Optimising Multiple Antenna Techniques for Physical Layer Security

Leonardo Nabil Romero Zurita

Submitted in accordance with the requirements for the degree of Doctor of Philosophy

The University of Leeds
School of Electronic and Electrical Engineering

August 2014

Declaration

The candidate confirms that the work submitted in this thesis is his own and that appropriate credit has been given where reference has been made to the work of others. The material contained in the chapters of this thesis has been previously published in research articles written entirely by the author of this work (Leonardo Nabil Romero Zurita) who appears as lead (first) author in all of them. The research has been supervised and guided by Prof. Mounir Ghogho and Dr. Des McLernon, and so they appear as co-authors of the articles. All the material included in this document is of the author's entire intellectual ownership.

The work in chapter 3 of the thesis has appeared in publication as follows:

- *Outage Probability Based Power Distribution between Data and Artificial Noise for Physical Layer Security,* by N. Romero-Zurita, M. Ghogho and D. McLernon. IEEE Signal Processing Letters. Feb. 2012.

- *PHY Layer Security Based on Protected Zone and Artificial Noise,* by N. Romero-Zurita, M. Ghogho, D. McLernon and A. Swami. IEEE Signal Processing Letters. May. 2013.

The work in chapter 4 of the thesis has appeared in publication as follows:

- *Physical Layer Security by Robust Masked Beamforming and Protected Zone Optimisation,* by N. Romero-Zurita, D. McLernon and M. Ghogho. IET Communications. Special Issue on Secure Physical Layer Communications. May. 2014.

- *Securing Wireless Networks by Robust Beamforming and Artificial Noise under a Close Eavesdropper,* by N. Romero-Zurita, M. Ghogho and D. McLernon. Symposium on the Convergence of Telecommunications, Networking and Broadcasting. Liverpool, UK. Jun. 2013.

The work in chapter 5 of the thesis has appeared in publication as follows:

- *Physical Layer Security of MIMO - OFDM Systems by Beamforming and Artificial Noise Generation,* by N. Romero-Zurita, M.Ghogho and D. McLernon. Physical Communication. Special Issue on Advances in MIMO-OFDM. Dec. 2011.

- *Physical Layer Security of MIMO Frequency Selective Channels by Beamforming and Noise Generation,* by N. Romero-Zurita, M. Ghogho and D. McLernon. EUSIPCO 2011 (19th European Signal Processing Conference). Barcelona, Spain. Aug. 2011

The work in chapter 6 of the thesis has appeared in publication as follows:

- *Security in Multiple Antenna Systems by Joint Transmitter/Receiver Artificial Noise Generation through Semidefinite Programming,* by N. Romero-Zurita, D. McLernon and M.Ghogho. IET Intelligent Signal Processing (ISP) Conference, London, UK, Dec. 2013.

This copy has been supplied on the understanding that it is copyright material and that no quotation from the thesis may be published without proper acknowledgement.

© 2014 The University of Leeds and Leonardo Nabil Romero Zurita

The right of Leonardo Nabil Romero Zurita to be identified as Author of this work has been asserted by him in accordance with the Copyright, Designs and Patents Act 1988.

This work is dedicated entirely to the loving memory of my dear sister Elena Abigail.

Cusumbito, esta va por vos bonita!

Tu ñañecito,
Nabil

Acknowledgements

In the next lines I would like to express my sincere appreciation and gratitude to my supervisors Professor Mounir Ghogho and Dr. Des McLernon. Thank you Prof. Mounir for your academic guidance and unconditional support. I am especially grateful for all the opportunities that you provided me. Thank you for believing in me and taking a chance on a student who one day in November 2008 approached you looking for a master project. Thank you Dr. Des for being a great supervisor in whom I could always find academic support and thoughtful advice. Many thanks for providing all the great opportunities within the EEE School, the University and beyond. You have been a tremendous mentor to me and a true friend that always supported me in my academic and personal life. Thank you for the endless political and philosophical rows, for the music and for providing a 'practical proof of concept' that shows there is still an essential place in the world for dreamers.

I wish to thank Prof. Stephen McLaughlin and Dr. Mohsen Razavi for being part of my thesis committee. My special recognition also goes to the University of Leeds, which economically supported my research studies through a Fully Funded International Research Scholarship. Furthermore, I would also like to thank all of my friends and fellow laboratory colleagues who supported me and always encouraged me to strive towards my goals.

A special gratitude goes to my family; the four emotional engines that propel my life and dreams. Many thanks to my mother Maria Elena for being my source of motivation and happiness; to my father Antonio Nabil for giving me support and guidance; and to my brother Antonio Jacob for offering me his encouragement and strength. My eternal

gratitude goes to my sister Elena Abigail too; thank you for your life, for your smile and for our never-ending struggles. Thank you for being my best opposite side and complement; for always being there for me. You always will be my example of rebellion and courage and remain alive in my heart accompanying me on my pathways. Thank you to the four of you for believing in my dreams and understanding all the sacrifices that they involve. I will always be indebted to you.

Finally, for the endless patience, unconditional support and generous understanding. For the love and the company. For being my life's adventure companion. For being just you. Thank you Andrea.

Abstract

Wireless communications offer data transmission services anywhere and anytime, but with the inevitable cost of introducing major security vulnerabilities. Indeed, an eavesdropper can overhear a message conveyed over the open insecure wireless media putting at risk the confidentiality of the wireless users. Currently, the way to partially prevent eavesdropping attacks is by ciphering the information between the authorised parties through complex cryptographic algorithms. Cryptography operates in the upper layers of the communication model, bit it does not address the security problem where the attack is suffered: at the transmission level.

In this context, physical layer security has emerged as a promising framework to prevent eavesdropping attacks at the transmission level. Physical layer security is based on information-theoretic concepts and exploits the randomness and the uniqueness of the wireless channel. In this context, this thesis presents signal processing techniques to secure wireless networks at the physical layer by optimising the use of multiple-antennas. A masked transmission strategy is used to steer the confidential information towards the intended receiver, and, at the same time, broadcast an interfering signal to confuse unknown eavesdroppers. This thesis considers practical issues in multiple-antenna networks such as limited transmission resources and the lack of accurate information between the authorised transmission parties. The worst-case for the security, that occurs when a powerful eavesdropper takes advantage of any opportunity to put at risk the transmission confidentiality, is addressed. The techniques introduced improve the security by offering efficient and innovative transmission solutions to

lock the communication at the physical layer. Notably, these transmission mechanisms strike a balance between confidentiality and quality to satisfy the practical requirements of modern wireless networks.

Contents

Abbreviations

AES	Advanced Encryption Standard
AF	Amplify and Forward
AN	Artificial Noise
AWGN	Additive White Gaussian Noise
CSI	Channel State Information
CDF	Cumulative Distribution Function
CJ	Cooperative Jamming
DF	Decode and Forward
DoF	Degree of Freedom
DoS	Denial of Service
FDD	Frequency-division Duplexing
FFT	Fast Fourier Transform
GSM	Global System for Mobile Communications
IDFT	Inverse Discrete Fourier Transform
iif	if and only if
KKT	Karush-Kuhn-Tucker (Optimality conditions)
LHS	Left Hand Side
LTE	Long-Term Evolution
LMI	Linear Matrix Inequality
MIMO	Multiple Input Multiple Output
MIMOME	Multiple Input Multiple Output Multiple Eavesdropper
MISO	Multiple Input Single Output
MRC	Maximal Ratio Combining
OFDM	Orthogonal Frequency Division Multiplexing
PMIF	Positive Monotonically-increasing Function
PZ	Protected Zone

QoS	Quality of Service
RSA	Rivest, Shamir and Adleman public-key cryptosystem
RHS	Right Hand Side
SISO	Single Input Single Output
SNR	Signal-to-Noise Ratio
SDP	Semidefinite Program
SVD	Singular Value Decomposition
TDD	Time-division Duplexing
UMTS	Universal Mobile Telecommunications System
WPA	Wi-Fi Protected Access

Chapter 1

Introduction

> 'We left the gold and gems for common thieves. Instead our mice stole letters, ledgers, charts… later, they would read them and leave them where they lay. Secrets are worth more than silver or sapphires', Varys claimed.
>
> George R.R. Martin

This introductory chapter provides an overview of the contents covered in this thesis. It first focuses on describing the security problem in wireless communications in an accessible manner, and then presents the research objectives pursued by this thesis and how it is structured. The concepts informally introduced here will be covered in later chapters with technical rigour.

1.1 Security in wireless networks

Wireless communications have experienced a dramatic boost during the last decade. Nowadays, the number of electronic devices connected wirelessly to the Internet has superseded the number of wired ones. Mobile devices are everywhere using wireless means as de facto technology to access to the Internet. Therefore, wireless networks, in all of their different technological flavours, have become pervasive in providing coverage and connectivity almost everywhere. As a result, mobile users

enjoy permanent data connectivity and freedom of mobility with high data rates and great levels of reliability. These technological advances have enabled the social communication revolution that we are experiencing today and it is reflected in the dramatic change in the way that people have been communicating with each other in the recent years. Moreover, the emerging *'Internet of Things'* foresees that wireless connectivity would play a starring technological role underpinning the access of millions of devices to the Internet to establish machine-to-machine communications. Remarkably, most of the information conveyed over wireless links is critical and sensitive in terms of security.

Wireless communications offer data transmission services anywhere and anytime. However, the freedom, mobility, and versatility introduced by the broadcast nature of wireless networks has a major drawback: Security [1]. Indeed, as a result of their open nature, wireless communications introduces major security breaches that can be exploited by hostile attackers. Moreover, the massive increase in personal devices carelessly connected to wireless networks, for instance using weak passwords, is attracting new types of threats targeting the end users' personal information. These factors have generated a dramatic increase in the number of cyber-attacks resulting in significant economic losses for business and individuals alike. This problem will only be exacerbated with the growth in technologies and applications that are focused around end users accessing a variety of information, ranging from conventional Internet traffic (email, web) to personal/confidential data (financial, health, location). These services will attract an unknown number of malicious attackers; therefore, securing them across a range of wireless technologies is a key challenge for the designers of next generation wireless systems.

Wireless systems are vulnerable to *eavesdropping* attacks occurring when a non-authorised party overhears a secret message transmitted over the open insecure media. Eavesdropping is referred to as a passive attack that involves a malicious attacker listening to the communication and recovering data without interaction with the network. In contrast, *data alteration* is regarded as an active attack in which the information exchanged between the transmission parties can suffer modifications. In addition, the lack of a physical connection in wireless networks facilitates *impersonation* attacks, where attackers fake legitimate user credentials to gain access to the network. Moreover, the openness of the wireless channel makes it susceptible to *denial-of-service* attacks. These attacks can be caused by

non-authorised users that *jam* the channel or by legitimate network clients *overusing* the communication resources [2, §1.1]. These intrinsic vulnerabilities of the wireless channel as well as the characteristics typical of a wireless environment, such as users roaming between networks, devices with limited power and processing capabilities and users misusing the technology, make the task of securing wireless networks cumbersome [3].

With the objective of securing wireless networks, industrialists and researchers have developed authentication, confidentiality, integrity, non-repudiation and privacy services. Notably, all of these services have been implemented by computational based technologies. Here, the intrinsic vulnerabilities of the wireless channel medium are addressed by services running in upper layers of the communication model without attacking the root of the security problem where it occurs; that is the wireless channel itself. Moreover, the mobility offered by wireless communications and the lack of appropriate user behaviours towards security cause many additional vulnerabilities. Unfortunately, most of these weaknesses are discovered only after the products and technologies are commercialised. These security issues demand software patches and partial a-posteriori solutions that have generated an inefficient threat-response cycle that is continuously repeated as new exploits are discovered [4].

One notable example of this security vulnerability trend is the way in which eavesdropping attacks are currently prevented in wireless networks. Confidentiality is provided by ciphering the information between the authorised parties by computational expensive cryptographic algorithms that rely on shared secret keys between the authorised users. These cryptographic techniques operate in the upper layers of the communication model not facing the security problem where it actually occurs: in the communication mechanism itself. Cryptographic techniques present many security vulnerabilities arising from the way that the algorithms are implemented and how they are used; therefore, they do not provide a totally secure wireless transmission [5]. Moreover, cryptographic services demand either security key distribution/management (symmetric cryptography) or computationally intensive algorithms (asymmetric cryptography) to cipher the sensitive information. These requirements become a great limitation in wireless networks topologies where key management is not possible due to accessibility difficulties

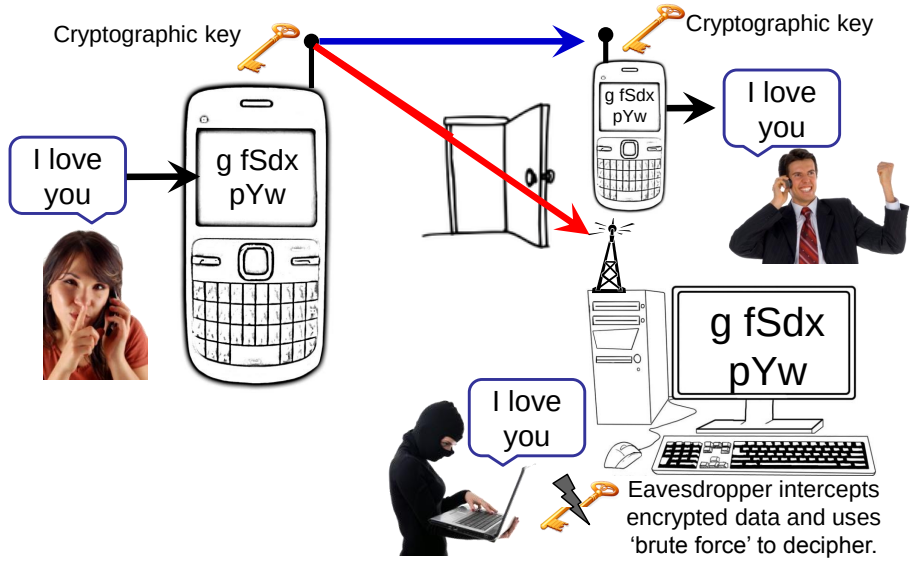
and where computation capabilities are limited due to the lack of power and implementation constraints, e.g., smart grid networks, wireless sensor networks, etc. [6].

The described scenario underlines the urgent necessity of addressing wireless security from a radically different approach in order to effectively *'lock the front door of the communication model'* by securing the actual wireless transmission directly at the transmission level.

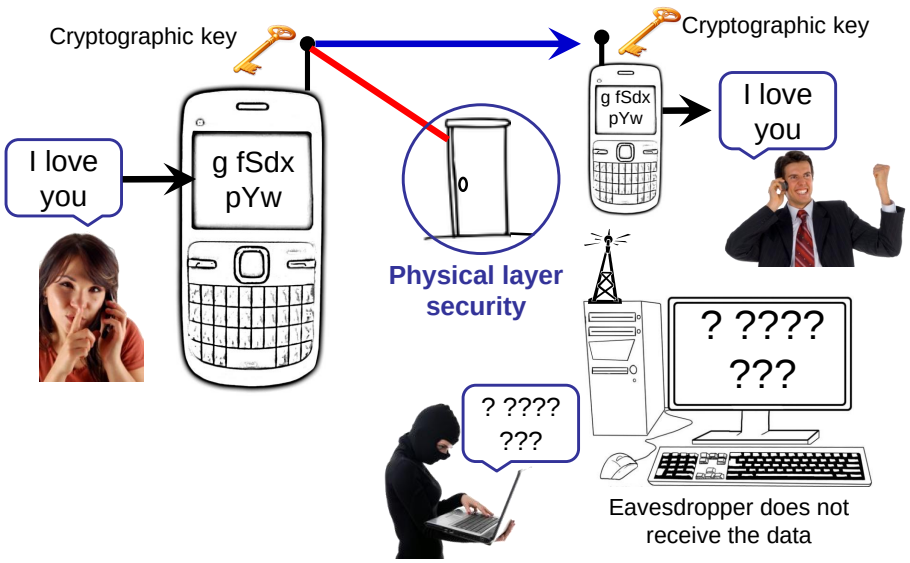
1.2 Locking at the front door of wireless communications

To illustrate the confidentiality problem of wireless security we use an analogy of the way that we secure our valuable belongings at home. Let us suppose that we have to leave home for a holiday and we sensibly decide to keep our treasured belongings, such as jewellery, cash, confidential information, etc., safe from burglars. A good security strategy is to keep the valuables safe by storing them in a safe box protected by a strong combinatorial key that only we know. Now that our valuables are safely stored, we are free to leave. However, here we ask ourselves a question: *'would we leave the front door of the house wide open while we are away?'*. The logical answer is *'No'*. In fact, the first intuitive step to keep our valuables safe is to close and lock the front door of the house irrespective of the additional security, such as the safe box, that we might put in place. By leaving our front door wide open, we are effectively inviting thieves to break in, to go straight to our safe box and then to try to open it by brute force or by simply guessing the security code. It is obvious that the first safety security measure at home is to close the front door of the house. After this basic common sense measure, the safe box is simply an additional security mechanism to reinforce the primary security offered by the front door.

Unfortunately, this primary level security is not provided in wireless communications. Indeed, the broadcasting nature of the radio frequency wireless channel effectively leaves the front door of the transmission (physical layer) wide open to attacks on the confidentiality of the information. Even though conventional strategies seek to secure wireless transmissions by deploying upper layer communications approaches such as encryption, they do not actually stop the attacker from



(a) *Confidentiality based on cryptography*



(b) *Confidentiality based on physical layer security*

Figure 1.1: *Ways to provide security in wireless networks.*

listening our transmission and intercepting the communication. In fact, whilst cryptographic security can act to prevent eavesdroppers from deciphering a confidential message, it does not stop them from receiving the transmitted signal and then going straight to our communication safe box to try to break the cryptographic security by computer *'brute force'*. This security flaw is depicted graphically in the Figure 1.1a.

In this scenario, the obvious counter-attack measure is to *'lock the front door'* of the communication model by securing the actual wireless transmission directly at the physical layer. This is the underpinning idea of '*physical layer security*'; a new security framework that allows us to effectively secure the wireless communications by exploiting the intrinsic characteristics of the wireless communications channel, such as the unique and random nature of the radio links between transmission. The objective is to incorporate security strategies right down at the transmission level, thus preventing attackers from even intercepting the encrypted message. Figure 1.1b illustrates how physical layer security acts over a wireless network.

1.3 Securing wireless networks at the physical layer

Physical layer security evolved from information theory and has been enriched by signal processing algorithms to introduce a set of techniques that offer wireless secrecy at the transmission level. It is particularly attractive to sophisticated wireless infrastructures that require a strong level of security or to networks with computationally limited resources. In the first case, securing sensitive information justify the cost in terms of capacity and quality that deploying physical layer security would demand on the network. In the second scenario, physical layer security can offer confidentiality services to networks that cannot afford computationally demanding cryptographic services. This is the case of body area sensor networks or smart grid networks, where security services have to be addressed from a novel point of view to ensure a good level of security under very tight power and implementation complexity budget constraints [7]. In this context, physical layer security can be one of the enabling tools to secure the emerging *'Internet of Things'*.

Physical layer security is based on the *'wiretap channel'* model that prevents eavesdropping attacks without cryptography by creating significantly stronger

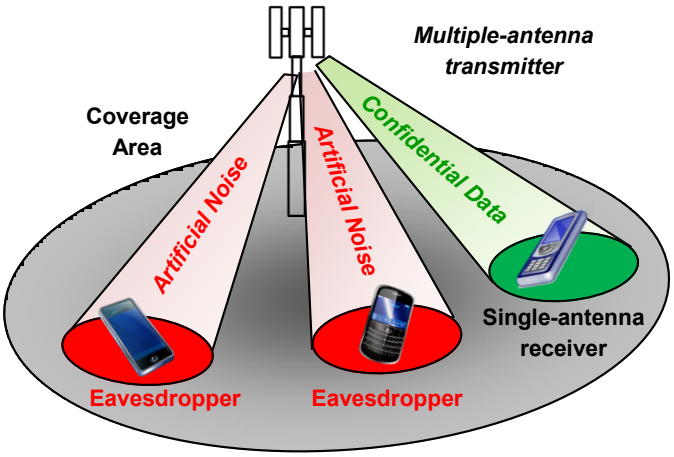


Figure 1.2: *Example of a network secured at the physical layer by steering the information towards the intended receiver and simultaneously jamming the eavesdroppers.*

signals at the intended receiver and simultaneously deteriorating the signal strength at the eavesdropper [8]. This can be done by applying signal processing techniques to multiple-antenna systems that allow the transmitter to steer the confidential message only towards the intended receiver. These techniques exploit the knowledge of the unique mathematical representation of the fading wireless channel between the transmission parties to mathematically convey the information towards the intended receiver. Additionally, multiple-antenna systems enable the transmitter to simultaneously confuse possible eavesdroppers by jamming them with an interfering *'artificial noise'* signal transmitted in such a way that it does not affect the legitimate receiver's quality of reception. This model is graphically depicted in Figure 1.2. Moreover, physical layer security can also offer strategies beyond the wiretap channel model to incorporate authentication mechanisms, distil secrecy keys for upper-layer ciphering, and code the information for secrecy to provide a reliable and secure system.

Physical layer security has become a popular research topic in the academic community that has foreseen the potential that this field has to offer to wireless security. Physical layer security has been nurtured by contributions from both the information-theoretic and the signal processing research communities. Indeed, during the last years there has been a remarkable amount of active research in physical layer security as evidenced in recently published books [9, 10], special

issues of top technical journals being devoted entirely to security in the physical layer [11, 12, 13] and special sessions in important technical conferences across the world exclusively centred on this topic.

In contrast to the huge academic interest and large theoretical work carried out in physical layer security, we notice a lack of practical proof of concept of operative wireless networks secured at the physical layer. The reasoning behind this fact is that there is still required fundamental theoretical research in order to answer crucial questions that will underpin the practical realisation of physical layer security. Particularly, this research has to marry theoretical solutions with practical deployments to allow the development of commercial networks. Additionally, current physical layer security endeavours address confidentiality issues in an isolated fashion, based on many idealised, non-practical system assumptions. Most importantly, physical layer security research currently does not consider a holistic design strategy towards practical implementations.

In this thesis we attempt to answer some of these open questions by devising signal processing transmission mechanisms to address practical issues that wireless security faces.

1.4 Objective

This thesis aims to provide efficient signal processing strategies to secure multiple-antenna networks at the physical layer against eavesdropping attacks; that is, attackers that listen to the communication and capture the transmitted information without transmitting any information.

With this objective in mind, we optimise multiple-antenna transmission strategies to mathematically steer the confidential message towards the intended receiver, and, at the same time, broadcast a jamming signal to confuse the eavesdroppers. The idea is to deliver wireless transmission strategies that not only secure the network but also offer good signal quality at the receiver. These transmission schemes have to provide valid answers to open questions in physical layer security arising from practical issues that pose serious security threats. In particular, we devise transmission schemes that consider constrained transmission resources in terms of power and antennas, limited or erroneous information regarding the link

between the transmission parties, and eavesdropping attackers that take advantage of any opportunity to threaten the physical layer based security.

To deliver this objective, we use mathematical tools, such as stochastic analysis, convex optimisation, linear algebra and statistical analysis, which through signal processing schemes enable transmission strategies that can cope with the security demands of current and future wireless networks.

1.5 Outline

This thesis is divided into seven chapters.

- *Chapter 2* covers physical layer security concepts from an information theoretic perspective. Particular attention is devoted to the wiretap channel as the underpinning model for eavesdropping attacks in multiple-antenna networks. Here the novel contribution of this thesis and the assumptions used throughout are detailed.

- *Chapter 3* addresses the threat of hidden eavesdroppers strategically located close to the transmitter to improve their chances to retrieve the confidential communication. The solution proposed is an outage based transmission technique that distributes the power between the information and the jamming signal to guarantee a high probability of secrecy. The deployment of a physical eavesdroppers-free area is proposed to prevent close quarter attacks.

- *Chapter 4* provides a solution to the practical problem arising from the lack of accuracy in the estimation of the link between the transmission parties. A robust transmission endeavour is devised to maximise the secrecy and also to reduce the use of power, even in the presence of errors in the mathematical representation of the link between the transmitter and receiver.

- *Chapter 5* presents a study about the possible practical contribution of frequency dispersive channels towards securing multiple-antenna networks. Here, we analyse the possible threats to the security posed by a powerful multiple-antenna attacker.

- *Chapter 6* introduces an alternative to secure resource constrained wireless systems at the physical layer by interfering attackers jointly from both the receiver and from the transmitter. The jamming source selection depends upon the transmission conditions and the availability of resources. We present techniques to reduce the level of associated complexity to secure the communication at the two legitimate ends of the transmission.

- *Chapter 7* concludes the thesis by summarising the most important insights and contributions presented in this research study. Moreover, new pathways for further research are presented and a brief discussion about the challenges that the physical layer security techniques introduced here face in terms of their implementation.

1.6 Notation

The following notation is used throughout this thesis. Boldface capital and lower case letters denote matrices and vectors respectively. $\mathbf{0}$ and $\mathbf{0}_N$ are respectively an N-size vector and an $N \times N$ matrix with all the elements zero. $\mathbf{I}_N$ denotes an $N \times N$ identity matrix. $\mathbb{C}^N$ denotes the set of N-dimensional complex vectors while $\mathbb{C}^{N\times M}$ denotes the set of the $N \times M$ dimensional complex matrices. $\mathbf{A}^H$, $\mathrm{Tr}(\mathbf{A})$, $\mathbf{A}^\dagger$, $\mathrm{rank}(\mathbf{A})$ and $\mathrm{vec}(\mathbf{A})$ denote the Hermitian (conjugate) transpose, the trace, the pseudo-inverse, the rank and the vectorisation operations of the matrix $\mathbf{A}$ respectively. $\mathbf{A} \succeq \mathbf{0}$ means that matrix $\mathbf{A}$ is a Hermitian positive semidefinite while $\mathbf{A} \succ \mathbf{0}$ means that $\mathbf{A}$ is a Hermitian positive definite matrix. The expressions $||\mathbf{A}||_F$ and $||\mathbf{a}||$ denote the Frobenius norm of the matrix $\mathbf{A}$ and the Euclidean norm of the vector $\mathbf{a}$. $\otimes$ represents the Kronecker product operator and $\mathrm{Re}\{\cdot\}$ the real part of a complex number. $\mathbb{E}\{\cdot\}$ is the statistical expectation operator and $\mathbb{P}$ denotes probability. $[a]^+$ represents $\max\{a, 0\}$. Finally, $\mathbf{a} \sim \mathcal{CN}(\boldsymbol{\alpha}, \boldsymbol{\Sigma})$ means that $\mathbf{a}$ is a random vector following a complex circular Gaussian distribution with mean $\boldsymbol{\alpha}$ and covariance matrix $\boldsymbol{\Sigma}$.

Chapter 2

Physical layer security

> 'Listen, do you want to know a
> secret? Do you promise not to tell?
> Closer, let me whisper in your ear,
> say the words you long to hear:
> I'm in love with you. I've known
> the secret for a week or two.
> Nobody knows, just we two.'
>
> J. Lennon, P. McCartney

Information confidentiality is a matter of paramount importance in wireless networks. Indeed, wireless devices have become increasingly pervasive offering a fertile ground for security attacks that jeopardise the privacy and integrity of wireless communications. The reason behind this vulnerability is the fact that wireless systems are particularly susceptible to security attacks because of the inherent openness of the transmission medium that leaves sensitive information within the reach of malicious eavesdroppers. As a result, data confidentiality has become a growing concern which is demanding new strategies, both from academia and industry, for locking the wireless communication in a holistic fashion starting from the transmission level upwards. This is the principal objective of physical layer security which uses signal processing techniques to ensure a level of information-theory security and to complement pre-existing, upper-layer cryptographic security services.

The purpose of this chapter is to provide a brief synopsis of the fundamental concepts that enable physical layer security and how it compares to and complements traditional cryptographic security policies. In this context, this chapter describes the open problems in multiple-antenna physical layer security, which are addressed in this thesis, and the novel contributions being developed towards their solution. Finally, we point out complementary, emerging physical layer security approaches that can enhance wireless security services by exploiting the intrinsic characteristics of the randomness and uniqueness nature of the wireless channel.

2.1 Information-theoretic security

Information-theoretic security is commonly accepted as the strictest form of security. It is based on the combination of cryptographic schemes with channel coding techniques to exploit the randomness of the wireless communication channel to prevent an eavesdropper from decoding a confidential message [14]. In the seminal work in [15], Shannon postulated the information-theoretic foundations and introduced the concept of perfect secrecy between a legitimate pair of communicating parties in the presence of an unauthorised receiver. Here, a confidential message M is coded into a codeword C through a non-reusable private key K and then it is transmitted over a noiseless channel. Perfect secrecy is attained when the eavesdropper can only randomly guess the confidential message in spite of having an identical copy of the intended receiver's coded message, being aware of the coding strategy applied and having infinite computational power at its disposal (although not having access to the key). This is achieved by ensuring that the message M and the output of the encoder C are statistically independent; in other words, the mutual information between M and C is exactly zero; i.e., $I(M;C) = 0$. This condition can only be guaranteed if the secret key has at least as much entropy as the original message; therefore, ensuring perfect secrecy requires that the secret key K to be at least as long as the message M. The immediate consequence of this remarkable conclusion is the impossibility to efficiently develop practical coding schemes capable of attaining perfect secrecy.

Motivated by these findings, Wyner considered the imperfections in the communication introduced by the channel and introduced the concept of the degraded wiretap channel [16]. This model was later extended to the non-degraded wiretap

channel by Csizar and Korner in [17]. These two ground-breaking contributions proved that there exist channel codes that can guarantee a low error probability at the destination subject to confidentiality constraints at the eavesdropper. Here, the enabling condition is to guarantee the existence of a quality advantage between the legitimate parties' channel and the eavesdropper's counterpart. However, this condition can be seen as restrictive; therefore, Diffie and Hellman in response developed an alternative method that ignores the effect of the channel and introduces the basic principles of public-key cryptography [18]. This work paved the way for the development of computation-based security to provide information confidentiality based on cryptographic algorithms that later would become the security scheme adopted by modern communication systems.

2.1.1 Cryptographic solutions for wireless networks

Confidentiality services in wireless networks have been traditionally addressed at higher layers of the communication model using cryptographic based protocols. For instance, current commercial Wi-Fi systems use Wi-Fi protected access (WPA) and WPA2 as security services which are based on cryptographic schemes, such as the temporal key integrity protocol (TKIP) and the counter mode cipher block chaining message authentication code protocol (CCMP) [19]. Both of these protocols use the advanced encryption standard (AES) that is a symmetric-key algorithm. In other words, a common key is used at both sides of the communication for encrypting and decrypting the confidential data. On the other hand, cellular 2G GSM networks uses the A3, A8, A5/2 and A5/3 stream ciphers for ensuring over-the-air voice privacy while 3G UMTS and 4G LTE systems use KASUMI block cipher based protocols [20]. All of these confidentiality services use symmetric-key cryptography to encrypt the data sent over the wireless link. In these cellular networks, the ciphering secret key is generated using an authentication key stored in the subscriber identity module (SIM) card of the device.

These symmetric encryption algorithms raise serious practical issues regarding the key distribution and management, effectively posing a major threat to computation-based data confidentiality. As an alternative to tackle these issues, asymmetric cryptographic algorithms such as RSA public-key cryptosystems do not require private key exchange; instead, they rely on highly computational, complex operations, such as factoring the product of two large prime numbers. Here,

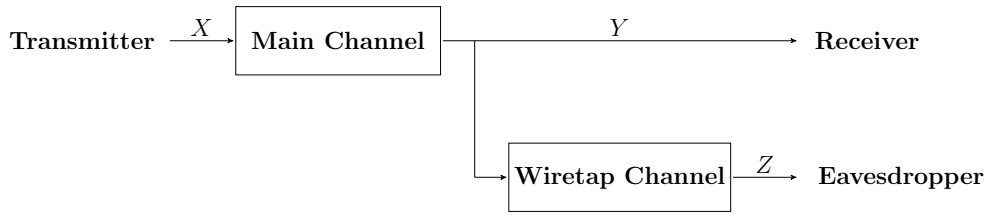
the security lies in the assumption that it is computationally infeasible for the attacker to recover the secret key from the publicly shared key due to the hardness of reversing the mathematical operations involved in its calculation [21, §8]. In other words, information confidentiality relies on a computational restriction imposed on the eavesdropper side that cannot be guaranteed in practical systems. Indeed, this premise becomes a serious vulnerability particularly due to the current relentless growth of computational power [1].

Beyond these intrinsic vulnerabilities of cryptographic schemes, the implementation stage in practical protocols of these algorithms has introduced major security flaws that have been widely exploited in order to break computational-based security. These attacks target vulnerabilities at the design and implementation stages, the insecure and naive behaviour of network users, the trust model of the system, and the physical deployment of the algorithms into the hardware [5]. As a result, we have seen a dramatic increase in the number of publicly known attacks to the security of wireless networks. For example, recently, a fundamental flaw in WPA2, named Hole 196, exposed design vulnerabilities at the authentication stage of Wi-Fi networks that can be exploited to perpetrate eavesdropping and man-in-the-middle attacks [22].

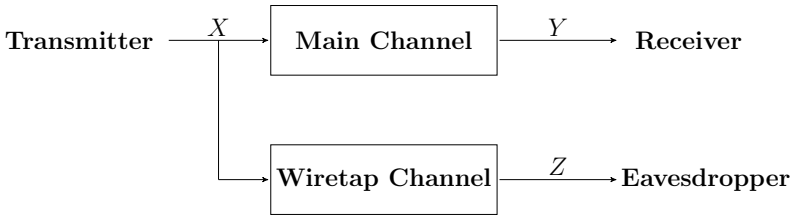
The security weaknesses in cryptography have motivated a resurgence of interest in information-theoretic secrecy operating at the physical layer. The objective is to augment already existing upper-layer security measures and therefore provide an holistic multilayer approach to significantly enhance the security of next generation data networks.

2.1.2 The Wiretap channel

In recent years, information-theoretic secrecy has demonstrated that taking advantage of the properties of transmission channels can ensure information confidentiality. Indeed, when the channel between the transmitter and the receiver is better than the one between the transmitter and the eavesdropper, a confidential message can be encoded so that only the intended receiver can reliably decode it. Meanwhile the eavesdropper retrieves nothing from the confidential message. Remarkably, instead of using cryptographic algorithms, this confidentiality is attained by channel coding techniques, known as secrecy or wiretap codes [14]. The transmission rate at which the confidential message can be reliably transmitted



(a) *Degraded wiretap channel*



(b) *Non-degraded wiretap channel*

Figure 2.1: *Wiretap channel models*

towards the intended receiver while keeping the eavesdropper ignorant about the content is referred to as the '*secrecy rate*'.

Information-theoretic security is based on the concept of the wiretap channel, which consists of a transmission source, an intended or legitimate receiving destination and an eavesdropper that attempts to intercept the confidential message conveyed from the transmitter to the receiver. The link between the transmitter and receiver is known as the main channel, while the transmitter to eavesdropper counterpart is denoted as the wiretap or the eavesdropping channel. Both are assumed to be discrete memoryless channels. In this scheme, the transmitter and the receiver agree a publicly-known encoding system. In other words, the eavesdropper is totally aware of the mechanism used to encode the confidential message. Indeed, it is assumed that the wiretapper does not have any computational limitation. In Wyner's degraded wiretap channel model [16], the eavesdropper's received signal is a degraded version of the legitimate receiver's signal (see Figure 2.1a) while in Csiszar and Korner's non-degraded wiretap channel model, the main channel and eavesdropping channels are supposed to be independent from each other (see Figure 2.1b) [17]. The latter is a suitable scenario to model the secrecy problem in wireless communications.

The objective of the wiretap channel is to ensure a transmission rate R in the main channel at which the information leaked to the eavesdropper is negligible.

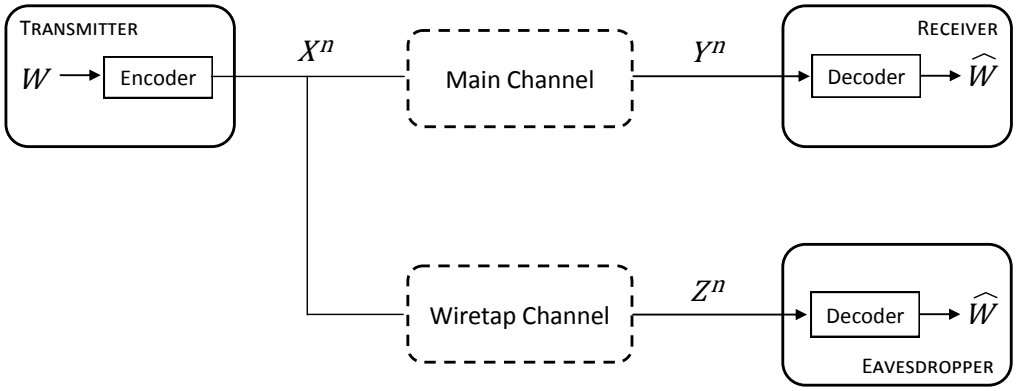


Figure 2.2: *Single-antenna wiretap channel model.*

Bearing this objective in mind, the transmitter encodes the confidential message W into a codeword X^n that is uniformly distributed over $\left\{1, \cdots, 2^{nR}\right\}$, where n is the block length of the communication. The information is transmitted over the main link and the legitimate receiver observes Y^n while the eavesdropper receives Z^n at the output of the wiretap channel. The wiretap channel model described is depicted in Figure 2.2. Here, the equivocation rate at the eavesdropper R_e represents the uncertainty about the message W, and it is given by the conditional entropy function H by

$$R_e = \frac{1}{n} H\left(W|Z^n\right). \tag{2.1}$$

Wyner's notion of security in [16] is defined by requiring that for a sufficiently large n and for every $\epsilon > 0$ it holds

$$R_e - \epsilon \leq \frac{1}{n} H\left(W|Z^n\right). \tag{2.2}$$

Perfect secrecy implies that as n goes to infinite, the information revealed to the eavesdropper vanished; i.e., the eavesdropper's equivocation rate R_e approaches the entropy of the message $H(W)$. Therefore, the information leaked to the eavesdropper is given by the mutual information function I by

$$R - R_e = \frac{1}{n} I\left(W; Z^n\right), \tag{2.3}$$

therefore, when the equivocation rate R_e is arbitrarily close to the information rate R as n goes to infinity and $\epsilon = 0$, then the message W is asymptotically perfectly secure from the eavesdropper. In other words, the eavesdropper's received signal

Z^n does not reveal any information about the confidential message W by simply enforcing

$$\lim_{n\to\infty}\left[\frac{1}{n}I\left(W;Z^n\right)\right]=0. \tag{2.4}$$

It is worth highlighting that Wyner's definition of secrecy in [16] is weaker than the one proposed by Shannon [15] because it assumes that the information leaked to the eavesdropper vanishes in the limit of a long code length. In contrast, Shannon's perfect secrecy requires the mutual information at the eavesdropper to be zero regardless of the code length. Wyner's requirement is called '*weak secrecy*' and it may not be rigorous enough to perfectly secure a system because it does not prevent few bits of the message W being leaked through the eavesdropper's received signal Z^n. As an alternative, this definition has been strengthened by introducing the concept of '*strong secrecy*' which considers that the total amount of information about W, after the eavesdropper observing Z^n, goes to zero as the code length increases towards infinity. In other words, strong secrecy enforces

$$\lim_{n\to\infty} I\left(W;Z^n\right)=0. \tag{2.5}$$

From these definitions, it is clear to see that

$$\text{perfect secrecy} \Rightarrow \text{strong secrecy} \Rightarrow \text{weak secrecy}.$$

Both security requirements, strong and weak secrecy, are valid security definitions that aim to completely confuse the eavesdropper about the message, leaving it no better informed that if it were not receiving any signal and with no other option than to randomly guess the confidential message. The definition of secrecy to be used would depend upon the level of secrecy required by the application. Interestingly, Mauler and Wolf have proven in [23], that in theory, both secrecy constraints are able to attain the same coding rates. However, practical stronger secrecy could be achieved by trading-off against coding rate, thereby reducing the information throughput of the system [24].

A transmission rate that satisfies the secrecy constraints mentioned above is referred to as the '*secrecy rate*' R_S. The '*secrecy capacity*' C_S of the wiretap channel is the supreme of the transmission secrecy rates between the transmitter and the intended receiver at which both reliability and information-theoretic security

against an eavesdropper are guaranteed. In general, the secrecy capacity of a wiretap channel is given by

$$\mathrm{C}_S = \max_{V \to X \to Y,Z} I(V;Y) - I(V;Z), \tag{2.6}$$

where V is an auxiliary variable that allows channel prefixing, which is the process of mapping the message carrying signal to the channel input X. In the case of a degraded wiretap channel as in [16], the legitimate receiver's and the eavesdropper's output channels Y and Z satisfy the Markov chain $X \to Y \to Z$ not requiring prefixing; i.e., $X = V$ is optimal. The degraded model effectively enforces a better quality main channel. Therefore, the secrecy capacity reduces to

$$\mathrm{C}_S = \max_{X} I(V;Y) - I(V;Z). \tag{2.7}$$

This means that, in the case of the Gaussian wiretap channel [25], the secrecy capacity is a function of the mutual information and, therefore, of the Shannon capacities of the main and wiretap channels given respectively by C_M and C_W. This is $\mathrm{C}_S = \mathrm{C}_M - \mathrm{C}_W$, which means that a main channel with a larger capacity than the eavesdropping link (i.e., main channel is better than wiretap one) yields non-zero secrecy capacity.

The secrecy capacity in (2.7) is achieved by a stochastic encoder. This means that a Gaussian input X maximises the difference in mutual information between the main and eavesdropping links and therefore delivers the largest secrecy capacity [25]. This condition implies that the confidential message is encoded using a random Gaussian codebook. However, in practical communications systems, the input codebooks consists of symbols from a finite-alphabet. As a result, the achievable secrecy capacity for a finite-alphabet input scenario can be dramatically reduced compared with the idealistic Gaussian codebook's secrecy capacity [26, 27].

It has to be noted that the above secrecy capacity expressions are derived based on the assumption that the eavesdropping channel's knowledge is perfectly available at the transmitter. This condition (arguably) is not practical. As a result, alternative secrecy metrics using the eavesdropper's channel statistics have been introduced, such as outage probability performance metrics. This has been particularly useful for addressing fading channels. For example, in [28], Barros and Rodrigues

analysed the outage probability and outage secrecy capacity of slow fading channels, showing that information-theoretic security can be attained, even when the eavesdropper's average signal-to-noise ratio (SNR) is better than the legitimate receiver's. In the case of fast varying fading channels, a message can be encoded across a large number of channel states to define an alternative secrecy metric based on the ergodic secrecy rate [29]. In this context, Li et al. showed in [30] that a non-zero ergodic secrecy rate can be achieved even if on average the wiretap channel is better than the main link. These two conclusions are based on the idea of opportunistic transmissions during the time intervals when the main channel is better than the eavesdropping one. It is worth pointing out that these secrecy metrics are weak owing to the fact that confidentiality is provided in a probabilistic or ergodic sense.

The total lack of information about the eavesdropper channel is a challenging problem from the point of view of the security. In this context, in [31], Liang et al introduce the concept of the compound wiretap channel to understand the information-theoretic limits of the wiretap channel that has no information regarding the eavesdropper. Here, security is enforced in any of the assumed states that the eavesdropper's channel can take from a finite known set of states. The compound wiretap channel can also be viewed as a multicast channel with multiple eavesdroppers where the transmitter conveys information towards all the receivers while keeping the information secret from all the wiretappers. This model of the wiretap channel has paved the way to address security issues in multi-user networks [32].

Finally, the information-theoretic capabilities of multiple-antenna systems have been studied through the multiple-antenna wiretap channel [33, 34, 35]. These contributions and the popularity of multiple-antenna systems have motivated a plethora of both information-theoretic studies about the secrecy capabilities of multiple-antenna systems and also about signal processing transmission approaches to enable confidential transmissions at the physical layer using the wiretap channel structure [36]. This thesis focuses on the latter (signal processing) scenario and seeks to deliver transmission strategies based on multi-antenna systems to devise innovative solutions to practical problems in securing multiple-antenna wireless networks.

2.2 The contribution of this thesis

In this thesis we study security in multiple antenna systems, both, in multiple-input single-output (MISO) and multiple-input multiple-output (MIMO) systems. We use information-theoretic concepts to devise novel signal processing techniques to address practical problems arising from securing wireless networks. In particular, we exploit the multiple-antenna degree of freedom to dynamically convey sensitive information in a secure fashion towards the legitimate receiver while the transmitter broadcasts an interfering signal to deteriorate the eavesdroppers' signal quality [37]. This masked channel precoding transmission technique has been proven to enhance the security of wireless transmissions in terms of secrecy rate improvements; however, it faces many open issues. The remainder of this thesis will focus on the following challenging problems:

- The security threat that multiple unknown eavesdroppers pose to the network. These attackers can be strategically located in the surroundings of the transmitter to increase their likelihood of successfully intercepting confidential information.

- The transmitter may only have inaccurate or outdated information about the intended receiver's channel.

- Achieving secure communications in networks with constrained resources; particularly, when the transmitter has limited resources in the form of transmitting antennas and power.

- Guaranteeing acceptable levels of quality at the intended receiver and at the same time providing an information-theoretic security to avoid eavesdropping attacks.

In this context, in this thesis we introduce efficient and innovative signal processing mechanisms to tackle these technical challenges. The novel contribution is summarised as follows:

- Guaranteeing a high probability of secrecy in the presence of unknown eavesdroppers by an intelligent outage based power allocation between information and the interfering signal.

- A study about the impact of the location of the eavesdroppers on the secrecy of the multiple-antenna wireless network.

- An enhancement in the wireless secrecy by avoiding close-quarters eavesdropping attacks through the deployment of an exclusion zone (named the protected zone). This security area also allows an efficient use of the available power. A strategy is presented to define the size of this exclusion zone in order to meet probabilistic secrecy objectives.

- A robust transmission scheme to maximise the secrecy rate when the transmitter has inaccurate (erroneous or outdated) information about the main channel under the presence of a close and unknown attacker.

- A robust transmission scheme to cope with uncertainties in the transmitter-to-receiver link's information to ensure an average secrecy rate where the size of the protected zone and the amount of power used is minimised by prioritising the use of resources.

- A study of the contribution of frequency selectiveness towards securing multiple-antenna wireless networks using OFDM signalling.

- A secure transmission mechanism when the jamming signal is jointly transmitted from both legitimate multiple-antenna communication parties; i.e., the transmitter and the receiver. This strategy is particularly attractive to a resource constrained transmitter conveying an information-theoretically secure confidential message.

- A robust scheme where the optimal transmission strategy is sought to maximise the secrecy rate in global and individual power constrained networks. Here the receiver and the transmitter can both jam the eavesdroppers, considering a degree of uncertainty in all the communication channels.

These signal processing channel precoding techniques offer valid answers to security problems in wireless networks by designing efficient transmission schemes that can cope with the security and quality requirements of practical wireless networks. Indeed, the proposed solutions have a great potential to be exploited by the telecommunications industry because they are flexible, scalable and cost-effective

ways to provide secure communications at the physical layer. These strategies not only tackle current security flaws, but also pre-empt new future security threats.

2.3 Assumptions used throughout this thesis

In this section we explicitly state the assumptions made and the definitions used throughout this thesis. These considerations will allow us to better contextualise the contribution and the scope of the work presented here. The assumptions are as follows.

- We address security from an information-theoretic point of view. As such, strong security is enforced by secrecy metrics such as secrecy rate and secrecy capacity. Security is provided at the physical layer without relying on upper layer cryptographic algorithms. Therefore, the analysis of the performance of complementary cryptographic techniques is beyond the scope of this thesis.

- It is assumed that legitimate users have been authenticated and their identities have been proven. In other words, the legitimate transmitter and receiver pair have previously gone through an authentication process and they do not pose a threat to the transmission. Impersonation attacks such as man-in-the-middle are outside of the context of this study.

- We consider the existence of a feedback channel between the transmitter and the eavesdropper. Therefore, both the legitimate transmission parties are aware of the channel state information (CSI) of their link; i.e., we use coherent detection. We consider perfect channel reciprocity; that is the uplink and downlink channels are subject to the same channel impulse response. We assume an error-free CSI unless it is stated otherwise; particularly, when robust problems are addressed to deal with mismatched CSI.

- We assume that the symbols transmitted are from a Gaussian codebook; that is, an non=practical infinite and random code alphabet.

- We address unicast single-user communications that may be eavesdropped by multiple attackers. In other words, a transmitter conveys a confidential

message to only one intended receiver at a time over the downlink channel in the presence of (an) eavesdropper(s). The receiver acts as a passive entity on the communication, and when the receiver communicates with the transmitter over the uplink channel,the receiver and transmitter effectively switch roles to establish again the one-direction wiretap channel model.

- We consider flat quasi-static fading wireless channels unless the contrary is clearly specified when we deal with frequency selective channels. In other words, the channel's fading coefficients remain constant during the duration of the transmission of the symbol and change randomly for the next one.

- We do not impose any computational or processing limitations at the eavesdropper side. However, depending upon the problem topology, we assume a single-antenna or multiple-antenna eavesdropper for the MISO and MIMO cases respectively.

- We address pure eavesdropping attacks in the sense that the attacker does not transmit information or alter the data conveyed by the transmitter. The attacker neither transmits an interfering signal to jam the communication between intended parties. In other words, the study of man-in-the-middle or jamming attacks are out of the scope of this thesis.

- Throughout this thesis we use the non-degraded Gaussian wiretap channel model. We use the '*main link*' to refer to the transmitter to receiver link, and '*eavesdropping*' or '*wiretap*' channel to refer to the transmitter to eavesdropper channel. We use the terms '*eavesdropper*', '*attacker*', '*wiretapper*' to refer to the malicious adversary pretending to overhear the confidential communication.

- Following the notation used in the wireless secrecy literature, we refer to the *'passive eavesdropping'* case as the scenario when the transmitter is not aware of the instantaneous CSI of the attackers. On the other hand, we refer to an *'active eavesdropping'* scenario when the eavesdroppers' instantaneous CSI is perfectly known by the transmitter.

2.4 Physical layer security beyond the wiretap channel model

The implementation of the wiretap channel model requires coding for secrecy. Indeed, signalling and coding techniques used in tandem can be particularly powerful towards the realisation of practical physical layer security [38]. This need has underpinned the construction of appropriate practical code designs, not only to offer error correction capabilities, but also to provide information-theoretic security. These codes have been based on low density parity check codes [39] and on nested coding [40].

Remarkably, in [23], Maurer introduced a strategy to achieve a positive transmission rate even when the main link channel is worse than the one that the eavesdropper observes. This work was based on the joint development of a secret key by the legitimate transmission pair communicating over a public, and therefore, insecure error-free feedback channel. This seminal work paved the way for a new field of research in information-theoretic secrecy, and in contrast to Wyner's key-less wiretap channel secrecy model, a key is used to secure information in practical networks. This work generated many contributions that exploit common randomness, take advantage of distillation, information reconciliation and privacy amplification procedures to agree on a secret key between the legitimate communication parties [41, 42, 43, 44]. The general idea is to exploit the randomness and uniqueness of the wireless channel to generate a key to secure confidential information.

Finally, it is worth remarking that the wiretap channel model is based on the assumption of a pre-authenticated main channel. In this context, authentication initiatives have been developed to provide alternative ways to validate the identity of the legitimate users using the transmission physical media. For instance, the transmitted message can be fingerprinted as a way to validate legitimate users' credentials [45].

All the aforementioned security techniques have the potential to complement and develop the level of information-theoretic security of the wiretap channel model towards practical implementations. Therefore, there is a clear necessity for a holistic multi-layer approach to combine secrecy strategies and then provide effective techniques to combat the current and future security threats faced by wireless communications.

It is important to remark that the aim of this thesis is to study signal processing techniques to provide information-theoretic security in single-user multiple antenna wireless networks by using the wiretap channel model. Therefore, security strategies such as those mentioned in this section, are out of the scope of this work. However, it is important to highlight their security potential to complement and enhance the security provided by the transmission strategies introduced in this work.

Chapter 3

Outage based physical layer security for MISO systems

> 'Apparently Seldon had been working up to his last moments on psychohistorical equations [...] it has been said that Hari Seldon left this life as lived it, for he died with the future he created unfolding all around him.' - Encyclopedia Galactica
>
> Isaac Asimov

In this chapter we address physical layer security in multiple-antenna communication systems in the presence of unknown passive eavesdroppers. Here, the additional degree of freedom that the multiple-input single-output channel (MISO) introduces over the system is exploited to enhance the security of a wireless network. We investigate a probabilistic resource allocation strategy to devise an efficient solution to tackle practical security challenges that MISO wireless networks face. For instance, we address threats arising from attackers that remain hidden in the network and might be strategically located near to the transmitter to receive a favourable signal and so effectively jeopardise the security of a transmission. Providing security in this scenario is challenging; particularly, when the availability of resources at the transmitter is limited; therefore, it is necessary

to use them efficiently to provide both security and good quality of service at the intended receiver.

To address the aforementioned practical problems, in this chapter we use a *'masked beamforming'* strategy that uses multiple-antennas at the transmitter to steer the information towards the intended receiver and to broadcast a jamming signal in the form of '*artificial noise*' to confuse passive eavesdroppers. In this scenario, providing total confidentiality is not possible; therefore, a probabilistic treatment of secrecy is necessary. Therefore, in this chapter we introduce two outage based power allocation mechanisms to guarantee a given probability of secrecy. We incorporate a study of the impact on the security of the distance between transmission parties by deploying a '*protected zone*' to quantify the cost in terms of power of providing secrecy under the presence of an eavesdropper located in the immediate vicinity of the transmitter.

The structure of this chapter is as follows. Section 3.1 provides a literature background to the existing signal processing techniques addressing physical layer security in MISO networks. In section 3.2 we model the MISO system under the presence of unknown eavesdroppers. Subsequently, in section 3.3 we introduce the first outage power allocation technique based on Quality of Service (QoS) constraints. The next section (3.4) features the second outage based technique that allocates resources considering the distance between transmission parties when a protected zone is deployed. Finally, section 3.5 concludes this chapter.

3.1 Physical layer security in MISO systems

The degree of freedom that multiple-antenna systems introduces in wireless communications offers not only the possibility of improvements in capacity and quality but also improvement in security. Indeed, the use of multiple-antenna techniques powered by signal processing algorithms has attracted the attention of the research community as a valid framework to provide new means to secure wireless networks [36]. In this context, the secrecy capabilities of multiple-antenna channels is studied for the first time by Shaffie and Ulukus in [46] and by Khisti et al. in [34, 47, 48] where the remarkable contribution that multiple-antennas introduce into the wireless security is highlighted.

In the case of a fully characterised MISO system, a transmission strategy using a Gaussian codebook with rank-one covariance matrix has been proven to be the optimal transmission strategy to achieve the secrecy capacity C_S [46]. In other words, when the CSI of the intended receiver and the eavesdropper are both perfectly known (i.e., active eavesdropping) and the channel input is restricted to Gaussian signalling, then the secrecy capacity is achieved by beamforming as close as possible to the intended receiver's channel direction and as orthogonal as possible to the eavesdropping channel direction. Interestingly, in [46] Shafiee also shows that in the case when the CSI of the eavesdropper is not available (i.e., passive eavesdropping), then the best secure strategy is to beamform towards the legitimate receiver. A similar study is carried out later in [49, 50] through semidefinite programming (SDP) proving that transmit beamforming is also a secrecy rate optimal strategy for MISO networks in the presence of multiple single-antenna eavesdroppers.

3.1.1 Masked beamforming

Beamforming has become a popular transmission mechanism to secure MISO communications; moreover, this technique can elegantly be enhanced by broadcasting *artificial noise* (AN) to confuse passive eavesdroppers [51]. Indeed, the additional degree of freedom that the multiple-antenna channel introduces allows simultaneously conveying the information towards the intended receiver and broadcasting a jamming signal which does not affect the receiver [37]. The resulting technique coined as *'beamforming and artificial noise generation'* or *'masked beamforming'* has received a lot of research attention as an effective way to secure networks where the eavesdroppers remain hidden in the network and therefore their CSIs are unknown or only partially known [52]. In the case of pure passive eavesdropping cases the information is steered towards the legitimate receiver while the AN is broadcast over the nullspace of the legitimate receiver channel's signature, so it does not 'jam' the receiver [53].

The lack of knowledge about the single-antenna eavesdropper's CSI prevents the beamforming strategy from achieving perfect secrecy because the multiple-antenna transmitter cannot null the eavesdroppers by conveying the confidential message over the eavesdropper channel's nullspace. Therefore, confidential information can be leaked to the attacker compromising the security. Under this

scenario, like in the single-antenna transmitter case [14], a statistical treatment of secrecy is necessary to formulate ergodic and outage definitions of secrecy. In the first case, the statistical information of the eavesdropper's link CSI is assumed to maximise (on average) the MISO ergodic secrecy rate [54]. Meanwhile, in the second case, the statistical information of the wiretap CSI is used to characterise the probability of having a secure communication [55, 56]. In all these contributions it is shown that either achieving an arbitrary low secrecy outage probability or maximising the ergodic secrecy rate cannot be achieved without judiciously adjusting the power allocated for the information and for the AN. In this context, in [57, 58] Zhou et al. introduce a power allocation mechanism to maximise the ergodic secrecy rate of MISO channels under the presence of unknown eavesdroppers showing that equal power distribution between information and AN is near-optimal as a strategy to maximise on average the secrecy rate. It is important to point out that these contributions do not address the power distribution problem from an outage perspective to ensure a given probability of secrecy.

All of the aforementioned transmission strategies consider the secrecy rate as the natural metric that determines the secrecy capabilities of the MISO link. However, a valid alternative to define a secure system is by enforcing *Quality of Service* (QoS) constraints at the transmission parties. In other words, a system is considered secure when the quality of the signal at the intended receiver, given by the SNR, satisfies a reliability constraint, and, at the same time, the quality signal of the eavesdropper is below a maximum security tolerable level [53, 55]. This strategy effectively fixes the secrecy rate to a value given by the difference in capacity between the required QoS thresholds at the legitimate receiver and eavesdropper. Using this definition of security, Liao et al. present in [59] an optimised masked beamforming technique to optimise the beamforming vector and the AN transmission covariance matrix to satisfy QoS requirements in a power constrained MISO network. This setup can deal with the passive eavesdropping case by assuming knowledge of the second order statistics of the eavesdropping channel; however, likewise [57, 58], only an average QoS based security is ensured rather than guaranteeing an outage based probability of secrecy.

3.1.2 Impact of the distance between transmission parties

Owing to the channel path-loss effect, the distance between the transmission parties is of prime importance in order to guarantee secrecy. In this context, single-antenna receivers and eavesdroppers randomly scattered in the space are considered to study the secrecy capacity between nodes [60]. The impact on throughput due to the inclusion of security constraints in a network with single-antenna random nodes distributed according a Poisson point process is investigated in [61]. Subsequently, in [62] a statistical framework is introduced to quantify the probability of secrecy in the presence of unknown eavesdroppers whose locations and channels are unknown. These approaches are extended to the case when masked beamforming is used as multiple-antenna security strategy in [63]. It is important to highlight that even though all these strategies consider the effect of the location of the nodes and the path losses associated, none of them consider the worst-case for the security; i.e.; issues that emerge when an attacker is located in the vicinity of the transmitter.

A major threat to security arises when unknown eavesdroppers are physically present in the immediate vicinity of the transmitter. In this scenario, and due to the reduced path losses, the quality of the eavesdropper's received signal is likely to be better than the further legitimate receiver counterpart, thus threatening the overall security of the system. Therefore, avoiding intruders close to the transmitter is of paramount importance in achieving a secure transmission. This can be realised, as is done in ad-hoc networks in [64], by controlling any nodes' presence in the transmitter's surrounding area. This idea is exploited in [65] where the transmitter is assumed to be able to detect eavesdroppers inside a '*Secrecy Guard Zone*' and then define its transmission strategy based on their existence or absence. By contrast, Chang et al. suggest in [66] that an eavesdroppers-free '*Secure Zone*' can significantly improve the secrecy rate and/or save transmit power in MISO networks; however, no mechanism is devised to quantify either the size of the exclusion area or its impact over security.

3.1.3 This chapter's contribution

In this chapter we endeavour to offer transmission strategies to address the important open issues regarding the distribution of power between information and AN

to enforce a given probability of secrecy and the security threat resulting from a close eavesdropper. Therefore, two probabilistic resource allocation strategies are introduced as follows

- The first outage based allocation strategy distributes the available power between information and AN to guarantee a given probability of secrecy that is defined based on QoS constraints to be satisfied at the transmission parties.
- The second resource distribution approach considers the effect of the distance between nodes to set the size of an eavesdropper exclusion zone (called the *Protected Zone* (PZ)) and the amount of power devoted for information and AN. Here a given probability of secrecy defined by the MISO secrecy rate is enforced.

These two outage based resource allocation techniques are based on formulating minimisation problems where the likelihood of achieving secrecy is defined by probabilistic constraints. These constraints are written as Gaussian quadratic forms whose CDF is evaluated by using step functions and their complex integral representation. This formulation allows us to solve the first outage based QoS power allocation problem by a closed-form expression while the second resource distribution problem is solved by numerical algorithms. Moreover, two particular cases of the second problem are studied offering valuable insight into the resource allocation behaviour when the transmission parties are equidistant and when the protected zone vanishes letting the attackers approach the transmitter without restriction. The numerical results show that the two introduced allocation strategies can guarantee a high probability of secrecy by prioritising the use of the available resources; i.e., the transmit power and the size of the protected zone. The improvement in secrecy obtained is illustrated when this approach is benchmarked against an existing technique that does not consider outage formulation and therefore can only provide security in average.

3.1.4 Very recent contributions

It is worth pointing out some important works on MISO security based on an outage formulation that have either appeared in the literature later than the original publication date of this work, or have been inspired by the ideas presented in this

chapter. In [67], Gerbracht et al. minimise the outage probability of secrecy of masked beamforming when the transmitter has only partial information about the eavesdropping channel. The analysis is generalised to the perfect eavesdropper's CSI knowledge and the unavailability of the eavesdropper channel signature cases showing that AN is not necessary for active eavesdropping. In [68], Zhang et al. design a masked beamforming system considering the power allocation and the rate parameters of the wiretap code to maximise the secrecy throughput constrained by a maximum allowable secrecy outage probability. Recently, in [69] the impact of the AN over the secrecy of a large scale decentralised MISO network was studied where the nodes' location follow Poisson point processes. In addition, the outage based power allocation strategy work presented in this chapter motivated the closed-form power allocation between information and AN introduced in [70] that minimises the secrecy rate outage probability in power constrained MISO networks. Finally, in [71] our novel concept of a the protected zone was used to study the security performance of a network with unknown eavesdroppers randomly distributed outside of the exclusion area.

3.2 System model

In this section, we model a MISO system in the presence of multiple unknown and non-colluding eavesdroppers; i.e., the eavesdroppers do not work in a cooperative fashion. The wireless secrecy model is followed, so the legitimate transmitter and receiver are named 'Alice' and 'Bob' respectively while the eavesdroppers are collectively referred to as 'the Eves'.

Alice is equipped with $N_t \geq 2$ antennas while Bob and all of the K Eves each have a single antenna. The Alice-to-Bob and Alice-to-the k^{th} Eve flat-fading channel vectors are denoted by $\mathbf{h}_b \in \mathbb{C}^{N_t}$ and $\mathbf{h}_{e_k} \in \mathbb{C}^{N_t}$. In order to consider the propagation path loss effect the distance between transmission parties is considered; therefore the channel vectors are given by $\mathbf{h}_b = r_b^{-\frac{\alpha}{2}} \tilde{\mathbf{h}}_b$ and $\mathbf{h}_e = r_{e_k}^{-\frac{\alpha}{2}} \tilde{\mathbf{h}}_{e_k}$ where r_b and r_{e_k} are the Alice-to-Bob and Alice-to-the k^{th} Eve distances and α is the path loss exponent ($\alpha \geq 2$). Finally, $\tilde{\mathbf{h}}_b$ and $\tilde{\mathbf{h}}_{e_k}$ are mutually independent small scale fading channel vectors that are not affected by the communication range. The vector $\tilde{\mathbf{h}}_b$ has uncorrelated zero-mean Gaussian distributed elements with variance

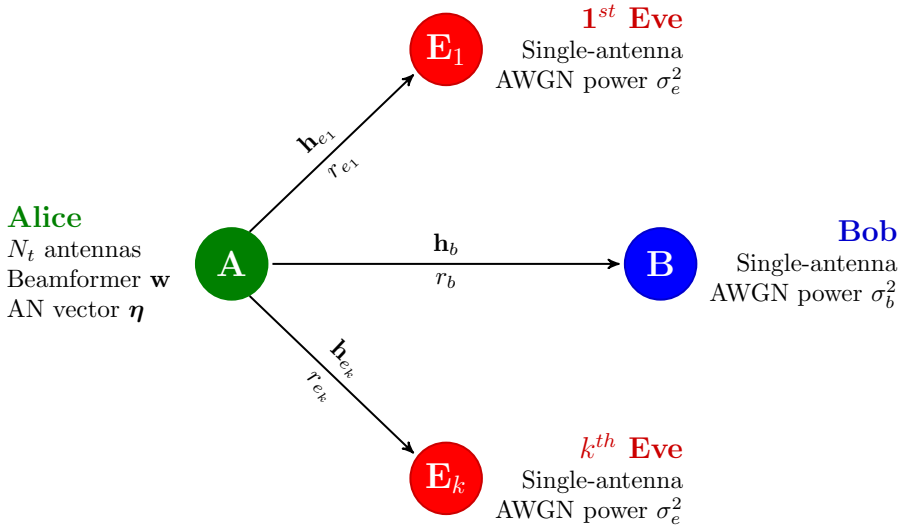


Figure 3.1: *MISO system model. A multi-antennas transmitter (Alice) conveys a secret message to the single-antenna receiver (Bob) in the presence of K single-antenna eavesdroppers (Eves).*

$\sigma^2_{\tilde{h}_b}$, i.e., $\tilde{\mathbf{h}}_b \sim \mathcal{CN}(0, \sigma^2_{\tilde{h}_b}\mathbf{I}_{N_t})$; similarly, $\tilde{\mathbf{h}}_{e_k} \sim \mathcal{CN}(0, \sigma^2_{\tilde{h}_{e_k}}\mathbf{I}_{N_t})$. The system is depicted in Figure 3.1. We consider a passive eavesdropping scenario; therefore $\mathbf{h}_b$ is perfectly known to Alice while $\mathbf{h}_{e_k}$ remains unknown to her. However, Alice can assume statistical information about Eve's channel.

We choose a masked beamforming secure transmission strategy that consists of steering information towards Bob and at the same time broadcasting AN to confuse unknown non-colluding eavesdroppers. So let $\mathbf{s} \in \mathbb{C}^{N_t}$ denote the beamformed signal vector transmitted by Alice modelled as

$$\mathbf{s} = \sqrt{a}\mathbf{w}d + \sqrt{b}\boldsymbol{\eta} \tag{3.1}$$

where the scalar variables a and b define the absolute powers allocated to the information and AN respectively. Here $\mathbf{w} \in \mathbb{C}^{N_t}$ is the unit norm beamforming vector; i.e., $||\mathbf{w}|| = 1$; $\boldsymbol{\eta} \in \mathbb{C}^{N_t}$ is the AN vector with covariance matrix $\mathbf{C}_\eta = \mathbb{E}\{\boldsymbol{\eta}\boldsymbol{\eta}^H\}$ s.t. $\mathrm{Tr}\{\mathbf{C}_\eta\} = 1$; and $d \in \mathbb{C}$ is the scalar, complex information symbol chosen from a Gaussian codebook with $\mathbb{E}\{|d|^2\} = 1$. The covariance matrix of the vector $\mathbf{s}$ is denoted by $\mathbf{C}_s = \mathbb{E}\{\mathbf{s}\mathbf{s}^H\}$ and $P = \mathrm{Tr}\{\mathbf{C}_s\} = a + b$ is Alice's total transmitted power.

In order to determine the transmission vectors $\mathbf{w}$ and $\boldsymbol{\eta}$, we use the same strategy as in [53, 72] that broadcasts AN in all directions except towards Bob. There-

fore, the beamforming vector $\mathbf{w}= \frac{\tilde{\mathbf{h}}_b}{||\tilde{\mathbf{h}}_b||}$ is the eigenvector ($\mathbf{t}_1$) corresponding to the single non-zero eigenvalue of the rank-one matrix $\tilde{\mathbf{h}}_b\tilde{\mathbf{h}}_b^H$. The AN vector $\boldsymbol{\eta}$ is then constructed by a linear combination of the remaining $N_t - 1$ eigenvectors so that orthogonality between the beamforming and AN vectors is preserved; i.e., $\mathbf{w}^H\boldsymbol{\eta} = 0$. Uniform power distribution among the remaining $N_t - 1$ eigenvectors $\{\mathbf{t}_i\}_{i=2}^{N_t}$ is enforced; therefore, $\boldsymbol{\eta}$ is obtained as follows

$$\boldsymbol{\eta} = \frac{1}{\sqrt{N_t - 1}} \sum_{i=2}^{N_t} \mathbf{t}_i \eta_i, \tag{3.2}$$

where $\mathbf{t}_i$ is the ith eigenvector of $\tilde{\mathbf{h}}_b\tilde{\mathbf{h}}_b^H$, and $\eta_i \in \mathbb{C}$ is an independent, complex, random variable with unit magnitude and uniformly distributed phase; i.e., $\eta_i = e^{j\varsigma_i}$ and $\varsigma_i \in [0, 2\pi)$. Thus the AN covariance matrix is given by

$$\mathbf{C}_\eta = \frac{1}{N_t - 1} \sum_{i=2}^{N_t} \mathbf{t}_i \mathbf{t}_i^H. \tag{3.3}$$

This technique effectively conveys the information only towards Bob and broadcasts the AN over the null space of the rank-one matrix $\tilde{\mathbf{h}}_b\tilde{\mathbf{h}}_b^H$. In other words, the AN is mathematically *'invisible'* to Bob but it can potentially confuse the Eves. This can be easily visualised by analysing the scalar signals received by Bob and the k^{th} Eve that are explicitly given by

$$u = \sqrt{a} r_b^{-\frac{\alpha}{2}} \tilde{\mathbf{h}}_b^H \mathbf{t}_1 d + n_b \tag{3.4}$$

$$v_k = \sqrt{a} r_{e_k}^{-\frac{\alpha}{2}} \tilde{\mathbf{h}}_{e_k}^H \mathbf{t}_1 d + \sqrt{b} r_{e_k}^{-\frac{\alpha}{2}} \tilde{\mathbf{h}}_{e_k}^H \boldsymbol{\eta} + n_{e_k} \tag{3.5}$$

where the scalar terms n_b and n_e represent complex additive Gaussian noise at Bob's and Eves' antennas such that $n_b \sim \mathcal{CN}(0, \sigma_b^2)$ and $n_e \sim \mathcal{CN}(0, \sigma_{e_k}^2)$.

Finally, the received SNRs at both Bob and at the k^{th} Eve are given by

$$\text{SNR}_b = \frac{a||\tilde{\mathbf{h}}_b||^2}{r_b^\alpha \sigma_b^2} \tag{3.6}$$

$$\text{SNR}_{e_k} = a\mathbf{t}_1^H \tilde{\mathbf{h}}_{e_k} \left[b\tilde{\mathbf{h}}_{e_k}^H \mathbf{C}_\eta \tilde{\mathbf{h}}_{e_k} + r_{e_k}^\alpha \sigma_{e_k}^2 \right]^{-1} \tilde{\mathbf{h}}_{e_k}^H \mathbf{t}_1 \tag{3.7}$$

while the achievable secrecy rate of the modelled system is

$$\text{R}_S = \left[\log_2 (1 + \text{SNR}_b) - \log_2 (1 + \text{SNR}_e) \right]^+ \text{[bps/Hz]}. \tag{3.8}$$

3.3 An outage security formulation based on Quality of Service

As explained before, under passive eavesdropping attacks it is not possible to offer perfect secrecy between the legitimate transmission parties; therefore, a probabilistic treatment of secrecy must be used. So in this section we introduce an outage probability based power distribution allocation to optimally allocate the available power between the information and AN to satisfy QoS requirements at the transmission parties. Here, secrecy is based on enforcing QoS constraints defined by the SNR both at the receiver and (probabilistically) at the unknown eavesdroppers.

3.3.1 Optimisation problem

The aim of the allocation strategy is to offer a given probability of secrecy defined by β, by enforcing a minimum SNR_b at Bob (γ_b) and ensuring probabilistically that the SNR_{e_k} at each eavesdropper is appropriately upper bounded by γ_e. In this section, and without loss of generality, we consider the Alice-to-Bob and Alice-to-Eve distances equal and normalised; i.e., $r_{ab} = r_{ae} = 1$.

We formulate an optimisation problem to find the optimal power allocation that minimises the transmitted power $(P = a + b)$ subject to guaranteeing a given probability of secrecy $\beta \in [0, 1)$ satisfying a given QoS as follows

$$\min_{a,b} \quad a + b \tag{3.9a}$$

$$\text{s.t.} \quad \text{SNR}_b \geq \gamma_b \tag{3.9b}$$

$$\mathbb{P}\left[\text{SNR}_{e_1} \leq \gamma_e, \cdots, \text{SNR}_{e_k} \leq \gamma_e\right] \geq \beta \tag{3.9c}$$

$$a > 0, b \geq 0. \tag{3.9d}$$

Since all $\mathbf{h}_{e_k}$ are mutually independent, after dropping the 'k' sub-index from SNR_{e_k}, the constraint in (3.9c) simplifies to

$$\left(\mathbb{P}\left[\text{SNR}_e \leq \gamma_e\right]\right)^K \geq \beta. \tag{3.10}$$

Now using the SNR definitions in (3.6) and (3.7) and the constraint in (3.10), the problem (3.9) becomes

$$\min_{a,b} \quad a + b \tag{3.11a}$$

$$\text{s.t.} \quad a||\tilde{\mathbf{h}}_b||^2 \left[\sigma_b^2\right]^{-1} \geq \gamma_b \tag{3.11b}$$

$$\mathbb{P}\left[a\mathbf{t}_1^H\tilde{\mathbf{h}}_e\left[b\tilde{\mathbf{h}}_e^H\mathbf{C}_\eta\tilde{\mathbf{h}}_e+\sigma_e^2\right]^{-1}\tilde{\mathbf{h}}_e^H\mathbf{t}_1 \leq \gamma_e\right] \geq \beta^{\frac{1}{K}} \tag{3.11c}$$

$$a>0, b\geq 0. \tag{3.11d}$$

We draw attention to the constraint in (3.11c). Its LHS can be written in terms of a random Hermitian quadratic form $Y=\tilde{\mathbf{h}}_e^H\mathbf{A}\tilde{\mathbf{h}}_e$ whose CDF can be evaluated in a closed-form expression by using step function representation and complex integration as introduced in [73]. We address this procedure in the next section.

Evaluating the CDF of a random Hermitian quadratic form

The LHS of the constraint (3.11c) can be re-written as follows

$$\mathbb{P}\left[\tilde{\mathbf{h}}_e^H\mathbf{A}\tilde{\mathbf{h}}_e \leq \sigma_e^2\right] \tag{3.12}$$

where

$$\mathbf{A}=\frac{a}{\gamma_e}\mathbf{t}_1\mathbf{t}_1^H - b\mathbf{C}_\eta. \tag{3.13}$$

Hence, (3.12) corresponds to the CDF of an indefinite Hermitian quadratic form ($Y=\tilde{\mathbf{h}}_e^H\mathbf{A}\tilde{\mathbf{h}}_e$) in the random vector $\tilde{\mathbf{h}}_e\sim\mathcal{CN}(\mathbf{0},\sigma_{\tilde{h}_e}^2\mathbf{I}_{N_t})$. In order to consider the general case of $\sigma_{\tilde{h}_e}^2\neq 1$ and still be able to apply the procedure in [73] developed for $\sigma_{\tilde{h}_e}^2=1$, an auxiliary variable $\overline{\mathbf{h}}_e=\frac{\tilde{\mathbf{h}}_e}{\sigma_{\tilde{h}_e}}$ is introduced such that $\overline{\mathbf{h}}_e\sim\mathcal{CN}(\mathbf{0},\mathbf{I}_{N_t})$. Therefore, Y is written as $Y=\overline{\mathbf{h}}_e^H\overline{\mathbf{A}\mathbf{h}}_e$; then $\overline{\mathbf{A}}=\sigma_{\tilde{h}_e}^2\mathbf{A}$ and the eigenvalues of $\overline{\mathbf{A}}$ are $\sigma_{\tilde{h}_e}^2\lambda_i(\mathbf{A})$. Considering the definitions of $\mathbf{C}_\eta$ in (3.3) and of $\mathbf{A}$ in (3.13) yields

$$\overline{\mathbf{A}}=\sigma_{\tilde{h}_e}^2\left[\frac{a}{\gamma_e}\mathbf{t}_1\mathbf{t}_1^H-\frac{b}{N_t-1}\mathbf{t}_2\mathbf{t}_2^H-\cdots-\frac{b}{N_t-1}\mathbf{t}_{N_t}\mathbf{t}_{N_t}^H\right]. \tag{3.14}$$

This expression corresponds to the effective eigen-decomposition of the matrix $\overline{\mathbf{A}}$ whose N_t eigenvalues are λ_1 and λ_2 with multiplicity orders equal to one and N_t-1 respectively. In other words, the eigenvalues of $\overline{\mathbf{A}}$ are

$$\left[\underbrace{\lambda_1,\lambda_2,\cdots,\lambda_2}_{N_t}\right]=\left[\frac{a\sigma_{\tilde{h}_e}^2}{\gamma_e},-\frac{b\sigma_{\tilde{h}_e}^2}{N_t-1},\cdots,-\frac{b\sigma_{\tilde{h}_e}^2}{N_t-1}\right]. \tag{3.15}$$

Following the procedure detailed in [73], and bearing in mind the described multiplicity order of the eigenvalues of $\overline{\mathbf{A}}$, the CDF of Y for a value y is

$$F_Y(y)=u(y)+\frac{\alpha_1}{|\lambda_1|}e^{-\frac{y}{\lambda_1}}u\left(\frac{y}{\lambda_1}\right)+\sum_{k=1}^{N_t-1}\frac{\alpha_{k+1}}{(k-1)!|\lambda_2|^k}y^{k-1}e^{-\frac{y}{\lambda_2}}u\left(\frac{y}{\lambda_2}\right) \tag{3.16}$$

where $u(x)$ denotes the unit step function.

Since in our problem $\lambda_1 > 0$ and $\lambda_2 < 0$, and as we are only interested in $F_Y(y)$ for positive values of y, since $y = \sigma_e^2 \geq 0$ (see (3.12)), then $\{\alpha_{k+1}\}_{k=1}^{N_t-1}$ in (3.16) can be neglected. Meanwhile α_1 is given by

$$\alpha_1 = -\frac{\lambda_1}{\left(1 - \frac{\lambda_2}{\lambda_1}\right)^{N_t-1}}. \tag{3.17}$$

Finally, using the eigenvalues of $\overline{\mathbf{A}}$ in (3.15), the equivalent CDF in (3.16) and the definition in (3.17) the final expression for $F_Y(y)$ for $y \geq 0$ is obtained as follows

$$F_Y(y) = 1 - \frac{1}{\left(1 + \frac{b}{a}\frac{\gamma_e}{N_t-1}\right)^{N_t-1}} e^{-\frac{\gamma_e}{a\sigma_{\tilde{h}_e}^2} y}, \; y \geq 0. \tag{3.18}$$

Once the CDF within the constraint (3.11c) has been evaluated, now it can be re-written as

$$1 - \frac{1}{\left(1 + \frac{b}{a}\frac{\gamma_e}{N_t-1}\right)^{N_t-1}} e^{-\frac{\gamma_e}{a\sigma_{\tilde{h}_e}^2} \sigma_e^2} \geq \beta^{\frac{1}{K}} \tag{3.19}$$

where (3.19) results from evaluating $F_Y(\sigma_e^2)$ in (3.18). Thus the resulting problem becomes

$$\begin{aligned}
\min_{a,b} \quad & a + b && \text{(3.20a)} \\
\text{s.t.} \quad & a||\tilde{\mathbf{h}}_b||^2 \left[\sigma_b^2\right]^{-1} \geq \gamma_b && \text{(3.20b)} \\
& 1 - \frac{1}{\left(1 + \frac{b}{a}\frac{\gamma_e}{N_t-1}\right)^{N_t-1}} e^{-\frac{\gamma_e}{a\sigma_{\tilde{h}_e}^2} \sigma_e^2} \geq \beta^{\frac{1}{K}} && \text{(3.20c)} \\
& a > 0, b \geq 0 && \text{(3.20d)}
\end{aligned}$$

and this can be solved to find the optimal power allocation given by $a^\star$ and $b^\star$ in closed-form expression as follows

$$a^\star = \frac{\gamma_b \sigma_b^2}{||\tilde{\mathbf{h}}_b||^2} \tag{3.21a}$$

$$b^\star = \left[\frac{a^\star(N_t - 1)}{\gamma_e}\left(\sqrt[N_t-1]{\frac{e^{-\frac{\gamma_e}{a^\star\sigma_{\tilde{h}_e}^2}\sigma_e^2}}{1 - \beta^{\frac{1}{K}}}} - 1\right)\right]^+. \tag{3.21b}$$

The closed-form solution in (3.21) shows that ensuring a given probability of secrecy is achieved at the expense of supplying power for AN generation. A high probability of secrecy can be provided by devoting additional power to the AN meanwhile the power allocated to the information transmission remains constant irrespective of the target probability of secrecy β.

In the case of a power constrained system, we define the maximum transmit power available at Alice as P_{max}. Therefore, in the case where the solution to the problem (3.9) given by (3.21) requires more than the available power; i.e., $a^\star + b^\star > P_{max}$, then the problem is infeasible. In this scenario, the system is considered in outage and, for the sake of the secrecy, Alice does not transmit any information for that particular channel realisation. As we will see in the next section, this has an impact on the secure throughput of the system.

3.3.2 Numerical results

In this section we present simulation results to show the achieved secrecy probability, the secrecy throughput and the power distribution for two cases:

1. the idealistic scenario where the total power available is not constrained (i.e., $P \in [0, \infty)$),

2. the practical case where the power available at the transmitter is limited (i.e., $P \in [0, P_{max}]$).

In order to evaluate the performance of the proposed outage based power allocation method, it is necessary to compare it against a technique that also defines security by QoS constraints as in [59]. In this referenced work, the authors assume that the Eves' CSIs are perfectly available at the transmitter. However, [59] also offers an option to use only statistical knowledge about the eavesdroppers, i.e., $\mathbb{E}\left\{\tilde{\mathbf{h}}_e \tilde{\mathbf{h}}_e^H\right\} = \sigma^2_{\tilde{h}_e} \mathbf{I}_{N_t}$. This setup is similar to the one used throughout the work presented in this chapter enabling us to fairly benchmark both techniques. The main difference is that our approach considers an optimisation problem based on outage probability formulation while [59] uses the statistical knowledge of the Eves' CSI to satisfy the QoS constraints in average. The instantaneous information of the legitimate channel is assumed to be exactly known by Alice for both approaches.

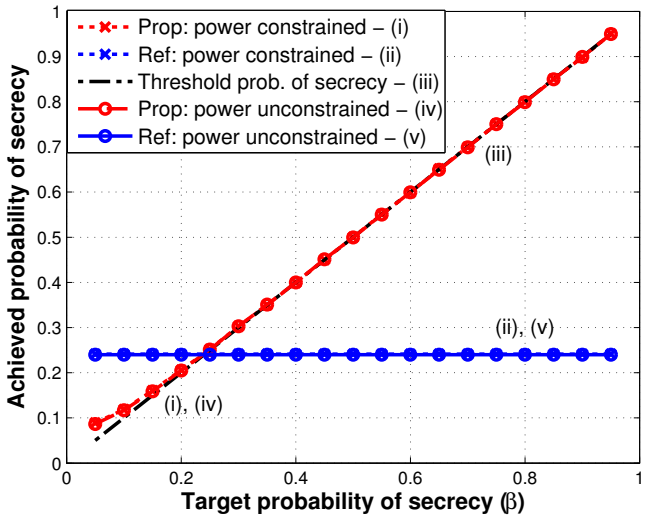
Table 3.1: *Simulation parameters setup.*

Parameter	Value	Description
N_t	5	Alice's number of antennas
$\sigma^2_{\tilde{h}_b}$	1	Main channel elements variance
$\sigma^2_{\tilde{h}_e}$	1	Eavesdropping channel elements variance
γ_b	10 dB	QoS constraint at Bob
γ_e	0 dB	QoS constraint at Eve
σ^2_b	1	Bob's AWGN power
σ^2_e	1	Eve's AWGN power
P_{max}	6	Maximal power for constrained systems normalised relative to the AWGN power

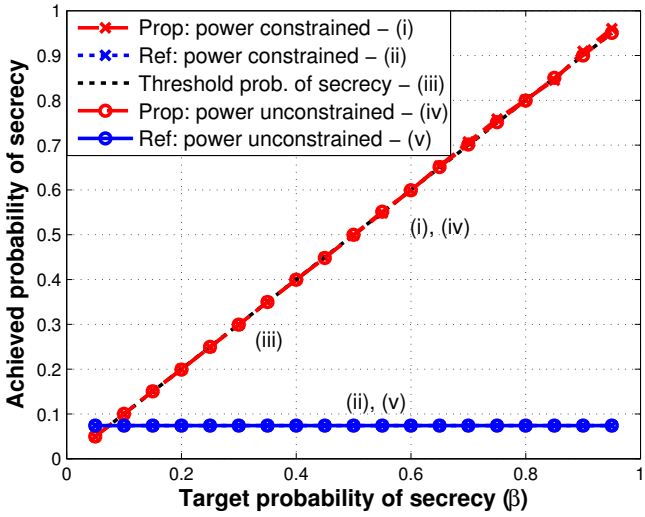
For the simulations, three and five eavesdroppers are considered ($K = 3, 5$) under the same channel and noise statistical conditions, so indices can be omitted. 200,000 Monte Carlo runs are considered with simulations parameters listed in Table 3.1. In all the figures, the proposed outage based power allocation method and the reference technique are referred to as 'Prop:' and 'Ref:' respectively.

In Figure 3.2 the achieved probability of secrecy resulting from the outage based power allocation technique in (3.21) is shown when the target probability of secrecy β varies from 0.05 to 0.95. From the graphs it is clear that the proposed approach guarantees the intended probability of secrecy (β) while the reference technique can only offer a constant probability of secrecy independent of the power available at the transmitter. Indeed, the referenced technique [59] offers a maximum achieved probability of secrecy even for the unconstrained power scenario because it does not consider outage probability in the allocation mechanism.

In the power constrained case, as explained before, transmission only takes place when (i): (3.9b) and (3.9c) are both satisfied and (ii): the solution in (3.21) requires $P = a^\star + b^\star \leq P_{max}$. So there is a trade-off between guaranteeing a high probability of secrecy (β) and the secrecy throughput. This behaviour is observed in the Figure 3.3 where the *normalised secrecy throughput* is depicted. Here, we define the normalised secrecy throughput as the achieved probability of secrecy times the ratio between the number of channel realisations whose information is 'securely transmitted' (i.e., constraint (3.9c) is satisfied) and the total number of

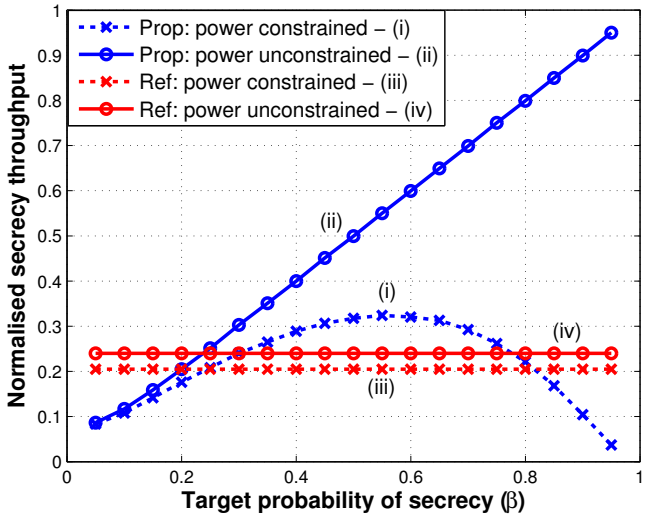


(a) *K=3*

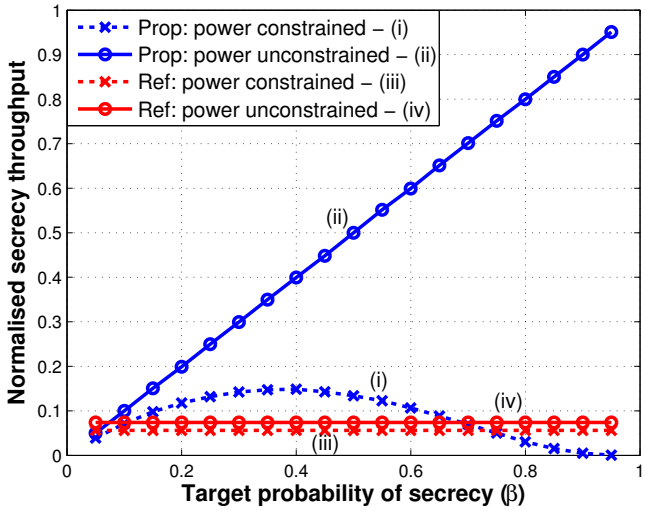


(b) *K=5*

Figure 3.2: *Achieved probability of secrecy versus target probability of secrecy (β) for unconstrained and constrained transmit power systems.*



(a) *K=3*



(b) *K=5*

Figure 3.3: *Achieved normalised secrecy throughput in attempting to achieve a target probability of secrecy (β) for both unconstrained and constrained transmit power systems.*

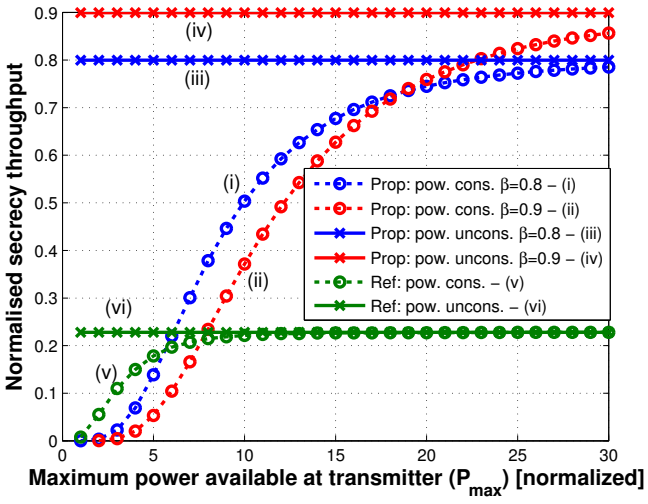
channel realisations considered in the simulations. From these plots the proposed technique in most of the cases offers a higher throughput than the reference one. Indeed, for the power unconstrained system, the target probability of secrecy is always guaranteed thus achieving the maximum possible secrecy throughput. On the other hand, for the power constrained case, as the security conditions become more demanding and the probability of secrecy β approaches one, the throughput decreases due to the fact that transmissions only take place for fewer channel realisations.

It is worth pointing out that in the case of power constrained systems, and unlike the reference technique in [59], the secrecy throughput of the proposed scheme can be improved by incrementing the power available at the transmitter. This is clearly shown in Figure 3.4 where the effect of increasing P_{max} is analysed for values of target probability of secrecy $\beta = 0.8, 0.9$. Here, for larger values of P_{max}, the proposed scheme is perfectly capable of guaranteeing the maximum secrecy throughput rates while the reference method is constrained to a fixed value of secrecy throughput, irrespective of P_{max}.

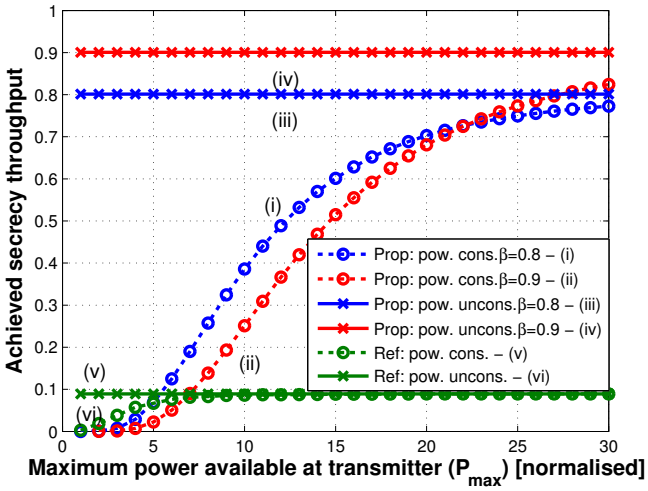
In Figure 3.5 the power distribution for the power unconstrained case is illustrated for different values of the target probability of secrecy (β). Here, the average power requested for the strategy is observed, where 'average power' is the mean value of P over those Monte Carlo runs where transmission takes place (i.e., $P \leq P_{max}$). In Figure 3.6 the trade-off between allocating power for AN and information is depicted for the power constrained scenario when the normalised $P_{max} = 6$ relative to the AWGN power.

Note that the outage based power allocation scheme is also capable of guaranteeing a given probability of secrecy for a larger number of eavesdroppers; however, it is necessary to provide more power at the transmitter. This can be seen from the closed-form result in (3.21) and in all the above figures when the results are considered for $K = 3$ and $K = 5$, especially in Figures 3.5 and 3.6 where the power distribution is shown.

Finally, it is important to remark upon the simplicity of the proposed outage based power allocation scheme that provides a closed-form expression to distribute power relying on simple mathematical calculations. This is in contrast to [59] that requires complex computational algorithms to solve the optimisation problem.

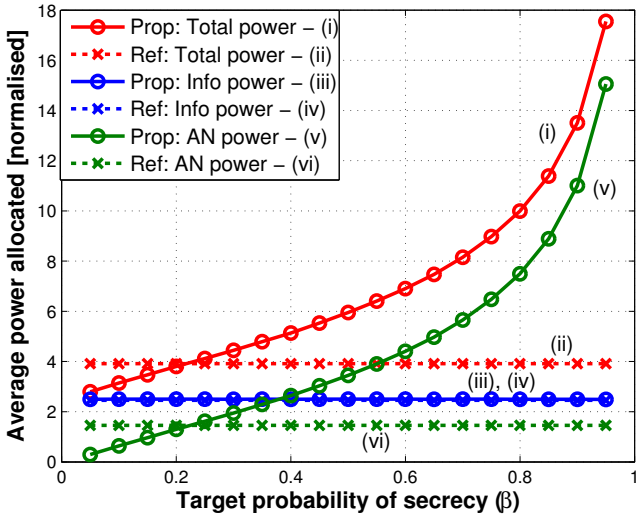


(a) *K=3*

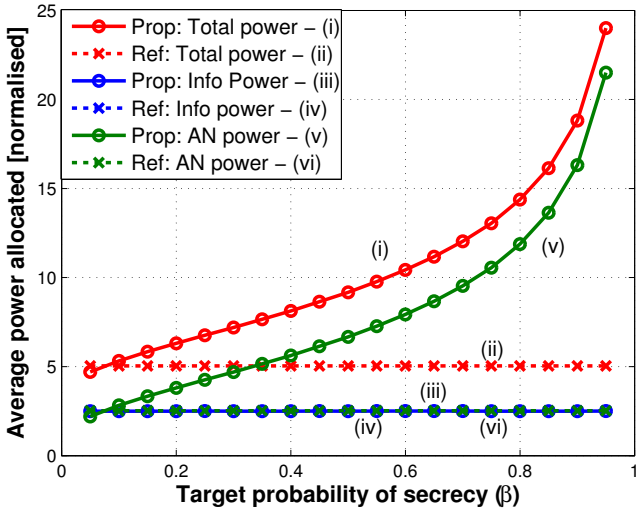


(b) *K=5*

Figure 3.4: *Normalised secrecy throughput for constrained transmit power systems under different values of maximum power (P_{max}) (normalised relative to the AWGN power) and unconstrained systems for $\beta = 0.8, 0.9$.*

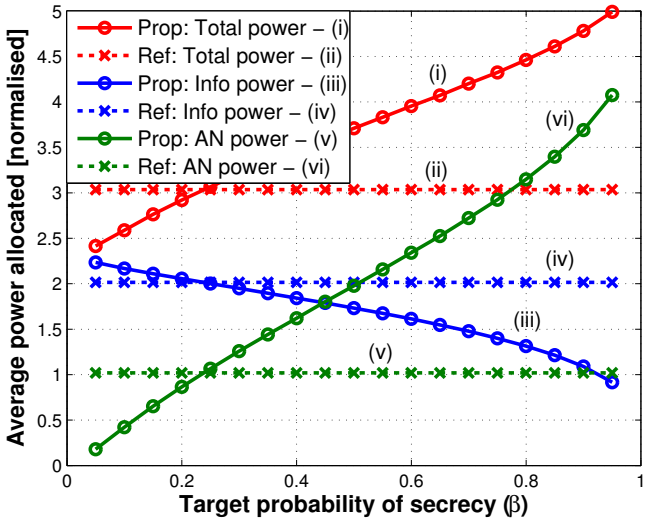


(a) *K=3*

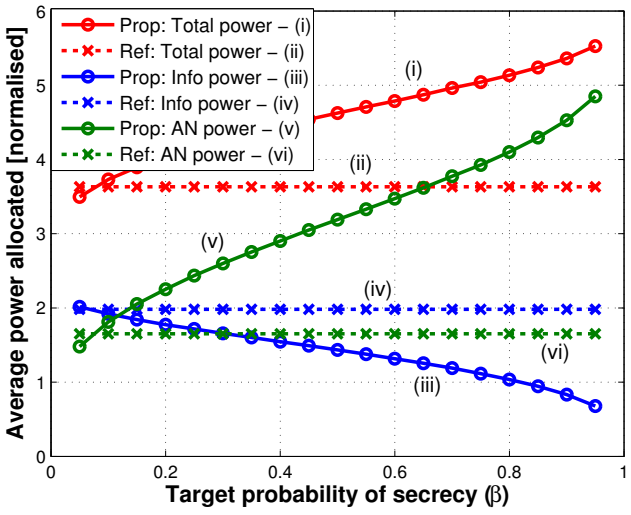


(b) *K=5*

Figure 3.5: *Power distribution between information and artificial noise (normalised relative to the AWGN's power) for achieving a given probability of secrecy (β) in an unconstrained transmit power system.*



(a) *K=3*



(b) *K=5*

Figure 3.6: *Power distribution between information and artificial noise for achieving a given probability of secrecy (β) in a constrained transmit power system.*

3.4 An outage secrecy rate formulation with protected zone

This section incorporates the analysis of the proximity of the nodes and how this influences the secrecy performance of the MISO system. Here the critical problem of having a physically close eavesdropper is examined and how this situation can become a serious threat to the system's security due to the advantageous (reduced) path losses affecting the eavesdropper compared to a more distant intended receiver.

As an effective way to prevent a closer unknown eavesdropper and to incorporate the distance effect under a worst-case scenario, we will introduce into the problem setup an eavesdropper exclusion area named the '*protected zone*' (PZ). In this context, a prioritised outage based optimisation problem is formulated to determine the minimum requested transmission power and the smallest size of the PZ to guarantee a given level of security (probabilistically defined). Here, the secrecy rate is used as the natural physical layer security metric rather than a restrictive QoS-based secrecy, as was done before in §3.3. This approach allows us to prioritise the use of power over enlarging the PZ, or to save power by deploying a large PZ. Furthermore, this formulation sheds light into the additional power consumption levels needed to achieve high security when an eavesdropper is close to the transmitter or, on the other hand, into the possible savings in power due to a distant attacker.

3.4.1 Protected zone

The *Protected Zone* (PZ) is a novel way to improve the security of the system by defining an eavesdropper-free area where Alice only allows the presence of authorised nodes by using physical means. The motivation for deploying a PZ is twofold. First, it contributes to the secrecy by preventing attacks at close-quarters; and second, it allows an efficient use of the available power.

To illustrate this concept, we can consider practical deployments where the transmission facilities are located in restricted-access areas thereby preventing the physical access of a potential attacker. Some examples are equipment rooms,

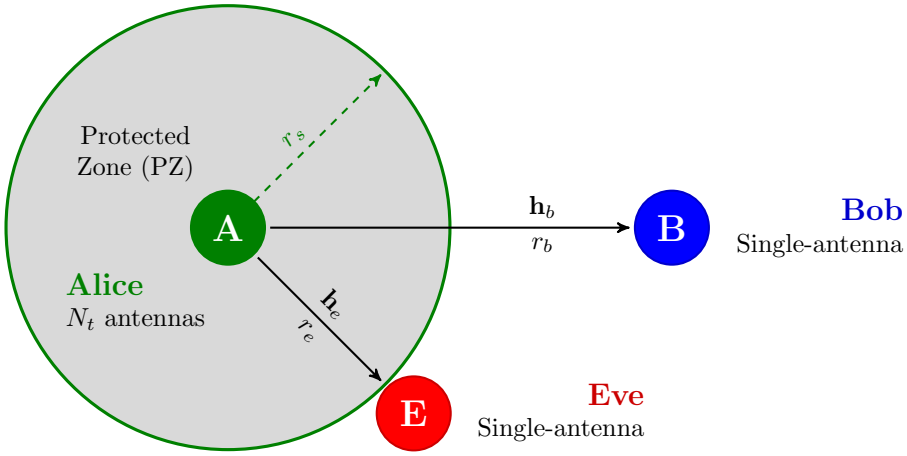


Figure 3.7: *MISO system model with a protected zone. A multi-antennas transmitter (Alice) conveys a secret message to the single-antenna receiver (Bob) in the presence of a single-antenna eavesdropper (Eve).*

transmission antennas placed on the top of communication towers or on roofs protected by restricted-access perimeters like the ones built into critical microwave backbone network repeaters or cellular base stations in high risk areas. These commonly deployed physical layouts inherently define a PZ; alternatively, where no PZ physically exists, a security perimeter may be intentionally deployed to achieve a given level of secrecy, especially in power constrained scenarios.

A PZ, as depicted in the Figure 3.7, is defined by the '*Security Radius*' (r_s) that is the transmitter-to-the PZ border distance. The inclusion of the PZ is equivalent to restricting the Alice-to-Eve distance (r_e) to be larger or equal than the secrecy radius; i.e., $r_e \geq r_s$. This formulation is meaningful not only because it improves the security, but also because it gives insights about the impact of the eavesdroppers' location over the security. Indeed, incorporating a PZ into the design allows us to quantify the additional power required to achieve high levels of security in the presence of a close attacker (i.e., $r_e \to 0$) or the possible savings in power when Eve is far away from Alice (i.e., $r_e \gg 0$).

In the remaining of this chapter, a PZ is incorporated into the analysis to formulate an optimisation problem that aims to determine the radius of a PZ (r_s) and the power distribution to deliver a probabilistically secured MISO network. For the sake of simplicity, and without loss of generality, the analysis is restricted to the case of one eavesdropper, i.e., $K = 1$. However, the extension to the multi-

ple eavesdropper case is straightforward following the guidelines presented in the previous section.

3.4.2 Optimisation Problem

The objective is to find the optimal resource allocation given by the size of the PZ and the power distribution between information and AN to ensure that the probability of secrecy is larger than a target β. Here, the probability of secrecy is defined as the likelihood that the secrecy rate R_S in (3.8) is guaranteed to be above or equal to the target secrecy rate R. In other words, the probability of secrecy is defined by

$$\mathbb{P}_{SEC}(R) = \mathbb{P}\left[\mathrm{R}_S \geq R\right]. \tag{3.22}$$

To achieve this goal, a *Weighted Normalised Cost Function* (WNCF) is introduced to efficiently allocate both available resources that affect the security performance: (i) the total transmitted power ($P = a + b$), and (ii) the PZ's size given by the secrecy radius (r_s). So the WNCF is

$$\mathrm{CF}(a, b, r_s) = \kappa_1 \frac{a+b}{P_{max}} + \kappa_2 \frac{r_s}{r_{s_{max}}}. \tag{3.23}$$

Here P_{max} and $r_{s_{max}}$ are the maximum available transmission power and the maximum allowable radius of the PZ while κ_1 and κ_2 are the weights to prioritise the use of one resource over the other. The values of κ_1 and κ_2 are chosen to reflect whether it is more convenient to use additional power rather than extending the PZ or vice versa. This design criteria can be motivated by either the resource availability or the practical feasibility to deploy a PZ. It is worth pointing out that normalising the cost function takes into account P_{max} and $r_{s_{max}}$, making meaningful weighting between absolute values rather than considering different and not related resources such as power and distance. This new idea effectively enables us to jointly distribute both network resources and to define how they are used.

Considering the restriction on the eavesdropper location introduced by the PZ, the optimisation problem can now be written as follows

$$\min_{a,b,r_s} \quad \mathrm{CF}\left(a, b, r_s\right) \tag{3.24a}$$

$$\text{s.t.} \quad \mathbb{P}_{SEC}(R) = \mathbb{P}\left[\mathrm{R}_S \geq R\right] \geq \beta \tag{3.24b}$$

$$a + b \leq P_{max}, 0 \leq r_s \leq r_{s_{max}} \tag{3.24c}$$

$$r_e \geq r_s, a > 0, b \geq 0. \tag{3.24d}$$

Substituting the definitions of the SNR_b in (3.6) and of the secrecy rate in (3.8) into the probabilistic constraint in (3.24b) yields

$$\mathbb{P}\left[\text{SNR}_e \leq \psi\right] \geq \beta, \text{ s.t. } \psi = 2^{-R}\left(1 + \frac{a||\tilde{\mathbf{h}}_b||^2}{r_b^{\alpha}\sigma_b^2}\right) - 1. \tag{3.25}$$

From (3.25), and considering that the SNR_e must be a positive value, then $\psi \geq \text{SNR}_e > 0 \Rightarrow \psi > 0$. Therefore, for $\beta > 0$, the probabilistic constraint (3.24b) and its equivalent expression in (3.25) imply that the problem is feasible if the total available power P_{max} can satisfy the minimum power required for the information (a) to guarantee the target secrecy rate R as follows

$$a > \frac{\gamma_b r_b^{\alpha}\sigma_b^2}{||\tilde{\mathbf{h}}_b||^2}, \text{ s.t. } \gamma_b = \left(2^R - 1\right). \tag{3.26}$$

Now, substituting the definition of SNR_e in (3.7) into the probabilistic constraint in (3.25) yields

$$\mathbb{P}\left[\tilde{\mathbf{h}}_e^H\left(a\mathbf{t}_1\mathbf{t_1}^H - b\psi\mathbf{C}_\eta\right)\tilde{\mathbf{h}}_e \leq r_e^{\alpha}\psi\sigma_e^2\right] \geq \beta, \tag{3.27}$$

which can be viewed in terms of the CDF of an indefinite Hermitian quadratic form $Y = \tilde{\mathbf{h}}_e^H\mathbf{A}\tilde{\mathbf{h}}_e$ in a random vector $\tilde{\mathbf{h}}_e$, where $\mathbf{A} = a\mathbf{t}_1\mathbf{t}_1^H - b\psi\mathbf{C}_\eta$. Following the same procedure detailed in §3.3.1 where the CDF of a random Hermitian quadratic form is evaluated, the CDF of this quadratic distribution is given by

$$F_Y(y) = 1 - \left(1 + \frac{b\psi}{a\left(N_t - 1\right)}\right)^{1-N_t}\exp\left(-\frac{y}{a\sigma_{\tilde{h}_e}^2}\right), y > 0. \tag{3.28}$$

Now, from the term inside of the brackets of the LHS of the probabilistic constrain in (3.27) and from the CDF in (3.28), we are only concerned with the scenario when $y = r_e^{\alpha}\psi\sigma_e^2 > 0$, not considering the infeasible case of $y = 0$. Indeed, $y = 0$ clearly neither satisfies (3.25) for $\beta > 0$ nor ensures the condition $\psi > 0$.

Substituting ψ from (3.25), and $y = r_e^{\alpha}\psi\sigma_e^2$ from (3.27) into the CDF in (3.28), the probabilistic constraint in (3.24b) becomes

$$1 - \left(1 + \frac{b}{a}\frac{\gamma_e}{\left(N_t - 1\right)}\right)^{1-N_t}\exp\left(-\frac{r_e^{\alpha}\gamma_e}{a\sigma_{\tilde{h}_e}^2}\sigma_e^2\right) \geq \beta \tag{3.29a}$$

$$\text{s.t. } \gamma_e = \frac{a||\tilde{\mathbf{h}}_b||^2 - r_b^\alpha \sigma_b^2 \left(2^R - 1\right)}{2^R \sigma_b^2 r_b^\alpha}. \tag{3.29b}$$

Finally, the resulting optimisation problem is formulated by considering the worst-case for the secrecy that happens when the eavesdropper lies exactly on the border of the PZ; i.e., $r_e = r_s$. Therefore, after taking into account the constraints (3.26) and (3.29), the problem becomes

$$\min_{a,b,r_s} \quad \kappa_1 \frac{a+b}{P_{max}} + \kappa_2 \frac{r_s}{r_{s_{max}}} \tag{3.30a}$$

$$\text{s.t.} \quad 1 - \frac{1}{\left(1 + \frac{b}{a}\frac{\gamma_e}{(N_t-1)}\right)^{N_t-1}} \exp\left(-\frac{r_s^\alpha \gamma_e}{a\sigma_{\tilde{h}_e}^2}\sigma_e^2\right) \geq \beta \tag{3.30b}$$

$$a > \frac{\gamma_b r_b^\alpha \sigma_b^2}{||\tilde{\mathbf{h}}_b||^2} \tag{3.30c}$$

$$a + b \leq P_{max}, 0 \leq r_s \leq r_{s_{max}}, b \geq 0 \tag{3.30d}$$

where γ_b and γ_e are given in (3.26) and (3.29b) respectively. It is worth pointing out that (3.30c) is implied by the condition $\gamma_e > 0$ in the constraint (3.30b) for $\beta > 0$ and might be omitted. However, this constraint is intentionally retained because it will later be useful to illustrate two particular cases of this optimisation problem.

The derivation of a closed-form solution to the problem in (3.30) is mathematically difficult due to the exponential nature of the constraint (3.30b). Therefore, in order to obtain additional insight into the internal structure of the problem and to devise an efficient way to solve it, we present in the next two sections an analysis of the asymptotic behaviour and the monotonically increasing characteristic of the probabilistic constraint in (3.30b).

Analysis of the asymptotic behaviour of the probabilistic constraint

In order to understand the behaviour of the probabilistic constraint in (3.30b), we replace γ_e from (3.29b) in the LHS of (3.30b) to write it explicitly as follows

$$F(a,b,r_s) = 1 - \frac{\exp\left(-\frac{r_s^\alpha \sigma_e^2 \left(a||\tilde{\mathbf{h}}_b||^2 - r_b^\alpha \sigma_b^2 \left(2^R-1\right)\right)}{2^R a r_b^\alpha \sigma_b^2 \sigma_{\tilde{h}_e}^2}\right)}{\left(1 + \frac{b}{a}\left(\frac{a||\tilde{\mathbf{h}}_b||^2 - r_b^\alpha \sigma_b^2 (2^R-1)}{2^R r_b^\alpha \sigma_b^2 (N_t-1)}\right)\right)^{N_t-1}}, \tag{3.31}$$

Table 3.2: *Analysis of the asymptotic behaviour of the probabilistic constraint.*

a	b	r_s	$A(a,b)$	$B(a,r_s)$	Asymptotic value of $F(a,b,r_s)$
$\frac{X}{\rho}$	0	0	1	0	0
$\frac{X}{\rho}$	0	∞	1	0	0
$\frac{X}{\rho}$	∞	0	1	0	0
$\frac{X}{\rho}$	∞	∞	1	0	0
∞	0	0	1	0	0
∞	0	∞	1	$r_s^\alpha \frac{Z\rho}{Y}$	$1-\exp\left(-r_s^\alpha \frac{Z\rho}{Y}\right)$
∞	∞	0	$\left(1+b\frac{\rho}{Y(N_t-1)}\right)^{N_t-1}$	0	$1-\frac{1}{\left(1+b\frac{\rho}{Y(N_t-1)}\right)^{N_t-1}}$
∞	∞	∞	$\left(1+b\frac{\rho}{Y(N_t-1)}\right)^{N_t-1}$	$r_s^\alpha \frac{Z\rho}{Y}$	$1-\frac{\exp\left(-r_s^\alpha \frac{Z\rho}{Y}\right)}{\left(1+b\frac{\rho}{Y(N_t-1)}\right)^{N_t-1}}$

that can be written as

$$F(a,b,r_s) = 1 - \frac{\exp\left(-r_s^\alpha \frac{Z}{Y}\left(\rho - \frac{X}{a}\right)\right)}{\left(1+\frac{b}{Y(N_t-1)}\left(\rho-\frac{X}{a}\right)\right)^{N_t-1}} \tag{3.32}$$

where X, Y, Z and ρ are all non-zero positive values (except for the trivial case when $R=0$) given by

$$X = r_b^\alpha \sigma_b^2 \left(2^R - 1\right) \tag{3.33a}$$

$$Y = 2^R r_b^\alpha \sigma_b^2 \tag{3.33b}$$

$$Z = \frac{\sigma_e^2}{\sigma_{\tilde{h}_e}^2} \tag{3.33c}$$

$$\rho = ||\tilde{\mathbf{h}}_b||^2. \tag{3.33d}$$

The minimum value that guarantees feasibility for a is given in (3.26), and by (3.33a) and (3.33d) corresponds to $a > \frac{X}{\rho}$. Moreover, the expression in (3.32) can be written as $F(a,b,r_s) = 1 - \frac{\exp(-B(a,r_s))}{A(a,b)}$ where $A(a,b)$ and $B(a,r_s)$ are functions that ease the analysis of the asymptotic behaviour of (3.30b) considering the three optimisation variables (a,b,r_s). This analysis is depicted in the Table 3.2.

Equation (3.32) reveals that for the information power (a) greater than and very close to $\frac{X}{\rho}$ ($a \gtrapprox \frac{X}{\rho}$), then $F(a,b,r_s) \approx 0$ irrespective of the value given for both the AN power (b) and the security radius (r_s); this is also the case when $b = r_s = 0$.

This case follows intuition because this condition implies that the $\text{SNR}_e = \infty$ due to the zero-value denominator in (3.7).

Table 3.2 also shows that when more power is devoted to the information (a) with the AN power $b > 0$ and/or secrecy radius $r_s > 0$, then (3.32) monotonically increases to its limiting value

$$\lim_{a\to\infty} F(a, b, r_s) = 1 - \frac{1}{\left(1 + b\frac{\rho}{Y(N_t-1)}\right)^{N_t-1}} \exp\left(-r_s^{\alpha}\frac{Z\rho}{Y}\right). \tag{3.34}$$

This analysis shows that by just providing increasing power for the information alone is not enough to achieve a high probability of secrecy; i.e., $F(a, b, r_s) \approx 1$. Therefore, a smart allocation strategy is needed to distribute the power between information and the AN or to consider an appropriate PZ size to keep Eve sufficiently far away from Alice. Also this analysis confirms that when Eve is close to Alice; i.e., $r_s \to 0$, a larger amount of AN power is required to achieve a high probability of secrecy. This follows the intuition that, in order to increase the likelihood of achieving secrecy, it is necessary not only to provide a good signal quality at Bob, but also to deteriorate in someway the quality of Eve's received signal by either broadcasting AN or enlarging the PZ.

Analysis of the positive monotonically increasing behaivour of the probabilistic constraint

In order to show that the LHS of the constraint (3.30b) is a positive monotonically-increasing function (PMIF), it is useful to analyse it as a composition of functions. Therefore, we rewrite (3.32) as

$$F(a, b, r_s) = 1 - \frac{1}{A(a, b)\exp\left(B(a, r_s)\right)} \tag{3.35}$$

where

$$A(a, b) = \left(1 + \frac{b}{Y(N_t - 1)}\left(\rho - \frac{X}{a}\right)\right)^{N_t-1} \tag{3.36a}$$

$$B(a, r_s) = r_s^{\alpha}\frac{Z}{Y}\left(\rho - \frac{X}{a}\right) \tag{3.36b}$$

and the definitions in (3.33) are used.

The function in (3.36a) can be expressed as the composite of two functions as follows

$$A(a,b) = (1 + f_1(b)f_2(a))^{N_t-1} \tag{3.37}$$

where

$$f_1(b) = \frac{b}{Y(N_t-1)} \tag{3.38a}$$

$$f_2(a) = \left(\rho - \frac{X}{a}\right). \tag{3.38b}$$

Recalling from (3.32), X, Y, Z and ρ are all positive values, so it is straightforward to see that $f_1(b)$ is a linear PMIF in b for $b > 0$. Likewise, $f_2(a)$ is a PMIF in a when $a > \frac{X}{\rho}$ and that comes from the feasibility condition in (3.30c). Thus, $A(a,b)$ becomes an exponential PMIF resulting from the multiplication of two PMIFs.

Following the same methodology, $B(a, r_s)$ in (3.36b) can be expressed as a composite function of the two PMIFs $f_3(r_s)$ and $f_2(a)$, where

$$f_3(r_s) = r_s^{\alpha}\frac{Z}{Y}. \tag{3.39}$$

Clearly $f_3(r_s)$ is an exponential PMIF in r_s for $r_s > 0$; therefore $B(a, r_s)$ is also a PMIF.

Finally, (3.35) and then the LHS of the constraint (3.30b) is the result of a subtracting from 1 the inverse of the multiplication on the denominator of two PMIFs; therefore it is also a PMIF in a, b and r_s that asymptotically approaches one.

Once the asymptotic behaviour and the positive monotonically increasing property of the probabilistic constraint (3.30b) have been discussed, we have enough insight to look for efficient means to solve the optimisation problem in (3.30). Indeed, as pointed out previously, the derivation of a closed-form solution to (3.30) is mathematically difficult. However, its objective function in (3.30a) and the inequalities (3.30c) and (3.30d) are linear in all the optimising variables. Moreover, the LHS of the constraint in (3.30b) is a positive monotonically-increasing function in all the optimising variables (a, b, r_s) within the boundaries of the feasible region and asymptotically approaches one. Therefore, considering the aforementioned characteristics of the problem (3.30), we can conclude that it can be efficiently solved by numerical methods with a reasonable level of complexity.

Finally, it is important to point out that when the problem (3.30) is infeasible for a specific channel condition, mainly due to not satisfying the power constraint

in (3.30d), then the system is considered to be in outage and in order to preserve the security, no transmission takes place.

In the next two sections we study two particular cases of the outage resource allocation optimisation problem. These scenarios enable us to stablish connections with previous works and offer additional insight into the power allocation and the PZ contribution towards the secrecy of a MISO system.

3.4.3 Resource allocations when the transmission parties are equidistant.

First, we consider the case when all the nodes are equidistant to the transmitter; i.e., $r_e = r_b = r_s$. Under this condition the resource allocation problem in (3.30) becomes a non-weighted power minimisation similar to the one studied in §3.3.1 but considering secrecy rate as the security metric rather than based on a QoS metric.

To analyse this problem we use the equidistant condition and set all the nodes' distances to $r_e = r_b = r_s = r$. Subsequently, the constraint in (3.30c) can be written as

$$\tilde{a} > \frac{\gamma_b \sigma_b^2}{||\tilde{\mathbf{h}}_b||^2}, \tag{3.40}$$

where $\tilde{a} = \frac{a}{r^\alpha}$. Now, the constraint (3.30b) is used to find an expression for $\tilde{b} = \frac{b}{r^\alpha}$ as follows

$$\tilde{b} \geq \frac{\tilde{a}\,(N_t - 1)}{\tilde{\gamma}_e} \left(\sqrt[N_t-1]{\frac{\exp\left(-\frac{\sigma_e}{\tilde{a}\sigma^2_{\tilde{h}_e}}\sigma_e^2\right)}{1-\beta}} - 1 \right), \tag{3.41}$$

where

$$\tilde{\gamma}_e = \frac{\tilde{a}||\tilde{\mathbf{h}}_b||^2 - \sigma_b^2\left(2^R - 1\right)}{2^R \sigma_b^2}. \tag{3.42}$$

These expressions for $\tilde{a}$ and $\tilde{b}$ are similar to the ones included in the closed-form solution in (3.21) for the outage QoS problem studied in §3.3 except that the equality does not hold for $\tilde{a}$. This difference results from considering a secrecy rate based formulation rather than a QoS constraints, and it hinders a straightforward solution for the resulting non-weighted power minimisation problem in closed-from. However, a non-weighted one-variable ($\tilde{a}$) minimisation problem can be

formulated by adding the expression for $\tilde{b}$ in (3.41) into the objective function for $\tilde{a}$. This problem is now as follows

$$\min_{\tilde{a}} \ \tilde{a} + \frac{\tilde{a}\,(N_t-1)}{\tilde{\gamma}_e}\left(\sqrt[N_t-1]{\frac{\exp\left(-\frac{\sigma_e}{\tilde{a}\sigma^2_{\tilde{h}_e}}\sigma_e^2\right)}{1-\beta}}-1\right) \tag{3.43a}$$

$$\text{s.t. } \tilde{a} > \frac{\gamma_b\sigma_b^2}{||\tilde{\mathbf{h}}_b||^2}, P \leq P_{max}. \tag{3.43b}$$

The above problem is convex in the optimisation variable $\tilde{a}$ because it results from adding to the linear (increasing) variable $\tilde{a}$ the monotonically decreasing function for $\tilde{b}$ (as a function of $\tilde{a}$) in (3.41). Indeed, the value for $\tilde{b}$ as a function of $\tilde{a}$ decreases from $\tilde{b} = +\infty$ (when $\tilde{a} = \frac{\gamma_b\sigma_b^2}{||\tilde{\mathbf{h}}_b||^2}$) to its asymptotic value given by

$$\lim_{\tilde{a}\to\infty} \tilde{b} = \frac{2^R\sigma_b^2\,(N_t-1)}{||\tilde{\mathbf{h}}_b||^2}\left(\sqrt[N_t-1]{\frac{1}{1-\beta}}-1\right). \tag{3.44}$$

From the above expression is clear to see the importance of allocating AN when the transmission parties are equidistant. Indeed, the asymptotic behaviour of $\tilde{b}$ reveals that allocating power to AN generation is always necessary irrespective of the amount of power devoted to information. The value will depend on the particular transmission conditions, (e.g., instantaneous channel, distance between nodes, number of antennas) and the probability of secrecy (β) that we have to satisfy. Finally, the solution for the above minimisation problem, as for the one in (3.30), can be efficiently obtained by numerical algorithms.

3.4.4 Resource allocation without a protected zone.

The second case of study arises when the PZ vanishes; i.e., $r_s = 0$. Therefore, the resources allocation problem in (3.30) becomes a single-variable (in a) non-weighted power minimisation problem. It is worth pointing out that not considering the PZ allows the eavesdropper to get close to Alice; indeed, the worst-case for security happens when Eve is co-located with Alice ($r_e = 0$) and this is mathematically equivalent to setting Eve's AWGN power to zero; i.e., $\sigma_e^2 = 0$. This assumption has been considered before in [55] as an effective way to formulate the worst-case

for security. Under this condition the SNR at Eve (from (3.7)) becomes

$$\text{SNR}_e = a\mathbf{t}_1^H\tilde{\mathbf{h}}_e\left[b\tilde{\mathbf{h}}_e^H\mathbf{C}_\eta\tilde{\mathbf{h}}_e\right]^{-1}\tilde{\mathbf{h}}_e^H\mathbf{t}_1 \tag{3.45}$$

and the probabilistic constraint in (3.30b) yields

$$b \geq a\left(\frac{1}{\sqrt[N_t-1]{1-\beta}}-1\right)\left(\frac{2^R r_b^\alpha\sigma_b^2\left(N_t-1\right)}{a||\tilde{\mathbf{h}}_b||^2+r_b^\alpha\sigma_b^2\left(1-2^R\right)}\right) \tag{3.46}$$

which can be substituted into the objective function of the original problem (3.30) to obtain the following non-weighted one-variable power minimisation problem

$$\min_a \; a + a\left(\frac{1}{\sqrt[N_t-1]{1-\beta}}-1\right)\left(\frac{2^R r_b^\alpha\sigma_b^2\left(N_t-1\right)}{a||\tilde{\mathbf{h}}_b||^2+r_b^\alpha\sigma_b^2\left(1-2^R\right)}\right) \tag{3.47a}$$

$$\text{s.t. } a > \frac{\gamma_b r_b^\alpha\sigma_b^2}{||\tilde{\mathbf{h}}_b||^2},\; P \leq P_{max}. \tag{3.47b}$$

The problem above is convex in the optimisation variable a because it results from adding the linear increasing value of a and the monotonically-decreasing function for b in (3.46). This last function decreases from $b = +\infty$ (when $a = \frac{\gamma_b r_b^\alpha\sigma_b^2}{||\tilde{\mathbf{h}}_b||^2}$) to its asymptotic value given by

$$\lim_{a\to\infty} b = \left(\frac{1}{\sqrt[N_t-1]{1-\beta}}-1\right)\left(\frac{2^R r_b^\alpha\sigma_b^2\left(N_t-1\right)}{||\tilde{\mathbf{h}}_b||^2}\right). \tag{3.48}$$

Therefore, the minimisation problem of (3.47) can be efficiently solved by using numerical algorithms. However, we note that the mathematical complexity of the problem in its current format has been reduced due to the simplification of the exponential term. Therefore, a closed-form solution can be provided by seeking the saddle point obtained when the gradient of the objective function is zero. Then, we take the first derivative of the objective function (3.47a) and we equalise it to zero to obtain a quadratic function in a that can be easily solved obtaining

$$a = \frac{\gamma_b r_b^\alpha\sigma_b^2}{||\tilde{\mathbf{h}}_b||^2}\left(1+\sqrt{\frac{2^R}{2^R-1}\left(\frac{1}{\sqrt[N_t-1]{1-\beta}}-1\right)}\right). \tag{3.49}$$

In the expression above, we only consider the positive root of the quadratic function because the negative one will lead to an infeasible value for a considering the constraint in (3.47b). The expression (3.49) determines the value of power

required for the information and enables us to compute the power for the AN (b) using (3.46).

As expected, the solution to this problem is similar to the one provided by the weighted resources optimisation problem in (3.30) when $r_{s_{max}}$ is set to a value arbitrarily close to zero. By setting $r_{s_{max}} = 0$, the problem is not mathematically tractable due to the division by a zero term in the cost function in (3.30a). It is worth pointing out that by assuming the worst-case condition for security (i.e., $r_e = 0$, equivalent to $\sigma_e^2 = 0$), this scenario demands additional power for the AN generation. This can be easily seen by comparing the terms within the radical expression in the solution for $b^\star$ in (3.21) against the one presented here in (3.46) where the exponential function has taken the maximum possible value of one. From these results, the feasibility rate of solving the problem is expected to decrease substantially in power constrained scenarios thus affecting the transmission throughput.

3.4.5 Numerical Results

The analysis of the outage based secrecy rate formulation is based on both, the resource allocation and the secrecy performance considering the feasibility of solving the problem and its impact on throughput. Thus, as in §3.3.2, the *normalised secrecy throughput* (T_{SEC}) is defined as the achieved probability of secrecy (P_{SEC}) times the ratio between the number of channel realisations where transmission takes place (i.e., the problem is feasible) and the total number of channel realisations in the simulations. Additionally, the parameter ϕ is defined as the ratio of the cost function weights, i.e., $\phi = \frac{\kappa_2}{\kappa_1}$. 4000 Monte Carlo simulations have been considered with setup values summarised in the Table 3.3.

Figure 3.8 depicts how the resources are allocated with respect to the total available power (P_{max}) (AWGN). The ratio of the cost function weights is $\phi = 1$; i.e., same priority for using power and enlarging the PZ. Here it is shown how the secrecy radius r_s (relative to r_b) required by the technique decreases as more power is made available; indeed, for a high target probability of secrecy (β) and low maximal power (P_{max}) the PZ approaches its maximum possible size given by $r_{s_{max}}$ (relative to Alice-to-Bob distance $r_b = 1$). Interestingly, the total allocated power ($P = a + b$) reaches a point where (on average) no more power is necessary to achieve the target probability of secrecy β even though that power is still

Table 3.3: *Parameters for the simulation.*

Parameter	Value	Description
N_t	5	Alice's number of antennas
$\sigma^2_{\tilde{h}_b}$	1	Bob's channel elements variance
$\sigma^2_{\tilde{h}_e}$	1	Eve's channel elements variance
σ^2_b	1	Bob's AWGN power
σ^2_e	1	Eve's AWGN power
P_{max}	6	Maximal power for constrained systems normalised relative to the AWGN power
α	2	Path loss exponent

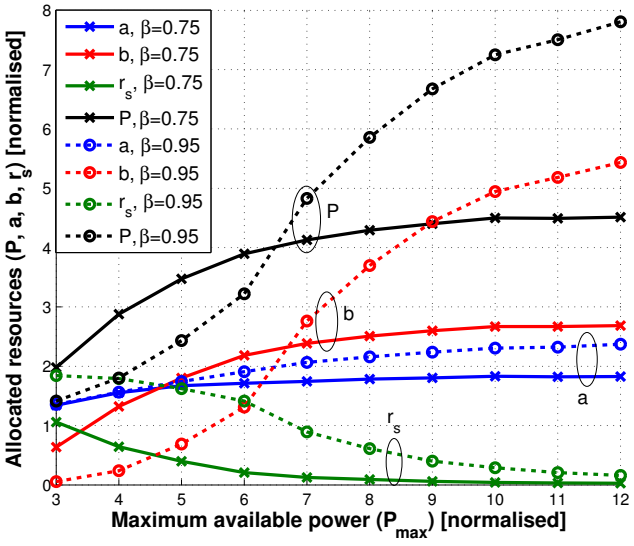


Figure 3.8: *Resources allocation. Transmit power* $(P = a + b)$ *and secrecy radius* (r_s) *(relative to* $r_b = 1$*) versus maximum available power* (P_{max}) *(normalised relative to AWGN power) for different values of probability of secrecy* (β) *when* $\phi = 1$*,* $R = 2$ *bps/Hz, and* $r_{s_{max}} = 2$ *(relative to* r_b*).*

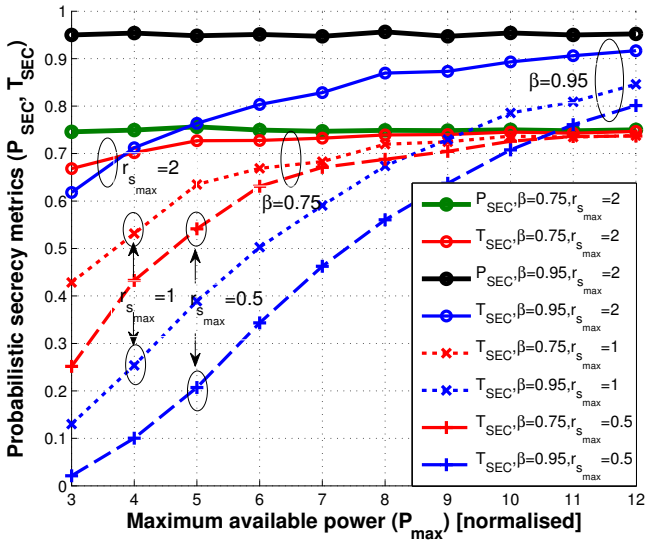
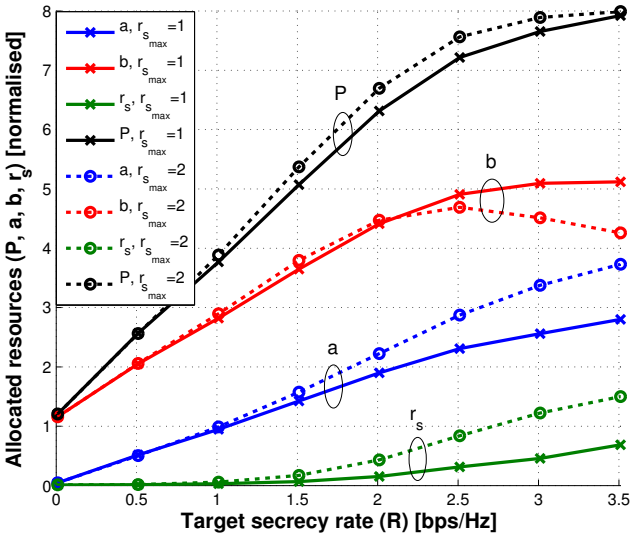


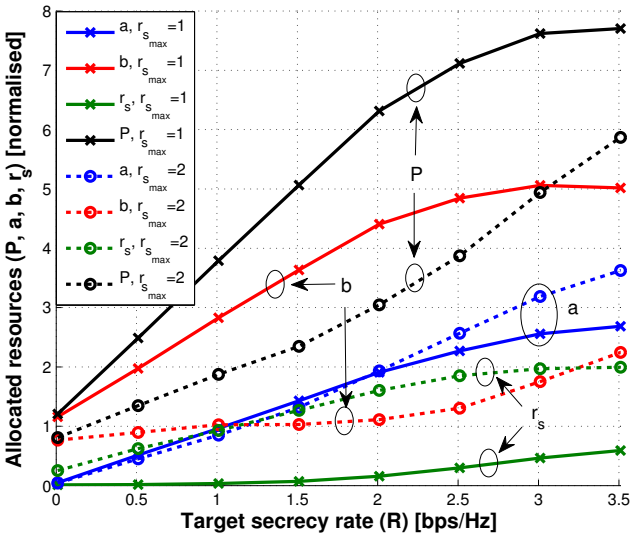
Figure 3.9: *Achieved probability of secrecy (P_{SEC}) and normalised secrecy throughput (T_{SEC}) versus maximum available power (P_{max}) (normalised relative to the AWGN power) for different values of probability of secrecy (β) and $r_{s_{max}}$ when $\phi = 1$ and $R = 2$ bps/Hz.*

available. However, Figure 3.9 implies that the availability of extra resources has a positive impact on the normalised secrecy throughput T_{SEC} because it improves the feasibility rate of the system. It is worth pointing out that the target probability of secrecy (β in (3.24b)) is achieved no matter what the available resources are; although, there is a cost to pay in throughput for high resource constrained conditions. It is also worth remarking on the high normalised secure throughput offered by the implementation of a large PZ even when the total available power (P_{max}) is low.

Now, let us devote our attention to the way that the resources are allocated. Prioritising the use of power rather than extending the size of the PZ (i.e., $\phi = 2$) results in a scenario where full power is used, mainly for AN generation, keeping the size of the PZ as small as possible. This behaviour is illustrated in Figure 3.10a. In contrast, as is seen in Figure 3.10b, when the ratio of the cost function weights prioritises saving power (i.e., $\phi = 0.5$), the PZ is extended to its maximum size for demanding conditions; i.e., a large R, devoting a smaller amount of power for AN generation. Whilst the amount of power devoted for information remains the same for both prioritising schemes, the trade-off between increasing power for AN generation and enlarging the PZ's size is clear because both methods pursue



(a) $\phi = \frac{\kappa_2}{\kappa_1} = 2$



(b) $\phi = \frac{\kappa_2}{\kappa_1} = 0.5$

Figure 3.10: *Resources allocation. Transmit power* $(P = a + b)$ *and secrecy radius* (r_s) *versus target secrecy rate* (R) *for different values of* $r_{s_{max}}$ *(relative to* r_b*) when normalised* $P_{max} = 8$ *(relative to the AWGN power) and* $\beta = 0.95$.

the same objective: deteriorate the quality of the eavesdropper's link. In both plots in Figure 3.10, making a larger PZ radius available (i.e., a larger $r_{s_{max}}$), not only contributes to saving transmit power, but it also has a positive impact on the secrecy throughput as is also shown in Figure 3.8. On the other hand, a small PZ given by a small $r_{s_{max}}$ demands high power and negatively affects the normalised secrecy throughput. This result corroborates the analytic findings in §3.4.4 where the worst-case security strategy is analysed when a PZ is not deployed; i.e., $r_s = r_e = 0$. Finally, it is worth pointing out that the considered weights in the WNCF in (3.23) given by κ_1 and κ_2 define how the resources are actually used while the security performance of the strategy is dictated by the availability of resources.

3.5 Discussion and summary

In this chapter we have presented two probabilistic frameworks to distribute the network resources in masked beamforming MISO networks under the presence of passive eavesdroppers. First, we have introduced a closed-form power distribution strategy between information and artificial noise to guarantee a given probability of secrecy defined by QoS constraints both at the intended receiver and at the eavesdroppers. Second, we have devised an approach to guarantee a given probability of secrecy defined by a target secrecy rate. Here, the technique distributes the network resources by allocating the power between information and artificial noise and also determines the required size of a protected zone to avoid close eavesdroppers.

Both approaches make an efficient use of the available resources to effectively guarantee a high probability of secrecy by striking a balance between secrecy and quality. There is a trade-off between achieving a high probability of secrecy and the secrecy throughput that can be improved by augmenting the total amount of power available at the transmitter. The introduced probabilistic outage based techniques compare favourably against methods that provide security in an average; therefore, the presented techniques use more efficiently the available power by improving the security performance.

Introducing a protected zone is a meaningful security measure that not only improves the security by avoiding close-quarter eavesdropping attacks, but also

enables us to quantify the impact in terms of power consumption through providing security in the presence of a close eavesdropper. In fact, providing secrecy in the absence of a protected zone requires a substantially larger amount of power mainly devoted for artificial noise generation. The introduced resources allocation method makes it possible to prioritise between using power for artificial noise generation and increasing the size of the protected zone to deteriorate the eavesdropper's received signal quality. Interestingly, the optimisation strategy prioritisation criterion does not affect the security performance of the system, which is given by the amount of resources available, but it does introduce a degree of flexibility in the system design.

The introduced techniques are attractive for practical implementation because they offer flexibility by efficiently using the network resources. For instance, the security level, given by the probability of secrecy, that a wireless user surfing the web requires might be different to that of a high security military application. Therefore, setting different targets of probability suits these different security needs allowing an efficient use of power. Moreover, the security is enhanced by taking advantage of physical network deployments that intrinsically define eavesdroppers' exclusion areas such as security perimeters or restricted access rooms. We have incorporated these criteria into the network design to enhance the security of a MISO system through deploying a protected zone to efficiently use the power.

Chapter 4

A MISO robust transmission for physical layer security

> 'You, secret, who feed me; you, secret, pledge of my freedom; for the guilt that I give you, for the kiss that you give me'
>
> Silvio Rodríguez

In this chapter we introduce a robust transmission strategy to convey confidential information from a multiple-antenna transmitter towards a single-antenna receiver in the presence of a single-antenna passive eavesdropper. We study the practical problem that arises when the measure of the main link's channel state information (CSI) available at the transmitter is subject to errors. Indeed, in practical networks it is not possible for the transmitter to obtain a perfect CSI of the main link due to errors during the channel estimation and feedback processes. This inaccuracy can jeopardise the security of the transmission strategy; therefore, it is necessary to devise robust transmission mechanisms that can cope with a degree of uncertainty in the main link's CSI and still provide a secure transmission.

In order to tackle this problem, we use a masked beamforming transmission scheme to formulate two robust optimisation problems to determine the transmission covariance matrices of the steering information signal and the artificial

noise. The objectives are to maximise the worst-case secrecy rate in a resource-constrained system and to minimise the use of resources to ensure a target worst-case average secrecy rate. We incorporate into the analysis the impact of the distance between the transmission parties and study how an eavesdropper physically located in the vicinity of the transmitter can put at risk the network's security. Therefore, as a countermeasure, we deploy a '*Protected Zone*' to prevent close-quarters eavesdropping attacks. The proposed robust masked beamforming scheme offers a secure performance even with erroneous estimates of the main channel enhancing the network security by deploying a PZ and therefore making an efficient use of the power.

Regarding this chapter's structure, in section 4.1 we present a review of the state-of-art of the existing secure robust transmission schemes. In section 4.2 we model the multiple-input multiple-output (MISO) system considering the robust formulation and the worst-case definition of secrecy. Subsequently, in section 4.3 the worst-case secrecy rate robust problem is studied while the robust transmission resources minimisation problem is addressed in section 4.4. In section 4.5 we carry out a detailed analysis of the properties of the optimal solutions of the two problems to provide valuable insight into the transmission strategy nature. Finally, the section 4.6 concludes this chapter.

4.1 Physical layer security robust schemes in MISO networks

Beamforming has been proven as the optimal transmit strategy to maximise the secrecy rate in MISO networks with perfect CSI available for the main link for both active and passive eavesdropping scenarios [46, 47, 49, 50]. Furthermore, this technique can be elegantly enhanced by broadcasting *artificial noise* (AN) to confuse unknown eavesdroppers [37]. Notwithstanding the remarkable contribution of *masked beamforming* based transmission schemes to improve wireless security in MISO systems, this technique still faces open issues regarding its practical implementation. Indeed, the transmitter might have access only to an erroneous version of the intended receiver's link CSI. This mismatch can occur due to either imperfect feedback links between the transmitter and receiver generating errors during

the channel estimation and feedback processes or outdated versions of the available CSI. Neglecting these errors introduces important security breaches resulting from steering the information into an incorrect direction and unintentionally jamming the intended receiver [74]. Moreover, an inaccurate version of the main link CSI can result in an intended receiver not being able to decode the package due to exceeding the transmission data rate that it can support [75]. Finally, an erroneous CSI would introduce errors into the optimal distribution of the available power between information and AN [76, 77]. In this scenario, the paramount importance of considering the practical limitations of acquiring an error-free CSI becomes clear. Therefore, in this chapter we introduce secure robust masked beamforming transmission strategies able to cope with a given degree of uncertainty in the main link's CSI in the presence of an unknown eavesdropper.

Robust precoding techniques have been introduced to deal with uncertainties in the CSI between multiple-antenna transmission parties. In general, we can use two kind of robust approximations to model the channel uncertainties. The first one considers a random Gaussian model where the channel errors are assumed to be random and normal distributed; therefore, they are associated with a channel uncertainty covariance [52, 78, 79, 80]. In other words, the channel uncertainties are assumed stochastic and they are statistically modelled to attain a given performance in a probabilistic fashion. The second approach is based on the assumption that all the possible states of the channel are defined deterministically within a given set whose norm is known [81, 82, 83, 84]. This second case is a conservative design because it considers the worst-case performance. Indeed, this model guarantees a given performance for any admissible CSI uncertainty within the deterministic set; even the worst one. Both robust formulation cases generally result into nonconvex and then hard-to-solve problems; indeed, the latest modelling leads to hard-to-solve *maximin* or *minimax* optimisation problems. In this scenario, convex optimisation machinery becomes a particularly useful mathematical tool to recast these problems into tractable convex formulations that can be efficiently solved by interior-point algorithms.

4.1.1 Secure robust beamfoming by convex optimisation

Convex optimisation has become a powerful mathematical framework widely used in the design and analysis of communication systems and signal processing algo-

rithms [85, 86]. Convex optimisation refers to the minimisation of a convex objective function subject to constraints that are either convex or affine functions. An important property of convex optimisation techniques is that in a convex problem a local optimal point is also a global optimal point and therefore rigorous optimality conditions and duality properties can be used to validate the optimality of the solution [87, §4.2]. Moreover, powerful numerical algorithms based on the interior-point method can efficiently provide a solution to convex problems with reasonable complexity [87, §11]. As a result, hard-to-solve nonconvex problems can be efficiently solved by recasting them into tractable convex equivalent problems.

Physical layer security MISO techniques have been nurtured from convex optimisation approaches; that is the case of the works presented in [49, 50, 59]. Regarding robust formulations to deal with channel uncertainties, in [88], Zhang et al. introduce an approach to model the partially known eavesdropping channel based on deterministic uncertainties. Here a steering information signal is solely conveyed to devise a transmission solution by establishing a relationship between the MISO cognitive radio and the MISO wireless security problem. In the work presented in [89], the MISO worst-case secrecy rate is maximised considering also the sole transmission of information. In contrast to these works, in [90], Li et al. consider a masked transmission method where steering information is transmitted along with AN. Here, the eavesdropping channel is partially known and stochastic channel uncertainties are assumed about the attacker channel to formulate an outage optimisation problem that looks towards maximising the secrecy rate. Now, in [91, 92], Huang and Swindlehurst also consider masked beamforming but use the deterministic model over the imperfect eveadropper link's CSI to address the worst-case secrecy rate maximisation. Finally, in [93, 94] Li and Ma extended this analysis to the multiple-antenna multi-eavesdroppers case considering the deterministic uncertainty model while Pei et al. assume in [95] a stochastic uncertainty scenario but enforce a minimum mean square error (MMSE) reception combiner at the multiple-antenna eavesdroppers.

Remarkably, all the aforementioned techniques conclude that the optimal information transmission covariance matrix is rank-one. In other words, transmit beamforming is the optimal strategy that maximises the secrecy rate for MISO systems when there is partial knowledge of the eavesdropping channel. All these

frameworks use robust formulations to model a partially known eavesdroppers' CSI; however, neither of them addresses the most demanding case for the security of a MISO network that arises when the main link is prone to estimation errors. This case is investigated in two contributions. First, in [96], a robust transmit design conveys steering information using deterministic uncertainties in both the partially know multiple-antenna eavesdropping channel and in the main channel. This work only considers steering information transmission without AN while in contrast, [72] introduces a robust masked beamforming framework using a second-order perturbation analysis of the singular value decomposition (SVD) of the main channel. It is worth pointing out that the latter approach does not use convex optimisation techniques. Indeed, here the definition of security is based on restrictive QoS constraints rather than in secrecy rate and the information is steered over the erroneous main channel signature while the AN is generated isotropically and orthogonal to the main channel.

4.1.2 This chapter's contribution

The contribution of this chapter is twofold. First, we consider a masked robust transmission strategy to deal with a mismatch in the MISO main channel without prior knowledge about the instantaneous eavesdropping link; that is a pure passive eavesdropping scenario. Second, we consider the effect of the distance between the nodes on the overall security and, as in the previous chapter's §3.4, we deploy a '*protected zone*' (PZ) to avoid close-quarters eavesdropping attacks and then make an efficient use of the available resources of the network. Our objective is to calculate the steering information and AN transmission covariance matrices along with the size of the PZ. We consider a conservative approach and assume deterministic uncertainties to formulate two worst-case optimisation problems:

- the maximisation of the average worst-case secrecy rate in a resource constrained network.
- the minimisation of the use of resources given by the power and size of the PZ subject to ensure a target average worst-case secrecy rate.

Both optimisation problems turn out to be nonconvex and hard-to-solve; therefore, we recast them into tractable convex semidefinitive programs (SDP) by using

convex optimisation tools. The equivalent SDPs can be solved by interior-point based solvers. We study the nature of the obtained optimal solutions by analysing their convex optimisation optimality conditions and thus showing two insights. The information transmission covariance matrices for both problems are unique and rank-one and the AN is isotropically generated over the nullspace spanned by the rank-one transmission covariance matrix. In other words, the optimal transmission for the average worst-case secrecy rate maximisation and the resources minimisation problems is beamforming while the AN is orthogonal to the beamformer vector and isotropically broadcast. For both problems numerical simulations are presented showing that not only do the resulting transmission strategies enhance the system security but also that restricting the presence of an attacker in the transmitter's vicinity allows us to save power.

4.1.3 Robust cooperative techniques for physical layer security

It is worth pointing out that similar robust approaches as the ones used in this chapter can be used for cooperative networks [97, 98]. Here, cooperative relays act as a virtual array to achieve spatial diversity similar to a multiple-antenna transmitter [99]. Moreover, an AN signal can be transmitted by using cooperative jamming techniques from trusted relays to confuse passive eavesdroppers [100, 101]. In this context, the authors of [91, 92] used a deterministic approach to formulate a robust transmission scheme to maximise the secrecy rate when cooperative jammers aid a multiple-antenna transmitter. We present an interesting alternative to cooperative techniques in chapter 6 of this thesis.

4.2 System model

In this section, we model a MISO system in the presence of an unknown single-antenna eavesdropper. We follow the wireless secrecy model where the transmitter, the legitimate receiver and the eavesdropper are named 'Alice', 'Bob' and 'Eve' respectively.

Alice is equipped with $N_t \geq 2$ antennas while Bob and Eve are single antenna nodes. The Alice-to-Bob and Alice-to-Eve channel vectors are denoted by

$\mathbf{h}_b \in \mathbb{C}^{N_t}$ and $\mathbf{h}_e \in \mathbb{C}^{N_t}$. In order to incorporate the impact of the distance between the transmission parties into the system model, we consider the path-loss effect in the channel modelling; therefore $\mathbf{h}_b = r_b^{-\frac{\alpha}{2}} \tilde{\mathbf{h}}_b$ and $\mathbf{h}_e = r_e^{-\frac{\alpha}{2}} \tilde{\mathbf{h}}_e$. Here, r_b and r_e are respectively the Alice-to-Bob and Alice-to-Eve distances and $\alpha \geq 2$ denotes the path loss exponent. The small-scale fading channel vectors $\tilde{\mathbf{h}}_b \sim \mathcal{CN}(\mathbf{0}, \sigma^2_{\tilde{h}_b} \mathbf{I})$ and $\tilde{\mathbf{h}}_e \sim \mathcal{CN}(\mathbf{0}, \sigma^2_{\tilde{h}_e} \mathbf{I})$ are mutually independent and not affected by the communication range. A pure passive eavesdropping scenario is considered and so $\mathbf{h}_e$ remains unknown to Alice; however, she can make statistical assumptions about it.

The masked beamforming secure transmission strategy considers the transmission of information and AN simultaneously; therefore, the transmitted signal vector $\mathbf{s} \in \mathbb{C}^{N_t}$ is modelled as $\mathbf{s} = \mathbf{w} + \boldsymbol{\eta}$. Here, the confidential information vector $\mathbf{w} \in \mathbb{C}^{N_t}$ is chosen from a Gaussian codebook, and it has covariance matrix $\mathbf{C}_w = \mathbb{E}\{\mathbf{w}\mathbf{w}^H\}$. Likewise, $\boldsymbol{\eta} \in \mathbb{C}^{N_t}$ is the AN vector with covariance matrix $\mathbf{C}_\eta = \mathbb{E}\{\boldsymbol{\eta}\boldsymbol{\eta}^H\}$. As a result, the covariance matrix of the transmitted signal vector $\mathbf{s}$ is $\mathbf{C}_s = \mathbb{E}\{\mathbf{s}\mathbf{s}^H\}$ and so Alice's total transmitted power is given by $P = \text{Tr}\{\mathbf{C}_s\} = \text{Tr}\{\mathbf{C}_w\} + \text{Tr}\{\mathbf{C}_\eta\}$.

The scalar signals received by the single-antenna Bob and Eve are respectively given by

$$u = r_b^{-\frac{\alpha}{2}} \tilde{\mathbf{h}}_b^H \mathbf{w} + r_b^{-\frac{\alpha}{2}} \tilde{\mathbf{h}}_b^H \boldsymbol{\eta} + n_b \tag{4.1}$$

$$v = r_e^{-\frac{\alpha}{2}} \tilde{\mathbf{h}}_e^H \mathbf{w} + r_e^{-\frac{\alpha}{2}} \tilde{\mathbf{h}}_e^H \boldsymbol{\eta} + n_e \tag{4.2}$$

where $n_b \sim \mathcal{CN}(0, \sigma_b^2)$ and $n_e \sim \mathcal{CN}(0, \sigma_e^2)$ are the additive Gaussian noise components at Bob's and Eve's antennas.

It is worth pointing out that here we use a totally different masked beamforming scheme from the one considered in the previous chapter 3's §3.2. Previously we restricted the analysis to the case when the transmitter steers the information towards the legitimate receiver alongside an AN signal generated over Bob's channel nullspace. In contrast, here we have not enforced any assumption about the information and the AN vectors' directions. As a result, the AN vector $\boldsymbol{\eta}$ may not be aligned orthogonally to Bob's channel signature and then it could effectively deteriorate the legitimate receiver's performance. This can be clearly seen when comparing the received signal at Bob's antenna in (4.1), where the AN vector $\boldsymbol{\eta}$ affects the legitimate received signal, against the expression in (3.4) where the AN effect is cancelled due to the fact that $\boldsymbol{\eta}$ is orthogonal to Bob's channel vector $\tilde{\mathbf{h}}_b$.

This system setup allows Alice to steer the information in a direction in such a way that secrecy can be achieved even when she has an erroneous CSI of the main link.

Finally, the received instantaneous signal-to-noise-ratios (SNRs) at Bob and Eve are

$$\mathrm{SNR}_b = \frac{\tilde{\mathbf{h}}_b^H \mathbf{C}_w \tilde{\mathbf{h}}_b}{\tilde{\mathbf{h}}_b^H \mathbf{C}_\eta \tilde{\mathbf{h}}_b + r_b^\alpha \sigma_b^2} \tag{4.3}$$

$$\mathrm{SNR}_e = \frac{\tilde{\mathbf{h}}_e^H \mathbf{C}_w \tilde{\mathbf{h}}_e}{\tilde{\mathbf{h}}_e^H \mathbf{C}_\eta \tilde{\mathbf{h}}_e + r_e^\alpha \sigma_e^2} \tag{4.4}$$

and they yield the achievable secrecy rate R_S of the modelled system as follows

$$\mathrm{R}_S = \left[\log_2\left(1+\mathrm{SNR}_b\right) - \log_2\left(1+\mathrm{SNR}_e\right)\right]^+ \left[\text{bps/Hz}\right]. \tag{4.5}$$

4.2.1 Worst-case robust transmit design

We consider that Alice has available an error-prone estimate of the intended receiver's link CSI due to errors during the channel estimation and feedback processes. Therefore, a worst-case (deterministic) robust model is now considered. In this scenario, the actual instantaneous channel lies within a known set of uncertainty values whose range represents the 'amount of uncertainty' about the channel. This is illustrated in Figure 4.1 where the system model of a deterministic robust system is depicted. A worst-case robust design achieves a given performance level for any channel realisation within the deterministically defined uncertainty set [84]. Therefore, we incorporate this robust formulation into our transmission strategy in order to deal with a mismatch in the main channel without prior knowledge about the instantaneous eavesdropping link considering the effect of the distance between the transmission nodes on the overall security. A '*Protected Zone*' (PZ) is deployed to avoid eavesdroppers close to the transmitter.

We define the Alice-to-Bob channel as

$$\mathbf{h}_b = \left(\hat{r}_b + \varsigma_b\right)^{-\frac{\alpha}{2}} \left(\hat{\mathbf{h}}_b + \boldsymbol{\delta}_b\right) \tag{4.6a}$$

$$\text{s.t. } \boldsymbol{\delta}_b \in \boldsymbol{\Delta}_b = \left\{\boldsymbol{\delta}_b : ||\boldsymbol{\delta}_b|| \leq \epsilon_b\right\}, \tag{4.6b}$$

$$\varsigma_b \in \xi_b = [0, \epsilon_{r_b}] \tag{4.6c}$$

where the actual instantaneous channel $\mathbf{h}_b$ is defined by both the error vector $\boldsymbol{\delta}_b \in \mathbb{C}^{N_t}$, by the error distance $\varsigma_b \in \mathbb{R}$ and by the observed mismatched version of the

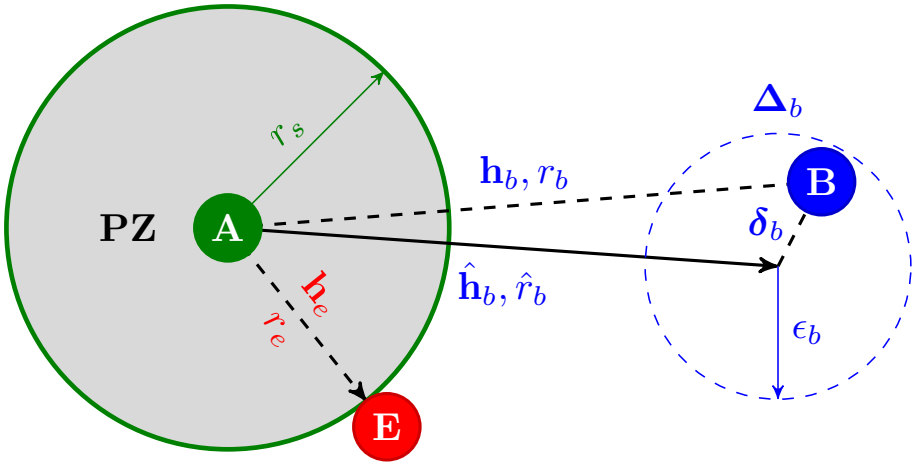


Figure 4.1: *System model with mismatched main channel and protected zone deployed. Alice knows both the erroneous channel* $\hat{\mathbf{h}}_b$ *and the range* ϵ_b *that define the uncertainty set* $\boldsymbol{\Delta}_b$ *within which the actual channel* $\mathbf{h}_b$ *lies.*

small-scale fading main channel $\hat{\mathbf{h}}_b$ and the erroneous distance between Alice and Bob $\hat{r}_b$. The errors $\boldsymbol{\delta}_b$ and ς_b are unknown to Alice, but they respectively lie within the sets $\boldsymbol{\Delta}_b$ and ξ_b upper-bounded by the known values of ϵ_b and ϵ_{r_b}.

Protected Zone

In order to avoid close-quarter eavesdropping attacks, we consider in the system model a *Protected Zone* (PZ) as introduced in the previous chapter's §3.4.1 and originally published in our work in [102]. The PZ is defined by the *Security Radius* (r_s) that is the transmitter-to-the PZ border distance. As illustrated in Figure 4.1, the inclusion of the PZ is equivalent to restricting the Alice-to-Eve distance to $r_e \geq r_s$. This formulation is meaningful and relevant by itself. Moreover, it allows us to quantify the impact on the security of the eavesdroppers' location and the additional power required by the robust strategy to preserve confidentiality in the presence of a close attacker (i.e., $r_s \to 0$). Also this formulation let us understand the possible savings in power resulting from an Eve located far away from Alice (i.e., $r_s \gg 0$).

4.2.2 Average worst-case secrecy rate

The problem of interest is the passive eavesdropping scenario; therefore, Alice can only model statistically the Eve's link CSI. In this context, and according to Shafiee and Ulukus [46] and Li and Petropulu [54], the ergodic secrecy rate (R_S) for a MISO system when the main link's CSI is perfectly known and only statistical information about the eavesdropper's channel is available at Alice, is given by

$$\mathrm{R}_S = \log_2\left(1+\frac{\tilde{\mathbf{h}}_b^H\mathbf{C}_s\tilde{\mathbf{h}}_b}{\sigma_b^2}\right) - \mathbb{E}_{\tilde{h}_e}\left\{\log_2\left(1+\frac{\tilde{\mathbf{h}}_e^H\mathbf{C}_s\tilde{\mathbf{h}}_e}{\sigma_e^2}\right)\right\}, \left[\frac{\text{bits}}{\text{Hz}}\right] \tag{4.7}$$

where we recall that $\mathbf{C}_s$ denotes the covariance matrix of the transmitted signal.

In this current work, and in contrast to the results presented in [46] and [54], the transmitted vector $\mathbf{s}$ is composed of both steering information and AN components. Moreover, as described in §4.2.1, Alice only knows an erroneous version of the actual Alice-to-Bob channel. Therefore, Alice can only assume statistics regarding the small-fading eavesdropping channel's elements that are given by the covariance matrix $\mathbf{R}_{\tilde{h}_e} = \mathbb{E}\{\tilde{\mathbf{h}}_e\tilde{\mathbf{h}}_e^H\} = \sigma^2_{\tilde{h}_e}\mathbf{I}_{N_t}$. Regarding the channel's path loss component associated with the distance between Alice-to-Eve, we consider the worst-case for the security in a system where a PZ has been deployed. This occurs when Eve lies exactly on the PZ boundary; i.e., $r_e = r_s$. Under this scenario, a security performance metric for our robust scheme is introduced to quantify the average worst-case security rate as follows

$$\mathrm{R}_S^{wc} = \left[\log_2\left(1+\min_{\substack{\boldsymbol{\delta}_b\in\boldsymbol{\Delta}_b,\\ \varsigma_b\in\xi_b}}\mathrm{SNR}_b\right) - \log_2\left(1+\overline{\mathrm{SNR}}_e\right)\right]^+, \left[\frac{\text{bits}}{\text{Hz}}\right] \tag{4.8}$$

where

$$\overline{\mathrm{SNR}}_e = \frac{\mathrm{Tr}\{\mathbf{C}_w\mathbf{R}_{\tilde{h}_e}\}}{\mathrm{Tr}\{\mathbf{C}_\eta\mathbf{R}_{\tilde{h}_e}\}+r_s^\alpha\sigma_e^2}. \tag{4.9}$$

The definition in (4.8) is a conservative estimate due to consideration of the worst-case SNR_b; i.e., the channel defined within the uncertainty $\boldsymbol{\Delta}_b$ set that delivers the worst performance at Bob given by his lowest achievable SNR_b. It is worth highlighting that in (4.8) the expected value of the logarithmic function in the second term of the RHS of (4.7) is approximated to the average SNR_e defined as $\overline{\mathrm{SNR}}_e$. Here, we have used the concavity property of the logarithm function and *Jensen's inequality*

$$\mathbb{E}\left\{\log_2\left(1+X\right)\right\} \leq \log_2\left(1+\mathbb{E}\left\{X\right\}\right) \tag{4.10}$$

where the expectation is taken over the random variable X [87, §3.1.8]. By this approximation, the problem is restricted to a potentially suboptimal solution by considering a lower-bound of the actual ergodic secrecy rate in (4.7). However, the problem formulation is simplified to allow us to later solve it in an efficient and tractable way. We will later benchmark the performance of our metric and the ergodic secrecy rate by simulations.

4.3 Worst-case secrecy rate maximisation problem

In this section we are interested in a robust transmission strategy to maximise the secrecy rate considering errors in the main link's CSI under the presence of a passive eavesdropper. The strategy should allocate the available resources to enhance the secrecy performance defined by the average worst-case secrecy rate in (4.8). In other words, we look for a transmission mechanism to maximise the secrecy considering the worst possible performance resulting from all the main link's uncertainties defined deterministically accordingly (4.6). To do this we formulate an optimisation problem that is recast as an SDP and offers direct connection to QoS-based security endeavours.

4.3.1 Optimisation problem

We aim to find the information and the AN optimal transmission covariance matrices ($\mathbf{C}_w$, $\mathbf{C}_\eta$) and also the radius of the PZ (defined by the r_s) to maximise the average worst-case secrecy rate R_S^{wc} in a resources constrained system. This problem is stated as follows

$$\max_{\mathbf{C}_w, \mathbf{C}_\eta, r_s} \quad \mathrm{R}_S^{wc} \tag{4.11a}$$

$$\text{s.t. } \mathbf{C}_w \succeq \mathbf{0}, \mathbf{C}_\eta \succeq \mathbf{0} \tag{4.11b}$$

$$P \leq P_{max}, 0 \leq r_s \leq r_{s_{max}} \tag{4.11c}$$

where P_{max} and $r_{s_{max}}$ denote the total available power and the PZ's maximum deployable radius respectively.

Problem (4.11) is hard to solve due to the nonconvexity nature of the objective function defined in (4.8). Therefore, as a first step to deal with this problem in a mathematically tractable fashion, we split the objective function (4.8) into two

terms. This is done by introducing the slack variable $\gamma_e > 0$ and so (4.11) becomes

$$\max_{\mathbf{C}_w, \mathbf{C}_\eta, r_s, \gamma_e} \quad \frac{1}{1+\gamma_e} \left(1 + \min_{\substack{\boldsymbol{\delta}_b \in \Delta_b, \\ \varsigma_b \in \xi_b}} \mathrm{SNR}_b \right) \tag{4.12a}$$

$$\text{s.t. } \overline{\mathrm{SNR}}_e \leq \gamma_e \tag{4.12b}$$

$$\mathbf{C}_w \succeq \mathbf{0}, \mathbf{C}_\eta \succeq \mathbf{0} \tag{4.12c}$$

$$P \leq P_{max}, 0 \leq r_s \leq r_{s_{max}}, \gamma_e > 0. \tag{4.12d}$$

Problem (4.12) is still nonconvex, so in order to recast it into a tractable convex formulation, we set γ_e to an arbitrary fixed value. Hereby, we are implicitly optimising the problem for a given SNR level at Eve as follows

$$\max_{\mathbf{C}_w, \mathbf{C}_\eta, r_s} \quad \min_{\substack{\boldsymbol{\delta}_b \in \Delta_b, \\ \varsigma_b \in \xi_b}} \mathrm{SNR}_b \tag{4.13a}$$

$$\text{s.t. } \overline{\mathrm{SNR}}_e \leq \gamma_e \tag{4.13b}$$

$$\mathbf{C}_w \succeq \mathbf{0}, \mathbf{C}_\eta \succeq \mathbf{0} \tag{4.13c}$$

$$P \leq P_{max}, 0 \leq r_s \leq r_{s_{max}}. \tag{4.13d}$$

The above formulation reminds us of QoS-based designs that, as in the previous chapter's §3.3, secrecy is defined by setting tolerable quality thresholds at the nodes. Here, the system is considered secure if the signal quality at Eve is below the threshold γ_e [53, 59, 72, 103]. In contrast to these techniques, now we are interested in maximising the secrecy rate irrespective of Eve's QoS, and so we devise an iterative algorithm to seek the optimal value of γ_e that delivers the best security performance at the cost of introducing an additional level of complexity.

To efficiently solve the nonconvex maximim optimisation problem in (4.13) we recast it as a mathematically tractable SDP. This procedure is detailed in the next section.

Problem reformulation into a semidefinite program

The first step to transform the problem (4.13) into a tractable SDP is done by using the Charnes-Cooper transformation [104]. The fractional nature of the objective function in (4.3) leads to a quasiconvex problem than can be handled by bisection [87, §4.2.5]. This procedure needs to solve several SDPs to converge to an optimal

solution. As an alternative, we can efficiently solve this problem by a single SDP by introducing the slack variable $\xi > 0$ and then replacing the optimisation variables by $\mathbf{C}_w = \frac{\tilde{\mathbf{C}}_w}{\xi}$ and $\mathbf{C}_\eta = \frac{\tilde{\mathbf{C}}_\eta}{\xi}$.

Now, we minimise the objective function (4.13a) by, as in [96], by separately maximising the denominator and minimising the numerator to address the worst-case formulation by considering separately the channel that delivers the worst performance for the transmitted information and the one that amplifies the effect of the AN. Finally, the robust definition in (4.6) is incorporated into the problem (4.13) to explicitly write it as

$$\max_{\substack{\tilde{\mathbf{C}}_w, \tilde{\mathbf{C}}_\eta, \\ r_s, \xi}} \frac{\min\limits_{\boldsymbol{\delta}_b \in \Delta_b} \left(\hat{\mathbf{h}}_b + \boldsymbol{\delta}_b\right)^H \tilde{\mathbf{C}}_w \left(\hat{\mathbf{h}}_b + \boldsymbol{\delta}_b\right)}{\max\limits_{\boldsymbol{\delta}_b \in \Delta_b} \left(\hat{\mathbf{h}}_b + \boldsymbol{\delta}_b\right)^H \tilde{\mathbf{C}}_\eta \left(\hat{\mathbf{h}}_b + \boldsymbol{\delta}_b\right) + \max\limits_{\varsigma_b \in \xi_b} \xi \left(\hat{r}_b + \varsigma_b\right)^\alpha \sigma_b^2} \tag{4.14a}$$

$$\text{s.t. } \text{Tr}\left\{\left[\frac{\tilde{\mathbf{C}}_w}{\gamma_e} - \tilde{\mathbf{C}}_\eta\right] \mathbf{R}_{\tilde{h}_e}\right\} - \xi r_s^\alpha \sigma_e^2 \leq 0 \tag{4.14b}$$

$$\text{Tr}\left\{\tilde{\mathbf{C}}_w\right\} + \text{Tr}\left\{\tilde{\mathbf{C}}_\eta\right\} \leq \xi P_{max} \tag{4.14c}$$

$$\tilde{\mathbf{C}}_w \succeq \mathbf{0}, \tilde{\mathbf{C}}_\eta \succeq \mathbf{0}, \xi > 0. \tag{4.14d}$$

The Charnes-Cooper transformation allows us, by introducing the slack variable $\xi > 0$, to set the denominator of (4.14a) to one. It is straightforward to see that for the problem above the maximiser for ς_b is its maximum admissible value given by ϵ_{r_b}. On the other hand, R_S^{wc} is maximised by considering the worst performance that we can enforce at Eve's $\overline{\text{SNR}}_e$. This is obtained by enlarging the size of the PZ to the maximum admissible value by setting $r_s = r_{s_{max}}$ in (4.14b) and therefore effectively keeping Eve as far away as possible. All these considerations yield a problem as follows

$$\max_{\substack{\tilde{\mathbf{C}}_w, \tilde{\mathbf{C}}_\eta, \\ \xi}} \min_{\boldsymbol{\delta}_b \in \Delta_b} \left(\hat{\mathbf{h}}_b + \boldsymbol{\delta}_b\right)^H \tilde{\mathbf{C}}_w \left(\hat{\mathbf{h}}_b + \boldsymbol{\delta}_b\right) \tag{4.15a}$$

$$\text{s.t. } \max_{\boldsymbol{\delta}_b \in \Delta_b} \left(\hat{\mathbf{h}}_b + \boldsymbol{\delta}_b\right)^H \tilde{\mathbf{C}}_\eta \left(\hat{\mathbf{h}}_b + \boldsymbol{\delta}_b\right) + \xi \left(\hat{r}_b + \epsilon_{r_b}\right)^\alpha \sigma_b^2 = 1 \tag{4.15b}$$

$$\text{Tr}\left\{\left[\frac{\tilde{\mathbf{C}}_w}{\gamma_e} - \tilde{\mathbf{C}}_\eta\right] \mathbf{R}_{\tilde{h}_e}\right\} - \xi r_{s_{max}}^\alpha \sigma_e^2 \leq 0 \tag{4.15c}$$

where the constraints (4.14c) and (4.14d) hold.

Now, in order to deal with the maximin problem in the objective function, we can introduce a slack variable $u \geq 0$ to effectively set a lower-bound for the inner minimisation. Therefore, by using the epigraph formulation [87, §4.1.3], the objective function in (4.15a) now becomes

$$\max_{\substack{\tilde{\mathbf{C}}_w, \tilde{\mathbf{C}}_\eta, \\ \xi, u}} \; u \tag{4.16a}$$

$$\text{s.t. } \left(\hat{\mathbf{h}}_b + \boldsymbol{\delta}_b\right)^H \tilde{\mathbf{C}}_w \left(\hat{\mathbf{h}}_b + \boldsymbol{\delta}_b\right) \geq u, \forall \boldsymbol{\delta}_b : ||\boldsymbol{\delta}_b|| \leq \epsilon_b \tag{4.16b}$$

where we also have incorporated the deterministic robust definition in (4.6) to enforce that the resulting channel, after considering all the uncertainties within the defined set $\boldsymbol{\Delta}_b$, is lower-bounded by u. The two inequalities in (4.16b) can be expanded as

$$-\boldsymbol{\delta}_b^H \tilde{\mathbf{C}}_w \boldsymbol{\delta}_b - 2\text{Re}\left\{\hat{\mathbf{h}}_b^H \tilde{\mathbf{C}}_w \boldsymbol{\delta}_b\right\} - \hat{\mathbf{h}}_b^H \tilde{\mathbf{C}}_w \hat{\mathbf{h}}_b + u \leq 0 \tag{4.17a}$$

$$\boldsymbol{\delta}_b^H \boldsymbol{\delta}_b - \epsilon_b^2 \leq 0. \tag{4.17b}$$

The above worst-case condition in (4.17a) is quadratic and convex in the channel error vector $\boldsymbol{\delta}_b$ for a fixed $\tilde{\mathbf{C}}_w$. Moreover, $\boldsymbol{\delta}_b$ is defined over a nonempty convex set $\boldsymbol{\Delta}_b$. Thus, according to the $\mathcal{S}$-*procedure* [87, Appendix B.2], the two quadratic inequalities in (4.17) hold iff there exists a variable $\mu_1 \geq 0$ such that

$$\begin{bmatrix} \mu_1 \mathbf{I}_{N_t} + \tilde{\mathbf{C}}_w & \tilde{\mathbf{C}}_w \hat{\mathbf{h}}_b \\ \hat{\mathbf{h}}_b^H \tilde{\mathbf{C}}_w & -\mu_1 \epsilon_b^2 + \hat{\mathbf{h}}_b^H \tilde{\mathbf{C}}_w \hat{\mathbf{h}}_b - u \end{bmatrix} \succeq \mathbf{0}. \tag{4.18}$$

Effectively, we have reformulated the worst-case inner minimisation problem in (4.15a) into a linear matrix inequality (LMI) that is independent of the deterministic value of the infinite possible channel error vectors $\boldsymbol{\delta}_b$ but which considers the definition of the set $\boldsymbol{\Delta}_b$ in which they lie.

Likewise, the worst-case constraint (4.15b) can be written as

$$\boldsymbol{\delta}_b^H \tilde{\mathbf{C}}_\eta \boldsymbol{\delta}_b + 2\text{Re}\left\{\hat{\mathbf{h}}_b^H \tilde{\mathbf{C}}_\eta \boldsymbol{\delta}_b\right\} + \hat{\mathbf{h}}_b^H \tilde{\mathbf{C}}_\eta \hat{\mathbf{h}}_b + \xi \left(\hat{r}_b + \epsilon_b\right)^\alpha \sigma_b^2 - 1 \leq 0 \tag{4.19a}$$

$$\boldsymbol{\delta}_b^H \boldsymbol{\delta}_b - \epsilon_b^2 \leq 0 \tag{4.19b}$$

where (4.19a) is introduced after considering the worst-case maximisation in (4.15b). It is worth pointing out that, in order to use the $\mathcal{S}$-*procedure*, the original equality in (4.15b) resulting from the Charnes-Cooper transformation has been relaxed to

the inequality in (4.19a). Here, it is straightforward to see that the optimal values are obtained when the equality holds. Finally, using the $\mathcal{S}$-*procedure*, the above two quadratic inequalities hold iff there exists a variable $\mu_2 \geq 0$ such that

$$\left[\begin{array}{cc} \mu_2 \mathbf{I}_{N_t} - \tilde{\mathbf{C}}_\eta & -\tilde{\mathbf{C}}_\eta \hat{\mathbf{h}}_b \\ -\hat{\mathbf{h}}_b^H \tilde{\mathbf{C}}_\eta & 1 - \mu_2 \epsilon_b^2 - \hat{\mathbf{h}}_b^H \tilde{\mathbf{C}}_\eta \hat{\mathbf{h}}_b - \xi \left(\hat{r}_b + \varsigma_b \right)^\alpha \sigma_b^2 \end{array} \right] \succeq \mathbf{0}. \tag{4.20}$$

Finally, the original problem in (4.13) is reformulated by considering the new objective function in (4.16a), the LMIs resulting from the worst-case formulations in (4.18) and (4.20), the constraints (4.15c), (4.14c), (4.14d) and the definitions of the introduced slack variables ξ, μ_1 and μ_2. The resulting convex SDP is

$$\min_{\substack{\tilde{\mathbf{C}}_w, \tilde{\mathbf{C}}_\eta, \\ \xi, \mu_1, \mu_2, u}} \quad -u \tag{4.21a}$$

$$\text{s.t. } \text{Tr} \left\{ \left[\frac{\tilde{\mathbf{C}}_w}{\gamma_e} - \tilde{\mathbf{C}}_\eta \right] \mathbf{R}_{\tilde{h}_e} \right\} - \xi r_{s_{max}}^\alpha \sigma_e^2 \leq 0 \tag{4.21b}$$

$$\left[\begin{array}{cc} \mu_1 \mathbf{I}_{N_t} + \tilde{\mathbf{C}}_w & \tilde{\mathbf{C}}_w \hat{\mathbf{h}}_b \\ \hat{\mathbf{h}}_b^H \tilde{\mathbf{C}}_w & -\mu_1 \epsilon_b^2 + \hat{\mathbf{h}}_b^H \tilde{\mathbf{C}}_w \hat{\mathbf{h}}_b - u \end{array} \right] \succeq \mathbf{0} \tag{4.21c}$$

$$\left[\begin{array}{cc} \mu_2 \mathbf{I}_{N_t} - \tilde{\mathbf{C}}_\eta & -\tilde{\mathbf{C}}_\eta \hat{\mathbf{h}}_b \\ -\hat{\mathbf{h}}_b^H \tilde{\mathbf{C}}_\eta & 1 - \mu_2 \epsilon_b^2 - \hat{\mathbf{h}}_b^H \tilde{\mathbf{C}}_\eta \hat{\mathbf{h}}_b - \xi \left(\hat{r}_b + \epsilon_{r_b} \right)^\alpha \sigma_b^2 \end{array} \right] \succeq \mathbf{0} \tag{4.21d}$$

$$\text{Tr} \left\{ \tilde{\mathbf{C}}_w \right\} + \text{Tr} \left\{ \tilde{\mathbf{C}}_\eta \right\} \leq \xi P_{max} \tag{4.21e}$$

$$\tilde{\mathbf{C}}_w \succeq \mathbf{0}, \tilde{\mathbf{C}}_\eta \succeq \mathbf{0}, u \geq 0, \xi \geq 0, \mu_i \geq 0, i = 1, 2 \tag{4.21f}$$

where we recall that we have defined $\mathbf{C}_w = \frac{\tilde{\mathbf{C}}_w}{\xi}$ and $\mathbf{C}_\eta = \frac{\tilde{\mathbf{C}}_\eta}{\xi}$. Note that $\xi > 0$ is relaxed to $\xi \geq 0$ with no effect on the problem since any feasible ξ has to be positive to satisfy the constraints (4.14c) and (4.19a).

The above SDP is efficiently solved by interior-point algorithms implemented by on-the-shelf tools like SeDuMi [105] and the parser applications Yalmip [106], and CVX [107].

Remark 1 *Owing to the instantaneous availability of the small-scale fading main channel $\hat{\mathbf{h}}_b$, the optimal solution for the information covariance matrix $\mathbf{C}_w^\star$ is unique and rank-one.*

Therefore, the transmitted information vector $\mathbf{w}$ becomes a beamforming vector that can be straightforwardly obtained as the principal eigen-vector corresponding to the unique nonzero eigen-value of $\mathbf{C}_w^\star$. We arrive to this conclusion

after the detailed analysis of the structure and characteristics of the SDP (4.21) and its solution $\mathbf{C}_w^\star$ that is carried out in the §4.5 of this chapter.

Remark 2 *Due to the lack of the instantaneous availability of the small-scale eavesdropping fading channel* $\hat{\mathbf{h}}_e$*, the strategy broadcasts the AN orthogonal to* $\hat{\mathbf{h}}_b$ *and* $\mathbf{w}$.

This empirical assertion is based on analysing the simulation results where the AN power is isotropically distributed over the $(N_t - 1)$ equal non-zero eigenvalues of $\mathbf{C}_\eta^\star$ that span the $(N_t - 1)$ dimensional space orthogonal to the rank-one space spanned by $\mathbf{C}_w^\star$ where $\hat{\mathbf{h}}_b$ lies. Indeed, the strategy allocates the AN isotropically into the nullspace of $\mathbf{C}_w^\star$ and thus not affecting the legitimate receiver's performance. This result coincides with [67, 90] and corroborates the effectiveness of AN isotropic designs for passive eavesdropping that broadcast the noise orthogonally to the steering beamforming vector's direction. This is the case for the secure strategy used in chapter 3.

4.3.2 Average worst-case secrecy rate lower bound

We recall that the SDP in (4.21) considers a fixed value of γ_e. Therefore, we have to find the optimal value for γ_e that offers the best secrecy performance; that is the largest R_S^{wc}. As a first step, now we have to evaluate R_S^{wc} for the fixed value of γ_e; thus it is necessary to determine the channel's error vector $\boldsymbol{\delta}_b^\star \in \boldsymbol{\Delta}_b$ that delivers the worst security performance. This can be done by formulating an optimisation problem that takes into account the optimal information and AN covariance matrices $\mathbf{C}_w^\star$ and $\mathbf{C}_\eta^\star$ obtained from solving the SDP (4.21). This problem is

$$\min_{\substack{\boldsymbol{\delta}_b \in \Delta_b, \\ \varsigma_b \in \xi_b}} \frac{\left(\hat{\mathbf{h}}_b + \boldsymbol{\delta}_b\right)^H \mathbf{C}_w^\star \left(\hat{\mathbf{h}}_b + \boldsymbol{\delta}_b\right)}{\left(\hat{\mathbf{h}}_b + \boldsymbol{\delta}_b\right)^H \mathbf{C}_\eta^\star \left(\hat{\mathbf{h}}_b + \boldsymbol{\delta}_b\right) + \left(\hat{r}_b + \varsigma_b\right)^\alpha \sigma_b^2} \tag{4.22a}$$

$$\text{s.t. } \boldsymbol{\delta}_b^H \boldsymbol{\delta}_b - \epsilon_b^2 \leq 0 \tag{4.22b}$$

$$0 \leq \varsigma_b \leq \epsilon_{r_b}. \tag{4.22c}$$

In the above problem, it is straightforward to see that the minimiser of (4.22a) for the error in distance ς_b is its maximum admissible value ϵ_{r_b} defined in (4.6c); i.e., Bob is located as far away as possible. Now, to find the minimiser value for $\boldsymbol{\delta}_b$, it is necessary to solve the quasiconvex problem in (4.22) and this can be done by using

the bisection methodology [87, §4.2.5]. This approach increases the complexity of our technique due to the necessity of solving several feasibility SDPs. Therefore, as a valid alternative, we take advantage of the nature of $\mathbf{C}_{\eta}^{\star}$ discussed in the Remark 2 to relax the problem (4.22) by considering that Alice broadcasts AN orthogonally to $\hat{\mathbf{h}}_b$ and $\mathbf{w}$ and then we approximate $\left(\hat{\mathbf{h}}_b + \boldsymbol{\delta}_b\right)^H \mathbf{C}_{\eta}^{\star} \left(\hat{\mathbf{h}}_b + \boldsymbol{\delta}_b\right) \approx 0$. Now, The problem (4.22) is relaxed to

$$\min_{\boldsymbol{\delta}_b \in \Delta_b} \quad \left(\hat{\mathbf{h}}_b + \boldsymbol{\delta}_b\right)^H \mathbf{C}_{w}^{\star} \left(\hat{\mathbf{h}}_b + \boldsymbol{\delta}_b\right) \tag{4.23a}$$

$$\text{s.t. } \boldsymbol{\delta}_b^H \boldsymbol{\delta}_b - \epsilon_b^2 \leq 0. \tag{4.23b}$$

The problem above is convex and it can be formulated as an SDP by introducing the slack variable $\boldsymbol{\Lambda}_b = \boldsymbol{\delta}_b \boldsymbol{\delta}_b^H$. This new variable is relaxed to $\boldsymbol{\Lambda}_b \succeq \boldsymbol{\delta}_b \boldsymbol{\delta}_b^H$ and subsequently expressed by the *Schur* complement [87, Appendix B.2]. The following equivalent formulation allows us to efficiently solve the problem in (4.22) by only one SDP as follows

$$\min_{\substack{\boldsymbol{\delta}_b \in \Delta_b, \\ \boldsymbol{\Lambda}_b}} \quad \text{Tr}\left\{\mathbf{C}_{w}^{\star} \boldsymbol{\Lambda}_b\right\} + 2\text{Re}\left\{\hat{\mathbf{h}}_b^H \mathbf{C}_{w}^{\star} \boldsymbol{\delta}_b\right\} + \hat{\mathbf{h}}_b^H \mathbf{C}_{w}^{\star} \hat{\mathbf{h}}_b \tag{4.24a}$$

$$\text{s.t. } \begin{bmatrix} \boldsymbol{\Lambda}_b & \boldsymbol{\delta}_b \\ \boldsymbol{\delta}_b^H & 1 \end{bmatrix} \succeq \mathbf{0} \tag{4.24b}$$

$$\text{Tr}\{\boldsymbol{\Lambda}_b\} \leq \epsilon_b^2. \tag{4.24c}$$

It is worth pointing out that simulations have shown that the approximation in (4.23) returns the same result as using the bisection methodology in (4.22). Therefore, the complexity of our technique, given by the number of SDPs that it has to solve to converge towards a solution, is reduced without affecting the performance. Indeed, $\left(\hat{\mathbf{h}}_b + \boldsymbol{\delta}_b^{\star}\right)^H \mathbf{C}_{\eta}^{\star} \left(\hat{\mathbf{h}}_b + \boldsymbol{\delta}_b^{\star}\right) = 0$ holds even for the worst-case channel $(\hat{\mathbf{h}}_b + \boldsymbol{\delta}_b^{\star})$. Now, R_S^{wc} can be evaluated for the fixed γ_e using the expression in (4.8).

4.3.3 Linear searching algorithm to maximise the worst-case secrecy rate

The next step is to find the optimum $\gamma_e^{\star}$ that maximises R_S^{wc}. To do this, we can take advantage of the nature of R_S^{wc} as a function of γ_e to develop a linear searching algorithm. To do this, we first analyse the structure of R_S^{wc} in (4.8).

Analysis of the concave nature of R_S^{wc}

The worst-case secrecy rate R_S^{wc} is a concave function in γ_e. This property results from the way that the strategy solves the SDP (4.21) and the rank-one property of the optimal information covariance matrix $\mathbf{C}_w^\star$. Let us start the analysis by highlighting the definition of the worst-case secrecy rate R_S^{wc} in (4.8). Here, in order to ensure $\mathrm{R}_S^{wc} > 0$ it is necessary that the worst-case $\mathrm{SNR}_b > \gamma_e \geq \overline{\mathrm{SNR}}_e$. Now, from the definitions of SNR_b in (4.3) and $\overline{\mathrm{SNR}}_e$ in (4.9) we can see that SNR_b increases as more power is devoted to the information transmission covariance matrix $\mathbf{C}_w$ while $\overline{\mathrm{SNR}}_e$ increases if less power is allocated to the AN's covariance matrix $\mathbf{C}_\eta$. Therefore, the technique effectively fixes $\overline{\mathrm{SNR}}_e$ to its largest admissible value (γ_e) to use the minimum power for AN generation and then allocate the maximum possible power to information in order to maximise R_S^{wc}. As a result, the SNR_b increases monotonically with γ_e until we arrive at the point where it is not possible to satisfy the condition $\mathrm{SNR}_b > \gamma_e$ that guarantees a positive worst-case secrecy rate; i.e., $\mathrm{R}_S^{wc} > 0$. Finally, R_S^{wc} in (4.8) is a function of the logarithmic difference between the worst-case SNR_b and $\overline{\mathrm{SNR}}_e$; thus, it increases with γ_e until a maximum saddle point and then decreases to approach zero. This characteristic is clearly seen in Figure 4.2, where the concave nature of R_S^{wc} in γ_e is shown for one particular channel realisation. Here, the considered small-scale fading channel is set to $\hat{\mathbf{h}}_b = [0.23{+}0.66i, -0.92{+}0.17i, -0.31{-}0.49i, 0.24{-}0.46i]^T$, the maximum power $P_{max} = 5$ (normalised relative to the AWGN power) and the secrecy radius $r_{s_{max}} = 0.5$ (relative to r_b). The uncertainties upper-bounds for the uncertainties are fixed to $\epsilon_b = 0.3$ and $\epsilon_{r_b} = 0.3$.

Now, the concave nature of R_S^{wc} as a function of γ_e can be exploited to develop a linear searching algorithm as follows.

Algorithm 1

- Initialise γ_e^{ini} to a value larger but approximately equal to 0; i.e., $\gamma_e^{ini} \gtrapprox 0$ and $\gamma_e^{end} = \frac{P_{max}||\hat{\mathbf{h}}_b||^2}{\hat{r}_b^\alpha \sigma_b^2}$.
- Define ρ as the accuracy tolerance for optimal $\gamma_e^\star$ and N intervals.
- Repeat while $\gamma_e^{end} - \gamma_e^{ini} > \rho$
  - $\gamma_e^i = \gamma_e^{ini} + \frac{(i-1)}{N}\left(\gamma_e^{end} - \gamma_e^{ini}\right), i \in [1, N+1]$

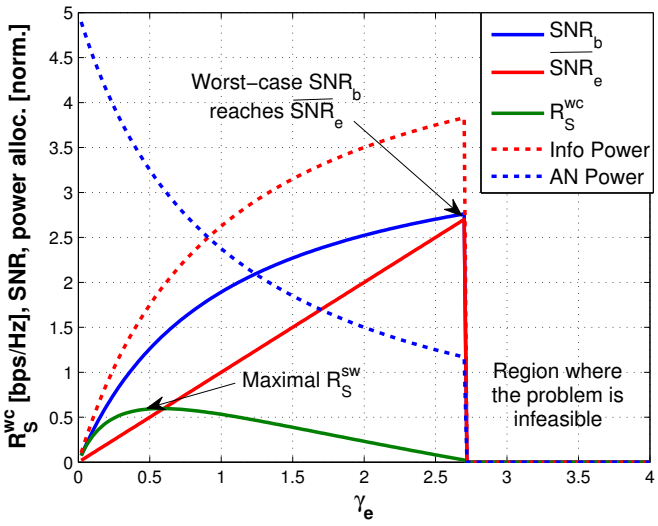


Figure 4.2: *Analysis of the concave nature of the worst-case secrecy rate R_S^{sw} as a function of γ_e.*

- Calculate $\mathrm{R}_S^{wc}(\gamma_e^i)$ by evaluating the SDPs (4.21) and (4.24) $\forall \gamma_e^i$
- Set $i_x = i$ corresponding to the maximum value among $\mathrm{R}_S^{wc}(\gamma_e^i)$
- $\gamma_e^{ini} = \begin{cases} \gamma_e^{ini}, i_x = 1 \\ \gamma_e^{i_x - 1}, i_x \neq 1 \end{cases}, \gamma_e^{end} = \begin{cases} \gamma_e^{i_x+1}, i_x \neq N+1 \\ \gamma_e^{end}, i_x = N+1 \end{cases}$

- Set $\gamma_e^\star = \frac{1}{2}\left(\gamma_e^{ini} + \gamma_e^{end}\right)$.

The transmission allocation that maximises the worst-case secrecy rate R_S^{wc} is the outcome of solving the SDP (4.21) for $\gamma_e^\star$.

Remark 3 *Owing to specific problem conditions such as the erroneous channel instantaneous realisation, power available, level of uncertainties, etc. and the value of γ_e, the results from the SDP in (4.21) might return $R_S^{wc} \leq 0$. If this remains the same for all $\gamma_e \in \left[\gamma_e^{ini}, \gamma_e^{end}\right]$, then there is not a feasible solution to guarantee $R_S^{wc} > 0$ and the system is considered to be in outage. For the sake of secrecy, transmission does not actually take place under this condition.*

4.3.4 Numerical results

In this section we address the performance analysis of the worst-case secrecy rate maximisation robust technique by numerical simulations. The analysis is based on

Table 4.1: *Parameters for the simulation.*

Parameter	Value	Description
N_t	4	Alice's number of antennas
$\sigma^2_{\tilde{h}_b}$	1	Bob's channel elements variance
$\sigma^2_{\tilde{h}_e}$	1	Eve's channel elements variance
σ^2_b	1	Bob's AWGN power
σ^2_e	1	Eve's AWGN power
P_{max}	5	Maximal power for constrained systems normalised relative to the AWGN power
α	2	Path loss exponent
$\hat{r}_b$	1	Alice-to-Bob erroneous distance normalised relative to r_b

the study of how the resources are allocated and the secrecy and the probabilistic performance of the robust security endeavour. The simulations are based on Monte Carlo trials with parameters detailed in Table 4.1.

Figure 4.3 depicts how the available power is allocated between the information and the AN as the uncertainty of the main channel increases. Under the high-uncertainty regime the strategy struggles to deliver a good quality communication over the main link. Therefore, it allocates less power to convey the information while giving more power to AN generation in order to enhance the worst-case secrecy rate R_S^{wc} by deteriorating the eavesdropping channel rather than trying to improve the highly inaccurate main Alice-to-Bob channel. Moreover, when a larger PZ is available and a larger security radius r_s can be deployed, the strategy allocates less power to AN generation making more power available to the information. This allocation criterion is due to the fact that distant eavesdroppers are subject to heavy path losses and so Alice does not need to devote so much power to AN generation. Thus she can smartly use the available power to allocate it mainly to information in order to enhance the secrecy rate. This behaviour is shown in Figure 4.4 where the security performance of our approximated security metric R_S^{wc} (estimated by Alice before transmission) is compared with the actual secrecy rate resulting from averaging randomly generated eavesdropping channels (R_S). For a fair comparison, both metrics take into account the worst-case

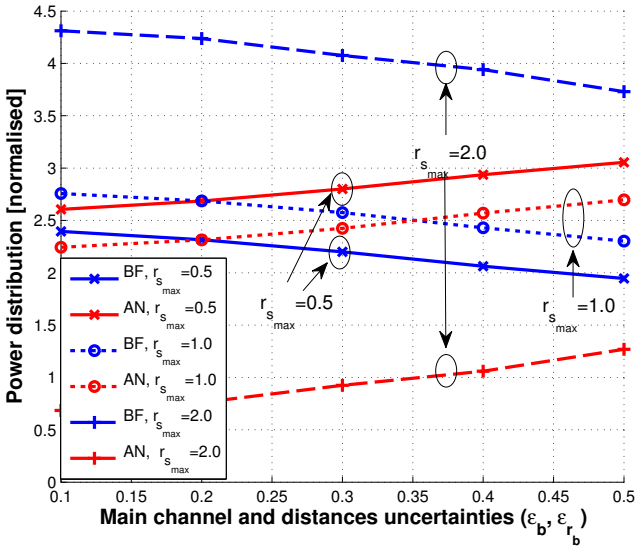


Figure 4.3: *Power distribution. Power allocated to information and AN (normalised relative to the AWGN power) versus main channel and distance uncertainties (ϵ_b, ϵ_{r_b}) for different size of PZ ($r_{s_{max}}$) (relative to r_b).*

main channel. As expected, R_S closely outperforms R_S^{wc}; therefore, the worst-case secrecy rate metric that we have introduced (R_S^{wc}) is effectively the lower-bound for the average secrecy rate. This result validates its use as a security performance and design metric for the current problem. In practical cases, we would expect the system to perform above R_S^{wc} because it is unlikely that the actual main channel corresponds to the worst-case channel considered for solving the problem.

On the other hand, Figures 4.4 and 4.5 show how a larger error on the main channel affects the secrecy rate and also show the probability of achieving a positive secrecy rate ($P_S = \mathbb{P}[R_S > 0]$). Here, as was done in the previous chapter in §3.3 and §3.4.1 and published in [103] and [102], the *normalised secrecy throughput* (T_S in the plots) is defined as a metric that quantifies the loss in throughput due to the infeasibility of solving the optimisation problem. Remarkably, in Figure 4.5, both P_S and T_S reach high values even in the high uncertainty regime, highlighting again the fact that close attackers represent the biggest threat to the security. Finally, to understand the secrecy improvement of our technique, in Figures 4.3 and 4.4 the performance of the '*naive*' scheme, that neglects the errors on both the main link CSI and Bob's location, is illustrated. Here a PZ is not deployed; there-

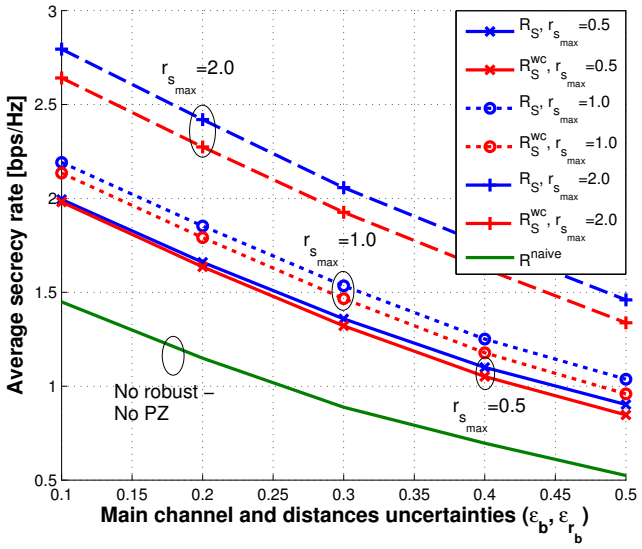


Figure 4.4: *Secrecy performance. Worst-case secrecy rate (R_S^{wc}) and achieved secrecy rate (R_S) versus main channel and distance uncertainties (ϵ_b, ϵ_{r_b}) for different size of PZ ($r_{s_{max}}$) (relative to r_b).*

fore, the eavesdroppers can be randomly located in the interval $(0, r_b]$. It is worth pointing out the security improvement achieved by the presented transmission technique in terms of both secrecy rate and probability of secrecy when compared to the naive scheme. This enhancement results from both the worst-case robust formulation and the PZ deployment.

4.4 Transmission resources minimisation problem

We look at a robust transmission strategy to minimise the networks' resources usage to enforce an average target worst-case secrecy rate under the presence of passive eavesdroppers when considering an erroneous main link's CSI. The strategy should be able to allocate the minimum amount of power devoted to information transmission and AN generation and the smallest size of the PZ by prioritising the use of one resource over the other. A robust optimisation problem is formulated when considering deterministic uncertainties over the main channel. This problem is recast as an SDP by using convex optimisation machinery to then solve it efficiently by interior-point based algorithms.

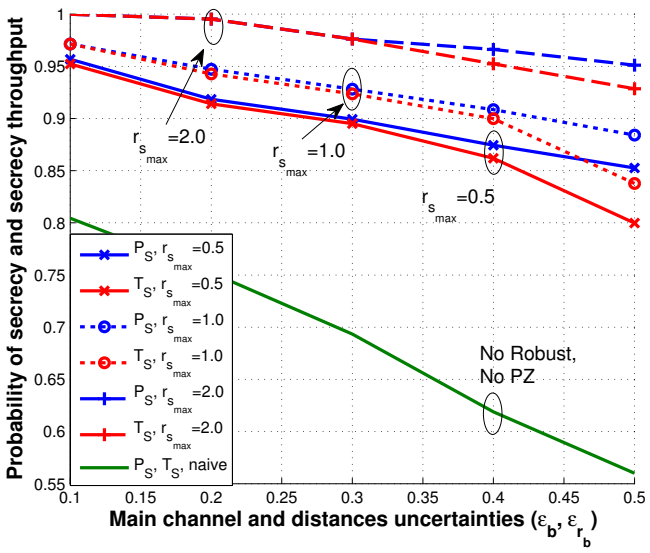


Figure 4.5: *Probabilistic analysis. Probability of secrecy (P_S) and secrecy throughput (T_S) versus main channel and distance uncertainties (ϵ_b, ϵ_{r_b}) for different size of PZ ($r_{s_{max}}$) (relative to r_b).*

4.4.1 Optimisation problem

We are interested in finding the optimal information and AN transmission covariance matrices ($\mathbf{C}_w$, $\mathbf{C}_\eta$) and the size of the PZ given by the secrecy radius r_s that ensure a worst-case secrecy rate $\mathrm{R}_S^{wc} \geq R$, where R is a target average secrecy rate. In order to efficiently allocate both available resources affecting the security performance (P and r_s), as in the §3.4 and in [102], we use a *Weighted Normalised Cost Function* (WNCF) that now it is defined as

$$\mathrm{CF} = \kappa_1 \frac{\mathrm{Tr}\{\mathbf{C}_w\} + \mathrm{Tr}\{\mathbf{C}_\eta\}}{P_{max}} + \kappa_2 \frac{r_s}{r_{s_{max}}} \tag{4.25}$$

where κ_1 and κ_2 are the weights to prioritise the use of one resource over the other and they are chosen to reflect whether it is more convenient to use additional power rather than extending the PZ or vice-versa. In (4.25), P_{max} and $r_{s_{max}}$ define the maximum available power and the largest PZ that could be physically deployed. The resources minimisation problem is

$$\min_{\mathbf{C}_w, \mathbf{C}_\eta, r_s} \quad \mathrm{CF} \tag{4.26a}$$

$$\text{s.t. } \mathrm{R}_S^{wc} \geq R \tag{4.26b}$$

$$\mathbf{C}_w \succeq \mathbf{0}, \mathbf{C}_\eta \succeq \mathbf{0} \tag{4.26c}$$

$$P \leq P_{max}, 0 \leq r_s \leq r_{s_{max}}. \tag{4.26d}$$

Note that while the objective function of the problem (4.26) defined in (4.25) is linear in all the optimising variables, the constraint (4.26b) is nonconvex. Therefore, we need to reformulate the problem in a mathematical tractable way. With this objective in mind, we introduce again the slack variable $\gamma_e > 0$ to split the worst-case secrecy rate (R_S^{wc} defined in (4.8)) in the constraint (4.26b) . The problem now becomes

$$\min_{\mathbf{C}_w, \mathbf{C}_\eta, r_s, \gamma_e} \kappa_1 \frac{\mathrm{Tr}\{\mathbf{C}_w\} + \mathrm{Tr}\{\mathbf{C}_\eta\}}{P_{max}} + \kappa_2 \frac{r_s}{r_{s_{max}}} \tag{4.27a}$$

$$\text{s.t.} \min_{\substack{\boldsymbol{\delta}_b \in \Delta_b, \\ \varsigma_b \in \xi_b}} \mathrm{SNR}_b \geq \gamma_b \tag{4.27b}$$

$$\overline{\mathrm{SNR}}_e \leq \gamma_e \tag{4.27c}$$

$$\mathbf{C}_w \succeq \mathbf{0}, \mathbf{C}_\eta \succeq \mathbf{0} \tag{4.27d}$$

$$P \leq P_{max}, 0 \leq r_s \leq r_{s_{max}}, \gamma_e > 0 \tag{4.27e}$$

where we define $\gamma_b = 2^R (1 + \gamma_e) - 1$. This problem offers us again a straight connection with QoS-constrained problems as the ones studied in [53, 59, 72, 103].

Although having split the former nonconvex constraint (4.26b) into the related QoS problem in (4.27), this is still nonconvex. Therefore, we use the same methodology as in §4.3.1 and, after fixing γ_e, we recast (4.27) into an equivalent convex SDP. We address this problem in the next section.

Problem reformulation into a semidefinite program

As pointed out before, the objective function in (4.27a) is linear in all the optimisation variables; therefore, we draw attention to the nonconvex contraint (4.27b). First, it is straightforward to see that the worst performance at Bob is obtained when the intended receiver is as distant as possible, and thus the SNR_b minimiser for ς_b is its maximum admissible value, ϵ_{r_b}. Then, the worst-case constraint in (4.27b) is reformulated as two quadratic inequalities as follows

$$-\left(\hat{\mathbf{h}}_b + \boldsymbol{\delta}_b\right)^H \left(\frac{\mathbf{C}_w}{\gamma_b} - \mathbf{C}_\eta\right) \left(\hat{\mathbf{h}}_b + \boldsymbol{\delta}_b\right) + \left(\hat{r}_b + \epsilon_{r_b}\right)^\alpha \sigma_b^2 \leq 0 \tag{4.28a}$$

$$\boldsymbol{\delta}_b^H \boldsymbol{\delta}_b - \epsilon_b^2 \leq 0. \tag{4.28b}$$

According to the *S-procedure* [87, Appendix B.2], these two quadratic inequalities hold iff there exists a slack variable $\mu \geq 0$ such that

$$\begin{bmatrix} \mu \mathbf{I}_{N_t} + \left(\frac{\mathbf{C}_w}{\gamma_b} - \mathbf{C}_\eta\right) & \left(\frac{\mathbf{C}_w}{\gamma_b} - \mathbf{C}_\eta\right)\hat{\mathbf{h}}_b \\ \hat{\mathbf{h}}_b^H\left(\frac{\mathbf{C}_w}{\gamma_b} - \mathbf{C}_\eta\right) & \hat{\mathbf{h}}_b^H\left(\frac{\mathbf{C}_w}{\gamma_b} - \mathbf{C}_\eta\right)\hat{\mathbf{h}}_b - \left(\hat{r}_b + \epsilon_{r_b}\right)^\alpha \sigma_b^2 - \mu\epsilon_b^2 \end{bmatrix} \succeq \mathbf{0}. \tag{4.29}$$

Here, the nonconvex contraint in (4.27b) is effectively formulated as an LMI.

Now, the constraint in (4.27c) is explicitly written as

$$\mathrm{Tr}\left\{\left[\frac{\mathbf{C}_w}{\gamma_e} - \mathbf{C}_\eta\right]\mathbf{R}_{\tilde{h}_e}\right\} - r_s^\alpha \sigma_e^2 \leq 0 \tag{4.30}$$

which is a nonconvex function because of the 'minus term' on the LHS involving the exponentiation of the optimising variable r_s. Therefore, by using the simple substitution $\tilde{r}_s = r_s^\alpha$, the constraint (4.30) becomes linear in all the optimisation variables. Subsequently, this substitution has to be considered in the former objective function (4.27a) and in the resources constraint (4.27e).

Finally, for a fixed value of $\gamma_e > 0$, the problem (4.27) is equivalent to the SDP

$$\min_{\substack{\mathbf{C}_w, \mathbf{C}_\eta, \\ \tilde{r}_s, \mu}} \ \kappa_1 \frac{\mathrm{Tr}\{\mathbf{C}_w\} + \mathrm{Tr}\{\mathbf{C}_\eta\}}{P_{max}} + \kappa_2 \frac{\tilde{r}_s}{r_{s_{max}}^\alpha} \tag{4.31a}$$

$$\text{s.t. } \mathrm{Tr}\left\{\left[\frac{\mathbf{C}_w}{\gamma_e} - \mathbf{C}_\eta\right]\mathbf{R}_{\tilde{h}_e}\right\} - \tilde{r}_s\sigma_e^2 \leq 0 \tag{4.31b}$$

$$\begin{bmatrix} \mu \mathbf{I}_{N_t} + \left(\frac{\mathbf{C}_w}{\gamma_b} - \mathbf{C}_\eta\right) & \left(\frac{\mathbf{C}_w}{\gamma_b} - \mathbf{C}_\eta\right)\hat{\mathbf{h}}_b \\ \hat{\mathbf{h}}_b^H\left(\frac{\mathbf{C}_w}{\gamma_b} - \mathbf{C}_\eta\right) & \hat{\mathbf{h}}_b^H\left(\frac{\mathbf{C}_w}{\gamma_b} - \mathbf{C}_\eta\right)\hat{\mathbf{h}}_b - \left(\hat{r}_b + \epsilon_{r_b}\right)^\alpha \sigma_b^2 - \mu\epsilon_b^2 \end{bmatrix} \succeq \mathbf{0} \tag{4.31c}$$

$$\mathrm{Tr}\left\{\mathbf{C}_w\right\} + \mathrm{Tr}\left\{\mathbf{C}_\eta\right\} \leq P_{max}, 0 \leq \tilde{r}_s \leq r_{s_{max}}^\alpha \tag{4.31d}$$

$$\mathbf{C}_w \succeq \mathbf{0}, \mathbf{C}_\eta \succeq \mathbf{0}, \mu \geq 0 \tag{4.31e}$$

where the secrecy radius parameter is given by $r_s = \tilde{r}_s^{\frac{1}{\alpha}}$ and μ is a slack variable.

The SDP (4.31) can be solved efficiently by interior-point algorithms by using the on-the-shelf solver SeDuMi [105] assisted by the parser tools Yalmip [106] or CVX [107].

Remark 4 *Due to the instantaneous availability of the erroneous main link's CSI* $\hat{\mathbf{h}}_b$*, the optimal solution for the information transmission covariance matrix* $\mathbf{C}_w^\star$ *of*

the SDP (4.31) is unique and rank-one. Moreover, due to the lack of the instantaneous availability of the eavesdropping channel $\hat{\mathbf{h}}_e$*, the strategy broadcasts the AN orthogonal to* $\mathbf{C}_w^\star$*.*

The first part of the claim in this remark above results from the analysis of the optimality conditions of the SDP (4.31). This study is addressed in detail in the §4.5 of this chapter. The second part of remark 4 results from the analysis of the simulation results where the power for AN generation is isotropically distributed over the $(N_t - 1)$ dimensional space orthogonal to the rank-one space spanned by $\mathbf{C}_w^\star$. This is equivalent to saying that the AN covariance matrix $\mathbf{C}_\eta^\star$ has $(N_t - 1)$ equal non-zero eigenvalues with the same magnitude.

4.4.2 Linear searching algorithm to minimise the transmission resources use

We recall that the SPD (4.31) has been solved for a fixed value of γ_e; therefore, it is necessary to find the optimal $\gamma_e^\star$ that delivers the minimal cost for the CF among all the costs resulting by considering all the admissible values for γ_e. This can efficiently be done by implementing an iterative algorithm that exploits the convex way in which the CF varies as a function of γ_e.

Analysis of the convex nature of CF

The weighted normalised cost function CF is evaluated after solving the SDP (4.31); therefore, it is useful to first understand how does the SDP allocate the network resources. First, in order to save power, the strategy sets the worst-case SNR_b and the $\overline{\text{SNR}}_e$ to their respective minimum and maximum admissible values (γ_b and γ_e) to guarantee R. The later can also be achieved by setting an appropriate PZ size defined by r_s; here, the strategy's outcome depends on the resources availability and prioritisation criteria. As explained in §4.3.3, the power devoted to the information covariance matrix $\mathbf{C}_w$ increases monotonically with γ_e. Regarding $\mathbf{C}_\eta$ and r_s, when $\gamma_e \gtrapprox 0$ we note that high power devoted to the AN generation and a large PZ are required simultaneously; indeed, the problem might be unfeasible under this condition. As γ_e increases, less power is devoted for $\mathbf{C}_\eta$ and a shorter r_s are admissible. On the other hand, the strategy makes more power available

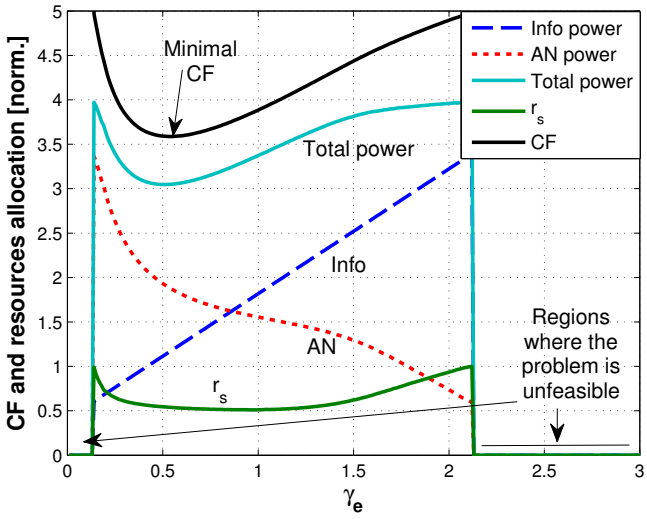


Figure 4.6: *Analysis of the convex nature of the weighted normalised cost function CF as a function of* γ_e *for* $\kappa_1 = \kappa_2 = 1$.

for the information $\mathbf{C}_w$ by increasing r_s rather than allocating power for broadcasting AN. Thus, after decreasing and reaching a saddle point, r_s increases again while the AN's power monotonically decreases. Finally, the CF is the normalised weighted summation of the increasing power for information as a function of γ_e, the decreasing power devoted for AN generation and the convex function in γ_e of the secrecy radius r_s. This results in a convex function depicted in Figure 4.6; where, the convex nature of CF as a function of γ_e is shown for one particular channel realisation $\hat{\mathbf{h}}_b = [0.23 + 0.66i, -0.92 + 0.17i, -0.31 - 0.49i, 0.24 - 0.46i]^T$. The maximum power is set to $P_{max} = 5$ and normalised relative to the AWGN power, the secrecy radius to $r_{s_{max}} = 0.5$ relative to r_b while the upper-bounds of the uncertainties are fixed to $\epsilon_b = 0.3$ and $\epsilon_{r_b} = 0.3$.

Now, we take advantage of the convex nature of the weighted cost function CF as a function of γ_e to develop a linear searching algorithm to seek the optimal $\gamma_e^\star$.

Algorithm 2

- Initialise γ_e^{ini} to a value larger but approximately equal to 0; i.e., $\gamma_e^{ini} \gtrapprox 0$ and $\gamma_e^{end} = \frac{P_{max}||\hat{\mathbf{h}}_b||^2}{\hat{r}_b^\alpha \sigma_b^2}$.

- Define ρ as the accuracy tolerance for the optimal $\gamma_e^\star$ and N intervals.

- Repeat while $\gamma_e^{end} - \gamma_e^{ini} > \rho$
  - $\gamma_e^i = \gamma_e^{ini} + \frac{(i-1)}{N}\left(\gamma_e^{end} - \gamma_e^{ini}\right), i \in [1, N+1]$
  - Calculate CF (γ_e^i) by solving (4.31) and then evaluating (4.25) $\forall \gamma_e^i$
  - Set $i_x = i$ corresponding to the minimum value among CF (γ_e^i).
  - $\gamma_e^{ini} = \begin{cases} \gamma_e^{ini}, i_x = 1 \\ \gamma_e^{i_x - 1}, i_x \neq 1 \end{cases}, \gamma_e^{end} = \begin{cases} \gamma_e^{i_x+1}, i_x \neq N+1 \\ \gamma_e^{end}, i_x = N+1 \end{cases}$
- Set $\gamma_e^\star = \frac{1}{2}\left(\gamma_e^{ini} + \gamma_e^{end}\right)$.

The transmission strategy that minimises the cost function CF is the outcome of solving the SDP (4.31) for $\gamma_e^\star$.

Remark 5 *In the case that the SDP in (4.31) is non-feasible for all* $\gamma_e \in \left[\gamma_e^{ini}, \gamma_e^{end}\right]$, *then the system is considered in outage and no transmission takes place to preserve the system security.*

4.4.3 Numerical results

For the analysis of the performance of the robust resources minimisation problem we consider Monte Carlo simulations with setup specified in Table 4.2. We draw attention to the way that the technique allocates resources for different prioritisation criteria and the secrecy probabilistic analysis of our robust strategy.

The Figures 4.7 and 4.8 depict the technique's requirements in terms of power and size of the PZ to achieve the average target secrecy rate R. Here we can see that as the uncertainty over the main channel increases, the system uses more resources to satisfy the security objective until they are depleted. Indeed, the required amount of total power and the size of the PZ defined by r_s are determined by the prioritisation weights κ_1 and κ_2 in (4.25). For instance, in Figure 4.7 the use of power is prioritised over extending the PZ. Meanwhile in Figure 4.8 the top priority is to save power and so the technique extends the size of the PZ. The introduced robust technique calculates the secrecy radius showing that both, an appropriate resources prioritisation criterion and the use of a PZ allow an efficient energy utilisation to provide an average secrecy rate target.

Figures 4.9 and 4.10 illustrate the secrecy probabilistic performance of the resources minimisation robust transmit strategy. Both figures show the probability

Table 4.2: *Parameters for the simulation.*

Parameter	Value	Description
N_t	4	Alice's number of antennas
$\sigma^2_{\tilde{h}_b}$	1	Bob's channel elements variance
$\sigma^2_{\tilde{h}_e}$	1	Eve's channel elements variance
σ^2_b	1	Bob's AWGN power
σ^2_e	1	Eve's AWGN power
P_{max}	3	Maximal power for constrained systems normalised relative to AWGN power
R	1 bps/Hz	Target average secrecy rate
α	2	Path loss exponent
$\hat{r}_b$	1	Alice-to-Bob erroneous distance relative to r_b

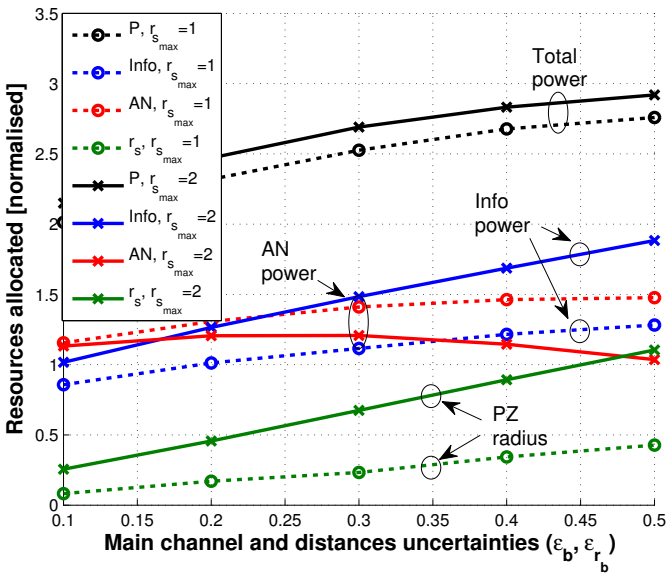


Figure 4.7: *Resources allocation. Transmit power for information, AN (normalised relative to AWGN power) and size of secrecy radius (r_s) versus main channel and distance uncertainties (ϵ_b, ϵ_{r_b}) for different size of PZ ($r_{s_{max}}$) (relative to r_b) and $\kappa_1 = 1, \kappa_2 = 3$.*

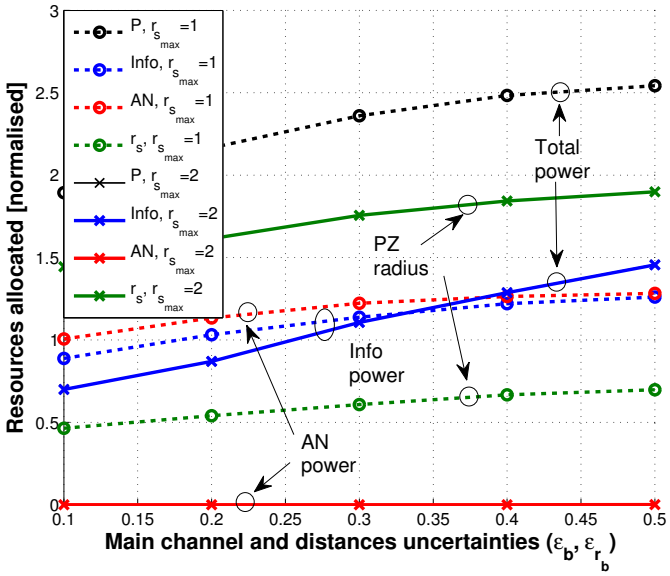


Figure 4.8: *Resources allocation. Transmit power for information, AN (normalised relative to AWGN power) and size of secrecy radius (r_s) versus main channel and distance uncertainties (ϵ_b, ϵ_{r_b}) for different size of PZ ($r_{s_{max}}$) (relative to r_b) and $\kappa_1 = 3, \kappa_2 = 1$.*

of achieving an average worst-case secrecy rate larger than the target secrecy rate R; i.e., $P_S = \mathbb{P}\left[\mathrm{R}_S^{wc} > R\right]$. Moreover, the *normalised secrecy throughput* T_S, as defined in §4.3.4, is also plotted to quantify the loss in throughput due to the infeasibility of solving the optimisation problem. Owing to the ergodic definition of secrecy considered in the metric R_S^{wc} in (4.8), in both figures the security constraint in (4.26b) is guaranteed on average. Therefore, the presented transmission mechanism can minimise the use of resources but at the cost of not providing a high probability of secrecy. These results suggest the need of an outage formulation to provide a high secrecy rate when the objective is to minimise the use of resources. This outage approach, as pointed out in §3.4.1 of chapter 2, has proven effective for the case of a MISO transmission with a perfect main link's CSI.

Figures 4.9 and 4.10 show that the probability of achieving a secrecy rate larger than R by this technique is not affected by the availability of resources. However, a larger PZ can have an important impact over the secrecy throughput, especially under the high main channel uncertainty regime.

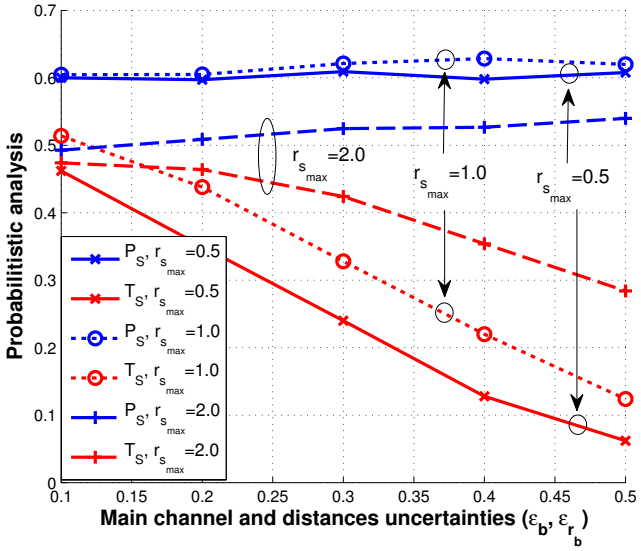


Figure 4.9: *Probabilistic analysis. Probability of secrecy (P_S) and secrecy throughput (T_S) versus main channel and distance uncertainties (ϵ_b, ϵ_{r_b}) for different size of PZ ($r_{s_{max}}$) (relative to r_b) and $\kappa_1 = 1, \kappa_2 = 3$.*

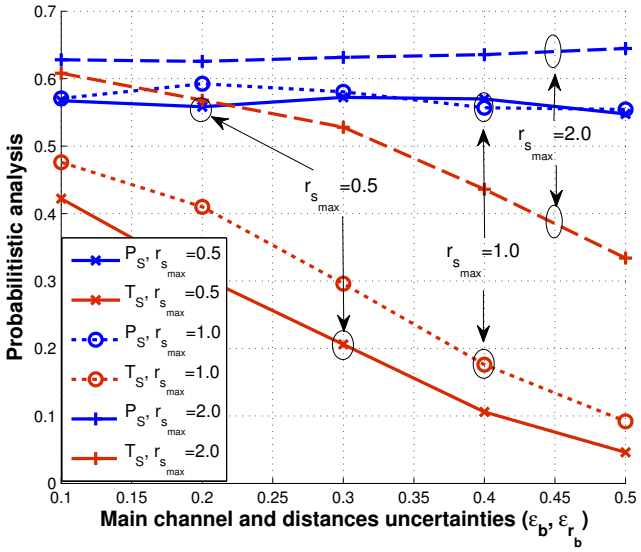


Figure 4.10: *Probabilistic analysis. Probability of secrecy (P_S) and secrecy throughput (T_S) versus main channel and distance uncertainties (ϵ_b, ϵ_{r_b}) for different size of PZ ($r_{s_{max}}$) (relative to r_b) and $\kappa_1 = 3, \kappa_2 = 1$.*

4.5 Analysis of the information transmission covariance matrix

In order to obtain valuable insight into the nature of the optimal solutions of the worst-case secrecy rate and the resources minimisation problems studied in §4.3 and §4.4, we analyse the internal structure of the SDPs (4.21) and (4.31). Indeed, we examine the *Karush-Kuhn-Tucker* (KKT) optimality conditions [87, §5.5.3] of both problems aiming to shed light into the internal structure of their optimal transmission information covariance matrix $\mathbf{C}_w^\star$.

For the sake of clarity, this analysis is split into two parts. First, we consider a transmission resources minimisation problem related to the secrecy rate maximisation problem. We prove that the optimal solution of this related problem is also optimal to the secrecy rate maximisation problem studied in §4.3.1. Therefore, we effectively establish a connection between the resources minimisation problem addressed in §4.4.1 and the secrecy rate maximisation problem analysed in §4.3.1 and their solutions. Second, we focus on the study of the KKT conditions of the resources minimisation problem in order to understand the properties of the optimal transmission information covariance matrix $\mathbf{C}_w^\star$. This analysis will show that the $\mathbf{C}_w^\star$ for both problems is unique and rank-one, which means that the optimal transmission scheme for our robust scheme is beamforming.

Connection between the secrecy rate maximisation and the resources minimisation problems

Let us drawn our attention to the transmission resources minimisation problem in (4.26) for the particular case of $\kappa_1 = \kappa_2 = 1$. This condition yields

$$\min_{\mathbf{C}_w, \mathbf{C}_\eta, r_s} \quad \frac{\mathrm{Tr}\{\mathbf{C}_w\} + \mathrm{Tr}\{\mathbf{C}_\eta\}}{P_{max}} + \frac{r_s}{r_{s_{max}}} \tag{4.32a}$$

$$\text{s.t. } \mathrm{R}_S^{wc} \geq R^\star \tag{4.32b}$$

$$\mathbf{C}_w \succeq \mathbf{0}, \mathbf{C}_\eta \succeq \mathbf{0} \tag{4.32c}$$

$$P \leq P_{max}, 0 \leq r_s \leq r_{s_{max}} \tag{4.32d}$$

where, $R^\star$ is the optimal worst-case secrecy rate that can be obtained by the secrecy rate maximisation problem (4.11) under the same power and secrecy radius constraints P_{max} and $r_{s_{max}}$.

Consider $(\mathbf{C}_w^{rm},\ \mathbf{C}_\eta^{rm}, r_s^{rm})$ to be the solution to the transmission resources minimisation problem in (4.32). Likewise, $(\mathbf{C}_w^{SM},\ \mathbf{C}_\eta^{SM}, r_s^{SM})$ is the solution of the secrecy rate maximisation problem (4.11). Bear in mind that we assume that both problems are constrained by the same resources availability; that is, $P \leq P_{max}, 0 \leq r_s \leq r_{s_{max}}$. Therefore, the solution to the SDP (4.21) resulting from reformulating (4.11) can satisfy the constraints of (4.32). Moreover, from the resource minimisation problem it holds

$$\begin{aligned}\frac{\mathrm{Tr}\{\mathbf{C}_w^{rm}\}+\mathrm{Tr}\{\mathbf{C}_\eta^{rm}\}}{P_{max}}+\frac{r_s^{rm}}{r_{s_{max}}} &\leq \frac{\mathrm{Tr}\{\mathbf{C}_w^{SM}\}+\mathrm{Tr}\{\mathbf{C}_\eta^{SM}\}}{P_{max}}+\frac{r_s^{SM}}{r_{s_{max}}}\\ &\leq \frac{P_{max}}{P_{max}}+\frac{r_{s_{max}}}{r_{s_{max}}}=2,\end{aligned} \tag{4.33}$$

which further implies that $(\mathbf{C}_w^{rm},\ \mathbf{C}_\eta^{rm}, r_s^{rm})$ is feasible to the secrecy rate maximisation problem in (4.11); that is, from $(\mathbf{C}_w^{rm},\ \mathbf{C}_\eta^{rm}, r_s^{rm})$, $\mathrm{R}_s^{wc} \leq R^\star$ holds. On the other hand, as an optimal solution of (4.32), then $(\mathbf{C}_w^{rm},\ \mathbf{C}_\eta^{rm}, r_s^{rm})$ must satisfy (4.32b), and so $\mathrm{R}_s^{wc} \geq R^\star$ holds. Therefore, $\mathrm{R}_s^{wc} = R^\star$ and that subsequently means that $(\mathbf{C}_w^{rm}, \mathbf{C}_\eta^{rm}, r_s^{rm})$ is optimal to both the resources minimisation problem (4.32) and the secrecy rate maximisation problem (4.11).

Once we have established this important connection between the transmission resources minimisation problem (4.26) and the worst-case secrecy rate maximisation problem (4.11) and their respective optimal solutions, in the following, and for the sake of simplicity, we study the KKT conditions of the resources minimisation problem.

Analysis of the KKT optimality conditions of the resources minimisation problem

Let us consider the SDP (4.31) that results from recasting the transmission resources minimisation problem in (4.26). First, and with the objective to ease the analysis, it is useful to split the LMI in the constraint (4.31c) into three constraints. Hence we use the $\mathcal{S}$-*procedure* [87, Appendix B.2] to transform the former worst-case QoS at the Bob constraint in (4.27b) into

$$u - v - \left(\hat{r}_b + \epsilon_{r_b}\right)^\alpha \sigma_b^2 \geq 0 \tag{4.34a}$$

$$\text{s.t.} \quad \begin{bmatrix} \mu_1 \mathbf{I}_{N_t} + \frac{\mathbf{C}_w}{\gamma_b} & \frac{\mathbf{C}_w}{\gamma_b}\hat{\mathbf{h}}_b \\ \hat{\mathbf{h}}_b^H \frac{\mathbf{C}_w}{\gamma_b} & \hat{\mathbf{h}}_b^H \frac{\mathbf{C}_w}{\gamma_b}\hat{\mathbf{h}}_b - \mu_1\epsilon_b^2 - u \end{bmatrix} \succeq \mathbf{0} \tag{4.34b}$$

$$\begin{bmatrix} \mu_2\mathbf{I}_{N_t} - \mathbf{C}_\eta & -\mathbf{C}_\eta\hat{\mathbf{h}}_b \\ -\hat{\mathbf{h}}_b^H\mathbf{C}_\eta & -\hat{\mathbf{h}}_b^H\mathbf{C}_\eta\hat{\mathbf{h}}_b - \mu_2\epsilon_b^2 + v \end{bmatrix} \succeq \mathbf{0} \tag{4.34c}$$

where $u \geq 0, v \geq 0$ and $\mu_i \geq 0, i = 1, 2$ are slack variables introduced by applying the $\mathcal{S}$-*procedure*.

The LMI in (4.31c) results from adding the LMIs (4.34b) and (4.34c) and replacing the value for $(u - v)$ from (4.34a) and $\mu = \mu_1 + \mu_2$ into the LMI resulting from the addition of the LMIs (4.34b) and (4.34c). After considering (4.34), the resulting SDP is

$$\min_{\substack{\mathbf{C}_w, \mathbf{C}_\eta, \\ \tilde{r}_s, \mu}} \quad \kappa_1 \frac{\mathrm{Tr}\{\mathbf{C}_w\} + \mathrm{Tr}\{\mathbf{C}_\eta\}}{P_{max}} + \kappa_2 \frac{\tilde{r}_s}{r_{s_{max}}^\alpha} \tag{4.35a}$$

$$\text{s.t. } \mathrm{Tr}\left\{\left[\frac{\mathbf{C}_w}{\gamma_e} - \mathbf{C}_\eta\right]\mathbf{R}_{\tilde{h}_e}\right\} - \tilde{r}_s\sigma_e^2 \leq 0 \tag{4.35b}$$

$$u - v - (\hat{r}_b + \epsilon_{r_b})^\alpha \sigma_b^2 \geq 0 \tag{4.35c}$$

$$\begin{bmatrix} \mu_1\mathbf{I}_{N_t} + \frac{\mathbf{C}_w}{\gamma_b} & \frac{\mathbf{C}_w}{\gamma_b}\hat{\mathbf{h}}_b \\ \hat{\mathbf{h}}_b^H\frac{\mathbf{C}_w}{\gamma_b} & \hat{\mathbf{h}}_b^H\frac{\mathbf{C}_w}{\gamma_b}\hat{\mathbf{h}}_b - \mu_1\epsilon_b^2 - u \end{bmatrix} \succeq \mathbf{0} \tag{4.35d}$$

$$\begin{bmatrix} \mu_2\mathbf{I}_{N_t} - \mathbf{C}_\eta & -\mathbf{C}_\eta\hat{\mathbf{h}}_b \\ -\hat{\mathbf{h}}_b^H\mathbf{C}_\eta & -\hat{\mathbf{h}}_b^H\mathbf{C}_\eta\hat{\mathbf{h}}_b - \mu_2\epsilon_b^2 + v \end{bmatrix} \succeq \mathbf{0} \tag{4.35e}$$

$$\mathrm{Tr}\{\mathbf{C}_w\} + \mathrm{Tr}\{\mathbf{C}_\eta\} \leq P_{max}, 0 \leq \tilde{r}_s \leq r_{s_{max}}^\alpha \tag{4.35f}$$

$$\mathbf{C}_w \succeq \mathbf{0}, \mathbf{C}_\eta \succeq \mathbf{0}, \mu \geq 0 \tag{4.35g}$$

where it is clear to see that the above SDP is equivalent to (4.31) but now considering the three constraints in (4.34) instead of the LMI in (4.31c). Now, we examine the KKT optimality conditions defined in [87, §5.5.3] for the equivalent SDP (4.35).

First, the LMI in (4.35d) can be expressed as

$$\begin{aligned} \mathbf{A} &= \begin{bmatrix} \mu_1\mathbf{I}_{N_t} & \mathbf{0} \\ \mathbf{0}^H & -\mu_1\epsilon_b^2 - u \end{bmatrix} + \begin{bmatrix} \frac{\mathbf{C}_w}{\gamma_b} & \frac{\mathbf{C}_w}{\gamma_b}\hat{\mathbf{h}}_b \\ \hat{\mathbf{h}}_b^H\frac{\mathbf{C}_w}{\gamma_b} & \hat{\mathbf{h}}_b^H\frac{\mathbf{C}_w}{\gamma_b}\hat{\mathbf{h}}_b \end{bmatrix} \\ &= \begin{bmatrix} \mu_1\mathbf{I}_{N_t} & \mathbf{0} \\ \mathbf{0}^H & -\mu_1\epsilon_b^2 - u \end{bmatrix} + \hat{\mathbf{H}}_b^H\frac{\mathbf{C}_w}{\gamma_b}\hat{\mathbf{H}}_b \succeq \mathbf{0} \end{aligned} \tag{4.36}$$

where $\hat{\mathbf{H}}_b = \left[\mathbf{I}_{N_t}\ \hat{\mathbf{h}}_b\right]$.

Now we write part of the KKT optimality conditions of the SDP (4.35) but consider (4.36) instead of (4.35d) as

$$\nabla_{\mathbf{C}_w}\mathcal{L} = \frac{\kappa_1}{P_{max}}\mathbf{I}_{N_t} + \frac{\rho_1}{\gamma_e}\mathbf{R}_{\tilde{h}_e} - \frac{1}{\gamma_b}\hat{\mathbf{H}}_b\boldsymbol{\Sigma}_1\hat{\mathbf{H}}_b^H - \boldsymbol{\Sigma}_2 + \rho_2\mathbf{I}_{N_t} = \mathbf{0}_{N_t} \tag{4.37a}$$

$$\mathbf{A}\boldsymbol{\Sigma}_1 = \mathbf{0}_{N_t} \tag{4.37b}$$

$$\mathbf{C}_w\boldsymbol{\Sigma}_2 = \mathbf{0}_{N_t} \tag{4.37c}$$

$$\mathbf{C}_w \succeq \mathbf{0}, \boldsymbol{\Sigma}_1 \succeq \mathbf{0}, \boldsymbol{\Sigma}_2 \succeq \mathbf{0}, \rho_1 \geq 0, \rho_2 \geq 0 \tag{4.37d}$$

where $\boldsymbol{\Sigma}_1, \boldsymbol{\Sigma}_2, \rho_1$ and ρ_2 are the Lagrange dual variables associated with the matrices $\mathbf{A}, \mathbf{C}_w$, the constraint in (4.35b) and the power constraint in (4.35f) respectively. Now, by pre-multiplying the KKT condition in (4.37a) by the information covariance matrix $\mathbf{C}_w$ and considering the condition in (4.37c) we obtain

$$\mathbf{C}_w \left[\left(\frac{\kappa_1}{P_{max}} + \rho_2 \right) \mathbf{I}_{N_t} + \frac{\rho_1}{\gamma_e} \mathbf{R}_{\tilde{h}_e} \right] = \frac{1}{\gamma_b} \mathbf{C}_w \hat{\mathbf{H}}_b \boldsymbol{\Sigma}_1 \hat{\mathbf{H}}_b^H. \tag{4.38}$$

Recalling that $\mathbf{R}_{\tilde{h}_e} = \sigma_{\tilde{h}_e}^2 \mathbf{I}_{N_t}$, the resulting matrix inside of the brackets of the LHS of (4.38) is a full-rank positive definite matrix irrespective of the values of the Lagrange dual variables ρ_1 and ρ_2. Thus

$$\text{rank}(\mathbf{C}_w) = \text{rank}(\mathbf{C}_w \hat{\mathbf{H}}_b \boldsymbol{\Sigma}_1 \hat{\mathbf{H}}_b^H) \leq \min \left[\text{rank}(\mathbf{C}_w), \text{rank}(\hat{\mathbf{H}}_b \boldsymbol{\Sigma}_1 \hat{\mathbf{H}}_b^H) \right]. \tag{4.39}$$

Now, we focus our attention to the rank of the matrix $\hat{\mathbf{H}}_b \boldsymbol{\Sigma}_1 \hat{\mathbf{H}}_b^H$. First, we incorporate the reformulation of the LMI (4.35d) in (4.36) into the KKT condition (4.37b). Subsequently, we pre-multiply it by $[\mathbf{I}_{N_t}\ \mathbf{0}]$ and post-multiply it by $\hat{\mathbf{H}}_b^H$ to obtain

$$\begin{aligned}[\mathbf{I}_{N_t}\ \mathbf{0}] \begin{bmatrix} \mu_1 \mathbf{I}_{N_t} & \mathbf{0} \\ \mathbf{0}^H & -\mu_1 \epsilon_b^2 - u \end{bmatrix} \boldsymbol{\Sigma}_1 \hat{\mathbf{H}}_b^H + [\mathbf{I}_{N_t}\ \mathbf{0}] \hat{\mathbf{H}}_b^H \frac{\mathbf{C}_w}{\gamma_b} \hat{\mathbf{H}}_b \boldsymbol{\Sigma}_1 \hat{\mathbf{H}}_b^H \\ = [\mu_1 \mathbf{I}_{N_t}\ \mathbf{0}] \boldsymbol{\Sigma}_1 \hat{\mathbf{H}}_b^H + \frac{\mathbf{C}_w}{\gamma_b} \hat{\mathbf{H}}_b \boldsymbol{\Sigma}_1 \hat{\mathbf{H}}_b^H = \mathbf{0}_{N_t}.\end{aligned} \tag{4.40}$$

Recalling that $\hat{\mathbf{H}}_b = \left[\mathbf{I}_{N_t}\ \hat{\mathbf{h}}_b \right]$, we rewrite $[\mu_1 \mathbf{I}_{N_t}\ \mathbf{0}]$ as $\mu_1 \left[\hat{\mathbf{H}}_b - \left[\mathbf{0}_{N_t}\ \hat{\mathbf{h}}_b \right] \right]$. Finally, (4.40) is expressed as

$$\left[\mu_1 \mathbf{I}_{N_t} + \frac{\mathbf{C}_w}{\gamma_b} \right] \hat{\mathbf{H}}_b \boldsymbol{\Sigma}_1 \hat{\mathbf{H}}_b^H = \mu_1 \left[\mathbf{0}_{N_t}\ \hat{\mathbf{h}}_b \right] \boldsymbol{\Sigma}_1 \hat{\mathbf{H}}_b^H. \tag{4.41}$$

Now, from the expression (4.40), $\mu_1 > 0$; otherwise, $\mathbf{C}_w \hat{\mathbf{H}}_b \boldsymbol{\Sigma}_1 \hat{\mathbf{H}}_b^H = \mathbf{0}_{N_t}$ only holds when the information covariance matrix $\mathbf{C}_w = \mathbf{0}$ and that is not feasible for the general case of the target average secrecy rate $R > 0$. Therefore, the resulting matrix within the brackets on the LHS of (4.41) is full-rank positive definite. Hence, it holds that

$$\text{rank}(\hat{\mathbf{H}}_b \boldsymbol{\Sigma}_1 \hat{\mathbf{H}}_b^H) = \text{rank}(\mu_1 \left[\mathbf{0}_{N_t}\ \hat{\mathbf{h}}_b \right] \boldsymbol{\Sigma}_1 \hat{\mathbf{H}}_b^H) \leq \text{rank}\left(\left[\mathbf{0}_{N_t}\ \hat{\mathbf{h}}_b \right] \right) \leq 1. \tag{4.42}$$

Finally, from (4.39) we conclude that rank $(\mathbf{C}_w) \leq$ rank $\left(\hat{\mathbf{H}}_b \mathbf{\Sigma}_1 \hat{\mathbf{H}}_b^H\right) \leq 1$. In other words, when the resources minimisation problem is feasible and for the non trivial case when the average target secrecy rate $R = 0$, then the covariance matrix of the information is rank-one; that corresponds to a beamforming transmission strategy.

An additional conclusion arises from the rank-one property of the optimal information transmission covariance matrix. The optimal $\mathbf{C}_w$ for a given resource minimisation problem is unique. This result can be seen by contradiction through exploiting the rank-one property of $\mathbf{C}_w$ by considering two different rank-one optimal solutions, $\mathbf{C}_{w_1}$ and $\mathbf{C}_{w_2}$. By the convexity optimisation property [87, §4], it holds that $\mathbf{C}_{w_3} = \theta \mathbf{C}_{w_1} + (1 - \theta)\mathbf{C}_{w_2}$ is also optimal to the SDP (4.35) where $0 \leq \theta \leq 1$. As $\mathbf{C}_{w_1} \neq \mathbf{C}_{w_2}$, they span two different subspaces, and so the operation above yields rank$(\mathbf{C}_{w_3}) = 2$. Therefore, $\mathbf{C}_{w_3}$ cannot be optimal to (4.35) unless $\mathbf{C}_{w_1} = \mathbf{C}_{w_2}$, confirming the uniqueness property of the optimal information transmission covariance matrix $\mathbf{C}_w$.

It is worth recalling the equivalence of the optimal solutions of the resources minimisation problem (4.26) and the worst-case secrecy rate maximisation problem in (4.11) studied in the §4.5. Therefore, we conclude that the solution of the worst-case secrecy rate maximisation problem is also unique and rank-one. In other words, the optimal transmission strategy for both problems that we have studied is beamforming. This property, as seen in the analysis above, results from the availability of the instantaneous erroneous main link's CSI and coincides with the results reported in [46, 67] for different configurations of MISO networks. The results discussed in this section allow us to confirm the statements contained in remarks 1 and 3.

4.6 Discussion and summary

In this chapter we have investigated a new, secure, robust transmit strategy to cope with errors in the main link of a MISO network under the presence of an unknown eavesdropper. The main channel mismatch has been modelled using a conservative approach that ensures a given performance for all the (known norm) deterministic uncertainties defined within a set. Therefore, we have formulated two optimisation problems to maximise the worst-case secrecy rate in a resources constrained

network and to minimise the use of resources subject to ensuring a target average worst-case secrecy rate. We have recast the resulting nonconvex problems into semidefinite programs that have been efficiently solved by interior-point based toolboxes. Subsequently, we have studied the structure of both problems and obtained valuable insight into the nature of the optimal solutions. Indeed, the two problems' optimal transmit information covariance matrices are unique and rank-one meaning that transmit beamforming is optimal to both problems. Moreover, the artificial noise covariance matrix is orthogonal to the one-dimensional space spanned by the transmit covariance matrix; that is, the artificial noise is generated over the nullspace of the information steering beamformer in an isotropic fashion. This result corroborates isotropic masked beamforming designs as valid approaches to convey securely information in MISO networks in the presence of passive eavesdroppers; even under uncertainties over the main channel.

The introduced robust techniques also use a protected zone to prevent spatially close eavesdroppers. Thus, our transmission approaches determines both the optimal size of this secure area and the transmission covariance matrices for both optimisation problems. The proposed approach improves the security by striking a balance between allocating transmission power and setting the size of the protected zone in resource constrained scenarios. These strategies shed light into the impact that a close unknown attacker can have over the security and the associated cost in power required to prevent close-quarters eavesdropping attacks.

In conclusion, in this chapter we have addressed a practical security problem arising from using an erroneous channel information of the main link to steer the information towards the intended receiver and to generate a jamming signal to confuse attackers. This characteristic affects practical networks and, if neglected, can jeopardise the security in MISO networks. The efficient transmission strategies here introduced incorporate into the design a degree of uncertainty about the main channel to address the worst-case security. Moreover, we consider an eavesdropper close to the transmitter; therefore, we take advantage of physical deployments in practical networks to enforce an exclusion area that allows us not only to enhance the security by preventing close attacks but also to make an efficient use of the available network resources.

Chapter 5

Physical layer security in MIMO-OFDM systems

> 'The silence always dawned with you, or perhaps I must say between us. Save the secret with me, in case you heard my voice'
>
> Alejandro Filio

This chapter presents an analysis of the contribution of frequency selectiveness to the secrecy of multiple-antenna systems when all the transmission parties use orthogonal frequency division multiplexing (OFDM) signalling. We address physical layer security in frequency selective multiple-input multiple-output (MIMO) wireless channels in the presence of a passive eavesdropper; i.e., the associated eavesdropping channel is unknown to the transmitter. Spatial masked beamforming is chosen as secure transmission strategy, so the information is steered towards the intended receiver while artificial noise (AN) is broadcast to confuse passive eavesdroppers. By their side, the legitimate receiver and the eavesdropper both employ multiple-antenna combining schemes to enhance their respective received signals. The contribution of channel frequency selectivity to improve the secrecy is presented by performance and probabilistic analysis. Moreover, we investigate the capability of the eavesdropper to jeopardise the security of the system by mitigating the interfering effect of the AN using zero forcing (ZF) as a receive beamforming strategy. The results suggest that an

eavesdropper equipped with a large number of antennas can threaten the overall security of the MIMO-OFDM system. This can be achieved by using an appropriate receiving beamforming multiple-antenna mechanism that exploits the knowledge that the attacker might have regarding the transmission strategy used by the transmitter.

We begin this chapter by summarising the most important existing secrecy contributions in MIMO-OFDM systems pointing out the novelty of the work presented here. Next, in section 5.2 we introduce the system modelling of a masked beamforming MIMO-OFDM network. In section 5.3 we show how multiple-antenna systems are used at both transmission and reception to secure the communication and how the power is allocated in the frequency-domain multi-carrier system. Here we analyse the performance of several combining strategies and their impact on secrecy. In section 5.4 we show an analysis of the numerical results based on simulations. Finally, this chapter ends with a brief discussion about the practicality of the analysed technique and some important conclusions about the secrecy performance of the system.

5.1 Physical layer security in frequency selective MIMO channels

In contrast to the two previous chapters where the multiple-input single-output (MISO) case was studied, in this chapter we address the scenario where both receiver nodes that are part of the wiretap model, the intended receiver and the eavesdropper, are equipped with multiple antennas. This case is referred to as the multiple-input multiple-output (MIMO) wiretap channel or multiple-input multiple-output multi-antenna eavesdropper (MIMOME) [48]. In this case, the legitimate transmitter and receiver can exploit the full degree of freedom that their MIMO channel offers in order to maximise the signal quality difference between the destination and the eavesdropper. The first work to point out that a proper exploitation of multiple-antenna space-time diversity can enhance information security and information-hiding capabilities was presented by Hero in [33]. This pioneer contribution opened the door to many studies about the security capabilities of the MIMO channel.

Looking at the MIMO channel's optimal precoding transmission strategy that achieves the secrecy capacity under a total power constraint is a cumbersome task that has attracted the attention of the research community. Indeed, the resulting optimisation problem is nonconvex and therefore difficult to solve, and in contrast to the MISO case, this does not necessarily accept a rank-one covariance matrix as an optimal solution. Indeed, in this scenario, beamforming is generally a suboptimal transmission scheme except in the particular case of a transmitter and receiver both equipped with two antennas each, while the eavesdropper has only one antenna [108]. The full MIMO channel secrecy capabilities are studied by Khisti et al. in [34, 48] and by Oggier and Hassibi in [35, 109]. Here, the secrecy rate maximisation problem is reformulated as a minimax problem and solved by finding numerically a saddle point. In contrast to these approaches, in [110] Bustin et al. introduce a closed-form solution to the secrecy rate maximisation problem subject to enforcing a minimum mean square error (MMSE) constraint in the transmission covariance matrix.

These findings have motivated the research community to provide tractable suboptimal alternative approaches to deal with the technically demanding problem of the MIMO wiretap channel secrecy rate maximisation. In this context, in [111] Mukherjee and Swindlerhurst enforce a suboptimal rank-one transmission strategy to study the secrecy capabilities of the MIMO channel using different types of steering beamforming vector designs at the transmitter and the legitimate and malicious receivers. Here, the performance of the intended receiver is obtained by allocating the minimum power to guarantee a target SNR and devoting the remaining available power to AN generation to confuse unknown eavesdroppers. A similar power allocation approach is used in [72] to study robust beamforming transmission schemes in the MIMO wiretap channel when the eavesdropper uses a MMSE design based combiner to mitigate the effect of the AN. Also in [95] Pei et al. allocate the maximum possible power for AN generation as a valid way to increase the probability of achieving security in a masked beamforming secure transmission by meeting MMSE constraints at both the intended receiver and the eavesdroppers. In [62, 63] a MMSE approach is also used at the receivers to present a probabilistic framework about the security enhancements of a masked beamforming transmission strategy where multiple-antenna eavesdroppers are randomly scattered over

the network. Finally, in [112] maximal ratio combining (MRC) and single combining (SC) are used at the receivers to study the secrecy capabilities of the MIMO wiretap channel when a suboptimal transmission scheme based on antenna selection is used.

All these aforementioned references,which enforce suboptimal rank-one transmission strategies to secure MIMO flat fading channels, do not pay attention to the further potential security opportunities that a frequency selective channel can offer. In contrast to these contributions, in [113] Kobayashi and Debbah study the secrecy capacity of frequency selective fading channels by introducing a Vandermonde precoding transmission that nulls active eavesdroppers by using masked beamforming to deal with passive attackers. Here it is proven that frequency selectiveness can be exploited in the security context. Interestingly, and in contrast to [113], in [114] Renna et al. study the secrecy capacity of single-antenna networks using OFDM considering a sophisticated eavesdropper that is not constrained to use OFDM signalling. This study concludes that the secrecy rate in single-antenna networks can substantially diminish as a result of an eavesdropper not using a fast Fourier transform (FFT)-based demodulator and taking advantage of the additional information that the transmitter encloses in the OFDM message within the cyclic prefix. Later in [115] the achievable ergodic secrecy rates and secrecy outage probabilities of single-antenna OFDM systems are studied and suggest that an intelligent power allocation between the subcarriers can lead to improvements in security. This objective is pursued in [116, 117] where power allocation mechanisms between subcarriers are investigated to secure users in a single-antenna multiple-users OFDM network. It is worth pointing out that neither of these works has addressed the security contribution of frequency selective channels in MIMO-OFDM systems.

5.1.1 This chapter's contribution

This chapter presents a novel analysis of the secrecy improvement resulting from frequency selectiveness in MIMO-OFDM systems. We use a suboptimal rank-one secure masked beamforming transmission mechanism where the AN is broadcast isotropically and orthogonal to the steering beamforming vector. We distribute the power in an opportunistic fashion between the OFDM subcarriers using a water-filling based allocation mechanism to enhance the likelihood of achieving security

in subcarriers with the best quality. Then, for each subcarrier we distribute the power between the information-bearing signal and the AN using three schemes. Firstly, we transmit information using the minimum required power to achieve a specified Quality of Service (QoS) requirement given by a target SNR to be met at the intended receiver while the rest of the power is devoted to AN generation. Secondly, we distribute the power equally between information and AN to maximise the average secrecy rate per subcarrier. Finally, we progressively vary the power devoted to the AN in order to understand its contribution to the secrecy of the MIMO-OFDM system. We study the performance of the system by using several multiple-antenna receiving beamforming mechanisms at the legitimate multi-antenna receiver and at the eavesdropper. The results suggest that frequency selectivity can contribute positively to the secrecy by allowing an opportunistic power allocation and exploiting the frequency diversity of the MIMO channel by using OFDM.

In addition to the aforementioned study, we also study how an eavesdropper that is aware of the transmission strategy used by the transmitter can put at risk the security of the MIMO-OFDM system. Indeed, and in contrast to the works in [53, 63, 72] where MMSE estimation is used to maximise the SNR at the eavesdropper side, here we investigate a novel and simple method based on Zero Forcing (ZF) through which the eavesdropper can mitigate, even null, the interfering effect of the AN. The results suggest that a multiple-antenna eavesdropper that is aware of the main link's channel state information (CSI) poses a major threat to the overall security of the system. Here the number of available antennas at the eavesdropper and the knowledge that the eavesdropper has regarding the transmit strategy play a critical role in the security of the system.

It is worth remarking that the analysis carried out in this chapter considers that all the nodes taking part of the communication use OFDM signalling. In other words, we assume that the eavesdropper has the same receiving capabilities as the legitimate receiver. This assumption can be seen as restrictive owing to the fact that we are effectively enforcing a limitation at the eavesdropper side. However, we assume the worst-case for the security by making available to the eavesdropper all the details of the transmission strategy used by the legitimate transmission parties. In other words, the attacker is aware of the transmission covariance matrices

of both the information and the AN and the perfect CSI between all the transmission parties. This assumption allows us to study the contribution of frequency selectivity in MIMO-OFDM networks and then obtain valuable insight into the improvements in secrecy and also the potential threats to confidentiality arising from a well informed attacker. The case of an eavesdropper with a more sophisticated demodulator and capability to exploit information contained in the OFDM cyclic prefix is out of the scope of the present study.

5.2 System model

In this section we model a MIMO-OFDM system using masked beamforming as a secure transmission strategy. We assume that the transmission is overhead by one eavesdropper also equipped with multiple antennas. Note that this scenario can be viewed as multiple single-antenna colluding eavesdroppers, that is multiple eavesdroppers contributing their reception efforts in a cooperative fashion. Following the well known wireless security model, the legitimate transmitter and receiver are named 'Alice' and 'Bob' while the eavesdropper is referred to as 'Eve'.

Alice, Bob and Eve are respectively equipped with $N_a \geq 2, N_b \geq 1$, and $N_e \geq 1$ antennas. We consider frequency selective channels with L multipath taps; therefore, these time dispersive MIMO channels can be described by L complex channel matrices $\mathbf{H}_{(l)} \in \mathbb{C}^{N_a \times N_b}$ and $\mathbf{G}_{(l)} \in \mathbb{C}^{N_a \times N_e}$ where $l \in [1, 2, \cdots, L]$ denotes the l^{th} tap of the MIMO Alice-to-Bob and Alice-to-Eve small-scale fading channels respectively. We suppose that the channels are subject to block fading; therefore, they remain constant over the transmission of the frame and vary independently from frame to frame. The L taps of both channels are mutually independent and they are modelled as complex matrices with uncorrelated, zero-mean, Gaussian distributed elements with variance σ_H^2/L and σ_G^2/L respectively. In other words, the l^{th} small scale fading matrix channels are $\mathbf{H}_{(l)} \sim \mathcal{CN}(\mathbf{0}, \frac{\sigma_H^2}{L}\mathbf{I})$ and $\mathbf{G}_{(l)} \sim \mathcal{CN}(\mathbf{0}, \frac{\sigma_G^2}{L}\mathbf{I})$. It is important to point out that here we do not consider the effect of the location of the nodes over the distance; in other words, Alice, Bob and Eve are considered equidistant with normalised distance of unity. We assume a passive eavesdropping scenario, and so the main link's CSI is perfectly known to Alice while the eavesdropping's counterpart remains unknown to her. However, we can assume that Alice has available statistical information regarding Eve's channel.

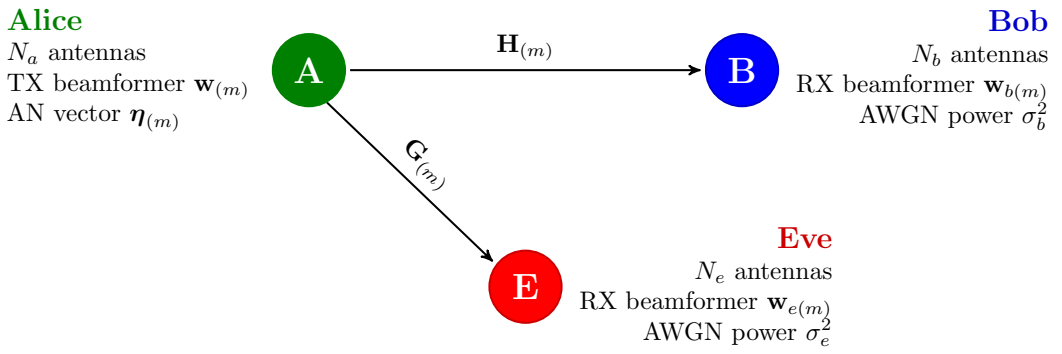


Figure 5.1: *System model of a MIMO-OFDM system. Secure communication between multiple-antenna legitimate parties in the presence of an eavesdropper over the m^{th} frequency domain subcarrier.*

We use OFDM signalling as an effective way to deal with time dispersive channels. Therefore, the MIMO-OFDM model exploits the frequency diversity resulting from the conversion of the time domain frequency selective channel into a set of parallel flat fading channels in the frequency domain [118, §9.1.2]. Therefore, the frequency selective multipath channel with L taps is now represented by an equivalent OFDM system of N parallel flat fading channels. In other words, we use the frequency domain representation of the multi-tap main and eavesdropping channels given by $\mathbf{H}_{(m)}$ and $\mathbf{G}_{(m)}$ where $m \in [0, N-1]$. Here, m represents the m^{th} subcarrier of the equivalent flat-fading Alice-to-Bob and Alice-to-Eve frequency-domain channel matrices. The frequency domain system is depicted in Figure 5.1.

Let $\mathbf{s}_{(m)} \in \mathbb{C}^{N_a}$ denote the steering beamforming signal vector transmitted by Alice over the m^{th} subcarrier where $m \in [0, \cdots, N-1]$. The covariance matrix of the transmitted steering vector $\mathbf{s}_{(m)}$ is given by $\mathbf{C}_{s(m)} = \mathbb{E}\{\mathbf{s}_{(m)}\mathbf{s}_{(m)}^H\}$; therefore, the power allocated to the m^{th} subcarrier is defined by $\rho_{(m)} = \mathrm{Tr}\{\mathbf{C}_{s(m)}\}$. We assume a total power constraint $P = \sum_{m=0}^{N-1} \rho_{(m)}$. Finally, a fraction $\epsilon_{(m)} \in [0, 1)$ of the power allocated to each subcarrier is devoted to the generation of AN. Thus the signal vector $\mathbf{s}_{(m)}$ transmitted over the m^{th} subcarrier is modelled as follows

$$\mathbf{s}_{(m)} = \sqrt{\rho_{(m)}}\left(\sqrt{1-\epsilon_{(m)}}\mathbf{w}_{(m)}d_{(m)} + \sqrt{\epsilon_{(m)}}\boldsymbol{\eta}_{(m)}\right) \tag{5.1}$$

where $\mathbf{w}_{(m)} \in \mathbb{C}^{N_a}$ is the normalised beamforming vector, that is $||\mathbf{w}_{(m)}|| = 1$, $d_{(m)}$ is the transmitted scalar complex information symbol from a Gaussian codebook with $\mathbb{E}\{|d_{(m)}|^2\} = 1$, and $\boldsymbol{\eta}_{(m)} \in \mathbb{C}^{N_a}$ is the AN vector with covariance matrix $\mathbf{C}_{\eta(m)} = \mathbb{E}\{\boldsymbol{\eta}_{(m)}\boldsymbol{\eta}_{(m)}^H\}$.

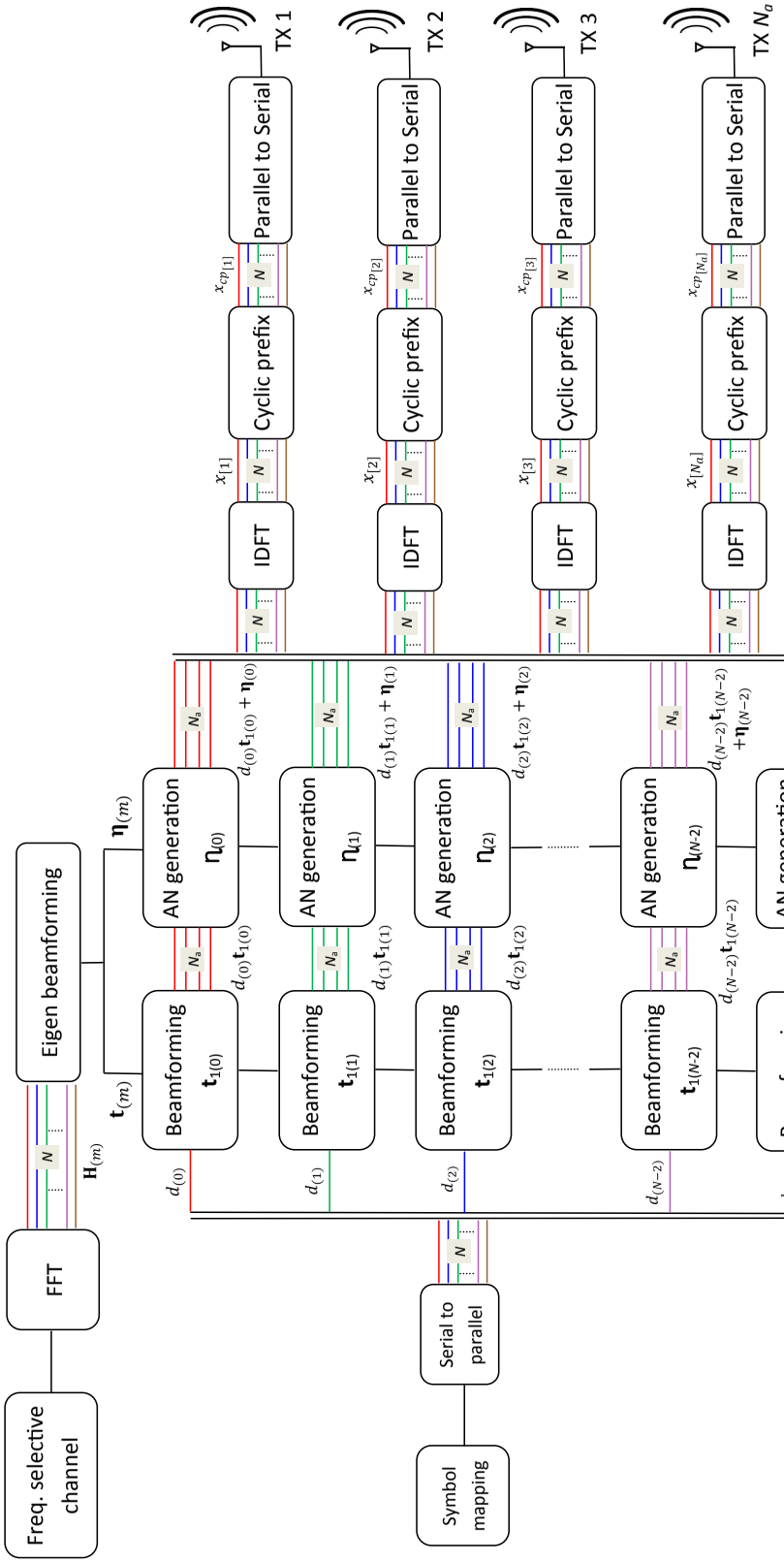


Figure 5.2: *Block schematic of the transmission stage of a masked beamforming MIMO-OFDM system.*

Figure 5.2 depicts a block diagram showing the implementation of the MIMO-OFDM transmission strategy. The figure illustrates how the masked beamforming strategy is implemented in the frequency domain using each one of the N subcarriers of the frequency domain main link's MIMO channel; i.e., $\mathbf{H}_{(m)}$. The output of the N masked beamforming blocks are scrambled to form the input of the N_a IDFT blocks to add later the cyclic prefix. Finally the parallel signal is de-multiplexed into a serial stream that feeds each one of the N_a transceivers at the transmission stage.

The signal vectors received by the multiple-antenna Bob and Eve on the m^{th} subcarrier are respectively given by:

$$\mathbf{u}_{(m)} = \mathbf{H}_{(m)}^{H}\mathbf{s}_{(m)} + \mathbf{n}_{b(m)} \tag{5.2}$$

$$\mathbf{v}_{(m)} = \mathbf{G}_{(m)}^{H}\mathbf{s}_{(m)} + \mathbf{n}_{e(m)} \tag{5.3}$$

where $\mathbf{H}_{(m)}$ and $\mathbf{G}_{(m)}$ are the m^{th} subcarrier of the Alice-to-Bob and Alice-to-Eve frequency-domain channel matrices. In addition, $\mathbf{n}_{b(m)} \in \mathbb{C}^{N_b}$ and $\mathbf{n}_{e(m)} \in \mathbb{C}^{N_e}$ are the mutually independent, zero-mean, complex, AWGN vectors at the m^{th} subcarrier such that $\mathbf{n}_{b(m)} \sim \mathcal{CN}(\mathbf{0}, \frac{\sigma_b^2}{N}\mathbf{I})$ and $\mathbf{n}_{e(m)} \sim \mathcal{CN}(\mathbf{0}, \frac{\sigma_e^2}{N}\mathbf{I})$.

In order to combine the signal received at the reception, we assume that Bob and Eve use a receiving beamformer vector given by $\mathbf{w}_{b(m)} \in \mathbb{C}^{N_b}$ and $\mathbf{w}_{e(m)} \in \mathbb{C}^{N_e}$ respectively. Therefore, the scalar signals at the output of the combiners are

$$y_b(m) = \mathbf{w}_{b(m)}^{H}\mathbf{u}_{(m)} \tag{5.4}$$

$$y_e(m) = \mathbf{w}_{e(m)}^{H}\mathbf{v}_{(m)}. \tag{5.5}$$

After the combining stage at the receiver, we can obtain the signal-to-noise ratios at Bob and Eve at the m^{th} subcarrier denoted by $\mathrm{SNR}_{b(m)}$ and $\mathrm{SNR}_{e(m)}$ respectively. The exact SNR expressions will depend upon the combining scheme used at the receiver; indeed, we consider different alternatives detailed in the next section §5.3.2. Finally, an achievable secrecy rate $\mathrm{R}_{S(m)}$ over the m^{th} subcarrier of the modelled system model is given by

$$\mathrm{R}_{S(m)} = \left[\log_2\left(1+\mathrm{SNR}_{b(m)}\right) - \log_2\left(1+\mathrm{SNR}_{e(m)}\right)\right]^{+} \text{[bps/Hz]}. \tag{5.6}$$

5.2.1 Probability of achieving secrecy

Let us recall that for the pure passive eavesdropping case perfect secrecy cannot be guaranteed. Indeed, when the transmitter is not aware of the eavesdropping link's instantaneous CSI, then perfect secrecy cannot be ensured and so a probabilistic framework is necessary to quantify the likelihood of achieving secrecy. We define the probability of achieving secrecy on the m^{th} subcarrier as the likelihood that the information can be transmitted secretly over the main link at a minimum target secrecy rate R; i.e., $P_S = \mathbb{P}\left[\mathrm{R}_{S(m)} \geq R\right]$. This is expressed by:

$$P_S = \mathbb{P}\left[\log_2\left(1 + \mathrm{SNR}_{b(m)}\right) - \log_2\left(1 + \mathrm{SNR}_{e(m)}\right) \geq R\right]. \tag{5.7}$$

5.3 A MIMO-OFDM masked beamforming transmission scheme

We aim to study the secrecy performance of a frequency selective MIMO system using masked beamforming as a secure transmission strategy. Following the procedure discussed in chapter 3 of this thesis and presented in [102, 103], a potentially suboptimal masked beamforming transmission strategy is enforced by steering the information towards the intended receiver Bob and broadcasting AN orthogonally to the beamforming vector $\mathbf{w}_{(m)}$ to confuse the unknown eavesdropper. Therefore, Alice chooses the beamforming vector $\mathbf{w}_{(m)}$ as the principal eigenvector $\mathbf{t}_{1(m)}$ corresponding to the largest eigenvalue of $\mathbf{H}_{(m)}\mathbf{H}_{(m)}^H$. Subsequently, the AN vector $\boldsymbol{\eta}_{(m)}$ is generated by the weighted linear combination of the remaining $N_a - 1$ eigenvectors. This means that the AN resulting from the equal power distribution among the $N_a - 1$ remaining eigenvector is broadcast isotropically and orthogonally to the steering beamforming vector $\mathbf{t}_{1(m)}$; i.e., $\mathbf{t}_{1(m)}^H \boldsymbol{\eta}_{(m)} = 0$. That is

$$\boldsymbol{\eta}_{(m)} = \frac{1}{\sqrt{N_a - 1}} \sum_{i=2}^{N_a} \mathbf{t}_{i(m)} \eta_i \tag{5.8}$$

where $\mathbf{t}_{i(m)}$ is the i^{th} eigenvector of $\mathbf{H}_{(m)}\mathbf{H}_{(m)}^H$ and η_i is a random, complex scalar with unit magnitude and random phase uniformly distributed; i.e., $\eta_i = e^{j\phi_i}$ and $\phi_i \in [0, 2\pi)$. Thus the AN covariance matrix is given by

$$\mathbf{C}_{\eta(m)} = \frac{1}{N_a - 1} \sum_{i=2}^{N_a} \mathbf{t}_{i(m)} \mathbf{t}_{i(m)}^H. \tag{5.9}$$

5.3.1 Power allocation

As explained before, and as a result of using OFDM signalling, we address a multi-carrier masked beamforming system. Therefore, it is necessary to devise two power allocation mechanisms. The first one will distribute the total available power among the subcarriers while the second one will allocate the power between information and AN within each subcarrier.

Let us first deal with the power allocation between subcarriers. The objective here is to increment the secrecy capabilities of the system. Based on the fact that the transmitter is not aware of the eavesdropping channel, a valid strategy to enlarge the secrecy rate of the multi-carrier masked beamforming system given by (5.6) is by enhancing the capacity of the main-link. This objective can be attained by allocating more power to the best subcarriers in an opportunistic fashion. Therefore, following the Proposition 4.1 in [118, §4] the total power P is distributed among the N subcarriers using the water-filling iterative technique as follows

$$\rho_{(m)} = \max\left(0, \frac{1}{\hat{N}}\left(\hat{P} + \sum_{i=1}^{N}\frac{1}{\gamma_{(i)}}\right) - \frac{1}{\gamma_{(i)}}\right) \tag{5.10}$$

where $\hat{P}$ is the available power for information once the power requested for the transmission of the cyclic prefix of length μ has been considered such that

$$\hat{P} = \sum_{m=1}^{N}\rho_{(m)} = \frac{PN}{N+\mu}. \tag{5.11}$$

In other words, we are effectively distributing the available power after considering the power required for transmitting the cyclic prefix.

We recall that waterfilling is an iterative power allocation mechanism; therefore, in (5.10) $\hat{N}$ is the total number of subcarriers which have have been initially allocated power; i.e., $\rho_{(m)} \neq 0$. This means that $\hat{N}$ subcarriers will be considered for the next round of power allocation. Finally, in (5.10) $\gamma_{(i)}$ denotes the channel's power to noise ratio and it is given by

$$\gamma_{(i)} = \frac{||\mathbf{H}_{(i)}||_F^2}{N_a N_b \sigma_{(m)}^2} \tag{5.12}$$

where $\sigma_{(m)}^2$ is the noise power per subcarrier equivalent to σ_b^2/N.

Once that the power per subcarrier ($\rho_{(m)}$) has been determined, we need to define the criterion to distribute it between information and AN. In other words, we have to calculate the fraction of power allocated to broadcast AN, i.e., $\epsilon_{(m)}\rho_{(m)}$, and the one used to transmit the information signal, i.e., $(1-\epsilon_{(m)})\rho_{(m)}$. To do this, we consider three different approaches as follows.

- The first allocation criterion is based on the idea introduced in [53] where a fixed QoS performance is enforced at the intended receiver. Here, the parameter $\epsilon_{(m)}$ is defined in such way that the minimal power is allocated to guarantee a target SNR at Bob's m^{th} subcarrier given by $\overline{\mathrm{SNR}}_{(m)}$. The remaining power is devoted for AN generation. The idea is to allocate the maximum amount of power for AN generation while ensuring a minimum acceptable performance at Bob. Hence, $\epsilon_{(m)}$ is obtained as:

$$\epsilon_{(m)} = 1 - \frac{\overline{\mathrm{SNR}}_{(m)}\sigma^2_{(m)}}{\rho_{(m)}\nu_{1(m)}} \tag{5.13}$$

  where $\nu_{1(m)}$ is the largest eigenvalue of $\mathbf{H}_{(m)}\mathbf{H}^H_{(m)}$.

- For the second power allocation method, we distribute the power per subcarrier $\rho_{(m)}$ following the findings in [57]. Here it is shown that equal power distribution between information and AN is nearly optimal to maximise the ergodic secrecy rate. Therefore, we set $\epsilon_{(m)} = 0.5$ for all the subcarriers that have been allocated power by the waterfilling algorithm.

- Finally, and with the aim of understanding the impact of the AN over the secrecy of the system and then obtaining valuable insight into the multicarrier strategy performance, we progressively vary the fraction of power ($\epsilon_{(m)}$) committed to AN generation.

We use these different power allocation criteria between AN and information to study the secrecy performance of the modelled MIMO-OFDM system.

5.3.2 Receiver's combining mechanisms

Now, let us drawn our attention to the combining mechanisms that both receivers Bob and Eve can use to enhance the received signal by exploiting their receiving

multiple-antenna capabilities. It is worth recalling that for this analysis we assume that Bob and Eve are also using OFDM signalling, therefore we constrain our analysis to the performance of the system described in §5.2. Therefore, Bob uses maximal ratio combining (MRC) while Eve combines the received signal by using receiving beamformers based on minimum mean square error (MMSE) and a zero-forcing (ZF) strategies. The latter receiving combining method allows the multiple-antenna eavesdropper, depending on its number of antennas, to cancel or at least to mitigate the effect of the AN generated by Alice jeopardising the security of the MIMO-OFDM system.

Receive beamforming by maximal ratio combining

The intended receiver Bob chooses MRC as the multiple-antenna combining technique in order to maximise its SNR. Therefore, we use again the principal eigenvector $\mathbf{t}_{1(m)}$ corresponding to the largest eigenvalue of $\mathbf{H}_{(m)}\mathbf{H}_{(m)}^{H}$ to obtain the receiving beamformer vector $\mathbf{w}_{b(m)}^{\text{MRC}}$ as

$$\mathbf{w}_{b(m)}^{\text{MRC}} = \mathbf{H}_{(m)}^{H}\mathbf{t}_{1(m)}. \tag{5.14}$$

After obtaining the scalar signal at the output of Bob's combiner, the SNR at the m^{th} subcarrier can be calculated as follows:

$$\text{SNR}_{b(m)}^{\text{MRC}} = \left(1-\epsilon_{(m)}\right)\rho_{(m)}\mathbf{t}_{1(m)}^{H}\mathbf{H}_{(m)}\left[\sigma_{(m)}^{2}\mathbf{I}_{N_b}\right]^{-1}\mathbf{H}_{(m)}^{H}\mathbf{t}_{1(m)}. \tag{5.15}$$

Note that selecting the receiving beamformer in (5.14) allows Bob to effectively cancel the effect of the AN generated by Alice due to the orthogonality condition between AN and the steering information beamformer vector; i.e., $\mathbf{t}_{1(m)}^{H}\boldsymbol{\eta}_{(m)} = 0$.

Receive beamforming using the minimum mean square error approach

Now, Eve attempts to recover the maximum possible information from the Alice-to-Bob transmission. So from her point of view, the best multiple-antenna combining method will be the one that provides the highest SNR. This condition effectively represents the worst-case for the security of the modelled MIMO-OFDM system. In this context, and following [53, 63, 72], Eve uses MMSE as an optimal receiver structure to maximise her SNR.

In order to calculate Eve's receiving beamforming vector, we assumed the worst-case for the security and therefore Eve is somehow aware of the transmission strategy used by Alice and defined by the transmitted steering beamforming vector ($\mathbf{t}_{1(m)}$), the AN covariance matrix ($\mathbf{C}_{\eta(m)}$) and the power allocation between information and AN ($\epsilon_{(m)}$).

Under this worst-case assumption, Eve's MMSE beamforming vector at the m^{th} subcarrier is given by:

$$\mathbf{w}_{e(m)}^{\text{MMSE}} = \left(\epsilon_{(m)}\rho_{(m)}\mathbf{G}_{(m)}^{H}\mathbf{C}_{\eta(m)}\mathbf{G}_{(m)} + \sigma_{e(m)}^{2}\mathbf{I}_{N_e}\right)^{-1}\mathbf{G}_{(m)}^{H}\mathbf{t}_{1(m)}. \tag{5.16}$$

Bearing in mind that Eve's scalar signal at the output of the beamformer is given by $y_{e(m)}^{\text{MMSE}} = \left(\mathbf{w}_{e(m)}^{\text{MMSE}}\right)^{H}\mathbf{v}_{(m)}$, then Eve's SNR at the m^{th} subcarrier is given by:

$$\begin{aligned}&\text{SNR}_{e(m)}^{\text{MMSE}} = \\ &\left(1-\epsilon_{(m)}\right)\rho_{(m)}\mathbf{t}_{1(m)}^{H}\mathbf{G}_{(m)}\left(\epsilon_{(m)}\rho_{(m)}\mathbf{G}_{(m)}^{H}\mathbf{C}_{\eta(m)}\mathbf{G}_{(m)} + \sigma_{e(m)}^{2}\mathbf{I}_{N_e}\right)^{-1}\mathbf{G}_{(m)}^{H}\mathbf{t}_{1(m)}.\end{aligned} \tag{5.17}$$

Receive beamforming by zero forcing

Here we address the case when Eve, through the knowledge of the transmitting strategy used by Alice, is able to mitigate the interfering effect of the AN. Under the same assumptions noted in the above section, i.e., Eve is fully aware of her own channel $\mathbf{G}_{(m)}$ and the steering beamforming vector $\mathbf{t}_{1(m)}$, Eve's ZF beamformer vector is

$$\mathbf{w}_{e(m)}^{\text{ZF}} = \left(\mathbf{G}_{(m)}^{\dagger}\right)^{H}\mathbf{t}_{1(m)} \tag{5.18}$$

with $\mathbf{G}_{(m)}^{\dagger} = \left(\mathbf{G}_{(m)}\mathbf{G}_{(m)}^{H}\right)^{-1}\mathbf{G}_{(m)}$ denoting the Moore-Penrose pseudo inverse. This receiving beamforming formulation vector allows Eve to mitigate the effect of the AN vector $\boldsymbol{\eta}_{(m)}$. This can be easily seen by considering the scalar signal at the output of Eve's combiner given by

$$y_{e(m)}^{\text{ZF}} = \left(\mathbf{w}_{e(m)}^{\text{ZF}}\right)^{H}\mathbf{v}_{(m)} \tag{5.19}$$

which can be explicitly written as

$$y_{e(m)}^{\text{ZF}} = \sqrt{1-\epsilon_{(m)}}\sqrt{\rho_{(m)}}\mathbf{t}_{1(m)}^{H}\mathbf{G}_{(m)}^{\dagger}\mathbf{G}_{(m)}^{H}\mathbf{t}_{1(m)}d_{(m)}$$

$$+ \sqrt{\epsilon_{(m)}}\sqrt{\rho_{(m)}}\mathbf{t}_{1(m)}^{H}\mathbf{G}_{(m)}^{\dagger}\mathbf{G}_{(m)}^{H}\boldsymbol{\eta}_{(m)} + \mathbf{t}_{1(m)}^{H}\mathbf{G}_{(m)}^{\dagger}\mathbf{n}_{e(m)}. \tag{5.20}$$

Here, assuming $N_e \geq N_a$, it is straightforward to see that the second term that contains the AN vector $\boldsymbol{\eta}_{(m)}$ is cancelled owing to $\mathbf{G}_{(m)}^{\dagger}\mathbf{G}_{(m)}^{H} = \mathbf{I}_{N_e}$ and $\mathbf{t}_{1(m)}^{H}\boldsymbol{\eta}_{(m)} = 0$. Therefore, Eve's SNR at the m^{th} subcarrier now is

$$\text{SNR}_{e(m)}^{\text{ZF}} = \left(1 - \epsilon_{(m)}\right)\rho_{(m)}\left[\sigma_{e(m)}^{2}\mathbf{t}_{1(m)}^{H}\mathbf{G}_{(m)}^{\dagger}\left(\mathbf{G}_{(m)}^{\dagger}\right)^{H}\mathbf{t}_{1(m)}\right]^{-1}. \tag{5.21}$$

In the case that $N_e < N_a$, then the AN nulling operation will not be completely successful. Therefore, Eve's SNR at the m^{th} subcarrier can be written as

$$\text{SNR}_{e(m)}^{\text{ZF}} = \frac{\left(1 - \epsilon_{(m)}\right)\rho_{(m)}|\mathbf{t}_{1(m)}^{H}\mathbf{G}_{(m)}^{\dagger}\mathbf{G}_{(m)}^{H}\mathbf{t}_{1(m)}|^{2}}{\mathbf{t}_{1(m)}^{H}\mathbf{G}_{(m)}^{\dagger}\left[\epsilon_{(m)}\rho_{(m)}\mathbf{G}_{(m)}^{H}\mathbf{C}_{\eta(m)}\mathbf{G}_{(m)} + \sigma_{e(m)}^{2}\mathbf{I}_{N_e}\right]\left(\mathbf{G}_{(m)}^{\dagger}\right)^{H}\mathbf{t}_{1(m)}}. \tag{5.22}$$

Although the ZF combiner in (5.18) mitigates the AN, unlike the receiving beamforming vector based on MMSE, it does not maximise the SNR due to the fact that the AWGN component is amplified. On the other hand, the MMSE based combining approach in (5.16) offers the best performance by striking a balance between AN cancellation and AWGN mitigation.

5.4 Numerical results

In this section we present simulation results to show the contribution to secrecy of the frequency selectivity in a MIMO-OFDM system. We also study the performance of both ZF and MMSE as Eve's beamforming receive strategies by analysing the achieved secrecy probability. For the simulations, frequency selective channels with L taps are considered, so the length of the cyclic prefix in the OFDM signalling is set to $L-1$ samples in order to avoid inter-symbol interference. The simulation parameters are detailed in Table 5.1

5.4.1 Frequency selectivity contribution to secrecy

In Figure 5.3, we use equal power distribution between the information and the AN, i.e., $\epsilon_{(m)} = 0.5$, to illustrate the effect on secrecy of increasing the number of

Table 5.1: *Parameters for the simulation.*

Parameter	Value	Description
N_a	5	Alice's number of antennas
N_b	5	Bob's number of antennas
σ_H^2	1	Bob's channel elements variance
σ_G^2	1	Eve's channel elements variance
σ_b^2	1	Bob's AWGN power
σ_e^2	1	Eve's AWGN power
L	4	Number of channel taps

OFDM subcarriers. All the nodes have the same number of antennas. Eve considers both MMSE and ZF as receiving beamforming methods; subsequently, we evaluate $\text{SNR}_{e(m)}^{\text{MMSE}}$ in (5.17) and $\text{SNR}_{e(m)}^{\text{ZF}}$ in (5.21). Here, when Eve is using MMSE, the secrecy rate, (i.e., the difference between the logarithm of Bob's and Eve's SNRs), increases with the number of subcarriers N. In contrast, when Eve uses ZF this gap remains constant due to Eve's AN cancellation capabilities. This interesting behaviour and the reasoning about why ZF outperforms MMSE will be analysed in detail later in this section. For the moment, we will concentrate on the case when Eve uses the MMSE approach.

In Figure 5.4, the impact of increasing the number of OFDM subcarriers over the system's secrecy is shown. Here, the power is allocated between the information and the AN to guarantee a varying target SNR; i.e., $\epsilon_{(m)}$ is calculated using (5.13). All the nodes are equipped with the same number of antennas. Eve chooses MMSE as the receiving beamforming strategy, that is Eve uses the combiner in (5.16). In this approach, the secrecy improvement resulting from the additional number of OFDM subcarriers is twofold. First, the gap between Bob's and Eve's SNR increases, and second, the maximum target SNR that Bob can achieve with the power available is extended. It is worth pointing out that as the target SNR at Bob increases, the system allocates less power for AN generation and therefore the gap between Bob's and Eve's SNR and subsequently the secrecy rate decreases. In fact, there is a point where the power available at Alice is exhausted and the system cannot provide larger target SNR values at Bob. In this scenario, there is no power remaining for AN generation; however, there is still a gap between Bob's

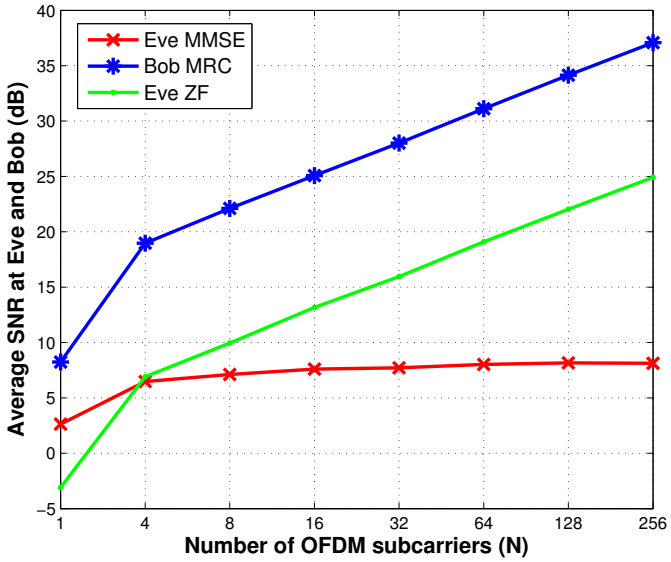


Figure 5.3: *System performance. Average SNR at Bob and Eve vs. number of OFDM subcarriers (N) when Eve uses MMSE and ZF with $\epsilon_{(m)} = 0.5$ and $N_e = 5$.*

and Eve's SNR owing to the gain introduced by steering the information towards Bob.

We again use the power allocation scheme in (5.13) to target a given performance at Bob to analyse the effect of increasing the number of antennas at Eve. This is depicted in Figure 5.5 where Eve's SNR improves as the number of antennas N_e increases. These results follow intuition; indeed, a large number of antennas enables Eve to mitigate the effect of the AN due to the extra spatial diversity available undermining the secrecy of the system. Indeed, there is a point in the plot where Eve outperforms Bob showing that an eavesdropper equipped with a large number of antennas is a great threat for the security of the system.

Now, we draw our attention to the probabilistic secrecy performance of the technique through the methodology introduced in §5.2.1. For ease of analysis, we consider the average secrecy rate over the subcarriers served by the water-filling algorithm. The improvement in secrecy due to the increase of the number of OFDM subcarriers can be clearly seen in the three cases illustrated in the Figure 5.6. Here, the power allocation mechanism that guarantees the target SNR at Bob in (5.13) fixes the maximum secrecy rate that the system can achieve. It is interesting to note that when the system becomes more demanding and requires a larger target SNR at Bob, the probability of achieving a given secrecy rate with few subcarriers

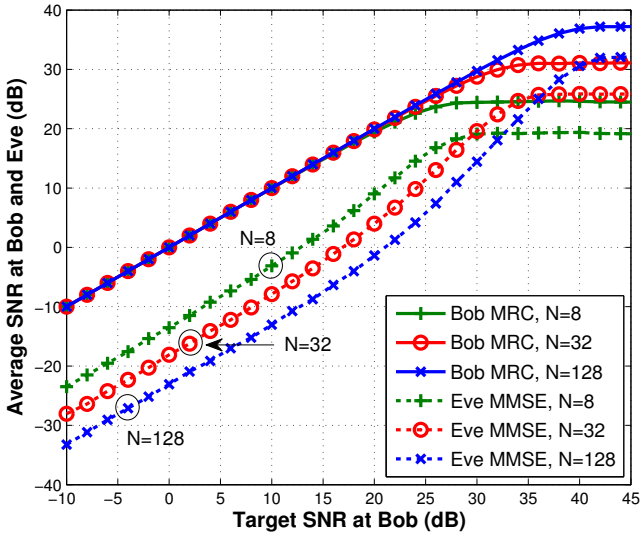


Figure 5.4: *System performance. Average SNR at Bob and Eve vs. target SNR at Bob for different number of OFDM subcarriers, ($N = 8, 32, 128$) when Eve uses MMSE and $N_e = 5$.*

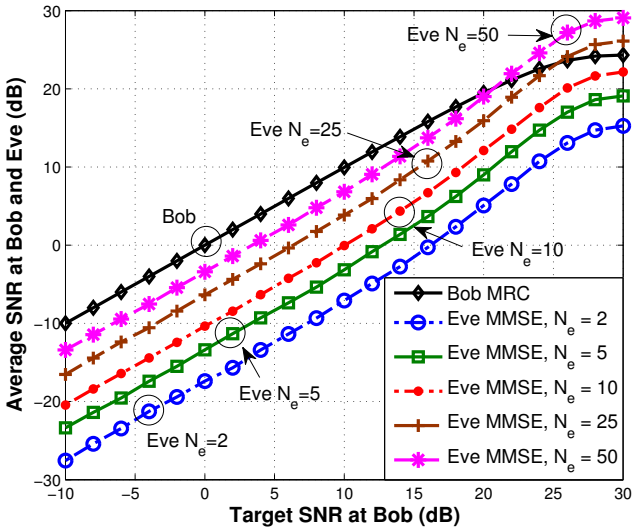


Figure 5.5: *System performance. Average SNR at Bob and Eve vs. target SNR at Bob for different number of antennas at Eve (N_e) when Eve uses MMSE and $N = 8$.*

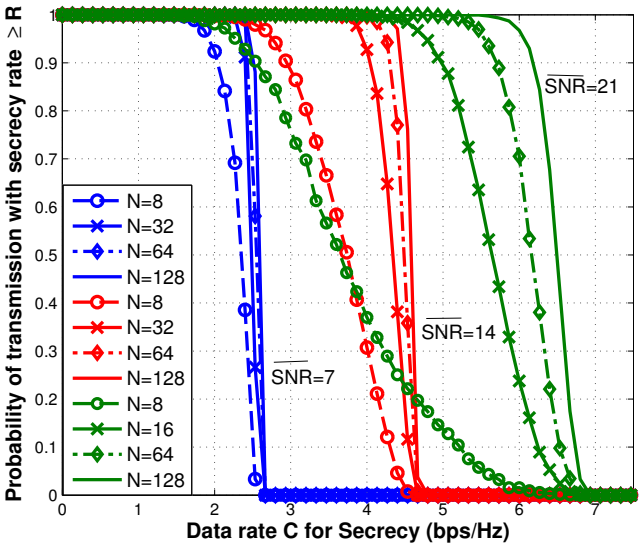


Figure 5.6: *Probabilistic performance. Probability of achieving a secrecy rate greater than R for several values of target SNR at Bob ($\overline{\mathrm{SNR}}$) for $N = 8, 32, 64, 128$ when Eve uses MMSE and $N_e = 5$.*

is low. This result shows again the utility of increasing the number of subcarriers to improve the security of the MIMO-OFDM system by taking advantage of the opportunistic power allocation between subcarriers.

In Figure 5.7 we investigate the relationship between the number of antennas at Eve and the probability of secrecy as defined in (5.7). The results suggest again that an eavesdropper equipped with a large number of antennas poses a major threat to the secrecy of the system.

5.4.2 Cancellation of the artificial noise

Now we turn our attention to the performance and impact over the secrecy of the multi-carrier MIMO-OFDM system of ZF and MMSE as Eve's combining schemes. Indeed, in this section we analyse in detail the secrecy performance of the system when Eve is able to mitigate the effect of the AN due to the knowledge that she has about the transmit strategy used by Bob. This is, Eve knows the steering beamforming vector, the covariance matrix of the AN and the power distribution criterion between information and AN. In this context, we compare the performance achieved by both receiving beamforming methods MMSE and ZF, respec-

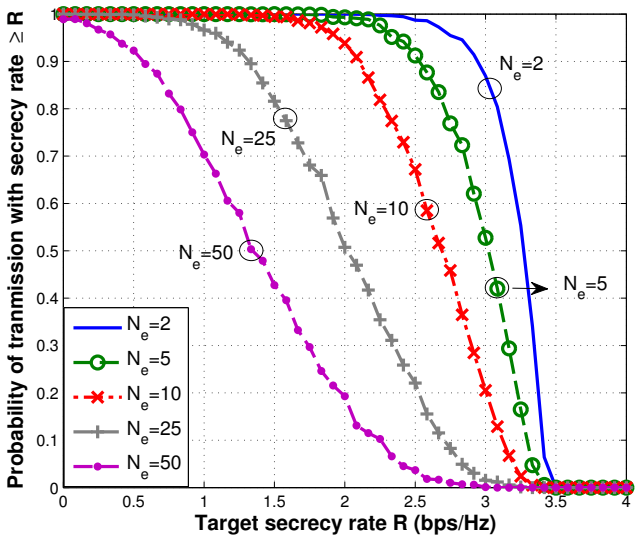


Figure 5.7: *Probabilistic performance. Probability of achieving a secrecy rate greater than R for different number of antennas at Eve $N_e = 2, 5, 10, 25, 50$ when Eve uses MMSE. The target SNR at Bob is $\overline{\text{SNR}} = 10$ and $N = 8$.*

tively given by expressions (5.17) and (5.21), under different AN conditions. Thus, we progressively vary the value of the fraction of the power allocated to AN ($\epsilon_{(m)}$) from zero AN power to the case when almost no power is allocated for the information; i.e., $\epsilon_{(m)} \in [0, 0.95]$. As done before, the SNR is calculated by averaging over the subcarriers that have been allocated power by the water-filling algorithm.

In Figure 5.8 the receiving beamforming schemes' performance is compared for frequency selective channels when all the nodes in the network are equipped with the same number of antennas. Here ZF achieves a better performance due to the effect of the AN cancellation. Indeed, for ZF the gap between Bob's and Eve's SNR remains constant for all the values of $\epsilon_{(m)}$ due to the effective AN cancellation. In contrast, for the MMSE combiner the gap depends on the amount of power devoted to the AN generation.

As previously pointed out in Figure 5.3 and confirmed in Figure 5.8, ZF outperforms MMSE even though that MMSE is well-know as the optimal strategy to maximise SNR in the presence of non-Gaussian interference [118, §1.4.2], which is the case for the AN. This performance is based on two observations. Firstly, ZF, as explained in §5.3.2, can effectively cancel the AN generated by Alice by knowing the transmission strategy. This can be observed by comparing the equations (5.17) and

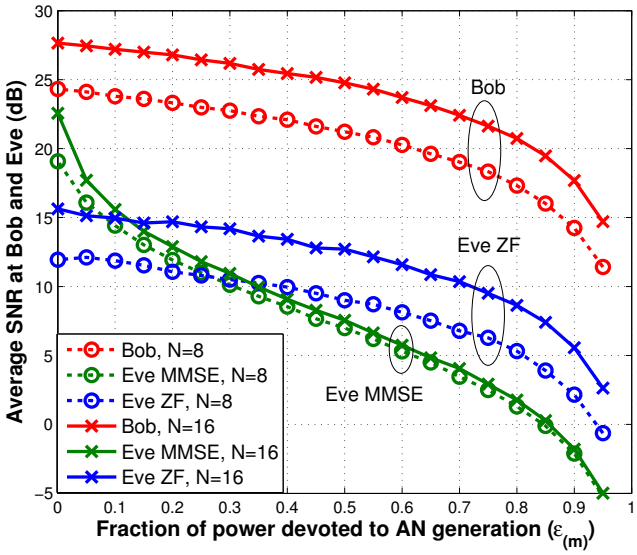


Figure 5.8: *System performance. Average SNR at Bob and Eve vs. fraction of power for AN generation ($\epsilon_{(m)}$) for different number of OFDM subcarriers ($N = 8, 16$) when Eve uses MMSE and ZF and $N_e = 5$.*

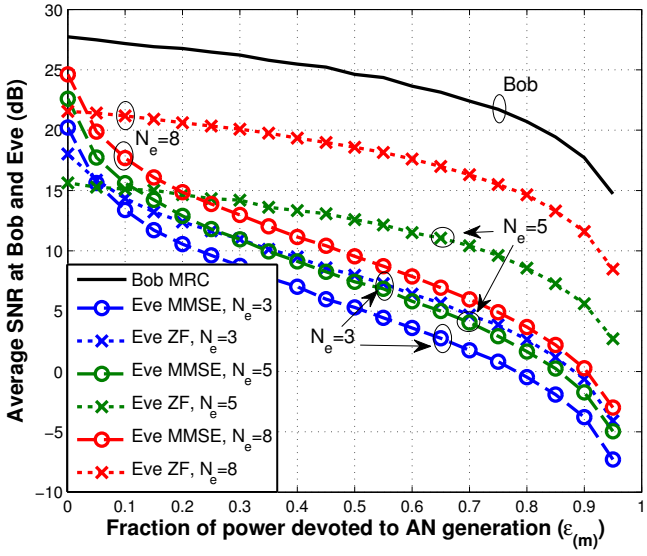


Figure 5.9: *System performance. Average SNR at Bob and Eve vs. fraction of power for AN generation ($\epsilon_{(m)}$) for different number of antennas at Eve ($N_e = 3, 5, 8$) when Eve uses MMSE and ZF and $N = 16$.*

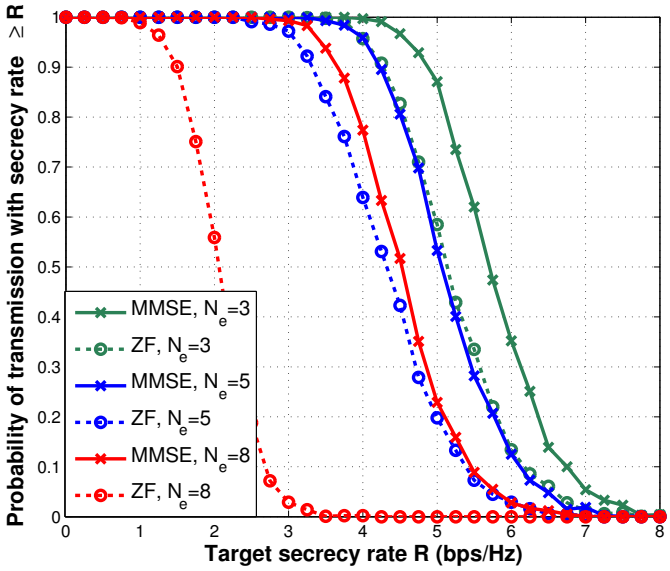


Figure 5.10: *Probabilistic performance. Probability of achieving a secrecy rate greater than R for different number of antennas at Eve ($N_e = 3, 5, 8$) when Eve uses MMSE and ZF and $N = 16$.*

(5.21) where the jamming effect of the AN is cancelled by ZF. Secondly, in (5.21), we observe that the ZF combiner, although that it cancels the AN, it enhances the AWGN; however, this AWGN amplification is not large enough to offset the AN cancellation effect. This behaviour is based on the fact that an OFDM multi-carrier system preserves the overall performance (given by the average SNR) by effectively distributing the power of both information and AWGN among the subcarriers [119, §4]. As a result, the N flat fading channels are subject to a lower AWGN in each subcarrier resulting from the distribution of the time-domain AWGN power across the frequency domain subcarriers. This effect is opportunistically exploited by the water-filling based power allocation; therefore, the AWGN enhancement penalty introduced by ZF is negligible. As a result, the ZF combining scheme enhances the achieved SNR by mitigating the AN's jamming effect without any trade-off.

In Figure 5.9 we investigate the link between the number of Eve's antennas and her AN cancellation ability. As expected, when the Alice-to-Eve channel corresponds to a square or tall matrix, i.e., $N_e \geq N_a$, Eve can effectively null the AN. Even though in the case of a fat channel matrix; i.e., $N_e < N_a$, Eve using ZF can only partially cancel the AN, this performance is still good enough to outperform its MMSE's counterpart. This is shown in Figure 5.9. These results are corrob-

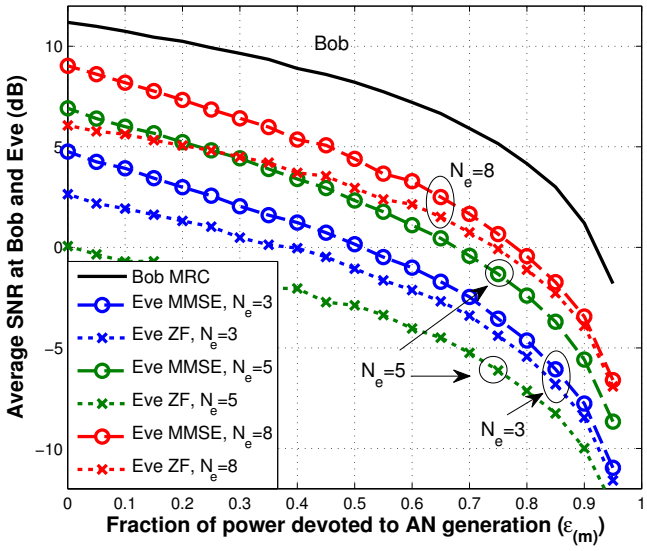


Figure 5.11: *System performance. Average SNR at Bob and Eve vs. fraction of power for AN generation ($\epsilon_{(m)}$) in flat fading channels for different number of antennas at Eve ($N_e = 3, 5, 8$) when Eve uses MMSE and ZF.*

orated by the achieved probability of secrecy depicted in Figure 5.10 where the likelihood of achieving a communication with secrecy rate R diminishes for all the cases when Eve uses ZF as the combining mechanism rather than MMSE.

Finally, in Figure 5.11 we extend this analysis to the flat fading channel scenario where we simply examine the performance of one subcarrier. Here the results show that, as expected, the best technique for receiving beamforming, from Eve's point of view and the worst-case for the secrecy, is MMSE rather than ZF. As explained before, in single-carrier systems the power of information and AWGN is not distributed among subcarriers and thus the optimal scheme to maximise the SNR is obtained through MMSE notwithstanding the AN cancelling capabilities of ZF.

5.5 Discussion and summary

In this section we briefly discuss the eavesdropper's ability and the required conditions to recover the information to cancel the AN broadcast by the transmitter in practical systems and then effectively jeopardise the security of the MIMO-OFDM

network. Recapitulating §5.3.2, if the eavesdropper uses MMSE as a receive beamforming strategy, the worst scenario for the secrecy of the system happens when Eve is fully aware of the transmission strategy used by Alice. In other words, Eve somehow has to know the CSI of the main link ($\mathbf{H}_{(m)}$) and therefore she can obtain the steering beamforming vector $\mathbf{t}_{1(m)}$. Also Eve has to know the AN covariance matrix $\mathbf{C}_{\eta(m)}$ and the power allocation strategy for the AN in every subcarrier ($\epsilon_{(m)}$). On the other hand, ZF only requires that Eve knows her own CSI ($\mathbf{G}_{(m)}$) and the beamformer vector ($\mathbf{t}_{1(m)}$) in order to attempt to null the AN. Considering that $\mathbf{t}_{1(m)}$ is chosen as the principal eigenvector corresponding to the largest eigenvalue of $\mathbf{H}_{(m)}^{H}\mathbf{H}_{(m)}$, then the security of the studied MIMO-OFDM system relies on keeping the Alice-to-Bob's CSI ($\mathbf{H}_{(m)}$) secret from Eve.

In this context, and assuming that Eve is perfectly capable of recovering her own channel, the main problem from the eavesdropper's perspective is how to recover the main channel's time domain signature ($\mathbf{H}$). Let us consider two scenarios about how Alice acquires $\mathbf{H}$. The first one assumes a frequency-division duplexing (FDD) system relying on the quantised feedback sent back by Bob to Alice using the feedback channel. The second scenario exploits channel reciprocity between uplink and downlink in time-division duplexing (TDD) systems so Alice and Bob estimate the channel separately. In the first case, Eve, in order to recover $\mathbf{H}$, might eavesdrop the non-secure Bob-to-Alice feedback channel to overhear the CSI when Bob sends it back to Alice. In the second channel reciprocity scenario, the task is more complicated for Eve and will require extra complexity at her side to incorporate blind channel estimation techniques. This approach will not lead to a completely accurate CSI and so the security of the system offered by the AN generation will be still partially preserved.

It is worth remarking that in this chapter we have considered that all the parties use OFDM signalling, including the eavesdropper. A potential threat for the security arises when the eavesdroppers is not constrained to use OFDM and it can exploit all the received frame to threaten the security. Indeed, as pointed out in [114, 120], an eavesdropper equipped with a more complex receiver architecture can take advantage of the redundant information included in the cyclic prefix to undermine the secrecy of the system. This case is out of the scope of the analysis presented in this chapter where we have assumed that the eavesdropper is a node of the network and therefore uses an OFDM.

In conclusion, in this work we have studied a suboptimal secure transmission scheme based on masked beamforming over frequency selective MIMO channels. This mechanism does not exploit the full spatial diversity that the MIMO channel offers and steers the information over the principal eigenvector of the main link between transmitter and receiver. The AN has been generated orthogonally to the steering beamformer signature; therefore, the legitimate receiver can null its effect by using an appropriate receiving combiner based on MRC. At the eavesdropper side, we have studied the secrecy performance obtained by two receiving combining mechanisms, MMSE and ZF. Note that ZF is based in an 'intelligent' design that allows the attacker to mitigate and even cancel the jamming effect of the AN. Finally we have assumed that all the transmission parties use OFDM signalling as an effective way to cope with the frequency selective channel.

The simulation of the MIMO-OFDM system has allowed us to investigate the contribution of frequency selectivity to the secrecy of the communication. The observed results suggest that frequency selectivity can contribute positively to the secrecy of the system allowing an opportunistic power distribution among the best OFDM subcarriers to enhance the achievable secrecy rate. However, an eavesdropper equipped with a large number of antennas that is fully aware of the main link's CSI can mitigate the interference introduced by the AN by choosing an appropriate multiple-antenna combining methodology. These scenarios effectively highlight a major weaknesses to the secrecy of the MIMO-OFDM system when using masked bemforming as a secure transmission strategy.

Chapter 6

Joint AN generation for physical layer security in MIMO systems

> 'Because speaking about you is to exile myself into the landscapes that I remember, like trying to find the key of your voice within the dominions of a secret.'
>
> Manuel García

This chapter introduces a novel transmission scheme where both transmitter and receiver, each equipped with multiple-antennas, contribute to the secrecy by jointly generating artificial noise (AN). In contrast to the traditional masked transmission mechanism where only the multiple-antenna *transmitter* generates a jamming signal, here we investigated if a multiple-antenna *receiver* can also actively enhance the secrecy rate of the multiple-antenna wiretap channel by broadcasting AN. In order to do this, the receiver has to devote part of its receiving resources to jam the eavesdroppers. This fact introduces an interesting trade-off in terms of what is the best approach for secrecy: i) to use the full receiving capabilities by employing all the antennas to receive the information or ii) to devote some of the receiver resources, in the form of antennas and power, to jam possible eavesdroppers.

In this context, we consider a joint AN generation optimisation problem that will allow us to investigate the aforementioned trade-off and study under what

conditions it is useful to transmit AN and from which source(s). We study the joint AN generation problem from two perspectives. The first one considers the non-practical case where the perfect channel state information (CSI) of all the nodes is available. This scheme will allow us to understand the potential contribution of the joint AN generation technique. The second case considers the most practical scenario where the CSI is subject to errors due to the imperfect channel estimation/feedback process. Here we also consider passive eavesdroppers that remain hidden on the network. Both cases will shed light into whether it is useful to allocate resources of the multiple-antenna receiver for jamming eavesdroppers. Moreover, these cases will allow us to understand the criteria to choose the AN generation source and under what conditions this strategy can make a positive contribution to the secrecy of the multiple-antenna system compared to the traditional masked transmission scheme.

This chapter is organised as follows. Section 6.1 presents a review of the relevant literature in the context of the secrecy of the multiple-antenna wiretap channel and highlights the novel contribution of this chapter. Section 6.2 models the multiple-input multiple-output (MIMO) wiretap channel in the presence of multiple-antenna eavesdroppers to be used to formulate the joint AN transmission optimisation problem. In section 6.3 we study the secrecy performance of the joint AN generation technique subject to perfect CSI knowledge. Here we introduce two strategies to opportunistically select the receiver antenna configuration that offers the best secrecy performance. Subsequently, section 6.4 addresses the practical case where all the CSI between all the links are subject to errors introducing a robust worst-case secrecy rate maximisation and a power consumption minimisation strategies. Finally, section 6.5 concludes this chapter.

6.1 Joint transmitter/receiver AN generation

During recent years, the capabilities of the multiple-input multiple-output (MIMO) wireless channel have received remarkable attention as a way to secure wireless communications at the physical layer. The first works in this field exploited the degree of freedom that the MIMO wiretap channel introduces to secure the communication by enhancing the transmission over the main link and, at the same time, impairing multi-antenna eavesdroppers reception [34, 35, 48, 109]. These

works have shown that the MIMO Gaussian wiretap channel secrecy capacity is given by

$$\mathrm{C}_S = \max_{\mathbf{C}_w \succeq \mathbf{0}, \mathrm{Tr}(\mathbf{C}_w) \leq P} \log_2 \det \left[\mathbf{I} + \mathbf{H}^H \mathbf{C}_w \mathbf{H}\right] - \log_2 \det \left[\mathbf{I} + \mathbf{G}^H \mathbf{C}_w \mathbf{G}\right] \quad (6.1)$$

where P is the total power budget, $\mathbf{C}_w$ is the covariance matrix of the transmit signal, $\mathbf{H}$ and $\mathbf{G}$ represent the MIMO main and eavesdropping channels respectively and the power of the AWGN is one; i,e., $\sigma^2 = 1$. Unfortunately, the aforementioned contributions do not determine the transmission scheme, given by the transmission covariance matrix $\mathbf{C}_w$, that can attain the secrecy capacity of the MIMO wiretap channel; i.e., the maximal transmission rate at which the information can be reliably decoded at the receiver while ensuring that the error rate at the eavesdropper cannot allow it to recover the message.

Determining the transmit covariance solution $\mathbf{C}_w$ for attaining the secrecy capacity of the MIMO wiretap channel is a challenging problem due to the nonconvex nature of maximising the expression in (6.1). In this context, many suboptimal attempts have been carried out to find the transmission scheme to enhance achievable MIMO wiretap secrecy rates [121, 122, 123, 124]. In contrast, Bustin et al. introduce in [110] a closed-form expression for determining $\mathbf{C}_w$ and the secrecy capacity of the MIMO Gaussian wiretap channel under an input covariance constraint. In other words, this work provided a valid expression for the secrecy capacity for any SNR but it is not applicable under an average total power constraint. This contribution offers an optimal transmit scheme by relaxing the average power constraint in (6.1) and setting a specific input covariance structure. Unfortunately, this scheme introduces non-desirable limits on the per-antenna power and transmit correlation structure in the resulting transmission strategy.

In order to find the secrecy capacity (C_S) subject to a total average power constraint, in [125] Fakoorian et al. study the rank properties of the optimal input covariance matrix $\mathbf{C}_w$ that achieves the secrecy capacity. These properties are derived from the channel matrices of the main and eavesdropping links and it is concluded that if $\mathbf{H}\mathbf{H}^H \preceq \mathbf{G}\mathbf{G}^H$ then the secrecy capacity is zero. In other words, if the wiretap channel is more capable than the main one, it is not possible to attain a positive secrecy capacity. Moreover, it is also shown that if $\mathbf{H}\mathbf{H}^H \succ \mathbf{G}\mathbf{G}^H$, then the optimal transmit covariance matrix $\mathbf{C}_w$ is full-rank; otherwise, it will be rank-deficient. These interesting insights about the relationship between the main

and eavesdropping channel lead to the introduction in [126] of the solution for the MIMO Gausssian Wiretap channel under an average power constraint when the input transmit covariance matrix is full-rank; i.e, when the channel's condition $\mathbf{H}\mathbf{H}^H \succ \mathbf{G}\mathbf{G}^H$ holds.

Subsequently, in [127, 128] the authors introduce the transmit covariance solution $\mathbf{C}_w$ required to attain the secrecy capacity of the MIMO Gaussian wiretap channel under a sum power constraint. In this remarkable contribution, Li et al. use an alternating optimisation approach that consists in an iterative process similar to water-filling to find the optimal $\mathbf{C}_w$ that delivers the C_S in (6.1). Here, the authors also study the AN aided scheme; i.e., a masked precoding transmission. Interestingly, it is shown that incorporating AN into the transmission does not offer any advantage in terms of a gain in secrecy rate for the case of one multi-antenna active eavesdropper; however, it turns out to be a very useful strategy to enhance the secrecy rate in the presence of multiple active eavesdroppers. Indeed, [128] proves that no-AN transmission is the secrecy capacity optimal achieving scheme for a single multiple-antenna fully determined (in terms of CSI) active eavesdropper.

It is worth pointing out that [128] has considered only the transmitter as a possible source of AN generation. Therefore, it is not know if an AN source different from the transmitter might enhance the secrecy rate of the multiple-antenna system. This AN source, external from the wiretap channel model, can be obtained from cooperative relays operating as jammers.

6.1.1 Cooperative jamming

An alternative way to achieve spatial degrees of freedom is to use cooperative techniques. Indeed, cooperative relaying techniques such as Decode and Forward (DF) and Amplify and Forward (AF) have been proposed in [98, 99, 129, 130, 131] either to secure single-antenna wireless communications at the physical layer or to enhance the security of multiple-antenna networks. Here the idea is to rely on cooperative nodes to emulate the effect of a multiple-antenna array to beamform the confidential information towards the intended receiver. In this context, Yang et al. propose in [132] a secure beamforming scheme by using AF relay networks in the presence of multiple eavesdroppers to maximise the secrecy rate while completely eliminating the information leakage to all eavesdroppers. By contrast, in

[99, 100, 101, 133, 134, 135] Cooperative Jamming (CJ) is used to enhance the secrecy rate by generating a jamming signal to confuse eavesdroppers from third-party sources (named cooperative jammers). This idea was originally proposed by Goel and Negi in [37] as an alternative to generate AN in single-antenna networks and so mask a confidential message. An application of these cooperative techniques is presented in [136] where the authors propose a joint cooperative beamforming and jamming scheme to enforce security in a cooperative network by using some nodes to beamform the information towards the intended receiver while other nodes jam the unknown eavesdroppers by CJ.

Cooperation for security has received significant interest from the research community as an interesting alternative to secure communications at the physical layer [97]. However, in contrast to multiple-antenna counterparts, they introduce important security issues arising from relying the security of the system on third-party cooperative nodes that might behave maliciously [137]. In this context the concepts of untrusted and friendly relays have been introduced to define the different degrees of trust within cooperative relays and therefore devise appropriate transmission strategies [138, 139].

Secure cooperation sums up another technical challenge to the system. Cooperative protocols require both synchronisation between the transmission/relaying parties and the availability of the global CSI at all the cooperative entities. This requirement represents an additional level of complexity compared to multi-antenna systems. This difficulty of realising secure cooperative networks has commonly been neglected in the literature and has not received much attention so far. Additionally, it is important to consider the willingness of the cooperative nodes to take part in securing a third party transmission. In other words, the relays might lack interest to compromise their resources by forwarding information and generating AN without receiving any benefit in return. Therefore, it is likely that cooperative relays are not interested in collaborating unless they receive some incentive for their cooperation. This fact again poses a threat for the security of the system. All these issues raise questions about the practicality of using cooperative techniques to secure wireless networks.

6.1.2 An artificial noise generating receiver

As described in the previous section, cooperative networks, and particularly cooperative jammers can contribute positively to the security of a network. Indeed, an AN interference generated from a physically different location than the transmitter's generates an additional difficulty for the eavesdropper to cancel or mitigate the AN. In this context, an alternative mechanism to exploit the potential security contribution of a third-party jamming node is highly desired, but without increasing the network complexity and not jeopardising the overall security of the transmission. This objective can be attained by considering a receiver that actively participates in the secure transmission strategy by generating AN. It is worth pointing out that the intended receiver is, alongside the transmitter, the main node interesting in preserving the confidentiality of the information; therefore, its contribution to guaranteeing the confidentiality of the transmission (in terms of committing resources) is very important.

The idea of a receiver generating AN to confuse eavesdroppers is very new. Li et al. introduce in [140] a scheme where a two-antenna legitimate receiver simultaneously transmits AN from one antenna and receives the confidential signal using the other one. Here, the receiver effectively masks the information conveyed by a single-antenna transmitter to prevent single-antenna eavesdropping attacks. Remarkably, this method is particularly useful when the receiver has more resources available that the transmitter and the eavesdropper is close to the receiver.

Even though the authors of [140] have shown the benefits of generating AN from the receiver in single-antenna networks, the most general case of a receiver generating AN in a multiple-antenna system has not been studied and remains as an open issue. Moreover, it is not known how does this technique compares to the optimal transmission scheme that attains secrecy capacity in the MIMO wiretap channel presented in [128].

6.1.3 Contribution of this chapter

This chapter's novel contribution is twofold. First, we study if the transmission of AN from the receiver can enhance security in multiple-antenna systems by proposing that both the transmitter and the receiver can jointly generate AN to confuse a multiple-antenna eavesdropper. The objective is to understand if, and

under what conditions, joint AN generation can enhance the MIMO wiretap channel's C_S. With this objective we formulate an optimisation problem that seeks to derive the transmission covariance matrices that maximise the secrecy rate in a globally power constrained system. The results suggest that a remarkable improvement in the secrecy rate can be achieved by generating AN solely from the receiver. This strategy becomes particularly useful when the eavesdropper's channel is better than the main link's counterpart. This scenario can occur when the eavesdropper is equipped with a large number of antennas and experiences better channel fading conditions than the legitimate channel, or when it is located close to the transmitter.

The second contribution of this chapter is to introduce a robust joint transmitter/receiver AN generation transmission strategy under uncertainty in all the transmission parties CSI links. Therefore, we seek the optimal transmission covariance matrices for the following two scenarios:

- to maximise the worst-case secrecy rate in global and individually power constrained systems for both active eavesdropping (subject to errors in the CSI eavesdropping link) and passive eavesdropping, and
- to minimise the use of the transmission power subject to ensuring a target worst-case secrecy rate.

We consider a mismatch in all the communication channels in order to formulate conservative or worst-case nonconvex optimisation problems which we approximate to tractable convex semidefinite programs (SDP). We study the trade-off between assigning the receiver's antennas to generate AN or to receive the information under multiple scenarios. The results suggest that that introducing flexibility in choosing the AN source improves the secrecy rate; indeed, broadcasting AN is particularly useful when the instantaneous eavesdropping link CSI is not available. The AN source depends upon the particular transmission conditions.

6.2 System model

In this section we model a MIMO system in the presence of a multiple-antenna eaveadropper. Following the standard wireless secrecy model, we name the transmitter, the legitimate receiver and the eavesdropper as 'Alice', 'Bob' and 'Eve'. They

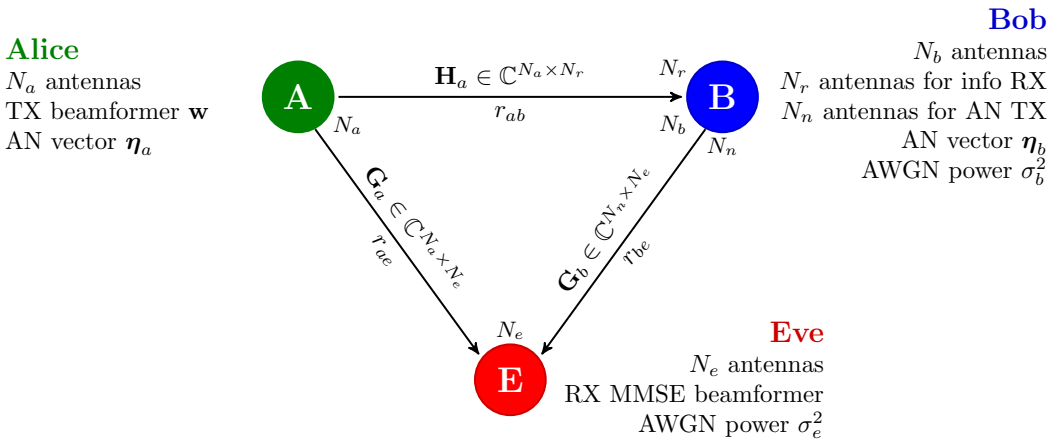


Figure 6.1: *System model of a MIMO system where AN is jointly generated by transmitter and receiver. The receiver Bob allocates N_r antennas for information reception and $N_n = N_b - N_r$ antennas for AN generation.*

are respectively equipped with $N_a \geq 2$, $N_b \geq 2$ and $N_e \geq 1$ antennas. The MIMO Alice-to-Bob and Alice-to-Eve channels are denoted by $\mathbf{H} \in \mathbb{C}^{N_a \times N_b}$ and $\mathbf{G}_a \in \mathbb{C}^{N_a \times N_e}$. We consider the path-loss effect in the channel modelling by setting $\mathbf{H} = r_{ab}^{-\frac{\alpha}{2}} \tilde{\mathbf{H}}$ and $\mathbf{G}_a = r_{ae}^{-\frac{\alpha}{2}} \tilde{\mathbf{G}}_a$ where r_{ab} and r_{ae} respectively denote the Alice-to-Bob and Alice-to-Eve distances, with $\alpha \geq 2$ being the path loss exponent, and $\tilde{\mathbf{H}} \sim \mathcal{CN}(\mathbf{0}, \sigma_{\tilde{H}}^2 \mathbf{I})$ and $\tilde{\mathbf{G}}_a \sim \mathcal{CN}(\mathbf{0}, \sigma_{\tilde{G}_a}^2 \mathbf{I})$ represents the independent small-scale fading of the Alice-to-Bob and Alice-to-Eve channels.

So, Bob receives the signal transmitted by Alice and, at the same time, transmits AN. Therefore, he allocates $N_r \geq 1$ antenna(s) for receiving information and $N_n = N_b - N_r$ antennas for AN generation. We denote the *actual* Alice-to-Bob channel by $\mathbf{H}_a \in \mathbb{C}^{N_a \times N_r}$, which is a subset of the full channel $\mathbf{H}$ consisting of only the N_r channel vectors associated with the information-receiving antennas. Similarly, we denote the Bob-to-Eve channel by $\mathbf{G}_b \in \mathbb{C}^{N_n \times N_e}$ which also considers the path-loss effect due to the Bob-to-Eve distance r_{be}; that is $\mathbf{G}_b = r_{be}^{-\frac{\alpha}{2}} \tilde{\mathbf{G}}_b$ where $\tilde{\mathbf{G}}_b \sim \mathcal{CN}(\mathbf{0}, \sigma_{\tilde{G}_b}^2 \mathbf{I})$. We depict this system in Figure 6.1.

Alice transmits a signal vector $\mathbf{s} \in \mathbb{C}^{N_a}$ given by $\mathbf{s} = \mathbf{w} + \boldsymbol{\eta}_a$ where $\mathbf{w}$ is the information steering vector using an idealised Gaussian codebook with covariance matrix $\mathbf{C}_w = \mathbb{E}\{\mathbf{w}\mathbf{w}^H\}$. On the other hand, $\boldsymbol{\eta}_a$ is Alice's AN vector with covariance matrix $\mathbf{C}_{\eta_a} = \mathbb{E}\{\boldsymbol{\eta}_a \boldsymbol{\eta}_a^H\}$. Likewise, Bob's AN vector is $\boldsymbol{\eta}_b \in \mathbb{C}^{N_n}$ with $\mathbf{C}_{\eta_b} = \mathbb{E}\{\boldsymbol{\eta}_b \boldsymbol{\eta}_b^H\}$. As in [140], we assume that the AN transmitted by Bob

is cancelled at his receiving antennas by using self-interference full duplex techniques [141]. It is worth pointing out that we assume that both legitimate transmission parties are aware of each other's transmission strategy; therefore, we let $P = \text{Tr}\{\mathbf{C}_w\} + \text{Tr}\{\mathbf{C}_{\eta_a}\} + \text{Tr}\{\mathbf{C}_{\eta_b}\}$ denote the global transmit power of the system.

We study the possible secrecy enhancements of jointly generating AN from 'both' or 'either' the transmitter and receiver compared to the classic MIMO wiretap channel secrecy capacity C_S in (6.1) where Bob acts as a passive receiver. Therefore, we assume that all the transmission parties' CSI and locations are known; therefore, the secrecy rate (in bps/Hz) of our system depicted in Figure 6.1 is

$$\text{R}_S = \left[\log_2 \det\left(\mathbf{I}_{N_r} + \mathbf{W}_1 \tilde{\mathbf{H}}_a^H \mathbf{C}_w \tilde{\mathbf{H}}_a\right) - \log_2 \det\left(\mathbf{I}_{N_e} + \mathbf{W}_2 \tilde{\mathbf{G}}_a^H \mathbf{C}_w \tilde{\mathbf{G}}_a\right)\right]^+ \tag{6.2}$$

where we define

$$\mathbf{W}_1 = \left[\tilde{\mathbf{H}}_a^H \mathbf{C}_{\eta_a} \tilde{\mathbf{H}}_a + r_{ab}^{\alpha} \sigma_b^2 \mathbf{I}_{N_r}\right]^{-1} \tag{6.3}$$

$$\mathbf{W}_2 = \left[\tilde{\mathbf{G}}_a^H \mathbf{C}_{\eta_a} \tilde{\mathbf{G}}_a + \rho^{\alpha} \tilde{\mathbf{G}}_b^H \mathbf{C}_{\eta_b} \tilde{\mathbf{G}}_b + r_{ae}^{\alpha} \sigma_e^2 \mathbf{I}_{N_e}\right]^{-1} \tag{6.4}$$

with $\rho = \frac{r_{ae}}{r_{be}}$ and σ_b^2 and σ_e^2 (respectively) the AWGN variances at the receiving antennas of both Bob and Eve.

6.3 Joint transmitter/receiver AN generation with perfect CSI

Our objective is to determine the transmission strategy that maximises the secrecy rate of the system by generating AN simultaneously from Alice and Bob in order to confuse a multiple-antenna Eve. In other words, we seek the information and AN transmission covariance matrices (from Bob and Alice) to maximise the secrecy rate. For the sake of fairness we consider the optimisation problem subject to a global power constraint P_{max}. This problem can be written as follow

$$\max_{\substack{\mathbf{C}_w, \mathbf{C}_{\eta_a}, \\ \mathbf{C}_{\eta_b}}} \quad \text{R}_S \tag{6.5a}$$

$$\text{s.t.} \quad P \leq P_{max} \tag{6.5b}$$

$$\mathbf{C}_w \succeq \mathbf{0}, \mathbf{C}_{\eta_a} \succeq \mathbf{0}, \mathbf{C}_{\eta_b} \succeq \mathbf{0}. \tag{6.5c}$$

The problem (6.5) is hard to solve due to the non-convex nature of the objective function in (6.2). Therefore, in the next section we introduce a sub-optimal approach based on MMSE to approximate (6.5) to an efficient solvable program that will shed light about the performance of the joint AN generation technique.

6.3.1 A QoS-MMSE approach to maximise the secrecy rate

As described in the previous chapter 5, published in [142, 143] and in [62, 63, 72, 95, 110, 111], we consider an MMSE approach only for Eve as a tractable pathway to study Eve's performance. This approach is potentially suboptimal by enforcing an MMSE combining receiver at Eve; however, this formulation will allow us to analyse the possible enhancements in secrecy from a joint AN strategy. In this context, we introduce the following metric $\bar{\mathrm{R}}_S$, as a suboptimal but tractable version of (6.2), as follows:

$$\bar{\mathrm{R}}_S = \left[\log_2 \det\left(\mathbf{I}_{N_r} + \mathbf{W}_1 \tilde{\mathbf{H}}_a^H \mathbf{C}_w \tilde{\mathbf{H}}_a\right) - \log_2\left(1 + \mathrm{SNR}_e\right)\right]^+ \tag{6.6}$$

where

$$\mathrm{SNR}_e = \mathrm{Tr}\left\{\tilde{\mathbf{G}}_a \mathbf{W}_2 \tilde{\mathbf{G}}_a^H \mathbf{C}_w\right\} \tag{6.7}$$

is the signal-to-noise ratio at Eve (SNR_e) after considering a MMSE combiner; i.e., Eve recovers the signal by using a MMSE receiver beamforming vector to maximise her SNR. As in[63, 72, 142], we consider the worst-case for security which assumes that Eve is perfectly aware of the transmission strategy given by $\mathbf{C}_w, \mathbf{C}_{\eta_a}, \mathbf{C}_{\eta_b}$.

We now maximise $\bar{\mathrm{R}}_S$, and so we rewrite the problem in (6.5) for the secrecy metric $\bar{\mathrm{R}}_S$ by introducing the slack variable β as follows

$$\max_{\substack{\mathbf{C}_w, \mathbf{C}_{\eta_a}, \\ \mathbf{C}_{\eta_b}, \beta}} \quad \log_2 \det\left(\mathbf{I}_{N_r} + \mathbf{W}_1 \tilde{\mathbf{H}}_a^H \mathbf{C}_w \tilde{\mathbf{H}}_a\right) - \log_2(\beta) \tag{6.8a}$$

$$\text{s.t.} \quad \log_2(\beta) \geq \log_2\left(1 + \mathrm{SNR}_e\right) \tag{6.8b}$$

$$P \leq P_{max} \tag{6.8c}$$

$$\mathbf{C}_w \succeq \mathbf{0}, \mathbf{C}_{\eta_a} \succeq \mathbf{0}, \mathbf{C}_{\eta_b} \succeq \mathbf{0}, \beta > 1. \tag{6.8d}$$

The problem above is still nonconvex due to the objective function in (6.8a); therefore, $\beta > 1$ is fixed to a given value, which is equivalent to introducing a Quality of Service (QoS) constraint to set the maximum admissible SNR_e at Eve.

This implies that the later problem has to be solved iteratively to find the QoS constraint β that delivers the largest $\bar{\mathrm{R}}_S$. Subsequently, we use the inequality

$$\det\left(\mathbf{I}+\mathbf{\Sigma}\right)=\prod_{i=1}^{r}\left(1+\lambda_i\right)\geq 1+\mathrm{Tr}(\mathbf{\Sigma}) \tag{6.9}$$

where $\mathbf{\Sigma}\succeq\mathbf{0}$, $r=\mathrm{rank}(\mathbf{\Sigma})$ and λ_i denotes the ith positive eigenvalue of $\mathbf{\Sigma}$. The equality in (6.9) holds iff $r=1$. Finally, we obtain the problem

$$\begin{aligned}
\max_{\substack{\mathbf{C}_w,\mathbf{C}_{\eta_a},\\ \mathbf{C}_{\eta_b}}} \quad & \frac{1}{\beta}\left(1+\mathrm{Tr}\left\{\mathbf{W}_1\tilde{\mathbf{H}}_a^H\mathbf{C}_w\tilde{\mathbf{H}}_a\right\}\right) && \text{(6.10a)}\\
\text{s.t.} \quad & \mathrm{Tr}\left\{\tilde{\mathbf{G}}_a\mathbf{W}_2\tilde{\mathbf{G}}_a^H\mathbf{C}_w\right\}\leq\beta-1 && \text{(6.10b)}\\
& P\leq P_{max} && \text{(6.10c)}\\
& \mathbf{C}_w\succeq\mathbf{0},\mathbf{C}_{\eta_a}\succeq\mathbf{0},\mathbf{C}_{\eta_b}\succeq\mathbf{0}. && \text{(6.10d)}
\end{aligned}$$

for a fixed value of β.

We now recast the problem in (6.10) as a SDP by using the Charness-Cooper transformation [104]. Therefore, we introduce the slack variable $\xi>0$ and define $\mathbf{C}_w=\frac{\tilde{\mathbf{C}}_w}{\xi}$, $\mathbf{C}_{\eta_a}=\frac{\tilde{\mathbf{C}}_{\eta_a}}{\xi}$ and $\mathbf{C}_{\eta_b}=\frac{\tilde{\mathbf{C}}_{\eta_b}}{\xi}$ to then set

$$\tilde{\mathbf{H}}_a^H\tilde{\mathbf{C}}_{\eta_a}\tilde{\mathbf{H}}_a+\xi r_{ab}^{\alpha}\sigma_b^2\mathbf{I}_{N_r}=\mathbf{I}_{N_r}. \tag{6.11}$$

Thus, we obtain the SDP

$$\begin{aligned}
\max_{\substack{\tilde{\mathbf{C}}_w,\tilde{\mathbf{C}}_{\eta_a},\\ \tilde{\mathbf{C}}_{\eta_b},\xi}} \quad & \frac{1}{\beta}\mathrm{Tr}\left\{\tilde{\mathbf{H}}_a^H\tilde{\mathbf{C}}_w\tilde{\mathbf{H}}_a\right\} && \text{(6.12a)}\\
\text{s.t.} \quad & \tilde{\mathbf{H}}_a^H\tilde{\mathbf{C}}_{\eta_a}\tilde{\mathbf{H}}_a+\left(\xi r_{ab}^{\alpha}\sigma_b^2-1\right)\mathbf{I}_{N_r}\preceq\mathbf{0} && \text{(6.12b)}\\
& \tilde{\mathbf{G}}_a^H\left[\left(\frac{\beta-1}{N_e}\right)\tilde{\mathbf{C}}_{\eta_a}-\tilde{\mathbf{C}}_w\right]\tilde{\mathbf{G}}_a+\\
& \left(\frac{\beta-1}{N_e}\right)\xi r_{ae}^{\alpha}\sigma_e^2\mathbf{I}_{N_e}+\left(\frac{\beta-1}{N_e}\right)\rho_k^{\alpha}\tilde{\mathbf{G}}_b^H\tilde{\mathbf{C}}_{\eta_b}\tilde{\mathbf{G}}_b\succeq\mathbf{0} && \text{(6.12c)}\\
& \mathrm{Tr}\left\{\tilde{\mathbf{C}}_w\right\}+\mathrm{Tr}\left\{\tilde{\mathbf{C}}_{\eta_a}\right\}+\mathrm{Tr}\left\{\tilde{\mathbf{C}}_{\eta_b}\right\}\leq\xi P_{max} && \text{(6.12d)}\\
& \mathbf{C}_w\succeq\mathbf{0},\mathbf{C}_{\eta_a}\succeq\mathbf{0},\mathbf{C}_{\eta_b}\succeq\mathbf{0},\xi\geq 0 && \text{(6.12e)}
\end{aligned}$$

where the linear matrix inequalities (LMIs) in (6.12b) and (6.12c) result from relaxing the equality in (6.11) and from replacing the definition of $\mathbf{W}_2$ from (6.4) into (6.12c). Finally, $\xi>0$ is relaxed to $\xi\geq 0$ without any consequence since $\xi=0$ is not feasible for (6.12d).

Table 6.1: *Bob's antenna configurations for $N_b = 3$. RX stands for a 'reception antenna' while AN represents 'AN generation'.*

Conf.	Antenna 1	Antenna 2	Antenna 3
1	RX	AN	AN
2	AN	RX	AN
3	AN	AN	RX
4	AN	RX	RX
5	RX	AN	RX
6	RX	RX	AN
7	RX	RX	RX

The SDP in (6.12) can be conveniently solved by using solvers based on interior-point algorithms such as SeDuMi [105] assisted by the parser toolboxes Yalmip [106] and CVX [107].

It is worth pointing out that the SDP (6.12) is solved for a fixed value of β. Therefore, an iterative exhaustive linear search algorithm, as used in chapter 4 §4.3.3 and in [143, 144], can also be used to find the value for β that delivers the largest $\bar{\mathrm{R}}_S$.

6.3.2 Numerical results

To illustrate the performance of the joint transmitter/receiver AN generation technique we consider a numerical example in which we set $N_a = N_b = N_e = 3$. As a result, there are $2^{N_b} - 1 = 7$ possible antenna configurations for Bob that are illustrated in the Table 6.1. This implies that, as explained in the system model in §6.2, in order to determine what is the Bob's best antenna configuration that delivers the largest $\bar{\mathrm{R}}_S$, we need to solve the SDP (6.12) for each one of the $2^{N_b} - 1 = 7$ possible channel configurations and then select the best configuration.

This is effectively done in the top plot of Figure 6.2 which depicts the maximum achieved $\bar{\mathrm{R}}_S$ of sixteen random channel realisations and the antenna configuration number (from Table 6.1) that attains it. This figure shows that joint AN generation can enhance the security of the system compared to the MIMO secrecy capacity C_S in [128] that uses all of Bob's antennas for reception; i.e., configuration 7 in Table 6.1. Also, we can see that the best antenna configuration for Bob changes

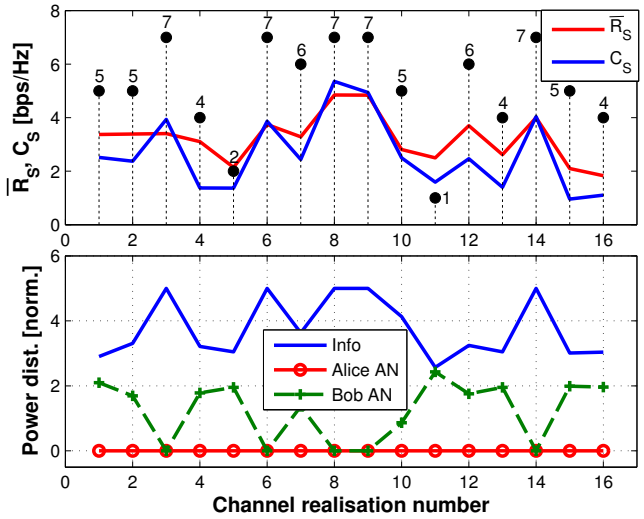


Figure 6.2: *Upper plot: secrecy analysis for 16 random channel realisations and Bob's best antenna configuration for* $r_{ab} = r_{ae} = r_{be} = 1$ *and* $N_a = N_b = N_e = 3$. *Lower plot: power allocation for a global power constraint* $P_{max} = 5$ *normalised relative to AWGN. The black numbered dots in the upper plot represent the best antenna configuration given in Table 6.1 for each channel realisation.*

across channel realisations. Remarkably, the power allocation (normalised relative to the AWGN power) depicted in the lower plot of Figure 6.2 suggests that transmitting AN from Alice is not necessary while broadcasting AN from Bob is useful to enhance $\bar{\mathrm{R}}_S$.

These remarkable results give rise to two main questions: i) under what circumstances is it convenient to transmit AN from Bob? ii) what is the antenna configuration that Bob should use to achieve the best security performance? We address these two questions in the following section by introducing two antenna configuration selection criteria that will not only offer answers to these two questions but also reduce substantially the complexity of the transmission technique.

6.3.3 Receiver's antenna configuration criteria

Although the potential benefits of Bob transmitting AN are now clear, analysing all the possible $2^{N_b} - 1$ antenna configurations at the receiver to maximise $\bar{\mathrm{R}}_S$ is a cumbersome task. Indeed for each antenna configuration, the problem in (6.12) needs to be solved. Therefore, it is desirable, in order to reduce the problem com-

plexity, to have a criterion to systematically choose the best configuration and solve the corresponding SDP in (6.12). This is not a trivial task, due to the existing trade-off between using all Bob's antennas for reception (to enhance the transmission rate in the main link) and increasing the number of Bob's antennas devoted for broadcasting a more directive AN to further jam Eve.

In this context, we now introduce two channel configuration mechanisms that will reduce the complexity of finding the best antenna configuration and also provide a useful insight into the problem nature. The objective here is to use alternative, low-complexity means to estimate in advance what would be the best antenna configuration. Once that this configuration has been determined, we will use it to solve the SDP in (6.12) and then opportunistically deliver the largest secrecy rate ($\bar{\mathrm{R}}_S$) that the instantaneous channel realisation might offer.

Degrees of freedom analysis

This criterion chooses the antenna configuration based on the analysis of the degrees of freedom (DoF) of the three wireless channels between Alice, Bob and Eve involved at the transmission. As pointed out in [125, 126, 128], the secrecy capability of the wiretap channel depends upon exploiting the DoF of $\mathbf{H}\mathbf{H}^H - \mathbf{G}_a\mathbf{G}_a^H$; indeed, the rank of the transmission covariance matrix corresponds to the number of positive eigenvalues of $\mathbf{H}\mathbf{H}^H - \mathbf{G}_a\mathbf{G}_a^H$. This implies that if $\mathbf{H}\mathbf{H}^H \preceq \mathbf{G}_a\mathbf{G}_a^H$ then achieving secrecy is not possible because the eavesdropping MIMO channel is more capable that the main one [125]. In this scenario, transmitting AN from Bob can be particularly useful in order to deteriorate Eve's signal quality thus allowing a positive $\bar{\mathrm{R}}_S$. As we consider AN generation from Bob, we carry out a similar analysis and then we take into account the DoF of $\mathbf{G}_b{}^H\mathbf{G}_b - \mathbf{G}_a{}^H\mathbf{G}_a$ that gives the *difference* between the channels that Eve sees for receiving the AN from Bob and the information from Alice.

We analyse all the possible $(2^{N_b} - 1)$ antenna configurations (defining the k^{th} configuration as $k \in [1, 2^{N_b} - 1]$) at Bob and consider the channels $\mathbf{H}_a^k \in \mathbb{C}^{N_a \times N_r^k}$ and $\mathbf{G}_b^k \in \mathbb{C}^{N_n^k \times N_e}$ between Alice-and-Bob and Bob-and-Eve where N_r^k and N_n^k are respectively the number of Bob's antennas for information reception and the number for AN generation in the k^{th} antenna configuration. Denote λ_i^k as the i^{th} positive eigenvalue of $\mathbf{H}_a^k\mathbf{H}_a^{k\,H} - \mathbf{G}_a\mathbf{G}_a^H$ and let μ_j^k be the j^{th} positive eigenvalue

of $\mathbf{G}_b^{k\,H}\mathbf{G}_b^k - \mathbf{G}_a{}^H\mathbf{G}_a$. Then we form two column vectors:

$$\boldsymbol{\delta}_a^k = \left[\lambda_1^k \cdots \lambda_i^k, 0, \cdots, 0\right]^T \in \mathbb{R}^{N_t} \tag{6.13}$$

$$\boldsymbol{\delta}_b^k = \left[\mu_1^k \cdots \mu_j^k, 0, \cdots, 0\right]^T \in \mathbb{R}^{N_e} \tag{6.14}$$

that we stack together (where $\alpha < 1$ is a weight for the vector $\boldsymbol{\delta}_b^k$). In other words, we form the matrix $\boldsymbol{\Delta} \in \mathbb{R}^{N_t+N_e \times 2^{N_b}-1}$ as follows:

$$\boldsymbol{\Delta} = \begin{bmatrix} \boldsymbol{\delta}_a^1 & \boldsymbol{\delta}_a^2 & \cdots & \boldsymbol{\delta}_a^k & \cdots & \boldsymbol{\delta}_a^{2^{N_b}-1} \\ \alpha\boldsymbol{\delta}_b^1 & \alpha\boldsymbol{\delta}_b^2 & \cdots & \alpha\boldsymbol{\delta}_b^k & \cdots & \alpha\boldsymbol{\delta}_b^{2^{N_b}-1} \end{bmatrix}. \tag{6.15}$$

Parameter α allows us to weight the contribution of the eigenvalues corresponding to the difference between AN and information received by Eve ($\boldsymbol{\delta}_b^k$) compared to those of the wiretap channel ($\boldsymbol{\delta}_a^k$). Subsequently, we perform the sum of the column vectors of the matrix $\boldsymbol{\Delta}$. The result of the sum is stored in a row vector $\bar{\boldsymbol{\delta}}_1$ where all its elements have been normalised by the maximum component of $\bar{\boldsymbol{\delta}}_1$ and sorted in descending order. Vector $\bar{\boldsymbol{\delta}}_1$ effectively represents the sorted channel configurations where the first element corresponds to the antenna configuration that delivers the best performance considering the DoF analysis presented here.

Eigen-transmission analysis

The second configuration selection criterion is based on the analysis of a suboptimal, but simple, eigen-transmission strategy for solving the problem (6.5). Again, we analyse all the possible $k \in [1, 2^{N_b} - 1]$ antenna configurations at Bob; that is, considering the k channels $\mathbf{H}_a^k$ and $\mathbf{G}_b^k$. Now, similar to the optimal MISO secrecy solution [46], we transmit using the beamforming vector $\mathbf{t}^k \in \mathbb{C}^{N_a}$ that corresponds to the principal eigenvector of the pencil $\left(\mathbf{I}_{N_a} + \mathbf{H}_a^k\mathbf{H}_a^{k\,H}, \mathbf{I}_{N_a} + \mathbf{G}_a\mathbf{G}_a{}^H\right)$. Therefore, we effectively simplify the problem by enforcing a suboptimal rank-one transmission scheme to evaluate the k different channel configurations to then select the best one and solve the SDP (6.12). Based on the results in §6.3.1, we do not consider AN generation from Alice; this strategy is consistent with the results reported in [46, 48, 109, 126, 128]. On the other hand, Bob steers the AN towards Eve by also beamforming the jamming signal over the direction of the principal eigenvector $\boldsymbol{\eta}^k \in \mathbb{C}^{N_n^k}$ associated to the largest eigenvalue of $\mathbf{G}_b^k\mathbf{G}_b^{k\,H}$. Hence, we consider again a potentially suboptimal rank-one transmission covariance matrix for Bob's AN. This strategy yields the following secrecy rate

$$\tilde{\mathrm{R}}_S^k = \log_2\left(1+\frac{\xi P_{max} r_{ab}^{-\alpha}\mathbf{t}^{k^H}\tilde{\mathbf{H}}_a^k\tilde{\mathbf{H}}_a^{k^H}\mathbf{t}^k}{\sigma_b^2}\right) - \log_2\left(1+\frac{\xi P_{max} r_{ae}^{-\alpha}\mathbf{t}^{k^H}\tilde{\mathbf{G}}_a\tilde{\mathbf{G}}_a^H\mathbf{t}^k}{(1-\xi)\,P_{max} r_{be}^{-\alpha}\boldsymbol{\eta}^{k^H}\tilde{\mathbf{G}}_b^k\tilde{\mathbf{G}}_b^{k^H}\boldsymbol{\eta}^k+\sigma_e^2}\right) \quad (6.16)$$

where $\xi \in (0,1]$ defines the global power distribution between Alice's transmitted information and Bob's AN. Subsequently, we maximise $\tilde{\mathrm{R}}_S$ over ξ. We write this problem as

$$\max_{0<\xi\leq 1} \frac{\left(\sigma_b^2+\xi P_{max}a^k\right)\left(P_{max}(1-\xi)c^k+\sigma_e^2\right)}{\sigma_b^2\left[(P_{max}(1-\xi)c^k+1)+\xi P_{max}b^k\right]} \quad (6.17)$$

where we define

$$a^k = r_{ab}^{-\alpha}\mathbf{t}^{k^H}\tilde{\mathbf{H}}_a^k\tilde{\mathbf{H}}_a^{k^H}\mathbf{t}^k \quad (6.18)$$

$$b^k = r_{ae}^{-\alpha}\mathbf{t}^{k^H}\tilde{\mathbf{G}}_a\tilde{\mathbf{G}}_a^H\mathbf{t}^k \quad (6.19)$$

$$c^k = r_{be}^{-\alpha}\boldsymbol{\eta}^{k^H}\tilde{\mathbf{G}}_b^k\tilde{\mathbf{G}}_b^{k^H}\boldsymbol{\eta}^k. \quad (6.20)$$

The power allocation problem in (6.17) can be efficiently solved by linear search algorithms, as has been done in §3.4.2 of chapter 3 in this thesis and also in [102]. Finally, for each k^{th} configuration we store the maximum value of $\tilde{\mathrm{R}}_S^k$ in a normalised decreasing-order vector $\bar{\boldsymbol{\delta}}_2$, similarly to what we have done for the normalised $\bar{\boldsymbol{\delta}}_1$. The first-element of the vector $\bar{\boldsymbol{\delta}}_2$ effectively corresponds to the antenna configuration that delivers the best performance using the eigen-transmission strategy.

Remark 6 *In the case where the selected antenna configuration for either method is to use all of Bob's antennas for reception ($N_r = N_b$), then the alternating optimisation strategy introduced in [128] offers the best performance due to the sub-optimality of our technique in §6.3.1.*

Remark 7 *When $\mathbf{H}\mathbf{H}^H - \mathbf{G}_a\mathbf{G}_a^H \succ \mathbf{0}$, i.e., all the eigenvalues are positive and non-zero, then broadcasting AN from Bob is not necessary as it cannot outperform the MIMO secrecy capacity C_S.*

In general, when the rank of the main channel is larger than the rank of the eavesdropping channel ($N_a > N_e$), there exists an effective null-space, and so the best configuration is to use the full degrees of freedom of the MIMO channel where all Bob's antennas are allocated for reception.

Remark 8 *It is advisable to set a threshold $\tau \in [0, 1]$ to define the channel configurations achieving a selection criterion performance larger than τ to be considered in the analysis.*

The two introduced selection strategies are based on approximation mechanisms and therefore they are not totally accurate, in particular, when the performance obtained from different antenna configurations is similar. In this scenario the differences between the elements within either of the vectors $\bar{\boldsymbol{\delta}}_1$ and $\bar{\boldsymbol{\delta}}_2$ corresponding to these configurations are small and could lead to not choosing the antenna configuration that delivers the largest secrecy rate. As a countermeasure, it is advisable (but optional) to set a threshold ($\tau \in [0, 1]$) to introduce into the analysis the channel configurations achieving a selection criterion performance larger than τ. We recall that the elements of $\bar{\boldsymbol{\delta}}_1$ and $\bar{\boldsymbol{\delta}}_2$ are ordered in descending magnitude starting from 1; therefore we will consider the elements larger or equal to τ that correspond to the selected antenna configurations. For example, we could analyse the secrecy performance offered by all the antenna configurations attaining a performance larger than than $\tau = 0.9$. This procedure improves the accuracy in selecting the best antenna configuration that will be used to solve the SDP (6.12) but increases the complexity of the strategy.

6.3.4 Numerical Results

Our analysis of the joint transmitter/receiver AN generation technique performance is based on both the average secrecy rate achieved ($\bar{\mathrm{R}}_S$) and the probability of achieving a joint AN generation's secrecy rate ($\bar{\mathrm{R}}_S$) larger than the MIMO wiretap channel secrecy capacity C_S. We also compare the performance delivered by the channel configuration selection strategies by looking at the level of accuracy in choosing the best channel configuration and the level of complexity associated with solving this the problem. We consider Monte Carlo simulations with setup values given in the Table 6.2.

First, we pay attention to the joint AN technique performance when the number of antennas at Eve increases. In Figure 6.3 we see that broadcasting AN from Bob is particularly useful when the eavesdropping channel's DoF increases. Indeed when $N_e < N_b$ our strategy is largely outperformed by the MIMO wiretap C_S in [128], therefore allocating Bob's resources for AN generation is useless. In

Table 6.2: *Simulation parameters setup.*

Parameter	Value	Description
N_a	3	Alice's number of antennas
N_b	3	Bob's number of antennas
$\sigma^2_{\tilde{H}_a}$	1	Alice-to-Bob's channel elements variance
$\sigma^2_{\tilde{G}_a}$	1	Alice-to-Eve's channel elements variance
$\sigma^2_{\tilde{G}_b}$	1	Bob-to-Eve's channel elements variance
σ^2_b	1	Bob's AWGN power
σ^2_e	1	Eve's AWGN power
P_{max}	5	Maximal power for constrained systems normalised relative to the noise power
α	2	Path loss exponent
r_{ab}	1	Alice-to-Bob normalised distance

contrast, when $N_e \geq N_b$, broadcasting AN from Bob is useful. Interestingly, joint AN generation yields the best performance at $N_e = 4$ because an eavesdropper equipped with a larger number of antennas can mitigate the effect of the AN thus reducing the effectiveness of an external interference.

We now turn our attention to the performance of the configuration selection strategies and their savings in complexity. As explained in remark 8, in order to increase the successful channel configuration selection rate (SCCSR) we consider a threshold τ to analyse the configurations that potentially might deliver a larger $\bar{\mathrm{R}}_S$. We study how τ affects the secrecy performance, the SCCSR and the associated complexity cost. Figure 6.4 shows that the eigen-transmission method is better than the DoF analysis across all the values considered for τ in terms of choosing the best channel configuration (SCCSR); however, the complexity associated is considerably higher. It is worth pointing out that we measure the complexity by calculating the ratio between the number of channel configurations chosen by the channel selection strategy above τ to the total number of possible channel configurations; i.e., $2^{N_b} - 1$. Interestingly, the eigen-transmission method outperforms C_S even when choosing $\tau \geq 0.9$. This behaviour is not found with the DoF analysis.

To analyse the effect of the location of the attacker on the security we consider a travelling eavesdropper moving in straight line from Alice towards Bob

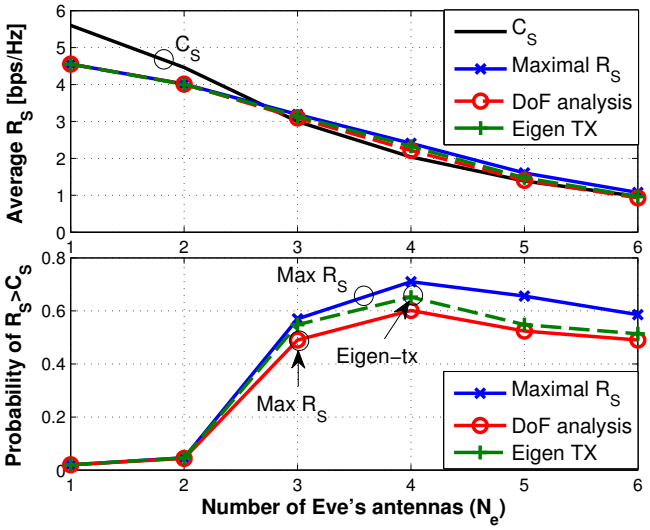


Figure 6.3: *System performance. Effect of the number of eavesdropper's antennas (N_e) on the average $\bar{R}_S$ and the probability of $\bar{R}_S > C_S$ for equidistant normalised receiving nodes distances $r_{ab} = r_{ae} = r_{be} = 1$ and $\tau = 0.75$ and $\tau = 0.85$ for the DoF and eigen-transmission strategies respectively.*

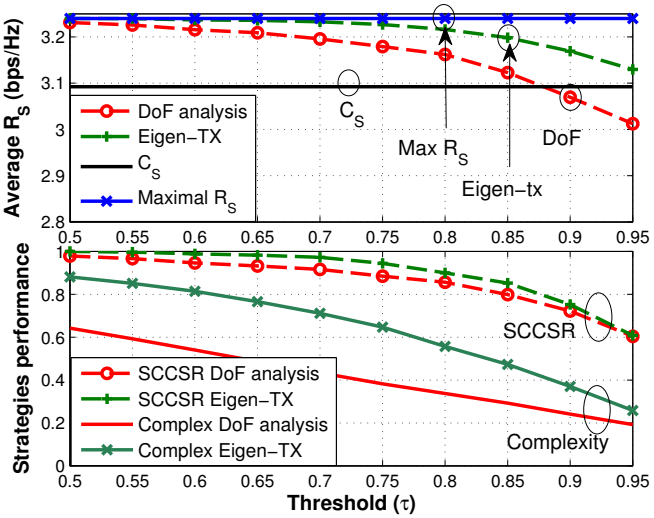


Figure 6.4: *Selection criteria performance. Effect of τ on the average secrecy rate $\bar{R}_S$ and the performance of antenna configuration selection strategy for equidistant normalised receiving nodes distances $r_{ab} = r_{ae} = r_{be} = 1$ when $N_e = 3$. Bottom figure shows both the successful channel configuration selection rate (SCCSR) and the associated complexity.*

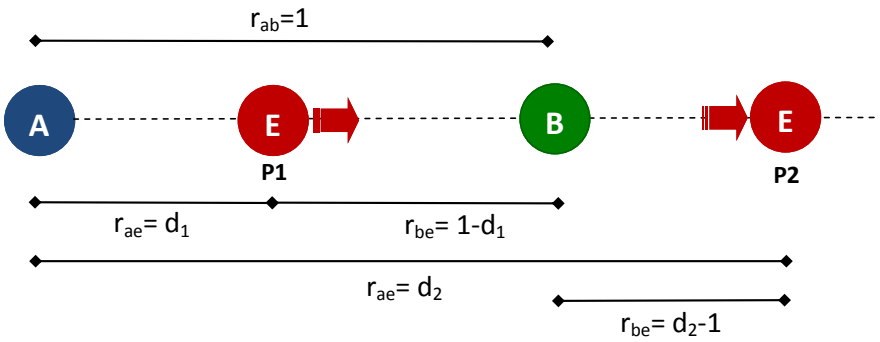


Figure 6.5: *A travelling Eve moving over a straight path from Alice towards Bob and beyond, when* $r_{ab} = 1$.

and beyond. This is depicted in Figure 6.5 where, based on a normalised Alice-to-Bob distance $r_{ab} = 1$, the Bob-to-Eve distance (r_{be}) can be easily inferred from the Alice-to-Eve distance (r_{ae}). For example, when Eve is moving from Alice towards Bob; i.e., $r_{ae} = d_1 < r_{ab}$; then $r_{be} = 1 - d_1$ (P1 in Figure 6.5). When Eve is travelling beyond Bob then $r_{ae} = d_2 > r_{ab}$ and $r_{be} = d_2 - 1$ (P2 in Figure 6.5). For the sake of clarity, in Figure 6.6 we only consider in the x-axes the Alice-to-Eve distance, so Bob-to-Eve's distance can be obtained as explained; e.g., $r_{ae} = 0.25 \Rightarrow r_{be} = 0.75; r_{ae} = 1 \Rightarrow r_{be} \to 0; r_{ae} = 1.25 \Rightarrow r_{be} = 0.25$. It is worth pointing out that the distances between nodes are relative to r_{ab}.

Figure 6.6 shows the possible improvements in terms of achievable secrecy rate by broadcasting AN from Bob when Eve is moving as described above. The gap between the maximal achievable $\bar{\mathrm{R}}_S$ and the MIMO wiretap channel C_S is larger when the attacker is closer to Alice due to the positive effect of jointly broadcasting AN that counters the smaller path losses that the eavesdropping link suffers under this condition. This gap decreases for $r_{ae} > r_{ab}$ meaning that it is not so useful generating AN from Bob under this scenario because the eavesdropping channel is already poor due to large path loses owing to Eve's large distance from Alice. This behaviour is confirmed in the lower plot in Figure 6.6 where the probability that the $\bar{\mathrm{R}}_S$ achieved by the joint AN strategy outperforms C_S is almost one when Eve is close to Alice. This proves that the generation of AN from Bob is particularly useful when Eve is under favourable channel conditions compared to the main link. Figure 6.6 also illustrates the good performance of the DoF and

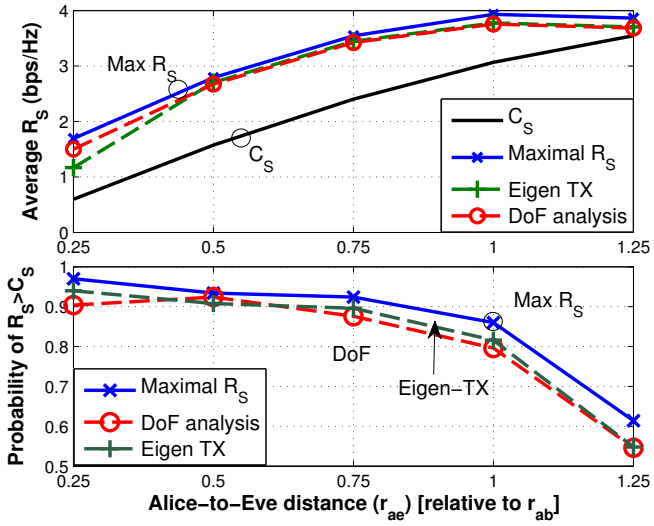


Figure 6.6: *System performance. Effect of the proximity of the eavesdropper on the average $\bar{R}_S$ and the probability of $\bar{R}_S > C_S$ when normalised $r_{ab} = 1$ and $N_e = 3$. τ for the DoF and eigen-transmission analysis has been set to 0.5 and 0.95 respectively.*

eigen-transmission strategies to select Bob's channel configuration. Here, again the eigen-transmission approach is the one that delivers the best performance.

In summary, in this section we have shown that the receiver can enhance the secrecy of the multiple antenna wiretap channel by transmitting AN from some of its antennas. Our study has proved that a judicious selection of the receiver's antennas to broadcast AN can provide a larger secrecy rate compared to the secrecy capacity C_S obtained when the receiver purely receives the information. In the next section, we study the performance of the joint transmitter/receiver AN generation technique under the realistic scenario where the CSI available at the nodes is either subject to errors or is not available.

6.4 Robust joint transmitter/receiver AN generation

In this section we consider a MIMO system where both Alice and Bob have available a mismatched version of all the transmission parties' CSI. We also draw attention to the practical case when the legitimate transmission parties are not aware of the presence of silent eavesdroppers hidden in the network. We refer to the

former scenario as active eavesdropping with partial information regarding the eavesdropping channel and the latter case as passive eavesdropping. In addition, we now consider that the transmission is overheard by K multiple non-colluding single-antenna eavesdroppers; therefore, here we do not enforce an MMSE approach as in §6.3.1. In order to concentrate our analysis in the performance of the joint AN generation technique, we study the average performance of many channel realisations instead of taking advantage of the particular channel conditions. In other words, in this section we do not consider a different antenna receiving configuration at Bob for each channel realisation as was done in §6.3.3. In contrast, here we study the average performance over many realisations that the joint AN generation technique offers for different antenna configurations.

In this context, we consider that Alice and Bob are equipped with $N_a \geq 2$ and $N_b \geq 2$ antennas while the k^{th} Eve is a single-antenna node. We take into account the same consideration regarding Bob's full-duplex capabilities; therefore, he uses $N_r \geq 1$ antennas to receive information and $N_n = N_b - N_r$ antennas to broadcast AN. As in §6.2, the effective MIMO Alice-to-Bob channel is a subset of the full channel $\mathbf{H}$ and it is denoted by $\mathbf{H}_a \in \mathbb{C}^{N_a \times N_r}$. Now, we denote the mutually independent Alice-to-the k^{th} Eve and Bob-to-the k^{th} Eve vector channels as $\mathbf{g}_{a_k} \in \mathbb{C}^{N_a}$ and $\mathbf{g}_{b_k} \in \mathbb{C}^{N_n}$. Here, we again consider separately the small-scale fading channels, $\tilde{\mathbf{g}}_{a_k} \sim \mathcal{CN}(\mathbf{0}, \sigma^2_{\tilde{g}_a}\mathbf{I})$ and $\tilde{\mathbf{g}}_{b_k} \sim \mathcal{CN}(\mathbf{0}, \sigma^2_{\tilde{g}_b}\mathbf{I})$, and the path-loss effect due to the free-space propagation over the distances from Alice and Bob to the kth Eve given respectively by r_{ae_k} and r_{be_k} with $k = 1, \cdots, K$. The system is depicted in Figure 6.7.

We follow the transmission scheme detailed in §6.2; therefore, Alice transmits a signal vector $\mathbf{s} = \mathbf{w} + \boldsymbol{\eta}_a$ formed by the steering information and the AN components. The transmission vector covariance matrix is $\mathbf{C}_w$ while Alice's AN covariance matrix is $\mathbf{C}_{\eta_a}$. Bob's AN vector is $\boldsymbol{\eta}_b$ with covariance matrix $\mathbf{C}_{\eta_b}$. Let $P = \text{Tr}\{\mathbf{C}_w\} + \text{Tr}\{\mathbf{C}_{\eta_a}\} + \text{Tr}\{\mathbf{C}_{\eta_b}\}$ denote the total transmit power of the system.

The received signals at Bob and the k^{th} Eve are respectively

$$\mathbf{y}_b = r_{ab}^{-\frac{\alpha}{2}} \tilde{\mathbf{H}}_a^H \mathbf{w} + r_{ab}^{-\frac{\alpha}{2}} \tilde{\mathbf{H}}_a^H \boldsymbol{\eta}_a + \mathbf{n}_b \tag{6.21}$$

$$y_{e_k} = r_{ae_k}^{-\frac{\alpha}{2}} \tilde{\mathbf{g}}_{a_k}^H \mathbf{w} + r_{ae_k}^{-\frac{\alpha}{2}} \tilde{\mathbf{g}}_{a_k}^H \boldsymbol{\eta}_a + r_{be_k}^{-\frac{\alpha}{2}} \tilde{\mathbf{g}}_{b_k}^H \boldsymbol{\eta}_b + n_{e_k} \tag{6.22}$$

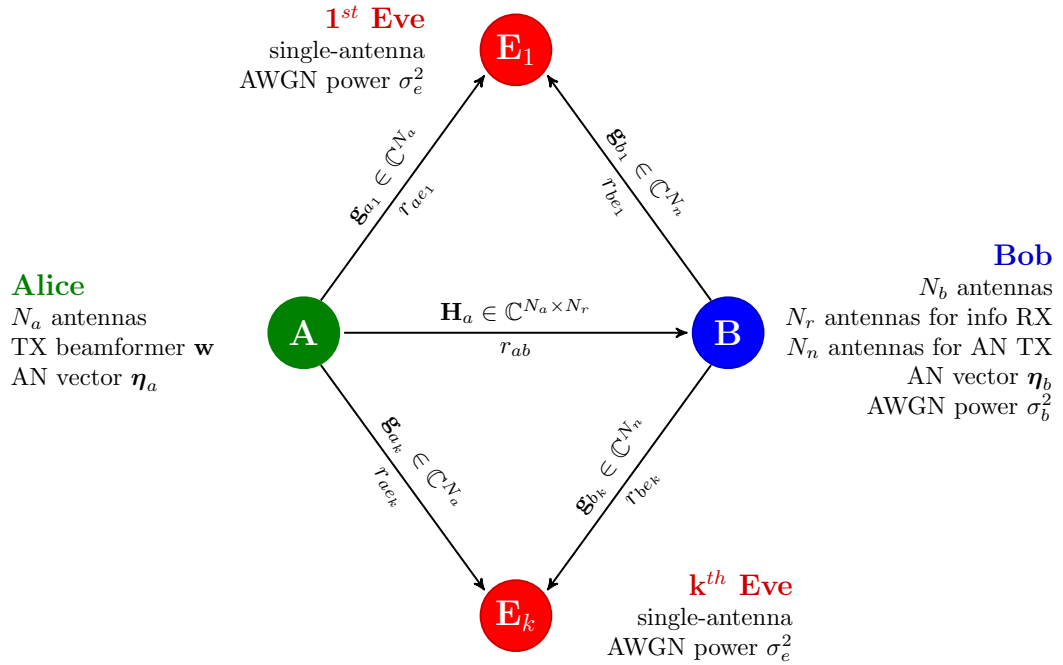


Figure 6.7: *System model of a MIMO configuration where AN is jointly generated by the transmitter and the receiver in the presence of multiple single-antenna eavesdroppers.*

where $\mathbf{n}_b \in \mathbb{C}^{N_r}$ and $n_{e_k} \in \mathbb{C}$ are independent AWGN such that $\mathbf{n}_b \sim \mathcal{CN}(\mathbf{0}, \sigma_b^2\mathbf{I})$ and $n_{e_k} \sim \mathcal{CN}(0, \sigma_e^2)$. For this system, the secrecy rate (in bps/Hz) is

$$\mathrm{R}_S = \left[\log_2 \det\left(\mathbf{I}_{N_r} + \mathbf{W}\tilde{\mathbf{H}}_a^H \mathbf{C}_w \tilde{\mathbf{H}}_a\right) - \max_{k=1,\cdots,K} \log_2\left(1+\omega_k\right)\right]^+ \tag{6.23}$$

where we define

$$\mathbf{W} = \left[\tilde{\mathbf{H}}_a^H \mathbf{C}_{\eta_a} \tilde{\mathbf{H}}_a + r_{ab}^{\alpha}\sigma_b^2 \mathbf{I}_{N_r}\right]^{-1} \tag{6.24}$$

$$\omega_k = \frac{\tilde{\mathbf{g}}_{a_k}^H \mathbf{C}_w \tilde{\mathbf{g}}_{a_k}}{\tilde{\mathbf{g}}_{a_k}^H \mathbf{C}_{\eta_a} \tilde{\mathbf{g}}_{a_k} + \rho_k^{\alpha} \tilde{\mathbf{g}}_{b_k}^H \mathbf{C}_{\eta_b} \tilde{\mathbf{g}}_{b_k} + r_{ae_k}^{\alpha}\sigma_e^2} \tag{6.25}$$

and $\rho_k = \frac{r_{ae_k}}{r_{be_k}}$ is the ratio between the Alice-to-the k^{th} Eve and Bob-to-the k^{th} Eve distances.

6.4.1 Robust transmission strategy

Our transmission model considers the practical assumption that Alice and Bob only have available a mismatched version of all the transmission parties' CSI.

Therefore, and similarly as in §4.2.1 of chapter 4, we use a deterministic robust model to consider the worst-case for the security. Therefore, the actual instantaneous channel lies within a known set of uncertainty values whose range represents the amount of uncertainty about the channel. This robust design leads to worst-case formulations that achieve a given performance for any channel realisation within the defined set [84]. The channel errors are defined as

$$\begin{aligned}
&\boldsymbol{\Delta} = \tilde{\mathbf{H}}_a - \hat{\mathbf{H}}_a, \text{ s.t. } \boldsymbol{\Delta} \in \boldsymbol{\xi}_{ab} = \{\boldsymbol{\Delta} : ||\boldsymbol{\Delta}||_F \leq \epsilon_{ab}\} \\
&\boldsymbol{\delta}_{a_k} = \tilde{\mathbf{g}}_{a_k} - \hat{\mathbf{g}}_{a_k}, \text{ s.t. } \boldsymbol{\delta}_{a_k} \in \boldsymbol{\xi}_{ae} = \{\boldsymbol{\delta}_{a_k} : ||\boldsymbol{\delta}_{a_k}|| \leq \epsilon_{ae}\} \\
&\boldsymbol{\delta}_{b_k} = \tilde{\mathbf{g}}_{b_k} - \hat{\mathbf{g}}_{b_k}, \text{ s.t. } \boldsymbol{\delta}_{b_k} \in \boldsymbol{\xi}_{be} = \{\boldsymbol{\delta}_{b_k} : ||\boldsymbol{\delta}_{b_k}|| \leq \epsilon_{be}\}
\end{aligned} \tag{6.26}$$

where $\hat{\mathbf{H}}_a$, $\hat{\mathbf{g}}_{a_k}$ and $\hat{\mathbf{g}}_{b_k}$ are the observed mismatched versions of the small-scale fading Alice-to-Bob, Alice-to-the k^{th} Eve and Bob-to-the k^{th} Eve channels. The errors $\boldsymbol{\Delta}$, $\boldsymbol{\delta}_{a_k}$ and $\boldsymbol{\delta}_{b_k}$ are unknown to Alice and Bob but lie within the deterministic sets ξ_{ab}, ξ_{ae} and ξ_{be} defined by the known values ϵ_{ab}, ϵ_{ae} and ϵ_{be}.

Once we have considered the above robust formulation, we define the worst-case secrecy rate (R_S^{wc}) as the lower-bound secrecy rate that our strategy can deliver for any channel uncertainty within the defined deterministic sets. This security metric is given by

$$\mathrm{R}_S^{wc} = \left[\min_{\boldsymbol{\Delta} \in \xi_{ab}} \log_2 \det \left(\mathbf{I}_{N_r} + \mathbf{W} \tilde{\mathbf{H}}_a^H \mathbf{C}_w \tilde{\mathbf{H}}_a \right) - \max_{k=1,\cdots,K} \max_{\substack{\boldsymbol{\delta}_{a_k} \in \boldsymbol{\xi}_{ae}, \\ \boldsymbol{\delta}_{b_k} \in \boldsymbol{\xi}_{be}}} \log_2 (1 + \omega_k) \right]^+ \tag{6.27}$$

where $\mathbf{W}$ and ω_k are defined in (6.24) and (6.25).

6.4.2 Robust worst-case secrecy rate maximisation

In this section we maximise the worst-case secrecy rate R_S^{wc} subject to deterministic errors in all the transmission channel signatures when both multiple antenna nodes, transmitter and receiver, can generate AN. This scenario can be seen as an active eavesdropping case where the legitimate communication parties have available partial knowledge of the eavesdroppers' CSI. In addition, we also consider the pure passive eavesdropping case where the transmitter and receiver use statistics regarding the eavesdropping channels. It is important to note that our model also assumes errors on the main channel that can be due to errors in the feedback process.

Regarding the power availability, two different network setups are studied. The first one considers that the network is globally power constrained while the second case is focused on the most practical scenario where transmitter and receiver have individual power budgets. The first setup represents the most challenging problem from the optimisation point of view owing to the fact that a joint optimisation process has to be carried out on both nodes, requiring a smart distribution of the total available power. Despite the complexity, as stated in §6.3, this case allows us to present a fair performance benchmarking against techniques generating AN solely from Alice. On the other hand, the individually constrained network reflects a practical situation in which each node has a given amount of power available and therefore a joint optimisation in terms of power distribution is not required. In the following, we study in detail both scenarios.

Globally constrained network

We aim to find the transmission covariance matrices $\mathbf{C}_w$, $\mathbf{C}_{\eta_a}$, and $\mathbf{C}_{\eta_b}$ to maximise R_S^{wc} in (6.27) in a globally power constrained system. Therefore, we write this problem as

$$\max_{\mathbf{C}_w, \mathbf{C}_{\eta_a}, \mathbf{C}_{\eta_b}} \quad \mathrm{R}_S^{wc} \tag{6.28a}$$

$$\text{s.t. } \mathbf{C}_w \succeq \mathbf{0}, \mathbf{C}_{\eta_a} \succeq \mathbf{0}, \mathbf{C}_{\eta_b} \succeq \mathbf{0} \tag{6.28b}$$

$$P \leq P_{max} \tag{6.28c}$$

where P_{max} is the total global available power.

Optimising the above problem is challenging due to the nonconvex nature of the objective function (6.28a). Therefore, as a first step to recast this problem into a tractable expression, we introduce the slack variable β, that, by the epigraph form [87, §4.1.3], allows us to split R_S^{wc} in (6.27) into two terms. Thus, (6.28) becomes

$$\max_{\substack{\mathbf{C}_w, \mathbf{C}_{\eta_a}, \\ \mathbf{C}_{\eta_b}, \beta}} \min_{\boldsymbol{\Delta} \in \xi_{ab}} \log_2 \det \left(\mathbf{I}_{N_r} + \mathbf{W} \tilde{\mathbf{H}}_a^H \mathbf{C}_w \tilde{\mathbf{H}}_a \right) - \log_2 \beta \tag{6.29a}$$

$$\text{s.t. } \max_{\substack{\boldsymbol{\delta}_{a_k} \in \boldsymbol{\xi}_{ae}, \\ \boldsymbol{\delta}_{b_k} \in \boldsymbol{\xi}_{be}}} (1 + \omega_k) \leq \beta, \forall k = 1, \cdots, K \tag{6.29b}$$

$$\mathbf{C}_w \succeq \mathbf{0}, \mathbf{C}_{\eta_a} \succeq \mathbf{0}, \mathbf{C}_{\eta_b} \succeq \mathbf{0} \tag{6.29c}$$

$$P \leq P_{max}, \beta > 1. \tag{6.29d}$$

Problem (6.29) is still nonconvex and so we need first to find an approximation for the objective function (6.29a) to later approximate it as a convex function. Therefore, we use the inequality in (6.9) to relax (6.29a) and set a mathematical tractable lower-bound for our security performance metric in (6.27). This relaxation potentially might lead to a suboptimal solution but it allows us to deal with the problem in an efficient and tractable fashion. The problem becomes

$$\max_{\substack{\mathbf{C}_w,\mathbf{C}_{\eta_a},\\ \mathbf{C}_{\eta_b},\beta}} \quad \min_{\boldsymbol{\Delta}\in\xi_{ab}} \frac{1}{\beta}\left(1+\mathrm{Tr}\left\{\mathbf{W}\tilde{\mathbf{H}}_a^H\mathbf{C}_w\tilde{\mathbf{H}}_a\right\}\right) \tag{6.30a}$$

$$\text{s.t.} \quad \max_{\substack{\boldsymbol{\delta}_a\in\boldsymbol{\xi}_{ae},\\ \boldsymbol{\delta}_b\in\boldsymbol{\xi}_{be}}} \omega_k \leq \beta-1, \forall k=1,\cdots,K \tag{6.30b}$$

$$\mathbf{C}_w \succeq \mathbf{0}, \mathbf{C}_{\eta_a} \succeq \mathbf{0}, \mathbf{C}_{\eta_b} \succeq \mathbf{0} \tag{6.30c}$$

$$P \leq P_{max}, \beta > 1. \tag{6.30d}$$

The relaxed problem (6.30) is still nonconvex and so we fix the slack variable β to an arbitrary value. By doing this, (6.30b) effectively sets the maximum allowed signal-to-noise ratio (SNR) at the Eves; therefore, we implicitly optimise the problem for a Quality-of-Service (QoS) level such as in §3.3 of chapter 3 and in [53, 59, 72, 103]. By contrast, here we are interested in maximising the secrecy rate irrespective of Eves' QoS; therefore, we look for the optimum $\beta^\star$ that delivers the largest R_S^{wc}. Although the QoS problem can be solved straightforwardly, it fixes the system performance to a QoS metric thus limiting the security performance of the technique. On the other hand, our endeavour offers the best security performance at the cost of introducing an extra level of complexity.

Now, we turn our attention to transforming the above nonconvex problem into an SDP. First, we use the Charnes-Cooper transformation [104] to deal with the term within the trace operator in (6.30a), and so we introduce the slack variable $\xi > 0$ to define $\mathbf{C}_w = \frac{\tilde{\mathbf{C}}_w}{\xi}$, $\mathbf{C}_{\eta_a} = \frac{\tilde{\mathbf{C}}_{\eta_a}}{\xi}$ and $\mathbf{C}_{\eta_b} = \frac{\tilde{\mathbf{C}}_{\eta_b}}{\xi}$. We obtain the following problem

$$\max_{\substack{\tilde{\mathbf{C}}_w,\tilde{\mathbf{C}}_{\eta_a},\\ \tilde{\mathbf{C}}_{\eta_b},\xi}} \quad \min_{\boldsymbol{\Delta}\in\xi_{ab}} \mathrm{Tr}\left\{\tilde{\mathbf{W}}\tilde{\mathbf{H}}_a^H\frac{\tilde{\mathbf{C}}_w}{\beta}\tilde{\mathbf{H}}_a\right\} \tag{6.31a}$$

$$\text{s.t.} \quad \max_{\substack{\boldsymbol{\delta}_{a_k}\in\boldsymbol{\xi}_{ae},\\ \boldsymbol{\delta}_{b_k}\in\boldsymbol{\xi}_{be}}} \frac{\tilde{\mathbf{g}}_{a_k}^H\tilde{\mathbf{C}}_w\tilde{\mathbf{g}}_{a_k}}{\tilde{\mathbf{g}}_{a_k}^H\tilde{\mathbf{C}}_{\eta_a}\tilde{\mathbf{g}}_{a_k}+\rho_k^\alpha\tilde{\mathbf{g}}_{b_k}^H\tilde{\mathbf{C}}_{\eta_b}\tilde{\mathbf{g}}_{b_k}+\xi r_{be_k}^\alpha\sigma_e^2} \leq \beta-1, \forall k=1,\cdots,K \tag{6.31b}$$

$$\text{Tr}\left\{\tilde{\mathbf{C}}_w\right\} + \text{Tr}\left\{\tilde{\mathbf{C}}_{\eta_a}\right\} + \text{Tr}\left\{\tilde{\mathbf{C}}_{\eta_b}\right\} \leq \xi P_{max} \tag{6.31c}$$

$$\tilde{\mathbf{C}}_w \succeq \mathbf{0}, \tilde{\mathbf{C}}_{\eta_a} \succeq \mathbf{0}, \tilde{\mathbf{C}}_{\eta_b} \succeq \mathbf{0}, \xi > 0 \tag{6.31d}$$

where, as in (6.24), we define $\tilde{\mathbf{W}} = \left[\tilde{\mathbf{H}}_a^H \tilde{\mathbf{C}}_{\eta_a} \tilde{\mathbf{H}}_a + \xi r_{ab}^{\alpha} \sigma_b^2 \mathbf{I}_{N_r}\right]^{-1}$.

We relax the above *maximin* problem by introducing into the problem the inequality

$$\tilde{\mathbf{H}}_a^H \tilde{\mathbf{C}}_{\eta_a} \tilde{\mathbf{H}}_a + \xi r_{ab}^{\alpha} \sigma_b^2 \mathbf{I}_{N_r} \preceq \mathbf{I}_{N_r} \tag{6.32}$$

that allows us to effectively split the objective function in (6.31a) leading to a new constraint resulting from the Charnes-Cooper transformation. We point out that when $\mathbf{\Sigma} \preceq \mathbf{\Phi}$ then it holds that $\text{Tr}\{\mathbf{\Sigma}\} \leq \text{Tr}\{\mathbf{\Phi}\}$, and so the problem can be written as

$$\max_{\substack{\tilde{\mathbf{C}}_w, \tilde{\mathbf{C}}_{\eta_a}, \\ \tilde{\mathbf{C}}_{\eta_b}, \xi}} \min_{\mathbf{\Delta} \in \xi_{ab}} \text{Tr}\left\{\tilde{\mathbf{H}}_a^H \frac{\tilde{\mathbf{C}}_w}{\beta} \tilde{\mathbf{H}}_a\right\} \tag{6.33a}$$

$$\text{s.t.} \max_{\mathbf{\Delta} \in \xi_{ab}} \text{Tr}\left\{\tilde{\mathbf{H}}_a^H \tilde{\mathbf{C}}_{\eta_a} \tilde{\mathbf{H}}_a + \xi r_{ab}^{\alpha} \sigma_b^2 \mathbf{I}_{N_r}\right\} \leq \text{Tr}\{\mathbf{I}_{N_r}\} \tag{6.33b}$$

where the constraints (6.31b), (6.31c), and (6.31d) still hold.

It is easy to see that the relaxation introduced in the previous step is tight when the equality in (6.33b) holds. Now, we use the definition of the Frobenius norm to rewrite the deterministic uncertainty set definition as follows

$$\mathbf{\Delta} \in \boldsymbol{\xi}_{ab} = \{\mathbf{\Delta} : ||\mathbf{\Delta}||_F \leq \epsilon_{ab}\} = \left\{\mathbf{\Delta} : \text{Tr}\left\{\mathbf{\Delta}^H \mathbf{\Delta}\right\} \leq \epsilon_{ab}^2\right\}. \tag{6.34}$$

Now, we use the well-known vectorisation property $\text{Tr}\left\{\mathbf{\Delta}^H \mathbf{\Delta}\right\} = \boldsymbol{\delta}^H \boldsymbol{\delta}$, where $\boldsymbol{\delta} = \text{vec}\{\mathbf{\Delta}\}$ is the vectorised version of the error matrix channel. We recall from (6.26) that the actual channel is given by $\tilde{\mathbf{H}}_a = \hat{\mathbf{H}}_a + \mathbf{\Delta}$. Therefore, we consider the vectorised version of the actual channel $\tilde{\mathbf{h}}_a = \hat{\mathbf{h}}_a + \boldsymbol{\delta}$, where $\tilde{\mathbf{h}}_a = \text{vec}\left\{\tilde{\mathbf{H}}_a\right\}$. Now, we can write (6.33a) as

$$\max_{\substack{\tilde{\mathbf{C}}_w, \tilde{\mathbf{C}}_{\eta_a}, \\ \tilde{\mathbf{C}}_{\eta_b}, \xi}} \min_{\mathbf{\Delta} \in \xi_{ab}} \left[\hat{\mathbf{h}}_a + \boldsymbol{\delta}\right]^H \left(\mathbf{I}_{N_r} \otimes \frac{\tilde{\mathbf{C}}_w}{\beta}\right) \left[\hat{\mathbf{h}}_a + \boldsymbol{\delta}\right]. \tag{6.35}$$

Subsequently, we lower-bound the minimum value for the inner minimisation in (6.35) by the slack variable $u \geq 0$, and then we expand the objective function to yield

$$\max_{\substack{\tilde{\mathbf{C}}_w, \tilde{\mathbf{C}}_{\eta_a}, \\ \tilde{\mathbf{C}}_{\eta_b}, \xi, u}} \quad u \tag{6.36a}$$

$$\text{s.t. } -\boldsymbol{\delta}^H\mathbf{A}\boldsymbol{\delta} - 2\text{Re}\left\{\hat{\mathbf{h}}_a^H\mathbf{A}\boldsymbol{\delta}\right\} - \hat{\mathbf{h}}_a^H\mathbf{A}\hat{\mathbf{h}}_a + u \leq 0 \tag{6.36b}$$

$$\boldsymbol{\delta}^H\boldsymbol{\delta} - \epsilon_{ab}^2 \leq 0 \tag{6.36c}$$

where $\mathbf{A} = \mathbf{I}_{N_r} \otimes \frac{\tilde{\mathbf{C}}_w}{\beta}$.

The above worst-case conditions in (6.36b) and (6.36c) are quadratic and convex in $\boldsymbol{\delta}$ for a fixed $\tilde{\mathbf{C}}_w$. Moreover, the channel error vector $\boldsymbol{\delta}$ is defined over the non-empty convex set $\boldsymbol{\xi}_{ab}$. Thus, according to the $\mathcal{S}$-*procedure* [87, §B.2], these two quadratic inequalities hold iff there exists $\mu_1 \geq 0$ such that

$$\begin{bmatrix} \mu_1\mathbf{I}_{N_t} + \mathbf{A} & \mathbf{A}\hat{\mathbf{h}}_a \\ \hat{\mathbf{h}}_a^H\mathbf{A} & -\mu_1\epsilon_{ab}^2 + \hat{\mathbf{h}}_a^H\mathbf{A}\hat{\mathbf{h}}_a - u \end{bmatrix} \succeq \mathbf{0}. \tag{6.37}$$

The objective function (6.33a) now is given by

$$\min_{\substack{\tilde{\mathbf{C}}_w, \tilde{\mathbf{C}}_{\eta_a}, \\ \tilde{\mathbf{C}}_{\eta_b}, \xi, u}} \quad -u \tag{6.38a}$$

$$\text{s.t. } \begin{bmatrix} \mu_1\mathbf{I}_{N_t} + \mathbf{A} & \mathbf{A}\hat{\mathbf{h}}_a \\ \hat{\mathbf{h}}_a^H\mathbf{A} & -\mu_1\epsilon_{ab}^2 + \hat{\mathbf{h}}_a^H\mathbf{A}\hat{\mathbf{h}}_a - u \end{bmatrix} \succeq \mathbf{0} \tag{6.38b}$$

Now we turn our attention to the inequality (6.33b) introduced by the Charnes-Cooper transformation. As was done before, after vectorising the channel matrices and considering the error definition in (6.34), we expand this constraint as

$$\left(\hat{\mathbf{h}}_a + \boldsymbol{\delta}\right)^H \mathbf{B}\left(\hat{\mathbf{h}}_a + \boldsymbol{\delta}\right) - (N_r)\left(1 - \xi r_{ab}^{\alpha}\sigma_b^2\right) \leq 0 \tag{6.39a}$$

$$\forall \boldsymbol{\delta}^H\boldsymbol{\delta} - \epsilon_{ab}^2 \leq 0 \tag{6.39b}$$

where $\mathbf{B} = \mathbf{I}_{N_r} \otimes \tilde{\mathbf{C}}_{\eta_a}$.

According the $\mathcal{S}$-*procedure*, the two quadratic inequalities in (6.39) hold iff there exists $\mu_2 \geq 0$ such that

$$\begin{bmatrix} \mu_2\mathbf{I}_{N_aN_r} - \mathbf{B} & -\mathbf{B}\hat{\mathbf{h}}_a \\ -\hat{\mathbf{h}}_a^H\mathbf{B} & -\mu_2\epsilon_{ab}^2 - \hat{\mathbf{h}}_a^H\mathbf{B}\hat{\mathbf{h}}_a + (N_r)\left(1 - \xi r_{ab}^{\alpha}\sigma_b^2\right) \end{bmatrix} \succeq \mathbf{0}. \tag{6.40}$$

Finally, we have to reformulate the eavesdropping constraint in (6.31b). Thus, we expand the former constraint as follows

$$\max_{\boldsymbol{\delta}_{a_k} \in \boldsymbol{\xi}_{ae}} \tilde{\mathbf{g}}_{a_k}^H\left(\tilde{\mathbf{C}}_w - (\beta-1)\tilde{\mathbf{C}}_{\eta_a}\right)\tilde{\mathbf{g}}_{a_k} - \min_{\boldsymbol{\delta}_{b_k} \in \boldsymbol{\xi}_{be}} \rho_k^{\alpha}(\beta-1)\tilde{\mathbf{g}}_{b_k}^H\tilde{\mathbf{C}}_{\eta_b}\tilde{\mathbf{g}}_{b_k}$$
$$- (\beta-1)\xi r_{be_k}^{\alpha}\sigma_e^2 \leq 0, \forall k = 1, \cdots, K. \tag{6.41}$$

To reformulate the above constraint, we introduce for each k^{th} Eve the upper and lower-bounds to the maximisation and minimisation operations in 6.41. These are respectively given by the slack variables $v_k \geq 0$ and $t_k \geq 0$. Recalling the deterministic robust definition in (6.26) we obtain

$$
\begin{aligned}
& v_k - t_k - (\beta - 1)\xi r_{be_k}^{\alpha}\sigma_e^2 \leq 0 && \text{(6.42a)}\\
\text{s.t. } & \left(\hat{\mathbf{g}}_{a_k} + \boldsymbol{\delta}_{a_k}\right)^H \mathbf{C}\left(\hat{\mathbf{g}}_{a_k} + \boldsymbol{\delta}_{a_k}\right) - v_k \leq 0 && \text{(6.42b)}\\
& \boldsymbol{\delta}_{a_k}^H \boldsymbol{\delta}_{a_k} - \epsilon_{ae}^2 \leq 0 && \text{(6.42c)}\\
& -\left(\hat{\mathbf{g}}_{b_k} + \boldsymbol{\delta}_{b_k}\right)^H (\beta - 1)\rho_k^{\alpha}\tilde{\mathbf{C}}_{\eta_b}\left(\hat{\mathbf{g}}_{b_k} + \boldsymbol{\delta}_{b_k}\right) + t_k \leq 0 && \text{(6.42d)}\\
& \boldsymbol{\delta}_{b_k}^H \boldsymbol{\delta}_{b_k} - \epsilon_{be}^2 \leq 0 && \text{(6.42e)}\\
& \forall k = 1, \cdots, K
\end{aligned}
$$

where he have defined the auxiliary variable $\mathbf{C} = \tilde{\mathbf{C}}_w - (\beta - 1)\tilde{\mathbf{C}}_{\eta_a}$.

We use again the $\mathcal{S}$-*procedure*, to express the two sets of two quadratic inequalities in (6.42b), (6.42c) and in (6.42d), (6.42e) for each k^{th} Eve. Thus, both sets hold iff for each k^{th} Eve there exists $\mu_{3_k} \geq 0$ and $\mu_{4_k} \geq 0$ such that

$$
\begin{bmatrix} \mu_{3_k}\mathbf{I}_{N_a} - \mathbf{C} & -\mathbf{C}\hat{\mathbf{g}}_{a_k} \\ -\hat{\mathbf{g}}_{a_k}^H\mathbf{C} & -\mu_{3_k}\epsilon_{ae}^2 - \hat{\mathbf{g}}_{a_k}^H\mathbf{C}\hat{\mathbf{g}}_{a_k} + v_k \end{bmatrix} \succeq \mathbf{0} \tag{6.43}
$$

and

$$
\begin{bmatrix} \mu_{4_k}\mathbf{I}_{N_n} + (\beta - 1)\rho_k^{\alpha}\tilde{\mathbf{C}}_{\eta_b} & (\beta - 1)\rho_k^{\alpha}\tilde{\mathbf{C}}_{\eta_b}\hat{\mathbf{g}}_{b_k} \\ (\beta - 1)\rho_k^{\alpha}\hat{\mathbf{g}}_{b_k}^H\tilde{\mathbf{C}}_{\eta_b} & \vartheta_{2_k} \end{bmatrix} \succeq \mathbf{0} \tag{6.44}
$$

where whe define the auxiliary variable

$$
\vartheta_{2_k} = -\mu_{4_k}\epsilon_{be}^2 + (\beta - 1)\rho_k^{\alpha}\hat{\mathbf{g}}_{b_k}^H\tilde{\mathbf{C}}_{\eta_b}\hat{\mathbf{g}}_{b_k} - t_k. \tag{6.45}
$$

Once we have reformulated the objective function and the eavesdropping constraint of the former problem in (6.31), we obtain an equivalent tractable SDP. We consider the reformulation of the objective function in (6.38), the LMI for the new Charnes-Cooper inequality in (6.40), the inequality (6.42a) and the LMIs in (6.43) and (6.44). We also keep the former constraints (6.31c) and (6.31d) to yield

$$
\begin{aligned}
& \min_{\substack{\tilde{\mathbf{C}}_w, \tilde{\mathbf{C}}_{\eta_a}, \tilde{\mathbf{C}}_{\eta_b}, \xi, u, \\ v_k, t_k, \mu_1, \mu_2, \mu_{3_k}, \mu_{4_k}}} \quad -u && \text{(6.46a)}\\
\text{s.t. } & \begin{bmatrix} \mu_1\mathbf{I}_{N_aN_r} + \mathbf{A} & \mathbf{A}\hat{\mathbf{h}}_a \\ \hat{\mathbf{h}}_a^H\mathbf{A} & -\mu_1\epsilon_{ab}^2 + \hat{\mathbf{h}}_a^H\mathbf{A}\hat{\mathbf{h}}_a - u \end{bmatrix} \succeq \mathbf{0} && \text{(6.46b)}
\end{aligned}
$$

$$\begin{bmatrix} \mu_2 \mathbf{I}_{N_a N_r} - \mathbf{B} & -\mathbf{B}\hat{\mathbf{h}}_a \\ -\hat{\mathbf{h}}_a^H \mathbf{B} & \vartheta_1 \end{bmatrix} \succeq \mathbf{0} \tag{6.46c}$$

$$v_k - t_k - (\beta - 1)\xi r_{be_k}^{\alpha} \sigma_e^2 \leq 0 \tag{6.46d}$$

$$\begin{bmatrix} \mu_{3_k} \mathbf{I}_{N_a} - \mathbf{C} & -\mathbf{C}\hat{\mathbf{g}}_{a_k} \\ -\hat{\mathbf{g}}_{a_k}^H \mathbf{C} & -\mu_{3_k}\epsilon_{ae}^2 - \hat{\mathbf{g}}_{a_k}^H \mathbf{C}\hat{\mathbf{g}}_{a_k} + v_k \end{bmatrix} \succeq \mathbf{0} \tag{6.46e}$$

$$\begin{bmatrix} \mu_{4_k} \mathbf{I}_{N_n} + (\beta - 1)\rho_k^{\alpha} \tilde{\mathbf{C}}_{\eta_b} & (\beta - 1)\rho_k^{\alpha} \tilde{\mathbf{C}}_{\eta_b} \hat{\mathbf{g}}_{b_k} \\ (\beta - 1)\rho_k^{\alpha} \hat{\mathbf{g}}_{b_k}^H \tilde{\mathbf{C}}_{\eta_b} & \vartheta_{2_k} \end{bmatrix} \succeq \mathbf{0} \tag{6.46f}$$

$$\text{Tr}\left\{\tilde{\mathbf{C}}_w\right\} + \text{Tr}\left\{\tilde{\mathbf{C}}_{\eta_a}\right\} + \text{Tr}\left\{\tilde{\mathbf{C}}_{\eta_b}\right\} \leq \xi P_{max} \tag{6.46g}$$

$$\tilde{\mathbf{C}}_w \succeq \mathbf{0}, \tilde{\mathbf{C}}_{\eta_a} \succeq \mathbf{0}, \tilde{\mathbf{C}}_{\eta_b} \succeq \mathbf{0}, \xi \geq 0, u \geq 0, v_k \geq 0, t_k \geq 0, \tag{6.46h}$$

$$\mu_1 \geq 0, \mu_2 \geq 0, \mu_{3_k} \geq 0, \mu_{4_k} \geq 0, \forall k = 1, \cdots, K \tag{6.46i}$$

where we use the slack variables $u, v_k, t_k, \xi, \mu_1, \mu_2, \mu_{3_k}, \mu_{4_k}$ and we relax $\xi > 0$ to $\xi \geq 0$ without consequence since $\xi = 0$ is not feasible for (6.31c).

It is worth pointing out that the objective covariance matrices are given by $\mathbf{C}_w = \frac{\tilde{\mathbf{C}}_w}{\xi}$, $\mathbf{C}_{\eta_a} = \frac{\tilde{\mathbf{C}}_{\eta_a}}{\xi}$ and $\mathbf{C}_{\eta_b} = \frac{\tilde{\mathbf{C}}_{\eta_b}}{\xi}$, and that we have defined

$$\begin{aligned} \mathbf{A} &= \mathbf{I}_{N_r} \otimes \frac{\tilde{\mathbf{C}}_w}{\beta}, \mathbf{B} = \mathbf{I}_{N_r} \otimes \tilde{\mathbf{C}}_{\eta_a}, \mathbf{C} = \tilde{\mathbf{C}}_w - (\beta - 1)\tilde{\mathbf{C}}_{\eta_a} \\ \vartheta_1 &= -\mu_2 \epsilon_{ab}^2 - \hat{\mathbf{h}}_a^H \mathbf{B} \hat{\mathbf{h}}_a + (N_r)\left(1 - \xi r_{ab}^{\alpha} \sigma_b^2\right) \\ \vartheta_{2_k} &= -\mu_{4_k} \epsilon_{be}^2 + (\beta - 1)\rho_k^{\alpha} \hat{\mathbf{g}}_{b_k}^H \tilde{\mathbf{C}}_{\eta_b} \hat{\mathbf{g}}_{b_k} - t_k. \end{aligned} \tag{6.47}$$

The above SDP is efficiently solved by interior-point algorithms implemented by on-the-shelf tools [105] assisted by the parser tools such as YALMIP [106] and CVX [107].

Remark 9 *The solution of the SDP (6.46) satisfies rank* $(\tilde{\mathbf{C}}_w) \leq$ *rank* $\left(\hat{\mathbf{H}}\hat{\mathbf{H}}^H\right)$. *In other words, our strategy might exploit the full degree of freedom of the Alice-to-Bob MIMO channel to convey information rather than using a transmission strategy using a rank-one covariance matrix, which is the case of beamforming.*

This implication has a further impact regarding the optimality of the regarding solution proposed in this section. Indeed, from (6.9), the relaxation in (6.30) is tight iff rank $(\tilde{\mathbf{C}}_w) =$ rank $\left(\hat{\mathbf{H}}\hat{\mathbf{H}}^H\right) = 1$. For uncorrelated channels, this condition is only satisfied in the case of MISO systems. Therefore, the solution offered by our technique is a suboptimal approximation to the maximal worst-case secrecy rate unless Bob uses one reception antenna and devotes $N_b - 1$ antennas to AN generation.

Secrecy rate lower bound

To evaluate the worst-case secrecy rate R_S^{wc} it is necessary to determine the matrix error channel $\boldsymbol{\Delta}^\star \in \boldsymbol{\xi}_{ab}$ that delivers the worst security performance that defines the secrecy rate lower bound. To achieve this objective we formulate an optimisation problem by considering the transmission covariance matrices $\mathbf{C}_w^\star$ and $\mathbf{C}_{\eta_a}^\star$ obtained from solving (6.46). This problems is as follows

$$\min_{\boldsymbol{\Delta}\in\xi_{ab}} \ \mathrm{Tr}\left\{\mathbf{Z}\left(\hat{\mathbf{H}}_a+\boldsymbol{\Delta}\right)^H \mathbf{C}_w^\star \left(\hat{\mathbf{H}}_a+\boldsymbol{\Delta}\right)\right\} \tag{6.48a}$$

$$\text{s.t. } \mathrm{Tr}\left\{\boldsymbol{\Delta}\boldsymbol{\Delta}^H\right\} \leq \epsilon_{ab}^2 \tag{6.48b}$$

where we define the auxiliary matrix variable

$$\mathbf{Z} = \left[\left(\hat{\mathbf{H}}_a+\boldsymbol{\Delta}\right)^H \mathbf{C}_{\eta_a}^\star \left(\hat{\mathbf{H}}_a+\boldsymbol{\Delta}\right) + r_{ab}^\alpha \sigma_b^2 \mathbf{I}_{N_r}\right]^{-1}. \tag{6.49}$$

Problem (6.48) is not convex, and so we need to recast it into a tractable way. To do so, we use the Charnes-Cooper transformation in (6.31) to rewrite it as

$$\begin{aligned}\min_{\boldsymbol{\Delta}\in\xi_{ab}} \ & \mathrm{Tr}\left\{\tilde{\mathbf{Z}}\left(\hat{\mathbf{H}}_a+\boldsymbol{\Delta}\right)^H \tilde{\mathbf{C}}_w^\star \left(\hat{\mathbf{H}}_a+\boldsymbol{\Delta}\right)\right\} \\ \text{s.t. } & \mathrm{Tr}\left\{\boldsymbol{\Delta}\boldsymbol{\Delta}^H\right\} \leq \epsilon_{ab}^2\end{aligned}$$

where $\tilde{\mathbf{C}}_w^\star = \xi^\star \mathbf{C}_w^\star$, $\tilde{\mathbf{C}}_{\eta_a}^\star = \xi^\star \mathbf{C}_{\eta_a}^\star$ are the solutions to SDP (6.46) and

$$\tilde{\mathbf{Z}} = \left[\left(\hat{\mathbf{H}}_a+\boldsymbol{\Delta}\right)^H \tilde{\mathbf{C}}_{\eta_a}^\star \left(\hat{\mathbf{H}}_a+\boldsymbol{\Delta}\right) + \xi^\star r_{ab}^\alpha \sigma_b^2 \mathbf{I}_{N_r}\right]^{-1}. \tag{6.51}$$

Using the inequality $\tilde{\mathbf{Z}} \preceq \mathbf{I}_{N_r}$ resulting from the Charnes-Cooper transformation we can write

$$\min_{\boldsymbol{\Delta}\in\xi_{ab}} \ \mathrm{Tr}\left\{\left(\hat{\mathbf{H}}_a+\boldsymbol{\Delta}\right)^H \tilde{\mathbf{C}}_w^\star \left(\hat{\mathbf{H}}_a+\boldsymbol{\Delta}\right)\right\} \tag{6.52a}$$

$$\text{s.t. } \mathrm{Tr}\left\{\left(\hat{\mathbf{H}}_a+\boldsymbol{\Delta}\right)^H \tilde{\mathbf{C}}_{\eta_a}^\star \left(\hat{\mathbf{H}}_a+\boldsymbol{\Delta}\right) + \xi^\star r_{ab}^\alpha \sigma_b^2 \mathbf{I}_{N_r}\right\} \leq \mathrm{Tr}\left\{\mathbf{I}_{N_r}\right\} \tag{6.52b}$$

$$\mathrm{Tr}\left\{\boldsymbol{\Delta}\boldsymbol{\Delta}^H\right\} \leq \epsilon_{ab}^2. \tag{6.52c}$$

Now, we use the vectorised version $\boldsymbol{\delta}$ of the error channel matrix $\boldsymbol{\Delta}$ and the channel uncertainty deterministic definition in (6.34) to introduce the slack variable $\boldsymbol{\Lambda} = \boldsymbol{\delta}\boldsymbol{\delta}^H$. This variable is subsequently relaxed to $\boldsymbol{\Lambda} \succeq \boldsymbol{\delta}\boldsymbol{\delta}^H$ and, by using

the *Schur complement* [87, §A.5.5], it is expressed as an LMI. Finally, we use the vectorised versions of the channel matrix $\hat{\mathbf{H}}_a$ given by $\hat{\mathbf{h}}_a$ to obtain the following SDP

$$\min_{\boldsymbol{\delta},\boldsymbol{\Lambda}} \ \mathrm{Tr}\left\{\left(\mathbf{I}_{N_r}\otimes\tilde{\mathbf{C}}_w^{\star}\right)\hat{\mathbf{h}}_a\hat{\mathbf{h}}_a^H\right\}+2\mathrm{Re}\left\{\hat{\mathbf{h}}_a^H\left(\mathbf{I}_{N_r}\otimes\tilde{\mathbf{C}}_w^{\star}\right)\boldsymbol{\delta}\right\}+\mathrm{Tr}\left\{\left(\mathbf{I}_{N_r}\otimes\tilde{\mathbf{C}}_w^{\star}\right)\boldsymbol{\Lambda}\right\} \tag{6.53a}$$

$$\text{s.t. } \mathrm{Tr}\left\{\left(\mathbf{I}_{N_r}\otimes\tilde{\mathbf{C}}_{\eta_a}^{\star}\right)\hat{\mathbf{h}}_a\hat{\mathbf{h}}_a^H\right\}+2\mathrm{Re}\left\{\hat{\mathbf{h}}_a^H\left(\mathbf{I}_{N_r}\otimes\tilde{\mathbf{C}}_{\eta_a}^{\star}\right)\boldsymbol{\delta}\right\}$$
$$+\mathrm{Tr}\left\{\left(\mathbf{I}_{N_r}\otimes\tilde{\mathbf{C}}_{\eta_a}^{\star}\right)\boldsymbol{\Lambda}\right\}+Nr\left(\xi^{\star}r_{ab}^{\alpha}\sigma_b^2-1\right)\leq 0 \tag{6.53b}$$

$$\begin{bmatrix}\boldsymbol{\Lambda} & \boldsymbol{\delta}\\ \boldsymbol{\delta}^H & 1\end{bmatrix}\succeq\mathbf{0},\mathrm{Tr}\left\{\boldsymbol{\Lambda}\right\}\leq\epsilon_{ab}^2. \tag{6.53c}$$

After solving this SDP by using interior-point based algorithms [105], we are ready to calculate R_S^{wc} for the fixed value of β. Hence

$$\mathrm{R}_S^{wc}(\beta)=\left[\log_2\det\left(\mathbf{I}_{N_r}+\mathbf{Z}^{\star}\left(\hat{\mathbf{H}}_a+\boldsymbol{\Delta}^{\star}\right)^H\mathbf{C}_w^{\star}\left(\hat{\mathbf{H}}_a+\boldsymbol{\Delta}^{\star}\right)\right)-\log_2(\beta)\right]^+ \tag{6.54}$$

where we emphasise that $\mathbf{C}_w^{\star}$ and $\mathbf{C}_{\eta_a}^{\star}$ are obtained by solving (6.46) and $\boldsymbol{\Delta}^{\star}$ is obtained by the SDP (6.53). We define

$$\mathbf{Z}^{\star}=\left[\left(\hat{\mathbf{H}}+\boldsymbol{\Delta}^{\star}\right)^H\mathbf{C}_{\eta_a}^{\star}\left(\hat{\mathbf{H}}+\boldsymbol{\Delta}^{\star}\right)+r_{ab}^{\alpha}\sigma_b^2\mathbf{I}_{N_r}\right]^{-1}. \tag{6.55}$$

It is worth remarking that we have determined the worst-case secrecy rate R_S^{wc} for the fixed value of β. As we are interested in finding the largest R_S^{wc} irrespective of β, then we have to look for the optimal value $\beta^{\star}$ that maximises R_S^{wc}. This can be found by one-dimensional exhaustive searching algorithms as in §4.3.3 of chapter 4 and also in [144]. It is important to note that due to specific problem conditions such as the instantaneous CSI, distance between nodes, power available, etc., the results from the SDP in (6.46) might not return a positive R_S^{wc} for all the defined range of β. In this case, there is not a feasible solution, so the system is considered in outage and transmission does not take place.

Individually constrained networks

In this section we study a robust security approach towards CSI uncertainties in a network subject to individual power constraints. In other words, we maximise the

worst-case secrecy rate looking at the practical case when both the transmitting and receiving parties each have a limited amount of available power. This problem is written as follows

$$\max_{\substack{\mathbf{C}_w,\mathbf{C}_{\eta_a},\\ \mathbf{C}_{\eta_b}}} \ \mathrm{R}_S^{wc} \tag{6.56a}$$

$$\text{s.t. } \mathbf{C}_w \succeq \mathbf{0}, \mathbf{C}_{\eta_a} \succeq \mathbf{0}, \mathbf{C}_{\eta_b} \succeq \mathbf{0} \tag{6.56b}$$

$$\mathrm{Tr}\left\{\mathbf{C}_w\right\} + \mathrm{Tr}\left\{\mathbf{C}_{\eta_a}\right\} \leq P_a \tag{6.56c}$$

$$\mathrm{Tr}\left\{\mathbf{C}_{\eta_b}\right\} \leq \ P_b \tag{6.56d}$$

where P_a and P_b are the available transmit power at Alice and Bob.

After analysing the structure of R_S^{wc} in (6.27) and owing to the separate individual power constraints, problem (6.56) can be split into two problems. First, we look for Bob's AN covariance matrix ($\mathbf{C}_{\eta_b}$) under a power constraint given by P_b, and then we design Alice's transmission covariance matrices $\mathbf{C}_w$ and $\mathbf{C}_{\eta_a}$ under Alice's power constraint P_a.

In this context, the objective of the first problem is to design an AN signal from Bob given its covariance matrix $\mathbf{C}_{\eta_b}$ that maximises the confusing effect at the eavesdroppers. This worst-case problem is formulated as

$$\max_{\mathbf{C}_{\eta_b}} \ \min_{k=1,\cdots,K} \min_{\boldsymbol{\delta}_{b_k}\in\xi_{be}} \tilde{\mathbf{g}}_{b_k}^H \mathbf{C}_{\eta_b} \tilde{\mathbf{g}}_{b_k} \tag{6.57a}$$

$$\text{s.t. } \mathbf{C}_{\eta_b} \succeq \mathbf{0} \tag{6.57b}$$

$$\mathrm{Tr}\left\{\mathbf{C}_{\eta_b}\right\} \leq \ P_b. \tag{6.57c}$$

As an effective way to deal with the above maximin optimisation problem, we introduce the slack variable $u \geq 0$ that effectively sets a lower-bound for the inner minimisations in (6.57a). Thus, the problem above becomes

$$\max_{\mathbf{C}_{\eta_b},u} \ u \tag{6.58a}$$

$$\text{s.t. } \left(\hat{\mathbf{g}}_{b_k} + \boldsymbol{\delta}_{b_k}\right)^H \mathbf{C}_{\eta_b} \left(\hat{\mathbf{g}}_{b_k} + \boldsymbol{\delta}_{b_k}\right) \geq u, \tag{6.58b}$$

$$\forall \boldsymbol{\delta}_{b_k}^H \boldsymbol{\delta}_{b_k} \leq \epsilon_{be}^2, \forall k = 1, \cdots, K \tag{6.58c}$$

$$\mathbf{C}_{\eta_b} \succeq \mathbf{0}, \mathrm{Tr}\left\{\mathbf{C}_{\eta_b}\right\} \leq \ P_b, u \geq 0. \tag{6.58d}$$

As in the previous section, the K sets of quadratic constraints in (6.58c) can be expressed by using the $\mathcal{S}$-*procedure* [87, §B.2] to obtain the following SDP

$$\min_{\mathbf{C}_{\eta_b},u,\mu_k} \ -u \tag{6.59a}$$

$$\text{s.t.} \begin{bmatrix} \mu_k \mathbf{I}_{N_n} + \mathbf{C}_{\eta_b} & \mathbf{C}_{\eta_b}\hat{\mathbf{g}}_{b_k} \\ \hat{\mathbf{g}}_{b_k}^H \mathbf{C}_{\eta_b} & -\mu\epsilon_{be}^2 + \hat{\mathbf{g}}_{b_k}^H \mathbf{C}_{\eta_b}\hat{\mathbf{g}}_{b_k} - u \end{bmatrix} \succeq \mathbf{0}, \forall k = 1, \cdots, K \tag{6.59b}$$

$$\mathbf{C}_{\eta_b} \succeq \mathbf{0}, \text{Tr}\left\{\mathbf{C}_{\eta_b}\right\} \leq \ P_b, u \geq 0, \mu_k \geq 0. \tag{6.59c}$$

Bob's AN covariance matrix $\mathbf{C}_{\eta_b}^\star$ is obtained by solving (6.59) using interior-point algorithms [105]. Subsequently, we have to evaluate the effect of Bob's AN at the eavesdroppers. Thus, we have to determine the worst-case channel error $\boldsymbol{\delta}_{b_k}^\star$ that delivers the worst performance for our strategy; i.e., the $\boldsymbol{\delta}_{b_k}$ within the deterministic set that minimises the effect of Bob's AN at the k^{th} Eve. This is found by solving the following problem for each k^{th} Eve

$$\min_{\boldsymbol{\delta}_{b_k}, \boldsymbol{\Lambda}_{b_k}} \ \text{Tr}\left\{\mathbf{C}_{\eta_b}^\star \boldsymbol{\Lambda}_{b_k}\right\} + 2\text{Re}\left\{\hat{\mathbf{g}}_{b_k}^H \mathbf{C}_{\eta_b}^\star \boldsymbol{\delta}_{b_k}\right\} + \text{Tr}\left\{\mathbf{C}_{\eta_b}^\star \hat{\mathbf{g}}_{b_k}\hat{\mathbf{g}}_{b_k}^H\right\} \tag{6.60a}$$

$$\text{s.t.} \begin{bmatrix} \boldsymbol{\Lambda}_{b_k} & \boldsymbol{\delta}_{b_k} \\ \boldsymbol{\delta}_{b_k}^H & 1 \end{bmatrix} \succeq \mathbf{0}, \text{Tr}\left\{\boldsymbol{\Lambda}_{b_k}\right\} \leq \epsilon_{be.}^2 \tag{6.60b}$$

In (6.60), the objective function (6.60a) results from expanding $\tilde{\mathbf{g}}_{b_k}^H \mathbf{C}_{\eta_b}^\star \tilde{\mathbf{g}}_{b_k}$, considering that $\tilde{\mathbf{g}}_{b_k} = \hat{\mathbf{g}}_{b_k} + \boldsymbol{\delta}_{b_k}$ and introducing the slack variable $\boldsymbol{\Lambda}_{b_k} = \boldsymbol{\delta}_{b_k}\boldsymbol{\delta}_{b_k}^H$. This variable is relaxed to $\boldsymbol{\Lambda}_{b_k} \succeq \boldsymbol{\delta}_{b_k}\boldsymbol{\delta}_{b_k}^H$ and expressed by the *Schur complement* [87, §A.5.5] in the LMI in (6.60b). Finally, the effect of the AN broadcast by Bob into the k^{th} Eve is evaluated as

$$AN_{b_k} = \left(\hat{\mathbf{g}}_{b_k} + \boldsymbol{\delta}_{b_k}^\star\right)^H \mathbf{C}_{\eta_b}^\star \left(\hat{\mathbf{g}}_{b_k} + \boldsymbol{\delta}_{b_k}^\star\right). \tag{6.61}$$

Once we have determined the effect of the AN broadcast by Bob into the K eavesdroppers, we now have to solve the second problem that seeks to determine Alice's transmission covariance matrices $\mathbf{C}_w$ and $\mathbf{C}_{\eta_a}$ to maximise the worst-case secrecy rate in (6.27). Therefore, we formulate the second problem as

$$\max_{\mathbf{C}_w, \mathbf{C}_{\eta_a}, \beta} \min_{\boldsymbol{\Delta} \in \xi_{ab}} \log_2 \det\left(\mathbf{I}_{N_r} + \mathbf{W}\tilde{\mathbf{H}}_a^H \mathbf{C}_w \tilde{\mathbf{H}}_a\right) - \log_2 \beta \tag{6.62a}$$

$$\text{s.t.} \max_{\substack{\boldsymbol{\delta}_{a_k} \in \boldsymbol{\xi}_{ae}, \\ \boldsymbol{\delta}_{b_k} \in \boldsymbol{\xi}_{be}}} \left(1 + \frac{\tilde{\mathbf{g}}_{a_k}^H \mathbf{C}_w \tilde{\mathbf{g}}_{a_k}}{\tilde{\mathbf{g}}_{a_k}^H \mathbf{C}_{\eta_a} \tilde{\mathbf{g}}_{a_k} + \rho_k^\alpha AN_{b_k} + r_{be_k}^\alpha \sigma_e^2}\right) \leq \beta, \forall k = 1, \cdots, K \tag{6.62b}$$

$$\mathbf{C}_w \succeq \mathbf{0}, \mathbf{C}_{\eta_a} \succeq \mathbf{0}, P \leq P_a, \beta > 0. \tag{6.62c}$$

where $\mathbf{W}$ is defined in (6.24). In (6.62) we have again split the problem by introducing a slack variable β as a way to recast it into a SDP.

We notice that the objective function (6.62a) is similar to the one in (6.29); moreover, the constraint in (6.62b) only differs from (6.29b) in the term regarding

Bob's AN; i.e., AN_{n_k}. Therefore, after considering a fixed β, we can follow the same methodology used in the previous section to reformulate (6.29) and recast (6.62) into the following SDP

$$\min_{\substack{\tilde{\mathbf{C}}_w,\tilde{\mathbf{C}}_{\eta_a},\xi,u,\\ \mu_1,\mu_2,\mu_{3_k}}} \quad -u \tag{6.63a}$$

$$\text{s.t.} \begin{bmatrix} \mu_1\mathbf{I}_{N_aN_r}+\mathbf{A} & \mathbf{A}\hat{\mathbf{h}}_a \\ \hat{\mathbf{h}}_a^H\mathbf{A} & -\mu_1\epsilon_{ab}^2+\hat{\mathbf{h}}_a^H\mathbf{A}\hat{\mathbf{h}}_a-u \end{bmatrix} \succeq \mathbf{0} \tag{6.63b}$$

$$\begin{bmatrix} \mu_2\mathbf{I}_{N_aN_r}-\mathbf{B} & -\mathbf{B}\hat{\mathbf{h}}_a \\ -\hat{\mathbf{h}}_a^H\mathbf{B} & \vartheta_1 \end{bmatrix} \succeq \mathbf{0} \tag{6.63c}$$

$$\begin{bmatrix} \mu_{3_k}\mathbf{I}_{N_a}-\mathbf{C} & -\mathbf{C}\hat{\mathbf{g}}_{a_k} \\ -\hat{\mathbf{g}}_{a_k}^H\mathbf{C} & \vartheta_{3_k} \end{bmatrix} \succeq \mathbf{0} \tag{6.63d}$$

$$\text{Tr}\left\{\tilde{\mathbf{C}}_w\right\}+\text{Tr}\left\{\tilde{\mathbf{C}}_{\eta_a}\right\} \leq \xi P_a \tag{6.63e}$$

$$\tilde{\mathbf{C}}_w \succeq \mathbf{0}, \tilde{\mathbf{C}}_{\eta_a} \succeq \mathbf{0}, \tilde{\mathbf{C}}_{\eta_b} \succeq \mathbf{0}, \xi \geq 0 \tag{6.63f}$$

$$u \geq 0, \mu_1 \geq 0, \mu_2 \geq 0, \mu_{3_k} \geq 0, \forall k = 1, \cdots, K \tag{6.63g}$$

where we include the slack variables u, ξ, μ_1, μ_2 and μ_{3_k}. In the reformulation process we again used the Charnes-Cooper transformation [104]; therefore, the former optimising variables are given by $\mathbf{C}_w = \frac{\tilde{\mathbf{C}}_w}{\xi}$ and $\mathbf{C}_{\eta_a} = \frac{\tilde{\mathbf{C}}_{\eta_a}}{\xi}$. We again let $\hat{\mathbf{h}}_a = \text{vec}\left(\hat{\mathbf{H}}_a\right)$ and the auxiliary variables $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ and ϑ_1 are defined in (6.47). Finally, in (6.63) we define

$$\vartheta_{3_k} = -\mu_{3_k}\epsilon_{ae}^2 - \hat{\mathbf{g}}_{a_k}^H\mathbf{C}\hat{\mathbf{g}}_{a_k} + (\beta-1)\xi\left(\rho_k^\alpha AN_{b_k} + r_{be_k}^\alpha\sigma_e^2\right). \tag{6.64}$$

The solution of the above SDP can be efficiently obtained by interior-point algorithm based tools [105]. It is worth pointing out that the SDP in (6.63) considers a fixed value of β; therefore, we have to find the $\beta^\star$ that maximises R_S^{wc}. This can be done using linear searching algorithms like the one introduced in §4.3.3 of chapter 4 and also in [144]. If a positive worst-case secrecy rate R_S^{wc} cannot be achieved for any of the admissible values for β, then the system is considered in outage and transmission does not take place.

Passive eavesdropping

In this section we now consider the practical case when Alice and Bob are not aware of the presence of passive eavesdroppers; therefore, they do not know the

instantaneous mismatched CSI of the eavesdropping links. As an alternative to model this challenging problem, the legitimate transmission parties can assume the second-order statistics of the eavesdropping channels.

In this scenario, as in §4.2.2 of chapter 4, we define a new secrecy metric given by the average worst-case secrecy rate ($\bar{\mathrm{R}}_S^{wc}$). This metric is based on the ergodic secrecy rate which considers that the intended transmission parties have available the main link's CSI but only statistical information about the eavesdropper's channel [46, 54]. In our problem, we transmit jointly AN from the receiver and transmitter; therefore, we consider that both, Alice and Bob assume statistics regarding the small-fading eavesdropping channel's elements. These are given by the covariance matrices $\mathbf{R}_{\tilde{g}_a} = \mathbb{E}\{\tilde{\mathbf{g}}_{a_k}\tilde{\mathbf{g}}_{a_k}^H\} = \sigma_{\tilde{g}_a}^2\mathbf{I}_{N_t}$ and $\mathbf{R}_{\tilde{g}_b} = \mathbb{E}\{\tilde{\mathbf{g}}_{b_k}\tilde{\mathbf{g}}_{b_k}^H\} = \sigma_{\tilde{g}_b}^2\mathbf{I}_{N_n}, \forall k = 1, \cdots, K$.

Subsequently, we use again the concavity property of the logarithm function and *Jensen's inequality* [87, §3.1.8] to approximate the ergodic secrecy rate to a tractable metric named average worst-case secrecy rate $\bar{\mathrm{R}}_S^{wc}$ that is given by

$$\bar{\mathrm{R}}_S^{wc} = \left[\min_{\mathbf{\Delta}\in\xi_{ab}} \log_2 \det\left(\mathbf{I}_{N_r} + \mathbf{W}\tilde{\mathbf{H}}_a^H\mathbf{C}_w\tilde{\mathbf{H}}_a\right) - \max_{k=1,\cdots,K} \log_2\left(1+\theta_k\right)\right]^+ \tag{6.65}$$

where $\mathbf{W}$ is defined in (6.24) and

$$\theta_k = \frac{\mathrm{Tr}\left\{\mathbf{C}_w\mathbf{R}_{\tilde{g}_a}\right\}}{\mathrm{Tr}\left\{\mathbf{C}_{\eta_a}\mathbf{R}_{\tilde{g}_a}\right\} + \rho_k^{\alpha}\mathrm{Tr}\left\{\mathbf{C}_{\eta_b}\mathbf{R}_{\tilde{g}_b}\right\} + r_{ae_k}^{\alpha}\sigma_e^2} \tag{6.66}$$

is effectively the mean SNR at the k^{th} Eve after using the assumed second-order statistics about the random eavesdropping channels.

We are aware that by this approximation our strategy might lead to a sub-optimal solution for the passive eavesdropping problem. However, the problem formulation is simplified, and by noting that, in (6.65), we consider the worst-case performance, the metric $\bar{\mathrm{R}}_S^{wc}$ effectively introduces a lower-bound on the actual ergodic secrecy rate to our current problem.

Now, we write the average worst-case secrecy rate maximisation problem subject to a global power constraint as

$$\max_{\substack{\mathbf{C}_w,\mathbf{C}_{\eta_a},\\ \mathbf{C}_{\eta_b}}} \quad \bar{\mathrm{R}}_S^{wc} \tag{6.67a}$$

$$\text{s.t. } \mathbf{C}_w \succeq \mathbf{0}, \mathbf{C}_{\eta_a} \succeq \mathbf{0}, \mathbf{C}_{\eta_b} \succeq \mathbf{0} \tag{6.67b}$$

$$P \leq P_{max} \tag{6.67c}$$

where the global available power in the network is defined by P_{max}.

This problem is nonconvex owing to the nature of the metric $\bar{\mathrm{R}}_S^{wc}$ in (6.65). However, we can follow the same procedure used in the previous section of this chapter to address the nonconvex problem (6.28). As a result we obtain a problem similar to (6.30) but replacing the eavesdropping constraint in (6.30b) by

$$\frac{\mathrm{Tr}\left\{\mathbf{C}_w\mathbf{R}_{\tilde{g}_a}\right\}}{\mathrm{Tr}\left\{\mathbf{C}_{\eta_a}\mathbf{R}_{\tilde{g}_a}\right\}+\rho_k^{\alpha}\mathrm{Tr}\left\{\mathbf{C}_{\eta_b}\mathbf{R}_{\tilde{g}_b}\right\}+r_{ae_k}^{\alpha}\sigma_e^2}\leq\beta-1,\forall k=1,\cdots,K. \tag{6.68}$$

After using again the Charnes-Cooper transformation, we let $\mathbf{C}_w=\frac{\tilde{\mathbf{C}}_w}{\xi}$, $\mathbf{C}_{\eta_a}=\frac{\tilde{\mathbf{C}}_{\eta_a}}{\xi}$ and $\mathbf{C}_{\eta_b}=\frac{\tilde{\mathbf{C}}_{\eta_b}}{\xi}$. Subsequently, the inequality (6.68) can be expressed as

$$\mathrm{Tr}\left\{\mathbf{C}\mathbf{R}_{\tilde{g}_a}\right\}-(\beta-1)\rho_k^{\alpha}\mathrm{Tr}\left\{\tilde{\mathbf{C}}_{\eta_b}\mathbf{R}_{\tilde{g}_b}\right\}-r_{ae_k}^{\alpha}\sigma_e^2(\beta-1)\xi\leq 0,\forall k=1,\cdots,K \tag{6.69}$$

where $\mathbf{C}$ is defined in (6.47).

By noting the connection between the problems (6.67) and (6.30) we can solve the passive eavesdropping average worst-case secrecy rate problem under a global power constraint by using the SDP (6.46) but considering the constraint (6.69) instead of the inequality (6.46d) and the LMIs (6.46e) and (6.46f). The resulting SDP is

$$\min_{\substack{\tilde{\mathbf{C}}_w,\tilde{\mathbf{C}}_{\eta_a},\tilde{\mathbf{C}}_{\eta_b}\\ \xi,u,\mu_1,\mu_2}} \quad -u \tag{6.70a}$$

$$\text{s.t.}\quad \begin{bmatrix} \mu_1\mathbf{I}_{N_aN_r}+\mathbf{A} & \mathbf{A}\hat{\mathbf{h}}_a \\ \hat{\mathbf{h}}_a^H\mathbf{A} & -\mu_1\epsilon_{ab}^2+\hat{\mathbf{h}}_a^H\mathbf{A}\hat{\mathbf{h}}_a-u \end{bmatrix}\succeq\mathbf{0} \tag{6.70b}$$

$$\begin{bmatrix} \mu_2\mathbf{I}_{N_aN_r}-\mathbf{B} & -\mathbf{B}\hat{\mathbf{h}}_a \\ -\hat{\mathbf{h}}_a^H\mathbf{B} & \vartheta_1 \end{bmatrix}\succeq\mathbf{0} \tag{6.70c}$$

$$\mathrm{Tr}\left\{\mathbf{C}\mathbf{R}_{\tilde{g}_a}\right\}-(\beta-1)\rho_k^{\alpha}\mathrm{Tr}\left\{\tilde{\mathbf{C}}_{\eta_b}\mathbf{R}_{\tilde{g}_b}\right\}-r_{ae_k}^{\alpha}\sigma_e^2(\beta-1)\xi\leq 0,\forall k=1,\cdots,K \tag{6.70d}$$

$$\mathrm{Tr}\left\{\tilde{\mathbf{C}}_w\right\}+\mathrm{Tr}\left\{\tilde{\mathbf{C}}_{\eta_a}\right\}+\mathrm{Tr}\left\{\tilde{\mathbf{C}}_{\eta_b}\right\}\leq\xi P_{max} \tag{6.70e}$$

$$\tilde{\mathbf{C}}_w\succeq\mathbf{0},\tilde{\mathbf{C}}_{\eta_a}\succeq\mathbf{0},\tilde{\mathbf{C}}_{\eta_b}\succeq\mathbf{0},\xi\geq 0,u\geq 0,v_k\geq 0,t_k\geq 0, \tag{6.70f}$$

$$\mu_1\geq 0,\mu_2\geq 0,\mu_{3_k}\geq 0,\mu_{4_k}\geq 0,\forall k=1,\cdots,K \tag{6.70g}$$

where u,ξ,μ_1,μ_2 are slack variables and $\mathbf{A}$, $\mathbf{B}$ and ϑ_1 are defined in (6.47).

As the SDP (6.70) considers a fixed β, we have to find the optimal $\beta^{\star}$ that maximises $\bar{\mathrm{R}}_S^{wc}$. This value can be obtained by linear searching algorithms as the one in §4.3.3 of chapter 4 or in [144].

Remark 10 *From the simulation results it turns out that Alice's AN is isotropically broadcast over the $N_a - r$ dimensional space orthogonal to the r-dimensional space spanned by $\mathbf{H}_a\mathbf{H}_a^H$, where $r = rank\left(\mathbf{H}_a\mathbf{H}_a^H\right)$. In other words, $\mathbf{C}_{\eta_a}^\star$ has $N_a - r$ equal non-zero eigenvalues. A special case arises when $N_a \leq N_r$. In this case, and as we assume independent distributed uncorrelated channels, $r = N_a$, and so $\mathbf{C}_{\eta_a}^\star$ is either zero-power or rank$(\mathbf{C}_{\eta_a}^\star) \geq 1$. This special situation means that Alice leaks AN to the receiver. As regards Bob, he distributes the power isotropically among the N_n equal eigenvalues of Bob's AN covariance matrix $\mathbf{C}_{\eta_b}^\star$.*

It is worth remarking that the use of an average secrecy metric, as in the case of $\bar{\mathrm{R}}_S^{wc}$, guarantees security only from an average point of view. This might be a weak criterion for the security of certain applications; therefore, for a stronger definition of security, an outage based formulation of secrecy can be enforced to offer a given probability of achieving secrecy. This stronger security approach has been considered for the MISO case in chapter 3 of this thesis and in [14, 55, 56, 67, 70, 90, 102, 103, 140]. The outage formulation for a MIMO problem studied in this chapter is a challenging problem that remains open in the literature. This is an interesting direction for further research.

6.4.3 Robust worst-case power consumption minimisation

The objective of this section is to find the optimal transmission covariance matrices at Alice and Bob that minimise the global power consumption subject to guaranteeing a target worst-case secrecy rate R. The legitimate transmission parties have available a mismatched version of the actual CSI of all the channels involved in the transmission. Therefore, the joint transmitter/receiver AN generation problem is written as follows

$$\min_{\substack{\mathbf{C}_w, \mathbf{C}_{\eta_a}, \\ \mathbf{C}_{\eta_b}}} \quad P \tag{6.71a}$$

$$\text{s.t. } \mathrm{R}_S^{wc} \geq R \tag{6.71b}$$

$$\mathbf{C}_w \succeq \mathbf{0}, \mathbf{C}_{\eta_a} \succeq \mathbf{0}, \mathbf{C}_{\eta_b} \succeq \mathbf{0}. \tag{6.71c}$$

The above problem is not convex due to the nature of the constraint (6.71b); therefore, as we did before, we introduce and fix the slack variable β to split R_S^{wc}

into two terms and this helps towards reformulating (6.71) into a tractable problem. To do so, we use the relaxation in (6.9) to approximate the original problem as

$$\min_{\substack{\mathbf{C}_w,\mathbf{C}_{\eta_a},\\ \mathbf{C}_{\eta_b}}} \operatorname{Tr}\{\mathbf{C}_w\} + \operatorname{Tr}\{\mathbf{C}_{\eta_a}\} + \operatorname{Tr}\{\mathbf{C}_{\eta_b}\} \tag{6.72a}$$

$$\text{s.t.} \min_{\boldsymbol{\Delta}\in\xi_{ab}} \operatorname{Tr}\left\{\mathbf{W}\tilde{\mathbf{H}}_a^H\mathbf{C}_w\tilde{\mathbf{H}}_a\right\} \geq 2^R\beta - 1 \tag{6.72b}$$

$$\max_{\substack{\boldsymbol{\delta}_{a_k}\in\boldsymbol{\xi}_{ae},\\ \boldsymbol{\delta}_{b_k}\in\boldsymbol{\xi}_{be}}} (1+\omega_k) \leq \beta, \forall k = 1,\cdots,K \tag{6.72c}$$

$$\mathbf{C}_w \succeq \mathbf{0}, \mathbf{C}_{\eta_a} \succeq \mathbf{0}, \mathbf{C}_{\eta_b} \succeq \mathbf{0}, \beta > 1 \tag{6.72d}$$

where $\mathbf{W}$ and ω_k are defined in (6.24) and (6.25).

We turn our attention to the objective function in (6.72a) to note that it is already linear, and so we concentrate on the nonconvex constraint (6.72b). By observing that $\boldsymbol{\Sigma} \preceq \boldsymbol{\Phi} \Rightarrow \operatorname{Tr}\{\boldsymbol{\Sigma}\} \leq \operatorname{Tr}\{\boldsymbol{\Phi}\}$, we can express (6.72b) as

$$\min_{\boldsymbol{\Delta}\in\xi_{ab}} \operatorname{Tr}\left\{\tilde{\mathbf{H}}_a^H\left(\mathbf{C}_w - \frac{\varpi}{N_r}\mathbf{C}_{\eta_a}\right)\tilde{\mathbf{H}}_a\right\} - \varpi r_{ab}^{\alpha}\sigma_b^2 \geq 0 \tag{6.73}$$

where $\varpi = 2^R\beta - 1$.

We use again the vectorisation property $\operatorname{Tr}\left\{\boldsymbol{\Delta}^H\boldsymbol{\Delta}\right\} = \boldsymbol{\delta}^H\boldsymbol{\delta}$ where $\boldsymbol{\delta} = \operatorname{vec}\{\boldsymbol{\Delta}\}$ to expand the inequality above and obtain

$$-\hat{\mathbf{h}}_a^H\mathbf{D}\hat{\mathbf{h}}_a - 2\text{Re}\left\{\hat{\mathbf{h}}_a^H\mathbf{D}\boldsymbol{\delta}\right\} - \boldsymbol{\delta}^H\mathbf{D}\boldsymbol{\delta} + \varpi r_{ab}^{\alpha}\sigma_b^2 \leq 0 \tag{6.74a}$$

$$\forall \boldsymbol{\delta}^H\boldsymbol{\delta} - \epsilon_{ab}^2 \leq 0 \tag{6.74b}$$

where we define

$$\mathbf{D} = \mathbf{I}_{N_r} \otimes \mathbf{C}_w - \frac{\varpi}{N_r}\mathbf{I}_{N_r} \otimes \mathbf{C}_{\eta_a}. \tag{6.75}$$

According the $\mathcal{S}$-*procedure* [87, §B.2], the two quadratic inequalities in (6.74) hold iff there exists $\mu_1 \geq 0$ such that

$$\begin{bmatrix} \mu_1\mathbf{I}_{N_aN_r} + \mathbf{D} & \mathbf{D}\hat{\mathbf{h}}_a \\ \hat{\mathbf{h}}_a^H\mathbf{D} & -\mu_1\epsilon_{ab}^2 + \hat{\mathbf{h}}_a^H\mathbf{D}\hat{\mathbf{h}}_a - \varpi r_{ab}^{\alpha}\sigma_b^2 \end{bmatrix} \succeq \mathbf{0}. \tag{6.76}$$

Now we observe that (6.72c) is exactly the same as (6.30b). Therefore we can reformulate it into a inequality similar to (6.42a) and the LMIs (6.43) and (6.44) but without considering the Charnes-Cooper transformation. Finally, we obtain for a fixed β the following SDP

$$\min_{\substack{\mathbf{C}_w,\mathbf{C}_{\eta_a},\mathbf{C}_{\eta_b},\\ v_k,t_k,\mu_1,\mu_{2_k},\mu_{3_k}}} \operatorname{Tr}\{\mathbf{C}_w\} + \operatorname{Tr}\{\mathbf{C}_{\eta_a}\} + \operatorname{Tr}\{\mathbf{C}_{\eta_b}\} \tag{6.77a}$$

$$\text{s.t.} \begin{bmatrix} \mu_1 \mathbf{I}_{N_a N_r} + \mathbf{D} & \mathbf{D}\hat{\mathbf{h}}_a \\ \hat{\mathbf{h}}_a^H \mathbf{D} & -\mu_1 \epsilon_{ab}^2 + \hat{\mathbf{h}}_a^H \mathbf{D} \hat{\mathbf{h}}_a - \varpi r_{ab}^{\alpha} \sigma_b^2 \end{bmatrix} \succeq \mathbf{0} \tag{6.77b}$$

$$v_k - t_k - (\beta - 1) r_{ae_k}^{\alpha} \sigma_e^2 \leq 0 \tag{6.77c}$$

$$\begin{bmatrix} \mu_{2_k} \mathbf{I}_{N_a} - \mathbf{C} & -\mathbf{C}\hat{\mathbf{g}}_{a_k} \\ -\hat{\mathbf{g}}_{a_k}^H \mathbf{C} & -\mu_{2_k} \epsilon_{ae}^2 - \hat{\mathbf{g}}_{a_k}^H \mathbf{C} \hat{\mathbf{g}}_{a_k} + v_k \end{bmatrix} \succeq \mathbf{0} \tag{6.77d}$$

$$\begin{bmatrix} \mu_{3_k} \mathbf{I}_{N_n} + (\beta - 1) \rho_k^{\alpha} \mathbf{C}_{\eta_b} & (\beta - 1) \rho_k^{\alpha} \mathbf{C}_{\eta_b} \hat{\mathbf{g}}_{b_k} \\ (\beta - 1) \rho_k^{\alpha} \hat{\mathbf{g}}_{b_k}^H \mathbf{C}_{\eta_b} & \vartheta_{4_k} \end{bmatrix} \succeq \mathbf{0} \tag{6.77e}$$

$$\mathbf{C}_w \succeq \mathbf{0}, \mathbf{C}_{\eta_a} \succeq \mathbf{0}, \mathbf{C}_{\eta_b} \succeq \mathbf{0}, v_k \geq 0, t_k \geq 0 \tag{6.77f}$$

$$\mu_1 \geq 0, \mu_{2_k} \geq 0, \mu_{3_k} \geq 0, \forall k = 1, \cdots, K \tag{6.77g}$$

where we use the slack variables $v_k, t_k, \mu_1, \mu_{2_k}, \mu_{3_k}$ and the vectorised channel $\hat{\mathbf{h}}_a = \text{vec}(\hat{\mathbf{H}}_a)$. We define the auxiliary variables

$$\begin{aligned} \mathbf{C} &= \mathbf{C}_w - (\beta - 1)\mathbf{C}_{\eta_a} \\ \mathbf{D} &= \mathbf{I}_{N_r} \otimes \mathbf{C}_w - \frac{\omega}{N_r} \mathbf{I}_{N_r} \otimes \mathbf{C}_{\eta_a} \\ \vartheta_{4_k} &= -\mu_{3_k} \epsilon_{be}^2 + (\beta - 1) \rho_k^{\alpha} \hat{\mathbf{g}}_{b_k}^H \mathbf{C}_{\eta_b} \hat{\mathbf{g}}_{b_k} - t_k \\ \varpi &= 2^R \beta - 1. \end{aligned} \tag{6.78}$$

The above SDP is efficiently solved by interior-point algorithms based software [105] assisted by toolboxes like the ones in [106, 107].

We note that the solution of the SDP (6.77) does not lead in general to a solution where rank($\mathbf{C}_w^{\star}$)=1 holds. Therefore, as discussed in remark 9, the solution for the SDP (6.77) is suboptimal to the original problem (6.71). Finally, we need to retrieve the optimal $\beta^{\star}$ that delivers the target R_S^{wc} with the minimum use of power. This can be done by using a linear searching algorithm similar to the one in §4.4.2 of chapter 4. If the SDP (6.77) is infeasible for all the analysed values of β, then the system is considered in outage and transmission does not take place.

6.4.4 Numerical results

We concentrate our analysis on the resource allocation and secrecy performance of our proposed jointly AN generation technique under various scenarios. In comparison to §6.3 where we take advantage of the characteristics of the instantaneous CSI of the links to select the best possible antenna configuration at the receiver that delivers the largest secrecy rate, here we study the overall average performance

Table 6.3: *Parameters values used for the simulations.*

Parameter	Value	Description
N_a	3	Alice's number of antennas
N_b	4	Bob's number of antennas
$\sigma^2_{\hat{g}_a}$	1	Alice-to-Eve's channel elements variance
$\sigma^2_{\hat{g}_b}$	1	Bob-to-Eve's channel elements variance
$\sigma^2_{\hat{H}}$	1	Alice-to-Bob's channel elements variance
ϵ_{ab}	0.1	Main channel uncertainty
σ^2_b	1	Bob's AWGN power
σ^2_e	1	Eve's AWGN power
α	2	Path loss exponent

of the technique by considering the mean performance between all the channel realisations. This procedure simplifies the analysis, but we lose the opportunity to take advantage of the instantaneous CSI between the transmission parties to enhance the secrecy. This average analysis is particularly useful and allows a fair comparison against the passive eavesdropping case where the eavesdropping links CSI are not available. Monte Carlo trials are considered with the parameters listed in Table 6.3.

It is worth remarking that, in contrast to the previous §6.3.1, here we have considered the case of multiple single-antenna eavesdroppers. This different assumption in the problem topology, as we will see in the results, will provide an interesting new insight for the power allocation, specially for the passive eavesdropping case not studied before. On the other hand, this setup will confirm that the best strategy for the security in the single-antenna active eavesdropping scenario is to use all the receiver's antennas for reception.

Figure 6.8 shows the eavesdropping links' CSI uncertainty effect over the power allocation strategy. Here, more power is devoted to AN generation in the high uncertainty regime; interestingly, and in contrast with the results in the MIMO wiretap channel case in §6.3.2, now the strategy generates jointly AN from both Alice (mainly) and from Bob to confuse the single-antenna eavesdroppers. This difference in the power allocation outcome is due to the presence of multiple single-antenna eavesdroppers. Indeed, Figure 6.9 confirms the previous result in remark 7 showing that in the presence of single-antenna active eavesdroppers, the best

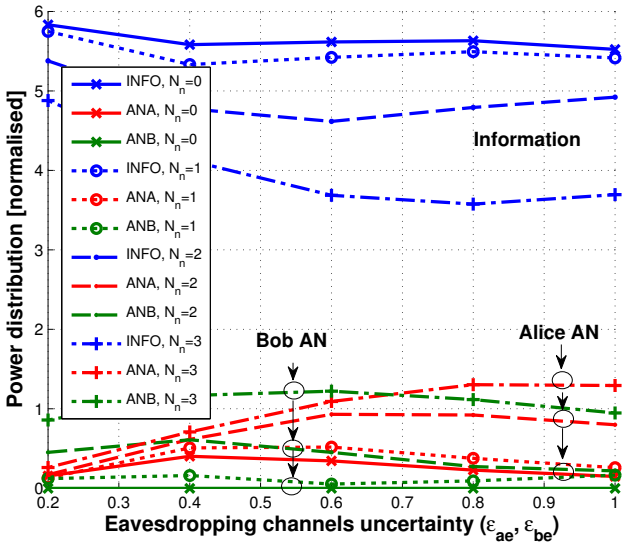


Figure 6.8: *Power allocation. Active eavesdropping power distribution between information (INFO), Alice AN (ANA) and Bob AN (ANB) vs. eavesdropping channel uncertainty* ($\epsilon_{ae}, \epsilon_{be}$) *for different receiving/AN-generating antennas at Bob* (N_r, N_n) *when* $K = 2$, $P_{max} = 6$ *(normalised relative to AWGN power) and* $r_{be} = r_{ae} = 1$ *(relative to* r_{ab}*).*

way to enhance the R_S^{wc} is to use all the available antennas at Bob to receive the information even under uncertainty in the eavesdropping link. In this scenario it is justified that Alice has to generate the AN. In other words, even under erroneous instantaneous CSI availability the best security strategy is to exploit the full degree of freedom of the MIMO main channel. Remarkably, the robust strategy presented can achieve high R_S^{wc} even under the eavesdropping links high CSI uncertainty. It is also worth pointing out that the joint AN generation scheme achieves the same average security performance as the traditional Alice-AN alone approach.

Now we turn our attention to the passive eavesdropping case studied in §6.4.2 and depicted in Figures 6.10 and 6.11 where the distances between nodes considered are available. As in §6.3.4 and illustrated in Figure 6.5, we again consider a travelling eavesdropper moving in a straight line from Alice towards Bob and beyond. Therefore, in Figures 6.10 and 6.11 the x-axis specifies only the Alice-to-Eve distance while the Bob-to-Eve distance can be easily inferred.

Figure 6.10 shows how the distance between the nodes influences the AN source selection. Interestingly, for the passive eavesdropping case, Bob is preferred as the AN generator while Alice only broadcasts AN when Eve is close to her. The se-

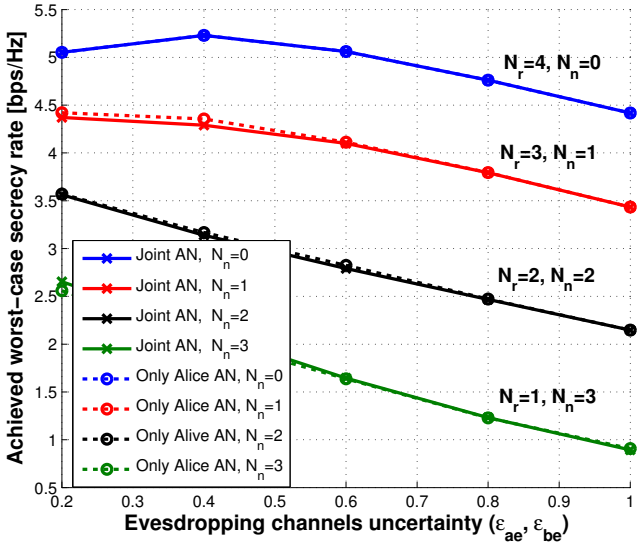


Figure 6.9: *System Performance. Active eavesdropping achieved worst-case secrecy rate (R_S^{wc}) comparison between joint AN and only Alice AN generation vs. eavesdropping channel uncertainty ($\epsilon_{ae}, \epsilon_{be}$) for different receiving/AN-generating antennas at Bob (N_r, N_n) when $K = 2$, $P_{max} = 6$ (norm. relative to AWGN power) and $r_{be} = r_{ae} = 1$ (relative to r_{ab}).*

curity performance is shown in Figure 6.11 where, and in contrast to the active eavesdropping case (under eavesdropping channel uncertainties), the best strategy now to maximise R_S^{wc} is to devote some of Bob's antennas to AN generation and leave Alice with only the information transmission task. The best performance is attained when Eve is close to Bob because less power is needed for AN leaving more resources to convey the information. The results in Figure 6.11 suggest that secrecy can be improved if the AN is broadcast by Bob compared to the traditional scheme where Alice solely generates AN. Figure 6.12 clearly compares the attained performance between passive and active eavesdropping (with eavesdropping channel uncertainties). Here it is shown that for the passive case, it is worth allocating the receiver's antennas to broadcast AN to maximise R_S^{wc} while for the active case, the best strategy (for single-antenna eavesdroppers) is to use all the receiver's antennas for reception.

Figure 6.13 illustrates the power allocation for the worst-case secrecy rate maximisation subject to individual power constraints in the presence of an active eavesdropper. This problem is studied in §6.4.2 where it is assumed that Alice and Bob have available an erroneous version of the eavesdropping links' CSI. The results

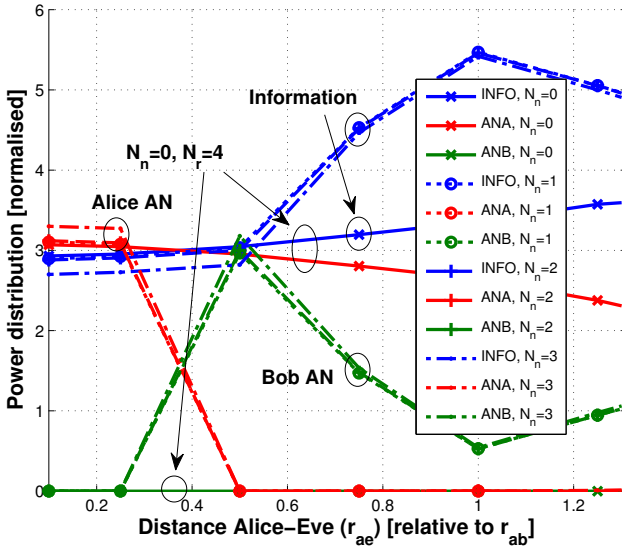


Figure 6.10: *Power allocation. Passive eavesdropping power distribution between information (INFO), Alice AN (ANA) and Bob AN (ANB) vs. Alice-Eve distance (r_{ae}) for different receiving/AN-generating antennas at Bob (N_r, N_n) when $P_{max} = 6$ (normalised relative to AWGN power) and $r_{be} = r_{ae} = 1$ (relative to r_{ab}).*

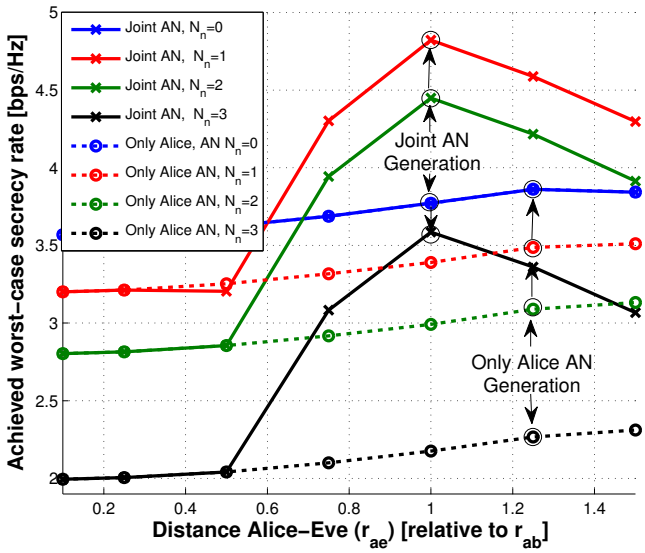


Figure 6.11: *System Performance. Achieved passive eavesdropping R_S^{wc} comparison between joint AN and only Alice AN vs. Alice-Eve distance (r_{ae}) for different receiving/AN-generating antennas at Bob (N_r, N_n) when $P_{max} = 6$ (normalised relative to AWGN power) and $r_{be} = r_{ae} = 1$ (relative to r_{ab}).*

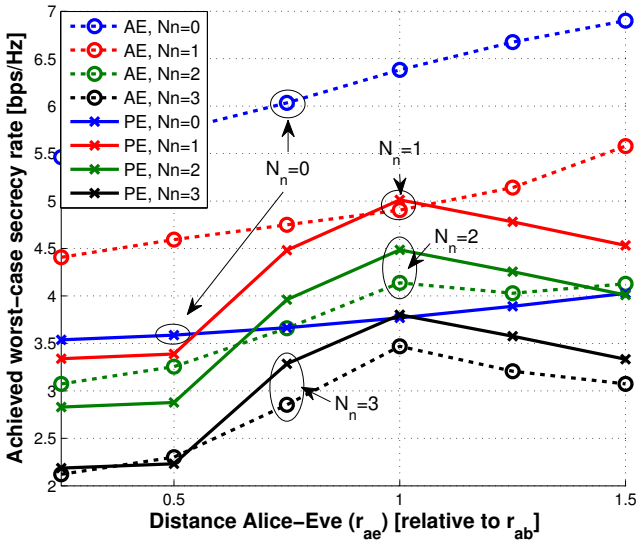


Figure 6.12: *System Performance. Achieved R_S^{wc} comparison between passive and active eavesdropping vs. Alice-Eve distance (R_{ae}) for different receiving/AN-generating antennas at Bob (N_r, N_n) when $P_{max} = 5$ (normalised relative to AWGN power) and $r_{be} = r_{ae} = 1$ (relative to r_{ab}).*

show that, following intuition, Bob uses all his available power to jam the attacker irrespective of its location. This strategy allows Alice to devote her power mainly to conveying the information; however, when Eve is close to Alice, she still broadcasts AN to secure the transmission in the presence of a close active single-antenna eavesdropper.

Now we devote our attention to the results of the power minimisation problem studied in §6.4.3. Figure 6.14 depicts the power allocation resulting from solving the SDP (6.77) to guarantee different values of the target worst-case secrecy rate R. Here, the results suggest that the robust joint AN technique consumes more power than transmitting AN only from Alice to achieve a target R. This result is corroborated in Figure 6.15 where it is obvious that for single-antenna active eavesdropping the best strategy to minimise the power consumption is to devote all of Bob's antennas for reception irrespective of the location of the eavesdropper. This result again coincides with our finding in the remark 7 where we concluded that allocating antennas at Bob is useful only when the rank of the MIMO main channel is equal to or smaller than the rank of the eavesdropping channel. That is not the case of the MISO eavesdropping channel (rank-one) case considered here.

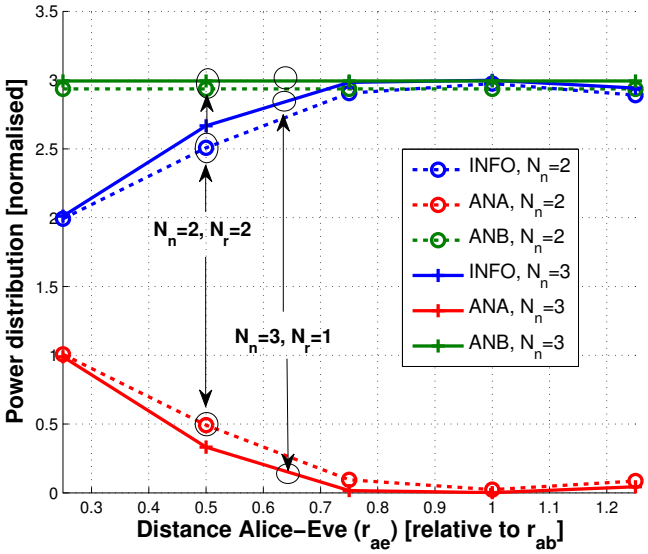


Figure 6.13: *Power allocation in an individually constrained network between information (INFO), Alice AN (ANA) and Bob AN (ANB) vs. Alice-Eve distance (r_{ae}). Active eavesdropping case for different receiving/AN-generating antennas at Bob (N_r, N_n) when $K = 1$, $P_{max} = 6$ (normalised relative to AWGN power), $\epsilon_{ae} = \epsilon_{be} = 0.5$ and $r_{be} = r_{ae} = 1$ (relative to r_{ab}).*

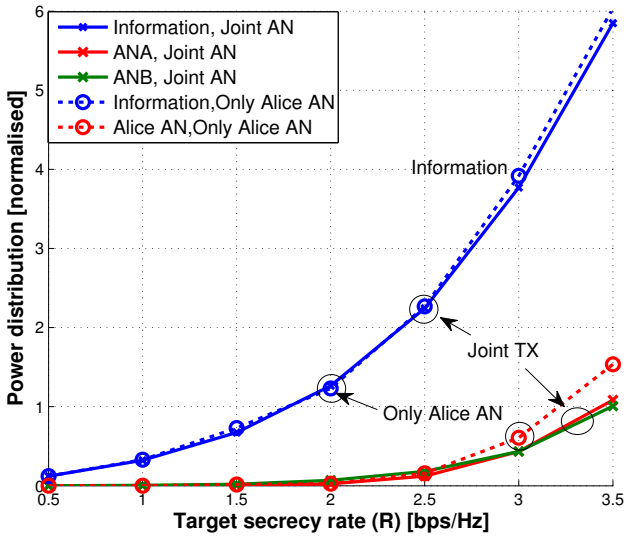


Figure 6.14: *Power allocation. Active eavesdropping minimum power (normalised relative to AWGN power) required for information, Alice AN (ANA) and Bob AN (ANB) to guarantee an average worst-case secrecy rate R. The receiving/AN-generating antennas at Bob are $N_r = N_n = 2$, $K = 1$, $\epsilon_{ae} = \epsilon_{be} = 0.5$ and $r_{be} = r_{ae} = 1$ (relative to r_{ab}).*

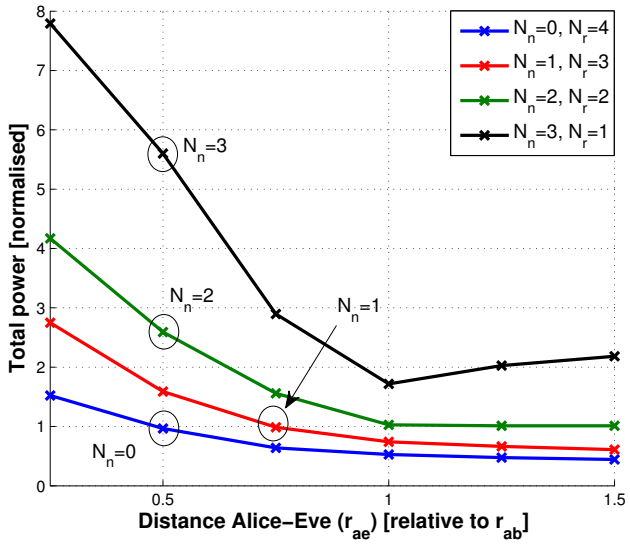
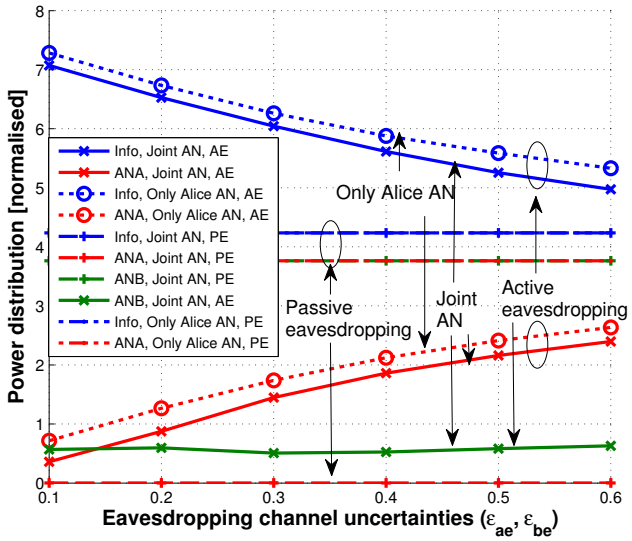
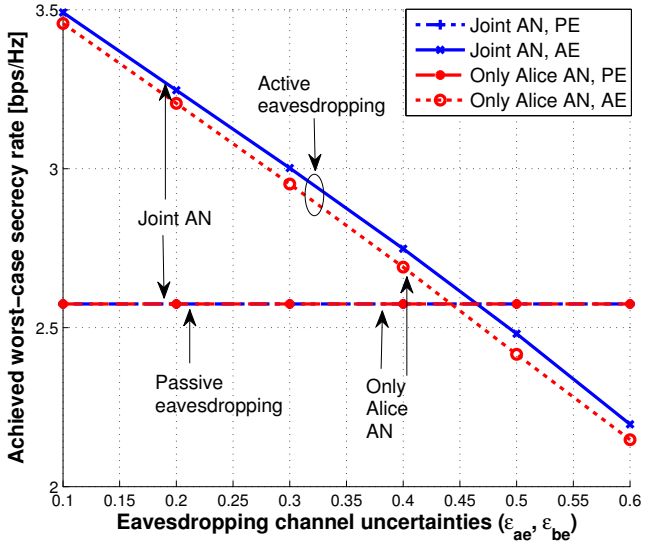


Figure 6.15: *Total power. Active eavesdropping minimum total power (normalised relative to AWGN power) to guarantee an average worst-case secrecy rate $R = 2$ bps/Hz vs. Alice-to-Eve distance (r_{ae}) (relative to r_{ab}) for different number of receiving/AN-generating antennas at Bob (N_r, N_n) when $K = 1$, and $\epsilon_{ae} = \epsilon_{be} = 0.5$.*

Finally, Figure 6.16a shows a comparison between the joint AN transmission strategy and the traditional approach where only Alice generates AN to maximise the worst-secrecy rate. Here we consider that Alice uses only one antenna for receiving information. Moreover, we assume the presence of two eavesdroppers and that the distances between all four nodes are set to unity. For the case of active eavesdropping (with uncertainty in the eavesdropping channel), our strategy generates AN from both Alice and Bob depending on the instantaneous channel conditions. By contrast, for the passive case our technique generates AN only from Bob rather than from Alice. Due to a lack of the eavesdropping links' instantaneous CSI, the approach avoids leaking Alice's AN to Bob, so Alice only conveys the information while Bob isotropically broadcasts AN. For the passive eavesdropping case the power allocated for information and AN is the same in both of the techniques benchmarked; however, the difference is that the joint AN generation strategy broadcasts the AN from Bob. The worst-case security rate achieved is depicted in Figure 6.16b; here, the flexibility introduced by the joint AN generation scheme is reflected in a slight improvement in R_S^{wc} for the active eavesdropping case whilst for the passive scenario both techniques achieve the same performance.



(a) *Power allocation*



(b) *Secrecy performance*

Figure 6.16: *Comparison of techniques for secrecy rate maximisation. Power allocation and* R_S^{wc} *vs. eavesdropping channels uncertainty* $(\epsilon_{ae}, \epsilon_{be})$ *for two eavesdroppers* $(K = 2)$ *when* $N_n = 3, r_{ae} = r_{be} = 1$ *(relative to* r_{ab}*) and* $P_{max} = 8$ *(normalised relative to AWGN power) for passive (PE) and active (AE) eavesdropping.*

6.5 Discussion and summary

In this chapter we have studied a joint transmitter and receiver AN generation technique to enhance the security of the wiretap MIMO channel. First, we have considered perfect channel state information in all the links in order to study whether the receiver can enhance the secrecy of the multiple antenna wiretap channel by transmitting AN from some of its antennas. Indeed, a judicious allocation of the receiver's antennas can provide a larger secrecy rate compared to the secrecy capacity obtained when the receiver uses all its antennas to receive information. In order to take advantage of the instantaneous channel conditions, we have introduced two low-complexity antenna selection techniques to determine the best antenna configuration that enhances the secrecy rate of the system. We have shown that transmitting AN from the receiver is particularly useful when the eavesdropping channel has greater capacity than the main channel; for instance, when the multi-antenna eavesdropper has more antennas than the receiver or it is closer to the transmitter. On the other hand, the technique has proved, like other contributions, that generating AN from the transmitter does not enhance the secrecy of the multiple-antenna wiretap channel.

Secondly, we have studied a practical case that arises when the channel state information of the transmission parties available at the legitimate nodes are subject to errors. To deal with this scenario, we have investigated a robust approach for multiple-antenna systems that generate AN from both legitimate communication parties. The strategy copes with inaccurate channel state information in all the instantaneous links to address the worst-case secrecy rate maximisation subject to global and individual power constraints and the total power consumption minimisation. Moreover, we have addressed the practical case when the eavesdroppers remain silent within the network and therefore only statistical information about the eavesdropping links can be assumed. The proposed suboptimal technique introduces a lower-bound approximation to the worst-case secrecy rate to deal with the optimisation problems in a tractable way. In contrast with the first case, here we have considered multiple single-antenna eavesdroppers. In this scenario, the results confirm that the best strategy to enhance the secrecy of the system when the attackers are totally or partially known is to exploit the full degree of freedom of the multiple-antenna main link; i.e., to use all the receiver's antennas to listen to

the communication. Here, transmitting AN from the transmitter might be useful; particularly, when the eavesdroppers are close to it. On the other hand, if there is no information regarding the eavesdroppers then allocating antennas at the receiver is useful to maximise the secrecy rate. The power distribution depends upon the instantaneous channel conditions and the location of the nodes.

It is important to point out that for fairness of comparison with the traditional scheme that generates AN only from the transmitter, this analysis has been carried out considering a global power constrained system. We also have considered the individually constrained network where the utility of our joint AN generation scheme in practical networks is larger. Indeed, the proposed transmission scheme is particularly attractive in systems where the resources of the transmitter (in terms of power and number of antennas) are restricted, such as the uplink of a wireless system. In such a system, the base station (the receiver) can improve the security by judiciously exploiting its available resources to jam eavesdroppers.

The secure approach presented in this chapter introduces flexibility regarding the AN generation to enhance the system security by generating a jamming signal from the receiver and/or from the transmitter. Indeed, the introduced secure scheme proposes to opportunistically jointly broadcast AN. The generation source selection will depend upon the particular transmission characteristics such as the number of antennas at the nodes, the instantaneous fading channel conditions, the location of the transmission nodes, etc. We have proposed an intelligent strategy to define the best transmission scheme to enhance security in the multiple-antenna wiretap channel. This endeavour compares positively with traditional secure masked transmission mechanisms where the AN is solely generated by the transmitter. The work proposed opens interesting fields for further research such as joint AN robust transmission techniques in the presence of multiple-antenna eavesdroppers. Of particular interest is the case where partial or no information about the eavesdropping channels is available at the legitimate nodes. These scenarios would require stronger and technically challenging security policies such as a probabilistic security definition based an in outage formulation.

Chapter 7

Conclusions

> 'You reached for the secret too
> soon; you cried for the moon.
> Shine on you crazy diamond.'
>
> R. Waters, R. Wright, D. Gilmour.

This thesis has described the security vulnerabilities of wireless communications and pointed out the paramount importance of addressing them from new perspectives. In particular, we have drawn attention to confidentiality issues arising from the broadcast nature of the radio frequency wireless channel. We have identified physical layer security as a promising framework to secure wireless networks against eavesdropping threats from an information-theoretic perspective. Physical layer security addresses wireless vulnerabilities where the weaknesses lie; i.e., at the transmission level.

We have provided signal processing multiple-antenna transmission schemes to secure wireless communications at the physical layer against eavesdropping attacks. We have chosen masked transmission strategies to improve the security by steering the information towards the intended receiver and at the same time broadcasting artificial noise to confuse eavesdroppers. We have considered practical scenarios where networks are constrained in transmission resources and only have erroneous information regarding the mathematical representation of the link between legitimate transmission parties. We have addressed worst-case security perspectives by considering eavesdroppers without computational restrictions that can take advantage of any situation to put at risk the security of the system.

The beginning of this thesis is devoted to the study of MISO systems; that is a multiple-antenna transmitter conveying a confidential message towards a single-antenna receiver in the presence of single-antenna eavesdroppers. In this scenario, we have distributed the power between information and artificial noise to guarantee a high probability of secrecy even in the presence of eavesdroppers close to the transmitter. We introduced a protected zone to physically prevent close-quarter eavesdropping attacks. We have quantified the secrecy improvements and the possible energy savings resulting from extending the size of the exclusion area. At the same time, we determined the additional amount of power required, mainly for artificial noise generation, to secure the networks from close eavesdroppers.

We have addressed the practical case of a transmitter only aware of an erroneous mathematical representation of the link between the legitimate transmission parties. In this context, a MISO robust transmission scheme has been presented to provide high levels of security, given by the worst-case secrecy rate, in the presence of unknown eavesdroppers. Again, we have considered closer attackers to provide security at the expense of additional power. We have also presented a strategy to prioritise and minimise the use of power and reduce the size of the protected zone to ensure an average worst-case secrecy rate. We have shown that the optimal transmission strategy that attains the largest secrecy rate is to beamform the information towards the intended receiver and broadcast the artificial noise isotropically and orthogonal in the direction of the steering message.

In the second part of this thesis, we have addressed security in the MIMO wiretap channel; that is, all the communication devices are equipped with multiple-antennas. First, we considered a suboptimal masked beamforming strategy to study the security opportunities that the frequency selective channel offers when all the nodes use OFDM signalling. Remarkably, we showed that the security of the system can be enhanced by taking advantage of an opportunistic power allocation between the OFDM subcarriers. We paid attention to a multiple-antenna eavesdropper that, by using smart combining schemes, can jeopardise the security by cancelling the jamming effect of the artificial noise.

Finally, we have introduced a secure transmission alternative for resources constrained networks. Here we have exploited the full degree of freedom of the MIMO wiretap channel instead of limiting the transmission technique to a beamforming scheme. We introduced the novel idea of a joint artificial noise transmis-

sion where the receiver allocates its resources to contribute actively to secure the communication. We have shown that a remarkable enhancement in the security can be attained; particularly, in cases when the main channel is worse than the eavesdropping one. Our technique has shown that generating artificial noise from the transmitter is not useful in improving the security. However, at the receiver's antenna array, if we opportunistically switch some of the antennas between reception and broadcasting artificial noise we can make a positive contribution to the system's security by taking advantage of the instantaneous channel conditions. We have provided two schemes to reduce the complexity of determining the best receiver's antenna distribution. Finally, we also have considered the effect of erroneous channel information between all the transmission nodes providing a robust scheme that can improve the security by dynamically choosing the jamming source.

In conclusion, this thesis has presented innovative and effective multiple-antenna signal processing strategies that take advantage of the wireless channel conditions to secure wireless networks at the physical layer. We have considered practical problems to devise smart secure endeavours that look at securing transmissions by preventing the eavesdroppers from even receiving the wireless signal.

7.1 Further research

The first problem that has already attracted our attention is providing a robust joint transmitter/receiver artificial noise generation transmission scheme in the presence of multiple-antenna eavesdroppers. As in §6.4.1 of chapter 6, two scenarios can be considered. First, the case of an eavesdropper whose channel signature is only partially known (subject to uncertainties), and second, a pure passive multiple-antenna eavesdropper. The maximisation of the secrecy rate is particularly complicated in both scenarios; indeed, outage formulations are needed to ensure secrecy from a probabilistic point of view. The resulting optimisation problems are particularly challenging and require sophisticated mathematical tools to reformulate them into tractable convex expressions [145]. To solve this problem we look at alternating optimisation techniques such as those used in [127, 128].

The work presented in this thesis addresses security and confidentiality issues in point-to-point single-user networks. In practical networks, the radio frequency

spectrum is shared among multiple users communicating with a centralised entity such as a base station or an access point. Therefore, it is crucial to address security issues in multi-user networks paying attention to the broadcasting and multicasting channels [32]. In the first scenario, a common message is transmitted to multiple legitimate receivers, while in the second scenario multiple confidential messages are transmitted to multiple intended receivers. These multi-user scenarios present new security issues arising from the cases when a legitimate user of the network becomes a potential eavesdropper of a message that is not intended for it. Physical layer security in multi-user networks has recently attracted attention in the information-theory research community. Here, the multi-receiver wiretap channel and the compound wiretap channel are the information-theoretic concepts that characterise broadcasting and multicasting networks respectively [31, 146, 147, 148]. Our particular research interest is in multi-user signal processing strategies considering joint artificial noise generation, and how this can improve the security of the system without interfering with other valid users.

Emerging multi-layer security approaches are an exciting direction of research that have the potential to offer a holistic approach towards securing wireless networks. For instance, as the wiretap model requires a pre-authenticated channel, and it does not confront security vulnerabilities arising from impersonation threats. Therefore, complementary security strategies, still based on the physical layer, are necessary to provide security services such as authentication. This could be done through introducing a unique mark on the transmitted information, by fingerprinting the conveyed message as a way to validate legitimate users credentials [45]. Moreover, the wireless channel's randomness can be exploited to distil security keys by taking advantage of the uniqueness and random characteristic of the instantaneous wireless link between the two legitimate users [149]. This potentially would overcome traditional cryptographic key administration and distribution issues. Both aforementioned strategies are traditionally performed at the upper layers of the communication model, so incorporating the physical layer as a source of secrecy leads to multiple-layer security approaches that promise to be a robust and effective way to secure wireless networks.

Finally, a crucial area for further research work is to provide practical proof-of-concept of physical layer security. Although the past few years have seen many theoretical advances in physical layer security, the lack of practical demonstrators

of these concepts is noticeable. Indeed, fundamental research is still necessary towards the realisation of practical secure networks at the physical layer. Here an integrated research perspective which considers the interdependence and interrelationships between different security approaches has to be considered. The objective is to close the gap between theory and practice and then create an integrated realisation of wireless networks secured at the physical layer where the wireless channel is the source of secrecy. This research approach will enable the development of solutions that have the potential to actually be deployed in the real world to confront current and emerging wireless security threats.

References

[1] F. T. Sheldon, J. M. Weber, S.-M. Yoo, and W. D. Pan, "The Insecurity of Wireless Networks," *Security Privacy, IEEE*, vol. 10, no. 4, pp. 54 –61, Aug. 2012. 2, 14

[2] L. Buttyan and J. Hubaux, *Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing*. Cambridge University Press, 2008. 3

[3] M. La Polla, F. Martinelli, and D. Sgandurra, "A Survey on Security for Mobile Devices," *Communications Surveys Tutorials, IEEE*, vol. 15, no. 1, pp. 446–471, Mar. 2013. 3

[4] Q. Li and G. Clark, "Mobile Security: A Look Ahead," *Security Privacy, IEEE*, vol. 11, no. 1, pp. 78–81, Jan. 2013. 3

[5] B. Schneier, "Cryptographic Design Vulnerabilities," *COMPUTER*, vol. 31, no. 9, pp. 29+, Sep. 1998. 3, 14

[6] X. Du and H.-H. Chen, "Security in wireless sensor networks," *Wireless Communications, IEEE*, vol. 15, no. 4, pp. 60–66, Aug 2008. 4

[7] W. Saad, X. Zhou, Z. Han, and H. Poor, "On the Physical Layer Security of Backscatter Wireless Systems," *Wireless Communications, IEEE Transactions on*, vol. 13, no. 6, pp. 3442–3451, Jun. 2014. 6

[8] E. A. Jorswieck, A. Wolf, and S. Gerbracht, *Secrecy on the Physical Layer in Wireless Networks*. Technische Universitt Dresden, 2010, ch. 20, pp. 413–435. 7

[9] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011. 7

[10] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer*. Springer, 2010. 7

[11] E. Jorswieck, L. Lai, W.-K. Ma, H. Poor, W. Saad, and A. L. Swindlehurst, "Guest editorial for Signal Processing for Wireless Physical Layer Security," *Selected Areas in Communications, IEEE Journal on*, vol. 31, no. 9, Sep. 2013, Special Issue on Signal Processing for Wireless Physical Layer Security. 8

[12] T. Duong, D. da Costa, K. Kim, K.-H. Liu, and V. Quoc Bao, "Guest editorial for Secure Physical Layer Communications," *Communications, IET*, vol. 8, no. 8, May 2014, Special Issue on Secure Physical Layer Communications. 8

[13] W. Trappe, V. Poor, H. Iwai, A. Yener, P. Prucnal, and J. Barros, "Guest editorial special issue on using the physical layer for securing the next generation of communication systems," *Information Forensics and Security, IEEE Transactions on*, vol. 6, no. 3, Sep. 2011, Special Issue on Using the Physical Layer for Securing the Next Generation of Communication Systems. 8

[14] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless Information-Theoretic Security," *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008. 12, 14, 30, 166

[15] C. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal, Vol 28, pp. 656-715*, Oct. 1949. 12, 17

[16] A. D. Wyner, "Wire-Tap Channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975. 12, 15, 16, 17, 18

[17] I. Csiszar and J. Korner, "Broadcast Channels with Confidential Messages," *Information Theory, IEEE Transactions on*, vol. 24, no. 3, pp. 339–348, May 1978. 13, 15

[18] W. Diffie and M. Hellman, "New directions in cryptography," *Information Theory, IEEE Transactions on*, vol. 22, no. 6, pp. 644–654, Nov. 1976. 13

[19] B. Zhou, A. Marshall, and T.-H. Lee, "Wireless Security Issues in Pervasive Computing," in *Genetic and Evolutionary Computing (ICGEC), 2010 Fourth International Conference on*, Dec. 2010, pp. 509–512. 13

[20] I. Rasheed, A. Amin, M. Chaudhary, S. Bukhari, M. Rizwan, and K. Ali, "Analyzing the security techniques used in LTE Advanced and their evaluation," in *Digital Information Management (ICDIM), 2013 Eighth International Conference on*, Sep. 2013, pp. 11–13. 13

[21] W. Mao, *Modern Cryptography: Theory and Practice.* Prentice Hall Professional Technical Reference, 2003. 14

[22] A. Paladino, K. Phanse, and S. Ahmad. (2010) Hole196 Vulnerability in WPA2. [Online]. Available: http://www.airtightnetworks.com/fileadmin/pdf/WPA2-Hole196-Webinar-Presentation.pdf 14

[23] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Advances in Cryptology - EUROCRYPT 2000*, ser. Lecture Notes in Computer Science, B. Preneel, Ed. Springer Berlin Heidelberg, 2000, vol. 1807, pp. 351–368. 17, 24

[24] A. Suresh, A. Subramanian, A. Thangaraj, M. Bloch, and S. McLaughlin, "Strong secrecy for erasure wiretap channels," in *Information Theory Workshop (ITW), 2010 IEEE*, Aug. 2010, pp. 1–5. 17

[25] S. Leung Yan Cheong and M. Hellman, "The Gaussian Wire-tap Channel," *Information Theory, IEEE Transactions on*, vol. 24, no. 4, pp. 451–456, Jul. 1978. 18

[26] S. Bashar, Z. Ding, and C. Xiao, "On Secrecy Rate Analysis of MIMO Wiretap Channels Driven by Finite-Alphabet Input," *Communications, IEEE Transactions on*, vol. 60, no. 12, pp. 3816–3825, 2012. 18

[27] Y. Wu, C. Xiao, Z. Ding, X. Gao, and S. Jin, "Linear Precoding for Finite-Alphabet Signaling over MIMOME Wiretap Channels," *Vehicular Technology, IEEE Transactions on*, vol. 61, no. 6, pp. 2599–2612, 2012. 18

[28] J. Barros and M. Rodrigues, "Secrecy Capacity of Wireless Channels," in *2006 IEEE International Symposium on Information Theory*, Jul. 2006, pp. 356–360. 18

[29] P. Gopala, L. Lai, and H. El Gamal, "On the Secrecy Capacity of Fading Channels," *Information Theory, IEEE Transactions on*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008. 19

[30] Y. Liang, H. V. Poor, and S. Shamai, "Secure Communication Over Fading Channels," *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008. 19

[31] Y. Liang, G. Kramer, H. V. Poor, and S. Shitz, "Compound Wiretap Channels," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, p. 142374, 2009. 19, 182

[32] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," *CoRR*, vol. abs/1011.3754, 2010. 19, 182

[33] A. Hero, "Secure space-time communication," *Information Theory, IEEE Transactions on*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003. 19, 104

[34] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO Wiretap Channel," in *Information Theory, 2007. ISIT 2007. IEEE International Symposium on*, Jun. 2007, pp. 2471–2475. 19, 28, 105, 130

[35] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Information Theory, 2008. ISIT 2008. IEEE International Symposium on*, Jul. 2008, pp. 524–528. 19, 105, 130

[36] Y.-W. Hong, P.-C. Lan, and C.-C. Kuo, "Enhancing Physical-Layer Secrecy in Multiantenna Wireless Systems: An Overview of Signal Processing Approaches," *Signal Processing Magazine, IEEE*, vol. 30, no. 5, pp. 29–40, Sep. 2013. 19, 28

[37] S. Goel and R. Negi, "Guaranteeing Secrecy using Artificial Noise," *Wireless Communications, IEEE Transactions on*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008. 20, 29, 66, 133

[38] W. Harrison, J. Almeida, M. Bloch, S. McLaughlin, and J. Barros, "Coding for Secrecy: An Overview of Error-Control Coding Techniques for Physical-Layer Security," *Signal Processing Magazine, IEEE*, vol. 30, no. 5, pp. 41–50, Sep. 2013. 24

[39] A. Thangaraj, S. Dihidar, A. Calderbank, S. McLaughlin, and J. M. Merolla, "Applications of LDPC Codes to the Wiretap Channel," *Information Theory, IEEE Transactions on*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007. 24

[40] R. Liu, Y. Liang, H. Poor, and P. Spasojevic, "Secure Nested Codes for Type II Wiretap Channels," in *Information Theory Workshop, 2007. ITW '07. IEEE*, Sep. 2007, pp. 337–342. 24

[41] J. Muramatu, "Secret key agreement from correlated source outputs using LDPC matrices," in *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on*, Jun. 2004, pp. 15–21. 24

[42] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. Secret sharing," *Information Theory, IEEE Transactions on*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993. 24

[43] U. Maurer and S. Wolf, "Unconditionally secure key agreement and the intrinsic conditional information," *Information Theory, IEEE Transactions on*, vol. 45, no. 2, pp. 499–514, Mar. 1999. 24

[44] C. Bennett, G. Brassard, C. Crepeau, and U. Maurer, "Generalized privacy amplification," *Information Theory, IEEE Transactions on*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995. 24

[45] P. Yu and B. Sadler, "MIMO Authentication via Deliberate Fingerprinting at the Physical Layer," *Information Forensics and Security, IEEE Transactions on*, vol. 6, no. 3, pp. 606–615, Sep. 2011. 24, 182

[46] S. Shafiee and S. Ulukus, "Achievable Rates in Gaussian MISO Channels with Secrecy Constraints," in *IEEE International Symposium on Information Theory. ISIT 2007*, Jun. 2007, pp. 2466–2470. 28, 29, 66, 74, 100, 143, 164

[47] A. Khisti and G. Wornell, "Secure Transmission With Multiple Antennas I: The MISOME Wiretap Channel," *Information Theory, IEEE Transactions on*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010. 28, 66

[48] ——, "Secure Transmission With Multiple Antennas II: The MIMOME Wiretap Channel," *Information Theory, IEEE Transactions on*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010. 28, 104, 105, 130, 143

[49] Q. Li and W.-K. Ma, "Optimal transmit design for MISO secrecy-rate maximization with general covariance constraints," in *Intelligent Signal Processing and Communication Systems (ISPACS), 2010 International Symposium on*, Dec. 2010, pp. 1–4. 29, 66, 68

[50] ——, "Secrecy Rate Maximization of a MISO channel with multiple multi-antenna Eavesdroppers via Semidefinite Programming," in *Acoustics Speech and Signal Processing (ICASSP), 2010 IEEE International Conference on*, Mar. 2010, pp. 3042–3045. 29, 66, 68

[51] R. Negi and S. Goel, "Secret communication using artificial noise," in *Vehicular Technology Conference, 2005. VTC-2005-Fall. 2005 IEEE 62nd*, vol. 3, Sep. 2005, pp. 1906 – 1910. 29

[52] S. Gerbracht, A. Wolf, and E. Jorswieck, "Beamforming for fading wiretap channels with partial channel information," in *Smart Antennas (WSA), 2010 International ITG Workshop on*, Feb. 2010, pp. 394–401. 29, 67

[53] A. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on*, Apr. 2009, pp. 2437–2440. 29, 30, 34, 76, 88, 107, 114, 115, 154

[54] J. Li and A. Petropulu, "On Ergodic Secrecy Rate for Gaussian MISO Wiretap Channels," *Wireless Communications, IEEE Transactions on*, vol. 10, no. 4, pp. 1176–1187, 2011. 30, 74, 164

[55] X. Zhang, X. Zhou, and M. McKay, "Benefits of multiple transmit antennas in secure communication: A secrecy outage viewpoint," in *Signals, Systems and Computers (ASILOMAR), 2011 Conference Record of the Forty Fifth Asilomar Conference on*, Nov. 2011, pp. 212 –216. 30, 56, 166

[56] X. Zhou, M. McKay, B. Maham, and A. Hjondrungnes, "Rethinking the Secrecy Outage Formulation: A Secure Transmission Design Perspective," *Communications Letters, IEEE*, vol. 15, no. 3, pp. 302–304, Mar. 2011. 30, 166

[57] X. Zhou and M. McKay, "Physical Layer Security with Artificial Noise: Secrecy Capacity and Optimal Power Allocation," in *Signal Processing and Communication Systems, 2009. ICSPCS 2009. 3rd International Conference on*, Sep. 2009, pp. 1–5. 30, 114

[58] ——, "Secure Transmission With Artificial Noise Over Fading Channels: Achievable Rate and Optimal Power Allocation," *Vehicular Technology, IEEE Transactions on*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010. 30

[59] W. C. Liao, T. H. Chang, W. K. Ma, and C. Y. Chi, "QoS-Based Transmit Beamforming in the Presence of Eavesdroppers: An Optimized Artificial-Noise-Aided Approach," *Signal Processing, IEEE Transactions on*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011. 30, 39, 40, 43, 68, 76, 88, 154

[60] P. Pinto, J. Barros, and M. Win, "Physical-layer Security in Stochastic Wireless Networks," in *Communication Systems, 2008. ICCS 2008. 11th IEEE Singapore International Conference on*, Nov. 2008, pp. 974–979. 31

[61] X. Zhou, R. Ganti, J. Andrews, and A. Hjorungnes, "Secrecy transmission capacity of decentralized wireless networks," in *Communication, Control, and Computing, 2011 49th Annual Allerton Conference on*, Sep. 2011, pp. 1726–1732. 31

[62] M. Ghogho and A. Swami, "Characterizing physical-layer secrecy with unknown eavesdropper locations and channels," in *Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on*, May 2011, pp. 3432–3435. 31, 105, 138

[63] ——, "Physical-Layer Secrecy of MIMO Communications in the Presence of a Poisson Random Field of Eavesdroppers," in *IEEE ICC Workshop on Physical Layer Security, 2011*, Jun. 2011. 31, 105, 107, 115, 138

[64] A. Hasan and J. Andrews, "The Guard Zone in Wireless Ad hoc Networks," *Wireless Communications, IEEE Transactions on*, vol. 6, no. 3, pp. 897–906, Mar. 2007. 31

[65] X. Zhou, R. Ganti, J. Andrews, and A. Hjorungnes, "On the Throughput Cost of Physical Layer Security in Decentralized Wireless Networks," *Wireless Communications, IEEE Transactions on*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011. 31

[66] N. Chang, C.-B. Chae, J. Ha, and J. Kang, "Secrecy Rate for MISO Rayleigh Fading Channels with Relative Distance of Eavesdropper," *Communications Letters, IEEE*, vol. 16, no. 9, pp. 1408 –1411, Sep. 2012. 31

[67] S. Gerbracht, C. Scheunert, and E. Jorswieck, "Secrecy Outage in MISO Systems with Partial Channel Information," *Information Forensics and Security, IEEE Transactions on*, vol. 7, no. 2, pp. 704 –716, Apr. 2012. 33, 80, 100, 166

[68] X. Zhang, X. Zhou, and M. McKay, "On the Design of Artificial-Noise-Aided Secure Multi-Antenna Transmission in Slow Fading Channels," *Vehicular Technology, IEEE Transactions on*, vol. 62, no. 5, pp. 2170–2181, Jun. 2013. 33

[69] P. Huang and X. Wang, "Secrecy enhancement with artificial noise in decentralized wireless networks: A stochastic geometry perspective," in *Wireless Communications and Networking Conference (WCNC), 2013 IEEE*, Apr. 2013, pp. 935–940. 33

[70] J. Xiong, K.-K. Wong, D. Ma, and J. Wei, "A Closed-Form Power Allocation for Minimizing Secrecy Outage Probability for MISO Wiretap Channels via Masked Beamforming," *Communications Letters, IEEE*, vol. 16, no. 9, pp. 1496 –1499, Sep. 2012. 33, 166

[71] S. Chae, W. Choi, J. Lee, and T. Quek, "Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone," *Information Forensics and Security, IEEE Transactions on*, vol. PP, no. 99, pp. 1–1, 2014. 33

[72] A. Mukherjee and A. Swindlehurst, "Robust Beamforming for Security in MIMO Wiretap Channels With Imperfect CSI," *Signal Processing, IEEE Transactions on*, vol. 59, no. 1, pp. 351–361, Jan. 2011. 34, 69, 76, 88, 105, 107, 115, 138, 154

[73] T. Al-Naffouri and B. Hassibi, "On the Distribution of Indefinite Quadratic Forms in Gaussian Random Variables," in *IEEE International Symposium on Information Theory. ISIT 2009*, Jul. 2009, pp. 1744–1748. 37

[74] J. Taylor, M. Hempel, H. Sharif, S. Ma, and Y. Yang, "Impact of channel estimation errors on effectiveness of Eigenvector-based jamming for physical layer security in wireless networks," in *Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2011 IEEE 16th International Workshop on*, Jun. 2011, pp. 122–126. 67

[75] B. He, X. Zhou, and T. D. Abhayapala, "Wireless Physical Layer Security with Imperfect Channel State Information: A Survey," *CoRR*, vol. abs/1307.4146, 2013. 67

[76] S.-C. Lin, T.-H. Chang, Y.-L. Liang, Y. Hong, and C.-Y. Chi, "On the Impact of Quantized Channel Feedback in Guaranteeing Secrecy with Artificial Noise: The Noise Leakage Problem," *Wireless Communications, IEEE Transactions on*, vol. 10, no. 3, pp. 901 –915, Mar. 2011. 67

[77] Y.-L. Liang, Y.-S. Wang, T.-H. Chang, Y.-W. Hong, and C.-Y. Chi, "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise," in *Information Theory, 2009. ISIT 2009. IEEE International Symposium on*, Jun. 2009, pp. 2351–2355. 67

[78] A. Abdel-Samad and A. Gershman, "Robust transmit eigen-beamforming with imperfect knowledge of channel correlations," in *Communications, 2005. ICC 2005. 2005 IEEE International Conference on*, vol. 4, May 2005, pp. 2292 – 2296 Vol. 4. 67

[79] V. Sharma, I. Wajid, A. Gershman, H. Chen, and S. Lambotharan, "Robust Downlink Beamforming Using Positive Semi-Definite Covariance Constraints," in *Smart Antennas, 2008. WSA 2008. International ITG Workshop on*, Feb. 2008, pp. 36–41. 67

[80] M. Shenouda and T. Davidson, "On the Design of Linear Transceivers for Multiuser Systems with Channel Uncertainty," *Selected Areas in Communications, IEEE Journal on*, vol. 26, no. 6, pp. 1015–1024, Aug. 2008. 67

[81] J. Byun, A. Mutapcic, S.-J. Kim, and J. Cioffi, "A Minimax Regret Approach to Robust Beamforming," in *Vehicular Technology Conference Fall (VTC 2009-Fall), 2009 IEEE 70th*, Sep. 2009, pp. 1–6. 67

[82] E. Song, Q. Shi, M. Sanjabi, R. Sun, and Z.-Q. Luo, "Robust SINR-Constrained MISO Downlink Beamforming: When is Semidefinite Programming Relaxation Tight?" in *Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on*, May 2011, pp. 3096–3099. 67

[83] A. Abdel-Samad, A. Gershman, and T. Davidson, "Robust transmit beamforming based on imperfect channel feedback," in *Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th*, vol. 3, Sep. 2004, pp. 2049 – 2053 Vol. 3. 67

[84] J. Wang and D. Palomar, "Worst-Case Robust MIMO Transmission with Imperfect Channel Knowledge," *Signal Processing, IEEE Transactions on*, vol. 57, no. 8, pp. 3086 –3100, Aug. 2009. 67, 72, 152

[85] D. P. Palomar and Y. C. Eldar, Eds., *Convex optimization in signal processing and communications*. Cambridge, UK, New York: Cambridge University Press, 2010. 68

[86] Z.-Q. Luo and W. Yu, "An introduction to convex optimization for communications and signal processing," *Selected Areas in Communications, IEEE Journal on*, vol. 24, no. 8, pp. 1426–1438, Aug. 2006. 68

[87] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2007. 68, 75, 76, 78, 81, 89, 96, 97, 98, 100, 153, 156, 160, 161, 162, 164, 167

[88] L. Zhang, Y.-C. Liang, Y. Pei, and R. Zhang, "Robust Beamforming Design: From Cognitive Radio MISO Channels to Secrecy MISO Channels," in *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, Dec. 2009, pp. 1 –5. 68

[89] W. Shi and J. Ritcey, "Robust Beamforming for MISO Wiretap Channel by Optimizing the Worst-case Secrecy Capacity," in *Signals, Systems and Computers (ASILOMAR), 2010 Conference Record of the Forty Fourth Asilomar Conference on*, Nov. 2010, pp. 300 –304. 68

[90] Q. Li, W.-K. Ma, and A.-C. So, "Safe Convex Approximation to Outage-based MISO Secrecy Rate Optimization under Imperfect CSI and with Artificial Noise," in *Signals, Systems and Computers (ASILOMAR), 2011 Conference Record of the Forty Fifth Asilomar Conference on*, Nov. 2011, pp. 207 –211. 68, 80, 166

[91] J. Huang and A. Swindlehurst, "Robust Secure Transmission in MISO Channels with Imperfect ECSI," in *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*, Dec. 2011, pp. 1 –5. 68, 70

[92] ——, "Robust Secure Transmission in MISO Channels Based on Worst-Case Optimization," *Signal Processing, IEEE Transactions on*, vol. 60, no. 4, pp. 1696 –1707, Apr. 2012. 68, 70

[93] Q. Li and W.-K. Ma, "A Robust Artificial Noise Aided Transmit Design for MISO Secrecy," in *Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on*, May 2011, pp. 3436–3439. 68

[94] ——, "Spatially Selective Artificial-Noise Aided Transmit Optimization for MISO Multi-Eves Secrecy Rate Maximization," *Signal Processing, IEEE Transactions on*, vol. 61, no. 10, pp. 2704–2717, May 2013. 68

[95] M. Pei, J. Wei, K.-K. Wong, and X. Wang, "Masked Beamforming for Multiuser MIMO Wiretap Channels with Imperfect CSI," *Wireless Communications, IEEE Transactions on*, vol. 11, no. 2, pp. 544–549, Feb. 2012. 68, 105, 138

[96] Q. Li and W.-K. Ma, "Optimal and Robust Transmit Designs for MISO Channel Secrecy by Semidefinite Programming," *Signal Processing, IEEE Transactions on*, vol. 59, no. 8, pp. 3799–3812, Aug. 2011. 69, 77

[97] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. Bloch, S. Ulukus, and A. Yener, "Cooperative Security at the Physical Layer: A Summary of Recent Advances," *Signal Processing Magazine, IEEE*, vol. 30, no. 5, pp. 16–28, Sep. 2013. 70, 133

[98] E. Ekrem and S. Ulukus, *Cooperative secrecy in wireless communications*. Eds. New York: Springer-verlag, 2009. 70, 132

[99] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Improving Wireless Physical Layer Security via Cooperating Relays," *Signal Processing, IEEE Transactions on*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010. 70, 132, 133

[100] E. Tekin, "The Gaussian multiple access wire-tap channel: wireless secrecy and cooperative jamming," in *Information Theory and Applications Workshop, 2007*, Jan. 2007, pp. 404–413. 70, 133

[101] E. Tekin and A. Yener, "The General Gaussian Multiple-Access and Two-Way Wiretap Channels: Achievable Rates and Cooperative Jamming," *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2735 –2751, Jun. 2008. 70, 133

[102] N. Romero-Zurita, D. McLernon, M. Ghogho, and A. Swami, "PHY Layer Security Based on Protected Zone and Artificial Noise," *Signal Processing Letters, IEEE*, vol. 20, no. 5, pp. 487–490, May. 2013. 73, 85, 87, 112, 144, 166

[103] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage Probability Based Power Distribution Between Data and Artificial Noise for Physical Layer Security," *Signal Processing Letters, IEEE*, vol. 19, no. 2, pp. 71–74, Feb. 2012. 76, 85, 88, 112, 154, 166

[104] A. Charnes and W. W. Cooper, "Programming with linear fractional functionals," *Naval Research Logistics Quarterly*, vol. 9, no. 3-4, pp. 181–186, 1962. 76, 139, 154, 163

[105] J. Sturm, "Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones," *Optimization Methods & Software*, vol. 11-2, no. 1-4, Sp. Iss. SI, pp. 625–653, 1999. 79, 89, 140, 158, 160, 162, 163, 168

[106] J. L. Öfberg, "YALMIP : A Toolbox for Modeling and Optimization in MATLAB," in *Proceedings of the CACSD Conference*, Taipei, Taiwan, 2004. 79, 89, 140, 158, 168

[107] CVX-Research Inc, "CVX: Matlab software for disciplined convex programming, version 2.0 beta," http://cvxr.com/cvx, Sep. 2012. 79, 89, 140, 158, 168

[108] S. Shafiee, N. Liu, and S. Ulukus, "Towards the Secrecy Capacity of the Gaussian MIMO Wire-Tap Channel: The 2-2-1 Channel," *Information Theory, IEEE Transactions on*, vol. 55, no. 9, pp. 4033–4039, Sep. 2009. 105

[109] F. Oggier and B. Hassibi, "The Secrecy Capacity of the MIMO Wiretap Channel," *Information Theory, IEEE Transactions on*, vol. 57, no. 8, pp. 4961 –4972, Aug. 2011. 105, 130, 143

[110] R. Bustin, R. Liu, H. V. Poor, and S. Shamai, "An MMSE Approach to the Secrecy Capacity of the MIMO Gaussian Wiretap Channel," *EURASIP Journal in Wireless Commununications Networks.*, vol. 2009, pp. 3:1–3:8, Mar. 2009. 105, 131, 138

[111] A. Mukherjee and A. Swindlehurst, "Utility of beamforming strategies for secrecy in multiuser MIMO wiretap channels," in *Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on*, Oct. 2009, pp. 1134 –1141. 105, 138

[112] N. Yang, P. Yeoh, M. Elkashlan, R. Schober, and I. Collings, "Transmit Antenna Selection for Security Enhancement in MIMO Wiretap Channels," *Communications, IEEE Transactions on*, vol. 61, no. 1, pp. 144–154, Jan. 2013. 106

[113] M. Kobayashi and M. Debbah, "On the secrecy capacity of frequency-selective fading channels: A practical Vandermonde precoding," in *Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on*, Sep. 2008, pp. 1–5. 106

[114] F. Renna, N. Laurenti, and H. Poor, "High SNR secrecy rates with OFDM signaling over fading channels," in *Personal Indoor and Mobile Radio Communications (PIMRC), 2010 IEEE 21st International Symposium on*, Sep. 2010, pp. 2692–2697. 106, 126

[115] ——, "Physical Layer Secrecy for OFDM systems," in *Wireless Conference (EW), 2010 European*, Apr. 2010, pp. 782–789. 106

[116] X. Wang, M. Tao, J. Mo, and Y. Xu, "Power and Subcarrier Allocation for Physical-Layer Security in OFDMA Networks," in *Communications (ICC), 2011 IEEE International Conference on*, Jun. 2011, pp. 1–5. 106

[117] ——, "Power and Subcarrier Allocation for Physical-Layer Security in OFDMA-Based Broadband Wireless Networks," *Information Forensics and Security, IEEE Transactions on*, vol. 6, no. 3, pp. 693–702, Sep. 2011. 106

[118] C. Oestges and B. Clerckx, *MIMO Wireless Communications: from real-world propagation to space-time code design*, Academic, Ed. Academic Press, 2007. 109, 113, 122

[119] J. Andrews, A. Ghosh, and R. Muhamed, *Fundamentals of WiMAX Understanding Broadband Wireless Networking*, T. S. Rappaport, Ed. Prentice Hall, 2007. 124

[120] E. Jorswieck and A. Wolf, "Resource allocation for the wire-tap multi-carrier broadcast channel," in *Telecommunications, 2008. ICT 2008. International Conference on*, Jun. 2008, pp. 1–6. 126

[121] J. Li and A. Petropulu, "Optimal input covariance for achieving secrecy capacity in Gaussian MIMO wiretap channels," in *Acoustics Speech and Signal Processing (ICASSP), 2010 IEEE International Conference on*, Mar. 2010, pp. 3362–3365. 131

[122] J. Li and A. P. Petropulu, "Transmitter Optimization for Achieving Secrecy Capacity in Gaussian MIMO Wiretap Channels," *CoRR*, vol. abs/0909.2622, 2009. 131

[123] J. Li and A. Petropulu, "On beamforming solution for secrecy capacity of MIMO wiretap channels," in *GLOBECOM Workshops, 2011 IEEE*, Dec. 2011, pp. 889–892. 131

[124] S. Fakoorian and A. Swindlehurst, "Optimal power allocation for GSVD-based beamforming in the MIMO Gaussian wiretap channel," in *Information*

Theory Proceedings (ISIT), 2012 IEEE International Symposium on, Jul. 2012, pp. 2321–2325. 131

[125] S. Fakoorian, J. Huang, and A. Swindlehurst, "Rank property of the MIMO Gaussian wiretap channel with an average power constraint," in *Signals, Systems and Computers (ASILOMAR), 2012 Conference Record of the Forty Sixth Asilomar Conference on*, Nov. 2012, pp. 421–425. 131, 142

[126] S. Fakoorian and A. Swindlehurst, "Full Rank Solutions for the MIMO Gaussian Wiretap Channel with an Average Power Constraint," *Signal Processing, IEEE Transactions on*, vol. 61, no. 10, pp. 2620–2631, May 2013. 132, 142, 143

[127] Q. Li, M. Hong, H.-T. Wai, W.-K. Ma, Y.-F. Liu, and Z.-Q. Luo, "An alternating optimization algorithm for the MIMO secrecy capacity problem under sum power and per-antenna power constraints," in *Acoustics, Speech and Signal Processing (ICASSP), 2013 IEEE International Conference on*, May 2013, pp. 4359–4363. 132, 181

[128] Q. Li, M. Hong, H.-T. Wai, Y.-F. Liu, W.-K. Ma, and Z.-Q. Luo, "Transmit Solutions for MIMO Wiretap Channels using Alternating Optimization," *Selected Areas in Communications, IEEE Journal on*, vol. 31, no. 9, pp. 1714–1727, Sep. 2013. 132, 134, 140, 142, 143, 144, 145, 181

[129] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Secure wireless communications via cooperation," in *Communication, Control, and Computing, 2008 46th Annual Allerton Conference on*, Sep. 2008, pp. 1132–1138. 132

[130] ——, "Amplify-and-Forward based cooperation for secure wireless communications," in *Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on*, Apr. 2009, pp. 2613–2616. 132

[131] J. Zhang and M. Gursoy, "Relay beamforming strategies for physical-layer security," in *Information Sciences and Systems (CISS), 2010 44th Annual Conference on*, Mar. 2010, pp. 1–6. 132

[132] Y. Yang, Q. Li, W.-K. Ma, J. Ge, and P. C. Ching, "Cooperative Secure Beamforming for AF Relay Networks With Multiple Eavesdroppers," *Signal Processing Letters, IEEE*, vol. 20, no. 1, pp. 35–38, Jan. 2013. 132

[133] L. Lai and H. El Gamal, "The Relay-Eavesdropper Channel: Cooperation for Secrecy," *Information Theory, IEEE Transactions on*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008. 133

[134] J. Huang and A. Swindlehurst, "Cooperative Jamming for Secure Communications in MIMO Relay Networks," *Signal Processing, IEEE Transactions on*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011. 133

[135] S. Fakoorian and A. Swindlehurst, "Solutions for the MIMO Gaussian Wiretap Channel With a Cooperative Jammer," *Signal Processing, IEEE Transactions on*, vol. 59, no. 10, pp. 5013–5022, Oct. 2011. 133

[136] H.-M. Wang, M. Luo, X.-G. Xia, and Q. Yin, "Joint Cooperative Beamforming and Jamming to Secure AF Relay Systems With Individual Power Constraint and No Eavesdropper's CSI," *Signal Processing Letters, IEEE*, vol. 20, no. 1, pp. 39–42, Jan. 2013. 133

[137] X. He and A. Yener, "Cooperation With an Untrusted Relay: A Secrecy Perspective," *Information Theory, IEEE Transactions on*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010. 133

[138] ——, "Two-Hop Secure Communication Using an Untrusted Relay: A Case for Cooperative Jamming," in *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, Nov. 2008, pp. 1–5. 133

[139] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical Layer Security for Two-Way Untrusted Relaying With Friendly Jammers," *Vehicular Technology, IEEE Transactions on*, vol. 61, no. 8, pp. 3693–3704, Oct. 2012. 133

[140] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure Communication via Sending Artificial Noise by the Receiver: Outage Secrecy Capacity/Region Analysis," *Communications Letters, IEEE*, vol. PP, no. 99, pp. 1–4, 2012. 134, 136, 166

[141] M. Jain, J. I. Choi, T. Kim, D. Bharadia, K. Srinivasan, S. Seth, P. Levis, S. Katti, and P. Sinha, "Practical, Real-time, Full Duplex Wireless," in *17th Annual International Conference on Mobile Computing and Networking (Mobicom 2011)*, Las Vegas, Nevada, 2011. 137

[142] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Physical Layer Security of MIMO - OFDM Systems by Beamforming and Artificial Noise Generation," *Physical Communication*, vol. 4, no. 4, pp. 313 – 321, 2011, special Issue on Advances in MIMO-OFDM. 138

[143] ——, "Physical Layer Security of MIMO Frequency Selective Channels by Beamforming and Noise Generation," in *EUSIPCO 2011 (19th European Signal Processing Conference)*, Barcelona, Spain, Aug. 2011, pp. 829–833. 138, 140

[144] N. Romero-Zurita, D. McLernon, and M. Ghogho, "Physical Layer Security by Robust Masked Beamforming and Protected Zone Optimisation," *Communications, IET*, vol. 8, no. 8, pp. 1248–1257, May 2014. 140, 160, 163, 165

[145] K.-Y. Wang, A. M.-C. So, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "Outage Constrained Robust Transmit Optimization for Multiuser MISO Downlinks: Tractable Approximations by Conic Optimization," *CoRR*, vol. abs/1108.0982, 2011. 181

[146] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure Broadcasting Over Fading Channels," *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2453–2469, Jun. 2008. 182

[147] E. Ekrem and S. Ulukus, "Degraded Compound Multi-Receiver Wiretap Channels," *Information Theory, IEEE Transactions on*, vol. 58, no. 9, pp. 5681–5698, Sep. 2012. 182

[148] ——, "Capacity Region of Gaussian MIMO Broadcast Channels With Common and Confidential Messages," *Information Theory, IEEE Transactions on*, vol. 58, no. 9, pp. 5669–5680, Sep. 2012. 182

[149] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-Theoretically Secret Key Generation for Fading Wireless Channels," *Information Forensics and Security, IEEE Transactions on*, vol. 5, no. 2, pp. 240–254, Jun. 2010. 182

Note that the last number(s) at the end of each reference indicate the page number(s) where this reference has been cited.

Leonardo Nabil Romero-Zurita

✉ *leonabil@ieee.org*

Biography

Nabil Romero-Zurita received the MSc (Distinction) in Modern Digital and Wireless Frequency Communications and the PhD degree in Signal Processing for Communications at the Electrical and Electronic Engineering school at the University of Leeds, UK. His research studies were funded by the University of Leeds through the Fully-Funded International Research Scholarship. His PhD research project was short-listed by the EPSRC in the Connected World category within the 2012 UK Pioneers competition. He has been recognised as exemplary reviewer of the IEEE Wireless Communications Letters journal during 2013. Dr. Romero-Zurita has industrial experience in radio frequency planning and optimising 2G and 3G cellular networks. Currently, he is part of the Digital Design Engineering team at Cambridge Silicon Radio, Cambridge, UK. His research interests are physical layer security, cooperative networks, Bluetooth, cognitive radio, convex optimisation and game theory applications for communications.

Education

PhD **Electrical and Electronic Eng. Signal Processing for Communications**

University of Leeds, UK. Aug. 2014.
Thesis title: Optimising multiple antenna techniques for physical layer security.
Supervisors: Dr. Des McLernon, Prof. Mounir Ghogho.
Funding body: University of Leeds Fully Funded International Research Scholarship.

MSc (Dist.) **Modern Digital and Radio Frequency Wireless Communications**

University of Leeds, Sep. 2009. UK.
Dissertation title: Physical and MAC layer design for cooperative communications.
Achievements: Top of the 2009 M.Sc. Electrical and Electronic Eng. Class.
Scholarship: University of Leeds Excellence Scholarship.

BSc **Electronic and Telecommunications Engineering**

ESPE - Army's Polytechnic School. Jul. 2003. Quito, Ecuador.
Scholarship: ESPE Scholarship

Research and Teaching Experience

2010–2014 **Signal Processing for Communications Group** *University of Leeds, UK.*

Signal processing techniques for securing wireless networks at the physical layer.
Achievements:

- *EPSRC UK ICT Pioneers. Connected World* category national finalist. London, Nov. 2012.
- *University of Leeds Showcase 2013*. Nominated by the Engineering faculty to the *Researcher of the Year* award. Leeds, Dec. 2013.
- University of Leeds *Make Some Noise 2012*. Research and Public Engagement Festival. Second award, oral presentation category. Apr. 2012.

2011–2014 **Teaching Assistant** *University of Leeds. School of Electrical and Electronic Eng, UK.*

Lecturing and demonstrating in digital communications modules at undergraduate and postgraduate levels. Supervision of master students dissertation.

Professional Experience

2014-Present **Digital Design Engineer** *Cambridge Silicon Radio, (CSR plc). Cambridge. UK.*

2010 **Radio Frequency Optimisation Engineer** *Optimi. Malaga, Spain.*

2005–2008 **Radio Frequency Planning Engineer** *Telefonica Movistar. Quito, Ecuador.*

2005–2008 **Wireless Terminals Homologation Engineer.** *BellSouth. Quito, Ecuador.*

Publications

1. Journal **Physical Layer Security by Robust Masked Beamforming and Protected Zone Optimisation**, *N. Romero-Zurita, D. McLernon and M. Ghogho*, IET Communications, Special Issue on Secure Physical Layer Communications, May. 2014.
2. Journal **PHY Layer Security Based on Protected Zone and Artificial Noise**, *N.Romero-Zurita, M. Ghogho, D. McLernon and A. Swami*, IEEE Signal Processing Letters, May. 2013.
3. Journal **Outage Probability Based Power Distribution Between Data and Artificial Noise for Physical Layer Security**, *N. Romero-Zurita, M. Ghogho and D. McLernon*, IEEE Signal Processing Letters, Feb. 2012.
4. Journal **Physical Layer Security of MIMO - OFDM Systems by Beamforming and Artificial Noise Generation**, *N. Romero-Zurita, M. Ghogho and D. McLernon*, Physical Communication. Special issue on Advances in MIMO-OFDM, Dec. 2011.
5. Conference **Physical Layer Security in Multiple Antenna Systems by Joint Transmitter/Receiver Artificial Noise Generation through Semidefinite Programming**, *N. Romero-Zurita, D. McLernon and M. Ghogho*, IET Intelligent Signal Processing. London, UK. Dec. 2013.
6. Conference **Securing Wireless Networks by Robust Beamforming and Artificial Noise under a Close Eavesdropper**, *N. Romero-Zurita*, M. Ghogho and D. McLernon, Symposium on the Convergence of Telecomms, networking and Broadcasting. Liverpool, UK. Jun. 2013.
7. Conference **Physical Layer Security of MIMO Frequency Selective Channels by Beamforming and Noise Generation**, *N Romero-Zurita, M. Ghogho and D. McLernon*, EUSIPCO 2011, 19th European Signal Processing Conference. Barcelona, Spain. Aug. 2011.

Professional Activities

Technical Committee Program Chair Globecom 2014's second workshop on trusted communications with physical layer security (TCPLS20014). Austin, TX. Dec. 2014

Exemplary Reviewer Recognised by the IEEE Communications Society as a exemplary reviewer of the IEEE Wireless Communications Letters journal during the year 2013.

University of Leeds Teaching Award - ULTA-1. Recognised as Associate Fellow of the Higher Education Academy (AFHEA).

Reviewer and TCP Served as peer-reviewer in more than 60 journal papers of the most important IEEE and IET journals and as TCP in important conferences such as IEEE ICC'15 Wireless Communications track.

Professional Memberships

IEEE **Institute of Electrical and Electronic Eng.**, *Member of the UK & Rep of Ireland Sec.*.

IET **The Institution of Engineering and Technology**, Member since Dec. 2013.

EURASIP **European Association for Signal Processing**, Member since Aug. 2011.

Other Activities

Clyde-sider **Glasgow 2014 CW Games**, *Wrestling field of play team leader*, Glasgow, Jul. 2014.

Business **Ernst & Young and FABSOC**, *First price in the* Young Enterprise-Entrepreneurship Competition, Leeds, Mar. 2013.

Games Maker **London 2012 Olympic Games**, *Wrestling Sport Information Team*, Olympic Village & Excel competition Venue, London, Jul.-Aug. 2012.

Debating **Leeds Debating Society**, *University of Leeds member*.