Wireless Physical Layer Security with CSIT Uncertainty

Dissertation by

Amal Hyadi

In Partial Fulfillment of the Requirements

For the Degree of

Doctor of Philosophy

King Abdullah University of Science and Technology

Thuwal, Kingdom of Saudi Arabia

September, 2017

EXAMINATION COMMITTEE PAGE

The dissertation of Amal Hyadi is approved by the examination committee.

Committee Chairperson: Prof. Mohamed-Slim Alouini
External Committee Member: Prof. Aylin Yener
Committee Members: Prof. Zouheir Rezki, Prof. Basem Shihada, Prof. Marc G. Genton

ABSTRACT

Wireless Physical Layer Security with CSIT Uncertainty

Amal Hyadi

Recent years have been marked by an enormous growth of wireless communication networks and an extensive use of wireless applications. In return, this phenomenal expansion induced more concerns about the privacy and the security of the users. Physical layer security is one of the most promising solutions that were proposed to enhance the security of next generation wireless systems. The fundamental idea behind this technique is to exploit the randomness and the fluctuations of the wireless channel to achieve security without conditional assumptions on the computational capabilities of the eavesdropper. In fact, while these elements have traditionally been associated with signal deterioration, physical layer security uses them to ensure the confidentiality of the users. Nevertheless, these technical virtues rely heavily on perhaps idealistic channel state information assumptions. In that regard, the aim of this thesis is to look at the physical layer security paradigm from the channel uncertainty perspective. In particular, we discuss the ergodic secrecy capacity of different wiretap channels when the transmitter is hampered by the imperfect knowledge of the channel state information (CSI). We consider two prevalent causes of uncertainty for the CSI at transmitter (CSIT); either an error of estimation occurs at the transmitter and he can only base his coding and the transmission strategies on a noisy version of the CSI, or the CSI feedback link has a limited capacity and the legitimate receivers can only inform the transmitter about the quantized CSI. We investigate both the single-user multiple-input multiple-output (MIMO) wiretap channel and the multi-user broadcast wiretap channel. In the latter scenario, we distinguish between two situations:

multiple messages transmission and common message transmission. We also discuss the broadcast channel with confidential messages (BCCM) where the transmitter has one common message to be transmitted to two users and one secret message intended to only one of them. In all cases, we show that by appropriately designing the coding and the transmission schemes, a secure communication can still be achieved even with an imperfect knowledge of the CSIT.

ACKNOWLEDGEMENTS

I thank Allah (SWT) for enabling me to complete this thesis. Without His guidance, my accomplishments would never have been possible.

I would like to sincerely thank my advisor, Professor Mohamed-Slim Alouini, for his continuous support, guidance, encouragement, and belief in me. Since my first days at KAUST, Professor Slim has always been supportive and helpful whether it comes to research, to academic work, or to life-related events. He is truly one of the most exceptional people I have ever met in my life. I would like to extend my gratitude to my Co-advisor Professor Zouheir Rezki from whom I learned a lot throughout this work. Our discussions have always been productive and have taught me to constantly question and understand even the simplest things that may seem evident.

I would like to thank my thesis committee members, Professor Aylin Yener, Professor Basem Shihada, and Professor Marc G. Genton for the valuable time they have devoted to read my thesis and for the invaluable comments and suggestions they provided me with. I also wish to thank, my dear teacher, Professor Ahmed Sultan, for his constructive comments on my work during my proposal.

During my time at KAUST, I have been fortunate to meet and work with some incredibly talented and bright people whom I fully admire and respect. I would like therefore to thank all my colleagues at KAUST, the ones who already left, and the one who are still leaving the KAUST dream. I have also been blessed by the friendship of many wonderful people. A warm thank you goes to my closest friends Fatma and Seif; we shared some unforgettable moments during this long journey. My sincere thank you also goes to Tsiky, Amal, Ikram, Abla, Emna, Leila, Doha, Hessa, Konpal, Annie, Nouha, and Wafa.

Finally, I am very thankful to my soul mate, my husband Mohamed, for always believing in me and pushing me forward, and to my beloved parents and brother for their constant emotional support.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AWGN	Additive White Gaussian Noise
BCC	Broadcast Channel with Confidential Messages
BEC	Binary Erasure Channel
BER	Bit Error Rate
CDF	Cumulative Distribution Function
CSI	Channel State Information
CSIR	Channel State Information at the Receiver
CSIT	Channel State Information at the Transmitter
DoF	Degree of Freedom
HARQ	Hybrid Automatic Retransmission Request
KKT	Karush-Kuhn-Tucker
LHS	Left-Hand Side
MIMO	Multiple-Input Multiple-Output
MISO	Multiple-Input Single-Output
MMSE	Minimum Mean Square Error
MRC	Maximum Ratio Combining
OFFT	Optimal Framework for Feedback and Transmission
PDF	Probability Density Function
PLS	Physical Layer Security
QoS	Quality of Service
RHS	Right-Hand Side
RVQ	Random Vector Quantization
SDoF	Secrecy Degrees of Freedom
SIMO	Single-Input Multiple-Output
SINR	Signal-to-Interference-plus-Noise Ratio
SNR	Signal-to-Noise Ratio
SVD	Singular Value Decomposition

LIST OF SYMBOLS

$H(X)$	Entropy of the random variable X
$H(X\|Y)$	Entropy of the random variable X conditioned on variable Y
$I(X;Y)$	Mutual information between the random variables X and Y
$I(X;Y\|Z)$	Mutual information between the random variables X and Y conditioned on variable Z
$X(k)$	The k-th element of X
X^n	A sequence of length n
$X^{[i,j]}$	A sequence of elements between i and j, i.e., $X^{[i,j]}=\{X(i), X(i+1), \cdots, X(j)\}$, with $i < j$
$X^{\kappa}(l)$	The l-th sequence of X of size κ, i.e., $X^{\kappa}(l)=\{X(\kappa l), X(\kappa l-1), \cdots, X(\kappa l-\kappa+1)\}$
$\{x\}^+$	The maximum between 0 and x
$\mathbb{E}[.]$	Expectation operation
$\mathbb{E}[.\|A]$	Conditional expectation given event A
$\Pr[A]$	Probability of event A
A^c	Complement of event A
$\|x\|$	Modulus of the scalar x
$\|X\|$	Determinant of matrix X
$\|\|.\|\|$	Euclidean norm
X^*	Hermitian transpose of matrix X
$\mathrm{tr}[X]$	Trace of matrix X
$X \succeq 0$	X is positive semidefinite
I_N	Identity matrix of size N
$f_X(.)$	Probability density function
$F_X(.)$	Cumulative distribution function
$X \sim \mathcal{CN}(\mu, \sigma^2)$	X is a circularly symmetric complex-valued Gaussian random variable with mean μ and variance σ^2

lim	Limit operator
$\delta(.)$	Dirac-Delta function
Ei(.)	Exponential integral function
$\Gamma(.)$	Gamma function
$I_0(.)$	Modified Bessel function of the first kind of order zero

LIST OF FIGURES

Chapter 1

Introduction

1.1 Physical Layer Security

The broadcast nature of the wireless channel makes radio transmissions vulnerable to eavesdropping attacks. To date, the security of wireless communications is mainly performed at the application layer using cryptographic techniques. However, with the emergence of ad-hoc and decentralized networks, these high-level techniques turn out to be complex and challenging to implement. Therefore, there has been a significant recent interest in studying the inherent ability of the physical layer to provide secure communications. This paradigm is known as wireless physical layer security. What distinguishes physical layer security compared to other high layers cryptographic techniques is that it exploits the randomness and the fluctuations of the wireless channel to achieve security at a remarkably reduced computational complexity. Information theoretic security dates back to 1949 when Shannon introduced his pioneer work on cipher systems [1]. Shannon's work considers the secure transmission of confidential information when a random secret key is shared between the legitimate parties, and a passive eavesdropper is intercepting the communication. To guarantee perfect secrecy, Shannon showed that the entropy of the shared secret key should exceed the entropy of the message, or in other words, this requires the key to be at least as long as the confidential message itself. Many years later, Wyner's work [2] came to shed some positive light on information theoretic security. Wyner's model, called a wiretap

channel, takes advantage of the channel's imperfections to secure a transmission at the physical layer without the need of a shared secret key. Since then, studies of the wiretap channel have multiplied and have extended to more general communication systems including broadcast channels, fading channels, multiuser networks, and many other wireless communication models.

In particular, securing fading channels from potential wiretapping attacks is of crucial interest, especially in regard to the unprecedented growth of wireless communication applications and devices. The fading wiretap channel has opened new research directions for information theoretic security. What is unique about the fading model is that it takes advantage of the randomness of the channel gain fluctuations to secure the transmission against potential eavesdroppers, at the physical layer itself. As a result, even if the eavesdropper has a better average signal-to-noise ratio (SNR) than the legitimate receiver, physical layer security can still be achieved over fading channels without requiring the sharing of a secret key. To make the most of what fading has to offer, the knowledge of the channel state information (CSI) at the transmitter (CSIT) is of primordial importance.

The number of research works on physical layer security has increased exponentially over the last few years. This number is certainly to continue growing with the deployment of 5G and beyond wireless communication systems. To capture the enormous growth of research works on physical layer security, multiple surveys, overview papers, and books have been published in recent years. A general detailed review of the theoretical foundations, coding techniques, practical implementations, challenges and opportunities of physical layer security is presented in [3–7]. The work in [8] provides a comprehensive survey describing the evolution of information theoretic security from point-to-point communication systems to multiple antenna and multiuser networks. A brief summary of challenges facing physical layer security is presented in [9] and in [10] for next generation networks. An overview of physical

layer security is also considered in [11–13] for cooperative systems, in [14] for massive multiple-input-multiple-output (MIMO) systems, and in [15] for cognitive radio networks. The authors, in [16], present an earlier survey on physical layer security under the imperfect channel state information assumption, with a particular focus on relay channels, cognitive system, and large-scale decentralized networks. The effect of having an outdated channel knowledge at the transmitter, on information theoretic security, is highlighted in [17], and a synopsis of how different levels of CSIT impact the system's security is provided in [18].

1.2 Motivation and Thesis Contributions

The vast majority of research works on physical layer security assume that the transmitter has a perfect knowledge of the legitimate receiver's CSI, usually referred to as the main CSI, or even of both the main and the eavesdropper's CSI. Although this assumption makes the analysis more tractable and allows the characterization of the full potential of the fading wiretap channel, it does not capture the practical aspect of the transmission model. In a wireless communication system, acquiring the CSIT requires the receiver to feed back its CSI constantly to the transmitter. This feedback process is typically accompanied by the introduction of uncertainty into the CSIT. Different phenomena can cause the CSIT to be imperfect. Most commonly, the uncertainty comes from an error of estimation at the transmitter who ends up with a noisy version of the CSI, or from a feedback link with a limited capacity which requires the transmission of quantized CSI, or also from a delayed feedback causing outdated CSIT. The aim of this thesis is to consider the more realistic scenario where only partial main CSI is available at the transmitter. In particular, we investigate the ergodic secrecy capacity of different wireless communication systems under the assumption of CSIT uncertainty.

The main contributions of this thesis can be summarized in the following points:

- We characterize the ergodic secrecy capacity of multi-user broadcast wiretap channels over fast fading channels with imperfect main CSIT. In particular, we analyze the effect of the noisy estimation of the CSI on the throughput of a broadcast channel where the transmission is intended for multiple legitimate receivers in the presence of an eavesdropper and we prove that a non-zero secrecy rate can still be achieved even when the CSI at the transmitter is noisy. The obtained results show that the secrecy rate when broadcasting a common message is limited by the legitimate receiver having, on average, the worst main channel link, i.e., the legitimate receiver with the lowest average SNR. For the independent messages case, we prove that the achievable secrecy sum-rate scales with the number of users K according to the scaling law $\log((1-\alpha)\log(K))$, where α is the estimation error variance of the CSIT. Asymptotic analysis at high-SNR, perfect and no-main CSI are addressed and the results are illustrated for the case of Rayleigh fading channels.

- We examine the impact of having finite CSI feedback on the secrecy throughput of multi-user block-fading broadcast channels. More specifically, we consider that the transmitter is unaware of the channel gains to the legitimate receivers and to the eavesdropper and that the main CSI feedback links are limited to b bits per fading block. These feedback bits are provided to the transmitter by each legitimate receiver, at the beginning of each coherence block, through error-free public links with limited capacity. Both the common message transmission, where the same message is broadcasted to all the legitimate receivers, and the independent messages transmission, where the source broadcasts multiple independent messages, are considered. Assuming an average power constraint at the transmitter, we provide an upper and a lower bounds on the ergodic secrecy capacity for the common message case, and an upper

and a lower bound on the secrecy sum-rate for independent messages. For the particular case of infinite feedback, we prove that our bounds coincide.

- We establish the secrecy capacity region of the block-fading broadcast channel with confidential messages (BCCM) when the transmitter has limited knowledge of the CSI. In particular, we consider a two-user communication system where the transmitter has one common message to be transmitted to both users and one confidential message intended to only one of them. The confidential message has to be kept secret from the other user to whom the information is not intended. The transmitter is not aware of the CSI of neither channel and is only provided by limited CSI feedback sent at the beginning of each fading block. Assuming an error-free feedback link, we characterize the secrecy capacity region of this channel and show that even with a 1-bit CSI feedback, a positive secrecy rate can still be achieved. Then, we look at the case where the feedback link is not error-free and is rather a binary erasure channel (BEC). In the latter case, we provide an achievable secrecy rate region and show that as long as the erasure event is not a probability one event, the transmitter can still transmit the confidential information with a positive secrecy rate.

- We investigate the ergodic secrecy capacity of multi-antenna block-fading wiretap channels with limited CSI feedback. We consider that the transmitter is unaware of the channel matrices of neither the main nor the eavesdropper channels, and is only provided by a finite CSI feedback sent by the legitimate receiver through a public, error-free, link with limited capacity. Assuming an average power constraint at the transmitter, we provide two achievable secrecy rates and an upper bound on the ergodic secrecy capacity. The first secrecy rate is achieved by using the feedback information not only to adapt the power but also to adjust the transmission rate during each fading block. For the second

achievable secrecy rate, the feedback is mainly employed for the power adaptation purpose. Besides, in order to maximize the secrecy rate, we present a framework to design the used codebooks for feedback and transmission. The presented framework is based on the iterative Lloyd's algorithm [19]. For the particular case of infinite feedback, we prove that the first achievable secrecy rate and the presented upper bound on the ergodic secrecy capacity coincide, hence, fully characterizing the ergodic secrecy capacity in this case. The high-SNR regime and the secrecy degrees of freedom (SDoF) of the system are also investigated.

1.3 Thesis Outline

The rest of this dissertation is organized as follows. Chapter 2 provides the reader with some fundamental concepts associated with the wiretap channel. In addition, it presents a comprehensive review of recent and ongoing research works on physical layer security. Chapter 3 analyzes the ergodic secrecy capacity of the broadcast wiretap channel when the transmitter is provided with a noisy estimation of the main CSI. The impact of having a finite CSI feedback on the secrecy throughput is examined in Chapter 4 for the multi-user broadcast wiretap channel, and in Chapter 5 for the two-user BCCM, considering both cases when the feedback link is error-free and when it is subject to erasure. Chapter 6 investigates the multi-antenna block-fading wiretap channel with limited CSI feedback. Finally, Chapter 7 offers some concluding remarks and briefly outlines some possible future directions.

Chapter 2

Background and Literature Review

2.1 Introduction

As mentioned earlier in the introductory chapter, information theoretic security was firstly introduced by Shannon in [1]. Shannon's model, called a cipher system, considers the transmission of confidential information to a legitimate receiver in the presence of a passive eavesdropper intercepting the communication, cf. Figure 2.1. The model also assumes that a random secret key is shared between the transmitter and the legitimate receiver and that the key is unknown to the eavesdropper. To guarantee perfect secrecy, the entropy of the shared secret key should exceed the entropy of the message. In other words, this requires the key to be at least as long as the confidential message itself. Three decades later, Wyner's work [2] came to shed some positive light on information theoretic security. Wyner's new secrecy model exploits the structure of the channel to transmit a message reliably and securely, to the intended receiver, without the need of a shared secret key.

The rest of this chapter is organized as follows. Section 2.2 briefly discusses possible countering measures for security threats. Section 2.3 provides a summary of some of the fundamental concepts associated with Wyner's wiretap channel. Section 2.4 addresses three different phenomena that can cause CSIT uncertainty. A detailed state-of-the-art review of physical layer security with perfect CSIT, and with CSIT uncertainty is presented in Section 2.5. Finally, Section 2.6 concludes the chapter.

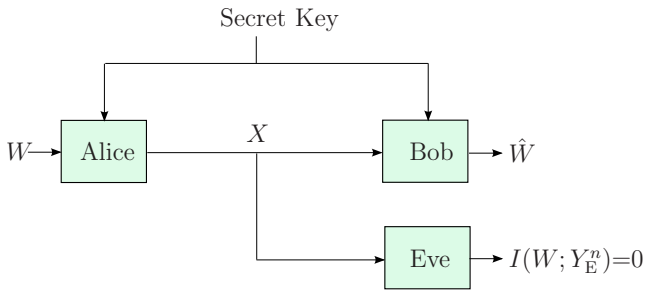


Figure 2.1: Shannon's cipher system.

2.2 Countering Security Threats

The open nature of the wireless channel makes it vulnerable to different types of security attacks. Generally speaking, we can distinguish between two types of attacks: passive attacks and active attacks. In a passive attack, the malicious node is solely interested in intercepting the communication between the legitimate entities. Therefore, the confidentiality of the transmitted information is the main issue in such a case. On the other hand, in an active attack, the malicious node aims to disrupt the system. Possible active attacks include jamming, denial-of-service (DOS), message modification, and localization through traffic analysis.

In this work, we consider the passive kind of attacks where the confidentiality of the transmitted information is the main focus. To date, countering the confidentiality threat is mainly addressed using cryptographic techniques. Accordingly, the confidential information is encrypted using a shared secret key that is only known to the legitimate parties. The generation and the sharing of this secret key represent a real challenge. Besides, it depends highly on the assumption of having limited time and limited computational resources at the wiretapper. The private key distribution and management are even more challenging in decentralized wireless systems and mobile networks with dynamic topologies. Indeed, this is one of the big issues facing the next wave of wireless systems known as the Internet-of-Things (IoT). Exploiting the ability

of the physical layer to achieve a confidential transmission is one of the promising approaches that are being studied to tackle this problem. It should be noted, however, that physical layer security is there to complement the existing security mechanisms, including encryption, ID and Passwords, denial of internet access, firewalls, backups, etc, rather than to compete with them.

2.3 The Wiretap Channel

This section provides the reader with an objective description of some fundamental concepts associated with the wiretap channel. First, we present the basic information theoretic model introduced by Wyner, which is colloquially known as the wiretap channel. We shed light on how Wyner's model take advantage of the channel's noisiness to secure a transmission, and we briefly explain the structure of the wiretap code. Then, we consider and discuss the usefulness of cooperative jamming to ensure or enhance the security of a wireless transmission. The last part of this section presents two key secrecy metrics used to evaluate and measure the performance of a system under confidentiality constraints, namely the secrecy capacity and the secrecy outage probability.

2.3.1 Wyner's Wiretap Channel

Wyner's channel model, also known as the wiretap channel, represents a generalization of Shannon's cipher system. The originality of Wyner's work comes straight from his pivotal idea to take advantage of the imperfection of the communication medium to secure a transmission at the physical layer. In Wyner's model, illustrated in Figure 2.2, the transmitter (Alice) tries to communicate a confidential message W to a legitimate receiver (Bob) in the presence of an eavesdropper (Eve) over a noisy memoryless link. Wyner's model assumes that Eve observes a degraded version of the signal obtained by Bob. The channel between Alice and Bob is usually referred

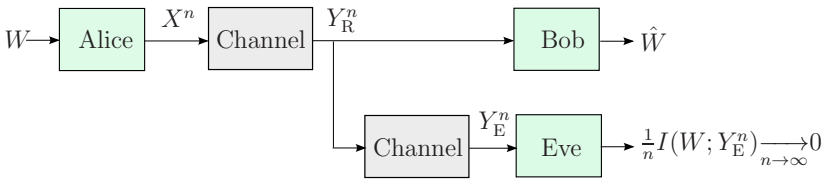


Figure 2.2: Wyner's wiretap channel.

to as the main channel or the legitimate channel while the channel between Alice and Eve is known as the wiretap channel or the eavesdropper's channel. The message W is encoded into a codeword X^n of length n and transmitted at a rate $\mathcal{R}_{\mathrm{s}}$. A $(2^{n\mathcal{R}_{\mathrm{s}}}, n)$ code consists of the following elements:

- A message set $\mathcal{W} = \left\{1, 2, \cdots, 2^{n\mathcal{R}_{\mathrm{s}}}\right\}$ with the messages $W \in \mathcal{W}$ independent and uniformly distributed over $\mathcal{W}$;
- A stochastic encoder $f : \mathcal{W} \to \mathcal{X}^n$ that maps each message w to a codeword $x^n \in \mathcal{X}^n$;
- A decoder at the legitimate receiver $g : \mathcal{Y}^n \to \mathcal{W}$ that maps a received sequence $y_{\mathrm{R}}^n \in \mathcal{Y}^n$ to a message $\hat{w} \in \mathcal{W}$.

A rate $\mathcal{R}_{\mathrm{s}}$ is an achievable secrecy rate if there exists a sequence of $(2^{n\mathcal{R}_{\mathrm{s}}}, n)$ code such that the reliability condition

$$\lim_{n\to\infty} \frac{1}{2^{n\mathcal{R}_{\mathrm{s}}}} \sum_{w=1}^{2^{n\mathcal{R}_{\mathrm{s}}}} \Pr\left[W \neq \hat{W} \middle| W = w\right] = 0, \tag{2.1}$$

and the secrecy condition

$$\lim_{n\to\infty} \frac{1}{n} I\left(W; Y_{\mathrm{E}}^n\right) = 0, \tag{2.2}$$

with Y_{E} representing the received signal at the eavesdropper, are both satisfied.

2.3.1.1 The Weak Secrecy Constraint

The secrecy constraint in (2.2) is called the weak secrecy condition. At the difference of Shannon's perfect secrecy, which requires the exact information leakage to be zero, i.e., $I\left(W;Y_{\mathrm{E}}^{n}\right)=0$, where W is the confidential information, and Y_{E}^{n} is the n-length received signal at the eavesdropper, the weak secrecy constraint only requires the rate of the information leaked to the eavesdropper to asymptotically vanish, i.e., $\lim_{n\to\infty}\frac{1}{n}I\left(W;Y_{\mathrm{E}}^{n}\right)=0$, where n is the length of the transmitted codeword. The weak secrecy condition can be further straightened to the strong secrecy constraint which reqires the absolute amount of secrecy leaked to the eavesdropper to go to zero as the length of the transmitted codeword becomes very large, i.e., $\lim_{n\to\infty}I\left(W;Y_{\mathrm{E}}^{n}\right)=0$. Generally, a specific code achieving a secure communication under the weak secrecy constraint does not necessarily achieve strong secrecy [20–23]. Yet, in all known instances to date, both weak and strong secrecy constraints result in the same secrecy capacity. Another interesting secrecy condition is the semantic security constraint that was firstly introduced in cryptography and was lately extended to the wiretap channel context [24]. This secrecy condition alleviates the assumptions on the transmitted confidential message, i.e., it does not assume that the message is random and uniformly distributed. This is a new challenging and promising direction for research on information theoretic security.

2.3.1.2 Wiretap Coding

The achieving secrecy code that guarantees both the reliability and the security of the transmitted information is called a wiretap code. It is a stochastic code having a nested structure. As a matter of fact, instead of fixing the codeword associated with each message W, the codeword is chosen at random according to a local random number generator $W'\in\left\{1,\cdots,2^{n\mathcal{R}_{\mathrm{e}}}\right\}$, with $\mathcal{R}_{\mathrm{e}}$ denoting the equivocation rate,

i.e., $\mathcal{R}_{\mathrm{e}}{=}I\left(W;Y_{\mathrm{E}}^{n}\right)$. The set of $2^{n\mathcal{R}_{\mathrm{e}}}$ codewords, corresponding to each secret message, forms what we call a bin or a subcode of the wiretap code. To date, practical constructions of wiretap codes are only possible for some particular channels.

Although Wyner's model builds on the assumption of a degraded wiretap channel, where the signal at the eavesdropper is a degraded version of the legitimate receiver's signal, it provides the essential elements required to understand information theoretic security without the complexity of a more general setup. Ulterior works generalized Wyner's work to the case of non-degraded channels [25], Gaussian channels [26], and fading channels [27–31], to cite only few. For more details about the wiretap channel, wiretap coding or alternative coding techniques for secret communications, we invite the reader to consider the following references [3, 5, 6, 32].

2.3.2 Cooperative Jamming

One of the effective approaches proposed to improve security at the physical layer is to exploit some of the resources of the legitimate system for the transmission of jamming signals. This technique, called cooperative jamming, was originally proposed by Tekin and Yener in [33], and was further studied in [34], and [35]. The main idea of the work comes from the observation that causing interference in a wiretap setup can potentially increase the secrecy rate between the legitimate pairs. In fact, the injected interference would eventually introduce additional randomness in the channel. Cooperative jamming can be either achieved using Gaussian noise [33–35], random codebooks [36–38], or structured random codebooks [39–41]. For a detailed review of the aforementioned three forms of cooperative jamming, we kindly invite the reader to consider the following two references [42] and [12].

The collaborative approach, presented in [33–35], was analyzed when using Gaussian signals over a multiple access channel. Nonetheless, the concept of cooperative jamming is much more widely applicable and can be captured in different multi-user

and multiple-antenna wiretap channels. Different variants of the cooperative jamming technique are considered in the literature. In particular, the transmission of artificial noise, the noise forwarding technique, and the interference assisted secret communication approach. Despite this difference in the naming conventions, all these techniques are a special case of cooperative jamming [33], and they all involve the introduction of interference into the channel in the sole interest to improve the secrecy throughput.

2.3.3 Secrecy Performance Measure

To evaluate the performance of a communication system with a security constraint, the most commonly used metric is the secrecy capacity. The secrecy capacity $\mathcal{C}_{\mathrm{s}}$ is defined as the maximum achievable secrecy rate, i.e.,

$$\mathcal{C}_{\mathrm{s}} \triangleq \sup \mathcal{R}_{\mathrm{s}}, \tag{2.3}$$

where the supremum is over all achievable secrecy rates. It could be seen as the homologue of the traditional channel capacity with a secrecy constraint. We note that the secrecy capacity is said to be ergodic when it is averaged over a sufficiently long time period.

For Wyner's wiretap channel, the secrecy capacity is given as the difference between a rate of reliable communication and a rate of information leaked to the eavesdropper, i.e.,

$$\mathcal{C}_{\mathrm{s}} = \max_{U \to X \to Y_{\mathrm{R}} \to Y_{\mathrm{E}}} \left(I\left(U; Y_{\mathrm{R}}\right) - I\left(U; Y_{\mathrm{E}}\right) \right), \tag{2.4}$$

where U is an auxiliary random variable and $U \to X \to Y_{\mathrm{R}} \to Y_{\mathrm{E}}$ forms a Markov chain. From (2.4), it is clear that the secrecy capacity is positive as long as the transmitter and the legitimate receiver have an advantage over the eavesdropper at the physical layer. This is the case for Wyner's model since Y_{R} is a degraded version of Y_{E}. For a general fading channel, this could be viewed as transmitting only over the channel

instants where the main channel is better than the eavesdropper's channel. This brings us back to the issue of having CSIT. We should note that the non-degraded channel case was considered by Csiszár and Körner [25], and that their model is the one used for continuous channels. Another interesting work that has rejuvenated the wiretap channel approaches could be found in [43].

The secrecy performance is sometimes analyzed using the secrecy outage probability, which is defined as the probability that a target secrecy rate is unachievable. Yet, the operational meaning of this metric is still unclear to many members of the research community.

2.4 Sources of CSIT Uncertainty

In a wireless communication system, the knowledge of the CSI at the receiver (CSIR) is usually possible through training signals sent by the transmitter. For wiretap channels, these training signals can also be used by the eavesdropper who gets to estimate its channel gain too. The estimation of the CSI at the receiving nodes is generally very accurate thanks to the receivers' capability to deploy rapid channel tracking. As for acquiring the CSIT, the receiver should feed back its CSI to the transmitter constantly. This feedback process is typically accompanied by the introduction of uncertainty into the CSIT. Different phenomena can cause the CSIT to be imperfect. Most commonly, the uncertainty comes from an error of estimation at the transmitter who ends up with a noisy version of the CSI, or from a feedback link with a limited capacity which requires the transmission of quantized CSI, or also from a delayed feedback causing outdated CSIT.

2.4.1 Estimation Error of the CSIT

Estimation error is one of the most common reasons behind CSIT uncertainty. Research on physical layer security, with an estimation error of the main CSIT, generally

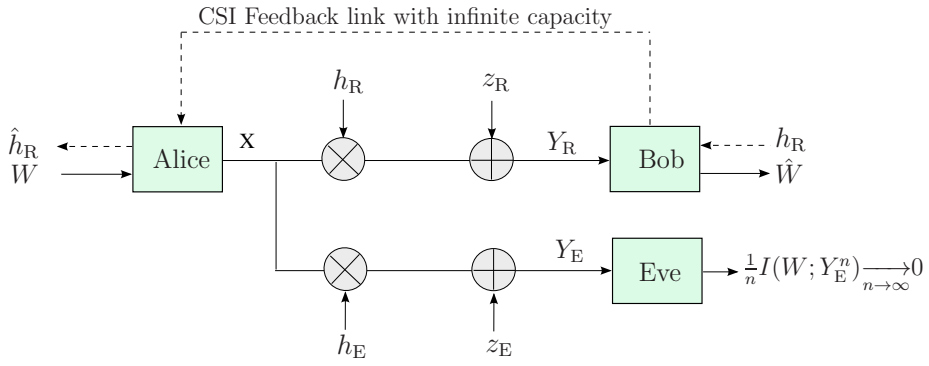


Figure 2.3: Fading wiretap channel with perfect CSIR and noisy estimation of the main CSIT.

assumes that the legitimate receiver sends its CSI to the transmitter through a feedback link with infinite capacity, cf. Figure 2.3.

The main channel gain estimation model can be formulated as

$$h_{\mathrm{R}}(t) = \sqrt{1-\alpha}\,\hat{h}_{\mathrm{R}}(t) + \sqrt{\alpha}\,\tilde{h}_{\mathrm{R}}(t), \tag{2.5}$$

where $h_{\mathrm{R}}(t)$ is the actual main CSI at time instant t, $\hat{h}_{\mathrm{R}}(t)$ is the noisy version of the CSI available at the transmitter, $\tilde{h}_{\mathrm{R}}(t)$ is the channel estimation error, and α is the estimation error variance ($\alpha \in [0,1]$). The case α=0 corresponds to the perfect main CSIT scenario while α=1 corresponds to the no main CSIT case. It is usually assumed that Bob can perfectly estimate its CSI and that Alice is only aware of the fading distribution of the wiretap channel. Besides, most research works consider the worst case scenario where the eavesdropper has a perfect knowledge of all channel gains.

2.4.2 CSI Feedback Link with Finite Capacity

Another cause of CSIT uncertainty is the transmission of the feedback information over finite-rate links. As a matter of fact, the process of procuring CSI is resource consuming in time-varying fading channels, and the accuracy of the obtained CSIT

is highly correlated with the size of the feedback overhead and the allocated power for feedback transmission. In block-fading channels, the acquisition of the CSIT during each coherence time takes place in three stages: transmission of a pilot signal destined for the receiver to estimates its channel gain, followed by CSI feedback to the transmitter, then data transmission, cf. Figure 2.4.

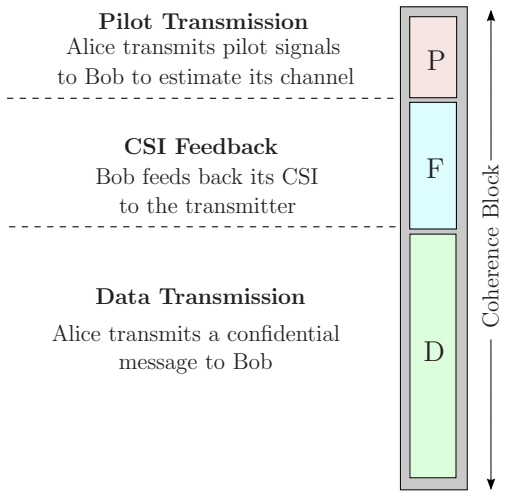


Figure 2.4: CSI training and data transmission over one coherence block.

Clearly, when more time is allocated to training, time for data transfer is reduced and vice versa. The fed back information is used to notify the transmitter about the forward link condition. A broad look at the field of limited feedback in wireless communication systems is provided in [44]. For works on information theoretic security with limited feedback, it is usually assumed that the receiver feeds back the index of a quantized version of the CSI, the index of the channel region in which the CSI lies, or the index of the quantized channel gain direction. It is also assumed, in most works, that the quantization codebook is fixed and known to all terminals, that the feedback link is error-free, and that both Bob and Eve estimate their respective channel gains perfectly.

2.4.3 Outdated CSIT

Delay in feedback transmission is one of the common sources of CSIT uncertainty. It causes the transmitter to base its transmission strategy on a time-delayed channel coefficient version of the current legitimate receiver's CSI. Considering a time-varying wiretap channel, where the main channel remains constant over a time slot and changes from one slot to another, it is generally assumed that the feedback delay is of the length of a time slot, i.e., at time instant t, Alice is aware of $h_{\mathrm{R}}(t-1)$. This particular scenario straightforwardly generalizes to the case when the delay is of multiple time slots length.

2.5 Literature Review

In this section, we present a comprehensive review of recent and ongoing research works on physical layer security. We focus on both information theoretic and signal processing approaches to the topic under different assumptions on the CSIT. Moreover, we provide a classification of these research works based on each of the three sources of CSIT uncertainty, presented in the previous section.

2.5.1 Physical Layer Security with Perfect CSIT

In recent years, the fading wiretap channel has opened new research directions for physical layer security. What is unique about the fading model is that even if the eavesdropper has a better SNR than the legitimate receiver, physical layer security can still be achieved without requiring the sharing of a secret key [27–29]. Figure 2.5 illustrates the fading wiretap channel where the respective received signals at the legitimate receiver and the eavesdropper can be represented as

$$\begin{aligned} Y_{\mathrm{R}}(t) &= h_{\mathrm{R}}(t)X(t) + z_{\mathrm{R}}(t) \\ Y_{\mathrm{E}}(t) &= h_{\mathrm{E}}(t)X(t) + z_{\mathrm{E}}(t) \end{aligned}, \tag{2.6}$$

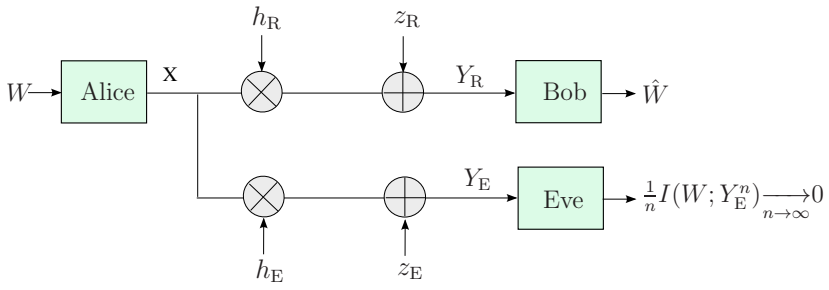


Figure 2.5: Fading wiretap channel.

where t denotes the time instant, $X(t)$ is the transmitted signal, $h_{\mathrm{R}}(t)$ and $h_{\mathrm{E}}(t)$ are the respective channel gains of Bob and Eve's channels, and $z_{\mathrm{R}}(t)$ and $z_{\mathrm{E}}(t)$ represent the additive white Gaussian noises at the respective receivers. The fading coefficients h_{R} and h_{E} are usually assumed mutually independent, and an average transmit power is generally imposed at the transmitter.

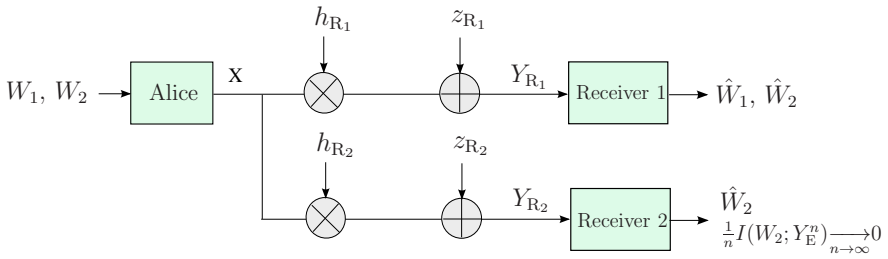
To make the most of what the fading channel has to offer to physical layer security, the knowledge of the CSIT is of primordial importance. A vast majority of works assume that the transmitter has a perfect knowledge of the CSI of both the main and the eavesdropper channels or at least of the main channel. In this subsection, we are interested in these research works where the perfect CSI assumption is made. We start by considering the case when both the main and the eavesdropper channel gains are revealed to the transmitter. Then, we look at the case when only the main CSI is perfectly known at the transmitter.

2.5.1.1 Both the Main and the Eavesdropper CSI are Perfectly Known:

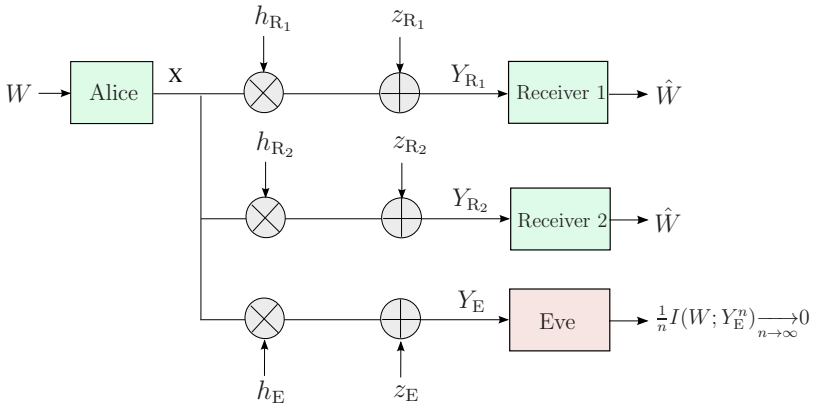
When the transmitter is perfectly aware of the legitimate receiver's and the eavesdropper's CSI, the optimal transmission scheme is to send the confidential information only

when the main CSI is better than the eavesdropper's CSI and adapt the transmitted power according to the instantaneous values of the channel gains. The block-fading wiretap channel is considered in [28], where the ergodic secrecy capacity is established in both cases, when the eavesdropper's CSI is available at the transmitter and when it is not. The effect of correlation between the main and the wiretap block-fading channels is investigated in [45, 46], where the loss engendered by the correlation is quantified in terms of the secrecy capacity. The authors in [47] examine the case of frequency-selective fading channels. The model of interest is the broadcast channel with confidential message, in which the source has a common message to transmit to two receivers (Receiver 1 and 2) and a confidential message to transmit to only one of the receivers (Receiver 1) while keeping it secret from the other (Receiver 2). Figure 2.6 highlights the difference between the broadcast channel with confidential information, the broadcast wiretap channel with common message transmission, and the broadcast wiretap channel with independent messages. The work in [47] proposes a practical Vandermonde precoding to exploits the zeros of Receiver 2's channel to hide the secret information in a similar way to spatial beamforming. The ergodic secrecy capacity region of the BCCM is established in [31]. Further results on the BCCM can be found in [48–50]. The frequency-selective fading model is also considered in [51], where the secure degrees of freedom of a K user interference channel are analyzed.

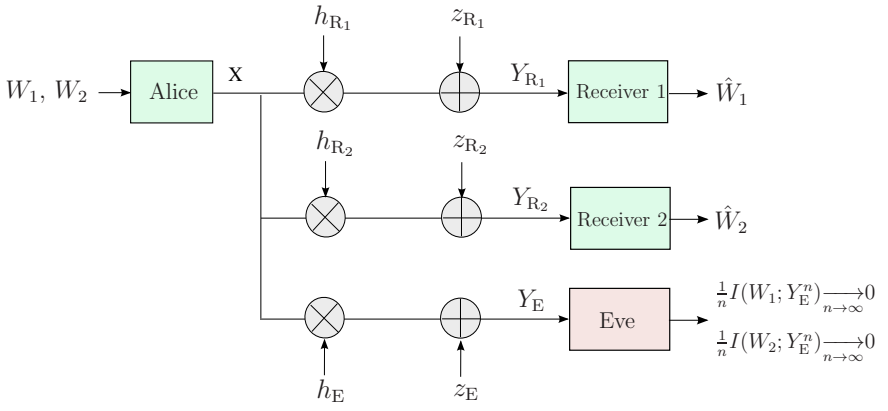
In the last few years, multiple antenna wiretap channels have become a compelling research topic. In [52] and [53], the authors investigate the secrecy capacity of a multi-antenna quasi-static fading wiretap channel and highlight the positive impact of deploying multiple antennas on the confidentiality of the system. The work in [54] considers the case of a degraded single-input-multiple-output (SIMO) wiretap channel and shows that the secrecy diversity gain is proportional to the number of receive antennas. The multiple-input-single-output (MISO) case is studied in [36,55,56]. The secrecy capacity of the MIMO wiretap channel with a single antenna eavesdropper



(a) Two-user broadcast channel with a confidential message.



(b) Two-user broadcast wiretap channel with common message transmission.



(c) Two-user broadcast wiretap channel with independent messages transmission.

Figure 2.6: Two-user broadcast channel with secrecy constraints.

is examined in [57], and the case of MIMO transmission with a multiple-antenna eavesdropper is considered in [37, 58–62] when the channel gain matrices are fixed and known to all terminals. Analysis on the secure degrees of freedom, the secrecy diversity gain, and the secrecy multiplexing gain can be found in [63] and references therein.

Other works on physical layer security with full CSIT include [38, 64–70] where the security of cooperative systems is investigated, [71–75] where cognitive systems with confidentiality constraints are considered, and [76–78] for secure massive MIMO.

2.5.1.2 Only the Main CSI is Perfectly Known at the Transmitter:

In this case, it is generally assumed that the transmitter is aware of the fading distribution of the eavesdropper's CSI but not of its instantaneous realizations. Baros and Rodrigues, [27], were one of the first to emphasize the key role fading channels play in enhancing the information theoretical security of wireless communication systems. Their model consists of a quasi-static Rayleigh fading channel where the channel gains remain constant over all channel uses, and only the main CSI is perfectly known to the transmitter. The work characterizes the outage secrecy capacity of the system and interestingly shows that secure transmission is possible even when the average SNR of the eavesdropper is better than that of the legitimate receiver. An extension of their work, considering the case when an imperfect estimation of the eavesdropper's CSI is also available at the transmitter, is presented in [29]. The authors in [79] investigate the achievable secrecy rate of a wiretap channel with a constant AWGN main channel and a time varying Rayleigh fading eavesdropper's channel. The ergodic secrecy capacity and the optimal transmission power for block-fading channels are examined in [28]. Block-fading channels are also considered in [80], where the secrecy outage probability of the system is evaluated under different secure hybrid auto-

matic re-transmission request (HARQ) protocols. The work in [81] and [30] analyses the ergodic secrecy capacity of parallel channels and fast fading broadcast channels. Both cases, when a common information is transmitted to all the legitimate receivers, and when each receiver is interested in an independent information, are considered. Research on multiple antenna wiretap channels assuming perfect main CSI and no eavesdropper's CSI at the transmitter may be found in [82–86] and in [87–99] for cooperative jamming. Another work, [100], study the optimal beamforming design for a MISO system with perfect main CSI and a noisy version of the eavesdropper's CSI available at the transmitter. Other works include [101–103].

2.5.1.3 Arbitrarily Varying Eavesdropper Channel

A particularly interesting case where the transmitter does not have any knowledge about the eavesdropper's channel, not even the statistical knowledge or the distribution of the wiretapper gain, is found in the framework of arbitrary varying eavesdropper channel [104]. Under such an assumption on the eavesdropper's channel state and assuming that the number of antennas of the eavesdropper is limited, the authors in [104] derived the SDoF of the MIMO wiretap channel. This work was later on extended to the multi-user setup in [105], [106], and [107].

Although the assumption of perfect main CSIT makes the secrecy analysis more tractable and allows the characterization of the full potential of the fading wiretap channel, it does not capture the practicality of the transmission system. On one hand, the knowledge of the eavesdropper's CSIT is far from possible in a real scenario as Eve is a passive node who does not transmit and whose sole interest is to intercept the communication between Alice and Bob. That is, the eavesdropper has no interest in giving Alice its CSI. This assumption is usually justified by considering that Eve belongs to the same communication network as Alice and Bob and that all users

provide the transmitter with their CSI prior to data transmission. However, as Eve is a malicious node, nothing guarantees that it will give Alice its actual CSI. On the other hand, in a practical communication system, only partial main CSI can be obtained at the transmitter. We will discuss this latter case in the following subsection.

2.5.2 Physical Layer Security with Main CSIT Uncertainty

Considering the three main causes of CSIT imperfection, presented earlier, we provide in what follows an exhaustive list of research works on physical layer security with main channel gain uncertainty. This list also takes into account the research work presented in the remaining of this thesis.

2.5.2.1 PLS with Noisy Main CSIT

One of the first works in this research area is [108] and its journal version [109], where the ergodic secrecy capacity, of a single-antenna single-user fast fading wiretap channel with a noisy CSIT, is characterized by a lower and an upper bound. The proposed achievable secrecy rate is based on a standard wiretap code with a Gaussian input and a simple on-off power transmission scheme while the upper bound is obtained using an appropriate correlation between the main and the wiretap channels. The authors show that even with a high estimation error, the transmitter can still achieve a positive secrecy rate, and that a simple constant rate on-off power scheme is enough to establish a secure communication. A concurrent work, presented in [110], investigates the achievable secrecy rate of ergodic and block-ergodic fading channels in the presence of imperfect CSIT about both the main channel and the eavesdropper's channel. The presented results suggest that CSIT uncertainty does not necessarily preclude security and that relatively little CSIT is required to take advantage of fading. The problem of secure multiuser broadcasting over fast fading channels with noisy CSIT is considered in Chapter 3 of this thesis, and was published

in [111] and [112]. The work derives bounds on the ergodic secrecy capacity when a common message is broadcasted to all legitimate receivers and bounds on the ergodic secrecy sum-capacity when multiple independent messages are broadcasted. In both scenarios, common message and independent messages, the transmitted information has to be kept secret from the eavesdropper. The scaling law of the system, when transmitting to a large number of legitimate receivers, is also analyzed.

Multiple antenna wiretap channels with an estimation error of the main CSIT have raised considerable research interset. The performance analyses of a multi-cell MISO downlink system, where a multi-antenna base station transmits confidential messages to its legitimate users with a passive eavesdropper present in each cell, are approached in [113] from a signal processing perspective. It is assumed that the receivers only feed back the channel gain directions, required to cancel out the inter-cell interference, and that an error of estimation occurs at the base station. Closed-form expression for the ergodic secrecy rate, the secrecy outage probability, and the interception probability are presented for Rayleigh fading channels. The ergodic secrecy capacity of MISO wiretap communication systems is characterized in [114] and the achievable secrecy rate is evaluated in [115] and [116] using transmit beamforming. The case when a noisy estimate of the eavesdroppers channel is also available at the transmitter is addressed in [116] and in [117] where different secrecy rate optimization techniques are proposed for MISO channels. An earlier work on MIMO wiretap channels with artificial noise transmission is conducted in [118]. The focus of this study is twofold. First, to maximize the amount of power available to broadcast a jamming signal while maintaining a predefined SINR at the desired receiver. Second, to assess the resulting performance degradation due to the presence of imperfect CSIT. Noisy estimation of the main CSIT is also considered in [119] for massive MIMO system, in [120] for cooperative wiretap channels, and in [121] for cognitive radio networks.

2.5.2.2 PLS with Limited Main CSI Feedback

In [122] and [123], the ergodic secrecy capacity of block-fading wiretap channels with limited-rate feedback is investigated. The study establishes lower and upper bounds on the secrecy capacity when the feedback information is sent at the beginning of each coherence block over an error-free public channel with finite capacity. The proposed bounds coincide as the capacity of the feedback link goes to infinity, hence, fully characterizing the secrecy capacity in this case. It is also shown that a positive secrecy rate can still be achievable even when only 1-bit ARQ feedback is sent to the transmitter at the end of each coherence block. Multiuser block-fading broadcast channels, where the transmission is intended for multiple legitimate receivers in the presence of an eavesdropper, is examined in Chapter 4 of this thesis, and was published in [124]. Here too, the presented lower and upper bounds on the ergodic secrecy capacity for the common message case and lower and upper bounds on the secrecy sum-rate for the independent messages case are shown to coincide for the particular case of infinite feedback. The ergodic secrecy capacity region of the block-fading BCCM in which the transmitter has common information for two receivers and confidential information intended for only one of them is tackled in Chapter 5 of this thesis, and was published in [125]. Both cases when the feedback link is error-free and when it is a BEC are analyzed. In the latter case, it is demonstrated that as long as the erasure event is not a probability 1 event, Alice can still transmit the confidential information with a positive secrecy rate.

The impact of having imperfect CSIT obtained via a limited rate feedback on the throughput of multiple antenna wiretap channels was elaborated first in [126–128]. The work considers both MISO and MIMO communication systems with artificial noise transmission and investigates the optimal power allocation strategy that maximizes the secrecy rate. The achievable secrecy rate of MIMO wiretap channels is also addressed in [129], [130], and [131]. In [129], a transmission strategy based on

cooperative jamming and linear precoding is proposed to overcome CSIT imperfection in the presence of an adversarial jammer. The main CSI feedback is quantized using Grassmannian quantization, [132], and sufficient conditions on the feedback bit rate scaling are derived to guarantee the same SDoF as for the perfect CSIT case. In [130], artificial noise assisted secure transmission is considered in the context of frequency-division duplexed MIMO wiretap channels. The work defines the achievable effective ergodic secrecy rate (ESR) and evaluates the optimal power allocation and training overhead that maximize it when the channel direction information of the eavesdropper is available at the transmitter. The transmission of jamming signals is also adopted in [131] with random vector quantization (RVQ). The results show that a positive secrecy rate can always be achieved when the number of feedback bits is large, the artificial noise power is high, and a constraint on the number of antennas at the eavesdropper is satisfied. A characterization of the ergodic secrecy capacity in terms of lower and upper bounds is presented in Chapter 6 of this thesis, and was published in [133]. The work also proposes an optimal framework for feedback and transmission which is based on the iterative Lloyd algorithm [19]. The ergodic secrecy sum-rate of multiuser multi-antenna downlink systems with limited main channel direction feedback is discussed in [134] and [128]. On another note, the authors in [135] assume that in addition to having a limited rate feedback, a CSI estimation error occurs at the legitimate receiver. Under this assumption, an upper bound on the secrecy rate loss is derived and used to design an optimal CSI feedback strategy that maintains a predefined secrecy service quality (QoS).

2.5.2.3 PLS with Outdated Main CSIT

The impact of outdated CSIT on the secrecy outage performance of MISO wiretap channels with transmit antenna selection (TAS) is evaluated in [136]. The authors present a closed-form expression for the secrecy outage probability when the trans-

mission is conveyed over Nakagami-m fading channels, and show that a significant diversity loss results from making use of the delayed CSI version to select the optimal transmit antenna. The secrecy outage performance with CSI feedback delay and TAS is also addressed in [137] and [138], for MIMO wiretap channels. The work in [137] proposes a new secure transmission scheme intended to defeat the detrimental effect the outdated CSI have on transmit antenna selection. The presented strategy requires two feedback phases sent in different time slots, take spatial correlation at the legitimate receiver into consideration, and guarantees a better outage performance. The probability of non-zero secrecy capacity is also investigated, and the loss in terms of the secrecy diversity is assessed. In [138], a general order TAS scheme is proposed to enhance the secrecy performance of Nakagami-m MIMO fading wiretap channels with outdated CSI. The work considers both cases when Alice is aware of Eve's instantaneous CSI and when it is not. In the first scenario, the average secrecy capacity of the system is analyzed while in the second scenario, the secrecy outage probability and the probability of non-zero secrecy capacity are derived.

Other research works on physical layer security with outdated main CSI analyze the repercussion of CSIT imperfection on the system's secure degrees of freedom. In [139], the SDoF of a two-user MIMO broadcast wiretap channel with outdated CSI is characterized. The achieving scheme is based on an aligned transmission of artificial noise along with the confidential information. The case when the transmitter has also access to a delayed version of the eavesdropper's CSI is also studied. Obviously, the secure performances in the latter case are better compared to when Alice is only aware of the outdated main CSI. The authors in [140] investigate the sum SDoF region of a two-user MIMO X-channel under secrecy constraints with a delayed CSIT sent over an asymmetric feedback link. The work highlights the importance of sending an asymmetric output feedback in conjunction with the outdated CSI to improve the secrecy performance of the system. Moreover, it shows that the sum SDoF region of

the adopted model is the same as the SDoF region of a two-user MIMO broadcast channel with feedback delay. Another work, presented in [141], examines the SDoF of a single antenna wiretap channel with a cooperative jammer and an arbitrary number of eavesdroppers. Assuming that both the transmitter and the jammer have access to outdated main CSI and that linear coding transmission strategies are employed, it is proven that a strictly positive SDoF is achievable irrespective of the number of eavesdroppers.

The effect of delayed feedback coupled with an estimation error of the CSI at the transmitter is discussed in [142]. The work investigates an optimal masked beamforming scheme to enhance the secure performance of a multiuser MIMO downlink wiretap channel with noisy and outdated CSIT. The presented technique aims to maximize the transmission power allocated to artificial noise while meeting individual minimum mean square error (MMSE) constraints of the legitimate users. The obtained results show that the adopted approach can significantly reduce the sensitivity of the system to CSIT imperfections.

2.6 Conclusion

In the last few years, research on physical layer security tends to consider practical communication scenarios. Indeed, there has been more and more interest is studying the impact of having imperfect CSIT on the secrecy performances of wireless communication systems with security constraints. The work presented in this thesis is one of the earliest research works on physical layer security with CSIT uncertainty.

Chapter 3

Secure Multi-User Broadcasting with Noisy CSIT

3.1 Introduction

In this chapter, we investigate the problem of secure broadcasting over fast fading channels with imperfect main CSIT. In particular, we analyze the effect of having an estimation error of the main CSIT on the secrecy throughput of a multi-user broadcast wiretap channel. First, we discuss the independent messages case where the transmitter broadcasts multiple confidential messages to the receivers. For this case, we present an expression for the achievable secrecy sum-rate and an upper bound on the secrecy sum-capacity and we show that, in the limit of large number of legitimate receivers K, our achievable secrecy sum-rate follows the scaling law $\log((1-\alpha)\log(K))$, where α is the estimation error variance of the main CSI. Then, we look at the common message transmission case where the source broadcasts the same secret information to all the legitimate receivers. For this case, we characterize the ergodic secrecy capacity of the system and we show that the secrecy rate is limited by the legitimate user having, on average, the worst main channel link. Also, we prove that a non-zero secrecy rate can still be achieved even with a noisy CSIT.

This chapter is organized as follows. Section 3.2 describes the system model. The main results along with the corresponding proofs are introduced in section 3.3 for the independent messages case and in section 3.4 for the common message case. Section 3.5 considers the illustrative example of Rayleigh fading. Finally, selected numerical results are presented in section 3.6 while section 3.7 concludes the chapter.

3.2 System Model

We consider a multi-user broadcast wiretap channel where a transmitter T communicates with K legitimate receivers $(\mathrm{R}_1, \cdots, \mathrm{R}_K)$, in the presence of an eavesdropper E, as depicted in Figure 3.1.

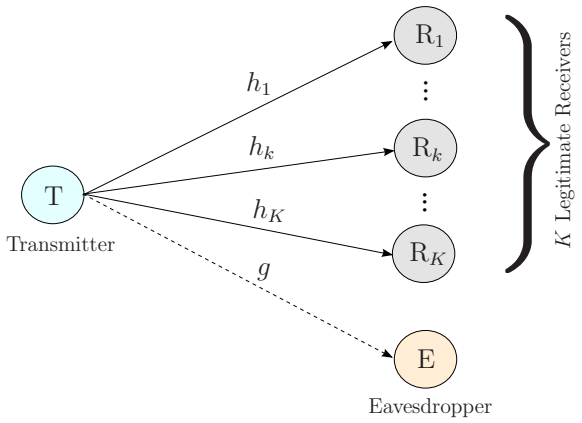


Figure 3.1: Multi-user broadcast wiretap channel.

Each terminal is equipped with a single antenna for transmission and reception. During each coherence interval $i \in \{1, \cdots, n\}$, the received signals by the k-th legitimate receiver $\mathrm{R}_k, k \in \{1, \cdots, K\}$, and the eavesdropper are respectively given by

$$\begin{cases} Y_k(i) = h_k(i)X(i) + v_k(i) \\ Z(i) = g(i)X(i) + w(i), \end{cases} \tag{3.1}$$

where $h_k(i) \in \mathbb{C}$ and $g(i) \in \mathbb{C}$ are zero-mean, unit-variance, complex Gaussian channel gains corresponding to the k-th legitimate channel and the eavesdropper's channel, respectively, $v_k(i) \in \mathbb{C}$ and $w(i) \in \mathbb{C}$ represent the zero-mean, unit-variance, circularly symmetric white Gaussian noise at R_k and E, respectively, and $X(i)$ is the transmitted codeword to all the receivers. An average transmit power constraint is imposed at

the transmitter such that

$$\frac{1}{n}\sum_{i=1}^{n}\mathbb{E}[|X(i)|^2] \leq P_{\text{avg}}, \tag{3.2}$$

where the expectation is over the input distribution.

The channel gains h_k and g are independent, ergodic, and stationary with bounded[1] probability density functions (PDFs). We consider that the transmitter is only aware of the distribution of the eavesdropper's CSI and not of its instantaneous channel realizations $g(i)$. Also, we assume that the transmitter is only provided with a noisy version of each $h_k(i)$, say $\hat{h}_k(i)$, such that the main channel estimation model can be written as

$$h_k(i) = \sqrt{1-\alpha}\hat{h}_k(i) + \sqrt{\alpha}\tilde{h}_k(i), \tag{3.3}$$

where α is the estimation error variance, $\alpha \in [0,1]$, and $\tilde{h}_k(i)$ is the channel estimation error. We assume that $\hat{h}_k(i)$ and $\tilde{h}_k(i)$ are uncorrelated and hence independent, and that h_k, $\hat{h}_k(i)$, $\tilde{h}_k(i)$, and g are all identically distributed[2]. To ensure correct decoding with high probability at the legitimate receivers' side, we assume that each receiver R_k has a perfect knowledge of its channel gain $h_k(i)$. Also, we assume that the eavesdropper is aware of its channel gain $g(i)$, and of all the legitimate receivers' channel gains $h_k(i), k \in \{1, \cdots, K\}$. Giving that the channel gains are ergodic and

---

[1]The bounded distributions' assumption means that the channel gains vary according to distributions with finite probabilistic measures, notably, finite means and variances. This ensures that the presented results are meaningful. Also, this is used in the derivations as the Jensens inequality fails in the infinite setting. We should note, though, that the probability distributions describing the fluctuations of fading channels are generally bounded. For peculiar fading channels, we believe the results still conceptually hold true but may require different mathematical formulations.

[2]We particularly need the assumption that $\tilde{h}_k$ and g are identically distributed for the proofs of the upper bounds. Besides, the reason why we opted for the same distribution for g and h_k is to ensure a fair comparison. It goes without saying that when, in average, the main channel is better than the eavesdropper channel, the secrecy capacity increases, while in the opposite case it decreases. As for $\hat{h}_k$ and $\tilde{h}_k$, we recall that they are related to h_k through the relation $h_k = \sqrt{1-\alpha}\hat{h}_k + \sqrt{\alpha}\tilde{h}_k$. That is, in the case when $\hat{h}_k$ and $\tilde{h}_k$ are $\mathcal{CN}(0,1)$, channel gain h_k is, as a matter of fact, $\mathcal{CN}(0,1)$ (using the fact that if $X_1 \sim \mathcal{CN}(\mu_1, \sigma_1^2)$ and $X_2 \sim \mathcal{CN}(\mu_2, \sigma_2^2)$, then $X_1 + X_2 \sim \mathcal{CN}(\mu_1+\mu_2, \sigma_1^2+\sigma_2^2)$ and $Y = aX_1 + b \sim \mathcal{CN}(a\mu_1+b, a^2\sigma_1^2)$, with $a, b \in \mathbb{R}$). In the other way round, if h_k is $\mathcal{CN}(0,1)$, then $\hat{h}_k$ and $\tilde{h}_k$ should also be $\mathcal{CN}(0,1)$. Indeed, if we suppose that $\hat{h}_k$ is $\mathcal{CN}(\hat{\mu}, \hat{\sigma})$ and $\tilde{h}_k$ is $\mathcal{CN}(\tilde{\mu}, \tilde{\sigma})$, then h_k should be $\mathcal{CN}(\sqrt{1-\alpha}\hat{\mu} + \sqrt{\alpha}\tilde{\mu}, (1-\alpha)\hat{\sigma} + \alpha\tilde{\sigma})$ for all values of α. Since h_k is $\mathcal{CN}(0,1)$, then for $\alpha = 1$ we get $\tilde{\mu} = 0$ and $\tilde{\sigma} = 1$, and for $\alpha = 0$ we get $\hat{\mu} = 0$ and $\hat{\sigma} = 1$.

stationary, the index time i can be omitted. In the remainder of this chapter, we denote $|h_k|^2$, $|\hat{h}_k|^2$, $|\tilde{h}_k|^2$ and $|g|^2$ by γ_k, $\hat{\gamma}_k$, $\tilde{\gamma}_k$ and γ_e, respectively.

We are interested in the broadcast secrecy capacity of such a channel when the transmitted codeword is large, i.e., $n \to \infty$. In accordance with Wyner's definition for weak secrecy, we consider that a secret transmission is achieved when the normalized leakage of information that the eavesdropper gets about the broadcasted message, by observing its channel output, vanishes in the limit of long block lengths.

3.3 Broadcasting Independent Messages

In this section, we consider the independent messages case when multiple confidential messages are transmitted to the legitimate receivers while being kept secret from the eavesdropper. Taking into account the adopted system model, we characterize the ergodic secrecy sum-capacity in the general case, then, we investigate the special cases of high-SNR and perfect main CSIT.

3.3.1 Secrecy Sum-Capacity Characterization

Here, we present the main results obtained for the ergodic secrecy sum-capacity with a noisy estimation of the CSIT. The proofs of the presented results are provided in the following subsection.

3.3.1.1 Lower and Upper Bounds

THEOREM 3.1. The ergodic secrecy sum-capacity of the multi-user fading broadcast wiretap channel with noisy main CSIT is characterized as

$$\widetilde{\mathcal{C}}_{\mathrm{s}}^{-} \leq \widetilde{\mathcal{C}}_{\mathrm{s}} \leq \widetilde{\mathcal{C}}_{\mathrm{s}}^{+}, \tag{3.4}$$

where $\widetilde{\mathcal{C}}_{\rm s}^{-}$ and $\widetilde{\mathcal{C}}_{\rm s}^{+}$ are given by

$$\widetilde{\mathcal{C}}_{\rm s}^{-} = \max_{P(\tau)} \mathop{\mathbb{E}}_{\substack{\gamma_e,\gamma_{\max}^{\rm est},\\ \hat{\gamma}_{\max}\geq\tau}} \left[\log\left(\frac{1+\gamma_{\max}^{\rm est}P(\tau)}{1+\gamma_e P(\tau)}\right)\right], \tag{3.5}$$

$$\widetilde{\mathcal{C}}_{\rm s}^{+} = \min\left\{\max_{P(\hat{\Gamma})} \mathop{\mathbb{E}}_{\gamma_{\max},\hat{\Gamma},\tilde{\gamma}} \left[\left\{\log\left(\frac{1+\gamma_{\max}P(\hat{\Gamma})}{1+\tilde{\gamma}P(\hat{\Gamma})}\right)\right\}^{+}\right], K\max_{P(\hat{\gamma})} \mathop{\mathbb{E}}_{\gamma,\hat{\gamma},\tilde{\gamma}} \left[\left\{\log\left(\frac{1+\gamma P(\hat{\gamma})}{1+\tilde{\gamma}P(\hat{\gamma})}\right)\right\}^{+}\right]\right\}, \tag{3.6}$$

with $P(\tau)=P_{\rm avg}/\left(1-F_{\hat{\gamma}_{\max}}(\tau)\right)$, $\gamma_{\max}^{\rm est}=|\sqrt{1-\alpha}\hat{h}_{\max}+\sqrt{\alpha}\tilde{h}|^2$, $\hat{\gamma}_{\max} = \max_{1\leq k\leq K}\hat{\gamma}_k$, $\hat{\Gamma}=(\hat{\gamma}_1,\hat{\gamma}_2,\cdots,\hat{\gamma}_K)$, $\gamma_{\max} = \max_{1\leq k\leq K}\gamma_k$, $\mathbb{E}[P(\hat{\Gamma})]\leq P_{\rm avg}$ and $\mathbb{E}[P(\hat{\gamma})]\leq P_{\rm avg}$.

Proof. A detailed proof of Theorem 3.1 is provided in the following subsection. From the obtained results, we can see that the upper bound on the secrecy sum-capacity is given as the minimum between two upper bounds. The reason behind choosing this particular representation was to ensure having the tightest possible upper bound for all the values of the error variance α. We would note that the second bound is a loose upper bound for the secrecy sum-rate for most values of α, especially when the number of users K is large. However, when the CSIT gets very noisy, i.e., $\alpha\to 1$, this bound becomes tighter.

3.3.1.2 High-SNR Regime

Corollary 3.1. At high SNR, the ergodic secrecy sum-capacity of the multi-user fading broadcast wiretap channel with noisy main CSIT is bounded as

$$\widetilde{\mathcal{C}}_{\text{H-SNR}}^{-} \leq \widetilde{\mathcal{C}}_{\rm s} \leq \widetilde{\mathcal{C}}_{\text{H-SNR}}^{+}, \tag{3.7}$$

where $\widetilde{\mathcal{C}}_{\text{H-SNR}}^{-}$ and $\widetilde{\mathcal{C}}_{\text{H-SNR}}^{+}$ are given by

$$\widetilde{\mathcal{C}}_{\text{H-SNR}}^{-} = \mathop{\mathbb{E}}_{\substack{\gamma_e,\gamma_{\max}^{\rm est},\\ \hat{\gamma}_{\max}\geq\tau}} \left[\log\left(\frac{\gamma_{\max}^{\rm est}}{\gamma_e}\right)\right], \tag{3.8}$$

$$\widetilde{\mathcal{C}}_{\text{H-SNR}}^{+} = \min\left\{\mathop{\mathbb{E}}_{\gamma_{\max},\tilde{\gamma}} \left[\left\{\log\left(\frac{\gamma_{\max}}{\tilde{\gamma}}\right)\right\}^{+}\right], K\mathop{\mathbb{E}}_{\gamma,\tilde{\gamma}} \left[\left\{\log\left(\frac{\gamma}{\tilde{\gamma}}\right)\right\}^{+}\right]\right\}, \tag{3.9}$$

with the transmission threshold τ satisfying $\mathop{\mathbb{E}}_{\gamma_{\max}^{\rm est}|\hat{\gamma}_{\max}}\left[\log(\gamma_{\max}^{\rm est})\,\middle|\,\hat{\gamma}_{\max}=\tau\right] - \mathop{\mathbb{E}}_{\gamma_e}\left[\log(\gamma_e)\right]=0$.

Proof. The proof of Corollary 3.1 is provided in the following subsection.

From the obtained high-SNR results, we can see that the asymptotic bounds depend on the number of legitimate receivers K. By considering a very large number of legitimate users, i.e., letting K go to ∞ in these asymptotic expressions, we characterize the scaling law of the system in Section 3.5.

3.3.1.3 Perfect Main CSI case

COROLLARY 3.2. When the transmitter has perfect knowledge of the legitimate receivers' CSI, the secrecy sum-capacity is bounded as

$$\widetilde{\mathcal{C}}^{-}_{\text{P-CSI}} \leq \widetilde{\mathcal{C}}_{\text{s}} \leq \widetilde{\mathcal{C}}^{+}_{\text{P-CSI}}, \tag{3.10}$$

where $\widetilde{\mathcal{C}}^{-}_{\text{P-CSI}}$ and $\widetilde{\mathcal{C}}^{+}_{\text{P-CSI}}$ are given by

$$\widetilde{\mathcal{C}}^{-}_{\text{P-CSI}} = \max_{P(\tau)} \mathop{\mathbb{E}}_{\gamma_e, \gamma_{\max} \geq \tau} \left[\log \left(\frac{1+\gamma_{\max} P(\tau)}{1+\gamma_e P(\tau)} \right) \right], \tag{3.11}$$

$$\widetilde{\mathcal{C}}^{+}_{\text{P-CSI}} = \max_{P(\gamma_{\max})} \mathop{\mathbb{E}}_{\gamma_{\max}, \gamma_e} \left[\left\{ \log \left(\frac{1+\gamma_{\max} P(\gamma_{\max})}{1+\gamma_e P(\gamma_{\max})} \right) \right\}^{+} \right], \tag{3.12}$$

with $P(\tau) = P_{\text{avg}} / \left(1 - F_{\gamma_{\max}}(\tau)\right)$ and $\mathbb{E}[P(\gamma_{\max})] \leq P_{\text{avg}}$.

Proof. The proof of Corollary 3.2 is provided in the following subsection.

Remark: When no main CSI is available at the transmitter, the secrecy sum-capacity of the system is equal to zero, i.e., $\widetilde{\mathcal{C}}_{\text{s}} = 0$.

3.3.2 Secrecy Sum-Capacity Analysis

In this subsection, we establish the obtained results for the ergodic secrecy sum-capacity presented in Theorem 3.1 and Corollaries 3.1 and 3.2.

3.3.2.1 Achievability Scheme in Theorem 3.1

The lower bound on the secrecy sum-capacity is achieved using a time division multiplexing scheme that selects instantaneously one receiver to transmit to. That is, at each time, the source only transmits to the user with the best estimated channel gain $\hat{h}_{\max}$. Since we are transmitting to only one legitimate receiver at a time, the achieving coding scheme consists on using independent standard single user wiretap codebooks with power $P(\hat{\gamma}_{\max})$ satisfying the constraint $\mathbb{E}[P(\hat{\gamma}_{\max})]\leq P_{\text{avg}}$. We consider an on-off power scheme that instantaneously adapts the power according to the value of $\hat{\gamma}_{\max}$ with regards to a prefixed threshold τ, i.e.,

$$P(\hat{\gamma}_{\max})=\begin{cases} P(\tau)=\dfrac{P_{\text{avg}}}{1-F_{\hat{\gamma}_{\max}}(\tau)} & \hat{\gamma}_{\max}\geq\tau \\ 0 & \text{otherwise.} \end{cases} \tag{3.13}$$

The achievable sum-rate is then given by

$$\widetilde{\mathcal{R}}^{-}=\mathop{\mathbb{E}}_{\substack{\gamma_e,\gamma_{\max}^{\text{est}},\\ \hat{\gamma}_{\max}\geq\tau}}\left[\log\left(\frac{1+\gamma_{\max}^{\text{est}}P(\tau)}{1+\gamma_e P(\tau)}\right)\right]. \tag{3.14}$$

To finish the proof, we maximize $\widetilde{\mathcal{R}}^{-}$ over $P(\tau)$ yielding the lower bound presented in Theorem 3.1. □

3.3.2.2 Proof of the Upper Bound in Theorem 3.1

We represent the upper bound on the secrecy sum-capacity as the minimum between two upper bounds, i.e.,

$$\widetilde{\mathcal{C}}_{\text{s}}^{+}=\min\left\{\widetilde{\mathcal{C}}_1^{+},\widetilde{\mathcal{C}}_2^{+}\right\}, \tag{3.15}$$

where $\widetilde{\mathcal{C}}_1^{+}$ and $\widetilde{\mathcal{C}}_2^{+}$ are respectively given by

$$\widetilde{\mathcal{C}}_1^{+}=\max_{P(\hat{\Gamma})}\mathop{\mathbb{E}}_{\gamma_{\max},\hat{\Gamma},\tilde{\gamma}}\left[\left\{\log\left(\frac{1+\gamma_{\max}P(\hat{\Gamma})}{1+\tilde{\gamma}P(\hat{\Gamma})}\right)\right\}^{+}\right] \quad \text{and} \quad \widetilde{\mathcal{C}}_2^{+}=K\max_{P(\hat{\gamma})}\mathop{\mathbb{E}}_{\gamma,\hat{\gamma},\tilde{\gamma}}\left[\left\{\log\left(\frac{1+\gamma P(\hat{\gamma})}{1+\tilde{\gamma}P(\hat{\gamma})}\right)\right\}^{+}\right].$$

The reason behind choosing this particular representation was to ensure having the tightest possible upper bound for all the values of the error variance α. We would note that $\widetilde{\mathcal{C}}_2^+$ is a loose upper bound for the secrecy sum-rate for most values of α, especially when the number of users K is large. However, when the CSI available at the transmitter gets very noisy, i.e., $\alpha \to 1$, $\widetilde{\mathcal{C}}_2^+$ becomes tighter then $\widetilde{\mathcal{C}}_1^+$. Moreover, for $\alpha=1$, $\widetilde{\mathcal{C}}_2^+$ vanishes, reflecting the fact that the secrecy capacity is zero for the no CSI case, while $\widetilde{\mathcal{C}}_1^+$ does not. To prove that $\widetilde{\mathcal{C}}_{\rm s}^+$ is an upper bound, we need then to prove that both $\widetilde{\mathcal{C}}_1^+$ and $\widetilde{\mathcal{C}}_2^+$ upper bound the secrecy sum-capacity of the system.

Using the result in (3.63), the secrecy capacity of each legitimate receiver is upper bounded by

$$\mathcal{UB}_k = \max_{P(\hat{\gamma}_k)} \mathop{\mathbb{E}}_{\gamma_k,\hat{\gamma}_k,\tilde{\gamma}_k} \left[\left\{ \log\left(\frac{1+\gamma_k P(\hat{\gamma}_k)}{1+\tilde{\gamma}_k P(\hat{\gamma}_k)} \right) \right\}^+ \right], \tag{3.16}$$

with $k \in \{1, \cdots, K\}$. Thus, $\sum_{k=1}^{K} \mathcal{UB}_k$ is a straightforward upper bound on the secrecy sum-capacity for the independent messages case. Since all the channel gains are identically distributed, we can directly deduce that $\widetilde{\mathcal{C}}_2^+$ upper bounds the secrecy sum-capacity of the system.

Now, we need to prove that $\widetilde{\mathcal{C}}_1^+$ is also an upper bound on the secrecy sum-capacity. For that, we consider a new channel whose capacity upper bounds the capacity of the K-receivers channel with imperfect CSI at the transmitter. In order to design this new genie aided channel, we need to take two facts into consideration:

- On one hand, the receiver in the new channel needs to instantaneously get the signal transmitted over the strongest channel.

- On the other hand, the transmitter has to know the estimated gains of all K channels of the original K-receivers channel.

In point of fact, if we only consider that the transmission is intended for the strongest receiver at each time, the capacity of this channel cannot be proven to upper bound the capacity of our K-receivers channel as the transmitter will have the estimated gain of only the strong channel. That is, the new channel needs to

observe all the K channels and to account for the strongest one at each time. This is what explain the idea behind considering a genie aided channel with a selection combining receiver equipped with a number of antennas equivalent to the number of legitimate receivers in the K-receivers channel. The selection combiner chooses the signal with the highest instantaneous gain and uses it for decoding. Picking the signal is equivalent to choosing the corresponding antenna among all receive antennas. The output signal of the genie aided receiver after selecting the strongest signal is $Y(i) = h_{\max}(i)X(i) + v(i)$, at time instant i, with $h_{\max}$ being the channel gain of the best legitimate channel, i.e., $|h_{\max}|^2{=}\gamma_{\max}$ and $\gamma_{\max}{=}\max_{1\leq k\leq K}\gamma_k$. The new channel can then be modeled as

$$\begin{cases} Y(i) = h_{\max}(i)X(i) + v(i) \\ Z(i) = \ g(i)X(i) \ + \ w(i). \end{cases} \tag{3.17}$$

We assume that the genie-aided receiver is aware of all the channel gains $h_1, h_2, \cdots, h_K$ as well as of the transmitter's estimated gains $\hat{h}_1, \hat{h}_2, \cdots, \hat{h}_k$. The proof is conducted in two steps. First, we prove that the secrecy capacity of this new channel upper bounds the secrecy sum-capacity of the K-receivers channel with imperfect CSI (Step 1). Then, we prove that $\widetilde{\mathcal{C}}_1^+$ in (3.15) upper bounds the secrecy capacity of the genie-aided channel (Step 2).

Step 1: To prove this first step, it is sufficient to show that if a secrecy rate point $(\mathcal{R}_1, \mathcal{R}_2, \cdots, \mathcal{R}_K)$ is achievable on the K-receivers channel with imperfect CSI then a secrecy sum-rate $\sum_{k=1}^{K}\mathcal{R}_k$ is achievable on the new channel.

Let $(W_1,W_2,\cdots,W_K)$ be the independent messages corresponding to the rates $(\mathcal{R}_1,\mathcal{R}_2,\cdots,\mathcal{R}_K)$, and $(\hat{W}_1, \hat{W}_2, \cdots, \hat{W}_K)$ the decoded messages. Thus, for any $\epsilon{>}0$ and n large enough, there exists a code of length n such that $\Pr[\hat{W}_k{\neq}W_k]{\leq}\epsilon$ at each

of the K receivers, and

$$H(W_k|W_1,\cdots,W_{k-1},W_{k+1},\cdots,W_K,Z^n,g^n,H^n,\hat{H}^n)/n \geq \mathcal{R}_k-\epsilon, \tag{3.18}$$

with $H^n=\{h_1(1),\cdots,h_1(n),h_2(1),\cdots,h_2(n),\cdots,h_K(1),\cdots,h_K(n)\}$ and $\hat{H}^n$ defined similarly by taking $\hat{h}$ instead of h. Now, we consider the transmission of message $W=(W_1,W_2,\cdots,W_K)$ to the genie-aided receiver using the same encoding scheme as for the K-receivers case. Adopting a decoding scheme similar to the one used at each of the K receivers, the genie-aided receiver can decode message W with a negligible probability of error, i.e., $\Pr(\hat{W}\neq W)\leq\epsilon$. For the secrecy condition, we have

$$H(W|Z^n,g^n,H^n,\hat{H}^n)/n = H(W_1,W_2,\cdots,W_K|Z^n,,g^n,H^n,\hat{H}^n)/n \tag{3.19}$$

$$\geq \sum_{k=1}^{K} H(W_k|W_1,\cdots,W_{k-1},W_{k+1},\cdots,W_K,Z^n,g^n,H^n,\hat{H}^n)/n \tag{3.20}$$

$$\geq \sum_{k=1}^{K} \mathcal{R}_k-K\epsilon, \tag{3.21}$$

which completes the first step of the proof.

Step 2: We have to prove that $\widetilde{\mathcal{C}}_1^+$ upper bounds the secrecy capacity of the genie-aided channel. Let $\widetilde{\mathcal{R}}_{\rm e}$ be the equivocation rate in the new channel. An upper bound on this rate can be derived as follows

$$n\widetilde{\mathcal{R}}_{\rm e} = H(W|Z^n,g^n,H^n,\hat{H}^n) \tag{3.22}$$

$$= I(W;Y^n|Z^n,g^n,H^n,\hat{H}^n)+H(W|Y^n,Z^n,g^n,H^n,\hat{H}^n) \tag{3.23}$$

$$\leq I(W;Y^n|Z^n,g^n,H^n,\hat{H}^n)+n\epsilon \tag{3.24}$$

$$= \sum_{i=1}^{n} I(W;Y(i)|Z^n,g^n,H^n,\hat{H}^n,Y^{i-1})+n\epsilon \tag{3.25}$$

$$= \sum_{i=1}^{n} H(Y(i)|Z^n,g^n,H^n,\hat{H}^n,Y^{i-1})-H(Y(i)|W,Z^n,g^n,H^n,\hat{H}^n,Y^{i-1})+n\epsilon \tag{3.26}$$

$$\leq \sum_{i=1}^{n} H(Y(i)|Z(i), g(i), h_{\max}(i), \hat{H}^i) - H(Y(i)|W, X(i), Z^n, g^n, H^n, \hat{H}^n, Y^{i-1}) + n\epsilon \quad (3.27)$$

$$= \sum_{i=1}^{n} H(Y(i)|Z(i), g(i), h_{\max}(i), \hat{H}^i) - H(Y(i)|X(i), Z(i), g(i), h_{\max}(i), \hat{H}^i) + n\epsilon \quad (3.28)$$

$$= \sum_{i=1}^{n} I(X(i); Y(i)|Z(i), g(i), h_{\max}(i), \hat{H}^i) + n\epsilon \quad (3.29)$$

$$= \sum_{i=1}^{n} \left\{ I(X(i); Y(i)|h_{\max}(i), \hat{H}^i) - I(X(i), Z(i)|g(i), \hat{H}^i) \right\}^+ + n\epsilon \quad (3.30)$$

where inequality (3.24) follows from $H(W|Y^n, Z^n, g^n, H^n, \hat{H}^n) \leq H(W|Y^n, H^n, \hat{H}^n)$ and Fano's inequality: $H(W|Y^n, H^n, \hat{H}^n) \leq n\epsilon$, and (3.30) is obtained by selecting the appropriate value for the noise correlation to form the Markov chain $X(i) \to Y(i) \to Z(i)$ if $|h_{\max}(i)| > |g(i)|$ or $X(i) \to Z(i) \to Y(i)$ if $|h_{\max}(i)| \leq |g(i)|$, as explained in [31].

We know that the right-hand side of (3.30) is maximized by a Gaussian input, then taking $X(i) \sim \mathcal{CN}\left(0, \sqrt{\rho_i(\hat{\Gamma}^i)}\right)$ with $\frac{1}{n}\sum_{i=1}^{n} \mathbb{E}\left[\rho_i(\hat{\Gamma}^i)\right] \leq P_{\text{avg}}$, we can write

$$n\widetilde{\mathcal{R}}_{\text{e}} \leq \sum_{i=1}^{n} \mathop{\mathbb{E}}_{\substack{\gamma_e(i), \hat{\Gamma}^i, \\ \gamma_{\max}(i)}} \left[\left\{ \log\left(\frac{1 + \gamma_{\max}(i)\, \rho_i(\hat{\Gamma}^i)}{1 + \gamma_e(i)\, \rho_i(\hat{\Gamma}^i)} \right) \right\}^+ \right] + n\epsilon \quad (3.31)$$

$$= \sum_{i=1}^{n} \mathop{\mathbb{E}}_{\substack{\gamma_e(i), \hat{\Gamma}(i), \\ \gamma_{\max}(i)}} \left[\mathop{\mathbb{E}}_{\hat{\Gamma}^{i-1}} \left[\left\{ \log\left(\frac{1 + \gamma_{\max}(i)\, \rho_i(\hat{\Gamma}^i)}{1 + \gamma_e(i)\, \rho_i(\hat{\Gamma}^i)} \right) \right\}^+ \middle| \hat{\Gamma}(i) \right] \right] + n\epsilon \quad (3.32)$$

$$\leq \sum_{i=1}^{n} \mathop{\mathbb{E}}_{\substack{\gamma_e(i), \hat{\Gamma}(i), \\ \gamma_{\max}(i)}} \left[\left\{ \log\left(\frac{1 + \gamma_{\max}(i) \mathop{\mathbb{E}}_{\hat{\Gamma}^{i-1}} \left[\rho_i(\hat{\Gamma}^i) \middle| \hat{\Gamma}(i) \right]}{1 + \gamma_e(i) \mathop{\mathbb{E}}_{\hat{\Gamma}^{i-1}} \left[\rho_i(\hat{\Gamma}^i) \middle| \hat{\Gamma}(i) \right]} \right) \right\}^+ \right] + n\epsilon, \quad (3.33)$$

$$\leq n \mathop{\mathbb{E}}_{\substack{\gamma_e, \hat{\Gamma}, \\ \gamma_{\max}}} \left[\left\{ \log\left(\frac{1 + \gamma_{\max}\, P(\hat{\Gamma})}{1 + \gamma_e\, P(\hat{\Gamma})} \right) \right\}^+ \right] + n\epsilon, \quad (3.34)$$

where (3.33) and (3.34) are obtained using Jensen's inequality. The i.i.d. assumption is also used to get (3.34) with $P(\hat{\Gamma}) = \frac{1}{n}\sum_{i=1}^{n} \mathop{\mathbb{E}}_{\hat{\Gamma}^{i-1}} \left[\rho_i(\hat{\Gamma}^i) \middle| \hat{\Gamma}(i) \right]$.

Finally, since $\gamma_{\max} = \max_k |\sqrt{1-\alpha}\hat{h}_k + \sqrt{\alpha}\tilde{h}_k|^2$ with $\tilde{h}_k$ independent and identically distributed as g, and since the transmitter only knows $\hat{h}_k$, the channel estimation error

$\tilde{h}_k$ is independent of X and we can substitute g by $\tilde{h}_k$, i.e., $g{=}\tilde{h}_k$. The justification for this substitution follows along similar lines as in [109]. Therefore, $\widetilde{\mathcal{C}}_1^+$ in (3.15) is an upper bound on the secrecy sum-capacity. This completes the proof. □

3.3.2.3 Proof of the High-SNR Results in Corollary 3.1

- Asymptotic Lower Bound: From Theorem 3.1, the secrecy rate

$$\widetilde{\mathcal{R}}_{\mathrm{s}}(\tau){=}\mathop{\mathbb{E}}_{\substack{\gamma_e,\gamma_{\max}^{\mathrm{est}},\\ \hat{\gamma}_{\max}\geq\tau}}\left[\log\left(\frac{1+\gamma_{\max}^{\mathrm{est}}P(\tau)}{1+\gamma_e P(\tau)}\right)\right] \tag{3.35}$$

is achievable for any $\tau \geq 0$. At high SNR, i.e., when $P_{\mathrm{avg}}{\to}\infty$, we have

$$\lim_{P_{\mathrm{avg}}\to\infty}\widetilde{\mathcal{R}}_{\mathrm{s}}(\tau) = \lim_{P_{\mathrm{avg}}\to\infty}\mathop{\mathbb{E}}_{\substack{\gamma_e,\gamma_{\max}^{\mathrm{est}},\\ \hat{\gamma}_{\max}\geq\tau}}\left[\log\left(\frac{1+\gamma_{\max}^{\mathrm{est}}P(\tau)}{1+\gamma_e P(\tau)}\right)\right] \tag{3.36}$$

since f_{γ_e} is continuous and bounded, $\mathop{\mathbb{E}}_{\substack{\hat{\gamma}_{\max}\geq\tau,\\ \gamma_{\max}^{\mathrm{est}}}}[\gamma_e] \leq \mathop{\mathbb{E}}_{\substack{\hat{\gamma}_{\max},\\ \gamma_{\max}^{\mathrm{est}}}}[\gamma_e] < \infty$,

$$\left|\log\left(\frac{1{+}\gamma_{\max}^{\mathrm{est}}P(\tau)}{1{+}\gamma_e P(\tau)}\right)\right| \leq \left|\log\left(\frac{\gamma_{\max}^{\mathrm{est}}}{\gamma_e}\right)\right|,$$

and $\left|\log\left(\frac{\gamma_{\max}^{\mathrm{est}}}{\gamma_e}\right)\right| < \infty$ then, using the Dominant Convergence Theorem, we can interchange the order of the limit and the expectation. We can then write

$$\lim_{P_{\mathrm{avg}}\to\infty}\widetilde{\mathcal{R}}_{\mathrm{s}}(\tau) = \mathop{\mathbb{E}}_{\substack{\gamma_e,\gamma_{\max}^{\mathrm{est}},\\ \hat{\gamma}_{\max}\geq\tau}}\lim_{P_{\mathrm{avg}}\to\infty}\left[\log\left(\frac{1+\gamma_{\max}^{\mathrm{est}}P(\tau)}{1+\gamma_e P(\tau)}\right)\right] \tag{3.37}$$

$$= \mathop{\mathbb{E}}_{\substack{\gamma_e,\gamma_{\max}^{\mathrm{est}},\\ \hat{\gamma}_{\max}\geq\tau}}\left[\log\left(\frac{\gamma_{\max}^{\mathrm{est}}}{\gamma_e}\right)\right]. \tag{3.38}$$

To complete the proof, we choose τ that maximizes (3.38). □

- Asymptotic Upper Bound: On one hand, we have

$$\lim_{P_{\text{avg}}\to\infty} \widetilde{\mathcal{C}}^{+}_{\text{H-SNR}}$$

$$= \lim_{P_{\text{avg}}\to\infty} \min\left\{ \max_{P(\hat{\Gamma})} \mathop{\mathbb{E}}_{\substack{\hat{\Gamma},\tilde{\gamma}\\ \gamma_{\max}}} \left[\left\{ \log\left(\frac{1+\gamma_{\max} P(\hat{\Gamma})}{1+\tilde{\gamma} P(\hat{\Gamma})} \right) \right\}^{+} \right], K \max_{P(\hat{\gamma})} \mathop{\mathbb{E}}_{\gamma,\hat{\gamma},\tilde{\gamma}} \left[\left\{ \log\left(\frac{1+\gamma P(\hat{\gamma})}{1+\tilde{\gamma} P(\hat{\gamma})} \right) \right\}^{+} \right] \right\} \tag{3.39}$$

$$\geq \lim_{P_{\text{avg}}\to\infty} \min\left\{ \mathop{\mathbb{E}}_{\substack{\tilde{\gamma}\\ \gamma_{\max}}} \left[\left\{ \log\left(\frac{1+\gamma_{\max} P_{\text{avg}}}{1+\tilde{\gamma} P_{\text{avg}}} \right) \right\}^{+} \right], K \mathop{\mathbb{E}}_{\gamma,\tilde{\gamma}} \left[\left\{ \log\left(\frac{1+\gamma P_{\text{avg}}}{1+\tilde{\gamma} P_{\text{avg}}} \right) \right\}^{+} \right] \right\} \tag{3.40}$$

$$= \min\left\{ \mathop{\mathbb{E}}_{\substack{\tilde{\gamma}\\ \gamma_{\max}}} \left[\left\{ \lim_{P_{\text{avg}}\to\infty} \log\left(\frac{1+\gamma_{\max} P_{\text{avg}}}{1+\tilde{\gamma} P_{\text{avg}}} \right) \right\}^{+} \right], K \mathop{\mathbb{E}}_{\gamma,\tilde{\gamma}} \left[\left\{ \lim_{P_{\text{avg}}\to\infty} \log\left(\frac{1+\gamma P_{\text{avg}}}{1+\tilde{\gamma} P_{\text{avg}}} \right) \right\}^{+} \right] \right\} \tag{3.41}$$

$$= \min\left\{ \mathop{\mathbb{E}}_{\substack{\tilde{\gamma}\\ \gamma_{\max}}} \left[\left\{ \log\left(\frac{\gamma_{\max}}{\tilde{\gamma}} \right) \right\}^{+} \right], K \mathop{\mathbb{E}}_{\gamma,\tilde{\gamma}} \left[\left\{ \log\left(\frac{\gamma}{\tilde{\gamma}} \right) \right\}^{+} \right] \right\}, \tag{3.42}$$

where (3.41) is obtained using a similar reasoning as for the asymptotic lower bound case. On the other hand, for any $P(\hat{\Gamma}) \geq 0$ and $P(\hat{\gamma}) \geq 0$, we have

$$\widetilde{\mathcal{C}}^{+}_{\text{H-SNR}} \leq \min\left\{ \max_{P(\hat{\Gamma})} \mathop{\mathbb{E}}_{\substack{\hat{\Gamma},\tilde{\gamma}\\ \gamma_{\max}}} \left[\left\{ \log\left(\frac{\gamma_{\max}}{\tilde{\gamma}} \right) \right\}^{+} \right], K \max_{P(\hat{\gamma})} \mathop{\mathbb{E}}_{\gamma,\hat{\gamma},\tilde{\gamma}} \left[\left\{ \log\left(\frac{\gamma}{\tilde{\gamma}} \right) \right\}^{+} \right] \right\} \tag{3.43}$$

$$= \min\left\{ \mathop{\mathbb{E}}_{\substack{\tilde{\gamma}\\ \gamma_{\max}}} \left[\left\{ \log\left(\frac{\gamma_{\max}}{\tilde{\gamma}} \right) \right\}^{+} \right], K \mathop{\mathbb{E}}_{\gamma,\tilde{\gamma}} \left[\left\{ \log\left(\frac{\gamma}{\tilde{\gamma}} \right) \right\}^{+} \right] \right\}. \tag{3.44}$$

Taking the limit on both sides of (3.44) completes the proof. □

3.3.2.4 Proof of the Perfect CSI Results in Corollary 3.2

Note that for the case of perfect main CSI at the transmitter, i.e., α=0, we have $\widetilde{\mathcal{C}}^{+}_{s}$=$\widetilde{\mathcal{C}}^{+}_{1}$, with $\widetilde{\mathcal{C}}^{+}_{1}$ and $\widetilde{\mathcal{C}}^{+}_{2}$ as defined in (3.15). Also, when α=0, we have $\hat{\gamma}_k$=γ_k, for all $k \in \{1, \cdots, K\}$. Using this substitution in Theorem 3.1, we obtain the result in Corollary 3.2.

3.4 Broadcasting a Common Message

In this section, we examine the impact of CSIT uncertainty on the secrecy throughput of multi-user broadcast wiretap channels when common confidential information is broadcasted to all the legitimate receivers. Taking into account the adopted system model, we characterize the ergodic secrecy capacity in the general case, then, we investigate the special cases of high-SNR and perfect main CSIT.

3.4.1 Secrecy Capacity Characterization

Here, we present the main results obtained for the ergodic common message secrecy capacity with a noisy estimation of the CSIT. The proofs of the presented results are provided in the following subsection.

3.4.1.1 Lower and Upper Bounds

THEOREM 3.2. The ergodic common message secrecy capacity of the multi-user fading broadcast wiretap channel with noisy main CSIT is characterized as

$$\mathcal{C}_{\mathrm{s}}^{-} \leq \mathcal{C}_{\mathrm{s}} \leq \mathcal{C}_{\mathrm{s}}^{+}, \tag{3.45}$$

where $\mathcal{C}_{\mathrm{s}}^{-}$ and $\mathcal{C}_{\mathrm{s}}^{+}$ are given by

$$\mathcal{C}_{\mathrm{s}}^{-} = \max_{P(\tau)} \min_{1\leq k\leq K} \mathop{\mathbb{E}}_{\substack{\gamma_e,\gamma_k,\\ \hat{\gamma}_k\geq\tau}} \left[\log\left(\frac{1+\gamma_k P(\tau)}{1+\gamma_e P(\tau)}\right)\right], \tag{3.46}$$

$$\mathcal{C}_{\mathrm{s}}^{+} = \min_{1\leq k\leq K} \max_{P(\hat{h}_k)} \mathop{\mathbb{E}}_{\hat{h}_k,\tilde{h}_k} \left[\left\{\log\left(\frac{1+|\sqrt{1-\alpha}\hat{h}_k+\sqrt{\alpha}\tilde{h}_k|^2 P(\hat{h}_k)}{1+|\tilde{h}_k|^2 P(\hat{h}_k)}\right)\right\}^{+}\right], \tag{3.47}$$

with $P(\tau) = P_{\mathrm{avg}}/(1-F_{|\hat{h}_k|^2}(\tau))$ and $\mathbb{E}[P(\hat{h}_k)] \leq P_{\mathrm{avg}}$.

Proof. A detailed proof of Theorem 3.2 is provided in the following subsection. On one hand, we note that the achievability of the lower bound $\mathcal{C}_{\mathrm{s}}^{-}$ follows by using wiretap coding along with a probabilistic transmission model where the communication is constrained by the estimated channel gains. The adopted transmission scheme

guarantees that all the legitimate receivers can decode the secret message while no extra information is leaked to the eavesdropper. We opted here for an on-off power scheme. Obviously, the achievable secrecy rate can be directly improved by optimizing over all power policies satisfying the average power constraint. On the other hand, the upper bound $\mathcal{C}_{\mathrm{s}}^{+}$ follows by properly correlating the main and the eavesdropper's channel gains. Indeed, since the estimation error $\tilde{h}_k$ is identically distributed as g, and since the transmitter is only aware of $\hat{h}_k$, which means that $\tilde{h}_k$ is independent of the transmitted signal X, then substituting g by $\tilde{h}_k$ is a valid choice that provides a tight upper bound.

Although the lower and the upper bounds in Theorem 3.2 do not generally coincide, they provide the best available characterization of the ergodic common message secrecy capacity with noisy CSIT. Also, from the obtained results, we can see that a nonzero secrecy rate can still be achieved even with a poor main channel estimator at the transmitter. Furthermore, a simple constant rate on-off power scheme is enough to achieve a positive secrecy rate.

3.4.1.2 High-SNR Regime

Corollary 3.3. At high SNR, the ergodic common message secrecy capacity of the multi-user fading broadcast wiretap channel with noisy main CSIT is bounded as

$$\mathcal{C}_{\text{H-SNR}}^{-} \leq \mathcal{C}_{\mathrm{s}} \leq \mathcal{C}_{\text{H-SNR}}^{+}, \tag{3.48}$$

where $\mathcal{C}_{\text{H-SNR}}^{-}$ and $\mathcal{C}_{\text{H-SNR}}^{+}$ are given by

$$\mathcal{C}_{\text{H-SNR}}^{-} = \min_{1\leq k\leq K} \mathop{\mathbb{E}}_{\substack{\gamma_e,\gamma_k,\\ \hat{\gamma}_k\geq\tau}} \left[\log\left(\frac{\gamma_k}{\gamma_e}\right)\right], \tag{3.49}$$

$$\mathcal{C}_{\text{H-SNR}}^{+} = \min_{1\leq k\leq K} \mathop{\mathbb{E}}_{\hat{h}_k,\tilde{h}_k} \left[\left\{\log\left(\frac{|\sqrt{1-\alpha}\hat{h}_k+\sqrt{\alpha}\tilde{h}_k|^2}{|\tilde{h}_k|^2}\right)\right\}^{+}\right], \tag{3.50}$$

with the transmission threshold τ satisfying $\mathop{\mathbb{E}}_{\gamma_k|\hat{\gamma}_k}\big[\log(\gamma_k)\,\big|\hat{\gamma}_k{=}\tau\big] - \mathop{\mathbb{E}}_{\gamma_e}\big[\log(\gamma_e)\big] = 0$.

Proof. The asymptotic high-SNR expressions in Corollary 3.3 can be deduced

from Theorem 3.2 by conducting a similar approach as the one used for the independent messages case. Clearly, the obtained asymptotic results states that the ergodic common message secrecy capacity is bounded at high SNR confirming that the secrecy multiplexing gain is equal to zero, regardless of the main channel estimation quality.

Remark: While the high-SNR analysis provide somehow a negative result in the sense that the capacity is bounded no matter how P_{avg} increases, at low SNR, the ergodic secrecy capacity is asymptotically equal to the capacity of the main channel as if there is no secrecy constraint [123]. Hence, the low-SNR analysis reveals the potential capacity gain provided by partial CSIT for any non-null channel estimation quality, i.e., $\alpha \neq 1$.

3.4.1.3 Perfect Main CSI Case

COROLLARY 3.4. When the transmitter has perfect knowledge of the legitimate receivers' CSI, the common message secrecy capacity is bounded as

$$\mathcal{C}^{-}_{\text{P-CSI}} \leq \mathcal{C}_{\text{s}} \leq \mathcal{C}^{+}_{\text{P-CSI}}, \tag{3.51}$$

where $\mathcal{C}^{-}_{\text{P-CSI}}$ and $\mathcal{C}^{+}_{\text{P-CSI}}$ are given by

$$\mathcal{C}^{-}_{\text{P-CSI}} = \max_{P(\tau)} \min_{1\leq k\leq K} \mathop{\mathbb{E}}_{\gamma_e,\gamma_k\geq\tau} \left[\log\left(\frac{1+\gamma_k P(\tau)}{1+\gamma_e P(\tau)}\right)\right], \tag{3.52}$$

$$\mathcal{C}^{+}_{\text{P-CSI}} = \min_{1\leq k\leq K} \max_{P(\gamma_k)} \mathop{\mathbb{E}}_{\gamma_k,\gamma_e} \left[\left\{\log\left(\frac{1+\gamma_k P(\gamma_k)}{1+\gamma_e P(\gamma_k)}\right)\right\}^{+}\right], \tag{3.53}$$

with $P(\tau) = P_{\text{avg}}/\left(1-F_{\gamma_k}(\tau)\right)$ and $\mathbb{E}[P(\gamma_k)] \leq P_{\text{avg}}$.

Proof. When the transmitter has perfect knowledge of the legitimate receivers' CSI, i.e., α=0, we have $\hat{\gamma}_k$=γ_k. Using this substitution in Theorem 3.2, we obtain the result in Corollary 3.4. This case captures the result in [30] with the difference that in our lower bound, we have chosen an on-off power scheme. □

Remark: When no main CSI is available at the transmitter, the common message secrecy capacity is equal to zero, i.e., $\mathcal{C}_{\rm s}$=0. Indeed, when the transmitter has no main CSI, i.e., α=1, each legitimate channel is statistically equivalent to $\tilde{h}$, and no power adaptation can be performed, i.e., $P(\hat{\gamma}_k)$=$P_{\rm avg}$. The eavesdropper channel is, then, equivalent to the legitimate channels, implying

$$\mathop{\mathbb{E}}_{\gamma_k,\gamma_e}\left[\log\left(1+\gamma_k P_{\rm avg}\right)\right] = \mathop{\mathbb{E}}_{\gamma_k,\gamma_e}\left[\log\left(1+\gamma_e P_{\rm avg}\right)\right]. \tag{3.54}$$

Thus, the upper bound vanishes, yielding $\mathcal{C}_{\rm s}=0$.

3.4.2 Secrecy Capacity Analysis

In this subsection, we establish the obtained results for the ergodic common message secrecy capacity presented in Theorem 3.2.

3.4.2.1 Achievability Scheme in Theorem 3.2

A detailed proof of achievability is provided in Appendix A.1. Here, we outline the adopted transmission scheme. We consider a probabilistic model where the transmission is constrained by the quality of the legitimate channels. Considering the case K=2, we define the following parameters:

- τ is a prefixed transmission threshold,
- $\mathcal{R}_w$=$\mathbb{E}\left[\log(1+\gamma_e P(\hat{\gamma}_k))\right]$, with $P(\hat{\gamma}_k)$ is chosen to satisfy the average power constraint,
- $\mathcal{R}_k$=$\mathbb{E}\left[\log(1+\gamma_k P(\hat{\gamma}_k))\,|\hat{\gamma}_k \geq \tau\right] - \mathcal{R}_w$,
- p_k=$\Pr\left[\hat{\gamma}_k \geq \tau\right]$,
- n_0=$p_k p_j n$, and n_1=$p_k(1-p_j)n$, with $k,j\in\{1,2\}/k\neq j$.

We use two independent Gaussian codebooks C_0 and C_1 constructed similarly to the standard wiretap codes. Codebook C_0 is a $(n_0, 2^{n_0\mathcal{R}_k})$ code, with $2^{n_0(\mathcal{R}_k+\mathcal{R}_w)}$ codewords randomly partitioned into $2^{n_0\mathcal{R}_k}$ bins, and codebook C_1 is a $(n_1, 2^{n_1\mathcal{R}_k})$ code, with $2^{n_1(\mathcal{R}_k+\mathcal{R}_w)}$ codewords randomly partitioned into $2^{n_1\mathcal{R}_k}$ bins. The transmitted common message is given in the form $W{=}(W_0, W_1)$, where W_0 and W_1 are uniformly distributed over the indices $\left\{1, 2, \cdots, 2^{n_0\mathcal{R}_k}\right\}$ and $\left\{1, 2, \cdots, 2^{n_1\mathcal{R}_k}\right\}$, respectively.

Next, we define the following events: $S_1{=}\{\hat{\gamma}_1{\geq}\tau\ ,\ \hat{\gamma}_2{\geq}\tau\}$, $S_2{=}\{\hat{\gamma}_1{\geq}\tau\ ,\ \hat{\gamma}_2{<}\tau\}$, $S_3{=}\{\hat{\gamma}_1{<}\tau\ ,\ \hat{\gamma}_2{\geq}\tau\}$ and $S_4{=}\{\hat{\gamma}_1{<}\tau\ ,\ \hat{\gamma}_2{<}\tau\}$. That is, the transmitter selects randomly a codeword $U_0^{n_0}$ associated with message W_0 and broadcasts it when he experiences event S_1. For message W_1, the transmitter selects two codewords uniformly and independently of one another; one codeword $U_1^{n_1}$ to be sent in state S_2 and the other one $U_2^{n_1}$ to be sent in state S_3. The source remains idle when experiencing event S_4. The randomness and the independence in the choice of the two codewords for message W_1 ensures that the eavesdropper does not take advantage of this repetition.

Since message W_0 is transmitted over channel state S_1 with $\Pr[S_1]{=}\Pr[\hat{\gamma}_1{\geq}\tau, \hat{\gamma}_2{\geq}\tau]$, S_1 occurs n_0/n times and the size of codebook $\mathcal{C}_0$ is therefore n_0. Similarly, message W_1 is transmitted over channel state S_2 and S_3 with $\Pr[S_2]{=}\Pr[S_3]{=}\Pr[\hat{\gamma}_k{\geq}\tau\ ,\ \hat{\gamma}_j{<}\tau]$, $k, j \in \{1, 2\}, k \neq j$. Thus, state S_2 and S_3 each occurs n_1/n times and the size of codebook $\mathcal{C}_1$ is n_1. The transmission stops when we have transmitted exactly n_0 symbols of $U_0^{n_0}$ and n_1 symbols each of $U_1^{n_1}$ and $U_2^{n_1}$. Given that the estimated channel gains are known globally, the receivers know the current state of the system and accordingly know which codeword the transmitted symbol belongs to. Decoder 1 uses the observations corresponding to the codewords $U_0^{n_0}$ and $U_1^{n_1}$ to recover message (W_0, W_1) while decoder 2 uses the ones corresponding to the codewords $U_0^{n_0}$ and $U_2^{n_1}$ to recover the message (W_0, W_1). Details on the codebook generation, the coding and the decoding schemes, and the secrecy analysis of this probabilistic transmission model are similar to the perfect CSI case presented in [81]. The overall achievable

rate can then be written as

$$\mathcal{R} = \min_{k} \left\{ \frac{n_0}{n} R_k + \frac{n_1}{n} R_k \right\} = \min_{k} p_k R_k, \tag{3.55}$$

which reduces to

$$\mathcal{R} = \min_{k} \mathop{\mathbb{E}}_{\substack{\gamma_e, \gamma_k, \\ \hat{\gamma}_k \geq \tau}} \left[\log \left(\frac{1+\gamma_k P(\hat{\gamma}_k)}{1+\gamma_e P(\hat{\gamma}_k)} \right) \right]. \tag{3.56}$$

The extension to the case $K \geq 2$ follows along similar lines as [81].

To finish the proof, we consider a transmission power that is instantaneously adapted according to the following on-off power scheme

$$P(\hat{\gamma}_k) = \begin{cases} P(\tau) = \dfrac{P_{\text{avg}}}{1 - F_{\hat{\gamma}_k}(\tau)} & \hat{\gamma}_k \geq \tau \\ 0 & \text{otherwise,} \end{cases} \tag{3.57}$$

then, we maximize the achievable rate $\mathcal{R}$ over $P(\tau)$ yielding the lower bound on the secrecy capacity presented in Theorem 3.2. The threshold τ should then be chosen to satisfy

$$\mathop{\mathbb{E}}_{\gamma_k, \hat{\gamma}_k \geq \tau} \left[\frac{\gamma_k P'(\tau)}{1 + \gamma_k P(\tau)} \right] - \mathop{\mathbb{E}}_{\gamma_e} \left[\frac{\gamma_e P'(\tau)}{1 + \gamma_e P(\tau)} \right] (1 - F_{\hat{\gamma}_k}(\tau)) =$$

$$f_{\hat{\gamma}_k}(\tau) \left(\mathop{\mathbb{E}}_{\gamma_k | \hat{\gamma}_k} \left[\log \left(1+\gamma_k P(\tau)\right) \big| \hat{\gamma}_k = \tau \right] - \mathop{\mathbb{E}}_{\gamma_e} \left[\log \left(1+\gamma_e P(\tau)\right) \right] \right). \tag{3.58}$$

□

Remark: We opted for the use of the On-Off power scheme, for the achievable common message secrecy rate, because it is near optimal and less complex. Clearly, by optimizing over all power policies satisfying the average power constraint, the achievable secrecy rate can be ameliorated. Indeed, a better rate could be achieved by solving

$$\mathcal{C}_{\text{s}}^{-} = \max_{P(\hat{\gamma}_k)} \mathop{\mathbb{E}}_{\gamma_e, \gamma_k, \hat{\gamma}_k} \left[\log \left(\frac{1+\gamma_k P(\hat{\gamma}_k)}{1+\gamma_e P(\hat{\gamma}_k)} \right) \right], \qquad k \in \{1, \cdots, K\}. \tag{3.59}$$

In general, the objective function in (3.59) is not convex. Using the Lagrange approach, we can obtain the necessary optimality condition via the Karush-Kuhn-Tucker (KKT) condition. The corresponding Lagrangian, to the optimization problem in (3.59), with the average power constraint $\mathbb{E}[P(\hat{\gamma}_k)] \leq P_{\text{avg}}$, can be written as

$$\mathcal{L}(P(\hat{\gamma}_k), \mu_k) = \mathop{\mathbb{E}}_{\gamma_e, \gamma_k | \hat{\gamma}_k} \left[\log \left(\frac{1+\gamma_k P(\hat{\gamma}_k)}{1+\gamma_e P(\hat{\gamma}_k)} \right) \right] - \mu_k \left(\mathbb{E}[P(\hat{\gamma}_k)] - P_{\text{avg}} \right), \tag{3.60}$$

with μ_k being the Lagrange multiplier. Differentiating $\mathcal{L}(P(\hat{\gamma}_k), \mu_k)$ with respect to $P(\hat{\gamma}_k)$ results in the following necessary condition for optimality

$$\mathop{\mathbb{E}}_{\gamma_e, \gamma_k | \hat{\gamma}_k} \left[\frac{\gamma_k - \gamma_e}{(1+\gamma_k P(\hat{\gamma}_k))(1+\gamma_e P(\hat{\gamma}_k))} \Big| \hat{\gamma}_k \right] = \mu_k. \tag{3.61}$$

Now, let us define the function

$$f_{\hat{\gamma}_k}(P) = \mathop{\mathbb{E}}_{\gamma_e, \gamma_k | \hat{\gamma}_k} \left[\frac{\gamma_k - \gamma_e}{(1+\gamma_k P(\hat{\gamma}_k))(1+\gamma_e P(\hat{\gamma}_k))} \Big| \hat{\gamma}_k \right].$$

Then, following similar lines as [110, Lemma 5], it can be shown that if there exists $\hat{\gamma}_{k_0}$, such that $\mathbb{E}\left[\gamma_k - \gamma_e | \hat{\gamma}_{k_0}\right] > 0$, i.e., such that $(1-\alpha)(\hat{\gamma}_{k_0} - 1) > 0$, then using the entire available power is optimal, and the power allocation scheme is given by

$$P(\hat{\gamma}_k) = \begin{cases} f_{\hat{\gamma}_k}^{-1}(\mu_k) & \text{if} \quad 0 \leq \mu_k \leq (1-\alpha)(\hat{\gamma}_k - 1) \\ 0 & \text{otherwise,} \end{cases} \tag{3.62}$$

under the power constraint $P(\mu_k) = \mathop{\mathbb{E}}_{\hat{\gamma}_k} \left[P(\hat{\gamma}_k) \right]$, i.e. each value of μ_k corresponds to an average power constraint $P_{\text{avg}} = P(\mu_k)$.

This optimal procedure, although complex and time-consuming, does not provide a substantial gain. Indeed, the rate achieved by the proposed On-Off power scheme and the one resulting from the KKT condition are very close.

3.4.2.2 Proof of the Upper Bound in Theorem 3.2

To establish the upper bound on the common message secrecy capacity, we start by supposing that the transmitter sends codeword X to only one legitimate receiver R_k. Using a similar approach, as in [109], we have

$$\mathcal{C}_{\mathrm{s}} \leq \max_{P(\hat{h}_k)} \mathop{\mathbb{E}}_{\hat{h}_k,\tilde{h}_k} \left[\left\{ \log \left(\frac{1+|\sqrt{1-\alpha}\hat{h}_k+\sqrt{\alpha}\tilde{h}_k|^2 P(\hat{h}_k)}{1+|\tilde{h}_k|^2 P(\hat{h}_k)} \right) \right\}^+ \right]. \tag{3.63}$$

This upper bound follows by properly correlating the main and the eavesdropper's channel gains. Indeed, since the estimation error $\tilde{h}_k$ is identically distributed as g, and since the transmitter is only aware of $\hat{h}_k$, which means that $\tilde{h}_k$ is independent of the transmitted signal X, then substituting g by $\tilde{h}_k$ is a valid choice that provides a tight upper bound. The presented upper bound has the following interpretation. In order to increase the information leakage, the eavesdropper sticks to the component of the main channel that is unknown to the transmitter.

The choice of the receiver to transmit to is arbitrary. In order to tighten this upper bound, we can then choose receiver R_k that minimizes this quantity, yielding the result in Theorem 3.2.

By setting $\hat{h}_k=\hat{\rho}_k \mathrm{e}^{i\hat{\theta}_k}$, $\tilde{h}_k=\tilde{\rho}_k \mathrm{e}^{i\tilde{\theta}_k}$ and $u_k=\hat{\theta}_k-\tilde{\theta}_k$, the upper bound on the secrecy capacity can be expressed as

$$\mathcal{C}_{\mathrm{s}}^{+}=\min_{1\leq k\leq K} \max_{P(\hat{\rho}_k)} \mathop{\mathbb{E}}_{\hat{\rho}_k\tilde{\rho}_k u_k} \left[\left\{ \log \left(\frac{1+\left((1-\alpha)\hat{\rho}_k^2+\alpha\tilde{\rho}_k^2+2\sqrt{\alpha(1-\alpha)}\hat{\rho}_k\tilde{\rho}_k\cos(u_k)\right) P(\hat{\rho}_k)}{1+\tilde{\rho}_k^2 P(\hat{\rho}_k)} \right) \right\}^+ \right]. \tag{3.64}$$

Note that the objective function in (3.64) is convex. The necessary and sufficient optimality condition can then be obtained using the KKT condition. The corresponding Lagrangian, with the average power constraint $\mathbb{E}[P(\hat{\rho}_k)]\leq P_{\mathrm{avg}}$, can be written as follows

$$\mathcal{L}(P(\hat{\rho}_k),\mu_k) \tag{3.65}$$

$$=\mathbb{E}\left[\left\{\log\left(\frac{1+\left((1-\alpha)\hat{\rho}_k^2+\alpha\tilde{\rho}_k^2+2\sqrt{\alpha(1-\alpha)}\hat{\rho}_k\tilde{\rho}_k\cos(u_k)\right)P(\hat{\rho}_k)}{1+\tilde{\rho}_k^2P(\hat{\rho}_k)}\right)\right\}^+\right]-\mu_k\left(\mathbb{E}[P(\hat{\rho}_k)]-P_{\text{avg}}\right),$$

with μ_k being the Lagrange multiplier. The term inside the expectation is positive if

$$\log\left(\frac{1+\left((1-\alpha)\hat{\rho}_k^2+\alpha\tilde{\rho}_k^2+2\sqrt{\alpha(1-\alpha)}\hat{\rho}_k\tilde{\rho}_k\cos(u_k)\right)P(\hat{\rho}_k)}{1+\tilde{\rho}_k^2P(\hat{\rho}_k)}\right)>0, \tag{3.66}$$

which is equivalent to

$$(1-\alpha)\hat{\rho}_k^2+2\sqrt{\alpha(1-\alpha)}\hat{\rho}_k\tilde{\rho}_k\cos(u_k)+(\alpha-1)\tilde{\rho}_k^2>0. \tag{3.67}$$

Solving the quadratic equation in the LHS of (3.67), we should have $\tilde{\rho}_k\leq\frac{\hat{\rho}_k}{\rho_0(u_k)}$, with

$$\rho_0(u_k)=\frac{\sqrt{(1-\alpha)(\alpha\cos(u_k)^2-\alpha+1)}-\sqrt{\alpha(1-\alpha)}\cos(u_k)}{1-\alpha},$$

to satisfy condition (3.67). Then, taking the derivative of (3.65) with respect to $P(\hat{\rho}_k)$ and equating to zero, the optimal power profile is the solution to the following optimality condition

$$\mathop{\mathbb{E}}_{\tilde{\rho}_k\leq\frac{\hat{\rho}_k}{\rho_0(u_k)}}\left[\frac{\xi(\hat{\rho}_k,\tilde{\rho}_k,u_k)}{1+\xi(\hat{\rho}_k,\tilde{\rho}_k,u_k)\,P(\hat{\rho}_k)}-\frac{\tilde{\rho}_k^2}{1+\tilde{\rho}_k^2P(\hat{\rho}_k)}\right]-\mu_k=0. \tag{3.68}$$

with $\xi(\hat{\rho}_k,\tilde{\rho}_k,u_k)=(1-\alpha)\hat{\rho}_k^2+\alpha\tilde{\rho}_k^2+2\sqrt{\alpha(1-\alpha)}\hat{\rho}_k\tilde{\rho}_k\cos(u_k)$. □

3.5 Illustrative Case: Rayleigh Fading Channels

In this section, we examine the obtained expressions for the lower and the upper bounds on the ergodic secrecy capacity when the channel gains are i.i.d. Rayleigh distributed. We start with the independent messages case, followed by the common message transmission case.

3.5.1 Broadcasting Independent Messages

Here, we analyze the results in Theorem 3.1, Corollary 3.1, and Corollary 3.2 in the case of Rayleigh fading channels.

3.5.1.1 Achievable Sum-Rate

When broadcasting independent messages to K legitimate receivers over i.i.d. Rayleigh fading channels with imperfect main CSIT, the lower bound on the secrecy capacity, presented in Theorem 3.1, is given by

$$\widetilde{\mathcal{C}}_{\rm s}^{-}=\max_{\tau}\Bigg\{\exp\!\left(\frac{1}{P(\tau)}\right)\mathrm{Ei}\!\left(-\frac{1}{P(\tau)}\right)\left(1-\left(1-\mathrm{e}^{-\tau}\right)^{K}\right)+K\sum_{k=0}^{K-1}\binom{K-1}{k}\frac{(-1)^k}{1+\alpha k}$$
$$\times\int_0^{\infty}\log(1+\gamma P(\tau))\exp\!\left(-\frac{(1+k)\gamma}{1+\alpha k}\right)\mathrm{Q}\left(\sqrt{2\frac{1-\alpha}{\alpha(1+\alpha k)}}\gamma,\sqrt{\frac{2\tau}{\alpha}(1+\alpha k)}\right)\mathrm{d}\gamma\Bigg\},\quad(3.69)$$

where Ei(.) is the exponential integral function [143, Eq.(8.211.1)], both exp(.) and $\mathrm{e}^{(.)}$ represent the exponential function, Q(.,.) stands for the Q-function [144, Eq.(16)], $\binom{\cdot}{\cdot}$ is the binomial coefficient, and $P(\tau)=P_{\rm avg}/\left(1-\left(1-\mathrm{e}^{-\tau}\right)^{K}\right)$.

Note that the integral term in (3.69) can be further represented in the form

$$\int_0^{\infty}\log(1+\gamma P(\tau))\exp\!\left(-\frac{(1+k)\gamma}{1+\alpha k}\right)\mathrm{Q}\left(\sqrt{2\frac{1-\alpha}{\alpha(1+\alpha k)}}\gamma,\sqrt{\frac{2\tau}{\alpha}(1+\alpha k)}\right)\mathrm{d}\gamma$$
$$=\sum_{n=0}^{\infty}\sum_{m=0}^{\infty}\frac{(1-\alpha)^{n+m}(1+\alpha k)^{-n}\tau^m}{\alpha^{m-1}\Gamma(1+m)\Gamma(1+n+m)}\exp\!\left(-\frac{\tau(1+\alpha k)}{\alpha}\right)\mathrm{G}_{3,2}^{1,3}\left(\alpha P(\tau)\,\middle|\,\begin{matrix}1,1,-n-m\\1,0\end{matrix}\right).\quad(3.70)$$

where $\Gamma(.)$ represents the Gamma function [143, Eq.(8.310.1)], and $\mathrm{G}_{\cdot,\cdot}^{\cdot,\cdot}\left(.\,\middle|\,\begin{matrix}\cdot\\\cdot\end{matrix}\right)$ is the Meijer G-function [143, Eq.(9.301)]. Details of derivation are provided in Appendix A.2.

- High-SNR Regime:

At high SNR, the lower bound on the independent messages secrecy sum-capacity in Corollary 3.1 reduces, for i.i.d. Rayleigh fading channels, to

$$\widetilde{\mathcal{C}}^{-}_{\text{H-SNR}}=\max_{\tau}\left\{K\sum_{k=0}^{K-1}\binom{K-1}{k}\frac{(-1)^k}{1+\alpha k}\left(-\text{Ei}(-(1+k)\tau)+\text{Ei}\left(-\frac{\tau(1+\alpha k)}{\alpha}\right)-\text{e}^{-(1+k)\tau}\right.\right.$$
$$\left.\left.\times\left(\text{Ei}\left(-\frac{1-\alpha}{\alpha}\tau\right)-\log\left(\frac{1-\alpha}{1+\alpha k}(1+k)\tau\right)+\log\left(\frac{1+k}{1+\alpha k}\right)\right)+\mathbf{C}\left(1-\left(1-\text{e}^{-\tau}\right)^K\right)\right)\right\}, \tag{3.71}$$

where $\mathbf{C}$ is Euler's constant [143, Eq.(8.367)].

- Perfect CSI Case:

When the transmitter has perfect CSI, the lower bound on the independent messages secrecy sum-capacity in Corollary 3.2 is given for i.i.d. Rayleigh fading channels as

$$\widetilde{\mathcal{C}}^{-}_{\text{P-CSI}}=\max_{\tau}\left\{\exp\left(\frac{1}{P(\tau)}\right)\text{Ei}\left(-\frac{1}{P(\tau)}\right)\left(1-\left(1-\text{e}^{-\tau}\right)^K\right)+K\sum_{k=0}^{K-1}\binom{K-1}{k}\frac{(-1)^k}{1+k}\right.$$
$$\left.\times\left(\text{e}^{-(1+k)\tau}\log(1+\tau P(\tau))-\exp\left(\frac{1+k}{P(\tau)}\right)\text{Ei}\left(-(1+k)\left(\frac{1}{P(\tau)}+\tau\right)\right)\right)\right\}. \tag{3.72}$$

3.5.1.2 Upper Bound

The upper bound on the independent messages secrecy sum-capacity with noisy main CSIT, presented in Theorem 3.1, can be expressed as $\widetilde{\mathcal{C}}^{+}_{s}=\min\left\{\widetilde{\mathcal{C}}^{+}_{1},\widetilde{\mathcal{C}}^{+}_{2}\right\}$, with $\widetilde{\mathcal{C}}^{+}_{1}$ and $\widetilde{\mathcal{C}}^{+}_{2}$ defined in (3.15). When transmitting to K legitimate receivers over Rayleigh fading channels, we have $\widetilde{\mathcal{C}}^{+}_{2}=K\mathcal{C}^{+}_{s}$, where $\mathcal{C}^{+}_{s}$ is given in (3.91). As for $\widetilde{\mathcal{C}}^{+}_{1}$, we have

$$\widetilde{\mathcal{C}}^{+}_{1}=\max_{P(\hat{\Gamma})}\int_0^\infty\int_0^\infty\int_0^\gamma\log\left(\frac{1+\gamma P(\hat{\Gamma})}{1+\tilde{\gamma}P(\hat{\Gamma})}\right)f_{\hat{\Gamma}|\gamma_{\max},\tilde{\gamma}}(\hat{\Gamma}|\gamma,\tilde{\gamma})f_{\gamma_{\max}|\tilde{\gamma}}(\gamma|\tilde{\gamma})f_{\tilde{\gamma}}(\tilde{\gamma})\,\text{d}\tilde{\gamma}\text{d}\gamma\text{d}\hat{\Gamma}, \tag{3.73}$$

where $f_{\tilde{\gamma}}(\tilde{\gamma}) = \mathrm{e}^{-\tilde{\gamma}}$,

$$f_{\gamma_{\max}|\tilde{\gamma}}(\gamma|\tilde{\gamma}) = \frac{1}{1-\alpha}\exp\left(-\frac{\gamma+\alpha\tilde{\gamma}}{1-\alpha}\right)\mathrm{I}_0\left(2\sqrt{\frac{\alpha}{(1-\alpha)^2}\gamma\tilde{\gamma}}\right)\left(1-\mathrm{e}^{-\gamma}\right)^{K-1} + (K-1)\mathrm{e}^{-\gamma}\left(1-\mathrm{e}^{-\gamma}\right)^{K-2}\left(1-\mathrm{Q}\left(\sqrt{\frac{2\alpha}{1-\alpha}}\tilde{\gamma}, \sqrt{\frac{2}{1-\alpha}}\gamma\right)\right), \quad (3.74)$$

and

$$f_{\hat{\Gamma}|\gamma_{\max},\tilde{\gamma}}(\hat{\Gamma}|\gamma,\tilde{\gamma}) = \frac{1}{\alpha}\exp\left(-\frac{\gamma+(1-\alpha)\hat{\gamma}}{\alpha}\right)\mathrm{I}_0\left(2\sqrt{\frac{1-\alpha}{\alpha^2}\gamma\hat{\gamma}}\right)\frac{\mathrm{e}^{-\hat{\gamma}}}{\mathrm{e}^{-\gamma}(1-\mathrm{e}^{-\gamma})^{K-1}} \times\left(1-\mathrm{Q}\left(\sqrt{\frac{2(1-\alpha)}{\alpha}}\hat{\gamma}, \sqrt{\frac{2}{\alpha}}\gamma\right)\right)^{K-1}\mathrm{e}^{-\hat{\gamma}_2}\cdots\mathrm{e}^{-\hat{\gamma}_K}. \quad (3.75)$$

- High-SNR Regime:

At high SNR, we have $\widetilde{\mathcal{C}}_2^+ = K\mathcal{C}_{\text{H-SNR}}^+$, where $\mathcal{C}_{\text{H-SNR}}^+$ is given in (3.92), and

$$\widetilde{\mathcal{C}}_1^+ = \int_0^\infty\int_0^\gamma \log\left(\frac{\gamma}{\tilde{\gamma}}\right)\mathrm{e}^{-\tilde{\gamma}} f_{\gamma_{\max}|\tilde{\gamma}}(\gamma|\tilde{\gamma})\,\mathrm{d}\tilde{\gamma}\mathrm{d}\gamma \quad (3.76)$$

- Perfect CSI Case:

When the transmitter has perfect CSI, the upper bound on the independent messages secrecy sum-capacity in Corollary 3.2 is given for Rayleigh fading channels as

$$\widetilde{\mathcal{C}}_{\text{P-CSI}}^+ = \max_{P(\gamma)} K\sum_{k=0}^{K-1}\binom{K-1}{k}(-1)^k \times\int_0^\infty \mathrm{e}^{-(k+1)\gamma}\left(\log(1+\gamma P(\gamma)) + \exp\left(\frac{1}{P(\gamma)}\right)\left(\mathrm{Ei}\left(-\frac{1}{P(\gamma)}\right) - \mathrm{Ei}\left(-\frac{1}{P(\gamma)}-\gamma\right)\right)\right)\mathrm{d}\gamma. \quad (3.77)$$

3.5.1.3 Scaling Law

In this subsection, we present an asymptotic analysis of the secrecy sum-capacity when transmitting to a large number of legitimate receivers, in the high-SNR regime, and over Rayleigh fading channels.

COROLLARY 3.5. The secrecy sum-capacity when broadcasting independent messages to a large number of legitimate receivers, i.e., $K\to\infty$, with an infinite average power constraint, i.e., $P_{\text{avg}}\to\infty$, is bounded by

$$\log((1-\alpha)\log(K)) \leq \widetilde{\mathcal{C}}_s \leq \log\log K, \qquad \text{for all} \quad \alpha\neq 1. \tag{3.78}$$

Proof. In the high-SNR regime, the secrecy sum-capacity is bounded by

$$\widetilde{\mathcal{C}}^{-}_{\text{H-SNR}} \leq \widetilde{\mathcal{C}}_s \leq \widetilde{\mathcal{C}}^{+}_{\text{H-SNR}}, \tag{3.79}$$

where $\widetilde{\mathcal{C}}^{-}_{\text{H-SNR}}$ and $\widetilde{\mathcal{C}}^{+}_{\text{H-SNR}}$ are given in Corollary 3.1. On one hand, we have,

$$\widetilde{\mathcal{C}}^{-}_{\text{H-SNR}} = \max_{\tau} \mathop{\mathbb{E}}_{\substack{\gamma_e,\gamma^{\text{est}}_{\max},\\ \hat{\gamma}_{\max}\geq\tau}} \left[\log\left(\frac{\gamma^{\text{est}}_{\max}}{\gamma_e}\right)\right] \geq \mathop{\mathbb{E}}_{\substack{\gamma_e,\gamma^{\text{est}}_{\max},\\ \hat{\gamma}_{\max}}} \left[\log\left(\frac{\gamma^{\text{est}}_{\max}}{\gamma_e}\right)\right]. \tag{3.80}$$

Since the distribution of the maximum $f_{\hat{\gamma}_{\max}}(\hat{\gamma}_{\max})$ converges toward $\delta(\hat{\gamma}_{\max}-\log K)$ as $K\to\infty$, with $\delta(.)$ is the Dirac-Delta function, it is almost sure that $\hat{\gamma}_{\max}=\log K$ as $K\to\infty$. We have then

$$\lim_{K\to\infty} \widetilde{\mathcal{C}}^{-}_{\text{H-SNR}} \geq \lim_{K\to\infty} \left(\Pr\left(\hat{\gamma}_{\max}=\log K\right) \mathop{\mathbb{E}}_{\gamma^{\text{est}}_{\max}} \left[\log\left(\gamma^{\text{est}}_{\max}\right) \middle| \hat{\gamma}_{\max}=\log K\right] - \mathop{\mathbb{E}}_{\gamma_e}\left[\log\left(\gamma_e\right)\right] \right).$$

Now, since $\Pr\left(\hat{\gamma}_{\max}=\log K\right) = 1$ as $K\to\infty$, and the variable γ_e does not depend on K; the term $\mathop{\mathbb{E}}_{\gamma_e}\left[\log\left(\gamma_e\right)\right]$ is asymptotically dominated by $\log\log K$, i.e., $\mathop{\mathbb{E}}_{\gamma_e}\left[\log\left(\gamma_e\right)\right]=o(\log\log K)$, then

$$\lim_{K\to\infty} \widetilde{\mathcal{C}}^{-}_{\text{H-SNR}} \geq \lim_{K\to\infty} \mathop{\mathbb{E}}_{\gamma^{\text{est}}_{\max}} \left[\log\left(\gamma^{\text{est}}_{\max}\right) \middle| \hat{\gamma}_{\max}=\log K\right]. \tag{3.81}$$

Furthermore, since $\gamma^{\text{est}}_{\max}=|\sqrt{1-\alpha}\hat{h}_{\max}+\sqrt{\alpha}\tilde{h}|^2$ and

$$\sqrt{1-\alpha}|\hat{h}_{\max}|-\sqrt{\alpha}|\tilde{h}| \leq |\sqrt{1-\alpha}\hat{h}_{\max}+\sqrt{\alpha}\tilde{h}| \leq \sqrt{1-\alpha}|\hat{h}_{\max}|+\sqrt{\alpha}|\tilde{h}|, \tag{3.82}$$

with $|\hat{h}_{\max}|=\sqrt{\hat{\gamma}_{\max}}\to\sqrt{\log K}$, and $|\tilde{h}|=o(\log\log K)$ as $K\to\infty$, then, $\gamma_{\max}^{\text{est}}\to(1-\alpha)\log K$ as $K\to\infty$. Thus, we have

$$\lim_{K\to\infty}\mathop{\mathbb{E}}_{\gamma_{\max}^{\text{est}}}\left[\log\left(\gamma_{\max}^{\text{est}}\right)\Big|\hat{\gamma}_{\max}=\log K\right]-\log\left((1-\alpha)\log K\right)=0,$$

yielding

$$\lim_{K\to\infty}\widetilde{\mathcal{C}}^{-}_{\text{H-SNR}}-\log\left((1-\alpha)\log K\right)\geq 0. \tag{3.83}$$

An alternative, more analytical, proof of the lower bound is provided in Appendix A.4.

On the other hand, we have

$$\widetilde{\mathcal{C}}^{+}_{\text{H-SNR}}=\min\left\{\mathop{\mathbb{E}}_{\gamma_{\max},\tilde{\gamma}}\left[\left\{\log\left(\frac{\gamma_{\max}}{\tilde{\gamma}}\right)\right\}^{+}\right],K\mathop{\mathbb{E}}_{\gamma,\tilde{\gamma}}\left[\left\{\log\left(\frac{\gamma}{\tilde{\gamma}}\right)\right\}^{+}\right]\right\} \tag{3.84}$$

$$\leq\mathop{\mathbb{E}}_{\gamma_{\max},\tilde{\gamma}}\left[\left\{\log\left(\frac{\gamma_{\max}}{\tilde{\gamma}}\right)\right\}^{+}\right]. \tag{3.85}$$

Considering the fact that $f_{\gamma_{\max}}(\gamma_{\max})\to\delta(\gamma_{\max}-\log K)$ and $\tilde{\gamma}=o(\log\log K)$ as $K\to\infty$, we get

$$\lim_{K\to\infty}\widetilde{\mathcal{C}}^{+}_{\text{H-SNR}}-\log\log K\leq 0. \tag{3.86}$$

Substituting (3.83) and (3.86) in (3.79) concludes the proof. □

It can be seen that, in the limit of large number of legitimate receivers K, the gap between the lower and the upper bounds on the secrecy sum-capacity is $\log(1-\alpha)$ for all $\alpha\neq 1$. Besides, we can see that this difference vanishes as the estimation error variance of the CSI decreases, i.e., $\alpha\to 0$.

3.5.2 Broadcasting a Common Message

Here, we analyze the results in Theorem 3.2, Corollary 3.3, and Corollary 3.4 in the case of Rayleigh fading channels.

3.5.2.1 Achievable Rate

The achievable common message secrecy rate with noisy main CSIT, presented in Theorem 3.2, can be expressed for the i.i.d. Rayleigh case as

$$\mathcal{C}_{\mathrm{s}}^{-}=\max_{\tau}\left\{\exp\left(\frac{\mathrm{e}^{-\tau}}{P_{\mathrm{avg}}}\right)\mathrm{Ei}\left(-\frac{\mathrm{e}^{-\tau}}{P_{\mathrm{avg}}}\right)\mathrm{e}^{-\tau}+\int_{0}^{\infty}\log(1+\gamma P_{\mathrm{avg}}\mathrm{e}^{\tau})\,\mathrm{e}^{-\gamma}\mathrm{Q}\left(\sqrt{2\frac{1-\alpha}{\alpha}\gamma},\sqrt{\frac{2\tau}{\alpha}}\right)\mathrm{d}\gamma\right\}, \tag{3.87}$$

Note that the integral term in (3.87) can be further represented in the form

$$\begin{aligned}\int_{0}^{\infty}&\log(1+\gamma P_{\mathrm{avg}}\mathrm{e}^{\tau})\exp(-\gamma)\,\mathrm{Q}\left(\sqrt{2\frac{1-\alpha}{\alpha}\gamma},\sqrt{\frac{2\tau}{\alpha}}\right)\mathrm{d}\gamma\\&=\sum_{n=0}^{\infty}\sum_{m=0}^{\infty}\frac{(1-\alpha)^{n+m}\tau^{m}\exp(-\tau/\alpha))}{\alpha^{m-1}\Gamma(1+m)\Gamma(1+n+m)}\,\mathrm{G}_{3,2}^{1,3}\left(\alpha P_{\mathrm{avg}}\mathrm{e}^{\tau}\middle|\begin{matrix}1,1,-n-m\\1,0\end{matrix}\right),\end{aligned} \tag{3.88}$$

Details of derivation are provided in Appendix A.3.

- High-SNR Regime:

At high SNR, the lower bound on the common message secrecy capacity in Corollary 3.3 reduces for i.i.d. Rayleigh fading channels to

$$\mathcal{C}_{\text{H-SNR}}^{-}=\max_{\tau}\left\{-\mathrm{Ei}(-\tau)+\mathrm{Ei}\left(-\frac{\tau}{\alpha}\right)-\mathrm{e}^{-\tau}\left(\mathrm{Ei}\left(-\frac{1-\alpha}{\alpha}\tau\right)-\log((1-\alpha)\tau)-\mathbf{C}\right)\right\}. \tag{3.89}$$

- Perfect CSI Case:

When the transmitter has perfect CSI, the lower bound on the common message secrecy capacity in Corollary 3.4 is given for i.i.d. Rayleigh fading channels as

$$\begin{aligned}\mathcal{C}_{\text{P-CSI}}^{-}=\max_{\tau}\Bigg\{&-\exp\left(\frac{\mathrm{e}^{-\tau}}{P_{\mathrm{avg}}}\right)\mathrm{Ei}\left(-\frac{\mathrm{e}^{-\tau}}{P_{\mathrm{avg}}}-\tau\right)\\&+\mathrm{e}^{-\tau}\left(\log(1+P_{\mathrm{avg}}\tau\mathrm{e}^{\tau})+\exp\left(\frac{\mathrm{e}^{-\tau}}{P_{\mathrm{avg}}}\right)\mathrm{Ei}\left(-\frac{\mathrm{e}^{-\tau}}{P_{\mathrm{avg}}}\right)\right)\Bigg\}.\end{aligned} \tag{3.90}$$

3.5.2.2 Upper Bound

The upper bound on the common message secrecy capacity, presented in Theorem 3.2, can be expressed for the i.i.d. Rayleigh fading channels' case as

$$\mathcal{C}_{\mathrm{s}}^{+}=\max_{P(\hat{\rho})}\int_{-\pi}^{\pi}\int_{0}^{\infty}\int_{0}^{\frac{\hat{\rho}}{\rho_0(u)}}\log\left(\frac{1+\xi(\hat{\rho},\tilde{\rho},u)\,P(\hat{\rho})}{1+\tilde{\rho}^2P(\hat{\rho})}\right)f_{\hat{\rho}}(\hat{\rho})f_{\tilde{\rho}}(\tilde{\rho})f_u(u)\mathrm{d}\hat{\rho}\mathrm{d}\tilde{\rho}\mathrm{d}u, \quad (3.91)$$

where $\xi(\hat{\rho}_k,\tilde{\rho}_k,u_k)=(1-\alpha)\hat{\rho}_k^2+\alpha\tilde{\rho}_k^2+2\sqrt{\alpha(1-\alpha)}\hat{\rho}_k\tilde{\rho}_k\cos(u_k)$, $f_{\hat{\rho}}(\hat{\rho})=f_{\tilde{\rho}}(\hat{\rho})=2\hat{\rho}\,\mathrm{e}^{-\hat{\rho}^2}$,

$$\rho_0(u_k)=\frac{\sqrt{(1-\alpha)(\alpha\cos(u_k)^2-\alpha+1)}-\sqrt{\alpha(1-\alpha)}\cos(u_k)}{1-\alpha},$$

and

$$f_u(u)=\begin{cases}(2\pi+u)/(2\pi)^2 & -2\pi\le u<0\\ (2\pi-u)/(2\pi)^2 & 0\le u<2\pi\\ 0 & \text{elsewhere}\end{cases}.$$

- High-SNR Regime:

At high SNR, the upper bound on the common message secrecy capacity in Corollary 3.3 can be written for i.i.d. Rayleigh fading channels as

$$\mathcal{C}_{\text{H-SNR}}^{+}=\frac{1}{\pi}\int_{-\pi}^{\pi}\int_{\rho_0(u)}^{\infty}\log\Big((1-\alpha)\rho^2+\sqrt{\alpha(1-\alpha)}\cos(u)\rho+\alpha\Big)\,\frac{\rho}{(1+\rho^2)^2}\,\mathrm{d}\rho\mathrm{d}u. \quad (3.92)$$

- Perfect CSI Case:

When the transmitter has perfect CSI, the upper bound on the common message secrecy capacity in Corollary 3.4 is given for i.i.d. Rayleigh fading channels as

$$\mathcal{C}_{\text{P-CSI}}^{+}=\max_{P(\gamma)}\int_{0}^{\infty}\mathrm{e}^{-\gamma}\left(\log(1+\gamma P(\gamma))+\exp\left(\frac{1}{P(\gamma)}\right)\left(\mathrm{Ei}\left(-\frac{1}{P(\gamma)}\right)-\mathrm{Ei}\left(-\frac{1}{P(\gamma)}-\gamma\right)\right)\right)\mathrm{d}\gamma. \quad (3.93)$$

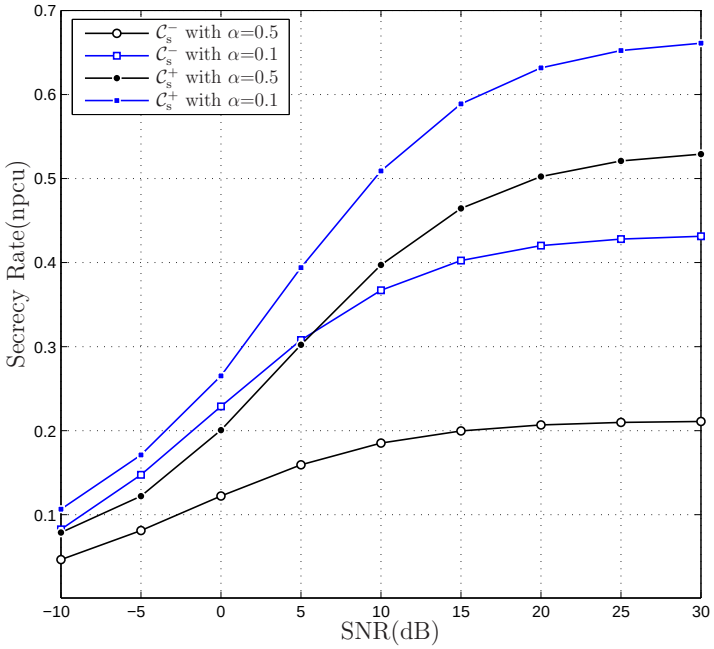


Figure 3.2: Lower and upper bounds on the common message secrecy capacity in the case of Rayleigh fading channels for two values of the estimation error variance α, i.e., α=0.5 and α=0.1.

3.6 Numerical Results

In this section, we provide selected numerical results for the case of i.i.d. Rayleigh fading channels. We consider that the system's variables, the main channel gains h_k, $k\in\{1,\cdots,K\}$, the estimated channel gains $\hat{h}_k$, the channel estimation errors $\tilde{h}_k$ and the eavesdropper's channel gain g, are all drawn from the zero-mean, unit-variance complex Gaussian distribution.

Figure 3.2 presents the lower and the upper bounds on the secrecy capacity, in nats per channel use (npcu), when transmitting a common message to two legitimate receivers with two values of the estimation error variance α=0.5 and α=0.1. The special cases of high-SNR and perfect main CSI are depicted in Figure 3.3. We can see that, at high SNR, the lower bound with perfect main CSI at the transmitter presented in this work coincides with the one provided in [30]. However, at low SNR, the curves of the two bounds differ. This difference, at the low SNR regime, is

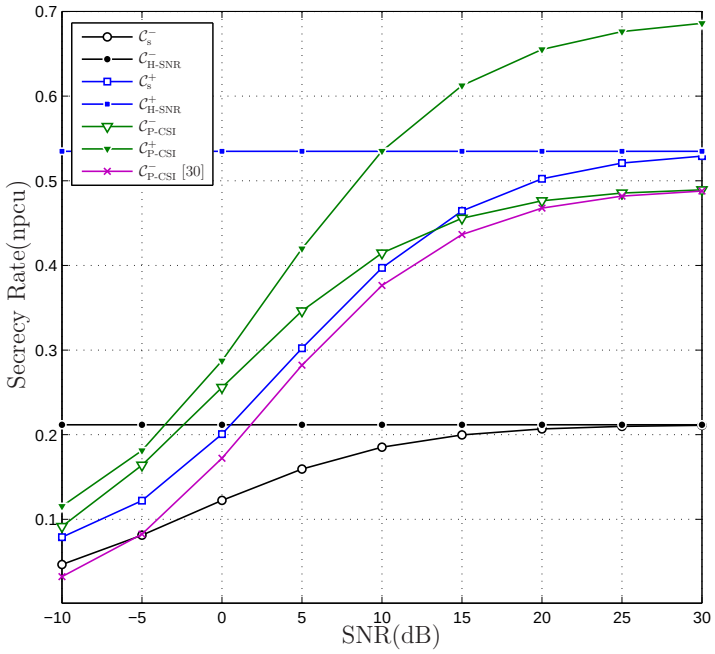


Figure 3.3: Comparison of the asymptotic results for high SNR and perfect CSI with the lower and upper bounds on the common message secrecy capacity with α=0.5.

explained by the use of different power transmission schemes.

The effect of changing the estimation error variance on the lower and the upper bounds on the secrecy capacity when broadcasting a common message to two legitimate receivers is illustrated in Figure 3.4. We consider three different values of the average power constraint P_{avg}=10 dB, P_{avg}=15 dB and P_{avg}=30 dB. It is clear from this figure that the secrecy capacity vanishes when no main CSI is available at the transmitter (α=1). Moreover, we can see that the gap between the achievable secrecy rate and the upper bound on the secrecy capacity gets narrower as the value of P_{avg} decreases.

Figure 3.5 illustrates the lower and the upper bounds on the secrecy capacity when transmitting independent messages to two legitimate receivers, i.e., K=2, with two different values of the error variance, α=0.5 and α=0.9. The results for the high-SNR regime and the perfect CSI case are presented in Figure 3.6 for α=0.5.

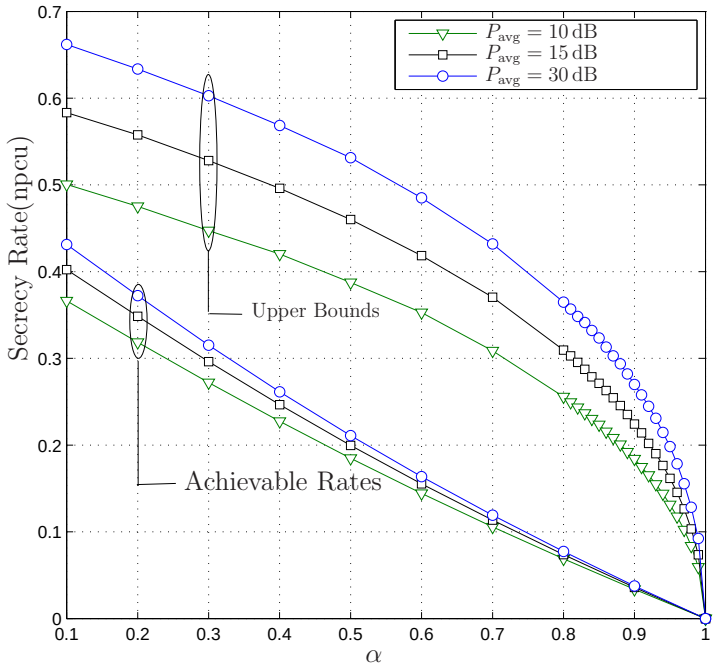


Figure 3.4: Lower and upper bounds on the common message secrecy capacity in function of α.

The variation of the threshold τ, of the On-Off power scheme, is presented in Figure 3.7 for both the common message and the independent messages cases. We can see that, for a given channel estimation error α, τ asymptotically converges towards a fixed value at high SNR. We can also observe that when fixing the value of the SNR, τ decreases with the channel estimation quality.

The motivation behind choosing the upper bound on the secrecy capacity as the minimum between $\widetilde{\mathcal{C}}_1^+$ and $\widetilde{\mathcal{C}}_2^+$, for the independent messages case, is highlighted in Figure 3.8. Indeed, a comparison between the upper bounds $\widetilde{\mathcal{C}}_{\text{s}}^+$ in Theorem 3.1 and $\widetilde{\mathcal{C}}_1^+$ in (3.15) is presented, in terms of α, for K=1, 2, and 3 with P_{avg}=30 dB. In accordance with what was stated in the proof of Theorem 3.1, we can see that $\widetilde{\mathcal{C}}_2^+$ is a loose upper bound for the secrecy sum-rate for most values of α, especially when the number of users K is large. That is, $\tilde{\mathcal{C}}_s^+$=$\tilde{\mathcal{C}}_1^+$ for most values of α. However, when the CSI available at the transmitter gets very noisy, i.e., $\alpha\to1$, $\widetilde{\mathcal{C}}_2^+$ becomes tighter then

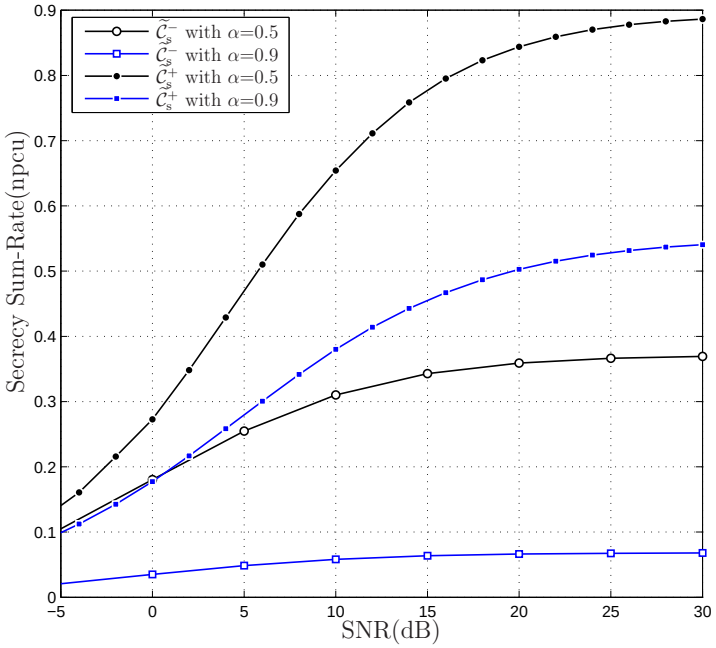


Figure 3.5: Lower and upper bounds on the independent messages secrecy sum-capacity in the case of Rayleigh fading channels with K=2 and two values of the estimation error variance α, i.e., α=0.5 and α=0.9.

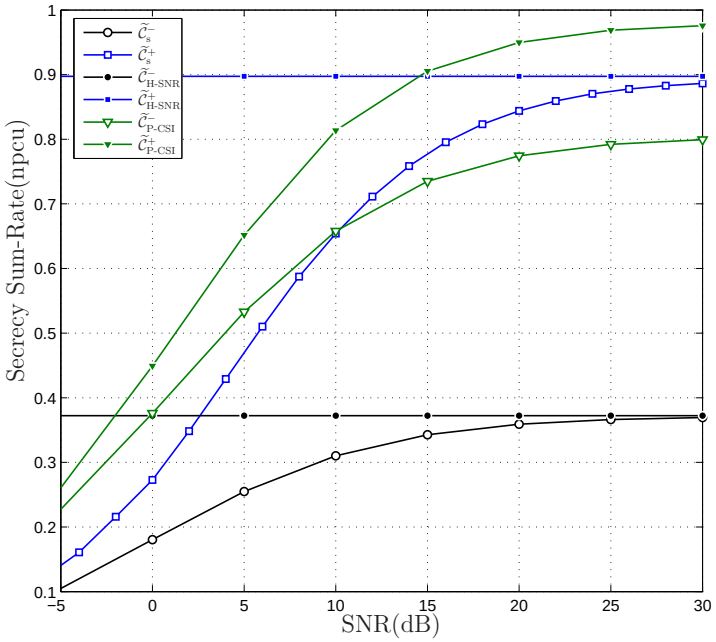
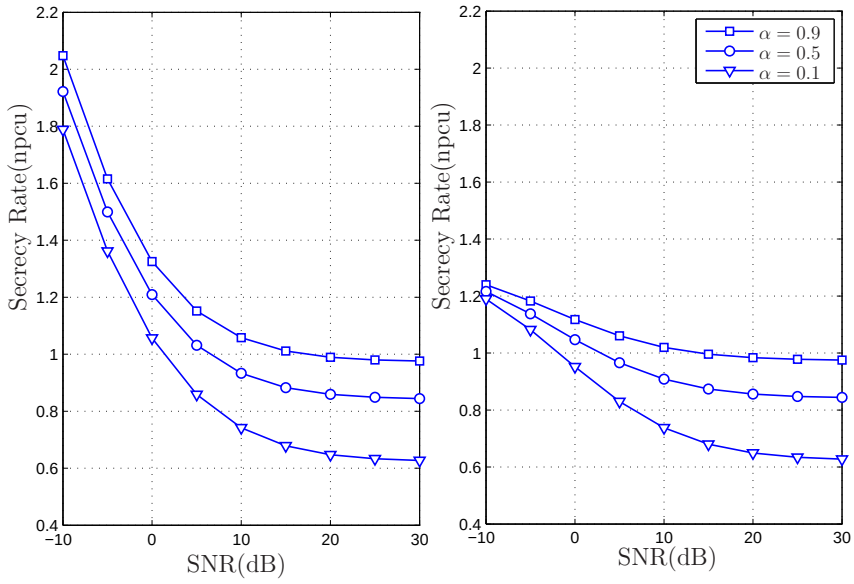


Figure 3.6: Comparison of the asymptotic results for high SNR and perfect CSI with the lower and upper bounds on the independent messages secrecy sum-capacity with K=2 and α=0.5.



(a) Common Message Case (b) Independent Messages Case

Figure 3.7: Optimal on-off power parameter τ versus SNR, for Rayleigh fading channels, with K=2 and various values of α. Subfigure (a) illustrates the common message case while subfigure (b) represents the independent messages case.

$\widetilde{\mathcal{C}}_1^+$. Moreover, for α=1, $\widetilde{\mathcal{C}}_2^+$ vanishes, reflecting the fact that the secrecy capacity is zero for the no CSI case, while $\widetilde{\mathcal{C}}_1^+$ does not.

The upper bound on the secrecy capacity, for the independent messages case, is presented in Figure 3.9 in function of the number of legitimate receiver K with P_{avg}=30 dB. We can observe that, when $K\to\infty$, the curves representing $\widetilde{\mathcal{C}}_{\text{s}}^+$ converge toward the perfect CSI curve (α=0) for all $\alpha > 1$. For the no CSI case (α=1), the secrecy capacity is zero.

Figure 3.10 considers the case when broadcasting independent messages to K legitimate receivers with an estimation error variance α=0.5 and two values for the average power constraint P_{avg}=10 dB and P_{avg}=30dB. From this figure, we can see that both the achievable secrecy sum-rate and the upper bound on the secrecy sum-rate, scale with the number of users K. That is, and in accordance with the multiuser diversity aim, the proposed achievable scheme is asymptotically optimal as the number of legitimate receivers grows. The figure shows also that

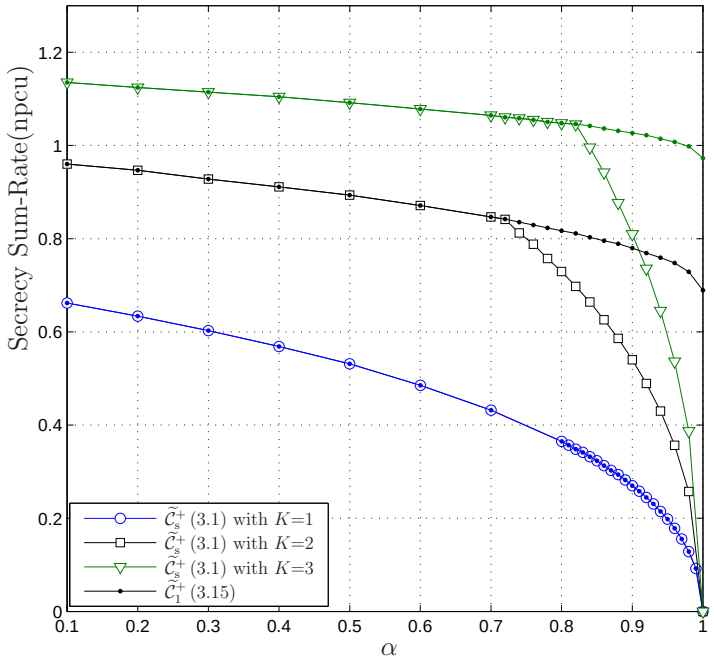


Figure 3.8: Comparison between the upper bounds $\widetilde{\mathcal{C}}_{\rm s}^{+}$ in (3.1) and $\widetilde{\mathcal{C}}_1^{+}$ in (3.15) for the independent messages case, in terms of α.

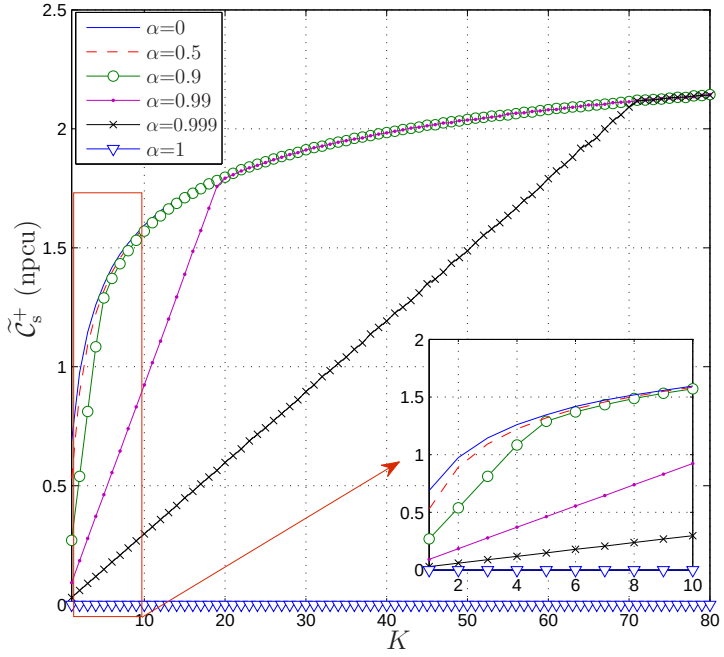


Figure 3.9: Upper bound on the secrecy capacity versus the number of legitimate receivers K for the independent messages case with different values of α.

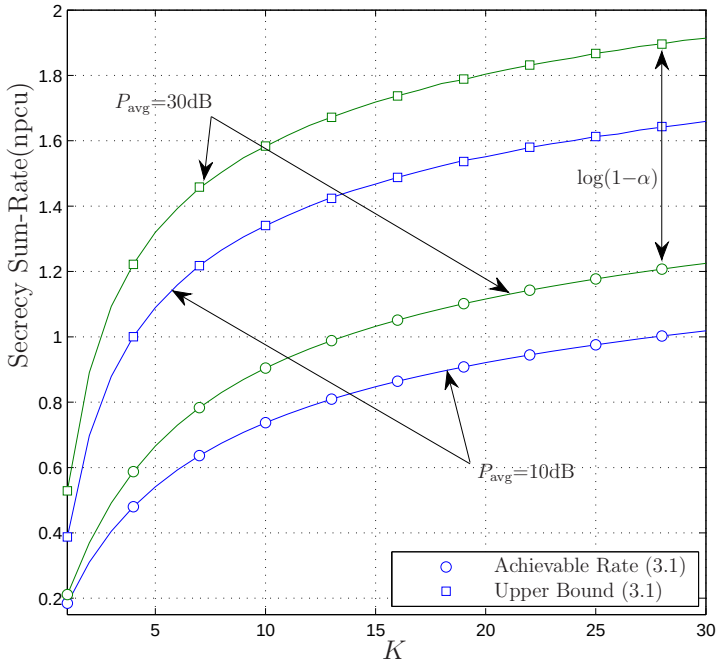


Figure 3.10: Upper and Lower bounds on the secrecy sum-rate versus the number of users K with α=0.5 and two values of P_{avg}.

the difference between the lower and the upper bounds on the secrecy sum-rate approaches $\log(1-\alpha)$ as the number of users increases. This supports our claim in Corollary 3.5. Note that all the results presented in this section have been verified through Monte Carlo simulations.

3.7 Conclusion

In this chapter, we examined the impact of CSIT uncertainty on the secrecy throughput of multi-user broadcast wiretap channels. We considered both cases when independent confidential messages and when a common secret message are broadcasted to multiple legitimate receivers in the presence of an eavesdropper. The obtained results show that even with a noisy CSIT, a non-zero secrecy rate can still be achieved. Asymptotic analysis at high SNR, perfect, and no-main CSIT were addressed and the results were illustrated for the case of Rayleigh fading channels.

Chapter 4

Multi-User Broadcast Wiretap Channel with Finite CSI Feedback

4.1 Introduction

This chapter investigates the problem of secure multi-user broadcasting over block-fading wiretap channels when the transmitter has limited knowledge about the main users' CSI. The CSI knowledge is obtained through finite rate feedback links used by the legitimate receivers to inform the transmitter about their channel prior to data transmission. The feedback links are public, which implies that the CSI information cannot be used as a source of secrecy. Assuming an average transmit power constraint, we establish upper and lower bounds on the ergodic secrecy capacity. We consider both the independent messages case, where the transmitter broadcasts multiple independent messages to the legitimate receivers, and the common message transmission case, where the source broadcasts the same information to all the receivers. In both scenarios, we show that as long as the transmitter has some knowledge about the main CSI, a positive secrecy rate can still be achieved. Also, the proposed lower and upper bounds, in both the common and the independent messages cases, are shown to coincide asymptotically as the capacity of the feedback links become large, i.e. $b \to \infty$, hence, fully characterizing the secrecy capacity in this first case and the secrecy sum-capacity in the second one.

The rest of this chapter is organized as follows. Section 4.2 describes the system model. The main results along with the corresponding proofs are introduced in sec-

tion 4.3 for the independent messages case and in section 4.4 for the common message transmission. Finally, selected simulation results are presented in section 4.5, while section 4.6 concludes the chapter.

4.2 System Model

We consider a block-fading broadcast wiretap channel where a transmitter communicates with K legitimate receivers in the presence of an eavesdropper, as depicted in Fig. 4.1. The respective received signals at each legitimate receiver R_k, $k\in\{1,\cdots,K\}$, and the eavesdropper, at fading block l, $l\in\{1,\cdots,L\}$, are given by

$$\begin{aligned} Y_k(l,j) &= h_k(l)X(l,j) + v_k(l,j) \\ Y_{\mathrm{e}}(l,j) &= h_{\mathrm{e}}(l)X(l,j) + w_{\mathrm{e}}(l,j), \end{aligned} \tag{4.1}$$

where $j\in\{1,\cdots,\kappa\}$, with κ representing the length of each fading block, $X(l,j)$ is the j-th transmitted codeword in the l-th fading block, $h_k(l)\in\mathbb{C}$, $h_{\mathrm{e}}(l)\in\mathbb{C}$ are the complex Gaussian channel gains corresponding to each legitimate channel and the eavesdropper's channel, respectively, and $v_k(l,j)\in\mathbb{C}$, $w_{\mathrm{e}}(l,j)\in\mathbb{C}$ represent zero-mean,

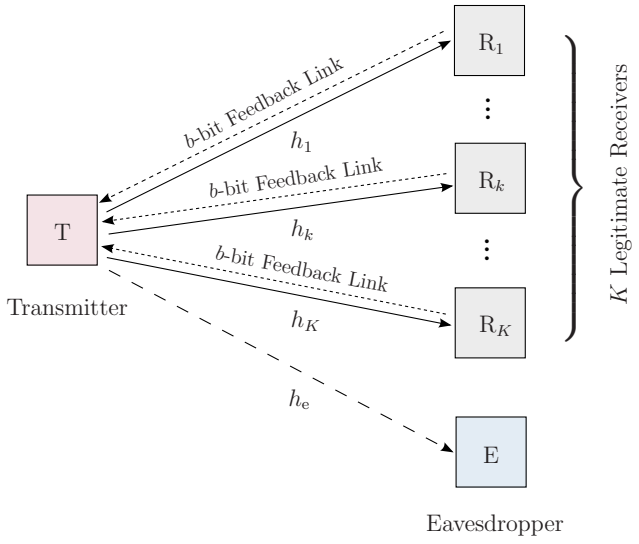


Figure 4.1: Multi-User broadcast wiretap channel with finite CSI feedback.

unit-variance circularly symmetric white Gaussian noises at R_k and E, respectively.

4.2.1 Channel Assumptions

We consider a block-fading channel where the channel gains remain constant within a fading block. We assume that the channel encoding and decoding frames span a large number of fading blocks, i.e., L is large, and that the blocks change independently from a fading block to another. An average transmit power constraint is imposed at the transmitter such that

$$\frac{1}{n}\sum_{t=1}^{n}\mathbb{E}\left[|X(t)|^2\right] \leq P_{\text{avg}}, \tag{4.2}$$

with $n{=}\kappa L$, and where the expectation is over the input distribution. The transmitted codeword can either correspond to a common message intended for all legitimate receivers or to a combination of independent messages each intended for a particular user. In both cases, the transmitted information should be kept secret from the eavesdropper.

The channel gains h_k and h_{e} are independent, ergodic and stationary with bounded PDFs. In the rest of this chapter, we denote $|h_k|^2$ and $|h_{\mathrm{e}}|^2$ by γ_k and γ_{e}, respectively. We assume that each legitimate receiver is instantaneously aware of its channel gain $h_k(l)$, and the eavesdropper knows $h_{\mathrm{e}}(l)$. The distributions of the main and the eavesdropping channels are known to all nodes. Further, we assume that the transmitter is not aware of the instantaneous channel realizations of neither channel. However, each legitimate receiver provides the transmitter with a b-bit CSI feedback through an error-free orthogonal channel with limited capacity. This feedback is transmitted at the beginning of each fading block and is also tracked by the other legitimate receivers, i.e., all communicating nodes are aware of each and every feedback information. The eavesdropper knows all channels and also track the feedback links so that they are not sources of secrecy.

4.2.2 Feedback Strategy

The adopted feedback strategy consists on partitioning the main channel gain support into Q intervals $[\tau_1, \tau_2), \cdots, [\tau_q, \tau_{q+1}), \cdots, [\tau_Q, \infty)$, where $Q{=}2^b$. That is, during each fading block, each legitimate receiver R_k determines in which interval, $[\tau_q, \tau_{q+1})$ with $q{=}1, \cdots, Q$, its channel gain γ_k lies and feeds back the associated index q to the transmitter. At the transmitter side, each feedback index q corresponds to a power transmission strategy P_q satisfying the average power constraint. We assume that all nodes are aware of the main channel gain partition intervals $[\tau_1, \tau_2), \cdots, [\tau_q, \tau_{q+1}), \cdots, [\tau_Q, \infty)$, and of the corresponding power transmission strategies $\{P_1, \cdots, P_Q\}$.

4.2.3 Secret Transmission

When transmitting K independent messages to the legitimate receivers, each intended for a particular user, a $(2^{n\mathcal{R}_1}, \cdots, 2^{n\mathcal{R}_K}, n)$ code consists of the following elements:

- K message sets $\mathcal{W}_k = \left\{1, 2, \cdots, 2^{n\mathcal{R}_k}\right\}$, $k \in \{1, \cdots, K\}$, with the messages $W_k \in \mathcal{W}_k$ independent and uniformly distributed;
- A stochastic encoder at the transmitter $f : \mathcal{W}_1 \times \cdots \times \mathcal{W}_K \to \mathcal{X}^n$ that maps each message tuple $(w_1, \cdots, w_K)$ to a codeword $x^n \in \mathcal{X}^n$;
- K decoders, one at each legitimate receiver, $g_k : \mathcal{Y}_k^n \to \mathcal{W}_1 \times \cdots \times \mathcal{W}_K$, $k \in \{1, \cdots, K\}$, that maps a received sequence $y_k^n \in \mathcal{Y}_k^n$ to $(\hat{w}_1, \cdots, \hat{w}_K) \in \mathcal{W}_1 \times \cdots \times \mathcal{W}_K$.

A rate tuple $(\mathcal{R}_1, \mathcal{R}_2, \cdots, \mathcal{R}_K)$ is said to be achievable if there exists a code such that the average error probability at each legitimate receiver,

$$P_{\mathrm{e}_k} = \frac{1}{2^{n\mathcal{R}_k}} \sum_{w=1}^{2^{n\mathcal{R}_k}} \Pr\left[W_k \neq \hat{W}_k \middle| W_k = w_k\right], \tag{4.3}$$

and the leakage rate at the eavesdropper

$$\frac{1}{n}I(W_1,\cdots,W_K;Y_e^n,h_e^L,h_1^L,\cdots,h_K^L,F_1^L,\cdots,F_K^L), \tag{4.4}$$

where F_k^L is the sequence of feedback information sent by the k-th receiver during L fading blocks, go to zero as n goes to infinity. The secrecy sum-rate is, then, given by $\widetilde{\mathcal{R}}_{\rm s}=\sum_{k=1}^{K}\mathcal{R}_k$, and the secrecy sum-capacity is defined, in this case, as $\widetilde{\mathcal{C}}_{\rm s}\triangleq\sup\widetilde{\mathcal{R}}_{\rm s}$.

4.3 Broadcasting Independent Messages

In this section, we consider the independent messages case when multiple confidential messages are broadcasted to the legitimate receivers in the presence of an eavesdropper. Taking into account the adopted system model, we present an upper and a lower bounds on the ergodic secrecy sum-capacity.

4.3.1 Main Results

THEOREM 4.1. The ergodic secrecy sum-capacity of the block-fading multi-user broadcast wiretap channel with an error free b-bit CSI feedback sent by each legitimate receiver, at the beginning of each fading block, is characterized as

$$\widetilde{\mathcal{C}}_{\rm s}^{-}\leq\widetilde{\mathcal{C}}_{\rm s}\leq\widetilde{\mathcal{C}}_{\rm s}^{+}, \tag{4.5}$$

where $\widetilde{\mathcal{C}}_{\rm s}^{-}$ and $\widetilde{\mathcal{C}}_{\rm s}^{+}$ are given by

$$\widetilde{\mathcal{C}}_{\rm s}^{-}=\max_{\{\tau_q;P_q\}_{q=1}^{Q}}\sum_{q=1}^{Q}\Pr\left[\tau_q\leq\gamma_{\max}<\tau_{q+1}\right]\mathop{\mathbb{E}}_{\gamma_{\rm e}}\left[\left\{\log\left(\frac{1+\tau_qP_q}{1+\gamma_{\rm e}P_q}\right)\right\}^{+}\right], \tag{4.6}$$

$$\widetilde{\mathcal{C}}_{\rm s}^{+}=\max_{\{\tau_q;P_q\}_{q=0}^{Q}}\sum_{q=0}^{Q}\Pr\left[\tau_q\leq\gamma_{\max}<\tau_{q+1}\right]\mathop{\mathbb{E}}_{\gamma_{\rm e},\gamma_{\max}}\left[\left\{\log\left(\frac{1+\gamma_{\max}P_q}{1+\gamma_{\rm e}P_q}\right)\right\}^{+}\middle|\,\tau_q\leq\gamma_{\max}<\tau_{q+1}\right], \tag{4.7}$$

with $\gamma_{\max}=\max_{1\leq k\leq K}\gamma_k$, $Q=2^b$, $\{\tau_q\,|\,0=\tau_0<\tau_1<\cdots<\tau_Q\}_{q=1}^{Q}$ are the reconstruction points describing the support of $\gamma_{\max}$ with $\tau_{Q+1}=\infty$ for convenience, and $\{P_q\}_{q=1}^{Q}$ are the power transmission strategies satisfying the average power constraint.

Proof. A detailed proof of Theorem 4.1 is provided in the following subsection.

The main difference between the bounds in Theorem 4.1 is that the feedback information is used to adapt both the transmission rate and the power for the achievable secrecy sum-rate and only the power in the upper bound. The secrecy sum-rate is achieved by transmitting only to the legitimate user with the best quantized CSI, in a given fading block. Under this strategy, the multi-user broadcast channel reduces to a point-to-point communication with the channel gain distributed as $\max_{1\leq k\leq K}\gamma_k$. One can think that encoding only for the strongest receiver is not valid to establish the secrecy sum-capacity. However, if we look for instance at the two users case, we can easily show that $I(X;Y_1|U)+I(U;Y_2)=I(X;Y_1)$, and hence that $\mathcal{R}_1+\mathcal{R}_2\leq I(X;Y_1)$, with the first receiver being always the strongest one and $U\rightarrow X\rightarrow Y_1\rightarrow Y_2$ forming a Markov chain. The proposed achievability scheme has then a time sharing interpretation to it and even if the result is given in terms of the secrecy sum-rate, the secrecy rate $\mathcal{R}_k$ of each legitimate receiver, $k\in\{1,\cdots,K\}$, can also be characterized. Indeed, we can write $\mathcal{R}_k\leq\mathcal{C}_{\rm s}^{-}\times\Pr[\text{user }k\text{ is the strongest receiver}]$.

Also, the result in Theorem 4.1 shows that even with a 1-bit CSI feedback, sent by each legitimate receiver at the beginning of each fading block, a non-zero secrecy sum-rate can still be achieved. Of course, as the number of feedback bits increases, the secrecy sum-throughput ameliorates, and when $Q\rightarrow\infty$, the bounds on the secrecy sum-capacity coincide, yielding the expression presented in the following corollary.

Corollary 4.1. The ergodic secrecy sum-capacity of a block fading multi-user broadcast wiretap channel, with perfect main CSIT, is given by

$$\widetilde{\mathcal{C}}_{\rm s}=\max_{P(\gamma_{\max})}\mathop{\mathbb{E}}_{\gamma_{\max},\gamma_{\rm e}}\left[\left\{\log\left(\frac{1+\gamma_{\max}P(\gamma_{\max})}{1+\gamma_{\rm e}P(\gamma_{\max})}\right)\right\}^{+}\right], \tag{4.8}$$

with $\gamma_{\max}=\max_{1\leq k\leq K}\gamma_k$, and $\mathbb{E}[P(\gamma_{\max})]\leq P_{\rm avg}$.

Proof. Corollary 4.1 results directly from Theorem 4.1 by letting $Q\rightarrow\infty$ and

following a similar reasoning as for the proof of Corollary 4.3. □

4.3.2 Secrecy Sum-Capacity Analysis

In this subsection, we establish the obtained results for the ergodic secrecy sum-capacity presented in Theorem 4.1.

4.3.2.1 Achievability Scheme in Theorem 4.1

The lower bound on the secrecy sum-capacity, presented in (4.6), is achieved using a time division multiplexing scheme that selects periodically one receiver to transmit to. More specifically, we consider that, during each fading block, the source only transmits to the legitimate receiver with the highest τ_q, and if there are more than one, we choose one of them randomly. Since we are transmitting to only one legitimate receiver at a time, the achieving coding scheme consists on using independent standard single user Gaussian wiretap codebooks.

During each fading block, the transmitter receives K feedback information about the CSI of the legitimate receivers. Since the channel gains of the K receivers are independent, there are $M{=}Q^K$ different states for the received feedback information, as discussed in the proof of achievability of Theorem 1. Each of these states, $\mathcal{J}_m; m \in \{1, \cdots, M\}$, represents one subchannel. The transmission scheme consists on sending an independent message, intended for the receiver with the highest τ_q, on each of the M subchannels, with a fixed rate. Let $\tau_m^{\max}$ be the maximum received feedback information on channel m. The overall achievable secrecy sum-rate can be written as

$$\widetilde{\mathcal{R}}_{\mathrm{s}}^{-} = \sum_{m=1}^{M} \Pr[\mathcal{J}_m] \mathop{\mathbb{E}}_{\gamma_{\mathrm{e}}} \left[\left\{ \log \left(\frac{1+\tau_m^{\max} P(\tau_m^{\max})}{1+\gamma_{\mathrm{e}} P(\tau_m^{\max})} \right) \right\}^{+} \right] \tag{4.9}$$

$$= \sum_{q=1}^{Q} \Pr[\tau_q \leq \gamma_{\max} < \tau_{q+1}] \mathop{\mathbb{E}}_{\gamma_{\mathrm{e}}} \left[\left\{ \log \left(\frac{1+\tau_q P_q}{1+\gamma_{\mathrm{e}} P_q} \right) \right\}^{+} \right], \tag{4.10}$$

where (4.9) is obtained by using a Gaussian codebook with power $P(\tau_m^{\max})$, satisfying

the average power constraint, on each subchannel m, and (4.10) follows by using the fact that $\tau_m^{\max} \in \{\tau_1, \cdots, \tau_Q\}$ and rewriting the summation over these indices. Also, we note that the probability of adapting the transmission with τ_q corresponds to the probability of having $\tau_q \leq \gamma_{\max} < \tau_{q+1}$, with $\gamma_{\max} = \max_{1\leq k\leq K} \gamma_k$. Maximizing over the main channel gain reconstruction points τ_q and the associated power transmission strategies P_q, for each $q \in \{1, \cdots, Q\}$, concludes the proof. □

4.3.2.2 Proof of the Upper Bound in Theorem 4.1

To prove that $\widetilde{\mathcal{C}}_{\rm s}^{+}$, presented in (4.7), is an upper bound on the secrecy sum-capacity, we consider a new genie-aided channel whose capacity upper bounds the capacity of the K-receivers channel with limited CSI feedback. The new channel has only one receiver that observes the output of the strongest main channel. The output signal of the genie-aided receiver is given by $Y_{\max}(t) = h_{\max}(t)X(t) + v(t)$, at time instant t, with $h_{\max}$ being the channel gain of the best legitimate channel, i.e., $|h_{\max}|^2 = \gamma_{\max}$ and $\gamma_{\max} = \max_{1\leq k\leq K} \gamma_k$. The new channel can then be modeled as

$$\begin{array}{l} Y_{\max}(t) = h_{\max}(t)X(t) + v(t) \\ Y_{\rm e}(t) \quad = h_{\rm e}(t)X(t) \; + \; w_{\rm e}(t) \end{array} \quad , \quad t = 1, \cdots, n. \tag{4.11}$$

Let $\tau_q, q \in \{1, \cdots, Q\}$, be the feedback information sent by the new receiver to the transmitter about its channel gain, i.e., τ_q is fed back when $\tau_q \leq \gamma_{\max} < \tau_{q+1}$. First, we need to prove that the secrecy capacity of this new channel upper bounds the secrecy sum-capacity of the K-receivers channel with limited CSI. To this end, it is sufficient to show that if a secrecy rate point $(\mathcal{R}_1, \mathcal{R}_2, \cdots, \mathcal{R}_K)$ is achievable on the K-receivers channel with limited CSI feedback, then, a secrecy sum-rate $\sum_{k=1}^{K} \mathcal{R}_k$ is achievable on the new channel.

Let $(W_1, W_2, \cdots, W_K)$ be the independent transmitted messages corresponding to the rates $(\mathcal{R}_1, \mathcal{R}_2, \cdots, \mathcal{R}_K)$, and $(\hat{W}_1, \hat{W}_2, \cdots, \hat{W}_K)$ the decoded messages. Thus, for any

$\epsilon>0$ and n large enough, there exists a code of length n such that $\Pr[\hat{W}_k \neq W_k] \leq \epsilon$ at each of the K receivers, and

$$\frac{1}{n} H(W_k|W_1,\cdots,W_{k-1},W_{k+1},\cdots,W_K,Y_{\rm e}^n,\gamma_{\rm e}^L,F^L) \geq \mathcal{R}_k - \epsilon, \tag{4.12}$$

with $F^L=\{F_1^L, F_2^L, \cdots, F_K^L\}$, and $F_k(l) \in \{\tau_1, \cdots, \tau_Q\}$ is the feedback information sent by receiver k in the l-th fading block. Now, we consider the transmission of message $W=(W_1,W_2,\cdots,W_K)$ to the genie-aided receiver using the same encoding scheme as for the K-receivers case. Adopting a decoding scheme similar to the one used at each of the K legitimate receivers, it is clear that the genie-aided receiver can decode message W with a negligible probability of error, i.e., $\Pr(\hat{W} \neq W) \leq \epsilon$. For the secrecy condition, we have

$$\begin{aligned}
\frac{1}{n} H(W|Y_{\rm e}^n, \gamma_{\rm e}^L, \gamma_{\max}^L, F_{\max}^L) &= \frac{1}{n} H(W_1,W_2,\cdots,W_K|Y_{\rm e}^n,\gamma_{\rm e}^L,\gamma_{\max}^L,F_{\max}^L) && (4.13)\\
&\geq \sum_{k=1}^{K} \frac{1}{n} H(W_k|W_1,\cdots,W_{k-1},W_{k+1},\cdots,W_K,Y_{\rm e}^n,\gamma_{\rm e}^L,\gamma_{\max}^L,F_{\max}^L) && (4.14)\\
&\geq \sum_{k=1}^{K} \frac{1}{n} H(W_k|W_1,\cdots,W_{k-1},W_{k+1},\cdots,W_K,Y_{\rm e}^n,\gamma_{\rm e}^L,\gamma_{\max}^L,F^L) && (4.15)\\
&\geq \sum_{k=1}^{K} \mathcal{R}_k - K\epsilon, && (4.16)
\end{aligned}$$

where $F_{\max}^L=\{F_{\max}(1),\cdots,F_{\max}(L)\}$ and $F_{\max}(l)$ is the feedback information sent by the genie-aided receiver in the l-th fading block, (4.15) follows from the fact that $F_{\max} \in \{F_1,\cdots,F_K\}$ and that conditioning reduces the entropy, and where (4.16) follows from the secrecy constraint (4.12).

Now, we need to prove that $\widetilde{\mathcal{C}}_{\rm s}^+$ upper bounds the secrecy capacity of the genie-aided channel. Let $\widetilde{\mathcal{R}}_{\rm e}$ be the equivocation rate of the new channel. We have

$$\begin{aligned}
n\widetilde{\mathcal{R}}_{\rm e} &= H(W|Y_{\rm e}^n, \gamma_{\rm e}^L, \gamma_{\max}^L, F_{\max}^L) && (4.17)\\
&= I(W;Y_{\max}^n|Y_{\rm e}^n,\gamma_{\rm e}^L,\gamma_{\max}^L,F_{\max}^L) + H(W|Y_{\max}^n,Y_{\rm e}^n,\gamma_{\rm e}^L,\gamma_{\max}^L,F_{\max}^L) && (4.18)\\
&\leq I(W; Y_{\max}^n|Y_{\rm e}^n, \gamma_{\rm e}^L, \gamma_{\max}^L, F_{\max}^L) + n\epsilon && (4.19)
\end{aligned}$$

$$= \sum_{l=1}^{L}\sum_{k=1}^{\kappa} I(W;Y_{\max}(l,k)|Y_{\mathrm{e}}^{n},\gamma_{\mathrm{e}}^{L},\gamma_{\max}^{L},F_{\max}^{L},Y_{\max}^{\kappa(l-1)+(k-1)})+n\epsilon \tag{4.20}$$

$$= \sum_{l=1}^{L}\sum_{k=1}^{\kappa} H(Y_{\max}(l,k)|Y_{\mathrm{e}}^{n},\gamma_{\mathrm{e}}^{L},\gamma_{\max}^{L},F_{\max}^{L},Y_{\max}^{\kappa(l-1)+(k-1)})$$

$$- H(Y_{\max}(l,k)|W,Y_{\mathrm{e}}^{n},\gamma_{\mathrm{e}}^{L},\gamma_{\max}^{L},F_{\max}^{L},Y_{\max}^{\kappa(l-1)+(k-1)})+n\epsilon \tag{4.21}$$

$$\leq \sum_{l=1}^{L}\sum_{k=1}^{\kappa} H(Y_{\max}(l,k)|Y_{\mathrm{e}}(l,k),\gamma_{\mathrm{e}}(l),\gamma_{\max}(l),F_{\max}^{l}) \tag{4.22}$$

$$- H(Y_{\max}(l,k)|W,X(l,k),Y_{\mathrm{e}}^{n},\gamma_{\mathrm{e}}^{L},\gamma_{\max}^{L},F_{\max}^{L},Y_{\max}^{\kappa(l-1)+(k-1)})+n\epsilon$$

$$= \sum_{l=1}^{L}\sum_{k=1}^{\kappa} H(Y_{\max}(l,k)|Y_{\mathrm{e}}(l,k),\gamma_{\mathrm{e}}(l),\gamma_{\max}(l),F_{\max}^{l}) \tag{4.23}$$

$$- H(Y_{\max}(l,k)|X(l,k),Y_{\mathrm{e}}(l,k),\gamma_{\mathrm{e}}(l),\gamma_{\max}(l),F_{\max}^{l})+n\epsilon$$

$$= \sum_{l=1}^{L}\sum_{k=1}^{\kappa} I(X(l,k);Y_{\max}(l,k)|Y_{\mathrm{e}}(l,k),\gamma_{\mathrm{e}}(l),\gamma_{\max}(l),F_{\max}^{l})+n\epsilon \tag{4.24}$$

$$\leq \sum_{l=1}^{L}\sum_{k=1}^{\kappa} \left\{I(X(l,k);Y_{\max}(l,k)|\gamma_{\max}(l),F_{\max}^{l})\right.$$

$$\left. -I(X(l,k);Y_{\mathrm{e}}(l,k)|\gamma_{\mathrm{e}}(l),F_{\max}^{l})\right\}^{+}+n\epsilon \tag{4.25}$$

$$= \sum_{l=1}^{L}\kappa\left\{I(X(l);Y_{\max}(l)|\gamma_{\max}(l),F_{\max}^{l})-I(X(l);Y_{\mathrm{e}}(l)|\gamma_{\mathrm{e}}(l),F_{\max}^{l})\right\}^{+}+n\epsilon, \tag{4.26}$$

where inequality (4.19) follows from the fact that

$$H(W|Y_{\max}^{n},Y_{\mathrm{e}}^{n},\gamma_{\mathrm{e}}^{L},\gamma_{\max}^{L},F_{\max}^{L}) \leq H(W|Y_{\max}^{n},\gamma_{\max}^{L},F_{\max}^{L}),$$

and Fano's inequality

$$H(W|Y_{\max}^{n},\gamma_{\max}^{L},F_{\max}^{L}) \leq n\epsilon,$$

and (4.25) holds true by selecting the appropriate value for the noise correlation to form the Markov chain $X(l)\rightarrow Y_{\max}(l)\rightarrow Y_{\mathrm{e}}(l)$ if $\gamma_{\max}(l)>\gamma_{\mathrm{e}}(l)$ or $X(l)\rightarrow Y_{\mathrm{e}}(l)\rightarrow Y_{\max}(l)$ if $\gamma_{\max}(l)\leq\gamma_{\mathrm{e}}(l)$, as explained in [31].

The right-hand side of (4.26) is maximized by a Gaussian input. That is, taking $X(l) \sim \mathcal{CN}\left(0,\omega_{l}^{1/2}(F_{\max}^{l})\right)$, with the power policy $\omega_{l}(F_{\max}^{l})$ satisfying the average

power constraint, we can write

$$n\widetilde{\mathcal{R}}_{\mathrm{e}} \leq \kappa \sum_{l=1}^{L} \mathbb{E}\left[\left\{\log\left(\frac{1+\gamma_{\max}(l)\omega_l(F_{\max}^l)}{1+\gamma_{\mathrm{e}}(l)\omega_l(F_{\max}^l)}\right)\right\}^+\right]+n\epsilon \tag{4.27}$$

$$= \kappa \sum_{l=1}^{L} \mathbb{E}\left[\mathbb{E}\left[\left\{\log\left(\frac{1+\gamma_{\max}(l)\omega_l(F_{\max}^l)}{1+\gamma_{\mathrm{e}}(l)\omega_l(F_{\max}^l)}\right)\right\}^+ \middle| F_{\max}(l), \gamma_{\max}(l), \gamma_{\mathrm{e}}(l)\right]\right]+n\epsilon \tag{4.28}$$

$$\leq \kappa \sum_{l=1}^{L} \mathbb{E}\left[\left\{\log\left(\frac{1+\gamma_{\max}(l)\mathbb{E}\left[\omega_l(F_{\max}^l)|F_{\max}(l),\gamma_{\max}(l),\gamma_{\mathrm{e}}(l)\right]}{1+\gamma_{\mathrm{e}}(l)\mathbb{E}\left[\omega_l(F_{\max}^l)|F_{\max}(l),\gamma_{\max}(l),\gamma_{\mathrm{e}}(l)\right]}\right)\right\}^+\right]+n\epsilon \tag{4.29}$$

$$= \kappa \sum_{l=1}^{L} \mathbb{E}\left[\left\{\log\left(\frac{1+\gamma_{\max}(l)\Omega_l(F_{\max}(l))}{1+\gamma_{\mathrm{e}}(l)\Omega_l(F_{\max}(l))}\right)\right\}^+\right]+n\epsilon \tag{4.30}$$

$$= \kappa \sum_{l=1}^{L} \mathbb{E}\left[\left\{\log\left(\frac{1+\gamma_{\max}\Omega_l(F_{\max})}{1+\gamma_{\mathrm{e}}\Omega_l(F_{\max})}\right)\right\}^+\right]+n\epsilon, \tag{4.31}$$

where (4.29) is obtained using Jensen's inequality, $\Omega_l(F_{\max}(l))$ in (4.30) is defined as

$$\Omega_l(F_{\max}(l))=\mathbb{E}\left[\omega_l(F_{\max}^l)|F_{\max}(l),\gamma_{\max}(l),\gamma_{\mathrm{e}}(l)\right],$$

and where (4.31) follows from the ergodicity and the stationarity of the channel gains. Thus, we have

$$\widetilde{\mathcal{R}}_{\mathrm{e}} \leq \frac{1}{L}\sum_{l=1}^{L} \mathbb{E}\left[\left\{\log\left(\frac{1+\gamma_{\max}\Omega_l(F_{\max})}{1+\gamma_{\mathrm{e}}\Omega_l(F_{\max})}\right)\right\}^+\right]+\epsilon \tag{4.32}$$

$$\leq \mathbb{E}\left[\left\{\log\left(\frac{1+\gamma_{\max}\Omega(F_{\max})}{1+\gamma_{\mathrm{e}}\Omega(F_{\max})}\right)\right\}^+\right]+\epsilon, \tag{4.33}$$

where (4.33) comes from applying Jensen's inequality once again, with

$$\Omega(F_{\max})=\frac{1}{L}\sum_{l=1}^{L}\Omega_l(F_{\max}).$$

Maximizing over the main channel gain reconstruction points τ_q and the associated power transmission strategies P_q, for each $q \in \{1, \cdots, Q\}$, concludes the proof. $\square$

4.3.3 Asymptotic Analysis at High-SNR

COROLLARY 4.2. In the high-SNR regime, the ergodic secrecy sum-capacity of the block-fading multi-user broadcast wiretap channel with an error free b-bit CSI feedback sent by each legitimate receiver, at the beginning of each fading block, is characterized as

$$\widetilde{\mathcal{C}}^{-}_{\text{H-SNR}} \leq \widetilde{\mathcal{C}}_{\text{s-HSNR}} \leq \widetilde{\mathcal{C}}^{+}_{\text{H-SNR}}, \tag{4.34}$$

where $\widetilde{\mathcal{C}}^{-}_{\text{H-SNR}}$ and $\widetilde{\mathcal{C}}^{+}_{\text{H-SNR}}$ are given by

$$\widetilde{\mathcal{C}}^{-}_{\text{H-SNR}} = \max_{\{\tau_q\}_{q=1}^{Q}} \sum_{q=1}^{Q} \Pr\left[\tau_q \leq \gamma_{\max} < \tau_{q+1}\right] \mathop{\mathbb{E}}_{\gamma_{\text{e}}} \left[\left\{ \log\left(\frac{\tau_q}{\gamma_{\text{e}}}\right) \right\}^{+} \right], \tag{4.35}$$

$$\widetilde{\mathcal{C}}^{+}_{\text{H-SNR}} = \mathop{\mathbb{E}}_{\gamma_{\text{e}},\gamma_{\max}} \left[\left\{ \log\left(\frac{\gamma_{\max}}{\gamma_{\text{e}}}\right) \right\}^{+} \right], \tag{4.36}$$

with $\gamma_{\max} = \max\limits_{1\leq k\leq K} \gamma_k$, $Q=2^b$, and $\{\tau_q \mid 0=\tau_0<\tau_1<\cdots<\tau_Q\}_{q=1}^{Q}$ are the reconstruction points describing the support of $\gamma_{\max}$ with $\tau_{Q+1}=\infty$ for convenience.

Proof: The result in Corollary 4.2 can be deduced directly from Theorem 4.1 by taking the limits of $\widetilde{\mathcal{C}}^{-}_{\text{s}}$ and $\widetilde{\mathcal{C}}^{+}_{\text{s}}$ when $P_{\text{avg}} \to \infty$.

We can see that the secrecy sum-capacity does not depend on P_{avg} at the high-SNR regime. However, since the obtained expressions are in terms of $\gamma_{\max}$, the secrecy performance scales with the number of legitimate receivers K.

4.4 Broadcasting a Common Message

In this section, we examine the case when a unique confidential information is broadcasted to all the legitimate receivers in the presence of an eavesdropper.

4.4.1 Main Results

THEOREM 4.2. The ergodic common message secrecy capacity of the block-fading multi-user broadcast wiretap channel with an error free b-bit CSI feedback sent by each legitimate receiver, at the beginning of each fading block, is characterized as

$$\mathcal{C}_{\mathrm{s}}^{-} \leq \mathcal{C}_{\mathrm{s}} \leq \mathcal{C}_{\mathrm{s}}^{+}, \tag{4.37}$$

where $\mathcal{C}_{\mathrm{s}}^{-}$ and $\mathcal{C}_{\mathrm{s}}^{+}$ are given by

$$\mathcal{C}_{\mathrm{s}}^{-} = \min_{1\leq k\leq K} \max_{\{\tau_q;P_q\}_{q=1}^{Q}} \sum_{q=1}^{Q} \Pr\left[\tau_q \leq \gamma_k < \tau_{q+1}\right] \mathop{\mathbb{E}}_{\gamma_{\mathrm{e}}} \left[\left\{ \log\left(\frac{1+\tau_q P_q}{1+\gamma_{\mathrm{e}} P_q} \right) \right\}^{+} \right], \tag{4.38}$$

$$\mathcal{C}_{\mathrm{s}}^{+} = \min_{1\leq k\leq K} \max_{\{\tau_q;P_q\}_{q=0}^{Q}} \sum_{q=0}^{Q} \Pr\left[\tau_q \leq \gamma_k < \tau_{q+1}\right] \mathop{\mathbb{E}}_{\gamma_{\mathrm{e}},\gamma_k} \left[\left\{ \log\left(\frac{1+\gamma_k P_q}{1+\gamma_{\mathrm{e}} P_q} \right) \right\}^{+} \middle| \tau_q \leq \gamma_k < \tau_{q+1} \right], \tag{4.39}$$

with $Q{=}2^b$, $\{\tau_q \,|\, 0{=}\tau_0{<}\tau_1{<}\cdots{<}\tau_Q\}_{q=1}^{Q}$ are the reconstruction points describing the support of γ_k with $\tau_{Q+1}{=}\infty$ for convenience, and $\{P_q\}_{q=1}^{Q}$ are the power transmission strategies satisfying the average power constraint.

Proof. A detailed proof of Theorem 4.2 is provided in the following subsection.

The main difference between the lower and the upper bounds in Theorem 4.2 is that the feedback information is used to adapt both the transmission rate and the power for the achievable secrecy rate while it is only used to adjust the transmission power for the upper bound. As a matter of fact, the key point in the proof of achievability of (4.38) is that the feedback information is exploited to fix the transmission rate during each coherence block. That is, if the legitimate receiver with the weakest average SNR informs the transmitter that its channel gain falls within the interval $[\tau_q, \tau_{q+1})$, $q \in \{1, \cdots, Q\}$, the transmitter conveys the codewords at rate $\mathcal{R}_q = \log\left(1{+}\tau_q P_q\right)$. Rate $\mathcal{R}_q$ changes only periodically and is held constant over the duration interval of a fading block. It may seem optimal to let the transmission rate vary with the actual value of the weakest channel gain instead of fixing it with regards

to the lower bound of the interval in which it lies. However, in this case, we will lose the $\{.\}^+$ inside the expectation, i.e., the eavesdropper can have a better rate than the legitimate receivers in some fading blocks. The considered setup guarantees that when $\gamma_{\rm e}{>}\tau_q$, the mutual information between the transmitter and the eavesdropper is upper bounded by $\mathcal{R}_q$. Otherwise, this mutual information is equal to $\log\left(1{+}\gamma_{\rm e}P_q\right)$.

It is also worth mentioning that, similarly to the case of multi-user common message transmission with no secrecy constraints, the obtained secrecy bounds are limited by the legitimate receiver with the lowest average SNR. It goes without saying that this limitation ensures that all legitimate receivers are able to recover the transmitted message reliably. We can also see from Theorem 4.2 that even with a 1-bit CSI feedback, sent by each legitimate receiver at the beginning of each fading block, a positive secrecy rate can still be achieved. Of course, as the number of feedback bits increases, the secrecy throughput ameliorates, and when $Q \to \infty$, our bounds coincide, yielding the result presented in the following corollary.

Corollary 4.3. The ergodic common message secrecy capacity of the block fading multi-user broadcast wiretap channel with perfect main CSIT is given by

$$\mathcal{C}_{\rm s} = \min_{1\leq k\leq K} \max_{P(\gamma_k)} \mathop{\mathbb{E}}_{\gamma_k,\gamma_{\rm e}} \left[\left\{ \log\left(\frac{1{+}\gamma_k P(\gamma_k)}{1{+}\gamma_{\rm e} P(\gamma_k)} \right) \right\}^+ \right], \tag{4.40}$$

with $\mathbb{E}[P(\gamma_k)] \leq P_{\rm avg}$.

Proof. Corollary 4.3 results directly from the expressions of the achievable rate in (4.38) and the upper bound in (4.39), by letting $\Pr\left[\tau_q{\leq}\gamma_k{<}\tau_{q+1}\right] = 1/Q$ and taking into consideration that as $Q{\to}\infty$, the set of reconstruction points, $\{\tau_1, \cdots, \tau_Q\}$, becomes infinite and each legitimate receiver R_k is basically forwarding γ_k to the transmitter. □

To the best of our knowledge, this result has not been reported in earlier works. For the special case of single user transmission, the secrecy capacity in Corollary 4.3

coincides with the result in Theorem 2 from reference [28].

The presented results for common message and independent messages transmissions, are also valid when multiple non-colluding eavesdroppers conduct the attack. In such a scenario, the transmitter has to limit its transmission with regards to the eavesdropper with the strongest wiretapping channel. Whereas, in the case of colluding eavesdroppers, the results can be extended by replacing the term γ_{e} with the squared norm of the vector of channel gains of the colluding eavesdroppers, i.e, this case could be seen as if the wiretapping attack is fulfilled by one eavesdropper equipped with multiple antennas and deploying maximum ratio combining (MRC). It is not hard to guess that the strongest the eavesdropper gets, the little is the secrecy we can achieve. Besides, in the analyzed system, we assumed unit variance Gaussian noises at all receiving nodes. The results can be easily extended to a general setup where the noise variances are different.

4.4.2 Secrecy Capacity Analysis

In this subsection, we establish the obtained results for the ergodic common message secrecy capacity presented in Theorem 4.2.

4.4.2.1 Achievability Scheme in Theorem 4.2

Since the transmission is controlled by the fed back information, we consider that, during each fading block, if the main channel gain of the receiver with the weakest channel gain falls within the interval $[\tau_q, \tau_{q+1})$, $q \in \{1, \cdots, Q\}$, the transmitter conveys the codewords at rate $\mathcal{R}_q = \log\left(1+\tau_q P_q\right)$. Rate $\mathcal{R}_q$ changes only periodically and is held constant over the duration interval of a fading block. This setup guarantees that when $\gamma_{\mathrm{e}}>\tau_q$, the mutual information between the transmitter and the eavesdropper is upper bounded by $\mathcal{R}_q$. Otherwise, this mutual information will be $\log\left(1+\gamma_{\mathrm{e}} P_q\right)$. Besides, we adopt a probabilistic transmission model where the communication is

constrained by the quality of the legitimate channels. Given the reconstruction points, $\tau_1<\tau_2<\cdots<\tau_Q<\tau_{Q+1}=\infty$, describing the support of each channel gain γ_k, and since the channel gains of all K receivers are independent, there are $M=Q^K$ different states for the received feedback information. Each of these states, $\mathcal{J}_m, m \in \{1,\cdots,M\}$, represents one subchannel. The transmission scheme consists on transmitting an independent codeword, on each of the M subchannels, with a fixed rate. We define the following rates, $\mathcal{R}_{\mathrm{e},m} = \underset{\gamma_\mathrm{e}}{\mathbb{E}}\left[\log\left(1+\gamma_\mathrm{e}P_m\right)\right]$, and

$$\mathcal{R}_\mathrm{s}^- = \sum_{m=1}^{M} \Pr\left[\mathcal{J}_m\right] \underset{\gamma_\mathrm{e}}{\mathbb{E}}\left[\left\{\log\left(\frac{1+\tau_m^{\min}P_m}{1+\gamma_\mathrm{e}P_m}\right)\right\}^+\right], \tag{4.41}$$

where $\tau_m^{\min}$ is the quantized channel gain corresponding to the weakest receiver in state $\mathcal{J}_m$ and P_m is the associated power policy satisfying the average power constraint.

Codebook Generation: We construct M independent codebooks $\mathcal{C}_1, \cdots, \mathcal{C}_M$, one for each subchannel, constructed similarly to the standard wiretap codes. Each codebook $\mathcal{C}_m$ is a $(n, 2^{n\mathcal{R}_\mathrm{s}^-})$ code with $2^{n(\mathcal{R}_\mathrm{s}^-+\mathcal{R}_{\mathrm{e},m})}$ codewords randomly partitioned into $2^{n\mathcal{R}_\mathrm{s}^-}$ bins.

Encoding and Decoding: Given a particular common message $w\in\{1,\cdots,2^{n\mathcal{R}_\mathrm{s}^-}\}$, to be transmitted, the encoder selects M codewords, one for each subchannel. More specifically, if the message to be sent is w, then for each subchannel m, the encoder randomly selects one of the codewords U_m^n from the wth bin in $\mathcal{C}_m$. During each fading block, of length κ, the transmitter experiences one of the events $\mathcal{J}_m$. Depending on the encountered channel state, the transmitter broadcasts $\kappa\mathcal{R}_q$ information bits of U_m^n using a Gaussian codebook. By the weak law of large numbers, when the total number of fading blocks L is large, the entire binary sequences are transmitted with high probability. To decode, each legitimate receiver considers the observations corresponding to all M subchannels. And since the transmission is adapted with regard to the receiver with the weakest average SNR, all legitimate receivers can recover the

transmitted codewords, with high probability, and hence recover message w. Details on the error probability evaluation are similar to the parallel channels case [30]. Since $\tau_{k,m} \in \{\tau_1, \cdots, \tau_Q\}$, by rewriting the summation over the states of each legitimate receiver, the expression of $\mathcal{R}_{\rm s}^-$ can then be reformulated as

$$\mathcal{R}_{\rm s}^- = \sum_{m=1}^{M} \Pr\left[\mathcal{J}_m\right] \mathop{\mathbb{E}}_{\gamma_{\rm e}} \left[\left\{ \log\left(\frac{1+\tau_m^{\min} P_m}{1+\gamma_{\rm e} P_m} \right) \right\}^+ \right] \tag{4.42}$$

$$= \min_{1\le k\le K} \sum_{m=1}^{M} \Pr\left[\mathcal{J}_m\right] \mathop{\mathbb{E}}_{\gamma_{\rm e}} \left[\left\{ \log\left(\frac{1+\tau_{k,m} P_m}{1+\gamma_{\rm e} P_m} \right) \right\}^+ \right] \tag{4.43}$$

$$= \min_{1\le k\le K} \sum_{m=1}^{M} \sum_{q=1}^{Q} \Pr\left[\mathcal{J}_m, \tau_{k,m}{=}\tau_q\right] \mathop{\mathbb{E}}_{\gamma_{\rm e}} \left[\left\{ \log\left(\frac{1+\tau_q P_q}{1+\gamma_{\rm e} P_q} \right) \right\}^+ \right] \tag{4.44}$$

$$= \min_{1\le k\le K} \sum_{q=1}^{Q} \Pr\left[\tau_q{\le}\gamma_k{<}\tau_{q+1}\right] \mathop{\mathbb{E}}_{\gamma_{\rm e}} \left[\left\{ \log\left(\frac{1+\tau_q P_q}{1+\gamma_{\rm e} P_q} \right) \right\}^+ \right], \tag{4.45}$$

where (4.43) results since the logarithm function is monotonic and the sum and the expectation are taking over positive terms, (4.44) is obtained by noting that $\tau_m^{\min} \in \{\tau_1, \cdots, \tau_Q\}$ and applying the total probability theorem, and (4.45) comes from the fact that

$$\sum_{m=1}^{M} \Pr\left[\mathcal{J}_m, \tau_{k,m}{=}\tau_q\right] = \Pr\left[\tau_q{\le}\gamma_k{<}\tau_{q+1}\right].$$

Since each user gets to know the feedback information of the other legitimate receivers, our proof is also valid when the reconstruction points $\{\tau_q\}_{q=1}^{Q}$, and the transmission strategies $\{P_q\}_{q=1}^{Q}$, associated with each legitimate receiver, are different. That is, we can choose these quantization parameters to satisfy (4.38).

Secrecy Analysis: We need to prove that the equivocation rate satisfies

$$\mathcal{R}_{\rm e} \ge \mathcal{R}_{\rm s}^- - \epsilon.$$

Let $\Gamma^L = \left\{\gamma_1^L, \gamma_2^L, \cdots, \gamma_K^L\right\}$ and $F^L = \left\{F_1^L, F_2^L, \cdots, F_K^L\right\}$, with $F_k(l) \in \{\tau_1, \cdots, \tau_Q\}$ being the feedback information sent by receiver k in the l-th fading block.

We have

$$n\mathcal{R}_{\rm e} = H(W|Y_{\rm e}^n, \gamma_{\rm e}^L, \Gamma^L, F^L) \tag{4.46}$$

$$\geq I(W; X^n|Y_{\rm e}^n, \gamma_{\rm e}^L, \Gamma^L, F^L) \tag{4.47}$$

$$= H(X^n|Y_{\rm e}^n,\gamma_{\rm e}^L,\Gamma^L,F^L) - H(X^n|Y_{\rm e}^n,\gamma_{\rm e}^L,\Gamma^L,F^L,W). \tag{4.48}$$

On one hand, we can write

$$\begin{aligned}
&H(X^n|Y_{\rm e}^n, \gamma_{\rm e}^L, \Gamma^L, F^L) \\
&\quad= \sum_{l=1}^{L} H(X^\kappa(l)|Y_{\rm e}^\kappa(l),\gamma_{\rm e}(l),\gamma_1(l),\cdots,\gamma_K(l),F_1(l),\cdots,F_K(l)) && (4.49)\\
&\quad\geq \sum_{l\in\mathcal{D}_L} H(X^\kappa(l)|Y_{\rm e}^\kappa(l),\gamma_{\rm e}(l),\gamma_1(l),\cdots,\gamma_K(l),F_1(l),\cdots,F_K(l)) && (4.50)\\
&\quad\geq \sum_{l\in\mathcal{D}_L} \kappa\left(\min_{1\leq k\leq K}\sum_{q=1}^{Q}\Pr\left[\tau_q\leq\gamma_k(l)<\tau_{q+1}\right]\left(\mathcal{R}_q-\log\left(1+\gamma_{\rm e}(l)P_q\right)\right)-\epsilon'\right) && (4.51)\\
&\quad= \sum_{l=1}^{L} \kappa\left(\min_{1\leq k\leq K}\sum_{q=1}^{Q}\Pr\left[\tau_q\leq\gamma_k(l)<\tau_{q+1}\right]\left\{\mathcal{R}_q-\log(1+\gamma_{\rm e}(l)P_q)\right\}^+-\epsilon'\right) && (4.52)\\
&\quad= n\min_{1\leq k\leq K}\sum_{q=1}^{Q}\Pr\left[\tau_q\leq\gamma_k<\tau_{q+1}\right]\mathop{\mathbb{E}}_{\gamma_{\rm e}}\left[\left\{\mathcal{R}_q-\log\left(1+\gamma_{\rm e}P_q\right)\right\}^+\right]-n\epsilon' && (4.53)\\
&\quad= n\mathcal{R}_{\rm s}^- - n\epsilon', && (4.54)
\end{aligned}$$

where (4.49) results from the memoryless property of the channel and the independence of the $X^\kappa(l)$'s, (4.50) is obtained by removing all the terms corresponding to the fading blocks $l \notin \mathcal{D}_L$, with $\mathcal{D}_L = \cup_{k\in\{1,\cdots,K\}}\{l \in \{1,\cdots,L\} : F_k(l) > h_{\rm e}(l)\}$, and (4.53) follows from the ergodicity of the channel as $L \to \infty$.

On the other hand, using list decoding argument at the eavesdropper side and applying Fano's inequality [28], $\frac{1}{n}H(X^n|Y_{\rm e}^n, \gamma_{\rm e}^L, \Gamma^L, F^L, W)$ vanishes as $n \to \infty$ and we can write

$$H(X^n|Y_{\rm e}^n, \gamma_{\rm e}^L, \Gamma^L, F^L, W) \leq n\epsilon''. \tag{4.55}$$

Substituting (4.54) and (4.55) in (4.48), we get $\mathcal{R}_{\rm e} \geq \mathcal{R}_{\rm s}^- - \epsilon$, with $\epsilon = \epsilon' + \epsilon''$, and ϵ' and ϵ'' are selected to be arbitrarily small. This concludes the proof. □

4.4.2.2 Proof of the Upper Bound in Theorem 4.2

To establish the upper bound on the common message secrecy capacity in (4.39), we start by supposing that the transmitter sends message w to only one legitimate receiver R_k. Using the result in [123], for single user transmission with limited CSI feedback, the secrecy capacity of our system can be upper bounded as

$$\mathcal{C}_{\mathrm{s}} \leq \max_{\{\tau_q;P_q\}_{q=1}^{Q}} \sum_{q=0}^{Q} \Pr\left[\tau_q{\leq}\gamma_k{<}\tau_{q+1}\right] \mathop{\mathbb{E}}_{\gamma_{\mathrm{e}},\gamma_k} \left[\left\{ \log\left(\frac{1{+}\gamma_k P_q}{1{+}\gamma_{\mathrm{e}} P_q}\right)\right\}^{+} \Big| \tau_q \leq \gamma_k < \tau_{q+1} \right]. \quad (4.56)$$

Since the choice of the receiver to transmit to is arbitrary, we tighten this upper bound by choosing the legitimate receiver R_k that minimizes this quantity, yielding

$$\mathcal{C}_{\mathrm{s}}^{+} = \min_{1\leq k\leq K} \max_{\{\tau_q;P_q\}_{q=1}^{Q}} \sum_{q=0}^{Q} \Pr\left[\tau_q{\leq}\gamma_k{<}\tau_{q+1}\right] \mathop{\mathbb{E}}_{\gamma_{\mathrm{e}},\gamma_k} \left[\left\{ \log\left(\frac{1{+}\gamma_k P_q}{1{+}\gamma_{\mathrm{e}} P_q}\right)\right\}^{+} \Big| \tau_q \leq \gamma_k < \tau_{q+1} \right].$$

This concludes the proof. □

4.4.3 Asymptotic Analysis at High-SNR

Corollary 4.4. In the high-SNR regime, the ergodic common message secrecy capacity of the block-fading multi-user broadcast wiretap channel with an error free b-bit CSI feedback sent by each legitimate receiver is characterized as

$$\mathcal{C}_{\text{H-SNR}}^{-} \leq \mathcal{C}_{\text{s-HSNR}} \leq \mathcal{C}_{\text{H-SNR}}^{+}, \quad (4.57)$$

where $\mathcal{C}_{\text{H-SNR}}^{-}$ and $\mathcal{C}_{\text{H-SNR}}^{+}$ are given by

$$\mathcal{C}_{\text{H-SNR}}^{-} = \min_{1\leq k\leq K} \max_{\{\tau_q\}_{q=1}^{Q}} \sum_{q=1}^{Q} \Pr\left[\tau_q{\leq}\gamma_k{<}\tau_{q+1}\right] \mathop{\mathbb{E}}_{\gamma_{\mathrm{e}}} \left[\left\{ \log\left(\frac{\tau_q}{\gamma_{\mathrm{e}}}\right)\right\}^{+} \right], \quad (4.58)$$

$$\mathcal{C}_{\text{H-SNR}}^{+} = \min_{1\leq k\leq K} \mathop{\mathbb{E}}_{\gamma_{\mathrm{e}},\gamma_k} \left[\left\{ \log\left(\frac{\gamma_k}{\gamma_{\mathrm{e}}}\right)\right\}^{+} \right], \quad (4.59)$$

with $Q{=}2^b$, and $\{\tau_q \,|\, 0{=}\tau_0{<}\tau_1{<}\cdots{<}\tau_Q\}_{q=1}^{Q}$ are the reconstruction points describing the support of γ_k with $\tau_{Q+1}{=}\infty$ for convenience.

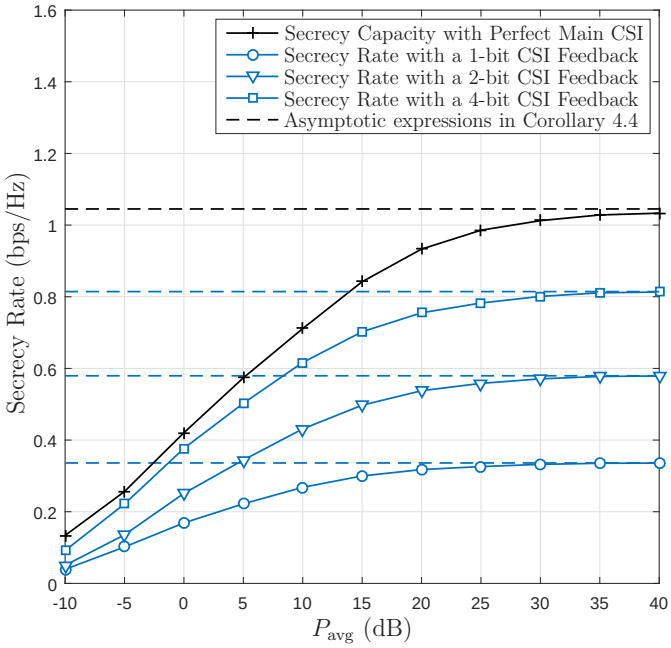


Figure 4.2: Common message secrecy rate in Theorem 4.2 for Rayleigh fading channels with K=3.

Proof: The result in Corollary 4.4 can be deduced directly from Theorem 4.2 by taking the limits of $\mathcal{C}_{\text{s}}^{-}$ and $\mathcal{C}_{\text{s}}^{+}$ when $P_{\text{avg}} \to \infty$.

The obtained result in Corollary 4.4 shows that the secrecy capacity is bounded at high SNR, i.e., it does not depend on P_{avg}.

4.5 Numerical Results

In this section, we provide selected simulation results for the illustrative case of independent and identically distributed Rayleigh fading channels. We consider that the system's variables, the main channel gains h_k, $k \in \{1, \cdots, K\}$, and the eavesdropper's channel gain h_{e}, are all distributed according to the zero-mean, unit-variance, complex Gaussian distribution.

Figure 4.2 illustrates the common message achievable secrecy rate $\mathcal{C}_{\text{s}}^{-}$, presented in Theorem 4.2, with K=3 and various b-bit feedback, b=1, 2, 4. The secrecy capacity $\mathcal{C}_{\text{s}}$, from Corollary 4.3, is also presented as a benchmark. It represents the secrecy

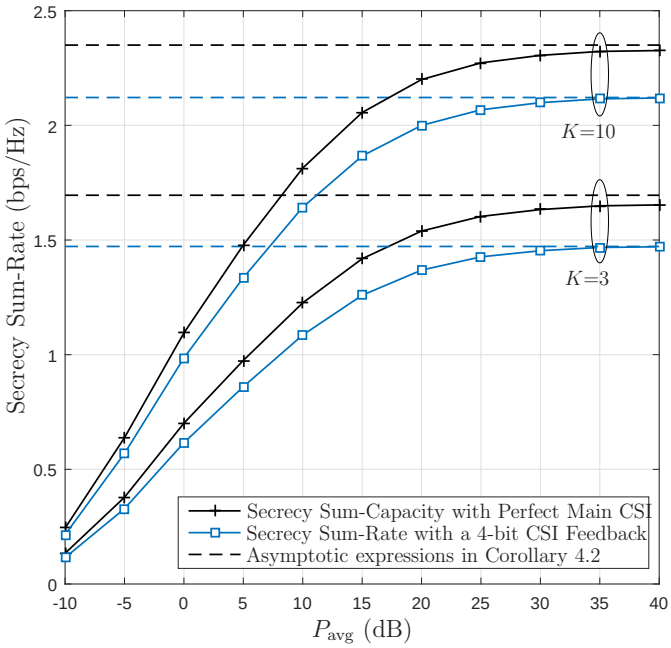


Figure 4.3: Independent messages secrecy sum-rate in Theorem 4.1 for Rayleigh fading channels with b=4.

capacity with full main CSI at the transmitter. We can see that as the capacity of the feedback link grows, i.e., the number of bits b increases, the achievable rate grows toward the secrecy capacity $\mathcal{C}_{\text{s}}$. The asymptotic expressions are also illustrated and show that the secrecy throughput is bounded at high SNR. The same observations can be made for the independent messages case; illustrated in figure 4.3. Two scenarios are considered here; the transmission of three independent messages to three legitimate receivers, K=3, and the transmission of ten independent messages with K=10. Both the achievable secrecy sum-rate in Theorem 4.1 and the secrecy sum-capacity in Corollary 4.1 are depicted. The impact of changing the number of legitimate receivers K on the secrecy sum-rate is illustrated in Figures 4.4 and 4.5 for different values of the average power constraint P_{avg} and of the number of feedback bits b. We can see from these two figures that the secrecy throughput of the system, when broadcasting multiple messages, increases with K.

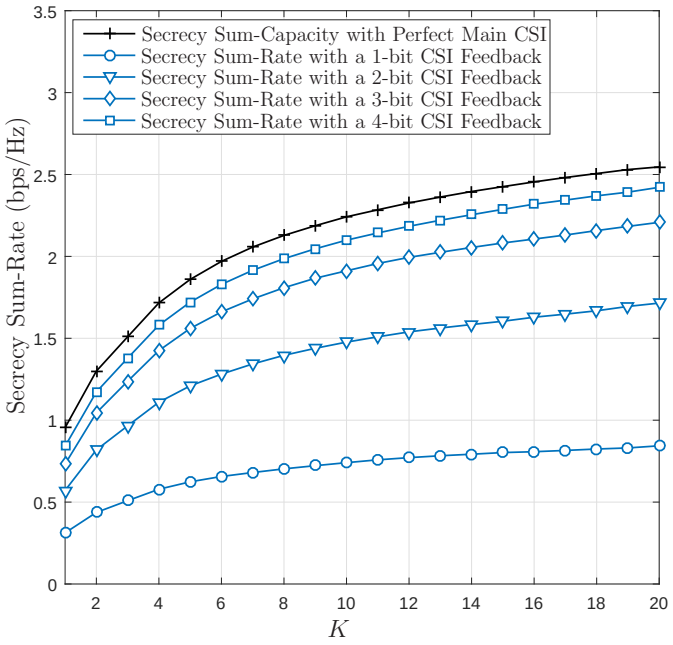


Figure 4.4: Independent messages secrecy sum-rate in Theorem 4.1 for Rayleigh fading channels with P_{avg}=20 dB.

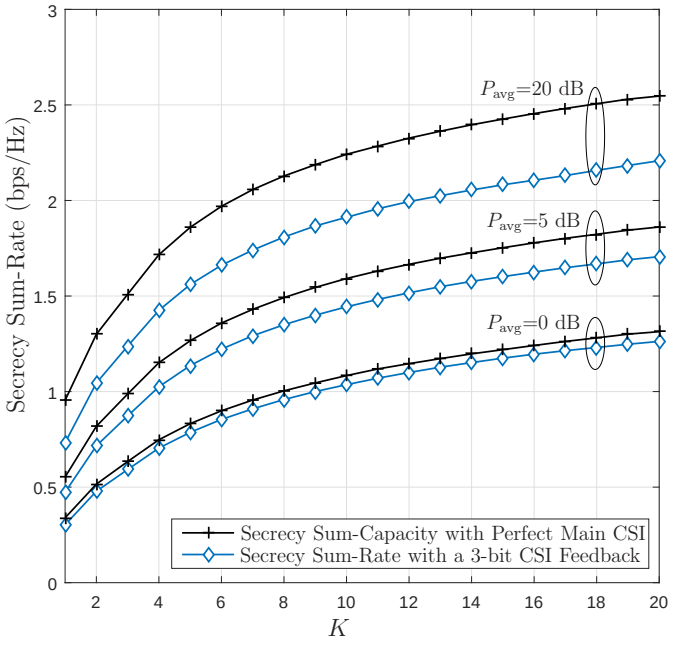


Figure 4.5: Independent messages secrecy sum-rate in Theorem 4.1 for Rayleigh fading channels with b=3.

4.6 Conclusion

The aim of this chapter was to study and understand the effect of having a limited knowledge of the CSIT on the ergodic secrecy throughput of multi-user broadcast wiretap channels. This limitation in the knowledge of the CSIT is the downside of the realistic assumption that the feedback links, used by the legitimate receivers to inform the transmitter about their CSI, have finite capacity. We considered both cases when independent confidential messages and when a common secret message are broadcasted to multiple legitimate receivers in the presence of an eavesdropper. In both cases, we showed that as long as the transmitter has some knowledge of the main CSI, a positive secrecy rate can still be achieved.

Chapter 5

On the Secrecy Capacity Region of the Block-Fading BCCM with Limited CSI Feedback

5.1 Introduction

In this chapter, we examine the secrecy capacity region of the block-fading broadcast channel with confidential messages (BCCM) when the transmitter has limited knowledge of the instantaneous channel realizations. In particular, we consider a two-user communication system where the transmitter has one common message to be transmitted to both users and one confidential message intended to only one of them. The confidential message has to be kept secret from the other user to whom the information is not intended. The transmitter is not aware of the CSI of neither channel and is only provided by limited CSI feedback sent at the beginning of each fading block. Assuming an error-free feedback link, we characterize the secrecy capacity region of this channel and show that even with a B-bit CSI feedback, a positive secrecy rate can still be achieved. Then, we look at the case where the feedback link is not error-free, and is rather a binary erasure channel (BEC). In the latter case, we provide an achievable secrecy rate region and show that as long as the erasure event is not a probability 1 event, the transmitter can still transmit the confidential information with a positive secrecy rate.

The remainder of this chapter is organized as follows. Section 5.2 describes the system model. The main results are introduced in section 5.3. The proof of achievability and the converse for the BCCM with an error-free B-bit feedback are presented

in section 5.4 and selected simulation results are presented in section 5.5. Finally, section 5.6 concludes the chapter.

5.2 System Model

We consider a broadcast channel where a transmitter T communicates with two receivers R_1 and R_2. As depicted in Figure 5.1, the transmitter wants to send a common message W_0 to both receivers and a confidential message W_1 to R_1 only. Message W_1 has to be kept secret from R_2. The respective received signals at R_1 and R_2, at fading block l, $l \in \{1, \cdots, L\}$, are given by

$$\begin{aligned} Y_1(l,j) &= h_1(l)X(l,j) + v_1(l,j) \\ Y_2(l,j) &= h_2(l)X(l,j) + v_2(l,j), \end{aligned} \tag{5.1}$$

where $j \in \{1, \cdots, \kappa\}$, with κ representing the length of each fading block, $X(l,j)$ is the transmitted signal, $h_1(l) \in \mathbb{C}$, $h_2(l) \in \mathbb{C}$ are stationary and ergodic complex channel gain coefficients, and $v_1(l,j) \in \mathbb{C}$, $v_2(l,j) \in \mathbb{C}$ represent zero-mean, unit-variance circularly symmetric white Gaussian noises at R_1 and R_2, respectively.

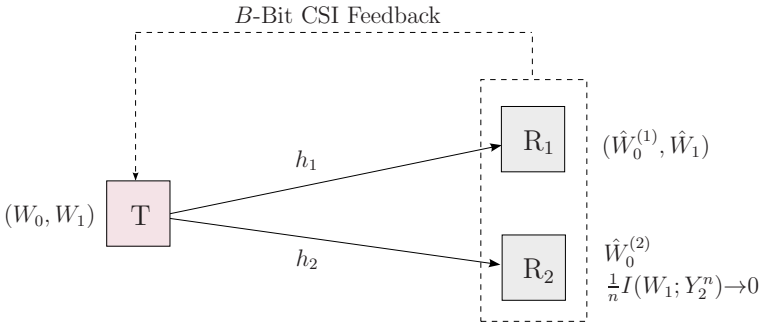


Figure 5.1: Block-fading BCCM with a B-bit CSI feedback sent at the beginning of each fading block over an error-free link.

5.2.1 Channel Assumptions

We consider a block-fading channel where the channel gains remain constant within a fading block. We assume that the channel encoding and decoding frames span a large number of fading blocks, i.e., L is large, and that the blocks change independently from a fading block to another. An average transmit power constraint is imposed at the transmitter such that

$$\frac{1}{n}\sum_{t=1}^{n}\mathbb{E}[|X(t)|^2] \leq P_{\text{avg}}, \tag{5.2}$$

where $n{=}\kappa L$, and the expectation is over the input distribution. We assume perfect CSI at the receiving nodes. That is, each receiver is instantaneously aware of its channel gain. Further, we assume that the transmitter is not aware of the instantaneous channel realizations of neither channel. However, the receivers provide the transmitter with a B-bit CSI feedback sent at the beginning of each fading block. The feedback bits are sent either by one of the receivers, if they share their CSI, or by a central controller who is aware of the CSI of both receivers. The last setting is possible since both receivers are interested by a common message. Hence, they both belong to the same network and their channels are more likely to be known by a controller center. First, we consider the case when the CSI feedback is sent over an error-free link. Then, as illustrated in Figure 5.2, we examine the case when the

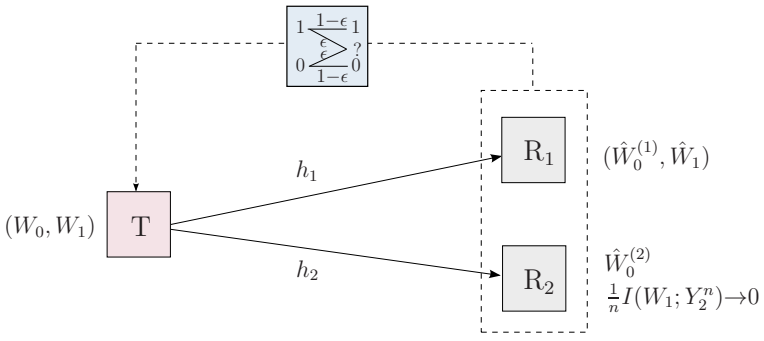


Figure 5.2: Block-fading BCCM with a B-bit CSI feedback sent at the beginning of each fading block over a BEC.

feedback information is sent over a BEC with erasure probability ϵ. In the rest of this chapter, we denote $|h_1|^2$ and $|h_2|^2$ by γ_1 and γ_2, respectively, and we let $\underline{\gamma} = [\gamma_1; \gamma_2]$.

5.2.2 Coding for the Two-User BCCM

A $(2^{n\mathcal{R}_0}, 2^{n\mathcal{R}_1}, n)$ code for the BCCM channel consists of the following elements:

- Two message sets: $\mathcal{W}_0 = \left\{1, 2, \cdots, 2^{n\mathcal{R}_0}\right\}$ and $\mathcal{W}_1 = \left\{1, 2, \cdots, 2^{n\mathcal{R}_1}\right\}$ with the messages $W_0 \in \mathcal{W}_0$ and $W_1 \in \mathcal{W}_1$ independent and uniformly distributed over the corresponding sets;
- A stochastic encoder $f : (\mathcal{W}_0, \mathcal{W}_1) \to \mathcal{X}^n$ that maps each message pair (w_0, w_1) to a codeword $x^n \in \mathcal{X}^n$;
- A decoder at the first receiver $g_1 : \mathcal{Y}_1^n \to (\mathcal{W}_0, \mathcal{W}_1)$ that maps a received sequence $y_1^n \in \mathcal{Y}_1^n$ to a message pair $(\hat{w}_0^{(1)}, \hat{w}_1) \in (\mathcal{W}_0, \mathcal{W}_1)$;
- A decoder at the second receiver $g_2 : \mathcal{Y}_2^n \to \mathcal{W}_0$ that maps a received sequence $y_2^n \in \mathcal{Y}_2^n$ to a message $\hat{w}_0^{(2)} \in \mathcal{W}_0$.

A rate pair $(\mathcal{R}_0, \mathcal{R}_1)$ is achievable if there exists a sequence of $(2^{n\mathcal{R}_0}, 2^{n\mathcal{R}_1}, n)$ code such that both the average error probability

$$P_{\mathrm{e}}^n = \Pr\left[(\hat{w}_0^{(1)}, \hat{w}_0^{(2)}, \hat{w}_1) \neq (w_0, w_0, w_1)\right], \tag{5.3}$$

and the leakage rate at receiver R_2, $\frac{1}{n} I(W_1; Y_2^n, \underline{\gamma}^L)$, go to zero as n goes to infinity.

Given the described system model, our goal is to characterize the secrecy capacity region that contains all achievable rate pairs.

5.3 Main Results

In this section, we present the main results obtained for the ergodic secrecy capacity region of the block-fading BCCM with a B-bit CSI feedback. First, we consider the case of the error-free feedback link. Then, we characterize the achievable secrecy rate region when the feedback link is a BEC.

5.3.1 Feedback Sent Over an Error-Free Link

5.3.1.1 B-Bit CSI Feedback

THEOREM 5.1. The ergodic secrecy capacity region of the block-fading BCCM with a B-bit CSI feedback, sent at the beginning of each coherence block over an error-free link, is given by

$$\mathcal{C}_{\rm s} = \bigcup_{\substack{(p_{01_q},p_{02_q},p_{1_q})\in\mathcal{P}\\ q\in\{1,\cdots,Q\}}} \left\{ \begin{array}{l} (\mathcal{R}_0,\mathcal{R}_1): \\ \mathcal{R}_0 \leq \min\Bigg\{ \displaystyle\sum_{q=1}^{Q} \mathop{\mathbb{E}}_{\underline{\gamma}} \left[\log\left(1+\frac{p_{01_q}\gamma_1}{1+p_{1_q}\gamma_1}\right)\Big|\underline{\gamma}\in\mathcal{A}\cap\mathcal{H}_q\right]\Pr[\underline{\gamma}\in\mathcal{A}\cap\mathcal{H}_q] \\ \qquad\qquad +\mathop{\mathbb{E}}_{\underline{\gamma}}\left[\log\left(1+p_{02_q}\gamma_1\right)\big|\underline{\gamma}\in\mathcal{A}^c\cap\mathcal{H}_q\right]\Pr[\underline{\gamma}\in\mathcal{A}^c\cap\mathcal{H}_q]; \\ \qquad\quad \displaystyle\sum_{q=1}^{Q} \mathop{\mathbb{E}}_{\underline{\gamma}} \left[\log\left(1+\frac{p_{01_q}\gamma_2}{1+p_{1_q}\gamma_2}\right)\Big|\underline{\gamma}\in\mathcal{A}\cap\mathcal{H}_q\right]\Pr[\underline{\gamma}\in\mathcal{A}\cap\mathcal{H}_q] \\ \qquad\qquad +\mathop{\mathbb{E}}_{\underline{\gamma}}\left[\log\left(1+p_{02_q}\gamma_2\right)\big|\underline{\gamma}\in\mathcal{A}^c\cap\mathcal{H}_q\right]\Pr[\underline{\gamma}\in\mathcal{A}^c\cap\mathcal{H}_q]\Bigg\} \\ \mathcal{R}_1 \leq \displaystyle\sum_{q=1}^{Q} \mathop{\mathbb{E}}_{\underline{\gamma}} \left[\log\left(\frac{1+p_{1_q}\gamma_1}{1+p_{1_q}\gamma_2}\right)\Big|\underline{\gamma}\in\mathcal{A}\cap\mathcal{H}_q\right]\Pr[\underline{\gamma}\in\mathcal{A}\cap\mathcal{H}_q], \end{array} \right. \tag{5.4}$$

where $Q = 2^{B-1}$, $\{\mathcal{H}_q\}_{q=1}^{Q}$ are the partition regions representing the space of $\underline{\gamma}$, $\mathcal{A}=\{\underline{\gamma}:\gamma_1>\gamma_2\}$ and

$$\mathcal{P}=\Big\{(p_{01_q},p_{02_q},p_{1_q}):\sum_{q=1}^{Q}(p_{01_q}+p_{1_q})\Pr[\underline{\gamma}\in\mathcal{A}\cap\mathcal{H}_q]+p_{02_q}\Pr[\underline{\gamma}\in\mathcal{A}^c\cap\mathcal{H}_q]\leq P_{\rm avg}\Big\}.$$

Proof. A detailed proof of Theorem 5.1 is provided in the following subsection.

The main idea here is to use one bit of feedback to indicate which channel is better and exploit the remaining $B-1$ bits to adapt the transmission power. We can see, from Theorem 5.1, that the common message W_0 is sent over all coherence blocks while the confidential message W_1 is transmitted only over the fading blocks where the channel to receiver R_1 is better than the one to R_2, i.e., $\underline{\gamma}\in\mathcal{A}$. That is, when $\underline{\gamma}\in\mathcal{A}$, we decode the common message considering the secure message as

noise, whereas when $\underline{\gamma} \in \mathcal{A}^c$, since the confidential message is not sent, the common message is decoded at a single user rate. The minimization is due to a bottleneck argument.

It is worth mentioning that, in order to adapt the power, the space of the channel gain vector $\underline{\gamma}$ is partitioned into Q regions. During each fading block, the index of the partition region where $\underline{\gamma}$ lies is fed back to the transmitter along with the indication bit. Furthermore, each partition index q corresponds to a transmission power profile p_{01_q} and p_{1_q} to transmit the common and the confidential messages when $\underline{\gamma} \in \mathcal{A}$ and p_{02_q} to transmit the common message solely when $\underline{\gamma} \in \mathcal{A}^c$, with p_{01_q}, p_{02_q} and p_{1_q} satisfying the average power constraint. The codebooks for the partition regions and the corresponding transmission power profiles should be known to all terminals. Also, it should be emphasized that when the feedback link has an infinite capacity, i.e., $Q \to \infty$, the secrecy capacity region in Theorem 5.1 coincides with the perfect CSIT result in [31].

5.3.1.2 Special Case: 1-Bit CSI Feedback

COROLLARY 5.1. The ergodic secrecy capacity region of the block-fading BCCM with a 1-bit CSI feedback, sent at the beginning of each coherence block over an error-free link, is given by

$$\mathcal{C}_{\mathrm{s}} = \bigcup_{(p_{01},p_{02},p_1)\in\mathcal{P}} \left\{ \begin{array}{l} (\mathcal{R}_0, \mathcal{R}_1): \\ \mathcal{R}_0 \leq \min\Big\{ \underset{\underline{\gamma}}{\mathbb{E}}\Big[\log\Big(1+\frac{p_{01}\gamma_1}{1+p_1\gamma_1}\Big)\,\Big|\underline{\gamma}\in\mathcal{A}\Big]\Pr[\underline{\gamma}\in\mathcal{A}] \\ \qquad\qquad + \underset{\underline{\gamma}}{\mathbb{E}}\big[\log\left(1+p_{02}\gamma_1\right)\big|\underline{\gamma}\in\mathcal{A}^c\big]\Pr[\underline{\gamma}\in\mathcal{A}^c]; \\ \qquad \underset{\underline{\gamma}}{\mathbb{E}}\Big[\log\Big(1+\frac{p_{01}\gamma_2}{1+p_1\gamma_2}\Big)\,\Big|\underline{\gamma}\in\mathcal{A}\Big]\Pr[\underline{\gamma}\in\mathcal{A}] \\ \qquad\qquad + \underset{\underline{\gamma}}{\mathbb{E}}\left[\log\left(1+p_{02}\gamma_2\right)\big|\underline{\gamma}\in\mathcal{A}^c\right]\Pr[\underline{\gamma}\in\mathcal{A}^c]\Big\} \\ \mathcal{R}_1 \leq \underset{\underline{\gamma}}{\mathbb{E}}\left[\log\left(1+p_1\gamma_1\right)-\log\left(1+p_1\gamma_2\right)\big|\underline{\gamma}\in\mathcal{A}\right]\Pr[\underline{\gamma}\in\mathcal{A}], \end{array} \right. \tag{5.5}$$

where $\mathcal{A} = \left\{\underline{\gamma} : \gamma_1 > \gamma_2\right\}$ and

$$\mathcal{P} = \left\{(p_{01}, p_{02}, p_1) : (p_{01}+p_1)\Pr[\underline{\gamma}\in\mathcal{A}]+p_{02}\Pr[\underline{\gamma}\in\mathcal{A}^c]\leq P_{\text{avg}}\right\}.$$

Proof. Corollary 5.1 is a special case of Theorem 5.1.

Corollary 5.1 states that even with a 1-bit CSI feedback, and as long as event $\mathcal{A}$ is not a zero probability event, a positive secrecy rate can still be achieved. The 1-bit feedback case is particularly important since we only need one bit of feedback to indicate which channel is better.

At the difference of the perfect CSIT case [31], the power cannot be instantaneously adapted to the channel realizations and will only depend on the received 1-bit CSI feedback according to a deterministic mapping. It is worth mentioning that p_{01} and p_{02} in Corollary 5.1 correspond to the power allocated to common message transmissions in $\mathcal{A}$ and $\mathcal{A}^c$, respectively, whereas p_1 is the power allocated to the confidential message.

5.3.1.3 Special Case: 2-Bit CSI Feedback

We would like here to connect our idea to use the feedback bits as indication bits to the two-user case considered in Chapter 3, Section 3.4.2.1.

We recall that the secrecy rate in Theorem 3.2 was achieved using a probabilistic transmission model that is constrained by the quality of the legitimate channels. In fact, for the particular case of K=2, we constructed two independent wiretap codebooks C_0 and C_1, and we considered that the transmitted common message is given in the form $W = (W_0, W_1)$. Then, we defined the following four events:

$$\begin{cases} S_1 = \left\{ |\hat{h}_1|^2 \geq \tau, |\hat{h}_2|^2 \geq \tau \right\} & \text{Select randomly a codeword associated with } W_0. \\ S_2 = \left\{ |\hat{h}_1|^2 \geq \tau, |\hat{h}_2|^2 < \tau \right\} & \text{For } W_1, \text{ the transmitter selects two independent codewords;} \\ S_3 = \left\{ |\hat{h}_1|^2 < \tau, |\hat{h}_2|^2 \geq \tau \right\} & \text{one to be sent in state } S_2 \text{ and the other one in state } S_3. \\ S_4 = \left\{ |\hat{h}_1|^2 < \tau, |\hat{h}_2|^2 < \tau \right\} & \text{Remain idle.} \end{cases}$$

where $\hat{h}_1$ and $\hat{h}_2$ are the estimated channel gains known at the transmitter and respectively corresponding to the actual realizations h_1 and h_2, and τ is a prefixed transmission threshold. The transmission of the common secret message was, then, adapted according to the occurrence of these events. We consider, here, that the estimation error variance α is equal to zero, i.e., $\hat{h}_1{=}h_1$ and $\hat{h}_2{=}h_2$, since we do not need each receiver to feed back the channel realization itself.

In Chapter 3, we have not imposed any limitation on the capacity of the CSI feedback link. We can see, though, that the secrecy rate in Theorem 3.2, can be achieved with only two bits of CSI feedback when $K{=}2$ and $\alpha{=}0$. The two bits of feedback would be used in this case as follows

$$\begin{cases} \text{When event } S_1 \text{ occurs} \longrightarrow \text{The feedback is equal to } 11 \\ \text{When event } S_2 \text{ occurs} \longrightarrow \text{The feedback is equal to } 10 \\ \text{When event } S_3 \text{ occurs} \longrightarrow \text{The feedback is equal to } 01 \\ \text{When event } S_4 \text{ occurs} \longrightarrow \text{The feedback is equal to } 00 \end{cases} . \tag{5.6}$$

This remark could be further generalized to the case when $K > 2$. In this case, the receivers need to send K feedback bits. Also, this special case does not require the receivers to cooperate to send the feedback information. The same secrecy rate

can still be achieved when each legitimate receiver sends a 1-bit feedback that would be used to compare the channel realization to the transmission threshold τ.

5.3.2 Feedback Sent Over a BEC

5.3.2.1 B-Bit CSI Feedback

COROLLARY 5.2. An achievable secrecy rate region of the block-fading BCCM with a B-bit CSI feedback, sent at the beginning of each coherence block over a BEC with erasure probability ϵ, is given by

$$\mathcal{R}_{\rm s} = \bigcup_{(p_{01},p_{02},p_1)\in\mathcal{P}} \left\{ \begin{array}{l} (\mathcal{R}_0,\mathcal{R}_1): \\ \mathcal{R}_0 \leq \min\Big\{ \underset{\underline{\gamma}}{\mathbb{E}}\left[\log\left(1+\frac{p_{01}\gamma_1}{1+p_1\gamma_1}\right)\Big| E^c_{B-bit}\,\&\,\underline{\gamma}\in\mathcal{A}\right](1-\epsilon^B)\Pr[\underline{\gamma}\in\mathcal{A}] \\ \qquad +\underset{\underline{\gamma}}{\mathbb{E}}\left[\log\left(1+p_{02}\gamma_1\right)\big| E_{B-bit} \text{ or } \left(E^c_{B-bit}\,\&\,\underline{\gamma}\in\mathcal{A}^c\right)\right]\left(\epsilon^B+(1-\epsilon^B)\Pr[\underline{\gamma}\in\mathcal{A}^c]\right); \\ \qquad\qquad \underset{\underline{\gamma}}{\mathbb{E}}\left[\log\left(1+\frac{p_{01}\gamma_2}{1+p_1\gamma_2}\right)\Big| E^c_{B-bit}\,\&\,\underline{\gamma}\in\mathcal{A}\right](1-\epsilon^B)\Pr[\underline{\gamma}\in\mathcal{A}] \\ \qquad +\underset{\underline{\gamma}}{\mathbb{E}}\left[\log\left(1+p_{02}\gamma_2\right)\big| E_{B-bit} \text{ or } \left(E^c_{B-bit}\,\&\,\underline{\gamma}\in\mathcal{A}^c\right)\right]\left(\epsilon^B+(1-\epsilon^B)\Pr[\underline{\gamma}\in\mathcal{A}^c]\right)\Big\} \\ \mathcal{R}_1 \leq \underset{\underline{\gamma}}{\mathbb{E}}\left[\log\left(\frac{1+p_1\gamma_1}{1+p_1\gamma_2}\right)\Big| E^c_{B-bit}\,\&\,\underline{\gamma}\in\mathcal{A}\right](1-\epsilon^B)\Pr[\underline{\gamma}\in\mathcal{A}], \end{array} \right. \tag{5.7}$$

where $\mathcal{A} = \left\{\underline{\gamma} : \gamma_1 > \gamma_2\right\}$, E_{B-bit} represents the event when all B feedback bits are erased, and

$$\mathcal{P} = \left\{(p_{01},p_{02},p_1) : (p_{01}+p_1)(1-\epsilon^B)\Pr[\underline{\gamma}\in\mathcal{A}]+p_{02}\left(\epsilon^B+(1-\epsilon^B)\Pr[\underline{\gamma}\in\mathcal{A}^c]\right) \leq P_{\rm avg}\right\}.$$

Proof: The achievability proof is provided in the following subsection. When the feedback is sent over a BEC, the transmission of the confidential message W_1 is restricted to the coherence blocks where $\gamma_1 > \gamma_2$ and the feedback information is not

erased. The common message W_0 is sent over all fading blocks. It is clear that the confidential rate $\mathcal{R}_1$ reduces as the erasure probability increases and vanishes when the erasure event is a sure event, i.e., the transmitter has no knowledge about the CSI. However, as long as $\epsilon \neq 1$ and event $\mathcal{A}$ is not a zero probability event, a positive secrecy rate can still be achieved.

In the previous subsection, we did see that when more than one bit of feedback is sent over an error-free link, one bit is used as an indication bit while the remaining extra bits are used to adapt the transmission power. Now, in the case when the feedback bits are sent over a BEC, it is more interesting to use all bits as redundant indication bits. By doing so, the probability of receiving a non-erased indication bit will increase, and this will eventually increase the probability of transmitting the secret information. Indeed, we can see, from Corollary 5.2, that the probability of transmitting the secret information depends on the erasure event E_{B-bit}, and is equal to $(1-\epsilon^B)\Pr[\underline{\gamma}\in\mathcal{A}]$. That is, as long as event $\mathcal{A}$ is not a zero probability event, increasing the number of redundant indication bits increases the probability of transmitting the secret message. This is particularly interesting when the probability of erasure ϵ is high.

5.4 Secrecy Capacity Region Analysis

In this section, we establish the obtained result for the ergodic secrecy capacity region presented in Theorem 5.1 and Corollary 5.2.

5.4.1 Achievability Scheme in Theorem 5.1

Since the transmission is controlled by the feedback information, we consider that, during each fading block, one feedback bit is used to indicate to the transmitter which channel is better, i.e., the indication bit is equal to 1 when $\gamma_1 > \gamma_2$ and equal to 0 otherwise, while the remaining $B-1$ bits are exploited to adapt the transmission

power. Therefore, the space of the channel gain vector $\underline{\gamma}$ is partitioned into $Q = 2^{B-1}$ regions, $\{\mathcal{H}_q\}_{q=1}^{Q}$. During each fading block, the index of the partition region where $\underline{\gamma}$ lies is fed back to the transmitter along with the indication bit. Furthermore, each partition index q corresponds to a transmission power profile $\left(p_{01_q}, p_{02_q}, p_{1_q}\right)$, $q \in \{1, \cdots, Q\}$. The achievability follows from [25, Corollary 1] by choosing the following input distributions:

- For $\underline{\gamma} \in \mathcal{A}$, $U \sim \mathcal{CN}(0, \sqrt{p_{01_q}})$, $X' \sim \mathcal{CN}(0, \sqrt{p_{1_q}})$, with X' independent of U and $V{=}X{=}U{+}X'$;
- For $\underline{\gamma} \in \mathcal{A}^c$, $U{=}V{=}X{\sim}\mathcal{CN}(0, \sqrt{p_{02_q}})$,

where $\mathcal{A} = \left\{\underline{\gamma} : \gamma_1 > \gamma_2\right\}$, U and V are the auxiliary random variables defined in [25], and the transmission powers $p_{01_q}, p_{02_q}, p_{1_q}$ are chosen to satisfy

$$\mathcal{P}{=}\Big\{(p_{01_q}, p_{02_q}, p_{1_q}){:}\sum_{q=1}^{Q}(p_{01_q}{+}p_{1_q})\Pr[\underline{\gamma}{\in}\mathcal{A}{\cap}\mathcal{H}_q]{+}p_{02_q}\Pr[\underline{\gamma}{\in}\mathcal{A}^c{\cap}\mathcal{H}_q]{\leq}P_{\text{avg}}\Big\}. \quad (5.8)$$

The codebooks for the partition regions and the corresponding transmission power profiles are known to all terminals.

5.4.2 Proof of the Converse in Theorem 5.1

5.4.2.1 Bound on the Common Rate $\mathcal{R}_0$

Let $F^L{=}\{F(1), F(2), \cdots, F(L)\}$, with $F(l) \in \{0, 1\}$ being the feedback information sent in the l-th fading block, $l \in \{1, \cdots, L\}$. We have

$$\begin{aligned} n\mathcal{R}_0 &= H(W_0|F^L) && (5.9)\\ &= I(W_0; Y_1^n|F^L) + H(W_0|F^L, Y_1^n) && (5.10)\\ &\leq I(W_0; Y_1^n|F^L) + n\eta_1 && (5.11)\\ &= \sum_{l=1}^{L}\sum_{k=1}^{\kappa} I(W_0; Y_1(l,k)|F^L, Y_1^{\kappa(l-1)+(k-1)}) + n\eta_1 && (5.12) \end{aligned}$$

$$\leq \sum_{l=1}^{L}\sum_{k=1}^{\kappa} I(W_0, Y_2^{[\kappa(l-1)+(k+1),n]}; Y_1(l,k)|F^L, Y_1^{\kappa(l-1)+(k-1)}) + n\eta_1 \tag{5.13}$$

$$\leq \sum_{l=1}^{L}\sum_{k=1}^{\kappa} I(W_0, Y_2^{[\kappa(l-1)+(k+1),n]}, Y_1^{\kappa(l-1)+(k-1)}; Y_1(l,k)|F^L) + n\eta_1, \tag{5.14}$$

where (5.11) is obtained using Fano's inequality. By defining the following auxiliary random variable $U(l,k) = (W_0, Y_2^{[\kappa(l-1)+(k+1),n]}, Y_1^{\kappa(l-1)+(k-1)})$, we can write

$$n\mathcal{R}_0 \leq \sum_{l=1}^{L}\sum_{k=1}^{\kappa} I(U(l,k); Y_1(l,k)|F^L) + n\eta_1 \tag{5.15}$$

$$= \sum_{l\in\mathcal{A}}\sum_{k=1}^{\kappa} I(U(l,k); Y_1(l,k)|F^L) + \sum_{l\in\mathcal{A}^c}\sum_{k=1}^{\kappa} I(U(l,k); Y_1(l,k)|F^L) + n\eta_1. \tag{5.16}$$

On one hand, when $l \in \mathcal{A}^c$, we have

$$I(U(l,k); Y_1(l,k)|F^L) \leq I(X(l,k); Y_1(l,k)|F^L) \tag{5.17}$$

$$= I(X(l,k); Y_1(l,k)|F^L, h_1(l)) \tag{5.18}$$

$$\leq \mathop{\mathbb{E}}_{F^l, \underline{\gamma}(l)}\left[\log\left(1+\gamma_1(l)\omega_l(F^l)\right)\Big|\underline{\gamma}(l)\in\mathcal{A}^c\right], \tag{5.19}$$

where (5.17) follows from $U(l,k) \to X(l,k) \to Y_1(l,k)$ is a Markov chain, (5.18) holds since given F^L, $X(l,k)$ is independent of $h_1(l)$, and (5.19) results since a Gaussian X maximizes the right hand side of (5.18), with $\omega_l(F^l) = \mathbb{E}\left[|X(l,k)|^2\Big|F^l\right]$. On the other hand, when $l \in \mathcal{A}$, we have

$$I(U(l,k); Y_1(l,k)|F^L) = I(U(l,k); Y_1(l,k)|F^L, h_1(l)) \tag{5.20}$$

$$= H(Y_1(l,k)|F^L, h_1(l)) - H(Y_1(l,k)\big|U(l,k), F^L, h_1(l)), \tag{5.21}$$

where (5.20) follows since given F^L, $U(l,k)$ is independent of $h_1(l)$, with

$$H(Y_1(l,k)\big|U(l,k), F^L, h_1(l)) \leq H(Y_1(l,k)\big|F^L, h_1(l)) \tag{5.22}$$

$$= \mathop{\mathbb{E}}_{F^l, \underline{\gamma}(l)}\left[\log\left(\pi e\left(1+\gamma_1(l)\delta_l(F^l)\right)\right)\Big|\underline{\gamma}(l)\in\mathcal{A}\right], \tag{5.23}$$

where (5.23) follows by taking $X(l,k) \sim \mathcal{CN}\left(0, \sqrt{\delta_l(F^l)}\right)$, and

$$H(Y_1(l,k)\big|U(l,k),F^L,h_1(l)) \geq H(Y_1(l,k)\big|X(l,k),F^L,h_1(l)) \tag{5.24}$$

$$= \log \pi e. \tag{5.25}$$

Hence, there exists $0 \leq \alpha_l \leq 1$ such that

$$H(Y_1(l,k)\big|U(l,k),F^L,h_1(l)) = \underset{F^l,\underline{\gamma}(l)}{\mathbb{E}}\left[\log\left(\pi e\left(1+\gamma_1(l)\alpha_l\delta_l(F^l)\right)\right)\big|\underline{\gamma}(l)\in\mathcal{A}\right]. \tag{5.26}$$

We can then write

$$I(U(l,k);Y_1(l,k)|F^L) \leq \underset{F^l,\underline{\gamma}(l)}{\mathbb{E}}\left[\log\left(\pi e\left(1+\gamma_1(l)\delta_l(F^l)\right)\right)\big|\underline{\gamma}(l)\in\mathcal{A}\right]$$

$$- \underset{F^l,\underline{\gamma}(l)}{\mathbb{E}}\left[\log\left(\pi e\left(1+\gamma_1(l)\alpha_l\delta_l(F^l)\right)\right)\big|\underline{\gamma}(l)\in\mathcal{A}\right] \tag{5.27}$$

$$= \underset{F^l,\underline{\gamma}(l)}{\mathbb{E}}\left[\log\left(1+\frac{\gamma_1(l)(1-\alpha_l)\delta_l(F^l)}{1+\gamma_1(l)\alpha_l\delta_l(F^l)}\right)\big|\underline{\gamma}(l)\in\mathcal{A}\right]. \tag{5.28}$$

Substituting (5.19) and (5.28) in (5.16), we get

$$n\mathcal{R}_0 \leq \sum_{l\in\mathcal{A}} \kappa \underset{F^l,\underline{\gamma}(l)}{\mathbb{E}}\left[\log\left(1+\frac{\gamma_1(l)(1-\alpha_l)\delta_l(F^l)}{1+\gamma_1(l)\alpha_l\delta_l(F^l)}\right)\big|\underline{\gamma}(l)\in\mathcal{A}\right]$$

$$+ \sum_{l\in\mathcal{A}^c} \kappa \underset{F^l,\underline{\gamma}(l)}{\mathbb{E}}\left[\log\left(1+\gamma_1(l)\omega_l(F^l)\right)\big|\underline{\gamma}(l)\in\mathcal{A}^c\right] + n\eta_1. \tag{5.29}$$

Noting that $\underset{F^l}{\mathbb{E}}[.] = \underset{F(l)}{\mathbb{E}}\left[\underset{F^{l-1}}{\mathbb{E}}[.|F(l)]\right]$, and applying Jensen's inequality, we get

$$\mathcal{R}_0 \leq \frac{1}{L}\sum_{l\in\mathcal{A}} \underset{\substack{F(l),\\ \underline{\gamma}(l)}}{\mathbb{E}}\left[\log\left(1+\frac{\gamma_1(l)(1-\alpha_l)\Delta_l(F(l))}{1+\gamma_1(l)\alpha_l\Delta_l(F(l))}\right)\big|\underline{\gamma}(l)\in\mathcal{A}\right]$$

$$+ \frac{1}{L}\sum_{l\in\mathcal{A}^c} \underset{\substack{F(l),\\ \underline{\gamma}(l)}}{\mathbb{E}}\left[\log(1+\gamma_1(l)\Omega_l(F(l)))\big|\underline{\gamma}(l)\in\mathcal{A}^c\right] + \eta_1 \tag{5.30}$$

$$= \frac{1}{L}\sum_{l\in\mathcal{A}} \underset{F(l),\underline{\gamma}}{\mathbb{E}}\left[\log\left(1+\frac{\gamma_1(1-\alpha_l)\Delta_l(F(l))}{1+\gamma_1\alpha_l\Delta_l(F(l))}\right)\big|\underline{\gamma}\in\mathcal{A}\right]$$

$$+ \frac{1}{L}\sum_{l\in\mathcal{A}^c} \underset{F(l),\underline{\gamma}}{\mathbb{E}}\left[\log(1+\gamma_1\Omega_l(F(l)))\big|\underline{\gamma}\in\mathcal{A}^c\right] + \eta_1, \tag{5.31}$$

with $\Delta_l(F(l))=\mathop{\mathbb{E}}_{F^{l-1}}\big[\delta_l(F^l)\big|F(l)\big]$, $\Omega_l(F(l))=\mathop{\mathbb{E}}_{F^{l-1}}\big[\omega_l(F^l)\big|F(l)\big]$, and (5.31) follows from the ergodicity and the stationarity of the channel gain. Applying Jensen's inequality once again, we get

$$\mathcal{R}_0 \leq \mathop{\mathbb{E}}_{\underline{\gamma}}\left[\log\left(1+\frac{\frac{\gamma_1}{L_{\mathcal{A}}}\sum_{l\in\mathcal{A}}(1-\alpha_l)\Delta_l(F(l))}{1+\frac{\gamma_1}{L_{\mathcal{A}}}\sum_{l\in\mathcal{A}}\alpha_l\Delta_l(F(l))}\right)\Big|\underline{\gamma}\in\mathcal{A}\right]\Pr\big[\underline{\gamma}\in\mathcal{A}\big] + \mathop{\mathbb{E}}_{\underline{\gamma}}\left[\log\left(1+\frac{\gamma_1}{L_{\mathcal{A}^c}}\sum_{l\in\mathcal{A}^c}\Omega_l(F(l))\right)\Big|\underline{\gamma}\in\mathcal{A}^c\right]\Pr\big[\underline{\gamma}\in\mathcal{A}^c\big]+\eta_1, \tag{5.32}$$

where $L_{\mathcal{A}}=\Pr\big[\underline{\gamma}\in\mathcal{A}\big]\,L$ and $L_{\mathcal{A}^c}=\Pr\big[\underline{\gamma}\in\mathcal{A}^c\big]\,L$.

Then, by taking $\Omega(F)=\dfrac{1}{L_{\mathcal{A}^c}}\sum_{l\in\mathcal{A}^c}\Omega_l(F(l))$, $\Delta_1(F)=\dfrac{1}{L_{\mathcal{A}}}\sum_{l\in\mathcal{A}}(1-\alpha_l)\Delta_l(F(l))$, and $\Delta_2(F)=\dfrac{1}{L_{\mathcal{A}}}\sum_{l\in\mathcal{A}}\alpha_l\Delta_l(F(l))$, we can write

$$\mathcal{R}_0 \leq \mathop{\mathbb{E}}_{\underline{\gamma}}\left[\log\left(1+\frac{\gamma_1\Delta_1(F)}{1+\gamma_1\Delta_2(F)}\right)\Big|\underline{\gamma}\in\mathcal{A}\right]\Pr\big[\underline{\gamma}\in\mathcal{A}\big] + \mathop{\mathbb{E}}_{\underline{\gamma}}\big[\log(1+\gamma_1\Omega(F))\big|\underline{\gamma}\in\mathcal{A}^c\big]\Pr\big[\underline{\gamma}\in\mathcal{A}^c\big]+\eta_1, \tag{5.33}$$

with $\Pr[\underline{\gamma}\in\mathcal{A}]\,(\Delta_1(F)+\Delta_2(F))+\Pr[\underline{\gamma}\in\mathcal{A}^c]\,\Omega(F)\leq P_{\text{avg}}$.

Similarly, we can prove that

$$\mathcal{R}_0 \leq \mathop{\mathbb{E}}_{\underline{\gamma}}\left[\log\left(1+\frac{\gamma_2\Delta_1(F)}{1+\gamma_2\Delta_2(F)}\right)\Big|\underline{\gamma}\in\mathcal{A}\right]\Pr\big[\underline{\gamma}\in\mathcal{A}\big] + \mathop{\mathbb{E}}_{\underline{\gamma}}\big[\log(1+\gamma_2\Omega(F))\big|\underline{\gamma}\in\mathcal{A}^c\big]\Pr\big[\underline{\gamma}\in\mathcal{A}^c\big]+\eta_2. \tag{5.34}$$

Now, using the fact that $F=\rho(\underline{\gamma})$, with $\rho(.)$ being a deterministic mapping that is conditioned on the region where vector $\underline{\gamma}$ lies, and taking η_1 and η_2 arbitrary small, we get the outer boundary on the common rate $\mathcal{R}_0$, presented in Theorem 5.1.

5.4.2.2 Bound on the Confidential Rate $\mathcal{R}_1$

Let us now bound the confidential rate $\mathcal{R}_1$. We have

$$
\begin{aligned}
n\mathcal{R}_1 &\leq n\mathcal{R}_{\mathrm{e}} && (5.35)\\
&= H(W_1|F^L,\underline{\gamma}^L,Y_2^n) && (5.36)\\
&= I(W_1;W_0|F^L,\underline{\gamma}^L,Y_2^n)+H(W_1|F^L,\underline{\gamma}^L,W_0,Y_2^n) && (5.37)\\
&\leq I(W_1;Y_1^n|F^L,\underline{\gamma}^L,W_0)-I(W_1;Y_2^n|F^L,\underline{\gamma}^L,W_0)\\
&\quad + H(W_1|F^L,\underline{\gamma}^L,W_0,Y_1^n)+H(W_0|F^L,\underline{\gamma}^L,Y_2^n) && (5.38)\\
&\leq I(W_1;Y_1^n|F^L,\underline{\gamma}^L,W_0)-I(W_1;Y_2^n|F^L,\underline{\gamma}^L,W_0)+n(\eta_1+\eta_2) && (5.39)\\
&= \sum_{l=1}^{L}\sum_{k=1}^{\kappa}\Big\{I(W_1;Y_1(l,k)|F^L,\underline{\gamma}(l),W_0,Y_1^{\kappa(l-1)+(k-1)})\\
&\quad - I(W_1;Y_2(l,k)|F^L,\underline{\gamma}(l),W_0,Y_2^{[\kappa(l-1)+(k+1),n]})\Big\}+n\eta && (5.40)\\
&= \sum_{l=1}^{L}\sum_{k=1}^{\kappa}\Big\{I(W_1,Y_2^{[\kappa(l-1)+(k+1),n]};Y_1(l,k)|F^L,\underline{\gamma}(l),W_0,Y_1^{\kappa(l-1)+(k-1)})\\
&\quad - I(Y_2^{[\kappa(l-1)+(k+1),n]};Y_1(l,k)|F^L,\underline{\gamma}(l),W_1,W_0,Y_1^{\kappa(l-1)+(k-1)})\\
&\quad - I(W_1,Y_1^{\kappa(l-1)+(k-1)};Y_2(l,k)|F^L,\underline{\gamma}(l),W_0,Y_2^{[\kappa(l-1)+(k+1),n]})\\
&\quad + I(Y_1^{\kappa(l-1)+(k-1)};Y_2(l,k)|F^L,\underline{\gamma}(l),W_1,W_0,Y_2^{[\kappa(l-1)+(k+1),n]})\Big\}+n\eta && (5.41)\\
&= \sum_{l=1}^{L}\sum_{k=1}^{\kappa}\Big\{I(W_1,Y_2^{[\kappa(l-1)+(k+1),n]};Y_1(l,k)|F^L,\underline{\gamma}(l),W_0,Y_1^{\kappa(l-1)+(k-1)})\\
&\quad - I(W_1,Y_1^{\kappa(l-1)+(k-1)};Y_2(l,k)|F^L,\underline{\gamma}(l),W_0,Y_2^{[\kappa(l-1)+(k+1),n]})\Big\}+n\eta && (5.42)\\
&= \sum_{l=1}^{L}\sum_{k=1}^{\kappa}\Big\{I(W_1;Y_1(l,k)|F^L,\underline{\gamma}(l),W_0,Y_1^{\kappa(l-1)+(k-1)},Y_2^{[\kappa(l-1)+(k+1),n]})\\
&\quad - I(W_1;Y_2(l,k)|F^L,\underline{\gamma}(l),W_0,Y_1^{\kappa(l-1)+(k-1)},Y_2^{[\kappa(l-1)+(k+1),n]})\Big\}+n\eta, && (5.43)
\end{aligned}
$$

where (5.39) is obtained using Fano's inequality, (5.42) and (5.43) follow from Lemma 7 in [25], and $\eta = \eta_1+\eta_2$. By defining $U(l,k) = (W_0,Y_2^{[\kappa(l-1)+(k+1),n]},Y_1^{\kappa(l-1)+(k-1)})$, and $V(l,k) = (W_1,U(l,k))$, such that $U(l,k) \to V(l,k) \to X(l,k) \to (Y_1(l,k),Y_2(l,k))$ is

a Markov chain, we can write

$$n\mathcal{R}_1 \leq \sum_{l=1}^{L}\sum_{k=1}^{\kappa}\big\{I(V(l,k);Y_1(l,k)|F^L,\underline{\gamma}(l),U(l,k)) - I(V(l,k);Y_2(l,k)|F^L,\underline{\gamma}(l),U(l,k))\big\} + n\eta. \tag{5.44}$$

When $l \in \mathcal{A}^c$, we have

$$\begin{aligned} &I(V(l,k);Y_1(l,k)|F^L,\underline{\gamma}(l),U(l,k)) - I(V(l,k);Y_2(l,k)|F^L,\underline{\gamma}(l),U(l,k)) \\ &\leq I(V(l,k);Y_1(l,k),Y_2(l,k)|F^L,\underline{\gamma}(l),U(l,k)) - I(V(l,k);Y_2(l,k)|F^L,\underline{\gamma}(l),U(l,k)) \\ &= I(V(l,k);Y_2(l,k)|F^L,\underline{\gamma}(l),U(l,k)) + I(V(l,k);Y_1(l,k)|F^L,\underline{\gamma}(l),Y_2(l,k),U(l,k)) \\ &\qquad - I(V(l,k);Y_2(l,k)|F^L,\underline{\gamma}(l),U(l,k)) \qquad (5.45) \\ &= 0, \qquad (5.46) \end{aligned}$$

where (5.46) results since $X(l,k)\to Y_1(l,k)\to Y_2(l,k)$ is a Markov chain when $l\in\mathcal{A}^c$. Hence, we have

$$\begin{aligned} \mathcal{R}_1 &\leq \frac{1}{n}\sum_{l\in\mathcal{A}}\sum_{k=1}^{\kappa}\big\{I(V(l,k);Y_1(l,k)|F^L,\underline{\gamma}(l),U(l,k)) - I(V(l,k);Y_2(l,k)|F^L,\underline{\gamma}(l),U(l,k))\big\} + \eta \qquad (5.47) \\ &\leq \frac{1}{n}\sum_{l\in\mathcal{A}}\sum_{k=1}^{\kappa}\big\{I(X(l,k);Y_1(l,k)|F^L,\underline{\gamma}(l),U(l,k)) - I(X(l,k);Y_2(l,k)|F^L,\underline{\gamma}(l),U(l,k))\big\} + \eta \qquad (5.48) \end{aligned}$$

Then, following similar lines as for the common rate case, we get

$$\mathcal{R}_1 \leq \mathop{\mathbb{E}}_{\underline{\gamma}}\Big[\log(1+\gamma_1\Delta_2(F)) - \log(1+\gamma_2\Delta_2(F))\Big|\underline{\gamma}\in\mathcal{A}\Big]\Pr\big[\underline{\gamma}\in\mathcal{A}\big] + \eta. \tag{5.49}$$

This concludes the proof of the converse. □

5.4.3 Achievability Scheme in Corollary 5.2

The achievability follows from [25, Corollary 1] by considering a similar feedback scheme as the one in Theorem 5.1. However, we consider here that during each

fading block, all B bits of feedback are redundantly used to indicate to the transmitter which channel is better (each of these bits is equal to 1 when $\gamma_1 > \gamma_2$ and equal to 0 otherwise). Besides, we consider that the confidential message is only transmitted over the coherence blocks where at least one indication bit is not erased and is equal to 1. The input distributions are chosen, in this case, as follows

- When $\underline{\gamma} \in \mathcal{A}$ and at least one indication bit is not erased, $U \sim \mathcal{CN}(0, \sqrt{p_{01}})$, $X' \sim \mathcal{CN}(0, \sqrt{p_1})$, with X' independent of U and $V{=}X{=}U{+}X'$;
- When $\underline{\gamma} \in \mathcal{A}^c$ or when all feedback bits are erased, $U{=}V{=}X \sim \mathcal{CN}(0, \sqrt{p_{02}})$,

where $\mathcal{A} = \left\{\underline{\gamma} : \gamma_1 > \gamma_2\right\}$, U and V are the auxiliary random variables defined in [25], and the transmission powers p_{01}, p_{02}, p_1 are chosen to satisfy

$$(p_{01}{+}p_1)(1{-}\epsilon^B)\Pr[\underline{\gamma}{\in}\mathcal{A}]{+}p_{02}\left(\epsilon^B{+}(1{-}\epsilon^B)\Pr[\underline{\gamma}{\in}\mathcal{A}^c]\right){\leq}P_{\text{avg}}.$$

5.5 Numerical Results

In this section, we provide selected simulation results for the illustrative case of independent and identically distributed Rayleigh fading channels. We consider that the system's variables, the main channel gains, h_1 and h_2, are distributed according to the zero-mean, complex Gaussian distribution.

Figure 5.3 illustrates the secrecy capacity region for the BCCM when 1-bit feedback is sent over an error-free link with $h_1 \sim \mathcal{CN}(0,1)$, $h_2 \sim \mathcal{CN}(0,\sigma_2^2)$, and $P_{\text{avg}}{=}5$dB. The boundary of the secrecy capacity region when perfect CSI is available at the transmitter is also presented as a benchmark. From Figure 5.3, we can see that when the channel to receiver R_1 is better than the channel to receiver R_2, i.e., when $\sigma_2^2{=}0.5$, the confidential rate $\mathcal{R}_1$ improves while the common rate $\mathcal{R}_0$ decreases.

The impact of having a binary erasure feedback link, on the achievable secrecy rate region, is illustrated in Figure 5.4, along with the boundaries on the secrecy

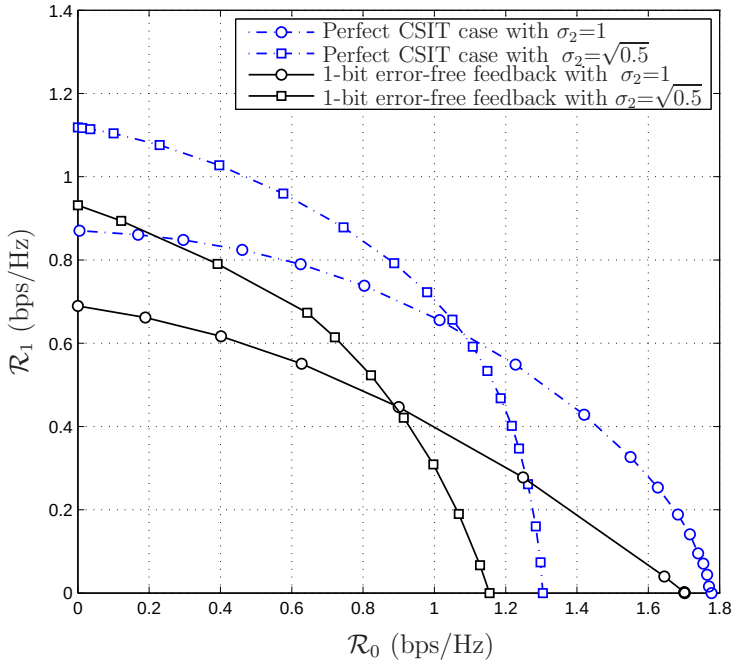


Figure 5.3: Secrecy capacity regions for the Rayleigh BCCM with an error-free CSI feedback.

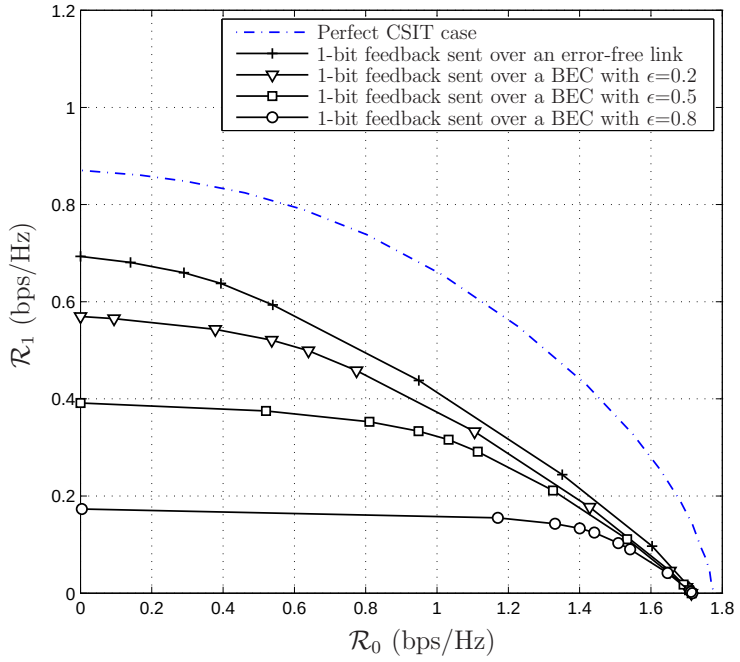


Figure 5.4: Secrecy capacity regions for the Rayleigh BCCM with a binary erasure feedback link.

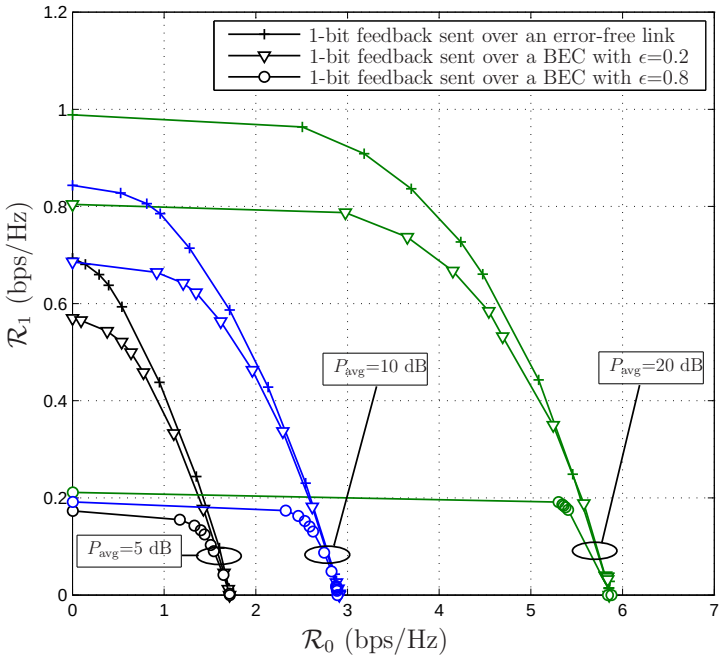


Figure 5.5: Secrecy capacity regions for Rayleigh BCCM with 1-bit CSI feedback.

capacity regions for the error-free feedback case and the perfect CSIT case, with $h_1 \sim \mathcal{CN}(0,1)$, $h_2 \sim \mathcal{CN}(0,1)$, P_{avg}=5 dB, and different values of the erasure probability ϵ=0.2, 0.5, and 0.8. As expected, we can see that the confidential rate $\mathcal{R}_1$ decreases as the probability of erasure increases since the transmission of the confidential message will be restricted, not only by the channel quality but also by the reception of a not erased feedback. The transmission of the common message solely is not affected by the erasure of the feedback information. Besides, from Figure 5.5, we can see that when the erasure probability is high; ϵ=0.8, the confidential rate does not improve much even when we increase the average power constraint from P_{avg}=5 dB to P_{avg}=20 dB. However, the secrecy rate can be significantly improved by using more redundant feedback bits as illustrated in Figure 5.6.

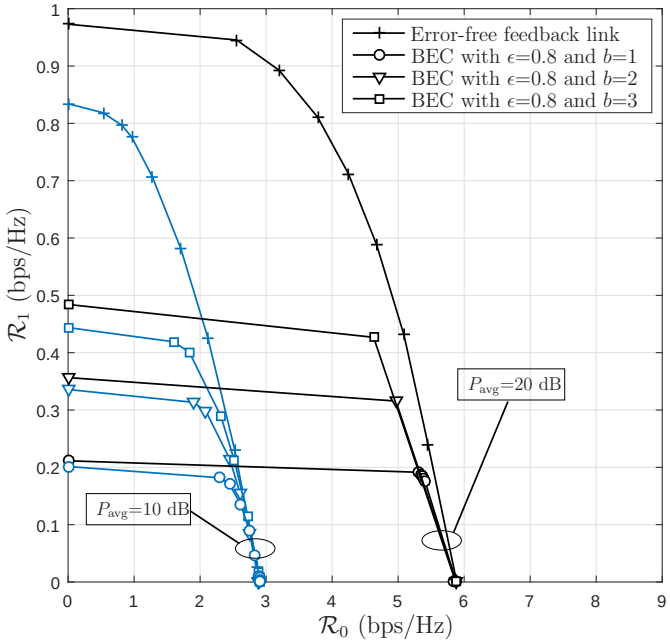


Figure 5.6: Secrecy capacity regions in Corollary 5.2 for Rayleigh BCCM with a B-bit CSI feedback.

5.6 Conclusion

In this chapter, we investigated the secrecy capacity region of the block-fading BCCM when the transmitter has limited knowledge of the CSI. More specifically, we considered that the transmitter in unaware of the instantaneous channel realizations of neither channel and is only provided by a B-bit CSI feedback sent at the beginning of each fading block. By utilizing one feedback bit to indicate which channel is better, we showed that a positive secrecy rate can still be achieved and that any additional feedback bits should be exploited to adapt the power. We examined both the case when the feedback link is error-free and the case when the feedback link is subject to erasure. In the first case, we characterized the BCCM secrecy capacity region, whereas in the latter case, we presented an achievable secrecy rate region.

Chapter 6

Secure Multiple-Antenna Block-Fading Wiretap Channels with Finite CSI Feedback

6.1 Introduction

In this chapter, we investigate the ergodic secrecy capacity of multiple-antenna block-fading wiretap channels with limited CSI feedback. We consider that the transmitter is unaware of the channel matrices of neither the main nor the eavesdropper channels, and is only provided by a finite CSI feedback sent by the legitimate receiver through a public, error-free, link with limited capacity. Assuming an average power constraint at the transmitter, we provide two achievable secrecy rates and an upper bound on the ergodic secrecy capacity. The first secrecy rate is achieved by using the feedback information not only to adapt the power but also to adjust the transmission rate during each fading block. The considered scheme guarantees that the best the eavesdropper can receive, during a given fading block, is the fixed transmission rate received at the legitimate node. For the second achievable secrecy rate, the feedback is mainly employed for the power adaptation purpose. Besides, in order to maximize the secrecy rate, we present a framework to design the used codebboks for feedback and transmission. The presented framework is based on the iterative Lloyd's algorithm [19]. For the particular case of infinite feedback, we prove that the first achievable secrecy rate and the presented upper bound on the ergodic secrecy capacity coincide, hence, fully characterizing the ergodic secrecy capacity in this case. The high-SNR regime and the SDoF are also investigated.

The chapter is organized as follows. Section 6.2 describes the system model. The main results are summarized in Section 6.3; the ergodic secrecy capacity is characterized in subsection 6.3.1, an asymptotic analysis in the high-SNR regime is presented in subsection 6.3.2, and an optimal framework for feedback and transmission is provided in subsection 6.3.3. In Section 6.4, we present details on the characterization of the achievable ergodic secrecy rates and the upper bound on the ergodic secrecy capacity. Finally, selected simulation results are illustrated in Section 6.5, and Section 6.6 concludes the chapter.

6.2 System Model

We consider a discrete-time memoryless wiretap channel where a transmitter wants to communicate a secret message to a legitimate receiver in the presence of an eavesdropper. The model of interest consists of a multiple-antenna channel with N_{T} transmit antennas, N_{R} receive antennas at the legitimate receiver, and N_{E} receive antennas at the eavesdropper. The respective received signals at the intended receiver and the eavesdropper, at time instant t, are given by

$$\begin{aligned} \mathbf{Y}_{\mathrm{R}}(t) &= \mathbf{H}_{\mathrm{R}}(t)\mathbf{X}(t) + \mathbf{Z}_{\mathrm{R}}(t) \\ \mathbf{Y}_{\mathrm{E}}(t) &= \mathbf{H}_{\mathrm{E}}(t)\mathbf{X}(t) + \mathbf{Z}_{\mathrm{E}}(t) \end{aligned} \tag{6.1}$$

where $\mathbf{X}(t)$ is the transmitted signal, $\mathbf{H}_{\mathrm{R}}(t) \in \mathbb{C}^{N_{\mathrm{R}} \times N_{\mathrm{T}}}$ and $\mathbf{H}_{\mathrm{E}}(t) \in \mathbb{C}^{N_{\mathrm{E}} \times N_{\mathrm{T}}}$ are the complex channel gain matrices, and $\mathbf{Z}_{\mathrm{R}}(t) \sim \mathcal{CN}(0, \sigma_{\mathrm{R}}^2 \mathbf{I}_{N_{\mathrm{R}}})$ and $\mathbf{Z}_{\mathrm{E}}(t) \sim \mathcal{CN}(0, \sigma_{\mathrm{E}}^2 \mathbf{I}_{N_{\mathrm{E}}})$ are independent and identically distributed (i.i.d.) additive complex Gaussian noise vectors. We consider a block-fading channel where the channel gain matrices remain constant within a fading block of length $\kappa >> 1$, i.e., $\mathbf{H}_{\mathrm{R}}(\kappa l) = \mathbf{H}_{\mathrm{R}}(\kappa l - 1) = \cdots = \mathbf{H}_{\mathrm{R}}(\kappa l - \kappa + 1)$ and $\mathbf{H}_{\mathrm{E}}(\kappa l) = \mathbf{H}_{\mathrm{E}}(\kappa l - 1) = \cdots = \mathbf{H}_{\mathrm{E}}(\kappa l - \kappa + 1)$, where $l = 1, \cdots, L$, and L is the total number of fading blocks. In the rest of this chapter, we denote

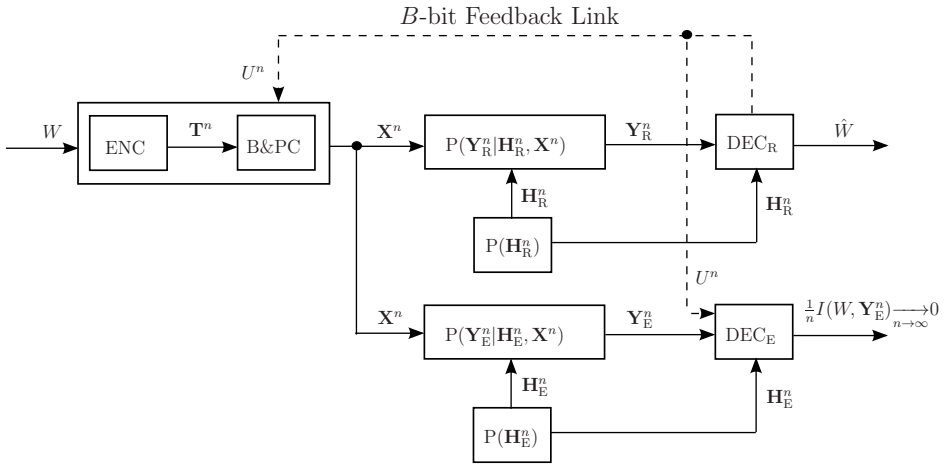


Figure 6.1: Block diagram of the channel model.

the respective main and eavesdropper channel gain matrices, during the l th fading block, as $\mathbf{H}_\mathrm{R}(l)$ and $\mathbf{H}_\mathrm{E}(l)$, $l = 1, \cdots, L$. We assume that the channel encoding and decoding frames span a large number of fading blocks, i.e., L is large, that the blocks change independently from a fading block to another, and that the entries of $\mathbf{H}_\mathrm{R}$ and $\mathbf{H}_\mathrm{E}$ have bounded distributions. The channel input $\{\mathbf{X}(t)\}_t$ is subject to an average total power constraint

$$\frac{1}{n}\sum_{t=1}^{n}||\mathbf{X}(t)||^2 \leq P_{\mathrm{avg}}, \tag{6.2}$$

where $n{=}\kappa L$. We assume perfect CSI at the receiver sides. That is, the legitimate receiver is instantaneously aware of its channel gain matrix $\mathbf{H}_\mathrm{R}(l)$, and the eavesdropper knows $\mathbf{H}_\mathrm{E}(l)$, with $l = 1, \cdots, L$. The fading distributions of the main and the eavesdropping channels are known to all nodes. Further, we assume that the transmitter is not aware of the instantaneous channel realizations of neither channel. However, the legitimate receiver provides the transmitter with a B-bit CSI feedback through an error-free channel with limited capacity. This feedback is transmitted at the beginning of each fading block and is also tracked by the eavesdropper. A block diagram of the communication system is presented in Fig. 6.1, where ENC represents

the encoder at the transmitter, B&PC is the beamforming and power control entity, and $\mathrm{DEC_R}$ and $\mathrm{DEC_E}$ are the respective decoders at the legitimate receiver and the eavesdropper.

6.2.1 Feedback Channel Model

For every fading block, and prior to payload data transmission, a preamble signal is sent to the legitimate receiver in order to estimate its channel gain. This preamble transmission is also tracked by the eavesdropper who gets to estimate its channel too. We assume that the channel gain matrices are perfectly estimated at the receiving sides. This is achievable for asymptotically large fading blocks [145]. Also, we consider that the feedback channel capacity is constrained to B bits per fading block, i.e., $\log_2 |\mathcal{U}| \leq B$, with $|\mathcal{U}|$ denoting the cardinality of the set, $\mathcal{U}$, of fed back symbols.

In the light of the work in [146], the adopted feedback strategy consists on partitioning the space of the main channel gain into Q regions $\{\mathcal{H}_1, \cdots, \mathcal{H}_Q\}$, where $Q = 2^B$. Knowing $\mathbf{H}_\mathrm{R}$ perfectly, the legitimate receiver determines in which region, $\mathcal{H}_q$ with q=$1, \cdots, Q$, the channel matrix lies. Also, the legitimate receiver associates the partition index q with each region $\mathcal{H}_q$, and transmits the index codeword u_q through the feedback channel. We assume that the partition regions $\{\mathcal{H}_1, \cdots, \mathcal{H}_Q\}$ are known to all terminals.

6.2.2 Adaptive Beamforming and Power Control Model

At the transmitter side, in addition to an encoder for secrecy, the confidential forward transmission is adapted using beamforming and power control. Since the only information available to the transmitter, about the main channel gain, is obtained through the limited feedback link, the choice of the relevant transmission strategy is based on what was fed back. In fact, each feedback information u_q corresponds to a Hermitian beamforming matrix $\mathbf{V}_q$ and a diagonal power control matrix $\mathbf{\Lambda}_q$ with $q = 1, \cdots, Q$.

That is, for each fading block, the transmitter uses the fed back information to apply the appropriate beamforming matrix and power control matrix to the encoded symbol $\mathbf{T}$. The forward signal $\mathbf{X}$ can then be written in the form $\mathbf{X} = \mathbf{V}_q \mathbf{\Lambda}_q^{1/2} \mathbf{T}$, and we let $\mathbb{E}[\mathbf{T}\mathbf{T}^*]=\mathbf{I}_{N_\mathrm{T}}$ for normalization. By taking $\boldsymbol{\rho}_q=\mathbf{V}_q \mathbf{\Lambda}_q \mathbf{V}_q^*$, the respective received SNRs at the legitimate receiver and the eavesdropper are $\frac{1}{\sigma_\mathrm{R}^2}\mathbf{H}_\mathrm{R}\boldsymbol{\rho}_q\mathbf{H}_\mathrm{R}^*$ and $\frac{1}{\sigma_\mathrm{E}^2}\mathbf{H}_\mathrm{E}\boldsymbol{\rho}_q\mathbf{H}_\mathrm{E}^*$. Note that the chosen set of beamforming and power control matrices should satisfy the average power constraint, i.e., $\mathrm{tr}\left[\mathbb{E}[\boldsymbol{\rho}_q]\right] \leq P_\mathrm{avg}$ for all $q \in \{1, \cdots, Q\}$, with the expectation taken over all channel gain realizations.

The adopted feedback and transmission strategies require the construction of a codebook for the partitioning of the main channel gain space into Q regions, as well as a codebook for the associated set of beamforming and power control matrices. In this work, we propose a design of fixed feedback and transmission codebooks that optimizes the secrecy performance of the system. Indeed, we present a framework to find the optimal feedback strategy $\{\mathcal{H}_1, \cdots, \mathcal{H}_Q\}$, as well as the optimal transmission strategy $\left\{\boldsymbol{\rho}_1, \cdots, \boldsymbol{\rho}_Q\right\}$, such that the average power constraint is satisfied, i.e., $\mathrm{tr}\left[\mathbb{E}[\boldsymbol{\rho}_q]\right] \leq P_\mathrm{avg}$, matrix $\boldsymbol{\rho}_q$ is positive semi-definite, i.e., $\boldsymbol{\rho}_q \succeq 0$, and the secrecy rate is maximized. It is assumed that all nodes are aware of the codebooks used for feedback and transmission. More details on the codebooks generation are available in the following section.

6.3 Main Results

In this section, we start by characterizing the ergodic secrecy capacity of the considered multiple-antenna system. Then, to better understand the correlation between the obtained expressions, the number of antennas deployed, and the number of feedback bits, we present an asymptotic analysis of the results. The SDoF of the system is also analyzed. Finally, a framework characterizing the generation of optimal codebooks for the feedback and the transmission strategies is introduced.

6.3.1 Lower and Upper Bounds on the Secrecy Capacity

6.3.1.1 Achievable Secrecy Rates

THEOREM 6.1. For the discrete-time memoryless multiple-antenna wiretap channel described in (6.1), with an error-free B-bit CSI feedback link, sent at the beginning of each fading block, the following secrecy rates are achievable

$$\mathcal{C}_{\mathrm{s}}^{-} = \sum_{q=1}^{Q} \max_{\{\mathcal{H}_q, \boldsymbol{\rho}_q\}} \mathop{\mathbb{E}}_{\mathbf{H}_{\mathrm{E}}|\mathbf{H}_{\mathrm{R}} \in \mathcal{H}_q} \left[\left\{ \log \frac{\min\limits_{\mathbf{H}_{\mathrm{R}} \in \mathcal{H}_q} \left| \mathbf{I}_{N_{\mathrm{R}}} + \frac{1}{\sigma_{\mathrm{R}}^2} \mathbf{H}_{\mathrm{R}} \boldsymbol{\rho}_q \mathbf{H}_{\mathrm{R}}^{*} \right|}{\left| \mathbf{I}_{N_{\mathrm{E}}} + \frac{1}{\sigma_{\mathrm{E}}^2} \mathbf{H}_{\mathrm{E}} \boldsymbol{\rho}_q \mathbf{H}_{\mathrm{E}}^{*} \right|} \right\}^{+} \right] P_q, \tag{6.3}$$

$$\widetilde{\mathcal{C}}_{\mathrm{s}}^{-} = \sum_{q=1}^{Q} \max_{\{\mathcal{H}_q, \boldsymbol{\rho}_q\}} \mathop{\mathbb{E}}_{\mathbf{H}_{\mathrm{E}}, \mathbf{H}_{\mathrm{R}}|\mathbf{H}_{\mathrm{R}} \in \mathcal{H}_q} \left[\log \frac{\left| \mathbf{I}_{N_{\mathrm{R}}} + \frac{1}{\sigma_{\mathrm{R}}^2} \mathbf{H}_{\mathrm{R}} \boldsymbol{\rho}_q \mathbf{H}_{\mathrm{R}}^{*} \right|}{\left| \mathbf{I}_{N_{\mathrm{E}}} + \frac{1}{\sigma_{\mathrm{E}}^2} \mathbf{H}_{\mathrm{E}} \boldsymbol{\rho}_q \mathbf{H}_{\mathrm{E}}^{*} \right|} \right] P_q, \tag{6.4}$$

where $Q{=}2^B$, $\mathrm{tr}\left[\mathbb{E}[\boldsymbol{\rho}_q]\right] {\leq} P_{\mathrm{avg}}$, $\boldsymbol{\rho}_q {\succeq} 0$, and $P_q{=}\Pr\left[\mathbf{H}_{\mathrm{R}} \in \mathcal{H}_q\right]$ for all $q \in \{1, \cdots, Q\}$.

Proof. A detailed proof of Theorem 6.1 is provided in the following section. Here, we outline the achievability scheme.

- Achievability scheme for $\mathcal{C}_{\mathrm{s}}^{-}$: We adopt a variable rate transmission controlled by the feedback information sent by the legitimate receiver. Thereby, during each fading block, if the main channel gain matrix falls within the partition region $\mathcal{H}_q$, $q \in \{1, \cdots, Q\}$, the transmitter conveys codewords at rate

$$R_q = \min_{\mathbf{H}_{\mathrm{R}} \in \mathcal{H}_q} \log \left| \mathbf{I}_{N_{\mathrm{R}}} + \frac{1}{\sigma_{\mathrm{R}}^2} \mathbf{H}_{\mathrm{R}} \boldsymbol{\rho}_q \mathbf{H}_{\mathrm{R}}^{*} \right|, \tag{6.5}$$

with the transmission strategy $\boldsymbol{\rho_q}$. Rate R_q changes only periodically and is held constant over the duration interval of a fading block. Let $\mathbf{T}_q$ be a channel gain matrix from $\mathcal{H}_q$ satisfying $\mathbf{T}_q = \arg\min\limits_{\mathbf{H}_{\mathrm{R}} \in \mathcal{H}_q} \left| \mathbf{I}_{N_{\mathrm{R}}} + \frac{1}{\sigma_{\mathrm{R}}^2} \mathbf{H}_{\mathrm{R}} \boldsymbol{\rho}_q \mathbf{H}_{\mathrm{R}}^{*} \right|$. The considered scheme guarantees that when the channel to the eavesdropper is better than the worst main channel gain in region $\mathcal{H}_q$, the mutual information between the transmitter and the eavesdropper is upper bounded by R_q. Otherwise, this mutual information will be

$\log\left|\mathbf{I}_{N_\mathrm{E}}+\frac{1}{\sigma_\mathrm{E}^2}\mathbf{H}_\mathrm{E}\boldsymbol{\rho}_q\mathbf{H}_\mathrm{E}^*\right|$. We can then optimize over the main channel gain regions, $\mathcal{H}_q$'s, and the transmission strategies, $\boldsymbol{\rho}_q$'s, to maximize the secrecy rate.

- Achievability scheme for $\widetilde{\mathcal{C}}_\mathrm{s}^-$: The proposed feedback and transmission procedure can be seen as a deterministic mapping that associates each feedback information with an appropriate transmission strategy. Accordingly, the adopted communication system can be equivalently modeled as a multiple-antenna memoryless channel without feedback where the mapping function becomes an amplification component of the new channel. The amplification matrix gain depends on which region the main channel gain lies in, i.e., if $\mathbf{H}_\mathrm{R}\in\mathcal{H}_q$, the transmitted signal $\mathbf{T}$ is amplified by $\mathbf{V}_q\boldsymbol{\Lambda}_q^{1/2}$.

Intuitively, Theorem 1 states that even a 1-bit CSI feedback, sent at the beginning of each fading block, ensures a positive secrecy rate. of course, the more the transmitter knows the better the secrecy performances are. As a matter of fact, increasing the number of feedback bits B, also increases the mutual information between the transmitted feedback information and the actual channel gain matrix. More specifically, when B increases, equivalently Q increases, the partitions $\{\mathcal{H}_q\}_q^Q$ will provide a better characterization for matrix $\mathbf{H}_\mathrm{R}$. That is, the transmitter will end up with more information about the main channel gain, which will allow a better adaptation of the transmission strategy and, hence, the achievement of a higher secrecy rate.

6.3.1.2 Upper Bound on the Secrecy Capacity

THEOREM 6.2. For the discrete-time memoryless multiple-antenna wiretap channel described in (6.1), with an error-free B-bit CSI feedback link, sent at the beginning of each fading block, an upper bound on the ergodic secrecy capacity is given by

$$\mathcal{C}_\mathrm{s}^+=\sum_{q=1}^{Q}\max_{\{\mathcal{H}_q,\boldsymbol{\rho}_q\}}\mathop{\mathbb{E}}_{\mathbf{H}_\mathrm{E},\mathbf{H}_\mathrm{R}|\mathbf{H}_\mathrm{R}\in\mathcal{H}_q}\left[\left\{\log\frac{\left|\mathbf{I}_{N_\mathrm{R}}+\frac{1}{\sigma_\mathrm{R}^2}\mathbf{H}_\mathrm{R}\boldsymbol{\rho}_q\mathbf{H}_\mathrm{R}^*\right|}{\left|\mathbf{I}_{N_\mathrm{E}}+\frac{1}{\sigma_\mathrm{E}^2}\mathbf{H}_\mathrm{E}\boldsymbol{\rho}_q\mathbf{H}_\mathrm{E}^*\right|}\right\}^+\right]P_q, \tag{6.6}$$

where $Q{=}2^B$, $\mathrm{tr}\left[\mathbb{E}[\boldsymbol{\rho}_q]\right] \leq P_{\mathrm{avg}}$, $\boldsymbol{\rho}_q \succeq 0$, and $P_q{=}\Pr\left[\mathbf{H}_{\mathrm{R}} \in \mathcal{H}_q\right]$ for all $q \in \{1, \cdots, Q\}$.

Proof. The proof is provided in the following section. We can see that the expression of the upper bound, in Theorem 6.2, is quite similar to the expression of $\mathcal{C}_{\mathrm{s}}^{-}$, in Theorem 6.1. The difference is that, for the achievable secrecy rate $\mathcal{C}_{\mathrm{s}}^{-}$, in the numerator, we have a minimization over all channels in each partition, whereas, in the upper bound, there is no such a minimization. The minimization, in the achievable secrecy rate, is required to ensure reliability as the transmitter has a limited knowledge of the main CSI.

6.3.1.3 Special Case: Single-Antenna System

Our aim here is to connect the obtained results for the multiple-antenna case to the single-antenna scenario considered in Chapter 4. In fact, when the transmitter, the legitimate receiver, and the eavesdropper are all equipped with a single antenna, i.e., $N_{\mathrm{T}}{=}N_{\mathrm{R}}{=}N_{\mathrm{E}}{=}1$, the achievable secrecy rate $\mathcal{C}_{\mathrm{s}}^{-}$, presented in Theorem 6.1, and the upper bound on the secrecy capacity $\mathcal{C}_{\mathrm{s}}^{+}$, presented in Theorem 6.2, both coincide with the secrecy capacity bounds presented in Theorem 4.1 with $K{=}1$. We should particularly mention that, for the single-antenna case, the channel gains are one dimensional and we can write $\mathbf{H}_{\mathrm{R}} = h_{\mathrm{R}}$ and $\mathbf{H}_{\mathrm{E}} = h_{\mathrm{E}}$. We can, therefore, partition the support of h_{R} into intervals, i.e., $\mathcal{H}_q = [\tau_q, \tau_{q+1}[$, $q \in \{1, \cdots, Q\}$, and there would be no beamforming at the transmitter in this case, i.e., $\boldsymbol{\rho}_q = P_q$. Making the appropriate substitutions in the expressions of $\mathcal{C}_{\mathrm{s}}^{-}$ and $\mathcal{C}_{\mathrm{s}}^{+}$, we retrieve the result in Theorem 4.1 with $K{=}1$.

6.3.1.4 Special Case: Infinite CSI Feedback

Letting Q goes to ∞, the lower bound in (6.3) and the upper bound in (6.6) coincide, hence, fully characterizing the ergodic secrecy capacity in this case.

COROLLARY 6.1. The ergodic secrecy capacity of a discrete-time memoryless multiple-antenna wiretap block fading channel with perfect main CSIT is given by

$$\mathcal{C}_{\mathrm{s}} = \max_{\boldsymbol{\rho}(\mathbf{H}_{\mathrm{R}})} \mathop{\mathbb{E}}_{\mathbf{H}_{\mathrm{E}},\mathbf{H}_{\mathrm{R}}} \left[\left\{ \log \frac{\left| \mathbf{I}_{N_{\mathrm{R}}} + \frac{1}{\sigma_{\mathrm{R}}^2} \mathbf{H}_{\mathrm{R}} \boldsymbol{\rho}(\mathbf{H}_{\mathrm{R}}) \mathbf{H}_{\mathrm{R}}^* \right|}{\left| \mathbf{I}_{N_{\mathrm{E}}} + \frac{1}{\sigma_{\mathrm{E}}^2} \mathbf{H}_{\mathrm{E}} \boldsymbol{\rho}(\mathbf{H}_{\mathrm{R}}) \mathbf{H}_{\mathrm{E}}^* \right|} \right\}^+ \right], \tag{6.7}$$

where $\mathrm{tr}\left[\mathbb{E}[\boldsymbol{\rho}(\mathbf{H}_{\mathrm{R}})]\right] \leq P_{\mathrm{avg}}$ and $\boldsymbol{\rho}(\mathbf{H}_{\mathrm{R}}) \succeq 0$.

Proof. Corollary 6.1 results directly from the expressions of the achievable rate in (6.3) and the upper bound in (6.6), by taking into consideration that as $Q \to \infty$, the set of partition regions, $\{\mathcal{H}_1, \cdots, \mathcal{H}_Q\}$, becomes infinite and the legitimate receiver is basically forwarding matrix $\mathbf{H}_{\mathrm{R}}$ to the transmitter.

To the best of our knowledge, this result has not been reported in earlier works. For the special case of N_{T}=N_{R}=N_{E}=1, the ergodic secrecy capacity in Corollary 6.1 coincides with the result in [28, Theorem 2].

6.3.2 Asymptotic Analysis in the High-SNR Regime

6.3.2.1 Finite CSI Feedback

COROLLARY 6.2. In the high-SNR regime, the ergodic secrecy capacity $\mathcal{C}_{\mathrm{s}}^{\mathrm{FF}}$ of the discrete-time memoryless multiple-antenna wiretap channel, with finite CSI feedback, can be characterized as follows

$$\lim_{P_{\mathrm{avg}} \to \infty} \left[\mathcal{C}_{\mathrm{s}}^{\mathrm{FF}} - \{r_{\mathrm{R}} - r_{\mathrm{E}}\}^+ \log \frac{P_{\mathrm{avg}}}{N_{\mathrm{T}}} \right] = \theta_1, \tag{6.8}$$

with

$$\begin{cases} \displaystyle\sum_{q=1}^{Q} \max_{\{\mathcal{H}_q\}} \mathop{\mathbb{E}}_{\boldsymbol{\lambda}_{\mathrm{E}} | \mathbf{H}_{\mathrm{R}} \in \mathcal{H}_q} \left[\min_{\substack{\boldsymbol{\lambda}_{\mathrm{R}} \\ \mathbf{H}_{\mathrm{R}} \in \mathcal{H}_q}} \sum_{i=1}^{r_{\mathrm{R}}} \log \frac{\lambda_{\mathrm{R}_i}}{\sigma_{\mathrm{R}}^2} - \sum_{i=1}^{r_{\mathrm{E}}} \log \frac{\lambda_{\mathrm{E}_i}}{\sigma_{\mathrm{E}}^2} \right] P_q \leq \theta_1 & \text{if } r_{\mathrm{R}} \geq r_{\mathrm{E}} \\ \theta_1 = 0 & \text{otherwise} \end{cases}, \tag{6.9}$$

and where r_{R}= $\min(N_{\mathrm{T}}, N_{\mathrm{R}})$, r_{E}= $\min(N_{\mathrm{T}}, N_{\mathrm{E}})$, and $\boldsymbol{\lambda}_{\mathrm{R}}$ and $\boldsymbol{\lambda}_{\mathrm{E}}$ are the respective

vectors of non-zeros eigenvalues of $\mathbf{H}_{\mathrm{R}}\mathbf{H}_{\mathrm{R}}^{*}$ and $\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{E}}^{*}$, i.e., $\boldsymbol{\lambda}_{\mathrm{R}}=\{\lambda_{\mathrm{R}_1},\cdots,\lambda_{\mathrm{R}_{r_{\mathrm{R}}}}\}$ and $\boldsymbol{\lambda}_{\mathrm{E}}=\{\lambda_{\mathrm{E}_1},\cdots,\lambda_{\mathrm{E}_{r_{\mathrm{E}}}}\}$.

Proof. The proof is provided in Appendix B.1.

We note that the lower bound on θ_1 is obtained by considering uniform power allocation over all transmit antennas. For the achievable secrecy rate $\mathcal{C}_{\mathrm{s}}^{-}$, uniform power allocation is nearly optimal when $N_{\mathrm{T}}\leq N_{\mathrm{R}}$. When $N_{\mathrm{T}}>N_{\mathrm{R}}$, using all transmit antennas to send the secret information is not the best that the transmitter can do. In this latter case, to transmit with fixed power, the transmitter may consider sending its confidential message over N_{T} antennas and exploits the remaining $N_{\mathrm{T}}-N_{\mathrm{R}}$ antennas to send jamming signals. This is, however, not easy to accomplish as the transmitter has limited knowledge of the main CSI and will end up disrupting not only to the eavesdropper but also to the legitimate receiver, especially when Q is small.

Secrecy degree of freedom: A figure-of-merit of interest is the so-called secrecy degree of freedom (SDoF) which has the same intuitive interpretation as the degree of freedom (DoF) widely used in the MIMO literature, but incorporates the secrecy constraint. Essentially, the SDoF is formally defined as

$$d_{\mathrm{s}}=\lim_{P_{\mathrm{avg}}\to\infty}\frac{\mathcal{C}_{\mathrm{s}}}{\log\left(P_{\mathrm{avg}}\right)}. \tag{6.10}$$

Theorem 6.3. The SDoF of the discrete-time memoryless multiple-antenna block-fading wiretap channel with finite CSI feedback is lower bounded as

$$d_{\mathrm{s}}^{\mathrm{FF}}\geq\left\{\min(N_{\mathrm{T}},N_{\mathrm{R}})-\min(N_{\mathrm{T}},N_{\mathrm{E}})\right\}^{+}. \tag{6.11}$$

Proof. The result can be deduced from Corollary 6.2. An upper bound on $d_{\mathrm{s}}^{\mathrm{FF}}$ is the SDoF with infinite CSI feedback that is characterized in the following subsection.

6.3.2.2 Perfect Main CSIT

COROLLARY 6.3. At high SNR, the ergodic secrecy capacity of the multiple-antenna wiretap channel, with perfect main CSI, can be characterized as follows

$$\lim_{P_{\text{avg}}\to\infty}\left[\mathcal{C}_{\text{s}}-\min\left(\{N_{\text{T}}-N_{\text{E}}\}^{+},N_{\text{R}}\right)\log\frac{P_{\text{avg}}}{N_{\text{T}}}\right]=\theta_2 \tag{6.12}$$

with

$$\theta_2\geq\begin{cases}0 & \text{if } N_{\text{T}}<N_{\text{E}}\\ \mathbb{E}_{\boldsymbol{\lambda}_{\text{R}},\boldsymbol{\lambda}_{\text{E}}}\left[\sum_{i=1}^{N_{\text{T}}}\log\frac{\lambda_{\text{R}_i}}{\sigma_{\text{R}}^2}-\sum_{i=1}^{N_{\text{E}}}\log\frac{\lambda_{\text{E}_i}}{\sigma_{\text{E}}^2}\right] & \text{if } N_{\text{E}}\leq N_{\text{T}}\leq N_{\text{R}}\\ \mathbb{E}_{\substack{\boldsymbol{\lambda}_{\text{R}},\boldsymbol{\lambda}_{\text{EZ}},\\ \boldsymbol{\lambda}_{\text{sum}}}}\left[\sum_{i=1}^{N_{\text{R}}}\log\frac{\lambda_{\text{R}_i}}{\sigma_{\text{R}}^2}+\sum_{i=1}^{\min(N_{\text{T}}-N_{\text{R}},N_{\text{E}})}\log\frac{\lambda_{\text{EZ}_i}}{\sigma_{\text{E}}^2}-\sum_{i=1}^{N_{\text{E}}}\log\frac{\lambda_{\text{sum}_i}}{\sigma_{\text{E}}^2}\right] & \text{if } N_{\text{T}}>\max(N_{\text{E}},N_{\text{R}})\end{cases},$$

and

$$\theta_2\leq\sum_{j:\alpha_j\geq 1}\log\alpha_j^2-o(1), \tag{6.13}$$

where $\boldsymbol{\lambda}_{\text{R}}$, $\boldsymbol{\lambda}_{\text{E}}$, $\boldsymbol{\lambda}_{\text{EZ}}$ and $\boldsymbol{\lambda}_{\text{sum}}$ are the respective vectors of non-zeros eigenvalues of $\mathbf{H}_{\text{R}}\mathbf{H}_{\text{R}}^{*}$, $\mathbf{H}_{\text{E}}\mathbf{H}_{\text{E}}^{*}$, $\mathbf{H}_{\text{E}}\mathbf{Z}\mathbf{Z}^{*}\mathbf{H}_{\text{E}}^{*}$ and $(\mathbf{H}_{\text{E}}\mathbf{H}_{\text{E}}^{*}+\mathbf{H}_{\text{E}}\mathbf{Z}\mathbf{Z}^{*}\mathbf{H}_{\text{E}}^{*})$, i.e., $\boldsymbol{\lambda}_{\text{R}}=\{\lambda_{\text{R}_1},\cdots,\lambda_{\text{R}_{r_{\text{R}}}}\}$, $\boldsymbol{\lambda}_{\text{E}}=\{\lambda_{\text{E}_1},\cdots,\lambda_{\text{E}_{r_{\text{E}}}}\}$, $\boldsymbol{\lambda}_{\text{EZ}}=\{\lambda_{\text{EZ}_1},\cdots,\lambda_{\text{EZ}_{r_{\text{EZ}}}}\}$ and $\boldsymbol{\lambda}_{\text{sum}}=\{\lambda_{\text{sum}_1},\cdots,\lambda_{\text{sum}_{r_{\text{sum}}}}\}$, with $\mathbf{Z}=\text{null}(\mathbf{H}_{\text{R}})$, the α_js represent the generalized singular values of $(\mathbf{H}_{\text{R}},\mathbf{H}_{\text{E}})$, and $o(1)$ is a vanishing term, i.e., $o(1)\to 0$.

Proof. The proof is provided in Appendix B.2. Since the entries of the channel gain matrices $\mathbf{H}_{\text{R}}$ and $\mathbf{H}_{\text{E}}$ have bounded distributions, the constant term θ_2 is finite and does not scale with P_{avg}. Also, it must be emphasized that the lower bound on θ_2, when $N_{\text{E}}\leq N_{\text{T}}\leq N_{\text{R}}$, is obtained by considering uniform power allocation over all transmit antennas. In the case when $N_{\text{T}}>\max(N_{\text{E}},N_{\text{R}})$, transmitting the secret information, solely, is no longer near optimal as the null space of $\mathbf{H}_{\text{R}}$ becomes nontrivial. In this case, we consider a transmission scheme that broadcasts jamming signals over the null space of $\mathbf{H}_{\text{R}}$. Details on the adopted system and the derived expressions are presented in Appendix B.2.

THEOREM 6.4. The SDoF of the discrete-time memoryless multiple-antenna block-fading wiretap channel with perfect main CSI is given by

$$d_{\mathrm{s}} = \min(\{N_{\mathrm{T}} - N_{\mathrm{E}}\}^{+}, N_{\mathrm{R}}). \tag{6.14}$$

Proof. The result can be deduced directly from Corollary 6.3. Note that even thought in our case the transmitter is not aware of the eavesdropper's instantaneous CSI, the obtained SDoF are the same as if the transmitter has a perfect knowledge of both the legitimate receiver's and the eavesdropper's CSI [37].

COROLLARY 6.4. At high SNR, and with uniform power allocation over all transmit antennas, the gap between the ergodic secrecy capacity with perfect main CSI and the achievable secrecy rates with finite CSI feedback can be characterized as follows

$$\lim_{P_{\mathrm{avg}}\to\infty}\left[\mathcal{C}_{\mathrm{s}} - \mathcal{C}_{\mathrm{s}}^{-}\right] = \mathop{\mathbb{E}}_{\boldsymbol{\lambda}_{\mathrm{R}}}\left[\sum_{i=1}^{N_{\mathrm{T}}}\log\lambda_{\mathrm{R}_i} - \sum_{q=1}^{Q}\max_{\{\mathcal{H}_q\}}\min_{\substack{\boldsymbol{\lambda}_{\mathrm{R}}\\ \mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q}}\sum_{i=1}^{N_{\mathrm{T}}}\log\lambda_{\mathrm{R}_i}P_q\right], \tag{6.15}$$

$$\lim_{P_{\mathrm{avg}}\to\infty}\left[\mathcal{C}_{\mathrm{s}} - \widetilde{\mathcal{C}}_{\mathrm{s}}^{-}\right] = \mathop{\mathbb{E}}_{\boldsymbol{\lambda}_{\mathrm{R}},\boldsymbol{\lambda}_{\mathrm{E}}}\left[\left\{(r_{\mathrm{E}} - N_{\mathrm{T}})\log\frac{P_{\mathrm{avg}}}{N_{\mathrm{T}}} + \sum_{i=1}^{r_{\mathrm{E}}}\log\frac{\lambda_{\mathrm{E}_i}}{\sigma_{\mathrm{E}}^2} - \sum_{i=1}^{N_{\mathrm{T}}}\log\frac{\lambda_{\mathrm{R}_i}}{\sigma_{\mathrm{R}}^2}\right\}^{+}\right], \tag{6.16}$$

with $N_{\mathrm{T}} \leq N_{\mathrm{R}}$, $r_{\mathrm{E}} = \min(N_{\mathrm{T}}, N_{\mathrm{E}})$, and $\boldsymbol{\lambda}_{\mathrm{R}}$ and $\boldsymbol{\lambda}_{\mathrm{E}}$ are the respective vectors of non-zeros eigenvalues of $\mathbf{H}_{\mathrm{R}}\mathbf{H}_{\mathrm{R}}^{*}$ and $\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{E}}^{*}$.

Proof: The proof is provided in Appendix B.3. It is worth mentioning that, on one hand, the asymptotic gap between $\mathcal{C}_{\mathrm{s}}$ and $\mathcal{C}_{\mathrm{s}}^{-}$ vanishes as the number of feedback bits increases, i.e., $Q\to\infty$. Indeed, we have

$$\sum_{q=1}^{Q}\max_{\{\mathcal{H}_q\}}\min_{\substack{\boldsymbol{\lambda}_{\mathrm{R}}\\ \mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q}}\sum_{i=1}^{N_{\mathrm{T}}}\log\lambda_{\mathrm{R}_i}P_q \xrightarrow[Q\to\infty]{} \sum_{i=1}^{N_{\mathrm{T}}}\log\lambda_{\mathrm{R}_i}.$$

On the other hand, the asymptotic gap between $\mathcal{C}_{\mathrm{s}}$ and $\widetilde{\mathcal{C}}_{\mathrm{s}}^{-}$ is independent of the number of feedback bits. A similar inference can be made in the case of $N_{\mathrm{T}} > N_{\mathrm{R}}$.

6.3.3 Optimal Feedback and Transmission (OFT)

6.3.3.1 OFT for the Achievable Secrecy Rate $\widetilde{\mathcal{C}}_{\mathrm{s}}^{-}$

Finding the optimal feedback strategy, $\{\mathcal{H}_1, \cdots, \mathcal{H}_Q\}$, and the optimal transmission strategy, $\{\boldsymbol{\rho}_1, \cdots, \boldsymbol{\rho}_Q\}$, that maximizes the achievable secrecy rate $\widetilde{\mathcal{C}}_{\mathrm{s}}^{-}$ in (6.4), is equivalent to the design of a vector quantizer with a modified distortion measure. Let λ be the Lagrange multiplier corresponding to the average transmit power constraint. We define the following distortion measure

$$\tilde{\delta}\left(\mathbf{H}_{\mathrm{R}}, \mathbf{H}_{\mathrm{E}}, \boldsymbol{\rho}_q\right) = -\left[\log \frac{\left|\mathbf{I}_{N_{\mathrm{R}}} + \frac{1}{\sigma_{\mathrm{R}}^2}\mathbf{H}_{\mathrm{R}}\boldsymbol{\rho}_q\mathbf{H}_{\mathrm{R}}^*\right|}{\left|\mathbf{I}_{N_{\mathrm{E}}} + \frac{1}{\sigma_{\mathrm{E}}^2}\mathbf{H}_{\mathrm{E}}\boldsymbol{\rho}_q\mathbf{H}_{\mathrm{E}}^*\right|} - \lambda \mathrm{tr}\boldsymbol{\rho}_q\right], \tag{6.17}$$

where $\boldsymbol{\rho}_q \succeq 0$ and $q = \{1, \cdots, Q\}$. We need to find the optimal $\{\mathcal{H}_1, \cdots, \mathcal{H}_Q\}$ and $\{\boldsymbol{\rho}_1, \cdots, \boldsymbol{\rho}_Q\}$ that minimizes the average distortion measure $\widetilde{\Delta}$ given by

$$\widetilde{\Delta} = \sum_{q=1}^{Q} \mathop{\mathbb{E}}_{\mathbf{H}_{\mathrm{E}}, \mathbf{H}_{\mathrm{R}} | \mathbf{H}_{\mathrm{R}} \in \mathcal{H}_q} \left[\tilde{\delta}\left(\mathbf{H}_{\mathrm{R}}, \mathbf{H}_{\mathrm{E}}, \boldsymbol{\rho}_q\right)\right] P_q. \tag{6.18}$$

To solve this optimization problem, we use Lloyd's algorithm [19]. The OFT for the achievable secrecy rate $\widetilde{\mathcal{C}}_{\mathrm{s}}^{-}$ is given in Algo.1[1]. It should be noted that since we are using Lloyd algorithm, the partitioning is performed according to the Voronoi diagram using the nearest neighbor rule, i.e.,

$$\mathcal{H}_q = \left\{\mathbf{H}_{\mathrm{R}} : \tilde{\delta}\left(\mathbf{H}_{\mathrm{R}}, \mathbf{H}_{\mathrm{E}}, \boldsymbol{\rho}_q\right) \leq \tilde{\delta}\left(\mathbf{H}_{\mathrm{R}}, \mathbf{H}_{\mathrm{E}}, \boldsymbol{\rho}_j\right); \forall j \in \{1, \cdots, Q\}, j \neq q\right\}. \tag{6.19}$$

The probability $P_q = \Pr\left[\mathbf{H}_{\mathrm{R}} \in \mathcal{H}_q\right]$ can then be characterized, in this case, as follows

$$P_q = \Pr\left[\tilde{\delta}\left(\mathbf{H}_{\mathrm{R}}, \mathbf{H}_{\mathrm{E}}, \boldsymbol{\rho}_q\right) \leq \tilde{\delta}\left(\mathbf{H}_{\mathrm{R}}, \mathbf{H}_{\mathrm{E}}, \boldsymbol{\rho}_j\right); \forall j \in \{1, \cdots, Q\}, j \neq q\right] \tag{6.20}$$

$$= \Pr\left[\tilde{\delta}\left(\mathbf{H}_{\mathrm{R}}, \mathbf{H}_{\mathrm{E}}, \boldsymbol{\rho}_q\right) \leq \max_{j \in \{1, \cdots, Q\}, j \neq q} \tilde{\delta}\left(\mathbf{H}_{\mathrm{R}}, \mathbf{H}_{\mathrm{E}}, \boldsymbol{\rho}_j\right)\right]. \tag{6.21}$$

[1] In general, there is no guarantee that Lloyd's algorithm converges to the global optimum [19]. In the simulations, we repeat the iterations multiple times and pick the one that gives us the largest secrecy rate.

Algorithm 1: OFT for $\widetilde{\mathcal{C}}_{\mathrm{s}}^{-}$

Input : Q, λ.
Output: Optimal feedback and transmission strategy $\{\mathcal{H}_1, \cdots, \mathcal{H}_Q\}$ and $\{\boldsymbol{\rho}_1, \cdots, \boldsymbol{\rho}_Q\}$.
Consider a random partition of the space of $\mathbf{H}_{\mathrm{R}}$: $\mathbb{H}_1 = \{\mathcal{H}_1, \cdots, \mathcal{H}_Q\}$;
Define $\mathbb{H}_0$ as the set of Q empty regions;
Let $itr = 1$;
while $\mathbb{H}_{itr} \neq \mathbb{H}_{itr-1}$ **do**
  for $q = 1 : Q$ **do**
    Find the optimal transmission strategy $\boldsymbol{\rho}_q$, given by the *generalized partition centroid*:
    $\boldsymbol{\rho}_q = \arg\min_{\boldsymbol{\rho}_q} \mathbb{E}_{\mathbf{H}_{\mathrm{E}}, \mathbf{H}_{\mathrm{R}} | \mathbf{H}_{\mathrm{R}} \in \mathcal{H}_q} \left[\tilde{\delta} \left(\mathbf{H}_{\mathrm{R}}, \mathbf{H}_{\mathrm{E}}, \boldsymbol{\rho}_q \right) \right] P_q$;
  for $q = 1 : Q$ **do**
    Find the optimal partition region $\mathcal{H}_q$, given the transmission strategies $\{\boldsymbol{\rho}_1, \cdots, \boldsymbol{\rho}_Q\}$, using the *nearest neighbor rule*:
    $\mathcal{H}_q = \left\{ \mathbf{H}_{\mathrm{R}} : \tilde{\delta} \left(\mathbf{H}_{\mathrm{R}}, \mathbf{H}_{\mathrm{E}}, \boldsymbol{\rho}_q \right) \leq \tilde{\delta} \left(\mathbf{H}_{\mathrm{R}}, \mathbf{H}_{\mathrm{E}}, \boldsymbol{\rho}_j \right) ; \forall j \in \{1, \cdots, Q\}, j \neq q \right\}$;
  $itr = itr + 1$;
  $\mathbb{H}_{itr} = \{\mathcal{H}_1, \cdots, \mathcal{H}_Q\}$;
$P_{\mathrm{avg}} = \sum_{q=1}^{Q} \mathrm{tr} \boldsymbol{\rho}_q \Pr \left[\mathbf{H}_{\mathrm{R}} \in \mathcal{H}_q \right]$.

We should also mention that the proposed scheme is an offline optimization algorithm and it only depends on the knowledge of the statistics of the channel gains.

6.3.3.2 OFT for the Achievable Secrecy Rate $\mathcal{C}_{\mathrm{s}}^{-}$

To design the optimal feedback and transmission codebooks that maximizes the achievable secrecy rate $\mathcal{C}_{\mathrm{s}}^{-}$ in (6.3), we consider the following modified distortion measure

$$\delta \left(\mathbf{H}_{\mathrm{R}}, \mathbf{H}_{\mathrm{E}}, \boldsymbol{\rho}_q \right) = - \left[\left\{ \log \frac{\left| \mathbf{I}_{N_{\mathrm{R}}} + \frac{1}{\sigma_{\mathrm{R}}^2} \mathbf{H}_{\mathrm{R}} \boldsymbol{\rho}_q \mathbf{H}_{\mathrm{R}}^{*} \right|}{\left| \mathbf{I}_{N_{\mathrm{E}}} + \frac{1}{\sigma_{\mathrm{E}}^2} \mathbf{H}_{\mathrm{E}} \boldsymbol{\rho}_q \mathbf{H}_{\mathrm{E}}^{*} \right|} \right\}^{+} - \lambda \mathrm{tr} \boldsymbol{\rho}_q \right], \tag{6.22}$$

Algorithm 2: OFT for $\mathcal{C}_{\rm s}^{-}$

Input : Q, λ.
Output: Optimal feedback and transmission strategy $\{\mathcal{H}_1, \cdots, \mathcal{H}_Q\}$ and $\{\boldsymbol{\rho}_1, \cdots, \boldsymbol{\rho}_Q\}$.
Consider a random partition of the space of $\mathbf{H}_{\rm R}$: $\mathbb{H}_1 = \{\mathcal{H}_1, \cdots, \mathcal{H}_Q\}$;
Define $\mathbb{H}_0$ as the set of Q empty regions;
Let $itr = 1$;
while $\mathbb{H}_{itr} \neq \mathbb{H}_{itr-1}$ **do**
  for $q = 1 : Q$ **do**
    $\mathbf{T}_q(\boldsymbol{\rho}_q) = \underset{\mathbf{H}_{\rm R} \in \mathcal{H}_q}{\arg\min} \left| \mathbf{I}_{N_{\rm R}} + \frac{1}{\sigma_{\rm R}^2} \mathbf{H}_{\rm R} \boldsymbol{\rho}_q \mathbf{H}_{\rm R}^{*} \right|$;
    Find the optimal transmission strategy:

$$\boldsymbol{\rho}_q = \arg\min_{\boldsymbol{\rho}_q} \underset{\mathbf{H}_{\rm E} | \mathbf{H}_{\rm R} \in \mathcal{H}_q}{\mathbb{E}} \left[\delta \left(\mathbf{T}_q(\boldsymbol{\rho}_q), \mathbf{H}_{\rm E}, \boldsymbol{\rho}_q \right) \right] P_q;$$

  for $q = 1 : Q$ **do**
    Find the optimal partition region:

$$\mathcal{H}_q = \left\{ \mathbf{H}_{\rm R} : \delta \left(\mathbf{H}_{\rm R}, \mathbf{H}_{\rm E}, \boldsymbol{\rho}_q \right) \leq \delta \left(\mathbf{H}_{\rm R}, \mathbf{H}_{\rm E}, \boldsymbol{\rho}_j \right); \quad \forall j \in \{1, \cdots, Q\}, j \neq q \right\};$$

  $itr = itr + 1$;
  $\mathbb{H}_{itr} = \{\mathcal{H}_1, \cdots, \mathcal{H}_Q\}$;

$$P_{\rm avg} = \sum_{q=1}^{Q} {\rm tr} \boldsymbol{\rho}_q \Pr \left[\mathbf{H}_{\rm R} \in \mathcal{H}_q \right].$$

where $\boldsymbol{\rho}_q \succeq 0$, $q = \{1, \cdots, Q\}$ and λ is the Lagrange multiplier. We need to find the optimal $\{\mathcal{H}_1, \cdots, \mathcal{H}_Q\}$ and $\{\boldsymbol{\rho}_1, \cdots, \boldsymbol{\rho}_Q\}$ that minimizes the average distortion measure

$$\Delta = \sum_{q=1}^{Q} \underset{\mathbf{H}_{\rm E} | \mathbf{H}_{\rm R} \in \mathcal{H}_q}{\mathbb{E}} \left[\delta \left(\mathbf{T}_q, \mathbf{H}_{\rm E}, \boldsymbol{\rho}_q \right) \right] P_q, \tag{6.23}$$

where $\mathbf{T}_q = \underset{\mathbf{H}_{\rm R} \in \mathcal{H}_q}{\arg\min} \left| \mathbf{I}_{N_{\rm R}} + \frac{1}{\sigma_{\rm R}^2} \mathbf{H}_{\rm R} \boldsymbol{\rho}_q \mathbf{H}_{\rm R}^{*} \right|$.

To solve this optimization problem, we use Lloyd's algorithm [19]. The OFT for the achievable secrecy rate $\mathcal{C}_{\rm s}^{-}$ is given in Algo.2.

6.4 Secrecy Capacity Analysis

In this section, we establish the lower and the upper bounds on the ergodic secrecy capacity presented in Theorem 6.1 and Theorem 6.2, respectively.

6.4.1 Proof of Achievability in Theorem 6.1

6.4.1.1 Proof of the Lower Bound $\mathcal{C}_{\mathbf{s}}^{-}$

Given a partition of the channel gain space $\{\mathcal{H}_1, \cdots, \mathcal{H}_Q\}$ and a transmission strategy $\{\boldsymbol{\rho}_1, \cdots, \boldsymbol{\rho}_Q\}$, let $\mathbf{T}_q$, $q \in \{1, \cdots, Q\}$, be the element of $\mathcal{H}_q$ that minimizes the function $\xi(\mathbf{H}_{\mathrm{R}}) = \left|\mathbf{I}_{N_{\mathrm{R}}} + \frac{1}{\sigma_{\mathrm{R}}^2}\mathbf{H}_{\mathrm{R}}\boldsymbol{\rho}_q\mathbf{H}_{\mathrm{R}}^*\right|$, i.e.,

$$\left|\mathbf{I}_{N_{\mathrm{R}}} + \frac{1}{\sigma_{\mathrm{R}}^2}\mathbf{T}_q\boldsymbol{\rho}_q\mathbf{T}_q^*\right| \leq \left|\mathbf{I}_{N_{\mathrm{R}}} + \frac{1}{\sigma_{\mathrm{R}}^2}\mathbf{H}_{\mathrm{R}}\boldsymbol{\rho}_q\mathbf{H}_{\mathrm{R}}^*\right|, \text{ for all } \mathbf{H}_{\mathrm{R}} \in \mathcal{H}_q. \tag{6.24}$$

We note that such a minimum exists since the function $\xi(\mathbf{H}_{\mathrm{R}})$ is logarithmically concave in $\mathbf{H}_{\mathrm{R}}$, and $\mathcal{H}_q$ corresponds to a Voronoi region which is by definition a convex set [147]. We assume that the rates

$$R_q = \log\left|\mathbf{I}_{N_{\mathrm{R}}} + \frac{1}{\sigma_{\mathrm{R}}^2}\mathbf{T}_q\boldsymbol{\rho}_q\mathbf{T}_q^*\right|, q \in \{1, \cdots, Q\}, \tag{6.25}$$

are selected in advance. We need to prove that the rate

$$R_{\mathrm{s}}^{-} = \sum_{q=1}^{Q} P_q \underset{\mathbf{H}_{\mathrm{E}}|\mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q}{\mathbb{E}}\left[\left\{R_q - \log\left|\mathbf{I}_{N_{\mathrm{E}}} + \frac{1}{\sigma_{\mathrm{E}}^2}\mathbf{H}_{\mathrm{E}}\boldsymbol{\rho}_q\mathbf{H}_{\mathrm{E}}^*\right|\right\}^{+}\right] - \epsilon_1, \tag{6.26}$$

is achievable. Let

$$R_{\mathrm{e}} = \sum_{q=1}^{Q} P_q \underset{\mathbf{H}_{\mathrm{E}}|\mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q}{\mathbb{E}}\left[\log\left|\mathbf{I}_{N_{\mathrm{E}}} + \frac{1}{\sigma_{\mathrm{E}}^2}\mathbf{H}_{\mathrm{E}}\boldsymbol{\rho}_q\mathbf{H}_{\mathrm{E}}^*\right|\right] - \epsilon_2. \tag{6.27}$$

The considered wiretap codebook is generated by uniformly and randomly partitioning the 2^{nR_m} length n sequences into $2^{nR_{\mathrm{s}}^{-}}$ bins; each containing $2^{nR_{\mathrm{e}}}$ codewords, where $R_m = \sum_{q=1}^{Q} P_q R_q - \epsilon$. That is, to transmit a message W, the transmitter selects the corresponding bin and then randomly chooses a binary sequence among all the uniformly distributed codewords in the selected bin. During each fading block, of

length κ, the transmitter sends κR_q information bits using the generated Gaussian codebook. Then, using the weak law of large numbers, when the number of spanned fading blocks L is large, the entire binary sequence is transmitted with high probability. Also, since $R_q \leq \log\left|\mathbf{I}_{N_\mathrm{R}} + \mathbf{H}_\mathrm{R}\boldsymbol{\rho}_q\mathbf{H}_\mathrm{R}^*\right|$ is valid for all fading blocks, the receiver can decode the transmitted signal with a negligible probability of error.

For the secrecy analysis, we need to prove that the equivocation rate R_e satisfies $R_\mathrm{e} \geq R_\mathrm{s}^- - \epsilon$. We have

$$nR_\mathrm{e} = H(W|\mathbf{Y}_\mathrm{E}^n, \mathbf{H}_\mathrm{E}^L, \mathbf{H}_\mathrm{R}^L, U^L) \tag{6.28}$$

$$\geq I(W; \mathbf{X}^n|\mathbf{Y}_\mathrm{E}^n, \mathbf{H}_\mathrm{E}^L, \mathbf{H}_\mathrm{R}^L, U^L) \tag{6.29}$$

$$= H(\mathbf{X}^n|\mathbf{Y}_\mathrm{E}^n, \mathbf{H}_\mathrm{E}^L, \mathbf{H}_\mathrm{R}^L, U^L) - H(\mathbf{X}^n|\mathbf{Y}_\mathrm{E}^n, \mathbf{H}_\mathrm{E}^L, \mathbf{H}_\mathrm{R}^L, U^L, W). \tag{6.30}$$

On one hand, we can write

$$H(\mathbf{X}^n|\mathbf{Y}_\mathrm{E}^n, \mathbf{H}_\mathrm{E}^L, \mathbf{H}_\mathrm{R}^L, U^L) = \sum_{l=1}^{L} H(X^\kappa(l)|\mathbf{Y}_\mathrm{E}^\kappa(l), \mathbf{H}_\mathrm{E}(l), \mathbf{H}_\mathrm{R}(l), U(l)) \tag{6.31}$$

$$\geq \sum_{l\in\mathcal{S}_L} H(X^\kappa(l)|\mathbf{Y}_\mathrm{E}^\kappa(l), \mathbf{H}_\mathrm{E}(l), \mathbf{H}_\mathrm{R}(l), U(l)) \tag{6.32}$$

$$\geq \sum_{l\in\mathcal{S}_L} \kappa\left(\sum_{q=1}^{Q} P_q\left(R_q - \log\left|\mathbf{I}_{N_\mathrm{E}} + \frac{1}{\sigma_\mathrm{E}^2}\mathbf{H}_\mathrm{E}(l)\boldsymbol{\rho}_q\mathbf{H}_\mathrm{E}^*(l)\right|\right) - \epsilon'\right) \tag{6.33}$$

$$= \sum_{l=1}^{L} \kappa\left(\sum_{q=1}^{Q} P_q\left\{R_q - \log\left|\mathbf{I}_{N_\mathrm{E}} + \frac{1}{\sigma_\mathrm{E}^2}\mathbf{H}_\mathrm{E}(l)\boldsymbol{\rho}_q\mathbf{H}_\mathrm{E}^*(l)\right|\right\}^+ - \epsilon'\right) \tag{6.34}$$

$$= n\sum_{q=1}^{Q} P_q \underset{\mathbf{H}_\mathrm{E}|\mathbf{H}_\mathrm{R}\in\mathcal{H}_q}{\mathbb{E}}\left[\left\{R_q - \log\left|\mathbf{I}_{N_\mathrm{E}} + \frac{1}{\sigma_\mathrm{E}^2}\mathbf{H}_\mathrm{E}\boldsymbol{\rho}_q\mathbf{H}_\mathrm{E}^*\right|\right\}^+\right] - n\epsilon' \tag{6.35}$$

$$= nR_\mathrm{s}^- - n\epsilon', \tag{6.36}$$

where (6.31) results from the memoryless property of the channel and the independence of the $X^\kappa(l)$'s, (6.32) is obtained by removing all the terms corresponding to the fading blocks $l \notin \mathcal{S}_L$, with $\mathcal{S}_L = \{l \in \{1, \cdots, L\} : \mathbf{T}_q(l) > \mathbf{H}_\mathrm{E}(l)\}$, and (6.35) follows from the ergodicity of the channel as $L \to \infty$.

On the other hand, using list decoding argument at the eavesdropper side and

applying Fano's inequality [28], $\frac{1}{n}H(\mathbf{X}^n|\mathbf{Y}_{\mathrm{E}}^n, \mathbf{H}_{\mathrm{E}}^L, U^L, W)$ vanishes as $n \to \infty$ and we can write

$$H(\mathbf{X}^n|\mathbf{Y}_{\mathrm{E}}^n, \mathbf{H}_{\mathrm{E}}^L, \mathbf{H}_{\mathrm{R}}^L, W) \leq n\epsilon''. \tag{6.37}$$

Substituting (6.36) and (6.37) in (6.30), we get $R_{\mathrm{e}} \geq R_{\mathrm{s}}^- - \epsilon$, with $\epsilon = \epsilon' + \epsilon''$, and ϵ' and ϵ'' are selected to be arbitrarily small. Maximizing over the main channel gain partition regions $\mathcal{H}_q$ and the associated transmission strategies $\boldsymbol{\rho}_q$, for each $q \in \{1, \cdots, Q\}$, concludes the proof. □

6.4.1.2 Proof of the Lower Bound $\widetilde{\mathcal{C}}_{\mathbf{s}}^-$

In the proposed communication system, the transmitter uses the fed back partition index to select the optimal beamforming and power control matrices for the forward transmission. This could be seen as a deterministic mapping that associates each feedback index u_q with a beamforming matrix $\mathbf{V}_q$ and a power control matrix $\mathbf{\Lambda}_q$. The adopted system model, illustrated in Fig. 6.1, can then be equivalently modeled by the block diagram in Fig. 6.2. That is, the original adaptive encoding function, which produces symbol X from message W using the feedback information U, is replaced by an encoding entity and a deterministic mapping function, φ, that becomes part of the channel.

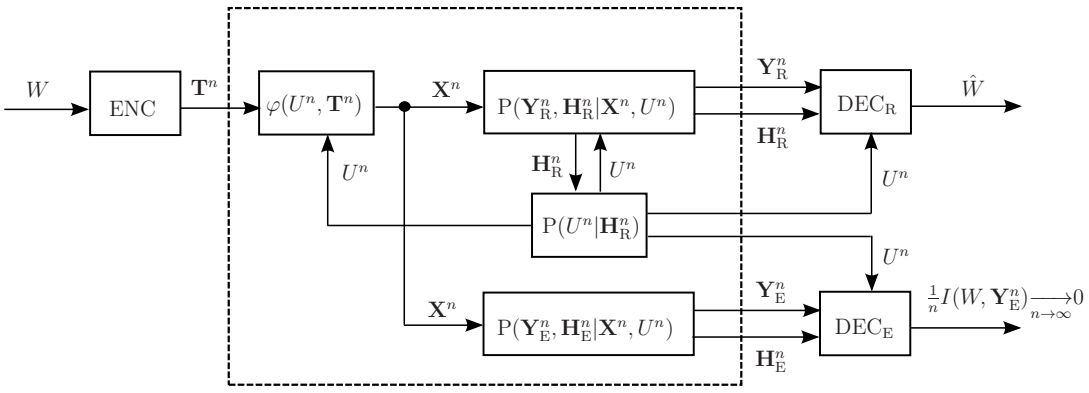


Figure 6.2: Equivalent channel model of the communication system with input $\mathbf{T}^n$ and outputs $\mathbf{Y}_{\mathrm{R}}^n$ and $\mathbf{H}_{\mathrm{R}}^n$, at the legitimate receiver, and $\mathbf{Y}_{\mathrm{E}}^n$ and $\mathbf{H}_{\mathrm{E}}^n$, at the eavesdropper.

The new encoder is independent of U and uses a wiretap codebook to construct the new channel input alphabet $\mathbf{T}$ from message W, whereas the mapping function f adapts the transmission of signal $\mathbf{T}$ using U, i.e., $\varphi(u_q, \mathbf{T}) = \mathbf{V}_q \mathbf{\Lambda}_q \mathbf{T}$. The equivalent channel model becomes a multiple-antenna memoryless channel without feedback, with input $\mathbf{T}$ and outputs $(\mathbf{Y}_{\mathrm{R}}, \mathbf{H}_{\mathrm{R}}, U)$ at the legitimate receiver, and $(\mathbf{Y}_{\mathrm{E}}, \mathbf{H}_{\mathrm{E}}, U)$ at the eavesdropper. Thus, using [148, Proposition 2] and [25, Corollary 2], the following secrecy rate is achievable

$$\widetilde{R}_{\mathrm{s}}^{-} = I(\mathbf{T}; \mathbf{Y}_{\mathrm{R}} | \mathbf{H}_{\mathrm{R}}, U) - I(\mathbf{T}; \mathbf{Y}_{\mathrm{E}} | \mathbf{H}_{\mathrm{E}}, U). \tag{6.38}$$

Now, since $I(\mathbf{T}; \mathbf{Y}_{\mathrm{R}} | \mathbf{H}_{\mathrm{R}}, U)$ can be expressed as

$$I(\mathbf{T}; \mathbf{Y}_{\mathrm{R}} | \mathbf{H}_{\mathrm{R}}, U) = \sum_{q=1}^{Q} \mathop{\mathbb{E}}_{\mathbf{H}_{\mathrm{R}} \in \mathcal{H}_q} \left[I(\mathbf{T}; \mathbf{Y}_{\mathrm{R}} | \mathbf{H}_{\mathrm{R}}, u_q) \right] P_q, \tag{6.39}$$

and $I(\mathbf{T}; \mathbf{Y}_{\mathrm{E}} | \mathbf{H}_{\mathrm{E}}, U)$ can be expressed similarly, then, taking $\mathbf{T} \sim \mathcal{CN}(0, \mathbf{I}_{N_{\mathrm{T}}})$, the achievable secrecy rate R_{s}^{-} can be rewritten as

$$\widetilde{R}_{\mathrm{s}}^{-} = \sum_{q=1}^{Q} \left(\mathop{\mathbb{E}}_{\mathbf{H}_{\mathrm{E}}, \mathbf{H}_{\mathrm{R}} | \mathbf{H}_{\mathrm{R}} \in \mathcal{H}_q} \left[\log \left| \mathbf{I}_{N_{\mathrm{R}}} + \frac{1}{\sigma_{\mathrm{R}}^2} \mathbf{H}_{\mathrm{R}} \boldsymbol{\rho}_q \mathbf{H}_{\mathrm{R}}^{*} \right| - \log \left| \mathbf{I}_{N_{\mathrm{E}}} + \frac{1}{\sigma_{\mathrm{E}}^2} \mathbf{H}_{\mathrm{E}} \boldsymbol{\rho}_q \mathbf{H}_{\mathrm{E}}^{*} \right| \right] \right) P_q.$$

Then, maximizing over the main channel gain partition regions $\mathcal{H}_q$ and the associated transmission strategies $\boldsymbol{\rho}_q$, for each $q \in \{1, \cdots, Q\}$, concludes the proof. $\square$

It is clear that the main difference between the two schemes is that, in the first scheme, we adapt both the rate and the power whereas, in the second scheme, we only adapt the power.

6.4.2 Proof of the Upper Bound in Theorem 6.2

Let R_{E} be the equivocation rate at the eavesdropper. We recall that $n{=}\kappa L$, with L being the total number of spanned fading blocks and κ the length of each fading block. We have

$$nR_{\mathrm{E}} = H(W | \mathbf{Y}_{\mathrm{E}}^{n}, \mathbf{H}_{\mathrm{E}}^{L}, \mathbf{H}_{\mathrm{R}}^{L}, U^{L}) \tag{6.40}$$

$$= I(W;\mathbf{Y}_{\mathrm{R}}^n|\mathbf{Y}_{\mathrm{E}}^n,\mathbf{H}_{\mathrm{E}}^L,\mathbf{H}_{\mathrm{R}}^L,U^L)+H(W|\mathbf{Y}_{\mathrm{R}}^n,\mathbf{Y}_{\mathrm{E}}^n,\mathbf{H}_{\mathrm{E}}^L,\mathbf{H}_{\mathrm{R}}^L,U^L) \tag{6.41}$$

$$\leq I(W;\mathbf{Y}_{\mathrm{R}}^n|\mathbf{Y}_{\mathrm{E}}^n,\mathbf{H}_{\mathrm{E}}^L,\mathbf{H}_{\mathrm{R}}^L,U^L)+n\epsilon \tag{6.42}$$

$$= \sum_{l=1}^{L}\sum_{k=1}^{\kappa} I(W;\mathbf{Y}_{\mathrm{R}}(l,k)|\mathbf{Y}_{\mathrm{E}}^n\mathbf{H}_{\mathrm{E}}^L\mathbf{H}_{\mathrm{R}}^L,U^L,\mathbf{Y}_{\mathrm{R}}^{\kappa(l-1)+(k-1)})+n\epsilon \tag{6.43}$$

$$\begin{aligned}= &\sum_{l=1}^{L}\sum_{k=1}^{\kappa} H(\mathbf{Y}_{\mathrm{R}}(l,k)|\mathbf{Y}_{\mathrm{E}}^n,\mathbf{H}_{\mathrm{E}}^L,\mathbf{H}_{\mathrm{R}}^L,U^L,\mathbf{Y}_{\mathrm{R}}^{\kappa(l-1)+(k-1)}) \\ &- H(\mathbf{Y}_{\mathrm{R}}(l,k)|W,\mathbf{Y}_{\mathrm{E}}^n,\mathbf{H}_{\mathrm{E}}^L,\mathbf{H}_{\mathrm{R}}^L,U^L,\mathbf{Y}_{\mathrm{R}}^{\kappa(l-1)+(k-1)})+n\epsilon\end{aligned} \tag{6.44}$$

$$\begin{aligned}\leq &\sum_{l=1}^{L}\sum_{k=1}^{\kappa} H(\mathbf{Y}_{\mathrm{R}}(l,k)|\mathbf{Y}_{\mathrm{E}}(l,k),\mathbf{H}_{\mathrm{E}}(l),\mathbf{H}_{\mathrm{R}}(l),U^l) \\ &- H(\mathbf{Y}_{\mathrm{R}}(l,k)|W,X(l,k),\mathbf{Y}_{\mathrm{E}}^n,\mathbf{H}_{\mathrm{E}}^L\mathbf{H}_{\mathrm{R}}^L U^L,\mathbf{Y}_{\mathrm{R}}^{\kappa(l-1)+(k-1)})+n\epsilon\end{aligned} \tag{6.45}$$

$$\begin{aligned}= &\sum_{l=1}^{L}\sum_{k=1}^{\kappa} H(\mathbf{Y}_{\mathrm{R}}(l,k)|\mathbf{Y}_{\mathrm{E}}(l,k),\mathbf{H}_{\mathrm{E}}(l),\mathbf{H}_{\mathrm{R}}(l),U^l) \\ &- H(\mathbf{Y}_{\mathrm{R}}(l,k)|X(l,k),\mathbf{Y}_{\mathrm{E}}(l,k),\mathbf{H}_{\mathrm{E}}(l),\mathbf{H}_{\mathrm{R}}(l),U^l)+n\epsilon\end{aligned} \tag{6.46}$$

$$= \sum_{l=1}^{L}\sum_{k=1}^{\kappa} I(X(l,k);\mathbf{Y}_{\mathrm{R}}(l,k)|\mathbf{Y}_{\mathrm{E}}(l,k),\mathbf{H}_{\mathrm{E}}(l),\mathbf{H}_{\mathrm{R}}(l),U^l)+n\epsilon \tag{6.47}$$

$$\leq \sum_{l=1}^{L}\sum_{k=1}^{\kappa} \mathop{\mathbb{E}}_{\substack{\omega_l,\mathbf{H}_{\mathrm{R}}(l)\\ \mathbf{H}_{\mathrm{E}}(l),}} \left[\left\{\log\frac{|\mathbf{I}_{N_{\mathrm{R}}}+\frac{1}{\sigma_{\mathrm{R}}^2}\mathbf{H}_{\mathrm{R}}(l)\omega_l(U^l)\mathbf{H}_{\mathrm{R}}^*(l)|}{|\mathbf{I}_{N_{\mathrm{E}}}+\frac{1}{\sigma_{\mathrm{E}}^2}\mathbf{H}_{\mathrm{E}}(l)\omega_l(U^l)\mathbf{H}_{\mathrm{E}}^*(l)|}\right\}^+\right]+n\epsilon \tag{6.48}$$

where (6.42) comes from Fano's inequality, (6.45) follows since conditioning reduces the entropy, and (6.48) holds true since given $\mathbf{H}_{\mathrm{R}}(l)$ and $\mathbf{H}_{\mathrm{E}}(l)$, the channel at hand is a multiple antenna wiretap channel and, hence, the bound in (6.47) is tight if $\mathbf{X}^n$ is a sequence with zero-mean Gaussian components $X(l,k)$, statistically independent conditionally on U^L, i.e., $X(l,k)\sim\mathcal{CN}\left(0,\omega_l^{1/2}(U^l)\right)$, with the power policy $\omega_l(U^l)$ satisfying the average power constraint.

Since the channel gains and the feedback information are constant during each fading block, we can write

$$nR_{\mathrm{E}} \leq \sum_{l=1}^{L}\kappa \mathop{\mathbb{E}}_{\substack{\omega_l,\mathbf{H}_{\mathrm{R}}(l)\\ \mathbf{H}_{\mathrm{E}}(l),}} \left[\left\{\log\frac{|\mathbf{I}_{N_{\mathrm{R}}}+\frac{1}{\sigma_{\mathrm{R}}^2}\mathbf{H}_{\mathrm{R}}(l)\omega_l(U^l)\mathbf{H}_{\mathrm{R}}^*(l)|}{|\mathbf{I}_{N_{\mathrm{E}}}+\frac{1}{\sigma_{\mathrm{E}}^2}\mathbf{H}_{\mathrm{E}}(l)\omega_l(U^l)\mathbf{H}_{\mathrm{E}}^*(l)|}\right\}^+\right]+n\epsilon \tag{6.49}$$

$$= \sum_{l=1}^{L} \kappa \underset{\substack{\omega_l, \\ \mathbf{H}_{\mathrm{R}}(l), \\ \mathbf{H}_{\mathrm{E}}(l)}}{\mathbb{E}} \left[\mathbb{E} \left[\left\{ \log \frac{|\mathbf{I}_{N_{\mathrm{R}}} + \frac{1}{\sigma_{\mathrm{R}}^2} \mathbf{H}_{\mathrm{R}}(l) \omega_l(U^l) \mathbf{H}_{\mathrm{R}}^*(l)|}{|\mathbf{I}_{N_{\mathrm{E}}} + \frac{1}{\sigma_{\mathrm{E}}^2} \mathbf{H}_{\mathrm{E}}(l) \omega_l(U^l) \mathbf{H}_{\mathrm{E}}^*(l)|} \right\}^+ \middle| U(l), \mathbf{H}_{\mathrm{R}}(l), \mathbf{H}_{\mathrm{E}}(l) \right] \right] + n\epsilon \quad (6.50)$$

$$\leq \sum_{l=1}^{L} \kappa \underset{\substack{\omega_l, \\ \mathbf{H}_{\mathrm{R}}(l), \\ \mathbf{H}_{\mathrm{E}}(l)}}{\mathbb{E}} \left[\left\{ \log \frac{|\mathbf{I}_{N_{\mathrm{R}}} + \frac{1}{\sigma_{\mathrm{R}}^2} \mathbf{H}_{\mathrm{R}}(l) \mathbb{E}[\omega_l(U^l)|U(l), \mathbf{H}_{\mathrm{R}}(l), \mathbf{H}_{\mathrm{E}}(l)] \, \mathbf{H}_{\mathrm{R}}^*(l)|}{|\mathbf{I}_{N_{\mathrm{E}}} + \frac{1}{\sigma_{\mathrm{E}}^2} \mathbf{H}_{\mathrm{E}}(l) \mathbb{E}[\omega_l(U^l)|U(l), \mathbf{H}_{\mathrm{R}}(l), \mathbf{H}_{\mathrm{E}}(l)] \, \mathbf{H}_{\mathrm{E}}^*(l)|} \right\}^+ \right] + n\epsilon \quad (6.51)$$

$$= \sum_{l=1}^{L} \kappa \underset{\substack{\Omega_l, \\ \mathbf{H}_{\mathrm{R}}(l), \\ \mathbf{H}_{\mathrm{E}}(l)}}{\mathbb{E}} \left[\left\{ \log \frac{|\mathbf{I}_{N_{\mathrm{R}}} + \frac{1}{\sigma_{\mathrm{R}}^2} \mathbf{H}_{\mathrm{R}}(l) \Omega_l(U(l)) \mathbf{H}_{\mathrm{R}}^*(l)|}{|\mathbf{I}_{N_{\mathrm{E}}} + \frac{1}{\sigma_{\mathrm{E}}^2} \mathbf{H}_{\mathrm{E}}(l) \Omega_l(U(l)) \mathbf{H}_{\mathrm{E}}^*(l)|} \right\}^+ \right] + n\epsilon \quad (6.52)$$

$$= \sum_{l=1}^{L} \kappa \underset{\Omega_l, \mathbf{H}_{\mathrm{R}}, \mathbf{H}_{\mathrm{E}}}{\mathbb{E}} \left[\left\{ \log \frac{|\mathbf{I}_{N_{\mathrm{R}}} + \frac{1}{\sigma_{\mathrm{R}}^2} \mathbf{H}_{\mathrm{R}} \Omega_l(U) \mathbf{H}_{\mathrm{R}}^*|}{|\mathbf{I}_{N_{\mathrm{E}}} + \frac{1}{\sigma_{\mathrm{E}}^2} \mathbf{H}_{\mathrm{E}} \Omega_l(U) \mathbf{H}_{\mathrm{E}}^*|} \right\}^+ \right] + n\epsilon, \quad (6.53)$$

where (6.51) results from Jensen's inequality since the function $X \rightarrow \left\{ \log \frac{|\mathbf{I} + \mathbf{A}\mathbf{X}\mathbf{A}^*|}{|\mathbf{I} + \mathbf{B}\mathbf{X}\mathbf{B}^*|} \right\}^+$ is concave over the set of nonnegative definite matrices, $\Omega_l(U(l))$ in (6.52) is defined as $\Omega_l(U(l)) = \mathbb{E}\left[\omega_l(U^l)|U(l)\right]$, since given $U(l)$, U^l is independent of $\mathbf{H}_{\mathrm{R}}(l)$ and $\mathbf{H}_{\mathrm{E}}(l)$, and where (6.53) follows from the ergodicity and the stationarity of the channel gains. Thus, we have

$$R_{\mathrm{E}} \leq \frac{1}{L} \sum_{l=1}^{L} \underset{\Omega_l, \mathbf{H}_{\mathrm{R}}, \mathbf{H}_{\mathrm{E}}}{\mathbb{E}} \left[\left\{ \log \frac{|\mathbf{I}_{N_{\mathrm{R}}} + \frac{1}{\sigma_{\mathrm{R}}^2} \mathbf{H}_{\mathrm{R}} \Omega_l(U) \mathbf{H}_{\mathrm{R}}^*|}{|\mathbf{I}_{N_{\mathrm{E}}} + \frac{1}{\sigma_{\mathrm{E}}^2} \mathbf{H}_{\mathrm{E}} \Omega_l(U) \mathbf{H}_{\mathrm{E}}^*|} \right\}^+ \right] + \epsilon \quad (6.54)$$

$$\leq \underset{\Omega_l, \mathbf{H}_{\mathrm{R}}, \mathbf{H}_{\mathrm{E}}}{\mathbb{E}} \left[\left\{ \log \frac{\left| \mathbf{I}_{N_{\mathrm{R}}} + \frac{1}{\sigma_{\mathrm{R}}^2} \mathbf{H}_{\mathrm{R}} \frac{1}{L} \sum_{l=1}^{L} \Omega_l(U) \mathbf{H}_{\mathrm{R}}^* \right|}{\left| \mathbf{I}_{N_{\mathrm{E}}} + \frac{1}{\sigma_{\mathrm{E}}^2} \mathbf{H}_{\mathrm{E}} \frac{1}{L} \sum_{l=1}^{L} \Omega_l(U) \mathbf{H}_{\mathrm{E}}^* \right|} \right\}^+ \right] + \epsilon \quad (6.55)$$

$$= \underset{\Omega, \mathbf{H}_{\mathrm{R}}, \mathbf{H}_{\mathrm{E}}}{\mathbb{E}} \left[\left\{ \log \frac{|\mathbf{I}_{N_{\mathrm{R}}} + \frac{1}{\sigma_{\mathrm{R}}^2} \mathbf{H}_{\mathrm{R}} \Omega(U) \mathbf{H}_{\mathrm{R}}^*|}{|\mathbf{I}_{N_{\mathrm{E}}} + \frac{1}{\sigma_{\mathrm{E}}^2} \mathbf{H}_{\mathrm{E}} \Omega(U) \mathbf{H}_{\mathrm{E}}^*|} \right\}^+ \right] + \epsilon, \quad (6.56)$$

where (6.55) comes from applying Jensen's inequality once again, and where $\Omega(U)$ in (6.56) is defined as $\Omega(U) = \sum_{l=1}^{L} \Omega_l(U)$. Maximizing over the main channel gain partition regions $\mathcal{H}_q$ and the associated transmission strategies $\boldsymbol{\rho}_q$, for each $q \in \{1, \cdots, Q\}$, concludes the proof. $\square$

6.5 Simulation Results

In this section, we provide selected simulation results for the illustrative case of independent and identically distributed Rayleigh fading channels. We consider that the system's variables, the entries of the main channel gain matrix $\mathbf{H}_{\mathrm{R}}$ and the eavesdropper's channel gain matrix $\mathbf{H}_{\mathrm{E}}$, are all drawn from the zero-mean, unit-variance Gaussian distribution.

Figure 6.3 and Figure 6.4 illustrate the achievable secrecy rates $\mathcal{C}_{\mathrm{s}}^{-}$ and $\widetilde{\mathcal{C}}_{\mathrm{s}}^{-}$, in nats per channel use (npcu), when the transmitter and the legitimate receiver have two antennas each, i.e. N_{T}=N_{R}=2. The eavesdropper is equipped with one antenna in Figure 6.3, i.e., N_{E}=1, and with two antennas in Figure 6.4, i.e., N_{E}=2. The upper bound $\mathcal{C}_{\mathrm{s}}^{+}$ and the ergodic secrecy capacity $\mathcal{C}_{\mathrm{s}}$, from Corollary 1, are also presented in both figures. On one hand, we can see, from both figures, that as the capacity of the feedback link grows, i.e., the number of bits B increases, the achievable secrecy rate $\mathcal{C}_{\mathrm{s}}^{-}$ grows toward the secrecy capacity $\mathcal{C}_{\mathrm{s}}$. On the other hand, we can observe that the secrecy rate $\widetilde{\mathcal{C}}_{\mathrm{s}}^{-}$, in Figure 6.3, is almost comparable to the secrecy rate $\mathcal{C}_{\mathrm{s}}^{-}$ with 12 bits CSI feedback; while, in Figure 6.4, $\widetilde{\mathcal{C}}_{\mathrm{s}}^{-}$ is very low even compared to $\mathcal{C}_{\mathrm{s}}^{-}$ with 4 bits CSI feedback. We should mention that, in both figures, we illustrate the achievable secrecy rate $\widetilde{\mathcal{C}}_{s}^{-}$ only for the case when $B = 4$. The reason behind this is that, through the conducted simulations, we noticed that increasing the number of feedback bits has a limited impact on $\widetilde{\mathcal{C}}_{s}^{-}$ compared to $\mathcal{C}_{s}^{-}$. Indeed, increasing B only results in a slight improvement of $\widetilde{\mathcal{C}}_{s}^{-}$, and only at very low SNR values where the achieved secrecy rates are small, making this improvement insignificant. The secrecy rate $\widetilde{\mathcal{C}}_{\mathrm{s}}^{-}$ is more convenient when the number of antennas at the eavesdropper is less than the number of antennas at the legitimate receiver, and the number of CSI feedback bits is small, which is in perfect agreement with Corollary 4 and Remark 1.

In Figure 6.5, the achievable secrecy rate $\mathcal{C}_{\mathrm{s}}^{-}$ is presented along with the secrecy capacity $\mathcal{C}_{\mathrm{s}}$ when both the transmitter and the legitimate receiver have two antennas

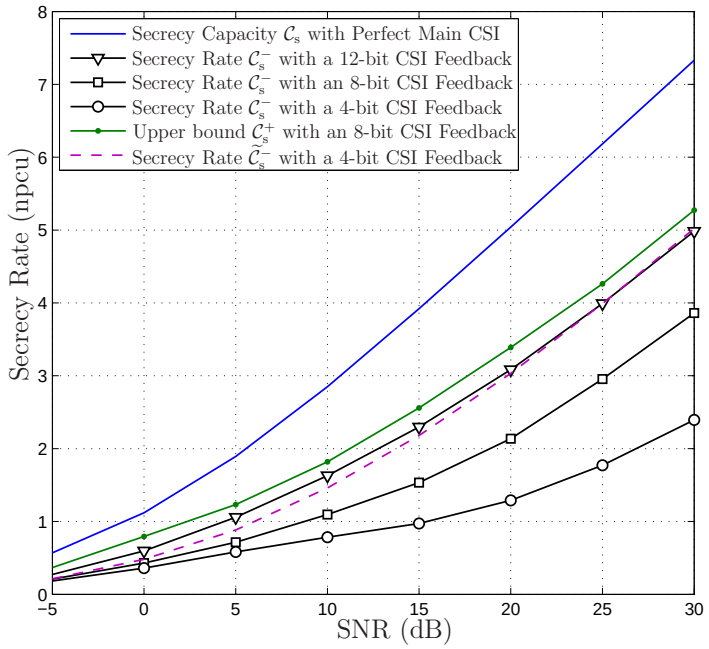


Figure 6.3: Achievable secrecy rates for Rayleigh fading channels with N_{T}=N_{R}=2, N_{E}=1 and various B-bit CSI feedback, B=4, 8, 12.

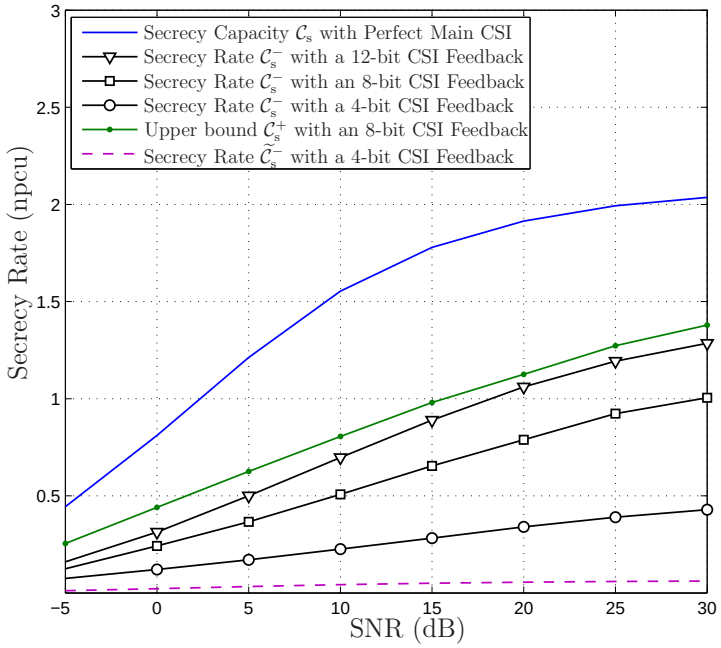


Figure 6.4: Achievable secrecy rates with N_{T}=N_{R}=N_{E}=2 and various B-bit CSI feedback, B=4, 8, 12.

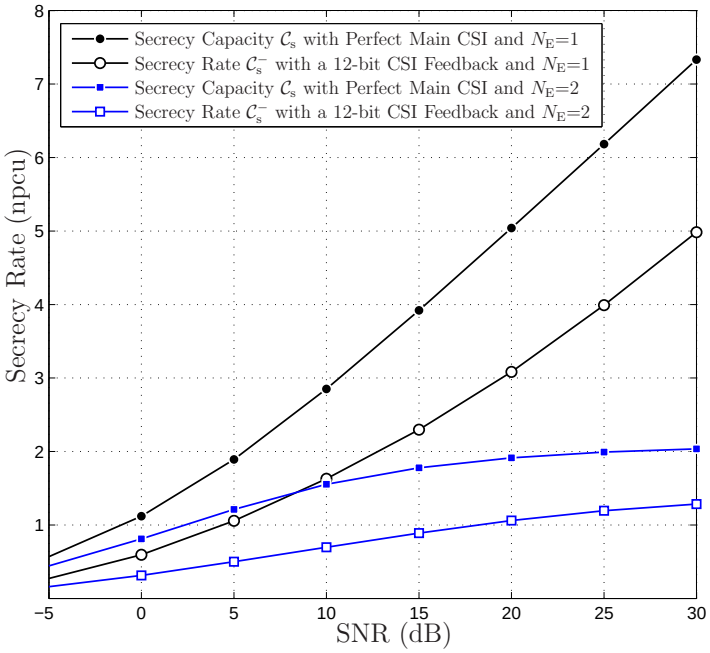


Figure 6.5: Comparison of the achievable secrecy rates when the eavesdropper has one and two antennas with N_T=N_R=2 and 12 bits feedback.

each, i.e. N_T=N_R=2, and twelve bits are used for CSI feedback, i.e. B=12. The figure compares the cases when the eavesdropper has only one antenna, i.e. N_E=1 and when he has two antennas, i.e. N_E=2. As expected, the secrecy rate is higher when the eavesdropper has fewer antennas compared to the transmitter and the legitimate user.

The effect of changing the number of antennas, at the legitimate receiver, is illustrated in Figure 6.6 when 8 bits are used for CSI feedback, N_T=2, N_E=1, and N_R varies between one and four antennas. Clearly, we can see that as we augment the number of antennas at the legitimate receiver, the achievable secrecy rate $\mathcal{C}_s^-$ increases. Also, we can notice that when the legitimate receiver has an equal number of antennas as the eavesdropper, N_R=N_E=1 in this case, the achievable secrecy rate is very low compared to when the legitimate receiver has more antennas.

In Figure 6.7, the achievable secrecy rate $\mathcal{C}_s^-$ is presented along with the secrecy capacity $\mathcal{C}_s$ when 8 bits are used for CSI feedback, N_R=2, and N_E=1. The figure compares the cases when the transmitter has one antenna, N_T=1, two antennas,

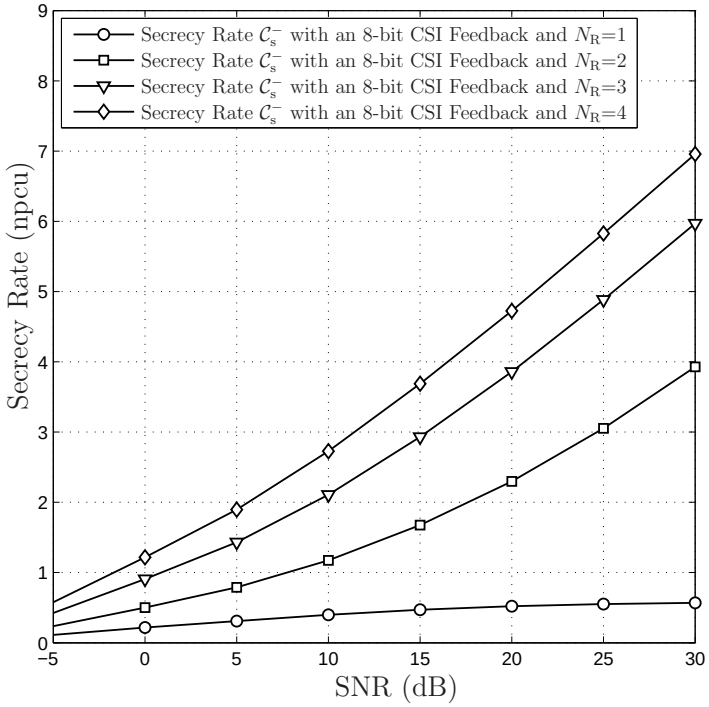


Figure 6.6: Achievable secrecy rate with N_{T}=2, N_{E}=1, 8 bits feedback, and different values for the number of antennas at the legitimate receiver, N_{R}=1, 2, 3, 4.

N_{T}=2, and four antennas, N_{T}=4. We can see that the secrecy throughput increases as the number of antennas at the transmitter augments. Also, we can see that the bounds are very tight when N_{T}=1 as the size of the main channel gain matrix is small compared to the other cases, i.e., $\mathbf{H}_{\mathrm{R}}$ is a 2 by 1 matrix in this case. An 8-bit CSI feedback almost achieves the secrecy capacity with perfect main CSI when N_{T}=1, N_{R}=2, and N_{E}=1.

Figure 6.8 illustrates the asymptotic analysis, in the high SNR regime, when the transmitter and the legitimate receiver has two antennas, i.e., N_{T}=N_{R}=2, and the eavesdropper is equipped with one antenna, i.e., N_{E}=1. The respective asymptotic curves representing the achievable secrecy rate $\mathcal{C}_{\mathrm{s}}^-$ and the secrecy capacity $\mathcal{C}_{\mathrm{s}}$ approach, very tightly, the exact curves. Besides, the asymptotic curve of the achievable secrecy rate $\widetilde{\mathcal{C}}_{\mathrm{s}}^-$ coincides perfectly with the exact curve.

A comparison between our achievable secrecy rates $\mathcal{C}_s^-$ and $\widetilde{\mathcal{C}}_s^-$, and the achiev-

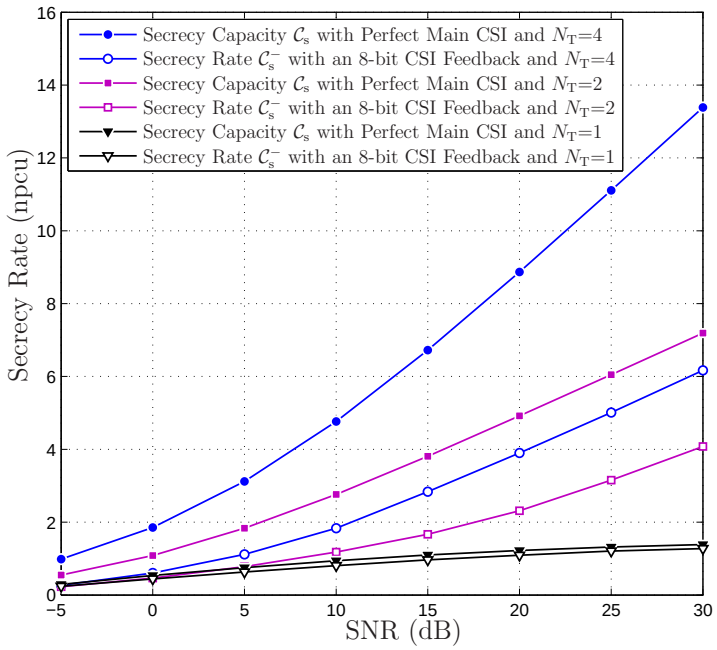


Figure 6.7: Comparison of the achievable secrecy rates when the transmitter has one, two, and four antennas with N_R=2, N_E=1 and 8 bits feedback.

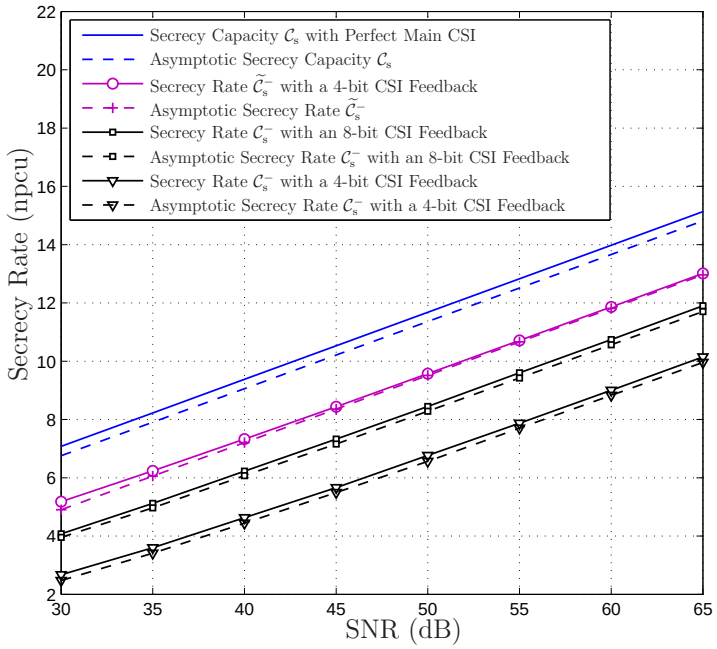


Figure 6.8: Asymptotic secrecy rates for Rayleigh fading channels with N_T=N_R=2, N_E=1 and two values for the number of CSI feedback bites, B=4 and B=8.

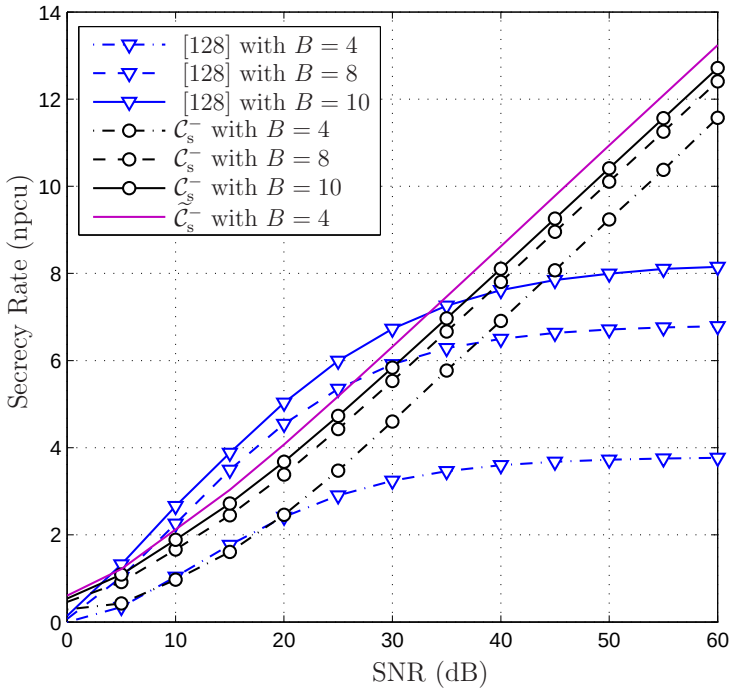


Figure 6.9: Achievable secrecy rates $\mathcal{C}_s^-$, $\widetilde{\mathcal{C}}_s^-$, and $\hat{R}_M(\alpha)$ in [128], with N_T=4, N_R=2, N_E=1, and α=0.5.

able secrecy rate studied by [128], given by eq. (27) in the reference in question, is illustrated in Figures 6.9 and 6.10. In Figure 6.9, we present the achievable secrecy rates for three different values of the number of feedback bits, $B = 4, 8$, and 10, with $N_T = 4$, $N_R = 2$, $N_E = 1$, and $\alpha = 0.5$. The parameter α, in [128], represents the power splitting factor, i.e., $\alpha P_{avg}/N_R$ is used for data transmission and $(1-\alpha)P_{avg}/(N_T-N_R)$ is used for AN transmission. We can see that the transmission of AN is preferable for certain values of the SNR especially when the number of feedback bits is large. However, as we can see from Figure 6.9, for a fixed value of B, the achievable secrecy rate in [128] is bounded while $\mathcal{C}_s^-$ and $\widetilde{\mathcal{C}}_s^-$ are not. In Figure 6.10, we illustrate the achievable secrecy rates in terms of the factor α for three different values of the SNR, SNR=0 dB, 10 dB, and 20 dB, with $N_T = 4$, $N_R = 2$, $N_E = 1$, and $B = 4$. As no AN transmission is considered in our work, the secrecy rates remain constant. In the case when SNR=0 dB, we can that the achievable secrecy rate in

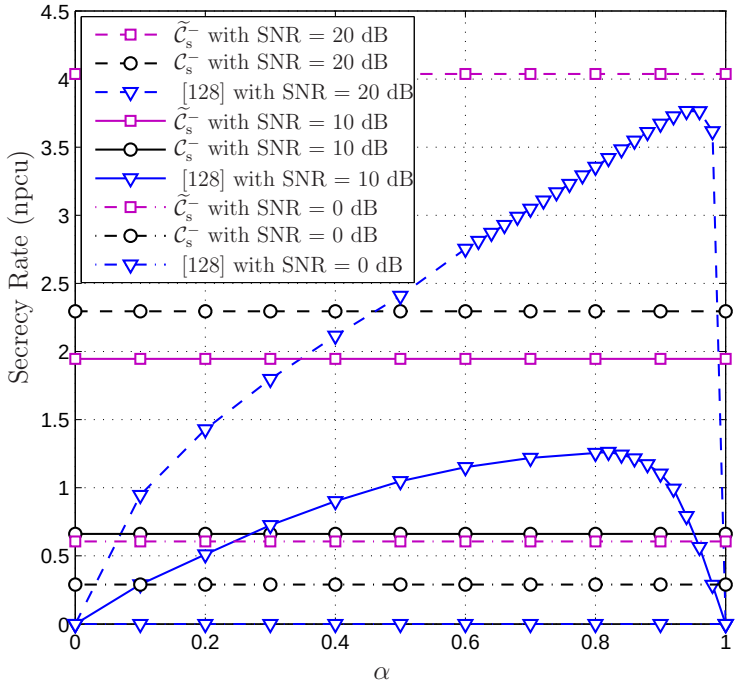


Figure 6.10: Achievable secrecy rates $\mathcal{C}_{\rm s}^-$, $\widetilde{\mathcal{C}}_{\rm s}^-$, and $\hat{R}_M(\alpha)$ in [128], with $N_{\rm T}$=4, $N_{\rm R}$=2, $N_{\rm E}$=1, and B=4.

[128] is equal to zero while $\mathcal{C}_s^-$ and $\widetilde{\mathcal{C}}_s^-$ are not. In the other two cases, we can see that the AN transmission is preferable compared to $\mathcal{C}_s^-$ only when the power allocated to the AN is restricted ($\alpha \gtrsim 0.5$).

6.6 Conclusion

The impact of having limited main CSI feedback on the ergodic secrecy performance of a multiple-antenna block-fading wiretap channel has been investigated. We presented two achievable secrecy rates $\mathcal{C}_{\rm s}^-$ and $\widetilde{\mathcal{C}}_{\rm s}^-$ and an upper bound on the ergodic secrecy capacity $\mathcal{C}_{\rm s}^+$, and showed that even with a 1-bit CSI feedback, a positive secrecy rate can still be achieved. The first achievable secrecy rate $\mathcal{C}_{\rm s}^-$ adapts both the power and the transmission rate and guarantees that the best the eavesdropper can receive is the fixed transmission rate received at the legitimate node. The second achievable rate $\widetilde{\mathcal{C}}_{\rm s}^-$ only adapt the power and is more convenient when the number of antennas

at the eavesdropper is less than the number of antennas at the legitimate receiver, and the number of CSI feedback bits is small. Furthermore, we showed that the achievable secrecy rate $\mathcal{C}_{\rm s}^{-}$ and the upper bound $\mathcal{C}_{\rm s}^{+}$ coincide, asymptotically, as the capacity of the feedback link becomes large, i.e. $B \to \infty$; hence, fully characterizing the ergodic secrecy capacity in this case. Asymptotic analysis, in the high SNR regime, were also presented, and the gap between the bounds was estimated. In particular, we characterized the scaling behavior of the presented bounds, and showed that the asymptotic gap between $\mathcal{C}_{\rm s}$ and $\mathcal{C}_{\rm s}^{-}$ vanishes as the number of feedback bits increases while the asymptotic gap between $\mathcal{C}_{\rm s}$ and $\widetilde{\mathcal{C}}_{\rm s}^{-}$ is independent of the number of feedback bits.

Chapter 7

Summary of Contributions and Future Directions

7.1 Summary of Contributions

The aim of this thesis was to analyze and understand the impact of CSIT uncertainty on the ergodic secrecy capacity of fading wiretap channels. Mainly, we showed that even though the secrecy performance of the system deteriorates compared to the case when the transmitter has perfect CSI, a positive secrecy rate can still be achieved as long as the transmitter has some knowledge of the main channel gain. We considered two common causes of CSIT imperfections, namely, the occurrence of an estimation error of the CSI at the transmitter and the limited capacity of the CSI feedback link. In both cases, we noticed that the more the transmitter knows about the main CSI, the better the secrecy performances are.

In particular, we characterized the ergodic secrecy capacity of multi-user broadcast wiretap channels over fast fading channels with imperfect main CSIT in Chapter 3. We proved that a non-zero secrecy rate can still be achieved even with a poor main channel estimator at the transmitter. In addition, we showed that the common message secrecy rate is limited by the legitimate receiver having the lowest average SNR, and that the achievable secrecy sum-rate, when broadcasting multiple independent messages, scales with the number of users K according to the scaling law $\log((1-\alpha)\log(K))$, where α is the estimation error variance of the CSIT. Asymptotic analysis at high-SNR, perfect and no-main CSI were addressed and the results were illustrated for the case of Rayleigh fading channels.

In Chapter 4, we evaluated the impact of having finite CSI feedback on the secrecy throughput of multi-user block-fading broadcast channels. More specifically, we considered that the feedback bits are provided to the transmitter by each legitimate receiver, at the beginning of each coherence block, through error-free public links with limited capacity. We examined both the common message transmission case, where the same message is broadcasted to all the legitimate receivers, and the independent messages transmission scenario, where the source broadcasts multiple independent messages to the users. Assuming an average power constraint at the transmitter, we provided an upper and a lower bounds on the ergodic secrecy capacity for the common message case, and an upper and a lower bounds on the secrecy sum-rate for the independent messages case. For the particular case of infinite feedback, we proved that our bounds coincide.

The secrecy capacity region of the block-fading BCCM with limited CSIT was established in Chapter 5. In particular, we considered a two-user communication system where the transmitter has one common message to be transmitted to both users and one confidential message intended to only one of them. The confidential message has to be kept secret from the other user to whom the information is not intended. The transmitter is not aware of the CSI of neither channel and is only provided by limited CSI feedback sent at the beginning of each fading block. Assuming an error-free feedback link, we characterized the secrecy capacity region of this channel and showed that even with a 1-bit CSI feedback, a positive secrecy rate can still be achieved. Then, we looked at the case where the feedback link is subject to erasure. In the latter case, we provided an achievable secrecy rate region and showed that as long as the erasure event is not a probability one event, the transmitter can still transmit the confidential information with a positive secrecy rate.

The ergodic secrecy capacity of multi-antenna block-fading wiretap channels with limited CSI feedback was investigated in Chapter 6. We provided two achievable secrecy rates and an upper bound on the ergodic secrecy capacity. The first secrecy rate is achieved by using the feedback information not only to adapt the power but also to adjust the transmission rate during each fading block. The considered scheme guarantees that the best the eavesdropper can receive, during a given fading block, is the fixed transmission rate received at the legitimate node. For the second achievable secrecy rate, the feedback is mainly employed for the power adaptation purpose. Besides, in order to maximize the secrecy rate, we proposed an iterative framework to design the used codebooks for feedback and transmission. For the particular case of infinite feedback, we proved that the first achievable secrecy rate and the presented upper bound on the ergodic secrecy capacity coincide, hence, fully characterizing the ergodic secrecy capacity in this case. The high-SNR regime and the SDoF of the system were also investigated.

7.2 Future Research Directions

Certainly, there are still open challenges related to physical layer security with CSIT uncertainty. First, we can see that, for most cases, the secrecy capacity of fading wiretap channels with partial CSIT is not perfectly known and is only characterized in terms of bounds. Also, we notice that a certain level of CSI knowledge is required at the transmitter, i.e., at least the fading distributions of the communicating channels should be known at the transmitter. It would be of interest to consider and study the case when even the distribution of the eavesdropper's channel cannot be obtained at the transmitter. The construction of practical wiretap codes is another open issue facing physical layer security either with perfect or partial CSIT.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Systems Technical Journal*, vol. 28, pp. 656–719, Oct. 1949.

[2] A. D. Wyner, "The wiretap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[3] Y. Liang, H. Poor, and S. Shamai, *Information Theoretic Security*. Foundations and Trends in Communications and Information Theory 5 (4-5), 2008.

[4] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer*. Norwell, MA, US: Springer, 2009.

[5] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, UK: Cambridge University Press, 2011.

[6] E. by X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. CRC Press, 2014.

[7] E. Jorswieck, A. Wolf, and S. Gerbracht, *Trends in Telecommunications Technologies: Secrecy on the Physical Layer in Wireless Networks*. InTech, 2010.

[8] A. Mukherjee, S. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications surveys and Tutorials*, vol. 16, no. 3, pp. 1550–1573, Third Quarter 2014.

[9] W. Trappe, "The challenges facing physical layer security," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 16–20, Jun. 2015.

[10] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[11] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, "Physical layer security in wireless cooperative relay networks: State of the art and beyond," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 32–39, Dec. 2015.

[12] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. R. Bloch, S. Ulukus, and A. Yener, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 16–28, Sep. 2013.

[13] A. Yener and S. Ulukus, "Wireless physical-layer security: Lessons learned from information theory," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1814–1825, Oct. 2015.

[14] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 21–27, Jun. 2015.

[15] Y. Zou, J. Zhu, L. Yang, Y.-C. Liang, and Y.-D. Yao, "Securing physical-layer communications for cognitive radio networks," *IEEE Communications Magazine*, vol. 53, no. 9, pp. 48–54, Sep. 2015.

[16] B. He, X. Zhou, and T. D. Abhayapala, "Wireless physical layer security with imperfect channel state information: A survey," *ZTE Communications*, no. 3, Sep. 2013.

[17] E. Jorswieck, S. Tomasin, and A. Sezgin, "Broadcasting into the uncertainty: Authentication and confidentiality by physical-layer processing," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1702–1724, Oct. 2015.

[18] T.-Y. Liu, P.-H. Lin, Y.-W. P. Hong, and E. Jorswieck, "To avoid or not to avoid CSI leakage in physical layer secret communication systems," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 19–25, Dec. 2015.

[19] S. Lloyd, "Least squares quantization in PCM," *IEEE Transactions on Information Theory*, vol. IT-28, no. 2, pp. 129–137, Mar. 1982.

[20] M. Hayashi, "General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap channels," *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1562–1575, Apr. 2006.

[21] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," *Advances in Cryptology - EUROCRYPT 2000 (Lecture Notes in Computer Science, vol. 1807), Bruges, Belgium: Springer-Verlag*, pp. 351–368, 2000.

[22] I. Csiszar, "Almost independence and secrecy capacity," *Problems of Information Transmission*, vol. 32, no. 1, pp. 40–47, Jan. 1996.

[23] M. Bloch and J. Laneman, "Strong secrecy from channel resolvability," *IEEE Transactions on Information Theory*, vol. 59, no. 12, pp. 8077–8098, Dec. 2013.

[24] M. Bellare, S. Tessaro, and A. Vardy, "A cryptographic treatment of the wiretap channel," in *Advances in Cryptology - (CRYPTO 2012)*, Santa Barbara, CA, US, Aug. 2012, p. 351.

[25] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[26] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wiretap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[27] J. Barros and M. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. International Symposiumon on Information Theory (ISIT'2006)*, Seattle, WA, US, Jul. 2006, pp. 356–360.

[28] P. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[29] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[30] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2453–2469, Jun. 2008.

[31] Y. Liang, H. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

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

[33] E. Tekin and A. Yener, "Achievable rates for the general gaussian multiple access wire-tap channel with collective secrecy," in *Proc. of the 44th Annual Allerton Conference on Communication, Control, and Computing, (Allerton'06)*, Monticello, IL, Sep. 2006, pp. 809–816.

[34] ——, "The gaussian multiple access wire-tap channel: Wireless secrecy and cooperative jamming," in *Proc. of the Information Theory and Applications Workshop (ITA'07)*, San Diego, CA, Jan. 2007, pp. 404–413.

[35] ——, "The general gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[36] A. Khisti and G. Womell, "Secure transmission with multiple antennas Part I: The MISOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[37] ——, "Secure transmission with multiple antennas Part II: The MIMOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[38] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[39] X. He and A. Yener, "The gaussian many-to-one interference channel with confidential messages," *IEEE Transactions on Information Theory, Special Issue on Interference Networks*, vol. 57, no. 5, pp. 2730–2745, May 2011.

[40] ——, "End-to-end secure multi-hop communication with untrusted relays," *IEEE Transactions on Wireless Communications*, vol. 12, no. 1, pp. 1–11, Jan. 2013.

[41] ——, "Providing secrecy with structured codes: Two-user gaussian channels," *IEEE Transactions on Information Theory*, vol. 60, no. 4, pp. 2121–2138, Apr. 2014.

[42] ——, *Cooperative Jamming: The Tale of Friendly Interference for Secrecy, Securing Wireless Communications at the Physical Layer, Editors: R. Liu and W. Trappe.* Springer, 2009.

[43] E. Tekin, S. Serbetli, and A. Yener, "On secure signaling for the gaussian multiple access wire-tap channel," in *Proc. of the 39th Asilomar Conference on Signals, Systems and Computers (Asilomar'05)*, Pasific Grove, CA, Nov. 2005, pp. 1747–1751.

[44] D. Love, R. Heath, V. Lau, D. Gesbert, B. Rao, and M. Andrews, "An overview of limited feedback in wireless communication systems," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 8, pp. 1341–1365, Oct. 2008.

[45] H. Jeon, N. Kim, M. Kim, H. Lee, and J. Ha, "Secrecy capacity over correlated ergodic fading channels," in *Proc. IEEE Military Communications Conference*, San Diego, CA, US, Nov. 2008, pp. 1–7.

[46] H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, "Bounds on secrecy capacity over correlated ergodic fading channels at high SNR," *IEEE Transactions on Information Theory*, vol. 57, no. 4, pp. 1975–1983, Apr. 2011.

[47] M. Kobayashi, M. Debbah, and S. Shamai, "Secured communication over frequency selective fading channels: A practical Vandermonde precoding," *EURASIP Journal on Wireless Communications and Networkin*, pp. 1–19, article ID 386 547, Aug. 2009.

[48] R. Liu, I. Maric, P. Spasojevic, and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.

[49] J. Xu, Y. Cao, and B. Chen, "Capacity bounds for broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 55, no. 10, pp. 4529–4542, Oct. 2009.

[50] S. Zou, Y. Liang, L. Lai, and S. Shamai, "Rate splitting and sharing for degraded broadcast channel with secrecy outside a bounded range," in *Proc. International Symposiumon on Information Theory (ISIT'2015)*, Hong Kong, Jun. 2015, pp. 1357–1361.

[51] O. O. Koyluoglu, H. E. Gamal, L. Lai, and H. V. Poor, "On the secure degrees of freedom in the k-user Gaussian interference channels," in *Proc. IEEE International Symposium on Information Theory (ISIT'2008)*, Toronto, Canada, Jul. 2008, pp. 384–388.

[52] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. International Symposiumon on Information Theory (ISIT'2008)*, Nice, France, Jul. 2008, pp. 524–528.

[53] A. Hero, "Secure space-time communication," *IEEE Transactions on Information Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.

[54] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. International Symposiumon on Information Theory (ISIT'2005)*, Adelaide, Australia, Sept. 2005, pp. 2152–2155.

[55] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proc. 41st Annual Conference on Information Sciences and Systems (CISS'2007)*, Baltimore, MD, Mar. 2007, pp. 905 –910.

[56] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. International Symposiumon on Information Theory (ISIT'2007)*, Nice, France, Jun. 2007, pp. 2466–2470.

[57] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, no. 4, pp. 2083–2114, Apr. 2011.

[58] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[59] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[60] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Transactions on Information Theory*, vol. 55, no. 9, pp. 4033–4039, Sep. 2009.

[61] R. Liu and H. V. Poor, "Secrecy capacity region of a multiple-antenna Gaussian broadcast channel with confidential messages," *IEEE Transactions on Information Theory*, vol. 55, no. 3, p. 12351249, Mar. 2009.

[62] R. Bustin, R. Liu, H. V. Poor, and S. Shamai, "An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel," *EURASIP J. Wireless Communications and Networking*, pp. 1–8, 2009.

[63] M. Yuksel and E. Erkip, "Diversity-multiplexing tradeoff for the multiple-antenna wire-tap channel," *IEEE Transactions on Wireless Communications*, vol. 10, no. 3, pp. 762–771, Mar. 2011.

[64] Z. Han, N. Marina, M. Debbah, and A. Hjorungnes, "Physical layer security game: Interaction between source, eavesdropper and friendly jammer," *EURASIP Journal on Wireless Communications and Networking (Special Issue on Wireless Physical Layer Security)*, Jun 2009.

[65] I. W. P. L. S. via Cooperating Relays, "L. dong and z. han and a. p. petropulu and h.v. poor," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[66] J. Zhang and M. C. Gursoy, "Relay beamforming strategies for physical layer security," in *Proc. IEEE Conference on Information Sciences and Systems (CISS'2010)*, Princeton, NJ, US, Mar. 2010, pp. 1–6.

[67] M. Yuksel, X. Liu, and E. Erkip, "A secure communication game with a relay helping the eavesdropper," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 818–830, Sep. 2011.

[68] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.

[69] A. Zewail and A. Yener, "Multi-terminal two-hop untrusted-relay networks with hierarchical security guarantees," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 9, pp. 2052–2066, Sep. 2017.

[70] M. Nafea and A. Yener, "Secure degrees of freedom for the mimo wire-tap channel with a multi-antenna cooperative jammer," *IEEE Transactions on Information Theory*, accepted Jul. 2017.

[71] Y. Pei, Y. Liang, L. Zhang, K. Teh, and K. Li, "Secure communication over MISO cognitive radio channels," *IEEE Transactions on Wireless Communications*, vol. 9, no. 4, pp. 1494–1502, Apr. 2010.

[72] Y. Wu and K. J. R. Liu, "An information secrecy game in cognitive radio networks," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 831–842, Sep. 2011.

[73] J. Zhang and M. C. Gursoy, "Secure relay beamforming over cognitive radio channels," in *Proc. IEEE Conference on Information Sciences and Systems (CISS'2011)*, Baltimore, MD, US, Mar. 2011, pp. 1–5.

[74] K. Lee, O. Simeone, C. Chae, and J. Kang, "Spectrum leasing via cooperation for enhanced physical-layer secrecy," in *Proc. IEEE International Conference on Communications Workshops (ICC'2011)*, Kyoto, Japan, Jun. 2011, pp. 1–5.

[75] I. Stanojev and A. Yener, "Improving secrecy rate via spectrum leasing for friendly jamming," *IEEE Transactions on Wireless Communications*, vol. 12, no. 1, pp. 134–145, Jan. 2013.

[76] J. Zhu, R. Schober, and V. Bhargava, "Secure transmission in multi-cell massive MIMO systems," in *Proc. IEEE Globecom Workshops (GC Workshps'2013)*, Atlanta, GA, US, Dec. 2013, pp. 1286–1291.

[77] ——, "Secrecy analysis of multi-cell massive MIMO systems with RCI precoding and artificial noise transmission," in *Proc. International Symposium on Communications, Control and Signal Processing (ISCCSP'2014)*, Athens, Greece, May 2014, pp. 101–104.

[78] Y. Long, Z. Chen, L. Li, and J. Fang, "Non-asymptotic analysis of secrecy capacity in massive MIMO system," in *Proc. IEEE International Conference on Communications Workshops (ICC'2015)*, London, UK, Jun. 2015, pp. 4587–4592.

[79] Z. Li, R. Yates, and W. Trappe, "Secret communication with a fading eavesdropper channel," in *Proc. IEEE International Symposiumon on Information Theory (ISIT'2007)*, Nice, France, Jul. 2007, pp. 1296–1300.

[80] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels," *IEEE Transactions on Information Theory*, vol. 55, no. 4, pp. 1575–1591, Apr. 2009.

[81] A. Khisti, A. Tchamkerten, and G. Wornell, "Secure broadcasting with multiuser diversity," in *Proc. 44th Allerton Conference on Communication, Control, and Computing*, Monticello, IL,US, Sep. 2006.

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

[83] J. Li and A. P. Petropulu, "On ergodic secrecy rate for gaussian MISO wiretap channels," *IEEE Transactions on Signal Processing*, vol. 10, no. 4, pp. 1176–1187, Apr. 2011.

[84] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Transactions on Communications*, vol. 61, no. 1, pp. 144–154, Jan. 2013.

[85] X. Wang, K. Wang, and X.-D. Zhang, "Secure relay beamforming with imperfect channel side information," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2140–2155, Jun. 2013.

[86] J. Zhu, R. Schober, and V. Bhargava, "Linear precoding of data and artificial noise in secure massive MIMO systems," *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 2245–2261, Mar. 2016.

[87] R. Negi and S. Goel, "Secret communication using artificial noise," in *IEEE Vehicular Technology Conference (VTC-2005-Fall)*, Dallas, US, Sept. 2005, pp. 1906–1910.

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

[89] S. Liu, Y. Hong, and E. Viterbo, "Practical secrecy using artificial noise," *IEEE Communication Letters*, vol. 17, no. 7, pp. 1483–1486, Jul. 2013.

[90] X. Zhou and M. McKay, "Secure transmission with artificial noise over fading channels:achievable rate and optimal power allocation," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[91] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Processing Letters*, vol. 19, no. 2, pp. 71–74, Feb. 2012.

[92] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization," *IEEE Transactions on Signal Processing*, vol. 61, no. 10, pp. 2704–2717, May 2013.

[93] P.-H. Lin, S.-H. Lai, S.-C. Lin, and H.-J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE Jour-*

nal on Selected Areas of Communication, vol. 31, no. 9, pp. 1728–1740, Sep. 2013.

[94] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis," *IEEE Communications Letters*, vol. 16, no. 10, pp. 1628–1631, Oct. 2012.

[95] X. Zhang, X. Zhou, and M. R. McKay, "Enhancing secrecy with multi-antenna transmission in wireless ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1802–1814, Nov. 2013.

[96] D. Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding, and K. Leung, "Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks," *IEEE Journal on Selected Areas of Communication*, vol. 29, no. 10, pp. 2067–2078, Dec. 2011.

[97] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference-assisted secret communication," in *Proc. IEEE Information Theory Workshop (ITW'2008)*, Porto, Portugal, May 2008, p. 164168.

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

[99] S. Liu, Y. Hong, and E. Viterbo, "Artificial noise revisited," *IEEE Transactions on Information Theory*, vol. 61, no. 7, pp. 3901–3911, Jul. 2015.

[100] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 704–716, Apr. 2012.

[101] J. Zhang and M. C. Gursoy, "Collaborative relay beamforming for secrecy," in *Proc. IEEE Wireless Communications Symposium (ICC'2010)*, Cape Town, South Africa, Jun. 2010, pp. 1–5.

[102] R. Bassily and S. Ulukus, "Deaf cooperation and relay selection strategies for secure communication in multiple relay networks," *IEEE Transactions on Signal Processing*, vol. 61, no. 6, pp. 1544–1554, Mar. 2013.

[103] K.-S. Hwang and M. Ju, "Secrecy outage probability of amplify-and-forward transmission with multi-antenna relay in presence of eavesdropper," in *Proc. IEEE Wireless Communications Symposium (ICC'2014)*, Sydney, Australia, Jun. 2014, pp. 5408–5412.

[104] X. He and A. Yener, "MIMO wiretap channels with unknown and varying eavesdropper channel states," *IEEE Transactions on Information Theory*, vol. 60, no. 11, pp. 6844–6869, Nov. 2014.

[105] ——, "The interference wiretap channel with an arbitrarily varying eavesdropper: Aligning interference with artificial noise," in *Proc. of the 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton'12)*, Monticello, IL, Oct. 2012, pp. 204–211.

[106] X. He, A. Khisti, and A. Yener, "Mimo multiple access channel with an arbitrarily varying eavesdropper: Secrecy degrees of freedom," *IEEE Transactions on Information Theory*, vol. 59, no. 8, pp. 4733–4745, Aug. 2013.

[107] ——, "Mimo broadcast channel with an unknown eavesdropper: Secrecy degrees of freedom," *IEEE Transactions on Communications*, vol. 62, no. 1, pp. 246–255, Jan. 2014.

[108] Z. Rezki, A. Khisti, and M.-S. Alouini, "On the ergodic secrecy capacity of the wiretap channel under imperfect main channel estimation," in *Proc. Forty Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR'2011)*, Pacific Grove, CA, US, Nov. 2011, pp. 952–957.

[109] ——, "On the secrecy capacity of the wiretap channel under imperfect main channel estimation," *IEEE Transactions on Communications*, vol. 62, no. 10, pp. 3652–3664, Sep. 2014.

[110] M. Bloch and J. Laneman, "Exploiting partial channel state information for secrecy over wireless channels," *IEEE Journal on Selected Areas of Communication*, vol. 31, no. 9, pp. 1840–1849, Sep. 2013.

[111] A. Hyadi, Z. Rezki, A. Khisti, and M.-S. Alouini, "On the secrecy capacity of the broadcast wiretap channel with imperfect channel state information," in *IEEE Global Communications Conference (GLOBECOM'2014)*, Austin, TX , US, Dec. 2014, pp. 1608–1613.

[112] ——, "Secure broadcasting with imperfect channel state information at the transmitter," *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 2215–2230, Mar. 2016.

[113] X. Chen and H.-H. Chen, "Physical layer security in multi-cell MISO downlinks with incomplete CSIa unied secrecy performance analysis," *IEEE Transactions on Signal Processing*, vol. 62, no. 23, pp. 6286–6297, Dec. 2014.

[114] Z. Rezki, B. Alomair, and M.-S. Alouini, "On the secrecy capacity of the MISO wiretap channel under imperfect channel estimation," in *Proc. IEEE Global Communications Conference (GLOBECOM2014)*, Austin, TX, USA, Dec. 2014, pp. 1602–1607.

[115] X. Zhou, Z. Rezki, B. Alomair, and M.-S. Alouini, "Achievable rates of secure transmission in gaussian MISO channel with imperfect main channel estimation," in *Proc. IEEE Globecom Workshops (GC Wkshps'2015)*, San Diego, CA, US, Dec. 2015, pp. 1–6.

[116] ——, "Achievable rates of secure transmission in gaussian MISO channel with imperfect main channel estimation," *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 4470–4485, Jun. 2016.

[117] Z. Chu, H. Xing, M. Johnston, and S. L. Goff, "Secrecy rate optimizations for a MISO secrecy channel with multiple multiantenna eavesdroppers," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 283–297, Jan. 2016.

[118] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Transactions on Signal Processing*, vol. 59, no. 1, pp. 351–360, Jan. 2011.

[119] A. Al-nahari, "Physical layer security using massive multiple-input and multiple-output: passive and active eavesdroppers," *IET Communications*, vol. 10, no. 1, pp. 50–56, 2016.

[120] D. W. K. Ng, E. S. Lo, and R. Schober, "Secure resource allocation and scheduling for OFDMA decode-and-forward relay networks," *IEEE Transactions on Wireless Communications*, vol. 10, no. 10, pp. 3528–3540, Oct. 2011.

[121] Y. Pei, Y.-C. Liang, K. C. Teh, and K. H. Li, "Secure communication in multiantenna cognitive radio networks with imperfect channel state information," *IEEE Transactions on Signal Processing*, vol. 59, no. 4, pp. 1683–1693, Apr. 2011.

[122] Z. Rezki, A. Khisti, and M.-S. Alouini, "On the ergodic secret message capacity of the wiretap channel with finite-rate feedback," in *Proc. IEEE International Symposium on Information Theory (ISIT'2012)*, Cambridge, MA, US, Jul. 2012, pp. 239–243.

[123] ——, "Ergodic secret message capacity of the wiretap channel with finite-rate feedback," *IEEE Transactions on Wireless Communications*, vol. 13, no. 6, pp. 3364–3379, Jun. 2014.

[124] A. Hyadi, Z. Rezki, and M.-S. Alouini, "On the secrecy capacity of the broadcast wiretap channel with limited CSI feedback," in *IEEE Information Theory Workshop (ITW'2016)*, Cambridge, UK, Sep. 2016.

[125] ——, "On the secrecy capacity region of the block-fading BCC with limited CSI feedback," in *IEEE Global Communications Conference (Globecom'2016)*, Washington, DC, US, Dec. 2016.

[126] 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 *Proc. IEEE International Symposiumon on Information Theory (ISIT'2009)*, Seoul, Korea, Jun. 2009, pp. 2351–2355.

[127] S.-C. Lin, T.-H. Chang, Y.-W. Hong, and C.-Y. Chi, "On the impact of quantized channel direction feedback in multiple-antenna wiretap channels," in *Proc. IEEE Wireless Communications Symposium (ICC'2010)*, Cape Town, South Africa, May 2010, pp. 1–5.

[128] S.-C. Lin, T.-H. Chang, Y.-L. Liang, Y.-W. Hong, and C.-Y. Chi, "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise: The noise leakage problem," *IEEE Transactions on Wireless Communications*, vol. 10, no. 3, pp. 901–915, Mar. 2011.

[129] T. Tsiligkaridis, "Secure MIMO communications under quantized channel feedback in the presence of jamming," *IEEE Transactions on Signal Processing*, vol. 62, no. 23, pp. 6265–6275, Dec. 2014.

[130] H.-M. Wang, C. Wang, and D. W. K. Ng, "Articial noise assisted secure transmission under training and feedback," *IEEE Transactions on Signal Processing*, vol. 63, no. 23, pp. 6285–6298, Dec. 2015.

[131] S. Liu, Y. Hong, and E. Viterbo, "Guaranteeing positive secrecy capacity for MIMOME wiretap channels with finite-rate feedback using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 14, no. 8, pp. 4193–4203, Aug. 2015.

[132] D. J. Love, R. W. Heath, and T. Strohmer, "Grassmannian beamforming for multiple-input multiple-output wireless systems," *IEEE Transactions on Information Theory*, vol. 49, no. 10, pp. 2735–2747, Oct. 2003.

[133] A. Hyadi, Z. Rezki, and M.-S. Alouini, "On the secrecy capacity of the multiple-antenna wiretap channel with limited CSI feedback," in *Proc. IEEE Global Communications Conference (Globecom'2015)*, San Diego, CA, US, Dec. 2015, pp. 1–6.

[134] X. Chen and R. Yin, "Performance analysis for physical layer security in multi-antenna downlink networks with limited CSI feedback," *IEEE Wireless Communications Letters*, vol. 2, no. 5, pp. 503–506, Oct. 2013.

[135] Z. Peng, W. Xu, J. Zhu, H. Zhang, and C. Zhao, "On performance and feedback strategy of secure multiuser communications with MMSE channel estimate," *IEEE Transactions on Wireless Communications*, vol. 15, no. 2, pp. 1602–1616, Feb. 2016.

[136] N. S. Ferdinand, D. B. da Costa, and M. Latva-aho, "Effects of outdated CSI on the secrecy performance of MISO wiretap channels with transmit antenna selection," *IEEE Communications Letters*, vol. 17, no. 5, pp. 864–867, May 2013.

[137] J. Hu, Y. Cai, N. Yang, and W. Yang, "A new secure transmission scheme with outdated antenna selection," *IEEE Transactions on Forensics and Security*, vol. 10, no. 11, pp. 2435–2446, Nov. 2015.

[138] Y. Huang, F. S. Al-Qahtani, T. Q. Duong, and J. Wang, "Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI," *IEEE Transactions on Communications*, vol. 63, no. 8, pp. 2959–2971, Aug. 2015.

[139] S. Yang, M. Kobayashi, P. Piantanida, and S. Shamai, "Secrecy degrees of freedom of MIMO broadcast channels with delayed CSIT," *IEEE Transactions on Information Theory*, vol. 59, no. 9, pp. 5244–5256, Sep. 2013.

[140] A. Zaidi, Z. H. Awan, S. Shamai, and L. Vandendorpe, "Secure degrees of freedom of MIMO X-channels with output feedback and delayed CSIT," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1760–1774, Nov. 2013.

[141] S. Lashgari and A. S. Avestimehr, "Blind wiretap channel with delayed CSIT," in *Proc. IEEE International Symposium on Information Theory (ISIT'2014)*, Honolulu, HI, US, Jul. 2014, pp. 36–40.

[142] M. Pei, J. Wei, K.-K. Wong, and X. Wang, "Masked beamforming for multiuser MIMO wiretap channels with imperfect CSI," *IEEE Transactions on Wireless Communications*, vol. 11, no. 2, pp. 544–549, Feb. 2012.

[143] I. S. Gradshteyn and I. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. Amsterdam: Elsevier/Academic Press, 2007.

[144] J. I. Marcum, "Statistical theory of target detection by pilsed radar: Mathematical appendix," in *RAND Corporation*, Santa Monica, California, Research Memorandum No. RM-753, Jul. 1948.

[145] B. Hassibi and B. Hochwald, "How much training is needed in multiple-antenna wireless links," *IEEE Transactions on Information Theory*, vol. 49, no. 4, pp. 951–963, Apr. 2003.

[146] V. Lau, Y. Liu, and T.-A. Chen, "On the design of MIMO block-fading channels with feedback-link capacity constraint," *IEEE Transactions on Communications*, vol. 52, no. 1, pp. 62–70, Jan. 2004.

[147] S. P. B. L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.

[148] G. Caire and S. Shamai, "On the capacity of some channels with channel state information," *IEEE Transactions on Information Theory*, vol. 45, no. 6, pp. 2007–2019, Sep. 1999.

[149] D. Morales-Jimenez, F. Lopez-Martinez, E. Martos-Naya, J. Paris, and A. Lozano, "Connections between the generalized Marcum Q-function and a class of hypergeometric functions," *IEEE Transactions on Information Theory*, vol. 60, no. 2, pp. 1077–1082, Feb. 2014.

[150] I. W. Research, *Mathematica Edition: Version 8.0*. Champaign Illinois: Wolfram Research, Inc., 2010.

Appendix A

A.1 Proof of Achievability in Theorem 3.2

To prove the achievability of the lower bound on the secrecy capacity in Theorem 3.2, we adopt a coding scheme similar to the one presented in [30]. We denote the message to be transmitted by W, and we let U be a sequence of independent random variables over some alphabet $\mathcal{U}$. Also, we adopt the following notation

H=$\{h_1, \cdots, h_K\}$, H^i=$\{h_1(1), \cdots, h_1(i), h_2(1), \cdots, h_2(i), \cdots, h_K(1), \cdots, h_K(i)\}$,

$\hat{H}$=$\{\hat{h}_1, \cdots, \hat{h}_K\}$, $\hat{H}^i$=$\{\hat{h}_1(1), \cdots, \hat{h}_1(i), \hat{h}_2(1), \cdots, h_2(i), \cdots, \hat{h}_K(1), \cdots, \hat{h}_K(i)\}$.

Let η_1 and η_2 be two positive constants. We define $\mathcal{R}_e = I(U; Z|g, H, \hat{H}) - \eta_2$, and

$$\mathcal{R} = \min_{1 \leq k \leq K} \left\{ I(U; Y_k|H, \hat{H}) - I(U; Z|g, H, \hat{H}) \right\} - \eta_1.$$

We construct K+1 independent random codebooks $C_1, \cdots, C_{K+1}$, for the K legitimate subchannels and the eavesdropper subchannel. For each message W, codebook C_k is randomly partitioned into $2^{n\mathcal{R}}$ bins, such that each bin contains $2^{n\mathcal{R}_e}$ codewords. To decode the received signal, each receiver will try to find a message W that is jointly typical with the channel output Y_k. The error probability analysis are similar to the case of perfect CSI [30]. For the secrecy analysis, we need to prove that, for n sufficiently large

$$\frac{1}{n} I(W; Z^n|g^n, H^n, \hat{H}^n) \leq \epsilon. \tag{A.1}$$

We have

$$I(W; Z^n|g^n, H^n, \hat{H}^n) = H(W|g^n, H^n, \hat{H}^n) - H(W|Z^n, g^n, H^n, \hat{H}^n), \tag{A.2}$$

and

$$H(W|Z^n,g^n,H^n,\hat{H}^n) = H(W,U^n|Z^n,g^n,H^n,\hat{H}^n) - H(U^n|W,Z^n,g^n,H^n,\hat{H}^n) \quad \text{(A.3)}$$

$$= H(U^n|Z^n,g^n,H^n,\hat{H}^n) - H(U^n|W,Z^n,g^n,H^n,\hat{H}^n) \quad \text{(A.4)}$$

$$\geq H(U^n|Z^n,g^n,H^n,\hat{H}^n) - n\epsilon_1 \quad \text{(A.5)}$$

$$= H(U^n|g^n,H^n,\hat{H}^n) - I(U^n;Z^n|g^n,H^n,\hat{H}^n) - n\epsilon_1 \quad \text{(A.6)}$$

$$= H(U^n,W|g^n,H^n,\hat{H}^n) - I(U^n;Z^n|g^n,H^n,\hat{H}^n) - n\epsilon_1 \quad \text{(A.7)}$$

$$= H(W|g^n,H^n,\hat{H}^n) + H(U^n|W,g^n,H^n,\hat{H}^n) - I(U^n;Z^n|g^n,H^n,\hat{H}^n) - n\epsilon_1 \quad \text{(A.8)}$$

$$= H(W|g^n,H^n,\hat{H}^n) + nI(U;Z|g,H,\hat{H}) - I(U^n;Z^n|g^n,H^n,\hat{H}^n) - n\epsilon_1 \quad \text{(A.9)}$$

$$\geq H(W|g^n,H^n,\hat{H}^n) - n\epsilon_1 - n\eta_2 - n\epsilon_2, \quad \text{(A.10)}$$

where (A.4) and (A.7) follows from the fact that each codeword U^n corresponds to one message W, i.e., W is deterministic given U^n, where (A.5) is obtained using Fano's inequality, i.e., $\frac{1}{n}H(U^n|W,Z^n,g^n,H^n,\hat{H}^n) \leq \frac{1}{n} + \eta_2 R_e \triangleq \epsilon_1$, where (A.9) follows from the fact that each bin contains nR_e codewords, i.e.,

$$H(U^n|W,g^n,H^n,\hat{H}^n) = nI(U;Z|g,H,\hat{H}) - n\eta_2, \quad \text{(A.11)}$$

and where (A.10) results since the codewords are equally likely to be transmitted [2], i.e., $\frac{1}{n}I(U^n;Z^n|g^n,H^n,\hat{H}^n) \leq I(U;Z|g,H,\hat{H}) + \epsilon_2$. Taking $\epsilon{=}\epsilon_1{+}\epsilon_2{+}\eta_2$, we deduce (A.1). To finish the proof, we consider the proposed on-off power scheme in (3.57), set $X{=}U{\sim}\mathcal{CN}(0,P(\tau))$ and adopt a probabilistic transmission model as explained in Section 3.4.2.1. □

A.2 Derivation Details of (3.69)

The lower bound on the secrecy sum capacity with imperfect main CSIT, presented in Theorem 3.1, can be written for i.i.d. Rayleigh fading channels as

$$\widetilde{\mathcal{C}}_{\rm s}^{-}=\max_{P(\tau)}\int_{\gamma=0}^{\infty}\int_{\hat{\gamma}=\tau}^{\infty}\int_{\gamma_e=0}^{\infty}\log\left(\frac{1+\gamma P(\tau)}{1+\gamma_e P(\tau)}\right)f_{\gamma_e}(\gamma_e)f_{\gamma_{\max}^{\rm est}|\hat{\gamma}_{\max}}(\gamma|\hat{\gamma})f_{\hat{\gamma}_{\max}}(\hat{\gamma})\mathrm{d}\gamma_e\mathrm{d}\gamma\mathrm{d}\hat{\gamma}, \quad (A.12)$$

with $P(\tau)=P_{\rm avg}/\left(1-\left(1-\mathrm{e}^{-\tau}\right)^K\right)$, $f_{\gamma_e}(\gamma_e)=\mathrm{e}^{-\gamma_e}$, $f_{\hat{\gamma}_{\max}}(\hat{\gamma})=K\mathrm{e}^{-\hat{\gamma}}(1-\mathrm{e}^{-\hat{\gamma}})^{K-1}$, and

$$f_{\gamma_{\max}^{\rm est}|\hat{\gamma}_{\max}}(\gamma|\hat{\gamma})=\frac{1}{\alpha}\exp\left(-\frac{\gamma+(1-\alpha)\hat{\gamma}}{\alpha}\right)\mathrm{I}_0\left(2\sqrt{\frac{1-\alpha}{\alpha^2}\gamma\hat{\gamma}}\right). \quad (A.13)$$

We can then express (A.12) such as $\mathcal{C}_{\rm s}^{-}=\max_{\tau}\left\{\widetilde{\mathcal{I}}_1-\widetilde{\mathcal{I}}_2\right\}$, (A.14)

with integrals $\widetilde{\mathcal{I}}_2$ and $\widetilde{\mathcal{I}}_1$, respectively, given by

$$\widetilde{\mathcal{I}}_2 = K\int_{\tau}^{\infty}\int_{0}^{\infty}\log\left(1+\gamma_e P(\tau)\right)\mathrm{e}^{-\gamma_e}\mathrm{e}^{-\hat{\gamma}}(1-\mathrm{e}^{-\hat{\gamma}})^{K-1}\mathrm{d}\gamma_e\mathrm{d}\hat{\gamma} \quad (A.15)$$

$$= -\left(1-\left(1-\mathrm{e}^{-\tau}\right)^K\right)\exp\left(\frac{1}{P(\tau)}\right)\mathrm{Ei}\left(-\frac{1}{P(\tau)}\right), \quad (A.16)$$

where (A.16) is obtained using [143, Eq.(4.337.2)], and

$$\widetilde{\mathcal{I}}_1 = \frac{K}{\alpha}\int_{0}^{\infty}\int_{\tau}^{\infty}\log\left(1+\gamma P(\tau)\right)\exp\left(-\frac{\gamma+(1-\alpha)\hat{\gamma}}{\alpha}\right)$$
$$\times\,\mathrm{I}_0\left(2\sqrt{\frac{1-\alpha}{\alpha^2}\gamma\hat{\gamma}}\right)\mathrm{e}^{-\hat{\gamma}}(1-\mathrm{e}^{-\hat{\gamma}})^{K-1}\mathrm{d}\hat{\gamma}\mathrm{d}\gamma. \quad (A.17)$$

Using the binomial theorem [143, Eq.(1.111)] along with equation (A.24), integral $\widetilde{\mathcal{I}}_1$ can be given by

$$\widetilde{\mathcal{I}}_1 = K\sum_{k=0}^{K-1}\binom{K-1}{k}\frac{(-1)^k}{1+\alpha k} \quad (A.18)$$
$$\times\int_{0}^{\infty}\log(1+\gamma P(\tau))\exp\left(-\frac{(1+k)\gamma}{1+\alpha k}\right)\mathrm{Q}\left(\sqrt{2\frac{1-\alpha}{\alpha(1+\alpha k)}\gamma},\sqrt{\frac{2\tau}{\alpha}(1+\alpha k)}\right)\mathrm{d}\gamma.$$

Substituting $\widetilde{\mathcal{I}}_2$ and $\widetilde{\mathcal{I}}_1$ in (A.14) by their respective expressions in (A.16) and (A.18), we get (3.69).

A.3 Derivation Details of (3.87)

When transmitting over i.i.d. Rayleigh fading, the lower bound on the common message secrecy capacity with imperfect main CSI at the transmitter, presented in Theorem 3.2, can be written as

$$\mathcal{C}_{\rm s}^{-} = \max_{P(\tau)} \int_{\gamma=0}^{\infty} \int_{\hat{\gamma}=\tau}^{\infty} \int_{\gamma_e=0}^{\infty} \log\left(\frac{1+\gamma P(\tau)}{1+\gamma_e P(\tau)}\right) f_{\gamma_e}(\gamma_e) f_{\gamma|\hat{\gamma}}(\gamma|\hat{\gamma}) f_{\hat{\gamma}}(\hat{\gamma}) \mathrm{d}\gamma_e \mathrm{d}\gamma \mathrm{d}\hat{\gamma}, \quad \text{(A.19)}$$

with $P(\tau) = P_{\rm avg}\mathrm{e}^{\tau}$, $f_{\gamma_e}(\gamma_e) = \mathrm{e}^{-\gamma_e}$, $f_{\hat{\gamma}}(\hat{\gamma}) = \mathrm{e}^{-\hat{\gamma}}$, and

$$f_{\gamma|\hat{\gamma}}(\gamma|\hat{\gamma}) = \frac{1}{\alpha} \exp\left(-\frac{\gamma+(1-\alpha)\hat{\gamma}}{\alpha}\right) \mathrm{I}_0\left(2\sqrt{\frac{1-\alpha}{\alpha^2}\gamma\hat{\gamma}}\right), \quad \text{(A.20)}$$

where $\mathrm{I}_0(.)$ is the modified Bessel function of the first kind [143, Eq.(8.406.3)].
We can then express (A.19) such as $\mathcal{C}_{\rm s}^{-} = \max_{\tau}\{\mathcal{I}_1 - \mathcal{I}_2\}$, with integrals $\mathcal{I}_2$ and $\mathcal{I}_1$, respectively, given by

$$\mathcal{I}_2 = \mathrm{e}^{-\tau} \int_0^{\infty} \log(1+\gamma_e P_{\rm avg}\mathrm{e}^{\tau})\, \mathrm{e}^{-\gamma_e} \mathrm{d}\gamma_e \quad \text{(A.21)}$$

$$= -\exp\left(\frac{\mathrm{e}^{-\tau}}{P_{\rm avg}}\right) \mathrm{Ei}\left(-\frac{\mathrm{e}^{-\tau}}{P_{\rm avg}}\right) \mathrm{e}^{-\tau}, \quad \text{(A.22)}$$

where (A.22) is obtained using [143, Eq.(4.337.2)], and

$$\mathcal{I}_1 = \frac{1}{\alpha} \int_0^{\infty} \log(1+\gamma P_{\rm avg}\mathrm{e}^{\tau}) \exp\left(-\frac{\gamma}{\alpha}\right) \int_{\tau}^{\infty} \exp\left(-\frac{\hat{\gamma}}{\alpha}\right) \mathrm{I}_0\left(2\sqrt{\frac{1-\alpha}{\alpha^2}\gamma\hat{\gamma}}\right) \mathrm{d}\hat{\gamma}\mathrm{d}\gamma. \quad \text{(A.23)}$$

Using the definition of the Q-function [144, Eq.(16)] and the appropriate change of variables, we have

$$\int_{\tau}^{\infty} \exp\left(-\frac{\hat{\gamma}}{\alpha}\right) \mathrm{I}_0\left(2\sqrt{\frac{1-\alpha}{\alpha^2}\gamma\hat{\gamma}}\right) \mathrm{d}\hat{\gamma} = \alpha \exp\left(\frac{1-\alpha}{\alpha}\gamma\right) \mathrm{Q}\left(\sqrt{2\frac{1-\alpha}{\alpha}\gamma}, \sqrt{\frac{2\tau}{\alpha}}\right), \quad \text{(A.24)}$$

which allows us to write

$$\mathcal{I}_1 = \int_0^{\infty} \log(1+\gamma P_{\text{avg}} \mathrm{e}^{\tau}) \exp(-\gamma)\, \mathrm{Q}\left(\sqrt{2\frac{1-\alpha}{\alpha}\gamma}, \sqrt{\frac{2\tau}{\alpha}}\right) \mathrm{d}\gamma. \tag{A.25}$$

Substituting $\mathcal{I}_2$ and $\mathcal{I}_1$ by their respective expressions in (A.22) and (A.25), we get(3.87).

Now, since

$$\mathrm{Q}(a,b) = \exp\left(-\frac{a^2+b^2}{2}\right) \sum_{n=0}^{\infty}\sum_{m=0}^{\infty} \frac{a^{2(n+m)} b^{2m}}{2^{n+2m}\Gamma(1+m)\Gamma(1+m+n)} \quad \text{[149, Eq.(9)]}, \tag{A.26}$$

we can rewrite $\mathcal{I}_1$ in the form

$$\mathcal{I}_1 = \sum_{n=0}^{\infty}\sum_{m=0}^{\infty} \frac{(1-\alpha)^{n+m}\tau^m \exp(-\tau/\alpha))}{\alpha^{n+2m}\Gamma(1+m)\Gamma(1+n+m)} \int_0^{\infty} \gamma^{n+m} \log(1+\gamma P_{\text{avg}} \mathrm{e}^{\tau}) \exp\Big(-\frac{\gamma}{\alpha}\Big)\, \mathrm{d}\gamma.$$

Using [150, Eq.(01.03.26.0004.01)], [150, Eq.(01.04.26.0003.01)], and [150, Eq.(07.34.21.0011.01)], we get

$$\mathcal{I}_1 = \sum_{n=0}^{\infty}\sum_{m=0}^{\infty} \frac{(1-\alpha)^{n+m}\tau^m \exp(-\tau/\alpha))}{\alpha^{m-1}\Gamma(1+m)\Gamma(1+n+m)}\, \mathrm{G}_{3,2}^{1,3}\left(\alpha P_{\text{avg}} \mathrm{e}^{\tau} \,\middle|\, \begin{matrix} 1, 1, -n-m \\ 1, 0 \end{matrix}\right). \tag{A.27}$$

A.4 Alternative Proof of the Lower Bound in Corollary 3.5

At high SNR, the achievable secrecy sum-rate is given by Corollary 3.1, i.e.,

$$\widetilde{\mathcal{C}}^{-}_{\text{H-SNR}} = \mathop{\mathbb{E}}_{\substack{\gamma_e, \gamma_{\max}^{\text{est}}, \\ \hat{\gamma}_{\max} \geq \tau}} \left[\log\left(\frac{\gamma_{\max}^{\text{est}}}{\gamma_e}\right)\right] \tag{A.28}$$

$$= \int_{\gamma=0}^{\infty}\int_{\hat{\gamma}=\tau}^{\infty}\int_{\gamma_e=0}^{\infty} \log\left(\frac{\gamma}{\gamma_e}\right) f_{\gamma_e}(\gamma_e) f_{\gamma_{\max}^{\text{est}}|\hat{\gamma}_{\max}}(\gamma|\hat{\gamma}) f_{\hat{\gamma}_{\max}}(\hat{\gamma}) \mathrm{d}\gamma_e \mathrm{d}\gamma \mathrm{d}\hat{\gamma}. \tag{A.29}$$

Since $f_{\hat{\gamma}_{\max}}(\hat{\gamma}_{\max}) \xrightarrow[K\to\infty]{} \delta(\hat{\gamma}_{\max} - \log K)$ as $K \to \infty$, then, we can write

$$\lim_{K\to\infty} \widetilde{\mathcal{C}}^{-}_{\text{H-SNR}} = \tag{A.30}$$
$$\lim_{K\to\infty} \left(\frac{1}{\alpha} \int_0^{\infty} \log(\gamma) \exp\left(-\frac{\gamma+(1-\alpha)\log K}{\alpha} \right) \mathrm{I}_0\left(2\sqrt{\frac{1-\alpha}{\alpha^2}\log K\gamma} \right) \mathrm{d}\gamma - \mathop{\mathbb{E}}_{\gamma_e}[\log \gamma_e] \right),$$

and since the variable γ_e does not depend on K, the term $\mathop{\mathbb{E}}_{\gamma_e}[\log(\gamma_e)]$ is asymptotically dominated by $\log\log K$, i.e., $\mathop{\mathbb{E}}_{\gamma_e}[\log(\gamma_e)] = o(\log\log K)$.

Thus, we have

$$\lim_{K\to\infty} \widetilde{\mathcal{C}}^{-}_{\text{H-SNR}} \tag{A.31}$$
$$= \lim_{K\to\infty} \left(\frac{1}{\alpha} \exp\left(\frac{\alpha-1}{\alpha}\log K \right) \int_0^{\infty} \log(\gamma) \exp\left(-\frac{\gamma}{\alpha}\right) \mathrm{I}_0\left(2\sqrt{\frac{1-\alpha}{\alpha^2}\log K\gamma} \right) \mathrm{d}\gamma \right)$$
$$\overset{(a)}{=} \lim_{K\to\infty} \left(\frac{1}{\alpha} \exp\left(\frac{\alpha-1}{\alpha}\log K \right) \sum_{m=0}^{\infty} \frac{1}{\Gamma(m+1)m!} \left(\frac{1-\alpha}{\alpha^2}\log K \right)^m \int_0^{\infty} \gamma^m \log(\gamma) \exp\left(-\frac{\gamma}{\alpha}\right) \mathrm{d}\gamma \right)$$
$$\overset{(b)}{=} \lim_{K\to\infty} \left(\frac{1}{\alpha} \exp\left(\frac{\alpha-1}{\alpha}\log K \right) \left(\left(\log\alpha - \mathbf{C}\right) \sum_{m=0}^{\infty} \frac{(1-\alpha)^m (\log K)^m}{\alpha^{m-1} m!} + \sum_{m=0}^{\infty} \frac{\mathrm{H}_m (1-\alpha)^m (\log K)^m}{\alpha^{m-1} m!} \right) \right)$$
$$\overset{(c)}{=} \lim_{K\to\infty} \left(\log((1-\alpha)\log K) - \mathrm{Ei}\left(-\frac{1-\alpha}{\alpha}\log K \right) \right),$$

where (a) is obtained using $\mathrm{I}_v(z) = \sum_{m=0}^{\infty} \frac{1}{\Gamma(m+v+1)m!} \left(\frac{z}{2}\right)^{2m+v}$, (b) follows from

$$\int_0^{\infty} \gamma^m \log(\gamma) \exp\left(-\frac{\gamma}{\alpha}\right) \mathrm{d}\gamma = \alpha^{m+1}\Gamma(m+1)\left(\log\alpha + \mathrm{H}_m - \mathbf{C}\right), \tag{A.32}$$

with H_m is the harmonic number, and (c) comes from $\sum_{m=0}^{\infty} \frac{(1-\alpha)^m (\log K)^m}{\alpha^{m-1} m!} = \alpha K^{\frac{1-\alpha}{\alpha}}$, and

$$\sum_{m=0}^{\infty} \frac{\mathrm{H}_m (1-\alpha)^m (\log K)^m}{\alpha^{m-1} m!} = \alpha K^{\frac{1-\alpha}{\alpha}} \left(\mathbf{C} - \mathrm{Ei}\left(-\frac{1-\alpha}{\alpha}\log K \right) + \log\left(\frac{1-\alpha}{\alpha}\log K \right) \right). \tag{A.33}$$

Now, since $\lim_{K\to\infty} \mathrm{Ei}\left(-\frac{1-\alpha}{\alpha}\log K \right) = 0$, then we have

$$\lim_{K\to\infty} \left[\widetilde{\mathcal{C}}^{-}_{\text{H-SNR}} - \log((1-\alpha)\log K) \right] = 0.$$

Appendix B

B.1 Proof of Corollary 6.2

Considering uniform power allocation over all transmit antennas, at all times, and using the expression of the achievable secrecy rate in (6.3), we have

$$\mathcal{C}_{\mathrm{s}}^{\mathrm{FF}} \geq \sum_{q=1}^{Q} \max_{\{\mathcal{H}_q\}} \mathop{\mathbb{E}}_{\mathbf{H}_{\mathrm{E}}|\mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q} \left[\left\{ \log \frac{\min\limits_{\mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q} \left| \mathbf{I}_{N_{\mathrm{R}}} + \frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{R}}^2 N_{\mathrm{T}}} \mathbf{H}_{\mathrm{R}} \mathbf{H}_{\mathrm{R}}^* \right|}{\left| \mathbf{I}_{N_{\mathrm{E}}} + \frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{E}}^2 N_{\mathrm{T}}} \mathbf{H}_{\mathrm{E}} \mathbf{H}_{\mathrm{E}}^* \right|} \right\}^+ \right] P_q \tag{B.1}$$

$$= \sum_{q=1}^{Q} \max_{\{\mathcal{H}_q\}} \mathop{\mathbb{E}}_{\boldsymbol{\lambda}_{\mathrm{E}}|\mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q} \left[\left\{ \min_{\substack{\boldsymbol{\lambda}_{\mathrm{R}} \\ \mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q}} \sum_{i=1}^{r_{\mathrm{R}}} \log\left(1+\frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{R}}^2 N_{\mathrm{T}}}\lambda_{\mathrm{R}_i}\right) - \sum_{i=1}^{r_{\mathrm{E}}} \log\left(1+\frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{E}}^2 N_{\mathrm{T}}}\lambda_{\mathrm{E}_i}\right) \right\}^+ \right] P_q, \tag{B.2}$$

with $r_{\mathrm{R}}=\min(N_{\mathrm{T}}, N_{\mathrm{R}})$, $r_{\mathrm{E}}=\min(N_{\mathrm{T}}, N_{\mathrm{E}})$, and $\boldsymbol{\lambda}_{\mathrm{R}}$ and $\boldsymbol{\lambda}_{\mathrm{E}}$ are the respective vectors of non-zeros eigenvalues of $\mathbf{H}_{\mathrm{R}}\mathbf{H}_{\mathrm{R}}^*$ and $\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{E}}^*$, i.e., $\boldsymbol{\lambda}_{\mathrm{R}}=\{\lambda_{\mathrm{R}_1}, \cdots, \lambda_{\mathrm{R}_{r_{\mathrm{R}}}}\}$ and $\boldsymbol{\lambda}_{\mathrm{E}}=\{\lambda_{\mathrm{E}_1}, \cdots, \lambda_{\mathrm{E}_{r_{\mathrm{E}}}}\}$. Taking $P_{\mathrm{avg}}\to\infty$, the terms $\frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{R}}^2 N_{\mathrm{T}}}\lambda_{\mathrm{R}_i}$ and $\frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{E}}^2 N_{\mathrm{T}}}\lambda_{\mathrm{E}_i}$, in (B.2), become dominant and we can write

$$\lim_{P_{\mathrm{avg}}\to\infty} \mathcal{C}_{\mathrm{s}}^{\mathrm{FF}} \geq \lim_{P_{\mathrm{avg}}\to\infty} \sum_{q=1}^{Q} \max_{\{\mathcal{H}_q\}} \mathop{\mathbb{E}}_{\boldsymbol{\lambda}_{\mathrm{E}}|\mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q} \left[\left\{ \min_{\substack{\boldsymbol{\lambda}_{\mathrm{R}} \\ \mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q}} \sum_{i=1}^{r_{\mathrm{R}}} \log\left(\frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{R}}^2 N_{\mathrm{T}}}\lambda_{\mathrm{R}_i}\right) - \sum_{i=1}^{r_{\mathrm{E}}} \log\left(\frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{E}}^2 N_{\mathrm{T}}}\lambda_{\mathrm{E}_i}\right) \right\}^+ \right] P_q$$

$$= \lim_{P_{\mathrm{avg}}\to\infty} \sum_{q=1}^{Q} \max_{\{\mathcal{H}_q\}} \mathop{\mathbb{E}}_{\boldsymbol{\lambda}_{\mathrm{E}}|\mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q} \left[\left\{ (r_{\mathrm{R}}-r_{\mathrm{E}}) \log \frac{P_{\mathrm{avg}}}{N_{\mathrm{T}}} + \min_{\substack{\boldsymbol{\lambda}_{\mathrm{R}} \\ \mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q}} \sum_{i=1}^{r_{\mathrm{R}}} \log \frac{\lambda_{\mathrm{R}_i}}{\sigma_{\mathrm{R}}^2} - \sum_{i=1}^{r_{\mathrm{E}}} \log \frac{\lambda_{\mathrm{E}_i}}{\sigma_{\mathrm{E}}^2} \right\}^+ \right] P_q. \tag{B.3}$$

We can, then, rewrite the limit in the following form

$$\lim_{P_{\mathrm{avg}}\to\infty} \left[\mathcal{C}_{\mathrm{s}}^{\mathrm{FF}} - \{r_{\mathrm{R}}-r_{\mathrm{E}}\}^+ \log \frac{P_{\mathrm{avg}}}{N_{\mathrm{T}}} \right] \geq \tag{B.4}$$

$$\lim_{P_{\mathrm{avg}}\to\infty} \sum_{q=1}^{Q} \max_{\{\mathcal{H}_q\}} \mathop{\mathbb{E}}_{\boldsymbol{\lambda}_{\mathrm{E}}|\mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q} \left[\left\{ (r_{\mathrm{R}}-r_{\mathrm{E}}) \log \frac{P_{\mathrm{avg}}}{N_{\mathrm{T}}} + \min_{\substack{\boldsymbol{\lambda}_{\mathrm{R}} \\ \mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q}} \sum_{i=1}^{r_{\mathrm{R}}} \log \frac{\lambda_{\mathrm{R}_i}}{\sigma_{\mathrm{R}}^2} - \sum_{i=1}^{r_{\mathrm{E}}} \log \frac{\lambda_{\mathrm{E}_i}}{\sigma_{\mathrm{E}}^2} \right\}^+ - \{r_{\mathrm{R}}-r_{\mathrm{E}}\}^+ \log \frac{P_{\mathrm{avg}}}{N_{\mathrm{T}}} \right] P_q.$$

In the special case when $r_{\mathrm{R}}{=}r_{\mathrm{E}}$, we get

$$\lim_{P_{\mathrm{avg}}\to\infty}\mathcal{C}_{\mathrm{s}}^{\mathrm{FF}}\geq\lim_{P_{\mathrm{avg}}\to\infty}\sum_{q=1}^{Q}\max_{\{\mathcal{H}_q\}}\mathop{\mathbb{E}}_{\boldsymbol{\lambda}_{\mathrm{E}}|\mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q}\left[\left\{\min_{\substack{\boldsymbol{\lambda}_{\mathrm{R}}\\ \mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q}}\sum_{i=1}^{r_{\mathrm{R}}}\log\frac{\lambda_{\mathrm{R}_i}}{\sigma_{\mathrm{R}}^2}-\sum_{i=1}^{r_{\mathrm{E}}}\log\frac{\lambda_{\mathrm{E}_i}}{\sigma_{\mathrm{E}}^2}\right\}^{+}\right]P_q. \quad \text{(B.5)}$$

When $r_{\mathrm{R}}\neq r_{\mathrm{E}}$, we use the fact that the term $(r_{\mathrm{R}}-r_{\mathrm{E}})\log\frac{P_{\mathrm{avg}}}{N_{\mathrm{T}}}$ is dominant, and that $\{a{+}b\}^{+}{-}\{a\}^{+}{=}\begin{cases}b & \text{if } a>0\\ 0 & \text{otherwise}\end{cases}$, when a is dominant[1], to get

$$\lim_{P_{\mathrm{avg}}\to\infty}\left[\mathcal{C}_{\mathrm{s}}^{\mathrm{FF}}{-}\{r_{\mathrm{R}}{-}r_{\mathrm{E}}\}^{+}\log\frac{P_{\mathrm{avg}}}{N_{\mathrm{T}}}\right]\geq\begin{cases}\displaystyle\sum_{q=1}^{Q}\max_{\{\mathcal{H}_q\}}\mathop{\mathbb{E}}_{\boldsymbol{\lambda}_{\mathrm{E}}|\mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q}\left[\min_{\substack{\boldsymbol{\lambda}_{\mathrm{R}}\\ \mathbf{H}_{\mathrm{R}}\in\mathcal{H}_q}}\sum_{i=1}^{r_{\mathrm{R}}}\log\frac{\lambda_{\mathrm{R}_i}}{\sigma_{\mathrm{R}}^2}-\sum_{i=1}^{r_{\mathrm{E}}}\log\frac{\lambda_{\mathrm{E}_i}}{\sigma_{\mathrm{E}}^2}\right]P_q & \text{if } r_{\mathrm{R}}{\geq}r_{\mathrm{E}}\\ 0 & \text{if } r_{\mathrm{R}}{<}r_{\mathrm{E}}\end{cases},$$

This concludes our proof. □

B.2 Proof of Corollary 6.3

- Lower Bounding the Secrecy Capacity with Perfect CSI at High SNR: We distinguish between two cases depending on the number of transmit antennas compared to the number of receive antennas.

- First Case: $N_{\mathrm{T}}{\leq}N_{\mathrm{R}}$

Using the expression of the ergodic secrecy capacity, in (6.7), and considering uniform power allocation over all transmit antennas, we can write

$$\lim_{P_{\mathrm{avg}}\to\infty}\mathcal{C}_{\mathrm{s}}\geq\lim_{P_{\mathrm{avg}}\to\infty}\mathop{\mathbb{E}}_{\mathbf{H}_{\mathrm{E}},\mathbf{H}_{\mathrm{R}}}\left[\left\{\log\frac{\left|\mathbf{I}_{N_{\mathrm{R}}}+\frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{R}}^2N_{\mathrm{T}}}\mathbf{H}_{\mathrm{R}}\mathbf{H}_{\mathrm{R}}^{*}\right|}{\left|\mathbf{I}_{N_{\mathrm{E}}}+\frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{E}}^2N_{\mathrm{T}}}\mathbf{H}_{\mathrm{E}}\mathbf{H}_{\mathrm{E}}^{*}\right|}\right\}^{+}\right] \quad \text{(B.6)}$$

$$=\lim_{P_{\mathrm{avg}}\to\infty}\mathop{\mathbb{E}}_{\boldsymbol{\lambda}_{\mathrm{R}},\boldsymbol{\lambda}_{\mathrm{E}}}\left[\left\{\sum_{i=1}^{N_{\mathrm{T}}}\log\left(1+\frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{R}}^2N_{\mathrm{T}}}\lambda_{\mathrm{R}_i}\right)-\sum_{i=1}^{\min(N_{\mathrm{T}},N_{\mathrm{E}})}\log\left(1+\frac{P_{\mathrm{avg}}}{\sigma_{\mathrm{E}}^2N_{\mathrm{T}}}\lambda_{\mathrm{E}_i}\right)\right\}^{+}\right] \quad \text{(B.7)}$$

[1] a is dominant in the sense that the sign of $a{+}b$ is dictated by the sign of a.

$$= \lim_{P_{\text{avg}}\to\infty} \mathop{\mathbb{E}}_{\boldsymbol{\lambda}_{\text{R}},\boldsymbol{\lambda}_{\text{E}}} \left[\left\{ \sum_{i=1}^{N_{\text{T}}} \log\left(\frac{P_{\text{avg}}}{\sigma_{\text{R}}^2 N_{\text{T}}}\lambda_{\text{R}_i}\right) - \sum_{i=1}^{\min(N_{\text{T}},N_{\text{E}})} \log\left(\frac{P_{\text{avg}}}{\sigma_{\text{E}}^2 N_{\text{T}}}\lambda_{\text{E}_i}\right) \right\}^+ \right] \tag{B.8}$$

$$= \lim_{P_{\text{avg}}\to\infty} \mathop{\mathbb{E}}_{\boldsymbol{\lambda}_{\text{R}},\boldsymbol{\lambda}_{\text{E}}} \left[\left\{ \{N_{\text{T}}-N_{\text{E}}\}^+ \log\frac{P_{\text{avg}}}{N_{\text{T}}} + \sum_{i=1}^{N_{\text{T}}} \log\frac{\lambda_{\text{R}_i}}{\sigma_{\text{R}}^2} - \sum_{i=1}^{\min(N_{\text{T}},N_{\text{E}})} \log\frac{\lambda_{\text{E}_i}}{\sigma_{\text{E}}^2} \right\}^+ \right], \tag{B.9}$$

where $\boldsymbol{\lambda}_{\text{R}}$ and $\boldsymbol{\lambda}_{\text{E}}$ are the respective vectors of non-zeros eigenvalues of $\mathbf{H}_{\text{R}}\mathbf{H}_{\text{R}}^*$ and $\mathbf{H}_{\text{E}}\mathbf{H}_{\text{E}}^*$, i.e., $\boldsymbol{\lambda}_{\text{R}}=\{\lambda_{\text{R}_1},\cdots,\lambda_{\text{R}_{r_{\text{R}}}}\}$ and $\boldsymbol{\lambda}_{\text{E}}=\{\lambda_{\text{E}_1},\cdots,\lambda_{\text{E}_{r_{\text{E}}}}\}$. Then, using the fact that, when a is dominant, $\{a+b\}^+-\{a\}^+ = \begin{cases} b & \text{if } a>0 \\ 0 & \text{otherwise} \end{cases}$, we get the following result

$$\lim_{P_{\text{avg}}\to\infty}\left[\mathcal{C}_{\text{s}} - \{N_{\text{T}}-N_{\text{E}}\}^+\log\frac{P_{\text{avg}}}{N_{\text{T}}}\right] \geq \begin{cases} 0 & \text{if } N_{\text{T}}<N_{\text{E}} \\ \mathop{\mathbb{E}}_{\boldsymbol{\lambda}_{\text{R}},\boldsymbol{\lambda}_{\text{E}}}\left[\sum_{i=1}^{N_{\text{T}}}\log\frac{\lambda_{\text{R}_i}}{\sigma_{\text{R}}^2} - \sum_{i=1}^{N_{\text{E}}}\log\frac{\lambda_{\text{E}_i}}{\sigma_{\text{E}}^2}\right] & \text{if } N_{\text{E}}\leq N_{\text{T}}\leq N_{\text{R}} \end{cases}.$$

- Second Case: $N_{\text{T}}>N_{\text{R}}$

When $N_{\text{T}}>N_{\text{R}}$, we consider a uniform power transmitting scheme that broadcasts artificial noise over the null space of $\mathbf{H}_{\text{R}}$. Let $\mathbf{H}_{\text{R}} = \mathbf{U}_{\text{R}}\boldsymbol{\lambda}_{\text{R}}\mathbf{V}_{\text{R}}^*$ be the singular value decomposition (SVD) of $\mathbf{H}_{\text{R}}$, where $\mathbf{U}_{\text{R}} \in \mathbb{C}^{N_{\text{R}}\times N_{\text{R}}}$ and $\mathbf{V}_{\text{R}} \in \mathbb{C}^{N_{\text{T}}\times N_{\text{T}}}$ are unitary matrices. Then, we can write matrix $\mathbf{V}_{\text{R}}$ in the form $\mathbf{V}_{\text{R}} = [\tilde{\mathbf{V}}_{\text{R}}, \mathbf{Z}]$, with $\mathbf{Z} = \text{null}(\mathbf{H}_{\text{R}}) \in \mathbb{C}^{N_{\text{T}}\times(N_{\text{T}}-N_{\text{R}})}$, such that $\mathbf{H}_{\text{R}}\mathbf{Z} = 0_{N_{\text{R}}\times(N_{\text{T}}-N_{\text{R}})}$ and the N_{R} columns of $\tilde{\mathbf{V}}_{\text{R}} \in \mathbb{C}^{N_{\text{T}}\times N_{\text{R}}}$ span the orthogonal complement subspace to $\mathbf{Z}$. Since perfect CSI is assumed in this case, the transmitter has perfect knowledge of the precoding matrix $\mathbf{V}_{\text{R}}$ and transmits $\mathbf{X}=\sqrt{P_{\text{avg}}/N_{\text{T}}}\left(\tilde{\mathbf{V}}_{\text{R}}\mathbf{u}+\mathbf{Z}\mathbf{v}\right)$, where $\mathbf{u} \in \mathbb{C}^{N_{\text{R}}}$ is the information vector and $\mathbf{v} \in \mathbb{C}^{N_{\text{T}}-N_{\text{R}}}$ is the artificial noise vector. Both $\mathbf{u}$ and $\mathbf{v}$ are assumed to be circular symmetric Gaussian random vectors with i.i.d. zero mean and unit variance entries. The respective received signals at the intended receiver and the eavesdropper can, then, be written as

$$\begin{aligned} \mathbf{Y}_{\text{R}} &= \sqrt{\frac{P_{\text{avg}}}{N_{\text{T}}}}\mathbf{H}_{\text{R}}\tilde{\mathbf{V}}_{\text{R}}\mathbf{u} + \mathbf{Z}_{\text{R}} \\ \mathbf{Y}_{\text{E}} &= \sqrt{\frac{P_{\text{avg}}}{N_{\text{T}}}}\mathbf{H}_{\text{E}}\tilde{\mathbf{V}}_{\text{R}}\mathbf{u} + \sqrt{\frac{P_{\text{avg}}}{N_{\text{T}}}}\mathbf{H}_{\text{E}}\mathbf{Z}\mathbf{v} + \mathbf{Z}_{\text{E}}. \end{aligned} \tag{B.10}$$

Hence, the secrecy capacity can be characterized, in the high-SNR regime, as

$$\lim_{P_{\rm avg}\to\infty}\mathcal{C}_{\rm s}\geq\lim_{P_{\rm avg}\to\infty}\mathop{\mathbb{E}}_{\mathbf{H}_{\rm E},\mathbf{H}_{\rm R}}\left[\left\{\log\left|\mathbf{I}_{N_{\rm R}}+\frac{P_{\rm avg}}{\sigma_{\rm R}^2N_{\rm T}}\mathbf{H}_{\rm R}\mathbf{H}_{\rm R}^*\right|-\log\frac{\left|\mathbf{I}_{N_{\rm E}}+\frac{P_{\rm avg}}{\sigma_{\rm E}^2N_{\rm T}}\mathbf{H}_{\rm E}\mathbf{H}_{\rm E}^*+\frac{P_{\rm avg}}{\sigma_{\rm E}^2N_{\rm T}}\mathbf{H}_{\rm E}\mathbf{Z}\mathbf{Z}^*\mathbf{H}_{\rm E}^*\right|}{\left|\mathbf{I}_{N_{\rm E}}+\frac{P_{\rm avg}}{\sigma_{\rm E}^2N_{\rm T}}\mathbf{H}_{\rm E}\mathbf{Z}\mathbf{Z}^*\mathbf{H}_{\rm E}^*\right|}\right\}^+\right]$$

$$=\lim_{P_{\rm avg}\to\infty}\mathop{\mathbb{E}}_{\boldsymbol{\lambda}_{\rm R},\boldsymbol{\lambda}_{\rm EZ},\boldsymbol{\lambda}_{\rm sum}}\left[\left\{\sum_{i=1}^{N_{\rm R}}\log\left(1+\frac{P_{\rm avg}}{\sigma_{\rm R}^2N_{\rm T}}\lambda_{{\rm R}_i}\right)+\sum_{i=1}^{\min(N_{\rm T}-N_{\rm R},N_{\rm E})}\log\left(1+\frac{P_{\rm avg}}{\sigma_{\rm E}^2N_{\rm T}}\lambda_{{\rm EZ}_i}\right)-\sum_{i=1}^{N_{\rm E}}\log\left(1+\frac{P_{\rm avg}}{\sigma_{\rm E}^2N_{\rm T}}\lambda_{{\rm sum}_i}\right)\right\}^+\right]$$

$$=\lim_{P_{\rm avg}\to\infty}\mathop{\mathbb{E}}_{\boldsymbol{\lambda}_{\rm R},\boldsymbol{\lambda}_{\rm EZ},\boldsymbol{\lambda}_{\rm sum}}\left[\left\{\sum_{i=1}^{N_{\rm R}}\log\left(\frac{P_{\rm avg}}{\sigma_{\rm R}^2N_{\rm T}}\lambda_{{\rm R}_i}\right)+\sum_{i=1}^{\min(N_{\rm T}-N_{\rm R},N_{\rm E})}\log\left(\frac{P_{\rm avg}}{\sigma_{\rm E}^2N_{\rm T}}\lambda_{{\rm EZ}_i}\right)-\sum_{i=1}^{N_{\rm E}}\log\left(\frac{P_{\rm avg}}{\sigma_{\rm E}^2N_{\rm T}}\lambda_{{\rm sum}_i}\right)\right\}^+\right]$$

$$=\lim_{P_{\rm avg}\to\infty}\mathop{\mathbb{E}}_{\substack{\boldsymbol{\lambda}_{\rm R},\boldsymbol{\lambda}_{\rm EZ},\\ \boldsymbol{\lambda}_{\rm sum}}}\left[\left\{\min\left(N_{\rm T}-N_{\rm E},N_{\rm R}\right)\log\frac{P_{\rm avg}}{N_{\rm T}}+\sum_{i=1}^{N_{\rm R}}\log\frac{\lambda_{{\rm R}_i}}{\sigma_{\rm R}^2}+\sum_{i=1}^{\min(N_{\rm T}-N_{\rm R},N_{\rm E})}\log\frac{\lambda_{{\rm EZ}_i}}{\sigma_{\rm E}^2}-\sum_{i=1}^{N_{\rm E}}\log\frac{\lambda_{{\rm sum}_i}}{\sigma_{\rm E}^2}\right\}^+\right]$$

where $\boldsymbol{\lambda}_{\rm R}$, $\boldsymbol{\lambda}_{\rm E}$, $\boldsymbol{\lambda}_{\rm EZ}$ and $\boldsymbol{\lambda}_{\rm sum}$ are the respective vectors of non-zeros eigenvalues of $\mathbf{H}_{\rm R}\mathbf{H}_{\rm R}^*$, $\mathbf{H}_{\rm E}\mathbf{H}_{\rm E}^*$, $\mathbf{H}_{\rm E}\mathbf{Z}\mathbf{Z}^*\mathbf{H}_{\rm E}^*$ and $(\mathbf{H}_{\rm E}\mathbf{H}_{\rm E}^*+\mathbf{H}_{\rm E}\mathbf{Z}\mathbf{Z}^*\mathbf{H}_{\rm E}^*)$, i.e., $\boldsymbol{\lambda}_{\rm R}=\{\lambda_{{\rm R}_1},\cdots,\lambda_{{\rm R}_{r_{\rm R}}}\}$, $\boldsymbol{\lambda}_{\rm E}=\{\lambda_{{\rm E}_1},\cdots,\lambda_{{\rm E}_{r_{\rm E}}}\}$, $\boldsymbol{\lambda}_{\rm EZ}=\{\lambda_{{\rm EZ}_1},\cdots,\lambda_{{\rm EZ}_{r_{\rm EZ}}}\}$ and $\boldsymbol{\lambda}_{\rm sum}=\{\lambda_{{\rm sum}_1},\cdots,\lambda_{{\rm sum}_{r_{\rm sum}}}\}$. Once again, using the fact that, when a is dominant, $\{a+b\}^+-\{a\}^+=\begin{cases}b & \text{if } a>0\\ 0 & \text{otherwise}\end{cases}$, we obtain

$$\lim_{P_{\rm avg}\to\infty}\left[\mathcal{C}_{\rm s}-\min\left(\{N_{\rm T}-N_{\rm E}\}^+,N_{\rm R}\right)\log\frac{P_{\rm avg}}{N_{\rm T}}\right]\geq$$

$$\begin{cases}0 & \text{if } N_{\rm T}<N_{\rm E}\\ \mathop{\mathbb{E}}_{\substack{\boldsymbol{\lambda}_{\rm R},\boldsymbol{\lambda}_{\rm EZ},\\ \boldsymbol{\lambda}_{\rm sum}}}\left[\sum_{i=1}^{N_{\rm R}}\log\frac{\lambda_{{\rm R}_i}}{\sigma_{\rm R}^2}+\sum_{i=1}^{\min(N_{\rm T}-N_{\rm R},N_{\rm E})}\log\frac{\lambda_{{\rm EZ}_i}}{\sigma_{\rm E}^2}-\sum_{i=1}^{N_{\rm E}}\log\frac{\lambda_{{\rm sum}_i}}{\sigma_{\rm E}^2}\right] & \text{if } N_{\rm T}>\max(N_{\rm E},N_{\rm R})\end{cases}. \tag{B.11}$$

- Upper Bounding the Secrecy Capacity with Perfect CSI at High SNR: Since the secrecy capacity when both the main and the eavesdropper's CSI are available at the transmitter upper bounds the secrecy capacity when only the main CSI is known at the transmitter, the upper bound in (6.13) results directly from [37, Theorem 2] and [63]. This concludes our proof. □

B.3 Proof of Corollary 6.4

Considering uniform power allocation over all transmit antennas, the constants θ_1 and θ_2 in Corollary 2 and Corollary 3, respectively, are equal to their respective lour bounding terms. Thus, the asymptotic difference between $\mathcal{C}_{\rm s}$ and $\mathcal{C}_{\rm s}^{-}$ can be characterized, when $N_{\rm T} \leq N_{\rm R}$, as

$$\begin{aligned}
&\lim_{P_{\rm avg}\to\infty}\left[\mathcal{C}_{\rm s}-\mathcal{C}_{\rm s}^{-}\right] \\
&= \mathop{\mathbb{E}}_{\boldsymbol{\lambda}_{\rm R},\boldsymbol{\lambda}_{\rm E}}\left[\sum_{i=1}^{N_{\rm T}}\log\frac{\lambda_{{\rm R}_i}}{\sigma_{\rm R}^2}-\sum_{i=1}^{N_{\rm E}}\log\frac{\lambda_{{\rm E}_i}}{\sigma_{\rm E}^2}\right]-\sum_{q=1}^{Q}\max_{\{\mathcal{H}_q\}}\mathop{\mathbb{E}}_{\boldsymbol{\lambda}_{\rm E}}\left[\min_{\substack{\boldsymbol{\lambda}_{\rm R}\\ \mathbf{H}_{\rm R}\in\mathcal{H}_q}}\sum_{i=1}^{N_{\rm T}}\log\frac{\lambda_{{\rm R}_i}}{\sigma_{\rm R}^2}-\sum_{i=1}^{N_{\rm E}}\log\frac{\lambda_{{\rm E}_i}}{\sigma_{\rm E}^2}\right]P_q \quad \text{(B.12)}\\
&= \mathop{\mathbb{E}}_{\boldsymbol{\lambda}_{\rm R},\boldsymbol{\lambda}_{\rm E}}\left[\sum_{i=1}^{N_{\rm T}}\log\frac{\lambda_{{\rm R}_i}}{\sigma_{\rm R}^2}-\sum_{i=1}^{N_{\rm E}}\log\frac{\lambda_{{\rm E}_i}}{\sigma_{\rm E}^2}-\sum_{q=1}^{Q}\max_{\{\mathcal{H}_q\}}\min_{\substack{\boldsymbol{\lambda}_{\rm R}\\ \mathbf{H}_{\rm R}\in\mathcal{H}_q}}\sum_{i=1}^{N_{\rm T}}\log\frac{\lambda_{{\rm R}_i}}{\sigma_{\rm R}^2}-\sum_{i=1}^{N_{\rm E}}\log\frac{\lambda_{{\rm E}_i}}{\sigma_{\rm E}^2}P_q\right] \quad \text{(B.13)}\\
&= \mathop{\mathbb{E}}_{\boldsymbol{\lambda}_{\rm R}}\left[\sum_{i=1}^{N_{\rm T}}\log\lambda_{{\rm R}_i}-\sum_{q=1}^{Q}\max_{\{\mathcal{H}_q\}}P_q\min_{\substack{\boldsymbol{\lambda}_{\rm R}\\ \mathbf{H}_{\rm R}\in\mathcal{H}_q}}\sum_{i=1}^{N_{\rm T}}\log\lambda_{{\rm R}_i}\right] \quad \text{(B.14)}
\end{aligned}$$

where $\boldsymbol{\lambda}_{\rm R}$ and $\boldsymbol{\lambda}_{\rm E}$ are the respective vectors of non-zeros eigenvalues of $\mathbf{H}_{\rm R}\mathbf{H}_{\rm R}^{*}$ and $\mathbf{H}_{\rm E}\mathbf{H}_{\rm E}^{*}$, i.e., $\boldsymbol{\lambda}_{\rm R}=\{\lambda_{{\rm R}_1},\cdots,\lambda_{{\rm R}_{r_{\rm R}}}\}$ and $\boldsymbol{\lambda}_{\rm E}=\{\lambda_{{\rm E}_1},\cdots,\lambda_{{\rm E}_{r_{\rm E}}}\}$. The gap between $\mathcal{C}_{\rm s}$ and $\widetilde{\mathcal{C}}_{\rm s}^{-}$ can be deduced, directly, using $\{a\}^{+}-a=\{-a\}^{+}$. $\square$

Appendix C

Submitted and Accepted Publications

Book Chapter:

• Amal Hyadi, Zouheir Rezki and Mohamed-Slim Alouini, "Secure Data Networks with Channel Uncertainty", *To appear in the upcoming IET Book: Trusted Communications with Physical Layer Security for 5G and Beyond*, Oct. 2017.

Journal Papers:

• Amal Hyadi, Zouheir Rezki, and Mohamed-Slim Alouini, "Secure Multiple-Antenna Block-Fading Wiretap Channels with Limited CSI Feedback", *accepted for publication in IEEE Transactions on Wireless Communications*.

• Amal Hyadi, Zouheir Rezki, and Mohamed-Slim Alouini, "An Overview of Physical Layer Security in Wireless Communication Systems with CSIT Uncertainty", *IEEE Access*, vol. 4, pp. 6121-6132, Sep. 2016.

• Amal Hyadi, Zouheir Rezki, Ashish Khisti and Mohamed-Slim Alouini, "Secure Broadcasting with Imperfect Channel State Information at the Transmitter", *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp 2215-2230, Mar. 2016.

• Amal Hyadi, Mustapha Benjillali, and Mohamed-Slim Alouini, "Outage Performance of Decode-and-Forward in Two-Way Relaying with Perfect and Outdated Channel State Information", *IEEE Transactions on Vehicular Technology*, vol. 64, no. 12, pp 5940-5947, Dec. 2015.

• Amal Hyadi, Mustapha Benjillali, Mohamed-Slim Alouini, and Daniel Benevides, "Performance Analysis of Underlay Cognitive Multihop Regenerative Relaying Systems with Multiple Primary Receivers", *IEEE Transactions on Wireless Communications*, vol. 12, no. 12, pp 6418-6429, Dec. 2013.

• Amal Hyadi, Zouheir Rezki, and Mohamed-Slim Alouini, "Securing Multi-User Broadcast Wiretap Channels with Finite CSI Feedback", *to be submitted shortly to IEEE Transactions on Information Theory.*

• Amal Hyadi, Zouheir Rezki, Fabrice Labeau, and Mohamed-Slim Alouini, "Physical Layer Security for D2D Communications Underlaying Cellular Networks", *to be submitted shortly to IEEE Journal on Selected Areas of Communication.*

Conference Papers:

• Amal Hyadi, Zouheir Rezki, Fabrice Labeau, and Mohamed-Slim Alouini, "Joint Secrecy for D2D Communications Underlaying Cellular Networks", *accepted for publication in IEEE Global Communications Conference (Globecom'2017) Proceedings.*

• Amal Hyadi, Zouheir Rezki, and Mohamed-Slim Alouini, "On the Secrecy Capacity Region of the Block-Fading BCC with Limited CSI Feedback", *in Proceedings of IEEE Global Communications Conference (Globecom'2016)*, Washington, DC, USA, Dec. 2016.

• Amal Hyadi, Zouheir Rezki, and Mohamed-Slim Alouini, "On the Secrecy Capacity of the Broadcast Wiretap Channel with Limited CSI Feedback", *in Proceedings of IEEE Information Theory Workshop (ITW'2016)*, Cambridge, UK, Sep. 2016.

• Amal Hyadi, Zouheir Rezki, and Mohamed-Slim Alouini, "On the Secrecy Capacity of the Multiple-Antenna Wiretap Channel with Limited CSI Feedback", *in Proceed-*

ings of IEEE Global Communications Conference (Globecom'2015), San Diego, CA, USA, Dec. 2015.

• Amal Hyadi, Zouheir Rezki, Ashish Khisti, and Mohamed-Slim Alouini, "On the Secrecy Capacity of the Broadcast Wiretap Channel with Imperfect Channel State Information", *in Proceedings of IEEE Global Communications Conference (Globecom'2014)*, Austin, TX, USA, Dec. 2014.

• Ibrahim Alabdulmohsin, Amal Hyadi, Laila Afify, and Basem Shihada, "End-to-End Delay Analysis in Wireless Sensor Networks with Service Vacation", *in Proceedings of IEEE Wireless Communications and Networking Conference (WCNC'2014)*, Istanbul, Turkey, Apr. 2014.

• Amal Hyadi, Mehdi Driouch, Wessam Ajib, and Mohamed-Slim Alouini, "Overlay Cognitive Radio Systems with Adaptive Two-Way Relaying", *in Proceedings of IEEE Global Communications Conference (Globecom'2013)*, Atlanta, GA, USA, Dec. 2013.

• Mustapha Benjillali, Amal Hyadi, Daniel Benevides, and Mohamed-Slim Alouini, "Performance Analysis of Cognitive Multihop Relaying with M-QAM Detect-and-Forward in Nakagami-m Fading Channels", *in Proceedings of IEEE 24th International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC'2013)*, London, UK, Sept. 2013, pp. 636-640.

• Amal Hyadi, Mustapha Benjillali, and Mohamed-Slim Alouini, "Outage Performance of Two-Way DF Relaying System swith a New Relay Selection Metric", *in Proceedings of IEEE Wireless Communications and Networking Conference (WCNC'2012)*, Paris, France, Apr. 2012, pp. 570-574.