To my family:
For their love and support
in any situations of my life

Jury Members

Dr. António Beça Gonçalves Porto
Professor Catedrático
Faculdade de Ciências da Universidade do Porto (Presidente)

Dr. Francisco António Bucho Cercas
Professor Catedrático
Departamento de Ciências e Tecnologias da Informação
Instituto Universitário de Lisboa

Dr. Adão Paulo Soares Silva
Professor Auxiliar
Departamento de Eletrónica
Telecomunicações e Informática
Universidade de Aveiro

Dr. Carlos Manuel Nogueira Gaspar Ribeiro
Professor Adjunto
Departamento de Engenharia Eletrotécnica
Escola Superior de Tecnologia e Gestão
Instituto Politécnico de Leiria

Dr. Aníbal João de Sousa Ferreira
Professor Associado
Faculdade de Engenharia da Universidade do Porto

Dr. Sérgio Armindo Lopes Crisóstomo
Professor Auxiliar
Faculdade de Ciências da Universidade do Porto

Dr. Miguel Raul Dias Rodrigues
Professor Associado Convidado
Faculdade de Ciências da Universidade do Porto (Orientador)

Acknowledgment

This dissertation would not be possible without the contributions of several people. First and foremost, I would like to thank from my heart to my supervisor, Dr. Miguel Rodrigues, whose encouragement, guidance and support from the initial to the final stages has enabled me to develop understanding of the subject.

I am very grateful to my collaborators, Hugo Reboredo and Francesco Renna, whose ideas and suggestions have benifited me a lot and Samah Ghanem who always support me as a friend.

I would like to thank all my lab mates who have made a comfortable working environment. My gratefulness to Alex and Elimary, who have been very kind and helpful throughout my stay at DCC (Departamento de Ciência de Computadores) and extended all administrative support.

I am thankful to Scientific members of MAP-Tele program and DCC. I would also like to thank to IT (Instituto de Telecomunicações) and FCT (Fundação para a Ciência e a Tecnologia) for the financial support during my PhD[1].

Finally, I am grateful to all of my family members for their patience and support. Without them, this work would never have come into existence.

Munnujahan Ara
October 2013

[1]This work was supported by Fundação para a Ciência e a Tecnologia (the Portuguese National Science Foundation) under grant SFRH/BD/61521/2009. Part of this work was also supported by Fundação para a Ciência e a Tecnologia, Portugal through the research project PTDC/EEATEL/100854/2008 and CMU-PT/SIA/0026/2009.

Resumo

O principal enfoque desta tese centra-se na utilização de técnicas de camada física para o desenho de sistemas de comunicações seguros e fiáveis.

Com o acentuado crescimento na procura por sistemas wireless de alto débito, a tecnologia Orthogonal Frequency Division Multiplexing (OFDM) - onde os dados são transportados com recurso a subportadoras paralelas e ortogonais - tem vindo a reclamar um papel fundamental devido à sua capacidade de comportar elevadas taxas de transmissão de dados de forma simples e eficaz em canais multicaminho. Desta forma, este trabalho centra-se no desenho de estratégias de transmissão que, para além de garantirem fiabilidade, oferecem também transmissões seguras em sistemas de comunicações baseados em OFDM.

Em particular, esta tese explora caracterizações de taxas de transmissão segura, baseadas em teoria da informação, para um conjunto de "wiretap channels" Gaussianos paralelos e independentes (um modelo aplicável a sistemas de comunicações OFDM), onde um transmissor e um receptor legítimos tentam comunicar na presença de um utilizador não legítimo ("eavesdropper") e de um outro elemento (amigável ou hostil), que introduz interferência de forma propositada ("jammer"). Esta abordagem tem o intuito de desenvolver estratégias, óptimas ou quase óptimas, de alocação de potência. Estas estratégias de alocação de potência são posteriormente caracterizadas com recurso a ferramentas de teoria de optimização e/ou teoria dos jogos.

As principais contribuições deste trabalho incluem:

Primeiramente, são adoptadas técnicas de teoria dos jogos para desenvolver estratégias óptimas para um "wiretap channel" Gaussiano paralelo, na presença de um "jammer" hostil. Assume-se que o "eavesdropper" é um utilizador passivo, mas que o "jammer" atua como um utilizador activo, injectando interferência no

canal de comunicação principal sob a forma de ruído aditivo. O principal objectivo do "jammer" hostil é o de minimizar a taxa de transmissão segura, enquanto o transmissor procura, por sua vez, maximizar a taxa de transmissão segura. É proposta uma formulação, baseada em teoria dos jogos, do jogo ("zero-sum game") de alocação de potência entre o transmissor e o "jammer" hostil em que a função de custo é a taxa de transmissão segura. Apresenta-se uma prova da existência de um equilíbrio de Nash para este "zero-sum game" e são também caracterizadas as alocações óptimas de potência para o transmissor e para o "jammer".

Em segundo lugar são propostos algoritmos para o desenvolvimento de estratégias óptimas de alocação de potência para o caso em que o "jammer" é amigável e não hostil. Neste cenário mantém-se o pressuposto de que o "eavesdropper" é um utilizador passivo e de que o "jammer" é um utilizador activo que, desta vez, injecta interferência no canal do "eavesdropper" sob a forma de ruído aditivo, com o objectivo de ajudar os utilizadores legítimos a maximizar a taxa de transferência segura. É apresentado um algoritmo para obter a estratégia óptima de alocação de potência do "jammer", que maximiza a taxa de transmissão segura, para o caso em que o canal "wiretap" é degradado, isto é, quando o canal entre o transmissor e o receptor legítimo é melhor que o canal de transmissão entre o transmissor e o "eavesdropper". É também apresentado um algoritmo responsável pela obtenção de estratégias conjuntas de alocação de potência entre o transmissor e o "jammer" no caso em que o canal "wiretap" não é necessariamente degradado, que apresenta ganhos consideráveis de desempenho em comparação com estratégias isotrópicas de alocação de potência.

Por fim, é tomado como base o trabalho desenvolvido nas contribuições anteriores para estudar o impacto das estratégias de alocação de potência propostas, em sistemas de comunicações OFDM na presença de desvanecimento e correlação sinal. Adicionalmente, a relação entre a porção de potência que deve ser destinada ao transmissor a a porção que deve ser atribuída ao "jammer" é também investigada, em cenários em que é imposta uma restrição de potência total.

Os resultados apresentados demonstram que a adopção de estratégias óptimas ou quase óptimas de alocação de potência podem ter um impacto dramático nas taxas de transmissão segura em "wiretap channels" paralelos e independentes. Este modelo teórico de análise, que foi validado através de extensivos resultados de simulação, oferece portanto um meio para desenvolver sistemas de comunicações OFDM fiáveis e seguros.

Abstract

This thesis considers the use of physical-layer based techniques in order to design reliable and secure wireless communication systems.

With the significant increase in demand for high data rate wireless systems, orthogonal frequency division multiplexing (OFDM) - where data is carried over parallel orthogonal subcarriers - has taken a role of paramount importance because it offers the means to convey high data rates with low-complex transceivers in multipath channels. As such, the focus is on the design of transmission strategies that - in addition to providing reliability - also lead to secure transmission in OFDM based communications systems.

In particular, the thesis capitalizes on information-theoretic characterizations of achievable secrecy rates for a bank of independent parallel Gaussian wiretap channels (a model applicable to OFDM communications systems), where a legitimate transmitter and a legitimate receiver communicate in the presence of an eavesdropper and a friendly or unfriendly jammer, in order to design optimal or nearly optimal power allocation strategies. The power allocation strategies associated with the legitimate or hostile parties are then characterized by using tools from optimization theory and/or game theory.

The main contributions include:

Firstly, we capitalize on game theoretic tools to devise optimal strategies for a parallel Gaussian wiretap channel in the presence of unfriendly jamming. The eavesdropper is assumed to be passive and the jammer acts as an active hostile player injecting interference in the main channel, in the form of additive noise. In this setting, the malicious jammer aims to minimize an achievable secrecy rate, while the transmitter intends to maximize the achievable secrecy rate. We introduce

a game-theoretic formulation of a zero-sum power allocation game between transmitter and the unfriendly jammer using the secrecy rate as the payoff function. We provide a proof of the existence of a Nash equilibrium and as such we also characterize the optimal transmission and jamming power allocation strategies.

Secondly, we introduce algorithmic approaches to devise optimal power allocation strategies for a parallel Gaussian wiretap channel in the presence of friendly jamming. In such scenario, the eavesdropper is also assumed to be passive but the jammer injects interference in the eavesdropper channel in the form of additive noise with the objective of helping the legitimate parties to increase the secrecy rates. We provide algorithms to compute the optimal power allocation strategy of the jammer for a degraded scenario, i.e., when the transmitter channel is better than the eavesdropper channel, which maximize the secrecy rate for a fixed transmitter power allocation strategy. We also provide an algorithm to compute a joint power allocation strategy for the jammer and the transmitter, in the case where degradedness is not assumed, which leads to significant performance gains in relation to isotropic jamming.

Finally, we build upon the previous contributions in order to study the impact of the proposed power allocation strategies in OFDM communications system in the presence of fading and correlation. Furthermore, the relation between the portion of power made available to the transmitter and to the jammer is also investigated, when a total power budget is imposed.

Our results demonstrate that the use of the optimal or nearly optimal power allocation strategies can have a dramatic effect on the secrecy rates of parallel independent wiretap channels. The theoretical framework, which has been validated via extensive simulation results, then provides the means to design both reliable and secure OFDM communications systems.

Contents

List of Figures

List of Tables

Abbreviations

ADSL	Asymmetic Digital Subscriber Line
ASK	Amplitude Shift Keying
AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
BPSK	Binary Phase Shift Keying
CDMA	Code Division Multiple Access
CIR	Channel Impulse Response
CP	Cyclic Prefix
CSI	Channel State Information
DAB	Digital Audio Broadcasting
DMC	Discrete Memory-less Channel
DVB	Digital Video Broadcasting
FDM	Frequency Division Multiplexing
FFT	Fast Fourier Transform
FSK	Frequency Shift Keying
HDSL	High-Bit-Rate Digital Subscriber Line
HF	High Frequency
HiperLAN	High-Performance LAN
ICI	Inter Channel Interference
IFFT	Inverse Fast Fourier Transform
ISI	Inter Symbol Interference
KKT	Karush Kuhn Tucker
LAN	Local Area Network
LOS	Line-of-Sight
MAC	Multiple Access Channel
MIMO	Multi Input Multi Output
MISO	Multi Input Single Output
MMAC	Multimedia Mobile Access Communication

MSE	Mean Squared Error
NE	Nash Equilibrium
NLOS	Non Line-of-Sight
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open Systems Interconnection
PDF	Probability Density Function
PDP	Power Delay Profile
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
S/P	Serial-to-Parallel Converter
P/S	Parallel-to-Serial Converter
SINR	Signal to Interference plus Noise Ratio
SISO	Single Input Single Output
SNR	Signal to Noise Ratio
TDMA	Time Division Multiple Access
VHDSL	Very High-Speed Digital Subscriber Line
WPLS	Wireless Physical Layer Security

Notations

$(\cdot)^*$	Optimal value.
$\bar{(\cdot)}$	Average value.
$det(\mathbf{A})$	Determinant of matrix $\mathbf{A}$.
$\mathbf{A}^\dagger$	Conjugate transpose (Hermitian) of matrix $\mathbf{A}$.
$\lambda(\mathbf{A})$	Vector of eigenvalues of matrix $\mathbf{A}$.
$\mathbb{E}[\cdot]$	Statistical expectation.
$log[\cdot]$	Logarithm in base 2.
$\|a\|$	Absolute value (modulus) of the scalar a.
$(a)^+$	Positive values of a, i.e., max(0,a).
$diag(\mathbf{A})$	The diagonal elements of a matrix $\mathbf{A}$.
$\Re$	Set of real numbers.
$\mathbb{C}^{n\times m}$	Set of complex numbers of dimensions $n \times m$.
$\mathbf{I}$	The identity matrix.
$\sim$	Distributed according.
$\mathcal{CN}(\mu, \sigma)$	Complex Gaussian vector distribution with mean μ and covariance σ.
C_s	Secrecy capacity.
R_s	Secrecy rate.
$I(X;Y)$	Mutual informations between the random varables X and Y.
σ_{x_i}	Transmitter inject power into the main i^{th} sub-channel.
σ_{j_i}	Jammer inject power into the jammer i^{th} sub-channel.
$\mathbf{\Lambda}_m$	Matrix containing gains of the paralle sub-channels of the main channel.
$\mathbf{\Lambda}_e$	Matrix containing gains of the paralle sub-channels of the eavesdropper channel.
$\mathbf{\Lambda}_j/\mathbf{\Lambda}_{j_e}$	Matrix containing gains of the paralle sub-channels of the jammer channel.
$a \to 0$	The limit of a approaches zero.
$\triangleq$	Defined as.
$\wedge$	And.

$\forall$ For all.

$\Rightarrow$ Implies.

$\Leftrightarrow$ If and only if.

$>$ Greater than.

$<$ Less than.

$\geq$ Greater than or equal to.

$\leq$ Less than or equal to.

$\in$ Belongs to.

Chapter 1
Introduction

1.1 Motivation

Security is one of the most important issues in wireless communications. Since wireless communications face security risks and threats, in view of the broadcast nature of the wireless medium, one of the hot topics in wireless communication at the moment is how to secure a wireless network.

Security can be defined in terms of confidentiality, availability, and integrity. Confidentiality guarantees that legitimate recipients successfully obtain source information, while malicious users are not able to interpret this information [1]. Availability relates to the access to confidential information by legitimate properly authenticated users [2]. When availability is compromised, the access is denied for legitimate users because of malicious activity. Integrity relates to the trustworthiness of information resources, with assurance that the information is authentic and complete, i.e, original source information is not modified by malicious parties during its transmission [1].

Figure 1.1 illustrates the different functionalities addressed within a standard network communication framework. Traditionally, security is viewed as an independent feature addressed above the physical layer, and all widely used cryptographic protocols are designed and implemented assuming the physical layer has already been established and provides an error-free link [3]. The purpose of the physical-layer is to guarantee error-free transmission, with security mechanisms typically operating at a higher layer of the protocol stack. State-of-the-art symmetric (secret-key) or public-key (asymmetric) cryptographic schemes [4, 5] are thus insensitive to the

characteristics of the communications channels, relying on the Shannon diffusion and confusion principles [6] or on presumably hard-to-compute mathematical operations, such as prime factorization or discrete logarithm calculation. However, this modular approach to data security is increasingly difficult to justify due to i) uncertainty about the correctness of the underlying intractability assumptions; ii) the possible advent of more efficient attacks and even quantum computers; and iii) fast and reliable communications over certain systems and applications require light and effective security architectures. This modular approach to system security may also lead to energy and transmission inefficiency in contemporary communications systems and networks.

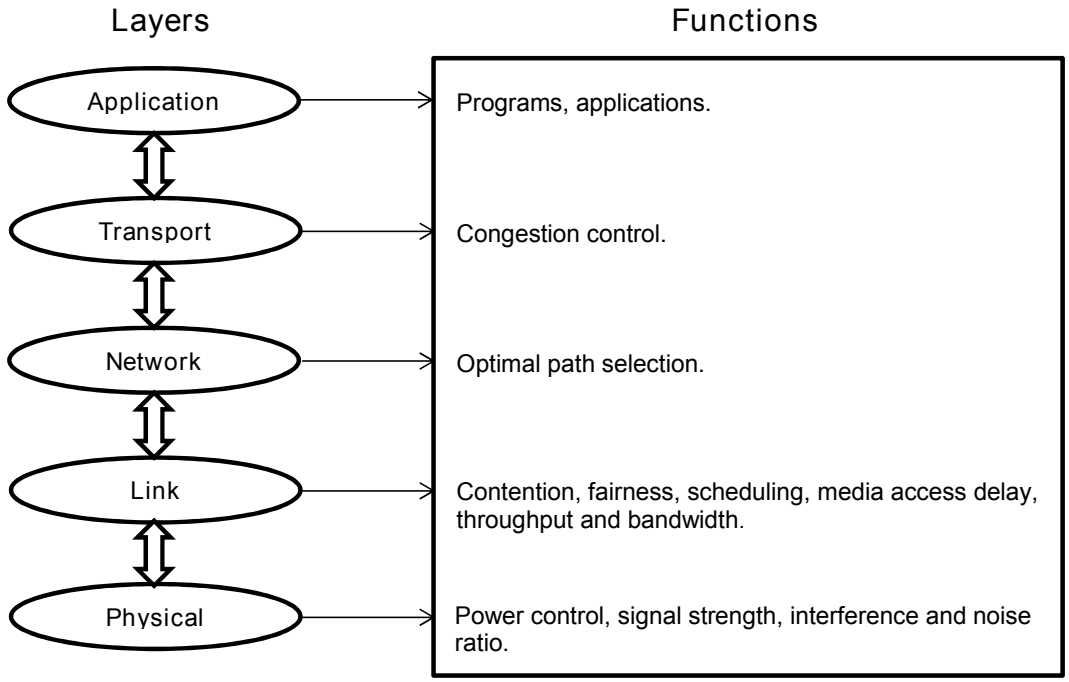

Figure 1.1: Standard network communication framework and its associated functions.

However, the recent years have witnessed a renewed interest on the basic principles and ideas behind information-theoretic security - widely accepted as the strictest notion of security - which calls for the use of standard physical-layer techniques that exploit the inherent randomness in the communications channels and media to provide not only robustness to transmission errors but also a certain degree of data confidentiality [1, 7]. The information-theoretic approach, which offers a promising new mechanism towards solving wireless networking security problems without using an encryption key, was initiated by Wyner [8] and by Csiszár and

Körner [9] in the 1970´s: in particular, according to this new paradigm, a transmitter intentionally adds structured randomness (Stochastic coding) to prevent potential eavesdroppers and attackers from intercepting useful information while guaranteeing that a legitimate receiver can obtain the information [1].

Physical-layer security is an emerging research area which capitalizes on the information-theoretic paradigm in order to explore the possibility of achieving perfect-secrecy data transmission among intended network nodes, while not disclosing information to possibly malicious nodes that eavesdrop upon the transmission for improving the security of wireless communication systems and networks. The breakthrough concept behind wireless physical layer security is to exploit the characteristics of the wireless channel, such as fading or noise, to provide secrecy for wireless transmissions. While these characteristics have traditionally been seen as impairments, physical layer security takes advantage of these characteristics for improving the security of wireless communication systems and networks.

The focus to date on physical-layer security research has been based on theoretical aspects concerning the characterization of the fundamental secrecy limits of various communications channels and networks, e.g., the secrecy capacity or the secrecy capacity region [10, 11, 12, 13]. However, the design of concrete efficient, reliable and secure physical-layer techniques is still an open problem at large.

In view of the ubiquitous deployment of OFDM systems in various standards such as third-generation, fourth-generation mobile communication systems and beyond, as well as WiFi IEEE 802.11, and Wimax IEEE 802.16 [14, 15], the focus of this thesis is on the design of optimal or sub-optimal power allocation schemes for wireless OFDM systems in the presence of jammers. These jammers could be purposely deployed by a network operator in order to assist in increasing the achievable secrecy rates between a legitimate transmitter and a legitimate receiver in the network in the presence of a eavesdropper, i.e. the jammers would be friendly. Alternatively, these jammers could also be deployed by malicious parties in order to assist in decreasing the achievable secrecy rates between the legitimate parties in the network in the presence of an eavesdropper, i.e. the jammers would be unfriendly. By adopting a parallel Gaussian wiretap channel model of the OFDM communications system, it will be seen that the design of appropriate power allocation policies can have a dramatic effect on the secrecy rates of the system. By carefully designing the power allocations across the various sub-channels associated with the OFDM

communications system, it will be possible to significantly increase the secrecy rates.

1.2 Thesis organization

In this thesis, we consider power allocation schemes for secure communications over a bank of parallel wiretap Gaussian channels, which can be used to model OFDM communications systems, where two legitimate parties (Alice and Bob) try to communicate in the presence of a unfriendly / friendly jammer and an eavesdropper (Eve). The eavesdropper is assumed to be passive[2] but the jammer acts as an active player injecting interference in the form of additive noise. The information-theoretic security metric used as a basis of the optimization of the power allocations is an achievable secrecy rate: a secrecy rate is achievable when there is a coding scheme such that the legitimate transmitter and the legitimate receiver can communicate reliably (with arbitrarily low probability of error) whereas the eavesdropper is unable to obtain any information (measured by its equivocation). When the jammer is unfriendly it generates interference in order to decrease the achievable secrecy rate; in contrast, when the jammer is friendly it generates interference in order to increase the achievable secrecy rate between the legitimate transmitter and receiver.

In Chapter 2, we give a brief overview of information-theoretic and physical-layer security as well as prior work in the area and its relation to the work in this thesis.

In Chapter 3, we address the problem where, on the one hand, the transmitter (Alice) tries to find the power allocation strategy that maximizes her secrecy rate and on the other hand an unfriendly jammer tries to employ the jamming power allocation strategy that minimizes this same secrecy rate by adding interference to the main channel. By capitalizing on game theory, we formulate a two person zero-sum game. We prove the existence of a Nash equilibrium, i.e., where each player (Alice and Jammer) chooses the best strategy against any opponent's strategy. We also characterize the optimal transmission and jamming power allocation strategies for a zero-sum game, which are specialized for key asymptotic regimes. A range of simulation results also illustrate the secrecy gains that an adaptive transmitter,

[2]The eavesdropper is assumed to be passive, which means that the eavesdropper only listens but does not transmit. Simply, the eavesdropper target is to decode the received signal from the transmitter but not to jam it or destruct it.

which adapts to the jammer power allocation strategy, exhibits over a non-adaptive one, which does not adapt its power allocation to the jammer's power allocation.

In Chapter 4, we analyze the problem where, two legitimate parties (Alice and Bob) communicate in the presence of a friendly jammer, which injects interference in the eavesdropper channel in the presence of additive noise, and an eavesdropper (Eve). The objective is to maximize the secrecy rate, between the source (Alice) and the destination (Bob) by putting forth power allocation algorithms for the jammer and joint power allocation algorithms for the jammer and the transmitter in both scenarios of degraded and general (degraded and non-degraded) channels. This is done by proposing both optimal and, whenever this is not possible due to non-convexity considerations, sub-optimal power allocation algorithms that lead to significant gains in relation to a simple isotropic power allocation strategy. We also characterize optimal power allocation strategies for general and low power regimes.

In Chapter 5, we use the results of Chapter 4 to study the impact of the power allocation policies in OFDM communications system in the presence of fading. This work focuses on the evaluation of the secrecy rates that can be achieved over Rayleigh / Rician fading scenario, with independent or correlated sub-channels. Moreover, we study the tradeoff that regulates the amount of power assigned to the transmitter and to the jammer, when a total available power constraint is imposed. We also observe the change of the average secrecy rate when the jammer is Rayleigh / Rician and when its sub-channels are independent / correlated, respectively.

Chapter 6 concludes this thesis, summarizing the main contributions and suggesting areas for future works.

1.3 Thesis contribution

The main contributions of this thesis are:

- Formulation of a zero-sum power allocation game associated with the maximization of the secrecy rate for the parallel Gaussian wiretap channel where a legitimate transmitter communicates with a legitimate receiver in the presence of an eavesdropper and an unfriendly jammer that injects interference in the

main channel in the form of additive noise. This power allocation game, which is played between the legitimate transmitter and the unfriendly jammer, uses an achievable secrecy rate as the payoff function and the total available power at the legitimate transmitter and the unfriendly jammer as constraints.

- Characterization of the optimal transmission and jamming power allocation strategies for the zero-sum game for general and asymptotic low power regimes

- Extensive simulation results demonstrate that a transmitter that adapts to the unfriendly jammer strategy can experience a much higher secrecy rate than a non-adaptive transmitter.

- Formulation of a power allocation optimization problem associated with the maximization of an achievable secrecy rate for a parallel Gaussian wiretap channel where a legitimate transmitter communicates with a legitimate receiver in the presence of an eavesdropper and a friendly jammer that injects interference in the eavesdropper channel in the form of additive noise.

- Characterizations of the optimal power allocation policies for the jammer and joint power allocation algorithms for the jammer and the transmitter both for general and low power regimes.

- Extensive simulation results demonstrate the effect of friendly jamming in increasing the secrecy rates.

- Additional results that show that additional secrecy rates can be extracted by optimally distributing a fixed power budget between the transmitter and the jammer in a wireless network.

- Application of the results to the scenario where the legitimate transmitter, the legitimate receiver, the eavesdropper and the friendly jammer employ OFDM modulation. The objective is to determine the impact of the derived optimal or nearly optimal power allocation policies in the presence of quasi-static Rayleigh or Ricean fading, and in the presence of independent or correllated

sub-channels. It is observed that the average achievable secrecy rate is higher when the sub-channels are independent than when sub-channels are correlated. It is also observed that the average achievable secrecy rate experiences higher when the jammer is Rician fading than when the jammer experiences Rayleigh fading.

These contributions have led to the following publications:

1. Munnujahan Ara, Hugo Reboredo, Francesco Renna, Miguel R. D. Rodrigues "Power Allocation Strategies For OFDM Gaussian Wiretap Channels With a Friendly Jammer", IEEE International Conference on Communications (ICC-2013), 9-13 June 2013, Budapest, Hungary.

2. Munnujahan Ara, Hugo Reboredo, Francesco Renna, Miguel R. D. Rodrigues "Power Allocation Strategies For OFDM Gaussian Wiretap Channels With a Friendly Jammer: The Degraded case", ConfTele-2013, 8-10 May 2013, Castelo Branco, Portugal.

3. Munnujahan Ara, Hugo Reboredo, Samah A. M. Ghanem, Miguel R. D. Rodrigues "A Zero-Sum Power Allocation Game in the Parallel Gaussian Wiretap Channel with an Unfriendly Jammer", The 13th IEEE International Conference on Communication Systems(ICCS-2012), 21-23 Nov. 2012, Singapore.

4. Hugo Reboredo, Munnujahan Ara, Miguel R. D. Rodrigues and João Xavier "Filter Design with Secrecy Constraints: The Degraded Multiple-Input Multiple-Output Gaussian Wiretap Channel", 2011 IEEE 73rd Vehicular Technology Conference: VTC2011-Spring 15-18 May 2011, Budapest, Hungary.

Chapter 2
Background on Information Theoretic Security and Physical Layer Security

The main objective of this Chapter is to introduce some concepts and ideas behind information-theoretic security. In particular, we present a set of standard models associated with physical layer security, including the Shannon's perfect secrecy model, Wyner's wiretap channel model, and other wiretap channel models that will be used throughout the thesis. We also introduce a prior work on physical layer security techniques with an emphasis on jamming techniques. Such techniques relate to the theme of this thesis, which revolves around the exploitation of different design approaches to secure wireless networks by causing interference.

2.1 Information-theoretic security

Information-theoretic security provides the theoretical foundations for physical-layer security. The main idea behind information-theoretic security relates to the usage of the inherent randomness of the physical medium, including noises and channel fluctuations due to fading, in order to secure transmitted and received data [8]. In particular, information-theoretic approaches to secure the transmission of messages, from a legitimate transmitter to a legitimate receiver, thus bypass the need to use any encryption mechanism. Such approaches guarantee that malicious attackers cannot decode, partly or fully, their received noisy versions of the transmitted message.

Shannon´s notion of perfect secrecy was the theoretical building block toward the introduction of information-theoretic security, which was laid by Wyner [8] and

later by Csiszár and Körner [9]. They proved in a set of seminal papers that there exist channel codes that can guarantee both robustness to transmission errors and a certain degree of data confidentiality. In the seventies and eighties, the impact of these works was limited due to, first, from a practical perspective, such wiretap codes were not available, second, from a theoretical perspective, a strictly positive secrecy capacity is limited to the assumption of degradedness of the channel of the legitimate parties, where in the classical wiretap channel setup the legitimate sender and receiver are assumed to have some advantage over the attacker in terms of channel quality. Moreover, a different notion of secrecy has also been proposed, almost at the same time, with the introduction of public-key cryptography by Diffie and Hellman [16], which was to be adopted almost by all contemporary security schemes.

In the nineties, Maurer [17] proved that even when the legitimate parties have a worse channel than the eavesdropper, it is yet possible to generate a secret key through public communication over an insecure authenticated channel. In particular, the evolution of wireless communications, which are susceptible to eavesdropping due to the broadcast nature of the wireless transmission medium, has also led to a keen interest an in-depth analysis of the secrecy potential of wireless networks.

In the early two thousands, Hero [18] introduced space-time signal processing techniques for secure communication over wireless links. Of particular relevance, the work by Barros and Rodrigues [10], who characterized in detail the outage secrecy capacity of slow fading channels, showed that fading alone guarantees information-theoretic security even when the eavesdropper has a better SNR on average than the legitimate receiver, without the need for public communication over a feedback channel. Almost at the same timeframe, Liang et al. [11], Li et al. [12] and Gopala et al. [13] derived independently the ergodic secrecy capacity of fading channels.

More recently, Bustin et al. [19] and Liu et al. [20] gave a complete characterization of the secrecy capacity of MIMO channels under a matrix covariance constraint on the input covariance matrix. Furthermore, when a total power constraint is considered, the secrecy capacity of a multiple-antenna wiretap channel was computed in the high-power regime, by Khisti et al. [21], and low-power regime, by Gursoy [22].

State of the art work on information-theoretic security usually models the OFDM

signalling as a set of parallel Gaussian wiretap channels [23, 24, 25], assuming that the eavesdropper utilizes OFDM demodulation. The secrecy capacity of the parallel Gaussian wiretap channel model and its corresponding power allocation have been derived in [23]. Optimal transmit and receive filters with secrecy constraints are derived for the parallel Gaussian wiretap channel model, with the minimum MSE used as the design criterion [26], [27].

2.1.1 Shannon´s model

Shannon was the first to introduce a cryptosystem to analyze the communication's secrecy via an information-theoretic approach [6]. Figure 2.1 illustrates Shannon's model of secrecy. In this model, a legitimate transmitter, say Alice, communicates with a legitimate receiver, say Bob, in the presence of an eavesdropper, Eve. The transmitter uses a key K to encrypt a source message W into an encrypted message X, also called ciphertext, and the key K is assumed to be shared by the legitimate transmitter and legitimate receiver but unknown to the eavesdropper. The eavesdropper is only considered to know the encryption functions.

Shannon strictest notion of perfect secrecy was defined in [6], where it was shown that perfect secrecy can be obtained if and only if the size of the secret key is at least as large as the size of the message. Such notion of perfect secrecy was built on two assumptions, first is that the legitimate receiver and the eavesdropper both receive the same version of the transmitted message, second is that the eavesdropper has limited time or limited computational resources which makes it unable to test all possible (keys) to extract the source transmitted message W [1].

Perfect secrecy entails that $p(W|X) = p(W)$, which means that the system is perfectly secure if the posteriori probability of the source message given encrypted message is equal to a priori probabilities of source message. This implies that the eavesdropper uncertainty about the message is not altered via the observation of the cipher-text (encrypted message) X.

Now the entropy $H(W)$, associated with the random variable that models the message, measures the uncertainty about the message, and the conditional entropy associated with the random variable that models the message given the random variable that models the encrypted message $H(W|X)$ measures the eavesdropper´s uncertainty about the message. On the other hand, the mutual information $I(W;X)$

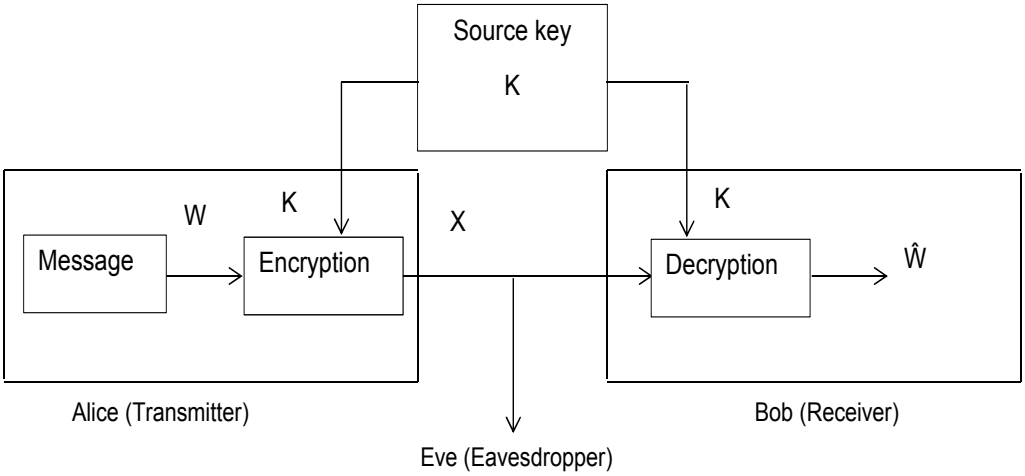

Figure 2.1: Shannon´s model of information-theoretic security.

can be seen as the amount of information that the encrypted message X contains about the original message W (information leakage). Therefore, the system is also said to be perfectly secure if:

$$H(W|X) = H(W) \text{ equivalently, } I(W;X) = H(W) - H(W|X) = 0 \qquad (2.1)$$

As shown in [6], in order to achieve perfect secrecy one requires the length of the key to be at least as large as the length of the message [1], or, $H(K) \geq H(W)$, where $H(K)$ corresponds to the entropy of the random variable that models the key K.

2.1.2 Wyner´s wiretap model

The theoretical basis of information-theoretic security builds Shannon's perfect secrecy system models a scenario where the channels, i.e. the main and the eavesdropper channels, do not introduce erros in the message. However, in reality, some form of noise is always present in a communications system. Therefore, Wyner [8] has introduced the wiretap channel model, illustrated in Figure 2.2.

In Wyner's wiretap channel model a legitimate transmitter, say Alice, communicates with a legitimate receiver, say Bob, in the presence of an eavesdropper, Eve. The random variable W denotes the source message, the random variable X denotes the symbols transmitted by the legitimate transmitter, the random variable Y_m denotes the symbols received by the legitimate receiver and the random variable Y_e denotes the symbols received by the eavesdropper. In turn, X^n denotes the

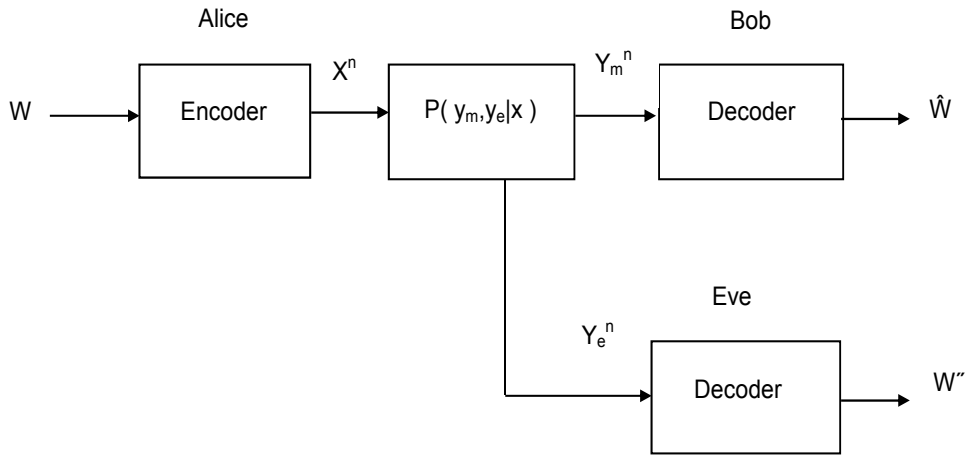

Figure 2.2: The Wyner´s channel model.

sequence of transmit symbols, Y_m^n denotes the sequence of receive symbols at the legitimate receiver and Y_e^n denotes the sequence of receive symols at the eavesdropper. The channel is represented by the probability mass function $P(y_m, y_e|x)$, which corresponds to the main difference between Wyner's model and Shannon's model, in that models the fact is that the legitimate receiver and the eavesdropper observe different noisy versions of the transmitted code word X^n. Therefore, the factor that facilitates secret exchange of the original message is no longer a shared key, but the availability of noise in the communications channel.

The legitimate transmitter, Alice, wishes to convey a (uniformly distributed) message $w \in W = 1, 2, \ldots, 2^{nR}$ to the legitimate receiver, Bob. The legitimate transmitter-receiver pair use an $(2^{nR}, n)$ code (assumed to be known also to the eavesdropper), where n denotes the number of channel uses, consisting of a stochastic encoding function $f : W \to \mathcal{X}^n$ that maps the message $w \in W = 1, 2, ..., 2^{nR}$ into a transmit codeword $X^n \in \mathcal{X}^n$, and a decoding function $g : Y^n \to W$ that maps the receive codeword Y^n into the message estimate $\hat{W}$.

The average error probability of the $(2^{nR}, n)$ code is:

$$P_e^n = \frac{1}{2^{nR}} \sum_{w \in W} P_r(w \neq \hat{w}|w \text{ sent}). \tag{2.2}$$

The objective is to maximize the transmission rate between the legitimate parties:

$$R = \frac{1}{n} H(W) = \frac{1}{n} log_2 2^{nR}. \tag{2.3}$$

subject to a certain equivocation rate between the legitimate transmitter and the eavesdropper:

$$R_e = \frac{1}{n} H(W|Y_e^n). \tag{2.4}$$

Therefore, the main two goals are: (i) maximize the rate of reliable communication (i.e. arbitrarily low probability of error) between transmitter and legitimate receiver (reliability condition); (ii) ensuring that the eavesdropper learns as little as possible about the original message (secrecy condition).

The pair $(\acute{R}, \acute{R}_e)$ is said to be achievable if for all $\epsilon > 0$, there exists a sequence of $(2^{nR}, n)$ codes such that $R \geq \acute{R} - \epsilon$, $R_e \geq \acute{R}_e - \epsilon$ and $P_e^n \leq \epsilon$. The perfect secrecy rate R_s is achievable if for all $\epsilon > 0$, there exists a sequence of $(2^{nR}, n)$ codes such that $R \geq R_s - \epsilon, R_e \geq R_s - \epsilon$ and $P_e^n \leq \epsilon$.

Finally, the secrecy capacity C_s corresponds to the supremum of the achievable perfect secrecy rates over a certain input alphabet. Csiszár and Körner have shown that the secrecy capacity of the wiretap channel is given by [9]:

$$C_s = \max_{p(U,X)} I(U;Y_m) - I(U;Y_e). \tag{2.5}$$

where, $I(U;Y_m)$ and $I(U,Y_e)$ represent mutual information and U is an auxiliary random variable over a certain alphabet that satisfies the Markov relationship $U \rightarrow X \rightarrow (Y_m, Y_e)$, and the outputs Y_m, Y_e at the receivers, respectively. In turn, the secrecy capacity of the degraded wiretap channel, defined as a wiretap channel with Bob´s channel being stronger than Eve´s channel, is given by [9]:

$$C_s = \max_{p(X)} [I(X;Y_m) - I(X;Y_e)]. \tag{2.6}$$

where $I(X;Y_m)$ and $I(X;Y_e)$ represent mutual informatoins between the random variable X and Y_m and Y_e respectively. It is shown in [9] that for the degraded wiretap channel, the secrecy rate is achievable when $U = X$.

2.1.3 Other wiretap models

In addition to the general wiretap channel model in Figure 2.2, there are various other models that aim to capture particular scenarios with relevance to contemporary communications systems.

2.1.3.1 Gaussian wiretap channel

In the Gaussian wiretap channel, the legitimate and the eavesdropper channels are modeled as:

$$Y_m = X + N_m. \tag{2.8}$$

$$Y_e = X + N_e. \tag{2.9}$$

where Y_m denotes the legitimate channel receive symbol at a certain time slot, Y_e denotes the eavesdropper channel receive symbol at a certain time slot, X denotes the transmit symbol at a certain time slot, N_m is a Gaussian random variable with mean zero and variance N_{0m} representing the noise in the main channel and N_e is a Gaussian random variable with mean zero and variance N_{0e} representing the noise in the eavesdropper channel. Yeung and Hellman [28] have shown that the secrecy capacity of the Gaussian wiretap channel is given by

$$C_s = (C_m - C_e)^+ = max\left[0, \frac{1}{2}log_2\left(1 + \frac{P}{N_{0m}}\right) - \frac{1}{2}log_2\left(1 + \frac{P}{N_{0e}}\right)\right]. \tag{2.10}$$

if the legitimate channel is less noisy than the eavesdropper channel ($N_{0m} < N_{0e}$), and

$$C_s = 0. \tag{2.11}$$

if the legitimate channel is more noisy than the eavesdropper channel ($N_{0m} > N_{0e}$). The variable P denotes the transmit power.

The Gaussian wiretap channel models basic communications systems where the transmissions are contaminated by thermal noise.

2.1.3.2 The parallel Gaussian wiretap channel

In the parallel Gaussian wiretap channel, the legitimate and the eavesdropper channels are modeled as:

$$\mathbf{y}_m = \mathbf{\Lambda}_m\mathbf{x} + \mathbf{n}_m. \tag{2.12}$$

$$\mathbf{y}_e = \mathbf{\Lambda}_e\mathbf{x} + \mathbf{n}_e. \tag{2.13}$$

where $\mathbf{y}_m \in \mathbb{C}^n$ denotes the vector of receive symbols at the legitimate receiver at a certain time instant, $\mathbf{y}_e \in \mathbb{C}^n$ denotes the vector of receive symbols at the eavesdropper at a certain time instant, $\mathbf{\Lambda}_m \in \mathbb{C}^n$ is diagonal matrix denotes the legitimate channel, $\mathbf{\Lambda}_e \in \mathbb{C}^n$ is diagonal matrix denotes the eavesdropper channel, $\mathbf{x} \in \mathbb{C}^n$ denotes the vector of transmit symbols at a certain time instant, $\mathbf{n}_m \in \mathbb{C}^n$ is a vector of Gaussian random variables with mean zero and identity covariance matrix and $\mathbf{n}_e \in \mathbb{C}^n$ is also a vector of Gaussian random variables with mean zero and identity covariance matrix. In turn, the secrecy capacity of independent parallel Gaussian wiretap channels is given by [12]

$$C_s = \sum_{i=1}^{n} \max_{x_i \to y_{m_i}, y_{e_i}} I\Big(x_i; y_{m_i}\Big) - I\Big(x_i; y_{e_i}\Big). \tag{2.14}$$

where the maximization is over all the distributions $P_{x_i}(x_i)$ of the random variables X, $i = 1, 2, \ldots, n$ is the number of sub-channels.

The parallel Gaussian wiretap channel models OFDM communications systems [29]. This model will be the basis for most of the work carried out in the thesis.

2.2 Physical-layer security: A review on the use of jamming to achieve enhanced secrecy

The main feature of communication security is the system reliability, which means that a certain message (encoded and transmitted over a wireless channel) intended for a specific user (or legitimate receiver), should be reliably received by that user. The enemy of system reliability is called a jammer. The purpose of a jammer is solely to (i) disrupt the process of communication by increasing the legitimate receiver's probability of decoding error, and / or by causing reliability outage, or secrecy capacity outage; hence called an unfriendly jammer or to (ii) increase the secrecy of wireless networks; and therefore called a friendly jammer.

2.2.1 Jamming concept in wireless communication

Jamming in wireless networks became a relevant topic since the late eighties. Several works studied the jamming effect on point to point communication systems.

The jammer was assumed to have access either to the transmitter / eavesdropper output [30], or the transmitter / eavesdropper input message [31].

The following sub-section provides an overview of the main contributions associated with unfriendly and friendly jamming in wireless communications systems.

2.2.1.1 Prior work on unfriendly jamming

The impact of malicious jammers, in addition to eavesdroppers, on the quality of the communication link is also a problem of long-standing interest. An information theoretic analysis of communications in the presence of a hostile jammer was presented by McEliece and Stark in 1981 [32]. They proved the existence of simultaneously optimal strategies for both the coder and jammer under certain restrictions. When the coder and jammer both have average power constraints the minimax strategies are shown to be Gaussian input, Gaussian jamming. However, Gaussian jamming is shown not to be a saddle point strategy when the input is restricted to be binary [32].

A two-player zero sum game was formulated where the payoff function is the square-difference distortion. The optimal policies (saddle-point) are obtained where the jammer taps the channel and feeds back a signal, at a given energy level, for the purpose of jamming the transmitter sequence [30]. The payoff function is to be maximized by the jammer and to be minimized by the transmitter and the receiver. By adopting a zero-sum game formulation, where the payoff function is the mean squared error, a complete set of solutions is obtained under two different sets of conditions, depending on whether the encoder mapping is deterministic or stochastic [31].

In [33], the authors introduce a power allocation game through which a wiretapper possesses the dual capability to act either as a passive eavesdropper and/or as an active jammer. They investigate transmission strategies in a MIMO wiretap channel with a transmitter, receiver and wiretapper, each equipped with multiple antennas. The wiretapper is able to act either as a passive eavesdropper or as an active jammer per channel use, under a half-duplex constraint. The transmitter therefore faces a choice between dynamically allocating all of its power for data; or broadcasting artificial noise along with the information signal in order to selectively degrade the eavesdropper´s channel. The work has been formulated as a zero-sum game, secrecy

rate as the payoff function, however, the transmitter power allocation strategy is predefined, either to use its full power when transmitting data, or a sufficient power to move the eavesdropper channel into a degraded one.

2.2.1.2 Prior work on friendly jamming

In general, secrecy rate can be increased in two ways: i) by improving the SNR of the legitimate receiver; or ii) by reducing the SNR of the eavesdropper. It is known that interference in wireless channels can be used effectively by cooperating nodes to improve the performance of wireless networks, for example, [34] addresses the secrecy sum rate maximization over a MAC and two-way wiretap channels via cooperative jamming between transmitters against the eavesdropper. A cooperative jamming is proposed, where users who are prevented from transmitting according to the secrecy sum rate maximizing power allocation policy jam the eavesdropper, thereby helping the remaining users.

Both [35] and [36] investigate physical layer security by using friendly jammer. The secrecy capacity can be improved by using friendly jammers that introduce extra interference to the eavesdroppers. In [35], the authors investigate the interaction between the source that transmits the useful data and friendly jammers who assist the source by causing interference to the eavesdropper. To select the friendly jammer, they introduce a game theoretic approach. The game is defined such that the source pays the jammers to interfere with the eavesdropper, therefore, increasing the secrecy rate. The friendly jammers charge the source with a certain price for the jamming, and there is a tradeoff for the price. If too low, the profit of the jammers is low; and if too high, the source would not buy the service (jamming power) or would buy it from other jammers. To analyze the game outcome, they investigate a Stackelberg type of game between the source and the friendly jammers as a power control scheme to achieve the optimized secrecy rate of the source, in which the source is treated as the sole buyer and the friendly jammers are the sellers. However [36] investigates a Stackelberg game for a two-way relay system where the two sources can only communicate through an untrusted intermediate relay.

The impact of friendly jamming on the secrecy outage probability of a quasi-static wiretap Rayleigh fading channel has been analyzed in [37] by computing the probability of secrecy outage in connection with two measures of physical-layer security: the jamming coverage and the jamming efficiency. A set of the jammer

selection strategies are proposed based on the position of the jammer to measure the jamming effect to increase the secrecy level between the legitimate transmitter and receiver.

2.2.2 Prior work on jamming associated with OFDM communications systems

In view of the fact that the wireless spectrum is a scarse and expensive resource, the quest for spectral efficiency has become the holy grail in wireless communications [38]. Over the past years, the wireless network industry has been growing significantly and developing high speed network products to provide wireless multimedia application based on OFDM due to the high data rates and robust communication characteristics of OFDM [39, 40]. In the 1980s, OFDM was studied for high-speed modems [41, 42], digital mobile communications and high density recording [43]. In the 1990s, OFDM was studied for HDSL [44], ADSL, VHDSL [45]. OFDM is a modulation technique that has been suggested for use in cellular radio [46, 47], DAB [48], DVB and wireless LAN systems such as IEEE 802.11, HIPERLAN, and MMAC [49]. In 1998, HiperLAN/2 (Europe) and MMAC (Japan) adopted OFDM in their physical layer specifications [50]. The primary benefit of using OFDM is spectral efficiency, which means that we can transmit more data faster in a given bandwidth in the presence of noise. In fact, it has been shown that OFDM leads to substantial improvements in capacity when compared to other standard modulation schemes [38], coming very close to the Shannon limit that defines channel capacity.

OFDM is a block modulation scheme where data symbols are transmitted in parallel by employing a (large) number of orthogonal sub-channels. A block of N serial data symbols, each of duration T_s, is converted into a block of N parallel data symbols, each with duration $T = NT_s$. The N parallel data symbols modulate N sub-channels that are spaced $1/T$ Hz apart [50]. Intersymbol interference is eliminated almost completely by introducing a guard time in every OFDM symbol. In the guard time, the OFDM symbol is cyclically extended to avoid intercarrier interference [51]. This process is succinctly described in Figure 2.3.

Before transmission, a stream of data is converted to parallel form where each bit is assigned to a carrier frequency. Then the IFFT is taken, a cyclic prefix is added to the data, transmission and reception occurs, the cyclic prefix is removed, and the

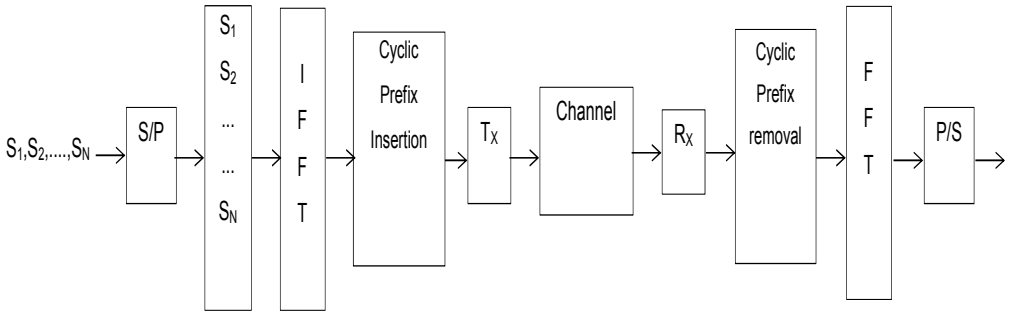

Figure 2.3: Structure of OFDM system.

FFT is taken to get the transmitted data at the receiver.

In view of the relevance of OFDM to current wireless systems, recently OFDM is also used to investigate physical layer security [52, 53], a number of works have also been looking at this scheme not only to improve the reliability but also the security of communications systems. In [53], authors consider the information theoretic secrecy rates that are achievable by an OFDM transmitter / receiver pair in the presence of an eavesdropper. The secrecy capacity is formulated as a maximization problem under a total power constraint on the transmitter signal, and numerical results are provided under a Rayleigh fading channel model and under dependence of the main and eavesdropper channels. Both works [52, 53] did not consider the model in the presence of friendly / unfriendly jamming.

In [12], the authors show that the secrecy capacity increases with the increase in the number of independent parallel sub-channels. Moreover, for such scenarios with OFDM being adopted, optimal power allocation strategies have been derived for the parallel independent channels [12], and for the multi-user broadcast channel in [24] and [25]. In [54], the authors proposed a method that makes use of channel randomness, reciprocity, and fast decorrelation in space to secure OFDM with low overheads on encryption, decryption, and key distribution.

In spite of the numerous theoretical contributions, the general problem of design of physical-layer transmission schemes for both reliable and secure communications over OFDM communications systems, which can be modelled using parallel Gaussian wiretap channels, is still widely open. In particular, the impact of unfriendly or friendly jammers to the achievable secrecy rates of OFDM communications systems is still open in general. The objective of this PhD research is to fill this vacuum.

Chapter 3
Parallel Gaussian Wiretap Channel with an Unfriendly Jammer: A Zero-Sum Power Allocation Game

3.1 Introduction

In this Chapter we are interested in the security aspect of the wireless communication network. On the physical layer, the computation of the secrecy capacity of different communication channels has been an important research topic in the last few decades [8], [10], [13], [6], [55], [56]. The impact of malicious jammers, in addition to eavesdroppers, on the quality of the communication link is also another problem of long-standing interest [57], [58], [59] and [60].

In the classical problem of increasing the reliable and secure information transmission rate between the input and the output of a system, called the secrecy rate, different approaches can be used which are: maximization of the mutual information via transmit diversity techniques with known CSI [61], [62], [63], [64], in the case of flat fading [65], [66], maximization of the SINR [67], minimization of the BER [67], [68], [69], [70], or minimization of the MSE [67], [27].

In general, secrecy rate can be increased in two ways: i) by improving the signal-to-noise ratio (SNR) of the legitimate receiver; or ii) by reducing the SNR of the eavesdropper, i.e., by impairing the reception at the eavesdropper. In this Chapter, we consider a scenario applicable to current OFDM communications systems consisting of a bank of parallel independent wiretap Gaussian channels, where two legitimate parties (Alice and Bob) communicate in the presence of a malicious jammer and an eavesdropper (Eve). The eavesdropper is assumed to be passive but

the jammer acts as an active player injecting interference to the main channel in the form of additive noise.

Recently, game theory has been of main interest in the information-theoretic research, particularly, in models where multiple players would exist; such as in the wiretap channel. Different game-theoretic approaches have been used to find optimal power allocation strategies for MIMO and SISO channels in [71], [72] respectively. Game theoretic power allocation strategies for maximizing Shannon´s capacity with relaying have been derived in [73], [74]. In [75], the Nash equilibria were analyzed for different types of relaying protocols. In [76], a Stackelberg game has been used to derive the optimal power allocation for a fading MAC channel. A two-player zero sum game was formulated in [30], where the payoff function is the mean-squared error of the decoded message relative to the transmitter message and the jammer taps the channel and feeds back a signal, at a given energy level, for the purpose of jamming the transmitted sequence. The mean-squared error is to be maximized by the jammer and to be minimized by the transmitter and the receiver.

The main contributions of this Chapter are as follows: (i) a game-theoretic formulation of the achievable secrecy rates[3] in the parallel Gaussian wiretap channel with an unfriendly jamming; (ii) a proof of the existence of a Nash equilibrium of the zero-sum game; and (iii) a characterization of the optimal transmission and jamming power allocation strategies for a zero-sum game, which are specialized for key asymptotic regimes. A range of simulation results also illustrate the secrecy gains that an adaptive transmitter exhibits over a non-adaptive one.

This chapter is organized as follows: Section 3.2 describes the problem setup. Section 3.3 analyzes the two-person zero-sum game, by establishing the existence of a pure strategy Nash equilibrium and by providing the best response of the transmitter for a fixed jammer strategy, the best response of the jammer for a fixed transmitter strategy as well as the Nash equilibrium achieving strategies in certain asymptotic regimes. Section 3.4 presents a set of numerical results that cast further insight into the nature of the optimal strategies as well as the Nash equilibrium. The results also unveils the secrecy gain of an adaptive transmitter over a non-adaptive one. In Section 3.5, we summarize the main contributions of this research work.

[3]The secrecy rate indicates the transmission rate at which the eavesdropper is unable to decode any informations and also note that the secrecy capacity is the maximum value of the secrecy rate.

3.2 Problem formulation

We consider the Gaussian wiretap channel model of Figure 3.1. The model considers a communication scenario where a legitimate user, Alice, tries to communicate with another legitimate user, Bob, in the presence of an eavesdropper, Eve, and an unfriendly jammer over banks of n parallel independent Gaussian channels. Note that this represents a simplification of typical wireless communications systems, where, due to the characteristics of wireless propagation, the jammer would introduce interference in both the main and the eavesdropper channels. Hence, this applies to scenarios where, with the intent of impairing the communication over the main channel between the legitimate parties, the jammer positions himself to be much closer to the legitimate receiver than the eavesdropper. Furthermore, this also applies to scenarios where the jammer colludes or cooperates with the eavesdropper so that the eavesdropper is able to subtract the interference from the jammer. Therefore, the interference caused by the jammer injected power will mainly harm the communication between the two legitimate parties, Alice and Bob.

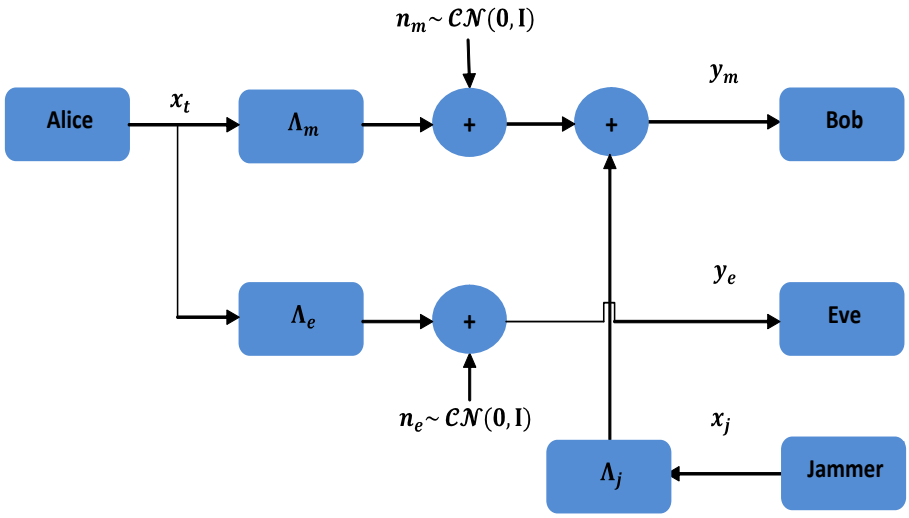

Figure 3.1: Gaussian wiretap channel model with an unfriendly jammer.

Bob observes the output of the main channel given by:

$$\mathbf{y}_m = \mathbf{\Lambda}_m \mathbf{x}_t + \mathbf{n}_m + \mathbf{\Lambda}_j \mathbf{x}_j \tag{3.1}$$

and Eve observes the output of the eavesdropper channel given by:

$$\mathbf{y}_e = \mathbf{\Lambda}_e \mathbf{x}_t + \mathbf{n}_e \tag{3.2}$$

where $\mathbf{y}_m \in \mathbb{C}^n$ and $\mathbf{y}_e \in \mathbb{C}^n$ represent the vectors of complex receive symbols at the output of the main and eavesdropper channels respectively, $\mathbf{x}_t \in \mathbb{C}^n$ represents the vector of complex transmit symbols with mean zero and covariance $\mathbf{\Sigma}_x = \mathbb{E}[\mathbf{x}_t \mathbf{x}_t^\dagger]$, and $\mathbf{n}_m \in \mathbb{C}^n$ and $\mathbf{n}_e \in \mathbb{C}^n$ represent vectors of circularly symmetric complex Gaussian noise random variables with zero-mean and identity covariance matrix, i.e., standard white Gaussian noise. We assume that $\mathbf{x}_j \in \mathbb{C}^n$ is a vector of circularly symmetric complex Gaussian noise with mean zero and covariance $\mathbf{\Sigma}_j = \mathbb{E}[\mathbf{x}_j \mathbf{x}_j^\dagger]$, which represents the jamming action. Note that this jamming strategy is not necessarily optimal but it is convenient both from the practical and the theoretical stand point. For example, this choice of distribution to the jamming action leads to closed form achievable secrecy rate expressions [59], [60]. We also assume that the random vectors $\mathbf{x}_t$, $\mathbf{x}_j$, $\mathbf{n}_m$, and $\mathbf{n}_e$ are independent.

$\mathbf{\Lambda}_m = diag\,(\lambda_{m_1}, \lambda_{m2}, \ldots, \lambda_{mn}) \in \mathbb{C}^n$ is a diagonal matrix that contains the complex gains of the parallel sub-channels of the main channel, $\mathbf{\Lambda}_e = diag\,(\lambda_{e_1}, \lambda_{e2}, \ldots, \lambda_{e_n}) \in \mathbb{C}^n$ is a diagonal matrix that contains the complex gains of the parallel sub-channels of the eavesdropper channel, and, likewise, $\mathbf{\Lambda}_j = diag\,(\lambda_{j_1}, \lambda_{j2}, \ldots, \lambda_{j_n}) \in \mathbb{C}^n$ is a diagonal matrix that contains the complex gains of the parallel sub-channels that compose the jammer channel. Note once again that this model arises in systems where Alice, Bob, Eve and the jammer adopt OFDM modulation and demodulation.

We assume that Alice, Bob, Eve and the jammer know the exact channel conditions. In general, the legitimate parties may not be able to estimate the state of the eavesdropper channel. For example, the legitimate parties may not even be aware of the presence of the eavesdropper. However, this assumption can be justified in situations where both the jammer and the eavesdropper are also active users in the wireless network, that employs time division multiple access (TDMA). In view of channel reciprocity, the users will be able to estimate other users channels or share the knowledge of other users channels [77].

Both the transmitter and the unfriendly jammer transmit independent symbols over the different sub-channels. Thus we take both the input and jamming covariance matrices to be diagonal, i.e., $\mathbf{\Sigma}_x = \mathbb{E}[\mathbf{x}_t \mathbf{x}_t^\dagger] = diag\,(\sigma_{x_1}, \sigma_{x_2}, \ldots, \sigma_{x_n})$ and $\mathbf{\Sigma}_j = \mathbb{E}[\mathbf{x}_j \mathbf{x}_j^\dagger] = diag\,(\sigma_{j_1}, \sigma_{j_2}, \ldots, \sigma_{j_n})$, respectively, where σ_{x_i} represents the power injected into the main sub-channel i and σ_{j_i} represents the power injected into the jammer sub-channel i, $i = 1, 2, \ldots, n$.

Additionally, we impose some power restrictions on both the transmitter and jammer, namely:

$$\sum_{i=1}^{n} \sigma_{x_i} \leq P \tag{3.3}$$

$$\sum_{i=1}^{n} \sigma_{j_i} \leq P_j \tag{3.4}$$

where P and P_j are the total transmitter and the jammer power respectively.

The secrecy capacity corresponds to the largest achievable reliable transmission rate with perfect secrecy [55]. The general expression of the secrecy capacity of a wiretap channel is given by [9]:

$$C_s = \max_{\mathbf{v} \to \mathbf{x}_t \to \mathbf{y}_m, \mathbf{y}_e} I\Big(\mathbf{v}; \mathbf{y}_m\Big) - I\Big(\mathbf{v}; \mathbf{y}_e\Big) \tag{3.5}$$

where the maximization is over all joint distributions $P_{\mathbf{v},\mathbf{x}_t}(\mathbf{v}, \mathbf{x}_t)$ such that the Markov chain $\mathbf{v} \to \mathbf{x}_t \to \mathbf{y}_m\ \mathbf{y}_e$ holds [4].

In [12, Theorem 1], it is shown that for a bank of independent parallel Gaussian wiretap channels the secrecy capacity in (3.5), as like (2.14), reduces to:

$$C_s = \sum_{i=1}^{n} C_{s_i} = \sum_{i=1}^{n} \max_{\mathbf{x}_{t_i} \to \mathbf{y}_{m_i}, \mathbf{y}_{e_i}} I\Big(\mathbf{x}_{t_i}; \mathbf{y}_{m_i}\Big) - I\Big(\mathbf{x}_{t_i}; \mathbf{y}_{e_i}\Big) \tag{3.6}$$

where C_{s_i} represents the secrecy capacity of the ith sub-channel and the maximizations are over all the distributions $P_{x_{t_i}}(x_{t_i}), i = 1, \ldots, n$ and x_{t_i} represents the complex transmit symbol in the i^{th} sub-channel, y_{m_i} represents the complex receive symbol in the i^{th} main sub-channel and y_{e_i} represents the complex receive symbol in the i^{th} eavesdropper sub-channel.

Note that the secrecy capacity of a bank of independent parallel Gaussian wiretap channels, which is achieved by independent complex Gaussian inputs, is equal to the sum of the secrecy capacities of the individual wiretap sub-channels [12].

Fix the input signal covariance $\mathbf{\Sigma}_x = diag(\sigma_{x_1}, \ldots, \sigma_{x_n})$ and the jammer signal covariance $\mathbf{\Sigma}_j = diag(\sigma_{j_1}, \ldots, \sigma_{j_n})$, where $\sigma_{x_1}, \ldots, \sigma_{x_n}$ and $\sigma_{j_1}, \ldots, \sigma_{j_n}$ represent the

[4] In this chapter we will use $\max_X$ where X is a random variable as a shorthand for the maximization over the choice of the probability distributions $P_X(x)$ of the random variable X.

set of powers that the transmitter and the jammer inject into the bank of parallel independent channels, respectively. Note that, we restrict the attention to scenarios where the jammer does not introduce correlated noise accross the sub-channels.

Then the secrecy capacity can be written as follows [12]:

$$\begin{aligned} C_s\left(\sigma_{x_1},\ldots,\sigma_{x_n},\sigma_{j_1},\ldots,\sigma_{jn}\right) &= \sum_{i=1}^{n} C_{s_i}(\sigma_{x_i},\sigma_{j_i}) \\ &= \sum_{i=1}^{n}\left[\log\left(1+\frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2}{1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2}\right)-\log\left(1+\sigma_{x_i}\left|\lambda_{e_i}\right|^2\right)\right]^+ \end{aligned} \tag{3.7}$$

where $[z]^+ = \max(0, z)$.

We study a zero-sum game between the transmitter and the jammer with a pay-off or utility function given by:

$$U\Big(\sigma_{x_1},\ldots,\sigma_{x_n};\sigma_{j_1},\ldots,\sigma_{j_n}\Big) = C_s\Big(\sigma_{x_1},\ldots,\sigma_{x_n};\sigma_{j_1},\ldots,\sigma_{j_n}\Big) \tag{3.8}$$

where the transmitter and the jammer determine adaptively the strategies, which are characterized by the respective power allocation policies, that maximize and minimize, respectively, the value of the utility function. We also impose the power restrictions in (3.3) and (3.4) as:

$$\sum_{i=1}^{n}\sigma_{x_i} \le P \tag{3.9}$$

with $\sigma_{x_i} \ge 0, \forall\ i$, and

$$\sum_{i=1}^{n}\sigma_{j_i} \le P_j \tag{3.10}$$

with $\sigma_{j_i} \ge 0, \forall i$, where P and P_j represent the transmitter and jammer available power, respectively. It is simple to show that for non degraded sub-channels, where $|\lambda_{m_i}|^2 < |\lambda_{e_i}|^2$, $(\sigma^*_{x_i}, \sigma^*_{j_i}) = (0, 0)$ is an optimal strategy. Therefore, the analysis concentrates only on degraded scenarios, where $|\lambda_{m_i}|^2 \ge |\lambda_{e_i}|^2$.

Le us now consider a scenario where the sub-channels are degraded. Now, note that

the secrecy capacity of the i^{th} sub-channel is equal to zero if and only if

$$\frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2}{1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2} \leq \sigma_{x_i}\left|\lambda_{e_i}\right|^2$$

$$\Leftrightarrow \frac{\left|\lambda_{m_i}\right|^2}{1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2} \leq \left|\lambda_{e_i}\right|^2$$

$$\Leftrightarrow \left|\lambda_{e_i}\right|^2\left(1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2\right) \geq \left|\lambda_{m_i}\right|^2$$

$$\Leftrightarrow \sigma_{j_i} \geq \frac{\left|\lambda_{m_i}\right|^2-\left|\lambda_{e_i}\right|^2}{\left|\lambda_{e_i}\right|^2\left|\lambda_{j_i}\right|^2} \tag{3.11}$$

Therefore, since by setting $\sigma_{j_i} \geq \frac{\left|\lambda_{m_i}\right|^2-\left|\lambda_{e_i}\right|^2}{\left|\lambda_{e_i}\right|^2\left|\lambda_{j_i}\right|^2}$, the secrecy capacity of the i^{th} sub-channel becomes equal to zero, it is only natural that a rational jammer will limit the powers injected on the sub-channels according to such constraints in view of the overall power constraint. Consequently, rather than considering the zero-sum game with the payoff function:

$$U\left(\sigma_{x_1},\ldots,\sigma_{x_n};\sigma_{j_1},\ldots,\sigma_{j_n}\right)=\sum_{i=1}^{n}\left[\log\left(1+\frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2}{1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2}\right)-\log\left(1+\sigma_{x_i}\left|\lambda_{e_i}\right|^2\right)\right]^+ \tag{3.12}$$

subject to the constraints $\sum_{i=1}^{n}\sigma_{x_i} \leq P$ with $\sigma_{x_i} \geq 0, \forall i$, and $\sum_{i=1}^{n}\sigma_{j_i} \leq P_j$ with $\sigma_{j_i} \geq 0, \forall i$, we will consider a zero-sum game with the slightly different payoff function:

$$U_1\left(\sigma_{x_1},\ldots,\sigma_{x_n};\sigma_{j_1},\ldots,\sigma_{j_n}\right)=\sum_{i=1}^{n}\left[\log\left(1+\frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2}{1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2}\right)-\log\left(1+\sigma_{x_i}\left|\lambda_{e_i}\right|^2\right)\right] \tag{3.13}$$

subject to the constraints $\sum_{i=1}^{n}\sigma_{x_i} \leq P$ with $\sigma_{x_i} \geq 0, \forall i$, and $\sum_{i=1}^{n}\sigma_{j_i} \leq P_j$ with $\sigma_{j_i} \leq \frac{\left|\lambda_{m_i}\right|^2-\left|\lambda_{e_i}\right|^2}{\left|\lambda_{e_i}\right|^2\left|\lambda_{j_i}\right|^2}$ and $\sigma_{j_i} \geq 0, \forall\ i$. This modification, which does not affect the solution of the game, is motivated by the fact that the payoff function in (3.13) exhibits convexity properties that the payoff function in (3.12) does not due to the operation $[.]^+$.

3.3 Analysis

We will now study the zero-sum game put forth in (3.13). In particular, we will establish the existence of a pure strategy Nash equilibrium and characterize the best response of Alice for a fixed jammer strategy, the best response of the jammer for a fixed Alice strategy and the Nash equilibrium in certain asymptotic regimes.

Definitions:

- *Pure strategy*: A pure strategy is a specific action that a player will follow in every possible attainable situation in a game, i.e., player´s actions are deterministic and are not regulated by probability distribution as like a mixed strategy.

- *Two person zero-sum game*: two person zero-sum game is a two player game, in which a player´s gains (or losses) of utility is exactly balanced by the losses (or gains) of the other player´s utility, i.e., when a player maximizes his payoff, he also simultaneously minimizes the other player payoff.

- *Nash equilibrium*: The Nash equilibrium is a solution concept of a non-cooperative game. If there is a set of strategies with such properties that no player can benefit by changing his strategy while other players keep their strategies unchanged, then that set of strategies and corresponding payoffs constitute the Nash equilibrium. Note that, for a two person zero-sum game, a pure strategy Nash equilibrium exists if and only if:

$$\max_i \min_j a_{i,j} = \min_j \max_i a_{i,j} \tag{3.14}$$

  where, i and j are indices that denote the strategies of two players and $a_{i,j}$ is the corresponding payoff function.

3.3.1 Existence of pure strategy Nash equilibrium

The following Theorem establishes the existence of a pure strategy Nash equilibrium, which consists of a set of fixed (non-probabilistic) player strategies.

Theorem 1. *Consider the zero-sum game between the transmitter and the jammer in* (3.13)*. Then, there exists a pure strategy Nash equilibrium.*

Proof. The proof capitalizes on [78, Theorem 5.2].

The transmitter pure strategies set is given by:

$$\Psi = \left\{ \sigma_{x_i} \in \Re_0^+, i = 1, 2, ..., n : \sum_{i=1}^{n} \sigma_{x_i} \leq P \right\} \tag{3.15}$$

The jammer pure strategies set is given by:

$$\Phi = \left\{ \sigma_{j_i} \in \Re_0^+, i = 1, 2, ..., n : \sum_{i=1}^{n} \sigma_{j_i} \leq P_j; \sigma_{j_i} \leq \frac{|\lambda_{m_i}|^2 - |\lambda_{e_i}|^2}{|\lambda_{e_i}|^2 |\lambda_{j_i}|^2} \right\} \tag{3.16}$$

It is clear that Ψ and Φ are both closed, bounded and non-empty convex subsets of finite dimensional Euclidean space.

It is also clear that the payoff $U_1(\sigma_{x_1}, \ldots, \sigma_{x_n}, \sigma_{j_1}, \ldots, \sigma_{j_n})$ is continuous in $\sigma_{x_i}, i = 1, 2, \ldots, n \in \Psi$ for given $\sigma_{j_i}, i = 1, 2, \ldots, n \in \Phi$ and the payoff $U_1(\sigma_{x_1}, \ldots, \sigma_{x_n}, \sigma_{j_1}, \ldots, \sigma_{j_n})$ is also continuous in $\sigma_{j_i}, i = 1, 2, \ldots, n \in \Phi$ for given $\sigma_{x_i}, i = 1, 2, \ldots, n \in \Psi$.

For a given transmitter strategy σ_{x_i}, the second order derivative of the payoff $U_1(\sigma_{x_1}, \ldots, \sigma_{x_n}, \sigma_{j_1}, \ldots, \sigma_{j_n})$ with respect to σ_{j_i}, for every $i = 1, 2, \ldots, n$, is:

$$\frac{\partial^2 U_1(\sigma_{x_i}, \sigma_{j_i})}{\partial {\sigma_{j_i}}^2} = \left[|\lambda_{j_i}|^4 |\lambda_{m_i}|^2 \sigma_{x_i} \left[\frac{1}{\left(1 + \sigma_{j_i}|\lambda_{j_i}|^2 + \sigma_{x_i}|\lambda_{m_i}|^2\right)^2 \left(1 + \sigma_{j_i}|\lambda_{j_i}|^2\right)} + \frac{1}{\left(1 + \sigma_{j_i}|\lambda_{j_i}|^2 + \sigma_{x_i}|\lambda_{m_i}|^2\right) \left(1 + \sigma_{j_i}|\lambda_{j_i}|^2\right)^2} \right] \right] \geq 0 \tag{3.17}$$

i.e., the payoff $U_1(\sigma_{x_1}, \ldots, \sigma_{x_n}, \sigma_{j_1}, \ldots, \sigma_{j_n})$ is concave in $\sigma_{x_i} \in \Psi$ for each σ_{j_i}.

And for given jammer strategy σ_{j_i}, the second order derivative of the payoff $U_1(\sigma_{x_1}, \ldots, \sigma_{x_n}, \sigma_{j_1}, \ldots, \sigma_{j_n})$ with respect to σ_{x_i}, for every $i = 1, 2, \ldots, n$, is:

$$\frac{\partial^2 U_1(\sigma_{x_i}, \sigma_{j_i})}{\partial {\sigma_{x_i}}^2} = \left[-\frac{1}{\left(\frac{1+\sigma_{j_i}|\lambda_{j_i}|^2}{|\lambda_{m_i}|^2} + \sigma_{x_i}\right)^2} + \frac{1}{\left(\frac{1}{|\lambda_{e_i}|^2} + \sigma_{x_i}\right)^2} \right] \leq 0 \tag{3.18}$$

This follows from Equation (3.11) because

$$\frac{|\lambda_{m_i}|^2}{1+\sigma_{j_i}|\lambda_{j_i}|^2} \geq |\lambda_{e_i}|^2$$

$$\Rightarrow \ \frac{1}{|\lambda_{e_i}|^2} \geq \frac{1+\sigma_{j_i}|\lambda_{j_i}|^2}{|\lambda_{m_i}|^2}$$

$$\Rightarrow \ \Big(\frac{1}{|\lambda_{e_i}|^2}+\sigma_{x_i}\Big)^2 \geq \Big(\frac{1+\sigma_{j_i}|\lambda_{j_i}|^2}{|\lambda_{m_i}|^2}+\sigma_{x_i}\Big)^2$$

$$\Rightarrow \ \left[-\frac{1}{\Big(\frac{1+\sigma_{j_i}|\lambda_{j_i}|^2}{|\lambda_{m_i}|^2}+\sigma_{x_i}\Big)^2}+\frac{1}{\Big(\frac{1}{|\lambda_{e_i}|^2}+\sigma_{x_i}\Big)^2}\right] \leq 0, \tag{3.19}$$

i.e., the payoff $U_1(\sigma_{x_1},\ldots,\sigma_{x_n},\sigma_{j_1},\ldots,\sigma_{j_n})$ is convex in $\sigma_{j_i}\in\Phi$ for each σ_{x_i}.

Therefore, by [78, Theorem 5.2], the two-person zero sum game has at least one pair of pure strategy NE $(\sigma^*_{x_i},\sigma^*_{j_i})$. □

In addition, in view of [78, Theorem 5.2], it also follows that the solution of the zero-sum game, i.e. the Nash equilibrium, satisfies the condition:

$$\max_{\sigma_{x_i},i=1,2,\ldots,n\in\Psi}\ \min_{\sigma_{j_i},i=1,2,\ldots,n\in\Phi} U_1\big(\sigma_{x_1},\ldots,\sigma_{x_n};\sigma_{j_1},\ldots,\sigma_{j_n}\big) = \min_{\sigma_{j_i},i=1,2,\ldots,n\in\Phi}\ \max_{\sigma_{x_i},i=1,2,\ldots,n\in\Psi} U_1\big(\sigma_{x_1},\ldots,\sigma_{x_n};\sigma_{j_1},\ldots,\sigma_{j_n}\big) \tag{3.20}$$

3.3.2 Characterization of best responses

We are now ready to characterize the best response of the jammer to a fixed transmitter strategy and, likewise, the best response of the transmitter to a fixed jammer strategy.

The following Theorem defines the best response of the jammer for a fixed transmitter strategy:

Theorem 2. *Fix the transmitter strategy $\sigma_{x_i}, i = 1, 2, ..., n$. Then, the optimal jammer strategy $\sigma^*_{j_i}, i = 1, 2, ..., n$, that solves the optimization problem:*

$$\min_{\sigma_{j_i}, i=1,2,...,n \in \Phi} U_1\Big(\sigma_{x_1}, \ldots, \sigma_{x_n}, \sigma_{j_1}, \ldots, \sigma_{j_n}\Big) \tag{3.21}$$

where Φ is defined in Equation (3.16), subject to: $\sum_{i=1}^{n} \sigma_{j_i} \leq P_j$, $\sigma_{j_i} \geq 0$ and $\sigma_{j_i} \leq \frac{|\lambda_{m_i}|^2 - |\lambda_{e_i}|^2}{|\lambda_{e_i}|^2 |\lambda_{j_i}|^2}$, $i = 1, 2, \ldots, n$ is given by:

$$\sigma^*_{j_i} = \begin{cases} \frac{\sqrt{\sigma^2_{x_i}|\lambda_{m_i}|^4 + \frac{4\sigma_{x_i}|\lambda_{m_i}|^2|\lambda_{j_i}|^2}{\nu}} - (2 + \sigma_{x_i}|\lambda_{m_i}|^2)}{2|\lambda_{j_i}|^2}, & \frac{\sigma_{x_i}|\lambda_{e_i}|^4|\lambda_{j_i}|^2}{|\lambda_{m_i}|^2\left(1+\sigma_{x_i}|\lambda_{e_i}|^2\right)} \leq \nu < \frac{\sigma_{x_i}|\lambda_{m_i}|^2|\lambda_{j_i}|^2}{1+\sigma_{x_i}|\lambda_{m_i}|^2} \\ \frac{|\lambda_{m_i}|^2 - |\lambda_{e_i}|^2}{|\lambda_{e_i}|^2|\lambda_{j_i}|^2}, & \nu < \frac{\sigma_{x_i}|\lambda_{e_i}|^4|\lambda_{j_i}|^2}{|\lambda_{m_i}|^2\left(1+\sigma_{x_i}|\lambda_{e_i}|^2\right)} \\ 0, & \nu \geq \frac{\sigma_{x_i}|\lambda_{m_i}|^2|\lambda_{j_i}|^2}{1+\sigma_{x_i}|\lambda_{m_i}|^2} \end{cases} \tag{3.22}$$

where ν such that $\sum_{i=1}^{n} \sigma^*_{j_i} = P_j$.

Proof. See Appendix A. □

The following Theorem, which also appears in a different context in [1] and [12], defines the best response of the transmitter for a fixed jammer strategy.

Theorem 3. *Fix the jammer strategy $\sigma_{j_i}, i = 1, 2, ...n$. Then, the optimal Alice strategy $\sigma^*_{x_i}, i = 1, 2, ..., n$, that solves the optimization problem:*

$$\max_{\sigma_{x_i}, i=1,2,...,n \in \Psi} U_1\Big(\sigma_{x_1}, \ldots, \sigma_{x_n}, \sigma_{j_1}, \ldots, \sigma_{j_n}\Big) \tag{3.23}$$

where Ψ is defined in Equation (3.15), subject to: $\sum_{i=1}^{n} \sigma_{x_i} \leq P$ and $\sigma_{x_i} \geq 0, i = 1, 2, ..., n$, is given by:

$$\sigma_{x_i}^* = \begin{cases} \frac{1}{2}\left[\sqrt{\left(\frac{1}{|\lambda_{e_i}|^2} - \frac{1+\sigma_{j_i}|\lambda_{j_i}|^2}{|\lambda_{m_i}|^2}\right)\left(\frac{4}{\eta} + \frac{1}{|\lambda_{e_i}|^2} - \frac{1+\sigma_{j_i}|\lambda_{j_i}|^2}{|\lambda_{m_i}|^2}\right)} - \left(\frac{1+\sigma_{j_i}|\lambda_{j_i}|^2}{|\lambda_{m_i}|^2} + \frac{1}{|\lambda_{e_i}|^2}\right)\right], \\ \qquad\qquad \eta < \frac{|\lambda_{m_i}|^2}{1+\sigma_{j_i}|\lambda_{j_i}|^2} - |\lambda_{e_i}|^2 \\ 0, \qquad\qquad \eta \geq \frac{|\lambda_{m_i}|^2}{1+\sigma_{j_i}|\lambda_{j_i}|^2} - |\lambda_{e_i}|^2 \end{cases} \tag{3.24}$$

where η *such that* $\sum_{i=1}^{n} \sigma_{x_i}^* = P$.

Proof. See Appendix B. □

These Theorems - in addition to specifying the best responses - also lead to algorithms to compute the best responses. However, and of particular relevance is the specialization of the best responses for the regimes of low available power. This specialization will lead to a simple characterization of the Nash equilibrium in such asymptotic regimes. The rational to study the Nash equilibrium in the asymptotic regimes of low available power is associated with the fact that, in mobile system, due to pure geometry users tend to lie in the periphery of the cell so users also tend to operate in the lower power regime, where almost 40% of geographical locations experience a signal-to-noise ratio below 0 dB while less than 10% display level above 10 dB [79], [80], [81].

In the regime of low transmitter available power, $P \to 0$, which implies that $\sigma_{x_i} \to 0, i = 1, \ldots, n$, so that the payoff function in (3.13) can be expanded by using a Taylor series as follows:

$$U_1\Big(\sigma_{x_1}, \ldots, \sigma_{x_n}, \sigma_{j_1}, \ldots, \sigma_{j_n}\Big) = \sum_{i=1}^{n} \left[\frac{\sigma_{x_i}|\lambda_{m_i}|^2}{1+\sigma_{j_i}|\lambda_{j_i}|^2} - \sigma_{x_i}|\lambda_{e_i}|^2 + \mathcal{O}(\sigma_{x_i}^2)\right] \tag{3.25}$$

This expansion leads to the characterization of the transmitter best response for a fixed jammer strategy, which is expressed in the following Theorem.

Theorem 4. *Fix the jammer strategy $\sigma_{j_i}, i = 1, 2, ..., n$. Then, as $P \to 0$, the transmitter best response is given by:*

$$\sigma_{x_i}^* = \begin{cases} P, & i = k \\ \\ 0, & i \neq k \end{cases} \tag{3.26}$$

where

$$k = \arg\max_i \frac{|\lambda_{m_i}|^2}{1 + \sigma_{j_i}|\lambda_{j_i}|^2} - |\lambda_{e_i}|^2 \tag{3.27}$$

Proof. See Appendix C. □

In contrast, in the regime of low jammer available power $P_j \to 0$, which implies that $\sigma_{j_i} \to 0, i = 1, 2, \ldots, n$, so that the payoff function in (3.13) can be expanded also by using a Taylor series as follows:

$$U_1\Big(\sigma_{x_i}, \sigma_{j_i}\Big) = \sum_{i=1}^{n} \left[\log\left(1 + \sigma_{x_i}|\lambda_{m_i}|^2\right) - \frac{\sigma_{x_i}\sigma_{j_i}|\lambda_{m_i}|^2|\lambda_{j_i}|^2}{1 + \sigma_{x_i}|\lambda_{m_i}|^2} - \log\left(1 + \sigma_{x_i}|\lambda_{e_i}|^2\right) + \mathcal{O}\Big(\sigma_{j_i}^2\Big) \right] \tag{3.28}$$

This expansion also leads to the jammer best response for a fixed transmitter strategy, which is expressed in the following Theorem.

Theorem 5. *Fix the transmitter strategy $\sigma_{x_i}, i = 1, 2, ..., n$. Then, as $P_j \to 0$, the jammer best response is given by:*

$$\sigma_{j_i}^* = \begin{cases} P_j, & i = k \\ \\ 0, & i \neq k \end{cases} \tag{3.29}$$

where

$$k = \arg\max_i \frac{\sigma_{x_i}|\lambda_{m_i}|^2|\lambda_{j_i}|^2}{1 + \sigma_{x_i}|\lambda_{m_i}|^2} \tag{3.30}$$

Proof. See Appendix D. □

Theorems 4 and 5 reveal that in the regime of low available power the transmitter and the jammer will inject power in a single sub-channel, which is specified by the index in (3.27) and (3.30), respectively. In contrast, for medium and high available powers the transmitter and the jammer will divide the power between the various sub-channels, as specified by Theorems 2 and 3. This aspect is further explored in the numerical results section.

3.3.3 Characterization of the Nash equilibrium in the asymptotic regimes of low available power

We will now characterize the Nash equilibrium in two asymptotic regimes: i) the asymptotic regime of low transmitter available power, where $P \to 0$; and ii) the asymptotic regime of low jammer available power, where $P_j \to 0$. This, which applies to various practical scenarios as specified earlier, casts insight into the nature of the optimal strategies. The characterization of the Nash equilibrium in such asymptotic regimes, which is not in general possible in non-asymptotic regimes, builds upon the best responses embodied in Theorems 4 and 5.

In particular, Theorem 4 suggests that in the regime of low transmitter power, and for any fixed jammer strategy, the transmitter will only inject power in a single sub-channel. This, together with the characterization of the value of the zero-sum game on the right hand side of (3.20) leads directly to Theorem 6.

Theorem 6. *When the transmitter available power is low, i.e., $P \to 0$, there exists a pure strategy Nash equilibrium which is given by:*

$$(\sigma_{x_i}^*, \sigma_{j_i}^*) = \begin{cases} \big(P, min\big(P_j, \frac{|\lambda_{m_i}|^2 - |\lambda_{e_i}|^2}{|\lambda_{e_i}|^2 |\lambda_{j_i}|^2}\big)\big), & i = k \\ \big(0, 0\big), & i \neq k \end{cases} \tag{3.31}$$

where the index k is expressed as:

$$k = \arg\max_i \left[\frac{P|\lambda_{m_i}|^2}{1 + min\big(P_j, \frac{|\lambda_{m_i}|^2 - |\lambda_{e_i}|^2}{|\lambda_{e_i}|^2 |\lambda_{j_i}|^2}\big)|\lambda_{j_i}|^2} - P|\lambda_{e_i}|^2 \right] \tag{3.32}$$

Proof. The proof is based on the fact that as $P \to 0$, Alice puts all her power on a single sub-channel for any fixed jammer strategy as specified in Theorem 4.

If $\sigma_{x_1} = P$ and $\sigma_{x_i} = 0$ for $i \neq 1$, then the jammer will put his power in the first sub-channel to minimize the utility (3.25), which becomes,

$$U_1\Big(\sigma_{x_1}, \ldots, \sigma_{x_n}, \sigma_{j_1}, \ldots, \sigma_{j_n}\Big) = \frac{P|\lambda_{m_1}|^2}{1 + min\Big(P_j, \frac{|\lambda_{m_1}|^2 - |\lambda_{e_1}|^2}{|\lambda_{e_1}|^2 |\lambda_{j_1}|^2}\Big)|\lambda_{j_1}|^2} - P|\lambda_{e_1}|^2 + \mathcal{O}(P) \tag{3.33}$$

If $\sigma_{x_2} = P$ and $\sigma_{x_i} = 0$ for $i \neq 2$, then the jammer will put his power in the second sub-channel to minimize the utility (3.25), which becomes,

$$U_1\Big(\sigma_{x_1}, \ldots, \sigma_{x_n}, \sigma_{j_1}, \ldots, \sigma_{j_n}\Big) = \frac{P|\lambda_{m_2}|^2}{1 + min\Big(P_j, \frac{|\lambda_{m_2}|^2 - |\lambda_{e_2}|^2}{|\lambda_{e_2}|^2 |\lambda_{j_2}|^2}\Big)|\lambda_{j_2}|^2} - P|\lambda_{e_2}|^2 + \mathcal{O}(P) \tag{3.34}$$

Likewise, if $\sigma_{x_n} = P$ and $\sigma_{x_i} = 0$ for $i \neq n$, then the jammer will put his power to the n^{th} sub-channel to minimize the utility (3.25), which becomes,

$$U_1\Big(\sigma_{x_1}, \ldots, \sigma_{x_n}, \sigma_{j_1}, \ldots, \sigma_{j_n}\Big) = \frac{P|\lambda_{m_n}|^2}{1 + min\Big(P_j, \frac{|\lambda_{m_n}|^2 - |\lambda_{e_n}|^2}{|\lambda_{e_n}|^2 |\lambda_{j_n}|^2}\Big)|\lambda_{j_n}|^2} - P|\lambda_{e_n}|^2 + \mathcal{O}(P) \tag{3.35}$$

It is clear from (3.25) that Alice chooses the sub-channel that leads to the best utility, where the index k is then given by

$$k = \arg\max_i \left[\frac{P|\lambda_{m_i}|^2}{1 + min\Big(P_j, \frac{|\lambda_{m_i}|^2 - |\lambda_{e_i}|^2}{|\lambda_{e_i}|^2 |\lambda_{j_i}|^2}\Big)|\lambda_{j_i}|^2} - P|\lambda_{e_i}|^2 \right] \tag{3.36}$$

Therefore, a Nash equilibrium exists as follows:

$$(\sigma^*_{x_i}, \sigma^*_{j_i}) = \begin{cases} \Big(P, min\Big(P_j, \frac{|\lambda_{m_i}|^2 - |\lambda_{e_i}|^2}{|\lambda_{e_i}|^2 |\lambda_{j_i}|^2}\Big)\Big), & i = k \\ \big(0, 0\big), & i \neq k \end{cases}$$

□

In addition, Theorem 5 suggests that in the regime of low jammer power, and for any fixed transmitter strategy, the jammer will only inject power in a single sub-channel. Once again, this together with the characterization of the value of the zero-sum game on the left hand side of (3.20) also leads directly to Theorem 7.

Theorem 7. *When the jammer available power is very low, i.e., $P_j \to 0$, there exists a pure strategy Nash equilibrium which is given by:*

$$(\sigma^*_{x_i}, \sigma^*_{j_i}) = \begin{cases} \big(\frac{1}{2}\big[\sqrt{\big(\frac{1}{|\lambda_{e_i}|^2} - \frac{1+P_j|\lambda_{j_i}|^2}{|\lambda_{m_i}|^2}\big)\big(\frac{4}{V} + \frac{1}{|\lambda_{e_i}|^2} - \frac{1+P_j|\lambda_{j_i}|^2}{|\lambda_{m_i}|^2}\big)} - \big(\frac{1+P_j|\lambda_{j_i}|^2}{|\lambda_{m_i}|^2} + \frac{1}{|\lambda_{e_i}|^2}\big)\big], P_j\big), \\ \qquad\qquad i = k \text{ and } V < \frac{|\lambda_{m_i}|^2}{1+P_j|\lambda_{j_i}|^2} - |\lambda_{e_i}|^2 \\ \big(0, P_j\big), \qquad\qquad i = k \text{ and } V \geq \frac{|\lambda_{m_i}|^2}{1+P_j|\lambda_{j_i}|^2} - |\lambda_{e_i}|^2 \\ \big(\frac{1}{2}\big[\sqrt{\big(\frac{1}{|\lambda_{e_i}|^2} - \frac{1}{|\lambda_{m_i}|^2}\big)^2 + \frac{4}{V}\big(\frac{1}{|\lambda_{e_i}|^2} - \frac{1}{|\lambda_{m_i}|^2}\big)} - \big(\frac{1}{|\lambda_{e_i}|^2} + \frac{1}{|\lambda_{m_i}|^2}\big)\big], 0\big), \\ \qquad\qquad i \neq k \text{ and } V < |\lambda_{m_i}|^2 - |\lambda_{e_i}|^2 \\ \big(0, 0\big), \qquad\qquad i \neq k \text{ and } V \geq |\lambda_{m_i}|^2 - |\lambda_{e_i}|^2 \end{cases} \tag{3.37}$$

where V is such that $\sum_{i=1}^{n} \sigma^*_{x_i} = P$ and the index k is expressed as:

$$k = \arg\min_{i} \max_{\sigma_{x_l}, l=1,\ldots,n \in \Psi} U_1(\sigma_{x_1}, \ldots, \sigma_{x_n}; \sigma_{j_1} = 0, \ldots, \sigma_{j_{i-1}} = 0, \sigma_{j_i} = P_j, \sigma_{j_{i+1}} = 0, \ldots, \sigma_{j_n} = 0) \tag{3.38}$$

Proof. See Appendix E. □

Theorems 6 and 7 define the pairs of pure strategies that lead to the Nash equilibrium of the zero-sum game. Theorem 6 defines the strategies explicitly, but Theorem 7 does not because the determination of the sub-channel where the jammer injects all the power is not put forth explicitly.

It is also interesting to note that in the regime of low transmitter power, the transmitter and the jammer inject power in a single sub-channel; in the regime of low jammer power, the transmitter injects power in various sub-channels but the jammer only injects power in a single sub-channel. In contrast, in general non-asymptotic regimes, the transmitter and the jammer will put power in various sub-channels, as shown in the following section.

3.4 Numerical Results

We consider for simplicity a 2×2 parallel Gaussian wiretap channel where the main, the eavesdropper and the jammer channel matrices are, respectively, given by:

$$\mathbf{\Lambda}_m = \begin{bmatrix} 5 & 0 \\ 0 & 3 \end{bmatrix} \quad ; \quad \mathbf{\Lambda}_e = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \quad ; \quad \mathbf{\Lambda}_j = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix} \tag{3.39}$$

The objective is to compare numerical results with the results predicted by the analysis embodied in the previous Theorems.

3.4.1 Regime of low transmitter power $(P \to 0)$

Figure 3.2 plots the best response of the transmitter as a function of the jammer strategy, namely, $\sigma^*_{x1}(\sigma_{j1})$, against the best response of the jammer as a function of the transmitter strategy, namely, $\sigma^*_{j1}(\sigma_{x1})$ for a low transmitter power (P = 0.01). It is clear that the Nash equilibrium, which is given by the crossover of the two best responses in Figure 3.2, corresponds to the strategy where both the transmitter and the jammer inject power in a single sub-channel, i.e., $(\sigma^*_{x1}, \sigma^*_{x2}) = (0.01, 0)$ and $(\sigma^*_{j1}, \sigma^*_{j2}) = (1, 0)$, as put forth in Theorem 6.

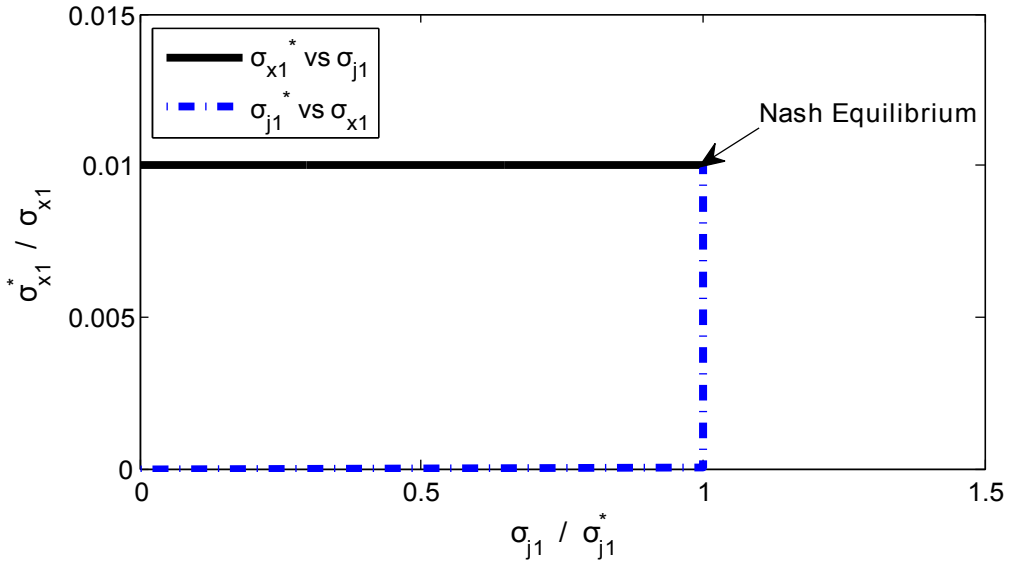

Figure 3.2: $\sigma_{x_1}{}^*$ *vs.* σ_{j_1} and $\sigma_{j_1}{}^*$ *vs.* σ_{x_1} for $P = 0.01$ and $P_j = 1$.

3.4.2 Regime of low jammer power ($P_j \to 0$)

Figure 3.3 also plots the best response of the transmitter as a function of jammer strategy, i.e., $\sigma^*_{x1}(\sigma_{j1})$, against the best response of the jammer as a function of the transmitter strategy, i.e., $\sigma^*_{j1}(\sigma_{x1})$ for a low jammer power ($P_j = 0.006$). The Nash equilibrium, which is given by the pair of pure strategies $(\sigma^*_{x1}, \sigma^*_{x2}) = (4.339, 1.661)$ and $(\sigma^*_{j1}, \sigma^*_{j2}) = (0.006, 0)$, is such that the jammer only injects power in a single sub-channel whereas the transmitter divides the power by the various sub-channels, as put forth in Theorem 7.

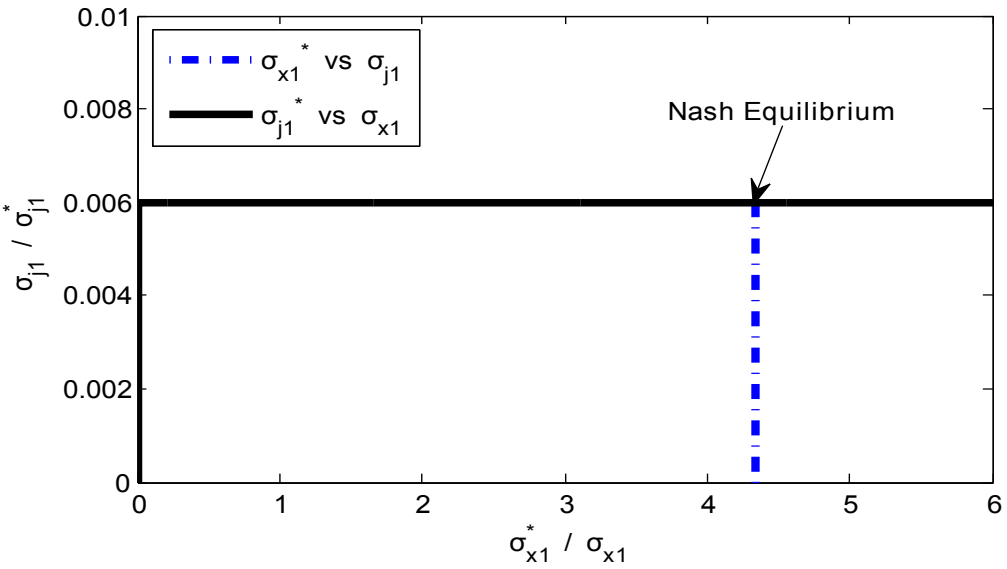

Figure 3.3: ${\sigma_{x_1}}^*$ *vs.* σ_{j_1} and ${\sigma_{j_1}}^*$ *vs.* σ_{x_1} for $P = 6$ and $P_j = 0.006$.

3.4.3 General regimes

In general available power regimes, Figure 3.4 shows that, as expected, the transmitter and the jammer will divide the power between the various sub-channels. In particular, in this case the Nash equilibrium is achieved with the pair of pure strategies: $(\sigma^*_{x1}, \sigma^*_{x2}) = (1.868, 0.132)$ and $(\sigma^*_{j1}, \sigma^*_{j2}) = (1.974, 0.026)$.

3.4.4 Secrecy gains

Finally, it is interesting to demonstrate the gains in secrecy rate (R_s) that a transmitter that adapts to a jammer, i.e., an adaptive transmitter enjoys over a

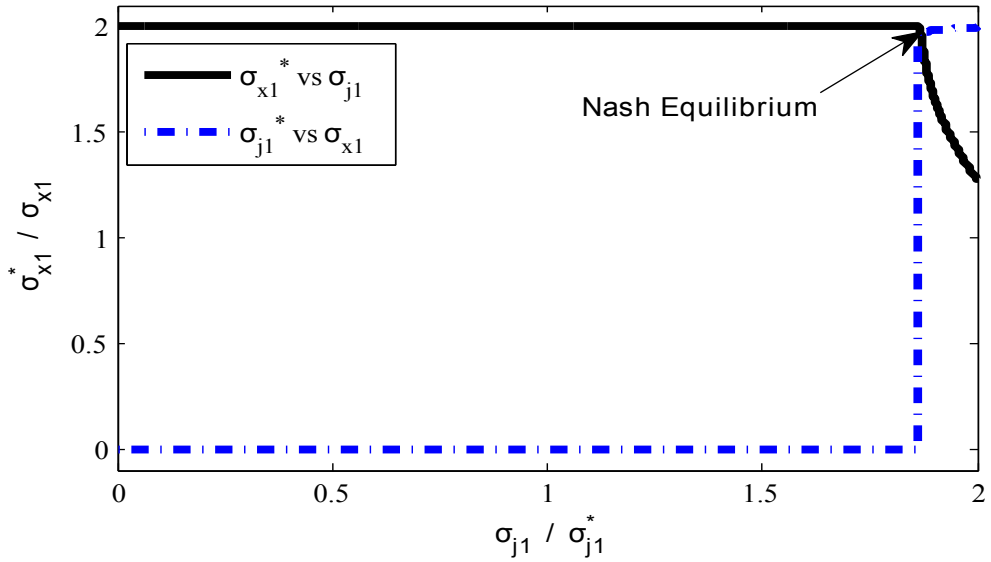

Figure 3.4: $\sigma_{x_1}{}^*$ *vs.* σ_{j_1} and $\sigma_{j_1}{}^*$ *vs.* σ_{x_1} for $P = P_j = 2$.

non-adaptive transmitter that injects equal power over the sub-channels irrespective of the jammer strategy. Figure 3.5 demonstrates that indeed the secrecy rate (R_s) of an adaptive transmitter, which corresponds to the value of the utility function at Nash equilibrium, can be considerably higher than the secrecy rate of the non-adaptive transmitter.

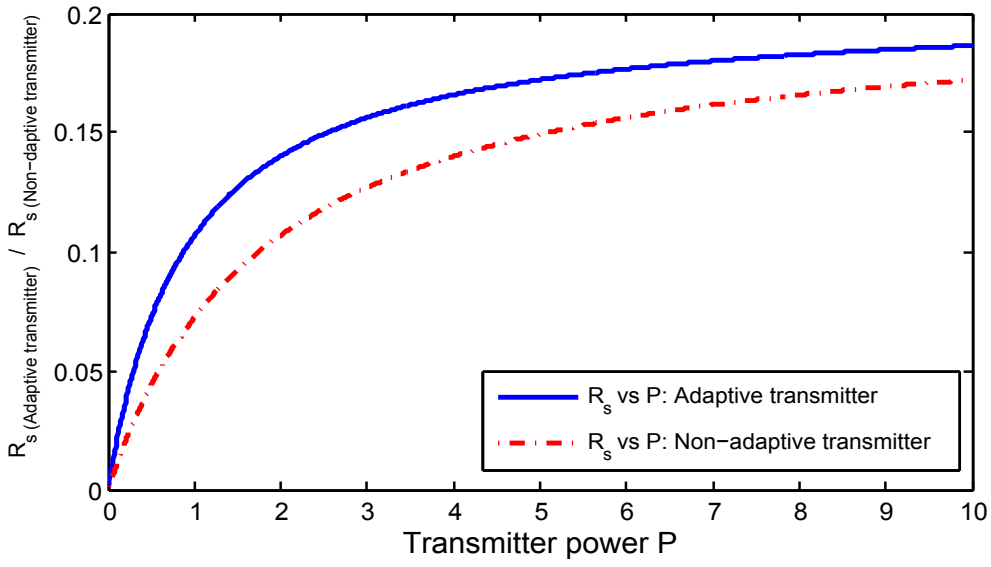

Figure 3.5: Secrecy rate with adaptive transmitter and secrecy rate with non-adaptive transmitter *vs.* transmitter power P for a fixed jammer power $P_j = 5$.

From the data that provided in Table 3.1, Figure 3.6, demonstrates different comparisons between the secrecy rate with adaptive transmitter and the secrecy rate with non-adaptive transmitter *vs.* transmitter power P. From Figure 3.6, it is clear that, the secrecy gain of a adaptive transmitter is much better than a non-adaptive one, when transmitter available power is much higher than the jammer available power. Of course, when the jammer´s available power is limited, then the interference effect of the jammer to the main channel is also limited.

Table 3.1: Secrecy rates under adaptive and non-adaptive transmitter

Jammer available power	R_s adaptive transmitter	R_s non-adaptive transmitter
$P_j = 0.1$	3.27	3.054
$P_j = 1$	1.58	1.46
$P_j = 5$	0.1703	0.1477

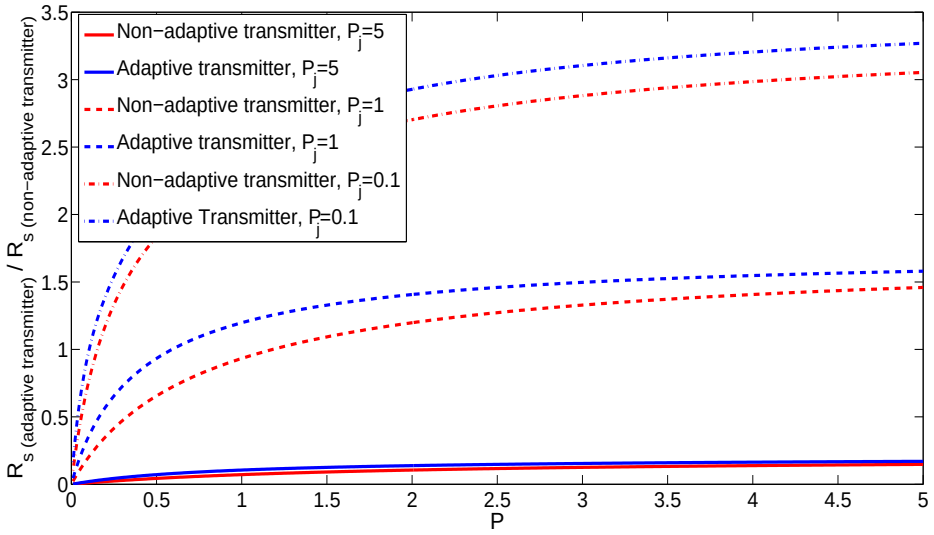

Figure 3.6: Secrecy rate with adaptive transmitter and secrecy rate with non-adaptive transmitter *vs.* transmitter power P for a fixed jammer power: i) $P_j = 5$, ii) $P_j = 1$ and iii) $P_j = 0.1$.

We can also observe that transmitter adaptation has higher importance as the jammer available power increased. For higher jammer available power, the relative gains in secrecy rate which can be achieved by adaptation are much higher than

those which can be achieved by a non-adaptive transmitter. For example, for a transmitter available power of $P = 5$, we have a relative secrecy gain of 7% by adapting the transmitter strategy to the one where the jammer available power is 0.1. In contrast, if the jammer available power is increased to 5, an adaptive transmitter can obtain a relative secrecy gain of 15%, as we can observe in Figure 3.6.

3.5 Conclusion

We have studied a zero-sum power allocation game over a bank of independent parallel Gaussian wiretap channels- applicable to OFDM communications systems- where a legitimate transmitter-receiver pair communicates in the presence of an eavesdropper and an unfriendly jammer. We provide a proof of the existence of a Nash equilibrium of such game; we also characterized the optimal transmission and jamming power allocation strategies for the game, which are specialized for key asymptotic regimes. Extensive results demonstrate that a transmitter that adapts to the jammer strategy can experience a much higher secrecy rate than a non-adaptive transmitter.

This chapter has concentrated on the analysis of achievable secrecy rates of parallel Gaussian wiretap channels in the presence of malicious jammer. The next chapter concentrates instead on the analysis of such secrecy rates for parallel Gaussian wiretap channels in the presence of friendly jammers.

Appendix A: Proof of Theorem 2

Consider the optimization problem in (3.21) given by,

$$\min_{\sigma_{j_i}} U_1\Big(\sigma_{x_1},\ldots,\sigma_{x_n},\sigma_{j_1},\ldots,\sigma_{j_n}\Big)=\min_{\sigma_{j_i}}\sum_{i=1}^{n}\left[\log\left(1+\frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2}{1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2}\right)-\log\left(1+\sigma_{x_i}\left|\lambda_{e_i}\right|^2\right)\right] \tag{3.40}$$

subject to:

$$\sum_{i=1}^{n}\sigma_{j_i}\leq P_j,\ \sigma_{j_i}\geq 0\ \text{ and }\ \sigma_{j_i}\leq\frac{\left|\lambda_{m_i}\right|^2-\left|\lambda_{e_i}\right|^2}{\left|\lambda_{e_i}\right|^2\left|\lambda_{j_i}\right|^2},\ i=1,2,...,n. \tag{3.41}$$

The Lagrangian of the optimization problem (3.40) and (3.41) can be expressed as:

$$\mathcal{L}\left(\sigma_{j_i},\nu,u_i,\eta_i\right)=U_1\Big(\sigma_{x_1},\ldots,\sigma_{x_n},\sigma_{j_1},\ldots,\sigma_{j_n}\Big)+\nu\Big(\sum_{i=1}^{n}\sigma_{j_i}-P_j\Big)-\sum_{i=1}^{n}\Big(u_i\sigma_{j_i}\Big)+$$
$$\sum_{i=1}^{n}\eta_i\Big(\sigma_{j_i}-\frac{\left|\lambda_{m_i}\right|^2-\left|\lambda_{e_i}\right|^2}{\left|\lambda_{e_i}\right|^2\left|\lambda_{j_i}\right|^2}\Big) \tag{3.42}$$

Where $\nu\geq 0$, $u_i\geq 0$ and $\eta_i\geq 0$ are the Lagrange multipliers associated with the problem constraints.

The KKT conditions state that:

$$\nabla_{\sigma_{j_i}}\mathcal{L}(\sigma_{j_i},\nu,u_i,\eta_i)=0,\qquad i=1,2,\ldots,n. \tag{3.43}$$

with $\nu(\sum_{i=1}^{n}\sigma_{j_i}-P_j)=0\ \forall\ \nu\geq 0,\quad u_i\sigma_{j_i}=0\ \forall\ u_i\geq 0,\forall\ i$ and
$\eta_i(\sigma_{j_i}-\frac{\left|\lambda_{m_i}\right|^2-\left|\lambda_{e_i}\right|^2}{\left|\lambda_{e_i}\right|^2\left|\lambda_{j_i}\right|^2})=0\ \forall\ \eta_i\geq 0,\forall\ i$

From (3.43) we have,

$$\nu-u_i+\eta_i=\frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{\Big(1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2\Big)\Big(1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2+\sigma_{x_i}\left|\lambda_{m_i}\right|^2\Big)} \tag{3.44}$$

Let us assume that $u_i = 0$ which implies that $\sigma_{j_i} \geq 0$

Then from (3.44) we have,

$$\nu + \eta_i = \frac{\sigma_{x_i} |\lambda_{m_i}|^2 |\lambda_{j_i}|^2}{\left(1 + \sigma_{j_i} |\lambda_{j_i}|^2\right)\left(1 + \sigma_{j_i} |\lambda_{j_i}|^2 + \sigma_{x_i} |\lambda_{m_i}|^2\right)} \tag{3.45}$$

When $\eta_i > 0$, then $\sigma_{j_i} - \frac{|\lambda_{m_i}|^2 - |\lambda_{e_i}|^2}{|\lambda_{e_i}|^2 |\lambda_{j_i}|^2} = 0$. Therefore, from (3.45) we have that,

$$\nu - \frac{\sigma_{x_i} |\lambda_{m_i}|^2 |\lambda_{j_i}|^2}{\left(1 + \sigma_{j_i} |\lambda_{j_i}|^2\right)\left(1 + \sigma_{j_i} |\lambda_{j_i}|^2 + \sigma_{x_i} |\lambda_{m_i}|^2\right)} = -\eta_i < 0 \tag{3.46}$$

or,

$$\nu < \frac{\sigma_{x_i} |\lambda_{m_i}|^2 |\lambda_{j_i}|^2}{\left(1 + \sigma_{j_i} |\lambda_{j_i}|^2\right)\left(1 + \sigma_{j_i} |\lambda_{j_i}|^2 + \sigma_{x_i} |\lambda_{m_i}|^2\right)} \tag{3.47}$$

and upon substituting $\sigma_{j_i} = \frac{|\lambda_{m_i}|^2 - |\lambda_{e_i}|^2}{|\lambda_{e_i}|^2 |\lambda_{j_i}|^2}$ in (3.47) we have:

$$\nu < \frac{\sigma_{x_i} |\lambda_{m_i}|^2 |\lambda_{j_i}|^2}{(1 + \frac{|\lambda_{m_i}|^2 - |\lambda_{e_i}|^2}{|\lambda_{e_i}|^2 |\lambda_{j_i}|^2} |\lambda_{j_i}|^2)(1 + \frac{|\lambda_{m_i}|^2 - |\lambda_{e_i}|^2}{|\lambda_{e_i}|^2 |\lambda_{j_i}|^2} |\lambda_{j_i}|^2 + \sigma_{x_i} |\lambda_{m_i}|^2)}$$

$$i.e., \quad \nu < \frac{\sigma_{x_i} |\lambda_{j_i}|^2 |\lambda_{e_i}|^4}{|\lambda_{m_i}|^2 (1 + \sigma_{x_i} |\lambda_{e_i}|^2)} \tag{3.48}$$

Thus, $\sigma_{j_i} = \frac{|\lambda_{m_i}|^2 - |\lambda_{e_i}|^2}{|\lambda_{e_i}|^2 |\lambda_{j_i}|^2} \Rightarrow \nu < \frac{\sigma_{x_i} |\lambda_{j_i}|^2 |\lambda_{e_i}|^4}{|\lambda_{m_i}|^2 \left(1 + \sigma_{x_i} |\lambda_{e_i}|^2\right)}$

Conversely, when $\nu < \frac{\sigma_{x_i} |\lambda_{j_i}|^2 |\lambda_{e_i}|^4}{|\lambda_{m_i}|^2 \left(1 + \sigma_{x_i} |\lambda_{e_i}|^2\right)}$, then from (3.45) we have,

$$\nu = \frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{\left(1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2\right)\left(1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2+\sigma_{x_i}\left|\lambda_{m_i}\right|^2\right)} - \eta_i < \frac{\sigma_{x_i}\left|\lambda_{j_i}\right|^2\left|\lambda_{e_i}\right|^4}{\left|\lambda_{m_i}\right|^2\left(1+\sigma_{x_i}\left|\lambda_{e_i}\right|^2\right)}$$

$$\Rightarrow\ \eta_i > \frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{\left(1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2\right)\left(1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2+\sigma_{x_i}\left|\lambda_{m_i}\right|^2\right)} - \frac{\sigma_{x_i}\left|\lambda_{j_i}\right|^2\left|\lambda_{e_i}\right|^4}{\left|\lambda_{m_i}\right|^2\left(1+\sigma_{x_i}\left|\lambda_{e_i}\right|^2\right)} \tag{3.49}$$

Now for each sub-channel we have:

$$\frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2}{1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2} \geq \sigma_{x_i}\left|\lambda_{e_i}\right|^2$$

$$\Rightarrow\ \frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2} \geq \sigma_{x_i}\left|\lambda_{e_i}\right|^2\left|\lambda_{j_i}\right|^2 \tag{3.50}$$

Again

$$\frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2}{1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2} \geq \sigma_{x_i}\left|\lambda_{e_i}\right|^2$$

$$\Rightarrow\ \frac{\left|\lambda_{m_i}\right|^2}{\left|\lambda_{e_i}\right|^2} \geq 1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2$$

$$\Rightarrow\ \frac{\left|\lambda_{m_i}\right|^2}{\left|\lambda_{e_i}\right|^2} + \sigma_{x_i}\left|\lambda_{m_i}\right|^2 \geq 1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2+\sigma_{x_i}\left|\lambda_{m_i}\right|^2$$

$$\Rightarrow\ \frac{\left|\lambda_{m_i}\right|^2\left(1+\sigma_{x_i}\left|\lambda_{e_i}\right|^2\right)}{\left|\lambda_{e_i}\right|^2} \geq 1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2+\sigma_{x_i}\left|\lambda_{m_i}\right|^2$$

$$\Rightarrow\ \frac{\left|\lambda_{e_i}\right|^2}{\left|\lambda_{m_i}\right|^2\left(1+\sigma_{x_i}\left|\lambda_{e_i}\right|^2\right)} \leq \frac{1}{1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2+\sigma_{x_i}\left|\lambda_{m_i}\right|^2} \tag{3.51}$$

From (3.50) and (3.51) it is clear that $\frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{\left(1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2\right)\left(1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2+\sigma_{x_i}\left|\lambda_{m_i}\right|^2\right)} - \frac{\sigma_{x_i}\left|\lambda_{j_i}\right|^2\left|\lambda_{e_i}\right|^4}{\left|\lambda_{m_i}\right|^2\left(1+\sigma_{x_i}\left|\lambda_{e_i}\right|^2\right)} \geq 0$, i.e., from (3.49) we have that $\eta_i > 0$, which implies that $\sigma_{j_i} = \frac{\left|\lambda_{m_i}\right|^2-\left|\lambda_{e_i}\right|^2}{\left|\lambda_{e_i}\right|^2\left|\lambda_{j_i}\right|^2}$.

Thus, $\nu < \frac{\sigma_{x_i}\left|\lambda_{j_i}\right|^2\left|\lambda_{e_i}\right|^4}{\left|\lambda_{m_i}\right|^2\left(1+\sigma_{x_i}\left|\lambda_{e_i}\right|^2\right)} \Rightarrow \sigma_{j_i} = \frac{\left|\lambda_{m_i}\right|^2-\left|\lambda_{e_i}\right|^2}{\left|\lambda_{e_i}\right|^2\left|\lambda_{j_i}\right|^2}$.

That is, $\sigma_{j_i} = \frac{\left|\lambda_{m_i}\right|^2-\left|\lambda_{e_i}\right|^2}{\left|\lambda_{e_i}\right|^2\left|\lambda_{j_i}\right|^2} \Leftrightarrow \nu < \frac{\sigma_{x_i}\left|\lambda_{j_i}\right|^2\left|\lambda_{e_i}\right|^4}{\left|\lambda_{m_i}\right|^2\left(1+\sigma_{x_i}\left|\lambda_{e_i}\right|^2\right)}$

On the other hand, $\eta_i = 0$ implies and is implied by $\sigma_{j_i} < \frac{\left|\lambda_{m_i}\right|^2-\left|\lambda_{e_i}\right|^2}{\left|\lambda_{e_i}\right|^2\left|\lambda_{j_i}\right|^2}$

To see this, note that from (3.44) we have,

$$\nu - u_i = \frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{(1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2)(1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2+\sigma_{x_i}\left|\lambda_{m_i}\right|^2)} \tag{3.52}$$

where the right hand side is monotonically decreasing in σ_{j_i}.

When $\sigma_{j_i} = 0$, then $u_i \geq 0$ and from (3.52) we have,

$$\nu - \frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{1+\sigma_{x_i}\left|\lambda_{m_i}\right|^2} = u_i \geq 0 \tag{3.53}$$

$$\text{i.e., } \nu \geq \frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{1+\sigma_{x_i}\left|\lambda_{m_i}\right|^2}$$

Thus, $\sigma_{j_i} = 0 \Rightarrow \nu \geq \frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{1+\sigma_{x_i}\left|\lambda_{m_i}\right|^2}$

Conversely, when $\nu \geq \frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{1+\sigma_{x_i}\left|\lambda_{m_i}\right|^2}$, then from (3.52) we have,

$$\nu = u_i + \frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{(1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2)(1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2+\sigma_{x_i}\left|\lambda_{m_i}\right|^2)} \geq \frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{1+\sigma_{x_i}\left|\lambda_{m_i}\right|^2}$$

$$\Rightarrow \; u_i \geq \frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{1+\sigma_{x_i}\left|\lambda_{m_i}\right|^2} - \frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{(1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2)(1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2+\sigma_{x_i}\left|\lambda_{m_i}\right|^2)}$$

$$\Rightarrow \; u_i \geq 0, \quad \text{which implies that, } \sigma_{x_i} = 0 \tag{3.54}$$

Thus, $\nu \geq \frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{1+\sigma_{x_i}\left|\lambda_{m_i}\right|^2} \Rightarrow \sigma_{x_i} = 0$.

That is, $\sigma_{j_i} = 0 \Leftrightarrow \nu \geq \frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{1+\sigma_{x_i}\left|\lambda_{m_i}\right|^2}$

When $\sigma_{j_i} > 0$, then $u_i = 0$ and from (3.52) we can write,

$$\nu = \frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{\left(1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2\right)\left(1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2+\sigma_{x_i}\left|\lambda_{m_i}\right|^2\right)} < \frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{1+\sigma_{x_i}\left|\lambda_{m_i}\right|^2} \tag{3.55}$$

Thus, $\sigma_{j_i} > 0 \Rightarrow \nu < \frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{1+\sigma_{x_i}\left|\lambda_{m_i}\right|^2}$

Conversely, when $\nu \geq \frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{1+\sigma_{x_i}\left|\lambda_{m_i}\right|^2}$, from (3.52) we have,

$$\nu = u_i + \frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{\left(1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2\right)(1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2+\sigma_{x_i}\left|\lambda_{m_i}\right|^2\right)} < \frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{1+\sigma_{x_i}\left|\lambda_{m_i}\right|^2} \tag{3.56}$$

It is clear that, we can only satisfy (3.56) with $\sigma_{j_i} > 0$. Indeed, we can not satisfy (3.56) with $\sigma_{j_i} = 0$, because, this implies $u_i > 0$.

Thus, $\nu < \frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{1+\sigma_{x_i}\left|\lambda_{m_i}\right|^2} \Rightarrow \sigma_{j_i} > 0$

That is, $\sigma_{j_i} > 0 \Leftrightarrow \nu < \frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{1+\sigma_{x_i}\left|\lambda_{m_i}\right|^2}$

From (3.55) we have,

$$\nu = \frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{\left(1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2\right)\left(1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2+\sigma_{x_i}\left|\lambda_{m_i}\right|^2\right)}$$

$$= \frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{1+\sigma_{x_i}\left|\lambda_{m_i}\right|^2+2\sigma_{j_i}\left|\lambda_{j_i}\right|^2+\sigma_{x_i}\sigma_{j_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2+{\sigma_{j_i}}^2\left|\lambda_{j_i}\right|^4}$$

$$\Rightarrow {\sigma_{j_i}}^2 \left|\lambda_{j_i}\right|^4 + \sigma_{j_i}\Big(2\left|\lambda_{j_i}\right|^2 + \sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2\Big)$$

$$+ \left(1 + \sigma_{x_i}\left|\lambda_{m_i}\right|^2 - \frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{\nu}\right) = 0$$

$$\Rightarrow \sigma_{j_i} = \frac{-(2+\sigma_{x_i}\left|\lambda_{m_i}\right|^2) \pm \sqrt{\sigma_{x_i}^2\left|\lambda_{m_i}\right|^4 + \frac{4\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{\nu}}}{2\left|\lambda_{j_i}\right|^2} \tag{3.57}$$

Since $\sigma_{j_i} > 0$, it follows that

$$\sigma_{j_i} = \frac{\sqrt{\sigma_{x_i}^2\left|\lambda_{m_i}\right|^4 + \frac{4\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{\nu}} - \left(2+\sigma_{x_i}\left|\lambda_{m_i}\right|^2\right)}{2\left|\lambda_{j_i}\right|^2} \tag{3.58}$$

For fixed Alice strategy $\sigma_{x_i}, i = 1, 2, ..., n$, the optimal jammer strategy $\sigma_{j_i}^*$ that minimize the utility (3.40), subject to the constraints in (3.41) is given by:

$$\sigma_{j_i}^* = \begin{cases} \frac{\sqrt{\sigma_{x_i}^2\left|\lambda_{m_i}\right|^4 + \frac{4\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{\nu}} - \left(2+\sigma_{x_i}\left|\lambda_{m_i}\right|^2\right)}{2\left|\lambda_{j_i}\right|^2}, & \frac{\sigma_{x_i}\left|\lambda_{e_i}\right|^4\left|\lambda_{j_i}\right|^2}{\left|\lambda_{m_i}\right|^2\left(1+\sigma_{x_i}\left|\lambda_{e_i}\right|^2\right)} \le \nu < \frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{1+\sigma_{x_i}\left|\lambda_{m_i}\right|^2} \\ \frac{\left|\lambda_{m_i}\right|^2 - \left|\lambda_{e_i}\right|^2}{\left|\lambda_{e_i}\right|^2\left|\lambda_{j_i}\right|^2}, & \nu < \frac{\sigma_{x_i}\left|\lambda_{e_i}\right|^4\left|\lambda_{j_i}\right|^2}{\left|\lambda_{m_i}\right|^2\left(1+\sigma_{x_i}\left|\lambda_{e_i}\right|^2\right)} \\ 0, & \nu \ge \frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{1+\sigma_{x_i}\left|\lambda_{m_i}\right|^2} \end{cases} \tag{3.59}$$

Appendix B: Proof of Theorem 3

Consider the optimization problem in (3.23) given by,

$$\max_{\sigma_{x_i}} U_1\Big(\sigma_{x_1}, \ldots, \sigma_{x_n}, \sigma_{j_1}, \ldots, \sigma_{j_n}\Big) = -\min_{\sigma_{x_i}} \sum_{i=1}^{n} \Bigg[\log\left(1 + \frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2}{1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2}\right) - \log\left(1+\sigma_{x_i}\left|\lambda_{e_i}\right|^2\right)\Bigg] \tag{3.60}$$

subject to:

$$\sum_{i=1}^{n} \sigma_{x_i} \leq P, \text{ and } \sigma_{x_i} \geq 0, \quad i = 1, 2, \ldots, n. \tag{3.61}$$

The Lagrangian of the optimization problem (3.60), subject to (3.61) is

$$\mathcal{L}\left(\sigma_{x_i}, \eta, u_i\right) = -U_1\Big(\sigma_{x_1}, \ldots, \sigma_{x_n}, \sigma_{j_1}, \ldots, \sigma_{j_n}\Big) + \eta\Big(\sum_{i=1}^{n} \sigma_{x_i} - P\Big) - \sum_{i=1}^{n} \Big(u_i \sigma_{x_i}\Big) \tag{3.62}$$

Where $\eta \geq 0$, and $u_i \geq 0,\ i = 1, 2, \ldots, n$ are the Lagrange multipliers associated with the problem constraints.

The KKT conditions state that :

$$\nabla_{\sigma_{x_i}} \mathcal{L}\left(\sigma_{x_i}, \eta, u_i\right) = 0, \quad i = 1, 2, \ldots, n \tag{3.63}$$

with $\eta(\sum_{i=1}^{n} \sigma_{x_i} - P) = 0 \ \forall\ \eta \geq 0, \quad u_i \sigma_{x_i} = 0 \ \forall\ u_i \geq 0, \quad i = 1, 2, \ldots, n$

Note that from (3.63) we have,

$$\eta - u_i = \frac{\left|\lambda_{m_i}\right|^2 \Big(1 + \sigma_{x_i} \left|\lambda_{e_i}\right|^2\Big) - \left|\lambda_{e_i}\right|^2 \Big(1 + \sigma_{x_i} \left|\lambda_{m_i}\right|^2 + \sigma_{j_i} \left|\lambda_{j_i}\right|^2\Big)}{\Big(1 + \sigma_{x_i} \left|\lambda_{e_i}\right|^2\Big)\Big(1 + \sigma_{x_i} \left|\lambda_{m_i}\right|^2 + \sigma_{j_i} \left|\lambda_{j_i}\right|^2\Big)} \tag{3.64}$$

where the right hand side is monotonically decreasing in σ_{x_i}.

Let us assume that $\sigma_{x_i} = 0$ which implies that $u_i \geq 0$

Then from (3.64) we have,

$$\eta - u_i = \frac{\left|\lambda_{m_i}\right|^2 - \left|\lambda_{e_i}\right|^2 \Big(1 + \sigma_{j_i} \left|\lambda_{j_i}\right|^2\Big)}{1 + \sigma_{j_i} \left|\lambda_{j_i}\right|^2} \tag{3.65}$$

or,

$$\eta - \frac{\left|\lambda_{m_i}\right|^2 - \left|\lambda_{e_i}\right|^2 \Big(1 + \sigma_{j_i} \left|\lambda_{j_i}\right|^2\Big)}{1 + \sigma_{j_i} \left|\lambda_{j_i}\right|^2} = u_i \geq 0 \tag{3.66}$$

or,

$$\eta \geq \frac{|\lambda_{m_i}|^2 - |\lambda_{e_i}|^2 \left(1 + \sigma_{j_i} |\lambda_{j_i}|^2\right)}{1 + \sigma_{j_i} |\lambda_{j_i}|^2} \tag{3.67}$$

i.e., $\sigma_{x_i} = 0 \Rightarrow \eta \geq \frac{|\lambda_{m_i}|^2 - |\lambda_{e_i}|^2 \left(1 + \sigma_{j_i} |\lambda_{j_i}|^2\right)}{1 + \sigma_{j_i} |\lambda_{j_i}|^2}$

Conversely, when $\eta \geq \frac{|\lambda_{m_i}|^2 - |\lambda_{e_i}|^2 \left(1 + \sigma_{j_i} |\lambda_{j_i}|^2\right)}{1 + \sigma_{j_i} |\lambda_{j_i}|^2}$, then from (3.64) we have,

$$\eta = u_i + \frac{|\lambda_{m_i}|^2 \left(1 + \sigma_{x_i} |\lambda_{e_i}|^2\right) - |\lambda_{e_i}|^2 \left(1 + \sigma_{x_i} |\lambda_{m_i}|^2 + \sigma_{j_i} |\lambda_{j_i}|^2\right)}{\left(1 + \sigma_{x_i} |\lambda_{e_i}|^2\right)\left(1 + \sigma_{x_i} |\lambda_{m_i}|^2 + \sigma_{j_i} |\lambda_{j_i}|^2\right)} \geq \frac{|\lambda_{m_i}|^2 - |\lambda_{e_i}|^2 \left(1 + \sigma_{j_i} |\lambda_{j_i}|^2\right)}{1 + \sigma_{j_i} |\lambda_{j_i}|^2}$$

$$\Rightarrow \; u_i \geq \frac{|\lambda_{m_i}|^2 - |\lambda_{e_i}|^2 \left(1 + \sigma_{j_i} |\lambda_{j_i}|^2\right)}{1 + \sigma_{j_i} |\lambda_{j_i}|^2} - \frac{|\lambda_{m_i}|^2 \left(1 + \sigma_{x_i} |\lambda_{e_i}|^2\right) - |\lambda_{e_i}|^2 \left(1 + \sigma_{x_i} |\lambda_{m_i}|^2 + \sigma_{j_i} |\lambda_{j_i}|^2\right)}{\left(1 + \sigma_{x_i} |\lambda_{e_i}|^2\right)\left(1 + \sigma_{x_i} |\lambda_{m_i}|^2 + \sigma_{j_i} |\lambda_{j_i}|^2\right)} \tag{3.68}$$

We have,

$$\frac{\sigma_{x_i} |\lambda_{m_i}|^2}{1 + \sigma_{j_i} |\lambda_{j_i}|^2} \geq \sigma_{x_i} |\lambda_{e_i}|^2$$

$$\Rightarrow \; \frac{1 + \sigma_{j_i} |\lambda_{j_i}|^2 + \sigma_{x_i} |\lambda_{m_i}|^2}{1 + \sigma_{j_i} |\lambda_{j_i}|^2} \geq 1 + \sigma_{x_i} |\lambda_{e_i}|^2$$

$$\Rightarrow \; 1 + \sigma_{j_i} |\lambda_{j_i}|^2 + \sigma_{x_i} |\lambda_{m_i}|^2 \geq \left(1 + \sigma_{j_i} |\lambda_{j_i}|^2\right)\left(1 + \sigma_{x_i} |\lambda_{e_i}|^2\right) \tag{3.69}$$

Now,

$$\frac{|\lambda_{m_i}|^2 - |\lambda_{e_i}|^2 \left(1 + \sigma_{j_i} |\lambda_{j_i}|^2\right)}{1 + \sigma_{j_i} |\lambda_{j_i}|^2} - \frac{|\lambda_{m_i}|^2 \left(1 + \sigma_{x_i} |\lambda_{e_i}|^2\right) - |\lambda_{e_i}|^2 \left(1 + \sigma_{x_i} |\lambda_{m_i}|^2 + \sigma_{j_i} |\lambda_{j_i}|^2\right)}{\left(1 + \sigma_{x_i} |\lambda_{e_i}|^2\right)\left(1 + \sigma_{x_i} |\lambda_{m_i}|^2 + \sigma_{j_i} |\lambda_{j_i}|^2\right)}$$

$$= \frac{|\lambda_{m_i}|^2 + \sigma_{x_i} |\lambda_{m_i}|^2 |\lambda_{e_i}|^2 + \sigma_{j_i} |\lambda_{j_i}|^2 |\lambda_{e_i}|^2 + |\lambda_{e_i}|^2}{\left(1 + \sigma_{x_i} |\lambda_{e_i}|^2\right)\left(1 + \sigma_{j_i} |\lambda_{j_i}|^2\right)} - \frac{|\lambda_{m_i}|^2 + \sigma_{x_i} |\lambda_{m_i}|^2 |\lambda_{e_i}|^2 + \sigma_{j_i} |\lambda_{j_i}|^2 |\lambda_{e_i}|^2 + |\lambda_{e_i}|^2}{1 + \sigma_{j_i} |\lambda_{j_i}|^2 + \sigma_{x_i} |\lambda_{m_i}|^2}$$

$$\geq 0, \quad \text{since, } 1 + \sigma_{j_i} |\lambda_{j_i}|^2 + \sigma_{x_i} |\lambda_{m_i}|^2 \geq \left(1 + \sigma_{j_i} |\lambda_{j_i}|^2\right)\left(1 + \sigma_{x_i} |\lambda_{e_i}|^2\right) \tag{3.70}$$

From (3.68) we have $u_i \geq 0$, which implies that $\sigma_{x_i} = 0$

Thus, $\eta \geq \frac{\left|\lambda_{m_i}\right|^2 - \left|\lambda_{e_i}\right|^2 \left(1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2\right)}{1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2} \Rightarrow \sigma_{x_i} = 0$

That is, $\sigma_{x_i} = 0 \Leftrightarrow \eta \geq \frac{\left|\lambda_{m_i}\right|^2 - \left|\lambda_{e_i}\right|^2 \left(1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2\right)}{1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2}$

On the other hand, if $\sigma_{x_i} > 0$, which implies $u_i = 0$ then

$$\eta = \frac{\left|\lambda_{m_i}\right|^2 \left(1 + \sigma_{x_i}\left|\lambda_{e_i}\right|^2\right) - \left|\lambda_{e_i}\right|^2 \left(1 + \sigma_{x_i}\left|\lambda_{m_i}\right|^2 + \sigma_{j_i}\left|\lambda_{j_i}\right|^2\right)}{\left(1 + \sigma_{x_i}\left|\lambda_{e_i}\right|^2\right)\left(1 + \sigma_{x_i}\left|\lambda_{m_i}\right|^2 + \sigma_{j_i}\left|\lambda_{j_i}\right|^2\right)}$$

$$< \frac{\left|\lambda_{m_i}\right|^2 - \left|\lambda_{e_i}\right|^2 \left(1 + \sigma_{j_i}\left|\lambda_{j_i}\right|^2\right)}{1 + \sigma_{j_i}\left|\lambda_{j_i}\right|^2} \tag{3.71}$$

Thus $\sigma_{x_i} > 0 \Rightarrow \eta < \frac{\left|\lambda_{m_i}\right|^2 - \left|\lambda_{e_i}\right|^2 \left(1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2\right)}{1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2}$

Conversely, when $\eta < \frac{\left|\lambda_{m_i}\right|^2 - \left|\lambda_{e_i}\right|^2 \left(1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2\right)}{1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2}$, then from (3.64) we have,

$$\eta = u_i + \frac{\left|\lambda_{m_i}\right|^2 \left(1 + \sigma_{x_i}\left|\lambda_{e_i}\right|^2\right) - \left|\lambda_{e_i}\right|^2 \left(1 + \sigma_{x_i}\left|\lambda_{m_i}\right|^2 + \sigma_{j_i}\left|\lambda_{j_i}\right|^2\right)}{\left(1 + \sigma_{x_i}\left|\lambda_{e_i}\right|^2\right)\left(1 + \sigma_{x_i}\left|\lambda_{m_i}\right|^2 + \sigma_{j_i}\left|\lambda_{j_i}\right|^2\right)}$$

$$< \frac{\left|\lambda_{m_i}\right|^2 - \left|\lambda_{e_i}\right|^2 \left(1 + \sigma_{j_i}\left|\lambda_{j_i}\right|^2\right)}{1 + \sigma_{j_i}\left|\lambda_{j_i}\right|^2} \tag{3.72}$$

It is clear that, we can only satisfy (3.72) with $\sigma_{x_i} > 0$. Indeed, we can not satisfy (3.72) with $\sigma_{x_i} = 0$, because, this implies $u_i > 0$.

Thus, $\eta < \frac{\left|\lambda_{m_i}\right|^2 - \left|\lambda_{e_i}\right|^2 \left(1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2\right)}{1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2} \Rightarrow \sigma_{x_i} > 0$

That is, $\sigma_{x_i} > 0 \Leftrightarrow \eta < \frac{\left|\lambda_{m_i}\right|^2 - \left|\lambda_{e_i}\right|^2 \left(1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2\right)}{1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2}$

From (3.64) we have,

$$\eta = \frac{|\lambda_{m_i}|^2 \left(1+\sigma_{x_i}|\lambda_{e_i}|^2\right) - |\lambda_{e_i}|^2 \left(1+\sigma_{x_i}|\lambda_{m_i}|^2+\sigma_{j_i}|\lambda_{j_i}|^2\right)}{\left(1+\sigma_{x_i}|\lambda_{e_i}|^2\right)\left(1+\sigma_{x_i}|\lambda_{m_i}|^2+\sigma_{j_i}|\lambda_{j_i}|^2\right)}$$

$$= \frac{|\lambda_{m_i}|^2 - \left(1+\sigma_{j_i}|\lambda_{j_i}|^2\right)|\lambda_{e_i}|^2}{\left(1+\sigma_{j_i}|\lambda_{j_i}|^2\right)+{\sigma_{x_i}}^2|\lambda_{m_i}|^2|\lambda_{e_i}|^2+\sigma_{x_i}[(1+\sigma_{j_i}|\lambda_{j_i}|^2)|\lambda_{e_i}|^2+|\lambda_{m_i}|^2]}$$

$$\Rightarrow {\sigma_{x_i}}^2|\lambda_{m_i}|^2|\lambda_{e_i}|^2+\sigma_{x_i}[\left(1+\sigma_{j_i}|\lambda_{j_i}|^2\right)|\lambda_{e_i}|^2+|\lambda_{m_i}|^2]+\left(1+\sigma_{j_i}|\lambda_{j_i}|^2\right)-$$

$$\frac{|\lambda_{m_i}|^2}{\eta}+\frac{\left(1+\sigma_{j_i}|\lambda_{j_i}|^2\right)|\lambda_{e_i}|^2}{\eta}=0$$

$$\Rightarrow \sigma_{x_i} = \frac{-\left(1+\sigma_{j_i}|\lambda_{j_i}|^2\right)|\lambda_{e_i}|^2+|\lambda_{m_i}|^2}{2|\lambda_{m_i}|^2|\lambda_{e_i}|^2}\pm$$

$$\frac{\sqrt{\left[\left(1+\sigma_{j_i}|\lambda_{j_i}|^2\right)|\lambda_{e_i}|^2+|\lambda_{m_i}|^2\right]^2-4|\lambda_{m_i}|^2|\lambda_{e_i}|^2\left(1+\sigma_{j_i}|\lambda_{j_i}|^2-\frac{|\lambda_{m_i}|^2}{\eta}+\frac{\left(1+\sigma_{j_i}|\lambda_{j_i}|^2\right)|\lambda_{e_i}|^2}{\eta}\right)}}{2|\lambda_{m_i}|^2|\lambda_{e_i}|^2} \tag{3.73}$$

Since $\sigma_{x_i} > 0$, it follows that

$$\text{i.e., } \sigma_{x_i} = \frac{1}{2}\left[\sqrt{\frac{\left(1+\sigma_{j_i}|\lambda_{j_i}|^2\right)^2}{|\lambda_{m_i}|^4}-\frac{2\left(1+\sigma_{j_i}|\lambda_{j_i}|^2\right)}{|\lambda_{m_i}|^2|\lambda_{e_i}|^2}+\frac{1}{|\lambda_{e_i}|^4}+\frac{4}{\eta}\left(\frac{1}{|\lambda_{e_i}|^2}-\frac{1+\sigma_{j_i}|\lambda_{j_i}|^2}{|\lambda_{m_i}|^2}\right)}\right]$$

$$-\frac{1}{2}\left(\frac{1+\sigma_{j_i}|\lambda_{j_i}|^2}{|\lambda_{m_i}|^2}+\frac{1}{|\lambda_{e_i}|^2}\right) \tag{3.74}$$

For fix jammer strategy $\sigma_{j_i}, i = 1, 2, ...n.$, the optimal Alice strategy $\sigma^*_{x_i}$ that

maximize (3.60) is given by:

$$\sigma_{x_i}^{*}=\begin{cases}\frac{1}{2}\left[\sqrt{\left(\frac{1}{\left|\lambda_{e_i}\right|^2}-\frac{1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2}{\left|\lambda_{m_i}\right|^2}\right)\left(\frac{4}{\eta}+\frac{1}{\left|\lambda_{e_i}\right|^2}-\frac{1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2}{\left|\lambda_{m_i}\right|^2}\right)}-\left(\frac{1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2}{\left|\lambda_{m_i}\right|^2}+\frac{1}{\left|\lambda_{e_i}\right|^2}\right)\right], & \\ & \eta<\frac{\left|\lambda_{m_i}\right|^2}{1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2}-\left|\lambda_{e_i}\right|^2 \\ 0, & \eta\geq\frac{\left|\lambda_{m_i}\right|^2}{1+\sigma_{j_i}\left|\lambda_{j_i}\right|^2}-\left|\lambda_{e_i}\right|^2\end{cases} \tag{3.75}$$

Appendix C: Proof of Theorem 4

When $P\to 0$, this implies that $\sigma_{x_i}\to 0,\ \ \forall\ i$, then the Taylor expansion of the payoff function in (3.13) can be expanded as follows:

$$U_1\left(\sigma_{x_1},\ldots,\sigma_{x_n};\sigma_{j_1},\ldots,\sigma_{j_n}\right)=\sum_{i=1}^{n}\left[\frac{\sigma_{x_i}|\lambda_{m_i}|^2}{1+\sigma_{j_i}|\lambda_{j_i}|^2}-\sigma_{x_i}|\lambda_{e_i}|^2+\mathcal{O}(\sigma_{x_i}^2)\right] \tag{3.76}$$

The optimization problem of the first order approximation becomes as:

$$\max_{\sigma_{x_i}}U_1\left(\sigma_{x_1},\ldots,\sigma_{x_n};\sigma_{j_1},\ldots,\sigma_{j_n}\right)=-\min_{\sigma_{x_i}}\sum_{i=1}^{n}\left[\frac{\sigma_{x_i}|\lambda_{m_i}|^2}{1+\sigma_{j_i}|\lambda_{j_i}|^2}-\sigma_{x_i}|\lambda_{e_i}|^2\right] \tag{3.77}$$

subject to:

$$\sum_{i=1}^{n}\sigma_{x_i}\leq P,\ \text{and}\ \sigma_{x_i}\geq 0,\quad i=1,2,\ldots,n \tag{3.78}$$

The Lagrangian of the optimization problem (3.77), subject to (3.78) is:

$$\mathcal{L}\left(\sigma_{x_i},V,u_i\right)=-U_1\Big(\sigma_{x_1},\ldots,\sigma_{x_n};\sigma_{j_1},\ldots,\sigma_{j_n}\Big)+V\Big(\sum_{i=1}^{n}\sigma_{x_i}-P\Big)-\sum_{i=1}^{n}\Big(u_i\sigma_{x_i}\Big) \tag{3.79}$$

where $V\geq 0$, and $u_i\geq 0$ are the Lagrange multipliers associated with the problem constraints.

The KKT conditions state that :

$$\nabla_{\sigma_{x_i}}\mathcal{L}\left(\sigma_{x_i},V,u_i\right)=0,\quad i=1,2,\ldots,n \tag{3.80}$$

with $V\Big(\sum_{i=1}^{n}\sigma_{x_i}-P\Big)=0 \;\; \forall\; V\geq 0$ and $u_i\sigma_{x_i}=0 \;\; \forall\; u_i\geq 0, \quad i=1,2,\ldots,n$

From (3.80) we have,

$$V-u_i=\frac{|\lambda_{m_i}|^2}{1+\sigma_{j_i}|\lambda_{j_i}|^2}-|\lambda_{e_i}|^2 \tag{3.81}$$

$\sigma_{x_i}>0$ means $u_i=0$

From (3.81) we have,

$$V=\frac{|\lambda_{m_i}|^2}{1+\sigma_{j_i}|\lambda_{j_i}|^2}-|\lambda_{e_i}|^2 \tag{3.82}$$

i.e., when $P\to 0$, for fix jammer strategy σ_{j_i}, Alice puts all her power in the strongest sub-channel and the strongest sub-channel is determined by the index k, where

$$k=\arg\max_i \frac{|\lambda_{m_i}|^2}{1+\sigma_{j_i}|\lambda_{j_i}|^2}-|\lambda_{e_i}|^2 \tag{3.83}$$

Therefore, for fix the jammer strategy $\sigma_{j_i}, i=1,2,...,n$, as $P\to 0$, the transmitter best response is given by:

$$\sigma^*_{x_i}=\begin{cases} P, & i=k \\ \\ 0, & i\neq k \end{cases}$$

Appendix D: Proof of Theorem 5

When $P_j\to 0$, this implies that $\sigma_{j_i}\to 0$, $\forall i$. Then the Taylor expansion of the payoff function in (3.13) can be expanded as follows:

$$U_1\left(\sigma_{x_1},\ldots,\sigma_{x_n};\sigma_{j_1},\ldots,\sigma_{j_n}\right)=$$

$$\sum_{i=1}^{n}\left[\log\left(1+\sigma_{x_i}|\lambda_{m_i}|^2\right)-\frac{\sigma_{x_i}\sigma_{j_i}|\lambda_{m_i}|^2|\lambda_{j_i}|^2}{1+\sigma_{x_i}|\lambda_{m_i}|^2}-\log\left(1+\sigma_{x_i}|\lambda_{e_i}|^2\right)+\mathcal{O}\left(\sigma_{j_i}^2\right)\right] \tag{3.84}$$

The optimization problem of the first order approximation become as:

$$\min_{\sigma_{j_i}} U_1\left(\sigma_{x_1},\ldots,\sigma_{x_n};\sigma_{j_1},\ldots,\sigma_{j_n}\right) =$$

$$\min_{\sigma_{j_i}} \sum_{i=1}^{n}\left[\log\left(1+\sigma_{x_i}\left|\lambda_{m_i}\right|^2\right)-\frac{\sigma_{x_i}\sigma_{j_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{1+\sigma_{x_i}\left|\lambda_{m_i}\right|^2}-\log\left(1+\sigma_{x_i}\left|\lambda_{e_i}\right|^2\right)\right] \tag{3.85}$$

subject to:

$$\sum_{i=1}^{n}\sigma_{j_i}\le P_j,\ \sigma_{j_i}\ge 0 \text{ and } \sigma_{j_i}\le\frac{\left|\lambda_{m_i}\right|^2-\left|\lambda_{e_i}\right|^2}{\left|\lambda_{e_i}\right|^2\left|\lambda_{j_i}\right|^2},\quad i=1,2,\ldots,n \tag{3.86}$$

The Lagrangian of the optimization problem (3.85), subject to (3.86) is,

$$\mathcal{L}\left(\sigma_{j_i},\nu,u_i,\eta_i\right)=U_1\Big(\sigma_{x1},\ldots,\sigma_{x1};\sigma_{j1},\ldots,\sigma_{j_n}\Big)+\nu\Big(\sum_{i=1}^{n}\sigma_{j_i}-P_j\Big)$$

$$-\sum_{i=1}^{n}\Big(u_i\sigma_{j_i}\Big)+\sum_{i=1}^{n}\left[\eta_i\Big(\sigma_{j_i}-\frac{\left|\lambda_{m_i}\right|^2-\left|\lambda_{e_i}\right|^2}{\left|\lambda_{e_i}\right|^2\left|\lambda_{j_i}\right|^2}\Big)\right] \tag{3.87}$$

where $\nu\ge 0$, $u_i\ge 0$ and $\eta_i\ge 0$ are the Lagrange multipliers associated with the problem constraints.

The KKT conditions state that :

$$\nabla_{\sigma_{j_i}}\mathcal{L}\left(\sigma_{j_i},\nu,u_i,\eta_i\right)=0 \tag{3.88}$$

with $\nu(\sum_{i=1}^{n}\sigma_{j_i}-P)=0\ \ \forall\ \nu\ge 0,\quad u_i\sigma_{j_i}=0\ \ \forall\ u_i\ge 0,\quad i=1,2,\ldots,n$
and $\eta_i(\sigma_{j_i}-\frac{\left|\lambda_{m_i}\right|^2-\left|\lambda_{e_i}\right|^2}{\left|\lambda_{e_i}\right|^2\left|\lambda_{j_i}\right|^2})=0\ \ \forall\ \eta_i\ge 0,\quad i=1,2,\ldots,n$

From (3.88) we have,

$$\nu-u_i+\eta_i=\frac{\sigma_{x_i}\left|\lambda_{m_i}\right|^2\left|\lambda_{j_i}\right|^2}{1+\sigma_{x_i}\left|\lambda_{m_i}\right|^2} \tag{3.89}$$

$\sigma_{j_i}>0$ means $u_i=0$ and $\sigma_{j_i}\le\frac{\left|\lambda_{m_i}\right|^2-\left|\lambda_{e_i}\right|^2}{\left|\lambda_{e_i}\right|^2\left|\lambda_{j_i}\right|^2}$ means $\eta_i=0$

From (3.89) we have,

$$\nu = \frac{\sigma_{x_i} |\lambda_{m_i}|^2 |\lambda_{j_i}|^2}{1 + \sigma_{x_i} |\lambda_{m_i}|^2} \tag{3.90}$$

i.e., when $P_j \to 0$, for fix Alice strategy σ_{x_i}, Jammer puts all his power in the strongest sub-channel and the strongest sub-channel is determined by the index k, where

$$k = \arg\max_i \frac{\sigma_{x_i} |\lambda_{m_i}|^2 |\lambda_{j_i}|^2}{1 + \sigma_{x_i} |\lambda_{m_i}|^2} \tag{3.91}$$

Therefore, for fix the transmitter strategy $\sigma_{x_i}, i = 1, 2, ..., n$, as $P_j \to 0$, the jammer best response is given by:

$$\sigma^*_{j_i} = \begin{cases} P_j, & i = k \\ \\ 0, & i \neq k \end{cases}$$

Appendix E: Proof of Theorem 7

The proof based on the fact that as $P_j \to 0$, the Jammer puts all his power on a single sub-channel for any fixed Alice strategy as specified in Theorem 5

If $\sigma_{j1} = P_j$ and $\sigma_{j_i} = 0$ for $i \neq 1$, then the utility function in (3.13) that Alice maximizes, can be written as,

$$U_1(\sigma_{x_1}, \ldots, \sigma_{x_n}; \sigma_{j_1}, \ldots, \sigma_{j_n}) = \log\left(1 + \frac{\sigma_{x_1} |\lambda_{m_1}|^2}{1 + P_j |\lambda_{j_1}|^2}\right) - \log\left(1 + \sigma_{x_1} |\lambda_{e_1}|^2\right)$$

$$+ \sum_{i=2}^{n} \left[\log\left(1 + \sigma_{x_i} |\lambda_{m_i}|^2\right) - \log\left(1 + \sigma_{x_i} |\lambda_{e_i}|^2\right)\right] \tag{3.92}$$

and the constraints are

$$\sum_{i=1}^{n} \sigma_{x_i} \leq P, \text{ and } \sigma_{x_i} \geq 0, \quad i = 1, 2, \ldots, n \tag{3.93}$$

Consider the KKT condition associated with the derivative of (3.92) with respect to σ_{x_1}. It states that:

$$V - u_1 = \frac{|\lambda_{m_1}|^2}{1 + \sigma_{x_1} |\lambda_{m_1}|^2 + P_j |\lambda_{j_1}|^2} - \frac{|\lambda_{e_1}|^2}{1 + \sigma_{x_1} |\lambda_{e_1}|^2} \tag{3.94}$$

which is monotonically decreasing function with respect to σ_{x_1}.

Here, $V(\sum_{i=1}^{n} \sigma_{x_i} - P) = 0 \ \ \forall\, V \geq 0$ and $u_i \sigma_{x_i} = 0 \ \ \forall\, u_i \geq 0, \quad i = 1, 2, \ldots, n$, where V and $u_i, \quad \forall\, i$, are the Lagrange multipliers associated with the problem constraints.

Now, assume that $\sigma_{x_1} = 0$ which implies that $u_1 \geq 0$. Them, from (3.94) we have

$$V - \frac{|\lambda_{m_1}|^2}{1 + P_j |\lambda_{j_1}|^2} - |\lambda_{e_1}|^2 = u_1 \geq 0 \tag{3.95}$$

and so,

$$V \geq \frac{|\lambda_{m_1}|^2}{1 + P_j |\lambda_{j_1}|^2} - |\lambda_{e_1}|^2 \tag{3.96}$$

Therefore, $\sigma_{x_1} = 0 \Rightarrow V \geq \frac{|\lambda_{m_1}|^2}{1+P_j|\lambda_{j_1}|^2} - |\lambda_{e_1}|^2$.

Conversely, now assume that $V \geq \frac{|\lambda_{m_1}|^2}{1+P_j|\lambda_{j_1}|^2} - |\lambda_{e_1}|^2$. Then from (3.94) we have,

$$V = \frac{|\lambda_{m_1}|^2}{1 + \sigma_{x_1} |\lambda_{m_1}|^2 + P_j |\lambda_{j_1}|^2} - \frac{|\lambda_{e_1}|^2}{1 + \sigma_{x_1} |\lambda_{e_1}|^2} + u_1 \geq \frac{|\lambda_{m_1}|^2}{1 + P_j |\lambda_{j_1}|^2} - |\lambda_{e_1}|^2$$

$$\Rightarrow \ u_1 \geq \frac{|\lambda_{m_1}|^2}{1 + P_j |\lambda_{j_1}|^2} - |\lambda_{e_1}|^2 - \frac{|\lambda_{m_1}|^2}{1 + \sigma_{x_1} |\lambda_{m_1}|^2 + P_j |\lambda_{j_1}|^2} + \frac{|\lambda_{e_1}|^2}{1 + \sigma_{x_1} |\lambda_{e_1}|^2} \tag{3.97}$$

Now,

$$\frac{|\lambda_{m_1}|^2}{1 + P_j |\lambda_{j_1}|^2} - |\lambda_{e_1}|^2 - \frac{|\lambda_{m_1}|^2}{1 + \sigma_{x_1} |\lambda_{m_1}|^2 + P_j |\lambda_{j_1}|^2} + \frac{|\lambda_{e_1}|^2}{1 + \sigma_{x_1} |\lambda_{e_1}|^2}$$

$$= \frac{|\lambda_{m_1}|^2 + \sigma_{x_1} |\lambda_{m_1}|^2 |\lambda_{e_1}|^2 + P_j |\lambda_{j_1}|^2 |\lambda_{e_1}|^2 + |\lambda_{e_1}|^2}{\left(1 + P_j |\lambda_{j_1}|^2\right)\left(1 + \sigma_{x_1} |\lambda_{e_1}|^2\right)}$$

$$- \frac{|\lambda_{m_1}|^2 + \sigma_{x_1} |\lambda_{m_1}|^2 |\lambda_{e_1}|^2 + P_j |\lambda_{j_1}|^2 |\lambda_{e_1}|^2 + |\lambda_{e_1}|^2}{1 + \sigma_{x_1} |\lambda_{m_1}|^2 + P_j |\lambda_{j_1}|^2}$$

$$\geq 0, \quad \text{since from (3.69) we have } 1 + \sigma_{x_1} |\lambda_{m_1}|^2 + P_j |\lambda_{j_1}|^2 \geq \left(1 + P_j |\lambda_{j_1}|^2\right)\left(1 + \sigma_{x_1} |\lambda_{e_1}|^2\right) \tag{3.98}$$

Then from (3.97) it is clear that $u_1 \geq 0$, which implies that $\sigma_{x_1} = 0$

Thus, $V \geq \frac{|\lambda_{m_1}|^2}{1+P_j|\lambda_{j_1}|^2} - |\lambda_{e_1}|^2 \Rightarrow \sigma_{x_1} = 0$

That is, $\sigma_{x_1} = 0 \Leftrightarrow V \geq \frac{|\lambda_{m_1}|^2}{1+P_j|\lambda_{j_1}|^2} - |\lambda_{e_1}|^2$

On the other hand, if $\sigma_{x_1} > 0$, which implies that $u_i = 0$. Then from (3.94) we have,

$$V = \frac{|\lambda_{m_1}|^2}{1 + \sigma_{x_1}|\lambda_{m_1}|^2 + P_j|\lambda_{j_1}|^2} - \frac{|\lambda_{e_1}|^2}{1 + \sigma_{x_1}|\lambda_{e_1}|^2} < \frac{|\lambda_{m_1}|^2}{1 + P_j|\lambda_{j_1}|^2} - |\lambda_{e_1}|^2 \qquad (3.99)$$

Conversely, if $V < \frac{|\lambda_{m_1}|^2}{1+P_j|\lambda_{j_1}|^2} - |\lambda_{e_1}|^2$, then from (3.94) we have,

$$\frac{|\lambda_{m_1}|^2}{1 + \sigma_{x_1}|\lambda_{m_1}|^2 + P_j|\lambda_{j_1}|^2} - \frac{|\lambda_{e_1}|^2}{1 + \sigma_{x_1}|\lambda_{e_1}|^2} + u_1 < \frac{|\lambda_{m_1}|^2}{1 + P_j|\lambda_{j_1}|^2} - |\lambda_{e_1}|^2 \qquad (3.100)$$

It is clear that, we can only satisfy (3.100) with $\sigma_{x_1} > 0$. We can not satisfy (3.100) with $\sigma_{x_1} = 0$, because, this implies that $u_i > 0$.

Thus, $V < \frac{|\lambda_{m_1}|^2}{1+P_j|\lambda_{j_1}|^2} - |\lambda_{e_1}|^2 \Rightarrow \sigma_{x_1} > 0$

That is, $\sigma_{x_1} > 0 \Leftrightarrow V < \frac{|\lambda_{m_1}|^2}{1+P_j|\lambda_{j_1}|^2} - |\lambda_{e_1}|^2$

It also follows from (3.99) that,

$$\begin{aligned} V &= \frac{|\lambda_{m_1}|^2}{1+\sigma_{x_1}|\lambda_{m_1}|^2+P_j|\lambda_{j_1}|^2} - \frac{|\lambda_{e_1}|^2}{1+\sigma_{x_1}|\lambda_{e_1}|^2} \\ &= \frac{|\lambda_{m_1}|^2\left(1+\sigma_{x_1}|\lambda_{e_1}|^2\right) - |\lambda_{e_1}|^2\left(1+\sigma_{x_1}|\lambda_{m_1}|^2+P_j|\lambda_{j_1}|^2\right)}{1+\sigma_{x_1}|\lambda_{m_1}|^2+P_j|\lambda_{j_1}|^2+\sigma_{x_1}|\lambda_{e_1}|^2+P_j\sigma_{x_1}|\lambda_{j_1}|^2|\lambda_{e_1}|^2+{\sigma_{x_1}}^2|\lambda_{m_1}|^2|\lambda_{e_1}|^2} \\ &\Rightarrow {\sigma_{x_1}}^2|\lambda_{m_1}|^2|\lambda_{e_1}|^2 + \sigma_{x_1}\left[\left(1+P_j|\lambda_{j_1}|^2\right)|\lambda_{e_1}|^2 + |\lambda_{m_1}|^2\right] + 1 + P_j|\lambda_{j_1}|^2 \\ &\qquad - \frac{|\lambda_{m_1}|^2 - P_j|\lambda_{j_1}|^2|\lambda_{e_1}|^2 - |\lambda_{e_1}|^2}{V} = 0 \end{aligned}$$

$$\Rightarrow \sigma_{x_1} = \frac{-\left(1+P_j\left|\lambda_{j_1}\right|^2\right)\left|\lambda_{e_1}\right|^2+\left|\lambda_{m_1}\right|^2}{2\left|\lambda_{m_1}\right|^2\left|\lambda_{e_1}\right|^2} \pm$$

$$\frac{\sqrt{[\left(1+P_j\left|\lambda_{j_1}\right|^2\right)\left|\lambda_{e_1}\right|^2+\left|\lambda_{m_1}\right|^2]^2-4\left|\lambda_{m_1}\right|^2\left|\lambda_{e_1}\right|^2\left(1+P_j\left|\lambda_{j_1}\right|^2-\frac{\left|\lambda_{m_1}\right|^2-P_j\left|\lambda_{j_1}\right|^2\left|\lambda_{e_1}\right|^2-\left|\lambda_{e_1}\right|^2}{V}\right)}}{2\left|\lambda_{m_1}\right|^2\left|\lambda_{e_1}\right|^2} \tag{3.101}$$

Since $\sigma_{x_1} > 0$, the only admissible solution in (3.101) is,

$$\sigma_{x_1} = \frac{1}{2}\left[\sqrt{\left(\frac{1}{\left|\lambda_{e_1}\right|^2}-\frac{1+P_j\left|\lambda_{j_1}\right|^2}{\left|\lambda_{m_1}\right|^2}\right)\left(\frac{4}{V}+\frac{1}{\left|\lambda_{e_1}\right|^2}-\frac{1+P_j\left|\lambda_{j_1}\right|^2}{\left|\lambda_{m_1}\right|^2}\right)}-\left(\frac{1+P_j\left|\lambda_{j_1}\right|^2}{\left|\lambda_{m_1}\right|^2}+\frac{1}{\left|\lambda_{e_1}\right|^2}\right)\right]$$

Therefore, the optimal ${\sigma_{x_1}}^*$ that maximize the utility (3.92) is given by

$$\sigma_{x_1}^* = \begin{cases} \frac{1}{2}\left[\sqrt{\left(\frac{1}{\left|\lambda_{e_1}\right|^2}-\frac{1+P_j\left|\lambda_{j_1}\right|^2}{\left|\lambda_{m_1}\right|^2}\right)\left(\frac{4}{V}+\frac{1}{\left|\lambda_{e_1}\right|^2}-\frac{1+P_j\left|\lambda_{j_1}\right|^2}{\left|\lambda_{m_1}\right|^2}\right)}-\left(\frac{1+P_j\left|\lambda_{j_1}\right|^2}{\left|\lambda_{m_1}\right|^2}+\frac{1}{\left|\lambda_{e_1}\right|^2}\right)\right], \\ \qquad\qquad V < \frac{\left|\lambda_{m_1}\right|^2}{1+P_j\left|\lambda_{j_1}\right|^2}-\left|\lambda_{e_1}\right|^2 \\ 0, \qquad\qquad V \geq \frac{\left|\lambda_{m_1}\right|^2}{1+P_j\left|\lambda_{j_1}\right|^2}-\left|\lambda_{e_1}\right|^2 \end{cases} \tag{3.102}$$

Consider the KKT condition associated with the derivative of (3.92) with respect to σ_{x_i}, $i \neq 1$. It states that:

$$V - u_i = \frac{\left|\lambda_{m_i}\right|^2}{1+\sigma_{x_i}\left|\lambda_{m_i}\right|^2} - \frac{\left|\lambda_{e_i}\right|^2}{1+\sigma_{x_i}\left|\lambda_{e_i}\right|^2} \tag{3.103}$$

with $V(\sum_{i=1}^{n}\sigma_{x_i} - P) = 0 \ \forall\, V \geq 0$ and $u_i\sigma_{x_i} = 0 \ \forall\, u_i \geq 0, \ \forall\, i$, where V and $u_i, \ \forall\, i$, are also the Lagrange multipliers associated with the problem constraints.

It is possible to repeat the previous analysis. Assume that $\sigma_{x_i} = 0$, which means that $u_i \geq 0$

From (3.103) we have,

$$V - u_i = |\lambda_{m_i}|^2 - |\lambda_{e_i}|^2 \tag{3.104}$$

and so,

$$V \geq |\lambda_{m_i}|^2 - |\lambda_{e_i}|^2 \tag{3.105}$$

Therefore, $\sigma_{x_i} = 0 \Rightarrow V \geq |\lambda_{m_i}|^2 - |\lambda_{e_i}|^2$

Conversely, assume now that $V \geq |\lambda_{m_i}|^2 - |\lambda_{e_i}|^2$. Then from (3.103) we have,

$$V = \frac{|\lambda_{m_i}|^2}{1 + \sigma_{x_i} |\lambda_{m_i}|^2} - \frac{|\lambda_{e_i}|^2}{1 + \sigma_{x_i} |\lambda_{e_i}|^2} + u_i \geq |\lambda_{m_i}|^2 - |\lambda_{e_i}|^2$$

$$\Rightarrow \; u_i \geq |\lambda_{m_i}|^2 - |\lambda_{e_i}|^2 - \frac{|\lambda_{m_i}|^2}{1 + \sigma_{x_i} |\lambda_{m_i}|^2} + \frac{|\lambda_{e_i}|^2}{1 + \sigma_{x_i} |\lambda_{e_i}|^2} \tag{3.106}$$

Now,

$$|\lambda_{m_i}|^2 - |\lambda_{e_i}|^2 - \frac{|\lambda_{m_i}|^2}{1 + \sigma_{x_i} |\lambda_{m_i}|^2} + \frac{|\lambda_{e_i}|^2}{1 + \sigma_{x_i} |\lambda_{e_i}|^2}$$

$$= \frac{|\lambda_{m_i}|^2 + \sigma_{x_i} |\lambda_{m_i}|^2 |\lambda_{e_i}|^2 + |\lambda_{e_i}|^2}{1 + \sigma_{x_i} |\lambda_{e_i}|^2} - \frac{|\lambda_{m_i}|^2 + \sigma_{x_i} |\lambda_{m_i}|^2 |\lambda_{e_i}|^2 + |\lambda_{e_i}|^2}{1 + \sigma_{x_i} |\lambda_{m_i}|^2}$$

$$\geq 0, \quad \text{since } 1 + \sigma_{x_i} |\lambda_{m_i}|^2 \geq 1 + \sigma_{x_i} |\lambda_{e_i}|^2 \tag{3.107}$$

So, from (3.106) it is clear that $u_i \geq 0$, which implies that $\sigma_{x_i} = 0$.

Thus, $V \geq |\lambda_{m_i}|^2 - |\lambda_{e_i}|^2 \Rightarrow \sigma_{x_i} = 0$

That is, $\sigma_{x_i} = 0 \Leftrightarrow V \geq |\lambda_{m_i}|^2 - |\lambda_{e_i}|^2$

On the other hand, $\sigma_{x_i} > 0$ leads to $u_i = 0$

From (3.103) we can write,

$$V = \frac{|\lambda_{m_i}|^2}{1 + \sigma_{x_i} |\lambda_{m_i}|^2} - \frac{|\lambda_{e_i}|^2}{1 + \sigma_{x_i} |\lambda_{e_i}|^2} < |\lambda_{m_i}|^2 - |\lambda_{e_i}|^2 \tag{3.108}$$

Conversely, $V < |\lambda_{m_i}|^2 - |\lambda_{e_i}|^2$ leads to $u_i = 0$ and $\sigma_{x_i} > 0$.

That is, $\sigma_{x_i} > 0 \Leftrightarrow V < |\lambda_{m_i}|^2 - |\lambda_{e_i}|^2$

From (3.108) we have,

$$V = \frac{|\lambda_{m_i}|^2}{1+\sigma_{x_i}|\lambda_{m_i}|^2} - \frac{|\lambda_{e_i}|^2}{1+\sigma_{x_i}|\lambda_{e_i}|^2}$$

$$= \frac{|\lambda_{m_i}|^2(1+\sigma_{x_i}|\lambda_{e_i}|^2) - |\lambda_{e_i}|^2\left(1+\sigma_{x_i}|\lambda_{m_i}|^2\right)}{\left(1+\sigma_{x_i}|\lambda_{m_i}|^2\right)\left(1+\sigma_{x_i}|\lambda_{e_i}|^2\right)}$$

$$\Rightarrow {\sigma_{x_i}}^2|\lambda_{m_i}|^2|\lambda_{e_i}|^2 + \sigma_{x_i}\left(|\lambda_{e_i}|^2 + |\lambda_{m_i}|^2\right) + 1 - \frac{|\lambda_{m_i}|^2 - |\lambda_{e_i}|^2}{V} = 0$$

$$\Rightarrow \sigma_{x_i} = \frac{-\left(|\lambda_{e_i}|^2 + |\lambda_{m_i}|^2\right) \pm \sqrt{\left(|\lambda_{e_i}|^2 + |\lambda_{m_i}|^2\right)^2 - 4|\lambda_{m_i}|^2|\lambda_{e_i}|^2\left(1 - \frac{|\lambda_{m_i}|^2 - |\lambda_{e_i}|^2}{V}\right)}}{2|\lambda_{m_i}|^2|\lambda_{e_i}|^2} \tag{3.109}$$

Since $\sigma_{x_i} > 0$, only admissible solution is,

$$\sigma_{x_i} = \frac{1}{2}\left[\sqrt{\left(\frac{1}{|\lambda_{e_i}|^2} - \frac{1}{|\lambda_{m_i}|^2}\right)^2 + \frac{4}{V}\left(\frac{1}{|\lambda_{e_i}|^2} - \frac{1}{|\lambda_{m_i}|^2}\right)} - \left(\frac{1}{|\lambda_{e_i}|^2} + \frac{1}{|\lambda_{m_i}|^2}\right)\right]$$

Therefore the optimal ${\sigma_{x_i}}^*$ that maximize the utility (3.92) is given by

$$\sigma^*_{x_i} = \begin{cases} \frac{1}{2}\left[\sqrt{\left(\frac{1}{|\lambda_{e_i}|^2} - \frac{1}{|\lambda_{m_i}|^2}\right)^2 + \frac{4}{V}\left(\frac{1}{|\lambda_{e_i}|^2} - \frac{1}{|\lambda_{m_i}|^2}\right)} - \left(\frac{1}{|\lambda_{e_i}|^2} + \frac{1}{|\lambda_{m_i}|^2}\right)\right], & \\ \qquad\qquad V < |\lambda_{m_i}|^2 - |\lambda_{e_i}|^2 \\ 0, \qquad\qquad V \geq |\lambda_{m_i}|^2 - |\lambda_{e_i}|^2 \end{cases} \tag{3.110}$$

The optimal utility under the scenario that $\sigma_{j_1} = P_j$ and $\sigma_{j_i} = 0,\ i \neq 1$ becomes

as,

$$U_{11}^{*}(\sigma_{x_i}^{*},\sigma_{j_i}^{*}) = \log\left(1+\frac{\sigma_{x_1}^{*}\left|\lambda_{m_1}\right|^2}{1+P_j\left|\lambda_{j_1}\right|^2}\right) - \log\left(1+\sigma_{x_1}^{*}\left|\lambda_{e_1}\right|^2\right)$$

$$+\sum_{i=2}^{n}\left[\log\left(1+\sigma_{x_i}^{*}\left|\lambda_{m_i}\right|^2\right) - \log\left(1+\sigma_{x_i}^{*}\left|\lambda_{e_i}\right|^2\right)\right] \tag{3.111}$$

Like wise, this process can be repeated for the scenario where $\sigma_{j_k} = P_j$ and $\sigma_{j_i} = 0, \forall\ k$, which would lead to the optimal power allocation policy

$$\sigma_{x_k}^{*} = \begin{cases} \frac{1}{2}\left[\sqrt{\left(\frac{1}{\left|\lambda_{e_k}\right|^2}-\frac{1+P_j\left|\lambda_{j_k}\right|^2}{\left|\lambda_{m_k}\right|^2}\right)\left(\frac{4}{V}+\frac{1}{\left|\lambda_{e_k}\right|^2}-\frac{1+P_j\left|\lambda_{j_k}\right|^2}{\left|\lambda_{m_k}\right|^2}\right)}-\left(\frac{1+P_j\left|\lambda_{j_k}\right|^2}{\left|\lambda_{m_k}\right|^2}+\frac{1}{\left|\lambda_{e_k}\right|^2}\right)\right], \\ \qquad\qquad V < \frac{\left|\lambda_{m_k}\right|^2}{1+P_j\left|\lambda_{j_k}\right|^2} - \left|\lambda_{e_k}\right|^2 \\ 0, \qquad\qquad V \geq \frac{\left|\lambda_{m_k}\right|^2}{1+P_j\left|\lambda_{j_k}\right|^2} - \left|\lambda_{e_k}\right|^2 \end{cases} \tag{3.112}$$

and

$$\sigma_{x_i}^{*} = \begin{cases} \frac{1}{2}\left[\sqrt{\left(\frac{1}{\left|\lambda_{e_i}\right|^2}-\frac{1}{\left|\lambda_{m_i}\right|^2}\right)^2+\frac{4}{\nu}\left(\frac{1}{\left|\lambda_{e_i}\right|^2}-\frac{1}{\left|\lambda_{m_i}\right|^2}\right)}-\left(\frac{1}{\left|\lambda_{e_i}\right|^2}+\frac{1}{\left|\lambda_{m_i}\right|^2}\right)\right], \\ \qquad\qquad V < \left|\lambda_{m_i}\right|^2 - \left|\lambda_{e_i}\right|^2 \\ 0, \qquad\qquad V \geq \left|\lambda_{m_i}\right|^2 - \left|\lambda_{e_i}\right|^2 \end{cases} \tag{3.113}$$

$\forall i \neq k$, and would also lead to the ultility function,

$$U_{1k}{}^{*}\left(\sigma_{x_i}{}^{*},\sigma_{j_i}{}^{*}\right) = \log\left(1+\frac{\sigma_{x_k}{}^{*}\left|\lambda_{m_k}\right|^2}{1+P_j\left|\lambda_{j_k}\right|^2}\right) - \log\left(1+\sigma_{x_k}{}^{*}\left|\lambda_{e_k}\right|^2\right)$$

$$+\sum_{i=1}^{k-1}\left[\log\left(1+\sigma_{x_i}{}^{*}\left|\lambda_{m_i}\right|^2\right) - \log\left(1+\sigma_{x_i}^{*}\left|\lambda_{e_i}\right|^2\right)\right] \tag{3.114}$$

In view of equation (3.114), jammer´s optimal strategies are ${\sigma_{jk}}^* = P_j$ and $\sigma_{j_i} = 0$ for $i \neq k$, where, $k = \arg\min_i {U_{1i}}^*$, i.e,

$$k = \arg\min_i \max_{\sigma_{x_l}, l=1,\ldots,n \in \Psi} U_1\big(\sigma_{x_1}, \ldots, \sigma_{x_n}; \sigma_{j_1} = 0, \ldots, \sigma_{j_{i-1}} = 0, \sigma_{j_i} = P_j, \sigma_{j_{i+1}} = 0, \ldots, \sigma_{j_n} = 0\big) \quad (3.115)$$

Therefore, a Nash equilibrium exists as follows:

$$(\sigma_{x_i}^*, \sigma_{j_i}^*) = \begin{cases} \big(\frac{1}{2}\big[\sqrt{\big(\frac{1}{|\lambda_{e_i}|^2} - \frac{1+P_j|\lambda_{j_i}|^2}{|\lambda_{m_i}|^2}\big)\big(\frac{4}{V} + \frac{1}{|\lambda_{e_i}|^2} - \frac{1+P_j|\lambda_{j_i}|^2}{|\lambda_{m_i}|^2}\big)} - \big(\frac{1+P_j|\lambda_{j_i}|^2}{|\lambda_{m_i}|^2} + \frac{1}{|\lambda_{e_i}|^2}\big)\big], P_j\big), \\ \qquad\qquad i = k \text{ and } V < \frac{|\lambda_{m_i}|^2}{1+P_j|\lambda_{j_i}|^2} - |\lambda_{e_i}|^2 \\ \big(0, P_j\big), \qquad\qquad i = k \text{ and } V \geq \frac{|\lambda_{m_i}|^2}{1+P_j|\lambda_{j_i}|^2} - |\lambda_{e_i}|^2 \\ \big(\frac{1}{2}\big[\sqrt{\big(\frac{1}{|\lambda_{e_i}|^2} - \frac{1}{|\lambda_{m_i}|^2}\big)^2 + \frac{4}{V}\big(\frac{1}{|\lambda_{e_i}|^2} - \frac{1}{|\lambda_{m_i}|^2}\big)} - \big(\frac{1}{|\lambda_{e_i}|^2} + \frac{1}{|\lambda_{m_i}|^2}\big)\big], 0\big), \\ \qquad\qquad i \neq k \text{ and } V < |\lambda_{m_i}|^2 - |\lambda_{e_i}|^2 \\ \big(0, 0\big), \qquad\qquad i \neq k \text{ and } V \geq |\lambda_{m_i}|^2 - |\lambda_{e_i}|^2 \end{cases}$$

Chapter 4
Parallel Gaussian Wiretap Channel with a Friendly Jammer: Power Allocation Strategies

4.1 Introduction

In this Chapter we are interested in the security aspect of the wireless communication network with the aid of friendly jammers. We consider a model which applies to scenarios where, with the intent of impairing the communication between the transmitter and eavesdropper, the jammer positions himself to be much closer to the eavesdropper than to the legitimate receiver (e.g. [82]).

It is known that interference in wireless channels can be used effectively by cooperating nodes to improve the level of security of wireless channels and networks (e.g. [37, 83, 84, 85, 82, 86, 87, 88, 89]). For example, in [37], the authors investigate the design of optimal jamming configurations and the relationship between jamming coverage, jamming efficiency and the probability of secrecy outage, in order to characterize the security level of a network in which a transmitter and a legitimate receiver try to communicate in the presence of an eavesdropper. [84] study a cooperative jamming approach to increase the security of a wiretap fading channel via distributed relays. In [85] the authors consider a MISO wiretap scenario where a group of friendly jammers independently transmit noise in the null space of the jammer-legitimate receiver channel in order to maximize the secrecy rate subject to probability of outage and power constraints. The authors of [82] use a game theoretic approach in order to characterize the interaction between the source, that transmits the useful data, and friendly jammers, that assist the source by introducing interference in the eavesdropper channel in order to increase the secrecy capacity

of the wiretap channel. In [89], the secrecy capacity of two nodes communicating in the presence of eavesdroppers, placed anywhere in a confined region, is investigated when friendly jammers, with different levels of channel state information, help the legitimate parties by causing interference to possible eavesdroppers.

In this Chapter, two legitimate parties (Alice and Bob) communicate in the presence of a friendly jammer and an eavesdropper (Eve). The eavesdropper is assumed to be passive but the jammer injects interference in the eavesdropper channel in the form of additive noise. In this scenario, we consider an OFDM communication framework where each of the parties transmits and receives over a bank of parallel independent Gaussian channels. The objective is to maximize the secrecy rate, between the source (Alice) and the destination (Bob) by characterizing the optimal power allocation policy for the jammer corresponding to the transmitter fixed power allocation.

This Chapter is organized as follows: In Section 4.2, we present the system model and the problem formulation. Section 4.3 analyzes the problems for the degraded and the general case respectively. Section 4.4 presents a set of numerical results that cast further insight into the nature of the optimal strategies. The results also unveil the secrecy gain of an adaptive transmitter and jammer over a non-adaptive one. In Section 4.5, we summarize the main contributions of this chapter work.

4.2 Problem formulation

We consider a communications scenario where a legitimate user, Alice, tries to communicate with another legitimate user, Bob, in the presence of an eavesdropper, Eve, and a friendly jammer over a bank of n parallel independent Gaussian channels. In particular, as in Chapter 3, we assume that the jammer interferes only with the eavesdropper channel (see Figure 4.1). Therefore, once again, this applies to scenarios where, with the intent of impairing the communication between the transmitter and eavesdropper, the jammer positions himself to be much closer to the eavesdropper than to the legitimate receiver.

Bob observes the output of the main channel given by:

$$\mathbf{y}_m = \mathbf{\Lambda}_m \mathbf{x}_t + \mathbf{n}_m \tag{4.1}$$

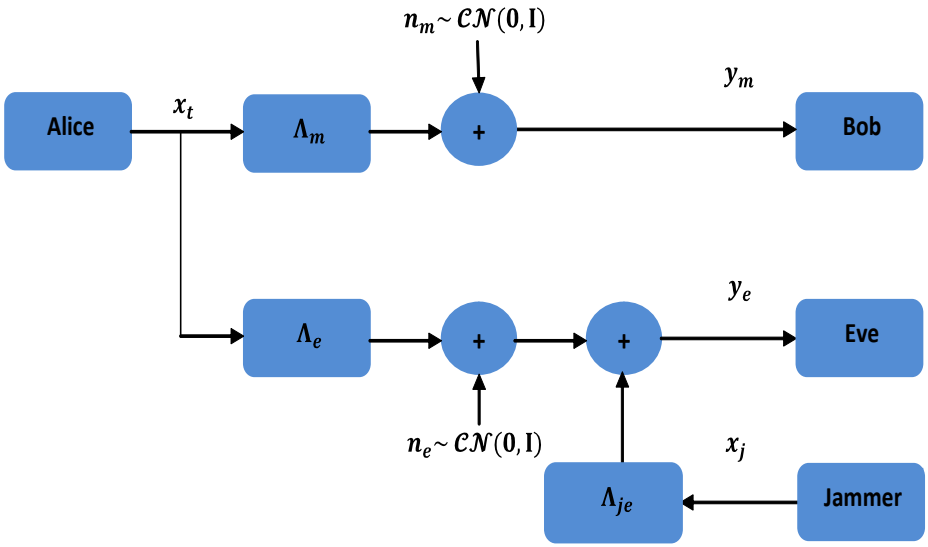

Figure 4.1: Parallel Gaussian wiretap channel model with a friendly jammer.

and Eve observes the output of the eavesdropper channel given by:

$$\mathbf{y}_e = \mathbf{\Lambda}_e \mathbf{x}_t + \mathbf{n}_e + \mathbf{\Lambda}_{j_e} \mathbf{x}_j \tag{4.2}$$

where $\mathbf{y}_m \in \mathbb{C}^n$ and $\mathbf{y}_e \in \mathbb{C}^n$ represent the vectors of complex received symbols at the output of the main and eavesdropper channels, respectively, $\mathbf{x}_t \in \mathbb{C}^n$ represents the vector of complex transmit symbols with zero mean and covariance $\mathbf{\Sigma}_x = \mathbb{E}[\mathbf{x}_t \mathbf{x}_t^\dagger]$, and $\mathbf{n}_m \in \mathbb{C}^n$ and $\mathbf{n}_e \in \mathbb{C}^n$ are vectors of circularly symmetric complex Gaussian noise random variables with zero-mean and identity covariance matrix. We assume that $\mathbf{x}_j \in \mathbb{C}^n$ is a vector of circularly symmetric complex Gaussian noise with zero mean and covariance $\mathbf{\Sigma}_j = \mathbb{E}[\mathbf{x}_j \mathbf{x}_j^\dagger]$, which represents the jamming signal power.

$\mathbf{\Lambda}_m = diag\left(\lambda_{m_1}, \lambda_{m2}, \ldots, \lambda_{mn}\right) \in \mathbb{C}^n$ is a diagonal matrix that contains the complex gains of the parallel sub-channels of the main channel, $\mathbf{\Lambda}_e = diag\left(\lambda_{e_1}, \lambda_{e2}, \ldots, \lambda_{e_n}\right) \in \mathbb{C}^n$ is a diagonal matrix that contains the complex gains of the parallel sub-channels of the eavesdropper channel, and, likewise, $\mathbf{\Lambda}_{je} = diag\left(\lambda_{je_1}, \lambda_{je_2}, \ldots, \lambda_{je_n}\right) \in \mathbb{C}^n$ is a diagonal matrix that contains the complex gains of the parallel sub-channels that compose the jammer channel. Note once again that this model arises in systems where Alice, Bob, Eve and the jammer adopt OFDM modulation and demodulation. We assume that Alice, Bob, Eve and the jammer know the exact channel conditions [77]. These assumptions can be realistic in some scenarios as argued in Chapter 3.

Both the transmitter and the friendly jammer transmit independent symbols over the different sub-channels. Thus we take both the input and jamming covariance matrices to be diagonal, i.e., $\mathbf{\Sigma}_x = \mathbb{E}[\mathbf{x}_t\mathbf{x}_t^\dagger] = diag\left(\sigma_{x_1}, \sigma_{x_2}, \ldots, \sigma_{x_n}\right)$ and $\mathbf{\Sigma}_j = \mathbb{E}[\mathbf{x}_j\mathbf{x}_j^\dagger] = diag\left(\sigma_{j_1}, \sigma_{j_2}, \ldots, \sigma_{j_n}\right)$, respectively, where σ_{x_i} represents the power injected into main sub-channels i and σ_{j_i} represents the power injected into friendly jammer sub-channels i, $i = 1, \ldots, n$.

Additionally we impose power restrictions on both for the transmitter and the jammer, namely:

$$\sum_{i=1}^{n} \sigma_{x_i} \leq P \tag{4.3}$$

$$\sum_{i=1}^{n} \sigma_{j_i} \leq P_j \tag{4.4}$$

where P and P_j are the transmitter and the jammer total power respectively.

Once again, the general expression of the secrecy capacity of a wiretap channel, which corresponds to the largest achievable reliable transmission rate with perfect secrecy [55], is given by [9]:

$$C_s = \max_{\mathbf{v} \to \mathbf{x}_t \to \mathbf{y}_m, \mathbf{y}_e} I(\mathbf{v}; \mathbf{y}_m) - I(\mathbf{v}; \mathbf{y}_e) \tag{4.5}$$

Where the maximization is over all joint distributions $P_{\mathbf{v},\mathbf{x}_t}\left(\mathbf{v}, \mathbf{x}_t\right)$ such that the Markov chain $\mathbf{v} \to \mathbf{x}_t \to \mathbf{y}_m\ \mathbf{y}_e$ holds.

Once again, according to [12, Theorem 1], the secrecy capacity of a bank of independent parallel Gaussian wiretap channels in (4.5), as like (2.14), reduces to:

$$C_s = \sum_{i=1}^{n} C_{s_i} = \sum_{i=1}^{n} \max_{\mathbf{x}_{t_i} \to \mathbf{y}_{m_i}, \mathbf{y}_{e_i}} I\Big(\mathbf{x}_{t_i}; \mathbf{y}_{m_i}\Big) - I\Big(\mathbf{x}_{t_i}; \mathbf{y}_{e_i}\Big) \tag{4.6}$$

where C_{s_i} represents the secrecy capacity of the i^{th} sub-channel and the maximizations are over all the distributions $P_{x_{t_i}}(x_{t_i}), i = 1, \ldots, n$ and x_{t_i} represents the complex transmit symbol in the i^{th} sub-channel, y_{m_i} represents the complex receive symbol in the i^{th} main sub-channel and y_{e_i} represents the complex receive symbol in the i^{th} eavesdropper sub-channel.

Let us fix the input signal covariance $\mathbf{\Sigma}_x = diag(\sigma_{x_1}, \ldots, \sigma_{x_n})$ and the jammer signal covariance $\mathbf{\Sigma}_j = diag(\sigma_{j_1}, \ldots, \sigma_{j_n})$, where $\sigma_{x_1}, \ldots, \sigma_{x_n}$ and $\sigma_{j_1}, \ldots, \sigma_{j_n}$ represent the set of powers that the transmitter and the jammer inject into the bank of parallel independent Gaussian channels, respectively. We do not claim that independent jamming is optimal. Instead, we restrict attention to scenarios where the jammer does not introduce correlated noise across the sub-channels[5]. Then, it is possible to write an achievable secrecy rate as follows:

$$R_s\left(\sigma_{x_1}, \ldots, \sigma_{x_n}; \sigma_{j_1}, \ldots, \sigma_{j_n}\right) = \sum_{i=1}^{n} \left[\log\left(1 + \sigma_{xi} \left|\lambda_{m_i}\right|^2\right) - \log\left(1 + \frac{\sigma_{xi} \left|\lambda_{e_i}\right|^2}{1 + \sigma_{j_i} \left|\lambda_{j_{ei}}\right|^2}\right) \right]^+ \tag{4.7}$$

where $[z]^+ = \max(0, z)$. This expression is the basis of the determination of the transmitter and power allocation policies that maximize the achievable secrecy rate.

4.3 Analysis

We will now study the optimal transmitter and jammer power allocation policies that maximize the achievable secrecy rate in (4.7) subject to the power constraints in (4.3) and (4.4). We consider separately the degraded scenario, where $\left|\lambda_{m_i}\right|^2 \geq \left|\lambda_{e_i}\right|^2, i = 1, \ldots, n$, and the more general non-degraded scenario.

4.3.1 The degraded case

We first consider a degraded parallel Gaussian wiretap channel where $\left|\lambda_{m_i}\right|^2 \geq \left|\lambda_{e_i}\right|^2, i = 1, \ldots, n$. We will study the optimal power allocation of the jammer for a fixed Alice power allocation. In this first case, the optimization problem can be written as follows:

$$\max_{\sigma_{j_i}, i=1,\ldots,n} R_s\Big(\sigma_{x_1}, \ldots, \sigma_{x_n}; \sigma_{j_1}, \ldots, \sigma_{j_n}\Big) = \sum_{i=1}^{n} \Big[\log\left(1 + \sigma_{x_i} \left|\lambda_{m_i}\right|^2\right) - \log\left(1 + \frac{\sigma_{xi} \left|\lambda_{e_i}\right|^2}{1 + \sigma_{j_i} \left|\lambda_{j_{ei}}\right|^2}\right) \Big] \tag{4.8}$$

[5]Note that, the secrecy capacity is the maximum value of the secrecy rate. Note also that the transmitter must know the optimal jammer power allocation in order to develop the coding scheme. In this work we assume that the jammer will inform the transmitter after optimizing its jamming strategy.

subject to the constraints:

$$\sum_{i=1}^{n} \sigma_{j_i} \leq P_j \text{ with } \sigma_{j_i} \geq 0, i = 1, \ldots, n \tag{4.9}$$

where P_j represent the total power available at the jammer. It is straightforward to show that the first optimization problem constitutes a standard convex optimization problem and thus, the optimal solution can be characterized by KKT conditions [90], which are necessary and sufficient.

We will also characterize the power allocation policies in general power and in asymptotic low power regimes.

4.3.1.1 Characterization of optimal power allocation policies

The following Theorem defines the optimal power allocation policy of the jammer for a fixed transmitter power σ_{x_i}, $i = 1, \ldots, n$:

Theorem 8. *Fix the transmitter power $\sigma_{x_i}, i = 1, 2, ..., n$. Then, the optimal jammer power allocation policy $\sigma^*_{j_i}, i = 1, 2, ..., n$, that solves the optimization problem*

$$\max_{\sigma_{j_i}, i=1,\ldots,n} R_s\left(\sigma_{x_1}, \ldots, \sigma_{x_n}, \sigma_{j_1}, \ldots, \sigma_{j_n}\right) \tag{4.10}$$

subject to: $\sum_{i=1}^{n} \sigma_{j_i} \leq P_j$, and $\sigma_{j_i} \geq 0$, $i = 1, \ldots, n$ is given by:

$$\sigma^*_{j_i} = \begin{cases} \dfrac{\sqrt{\sigma^2_{x_i}\left|\lambda_{e_i}\right|^4 + \frac{4\sigma_{x_i}\left|\lambda_{e_i}\right|^2\left|\lambda_{je_i}\right|^2}{\nu}} - \left(2 + \sigma_{x_i}\left|\lambda_{e_i}\right|^2\right)}{2\left|\lambda_{je_i}\right|^2}, & \nu < \dfrac{\sigma_{xi}\left|\lambda_{e_i}\right|^2\left|\lambda_{je_i}\right|^2}{1+\sigma_{xi}\left|\lambda_{e_i}\right|^2} \\ 0, & \nu \geq \dfrac{\sigma_{x_i}\left|\lambda_{e_i}\right|^2\left|\lambda_{je_i}\right|^2}{1+\sigma_{x_i}\left|\lambda_{e_i}\right|^2} \end{cases} \tag{4.11}$$

with ν such that $\sum_{i=1}^{n} \sigma^*_{j_i} = P_j$.

Proof. See Appendix F. □

The solution embodied in Theorem 8, akin to other power allocation solution in literature (e.g. [91]), shows that the jammer may only inject power in some sub-channels. In particular, if the effective i^{th} sub-channel strength given by $\frac{\sigma_{x_i}|\lambda e_i|^2|\lambda_{je_i}|^2}{1+\sigma_{x_i}|\lambda e_i|^2}$

is below a certain threshold, then the jammer does not inject power in the i^{th} sub-channel. Otherwise, if the effective sub-channel strength given by $\frac{\sigma_{x_i}|\lambda e_i|^2|\lambda_{je_i}|^2}{1+\sigma_{x_i}|\lambda e_i|^2}$ is above the threshold, then the jammer injects an appropriate fraction of its available power in the i^{th} sub-channel. The solution in Theorem 8 also leads to a simple algorithm that produces the optimal power allocation policy in a finite number of iterations (see Algorithm 1). Let us define:

$$a_i = \frac{\sigma_{x_i}|\lambda e_i|^2|\lambda_{je_i}|^2}{1+\sigma_{x_i}|\lambda e_i|^2} \tag{4.12}$$

and

$$b_i = \frac{\sqrt{\sigma_{x_i}^2\left|\lambda_{e_i}\right|^4 + \frac{4\sigma_{x_i}\left|\lambda_{e_i}\right|^2|\lambda_{je_i}|^2}{\nu}} - \left(2+\sigma_{x_i}\left|\lambda_{e_i}\right|^2\right)}{2\left|\lambda_{je_i}\right|^2} \tag{4.13}$$

Note that this iterative algorithm bypasses the need to implement standard convex optimization procedures and it converges in a maximum on n steps. Note also that the optimal solution differs from standard waterfilling. The most complex step of the algorithm only requires solving a nonlinear equation, in order to determine the value of Lagrange multiplier (see step 3). This can be accomplished using standard simple numerical procedures (e.g., Newton-Raphson, Secant or Steffensen's methods [92]).

4.3.1.2 Characterization of the optimal power allocation in the asymptotic low power regime

We will now characterize the optimal power allocation in two asymptotic low power regimes of great operational relevance: i) the asymptotic regime of low transmitter available power, where $P \to 0$; and ii) the asymptotic regime of low jammer available power, where $P_j \to 0$. This particular characterization, which applies to some practical scenarios as also argued in Chapter 3, casts further insight into the nature of the optimal power allocation policies.

4.3.1.2.1 Low transmitter available power

When $P \to 0$, then also $\sigma_{x_i} \to 0, i = 1, \ldots, n,$. Therefore, the Taylor expansion of

Algorithm 1: Algorithm to compute the set of optimal $\sigma_{j_i}^*$, for fixed σ_{x_i}, $i = 1, \ldots, n$, for the degraded case.

Input : Number of available sub-channels n, set of values λ_{je_i}, λ_{e_i}, $\sigma_{x_i}, i = 1, \ldots, n$, and P_j

Output: Set of optimal values $\sigma_{j_i}^*, i = 1, \ldots, n$, value of ν, number of active sub-channels n_{act} and number of inactive sub-channels n_{inact}.

1 • **Re-order** the sub-channels such that the values a_i are in a decreasing order (define also $a_{n+1} \stackrel{\triangle}{=} 0$).

Set $n_{inact} = 0$; **Set** $\widetilde{n} = n$.

2 • **Set** $\nu = a_{\widetilde{n}}$

3 • **if** $a_{\widetilde{n}} = 0$ **then**

- **Set** $\sigma_{j_{\widetilde{n}}}^* = 0$; $\widetilde{n} = \widetilde{n} - 1$; $n_{inact} = n_{inact} + 1$;
- **go to** step 2.

• **else if** $\sum_{i=1}^{\widetilde{n}} b_i \geq P_j$ **then**

- **Set** $\sigma_{j_{\widetilde{n}}}^* = 0$; $\widetilde{n} = \widetilde{n} - 1$; $n_{inact} = n_{inact} + 1$;
- **go to** step 2.

• **else**

- **Set** $n_{act} = \widetilde{n}$; **Set** ν such that: $\sum_{i=1}^{\widetilde{n}} b_i = P_j$;

Set $\sigma_{j_i}^* = b_i$, $i = 1, \ldots, n_{act}$;

- **Undo** the reordering done at step 1.

the secrecy rate in (4.8) can be expanded as follows:

$$R_s\left(\sigma_{x_i}, \sigma_{j_i}\right) = \sum_{i=1}^{n} \left[\sigma_{x_i}|\lambda_{m_i}|^2 - \frac{\sigma_{x_i}|\lambda_{e_i}|^2}{1 + \sigma_{j_i}|\lambda_{je_i}|^2} + \mathcal{O}(\sigma_{x_i}^2)\right] \tag{4.14}$$

The following Theorem defines the optimal power allocation of the jammer when the transmitter power is very low.

Theorem 9. *Fix the transmitter power allocation policy $\sigma_{x_i}, i = 1, \ldots, n$. Then the*

jammer optimal power that maximizes the secrecy rate as $P \to 0$ is given by:

$$\sigma_{j_i}^* = \begin{cases} \frac{\sqrt{\frac{\sigma_{x_i}|\lambda_{e_i}|^2\left|\lambda_{je_i}\right|^2}{V}}-1}{\left|\lambda_{je_i}\right|^2}, & V < \sigma_{x_i}|\lambda_{e_i}|^2|\lambda_{je_i}|^2 \\ 0, & V \geq \sigma_{x_i}|\lambda_{e_i}|^2|\lambda_{je_i}|^2 \end{cases} \tag{4.15}$$

with V such that $\sum_{i=1}^{n} \sigma_{j_i}^* = P_j$.

Proof. See Appendix G. □

Theorem 9 reveals that, in low available transmit power, the jammer will inject power in a single sub-channel as like transmitter as we shown in Chapter 3.

4.3.1.2.2 Low jammer available power

When $P_j \to 0$, then $\sigma_{j_i} \to 0, i = 1, \ldots, n,$. Therefore, the secrecy rate in (4.8) can be also expanded by using a Taylor series as follows:

$$R_s\left(\sigma_{x_1}, \ldots, \sigma_{x_n}; \sigma_{j_1}, \ldots, \sigma_{j_n}\right) = \sum_{i=1}^{n} \Big[\log\left(1 + \sigma_{x_i}|\lambda_{m_i}|^2\right) - \log\left(1 + \sigma_{x_i}|\lambda_{e_i}|^2\right) + \frac{\sigma_{x_i}\sigma_{j_i}|\lambda_{e_i}|^2|\lambda_{je_i}|^2}{1 + \sigma_{x_i}|\lambda_{je_i}|^2} + \mathcal{O}(\sigma_{j_i}^2) \Big] \tag{4.16}$$

The following Theorem defines the optimal power allocation of the jammer when the jammer power is very low.

Theorem 10. *Fix the transmitter power allocation policy $\sigma_{x_i}, i = 1, \ldots, n$. Then, the jammer optimal power allocation policy that maximizes the secrecy rate as $P_j \to 0$ is given by:*

$$\sigma_{j_i}^* = \begin{cases} P_j, & i = k \\ 0, & i \neq k \end{cases} \tag{4.17}$$

where

$$k = \arg\max_i \left[\frac{|\lambda_{je_i}|^2}{1 + \frac{1}{\sigma_{x_i}|\lambda_{e_i}|^2}} \right] \tag{4.18}$$

Proof. See Appendix H. □

Theorem 10 reveal that in the regime of low jammer power, the jammer will inject power in a single sub-channel, which is specified by index (4.18)

4.3.2 The general case

We now start by discussing how compute the optimal power allocation policy for the jammer in the general scenario where the optimization problem is not necessarily convex. The optimization problem can now be written as follows:

$$\max_{\sigma_{j_i}, i=1,\ldots,n} R_s\Big(\sigma_{x_1},\ldots,\sigma_{x_n};\sigma_{j_1},\ldots,\sigma_{j_n}\Big) =$$

$$\sum_{i=1}^{n}\Big[\log\Big(1+\sigma_{x_i}|\lambda_{m_i}|^2\Big)-\log\Big(1+\frac{\sigma_{xi}|\lambda_{e_i}|^2}{1+\sigma_{j_i}|\lambda_{j_{ei}}|^2}\Big)\Big]^+ \tag{4.19}$$

subject to the constraints:

$$\sum_{i=1}^{n}\sigma_{j_i}\leq P_j \text{ with } \sigma_{j_i}\geq 0,\ i=1,\ldots,n \tag{4.20}$$

It is relevant to note that the optimization problem in (4.19), contrary to the optimization problem in (4.7), is not necessarily convex in the presence of non-degradedness – where $|\lambda_{m_i}|^2 < |\lambda_{e_i}|^2$. However a simple argument enables us to transform problem (4.7) into a set of convex optimization problems. In particular it is evident that the secrecy rate of a certain non-degraded sub-channel i is zero when,

$$|\lambda_{m_i}|^2 \leq \frac{|\lambda_{e_i}|^2}{1+\sigma_{j_i}|\lambda_{j_{ei}}|^2}$$

$$\Leftrightarrow 1+\sigma_{j_i}|\lambda_{j_{ei}}|^2 \leq \frac{|\lambda_{e_i}|^2}{|\lambda_{m_i}|^2}$$

$$\Leftrightarrow \sigma_{j_i}|\lambda_{j_{ei}}|^2 \leq \frac{|\lambda_{e_i}|^2}{|\lambda_{m_i}|^2}-1$$

$$\Leftrightarrow \sigma_{j_i} \leq \frac{1}{|\lambda_{je_i}|^2}\left[\frac{|\lambda_{e_i}|^2}{|\lambda_{m_i}|^2}-1\right] \tag{4.21}$$

This means that the jammer, with the intent to maximize the secrecy rate of the parallel Gaussian wiretap channel, has only a pair of strategies for a certain non-degraded sub-channel i: either $\sigma_{j_i} = 0$ or $\sigma_{j_i} \geq \frac{1}{|\lambda_{je_i}|^2}\left[\frac{|\lambda_{e_i}|^2}{|\lambda_{m_i}|^2} - 1\right]$, provided that it respects the available power constraint P_j.

In particular, let w denote the number of degraded sub-channels and $l = n - w$ denote the number of non-degraded sub-channels. Let us also re-order the sub-channels such that $\alpha_1 \leq \alpha_2 \leq ..... \leq \alpha_w \leq \alpha_{w+1} \leq ..... \leq \alpha_n$, when $\alpha_i = \max\left(0, \frac{1}{|\lambda_{je_i}|^2}\left[\frac{|\lambda_{e_i}|^2}{|\lambda_{m_i}|^2} - 1\right]\right), i = 1, 2, ..., n$.

A possible procedure to determine the solution to the power allocation problem in the general scenario would then involve setting up various optimization problems, where the individual optimization problem are associated with different feasible jammer strategies for non-degraded sub-channels (i.e. $\sigma_{j_i} = 0$ or $\sigma_{j_i} \geq \frac{1}{|\lambda_{je_i}|^2}\left[\frac{|\lambda_{e_i}|^2}{|\lambda_{m_i}|^2} - 1\right]$ for a particular non-degraded sub-channel i).

For example, the optimization problem where it is assumed that $\sigma_{j_i} = 0$, $i \in S_1$ and $\sigma_{j_i} \geq \frac{1}{|\lambda_{je_i}|^2}\left[\frac{|\lambda_{e_i}|^2}{|\lambda_{m_i}|^2} - 1\right]$, $i \in S_2$, where S_1 and S_2 are disjoint sets of indices of non-degraded sub-channels whose union corresponds to the set of indices of the ordered non-degraded sub-channels, i.e., $w+1, \ldots, n$ (and also $\sum_{i\in S_2} \frac{1}{|\lambda_{je_i}|^2}\left[\frac{|\lambda_{e_i}|^2}{|\lambda_{m_i}|^2} - 1\right] \leq P_j$ to guarantee that the problem is feasible) is given by:

$$\max_{\sigma_{j_i}} R_s\Big(\sigma_{x_1}, \ldots, \sigma_{x_n}; \sigma_{j_1}, \ldots, \sigma_{j_n}\Big) = \sum_{i=1}^{w}\Big[\log\Big(1 + \sigma_{x_i}|\lambda_{m_i}|^2\Big)$$

$$- \log\Big(1 + \frac{\sigma_{xi}|\lambda_{e_i}|^2}{1 + \sigma_{j_i}|\lambda_{j_{ei}}|^2}\Big)\Big] + \sum_{i\in S_2}\Big[\log\big(1 + \sigma_{x_i}|\lambda_{m_i}|^2\big) - \log\big(1 + \frac{\sigma_{xi}|\lambda_{e_i}|^2}{1 + \sigma_{j_i}|\lambda_{j_{ei}}|^2}\big)\Big] \tag{4.22}$$

subject to:

$$\sigma_{j_i} \geq 0,\ i = 1, \ldots, w,\ \sigma_{j_i} \geq \frac{1}{|\lambda_{je_i}|^2}\left[\frac{|\lambda_{e_i}|^2}{|\lambda_{m_i}|^2} - 1\right],\ i \in S_2 \text{ and } \sum_{i=1}^{n}\sigma_{j_i} \leq P_j \tag{4.23}$$

Note that, the sub-channels with indices $i \in S_1$ do not contribute to the total secrecy rate due to the fact that those are non-degraded sub-channels. Now (4.22) is a standard convex optimization problem.

The desired solution is then associated with the optimization problem that leads to the highest secrecy rate out of the various optimization problems. We recognize that this approach to handle the non-convexity of the original problem is combinatorial in nature, so does not scale with the number non-degraded sub-channels. As an alternative we now present a sub-optimal iterative procedure in order to obtain not only the jammer but also the transmitter power allocation policies. We attempt in fact to provide an algorithm that approximates the joint power allocation policies that maximize the objective in (4.7) rather than an algorithm that approximates only the jammer power allocation policy that maximizes (4.7).

The rationale behind this procedure is to iteratively adapt the jammer and the transmitter strategies to each other. The procedure involves key steps: i) we start with a fixed transmitter strategy, e.g. isotropic power allocation where the transmitter divides the available power equally among the various sub-channels; ii) the jammer adapts its strategy to the transmitter strategy and selects a certain set of degraded (w) and non-degraded (S_2) sub-channels to distribute its available power; iii) the transmitter then adapts its strategy to the jammer strategy in ii) (the effect of the jammer strategy is in fact to create a new equivalent jammer channel); and iv) this procedure is repeated iteratively resulting in the final transmitter and jammer power allocation.

There are some important remarks to be made about this iterative procedure: First, while sub-optimal, this procedure is much more efficient than the alternative combinatorial approach and, as presented in the next section, it achieves remarkable gains when compared with other feasible approaches; Second, this procedure also builds upon a modified version of Algorithm 1 to obtain the values of $\sigma_{j_i} > 0$, for the fixed σ_{x_i}, thus inheriting its simplicity and efficiency; Third, key to the algorithm is the selection of the set of non-degraded sub-channels where the jammer injects power ($i.e., R_1$) – this is based on the amount of power that a specific non-degraded sub-channel needs to become degraded (the jammer selects the channel that needs the least amount of power, subject to its power constraint); Fourth, a very important aspect of this procedure, which plays a crucial role on its performance, is to jam only sub-channels where the transmitter also introduces power. This procedure is formally presented in Algorithm 2. Although it is not straightforward to analytically prove that this algorithm 2 always converges, we observed through extensive numerical simulations that this algorithm indeed converges (though not necessarily to the optimal solution) in a finite number of iterations.

The modified version of Algorithm 1 works as follows: The original Algorithm 1 follows from the KKT conditions associated with the power allocation optimization problem, which is convex in view of degradedness. The modified Algorithm 1 also follows from the KKT conditions associated with the optimization problem (4.22), which is also convex in view of the fact that the additional constraint $\sigma_{j_i} \geq \frac{1}{|\lambda_{je_i}|^2}\left[\frac{|\lambda_{e_i}|^2}{|\lambda_{m_i}|^2}-1\right]$ is imposed on the set of selected non-degraded sub-channels. The key modifications in Algorithm 1 are: i) in step 1 sub-channels are reordered such that the values of $a_i = \frac{\sigma_{x_i}|\lambda e_i|^2|\lambda_{je_i}|^2}{\left(1+\alpha_i|\lambda_{j_{ei}}|^2\right)\left(1+\alpha_i|\lambda_{j_{ei}}|^2+\sigma_{x_i}|\lambda e_i|^2\right)}$ are in a decreasing order; ii) in step 3 the new test condition is $\sum_{i=1}^{\widetilde{n}} b_i + \sum_{i=\widetilde{n}+1}^{n} \alpha_i \geq P_j$, and thus the value of ν is set such that $\sum_{i=1}^{\widetilde{n}} b_i + \sum_{i=\widetilde{n}+1}^{n} \alpha_i = P_j$.

4.4 Numerical results

We consider a 64×64 parallel Gaussian random wiretap channel, which is applicable to an OFDM based system, like WiFi IEEE802.11, where the complex values of the main, eavesdropper and jammer sub-channel gains are independently randomly generated according to a complex Gaussian distribution. Therefore, the system is composed of both degraded and non-degraded sub-channels.

Figure 4.2 depicts the value of the achieved secrecy rate *vs.* the jammer available power, when the transmitter available power is $P = 5$, for the following scenarios: i) the jammer and the transmitter optimize their power allocation strategies according to the proposed iterative procedure; ii) the jammer optimizes its power allocation strategy, for a fixed transmitter power allocation policy (the transmitter adopts the optimal power allocation presented in [12] for the case without the presence of the jammer), jamming only the degraded sub-channels (solution presented in Theorem 8); iii) the jammer distributes his power equally across all the degraded sub-channels; and iv) the scenario where there is no jammer present in the system. We can observe the clear benefits of jamming the eavesdropper channel.

Note that the curve in scenario i) is not smooth due to the nature of the iterative procedure that forces the jammer to sub-optimally allocate power to some sub-channels. Nonetheless, it is evident the advantage of iteratively adapting the jammer and the transmitter power allocation strategies, when compared with jamming the degraded sub-channels for a fixed transmitter power allocation policy or equally

Algorithm 2: Algorithm to compute the set of values for the transmitter and jammer power allocation strategies.

Input : Number of available sub-channels n, set of values λ_{m_i}, λ_{e_i}, λ_{je_i}, $\sigma_{x_i}, i = 1, \ldots, n$, transmitter available power P_x, jammer available power P_j and the number of iterations itr.

Output: Set of jammer power allocation policy values $\sigma_{j_i}, i = 1, \ldots, n$, set of transmitter power allocation policy values $\sigma_{x_i}, i = 1, \ldots, n$.

1 • **Re-order** the sub-channels such that the values $\alpha_i = \max\left(0, \frac{1}{|\lambda_{je_i}|^2}\left[\frac{|\lambda_{e_i}|^2}{|\lambda_{m_i}|^2} - 1\right]\right), i = 1, \ldots, n$ are in increasing order;
Set $\sigma_{x_i} = \frac{P_x}{n}, i = 1, \ldots, n$;.

2 • **Define** R_1 as the set of indices i such that $R_1 = \left\{i : \sum_{i=1}^{L} \alpha_i \leq P_j \wedge \sigma_{x_i} > 0\right\}$ (sub-channels where the jammer will put power);
Define R_2 as the set of the remaining indices i.

3 • **Set** $\sigma_{j_i} = 0, i \in R_2$; **Obtain** $\sigma_{j_i}, i \in R_1$ using a modified version of Algorithm 1 (with the additional constraint $\sigma_{j_i} \geq \frac{1}{|\lambda_{je_i}|^2}\left[\frac{|\lambda_{e_i}|^2}{|\lambda_{m_i}|^2} - 1\right]$ that guarantees convexity);
Recompute a new eavesdropper channels such that $|\lambda'_{e_i}|^2 = \frac{|\lambda_{e_i}|^2}{1+\sigma_{j_i}|\lambda_{j_{ei}}|^2}$;
Obtain $\sigma_{x_i}, i = 1, \ldots, n$, using λ_{m_i}, λ'_{e_i} and P_x (see, e.g., [12]); **Set** $itr = itr - 1$.

4 • **if** $itr > 0$ **then**
• **go to** step 2.
• **else**
• **Undo** the reordering done at step 1.

dividing the power across all the sub-channels.

Figure 4.3 shows the value of the achieved secrecy rate *vs.* the transmitter available power, when $P_j = 10$, for the same previous different scenarios. Once more we can clearly verify the impact of the jammer in the achieved secrecy rates. In fact one can observe that the secrecy rate gain, provided by the increase of the transmitter available power, starts to saturate above a certain value of P, and that the choice of the jamming strategy (especially the one obtained through the proposed iterative

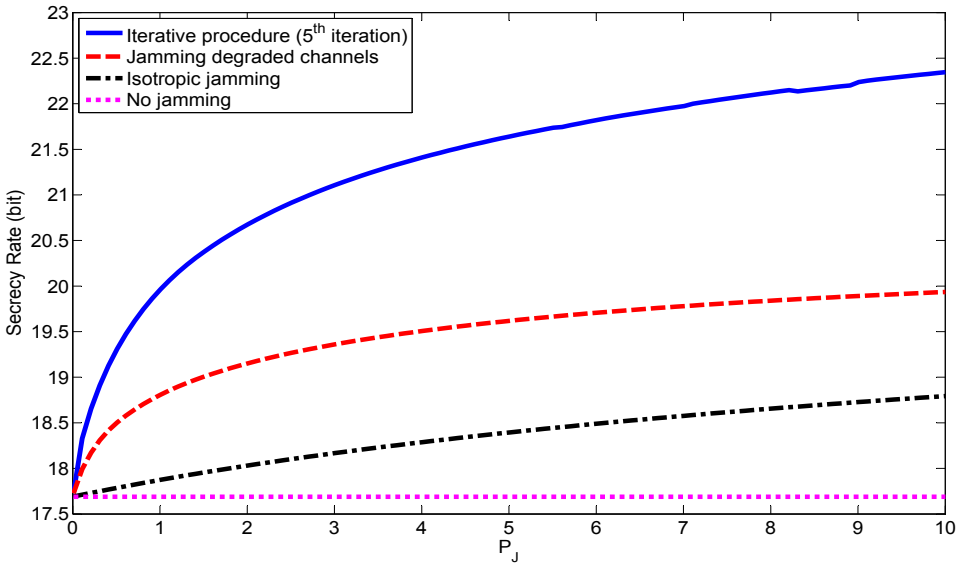

Figure 4.2: Secrecy rate *vs.* P_j, for several power allocation policies ($P = 5$).

procedure) can induce dramatic increases in the achievable secrecy rates.

Note also that the iterative procedure takes very few iterations to converge to the final solution.

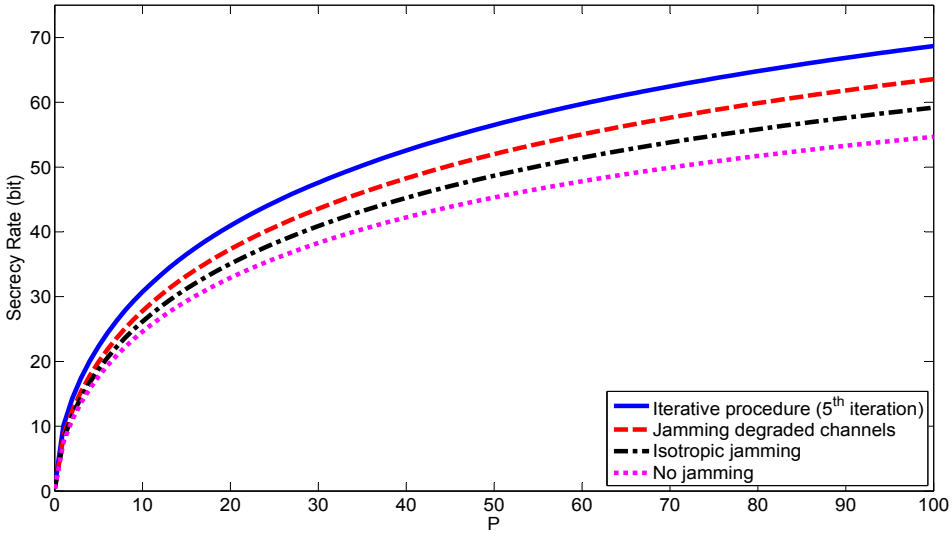

Figure 4.3: Secrecy rate *vs.* P, for several power allocation policies ($P_j = 10$).

Table 4.1 provides a summary of secrecy rates obtained under a different set of

jamming techniques in comparison to no jamming, for different numbers of sub-channels. Note that the values in the table are extracted at the jammer available power $P_j = 10$, and transmitter available power $P = 5$.

Table 4.1: Secrecy rates under a different set of jamming techniques

No of sub-channels	No jamming	Isotropic jamming	Jamming degraded channels	Iterative procedure
8	4.929	6.170	6.421	6.712
16	10.170	11.020	11.830	12.120
32	17.750	19.110	19.720	19.920

From the data provided in Table 4.1, Figure 4.4 shows the value of the achieved secrecy rate vs. number of sub-channels, when the transmitter available power is $P = 5$ and the jammer available power is $Pj = 10$, for the same previous different scenarios. Figure 4.4 illustrates the effect of different jamming techniques to the one without jamming with respect to the number of sub-channels used. It can be easily depicted how friendly jamming techniques outperform the one without jamming for the same number of sub-channels. For example, the secrecy rate obtained without jamming is 73% to 89% of the one obtained via iterative jamming, for the same number of sub-channels: 8 and 32, respectively. This bear witness that the increase of the number of sub-channels provides one robust way to increase the secrecy rate.

However, it is worth to note that for the case of no jamming, to obtain a secrecy rate similar to the one that can be obtained via one of the jamming techniques (like isotropic jamming channels), more number of sub-channels need to be used. This also follows more number of sub-channels needs to be used to obtain higher secrecy rates, via no jamming, in comparison to the ones required with jamming techniques. For example, it is clear that we can obtain a secrecy rate of approximately 6 bits by using 8 sub-channels when isotropic jamming is used, however, approximately 10 bits are obtained by using 16 sub-channels when no jamming exists. Therefore, of particular relevance is the usage of jamming techniques to the increase in the secrecy rate and to the efficient use of the channel resources at the price of some algorithmic complexity.

Figure 4.5 shows the value of the achieved secrecy rate *vs.* the transmitter available

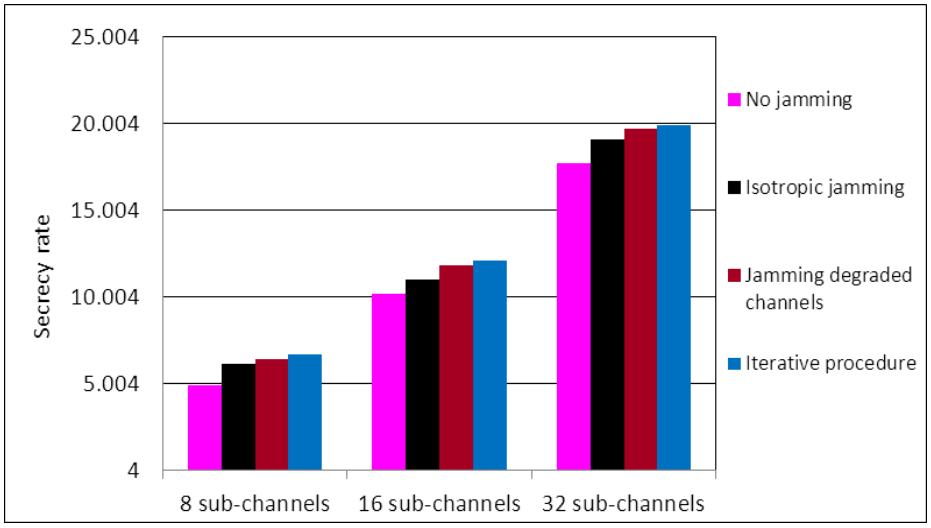

Figure 4.4: Secrecy rate *vs.* number of sub-channels, for several power allocation policies ($P_j = 10$ and $P = 5$).

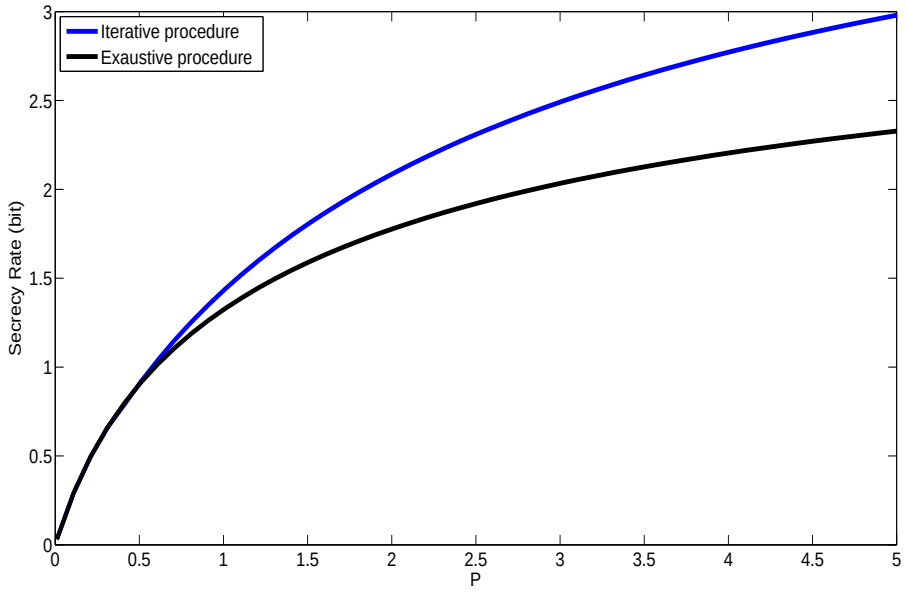

Figure 4.5: Secrecy rate *vs.* P, for proposed iterative and exaustive search procedure ($P_j = 5$).

power, when the jammer available power is $P_j = 5$, for the following scenarios: i) the jammer and the transmitter optimize their power allocation strategies according to our proposed iterative procedure; ii) the jammer optimizes its power allocation strategy, for a fixed transmitter power allocation policy (the transmitter optimizes

its power allocation, presented in [12], for the case without the presence of the jammer) according to exaustive search (Brute-force) procedure. Intuitively, Figure 4.5 demonstrates that, the secrecy rates, by using our proposed iterative procedure, is considerably higher than the secrecy rate that we receive by exaustive search process.

4.5 Conclusion

We addressed the secrecy rate gains obtained via friendly jamming. We studied a scenario where the two legitimate parties (Alice and Bob) communicate in the presence of a friendly jammer and an eavesdropper (Eve). The eavesdropper is assumed to be passive but the jammer injects interference in the eavesdropper channel in the form of additive noise. Therefore, the jammer acts as a friendly jammer who aims to help the legitimate parties to communicate with higher secrecy rates. We have studied power allocation strategies over a bank of independent parallel Gaussian wiretap channels-applicable to OFDM communications systems, where a legitimate transmitter-receiver pair communicate in the presence of an eavesdropper and a friendly jammer and all admit OFDM communication. In particular, we put forth power allocation algorithms for the jammer and joint power allocation algorithms for the jammer and the transmitter in different scenarios. Simulation results demonstrate that these algorithms can lead to significant secrecy rate gains in comparison to other power allocation approaches.

Appendix F: Proof of Theorem 8

The optimization problem of (4.10) can be expressed as,

$$\max_{\sigma_{j_i}} R_s\Big(\sigma_{x_1},\ldots,\sigma_{x_n},\sigma_{j_1},\ldots,\sigma_{j_n}\Big) = -\min_{\sigma_{j_i}} \sum_{i=1}^{n}\Big[\log\Big(1+\sigma_{x_i}\left|\lambda_{m_i}\right|^2\Big) - \log\Big(1+\frac{\sigma_{x_i}\left|\lambda_{e_i}\right|^2}{1+\sigma_{j_i}\left|\lambda_{je_i}\right|^2}\Big)\Big] \tag{4.24}$$

subject to:

$$\sum_{i=1}^{n}\sigma_{j_i} \le P_j \text{ and } \sigma_{j_i}\ge 0, i=1,\ldots,n. \tag{4.25}$$

It is straightforward to show that the first optimization problem constitutes a standard convex optimization problem with respect to σ_{j_i} and thus, the optimal solution can be characterized by KKT conditions [90], which are necessary and sufficient.

The Lagrangian of the optimization problem (4.24), subject to (4.25) is,

$$\mathcal{L}\Big(\sigma_{j_i},\nu,u_i\Big) = -R_s\Big(\sigma_{x_1},\ldots,\sigma_{x_n},\sigma_{j_1},\ldots,\sigma_{j_n}\Big) + \nu\Big(\sum_{i=1}^{n}\sigma_{j_i}-P_j\Big) - \sum_{i=1}^{n}\Big(u_i\sigma_{j_i}\Big) \tag{4.26}$$

Where $\nu\ge 0$ and $u_i\ge 0,\ i=1,\ldots,n$ are the Lagrange multipliers associated with the problem constraints.

The KKT conditions state that:

$$\nabla_{\sigma_{j_i}}\mathcal{L}\Big(\sigma_{j_i},\nu,u_i\Big)=0, i=1,\ldots,n \tag{4.27}$$

with $\nu(\sum_{i=1}^{n}\sigma_{j_i}-P_j)=0\ \ \forall\ \nu\ge 0$, and $u_i\sigma_{j_i}=0\ \ \forall\ u_i\ge 0,\ i=1,\ldots,n$

From (4.27) we have:

$$\nu-u_i = \frac{\sigma_{x_i}\left|\lambda_{ei}\right|^2\left|\lambda_{je_i}\right|^2}{\Big(1+\sigma_{j_i}\left|\lambda_{je_i}\right|^2\Big)\Big(1+\sigma_{j_i}\left|\lambda_{je_i}\right|^2+\sigma_{x_i}\left|\lambda_{ei}\right|^2\Big)} \tag{4.28}$$

Assume that $\sigma_{j_i} = 0$, which implies that means $u_i \geq 0$. Them, from (4.28) we have

$$\nu - u_i = \frac{\sigma_{x_i} |\lambda_{ei}|^2 |\lambda_{je_i}|^2}{1 + \sigma_{x_i} |\lambda_{e_i}|^2} \tag{4.29}$$

Therefore from (4.29) we have:

$$\nu - \frac{\sigma_{x_i} |\lambda_{ei}|^2 |\lambda_{je_i}|^2}{1 + \sigma_{x_i} |\lambda_{e_i}|^2} = u_i \geq 0 \tag{4.30}$$

$$\text{i.e., } \sigma_{j_i} = 0 \Rightarrow \nu \geq \frac{\sigma_{x_i} |\lambda_{ei}|^2 |\lambda_{je_i}|^2}{1 + \sigma_{x_i} |\lambda_{e_i}|^2} \tag{4.31}$$

Conversely, when $\nu \geq \frac{\sigma_{x_i}|\lambda_{ei}|^2|\lambda_{je_i}|^2}{1+\sigma_{x_i}|\lambda_{e_i}|^2}$, then from (4.28) we have:

$$\nu = \frac{\sigma_{x_i} |\lambda_{ei}|^2 |\lambda_{je_i}|^2}{(1 + \sigma_{j_i} |\lambda_{je_i}|^2)(1 + \sigma_{j_i} |\lambda_{je_i}|^2 + \sigma_{x_i} |\lambda_{ei}|^2)} + u_i \geq \frac{\sigma_{x_i} |\lambda_{ei}|^2 |\lambda_{je_i}|^2}{1 + \sigma_{x_i} |\lambda_{e_i}|^2}$$

$$\Rightarrow u_i \geq \frac{\sigma_{x_i} |\lambda_{ei}|^2 |\lambda_{je_i}|^2}{1 + \sigma_{x_i} |\lambda_{e_i}|^2} - \frac{\sigma_{x_i} |\lambda_{ei}|^2 |\lambda_{je_i}|^2}{(1 + \sigma_{j_i} |\lambda_{je_i}|^2)(1 + \sigma_{j_i} |\lambda_{je_i}|^2 + \sigma_{x_i} |\lambda_{ei}|^2)} \geq 0 \tag{4.32}$$

which implies that $\sigma_{j_i} = 0$

Thus, $\nu \geq \frac{\sigma_{x_i}|\lambda_{ei}|^2|\lambda_{je_i}|^2}{1+\sigma_{x_i}|\lambda_{e_i}|^2} \Rightarrow \sigma_{j_i} = 0$

That is, $\sigma_{j_i} = 0 \Leftrightarrow \nu \geq \frac{\sigma_{x_i}|\lambda_{ei}|^2|\lambda_{je_i}|^2}{1+\sigma_{x_i}|\lambda_{e_i}|^2}$

Assume now that $\sigma_{j_i} > 0$ which implies that $u_i = 0$. Then from (4.28) we can write,

$$\nu = \frac{\sigma_{x_i} |\lambda_{ei}|^2 |\lambda_{je_i}|^2}{\left(1 + \sigma_{j_i} |\lambda_{je_i}|^2\right)\left(1 + \sigma_{j_i} |\lambda_{je_i}|^2 + \sigma_{x_i} |\lambda_{ei}|^2\right)} < \frac{\sigma_{x_i} |\lambda_{ei}|^2 |\lambda_{je_i}|^2}{1 + \sigma_{x_i} |\lambda_{ei}|^2} \tag{4.33}$$

Thus $\sigma_{j_i} > 0 \Rightarrow \nu < \frac{\sigma_{x_i}|\lambda_{ei}|^2|\lambda_{je_i}|^2}{1+\sigma_{x_i}|\lambda_{ei}|^2}$

Conversely, when $\nu < \frac{\sigma_{x_i}|\lambda_{ei}|^2\left|\lambda_{je_i}\right|^2}{1+\sigma_{x_i}|\lambda_{ei}|^2}$, then (4.28) can be expressed as,

$$\nu = \frac{\sigma_{x_i}\left|\lambda_{ei}\right|^2\left|\lambda_{je_i}\right|^2}{\left(1+\sigma_{j_i}\left|\lambda_{je_i}\right|^2\right)\left(1+\sigma_{j_i}\left|\lambda_{je_i}\right|^2+\sigma_{x_i}\left|\lambda_{ei}\right|^2\right)} + u_i < \frac{\sigma_{x_i}\left|\lambda_{ei}\right|^2\left|\lambda_{je_i}\right|^2}{1+\sigma_{x_i}\left|\lambda_{e_i}\right|^2} \tag{4.34}$$

It is clear that we can only satisfy (4.34) with $\sigma_{j_i} > 0$. Indeed, we cannot satisfy (4.34) with $\sigma_{j_i} = 0$ because this implies that $u_i > 0$.

Thus $\nu < \frac{\sigma_{x_i}|\lambda_{ei}|^2\left|\lambda_{je_i}\right|^2}{1+\sigma_{x_i}|\lambda_{ei}|^2} \Rightarrow \sigma_{j_i} > 0$

That is, $\sigma_{j_i} > 0 \Leftrightarrow \nu < \frac{\sigma_{x_i}|\lambda_{ei}|^2\left|\lambda_{je_i}\right|^2}{1+\sigma_{x_i}|\lambda_{ei}|^2}$

From (4.33) we have:

$$\nu = \frac{\sigma_{x_i}\left|\lambda_{ei}\right|^2\left|\lambda_{je_i}\right|^2}{\left(1+\sigma_{j_i}\left|\lambda_{je_i}\right|^2\right)\left(1+\sigma_{j_i}\left|\lambda_{je_i}\right|^2+\sigma_{x_i}\left|\lambda_{ei}\right|^2\right)}$$

$$= \frac{\sigma_{x_i}\left|\lambda_{ei}\right|^2\left|\lambda_{je_i}\right|^2}{1+\sigma_{x_i}\left|\lambda_{ei}\right|^2+2\sigma_{j_i}\left|\lambda_{je_i}\right|^2+\sigma_{x_i}\sigma_{j_i}\left|\lambda_{ei}\right|^2\left|\lambda_{je_i}\right|^2+{\sigma_{j_i}}^2\left|\lambda_{je_i}\right|^4}$$

$$\Rightarrow {\sigma_{j_i}}^2\left|\lambda_{je_i}\right|^4+\sigma_{j_i}\left(2\left|\lambda_{je_i}\right|^2+\sigma_{x_i}\left|\lambda_{ei}\right|^2\left|\lambda_{je_i}\right|^2\right)$$

$$+\left(1+\sigma_{x_i}\left|\lambda_{ei}\right|^2-\frac{\sigma_{x_i}\left|\lambda_{ei}\right|^2\left|\lambda_{je_i}\right|^2}{\nu}\right)=0$$

$$\Rightarrow \sigma_{j_i} = \frac{-\left(2+\sigma_{x_i}\left|\lambda_{ei}\right|^2\right) \pm \sqrt{\sigma_{x_i}^2\left|\lambda_{ei}\right|^4+\frac{4\sigma_{x_i}|\lambda_{ei}|^2\left|\lambda_{je_i}\right|^2}{\nu}}}{2\left|\lambda_{je_i}\right|^2} \tag{4.35}$$

Since $\sigma_{j_i} > 0$, it follows that the only admissible solution is

$$\sigma_{j_i} = \frac{\sqrt{\sigma_{x_i}^2\left|\lambda_{e_i}\right|^4+\frac{4\sigma_{x_i}\left|\lambda_{e_i}\right|^2\left|\lambda_{je_i}\right|^2}{\nu}}-\left(2+\sigma_{x_i}\left|\lambda_{e_i}\right|^2\right)}{2\left|\lambda_{je_i}\right|^2} \tag{4.36}$$

Finally, for fixed Alice strategy $\sigma_{x_i}, i = 1, 2, ..., n$, the optimal Jammer strategy $\sigma_{j_i}^*$

that minimize the utility (4.24) is given by:

$$\sigma_{j_i}^{*}=\begin{cases}\dfrac{\sqrt{\sigma_{x_i}^{2}\left|\lambda_{e_i}\right|^{4}+\frac{4\sigma_{x_i}\left|\lambda_{e_i}\right|^{2}\left|\lambda_{je_i}\right|^{2}}{\nu}}-\left(2+\sigma_{x_i}\left|\lambda_{e_i}\right|^{2}\right)}{2\left|\lambda_{je_i}\right|^{2}}, & \nu<\frac{\sigma_{x_i}\left|\lambda_{e_i}\right|^{2}\left|\lambda_{je_i}\right|^{2}}{1+\sigma_{x_i}\left|\lambda_{e_i}\right|^{2}}\\ 0, & \nu\geq\frac{\sigma_{x_i}\left|\lambda_{e_i}\right|^{2}\left|\lambda_{je_i}\right|^{2}}{1+\sigma_{x_i}\left|\lambda_{e_i}\right|^{2}}\end{cases}\tag{4.37}$$

Therefore Theorem 8 has been proved.

Appendix G: Proof of Theorem 9

When $P\rightarrow 0$, this implies that $\sigma_{x_i}\rightarrow 0$, $\forall i$. Then the Taylor expansion of the objective function in (4.8) leads to:

$$R_s(\sigma_{x_i},\sigma_{j_i})=\sum_{i=1}^{n}\left[\sigma_{x_i}|\lambda_{m_i}|^{2}-\frac{\sigma_{x_i}|\lambda_{e_i}|^{2}}{1+\sigma_{j_i}\left|\lambda_{j_{e_i}}\right|^{2}}+\mathcal{O}(\sigma_{x_i}^{2})\right]\tag{4.37}$$

Therefore, the optimization problem reduces to:

$$\max_{\sigma_{j_i}}R_s\Big(\sigma_{x_i},\sigma_{j_i}\Big)=-\min_{\sigma_{j_i}}\sum_{i=1}^{n}\left[\sigma_{x_i}|\lambda_{m_i}|^{2}-\frac{\sigma_{x_i}|\lambda_{e_i}|^{2}}{1+\sigma_{j_i}\left|\lambda_{j_{e_i}}\right|^{2}}+\mathcal{O}(\sigma_{x_i}^{2})\right]\tag{4.38}$$

subject to:

$$\sum_{i=1}^{n}\sigma_{j_i}\leq P_j,\ \text{and}\ \sigma_{j_i}\geq 0,\ i=1,\ldots,n\tag{4.39}$$

The Lagrangian of the optimization problem (4.38), subject to (4.39) is:

$$\mathcal{L}(\sigma_{j_i},V,\eta_i)=-R_s(\sigma_{x_i},\sigma_{j_i})+V(\sum_{i=1}^{n}\sigma_{j_i}-P_j)-\sum_{i=1}^{n}(\eta_i\sigma_{j_i}),\ i=1,\ldots,n\tag{4.40}$$

Where $V\geq 0$, and $\eta_i\geq 0$ are the Lagrange multipliers associated with the optimization constraints.

The KKT conditions state that:

$$\nabla_{\sigma_{j_i}}\mathcal{L}(\sigma_{j_i},V,\eta_i)=0,\ i=1,\ldots,n\tag{4.41}$$

with $V(\sum_{i=1}^{n} \sigma_{j_i} - P) = 0 \ \ \forall\ V \geq 0$ and $\eta_i \sigma_{j_i} = 0 \ \ \forall\ \eta_i \geq 0,\ i = 1, \ldots, n$

From (4.41) we have:

$$V - \eta_i = \frac{\sigma_{x_i} \left|\lambda_{e_i}\right|^2 \left|\lambda_{j_{e_i}}\right|^2}{\left(1 + \sigma_{j_i} \left|\lambda_{j_{e_i}}\right|^2\right)^2} \tag{4.42}$$

Assume that $\sigma_{j_i} > 0$, which implies that $\eta_i = 0$. Therefore, from (4.42) we have

$$V = \frac{\sigma_{x_i} \left|\lambda_{e_i}\right|^2 \left|\lambda_{j_{e_i}}\right|^2}{\left(1 + \sigma_{j_i} \left|\lambda_{j_{e_i}}\right|^2\right)^2} < \sigma_{x_i} \left|\lambda_{e_i}\right|^2 \left|\lambda_{j_{e_i}}\right|^2 \tag{4.43}$$

Conversely, when $V < \sigma_{x_i} \left|\lambda_{e_i}\right|^2 \left|\lambda_{j_{e_i}}\right|^2$, then from (4.42) we have

$$V = \frac{\sigma_{x_i} \left|\lambda_{e_i}\right|^2 \left|\lambda_{j_{e_i}}\right|^2}{\left(1 + \sigma_{j_i} \left|\lambda_{j_{e_i}}\right|^2\right)^2} + \eta_i < \sigma_{x_i} \left|\lambda_{e_i}\right|^2 \left|\lambda_{j_{e_i}}\right|^2 \tag{4.44}$$

It is clear that we can only satisfy (4.44) with $\sigma_{j_i} > 0$. In deed, we cannot satisfy (4.44) with $\sigma_{j_i} = 0$ because this implies that $\eta_i > 0$.

Thus, $V < \sigma_{x_i} \left|\lambda_{e_i}\right|^2 \left|\lambda_{j_{e_i}}\right|^2 \Rightarrow \sigma_{j_i} > 0$

That is, $\sigma_{j_i} > 0 \Leftrightarrow V < \sigma_{x_i} \left|\lambda_{e_i}\right|^2 \left|\lambda_{j_{e_i}}\right|^2$

On the other hand, assume now that $\sigma_{j_i} = 0$, which implies that $\eta_i \geq 0$ Therefore, from (4.42) we have that

$$V \geq \sigma_{x_i} \left|\lambda_{e_i}\right|^2 \left|\lambda_{j_{e_i}}\right|^2 \tag{4.45}$$

Conversely, when $V \geq \sigma_{x_i} \left|\lambda_{e_i}\right|^2 \left|\lambda_{j_{e_i}}\right|^2$, then from (4.42) we have,

$$V = \frac{\sigma_{x_i} \left|\lambda_{e_i}\right|^2 \left|\lambda_{j_{e_i}}\right|^2}{\left(1 + \sigma_{j_i} \left|\lambda_{j_{e_i}}\right|^2\right)^2} + \eta_i \geq \sigma_{x_i} \left|\lambda_{e_i}\right|^2 \left|\lambda_{j_{e_i}}\right|^2$$

$$\Rightarrow \eta_i \geq \sigma_{x_i} \left|\lambda_{e_i}\right|^2 \left|\lambda_{j_{e_i}}\right|^2 - \frac{\sigma_{x_i} \left|\lambda_{e_i}\right|^2 \left|\lambda_{j_{e_i}}\right|^2}{\left(1 + \sigma_{j_i} \left|\lambda_{j_{e_i}}\right|^2\right)^2} \geq 0 \tag{4.46}$$

which implies that $\sigma_{j_i} = 0$.

Thus, $V \geq \sigma_{x_i} |\lambda_{e_i}|^2 \left|\lambda_{j_{e_i}}\right|^2 \Rightarrow \sigma_{j_i} = 0$

That is, $\sigma_{j_i} = 0 \Leftrightarrow V \geq \sigma_{x_i} |\lambda_{e_i}|^2 \left|\lambda_{j_{e_i}}\right|^2$

Now from (4.43) we have:

$$V = \frac{\sigma_{x_i} |\lambda_{e_i}|^2 \left|\lambda_{j_{e_i}}\right|^2}{\left(1 + \sigma_{j_i} \left|\lambda_{j_{e_i}}\right|^2\right)^2}$$

$$\Rightarrow 1 + \sigma_{j_i} \left|\lambda_{j_{e_i}}\right|^2 = \pm\sqrt{\frac{\sigma_{x_i} |\lambda_{e_i}|^2 \left|\lambda_{j_{e_i}}\right|^2}{V}}$$

$$\Rightarrow \sigma_{j_i} = \frac{\sqrt{\frac{\sigma_{x_i}\left|\lambda_{e_i}\right|^2\left|\lambda_{j_{e_i}}\right|^2}{V}} - 1}{\left|\lambda_{j_{e_i}}\right|^2}, \text{ since } \sigma_{j_i} > 0 \tag{4.47}$$

So, when $P \to 0$ and the transmitter power allocation is fixed. Then the jammer optimal power allocation policy that maximizes the secrecy rate is given by:

$$\sigma_{j_i}^* = \begin{cases} \frac{\sqrt{\frac{\sigma_{x_i}|\lambda_{e_i}|^2\left|\lambda_{je_i}\right|^2}{V}}-1}{\left|\lambda_{je_i}\right|^2}, & V < \sigma_{x_i}|\lambda_{e_i}|^2|\lambda_{je_i}|^2 \\ 0, & V \geq \sigma_{x_i}|\lambda_{e_i}|^2|\lambda_{je_i}|^2 \end{cases} \tag{4.48}$$

Therefore Theorem 9 has been proved.

Appendix H: Proof of Theorem 10

When $P_j \to 0$, this implies that $\sigma_{j_i} \to 0$, $i = 1, \ldots, n$. Then the Taylor expansion of the objective function in (4.8) is as follows:

$$R_s(\sigma_{x_i}, \sigma_{j_i}) = \sum_{i=1}^{n} \left[\frac{\sigma_{x_i}\sigma_{j_i}|\lambda_{e_i}|^2\left|\lambda_{j_{e_i}}\right|^2}{1 + \sigma_{x_i}|\lambda_{e_i}|^2} + \mathcal{O}(\sigma_{j_i}^2)\right] \tag{4.49}$$

The optimization problem then becomes:

$$\max_{\sigma_{j_i}} R_s(\sigma_{x_i}, \sigma_{j_i}) = -\min_{\sigma_{j_i}} \sum_{i=1}^{n} \left[\frac{\sigma_{x_i}\sigma_{j_i}|\lambda_{e_i}|^2 \left|\lambda_{j_{e_i}}\right|^2}{1+\sigma_{x_i}|\lambda_{e_i}|^2} + \mathcal{O}(\sigma_{j_i}^2) \right] \tag{4.50}$$

subject to:

$$\sum_{i=1}^{n} \sigma_{j_i} \leq P_j, \text{ and } \sigma_{j_i} \geq 0, \ i = 1, \ldots, n \tag{4.51}$$

The Lagrangian of the optimization problem in (4.50) and (4.51) is:

$$\mathcal{L}\Big(\sigma_{j_i}, \nu, u_i\Big) = -R_s\Big(\sigma_{x_i}, \sigma_{j_i}\Big) + \nu\Big(\sum_{i=1}^{n} \sigma_{j_i} - P_j\Big) - \sum_{i=1}^{n} \Big(u_i \sigma_{j_i}\Big) \tag{4.52}$$

Where $\nu \geq 0$, and $u_i \geq 0, \ i = 1, \ldots, n$ are the Lagrenge multipliers associated with the problem constraints.

The KKT conditions state that:

$$\nabla_{\sigma_{j_i}} \mathcal{L}(\sigma_{j_i}, \nu, u_i) = 0, \ i = 1, \ldots, n \tag{4.53}$$

with $\nu(\sum_{i=1}^{n} \sigma_{j_i} - P_j) = 0 \ \ \forall \ \nu \geq 0$ and $u_i \sigma_{j_i} = 0 \ \ \forall \ u_i \geq 0, \ i = 1, \ldots, n$

From (4.53) we have:

$$\nu - u_i = \frac{\sigma_{x_i} |\lambda_{e_i}|^2 \left|\lambda_{j_{e_i}}\right|^2}{1+\sigma_{x_i} |\lambda_{e_i}|^2} \tag{4.54}$$

In view of the form of (4.54), when $P_j \to 0$, it is simple to infer that the jammer puts all its power in the strongest sub-channel and the strongest sub-channel is determined by the index k, where

$$k = \arg\max_i \left[\frac{\sigma_{x_i} |\lambda_{e_i}|^2 \left|\lambda_{j_{e_i}}\right|^2}{1+\sigma_{x_i} |\lambda_{e_i}|^2} \right] \tag{4.55}$$

So, when $P_j \to 0$, then the jammer´s optimal power is:

$$\sigma_{j_i}^* = \begin{cases} P_j, & i = k \\ \\ 0, & i \neq k \end{cases} \tag{4.56}$$

Therefore Theorem 10 has been proved.

Chapter 5
Achievable Average Secrecy Rates over a Bank of Parallel Independent Fading Channels with Friendly Jamming: A Case Study

5.1 Introduction

In this Chapter we evaluate the performance of the friendly jamming strategy over a bank of parallel independent fading wiretap channel: the objective is to capitalize on the algorithms put forth in previous chapters in order to assess the improvements in secrecy rate brought about by the use of friendly jamming.

Fading phenomena has been a problem of long standing interest to information theorists. The growing demand for wireless communications makes it important to determine the capacity limits of fading channels. Many works have been done to assess the information theoretic limits of Gaussian fading channels in [93, 94, 95, 96, 97, 98].

The flat-fading channel with channel-state information available to both receiver and transmitter is examined in [99] and [100]. Authors in [94] obtain capacity of a single-user fading channel with channel side information at the transmitter and receiver, and at the receiver alone. In [101], it is shown that the use of multiple antennas increase the achievable rates on fading channels if the channel parameters can be estimated at the receiver and if the path gain between different antenna pairs behave independently. The secrecy capacity of the slow fading channel was characterized in [13] and one of the interesting results is that, a non-zero perfectly

secure rate is achievable in the fading channel even when the eavesdropper is more capable than the legitimate receiver. In [10], two legitimate partners communicate over a quasi-static fading channel and an eavesdropper observes their transmission through another independent quasi-static fading channel. The authors in [10] defined the secrecy capacity in terms of outage probability and provide a complete characterization of the maximum transmission rate at which the eavesdropper is unable to decode any information.

In this Chapter, it is assumed that two legitimate parties (Alice and Bob) communicate in the presence of a friendly jammer and an eavesdropper (Eve) over Rayleigh or Rician fading channels. It is also assumed that the eavesdropper is passive whereas the jammer injects interference in the eavesdropper channel in the form of additive noise. We consider transmissions over a bank of parallel fading channels so that the results are also applicable to orthogonal frequency division multiplexing (OFDM) systems. By assuming that the friendly jammer adopts particular power allocation policies, the goal of the work is to evaluate average secrecy rates that can be achieved over Rayleigh or Rician fading , with independent or correlated sub-channels.

This Chapter is organized as follows: In Section 5.2, we present the system model and the problem formulation. Section 5.3 presents a brief description of fading models for wireless communications. The gain in secrecy rates caused by the presence of a friendly jammer for both cases when sub-channels are independent and correlated is described in section 5.4. In Section 5.5, numerical results describe the tradeoff between transmitter and jamming power under a total power constraint. In Section 5.6, we summarize the main contributions of this Chapter.

5.2 Problem formulation

We consider communications over a bank of parallel fading channels where a legitimate user, Alice, tries to communicate with another legitimate user, Bob, in the presence of an eavesdropper and a friendly jammer that interferes only with the eavesdropper channel (see Figure 5.1). Note that this represents a simplification of typical wireless communications systems where, due to the characteristics of wireless propagation, the jammer would introduce interference in both the main and the

eavesdropper channels. The justification for the validity of such assumptions has already been put forth in Chapters 3 and 4.

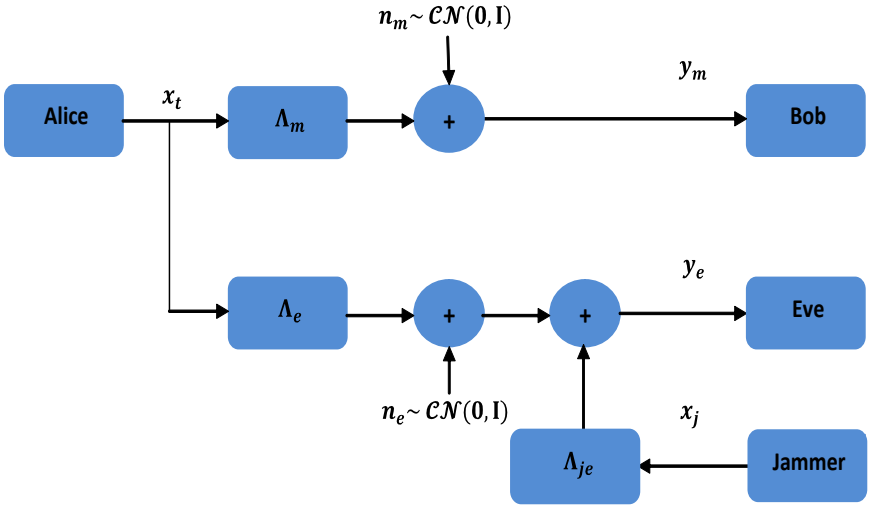

Figure 5.1: Parallel Gaussian wiretap channel model with a friendly jammer.

We assume that Alice wishes to convey to Bob the vector of symbols $\mathbf{x}_t(l) \in \mathbb{C}^n$ at time l, where n represents the number of parallel sub-channels. The output of the main channel at time l is represented as:

$$\mathbf{y}_m(l) = \mathbf{\Lambda}_m(l)\mathbf{x}_t(l) + \mathbf{n}_m(l) \tag{5.1}$$

and the output of the eavesdropper channel at time l is represented as:

$$\mathbf{y}_e(l) = \mathbf{\Lambda}_e(l)\mathbf{x}_t(l) + \mathbf{n}_e(l) + \mathbf{\Lambda}_{j_e}(l)\mathbf{x}_j(l), \tag{5.2}$$

where $\mathbf{y}_m(l) \in \mathbb{C}^n$ and $\mathbf{y}_e(l) \in \mathbb{C}^n$ represent the vectors of complex received symbols at the output of the main and eavesdropper channels, respectively, $\mathbf{n}_m(l) \in \mathbb{C}^n$ and $\mathbf{n}_e(l) \in \mathbb{C}^n$ are independent and identically distributed (i.i.d.) circularly symmetric complex Gaussian random vectors with zero mean and identity covariance matrix and:

$$\mathbf{\Lambda}_m(l) = \text{diag}\left(\lambda_{m_1}(l), \lambda_{m_2}(l), \ldots, \lambda_{m_n}(l)\right) \tag{5.3}$$

$$\mathbf{\Lambda}_e(l) = \text{diag}\left(\lambda_{e_1}(l), \lambda_{e_2}(l), \ldots, \lambda_{e_n}(l)\right) \tag{5.4}$$

$$\mathbf{\Lambda}_{je}(l) = \text{diag}\left(\lambda_{je_1}(l), \lambda_{je_2}(l), \ldots, \lambda_{je_n}(l)\right) \tag{5.5}$$

i.e., $\mathbf{\Lambda}_m(l), \mathbf{\Lambda}_e(l), \mathbf{\Lambda}_{je}(l) \in \mathbb{C}^{n\times n}$ are diagonal matrices that contain the complex gains of the parallel sub-channels associated with the main, eavesdropper and jammer channels, respectively.

We take the main sub-channels, the eavesdropper sub-channels and the jammer sub-channels to be quasi-static fading, so that $\mathbf{\Lambda}_m(l), \mathbf{\Lambda}_e(l)$ and $\mathbf{\Lambda}_{je}(l)$ remain fixed during the entire transmission frame $l = 1, 2, ..., M$. Therefore, we omit the time index l for simplicity in the sequel. We also take the sub-channel fading coefficients in the main, eavesdropper and jammer channels to be particular realizations of Rayleigh or Rician channels. In addition, as in previous Chapters, we assume that the exact channel state is known to the transmitter, the receiver, the eavesdropper and the jammer.

The objective of this work is to evaluate the achievable average secrecy rate over a bank of parallel fading channels in the presence of friendly jamming under the different fading regimes. We assume that the transmitter and the friendly jammer send independent zero-mean Gaussian symbols over the different sub-channels, so that $\mathbf{\Sigma}_x = \mathbb{E}[\mathbf{x}_t\mathbf{x}_t^\dagger] = \text{diag}(\sigma_{x_1}, \ldots, \sigma_{x_n})$ and $\mathbf{\Sigma}_j = \mathbb{E}[\mathbf{x}_j\mathbf{x}_j^\dagger] = \text{diag}(\sigma_{j_1}, \ldots, \sigma_{j_n})$ where σ_{x_i} is the power of the data-bearing signal transmitted on the i-th sub-channel and σ_{j_i} is the power of the jamming signal introduced on the i-th sub-channel, and we assume that the transmitter and the jammer satisfy the power constraints $\sum_{i=1}^n \sigma_{x_i} \leq P$ and $\sum_{i=1}^n \sigma_{j_i} \leq P_j$, respectively. An achievable average secrecy rate in this scenario is given by:

$$\bar{R}_s = \mathbb{E}\left[\max_{\sigma_{j_i}} R_s\Big(\sigma_{j_1} \ldots \sigma_{j_n}\Big)\right], \tag{5.6}$$

where the expectation is with respect to the fading statistics of the sub-channels and

$$R_s(\sigma_{j_1} \ldots \sigma_{j_n}) = \sum_{i=1}^{n}\left[\log\left(1+\sigma_{x_i}\left|\lambda_{m_i}\right|^2\right) - \log\left(1+\frac{\sigma_{x_i}\left|\lambda_{e_i}\right|^2}{1+\sigma_{j_i}\left|\lambda_{je_i}\right|^2}\right)\right]^+ \tag{5.7}$$

with $[z]^+ = \max(0, z)$.

Note that, the friendly jammer power allocation policy that maximizes the achievable secrecy rate in (5.7) for fixed channel realizations has been solved in Chapter 4 under a total jammer power constraints (see also [102, 103]).

In particular, recall that we have posed the optimization problem:

$$\max_{\sigma_{j_i}, i=1,..,n} R_s\Big(\sigma_{j_1} \dots \sigma_{j_n}\Big) \tag{5.8}$$

subject to the constraints:

$$\sum_{i=1}^{n} \sigma_{j_i} \leq P_j, \text{ and } \sigma_{j_i} \geq 0, i = 1, \dots, n \tag{5.9}$$

This work capitalizes on such a characterization of the optimal jammer power allocation policy to study the achievable average secrecy rate in (5.6) under different fading scenarios.

5.3 Fading environment

The wireless channel environment governs the performance of wireless communication systems and 'fading' is a unique characteristic in a wireless channel. In general, the wireless environment for any wireless channel in either an indoor or outdoor scenario may be subject to LOS or NLOS transmission [104]. Figure 5.2 illustrates the difference between LOS and NLOS.

The received signal distribution in a LOS environment typically follows a Rician distribution, while that in the NLOS environment follows the Rayleigh distribution. In Rayleigh fading, there is no dominant component to the scatter (LOS), so such process has zero mean. Rician fading occurs when one of the paths, typically a LOS, is much stronger than the others, so that the mean of the random process will no longer be zero, varying instead around the power-level of the dominant path. The received signal in the propagation environment for a wireless channel can be considered as the sum of the received signals from an infinite number of scatters which can be represented by a Gaussian random variable due to the central limit theorem [104]. This justifies the modelling assumptions invoked in the sequel.

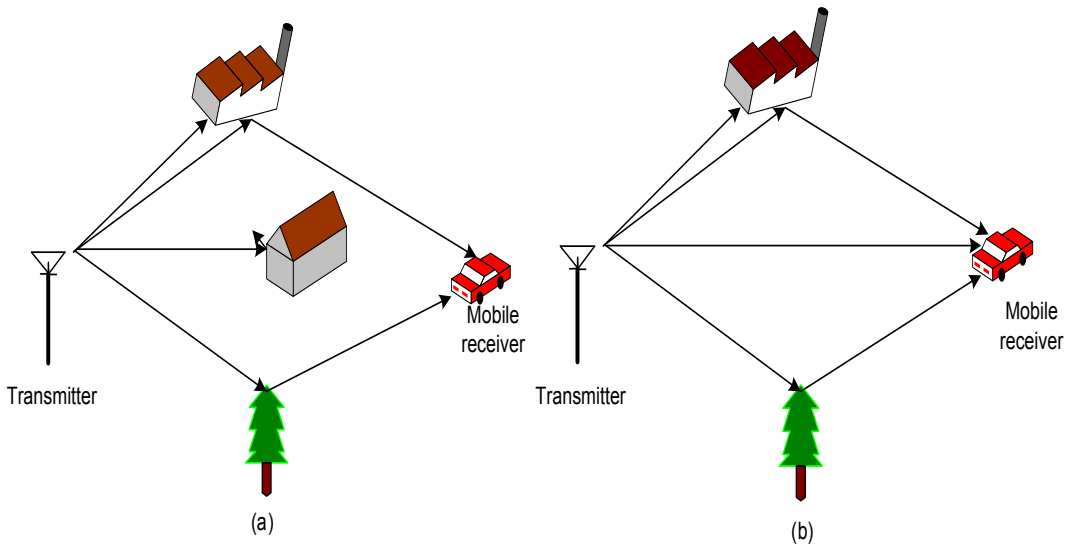

Figure 5.2: (a)Non light of sight environment (b) Light of sight environment.

5.4 Effect of a friendly jammer on the secrecy gain with Rayleigh and Rician fading

In this section, we study the effect of a friendly jammer on the secrecy gain with Rayleigh and Rician fading. We characterize the achievable average secrecy rate in the scenarios where:

1. the jammer sub-channels are Rayleigh, such that λ_{je_i} are zero-mean complex Gaussian variables, i.e., $\lambda_{je_i} \sim \mathcal{CN}(0, \tau_{je}), i = 1, \ldots, n$, where $\tau_{je} = \mathbb{E}[|\lambda_{je_i}|^2]$ is the average power gain of the various jammer sub-channels;
2. the jammer sub-channels are Rician, so that $\lambda_{je_i} \sim \mathcal{CN}\left(\sqrt{\frac{K\tau_{je}}{1+K}}, \frac{\tau_{je}}{1+K}\right), i = 1, ..., n$, where $\tau_{je} = \mathbb{E}[|\lambda_{je_i}|^2]$ is the average power gain of the various jammer sub-channels.

The main and the eavesdropper sub-channels are all assumed to be Rayleigh so that

$$\lambda_{m_i} \sim \mathcal{CN}(0, \tau_m), \ i = 1, \ldots, n \tag{5.10}$$

where $\tau_m = \mathbb{E}[|\lambda_{m_i}|^2]$ and

$$\lambda_{e_i} \sim \mathcal{CN}(0, \tau_e), \ i = 1, \ldots, n \tag{5.11}$$

where $\tau_e = \mathbb{E}[|\lambda_{e_i}|^2]$.

We also characterize the achievable average secrecy rate in scenarios where:

1. the fading across the sub-channels are independent, so that the complex Gaussian random variables corresponding to gains of different main, eavesdropper and jammer sub-channels are independent;
2. the fading across the sub-channels are correlated, so that the complex Gaussian random variables corresponding to gains of different main, eavesdropper and jammer sub-channels are correlated.

5.4.1 Sub-channels correlation

We model correlation across sub-channels by considering OFDM transmissions where the duration of the CP is a fraction μ of the OFDM symbol duration nT_s, over a frequency selective (dispersive) channel with exponentially decaying PDP, where, a block is modeled with n serial data symbols, each of duration T_s. We denote by $h(mT_s)$, $m = 0, 1, \ldots, L-1$, the time domain CIR of the time dispersive (frequency selective) channel. We assume that - by proper system design - the length of LT_s of the CIR is $LT_s \leq \mu n T_s$, the OFDM system becomes equivalent to n flat fading parallel channels with gains that are given by the n-size Fourier transform of the samples of the CIR, that is the channel frequency response [50], namely:

$$g(kF) = \frac{1}{\sqrt{n}} \sum_{m=0}^{L-1} h(mT_s) e^{-j2\pi m T_s k F} = \frac{1}{\sqrt{n}} \sum_{m=0}^{L-1} h(mT_s) e^{-j2\pi mk/n}, \qquad k = 0, \ldots, n-1. \tag{5.12}$$

where the channel frequency F equals to k/n cycles per sample.

Note that, we have used the multiplying factor $\frac{1}{\sqrt{n}}$ so that $h(mT_s)$ and $g(kF)$ have the same energy.

Consider the fact that the CIR is a random quantity and, in particularl, each value $h(mT_s)$ for $m = 0, \ldots, L-1$ is a complex random variable that is associated with a particular reflection of the transmitted signal. Assume that the different random variables $h(mT_s)$ are independent, complex Gaussian random variables with zero mean and different variances, $\mathbb{E}[|h(mT_s)|^2] = PDP(m), \quad m = 0, \ldots, L-1$. We call the function $PDP(m)$ the power delay profile of the channel.

Then, the statistical power of the independent gains corresponding to the L different paths in the CIR is given by [105]:

$$PDP(m) = \beta e^{-\frac{m}{\alpha}}, m = 0, \ldots, L-1, \tag{5.13}$$

where, $\alpha, \beta > 0$ determine the decay rate and average power gain of the channel respectively.

By expressing the relationship between the CIR $h(mT_s)$ and the frequency response $g(kF)$ in matrix form, it is possible to determine the correlation among the sub-channel gains $g(kF)$ in terms of PDP. In particular, we collect the samples of the CIR in $n \times 1$ column vector as:

$$\mathbf{h} = \begin{bmatrix} h(0) \\ h(T_s) \\ \vdots \\ h((L-1)T_s) \\ 0 \\ \vdots \\ 0 \end{bmatrix} \tag{5.14}$$

and the samples of the channel frequency response in the $n \times 1$ column vector as:

$$\mathbf{g} = \begin{bmatrix} g(0) \\ g(F) \\ \vdots \\ \vdots \\ g((n-1)F) \end{bmatrix} \tag{5.15}$$

The relationship between $\mathbf{g}$ and $\mathbf{h}$ can now be expressed as follows

$$\mathbf{g} = \mathbf{F}\mathbf{h} \tag{5.16}$$

in which, $\mathbf{F}$ is n-size Fourier matrix whose entry in the k-th row, m-th column is $[F]_{km} = \frac{1}{\sqrt{n}} e^{-j2\pi(k-1)(m-1)/n}$. Then the covariance matrix of the sub-channel gains will be simply given by:

$$\mathbf{\Sigma}_g = \mathbb{E}[\mathbf{g}\mathbf{g}^\dagger] = \mathbf{F}\mathbf{\Sigma}_\mathbf{h}\mathbf{F}^\dagger, \tag{5.17}$$

where

$$\mathbf{\Sigma}_h = \mathbb{E}[\mathbf{h}\mathbf{h}^\dagger] = \text{diag}(PDP(0), \ldots, PDP(L-1), 0, \ldots, 0) \tag{5.18}$$

So it is possible to retrieve directly from (5.17) the correlation between any two sub-channel gains.

In the following sections we will analyze the effect of friendly jamming under Rayleigh and Rician fading. We consider a 64×64 parallel fading wiretap channel with $\mu = \frac{1}{4}$, $L = 13$, $\alpha = 2$ and β is chosen according to the average power gain of the channel. Therefore, the duration of the CP which is equal to 16 T_s is larger than the duration of the CIR which is equal to 13 T_s, so that ISI and ICI do not arise.

5.4.2 Achievable average secrecy rates over Rayleigh fading

We now consider the gain in the achievable secrecy rates due to the presence of a friendly jammer, for the case where sub-channels are independent and Rayleigh fading.

Figure 5.3 shows the value of the achieved average secrecy rate vs. the transmitter available power P when the various sub-channels are subject to independent Rayleigh fading. In particular, we set $P_j = 5$ and the average power gains of the main, eavesdropper and jammer channels to be the same, i.e., $\tau_m = \tau_e = \tau_{je} = 1$. We consider three different power allocation policies. In particular, we analyze the scenario where, i) the transmitter adopts the power allocation scheme that achieves the secrecy capacity without the presence of a friendly jammer for each sub-channels realizations [83]; ii) the jammer distributes its power equally across all the sub-channels; and iii) the jammer and the transmitter optimize their power allocation policies according to the proposed iterative procedure (Algorithm 2, Chapter 4) to maximize the secrecy rate for each sub-channels realizations. We can clearly observe the increase in the achievable average secrecy rates due to the presence of the friendly jammer.

Figure 5.4 shows the average secrecy rate obtained over independent and correlated Rayleigh fading channels vs. the transmitter available power P. We also set $P_j = 5$ and consider the cases where: (i) the jammer and the transmitter optimize their power allocation policies according to the proposed iterative way (Algorithm 2,

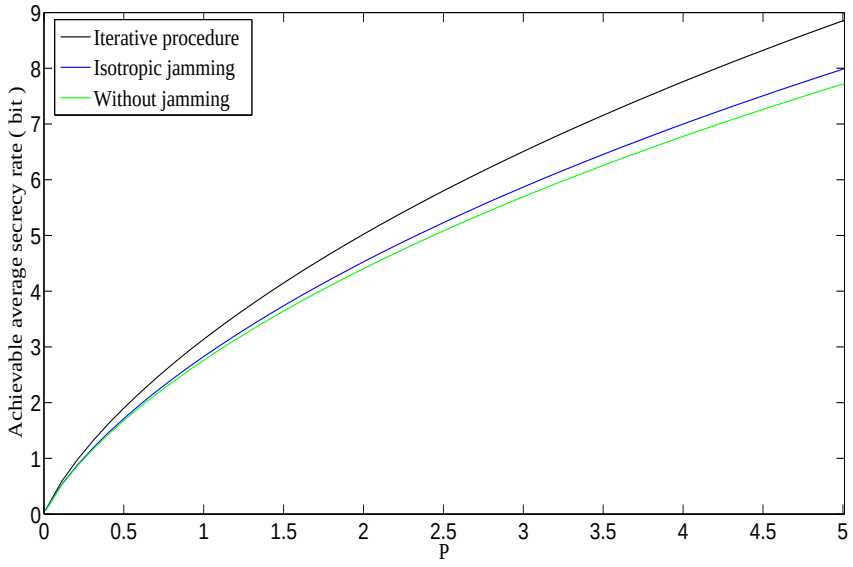

Figure 5.3: Achievable average secrecy rate $\bar{R}_s$ *vs.* P for $P_j = 5$, when the transmitter, eavesdropper and jammer channel are subject to independent Rayleigh fading for the different power allocation strategies. $\tau_m = \tau_e = \tau_{je} = 1$.

Chapter 4) and (ii) the transmitter optimize its power allocation policy assuming equal jammer power allocation for each sub-channels in order to maximize the secrecy rate for each sub-channels realizations. We consider three different channel configurations, corresponding to different relations between the average power gain of the main, eavesdropper and jammer channels which are: a) the transmitter average power gain is 15 times larger than the eavesdropper and the jammer average power gains, i.e., $\tau_m = 15$, $\tau_e = 1$ and $\tau_{je} = 1$; b) the transmitter, eavesdropper and jammer average power gains are same, i.e., $\tau_m = \tau_e = \tau_{je} = 1$; and c) the eavesdropper average power gain is 15 times larger than the transmitter and the jammer average power gain, i.e., $\tau_e = 15$, $\tau_m = 1$ and $\tau_{je} = 1$.

We observe, in Figure 5.4, that the achieved average secrecy rate obtained with correlated sub-channels is less than the achieved average secrecy rate for the case of independent sub-channels. This fact can be explained by noting that independent sub-channels provide a higher level of diversity to be exploited to guarantee favorable channel realizations for the legitimate receiver. It turns out that the relative loss due to the presence of sub-channels correlation is higher when the eavesdropper channel average power gain is much better than the main channel average power gain (see in Figure 5.4:(c)).

5.4.3 Achievable average secrecy rates over Rician fading

We consider the gain in the achievable secrecy rates due to the presence of a line-of-sight channel for the jammer, for both the cases when sub-channels are independent and correlated.

Figure 5.5 and Figure 5.6 also show the value of the achieved average secrecy rate vs. the transmitter available power P when the various sub-channels are subject to independent or correlated fading, the main and eavesdropper sub-channels are subject to Rayleigh fading, and the jammer sub-channels are subject to Rayleigh or Rician fading. We also set $P_j = 5$ and consider the cases where: i) the jammer and the transmitter optimize their power allocation policies according to the proposed iterative algorithm (Algorithm 2, Chapter 4) and (ii) the transmitter optimizes its power allocation strategy assuming equal jammer power allocation for each sub-channels in order to maximize the secrecy rate for each sub-channels realizations. We also consider the previous channel configurations corresponding to the different relations between the average power gain of the main, eavesdropper and jammer channel, which are: a) $\tau_m = 15$, $\tau_e = 1$ and $\tau_{je} = 1$; b) $\tau_m = \tau_e = \tau_{je} = 1$; and c) $\tau_e = 15$, $\tau_m = 1$ and $\tau_{je} = 1$.

Figure 5.5 depicts the case in which sub-channels are independent, whereas in Figure 5.6 sub-channels are correlated. In both cases, it is clear that the gain of the achievable secrecy rates is higher when the friendly jammer channel is Rician than when the friendly jammer channel is Rayleigh. This result relates to the fact that the jammer can benefit from the LOS component present in the Rician fading model to impair the eavesdropper in a more efficient manner. It is also clear that the relative loss due to the presence of sub-channels correlation is higher when the eavesdropper channel average power gain is much better than the main channel average power gain.

5.5 Fixed total power budget

It is also interesting to analyze the scenario where there is a fixed power budget to be distributed between the transmitter and the jammer. This could have various implications for wireless network operators that intend to use jammers to augment

the security of their network, but yet have a certain budget power to be shared between the transmitter (e.g. a base station) and the deployed jammers.

We analyze numerical results for the case of Rayleigh and Rician fading with independent sub-channels[6], with a total power budget of 5 to be distributed between the transmitter and the jammer (i.e., $P_j = 5 - P$). We restrict the analysis to the case where the transmitter uses the power allocation policy that maximizes the instantaneous secrecy capacity for each sub-channels realizations (see [83]) whereas the jammer uses the power allocation policy embodied in the optimization problem in (5.8) also for each sub-channels realizations.

The fraction of power devoted to data transmission and the one for jamming are determined in order to maximize the achievable average secrecy rate. This way, we want to provide some insight on which amount of the total available power should be devoted to the friendly jammer for the different channel scenarios under consideration.

Figure 5.7, Figure 5.8, Figure 5.9 and Figure 5.10 show the optimal value of the power that should be allocated to the transmitter considering different relations between the average power gain of the main and eavesdropper sub-channels, for various average power gains of the jammer sub-channels: in Figure 5.7 and Figure 5.8, the average power gains of the main and the eavesdropper sub-channels are equal, i.e., $\tau_m = \tau_e$; whereas in Figure 5.9 and Figure 5.10, the average power gains of the main sub-channels are 15 times higher than those of the eavesdropper channel, i.e., $\tau_m = 15\ \tau_e$. For both cases the main and the eavesdropper sub-channels are subject to Rayleigh fading, and the jammer sub-channels are subject to either Rayleigh or Rician fading . We also consider the case where the average power gains of the eavesdropper sub-channels are 15 times higher than those of the main sub-channels, i.e., $\tau_e = 15\ \tau_m$. But since in this case, higher fraction of the available power of the jammer is allocated to the eavesdropper channel to decrease the eavesdropper channel quality, the secrecy rate is not sufficiently increase and for this reason, we did not put any figure related this case.

It is clear that, when the transmitter / eavesdropper average power gain is low, there is less opportunity to effectively jam the eavesdropper: in fact, we can observe a

[6]Numerical results with correlated sub-channels show the same trends that are observed in the case of independent Rayleigh and Rician fading.

phase transition point that determines whether or not it is relevant to allocate any power for the jammer to jam the eavesdropper. In contrast, when the average power gain of the transmitter / eavesdropper is higher, we should allocate more power to the jammer in order to increase the secrecy rate. It is possible to observe identical trends in both cases when the average power gains at the main and eavesdropper channels are balanced or when the main channel enjoys a clear advantage. As expected, in this last case, a higher fraction of the available power is allocated to the transmitter, because further decreasing the quality of the eavesdropper channel via jamming does not result in a significant increase of the secrecy rate.

To conclude, when the transmitter channel average power gain is higher than the eavesdropper channel average power gain, the transmitter can leverage its advantage over the eavesdropper to obtain a positive average secrecy rate. On the other hand, when the eavesdropper channel average power gain is higher than the transmitter channel average power gain, positive secrecy rates are obtained with the help of friendly jamming.

5.6 Conclusion

We have studied the performance of transmitter / jammer power allocation strategies for secure communication over a bank of parallel, quasi-static fading channels in the presence of an eavesdropper and a friendly jammer. We characterized the effect of the optimal jammer power allocation policy, for any fixed transmitter power allocation policy over Rayleigh or Rician fading scenarios. The results demonstrate the increase in the average achievable secrecy rate obtained with friendly jamming. The achieved average secrecy rate is higher for independent sub-channels than when sub-channels are correlated. On the other hand, higher secrecy rates can be achieved when the channel from the friendly jammer to the eavesdropper is Rician with respect to the case of Rayleigh fading. We have also highlighted the loss due to correlation among the sub-channels in different fading scenarios: correlation has the most detrimental effect when the eavesdropper enjoys better channel conditions than the legitimate parties. We also investigated the distribution of power between the transmitter and the jammer, when there is a fixed total power budget. Overall, these results showcase the efficacy of friendly jamming for OFDM type of communications systems in various operating regimes.

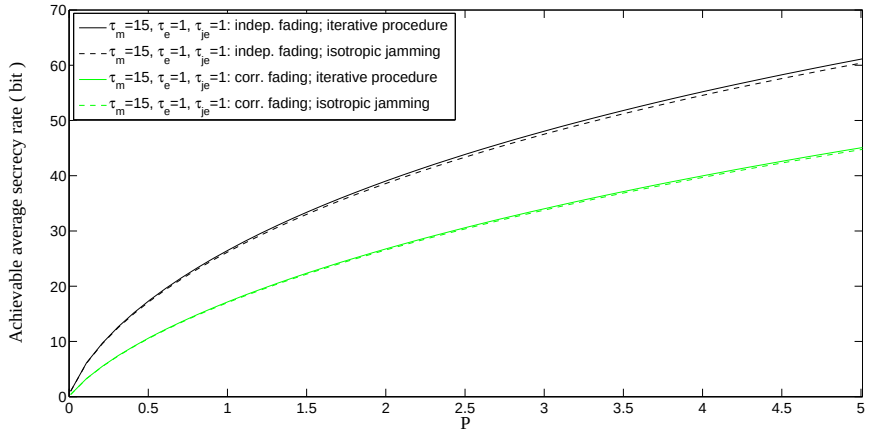

Figure 5.4: (a)

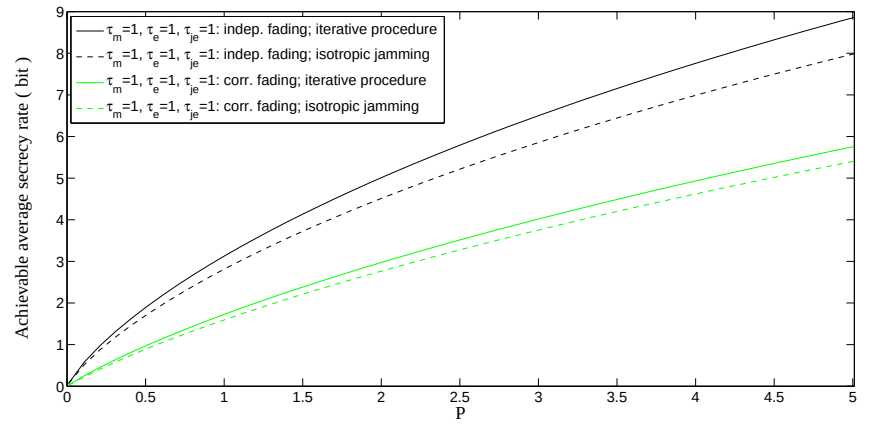

Figure 5.4: (b)

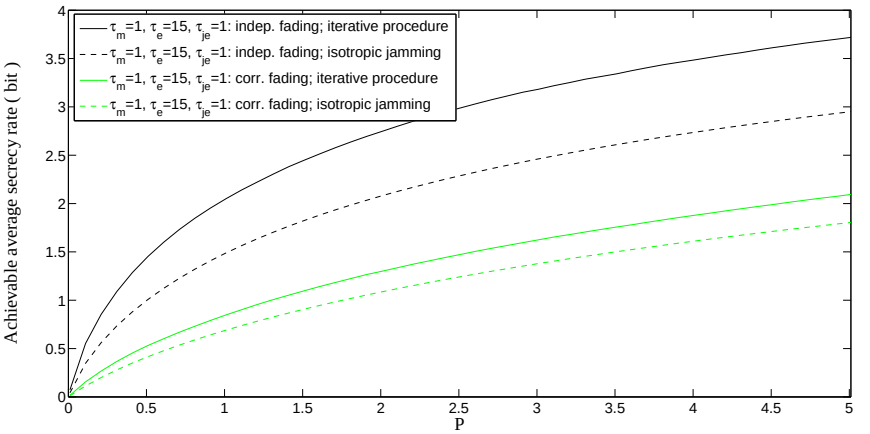

Figure 5.4: (c)

Figure 5.4: Achievable average secrecy rate $\bar{R}_s$ *vs.* P for $P_j = 5$. The transmitter, eavesdropper and jammer channels are subject to independent or correlated Rayleigh fading for different average power gains, when (i) the jammer and the transmitter optimize their power allocation policies according to the proposed iterative way and (ii) isotropic jamming, where, (a) $\tau_m = 15$, $\tau_e = 1$ and $\tau_{je} = 1$; (b) $\tau_m = \tau_e = \tau_{je} = 1$; and (c) $\tau_e = 15$, $\tau_m = 1$ and $\tau_{je} = 1$.

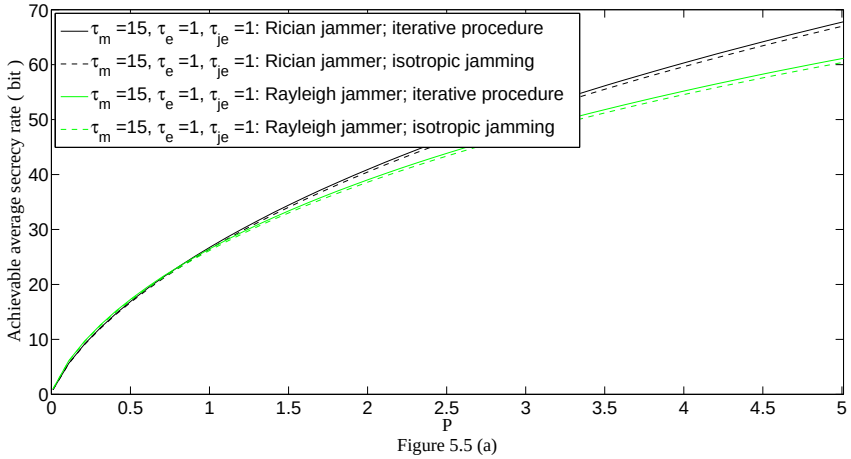

Figure 5.5 (a)

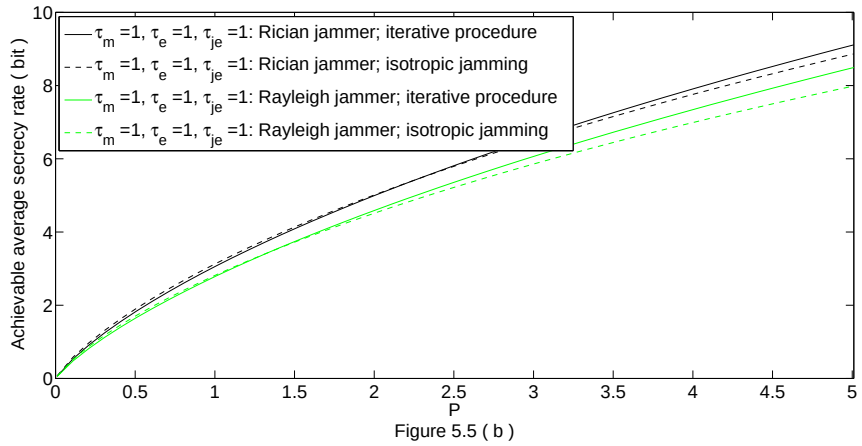

Figure 5.5 (b)

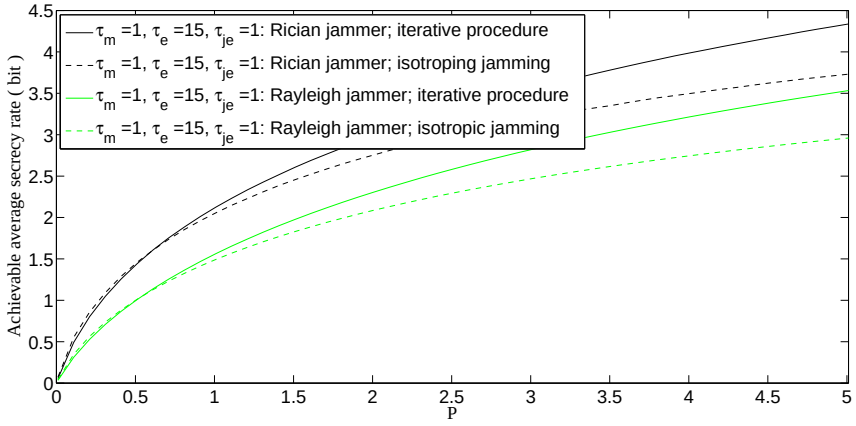

Figure 5.5 (c)

Figure 5.5: Achievable average secrecy rate $\bar{R}_s$ *vs.* P for $P_j = 5$. The transmitter and eavesdropper channels are subject to correlated Rayleigh fading and jammer channel is subject to independent Rayleigh or Rician fading for different average power gains, when (i) the jammer and the transmitter optimize their power allocation policies according to the proposed iterative way and (ii) isotropic jamming, where, (a) $\tau_m = 15$, $\tau_e = 1$ and $\tau_{je} = 1$; (b) $\tau_m = \tau_e = \tau_{je} = 1$; and (c) $\tau_e = 15$, $\tau_m = 1$ and $\tau_{je} = 1$.

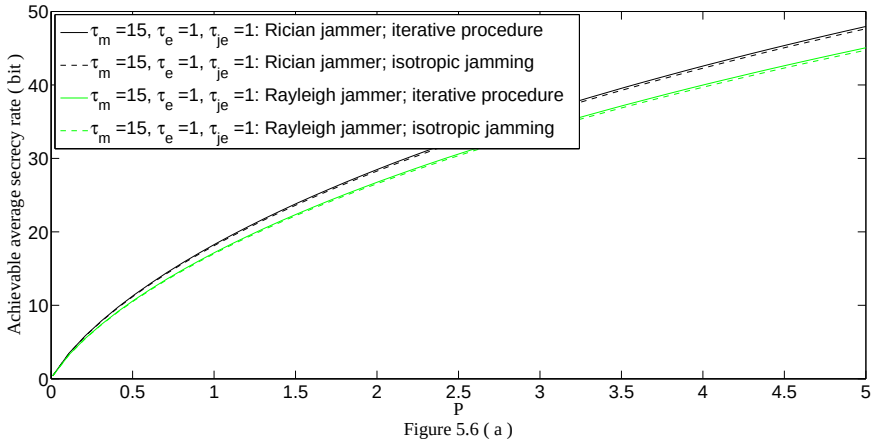

Figure 5.6 (a)

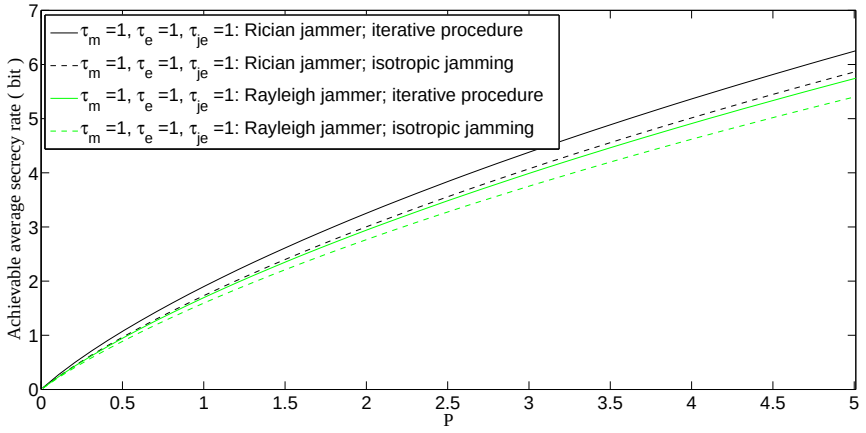

Figure 5.6 (b)

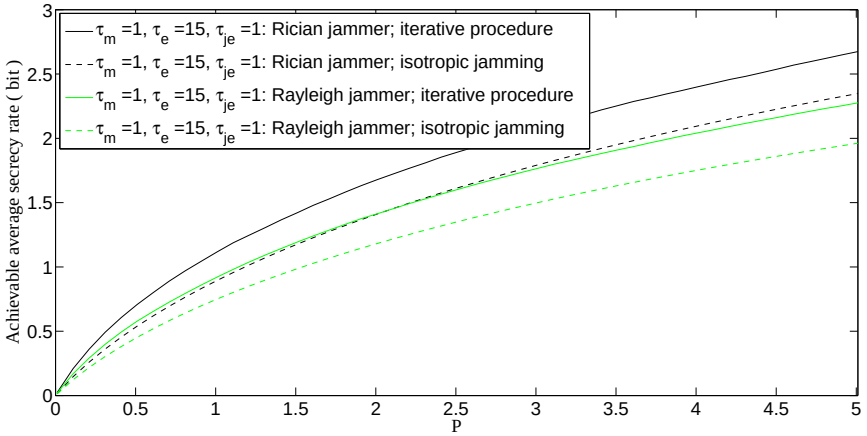

Figure 5.6 (c)

Figure 5.6: Achievable average secrecy rate $\bar{R}_s$ *vs.* P for $P_j = 5$. The transmitter and eavesdropper channels are subject to correlated Rayleigh fading and jammer channel is subject to correlated Rayleigh or Rician fading for different average power gains, when (i) the jammer and the transmitter optimize their power allocation policies according to the proposed iterative way and (ii) isotropic jamming, where, (a) $\tau_m = 15$, $\tau_e = 1$ and $\tau_{je} = 1$; (b) $\tau_m = \tau_e = \tau_{je} = 1$; and (c) $\tau_e = 15$, $\tau_m = 1$ and $\tau_{je} = 1$.

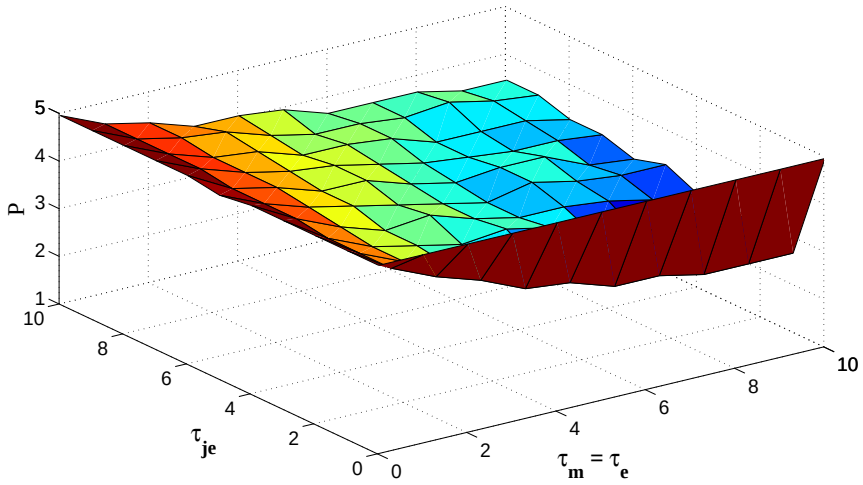

Figure 5.7: Optimal transmitter power *vs.* average power gains of the channels when sub-channels are independent and the transmitter and the eavesdropper channels are Rayleigh and the jammer channel is also Rayleigh for $\tau_m = \tau_e$. Total power budget of $P + P_j = 5$

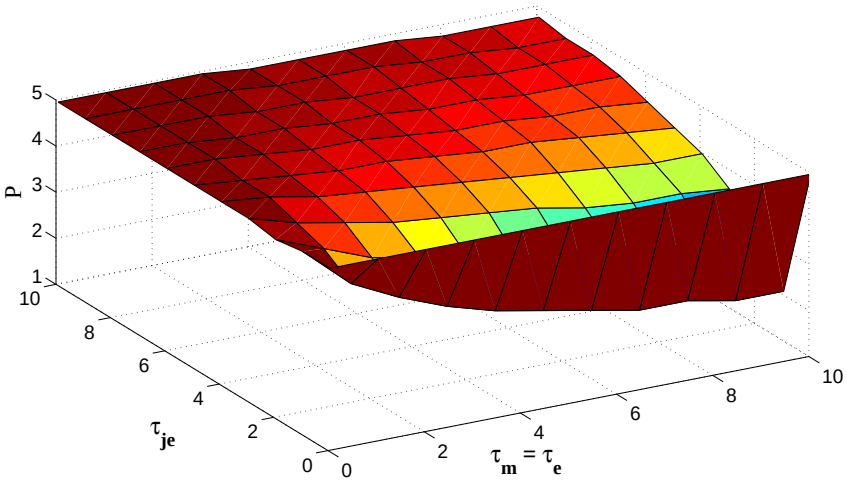

Figure 5.8: Optimal transmitter power *vs.* average power gains of the channels when sub-channels are independent and the transmitter and the eavesdropper channels are Rayleigh and jammer channel is Rician for $\tau_m = \tau_e$. Total power budget of $P + P_j = 5$

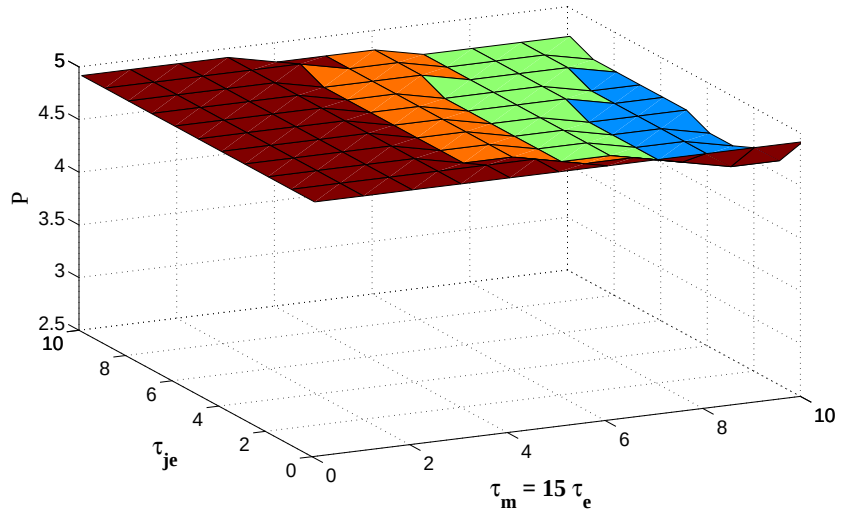

Figure 5.9: Optimal transmitter power *vs.* average power gains of the channels when sub-channels are independent and the transmitter and the eavesdropper are Rayleigh and the jammer channel is also Rayleigh for $\tau_m = 15\ \tau_e$. Total power budget of $P + P_j = 5$

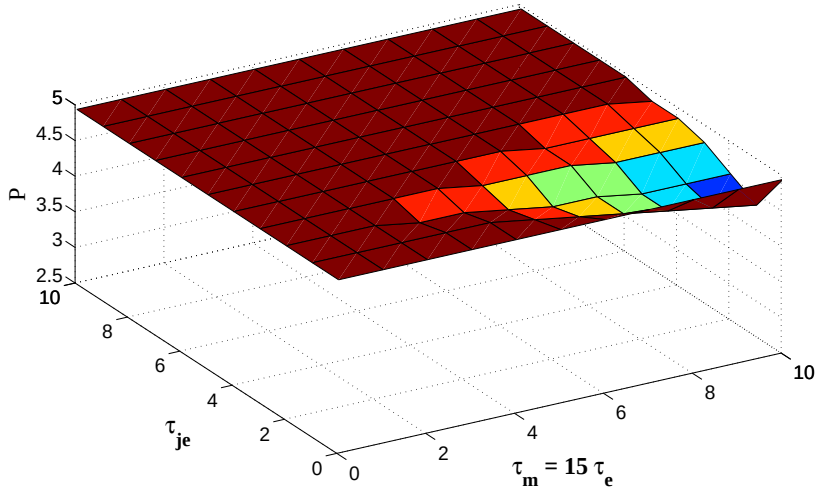

Figure 5.10: Optimal transmitter power *vs.* average power gains of the channels when sub-channels are independent and the transmitter and the eavesdropper are Rayleigh and the jammer channel is Rician for $\tau_m = 15\ \tau_e$. Total power budget of $P + P_j = 5$

Chapter 6
Concluding Remarks

This thesis has been concerned with the design of physical layer transmission schemes that aim to improve the reliability and security of data conveyed over the wireless medium. In particular, by capitalizing on an explicit information-theoretic characterization of achievable secrecy rates, we determine optimal power allocation strategies that a legitimate transmitter with / without a friendly jammer can use to mitigate any external risks of breaking the physical security of the transmission. Further, we provide characterizations of the optimal power allocation policies of a friendly / an unfriendly, who can be used to help / deteriorate the security of the legitimate parties.

This study has been carried out in the context of parallel Gaussian wiretap channels with friendly or unfriendly jammers, which can act as a model for the widely used OFDM communications systems.

By adopting tools of game theory, together with the information-theoretic characterization of the achievable secrecy rates, it has been possible to determine the power allocation policies for systems where the legitimate parties communicate in the presence of an eavesdropper and an unfriendly jammer. On the other hand, by adopting tools from optimization theory, it has also been possible to determine the power allocation policies for the scenario where the legitimate parties communicate in the presence of an eavesdropper and a friendly jammer. Such a study has then unveiled the secrecy gains that transmitters that adapt to the jammer power allocation policy experience over transmitters that do not perform such an adaptation.

In addition, through the application of the developed power allocation algorithms

to a concrete situations associated with the transmission of OFDM signals through a wireless channel in the presence of an eavesdropper and a friendly jammer, the thesis has also unveiled the set of average achievable secrecy rates in various fading scenarios: in the presence of Rayleigh or Rician fading, and independent or correlated fading across the sub-channels. This study can then act as a basis to gauge the achievable secrecy rate associated with a range of practical OFDM based communications systems.

Overall, the main contributions of the PhD thesis are as follows:

1. In the first part we have used game theoretic tools to devise optimal power allocation strategies for parallel Gaussian wiretap channel in the presence of unfriendly jamming, where, the jammer intends to minimize the achievable secrecy rate whereas the transmitter aims to maximize the achievable secrecy rate. We have introduced a game-theoretic formulation of a zero-sum power allocation game between transmitter and the unfriendly jammer when the payoff function is an achievable secrecy rate. We have provided a proof of the existence of a Nash equilibrium of the zero-sum game. We have characterized the optimal transmission and jamming power allocation strategies for the game, which have also been specialized for key asymptotic regimes to shed further insight. Our results show a transmitter that adapts to the jammer strategy, can experience a much higher secrecy rate than a non-adaptive transmitter.

2. In the second part we have introduced algorithms to devise optimal power policies for parallel Gaussian wiretap channel in the presence of friendly jamming, i.e., in this scenario, the jammer aims to help the legitimate parties to increase the secrecy rate by introducing more interference in the eavesdropper channel. In particular, we have introduced algorithms - that stem directly from a formulation of the power allocation optimization problem and its solution - to compute the optimal (or a nearly optimal) power allocation policy for the jammer both in degraded and non-degraded scenarios. We have also introduced an algorithm to compute a joint power allocation policy both for the transmitter and the jammer that leads to significant performance gains in relation to isotropic jamming. Simulation results demonstrate that these algorithms can lead to significant secrecy rate gains in comparison to other power allocation approaches.

3. The third mains contribution builds upon the second contribution of the thesis contributions to study the impact of power allocation policies in OFDM communications system in the presence of quasi-static fading. In this part, we investigate the achievable average secrecy rate in parallel fading wiretap channels subject to Rayleigh and Rician fading. In particular, we study the impact that the presence of absence of LOS components have on the average achievable secrecy rate. We also study the impact that the presence of absence of fading correlation across the sub-channels have on such an average achievable secrecy rate. Moreover, we also investigate the tradeoff between the transmission power and the jamming power when there is a fixed total power budget. The results demonstrate the increase in the achievable average secrecy rate obtained with friendly jamming. The achieved average secrecy rate is higher for independent sub-channels than when sub-channels are correlated. On the other hand, higher secrecy rates can be achieved when the channel from the friendly jammer to the eavesdropper is Rician with respect to the case of Rayleigh fading. We have also highlighted the loss due to correlation among the sub-channels in different fading scenarios: correlation has the most detrimental effect when the eavesdropper enjoys better channel conditions than the legitimate parties.

6.1 Recommendations for future research

The research work carried out in this thesis also opens various directions for future research:

- This thesis has concentrated primarily on scenarios where the unfriendly jammer interferes only with the main channel and the friendly jammer interferes only with the eavesdropper channel. This can be justified in situations where the jammer can position himself to be much closer to one of the parties or the jammer can collude with one of the parties. However, in view of the broadcast characteristics of the wireless propagation channel, it may also be relevant to consider scenarios where the jammer (unfriendly or friendly) interferes both with the main and the eavesdropper channel in order to imbue the formulations with further realism. This may lead to game-theoretic or optimization formulations where desired convexity or concavity properties are

lost, hence more difficult to tackle.

- This thesis has also concentrated primarily on scenarios where the channel states are known to all the parties, i.e. the legitimate transmitter and receiver, the eavesdropper and the jammer. This assumption can be justified in some scenarios, e.g. when the entities are members of a wireless network. However, it would also be relevant to relax this assumption in order to consider situations where some of the parties do not have access to the exact channel state but only to the distribution of the channel instead.

- It has been assumed throughout that the legitimate transmitter uses Gaussian signalling to convey information to the legitimate receiver where as the jammer uses Gaussian noise to interfere with the transmissions. One of the advantages of such a formulation is associated with the existence of closed form and tractable expressions for an achievable secrecy rate. Clearly, by relaxing such assumptions it may be possible to conceive strategies that lead to additional secrecy gains.

- Finally, and in addition to the quasi-static fading channel model, it may also be instructive to examine scenarios where the channels experience block fading or ergodic fading.

- The generalization of the work to these various settings may lead to a deeper understanding of the potential of OFDM to secure wireless communications both in the presence of friendly or unfriendly jamming.

References

[1] Y. Liang, H. V. Poor and S. Shamai (Shitz), *Information Theoretic security*. Foundation & Trends (FnT) Doudrecht, The Netherlands, NOW Publishers, 2009.

[2] Aaron E. Earle , *Wireless Security Handbook*. Taylor and Francis group, 6000 Broken Sound Parkway NW, Suite 300, Boca Raton, FL 33487-2748: Auerbach Publications, 2006.

[3] M. Debbah, H. El-Gamal, H. V. Poor and S. Shamai (Shitz), "Wireless Physical Layer Security," *Hindawi Publishing Corporation, EURASIP Journal on Wireless Communications and Networking*, 2009.

[4] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, "Handbook of Applied Cryptography," *Boca Raton, FL, USA: CRC Press*, 1996.

[5] W. Stallings, *Cryptography and Network Security Principles and Practicies*. Upper Saddle River, NJ, USA: Prentice Hall, 3^{rd} ed., 2003.

[6] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, 1949.

[7] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[8] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.

[9] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–349, May 1978.

[10] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," *IEEE International Symposium on Information Theory*, pp. 356–360, Jul. 2006.

[11] Y. Liang, H. V. Poor and S. Shamai, "Secrecy capacity region of fading broadcast channels," *Proc. IEEE International Symposium on Information Theory, Nice, France*, Jun. 2007.

[12] Z. Li, R. Yates and W. Trappe, "Secrecy capacity of independent parallel channels," *44th Annual Allerton Conference on Communication, Control, and Computing. Monticello, Illinois.*, Sep.27-29 2006.

[13] P. K. Gopala, L. Lai and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE International Symposium on Information Theory*, pp. 1306–1310, Jun. 2007.

[14] http://standards.ieee.org/about/get/802/802.11.html, "IEEE 802.11."

[15] http://standards.ieee.org/about/get/802/802.16.html, "IEEE 802.16."

[16] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, pp. 644–654, 1976.

[17] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, pp. 733–742, 1993.

[18] A. O. Hero, "Secure space-time communication," *IEEE Transactions on Information Theory*, vol. 49, pp. 3235–3249, 1993.

[19] R. Bustin, R. Liu, H. V. Poor and S. Shamai (Shitz), "An MMSE Approach To The Secrecy Capacity Of The MIMO Gaussian Wiretap Channel," in *EURASIP Journal on Wireless Communications and Networking, vol. 2009, article ID 370970, 8 pages.*

[20] R. Liu, T. Liu, H. V. Poor and S. Shamai (Shitz), "Multiple-input multiple-output Gaussian broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 56, no.9, pp. 4215–4227, Sep. 2010.

[21] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas-II: The MIMOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no.11, pp. 5515–5532, Nov. 2010.

[22] M. C. Gursoy, "Secure communication in the low-SNR regime: A characterization of the energy-secrecy tradeoff," *in Proc.IEEE International Symposium on Information Theory, Seoul, Korea*, Jun. 2009.

[23] R. Y. Z. Li and W. Trappe, "Secrecy capacity of independent parallel channels," *Proc. of 44th Annual Allerton Conference, Monticello, IL, USA*, Sep. 2006.

[24] E. Jorswieck and A. Wolf, "Resource allocation for the wire-tap multi-carrier broadcast channel," *in Proc. International Workshop on Multiple Access Communications (MACOM), St. Petersbutg, Russia*, Jun. 2008.

[25] E. Jorswieck and S. Gerbracht, "Secrecy rate region of downlink OFDM systems: efficient resource allocation," *in Proc. of 14th International OFDM-Workshop (InOWo), Hamburg, Germany*, Sep. 2009.

[26] M. R. D. Rodrigues and P. D. M. Almeida, "Filter design with secrecy constraints: The degraded parallel Gaussian wiretap channel," *IEEE Global Communications Conference*, Dec. 2008.

[27] H. Reboredo, M. Ara, M. R. D. Rodrigues, and J. Xavier, "Filter Design with Secrecy Constraints: The Degraded Multiple-Input Multiple-Output Gaussian Wiretap Channel," *2011 IEEE 73rd Vehicular Technology Conference (VTC Spring)*, pp. 1–5, 2011.

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

[29] J. A. C. Bingham, "Multicarrier modulation for data transmission: an idea whose time has come," *IEEE Communications Magazine*, vol. 28, no. 5, pp. 5–14, 1990.

[30] T. Basar, "The Gaussian test channel with an intelligent jammer," *IEEE Transactions on Information Theory*, vol. 29, no. 1, pp. 152–157, Jan. 1983.

[31] T. Basar and Y.-W. Wu , "A complete characterization of minimax and maximin encoder- decoder policies for communication channels with incomplete statistical description," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 482–489, Jul. 1985.

[32] R. J. McEliece and W. E. Stark , "An information theoretic study of communication in the presence of jamming," *IEEE International Conference on Communications*, pp. 45.3.1–45.3.5, 1981.

[33] A. Mukherjee and A. L. Swindlehurst, "Optimal strategies for countering dual-threat jamming/eavesdropping-capable adversaries in MIMO channels,"

IEEE Millitary Communications Conference (MILCOM), pp. 1695–1700, Oct. 31-Nov. 3 2010.

[34] E. Tekin and A. Yener, "The general Gaussian Multiple-Access and Two-Way wiretap channels: achievable rates and cooperative jamming," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[35] Z. Han, N. Marina, M. Debbah and A. Hjørungnes, "Physical layer security game: interaction between source, eavesdropper, and friendly jammer," *EURASIP Journal on Wireless Communications and Networking, Volume 2009*.

[36] R. Zhang, L. Song, Z. Han and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 8, pp. 3693–3704, Oct. 2012.

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

[38] http://mobiledevdesign.com/tutorials/ofdm, "Orthogonal Frequency-Division Multiplexing (OFDM): FAQ Tutorial."

[39] J. A. C. Bingham, "Multicarrier modulation for data transmission: an idea whose time has come," *IEEE Communications Magazine*, vol. 28, no. 5, pp. 5–14, May 1990.

[40] W. Y. Zou and W. Yiyan, "COFDM: an overview," *IEEE Transactions on Broadcasting*, vol. 41, no. 1, pp. 1–8, Mar. 1995.

[41] B. Hirosaki, "An Analysis of Automatic Equalizers for Orthogonally Multiplexed QAM Systems," *IEEE Transactions on Communications*, vol. 28, no. 1, pp. 73–83, Jan. 1980.

[42] B. Hirosaki, S. Hasegawa and Sabato, A., "Advanced Groupband Data Modem Using Orthogonally Multiplexed QAM Technique," *IEEE Transactions on Communications*, vol. 34, no. 6, pp. 587–592, Jun. 1986.

[43] L. J. Cimini, "Analysis and Simulation of a Digital Mobile Channel Using Orthogonal Frequency Division Multiplexing," *IEEE Transactions on Communications*, vol. 33, no. 7, pp. 665–675, Jul. 1985.

[44] J.S. Chow, J. C. Tu and Cioffi, J.M., "A discrete multitone transceiver system for HDSL applications," *IEEE Journal on selected areas in Communications*, vol. 9, no. 6, pp. 895–908, Aug. 1991.

[45] P. S. Chow, J. C. Tu and Cioffi, J.M., "Performance evaluation of a multichannel transceiver system for ADSL and VHDSL services," *IEEE Journal on selected areas in Communications*, vol. 9, no. 6, pp. 909–919, Aug. 1991.

[46] Jr. L. Cimini, "Analysis and simulation of a digital mobile channel using orthogonal frequency division multiplexing," *IEEE Transactions on Communications*, vol. 33, pp. 665–675, Jul. 1985.

[47] M. A. Birchler and S. C. Jasper, "A 64 kbps digital land mobile radio system employing M-16QAM," *5th Nordic Sem. Land Mobile Radio, Helsinki, Finland*, pp. 237–241, Dec. 1992.

[48] B. L. Floch, R. Halbert-Lassalle and D. Castelain, "Digital sound broadcasting to mobile receivers," *IEEE Transactions on Consumer Electronics*, vol. 35, pp. 493–503, Aug. 1989.

[49] R. V. Nee, G. Awater, M. Morikura, H. Takanashi, M. Webster, and K. W. Halford, "New High-Rate Wireless LAN Standards," *IEEE Communications Magazine*, pp. 82–88, Dec. 1999.

[50] G. L. Stüber, *Principles of Mobile Communications.* 2nd. ed. Kluwer Academic Publisher, 2002.

[51] Ramjee Prasad, *OFDM for wireless communication system.* Bosto, London: Artech House, Inc., 2004.

[52] N. Romero-Zurita, M. Ghogho and D. McLernon1, "Physical Layer Security of MIMO Frequency Selective Channels by Beamforming and Noise Generation," *19th European Signal Processing Conference, Barcelona, Spain*, 2011.

[53] F. Renna, N. Laurenti and Poor, H.V., "Physical-Layer Secrecy for OFDM Transmissions Over Fading Channels," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 4, pp. 1354–1367, Aug. 2012.

[54] Gill R. Tsouri and Dov Wulich, "Securing OFDM over Wireless Time-Varying Channels Using Subcarrier Overloading with Joint Signal Constellations," *Hindawi Publishing Corporation, EURASIP Journal on Wireless Communications and Networking*, 2009.

[55] Y. Liang, H. V. Poor and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Transactions on Information Theory, Special Issue on Information Theoretic Security*, vol. 54, pp. 2470–2492, Jun. 2008.

[56] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE International Symposium on Information Theory*, pp. 524–528, jul 2008.

[57] R. J. McEliece, "Communication in the presence of jamming- An information theoretic approach," *Secure Digital Communications,CISM Courses and Lectures, G. Longo, Ed. New York: Springer-Verlag*, 1983.

[58] M. Médard, "Capacity of correlated jamming channels," *Proc. 35th Annu. Allerton Conf. Communications, Control and Computing, Monticello, IL*, Sep.-Oct. 1997.

[59] S. Shafiee and S. Ulukus, "Correlated Jamming in Multiple Access Channel," *Conference on Information Science and System, The Johns Hopkins University*, 16-18 Mar. 2005.

[60] ——, "Mutual Information Games in Multiuser Channels with Correlated Jamming," *IEEE Transaction on Information Theory*, vol. 55, no.10, Oct. 2009.

[61] S. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 8, pp. 1451–1458, 1998.

[62] Vahid Tarokh, A. Naguib, N. Seshadri and A. R. Calderbank, "Space-time codes for high data rate wireless communication: performance criteria in the presence of channel estimation errors, mobility, and multiple paths," *IEEE Transactions on Communications*, vol. 47, no. 2, pp. 199–207, 1999.

[63] A.F. Naguib, Vahid Tarokh, N. Seshadri and A. R. Calderbank, "A space-time coding modem for high-data-rate wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 8, pp. 1459–1478, 1998.

[64] Vahid Tarokh, A. Naguib, N. Seshadri and A. R. Calderbank, "Combined array processing and space-time coding," *IEEE Transactions on Information Theory*, vol. 45, no. 4, pp. 1121–1128, 1999.

[65] G. J. Foschini, "Layered space-time architecture for wireless communication in a fading environment when using multi element antennas," *Bell Labs. Technical Journal*, vol. 1, no. 2, 1996.

[66] B.M. Hochwald and T.L. Marzetta, "Unitary space-time modulation for multiple-antenna communications in Rayleigh flat fading," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 543–564, 2000.

[67] D. P. Palomar, J. M. Cioffi and M. A. Lagunas, "Joint tx-rx beamforming design for multicarrier MIMO channels: A unified framework for convex optimization," *IEEE Transactions on Signal Processing*, vol. 51, no. 9, pp. 2381–2401, Sep. 2003.

[68] Jian Yang and S. Roy, "On joint transmitter and receiver optimization for multiple-input-multiple-output (MIMO) transmission systems," *IEEE Transactions on Communications*, vol. 42, no. 12, pp. 3221–3231, 1994.

[69] A. Scaglione, P. Stoica, S. Barbarossa, G. B. Giannakis and H. Sampath, "Optimal designs for space-time linear precoders and decoders," *IEEE Transactions on Signal Processing*, vol. 50, no. 5, pp. 1051–1064, 2002.

[70] M. L. Honig and P. Crespo and K. Steiglitz, "Suppression of near- and far-end crosstalk by linear pre- and post-filtering," *IEEE Journal on Selected Areas in Communications*, vol. 10, no. 3, pp. 614–629, 1992.

[71] D. P. Palomar, *A unified framework for communications through MIMO channels, Ph.D. dissertation.* Technical Univ. Catalonia (UPC), 2003.

[72] M. Yuksel, X. Liu and E. Erkip, "A secrecy game with an informed jammer relay," *IEEE 21st International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC)*, pp. 2687–2691, 2010.

[73] M. Janzamin, M. Pakravan and H. Sedghi, "A Game-Theoretic Approach for Power Allocation in Bidirectional Cooperative Communication," *Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, 2010.

[74] Y. Shi, J. H. Wang, W. L. Huang and K.Ben Letaief, "Power Allocation in Gaussian Interference Relay Channels via Game Theory," *IEEE GLOBECOM*, pp. 1–5, Nov. 30 2008-Dec. 4 2008 2008.

[75] E. V. Belmega, B. Djeumou and S. Lasaulce, "Power Allocation Games in Interference Relay Channels: Existence Analysis of Nash Equilibria," *To*

appear in EURASIP Journal on Wireless Communications and Networking (JWCN), 2011.

[76] L. Lai and H. E. Gamal, "The Water-Filling Game in Fading Multiple-Access Channels," *IEEE Transactions on Information Theory*, vol. 54, No.5, May 2008.

[77] M. Bloch, J. Barros, M. R. D. Rodrigues and S. W. McLaughlin, "Wireless Information-Theoretic Security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[78] A. R. Washburn, *Two Person Zero-sum Games,3rd edition.* MAS institute for operation research and the management sciences: Linthicum, MD 21090, USA, 2003.

[79] P. Bender, P. Black, M. Grob, N. Sindhushayana and A. Viterbi, "CDMA/HDR: A bandwith-efficient high-speed wireless data service for nomadic users," *IEEE Communications Magazine*, vol. 38, pp. 70–77, Jul. 2000.

[80] 3rd Generation Partnership Project; Technical Specification Group Radio Access Network, "UTRA High Speed Downlink Packet Access," *Tech. Rep., 3GRTR25.950*, Mar. 2001.

[81] A. Lozano, A. M. Tulino and S. Verdú, "Mutiple-Antenna Capacity in the Low-Power Regime," *IEEE Transactions on Information Theory*, vol. 49, no. 10, Oct. 2003.

[82] Z. Han, N. Marina, M. Debbah and H. Are, "Physical Layer Security Game: Interaction between Source, Eavesdropper, and Friendly Jammer," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, 2009.

[83] P. K. Gopala, L. Lai and H. El Gamal, "On the Secrecy Capacity of Fading Channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[84] G. Zheng, L. Choo and K.K Wong, "Optimal Cooperative Jamming to Enhance Physical Layer Security Using Relays," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.

[85] S. Luo, J. Li and A. Petropulu, "Outage constrained secrecy rate maximization using cooperative jamming," *Proc. of IEEE Statistical Signal Processing Workshop (SSP)*, pp. 389–392, Aug. 2012.

[86] X. He and A. Yener, "Two-Hop Secure Communication Using an Untrusted Relay: A Case for Cooperative Jamming," *IEEE Global Telecommunications Conference (GLOBECOM)*, pp. 1–5, Dec. 2008.

[87] J. P. Vilela, P. C. Pinto and J. Barros, "Jammer Selection Policies for Secure Wireless Networks," *IEEE International Conference on Communications Workshops (ICC)*, pp. 1–6, Jun. 2011.

[88] X. He and A. Yener, *Cooperative jamming: The tale of friendly interference for secrecy.* in Securing Wireless Communications at the Physical Layer, Eds. New York: Springer, pp.65-88, 2009.

[89] P. C. Pinto, J. Barros and M. Z. Win, "Wireless physical-layer security: the case of colluding eavesdroppers," *in Proc. of the IEEE International Symposium on Information Theory (ISIT), Seoul, korea*, Jun. 28-Jul. 3 2009.

[90] S. Boyd and L. Vandenberghe, *Convex Optimization.* Cambridge, U.K.: Cambridge University Press, 2004.

[91] X. Tang, R. Liu, SP. Spasojevic and H. V. Poor, "The Gaussian wiretap channel with a helping interferer," *in Proceedings of IEEE International Symposium on Information Theory (ISIT), Toronto, Canada*, pp. 389–393, Jul. 2008.

[92] S. S. Sastry, *Introductory Methods of Numerical Analysis, 4th ed.* New Dilhi, India: Prentice-Hall of India Private Limited, 2005.

[93] T. Ericsson, "A Gaussian channel with slow fading," *IEEE Transactions on Information Theory*, vol. 16, no. 3, pp. 353–356, May 1970.

[94] A. Goldsmith and P. Varaiya, "Capacity of fading channels with channel side information," *IEEE Transactions On Information Theory*, vol. 43, no. 6, pp. 1986–1992, Nov. 1997.

[95] L. Ozarow, S. Shamai and A. D. Wyner, "Information theoretic considerations for cellular mobile radio," *IEEE Transactions on vehicular technology*, vol. 43, no. 2, pp. 353–356, May 1994.

[96] G. Kaplan and S. Shamai, "Error probabilities for the block-fading Gaussian channel," *International Journal of Electronics and Communications (AEU)*, vol. 49, no. 4, pp. 192–205, 1995.

[97] M. Khansari and M. Vetterli, "Source coding and transmission of signals over time-varying channels with side information," *IEEE International Symposium on Information Theory (ISIT), Whistler, Canada*, Sep. 1995.

[98] M. Médard and A. Goldsmith, "Capacity of time-varying channels with channel side information," *IEEE International Symposium on Information Theory (ISIT), Ulm, Germany*, p. 372, Jun. 29-Jul. 4 1997.

[99] E. Biglieri, G. Caire and G. Taricco, "Minimum outage probability for slowly-varying fading channels," in *Proc. IEEE International Symposium on Information Theory*, 1998.

[100] G. Caire, G. Taricco and E. Biglieri, "Optimum power control over fading channels," *IEEE Transactions on Information Theory*, vol. 45, no. 5, pp. 1468–1489, 1999.

[101] E. Telatar, "Capacity of Multi-antenna Gaussian channels," *European Transictions on Telecommunications*, vol. 10, no. 6, pp. 585–595, Nov.-Dec. 1999.

[102] M. Ara, H. Reboredo, F. Renna and M. R. D. Rodrigues, "Power allocation strategies for OFDM Gaussian wiretap channels with a friendly jammer," *in Proc. of IEEE International Conference on Communications (ICC), Budapest, Hungrary*, Jun. 2-5 2013.

[103] ——, "Power Allocation Strategies For OFDM Gaussian Wiretap Channels With a Friendly Jammer: The Degraded case," in *Conference on Telecommunications (Conftele-2013), Castelo Branco, Portugal*, 8-10 May 2013.

[104] Y. S. Cho, J. Kim, W. Y. Yang, and C. G. Kang, *MIMO-OFDM Wireless Communications with MATLAB*. 2 Clementi Loop, Singapore 129809: John Wile and Sons (Asia) Pte Ltd, 2010.

[105] Andrea Goldsmith, *Wireless Communications*. Cambridge University Press, 2005.