Hindawi
Security and Communication Networks
Volume 2018, Article ID 9065856, 13 pages
https://doi.org/10.1155/2018/9065856

Research Article

Optimal Improper Gaussian Signaling for Physical Layer Security in Cognitive Radio Networks

Guilherme Oliveira,[1] **Evelio Fernández**,[1] **Samuel Mafra**,[2] **Samuel Montejo-Sánchez**,[3] **and César Azurdia-Meza**[4]

[1] *The Federal University of Paraná (UFPR), Curitiba, PR, Brazil*
[2] *The National Institute of Telecommunications (Inatel), Santa Rita do Sapucaí, MG, Brazil*
[3] *Programa Institucional de Fomento a la I+D+i, Universidad Tecnológica Metropolitana, Santiago, Chile*
[4] *The Universidad de Chile, Santiago, Chile*

Correspondence should be addressed to Guilherme Oliveira; gui.schunemann@gmail.com

Received 27 July 2018; Revised 14 November 2018; Accepted 10 December 2018; Published 25 December 2018

Guest Editor: Nurul H. Mahmood

The next generations of wireless communications are expected to have great demand for security and spectrum efficiency, and the current secrecy solutions may not be enough. In this paper we propose an optimization framework to address the physical layer security in cognitive radio networks when the secondary users employ improper Gaussian signaling. We resort to genetic algorithms to find optimal values of the secondary transmit power and the degree of impropriety, simultaneously. Then, two different problems regarding the system performance are solved: minimizing the secrecy outage probability and maximizing the secondary achievable rate. In both problems we evaluate, besides the secrecy outage probability, the effective secure throughput and the secure energy efficiency of the system as well. The results show that the secondary network using improper signaling outperforms conventional proper signaling in terms of secrecy outage probability and the effective secure throughput, while in terms of the secure energy efficiency, adopting proper signals attains better performance than improper ones.

1. Introduction

Cognitive radio (CR) is a key-technology to promote a more efficient spectrum usage, since it is an intelligent system capable of learning from its external environment and adapting its operating parameters to the channel conditions. In the underlay CR paradigm the unlicensed users, or secondary users (SUs), are allowed to share the same frequency band of licensed users, or primary users (PUs), provided that the interference caused at the PUs does not exceed a predefined threshold [1].

Despite the advantages that can be reaped by CR networks in terms of spectrum sharing, the inherent broadcast nature of the wireless media coupled with the opening of the licensed spectrum to cognitive users facilitates malicious attacks on the legitimate channels, such as eavesdropping [2]. Hence, to make CR a feasible solution to the growing demand for frequency spectrum, it is imperative that these networks can provide not only high rate and error free transmissions, but also secure exchange of messages between devices.

Traditionally, the security of communications networks is obtained through data cryptography and key-distribution techniques at higher layers [2]. Nonetheless, every day more features (such as Internet banking through smart phones, auto-driven vehicles, sensor networks, and the Internet of things) are being performed through wireless and mobile access. Thus, next generation systems require even more secrecy capacity, and these traditional security techniques may not be enough.

Although these techniques have shown their applicability and efficiency, they demand high computational costs, which is a limiting factor to some devices/gadgets. In addition, the broadcast nature of wireless channels allows relatively easy access to encrypted data, which favors malicious attacks using

brute computational force. For this reason, physical layer security (PLS) has been proposed as a complement to other higher layer security techniques that might also be used. PLS is based on the concept of information-theoretic perfect secrecy, whose goal is to guarantee higher mutual information in the legitimate links (SU⟷SU or PU⟷PU), in comparison to that of the eavesdropper link [2, 3].

Usually, diversity techniques such as using auxiliary nodes to aid in the transmission (cooperative diversity) [4] or furnishing legitimate nodes with multiple antennas (antenna diversity) [5, 6] have been employed to enhance the security of CR wireless systems. Additionally, other techniques, such as beam-forming [7], artificial noise [8], and error control coding [9, 10] are also able to improve these systems secrecy performance.

A comprehensive review regarding PLS for CR networks can be found in [2] and in references therein. The main point is that most existing PLS techniques attempt to improve the legitimate channels quality in comparison to the eavesdropper channel, that is to say, achieving better transmission rates between legitimate users while maintaining the interference caused at the PUs below an acceptable threshold.

1.1. Related Works. Recently, improper Gaussian signaling (IGS) has been used to improve the performance of systems subject to interference constraints regarding achieving higher transmission rates [11–15]. Differently from the proper Gaussian signaling (PGS), improper (or asymmetric) signals have their in-phase and quadrature components correlated or with uneven powers [16].

In these communications scenarios with interference constraints, sometimes referred to as the interference channel (IC), the benefits of employing IGS for secrecy reasons are related to those regarding the differential entropy of improper signals [16]. Knowing that the mutual information between two nodes in a network represents the amount of information shared between these two users, i.e., the achievable transmission rate [17], the premise of PLS is that if the legitimate channel has better condition than the eavesdropper channel, there is a transmission rate at which legitimate users can securely communicate.

Therefore, the secrecy performance when studying PLS is directly related to the achievable rates between a transmitter and a receiver. In this regard, it is well known that for some scenarios, such as the broadcast, the point-to-point, and the multiple access channels, adopting PGS achieves optimal performance when it comes to maximizing achievable rates [15, 16]. This is because proper signals attain maximum differential entropy and, therefore, higher achievable rates in the aforementioned scenarios.

Nonetheless, for the IC, which is the case of underlay CR networks, there is not a known optimal signal input alphabet yet, regarding maximum achievable rates. As a matter of fact, when interference is treated as noise, increasing the differential entropy of the interference reduces the transmission rate [16]. Hence, when a transmitter uses improper signals, which have lower differential entropy than proper ones [18], it is possible to increase the achievable rates for this transmitter and its receiver [11, 15, 19], due to the lower differential entropy of asymmetric signals.

Another interesting result regarding the secrecy performance of the IC when adopting IGS is that the transmitters who adopt improper signals may transmit with more power without exceeding the network interference constraint. That is to say, the interference caused by the improper signal is actually less harmful than that caused by proper signals. One can note that the interference can be the same, nonetheless improper signals can be aligned in such a way that the impact of interference on legitimate users is reduced [19].

Several works considering underlay CR networks have shown this behavior: in [12, 15], the authors report that the achievable rate of the SUs increases significantly when adopting IGS, but only when the gain of the interference channel surpasses a limit that depends on the rate achieved by the interfered user. In [13, 14] the outage performance of different CR network configurations is analyzed when the SU transmits with IGS: a single hop system and a system with in-band full-duplex nodes, respectively.

In addition, not only in underlay CR scenarios were these benefits of improper signals shown. For example, the interweave and overlay CR protocols were studied in [20, 21], respectively. In these works, it was shown that adopting IGS could enhance transmission rates and, consequently, achieve better performance when compared to proper signaling.

Moreover, the benefits of IGS regarding achieving higher transmission rates were also observed in noncognitive scenarios with interference. In [22], the performance of a full-duplex relay adopting IGS to alleviate its residual self-interference was examined; in [23], the authors proposed and assessed a system comprising an alternate relaying scheme in which IGS could be adopted by the transmitters. Nonetheless, differently from previously cited papers, our work focuses on the security benefits that stem from adopting IGS and mainly addresses the underlay CR paradigm.

In this regard, there is a trade-off between how much improper the signal will be and with how much power it will be transmitted [24]. Exploiting this trade-off to achieve higher rates for SUs, consequently improving the network secrecy performance, is the main idea of this work.

In [25], the usage of IGS in a scenario where underlay SUs are being eavesdropped was analyzed. A closed-form expression for the secrecy outage probability (SOP) when only statistical channel state information was available at the secondary transmitter was derived. Motivated by the results that showed that IGS can be beneficial for the SUs secrecy, in this paper we carry on the work presented in [25], aiming to optimize the secrecy performance of an underlay CR network when SUs are being eavesdropped and can employ IGS in their transmissions.

1.2. Contributions and Organization of the Paper. In this work we resort to optimization techniques in order to provide a design framework which optimizes system parameters while maintaining an acceptable quality of service (QoS) at the PUs.

Finding optimal expressions through classic differential optimization techniques is not trivial. Since the search space

Table 1: List of symbols.

Symbol	Description
P_a	Secondary transmit power
P_s	Primary transmit power
λ_{ij}	Average channel gain
α	Path loss exponent
R	Circular cell radius
δ_m	Fraction of the radius R
C_x	Degree of impropriety
$\mathcal{O}_s$	Secrecy outage probability
$\mathcal{T}_s$	Effective secure throughput
η_s	Secure energy efficiency

is not so well understood and is relatively unstructured and the expressions are highly nonlinear, we aim to find the best secrecy performance in the proposed system resorting to genetic algorithms (GAs) [26, 27]. In this fashion, the main contributions of our work are

(i) demonstrating the occurrence of optimal or suboptimal values of the SU transmit power and degree of impropriety, concurrently, and its impact on the secrecy performance of the system;

(ii) evaluating the secrecy performance in terms of the secrecy outage probability, the secure throughput, and the energy efficiency cost of the proposed transmission scheme on an underlay CR network when SUs can employ either PGS or IGS and are randomly distributed in a primary cell.

These are the first results regarding the secrecy performance optimization of CR networks when SUs may adopt IGS to the best of the authors' knowledge.

This paper is organized as follows. Section 2 presents the system model as well as basic concepts about IGS. In Section 3 the main secrecy performance metrics used to assess the PLS performance of the proposed system are analyzed. Section 4 briefly presents the proposed optimization problems and the algorithm used to solve it. Sections 5 and 6 show numerical results and concluding remarks, respectively. In addition, Table 1 shows the main symbols and variables used throughout the paper.

2. System Model

The proposed system comprises five nodes: a primary transmitter (Source, S), a primary receiver (Destination, D), a secondary transmitter (Alice, A), a secondary receiver (Bob, B), and an eavesdropper (Eve, E), which spies on secondary transmissions (A⟶B).

In addition, all nodes are single antenna and it is assumed that S only uses PGS, whereas A can employ either PGS or IGS. This assumption is made since in the underlay protocol there is no cooperation between PUs and SUs [12, 13].

Main and interference channels coefficients between transmitter i and receiver j are denoted by h_{ij} and g_{ij}, respectively. Here, $i \in \{a, s\}$, $j \in \{b, d, e\}$, and $\{s, d, a, b, e\}$ denote Source, Destination, Alice, Bob, and Eve, respectively. All channels experience quasi-static Rayleigh fading with equal block length and are independent.

Alice does not have full knowledge of all channel state information (CSI), since the perfect knowledge of other users is difficult to obtain in practice [28]. Hence, it is assumed that only statistical CSI (SCSI) is available at the SUs; i.e., Alice only knows the approximate location of other users in the network, as in the adaptive transmission scheme presented in [25], in the optimization framework [29], and in the cooperative scheme [30]. In other words, Alice is only aware of other channel gains' expected value, except that from its direct link to Bob, h_{ab}. The knowledge of other channels SCSI can be done by estimating their position in the network or from indirect feedback from band manager [31].

The average channel gains are given by $\lambda_{ij} = d_{ij}^{-\alpha}$, where d_{ij} is the distance between nodes and α is the path-loss exponent. Note that h_{ij} and g_{ij} depend on d_{ij}, according to the path-loss model previously stated.

The primary network coverage area is a circular cell of radius R, where S is located at the center of the cell, while D, A, and E are uniformly distributed within the primary coverage area and B is located randomly within a circular region around A. Consequently, the polar coordinates of A, B, D, and E can be generated as

$$r_m = \delta_m R \sqrt{\beta_{m_1}}, \qquad \Theta_m = 2\pi\beta_{m_2}, \tag{1}$$

where $m \in \{a, b, d, e\}$, r_m is the node distance from S (or A, in the case of B), Θ_m is the angle of the node coordinates, respectively, δ_m, with $0 \le \delta_m \le 1$, denotes a fraction of the radius R, and β_{m_1} and β_{m_2} are random numbers uniformly distributed in the real $[0, 1]$ interval. Figure 1 depicts a possible node distribution for the system topology.

Hence, in this scenario, the locations of the users are not arbitrarily defined. This is a more realistic assumption since mobile users, for example, may be at different positions in the network at a given time.

The received signals at D, B, and E at time t are expressed, respectively, by

$$y_d[t] = \sqrt{P_s} h_{sd} x_s[t] + \sqrt{P_a} g_{ad} x_a[t] + n_d[t], \tag{2}$$

$$y_b[t] = \sqrt{P_a} h_{ab} x_a[t] + \sqrt{P_s} g_{sb} x_s[t] + n_b[t], \tag{3}$$

$$y_e[t] = \sqrt{P_a} h_{ae} x_a[t] + \sqrt{P_s} g_{se} x_s[t] + n_e[t], \tag{4}$$

where P_s and P_a are the Source and Alice's transmit powers, respectively, $x_s[t]$ and $x_a[t]$ are the transmitted signals by S and A, respectively, and $n_d[t]$, $n_b[t]$ and $n_e[t]$ represent the additive white Gaussian noise (AWGN) at D, B, and E, respectively.

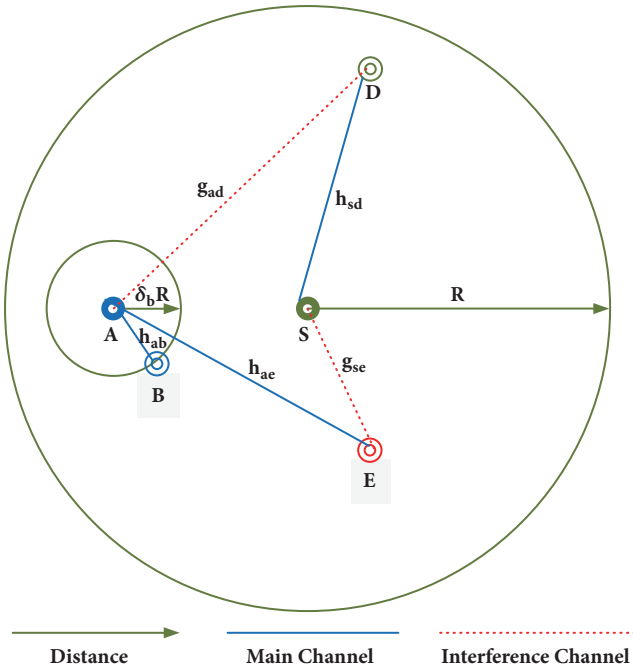

FIGURE 1: System model for an underlay CR network with eavesdropper.

Thus, when PGS is used, the signal-to-interference-plus-noise ratio (SINR) for each ij link can be written as

$$\gamma_{ij} = \frac{P_i \left|h_{ij}\right|^2}{P_k \left|g_{kj}\right|^2 + N_0}, \tag{5}$$

where $k \in \{a, s\} : k \neq i$.

Since IGS signals are statistically circularly asymmetric, the degree of impropriety of Alice's signal, $x_a[t]$, is measured by its circularity coefficient [18]

$$C_x = \frac{\left|\widetilde{\sigma}^2_{x_a}\right|}{\sigma^2_{x_a}}, \tag{6}$$

where $\sigma^2_{x_a} = \mathbb{E}[|x_a|^2]$ and $\widetilde{\sigma}^2_{x_a} = \mathbb{E}[x_a^2]$ are the variance and pseudo-variance of Alice's signal, respectively. Knowing that $0 \leq C_x \leq 1$, a signal is called proper if $C_x = 0$; otherwise, it is called improper [32].

Now, in order to express the mutual information between a transmitter employing IGS and a receiver, it is more convenient to separate the received signal from the interference-plus-noise terms at the receiver. In this work the analyses are normalized with respect to the bandwidth. Moreover, unitary bandwidth is considered; then, the achievable rates are expressed in bits/s/Hz.

Hence, when Alice adopts IGS and interference is considered as Gaussian noise, the circularity coefficients of the received signal and of the interference-plus-noise signal at D can be expressed in terms of the circularity coefficient of the signal transmitted by Alice (C_x), respectively, as [11, 24, 25]

$$\begin{aligned} C_{y_d} &= \frac{P_a \left|g_{ad}\right|^2 C_x}{P_a \left|g_{ad}\right|^2 + P_s \left|h_{sd}\right|^2 + N_0}, \\ C_{i_d} &= \frac{P_a \left|g_{ad}\right|^2 C_x}{P_a \left|g_{ad}\right|^2 + N_0}. \end{aligned} \tag{7}$$

Hence, using (7), the mutual information of the S⟶D link can be expressed as [11, 25]

$$I_{sd} = \log_2 \left[\left(1 + \gamma_{sd}\right) \sqrt{\frac{1 - C^2_{y_d}}{1 - C^2_{i_d}}} \right]. \tag{8}$$

Since PUs only transmit using PGS, the improper interference-plus-noise signal, C_{i_l} (with $l \in \{b, e\}$), vanishes at the secondary side. The result is that the mutual information for the A⟶B and A⟶E links can be expressed as

$$I_{al} = \log_2 \left[\left(1 + \gamma_{al}\right) \sqrt{1 - C^2_{y_l}} \right], \tag{9}$$

where C_{y_l} is the circularity coefficient of the signal received at l, given by

$$C_{y_l} = \frac{P_a \left|h_{al}\right|^2 C_x}{P_s \left|g_{sl}\right|^2 + P_a \left|h_{al}\right|^2 + N_0}. \tag{10}$$

It is important to note that Bob and Eve are aware that Alice can transmit either with PGS or IGS, in order to have a fair comparison between them.

Finally, regarding the interference constraint of the underlay paradigm, the secondary power must be limited. Similar to [15, 25], Alice's transmit power, P_a, is limited with respect to a target primary transmission rate, R_s. Then, making $I_{sd} = R_s$ in (8), one can compute P_a as a function of R_s as

$$P_a^{\dagger}\left(C_x, R_s\right) = \frac{P_s \lambda_{sd} - N_0 \left(2^{2R_s} - 1\right)}{\left(1 - C_x^2\right)\left(2^{2R_s} - 1\right)\lambda_{ad}} + \sqrt{\theta_1}, \tag{11}$$

where

$$\theta_1 = \frac{P_s^2 \lambda_{sd}^2 2^{2R_s} + C_x^2 \left(N_0^2 2^{2R_s} - \left(N_0 + \lambda_{sd} P_s\right)^2\right)}{\left(1 - C_x^2\right)^2 \left(2^{2R_s} - 1\right)^2 \lambda_{ad}^2}. \tag{12}$$

It is worth noting that all expressions from (8) to (12) return to the known PGS case when $C_x = 0$.

Finally, looking at (9), it is noticeable that increasing C_x decreases I_{al}. On the other hand, another consequence of adopting IGS is that Alice can increase its transmission power, since the interference caused at the PUs is less harmful than a proper one. Hence, it is possible to achieve higher transmission rates and to improve the secrecy performance at the SUs, due to the lower differential entropy of asymmetric signals, if interference is treated as noise. In other words, there is a trade-off between how much improper will the signal be and how much power will be transmitted, i.e., a trade-off between C_x and $P_{a,IGS}$.

The next section presents the main performance metrics adopted to assess the proposed system.

3. Secrecy Performance Analysis

Three secrecy metrics were adopted to assess the performance of the proposed system, the secrecy outage probability (SOP), the secure throughput (ST), and the secure energy efficiency (SEE).

The SOP can be defined as the probability that the mutual information of the legitimate channel is less than or equal to that of the wiretap channel. Hence, when only SCSI is available at the SU side and using (9), the SOP can be expressed as

$$\begin{aligned}\mathcal{O}_s &= \Pr\left[I_{ab} - I_{ae} < R_a\right] \\ &= \Pr\left[\frac{\left(1+\gamma_{ab}\right)^2\left(1-C_{y_b}^2\right)}{\left(1+\gamma_{ae}\right)^2\left(1-C_{y_e}^2\right)} < 2^{2R_a^{th}}\right],\end{aligned} \tag{13}$$

where R_a^{th} is the target secrecy data rate.

In addition, finding the cumulative distribution function (CDF) of the random variable $|h_{ab}|^2$, which is exponentially distributed due to the Rayleigh fading assumption, one can show, in a similar way as [14], that a closed-form expression for the system SOP can be expressed as [25]

$$\begin{aligned}\mathcal{O}_s &= \int_0^{\psi} \frac{\exp\left(-\left|h_{ab}\right|^2/\lambda_{ab}\right)}{\lambda_{ab}} d\left|h_{ab}\right|^2 \\ &= 1 - \exp\left(-\frac{\psi}{\lambda_{ab}}\right).\end{aligned} \tag{14}$$

The upper limit of the integral in (14) is obtained by solving the inequality in (13) with respect to h_{ab} and is found to be

$$\psi = \frac{\left(\left(P_s\lambda_{sb}+N_0\right)/\left(P_s\lambda_{se}+N_0\right)\right)\sqrt{\theta_2} - P_s\lambda_{sb} - N_0}{\left(1-C_x^2\right)P_a}, \tag{15}$$

where

$$\begin{aligned}\theta_2 &= C_x^2\left(N_0+P_s\lambda_{se}\right)^2 - 2^{2R_a^{th}}\left(1-C_x^2\right) \\ &\quad\times\left[\left(C_xP_a\lambda_{ae}\right)^2 - \left(P_a\lambda_{ae}+P_s\lambda_{se}+N_0\right)^2\right].\end{aligned} \tag{16}$$

From (9), it is noticeable that I_{al} decreases with the increment of C_x. However, Alice can increase its power, because by transmitting improper signals, the interference caused at PUs is less harmful than a proper one. In addition, it is worth noting that from (8), increasing C_x increases I_{sd} as well. Therefore, it is possible to achieve the same I_{sd} with higher values of P_a, if larger values of C_x are also employed.

Then, it is possible for the SUs to increase their achievable rate and, consequently, lower SOP values can be achieved by optimizing the transmission parameters C_x and P_a. Naturally, this optimization must respect the underlay interference constraint, here imposed by R_s.

From the previous analysis we can estimate the achievable SOP that guarantees a target secrecy rate. Similarly, it is possible to attain the secrecy rate that can be achieved to ensure a target SOP, i.e., a maximum allowable value for the SOP, say $\mathcal{O}^{th}$.

Note that ensuring a target SOP can be done by guaranteeing that the achievable rate at the secondary side, R_a, respects this predefined SOP threshold. Hence, an expression that gives R_a as a function of $\mathcal{O}^{th}$ is necessary. Solving (14) with respect to R_a and making $\mathcal{O}_s = \mathcal{O}^{th}$ give

$$R_a\left(\mathcal{O}^{th}\right) = \frac{1}{2}\log_2\left[\frac{\theta_3}{\theta_4}\right], \tag{17}$$

where

$$\begin{aligned}\theta_3 &= C_x^2\left(N_0+P_s\lambda_{se}\right)^2 \\ &\quad - \frac{\left(N_0+P_s\lambda_{se}\right)^2\left(N_0+P_s\lambda_{sb}-\left(1-C_x^2\right)P_a\lambda_{ab}\log\left[1-\mathcal{O}^{th}\right]\right)^2}{\left(N_0+P_s\lambda_{sb}\right)^2},\end{aligned} \tag{18}$$

and

$$\begin{aligned}\theta_4 &= \left(1-C_x^2\right)\left(\left(C_xP_a\lambda_{ae}\right)^2 - \left(N_0+P_a\lambda_{ae}+P_s\lambda_{se}\right)^2\right).\end{aligned} \tag{19}$$

Since it is not possible to achieve $\mathcal{O}_s = 0$, then, to evaluate the energy efficiency of the system with security constraints, the SEE metric is adopted, which is related to the throughput at the secondary side. For the adaptive scheme, i.e., when the only instantaneous channel gain available to the SUs is the one from the direct link, $|h_{ab}|^2$, the effective secure throughput (ST) can be expressed as [29]

$$\mathcal{T}_s = R_a\left(1-\mathcal{O}_s\right), \tag{20}$$

where R_a may be substituted by R_a^{th} and $\mathcal{O}_s$ by $\mathcal{O}^{th}$, depending on the case. Note that $\mathcal{T}_s$ represents the number of bits per channel use that can be safely transmitted from Alice to Bob.

Nonetheless, only the effective ST does not impose any constraint regarding the maximum allowable SOP. Then, in [33], the authors propose a variation of the effective ST, limiting $\mathcal{T}_s$ as

$$\mathcal{T}_s^{th} = \begin{cases}\mathcal{T}_s, & \text{if } \mathcal{O}_s \le \mathcal{O}^{th}; \\ 0, & \text{if } \mathcal{O}_s > \mathcal{O}^{th}.\end{cases} \tag{21}$$

Hence, the $\mathcal{O}^{th}$ is taken into account when calculating the effective ST in the later optimizations, and $\mathcal{T}_s$ is obtained using (21).

Additionally, it is possible to define the SEE as the ratio between the effective ST and the secondary transmit power. Using (21), the SEE can be expressed as [34]

$$\eta_s = \frac{\mathcal{T}_s}{P_a}, \tag{22}$$

where η_s is the SEE in bits/Joule/Hz (bits/J/Hz).

Unfortunately, due to the mathematical intractability of the expressions regarding the mutual information between users when transmitters adopt IGS [11, 14–16, 25], finding

$p \longleftarrow 1$
create a random initial population ρ_0 of size γ
set current population ρ_p equal to ρ_0
repeat
    evaluate each member of ρ_p according to its fitness value
    assign a rank to each member of ρ_p based on its fitness
    compute the expectation of each member of ρ_p based on its rank
    if $P_a^* < P_a^\dagger$ **then**
        $P_a \longleftarrow P_a^*$
    else
        $P_a \longleftarrow P_{\mathrm{a}}^\dagger$
    end if
    select γ_{pp} parent individuals
    create γ_c crossover children from the parents
    create γ_m mutation children from the parents
    select γ_e elite individuals
    replace the current population
    $p \longleftarrow p + 1$
until the maximum number of generations is reached

Algorithm 1: Genetic algorithm.

closed-form expressions that indicate precisely when IGS is more beneficial than PGS in general scenarios turns out to be a very complicated task. Nonetheless, assessing such systems via a numerical approach is trivial. This is why in the next section we define two optimization problems, one for the SOP and another involving R_a.

4. Optimization Problems

The goal is to minimize the SOP given in (14) and maximize the ST given in (21) by finding optimal values of P_a and C_x simultaneously, as well as respecting the underlay interference constraint given by (11).

As previously stated, we resort to GAs to solve optimization problems in this work. Using GAs is suitable for this kind of problem since the expressions are nonlinear and the nodes locations in the system are stochastic. Moreover, since we are focused on demonstrating how the adequate optimization of C_x and P_a at the same time allows enhancing the secrecy performance of CR networks, regarding the SOP, using GAs represents a feasible technique. In this regard, it is well known that GAs perform well when the task does not require a global optimum to be found, in other words, if finding a sufficiently good solution quick is good enough [35].

A GA firstly creates a random set of feasible individuals that solve the problem. In the present case, a candidate is composed by two variables, P_a and C_x. After this first generation is tested, the best-fitted candidates are kept for the next generation, sometimes called the "elite count" or "champions" [27]. Other individuals from this first generation are subjected to crossover and mutation operations [26, 27].

Crossover and mutation change the next generation individuals slightly, compared to their parents. A crossover mixes two individuals of the previous generation to create a new one, and a mutation changes randomly the individual, without any relation to others. The idea is to enhance the chances of finding global optima [35].

This process goes on until a best individual is found. Common ways to end the optimization are when a found solution satisfies minimum criteria or when a fixed number of generations is reached. In this work, we use the latter stop criteria.

Due to the inherent randomness of the nodes positions and, consequently, of the mutual information between them, the GA that optimizes the system performance metrics is run several times, one for each network topology. In each topology, the positions of the nodes are drawn again, according to (1). After running for M different topologies, the mean of the optimized parameters is computed, analogous to a Monte-Carlo simulation.

The pseudo-code for the optimization process described above can be seen in Algorithm 1, where the superscript $*$ denotes the optimum value of a variable or the best performance of this generation. In addition, denoting γ_c, γ_m, and γ_e as the number of crossover, mutation, and elite individuals in the population, the population size is given by $\gamma = \gamma_c + \gamma_m + \gamma_e$. If γ and γ_e are fixed values, the number of crossover and mutation children can be determined through the crossover fraction, defined as $\kappa = \gamma_c/(\gamma_c + \gamma_m)$.

In order to exploit the trade-off between the degree of impropriety and the secondary transmit power, two problems were formulated.

4.1. Problem I: Minimizing the SOP. The first problem minimizes the system SOP by finding optimal combinations of P_a and C_x concurrently. It is formulated as

$$\min_{P_a, C_x} \quad \mathcal{O}_s\left(P_a, C_x\right)$$

Table 2: Simulation parameters.

$R = 100$ units of length	$P_{a_{max}} = 20$ dB	$P_s = 20$ dB
$R_s = R_a = 1$ bits/s/Hz	$\delta_a = \delta_d = \delta_e = 1$	$\delta_b = 0.1$
$\alpha = 4$	$\mathcal{O}^{th} = 0.1$	$M = 10^4$

$$\begin{aligned} \text{s.t.} \quad & 0 \le P_a \le P_{a_{max}}, \\ & 0 \le C_x \le 1, \end{aligned} \tag{23}$$

where $P_{a_{\max}}$ is Alice's maximum hardware power. Note that the problem constraints are treated as lower and upper bounds of the problem variables. Moreover, the underlay interference constraint is within the $P_a^{\dagger}$ expression in (11).

With the found values of $\mathcal{O}_s^*$, the effective ST (21) and the SEE (22) can be obtained subsequently, given a predefined R_a^{th}.

4.2. Problem II: Maximizing the ST. The second problem involves the ST metric. It is desirable that the system can transmit the highest number of bits in any transmission attempt. In this regard, it is worth noting that, since it is interesting to maintain the SOP always below a predefined threshold, $\mathcal{O}^{th}$, maximizing the effective ST is the same as maximizing R_a itself. Hence, a fair and unbiased suboptimal approach is to maximize the secondary achievable rate in (17), and Problem II can then be formulated as

$$\begin{aligned} \max_{P_a, C_x} \quad & R_a\left(P_a, C_x, \mathcal{O}^{th}\right) \\ \text{s.t.} \quad & 0 \le P_a \le P_{a_{max}}, \\ & 0 \le C_x \le 1, \\ & \mathcal{O}_s = \mathcal{O}^{th}. \end{aligned} \tag{24}$$

Similarly to Problem I, with the found values of R_a^*, the effective ST (21) and the SEE (22) can be obtained subsequently.

4.3. GA Parameter Tuning. Before running the GA on the problems themselves, it is necessary to find which GA parameters attain better performance while solving the formulated problems in the proposed system model. The idea is to find which values of some optimization parameters attain a sufficient result and, therefore, there is no need to increment them anymore.

The following GA parameters were tested for Problems I and II: the crossover fraction, the number of generations, and the population size of each generation. In each of the tunings, the optimum values of the performance metrics, the SOP and the ST, hereinafter denoted by $\mathcal{O}_s^*$ and $\mathcal{T}_s^*$, respectively, were evaluated as functions of the parameter of interest for $M = 10^4$ different network topologies.

For example, for each topology, the best result obtained in the first generation is estimated and stored. Then, the number of generations is incremented, and in the next round of optimization, the best result is again estimated and stored. The result always becomes better while increasing the generation number, since in the first round, the selected individual corresponds to an elite one, which cannot be eliminated, only replaced by another individual which attains better result in the next iteration. Then, the different topologies values are averaged for each stored generation value.

Other system parameters used to tune the GA are shown in Table 2.

The tuning proceeded selecting a population of 100 individuals and 100 generations to find the crossover fraction. Then, with the selected crossover value and 100 individuals, the number of generations was determined and, finally, the minimum number of individuals required was obtained.

Hence, after tuning the aforementioned parameters, to obtain the results shown in the next section the following values for the GA variables were adopted for both Problems I and II: 0.6 for the crossover fraction, 30 generations for each optimization run, and, for each generation, 30 individuals (population size).

5. Numerical Results

In this section, numerical results are provided in order to illustrate the findings presented previously. The final results are obtained through the mean of the $M = 10^4$ optimization rounds, one for each system nodes random distribution. Other parameters to obtain the following results are shown in Table 2, which represent a realistic set of values in practical scenarios of the proposed system model [14].

5.1. Primary Transmit Power Influence. First, the system performance was assessed when the primary transmitter power was increased. The optimal values of the degree of impropriety and of the secondary transmit power as functions of P_s for the M optimization rounds are shown in Table 3.

The optimal signal tends to be proper when P_s increases. On the other hand, when $P_s < P_{a_{max}} = 20$ dB, higher values of C_x^* are found. In addition, regarding the analysis in Figure 2, the use of GA allows obtaining the best performance of the system in terms of SOP for all values of S's transmission power. When $P_s < P_a$, the performance of the maximally improper scheme is greater than that of the PGS, due to the lower impact of the improper interference. However, when $P_s > P_a$, the scheme tends to the classic underlay paradigm, and the performance of the PGS system exceeds that of the maximally improper in terms of SOP.

When maximizing R_a (Figure 3), the system performance, assessed through the effective ST, also deteriorates

Table 3: Optimal degree of impropriety and secondary transmit power as a function of the primary transmit power.

P_s [dB]	0	10	20	30	40
C_x^* **min** $\mathcal{O}_s$	0.59	0.45	0.22	0.10	0.05
C_x^* **max** R_a	0.48	0.41	0.23	0.11	0.06
P_a^* [dB] **min** $\mathcal{O}_s$	17.65	18.98	19.61	19.66	19.47
P_a^* [dB] **max** R_a	16.73	18.11	18.76	18.92	18.97

Table 4: Optimal degree of impropriety and secondary transmit power as a function of δ_a.

δ_a	0.1	0.3	0.5	0.7	0.9
C_x^* **min** $\mathcal{O}_s$	0.27	0.30	0.27	0.23	0.19
C_x^* **max** R_a	0.29	0.29	0.26	0.22	0.19
P_a^* [dB] **min** $\mathcal{O}_s$	16.23	19.65	19.61	19.60	19.64
P_a^* [dB] **max** R_a	5.53	18.58	19.01	19.19	19.31

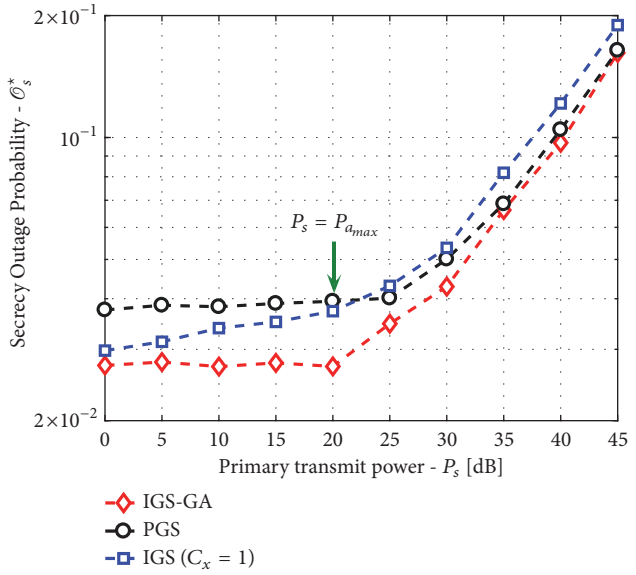

Figure 2: Optimal secrecy outage probability as a function of the primary transmit power.

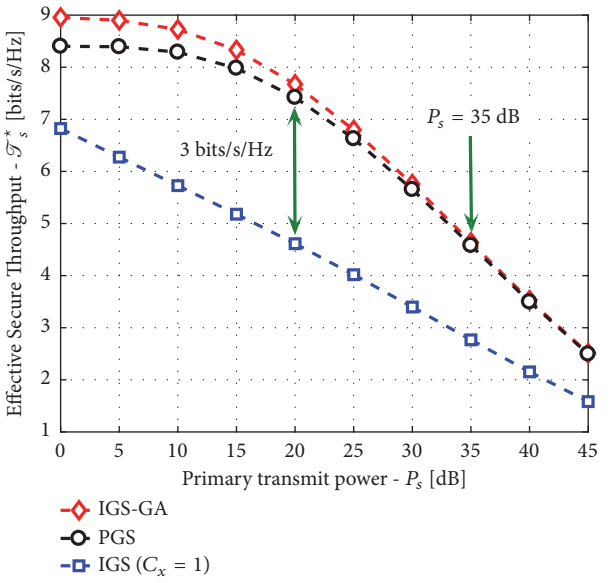

Figure 3: Optimal secure throughput as a function of the primary transmit power, maximizing the secrecy data rate.

when P_s increases. Nonetheless, for higher values of P_s, optimizing C_x and adopting PGS attain the same performance. Moreover, when maximizing R_a, the IGS-GA scheme obtains the best performance in terms of the effective ST for all values of P_s. However, the benefits over the PGS scheme for $P_s > 35$ dB are not significant. In addition, the maximally improper scheme has the worst performance in terms of the effective ST, being 3 bits/s/Hz lower than that of the PGS scheme when $P_s = P_a$.

Finally, another interesting analysis is to observe how efficient the proposed system can be in terms of energy spent for each transmitted bit. Figure 4 depicts the SEE as a function of P_s. In terms of the SEE, the best performance is still obtained through the PGS scheme for all P_s values. Nonetheless, for $P_s > 35$ dB the IGS-GA scheme presents results very close to those obtained by the PGS one. In addition, when IGS is used with $C_x = 1$ the energy efficiency of the system drops to 60% when compared to the IGS-GA scheme.

This is an expected result, since the SEE metric, η_s, requires lower values of P_a, but the IGS scheme achieves its benefits precisely by increasing the transmission power due to the lower differential entropy of improper signals, i.e., a less harmful interference at the PUs.

5.2. Network Topology Influence. Afterwards, the system was assessed when Alice moved away from S in a straight line, starting with $\delta_a = 0.1$ to $\delta_a = 1.0$ with increments of 0.1, up to the border of the circular cell.

Table 4 shows the optimal values of the degree of impropriety and of the secondary transmit power for each value of δ_a. The optimal degree of impropriety decreases when Alice moves farther from S, either when optimizing the SOP or R_a. Nonetheless, C_x^* is never equal to zero.

Table 5: Optimal degree of impropriety and secondary transmit power as a function of δ_b.

δ_b	0.1	0.3	0.5	0.7	0.9
C_x^* **min** $\mathcal{O}_s$	0.23	0.23	0.23	0.24	0.25
C_x^* **max** R_a	0.23	0.25	0.26	0.28	0.28
P_a^* **[dB] min** $\mathcal{O}_s$	19.59	18.29	16.31	14.27	11.23
P_a^* **[dB] max** R_a	18.56	13.70	9.83	6.96	4.43

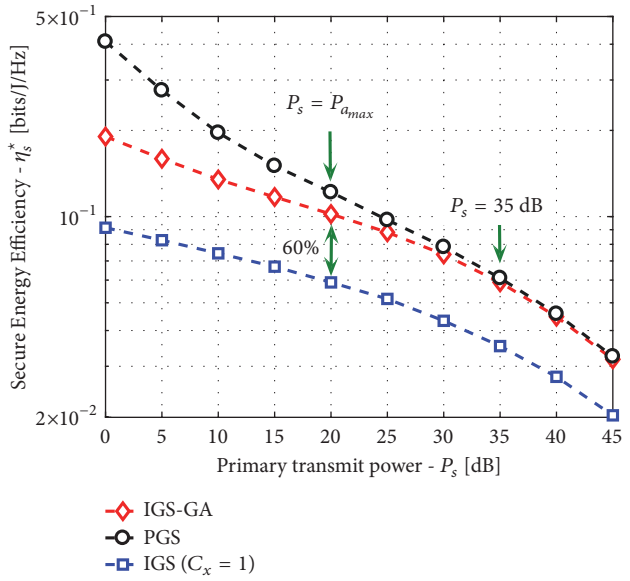

Figure 4: Optimal secure energy efficiency as a function of the primary transmit power, maximizing the secrecy data rate.

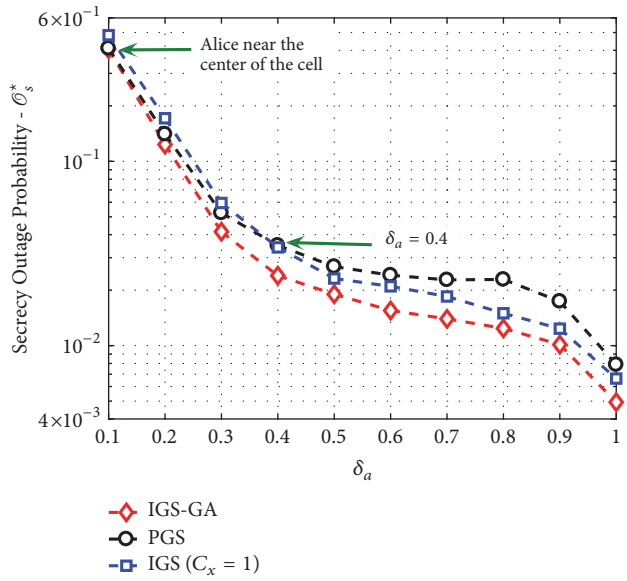

Figure 5: Optimal secrecy outage probability as a function of δ_a.

Regarding the secondary transmit power, P_a almost reaches $P_{a_{max}}$ independently of the δ_a value, either when minimizing $\mathcal{O}_s$ or when maximizing R_a.

Figure 5 shows the optimal SOP as a function of δ_a. In terms of SOP the IGS-GA scheme is the one with the best performance regardless of the relative position of Alice with respect to S, although its superiority over PGS is not significant when Alice is very close to S. When Alice is close to S ($\delta_a \leq 0.4$), using PGS is more convenient than using maximally IGS. On the other hand, when Alice is away from S ($\delta_a > 0.4$), using IGS with $C_x = 1$ is more convenient than PGS.

In addition, Figure 6 depicts the effective ST as a function of δ_a. This result was attained using (21) after maximizing R_a. It is noticeable that the optimal performance is similar to the case when PGS is used; however the value of $\mathcal{T}_s^*$ always increases as δ_a also increases.

Moreover, in terms of the effective ST, the performance of the IGS-GA is better for all values of δ_a, increasing the difference when Alice is farthest from S. The benefits of PGS over maximally improper signals are significant, and they increase while Alice moves away from S, being 2 bits/s/Hz when Alice is at the midpoint of the coverage range and 4 bits/s/Hz when Alice is near the edge of the primary cell.

Later, the system secrecy performance is evaluated when Alice coverage area increases, i.e., δ_b increases. The results are shown in Table 5 and Figures 7 and 8. One can note that C_x^* remains almost constant as δ_b increases, either when minimizing $\mathcal{O}_s$ or maximizing R_a. Nonetheless, the best performance is achieved when C_x is approximately 0.25, that is, neither PGS nor maximally IGS is being used.

Observing Table 5, it is clear that P_a^* always decreases when Bob may be farther from Alice. However, P_a^* decreases faster when maximizing R_a. This behavior is due to the fact that, when Alice coverage area is larger, it is more difficult to achieve higher rates while respecting the $\mathcal{O}^{th}$.

Regarding the $\mathcal{O}_s^*$ as a function of δ_b, shown in Figure 7, it is noticeable that, in the proposed scenario, there is no significant difference in terms of the SOP whether Bob lies near or far from Alice, and whether IGS-GA, PGS, or a maximally improper signal is employed.

When looking at $\mathcal{T}_s^*$ as a function of δ_b, depicted in Figure 8, it can be noted that the effective ST decreases when Alice's coverage area becomes larger, and the maximally improper case attains the worst performance.

The analysis based on the distance between Alice and Bob also allows demonstrating the superiority of the IGS-GA scheme over the other schemes, being more significant when both SUs are closer. It should be noted that when the distance between Alice and Bob is less than 10% of the radius R, the benefit of using IGS-GA over maximally improper signals in terms of $\mathcal{T}_s$ is of the order of 3 bits/s/Hz, which represents

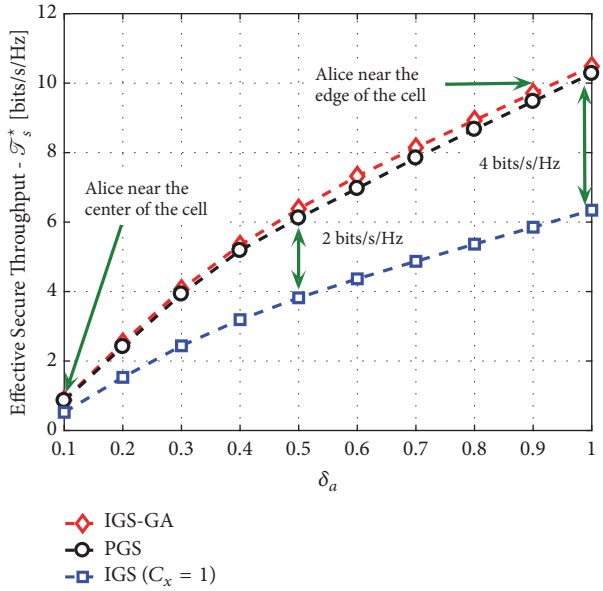

FIGURE 6: Optimal secure throughput as a function of δ_a, maximizing the secrecy data rate.

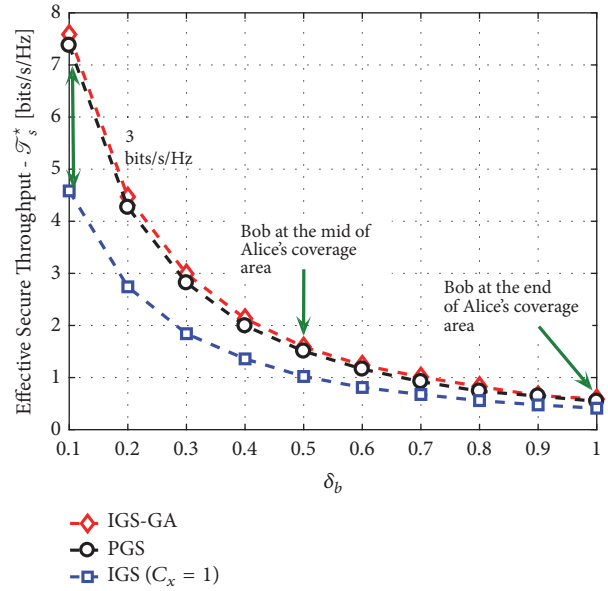

FIGURE 8: Optimal secure throughput as a function of δ_b, maximizing the secrecy data rate.

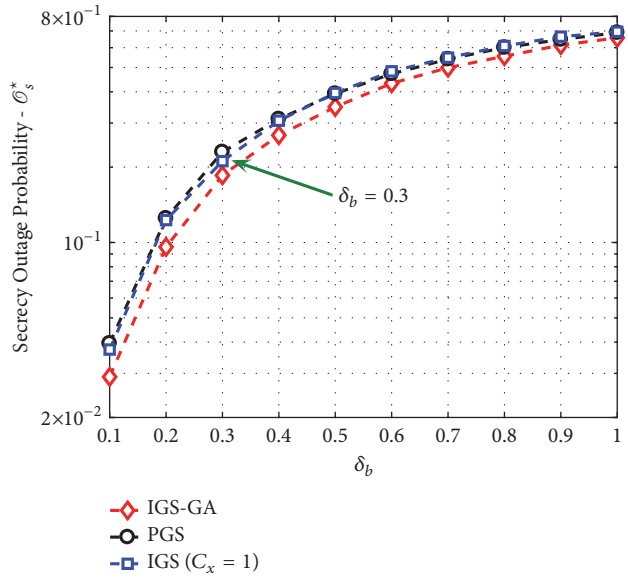

FIGURE 7: Optimal secrecy outage probability as a function of δ_b.

almost 66% of the effective ST when a maximally improper signal is employed.

Finally, in order to be able to see the impact of the system topology on the optimal degree of impropriety value, the PU receiver location was fixed. D was set in the middle of the path between S and the edge of the cell, radially. Then, the location of Alice in the cell with respect to the optimum degree of impropriety found by the GA, C_x^*, was plotted. This was done by considering $C_x^* < 0.001$ a PGS case, $C_x^* > 0.999$ a maximally improper case, and otherwise an IGS case, but not maximal. This scatter plot is shown in Figure 9 for $M = 10^3$ topology samples. In Figure 9 the axes represent the circumference radius of the cell.

One can see that when $C_x^* \neq 0$, i.e., the optimal signal is improper, employing a maximally improper signal is only the best option when Alice is near D (approximately when $d_{ad} \leq 0.3$). In addition, it seems that the location of Alice for the other two cases (PGS or a nonmaximal IGS) is not much affected by d_{ad}, remaining uniformly distributed around S.

Obviously, the fact that Alice has another degree of freedom to tune its signal, due to the concurrent optimization of P_a and C_x, plays a major role in improving the secrecy performance of the proposed system. Of a total of $M = 10^3$ different topologies, 77.6% of the C_x^* values correspond to the IGS case, 21.44% to the PGS case, and only 0.96% to the maximally improper case. These percentages are the mean for five different simulation runs, each one with $M = 10^3$ system topologies and different GA initial points. These percentages were almost the same when this analysis was made for $M = 10^4$ system topologies.

Moreover, it is important to recall that the upper and lower bounds of C_x are equal to 0 and 1, respectively. Thus, the proper and maximally improper cases lie within the possible optimization range of values for this variable.

It is interesting to note that these results are aligned with those found in [12, 25], in the sense that IGS attains better performance when λ_{ad} surpasses a threshold. Moreover, selecting PGS or IGS also depends on the distance d_{ab}.

With this in mind, in practical applications the secondary transmitter could define some regions inside the cell where it would be more convenient to use a given C_x value. For example, if $d_{ad} \leq 0.3$, use $C_x = 1$; if $0.3 < d_{ad} < 0.6$, use $C_x = 0.3$; and if $d_{ad} \geq 0.6$, use proper signals. In this regard, Table 6 shows the expected value and the variance for the optimal SOP when using the IGS-GA scheme and for this

Table 6: $\mathcal{O}^*$ expected value and variance.

C_x allocation scheme	IGS-GA	Distance based
$\mathbb{E}[\mathcal{O}^*]$	3.14E-2	3.08E-2
$\mathrm{Var}[\mathcal{O}^*]$	2.47E-6	1.85E-5

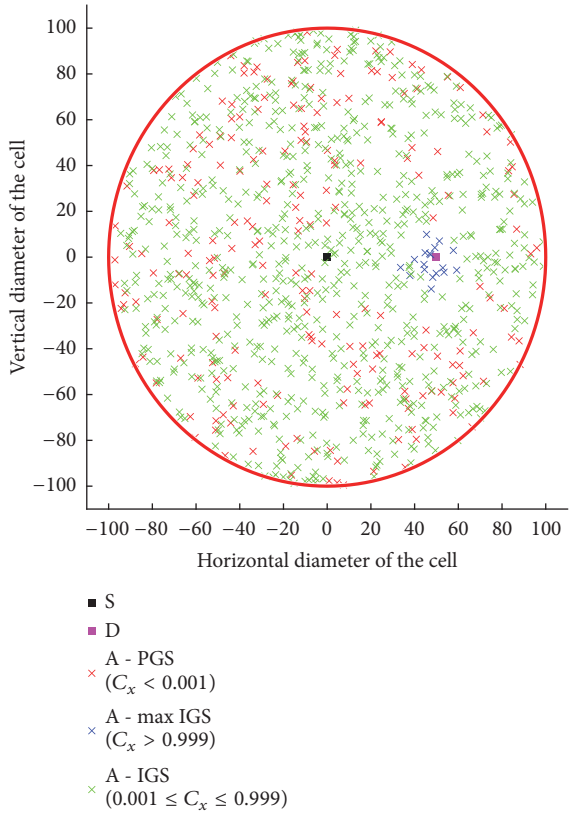

Figure 9: Alice location with respect to C_x^*. The diameter is expressed in units of length.

distance-based degree of impropriety allocation, optimizing only P_a. These results are for ten different simulation runs, each one with $M = 10^3$ system topologies and different GA initial points.

Despite the fact that the variance for the distance-based scheme is greater than that of the IGS-GA, both expected values are similar. This result indicates that this distance-based degree of impropriety allocation approach to the decision making process would benefit more if the SUs were aware of the instantaneous CSI of the primary destination as well, say, in a scenario with cooperation between PUs and SUs.

6. Conclusion

In this paper, the secrecy performance of a CR network when the SUs may transmit employing improper signaling was optimized. The proposed system model tried to capture a realistic scenario, in which system nodes were randomly distributed within the coverage area of a primary transmitter. In addition, except for the direct link between the secondary transmitter and receiver, only statistical CSI was considered available at the secondary side. Results indicate that, for the interference channel, when searching for lower secrecy outage probabilities, it is always a better strategy for the SUs to adopt some degree of impropriety in their transmissions. In addition, adopting IGS can also improve the achievable secure rates at the SUs side in underlay CR networks. However, in terms of the energy efficiency of the system, optimizing only the secondary transmit power while employing PGS achieves the best performance. The results presented in this work are promising, since in many wireless channels there are interference constraints and IGS could attain better performance than PGS, the current paradigm. Future research includes considering nodes with directional antennas based on the knowledge of the secondary receiver location. Also, proposing a scenario with cooperative communication, in which full-duplex relay nodes could transmit adopting improper signals, another interesting possibility in which we are already working on is to propose lower complexity algorithms which not only enhance the secrecy performance of the system, but also lower the computational costs of the joint optimization proposed in this research.

Data Availability

All data supporting the results are of our own authorship. In addition, all data supporting the findings of this study are presented within the article. When there is information reported in a published article from other authors, we properly cite it and include it as a reference work in the manuscript.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was partially supported by CAPES and Araucaria Foundation (Brazil), as well as FONDECYT Postdoctoral Grant No. 3170021 (Chile).

References

[1] C. Tang, G. Pan, and T. Li, "Secrecy outage analysis of underlay cognitive radio unit over Nakagami-m fading channels," *IEEE Wireless Communications Letters*, vol. 3, no. 6, pp. 609–612, 2014.

[2] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: technical challenges, recent advances, and future

trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[3] X. Chen, D. W. Ng, W. H. Gerstacker, and H. Chen, "A Survey on Multiple-Antenna Techniques for Physical Layer Security," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 1027–1053, 2017.

[4] J. Mo, M. Tao, and Y. Liu, "Relay placement for physical layer security: A secure connection perspective," *IEEE Communications Letters*, vol. 16, no. 6, pp. 878–881, 2012.

[5] M. A. Chiodi, J. L. Rebelatto, R. D. Souza, and G. Brante, "Achieving negative security gaps with transmit antenna selection and frame scrambling in quasi-static fading channels," *IEEE Electronics Letters*, vol. 51, no. 3, pp. 200–202, 2015.

[6] T. Zhang, Y. Cai, Y. Huang, T. Q. Duong, and W. Yang, "Secure Transmission in Cognitive MIMO Relaying Networks with Outdated Channel State Information," *IEEE Access*, vol. 4, pp. 8212–8224, 2016.

[7] V.-D. Nguyen, T. Q. Duong, O. A. Dobre, and O.-S. Shin, "Joint Information and Jamming Beamforming for Secrecy Rate Maximization in Cognitive Radio Networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2609–2623, 2016.

[8] B. Fang, Z. Qian, W. Shao, and W. Zhong, "Precoding and Artificial Noise Design for Cognitive MIMOME Wiretap Channels," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6753–6758, 2016.

[9] M. Bloch, M. Hayashi, and A. Thangaraj, "Error-Control Coding for Physical-Layer Secrecy," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1725–1746, 2015.

[10] E. Hodgson, G. Brante, R. D. Souza, and J. L. Rebelatto, "On the physical layer security of analog joint source channel coding schemes," in *Proceedings of the 16th IEEE International Workshop on Signal Processing Advances in Wireless Communications, SPAWC 2015*, pp. 585–589, Sweden, July 2015.

[11] Y. Zeng, C. M. Yetis, E. Gunawan, Y. . Guan, and R. Zhang, "Transmit optimization with improper Gaussian signaling for interference channels," *IEEE Transactions on Signal Processing*, vol. 61, no. 11, pp. 2899–2913, 2013.

[12] C. Lameiro, I. Santamaría, and P. J. Schreier, "Benefits of improper signaling for underlay cognitive radio," *IEEE Wireless Communications Letters*, vol. 4, no. 1, pp. 22–25, 2015.

[13] O. Amin, W. Abediseid, and M.-S. Alouini, "Underlay Cognitive Radio Systems with Improper Gaussian Signaling: Outage Performance Analysis," *IEEE Transactions on Wireless Communications*, vol. 15, no. 7, pp. 4875–4887, 2016.

[14] M. Gaafar, O. Amin, W. Abediseid, and M.-S. Alouini, "Underlay Spectrum Sharing Techniques with In-Band Full-Duplex Systems Using Improper Gaussian Signaling," *IEEE Transactions on Wireless Communications*, vol. 16, no. 1, pp. 235–249, 2017.

[15] C. Lameiro, I. Santamaría, and P. J. Schreier, "Rate region boundary of the SISO Z-Interference channel with improper signaling," *IEEE Transactions on Communications*, vol. 65, no. 3, pp. 1022–1034, 2017.

[16] S. Lagen, A. Agustin, and J. Vidal, "On the Superiority of Improper Gaussian Signaling in Wireless Interference MIMO Scenarios," *IEEE Transactions on Communications*, vol. 64, no. 8, pp. 3350–3368, 2016.

[17] A. Goldsmith, *Wireless Communications*, Cambridge University Press, New York, NY, USA, 2005.

[18] F. D. Neeser and J. L. Massey, "Proper complex random processes with applications to information theory," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 39, no. 4, pp. 1293–1302, 1993.

[19] C. Hellings and W. Utschick, "On the worst-case noise in gaussian mimo systems with proper and with improper signaling," in *Proceedings of the WSA 2017; 21th International ITG Workshop on Smart Antennas*, pp. 1–7, March 2017.

[20] W. Hedhly, O. Amin, and M. Alouini, "Interweave Cognitive Radio with Improper Gaussian Signaling," in *Proceedings of the 2017 IEEE Global Communications Conference (GLOBECOM 2017)*, pp. 1–6, Singapore, December 2017.

[21] O. Amin, W. Abediseid, and M.-S. Alouini, "Overlay Spectrum Sharing Using Improper Gaussian Signaling," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 1, pp. 50–62, 2017.

[22] M. Gaafar, M. G. Khafagy, O. Amin, R. F. Schaefer, and M.-S. Alouini, "Full-Duplex Relaying with Improper Gaussian Signaling over Nakagami- m Fading Channels," *IEEE Transactions on Communications*, vol. 66, no. 1, pp. 64–78, 2018.

[23] M. Gaafar, O. Amin, A. Ikhlef, A. Chaaban, and M.-S. Alouini, "On Alternate Relaying with Improper Gaussian Signaling," *IEEE Communications Letters*, vol. 20, no. 8, pp. 1683–1686, 2016.

[24] Y. Zeng, R. Zhang, E. Gunawan, and Y. L. Guan, "Optimized transmission with improper gaussian signaling in the K-user MISO interference channel," *IEEE Transactions on Wireless Communications*, vol. 12, no. 12, pp. 6303–6313, 2013.

[25] G. Oliveira, E. Fernandez, S. Mafra, and S. Montejo-Sanchez, "Physical Layer Security in Cognitive Radio Networks Using Improper Gaussian Signaling," *IEEE Communications Letters*, vol. 22, no. 9, pp. 1886–1889, 2018.

[26] R. Lopez, S. Sanchez, E. Fernandez, R. Souza, and H. Alves, "Genetic Algorithm Aided Transmit Power Control in Cognitive Radio Networks," in *Proceedings of the 9th International Conference on Cognitive Radio Oriented Wireless Networks*, pp. 61–66, Oulu, Finland, June 2014.

[27] U. Mehboob, J. Qadir, S. Ali, and A. Vasilakos, "Genetic algorithms in wireless networking: techniques, applications, and issues," *Soft Computing*, vol. 20, no. 6, pp. 2467–2501, 2016.

[28] X. Chen, J. Chen, H. Zhang, Y. Zhang, and C. Yuen, "On Secrecy Performance of Multiantenna-Jammer-Aided Secure Communications with Imperfect CSI," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 10, pp. 8014–8024, 2016.

[29] S. Yan, G. Geraci, N. Yang, R. Malaney, and J. Yuan, "On the target secrecy rate for SISOME wiretap channels," in *Proceedings of the 2014 1st IEEE International Conference on Communications, ICC 2014*, pp. 987–992, Australia, June 2014.

[30] R. Bordon, S. Montejo-Sanchez, R. D. Souza, G. Brante, and E. M. Fernandez, "Energy Efficient Cooperation Based on Relay Switching ON–OFF Probability for WSNs," *IEEE Systems Journal*, vol. 12, no. 4, pp. 3369–3380, 2018.

[31] L. Fan, S. Zhang, T. Q. Duong, and G. K. Karagiannidis, "Secure switch-and-stay combining (SSSC) for cognitive relay networks," *IEEE Transactions on Communications*, vol. 64, no. 1, pp. 70–82, 2016.

[32] P. J. Schreier and L. L. Scharf, "Second-order analysis of improper complex random vectors and processes," *IEEE Transactions on Signal Processing*, vol. 51, no. 3, pp. 714–725, 2003.

[33] M. E. P. Monteiro, J. L. Rebelatto, R. D. Souza, and G. Brante, "Maximum Secrecy Throughput of Transmit Antenna Selection with Eavesdropper Outage Constraints," *IEEE Signal Processing Letters*, vol. 22, no. 11, pp. 2069–2072, 2015.

[34] S. M. Sanchez, R. D. Souza, E. M. Fernandez, and V. A. Reguera, "Rate and Energy Efficient Power Control in a Cognitive Radio Ad Hoc Network," *IEEE Signal Processing Letters*, vol. 20, no. 5, pp. 451–454, 2013.

[35] M. Mitchell, *An Introduction to Genetic Algorithms*, MIT Press, Cambridge, MA, USA, 1998.