

UNIVERSIDADE FEDERAL DO PARANÁ

GUILHERME AUGUSTO QUEIROZ SCHÜNEMANN MANFRIN DE  
OLIVEIRA

PHYSICAL LAYER SECURITY IN COGNITIVE RADIO NETWORKS  
USING IMPROPER GAUSSIAN SIGNALING

CURITIBA

2018

GUILHERME AUGUSTO QUEIROZ SCHÜNEMANN MANFRIN DE  
OLIVEIRA

PHYSICAL LAYER SECURITY IN COGNITIVE RADIO NETWORKS  
USING IMPROPER GAUSSIAN SIGNALING

Tese apresentada ao Programa de Pós-Graduação em Engenharia Elétrica, Setor de Tecnologia, Universidade Federal do Paraná, como requisito parcial para obtenção do título de doutor em Engenharia Elétrica.

Orientador: Prof. Dr. Evelio Martin Garcia Fernandez

Coorientador: Prof. Dr. Samuel Baraldi Mafra

CURITIBA

2018

Catálogo na Fonte: Sistema de Bibliotecas, UFPR  
Biblioteca de Ciência e Tecnologia

O48p

Oliveira, Guilherme Augusto Queiroz Schünemann Manfrin de  
Physical layer security in cognitive radio networks using improper gaussian  
signaling / Guilherme Augusto Queiroz Schünemann Manfrin de Oliveira. –  
Curitiba, 2018.

Tese - Universidade Federal do Paraná, Setor de Tecnologia, Programa  
de Pós-Graduação em Engenharia Elétrica, 2018.

Orientador: Evelio Martin Garcia Fernandez. - Coorientador: Samuel  
Baraldi Mafra. -

1. Redes cognitivas de rádio. 2. Segurança na camada física. 3.  
Probabilidade de falha de segurança. I. Universidade Federal do Paraná. II.  
Fernandez, Evelio Martin Garcia. III. Mafra, Samuel Baraldi IV. Título.

CDD: 005.8

Bibliotecária: Vanusa Maciel - CRB - 9/1928




MINISTÉRIO DA EDUCAÇÃO  
SETOR TECNOLOGIA  
UNIVERSIDADE FEDERAL DO PARANÁ  
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO  
PROGRAMA DE PÓS-GRADUAÇÃO ENGENHARIA  
ELÉTRICA

## TERMO DE APROVAÇÃO

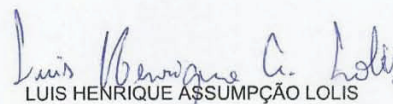
Os membros da Banca Examinadora designada pelo Colegiado do Programa de Pós-Graduação em ENGENHARIA ELÉTRICA da Universidade Federal do Paraná foram convocados para realizar a arguição da tese de Doutorado de **GUILHERME AUGUSTO QUEIROZ SCHUNEMANN MANFRIN DE OLIVEIRA** intitulada: **Physical Layer Security in Cognitive Radio Networks using Improper Gaussian Signaling**, após terem inquirido o aluno e realizado a avaliação do trabalho, são de parecer pela sua APROVAÇÃO no rito de defesa.

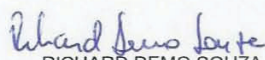
A outorga do título de doutor está sujeita à homologação pelo colegiado, ao atendimento de todas as indicações e correções solicitadas pela banca e ao pleno atendimento das demandas regimentais do Programa de Pós-Graduação.

Curitiba, 26 de Outubro de 2018.

  
EVELIO MARTÍN GARCÍA FERNÁNDEZ  
Presidente da Banca Examinadora

  
GLAUBER GOMES DE OLIVEIRA BRANTE  
Avaliador Externo

  
LUIS HENRIQUE ASSUMPCÃO LOLIS  
Avaliador Interno

  
RICHARD DEMO SOUZA  
Avaliador Externo

  
SAMUEL BARALDI MAFRA  
Avaliador Interno

## ACKNOWLEDGMENTS

Agradeço aos meus orientadores, professores Evelio e Samuel, pela amizade, confiança em mim, orientação durante o doutorado, atenção dedicada e aconselhamentos que guiaram de forma excelente minhas atividades acadêmicas. Obrigado.

Agradeço ao professor Samuel Montejo-Sánchez pelo auxílio com esta pesquisa. Mesmo sem nos conhecermos pessoalmente, foi sempre muito prestativo, proporcionando uma troca de ideias profícua para os resultados desta tese. Muchas gracias.

Agradeço aos professores Luis Lolis, Glauber Brante e Richard Souza, pelos comentários e ideias que contribuíram enormemente para o melhoramento da pesquisa contida neste trabalho.

Um agradecimento especial aos colegas dos laboratórios de pesquisa da UFPR, que de forma direta ou indireta me ajudaram a começar e terminar essa caminhada acadêmica. Obrigado pela convivência, pelas conversas, debates e ideias.

Por fim o agradecimento mais importante. Agradeço à minha família, especialmente aos meus pais, Marcus e Maria Inês, por estarem sempre presentes.

O presente trabalho foi parcialmente realizado com apoio da CAPES/CNPq - Brasil.

*“Coragem! Levanta-te! Ele te chama.”.  
O cego se levanta, joga seu manto fora e pede que veja.  
Curado de sua cegueira, Bartimeu segue o caminho da verdade.*

Adaptado do evangelho de Sao Marcos

## RESUMO

Em redes de comunicação sem fio que possuem restrições de interferência, a adoção de sinais assimétricos ou impróprios pode atingir taxas de transmissão mais altas do que as obtidas com sinais próprios, devido à maior entropia diferencial destes. Portanto, uma vez que o desempenho de segurança de uma rede está diretamente relacionado à taxa de transmissão de seus usuários, esta tese propõe o emprego de sinais impróprios para melhorar o desempenho do sigilo em redes de Rádio Cognitivo. Até onde sabemos, este é o primeiro trabalho que aborda a Segurança da Camada Física deste tipo de sistema usando sinais assimétricos. Os resultados foram obtidos para dois cenários diferentes em um mesmo modelo de sistema: uma rede cognitiva *underlay* com uma ligação direta entre o transmissor secundário e seu receptor, cuja comunicação está sendo espionada. Usuários primários e secundários causam interferência entre si. Em ambos os cenários, apenas a informação estatística do estado do canal foi considerada disponível para os usuários cognitivos. Para o primeiro cenário, em que a localização dos nós do sistema foi definida arbitrariamente, derivamos uma expressão analítica para a Probabilidade de Falha de Sigilo, a principal métrica de desempenho analisada, e foi mostrado que a adoção de sinalização imprópria pode ser benéfica tanto para os usuários que causam quanto para os que recebem interferência. Em um segundo cenário, em que a localização dos nós foi distribuída uniformemente sobre uma célula circular, encontramos valores ótimos ou sub-ótimos para a potência de transmissão e grau de impropriedade dos sinais dos usuários secundários simultaneamente, a fim de otimizar o desempenho de segurança da rede. A otimização foi feita com o auxílio de Algoritmos Genéticos. Em seguida, os benefícios do esquema de transmissão em termos da probabilidade de falha de sigilo e da vazão de dados segura do sistema, bem como o custo de eficiência energética foram avaliados. Os resultados indicam que, para sistemas limitados por interferência, ao buscar por baixas probabilidades de falha de sigilo, é sempre uma estratégia melhor para os usuários secundários adotar algum grau de impropriedade em suas transmissões. Além disso, a adoção de sinais impróprios também pode melhorar as taxas seguras atingíveis no lado dos usuários cognitivos em redes *underlay*. No entanto, em termos de eficiência energética do sistema, otimizar apenas a potência de transmissão secundária e adotar sinais próprios obtém o melhor desempenho. Os resultados apresentados nesta pesquisa são promissores, uma vez que em muitas redes sem fio, inclusive cognitivas, existem restrições de interferência e sinais assimétricos poderiam alcançar um desempenho melhor do que os próprios, o paradigma atual.

**Palavras-chave:** Rádio Cognitivo, Segurança na Camada Física, Sinais Impróprios, Probabilidade de Falha de Segurança.

## ABSTRACT

In interference constrained wireless communication networks, adopting asymmetric or improper signals may attain higher transmission rates than those achieved by proper ones, due to the higher differential entropy of the latter. Therefore, since the secrecy performance of a network is directly related to the transmission rate of its users, this thesis proposes employing improper signals in order to enhance the secrecy performance of Cognitive Radio networks. As far as we know, this is the first work that addresses the Physical Layer Security of these type of system by using asymmetric signals. The results were obtained for two different scenarios in the same system model: an underlay cognitive network with a direct link between secondary transmitter and receiver, whose communication is being eavesdropped. Both primary and secondary users cause interference at each other. In both scenarios only Statistical Channel State Information was considered available at the cognitive users. For the first scenario, in which nodes locations were defined arbitrarily, we derived an analytical expression for the Secrecy Outage Probability, the main performance metric analyzed, and it was shown that adopting improper signaling can be beneficial for users either causing or receiving interference. In a second scenario, in which nodes locations were uniformly distributed over a circular cell, we found optimal or suboptimal values of the secondary users transmit power and degree of impropriety, concurrently, in order to optimize the secrecy performance, with the aid of Genetic Algorithms. Then, the benefits of the transmission scheme in terms of the Secrecy Outage Probability and the Secure Throughput of the system, as well as the Secure Energy Efficiency cost were assessed. Results indicate that, for systems with interference constraints, when searching for lower Secrecy Outage Probabilities, it is always a better strategy for the Secondary Users to adopt some degree of impropriety in their transmissions. In addition, adopting improper signals can also improve the achievable secure rates at the cognitive users side in underlay networks. However, in terms of the energy efficiency of the system, optimizing only the secondary transmit power while employing proper signals achieves the best performance. The results presented in this research are promising, since in many wireless channels, including Cognitive Networks, there are interference constraints and asymmetric signals could attain better performance than proper ones, the current paradigm.

**Keywords:** Cognitive Radio Networks, Physical Layer Security, Improper Gaussian Signaling, Secrecy Outage Probability.



## LIST OF FIGURES

3.1	Scenario 1 System Model Topology . . . . .	31
3.2	Scenario 2 System Model Topology . . . . .	32
4.1	Scenario 1 Secrecy Outage Probability <i>vs.</i> the degree of impropriety . . . .	42
4.2	Scenario 1 Secrecy Outage Probability <i>vs.</i> the maximum Alice power . . .	43
4.3	Scenario 1 Secrecy Outage Probability <i>vs.</i> the Source transmission power .	44
4.4	Scenario 1 Secrecy Outage Probability for the moving eavesdropper topology	44
4.5	Scenario 2 Optimal Secrecy Outage Probability <i>vs.</i> the primary transmit power . . . . .	46
4.6	Scenario 2 Optimal Secure Throughput <i>vs.</i> the primary transmit power - maximizing the secrecy data rate . . . . .	47
4.7	Scenario 2 Optimal Secure Energy Efficiency <i>vs.</i> the primary transmit power - maximizing the secrecy data rate . . . . .	47
4.8	Scenario 2 Optimal Secrecy Outage Probability <i>vs.</i> the $\delta_a$ portion of the cell radius . . . . .	49
4.9	Scenario 2 Optimal Secure Throughput <i>vs.</i> the $\delta_a$ portion of the cell radius - maximizing the secrecy data rate . . . . .	49
4.10	Scenario 2 Optimal Secrecy Outage Probability <i>vs.</i> the $\delta_b$ portion of the Alice cell radius . . . . .	50
4.11	Optimal Secure Throughput <i>vs.</i> the $\delta_b$ portion of the Alice cell radius - maximizing the secrecy data rate . . . . .	51

## LIST OF TABLES

3.1	Simulation Parameters . . . . .	40
3.2	$C_x$ expected value and variance for different GA starting points . . . . .	41
4.1	Optimal degree of impropriety and secondary transmit power <i>vs.</i> the primary transmit power . . . . .	45
4.2	Optimal degree of impropriety and secondary transmit power <i>vs.</i> the $\delta_a$ portion of the cell radius . . . . .	48
4.3	Optimal degree of impropriety and secondary transmit power <i>vs.</i> the $\delta_b$ portion of the Alice cell radius . . . . .	50

## LIST OF ABBREVIATIONS

CR	<i>Cognitive Radio</i>
SU	<i>Secondary User</i>
PU	<i>Primary User</i>
PLS	<i>Physical Layer Security</i>
PGS	<i>Proper Gaussian Signaling</i>
IGS	<i>Improper Gaussian Signaling</i>
QoS	<i>Quality of Service</i>
OSI	<i>Open Systems Interconnection</i>
RV	<i>Random Variable</i>
SOP	<i>Secrecy Outage Probability</i>
CSI	<i>Channel State Information</i>
SCSI	<i>Statistical Channel State Information</i>
IC	<i>Interference Channel</i>
PDF	<i>Probability Density Function</i>
MIMO	<i>Multiple-Input Multiple-Output</i>
AWGN	<i>Additive White Gaussian Noise</i>
SINR	<i>Signal-to-Interference-Plus-Noise Ratio</i>
ST	<i>Secure Throughput</i>
SEE	<i>Secure Energy Efficiency</i>
CDF	<i>Cumulative Distribution Function</i>
GA	<i>Genetic Algorithm</i>

## LIST OF SYMBOLS

$C$	Channel capacity
$I\{X;Y\}$	Mutual information bewteen two random variables $X$ and $Y$
$p_X(x)$	Marginal probability distribution of a random variable $X$
$C_{\text{legitimate}}$	Legitimate users channel capacity
$C_{\text{wiretap}}$	Wiretap channel capacity
$\mathcal{O}_s$	Secrecy Outage Probability
$I_{\text{legitimate}}$	Legitimate users mutual information
$I_{\text{wiretap}}$	Illegitimate users mutual information
$R_a$	Secure transmission rate
$f_X(x)$	Probability density function of a random variable $X$
$\mathcal{H}_X$	Differential entropy of a random variable $X$
$h_{ij}$	Main channel coeficcient
$g_{ij}$	Interference channel coeficcient
$\lambda_{ij}$	Average channel gain between nodes $i$ and $j$
$d_{ij}$	Distance between nodes $i$ and $j$
$\alpha$	Path-loss exponent
$P_s$	Primary Transmit Power
$P_a$	Secondary Transmit Power
$N_0$	Noise power spectral density
$\gamma$	Proper signal-tointerference-plus-noise ratio
$C_x$	Circularity Coefficient of a Signal
$R_s$	Target Primary Transmission Rate
$R$	Radius of the Circular Cell

$r_m$	Node Distance From $m$
$\Theta_m$	Angle of the Node Polar Coordinates
$\delta_m$	Fraction of the Cell Radius $R$
$\mathcal{T}_s$	Effective Secure Throughput
$\eta_s$	Secure Energy Efficiency
$M$	Number of Different System Topologies in Scenario 2
$\zeta$	Size of the Initial Genetic Algorithm Population
$\kappa$	Genetic Algorithm Crossover Fraction
$P_{a_{\max}}$	Secondary Transmitter Maximum Hardware Power

# CONTENTS

<b>1</b>	<b>INTRODUCTION</b>	<b>16</b>
1.1	Motivation and Justification . . . . .	16
1.2	Objectives . . . . .	18
1.3	Scientific Contributions . . . . .	18
1.4	Document Structure . . . . .	19
<b>2</b>	<b>THEORETICAL BACKGROUND</b>	<b>20</b>
2.1	Physical Layer Security . . . . .	20
2.2	Improper Gaussian Signaling . . . . .	23
<b>3</b>	<b>RESEARCH METHODOLOGY</b>	<b>27</b>
3.1	System Model . . . . .	27
3.1.1	Scenario 1 - nodes with static locations . . . . .	30
3.1.2	Scenario 2 - nodes uniformly distributed . . . . .	31
3.2	Secrecy Performance Analysis . . . . .	32
3.3	Optimization Problems . . . . .	36
3.3.1	Genetic Algorithms . . . . .	36
3.3.2	Problem I - Minimizing the SOP . . . . .	39
3.3.3	Problem II - Maximizing the ST . . . . .	39
3.3.4	GA parameter tuning . . . . .	40
<b>4</b>	<b>RESULTS AND DISCUSSION</b>	<b>42</b>
4.1	Scenario 1 Numerical Results . . . . .	42
4.2	Scenario 2 Numerical Results . . . . .	45
4.2.1	Primary Transmit Power Influence . . . . .	45
4.2.2	Network Topology Influence . . . . .	48

**5 CONCLUDING REMARKS** **52**

    5.1 Future Works . . . . . 53

**BIBLIOGRAPHY** **54**

## CHAPTER 1

### INTRODUCTION

#### 1.1 Motivation and Justification

Cognitive Radio (CR) is considered to be a key-technology in order to promote a more efficient spectrum usage, since it is an intelligent system capable of learning its surroundings and adapting its parameters. Allowing unlicensed users to share the same frequency band of licensed users can be achieved by using one of the following CR protocols: overlay, underlay and interweave (Goldsmith *et al.*, 2009).

In the underlay protocol, unlicensed users may transmit if the interference caused at licensed users is kept below an acceptable threshold. Unlicensed and licensed users are also called Secondary Users (SU) and Primary Users (PU), respectively. The concurrent transmissions in the overlay protocol is based on interference cancellation, whereas in the interweave protocol SUs must be able to detect spectrum holes in the licensed frequency band in order to communicate.

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 facilitate malicious attacks on the legitimate channels, such as eavesdropping. 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 the secure exchange of messages between devices.

Traditionally, the security of communications networks is obtained through data cryptography and key-distribution techniques at higher layers (Zou *et al.*, 2016). Nonetheless, everyday 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 the access to encrypted data relatively easy, 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 (Barros and Rodrigues, 2006). PLS is based on the concept of information-theoretic perfect secrecy, whose goal is to guarantee higher mutual information in the legitimate links ( $SU \leftrightarrow SU$  or  $PU \leftrightarrow PU$ ), in comparison to that of the eavesdropper link (Zou *et al.*, 2016, Chen *et al.*, 2017).

In this way, most existing PLS techniques attempts to improve the legitimate channels quality in comparison to that of 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. However, independently of the technique employed, the use of Proper Gaussian Signaling (PGS), i.e. signals with their in-phase and quadrature parts uncorrelated, to transmit information is practically taken for granted in the vast majority of the works found thus far.

That is no surprise, since PGS presents optimal performance in terms of achievable transmission rates for several known transmission schemes/scenarios. However, PGS benefits are questionable in interference-limited scenarios, which is the case of CR networks (Lameiro *et al.*, 2015, Lagen *et al.*, 2016).

Recently, Improper Gaussian Signaling (IGS) has been used to improve the performance of systems subject to interference constraints regarding achieving higher transmission rates (Zeng *et al.*, 2013a,b, Lameiro *et al.*, 2015, Amin *et al.*, 2016b, Gaafar *et al.*, 2017, Lameiro *et al.*, 2017). Differently from the PGS, improper (or asymmetric) signals have their in-phase and quadrature components correlated or with uneven powers (Lagen *et al.*, 2016). Therefore, when a transmitter uses improper signals, which have lower differential entropy than proper ones (Neeser and Massey, 1993), and interference is treated as noise, it is possible to increase the achievable rates in scenarios with interference

constraints (Santamaria *et al.*, 2018).

Nonetheless, the aforementioned works exploit IGS to improve the system performance but are not concerned with the information security of the studied systems. However, if the transmission rate of legitimate users with interference constraints is related to the use of improper signals, then the security at the secondary network can be improved through the use of IGS. Finally, exploiting this characteristic of improper signals to enhance the system security performance has not been studied in the literature yet, being a novel research area.

## 1.2 Objectives

The main goal of this research is to demonstrate the application and feasibility of IGS for secrecy purposes in CR networks. Specific goals, in order to achieve the main objective, are:

- To make a theoretical background of the most relevant subjects to the thesis;
- To analyze the secrecy performance of underlay CR networks in which the SUs are subject to eavesdropping and transmit using IGS;
- To provide a design framework which optimizes system performance parameters while maintaining an acceptable Quality of Service (QoS) at the PUs.

## 1.3 Scientific Contributions

Finally, a list with papers containing the findings of this doctorate research and submitted to the academic community is presented below. The first one is regarding the second specific goal proposed above, and the second work refers to the third specific objective of this dissertation. In addition, the third work is a correlated work, which only studied PLS but not with the adoption of IGS.

1. G. de Oliveira, S. Mafra, S. Montejo-Sánchez and E. Fernández, “Secrecy In Cognitive Radio Networks Using Improper Gaussian Signaling,” Published at the **IEEE Communications Letters**, in July, 2018;
2. G. de Oliveira, Evelio Fernández, S. Mafra, S. Montejo-Sánchez, C. Azurdia-Meza, “Optimal Improper Gaussian Signaling for Physical Layer Security in Cognitive Radio Networks,” Submitted to the **Security and Communication Networks** journal, in July, 2018;
3. G. de Oliveira, S. Mafra, and E. Fernández, “Secure Switch and Stay Combining With Multiple Antennas In Cognitive Radio Networks,” Published at **Simpósio Brasileiro de Telecomunicações (SBrT)**, in September, 2017;

## 1.4 Document Structure

The rest of this document is organized as follows: Chapter 2 gives a brief introduction to PLS and IGS, presenting the theoretical background and some related works to the understanding of this research. Chapter 3 shows the methodology adopted to achieve the found results, which are presented in Chapter 4. In addition, Chapter 5 concludes this dissertation, as well as propose some future works within its subject.

## CHAPTER 2

### THEORETICAL BACKGROUND

#### 2.1 Physical Layer Security

The Open Systems Interconnection (OSI) protocol architecture is composed by layers: Application, Transport, Network, Medium Access Control and Physical. Whether it is a wired or a wireless communication system, data packets sent from one user pass through all the layers at a transmitter node, which results in an encapsulated packet. Then, the packet is transmitted through the wired or wireless medium, and finally is decapsulated at a receiver user node.

Information transmitted by these packets are vulnerable to security threats, such as computer hacking, data forging, financial information theft and eavesdropping. Hence, some security requirements were defined, namely (Zou *et al.*, 2016):

- authenticity: related to identifying the legitimate identity of a system node;
- confidentiality: only intended users should be able to access the data;
- integrity: the information transmitted must be accurate and capable of being decoded at the receiver side;
- availability: guarantee that legitimate and intended users actually can access the communication medium.

These requirements are specially difficult to meet in wireless communications, due to the broadcast nature of the systems. As long as a malicious user is placed in the coverage area of a legitimate transmitter, physical-layer attacks such as eavesdropping and jamming can compromise the security of the system. In this connection, the idea behind PLS is to protect information exploring the intrinsic random characteristics of the physical medium between users (Barros and Rodrigues, 2006, Bloch *et al.*, 2008).

Traditional secrecy techniques at the higher layers are based on computational security, in which legitimate users exchange encrypted keys and, even if an eavesdropper intercepts the messages, it will not be able to decode the encryption. However, this kind of technique is based on the premise that the eavesdropper has limited computational capacity, which is no longer true.

On the other hand, PLS foundation lies on information-theoretic perfect secrecy. Independently of the users computational capacity, if the main channel has better condition than that of the wiretap channel, there is a transmission rate at which legitimate users can reliably communicate. The condition of a channel is typically measured in terms of the mutual information between two system nodes or the channel capacity: the maximum amount of information transmitted reliably from a transmitter to a receiver (Shannon, 1948, Goldsmith, 2005, Oggier and Hassibi, 2015):

$$C = \max_{p_X(x)} I\{X; Y\}, \quad (2.1)$$

where  $C$  is the channel capacity,  $I\{X; Y\}$  is the mutual information between two random variables (RV) representing the input ( $X$ ) and output ( $Y$ ) of the channel, and  $p_X(x)$  is the *a priori* probability distribution of the input alphabet. The premise is that legitimate links channel capacity is greater than illegitimate ones. Mathematically, this can be stated as:

$$C_{\text{legitimate}} - C_{\text{wiretap}} > 0, \quad (2.2)$$

where  $C_{\text{legitimate}}$  is the capacity of the channel between legitimate users and  $C_{\text{wiretap}}$  is the capacity of the channel between a legitimate transmitter and an eavesdropper. It is important mentioning that channel capacity is, in fact, an achievable rate measured in bits per second per Hertz (bits/s/Hz), for example.

One can define the probability that the difference in (2.2) falls below a predefined threshold as the Secrecy Outage Probability (SOP) of a given link:

$$\mathcal{O}_s = \Pr\{I_{\text{legitimate}} - I_{\text{wiretap}} < R_a\}, \quad (2.3)$$

where  $\mathcal{O}_s$  is the link SOP,  $I_{\text{legitimate}}$  and  $I_{\text{wiretap}}$  are the mutual informations between legitimate and illegitimate users, respectively, and  $R_a$  is a secure transmission rate, in bits/s/Hz. Hence, the SOP is a useful security metric when legitimate users do not have access to the eavesdropper Channel State Information (CSI). These situations requires the legitimate transmitter to set its secrecy rate to a constant, here represented by  $R_a$  (Bloch *et al.*, 2008).

As a matter of fact, it is impractical to assume that the legitimate transmitter is aware of the instantaneous CSI of the wiretap channel. Moreover, it would be impossible for legitimate users to ensure that the target secrecy rate ( $R_a$ ) would always be greater than the wiretap channel capacity ( $C_{\text{wiretap}}$ ) when only statistical CSI (SCSI) is available at the legitimate side (Yan *et al.*, 2014). Therefore, the secrecy performance of wireless channels can be assessed in terms of the SOP, which represents a fraction of fading realizations for which the wireless media can support a secure rate of bits per channel use (Bloch *et al.*, 2008, Yan *et al.*, 2014, Bloch *et al.*, 2015, Zou *et al.*, 2016).

Usually, diversity techniques such as using auxiliary nodes to aid in the transmission (cooperative diversity) (Mo *et al.*, 2012) or furnishing legitimate nodes with multiple antennas (antenna diversity) (Chiodi *et al.*, 2015, Zhang *et al.*, 2016) have been employed to enhance the security of CR wireless systems at the Physical Layer. Additionally, other techniques, such as beam-forming (Nguyen *et al.*, 2016), artificial noise (Fang *et al.*, 2016) and error control coding (Bloch *et al.*, 2015, Hodgson *et al.*, 2015) are also able to improve these systems secrecy performance. A comprehensive review regarding PLS for CR networks can be found in (Zou *et al.*, 2016) and in references therein.

The main point is that the techniques mentioned in the previous paragraph aims at achieving higher mutual information between legitimate users links in order to attain secrecy gains. However, in all the related works regarding PLS, it is always assumed that users transmit adopting PGS. Nonetheless, as previously mentioned in Chapter 1, employing IGS may achieve higher transmission rates in scenarios with interference constraints and, consequently, could improve the secrecy performance of these networks as well. Describing how these advantages are attained is the intention of the next section.

## 2.2 Improper Gaussian Signaling

Communication channels are inherently random, and in wireless communications the baseband of transmitted signals is represented by a complex function, i.e. a complex envelope of the real signal. In addition, in communications scenarios with interference constraints, sometimes referred to as the Interference Channel (IC), the benefits of employing IGS for secrecy reasons are related to the differential entropy of improper signals (Lagen *et al.*, 2016).

In wireless media, the amount of discrete information that could be transmitted over a specific channel is given by the differential entropy of the signals. In other words, the differential entropy could be seen as the expected number of bits required to optimally encode a message, given the probability distribution of the alphabet being used (Santamaria *et al.*, 2018). In addition, the differential entropy of a RV  $X$  with Probability Density Function (PDF)  $f_X(x)$  can be expressed as (Cover and Thomas, 1991):

$$\mathcal{H}_X = - \int_{-\infty}^{\infty} f_X(x) \ln f_X(x) dx, \quad (2.4)$$

where  $\mathcal{H}_X$  denotes the differential entropy.

As stated in Chapter 1, proper signals differ from improper ones because the latter have their in-phase and quadrature components correlated. Since there is no correlation between these components in PGS, proper signals tend to achieve higher differential entropy when compared to asymmetric ones (Neeser and Massey, 1993).

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 (Goldsmith, 2005), the premise of PLS is that if the legitimate channel has better condition than that of the eavesdropper channel, there is a transmission rate at which legitimate users can securely communicate. This is how the differential entropy of a signaling scheme is related to the secrecy performance of CR networks.

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 Multiple-Input Multiple-Output (MIMO) point-to-point channel and for the Gaussian MIMO broadcast channel, adopting PGS achieves optimal performance when it comes to maximizing achievable rates (Lagen *et al.*, 2016, Lameiro *et al.*, 2017). 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 for the transmitter with increased  $\mathcal{H}$  (Lagen *et al.*, 2016).

This is because transmitters who adopt improper signals at the IC may transmit with more power without exceeding the network interference constraint. That is to say that the interference caused by improper signals is actually less harmful than that caused by proper signals. 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 (Hellings and Utschick, 2017).

Hence, when a transmitter uses improper signals at the IC, it is possible to increase the achievable rates for this transmitter and its receiver (Zeng *et al.*, 2013a, Lameiro *et al.*, 2017, Hellings and Utschick, 2017), due to the lower differential entropy of asymmetric signals, which may result in enhanced transmit power (Santamaria *et al.*, 2018).

Several works have shown this behavior: in (Lameiro *et al.*, 2015) and (Lameiro *et al.*, 2017), the authors report that the achievable rate of the SUs increases significantly when adopting IGS, but only when the gain of the interference channel surpass a limit that depends on the rate achieved by the interfered user. In addition, the performance of a Full-Duplex relay adopting IGS to alleviate its residual self-interference was examined in (Gaafar *et al.*, 2016b). In (Amin *et al.*, 2016a), (Gaafar *et al.*, 2016a) and (Gaafar *et al.*, 2017) the outage performance of different CR network configurations is analyzed when the SU transmits with IGS: a single hop system, a system comprising an alternate relaying scheme and a system with in-band Full-Duplex nodes, respectively.



Therefore, it would be possible to exploit these characteristics to obtain higher mutual information between legitimate users in interference-constrained networks, which would, consequently, guarantee better secrecy performance.

However, mathematically, PGS can be completely defined in terms only of the transmitted signals covariance matrices. On the other hand, to completely define improper signals the second-order statistics need to be fully specified, i.e., one must characterize not only the covariance matrices of the signals, but also the pseudo-covariance ones. As a matter of fact, PGS can be considered as a particular case of IGS. For this reason, the following definitions are necessary to elucidate some aspects about improper complex signals (Neeser and Massey, 1993, Schreier and Scharf, 2003).

*Definition 1:* The variance and pseudo-variance of a zero mean complex stationary signal  $Z[t]$  are defined, respectively, as  $\sigma_Z^2 = \mathbb{E}[|Z|^2] = \mathbb{E}[(Z - \mu_Z)(Z - \mu_Z)^*]$  and  $\tilde{\sigma}_Z^2 = \mathbb{E}[Z^2] = \mathbb{E}[(Z - \mu_Z)(Z - \mu_Z)]$ , where  $\mu_Z$  is the expected value of  $Z$ ,  $\mathbb{E}[\cdot]$  is the expected value operator and  $*$  is the complex conjugate operator.

*Definition 2:* A complex stationary signal  $Z[t]$  with  $\tilde{\sigma}_Z^2 = 0$  is called proper, otherwise it is called improper.

*Definition 3:* The impropriety degree of a complex stationary signal  $Z[t]$  is measured by its circularity coefficient  $C_Z = |\tilde{\sigma}_Z^2|/\sigma_Z^2$ , and  $0 \leq C_Z \leq 1$ .

Note that the circularity coefficient of a complex signal represents the correlation between the real and imaginary parts of the signal. Moreover, if a complex improper signal is stationary, its variance, pseudo-variance and, consequently, circularity coefficient are time invariant.

Besides the higher transmission rates that can be achieved by IGS for the IC, the interest towards IGS has become greater lately, since it is possible to have extra degrees of freedom for optimization when adopting IGS. This is because the signals' received power does not depend only on the channel quality, but also on the circularity coefficient  $C_Z$  (Ho and Jorswieck, 2012, Zeng *et al.*, 2013a). These extra degrees of freedom give opportunities to achieve even higher transmission rates in interference constrained networks, which is the case of CR networks.

The next chapter (Chapter 3) draw on these concepts to elucidate the methodology used in this research, presenting the proposed system model as well as the means to achieve the results shown in Chapter 4.

## CHAPTER 3

### RESEARCH METHODOLOGY

In order to achieve the goals of this research, a system to assess the performance of an underlay CR network in which secondary transmissions are subject to eavesdropping is proposed. Then, for the same system model, two scenarios were evaluated: a more simple one, where nodes locations were arbitrarily defined - Scenario 1; and another more realistic one, where nodes locations were uniformly distributed over a cell of circular area - Scenario 2. The information regarding the system model in the following section pertains to both proposed scenarios. Their singularities regarding the system topology are detailed within their own subsections.

#### 3.1 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 the primary transmitter S only uses PGS, whereas Alice can employ either PGS or IGS. This assumption is made since in the underlay protocol there is no cooperation between PUs and SUs (Lameiro *et al.*, 2015, Amin *et al.*, 2016b).

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 (Chen *et al.*, 2016). 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 the adaptive transmission scheme presented in (Yan *et al.*, 2014), (Chiodi *et al.*, 2015) and (Oliveira *et al.*, 2018), in the optimization framework (Yan *et al.*, 2014) and in the cooperative scheme (Bordon *et al.*, 2017). In other words, Alice is only aware of other channel gains expected value, except 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 (Fan *et al.*, 2016).

The average channel gains are given by  $\lambda_{ij} = d_{ij}^{-\alpha}$ , where  $d_{ij}$  is the distance between nodes and  $\alpha$  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 received signals at D, B and E at time  $t$  are expressed, respectively, by

$$y_d[t] = \sqrt{P_s}h_{sd}x_s[t] + \sqrt{P_a}g_{ad}x_a[t] + n_d[t], \quad (3.1)$$

$$y_b[t] = \sqrt{P_a}h_{ab}x_a[t] + \sqrt{P_s}g_{sb}x_s[t] + n_b[t], \quad (3.2)$$

$$y_e[t] = \sqrt{P_a}h_{ae}x_a[t] + \sqrt{P_s}g_{se}x_s[t] + n_e[t], \quad (3.3)$$

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), with power spectral density  $N_0$ , at D, B and E, respectively.

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. One can note that when normalizing the analysis with respect a unitary bandwidth, the noise variance is equal to the noise power spectral density.

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

$$\gamma_{ij} = \frac{P_i|h_{ij}|^2}{P_k|g_{kj}|^2 + N_0}, \quad (3.4)$$

where  $\gamma$  is the proper SINR and  $k \in \{a, s\} : k \neq i$ .

Since IGS signals are statistically circularly asymmetric, the degree of impropriety of

Alice's signal,  $x_a[t]$ , is measured by its circularity coefficient

$$C_x = |\tilde{\sigma}_{x_a}^2|/\sigma_{x_a}^2, \quad (3.5)$$

where  $\sigma_{x_a}^2 = \mathbb{E}[|x_a|^2]$  and  $\tilde{\sigma}_{x_a}^2 = \mathbb{E}[x_a^2]$  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 (Schreier and Scharf, 2003).

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. 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 (Zeng *et al.*, 2013a,b, Oliveira *et al.*, 2018):

$$\begin{aligned} C_{y_d} &= \frac{P_a |g_{ad}|^2 C_x}{P_a |g_{ad}|^2 + P_s |h_{sd}|^2 + N_0}, \\ C_{i_d} &= \frac{P_a |g_{ad}|^2 C_x}{P_a |g_{ad}|^2 + N_0}. \end{aligned} \quad (3.6)$$

Then, using (3.6), the mutual information of the S→D link can be expressed as (Zeng *et al.*, 2013a, Oliveira *et al.*, 2018):

$$I_{sd} = \log_2 \left[ (1 + \gamma_{sd}) \sqrt{\frac{1 - C_{y_d}^2}{1 - C_{i_d}^2}} \right]. \quad (3.7)$$

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

$$I_{al} = \log_2 \left[ (1 + \gamma_{al}) \sqrt{1 - C_{y_l}^2} \right], \quad (3.8)$$

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

$$C_{y_l} = \frac{P_a |h_{al}|^2 C_x}{P_s |g_{sl}|^2 + P_a |h_{al}|^2 + N_0}. \quad (3.9)$$

It is noticeable that the SUs transmission rate can only be improved with IGS by choosing  $C_{y_l}$  values that make the term inside the square root in (3.8) strictly positive. Moreover,  $C_{y_d}$  and  $C_{i_d}$ , in (3.7), must be tuned properly to guarantee the QoS at the PUs, i.e.,  $I_{sd} \geq R_s$ , where  $R_s$  denotes a target primary transmission rate.

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 (Lameiro *et al.*, 2017) and (Oliveira *et al.*, 2018), Alice's transmit power,  $P_a$ , is limited with respect to  $R_s$ . Then, making  $I_{sd} = R_s$  in (3.7), one can compute  $P_a$  as a function of  $R_s$  as

$$P_a^\dagger(C_x, R_s) = \frac{P_s \lambda_{sd} - N_0 (2^{2R_s} - 1)}{(1 - C_x^2)(2^{2R_s} - 1)\lambda_{ad}} + \sqrt{\theta_1}, \quad (3.10)$$

where:

$$\theta_1 = \frac{P_s^2 \lambda_{sd}^2 2^{2R_s} + C_x^2 (N_0^2 2^{2R_s} - (N_0 + \lambda_{sd} P_s)^2)}{(1 - C_x^2)^2 (2^{2R_s} - 1)^2 \lambda_{ad}^2}. \quad (3.11)$$

It is worth noting that all expressions from (3.7) to (3.11) return to the known PGS case when  $C_x = 0$ . As previously stated, both scenarios only differ in terms of the network topology, hence, the following subsections portray the network topology for each proposed scenario.

### 3.1.1 Scenario 1 - nodes with static locations

In this scenario, the five system nodes have their locations fixed at a given position, as depicted in Fig. 3.1.

In order to suitably select the circularity coefficient  $C_x$  in this scenario, two different settings regarding the relative distance between nodes were assessed, since channels gains

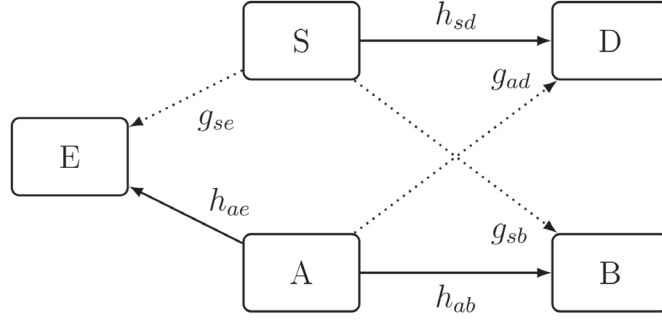


Figure 3.1: Scenario 1 System Model Topology

are directly dependent on the distance between nodes. In both settings the distances between nodes were normalized with respect to the distance between S and B ( $d_{sb} = 1.0$ ).

Hence, the following values for the remaining distances between nodes for the first and second settings were considered, respectively, (I)  $d_{ab} = d_{ad} = 0.5$ ,  $d_{sd} = d_{ae} = 0.7$  and  $d_{se} = 0.3$ ; (II)  $d_{ab} = d_{se} = 0.3$  and  $d_{ad} = d_{sd} = d_{ae} = 0.7$ . Setting I illustrates a case where it is most likely that  $\lambda_{ab} = \lambda_{ad}$ , while Setting II depicts a case in which  $\lambda_{ab} > \lambda_{ad}$ .

### 3.1.2 Scenario 2 - nodes uniformly distributed

In Scenario 2, 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

$$\begin{aligned} r_m &= \delta_m R \sqrt{\beta_{m_1}}, \\ \Theta_m &= 2\pi\beta_{m_2}, \end{aligned} \tag{3.12}$$

where  $m \in \{a, b, d, e\}$ ,  $r_m$  is the node distance from S (or A, in the case of B),  $\Theta_m$  is the angle of the node coordinates, respectively,  $\delta_m$ , with  $0 \leq \delta_m \leq 1$ , denotes a fraction of the radius  $R$ , which is not random. In addition,  $\beta_{m_1}$  and  $\beta_{m_2}$  are random numbers uniformly distributed in the real  $[0, 1]$  interval. Fig. 3.2 depicts a possible node distribution for this system topology.

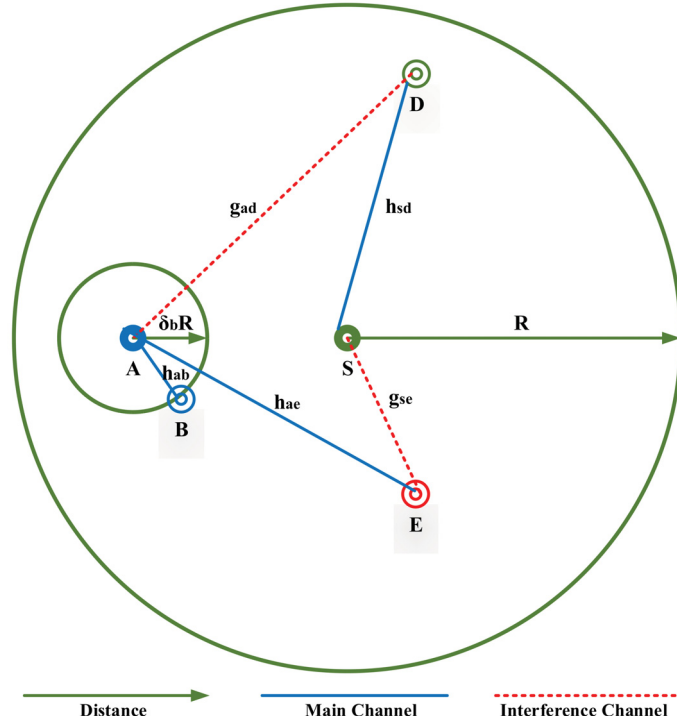


Figure 3.2: Scenario 2 System Model Topology

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.

### 3.2 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 SCS is available at the SU side and using (3.8), the SOP can be expressed as

$$\mathcal{O}_s = \Pr[I_{ab} - I_{ae} < R_a] = \Pr \left[ \frac{(1 + \gamma_{ab})^2 (1 - C_{y_b}^2)}{(1 + \gamma_{ae})^2 (1 - C_{y_e}^2)} < 2^{2R_a^{th}} \right], \quad (3.13)$$

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 (Gaafar *et al.*, 2017), that a closed-form expression for the system SOP can be expressed as (Oliveira *et al.*, 2018):

$$\mathcal{O}_s = \int_0^\psi \frac{\exp\left(-\frac{|h_{ab}|^2}{\lambda_{ab}}\right)}{\lambda_{ab}} d|h_{ab}|^2 = 1 - \exp\left(-\frac{\psi}{\lambda_{ab}}\right). \quad (3.14)$$

The upper limit of the integral in (3.14) is obtained by solving the inequality in (3.13) with respect to  $h_{ab}$ , and is found to be

$$\psi = \frac{\frac{P_s \lambda_{sb} + N_0}{P_s \lambda_{se} + N_0} \sqrt{\theta_2} - P_s \lambda_{sb} - N_0}{(1 - C_x^2) P_a}, \quad (3.15)$$

where

$$\theta_2 = C_x^2 (N_0 + P_s \lambda_{se})^2 - 2^{2R_a^{th}} (1 - C_x^2) [(C_x P_a \lambda_{ae})^2 - (P_a \lambda_{ae} + P_s \lambda_{se} + N_0)^2]. \quad (3.16)$$

The closed-form expression found in (3.14) is already a result of this research. One can note that the lower the  $\psi$  value, the lower the SOP as well. Moreover, note that  $I_{al}$ , in (3.8), decreases with the increment of  $C_x$ . However, Alice can increase its transmission power, because by transmitting improper signals, the interference caused at PUs is lower compared to what it would have been if PGS was used. Then, it is possible for the SUs to increase their achievable rate and, consequently, achieve lower SOP values. This behavior is due to the fact that complex improper signals, since its in-phase and quadrature components are correlated, has lower differential entropy compared to complex proper signals.

Thus, when interference is treated as noise, an improper interference increases the achievable rates in scenarios with interference constraints. Consequently, achieving lower SOP values depends on a trade-off between how much improper will the signal be and with how much power will it be transmitted, i.e., a trade-off between  $C_x$  and  $P_{a,IGS}$ , without forgetting to meet the  $R_s$  constraint. In addition, since the SOP is related to the

ratio between  $I_{ab}$  and  $I_{ae}$ , there is a high dependency of the SOP on the average channel gains and on the distance between nodes.

In practical implementations, Alice and Bob can always decide to transmit with PGS if better results can be achieved regarding some performance metric (SOP or power consumption). In terms of the SOP, it is only necessary to verify the inequality  $\mathcal{O}_{s,IGS} < \mathcal{O}_{s,PGS}$ : if true, use IGS, else, use PGS. Although, solving the inequality for  $C_x$  is a very complicated task, meanwhile its numerical solution is trivial. This is why in Scenario 2 the assessment of the system performance is made by means of optimization problems.

In a scenario where it is only mandatory to respect a SOP threshold, one could even test what scheme, PGS or IGS, meets the condition and, in case both PGS and IGS are below the SOP threshold, SUs could pick the one whose power consumption or computational cost is lower.

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 one could 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 (3.14) with respect to  $R_a$  and making  $\mathcal{O}_s = \mathcal{O}^{th}$  gives:

$$R_a(\mathcal{O}^{th}) = \frac{1}{2} \log_2 \left[ \frac{\theta_3}{\theta_4} \right], \quad (3.17)$$

where

$$\theta_3 = C_x^2(N_0 + P_s\lambda_{se})^2 - \frac{(N_0 + P_s\lambda_{se})^2(N_0 + P_s\lambda_{sb} - (1 - C_x^2)P_a\lambda_{ab} \log [1 - \mathcal{O}^{th}])^2}{(N_0 + P_s\lambda_{sb})^2}, \quad (3.18)$$

and

$$\theta_4 = (1 - C_x^2) \left( (C_x P_a \lambda_{ae})^2 - (N_0 + P_a \lambda_{ae} + P_s \lambda_{se})^2 \right). \quad (3.19)$$

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 (Yan *et al.*, 2014):

$$\mathcal{T}_s = R_a(1 - \mathcal{O}_s), \quad (3.20)$$

where  $R_a$  may be substituted by  $R_a^{th}$  and  $\mathcal{O}_s$  by  $\mathcal{O}^{th}$ , depending on the case: when making  $\mathcal{O}_s = \mathcal{O}^{th}$  in (3.20), it is possible to find  $R_a$  using (3.17); on the other hand, when making  $R_a = R_a^{th}$  in (3.20) one can find  $\mathcal{O}_s$  using (3.14).

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 (Monteiro *et al.*, 2015), the authors propose a variation of the effective ST, limiting  $\mathcal{T}_s$  as:

$$\mathcal{T}_s^{th} = \begin{cases} \mathcal{T}_s, & \text{if } \mathcal{O}_s \leq \mathcal{O}^{th}; \\ 0, & \text{if } \mathcal{O}_s > \mathcal{O}^{th}. \end{cases} \quad (3.21)$$

Hence, the  $\mathcal{O}^{th}$  is taken into account when calculating the effective ST in the afterwards optimization problems, and  $\mathcal{T}_s$  is obtained using (3.21).

Additionally, it is possible to define the SEE as the ratio between the effective ST and the secondary transmit power. Using (3.21), the SEE can be expressed as

$$\eta_s = \frac{\mathcal{T}_s}{P_a}, \quad (3.22)$$

where  $\eta_s$  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 (Zeng *et al.*, 2013a, Lagen *et al.*, 2016, Gaafar *et al.*, 2017, Lameiro *et al.*, 2017, Oliveira *et al.*, 2018), finding 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.

Therefore, in the next section two optimization problems are defined, one for the SOP and another involving  $R_a$ . These optimization problems were solved only for the analysis of Scenario 2, since in Scenario 1 we were concerned in validating the feasibility of the analytical expression found as a result of adopting IGS for secrecy reasons in CR networks.

### 3.3 Optimization Problems

The goal is to minimize the SOP given in (3.14) and maximize the ST given in (3.21) by finding optimal values of  $P_a$  and  $C_x$  simultaneously, as well as respecting the underlay interference constraint given by (3.10). In this work, we resort to Genetic Algorithms (GAs) to solve the proposed optimization problems. That is why in the next subsection a brief explanation on the basis of GAs and why they are suitable for this research is presented.

#### 3.3.1 Genetic Algorithms

The idea of employing optimization techniques in this research is to provide a design framework which optimizes system parameters while maintaining an acceptable QoS at the PUs. The objective is to optimize some secrecy performance metrics, e.g. minimizing the SOP, or pursuing maximal secure rates. However, finding optimal expressions through classic differential optimization techniques is not trivial. For example, the computational cost associated to an exhaustive search method makes it unfeasible as an option. On the other hand, a GA is more suitable for this kind of problem. While it is true that for

smooth and unimodal spaces GAs may perform poorly when compared to gradient-ascent algorithms, they tend to be competitive or even surpass the performance of other non domain-specific methods when (Mitchell, 1998):

- the search space is large or it is known that it is not perfectly smooth and unimodal;
- the search space is not well understood;
- the task does not require a global optimum to be found or, in other words, if finding a sufficiently good solution quick is good enough.

One can note that all the aforementioned characteristics are common to the problem of this research. Therefore, using GAs is suitable for this kind of problem since the expressions are non linear and the nodes locations in the system are stochastic. Moreover, since we are focused on demonstrating the feasibility of adopting IGS to enhance the secrecy performance of CR networks, regarding some performance metrics, using GAs represents a feasible technique (Lopez *et al.*, 2014).

Basically, a GA firstly creates a random set of feasible individuals that solve the problem. A candidate may be composed by any number of system parameters or variables. After this first generation is tested, the best-fitted candidates are kept for the next generation, sometimes called the “elite count” or “champions”. Other individuals from this first generation are subjected to crossover and mutation operations (Mehboob *et al.*, 2016).

Crossover and mutation changes 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.

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 in Scenario 2 and, consequently, of the mutual information between them, the GA that optimizes the system performance metrics is run several times, one for each network node distribution. In each topology,

the positions of the nodes are drawn again, according to (3.12). After running for  $M$  different topologies, the mean of the optimized parameters are computed, analogous to a Monte-Carlo simulation. Hence, for each one of the  $M$  different network topology, the GA is run until the maximum number of generations.

---

**Algorithm 1** Genetic Algorithm
 

---

```

1:  $p \leftarrow 1$ 
2: create a random initial population  $\rho_0$  of size  $\zeta$ 
3: set current population  $\rho_p$  equal to  $\rho_0$ 
4: repeat
5:   evaluate each member of  $\rho_p$  according to its fitness value
6:   assign a rank to each member of  $\rho_p$  based on its fitness
7:   compute the expectation of each member of  $\rho_p$  based on its rank
8:   if  $P_a^* < P_a^\dagger$  then
9:      $P_a \leftarrow P_a^*$ 
10:  else
11:     $P_a \leftarrow P_a^\dagger$ 
12:  end if
13:  select  $\zeta_{pp}$  parent individuals
14:  create  $\zeta_c$  crossover children from the parents
15:  create  $\zeta_m$  mutation children from the parents
16:  select  $\zeta_e$  elite individuals
17:  replace the current population
18:   $p \leftarrow p + 1$ 
19: until the maximum number of generations is reached

```

---

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. Note that the main objective of the optimization process described in Algorithm 1 is the adequate optimization of  $C_x$  and  $P_a$  at the same time. Thus, both variables compose individuals of each population, and their fitness value depends on the performance metric being assessed.

In addition, denoting  $\zeta_c$ ,  $\zeta_m$  and  $\zeta_e$  as the number of crossover, mutation and elite individuals in the population, the population size is given by  $\zeta = \zeta_c + \zeta_m + \zeta_e$ . If  $\zeta$  and  $\zeta_e$  are fixed values, the number of crossover and mutation children can be determined through the crossover fraction, defined as  $\kappa = \zeta_c / (\zeta_c + \zeta_m)$ .

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

### 3.3.2 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:

$$\begin{aligned}
 \min_{P_a, C_x} \quad & \mathcal{O}_s(P_a, C_x, R_a^{th}) \\
 \text{s.t.} \quad & 0 \leq P_a \leq P_{a_{max}}, \\
 & 0 \leq C_x \leq 1, \\
 & R_a = R_a^{th}.
 \end{aligned} \tag{3.23}$$

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 (3.10). With the found values of  $\mathcal{O}_s^*$ , the effective ST (3.21) and the SEE (3.22) can be obtained subsequently, given a predefined  $R_a^{th}$ .

### 3.3.3 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 sub-optimal approach is to maximize the secondary achievable rate in (3.17), and Problem II can then be formulated as

$$\begin{aligned}
 \max_{P_a, C_x} \quad & R_a(P_a, C_x, \mathcal{O}^{th}) \\
 \text{s.t.} \quad & 0 \leq P_a \leq P_{a_{max}}, \\
 & 0 \leq C_x \leq 1, \\
 & \mathcal{O}_s = \mathcal{O}^{th}.
 \end{aligned} \tag{3.24}$$

Similarly to Problem I, with the found values of  $R_a^*$ , the effective ST (3.21) and the SEE (3.22) can be obtained subsequently.

### 3.3.4 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 for the proposed system model Scenario 2. 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, starting with 10 generations.

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 can not 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 3.1.

Table 3.1: Simulation Parameters

$R = 100$ units of length	$N_0 = 1$
$P_{a_{max}} = 20$ dB	$P_s = 20$ dB
$R_s = R_a = 1$ bits/s/Hz	$\delta_a = \delta_d = \delta_e = 1$
$\delta_b = 0.1$	$\alpha = 4$
$\mathcal{O}^{th} = 0.1$	$M = 10^4$

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.



Then, the expected value and the variance associated with the  $C_x$  value for several different GA starting points were evaluated (Table 3.2). Each evaluation with different starting points was called an experiment. The simulation parameters were the same as those presented in Table 3.1.

Table 3.2:  $C_x$  expected value and variance for different GA starting points

<b>Experiment</b>	1	2	3	4	5
$\mathbb{E}[C_x]$	0.2247	0.2329	0.2321	0.2314	0.2275
$\text{Var}[C_x]$	0.1443	0.1486	0.1479	0.1475	0.1482

One can see that there is no significant variation in the results, regardless of the initial values used by the GA. This result indicates that the GA is converging to values close to a global optimum.

Hence, after tuning the aforementioned parameters, to obtain the results shown in Chapter 4 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).

## CHAPTER 4

### RESULTS AND DISCUSSION

This Chapter presents results regarding both topology scenarios, illustrating the previous findings of this research.

#### 4.1 Scenario 1 Numerical Results

In this section, numerical results are provided in order to illustrate the findings for the scenario where nodes locations were static. For the Scenario 1, it was assumed that transmit power of the secondary source S was  $P_s = 10$  dB. Moreover, in the following sequence of figures, Monte Carlo simulations are represented by red circles.

In Fig. 4.1 the system SOP (3.14) was analyzed as a function of  $C_x$ , assessing whether IGS is beneficial to the SOP. It is shown that employing PGS is a slightly better strategy for the SUs when  $P_{a_{\max}} < P_s$  in both distance settings. When  $P_{a_{\max}} = P_s = 10$  dB, there is a clear behavior change among the two distance settings. For distance Setting I, IGS can be beneficial to the system performance, as noticeable from the dashed blue lines.

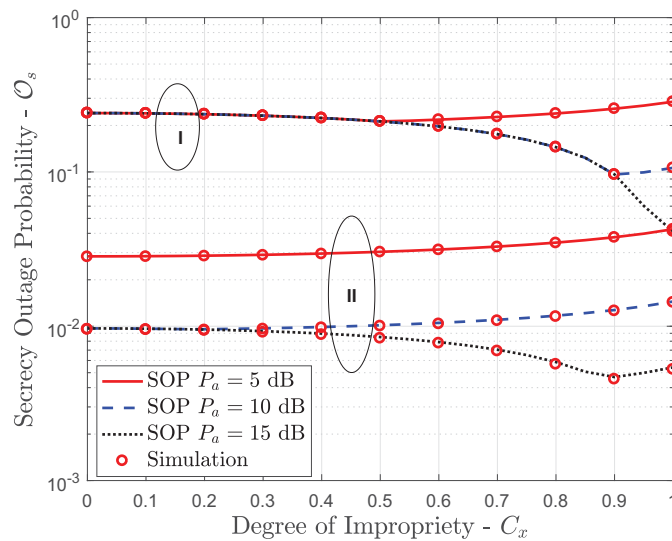


Figure 4.1: Scenario 1 Secrecy Outage Probability *vs.* the degree of impropriety

In addition, when  $P_{a_{\max}} > P_s$ , employing IGS is always a better strategy for the SUs. This result confirms the premise that IGS allows Alice to enhance its transmit power without degrading the performance of the primary network. However, Settings I and II differ with respect to the optimal degree of impropriety to be employed. Hence, due to the analysis presented in Fig. 4.1 the results hereinafter are obtained adopting  $C_x = 1.0$  for distance Setting I and  $C_x = 0.9$  for distance Setting II.

Now, in order to analyze the system secrecy performance when Alice employs PGS or IGS, in Fig. 4.2 the SOP is plotted as a function of  $P_{a_{\max}}$ . It is noticeable that IGS can be beneficial to the secrecy performance of the system if Alice's power is high enough. At some point, the SOP when Alice employs PGS remains constant, indicating that no more benefits could be obtained even when  $P_{a_{\max}}$  increases. From this point on, adopting IGS is a better strategy for the SUs. This result is aligned with the behavior difference between the two distance settings, and the exchange point to obtain lower SOP with IGS is related to the ratio between  $P_s$  and  $P_{a_{\max}}$ . Thus, when adopting an optimal  $C_x$ , it is possible to attain better system performance without affecting the PU performance for both distance settings.

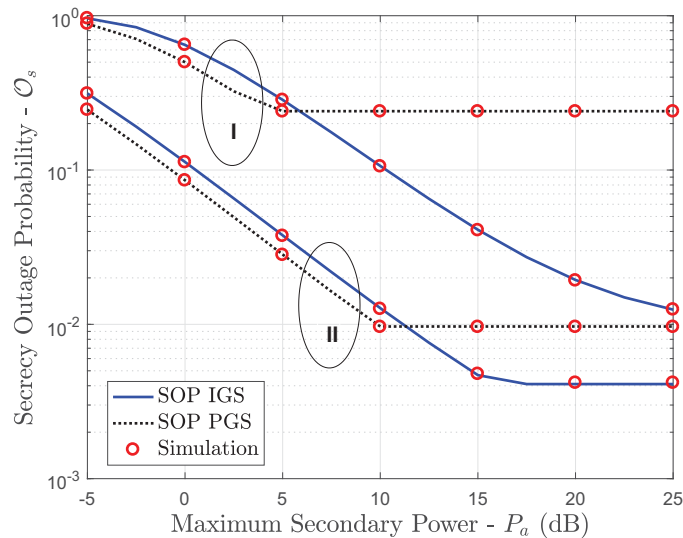


Figure 4.2: Scenario 1 Secrecy Outage Probability *vs.* the maximum Alice power

Fig. 4.3 shows the SOP as a function of  $P_s$  and considering  $P_{a_{\max}} = 15$  dB. It can be noticed that, as  $P_s$  increases, employing IGS is not the best strategy for the SU in

terms of the SOP for both distance settings. However, when  $P_s < P_{a_{\max}}$  there is a larger performance gain region for IGS over PGS in distance Setting I.

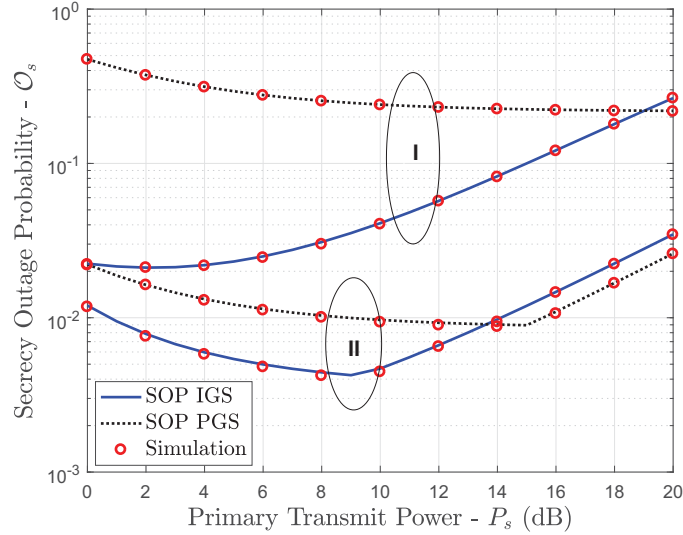


Figure 4.3: Scenario 1 Secrecy Outage Probability *vs.* the Source transmission power

A last interesting analysis is to observe the performance of the system in Scenario 1 when Eve is no longer at a fixed position. In this scenario, S, D, A and B are located at coordinates  $[1, 1]$ ,  $[0.5, 0.5]$ ,  $[1, 0]$  and  $[1.5, 0]$  on a bi dimensional Cartesian plane, respectively. Eve coordinates on this Cartesian plane are denoted by  $[x, y]$ , where  $x = y = \rho$ . Through Monte-Carlo simulations, Fig. 4.4 shows the SOP as a function of  $\rho$  while Eve moves from  $[0, 0]$  to  $[1, 1]$ , with increments of 0.1 in both axis simultaneously.

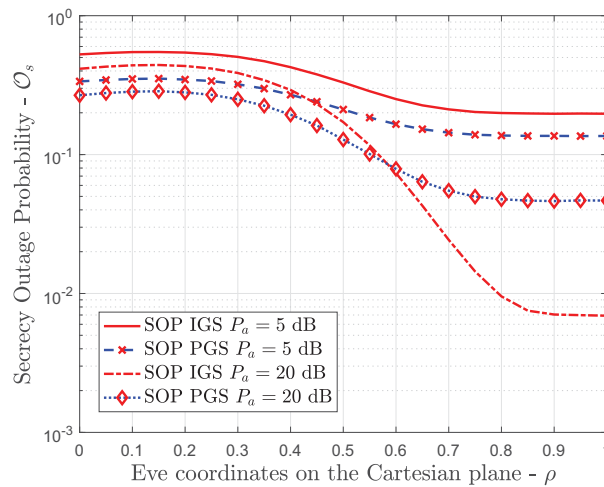


Figure 4.4: Scenario 1 Secrecy Outage Probability for the moving eavesdropper topology

As Eve moves farther from D, the value of the system SOP decreases for both PGS and IGS signaling. However, when  $\rho > 0.6$ , IGS attains better performance than PGS, since it can reach lower values of SOP when  $P_{a_{\max}} = 20$  dB. This result confirms the potential gain that can be attained using IGS for security interests, indicating that the initial idea of this work is feasible in practice.

## 4.2 Scenario 2 Numerical Results

This section presents the results of the analysis when the location of the nodes were uniformly distributed over a circular area cell. 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 3.1.

### 4.2.1 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 4.1.

Table 4.1: Optimal degree of impropriety and secondary transmit power *vs.* 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
$P_a^*[\text{dB}] \min \mathcal{O}_s$	17.65	18.98	19.61	19.66	19.47
$P_a^*[\text{dB}] \max R_a$	16.73	18.11	18.76	18.92	18.97

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 Fig. 4.5, the use of GA allows to obtain 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.

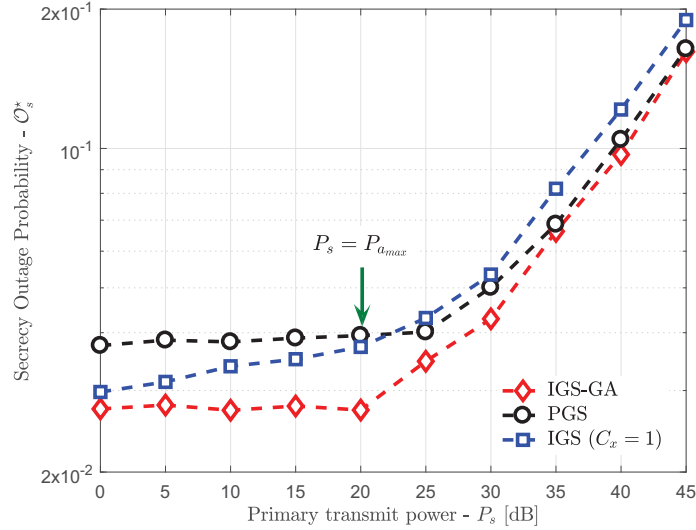


Figure 4.5: Scenario 2 Optimal Secrecy Outage Probability *vs.* the primary transmit power

When maximizing  $R_a$  (Fig. 4.6), the system performance, assessed through the effective ST, also deteriorates 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. Fig. 4.7 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.

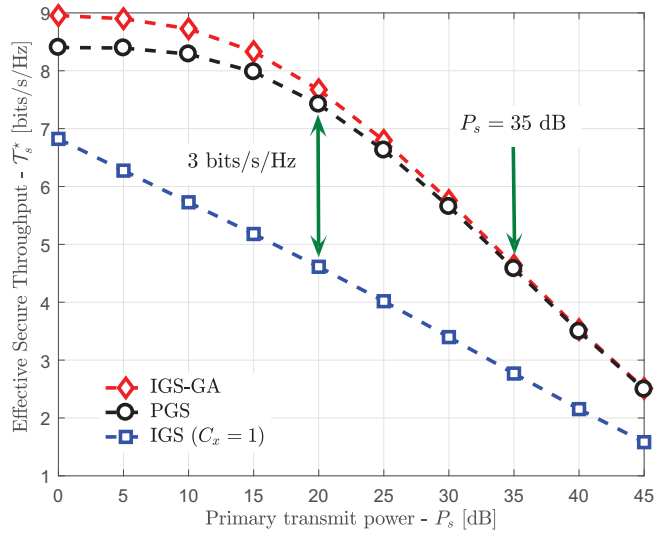


Figure 4.6: Scenario 2 Optimal Secure Throughput *vs.* the primary transmit power - maximizing the secrecy data rate

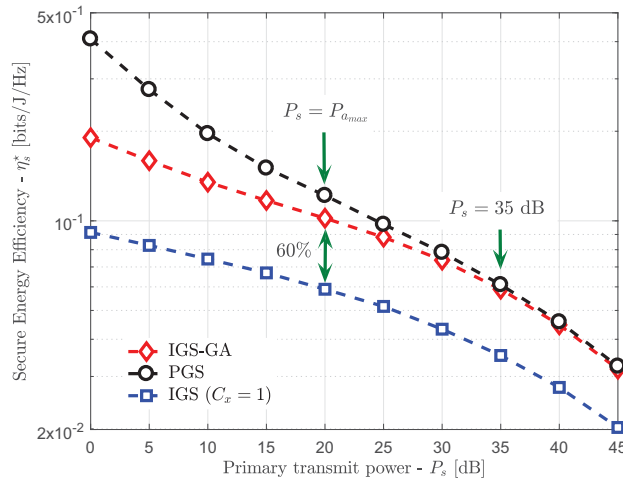


Figure 4.7: Scenario 2 Optimal Secure Energy Efficiency *vs.* the primary transmit power - maximizing the secrecy data rate

This is an expected result, since the SEE metric,  $\eta_s$ , 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.

## 4.2.2 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 4.2 shows the optimal values of the degree of impropriety and of the secondary transmit power for each value of  $\delta_a$ . 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. Regarding the secondary transmit power,  $P_a$  almost reaches  $P_{a_{max}}$  independently of the  $\delta_a$  value, either when minimizing  $\mathcal{O}_s$  or when maximizing  $R_a$ .

Table 4.2: Optimal degree of impropriety and secondary transmit power *vs.* the  $\delta_a$  portion of the cell radius

$\delta_a$	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
$P_a^* [\text{dB}] \min \mathcal{O}_s$	16.23	19.65	19.61	19.60	19.64
$P_a^* [\text{dB}] \max R_a$	5.53	18.58	19.01	19.19	19.31

Fig. 4.8 shows the optimal SOP as a function of  $\delta_a$ . 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, Fig. 4.9 depicts the effective ST as a function of  $\delta_a$ . This result was attained using (3.21) 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  $\delta_a$  also increases.

Moreover, in terms of the effective ST, the performance of the IGS-GA is better for all values of  $\delta_a$ , 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



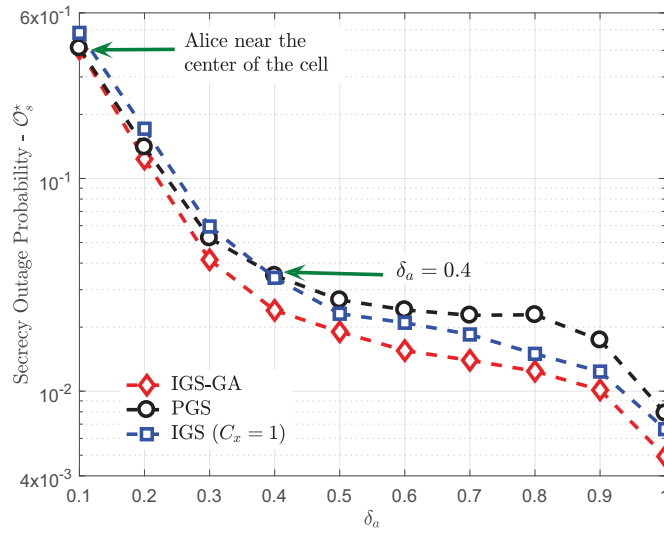


Figure 4.8: Scenario 2 Optimal Secrecy Outage Probability *vs.* the  $\delta_a$  portion of the cell radius

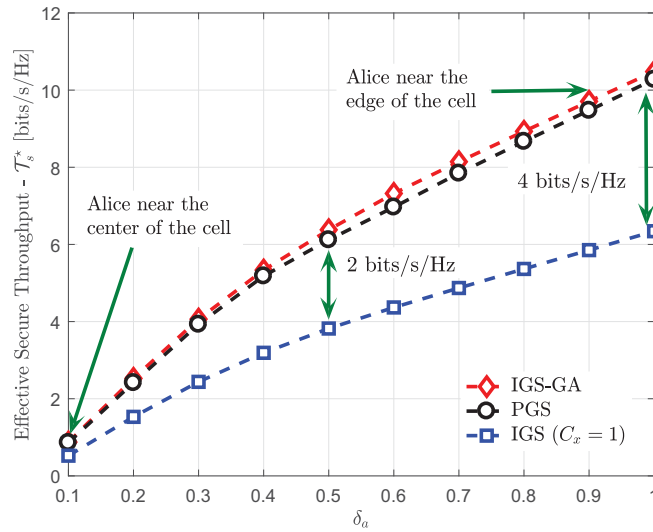


Figure 4.9: Scenario 2 Optimal Secure Throughput *vs.* the  $\delta_a$  portion of the cell radius - maximizing the secrecy data rate

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.  $\delta_b$  increases. The results are shown in Table 4.3 and Fig. 4.10 and 4.11. One can note that  $C_x^*$  remains almost constant as  $\delta_b$  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 are being used.

Table 4.3: Optimal degree of impropriety and secondary transmit power *vs.* the  $\delta_b$  portion of the Alice cell radius

$\delta_b$	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
$P_a^* [\text{dB}] \min \mathcal{O}_s$	19.59	18.29	16.31	14.27	11.23
$P_a^* [\text{dB}] \max R_a$	18.56	13.70	9.83	6.96	4.43

Observing Table 4.3, 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  $\mathcal{O}^{th}$ .

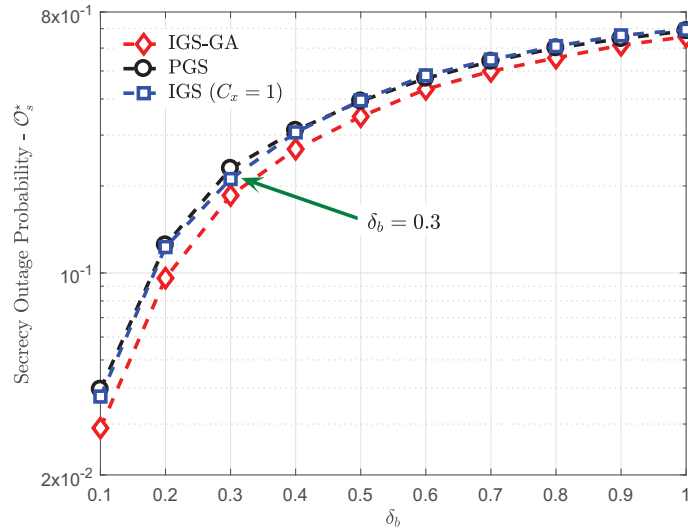


Figure 4.10: Scenario 2 Optimal Secrecy Outage Probability *vs.* the  $\delta_b$  portion of the Alice cell radius

Regarding the  $\mathcal{O}_s^*$  as a function of  $\delta_b$ , shown in Fig. 4.10, 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  $\delta_b$ , depicted in Fig. 4.11, 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.

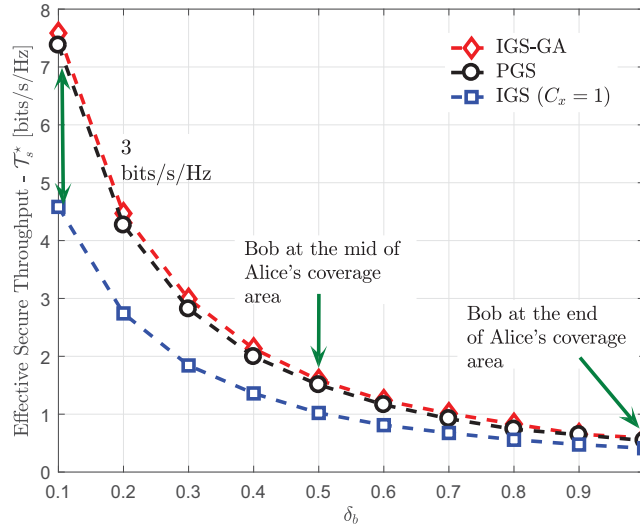


Figure 4.11: Optimal Secure Throughput *vs.* the  $\delta_b$  portion of the Alice cell radius - maximizing the secrecy data rate

The analysis based on the distance between Alice and Bob also allows to demonstrate 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 almost 66% of the effective ST when a maximally improper signal is employed.

## CHAPTER 5

### CONCLUDING REMARKS

Based on the fact that asymmetric signals can achieve higher transmission rates in networks with interference constraints, due to their lower differential entropy when compared to proper ones, we proposed employing Improper Gaussian Signaling to enhance the secrecy performance of wireless networks.

Specifically, we focused on the Physical Layer Security analysis of an underlay Cognitive Radio network, in which unlicensed users are being eavesdropped and may transmit using improper signals. The PLS metrics adopted in this research were three: the Secrecy Outage Probability, the Secure Throughput and the Secure Energy Efficiency.

In the proposed system model, we assumed quasi-static Rayleigh block fading and single antenna nodes. In addition, we considered that only statistical CSI was available at the secondary side, except for the direct link between the secondary transmitter and receiver. For this system model, we analyzed two different topology scenarios: one where the location of the network nodes is arbitrarily defined (Scenario 1); and another one more realistic, in which network nodes were randomly distributed within the coverage area of a primary transmitter (Scenario 2).

Studying Scenario 1, a closed form expression for the Secrecy Outage Probability was derived, and the Results showed that IGS can be beneficial to the system secrecy performance, as initially expected. These results are the first regarding the use of IGS to enhance the PLS of CR networks.

Later, when analyzing Scenario 2 and using the SOP analytical expression previously derived, the secrecy performance of the proposed network was optimized with the aid of Genetic Algorithms. For this optimization assessment, 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.

## 5.1 Future Works

The main ideas for future research include extending the secrecy analysis to different system models when users are able to employ improper signals. For example:

- analyzing the secrecy performance of CR networks in the interweave protocol, extending the research made in Hedhly *et al.* (2017);
- analyzing the secrecy performance of CR networks in the overlay protocol, extending the research made in Amin *et al.* (2016a);
- propose a system model in which PUs and SUs are able to employ IGS and cooperate with each other to achieve better secrecy performance at both sides of CR networks, as in Al-Talabani *et al.* (2016);
- propose lower complexity algorithms which enhance not only the secrecy performance of the system, but also lower the computational costs of the joint optimization proposed in this research.

Other possible unfolding of this research would comprise adding other PLS techniques to the already proposed system model with IGS, such as diversity and cooperative diversities, beam-forming or artificial noise. Some possible ideas are listed below:

- considering nodes with directional antennas based on the knowledge of the secondary receiver location;

- consider cooperative communication scenarios, in which Full-Duplex relay nodes could transmit adopting improper signals, since a Full-Duplex scheme involves the auto interference of the relay node (Gaafar *et al.*, 2016b, Kariminezhad *et al.*, 2017);
- consider the possibility of SUs transmit artificial noise to confuse the eavesdropper in a given time slot. This noise could be proper, whereas the message to the legitimate secondary receiver itself could be transmitted with improper signals.

Future works could involve the proposition of better coding schemes for improper signals, aiming to find more secure alphabets for wireless communications networks with interference constraints, inspired by the works presented in Bloch *et al.* (2015) and Santamaria *et al.* (2018).

Finally, stepping out of the secrecy area, future works could focus on the performance analysis of network coding coupled with the adoption of improper signals, extending works such as the one presented by Gabriel *et al.* (2018). Another interesting research line which could be explored is the application of IGS coupled with the promising paradigm of the network slicing, in order to enhance achievable transmission rates in sliced portions of a shared network.

## BIBLIOGRAPHY

- AL-TALABANI, A., DENG, Y., NALLANATHAN, A., and NGUYEN, H. X., *Enhancing Secrecy Rate in Cognitive Radio Networks via Multilevel Stackelberg Game*, **IEEE Communications Letters**, 20(6), 1112–1115, doi:10.1109/LCOMM.2016.2541658, 2016.
- AMIN, O., ABEDISEID, W., and ALOUINI, M. S., *Overlay Spectrum Sharing using Improper Gaussian Signaling*, **IEEE Journal on Selected Areas in Communications**, 35(1), 1–1, doi:10.1109/JSAC.2016.2632600, 2016a.
- AMIN, O., ABEDISEID, W., and ALOUINI, M. S., *Underlay Cognitive Radio Systems With Improper Gaussian Signaling: Outage Performance Analysis*, **IEEE Transactions on Wireless Communications**, 15(7), 4875–4887, doi:10.1109/TWC.2016.2547918, 2016b.
- BARROS, J., and RODRIGUES, M. R. D., *Secrecy Capacity of Wireless Channels*, in **2006 IEEE International Symposium on Information Theory**, pp. 356–360, doi:10.1109/ISIT.2006.261613, 2006.
- BLOCH, M., BARROS, J., RODRIGUES, M. R. D., and MCLAUGHLIN, S. W., *Wireless Information-Theoretic Security*, **IEEE Transactions on Information Theory**, 54(6), 2515–2534, doi:10.1109/TIT.2008.921908, 2008.
- BLOCH, M., HAYASHI, M., and THANGARAJ, A., *Error-Control Coding for Physical-Layer Secrecy*, **Proceedings of the IEEE**, 103(10), 1725–1746, doi:10.1109/JPROC.2015.2463678, 2015.
- BORDON, R., MONTEJO-SANCHEZ, S., SOUZA, R. D., BRANTE, G., and FERNANDEZ, E. M. G., *Energy Efficient Cooperation Based on Relay Switching ON-OFF Probability for WSNs*, **IEEE Systems Journal**, pp. 1–12, doi:10.1109/JSYST.2017.2718499, 2017.

- CHEN, X., CHEN, J., ZHANG, H., ZHANG, Y., and YUEN, C., *On Secrecy Performance of Multiantenna-Jammer-Aided Secure Communications With Imperfect CSI*, **IEEE Transactions on Vehicular Technology**, 65(10), 8014–8024, doi:10.1109/TVT.2015.2510502, 2016.
- CHEN, X., NG, D. W. K., GERSTACKER, W. H., and CHEN, H. H., *A Survey on Multiple-Antenna Techniques for Physical Layer Security*, **IEEE Commun. Surv. Tutor.**, 19(2), 1027–1053, doi:10.1109/COMST.2016.2633387, 2017.
- CHIODI, M. A., REBELATTO, J. L., SOUZA, R. D., and BRANTE, G., *Achieving negative security gaps with transmit antenna selection and frame scrambling in quasi-static fading channels*, **Electronics Letters**, 51(3), 200–202, doi:10.1049/el.2014.3244, 2015.
- COVER, T. M., and THOMAS, J. A., **Elements of Information Theory**, Wiley-Interscience, New York, NY, USA, 1991.
- FAN, L., ZHANG, S., DUONG, T. Q., and KARAGIANNIDIS, G. K., *Secure switch-and-stay combining (SSSC) for cognitive relay networks*, **IEEE Transactions on Communications**, 64(1), 70–82, doi:10.1109/TCOMM.2015.2497308, 2016.
- FANG, B., QIAN, Z., SHAO, W., and ZHONG, W., *Precoding and Artificial Noise Design for Cognitive MIMOME Wiretap Channels*, **IEEE Transactions on Vehicular Technology**, 65(8), 6753–6758, doi:10.1109/TVT.2015.2477305, 2016.
- GAAFAR, M., AMIN, O., IKHLEF, A., CHAABAN, A., and ALOUINI, M.-S., *On Alternate Relaying with Improper Gaussian Signaling*, **IEEE Communications Letters**, 20(8), 1683–1686, doi:10.1109/LCOMM.2016.2577029, 2016a.
- GAAFAR, M., KHAFAGY, M. G., AMIN, O., and ALOUINI, M. S., *Improper Gaussian signaling in full-duplex relay channels with residual self-interference*, **IEEE ICC 2016**, doi:10.1109/ICC.2016.7511009, 2016b.



- GAAFAR, M., AMIN, O., ABEDISEID, W., and ALOUINI, M. S., *Underlay Spectrum Sharing Techniques With In-Band Full-Duplex Systems Using Improper Gaussian Signaling*, **IEEE Transactions on Wireless Communications**, 16(1), 235–249, doi:10.1109/TWC.2016.2621767, 2017.
- GABRIEL, F., NGUYEN, G. T., SCHMOLL, R., CABRERA, J. A., MUEHLEISEN, M., and FITZEK, F. H. P., *Practical deployment of network coding for real-time applications in 5G networks*, in **2018 15th IEEE Annual Consumer Communications Networking Conference (CCNC)**, pp. 1–2, doi:10.1109/CCNC.2018.8319320, 2018.
- GOLDSMITH, A., **Wireless Communications**, Cambridge University Press, New York, NY, USA, 2005.
- GOLDSMITH, A., JAFAR, S. A., MARIC, I., and SRINIVASA, S., *Breaking Spectrum Gridlock With Cognitive Radios: An Information Theoretic Perspective*, **Proceedings of the IEEE**, 97(5), 894–914, doi:10.1109/JPROC.2009.2015717, 2009.
- HEDHLY, W., AMIN, O., and ALOUINI, M., *Interweave Cognitive Radio with Improper Gaussian Signaling*, in **GLOBECOM 2017 - 2017 IEEE Global Communications Conference**, pp. 1–6, doi:10.1109/GLOCOM.2017.8254229, 2017.
- HELLINGS, C., and UTSCHICK, W., *On the Worst-Case Noise in Gaussian MIMO Systems with Proper and with Improper Signaling*, in **WSA 2017; 21th International ITG Workshop on Smart Antennas**, pp. 1–7, 2017.
- HO, Z. K. M., and JORSWIECK, E., *Improper Gaussian signaling on the two-user SISO interference channel*, **IEEE Transactions on Wireless Communications**, 11(9), 3194–3203, doi:10.1109/TWC.2012.071612.111338, 2012.
- HODGSON, E., BRANTE, G., SOUZA, R. D., and REBELATTO, J. L., *On the physical layer security of analog joint source channel coding schemes*, in **2015 IEEE 16th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)**, pp. 585–589, doi:10.1109/SPAWC.2015.7227105, 2015.

- KARIMINEZHAD, A., SEZGIN, A., and PESAVENTO, M., *Power efficiency of improper signaling in MIMO full-duplex relaying for K-user interference networks*, in **2017 IEEE International Conference on Communications (ICC)**, pp. 1–6, doi:10.1109/ICC.2017.7996880, 2017.
- LAGEN, S., AGUSTIN, A., and VIDAL, J., *On the Superiority of Improper Gaussian Signaling in Wireless Interference MIMO Scenarios*, **IEEE Transactions on Communications**, 64(8), 3350–3368, doi:10.1109/TCOMM.2016.2584601, 2016.
- LAMEIRO, C., SANTAMARIA, I., and SCHREIER, P. J., *Benefits of Improper Signaling for Underlay Cognitive Radio*, **IEEE Wireless Communications Letters**, 4(1), 22–25, doi:10.1109/LWC.2014.2360179, 2015.
- LAMEIRO, C., SANTAMARIA, I., and SCHREIER, P. J., *Rate Region Boundary of the SISO Z-Interference Channel With Improper Signaling*, **IEEE Transactions on Communications**, 65(3), 1022–1034, doi:10.1109/TCOMM.2016.2641948, 2017.
- LOPEZ, R. B., SANCHEZ, S. M., FERNANDEZ, E. M. G., SOUZA, R. D., and ALVES, H., *Genetic algorithm aided transmit power control in cognitive radio networks*, in **2014 9th International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM)**, pp. 61–66, doi:10.4108/icst.crowncom.2014.255393, 2014.
- MEHBOOB, U., QADIR, J., ALI, S., and VASILAKOS, A., *Genetic Algorithms in Wireless Networking: Techniques, Applications, and Issues*, **Soft Computing**, 20(6), 2467–2501, 2016.
- MITCHELL, M., **An Introduction to Genetic Algorithms**, MIT Press, Cambridge, MA, USA, 1998.
- MO, J., TAO, M., and LIU, Y., *Relay placement for physical layer security: A secure connection perspective*, **IEEE Communications Letters**, 16(6), 878–881, doi:10.1109/LCOMM.2012.042312.120582, 2012.

- MONTEIRO, M. E. P., REBELATTO, J. L., SOUZA, R. D., and BRANTE, G., *Maximum Secrecy Throughput of Transmit Antenna Selection with Eavesdropper Outage Constraints*, **IEEE Signal Processing Letters**, 22(11), 2069–2072, doi:10.1109/LSP.2015.2458573, 2015.
- NEESER, F. D., and MASSEY, J. L., *Proper complex random processes with applications to information theory*, **IEEE Transactions on Information Theory**, 39(4), 1293–1302, doi:10.1109/18.243446, 1993.
- NGUYEN, V. D., DUONG, T. Q., DOBRE, O. A., and SHIN, O. S., *Joint Information and Jamming Beamforming for Secrecy Rate Maximization in Cognitive Radio Networks*, **IEEE Transactions on Information Forensics and Security**, 11(11), 2609–2623, doi:10.1109/TIFS.2016.2594131, 2016.
- OGGIER, F., and HASSIBI, B., *A Perspective on the MIMO Wiretap Channel*, **Proceedings of the IEEE**, 103(10), 1874–1882, doi:10.1109/JPROC.2015.2468077, 2015.
- OLIVEIRA, G., FERNANDEZ, E., MAFRA, S., and MONTEJO-SANCHEZ, S., *Physical Layer Security in Cognitive Radio Networks Using Improper Gaussian Signaling*, **IEEE Communications Letters**, 22(9), 1886–1889, doi:10.1109/LCOMM.2018.2853629, 2018.
- SANTAMARIA, I., CRESPO, P. M., LAMEIRO, C., and SCHREIER, P. J., *Information-Theoretic Analysis of a Family of Improper Discrete Constellations*, **Entropy**, 20(1), doi:10.3390/e20010045, 2018.
- SCHREIER, P. J., and SCHARF, L. L., *Second-order analysis of improper complex random vectors and processes*, **IEEE Transactions on Signal Processing**, 51(3), 714–725, doi:10.1109/TSP.2002.808085, 2003.
- SHANNON, C. E., *A mathematical theory of communication*, **The Bell System Technical Journal**, 27(3), 379–423, doi:10.1002/j.1538-7305.1948.tb01338.x, 1948.

YAN, S., GERACI, G., YANG, N., MALANEY, R., and YUAN, J., *On the target secrecy rate for SISOME wiretap channels*, in **2014 IEEE International Conference on Communications (ICC)**, pp. 987–992, doi:10.1109/ICC.2014.6883448, 2014.

ZENG, Y., YETIS, C. M., GUNAWAN, E., GUAN, Y. L., and ZHANG, R., *Transmit optimization with improper gaussian signaling for interference channels*, **IEEE Transactions on Signal Processing**, 61(11), 2899–2913, doi:10.1109/TSP.2013.2254480, 2013a.

ZENG, Y., ZHANG, R., GUNAWAN, E., and GUAN, Y. L., *Optimized transmission with improper gaussian signaling in the K-user MISO interference channel*, **IEEE Transactions on Wireless Communications**, 12(12), 6303–6313, doi:10.1109/TWC.2013.103013.130439, 2013b.

ZHANG, T., CAI, Y., HUANG, Y., DUONG, T. Q., and YANG, W., *Secure Transmission in Cognitive MIMO Relaying Networks With Outdated Channel State Information*, **IEEE Access**, 3536(c), 1–1, doi:10.1109/ACCESS.2016.2608966, 2016.

ZOU, Y., ZHU, J., WANG, X., and HANZO, L., *A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends*, **Proceedings of the IEEE**, 104(9), 1727–1765, doi:10.1109/JPROC.2016.2558521, 2016.