess the jamming scheme proposed in this work is the secrecy capacity C_s, which is given by,

$$C_s = [I(d; y_B) - I(d; \mathbf{y}_E)]^+ \tag{3}$$

where $I(d; y_B)$ is the mutual information between the source of information d and the signal observed at the legitimate receiver. The amount of information regarding the source that is extracted by the eavesdropper through the observation of signal, $\mathbf{y}_E$ is quantified in $I(d; \mathbf{y}_E)$. The mutual information terms in (3) can be defined as

$$I(d; y_B) = h(d) - h(d|y_B) \tag{4}$$

$$I(d; \mathbf{y}_E) = h(d) - h(d|\mathbf{y}_E) \tag{5}$$

where $h(d)$ is the entropy of the data source with $h(d|y_B)$ and $h(d|\mathbf{y}_E)$ being the equivocations at the legitimate terminal and at the eavesdropper, respectively.

III. PROPOSED JAMMING SCHEME

The main idea behind the secrecy scheme proposed in this work is to use the phase of the reciprocal wireless channel to define discrete jamming signals at 'A' and 'B'. After the selection of the jamming signals at 'A', information data is combined with the jamming component at the legitimate transmitter, being that component posteriorly canceled at 'B'. In the suggested scheme, M-QAM constellations are used in the definition of d as well for the jamming terms u_k that compose the jamming component $u(\theta_{BA})$ formulated in (7).

Taking into account the polar representation of the legitimate channel $h_{BA} = |h_{BA}|\, e^{j\theta_{BA}}$, the signal transmitted at 'A' is given by

$$x_A = d + u(\theta_{BA}), \tag{6}$$

with the jamming component formulated as the superposition of the N jamming signals $u_k, k = 1, \ldots, N$ as follows

$$u(\theta_{BA}) = \sum_{k=1}^{N} u_k. \tag{7}$$

Additionally, we consider that the power constraint P is equally divided between d and each jamming term u_k in (7), i.e. to each jamming term in (7) and to d is assigned $P/(N+1)$.

While d is selected uniformly from a single square M-QAM constellation, the jamming component $u(\theta_{BA})$ is generated combining N square M-QAM constellations taking into account the phase θ_{BA} of the reciprocal channel. For a single antenna at node 'A', the amount of information that must be extracted from the channel phase θ_{BA} in order to define $u(\theta_{BA})$ is equal to $\log_2(M^N)$ bits, where each group $b_k \in \mathbb{B}^{\log_2 M}$, $k = 1, 2, \ldots, N$ of $\log_2(M)$ bits is a random variable used to select randomly the specific constellation point for a single u_k, $k = 1, 2, \ldots, N$. Defining the M-QAM constellation set as $Q = \{\, q_0\ q_1\ \ldots.\ q_{M-1}\,\}$, the discrete jamming points are given by $u_k = q_{j_k}$, where $j_k = f(b_k)$ is computed using a bijective function defined as $f : \mathbb{B}^{\log_2 M} \mapsto Q$, i.e. f makes a one-to-one mapping between the binary words in $\mathbb{B}^{\log_2 M}$ and the constellation points in Q.

In order to allow an easier understanding regarding the mapping process between θ_{BA} and the construction of $u(\theta_{BA})$, let's consider the case where $N = 2$ and $M = 4$, i.e. $u(\theta_{BA}) = u_1 + u_2$ with u_1, u_2 selected independently and uniformly from a 4-QAM set defined as $Q = \{\, q_0\ q_1\ q_2\ q_3\,\}$. Since $N = 2$ and $M = 4$, the amount of information that we have to extract from the channel to define $u(\theta_{BA})$ is equal to $\log_2(4^2) = 4$ bits, i.e. sixteen different combinations of u_1, u_2 must be indexed by the channel phase. Therefore, as depicted in Fig. 2, what we do is divide the phase range of θ_{BA} in sixteen equal size slices, being each slice used to index a specific pair u_1, u_2. The numbers in the inner part of Fig. 2 are the indexes of the symbols in Q that will define the pair u_1, u_2, while the respective binary representations are defined in the outer part. For instance, suppose that in a given realization of the channel $0 \leq \theta_{BA} < \pi/8$, in this case $u_1 = q_0$ and $u_2 = q_3$.

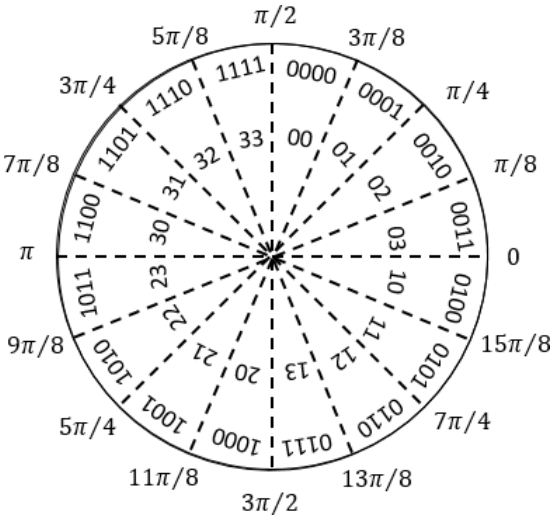


FIGURE 2. Mapping between the channel phase θ_{BA} and $u(\theta_{BA})$ considering the case of $N = 2$ and $M = 4$.

Since θ_{BA} is uniformly distributed, and the phase range of θ_{BA} is equally divided, the symbols u_1, u_2 are independent of each other. For instance, if the first selected symbol is $u_1 = q_0$, then the conditional probability for u_2 assuming that $u_1 = q_0$, is $p(q_0|q_0) = p(q_1|q_0) = p(q_2|q_0) = p(q_3|q_0)$.

After the legitimate transmitter computes $u(\theta_{BA})$, the signals received at 'B' and 'E' are given by,

$$y_B = h_{BA}\left[d + \sum_{k=1}^{N} u_k\right] + n_B, \tag{8}$$

$$\mathbf{y}_E = \mathbf{h}_{EA}\left[d + \sum_{k=1}^{N} u_k\right] + \mathbf{n}_E. \tag{9}$$

One of the targets of this work is to analyze the amount of information that 'B' and 'E' can obtain from the observation of (8) and (9), respectively. Considering that node 'B' has access to h_{BA}, N and M, the amount of uncertainty created by $u(\theta_{BA})$ can be fully eliminated at 'B'. In the case of node 'E', information regarding $\mathbf{h}_{EA}$, N and M is not enough to eliminate the equivocation generated by the jamming component. In order quantify the secrecy level of the proposed jamming scheme, the mathematical derivation of the theoretical secrecy capacity is described in section IV.

IV. ANALYSIS OF SECRECY CAPACITY

The purpose of this section is to compute analytically the secrecy capacity of the jamming scheme described in section III. The analytical evaluation is done for general M and N parameters considering both the noiseless and noisy channel cases.

A. NOISELESS CHANNEL

In this first scenario it is assumed that the noise variance at the legitimate receiver as well at the eavesdropper is zero, i.e. $\sigma_B^2 = 0$ and $\sigma_E^2 = 0$, respectively.

1) CLOSED FORM FORMULATION FOR GENERAL N AND M

In order to compute the secrecy capacity formulated in (3), we will start by deriving the individual channel capacities at 'B' and 'E' using the expressions defined in (4), (5), (8) and (9). In the case of the legitimate channel capacity, the amount of information extracted by 'B' from the observation of y_B is,

$$\begin{aligned} I\left(d; y_B, h_{BA}\right) &= h(d) - h\left(d|y_B, h_{BA}\right) \\ &= log_2(M) - h\left(d|h_{BA}\left[d + \sum_{k=1}^{N} u_k\right], h_{BA}\right) \\ &= \log_2(M)\ bits\,. \end{aligned} \tag{10}$$

Note that the knowledge of h_{BA}, N and M at node 'B' allows the legitimate receiver to compute $u(\theta_{BA})$, therefore the level of equivocation at 'B' due to the jamming component is equal to

$$\begin{aligned} h\left(d|h_{BA}\left[d + \sum_{k=1}^{N} u_k\right], h_{BA}\right) &= h\left(d|d\right) \\ &= 0\ bits\,, \end{aligned} \tag{11}$$

resulting in a legitimate channel capacity of $\log_2(M)$ bits.

Regarding the capacity of the eavesdropper, since the jamming component $u(\theta_{BA})$ is aligned in the same signal dimension of d, it is impossible for the eavesdropper separate $u(\theta_{BA})$ from d, even considering $N_E \to \infty$, i.e. unlimited number of antennas at Eve. Therefore, assuming that $\mathbf{h}_{EA}$, N and M is the only information available at 'E', the eavesdropper channel capacity is formulated as

$$\begin{aligned} I(d; \mathbf{y}_E) &= h(\mathbf{y}_E) - h(\mathbf{y}_E|d) \\ &= h\left(\mathbf{h}_{EA}\left[d + \sum_{k=1}^{N} u_k\right]\right) - h\left(\mathbf{h}_{EA}\left[d + \sum_{k=1}^{N} u_k\right]|d\right) \\ &= h\left(d + \sum_{k=1}^{N} u_k\right) - h\left(d + \sum_{k=1}^{N} u_k|d\right) \\ &= h\left(d + \sum_{k=1}^{N} u_k\right) - h\left(\sum_{k=1}^{N} u_k\right). \end{aligned} \tag{12}$$

Because of the independent relation between the imaginary and real parts of a square M-QAM constellation, the amount of information contained in this type of modulation is equally divided by the real and imaginary components. As derived in (13), the capacity of the eavesdropper channel can be computed using just the real part of the signal observed at 'E'.

$$\begin{aligned} I(d; \mathbf{y}_E) &= h\left(d + \sum_{k=1}^{N} u_k\right) - h\left(\sum_{k=1}^{N} u_k\right) \\ &= h\left(\Re\left\{d + \sum_{k=1}^{N} u_k\right\}\right) - h\left(\Re\left\{\sum_{k=1}^{N} u_k\right\}\right) \\ &\quad + h\left(\Im\left\{d + \sum_{k=1}^{N} u_k\right\}\right) - h\left(\Im\left\{\sum_{k=1}^{N} u_k\right\}\right) \\ &= 2 \times \left[h\left(\Re\left\{d\right\} + \sum_{k=1}^{N} \Re\left\{u_k\right\}\right) - h\left(\sum_{k=1}^{N} \Re\left\{u_k\right\}\right)\right] \end{aligned} \tag{13}$$

Since the real part of a square M-QAM constellation is defined as an L-PAM signal with $M = L^2$, the computation of the eavesdropper channel capacity reduces to the calculation of the entropy of the summation of several independent uniformly distributed L-PAM signals. Considering the discrete entropy formulation, and defining the random variables Z_{N+1} and Z_N as in (14) and (15),

$$Z_{N+1} = \Re\left\{d\right\} + \sum_{k=1}^{N} \Re\left\{u_k\right\} \tag{14}$$

$$Z_N = \sum_{k=1}^{N} \Re\left\{u_k\right\} \tag{15}$$

the capacity of the eavesdropper channel can be simplified as follows in (16).

$$\begin{aligned} I(d, \mathbf{y}_E) = 2 \times \sum_{z_N} p(z_N) \log_2 p(z_N) \\ -2 \times \sum_{z_{N+1}} p(z_{N+1}) \log_2 p(z_{N+1}) \end{aligned} \tag{16}$$

Taking into account the fact that Z_{N+1} and Z_N are generated as a sum of $N+1$ and N uniformly distributed L-PAM random variables respectively, the next step required to calculate $I(d, \mathbf{y}_E)$ is to compute the probability mass function (pmf) of Z_{N+1} and Z_N for general number of jamming terms N and constellation order L. According to [29], the pmf of the sum of n independent random variables with discrete uniform distribution over a set of equally spaced points with cardinality L can be computed using the coefficients of the polynomial expansion of (17), which are referred as the multinomial coefficients.

$$g(x) = \left(\sum_{\alpha=0}^{L-1} x^{\alpha}\right)^{n} \tag{17}$$

Therefore, using the results in [29], the probability distributions of (14) and (15) can be computed applying the general pmf formulation defined in (18) considering $q_n \in \{0, 1, \ldots, n(L-1)\}$.

$$p(q_n) = \frac{n}{L^n}\left(\sum_{p=0}^{\lfloor q_n/L \rfloor} \frac{\Gamma(1+n+q_n-pL)(-1)^p}{\Gamma(p+1)\Gamma(2+n-p)\Gamma(q_n-pL+1)}\right) \tag{18}$$

$$
\begin{aligned}
&I(d,\mathbf{y}_E)\\
&= 2\sum_{q_N=0}^{N(L-1)}\left[\frac{N}{L^N}\left(\sum_{p=0}^{\lfloor q_N/L\rfloor}\frac{\Gamma(N+q_N-pL)(-1)^p}{\Gamma(p+1)\Gamma(1+N-p)\Gamma(q_N-pL+1)}\right)\log_2\left(\frac{N}{L^N}\sum_{p=0}^{\lfloor q_N/L\rfloor}\frac{\Gamma(N+q_N-pL)(-1)^p}{\Gamma(p+1)\Gamma(1+N-p)\Gamma(q_N-pL+1)}\right)\right]\\
&\quad -2\sum_{q_{N+1}=0}^{(N+1)(L-1)}\left[\frac{N+1}{L^{N+1}}\left(\sum_{p=0}^{\lfloor q_{N+1}/L\rfloor}\frac{\Gamma(1+N+q_{N+1}-pL)(-1)^p}{\Gamma(p+1)\Gamma(2+N-p)\Gamma(q_{N+1}-pL+1)}\right)\right.\\
&\quad \left.\times\log_2\left(\frac{N+1}{L^{N+1}}\sum_{p=0}^{\lfloor q_{N+1}/L\rfloor}\frac{\Gamma(1+N+q_{N+1}-pL)(-1)^p}{\Gamma(p+1)\Gamma(2+N-p)\Gamma(q_{N+1}-pL+1)}\right)\right]
\end{aligned}
\tag{19}
$$

Replacing in (18) the n parameter by $N+1$ and N, the probability distributions of (14) and (15) can be obtained. Additionally, using the resulting probability distributions of (14) and (15) into (16), a closed formulation for the eavesdropper channel capacity is computed in (19), as shown at the top of this page. Finally, applying (10) and (19) to (3), the closed formulation for the secrecy capacity of the proposed jamming scheme is obtained for general N and M parameters.

2) ASYMPTOTIC SECRECY CAPACITY FOR 4-QAM MODULATION

The purpose of this point is to make an asymptotic analysis for $N\to\infty$ of the secrecy capacity of the scheme described in section III considering 4-QAM signals, i.e. $L=\sqrt{4}=2$. In this case, the pmf's of Z_{N+1} and Z_N follow a binomial distribution. The analysis of the asymptotic behavior is done using the *DeMoivre-Laplace Theorem* formulated in *Theorem 1*.

Theorem 1 (DeMoivre-Laplace Theorem [30]): When $N\to\infty$ with p fixed, considering $p+q=1$ conditioned to $p,q>0$. Then, for k in the $\sqrt{Npq}$ neighborhood of Np, we can approximate

$$
\binom{N}{k}p^k q^{N-k}\simeq\frac{1}{\sqrt{2\pi Npq}}\exp\left[\frac{-(k-Np)^2}{2Npq}\right]. \tag{20}
$$

This theorem states that a binomial distribution can be approximated by a normal distribution with mean Np and variance Npq assuming that $N\to\infty$ and $p,q>0$. Therefore, using the normal distribution approximation defined in *Theorem 1*, the normalized capacity of the eavesdropper channel for $N\to\infty$ and $L=2$ is derived in (21) applying the already known formulation of the entropy of a normal distribution.

$$
\begin{aligned}
&\lim_{N\to\infty}\frac{I(d,\mathbf{y}_E)}{\log_2(4)}\\
&=\lim_{N\to\infty}\left[h(z_{N+1})-h(z_N)\right]\\
&=\frac{1}{2}\times\lim_{N\to\infty}\left(\log_2\left[2\pi e(N+1)pq\right]-\log_2\left[2\pi eNpq\right]\right)\\
&=\frac{1}{2}\times\lim_{N\to\infty}\left(\log_2\left[2\pi e\left(\frac{N+1}{4}\right)\right]-\log_2\left[2\pi e\frac{N}{4}\right]\right)\\
&=\frac{1}{2}\times\lim_{N\to\infty}\left[\log_2\left(\frac{N+1}{N}\right)\right]\le\frac{1}{2N}\\
&=0\ \textit{bits}
\end{aligned}
\tag{21}
$$

Finally, through (21) is possible to conclude that for $L=2$ and $N\to\infty$, the leakage of information at the eavesdropper tends to zero, making the secrecy capacity equal to the capacity of the legitimate channel, i.e. $\log_2(M)$ bits.

3) ASYMPTOTIC SECRECY CAPACITY FOR N = 1

In this case, the objective is to demonstrate that the normalized secrecy capacity of the scheme in III tends to $\log_2(M)$ when $N=1$ and $M\to\infty$. Since the cardinality of $\Re\{d\}+\Re\{u_1\}$ is equal to $|\Re\{d\}+\Re\{u_1\}|=2L-1$, it follows that $h(\Re\{d\}+\Re\{u_1\})\le\log_2(2L-1)$ which leads to the upper bound (22) on the normalized capacity of the eavesdropper channel.

$$
\begin{aligned}
\frac{I(d,\mathbf{y}_E)}{\log_2(M)}&=\frac{h(d+u_1)-h(u_1)}{\log_2(M)}\\
&=2\times\frac{h(\Re\{d\}+\Re\{u_1\})-h(\Re\{u_1\})}{\log_2(L^2)}\\
&\le 2\times\frac{\log_2(2L-1)-\log_2(L)}{\log_2(L^2)}\\
&=\log_2\left(2-\frac{1}{L}\right)\times\frac{1}{\log_2(L)}
\end{aligned}
\tag{22}
$$

As demonstrated in (23), the limit of the upper bound in (22) for $L\to\infty$ is zero. This result allows to conclude that when the constellations order $M=L^2$ goes to infinite, the leakage of information at the eavesdropper is zero.

$$
\begin{aligned}
&\lim_{L\to\infty}\left[\log_2\left(2-\frac{1}{L}\right)\times\frac{1}{\log_2(L)}\right]\\
&=\lim_{L\to\infty}\left[\log_2\left(2-\frac{1}{L}\right)\right]\times\lim_{L\to\infty}\left[\frac{1}{\log_2(L)}\right]\\
&=0\ \textit{bits}
\end{aligned}
\tag{23}
$$

Once more, applying the result derived in (23) to expression (3), an asymptotic secrecy capacity of $\log_2(M)$ bits is achieved.

B. NOISY CHANNEL

In order to analyze the secrecy performance of the proposed jamming scheme in a more realistic scenario, a lower bound on the secrecy capacity is formulated in this sub-section considering receiver noise at 'B' and 'E'. The secrecy capacity bound is obtained by computing an upper bound on the eavesdropper channel capacity, as well as a lower bound on the legitimate channel capacity. Applying directly the *Data Processing Inequality Theorem* [31] to the capacity of the eavesdropper channel computed for the noiseless scenario, it is possible to conclude that the results in (19), (21) and (22) are upper bounds of the eavesdropper channel capacity. In regular words, the *Data Processing Inequality Theorem* states that the addition of independent random noise $\mathbf{n}_E$ at the eavesdropper, never increases the amount of information regarding d that node 'E' can extract from the observed signal $\mathbf{y}_E$.

At the legitimate receiver, a lower bound on the channel capacity is derived applying the *Fano's Inequality Theorem* formulated in *Theorem 2* [31]. The *Fano* inequality establishes a relation between the error probability P_e and the equivocation rate; therefore, computing P_e, an upper bound on $h(d|y_B)$ can be calculated.

Theorem 2 (Fano's Inequality) [31]: For any estimator $\hat{X}$ considering the Markov chain, $X \rightarrow Y \rightarrow \hat{X}$ with $P_e = P\{\hat{X} \neq X\}$, an upper bound on the equivocation is defined as

$$h\left(X|Y\right) \leq h\left(X|\hat{X}\right) \leq h(P_e) + P_e \log_2\left(|X| - 1\right) \quad (24)$$

with $h(P_e)$ being the binary entropy given by

$$h(P_e) = -P_e \log_2 P_e - (1 - P_e)\log_2(1 - P_e). \quad (25)$$

As considered in (13), the calculation of the legitimate channel capacity $I(d; y_B)$ for a square QAM signal d is done exploring the fact that an M-QAM constellation can be decomposed in two independent L-PAM constellations when $M = L^2$. Therefore, d is drawn uniformly from an L-PAM set in the following mathematical demonstration.

The first step to compute $h(d|y_B)$ will be to derive an analytical upper bound on the error probability P_e of the signal $\hat{y}_B$ estimated at the legitimate receiver. As formulated in (26), in the first phase of the estimation process at node 'B', perfect cancelation of $u(\theta_{BA})$ in y_B is done as follows

$$\begin{aligned} y_{B,c} &= y_B - h_{BA}u(\theta_{BA}) \\ &= h_{BA}d + n_B. \end{aligned} \quad (26)$$

After the cancelation of the jamming component, the estimated signal $\hat{y}_B$ is computed by equalizing $y_{B,c}$ with $u = e^{-j\theta_{BA}}$:

$$\begin{aligned} \hat{y}_B &= u y_{B,c} \\ &= |h_{BA}|\, d + e^{-j\theta_{BA}} n_B \\ &= |h_{BA}|\, d + \tilde{n}_B. \end{aligned} \quad (27)$$

Note that the noise distribution $\tilde{n}_B = e^{-j\theta_{BA}} n_B$ in (27) is the same of n_B; therefore, using (27) and defining $a = |h_{BA}|$ as a Rayleigh random variable and $d_{\min}$ as the minimal distance between the constellation points in d, an upper bound on the instantaneous error probability for a static realization of h_{BA} is obtained as follows

$$P_{e,awgn}\left(a\right) \leq \exp\left[\frac{-\left(d_{\min}a\right)^2}{8\sigma_B^2}\right]. \quad (28)$$

Then, averaging $P_{e,awgn}(a)$ over the probability distribution

$$p_{ray}(a) = \frac{a}{\sigma_r^2} \times \exp\left(-\frac{a^2}{2\sigma_r^2}\right) \quad (29)$$

of a Rayleigh random variable with fixed scale parameter σ_r^2, follows

$$\begin{aligned} P_E &= \int_0^{+\infty} P_{e,awgn}\left(a\right) \times p_{ray}\left(a\right) da \\ &= \int_0^{+\infty} \frac{a}{\sigma_r^2} \times \exp\left[-a^2 \times \left(\frac{d_{\min}^2}{8\sigma_B^2} + \frac{1}{2\sigma_r^2}\right)\right] da \\ &= \frac{4\sigma_B^2}{\sigma_r^2 d_{\min}^2 + 4\sigma_B^2}, \end{aligned} \quad (30)$$

which accordingly to (30) leads to the following upper bound on the error probability of (27)

$$P_e \leq \min\left(\frac{L-1}{L}; P_E\right). \quad (31)$$

Note that $d_{\min}$ can be increased changing the value of the transmit power P or the order L of the PAM constellation. The derivation of $d_{\min}$ as a function of L and P is formulated in [32] as

$$d_{\min} = \sqrt{\frac{12}{L^2 - 1} \times \left(\frac{P}{N + 1}\right)}. \quad (32)$$

Applying the result in (31) to (24), a lower bound on the legitimate channel capacity for a square M-QAM constellation with $M = L^2$, is obtained as follows

$$\begin{aligned} I(d; \hat{y}_B) &\geq 2 \times \left[h(d) - h(d|\hat{y}_B)\right] \\ &= 2 \times \log_2\left(L\right) - 2 \times \left[h_b\left(P_e\right) + P_e \log_2\left(|d| - 1\right)\right] \\ &= \log_2\left(M\right) - 2 \times \left[h_b\left(P_e\right) + P_e \log_2\left(L - 1\right)\right]. \end{aligned} \quad (33)$$

The analysis of (30)-(33) allows to conclude that for a fixed value of L and σ_B^2, the legitimate channel can reach the full capacity of $\log_2(M) = 2 \times \log_2(L)$ increasing P.

In order to ensure secrecy, the jamming component must be generated independently for each information data symbol transmitted, hence, in average the transmission of information is limited to the minimum rate at which we can get independent channel estimates multiplied by the number of bits that is possible to extract in each estimation. However, this kind of techniques, where the secrecy is fully supported by the randomness of the wireless channel, is targeted to secure small blocks of highly sensitive information.

Possible examples include the exchange of banking information like credit card numbers, predefined secret keys or any other sensitive information that requires perfect secrecy. In these cases, the legitimate nodes can store the reciprocal past channel estimates, and when some credit card number or other sensitive information needs to be transmitted, the legitimate terminals use the stored past channel estimates to send this information in secrecy. Then, the secured information can be sent at the rate(s) offered by the wireless communication system (e.g. 802.11, LTE).

V. RESULTS

This section presents the numerical and theoretical secrecy capacity results regarding the jamming scheme proposed in III. The capacity results in bits per channel use (Bpcu) are divided by $\log_2(|d|)$, with $|d|$ defining the cardinality of the information source, i.e. the presented results are normalized in interval [0,1]. Therefore, if the result is one, all the information from the source is obtained, however, if the result is zero, no information is extracted from the observed signal.

A. RESULTS FOR NOISELESS CHANNEL

In this first set of results, the secrecy performance for the noiseless scenario is evaluated considering just the eavesdropper channel capacity. Note that for $\sigma_B^2 = 0$, the capacity of the legitimate channel is always equal to $I(d, y_B) = \log_2(M)$ bits; therefore, under these conditions the secrecy level can be assessed analyzing just the eavesdropper channel capacity.

The simulated and theoretical results depicted in Fig. 3 consider N ranging from one to nine, with 4-QAM modulation for both d and u_k, $k = 1, 2, \ldots, N$. It is possible to check that when the jamming component $u(\theta_{BA})$ is formed by a single term, i.e. $N = 1$, the eavesdropper has access to half of the information exchanged between the legitimate parties. However, as shown in Fig. 3 and demonstrated in (21), the eavesdropper channel capacity tends to zero when the number of jamming terms N in $u(\theta_{BA})$ goes to infinite. Besides the exact eavesdropper channel capacity curves, in Fig. 3 is also depicted the theoretical approximation considered in (21), i.e. $0.5\log_2[(N+1)/N]$. As expected, when the value of N grows, the theoretical approximation converges to the exact capacity of the eavesdropper channel.

Instead of varying N for a fixed M, the curves in Fig. 4 expose the secrecy level of the proposed jamming scheme when a single term is used for the jamming component $u(\theta_{BA})$. As derived in (22) and (23), the curves in Fig. 4 confirm that increasing the order M of the square QAM constellations used for d and u_1, the secrecy level of the proposed secrecy technique tends asymptotically to $\log_2(M)$, i.e. the leakage of information at the eavesdropper goes to zero. The theoretical upper bound derived in (22) is also depicted in Fig. 4.

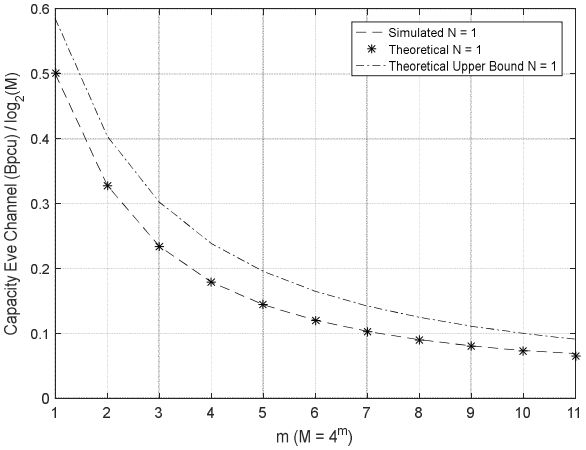


FIGURE 4. Eve capacity in noiseless channel for N = 1 and general M-QAM constellations for data and jamming components.

The results presented in Fig. 5 were acquired for $N \in \{1, 2, 5\}$ and $M = 4^m$, $m = \{1, 2, \ldots, 8\}$. As expected, for a fixed constellation order M, the level of equivocation at

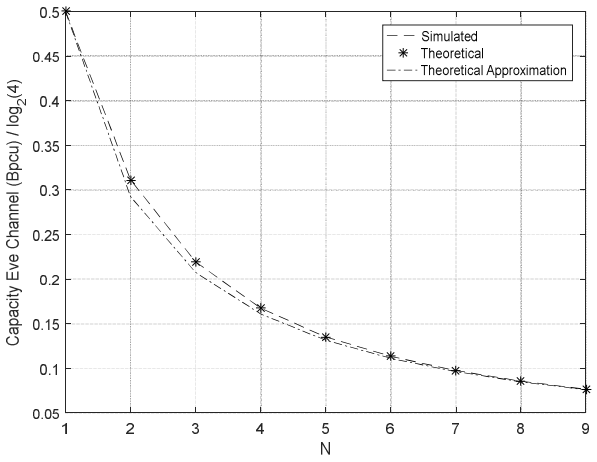


FIGURE 3. Eve capacity in noiseless channel for general *N* and 4-QAM constellations for data and jamming components.

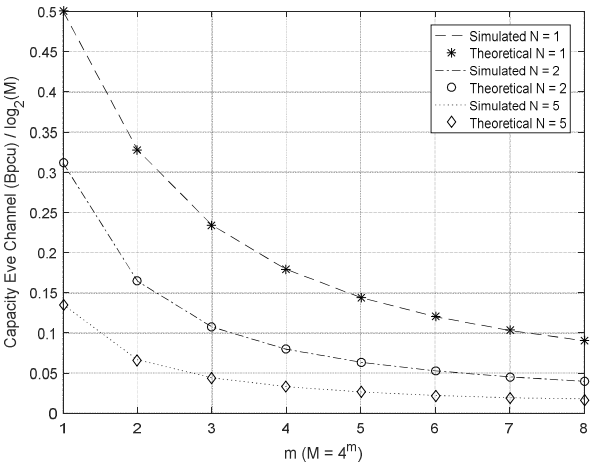


FIGURE 5. Eve capacity in noiseless channel for $N = \{1, 2, 5\}$ and general M-QAM constellation for data and jamming components.

the eavesdropper increases for a larger number of jamming terms N in the jamming component $u(\theta_{BA})$. In Fig. 6, the capacity of the eavesdropper channel was assessed as a function of the number of bits extracted from the channel assuming two different parameter configurations for the jamming component in (7), which are: variable N with $M = 4$ fixed; and $N = 1$ fixed with variable M. Observing the curves in Fig. 6 is possible to conclude that for the same number of bits extracted from the channel, the level of secrecy is larger in the case of $M = 4$ fixed and N variable. In other words, the capacity of the eavesdropper channel is lower when the channel-extracted bits are used to increase the number of 4-QAM jamming terms instead of used to increase the constellation order M when a single jamming term is considered. In summary, the three main conclusions obtained from this first evaluation are: the proposed scheme achieves asymptotically a full secrecy capacity; the theoretical derivations for the secrecy capacity confirm the simulated results; and for the same number of bits extracted from the channel, increasing the number of jamming terms N in (7) allows to reach higher secrecy capacity.

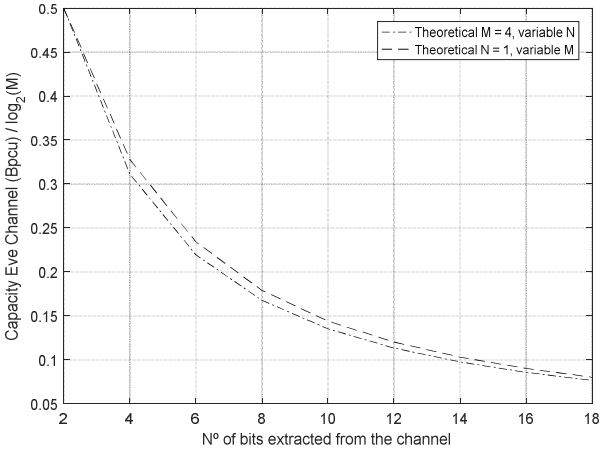


FIGURE 6. Capacity Eve channel for $N = 1$ and $M = 4$ in function of the number of bits extracted from the channel.

B. RESULTS FOR NOISY CHANNEL

In the noisy channel scenario, a lower bound on the secrecy level is obtained computing an upper bound on the eavesdropper channel capacity, and a lower bound in the case of the legitimate channel capacity. The evaluation of the secrecy capacity lower bound regarding the jamming scheme proposed in this work is depicted in Fig. 7 for $N = 9$ and $M \in \{4, 16, 64\}$. The simulated results were acquired using the *Fano's Inequality Theorem* considering a maximum likelihood (ML) equalizer to compute the probability of error of the estimated signal in (27).

In the case of the theoretical results, the derivations in (30) and (31) were directly used in theorem 2. The results in Fig. 7 show that in the high SNR regime, for fixed $N = 9$ and $M = 64$, the secrecy capacity lower bound is pretty close of the full secrecy capacity. Another important observation is related to the fact that when the value of M grows, an increase

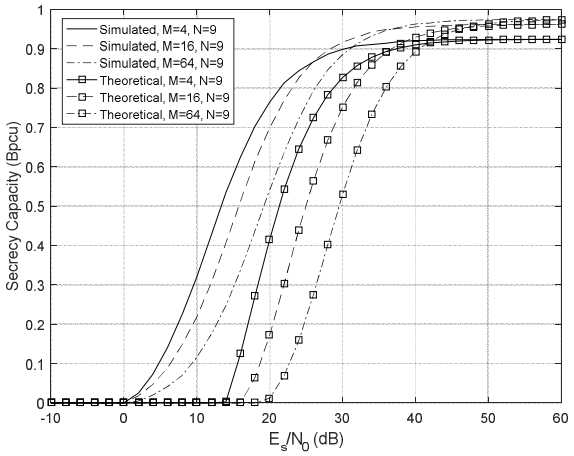


FIGURE 7. Lower bound on secrecy capacity for noisy channel considering $N = 9$ and $M = \{4, 16, 64\}$.

on the SNR conditions must be verified in order to maintain the same level of secrecy. Note that in the high SNR regime a full capacity of $\log_2(M)$ is always achieved for the legitimate channel, therefore, the secrecy capacity will depend on the capacity of the eavesdropper channel, which in turn is a function of N and M. As shown in (21) and (23), when N or M increase, the capacity of the eavesdropper channel tends to zero. This means that in the high SNR regime for large N or M, full secrecy capacity is asymptotical achieved. The difference between the simulated and theoretical results is explained by the fact that while in the simulated results the error probability was computed numerically using a Monte Carlo integration method, in the case of the theoretical results the upper bound (31) was considered for the error probability. Nevertheless, the asymptotical behavior of the simulated and theoretical results is identical, i.e. both show that full secrecy is reached in the high SNR regime increasing M or N.

VI. CONCLUSION

In this work, we proposed a jamming scheme that exploits the reciprocal wireless channel with the aim to create equivocation at the eavesdropper without affecting the channel capacity of the legitimate receiver. We derived closed form solutions for the secrecy capacity and proved through an asymptotic analysis that in the high power regime the proposed scheme achieves full secrecy capacity independently of the number of antennas at the eavesdropper. Additionally, the study of the secrecy level provided by different configurations of the jamming component allowed to conclude that for the same number of bits extracted from the channel, increasing the number of low cardinality jamming terms in the jamming component allows to reach higher secrecy capacity than using a single jamming term with increased cardinality.

ACKNOWLEDGMENT

This work was presented in part at the Wireless Days Conference in 2017.

REFERENCES

[1] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[2] M. Atallah, G. Kaddoum, and L. Kong, "A survey on cooperative jamming applied to physical layer security," in *Proc. IEEE Int. Conf. Ubiquitous Wireless Broadband (ICUWB)*, Montreal, QC, Canada, Oct. 2015, pp. 1–5.

[3] B. Schneier, "Cryptographic design vulnerabilities," *Computer*, vol. 31, no. 9, pp. 29–33, Sep. 1998.

[4] M. Sandirigama and R. Idamekorala, "Security weaknesses of WEP protocol IEEE 802.11b and enhancing the security with dynamic keys," in *Proc. IEEE Toronto Int. Conf. Sci. Technol. Humanity (TIC-STH)*, Toronto, ON, Canada, Sep. 2009, pp. 433–438.

[5] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 2014.

[6] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[7] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[8] S. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

[9] M. Bloch, M. Hayashi, and A. Thangaraj, "Error-control coding for physical-layer secrecy," *Proc. IEEE*, vol. 103, no. 10, pp. 1725–1746, Oct. 2015.

[10] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, "Coding for secrecy: An overview of error-control coding techniques for physical-layer security," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 41–50, Sep. 2013.

[11] D. Sarmento, J. P. Vilela, W. K. Harrison, and M. Gomes, "Interleaved coding for secrecy with a hidden key," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, San Diego, CA, USA, Dec. 2015, pp. 1–6.

[12] J. P. Vilela, M. Gomes, W. K. Harrison, D. Sarmento, and F. Dias, "Interleaved concatenated coding for secrecy in the finite blocklength regime," *IEEE Signal Process. Lett.*, vol. 23, no. 3, pp. 356–360, Mar. 2016.

[13] V. R. Cadambe and S. A. Jafar, "Interference alignment and degrees of freedom of the K-user interference channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3425–3441, Aug. 2008.

[14] D. Castanheira, A. Silva, and A. Gameiro, "Retrospective interference alignment: Degrees of freedom scaling with distributed transmitters," *IEEE Trans. Inf. Theory*, vol. 63, no. 3, pp. 1721–1730, Mar. 2017.

[15] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[16] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Apr. 2009, pp. 2437–2440.

[17] J. Wang and A. Lee Swindlehurst, "Cooperative jamming in MIMO ad-hoc networks," in *Proc. Conf. Rec. 43rd Asilomar Conf. Signals, Syst. Comput.*, Nov. 2009, pp. 1719–1723.

[18] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 256–266, Jun. 2011.

[19] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[20] J. Yang, I.-M. Kim, and D. I. Kim, "Optimal cooperative jamming for multiuser broadcast channel with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2840–2852, Jun. 2013.

[21] J. Xie and S. Ulukus, "Secure degrees of freedom of the Gaussian wiretap channel with helpers and no eavesdropper CSI: Blind cooperative jamming," in *Proc. 47th Annu. Conf. Inf. Sci. Syst.*, Baltimore, MD, USA, Mar. 2013, pp. 1–5.

[22] J. Xie and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks," *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3359–3378, Jun. 2014.

[23] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[24] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4766–4781, Sep. 2014.

[25] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Commun.*, vol. 18, no. 4, pp. 6–12, Aug. 2011.

[26] Q. Wang, K. Xu, and K. Ren, "Cooperative secret key generation from phase estimation in narrowband fading channels," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 9, pp. 1666–1674, Oct. 2012.

[27] G. Anjos, D. Castanheira, A. Silva, and A. Gameiro, "Exploiting reciprocal channel estimations for jamming to secure wireless communications," in *Proc. Wireless Days*, Mar. 2017, pp. 136–142.

[28] B. Chen, C. Zhu, W. Li, J. Wei, V. C. M. Leung, and L. T. Yang, "Original symbol phase rotated secure transmission against powerful massive MIMO eavesdropper," *IEEE Access*, vol. 4, pp. 3016–3025, 2016.

[29] C. C. S. Caiado and P. N. Rathie, "Polynomial coefficients and distribution of the sum of discrete uniform variables," in *Proc. 8th Annu. Conf. Soc. Special Functions Appl.*, Pala, India, 2007, pp. 1–13.

[30] A. Papoulis and S. Pillai, *Probability—Random Variables and Stochastic Processes*. New York, NY, USA: McGraw-Hill, 2002.

[31] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Hoboken, NJ, USA: Wiley, 2006.

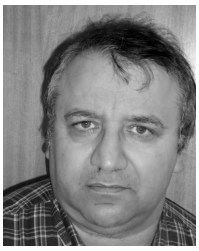
[32] J. G. Proakis and M. Salehi, *Digital Communications*. New York, NY, USA: McGraw-Hill, 2008.

[33] W. Stallings, *Cryptography and Network Security: Principles and Practice*. New York, NY, USA: Prentice-Hall, 2006, pp. 266–291.

GUSTAVO ANJOS received the M.Sc. degree in electronics and telecommunications engineering from the University of Aveiro, Aveiro, Portugal, in 2013, where he is currently pursuing the Ph.D. degree in electrical engineering with the Instituto de Telecomunicações. He was with the Instituto de Telecomunicações, where he developed research work in Flexicell Project–Development of a Multimode/Multiband Remote Radio Header under the context of Cloud–Radio Access Network architecture. His current research interests are focused on physical layer security for wireless communications systems.

DANIEL CASTANHEIRA received the Licenciatura degree (ISCED level 5) and Ph.D. degree in electronics and telecommunications from the University of Aveiro in 2007 and 2012, respectively. In 2011, he joined the Departamento de Eletrónica, Telecomunicações e Informática, Aveiro University, as an Assistant Professor. He is currently an Auxiliary Researcher with the Instituto the Telecomunicações, Aveiro, Portugal. He is involved in several national and European projects, namely, RETIOT, SWING2, PURE-5GNET, HETCOP, COPWIN, PHOTON, within the FCT Portuguese National Scientific Foundation, and CODIV, FUTON, and QOSMOS with the FP7 ICT. His research interests lie in signal processing techniques for digital communications, with emphasis for physical layer issues including channel coding, precoding/equalization, and interference cancelation.

ADÃO SILVA received the M.Sc. and Ph.D. degrees in electronics and telecommunications from the University of Aveiro, in 2002 and 2007, respectively. He is currently an Assistant Professor with the Department of Electronics, Telecommunications and Informatics, University of Aveiro, and a Senior Researcher with the Instituto de Telecomunicações. He participates in several national and European projects, namely, the ASILUM, MATRICE, 4MORE within the ICT Program, and the FUTON and CODIV projects with the FP7 ICT. He has led several research projects, in the broadband wireless communications area, at the national level. His interests include multiuser multi-in multi-out (MIMO), multicarrier-based systems, cooperative networks, precoding, multiuser detection, massive MIMO, and millimeter-wave communications. He was a TPC Member of several international conferences.



ATÍLIO GAMEIRO received the Licenciatura and Ph.D. degrees from the University of Aveiro, Aveiro, in 1985 and 1993, respectively. He is currently an Associate Professor with the Department of Electronics and Telecommunications, University of Aveiro, and a Researcher with the Instituto de Telecomunicações, where he is the Head of the Mobile Networks Group. His industrial experience includes a period of one year with BT Labs and one year with NKT Elektronik. He has authored over 200 technical papers in international journals and conferences. His main interests lie in signal processing techniques for digital communications and communication protocols, and within this research line, he has done work for optical and mobile communications, either at the theoretical or experimental level. His current research activities involve space-time-frequency algorithms for the broadband wireless systems and cross-layer design. He involved and led IT or University of Aveiro participation on more than 20 national and European projects.

MARCO GOMES (S'07–M'11) was born in Coimbra, Portugal, in 1977. He received the M.Sc. and Ph.D. degrees in electrical and computer engineering with specialization in telecommunications from the University of Coimbra in 2004 and 2011, respectively. He is currently an Assistant Professor with the Department of Electrical and Computer Engineering, Faculty of Science and Technology of the University of Coimbra. He is also a Researcher with the Instituto de Telecomunicações and performs different collaborations under his research and development activities with other institutions and universities worldwide. His main research interests include wireless digital communications, general signal processing for communications and ultrasound systems, error control coding and physical layer security, electronics and SDRs, FPGAs, and DSPs. He is a member of the IEEE Communications Society and the IEEE Vehicular Technology Society.

JOÃO P. VILELA is an assistant professor at the Department of Informatics Engineering of the University of Coimbra. He received a Ph.D. in Computer Science from the University of Porto in 2011, period during which we was a visiting researcher at Georgia Tech and MIT (USA) working on wireless physical-layer security and security for network coding. In recent years, Dr. Vilela has been coordinator and team member of several national, bilateral, and European-funded projects in security and privacy. His main research interests are in security and privacy of computer and communication systems, with focus on wireless networks, cloud computing and mobile devices. Other research interests include anticipatory networks and intelligent transportation systems.