2009

Physical layer security in wireless networks: intelligent jamming and eavesdropping

George Traian Amariucai
Louisiana State University and Agricultural and Mechanical College

PHYSICAL LAYER SECURITY IN WIRELESS NETWORKS: INTELLIGENT JAMMING AND EAVESDROPPING

A Dissertation

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

in

The Department of Electrical and Computer Engineering

by
George Traian Amariucai
B.S., University Politehnica of Bucharest, 2003
M.S., University Politehnica of Bucharest, 2004
August, 2009

Acknowledgments

This dissertation would not be possible without the contribution of several people. First and foremost, I would like to thank my adviser, Dr. Shuangqing Wei, for carefully guiding my steps and for providing me with the best work environment. Our discussions helped me tremendously in acquiring a good understanding of many topics, both related and unrelated to this dissertation.

Special thanks to Dr. Rajgopal Kannan for providing insights into some of the problems encountered along the way, and to all the other members of my dissertation committee for their constructive comments: Dr. Blaise Bourdin, Dr. Guoxiang Gu and Dr. Morteza Naraghi-Pour.

I would like to thank my best friend and fiancee, Raluca Cozma, for making my life wonderful all these years, and for being equally enthusiastic and helpful about all my ideas of having fun, whether it was going fishing at 4 a.m. or replacing the clutch on the car.

I dedicate this work to my mother, Geta Amariucai, to whom I owe more than I will ever be able to repay.

Table of Contents

Abstract

This work aims at addressing two critical security issues residing in the physical layer of wireless networks, namely, intelligent jamming and eavesdropping.

In the first two chapters we study the problem of jamming in a fixed-rate transmission system with fading, under the general assumption that the jammer has no knowledge about either the codebook used by the legitimate communication terminals, or the source's output. Both transmitter and jammer are subject to power constraints which can be enforced over each codeword (peak) or over all codewords (average). All our jamming problems are formulated as zero-sum games, having the probability of outage as pay-off function and power control functions as strategies. We provide a comprehensive coverage of these problems, under fast and slow fading, peak and average power constraints, pure and mixed strategies, with and without channel state information (CSI) feedback.

Contributions to the eavesdropping problem include a novel feedback scheme for transmitting secret messages between two legitimate parties, over an eavesdropped communication link, presented in Chapter 4. Relative to Wyner's traditional encoding scheme, our feedback-based encoding often yields larger rate-equivocation regions and achievable secrecy rates. More importantly, by exploiting the channel randomness inherent in the feedback channels, our scheme achieves a strictly positive secrecy rate even when the eavesdropper's channel is less noisy than the legitimate receiver's channel.

In Chapter 5, we study the problem of active eavesdropping in fast fading channels. The active eavesdropper is a more powerful adversary than the classical eavesdropper. It can choose between two functional modes: eavesdropping the transmission between the legitimate parties (Ex mode), and jamming it (Jx mode) – the active eavesdropper cannot function in full duplex mode. We consider two scenarios: the best-case scenario, when the transmitter knows the eavesdropper's strategy in advance – and hence can adaptively choose an encoding strategy – and the worst-case scenario,

when the active eavesdropper can choose its strategy based on the legitimate transmitter-receiver pair's strategy – and thus the transmitter and legitimate receiver have to plan for the worst. For the second scenario, we introduce a novel encoding scheme, based on very limited and unprotected feedback – the *Block-Markov Wyner (BMW) encoding scheme* – which outperforms any schemes currently available.

Chapter 1
Introduction

As the title suggests, the present dissertation is focused on the physical layer security in wireless networks. The concept of *communication security* is linked to two main desired features. The first of these is the *system reliability*, which means that a certain message (encoded for transmission and transmitted over a wireless channel) intended for a specific user (or "legitimate receiver"), should be reliably received by that user. In practical terms, the legitimate receiver's decoding error should satisfy an acceptable specification. The "enemy" of system reliability is called a *jammer*. The purpose of a jammer is solely to disrupt the process of communication by increasing the legitimate receiver's probability of decoding error, and/or by causing "reliability outage".

The second of the desired features is *message secrecy*, which means that under certain conditions, a transmitter may want to communicate a secret message to a legitimate receiver. The "enemy" of message secrecy is called an *eavesdropper*. The sole purpose of an eavesdropper is to listen to the transmission, and try to understand the secret messages encoded therein.

In this dissertation, we treat the issues of security at the *physical layer* of the Open Systems Interconnection (OSI) reference model. Although throughout the following chapters we may sometimes specify simple protocols pertaining to upper layers, our main focus will remain on channel encoding and power allocation.

In the next two sections we provide a series of brief comments about the evolution and the main ideas behind *system reliability* and *message secrecy*.

1.1 Jamming in Wireless Networks

The problem of jamming in wireless networks started to attract interests in the 80's when several works [3, 4] studied simple, point-to-point communication systems affected by intelligent jammers, as shown in Figure 1.1. The jammer was assumed to have access to either a noise-distorted version

of the transmitter's output [3], or the transmitter's input message [4]. The jamming problem was formulated as a two-player, zero-sum game, with the mean-squared error of the decoded message, relative to the transmitted message, as objective.

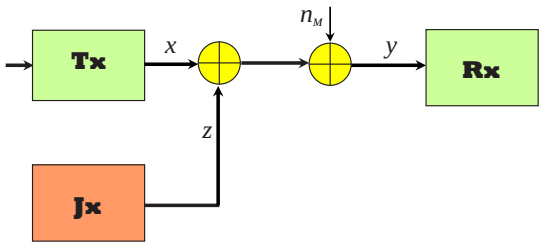

FIGURE 1.1. A simple point-to-point jamming problem.

The saddle-point policy of the jamming game formulated in [3] consists of an amplifying transmitter and a jammer that performs a linear transformation of the transmitter's output signal. A deterministic problem (shown to display no saddle point) and a probabilistic one are investigated in [4]. It is interesting to note that for the probabilistic formulation, the saddle point is attained when the jammer ignores its information about the transmitter's output. Similar results were obtained in [5] for correlated jammers suffering from phase/time jitters at acquisition or at transmission. Again the jamming problem was formulated as a game, but this time having the channel capacity as objective function.

Relatively few papers on this subject followed until lately, when several extensions to more complex, multi-user channels with fading were derived in [6–10]. It is shown in [7] that, in the absence of channel state information (CSI) at both transmitter and jammer, an equilibrium point is obtained when the jammer completely ignores its information about the encoder's output.

Broadcast (BC) and multiple access channels (MAC) are investigated in [8] under the assumption of complete CSI and uncorrelated jammer. The sum-rate is used as objective of the jamming game for the broadcast channel scenario, while this role is played by an arbitrary weighting of the user's rates for the MAC. Proofs of existence of multiple Nash equilibria and conditions for uniqueness are provided. Similar results for the multiple access channel are presented in [9]. The

paper covers all possible cases in terms of CSI and correlation of the jammer with transmitter's output, for a two-transmitter, one jammer scenario.

The general tendency seems to be in favor of an assumption that the jammer has access to either the transmitter's output or input and consequently is able to produce correlated jamming signals. Uncorrelated jammers are often studied only as particular cases of the more complex correlated jamming scenarios.

Most of the recent works [7, 9] that study the jamming games in fading channels focus on fast fading, and consequently adopt the ergodic capacity as objective of the game. An interesting point of view is expressed in [11], where the jamming problem is differently viewed as a special case of an arbitrarily varying channel. The capacity (when it exists) and λ-capacity (maximum transmission rate that guarantees a probability of error less than λ) are given for both peak and average power constraints, under random coding.

1.2 Eavesdropping in Wireless Networks

The pioneering work in message secrecy at the physical layer belongs to Wyner [12]. In 1975, Wyner shows that physical layer secrecy is possible without the use of a secret key. The concept of *wire-tap channel* is introduced by [12] for the first time. The wire-tapper is a particular form of eavesdropper, with the specific characteristic that the wire-tapper's channel is a degraded version of the legitimate receiver's channel, as shown in Figure 1.2.

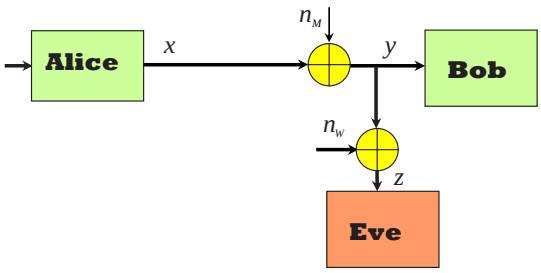

FIGURE 1.2. Wyner's wiretapper channel.

The secrecy, or "equivocation" is defined as the wire-tapper's conditional entropy (or uncertainty) of the secret message, given its own received signal. Unlike the previous cryptographic

approach to message secrecy, which assumes that the eavesdropper is unable to solve certain computational problems, Wyner's information-theoretic secrecy guarantees the privacy of the transmitted message at the physical layer, without any assumptions on the wire-tapper's capabilities. In that sense, physical layer secrecy is the strongest form of secrecy available to communication systems.

It is shown in [12] that for any discrete channels, the secrecy rate is given by the supremum over all possible input distributions of the difference between two information quantities: the mutual information between transmitter and legitimate receiver, and the mutual information between transmitter and wiretapper.

The generalization to the case when the eavesdropper's channel is not necessarily a degraded version of the receiver's channel (hence the introduction of the term "eavesdropper") was tackled in [13], in the extended context of a broadcast channel, where secret, non-secret and common messages need to be communicated. The achievable secrecy rate is shown to be always positive only if the legitimate receiver's channel is in a certain relationship with the eavesdropper's channel. In [13], this relationship was first denoted by saying that the main channel is *less noisy* than the eavesdropper's channel. It is also notable that the results in [13] imply that when secret messages are transmitted to the legitimate receiver at a rate arbitrarily close to the secrecy capacity, no common message (i.e. a message intended for both the legitimate receiver and the eavesdropper) can be successfully transmitted.

However, the results of [13] are mainly formulated in terms of single letter information measures, which means that for finding the secrecy capacity of a specific eavesdropper channel, one would have to perform a functional optimization over at least one probability distribution. This is why we should recognize the importance of more recent works, which elaborate the generic results of [13] for special, widely used channel models. For example, [14] shows that for any pair of discrete channels of which the eavesdropper's channel is *more noisy* in the sense of [13], the secrecy capacity equals the difference between the receiver's and wiretapper's channel capacities.

An extension to continuous alphabets appears in [15], which uses similar techniques as [12] to prove that the same result holds for Gaussian wire-tap channel.

A geometrical interpretation of the encoding technique used in [12], [15] for achieving the secrecy capacity is shown in Figure 1.3 for Gaussian channels. To understand this description, the reader should already be familiar to the geometric interpretation of the *channel coding theorem*.

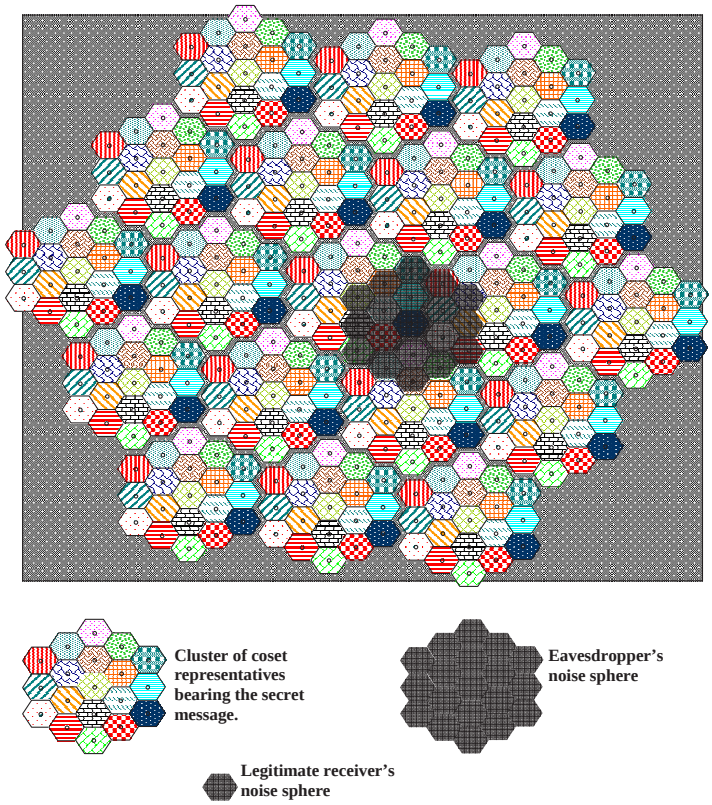

FIGURE 1.3. Achieving the secrecy capacity of an eavesdropped Gaussian channel.

In Figure 1.3 a randomly generated Gaussian codebook is divided into equivalent subcodes (or bins). The transmitter encodes the secret message into the indices of the bins formed in this in way. A codeword belonging to the chosen bin is picked randomly and transmitted. This corresponds to randomly picking one of the clusters shown in Figure 1.3, and transmitting the corresponding bin representative belonging to this cluster. Note that for high-dimensional codebooks, the *equipartition* characteristic of Figure 1.3 holds with high probability.

Note that the noise sphere (represented for convenience as a hexagon in Figure 1.3) of the legitimate receiver permits the asymptotically perfect decoding of the transmitted codeword. Thus, both the chosen bin (bearing the secret message) and the randomly picked cluster are available to the receiver. If the "radius" of each cluster is picked such that it equals the eavesdropper's noise sphere "radius", then the eavesdropper's noise sphere centered around the transmitted codeword contains a bin representative from each bin. Therefore, from the eavesdropper's point of view, all secret messages are asymptotically (as the codeword length approaches infinity) equally likely. Moreover, the eavesdropper cannot even be certain about the cluster to which the transmitted codeword belongs, and thus no common message can be transmitted while aiming for the secrecy capacity.

A different scenario is that where the secrecy constraint is abandoned in favor of a common message [13], [16]. This scenario is depicted in Figure 1.4). A similar representation can be found in [16]. Note that the cluster to which the transmitter codeword belongs can be identified by the

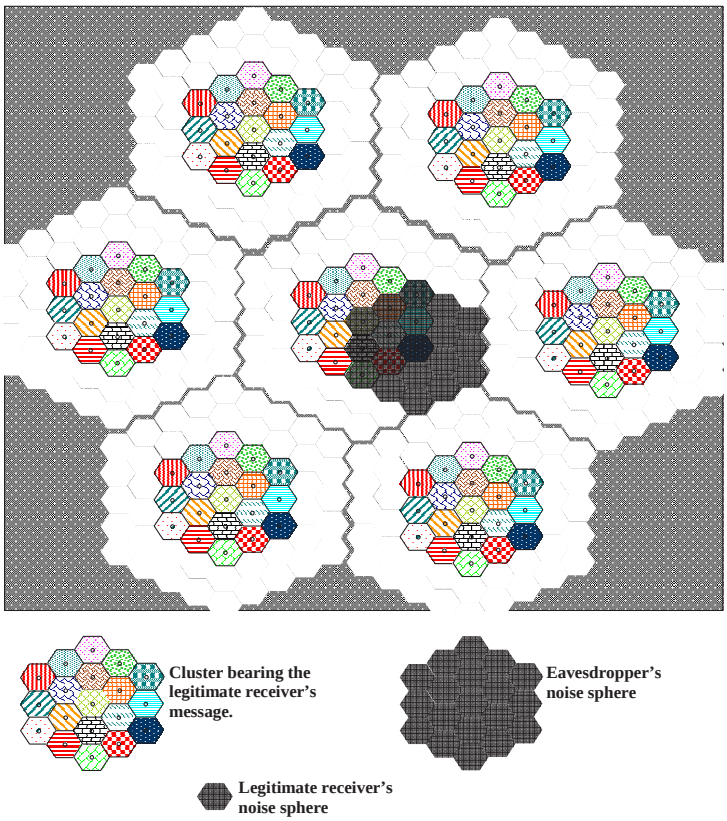

FIGURE 1.4. Transmission of common and private (although not secret) messages.

eavesdropper. The common message can thus be encoded in the centers of the clusters, while the legitimate receiver's *private* message can be encoded in the indices of the bins, as before. However, the receiver's private message is not perfectly secret to the eavesdropper. For instance, given its observation, the eavesdropper can compute a short list of possible transmitted codewords. Note that although we represent the two encoding schemes in Figures 1.3 and 1.4 in a similar way, the two encoding techniques are fundamentally different. An example of the confusion arising from the similar geometric interpretation is the wrong encoding scheme of [2], which is discussed in Chapter 5.

In order to achieve a positive secrecy rate, the receiver's rate has to be decreased [13], as shown in Figure 1.5). The "short list" of possible transmitted codewords that is computable by the eavesdropper has to contain a representative of the bin corresponding to each secret message.

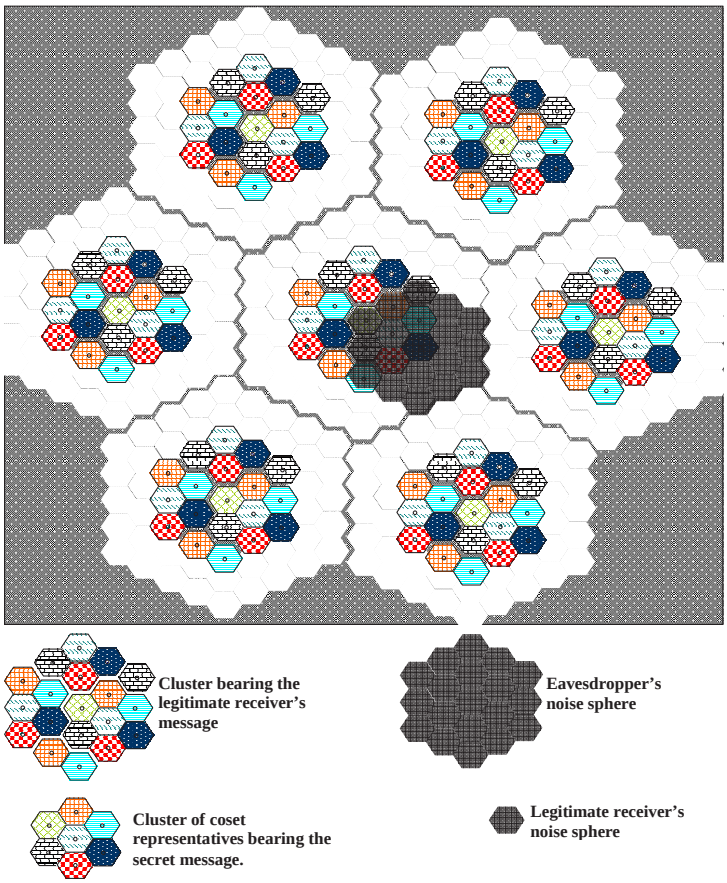

FIGURE 1.5. Achieving a positive secrecy rate in the presence of common messages.

Just like the case of jamming problems, the concept of eavesdropping had escaped much attention for several decades until lately, when security issues have become one of the biggest concerns in wireless networks. The flexibility of these networks amounts to a greater risk, but also creates the optimal environment for multiuser defense strategies.

A recent attempt to extend the eavesdropper problem to Gaussian multiple-access wire-tap channels (with and without fading) can be found in [17], [2]. In [17], the secrecy is defined in two different ways: individual (which means secrecy is preserved for each user even when the other users are compromised), and collective (when all users are supposed to trust each other and achieve a larger overall secrecy rate).

A different multiuser approach [18] investigates the eavesdropper scenario where the transmitter can request the help of a trusted relay node. The relay can either send independent codewords in order to confuse the wiretapper ("noise forwarding"), or forward quantized versions of its noisy observations of the transmitter's signal to the destination ("compress and forward"). However, sometimes the relay may not be fully trusted with the secret message. The scenario where the relay needs to be kept from learning the secret message, but at the same time can still be used for enhancing communication reliability is discussed in [19].

A different direction in the fight against eavesdroppers, arising from the field of cryptography, is encryption by means of a secret key. For wireless environments, the secret key needs to be generated by using the available resources, and in the presence of the eavesdropper. Significant contributions in this direction were brought in [20], [21]. The main idea behind the secret key generation process is that the legitimate parties take advantage of some form of "common randomness". Such randomness could be provided if all terminals decode (with errors) a sequence of random bits, as for example those transmitted by a satellite at a very low signal to noise ratio (SNR) [20]. A multi-step protocol is presented in [20], which is designed to put the eavesdropper at a disadvantage, and thus to make possible the agreement upon a secret key.

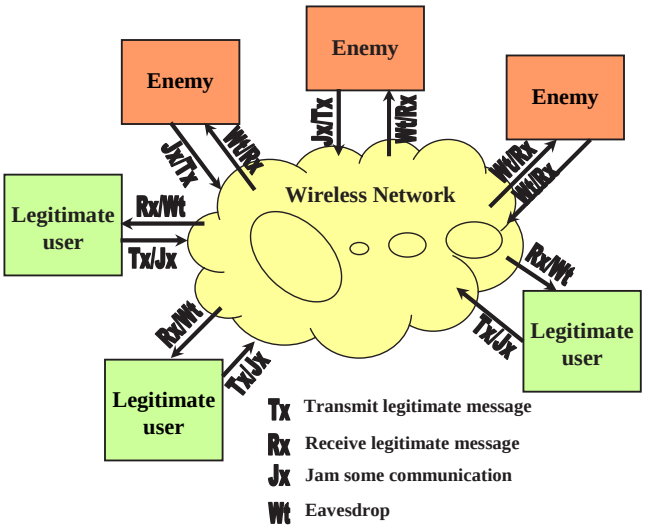

FIGURE 1.6. General framework.

More recent works, like [22], [23], [24] or [25] have been focused on ergodic-fading eavesdropper channels. Although achievable secrecy rates and the benefits of noise injection at the transmitter are discussed by [22], the secrecy capacity of fast-fading eavesdropper channels remains unknown. A secrecy capacity is derived in [23], for a modified channel model, which assumes that the ergodic fading is slow enough to be considered constant for extremely long intervals, each of which may therefore accommodate an entire codeword. Similarly, [24] and [25], treat the fading broadcast channel with confidential messages as a particular case of parallel AWGN broadcast channel with confidential messages.

Slow fading eavesdropper channels with delay constraints have been investigated in [26] and [27]. Since under block fading (when the channel state information is not available to the transmitter in a non-causal manner) one cannot guarantee either the secrecy or the intelligibility of the secret message, these works evaluate system performance by quantities like the outage probability (referring to intelligibility outage), combined with the probability of *secrecy outage*.

1.3 The Big Picture

This dissertation represents the first and most fundamental steps towards creating and developing a framework in which the eavesdropping and intelligent jamming problems are intertwined. As a

general scenario, we envision a wireless network with nodes of similar capabilities, where nodes may create alliances aimed either at sharing confidential messages in the most efficient way, or at eavesdropping and disrupting an enemy alliance.

The first type of alliance, or the "legitimate users" are fully aware of the existence of enemy alliances (or simply "enemies"). As a consequence, they attempt to find and implement optimal strategies against both eavesdropping and jamming. On the other hand, the enemies may collaborate in order to obtain as much information about their opponents as possible, and to use it in an optimal manner for disrupting the communication.

A very general description of our model is depicted in Figure 1.6. Note that while the enemies' primary purpose is to eavesdrop and/or jam the legitimate alliance, they may find it optimal to communicate to each other by sending and receiving "legitimate" messages. In turn, in addition to communicating legitimate messages, the legitimate users could attempt to intercept and, once the enemies have been identified and labeled, even disrupt the communication between them.

We begin the present dissertation by a separate treatment of the jamming and the wiretapping problems. An application-oriented scenario for uncorrelated jamming is first investigated in Chapters 2 and 3. The outage probability is adopted as an objective function, over which the transmitter aims at minimization and the jammer aims at maximization by selecting their respective optimal power control strategies. We provide a comprehensive coverage of the problem, by studying multiple scenarios: fast and slow fading, peak and average power constraints, pure and mixed strategies, with and without channel state information (CSI) feedback.

For the eavesdropping problem, we bring some improvements to the present state of the art, by developing a novel scheme that can guarantee strictly positive secrecy rates even when the eavesdropper's channel is better than the legitimate receiver's channel. A particular implementation of the scheme for binary symmetric channels is presented in Chapter 4.

Finally, in Chapter 5 we make the first steps towards the joint jamming and eavesdropping problem. For the first time in the related literature, we consider the scenario of an "active eavesdropper"

whose purpose is to decrease the achievable secrecy rate of a pair of legitimate users. We show how an active eavesdropper can seriously degrade the achievable secrecy rate over a fast fading channel, and we provide an ingenious sequential secrecy scheme that can significantly ameliorate these effects.

Chapter 2

Jamming in Fixed-Rate Wireless Systems with Power Constraints - Part I: Fast Fading Channels

2.1 Introduction

The importance of designing anti-jamming strategies cannot be overstated, due to the extremely wide deployment of wireless networks, the very essence of which makes them vulnerable to attacks. Although the bases of jamming and anti-jamming strategies have been set in the 80's and 90's [3–5], new interest has been recently generated by the increasing demand for wireless security. Jamming and anti-jamming strategies were developed for the broadcast channel [8], the multiple access channel [9], and even studied from the perspective of an arbitrarily varying channel [11]. Under all scenarios, the jamming problem is formulated as a two-player, zero-sum game. The corresponding objective functions are the sum-rate [8], the ergodic capacity [9] or the λ-capacity [11]. Although most often the jammer is assumed to have access to either the transmitter's output or input [3, 5, 10] and consequently is able to produce correlated jamming signals, the correlation assumption can only be accurate for repeater protocols, or other situations where the jammer gets the chance to jam a signal about which it has already obtained some information from eavesdropping previous transmissions.

The approach of [11] is quite relevant to our work. The jamming problem is viewed as a special case of an arbitrarily varying channel (AVC). Constraints are placed either on the power invested in each codeword (peak power constraints), or on the power averaged over all codewords (average power constraints). The λ-capacity, which is used to evaluate system performance, is defined as the maximum transmission rate that guarantees a probability of codeword error less than λ, under random coding. It is shown that when peak power constraints are imposed on both transmitter and jammer, the λ-capacity is constant for $0 \leq \lambda < 1$, and therefore is the same as the channel capacity. No fading is assumed in [11], and consequently no power control strategies are necessary.

Fading channels are often the more practical models for wireless applications. Traditionally, fast fading channels are characterized by their *ergodic capacity*, which is completely determined by the probability distribution of the channel coefficient and the transmitter power constraints. The physical interpretation of this measure of channel quality is related to the capabilities of channel codes. In the fast fading scenario, the codewords are assumed long enough to reveal the long-term statistical properties of the fading coefficient (in practical systems, this requirement may be satisfied by the use of interleaving [28]). Implicitly, power constraints are imposed over each codeword. Therefore, for achieving asymptotic error free communication, all codewords need to be transmitted at the same rate not exceeding the channel's ergodic capacity.

However, applications like video streams in multimedia often require fixed data rates that could exceed the channel's ergodic capacity, but can tolerate non-zero codeword error probabilities. Therefore, in situations when the transmitter's available power is not sufficient for supporting a certain rate for each codeword in the traditional framework, the transmitter can choose to concentrate its power on transmitting only a subset of the codewords, while dropping the others. This maneuver ensures error free decoding of the transmitted messages, at the cost of a non-zero probability of message decoding error, which is feasible when power constraints are imposed over the ensemble of all codewords, instead of over each single codeword. This justifies the evaluation of fixed rate systems in fast fading channels by a quantity that is best known to characterize slow fading channels: the *outage probability*. Note that unlike the case of slow fading, in fast fading channels, due to the large codeword length, the channel conditions affecting the transmission of different codewords are asymptotically identical.

In this chapter, we consider a fast fading AWGN channel where codewords (we denote the span of a codeword by the term *frame*) are considered long enough to reveal the long-term statistical properties of the fading coefficient. Our channel model is depicted in Figure 2.1. It was shown in [29] that the ergodic capacity of the fast fading AWGN channel can be achieved by a constant-rate, constant-power Gaussian codebook, provided that when the fading coefficients are available at the

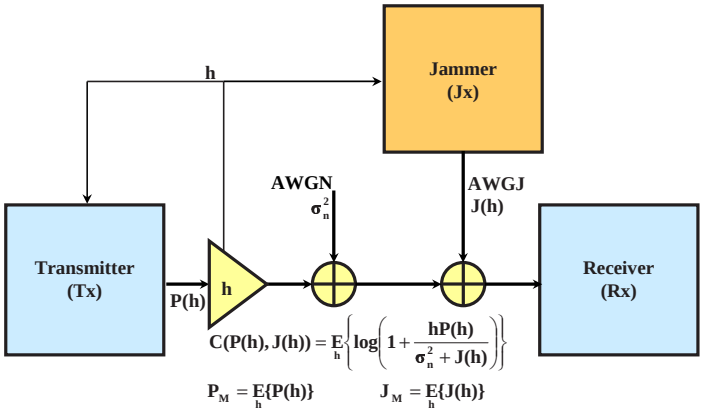

FIGURE 2.1. Channel model

transmitter, the transmitter employs a dynamic scaling of the code symbols, by the appropriate power allocation function. For this reason we assume in out model that the transmitter uses a capacity-achieving complex Gaussian codebook. The jammer is assumed to have no knowledge about this codebook or the actual output of the transmitter, and hence its most harmful strategy is to transmit white complex Gaussian noise [30].

The channel coefficient is a complex number, the squared absolute value of which will be denoted throughout this chapter by h. The average powers invested by the transmitter and jammer in transmitting and jamming a codeword, respectively, are denoted by P_M and J_M. The transmitter and the jammer are subject to either peak power constraints (over each frame, or codeword) of the form $P_M \leq \mathcal{P}$ and $J_M \leq \mathcal{J}$, or average power constraints (over all frames) of the form $\mathbf{E}P_M \leq \mathcal{P}$ and $\mathbf{E}J_M \leq \mathcal{J}$, where the expectation is taken with respect to the players' strategies of allocating the powers $\mathcal{P}$ and $\mathcal{J}$ between frames.

A codeword is decoded with strictly positive probability of error (i.e. outage) if the ergodic capacity calculated over the frame is below the fixed rate R. The probability of this event (the equivalent of λ in [11]) will be denoted as the *probability of outage* P_{out}. The transmitter aims at minimizing the probability of outage for a fixed rate R, while the jammer attempts to maximize it. Our contributions can be summarized as below:

- We first investigate the scenario where full channel state information (CSI) is available to all parties. For this case we show that peak power constraints are not efficient for high rate transmissions or large jammer power;

- We formulate the scenario of average transmitter/jammer power constraints as a two-person, zero-sum game with the probability of outage as the pay-off function.

- Under average power constraints, we first investigate pure strategies and find the maximin and minimax solutions, as a result of two levels of power control: one within frames and one concerning the additional randomization introduced by the transmitter. Optimal strategies are derived for both levels, and it is shown that a Nash equilibrium of pure strategies does not exist in general.

- As a result, we investigate mixed strategies and find the (unique) Nash equilibrium by solving a generalized version of a game that was first discussed by Bell and Cover [31] and then extended by Hughes and Narayan [11].

- Finally, for comparison purposes, we find the optimal transmitter and jammer mixed strategies for the case when the receiver does not feed back the CSI. Our results show that CSI feedback only brings slight improvements in the overall transmission quality.

One comment is in order. Note that Nash equilibria of mixed strategies are not always the best approach to practical jamming situations. An equilibrium of mixed strategies usually assumes that none of the two players knows exactly when or with what power the other player is going to transmit. While this may generally be true for the legitimate transmitter, a smart jammer might constantly eavesdrop the channel and detect both the legitimate transmitter's presence and its power level. Therefore, many real jamming scenarios might be more accurately characterized by the solutions of the *maximin problem formulation with pure strategies* when the jammer tries to minimize and the transmitter tries to maximize the objective, and the solutions of the *minimax problem*

formulation with pure strategies when the jammer tries to maximize and the transmitter tries to minimize the objective (the latter case applies to the present chapter). At worst, these solutions provide a valid lower bound on system performance.

The chapter is organized as follows. Section 2.2 formalizes the peak power constrained problem when full CSI is available to all parties. It turns out that this problem has an intuitive solution. Under the same full CSI assumption, Section 2.3 studies the problem of average power constraints and pure strategies, and is divided into three subsections. The first one presents the optimal strategies for allocating power over one frame. Using the results therein, the maximin and minimax solutions are derived in Subsection 2.3.2. Some numerical results are shown in Subsection 2.3.3. Section 2.4 investigates the problem of full CSI, average power constraints and mixed strategies and provides the Nash equilibrium point. The scenario when the channel coefficients are only known to the receiver is investigated in Section 2.5. Finally, conclusions are drawn in Section 2.6.

2.2 CSI Available to All Parties. Jamming Game with Peak Power Constraints

This game represents a more general version of the game discussed in Section IV.B of [9], and its solution relies on the results therein. The transmitter's goal is to:

$$\begin{cases} \text{Minimize} & \Pr(C(P(h), J(h)) < R) \\ \text{Subject to} & P_M = \mathbf{E}_h[P(h)] \leq \mathcal{P}, \end{cases} \tag{2.1}$$

while the jammer's goal is to:

$$\begin{cases} \text{Maximize} & \Pr(C(P(h), J(h)) < R) \\ \text{Subject to} & J_M = \mathbf{E}_h[J(h)] \leq \mathcal{J}, \end{cases} \tag{2.2}$$

where

$$C(P(h), J(h)) = \mathbf{E}_h \left[\log \left(1 + \frac{hP(h)}{\sigma_N^2 + J(h)} \right) \right].$$

is the ergodic capacity, which is completely determined by the p.d.f. of the channel coefficient $p(h)$ and the transmitter/jammer power control strategies $P(h)$ and $J(h)$. The expectation is defined as $\mathbf{E}_h[f(h)] = \int_h f(h)p(h)dh$.

We prove that this game is closely related to the two player, zero-sum game of [9], which has the mutual information between Tx and Rx as cost/reward function:

$$\text{Tx} \begin{cases} \text{Maximize} & C(P(h), J(h)) \\ \text{Subject to} & P_M \leq \mathcal{P}, \end{cases} \tag{2.3}$$

$$\text{Jx} \begin{cases} \text{Minimize} & C(P(h), J(h)) \\ \text{Subject to} & J_M \leq \mathcal{J}. \end{cases} \tag{2.4}$$

This latter game is characterized by the following proposition, proved in Section IV.B of [9]:

Proposition 2.1. *The game of (2.3) and (2.4) has a Nash equilibrium point given by the following strategies:*

$$P^*(h) = \begin{cases} \left[\frac{1}{\lambda} - \frac{\sigma_N^2}{h}\right]_+ & \textit{if} \quad h < \frac{\sigma_N^2 \lambda}{1-\sigma_N^2 \nu} \\ \frac{h}{\lambda(h+\frac{\lambda}{\nu})} & \textit{if} \quad h \geq \frac{\sigma_N^2 \lambda}{1-\sigma_N^2 \nu} \end{cases} \tag{2.5}$$

$$J^*(h) = \begin{cases} 0 & \textit{if} \quad h < \frac{\sigma_N^2 \lambda}{1-\sigma_N^2 \nu} \\ \frac{h}{\nu(h+\frac{\lambda}{\nu})} - \sigma_n^2 & \textit{if} \quad h \geq \frac{\sigma_N^2 \lambda}{1-\sigma_N^2 \nu} \end{cases} \tag{2.6}$$

where λ and ν are constants that can be determined from the power constraints and $[x]_+ = \max\{x, 0\}$.

The connection between the two games above is made clear in the following theorem, the proof of which follows in the footsteps of [32] and is given in Section 2.7.

Theorem 2.2. *Let $P^*(h)$ and $J^*(h)$ denote the Nash equilibrium solutions of the game described by (2.3) and (2.4). Then the original game of (2.1), (2.2) has a Nash equilibrium point, which is given by the following pair of strategies:*

$$\widehat{P}(h) = \begin{cases} P^*(h) & \textit{if} \quad C(P^*(h), J^*(h)) \geq R \\ P_a(h) & \textit{if} \quad C(P^*(h), J^*(h)) < R \end{cases} \tag{2.7}$$

$$\widehat{J}(h) = \begin{cases} J_a(h) & \textit{if} \quad C(P^*(h), J^*(h)) > R \\ J^*(h) & \textit{if} \quad C(P^*(h), J^*(h)) \leq R, \end{cases} \tag{2.8}$$

where $P_a(h)$ and $J_a(h)$ are some arbitrary power allocations satisfying the respective power constraints. (Note that no particular improvements are obtained by setting $P_a(h) = J_a(h) = 0$, since only peak power constraints are in effect.)

The results are intuitive: if the ergodic capacity under the optimal jammer/transmitter strategies is larger than the fixed rate R, reliable communication can be established over each frame, and hence the probability of outage is $P_{out} = 0$. In this case, the actual power allocation of the jammer does not matter anymore, since the jammer has already lost the game.

On the other hand, if the ergodic capacity is less than R, outage occurs on all frames ($P_{out} = 1$), and the actual transmitter strategy makes no difference. As will be shown in the next section, enforcing average power constraints in this case gives the transmitter more freedom, and results in a smaller outage probability.

2.3 CSI Available to All Parties. Jamming Game with Average Power Constraints: Pure Strategies

In this section power constraints are imposed over a large number of frames rather than on each frame. The transmitter and jammer may increase their transmission and jamming powers over any frame from $\mathcal{P}$ to P_M, and from $\mathcal{J}$ to J_M, respectively. To satisfy the average power constraints

imposed by $\mathcal{P}$ and $\mathcal{J}$, less power has to be allocated to other frames. We shall prove that for both players, the optimal way to control the power allocation between frames is to employ ON/OFF strategies. Since all frames are equivalent from the point of view of their corresponding channel realizations, the manner in which the "discarded" codewords are picked is somewhat random. However, note that this type of randomization only aims at ensuring that a possibly larger P_M or J_M is obtained. We don't consider mixing strategies in this section [33]. Although each player picks up a frame randomly, we assume this is known by its opponent when considering the maxmin and minimax problems as formulated below. That is, the maximin scenario assumes the transmitter has perfect non-causal access to the jammer's strategy (we say the jammer "plays first"), while the minimax case assumes the jammer has perfect, non-causal access to the transmitter's strategy (we say the transmitter "plays first"). The first player in the minimax or maxmin cases is always more vulnerable in the sense that the follower has the freedom to adapt its strategy such that it minimizes the first player's payoff.

The minimax scenario is the more practical one. In addition to being pessimistic from the system designer's point of view, it accurately models the situation where the jammer (who is not interested in exchanging any information of its own) listens to the feedback carrying the channel coefficients and senses the transmitter's presence and power level, hence estimating the transmitter's strategy. The maximin scenario is not of less importance, since it is required for determining the non-existence of a Nash equilibrium and for comparison with the minimax approach.

An important remark should be made here. We shall prove in the sequel that under both the pure strategies and the mixed strategies scenarios, the optimal power allocation over a frame is done similarly. Therefore, the major difference between the two cases is in the strategies of allocating power to different frames. We should note that it is easier for one of the players to detect the presence of the other player over a frame, than to estimate the other player's transmission power. Under the minimax solution of pure strategies, the jammer only needs to detect the presence of the transmitter (the optimal strategies are of ON/OFF type) to have complete information about

the transmitter's behavior. However, if the transmitter chose to use mixed strategies, a complete characterization of its behavior would require not only knowledge about its presence, but also about the power it decided to allocate to that frame.

The average power constrained jamming game can be formulated as:

$$\text{Tx} \begin{cases} \text{Minimize} & \Pr(C(P(h), J(h)) < R) \\ \text{Subject to} & E[P_M] \leq \mathcal{P} \end{cases} \tag{2.9}$$

$$\text{Jx} \begin{cases} \text{Maximize} & \Pr(C(P(h), J(h)) < R) \\ \text{Subject to} & E[J_M] \leq \mathcal{J} \end{cases} \tag{2.10}$$

where P_M and J_M are defined as in (2.1), (2.2), the expectation is taken over all frames with respect to the power allocation strategies introduced by the transmitter and jammer, and $\mathcal{P}$ and $\mathcal{J}$ are the upper-bounds on average transmission power of the source and jammer, respectively.

2.3.1 Power Allocation within a Frame

The game between transmitter and jammer has two levels. The first (coarser) level is about power allocation between frames, and has the probability of outage as a cost/reward function. The probability of outage is determined by the number of frames over which the transmitter is not present or the jammer is successful in inducing outage. This set is established in the first level of power control which is investigated in detail in the next two subsections, but which cannot be derived before the second level strategies are available.

The second (finer) level is that of power allocation within a frame. In this subsection we derive the optimal second level of power allocation strategies for both maximin and minimax problems, and show they are connected by a special kind of duality.

Note that decomposing the problem into several (two or three) levels and solving each one separately does not restrict the generality of our solution. Our proofs are of a contradictory type. Instead of directly deriving each optimal strategy, we assume an optimal solution has already been reached

and show it has to satisfy a set of properties. We first assume these properties are not satisfied, and then show that under this assumption there is room for improvement. Thus we prove that any solution not satisfying our set of properties cannot be optimal (i.e. the properties are necessary). We pick the properties in such a manner that they are sufficient for the complete characterization of the optimal solution. That is, we make sure that the system of necessary properties has a unique solution.

In the maximin case (when jammer plays first), assume that the jammer has already allocated some power J_M to a given frame. Depending on the value of J_M, and its own power constraints, the transmitter decides whether it wants to achieve reliable communication over that frame. If it decides to transmit, it needs to spend as little power as possible (the transmitter will be able to use the saved power for achieving reliable communication over another set of frames, and thus to decrease the probability of outage). Therefore, the transmitter's objective is to minimize the power P_M spent for achieving reliable communication over each frame. Note that if the jammer is present over a frame, the value of P_M required to achieve reliable communication over that frame is a function of J_M. However, the transmitter should attempt to minimize the required P_M even when the jammer is absent. The jammer's objective is then to allocate the given power J_M over the frame such that the required P_M is maximized.

In the minimax scenario (when transmitter plays first) the jammer's objective is to minimize the power J_M used for jamming the transmission over a given frame. The jammer will only transmit if the transmitter is present with some P_M. The transmitter's objective is to distribute P_M within a frame such that the power required for jamming is maximized.

The two problems can be formulated as follows:

Problem 1 (for the maximin solution - jammer plays first)

$$\max_{J(h)\geq 0}\Big[\min_{P(h)\geq 0} P_M = \mathbf{E}_h[P(h)],\ \text{s.t. } C(P(h),J(h)) \geq R\Big]\text{s.t. } \mathbf{E}_h\left[J(h)\right] \leq J_M; \tag{2.11}$$

Problem 2 (for the minimax solution - transmitter plays first)

$$\max_{P(h)\geq 0}\Big[\min_{J(h)\geq 0} J_M=\mathbf{E}_h[J(h)],\ \text{s.t. } C(P(h),J(h))\leq R\Big]\text{s.t. } \mathbf{E}_h[P(h)]\leq P_M. \tag{2.12}$$

Let $\mathfrak{m}$ denote the probability measure introduced by the probability density function (p.d.f.) of h, i.e., for a set $\mathscr{A}\subseteq\mathbb{R}_+$, we have $\mathfrak{m}(\mathscr{A})=\int_{\mathscr{A}}p(h)dh$. Denote $x(h)=J(h)+\sigma_N^2$. Note that the expectation is defined as $\mathbf{E}_h[f(h)]=\int_h f(h)p(h)dh$. Similarly, we define $\mathbf{E}_{h\in\mathscr{X}}[f(h)]=\int_{h\in\mathscr{X}}f(h)p(h)dh$.

Solution of Problem 1

The transmitter's optimization problem:

$$\min_{P(h)\geq 0}\mathbf{E}_h[P(h)],\ \text{s. t. }\mathbf{E}_h\left[\log\left(1+\frac{hP(h)}{\sigma_N^2+J(h)}\right)\right]\geq R \tag{2.13}$$

has linear cost function and convex constraints. Write the Lagrangian as:

$$\mathbf{L_1}=\mathbf{E}_h[P(h)]-\lambda\left\{\mathbf{E}_h\left[\log\left(1+\frac{hP(h)}{\sigma_N^2+J(h)}\right)\right]-R\right\}. \tag{2.14}$$

With the notation $c=\exp(R)$, the resulting KKT conditions yield the unique solution [34]:

$$P(h)=\left[\lambda-\frac{x(h)}{h}\right]_+,\ h\in\mathbb{R}_+, \tag{2.15}$$

where

$$\lambda=c^{\frac{1}{\mathfrak{m}(\mathscr{M}')}}\left\{\exp\left[\mathbf{E}_{h\in\mathscr{M}'}\left(\log\frac{x(h)}{h}\right)\right]\right\}^{\frac{1}{\mathfrak{m}(\mathscr{M}')}}, \tag{2.16}$$

and $\mathscr{M}'\subset\mathbb{R}_+$ is the set of channel coefficients over which $\lambda\geq x(h)/h$, and $[z]_+=\max\{z,0\}$. We say the transmitter is "non-absent" over $\mathscr{M}'$, and "absent" on $\mathbb{R}_+\setminus\mathscr{M}'$.

The following proposition, the proof of which is given in Section 2.8.1, states that the jammer should only be present where the transmitter is non-absent.

Proposition 2.3. *The jammer should only transmit where the transmitter is "non-absent". Otherwise, if $J(h) > 0$ and $\lambda < x(h)/h$ for h in some set $\mathscr{S} \subset \mathbb{R}_+$, the jammer can decrease $J(h)$ over $h \in \mathscr{S}$ and maintain the same required transmitter power over the frame.*

Substituting (2.16) in (2.13), the jammer's problem can be formulated as:

$$\text{Find} \max_{x(h) \geq \sigma_N^2} c^{\frac{1}{\mathfrak{m}(\mathscr{M}')}} \mathfrak{m}(\mathscr{M}') \cdot \left\{ \exp\left[\mathbf{E}_{h \in \mathscr{M}'} \left(\log \frac{x(h)}{h} \right) \right] \right\}^{\frac{1}{\mathfrak{m}(\mathscr{M}')}} - \mathbf{E}_{h \in \mathscr{M}'} \left(\frac{x(h)}{h} \right) \tag{2.17}$$

$$\text{subject to } \mathbf{E}_h[x(h)] \leq (J_M + \sigma_N^2) \tag{2.18}$$

Since the set $\mathscr{M}'$ depends on the jammer power allocation $J(h)$, solving the optimization problem above analytically is difficult. This is why we next provide an alternative method for finding the solution. Our method examines the properties of the sets $\mathscr{M}'$ over which the transmitter is present and $\mathscr{M}''$ over which the jammer is present, as well as those of the optimal transmitter/jammer strategies.

Fixing $\mathscr{M}'$, the Lagrangian for the jammer's optimization problem can be written as

$$\mathbf{L_2} = -P_M + \mu \left\{ \mathbf{E}_h[x(h)] - (J_M + \sigma_N^2) \right\}. \tag{2.19}$$

This yields the new KKT conditions:

$$\frac{1}{x(h)} \left\{ \exp\left[\mathbf{E}_{h \in \mathscr{M}'} \left(\log \frac{x(h)}{h} \right) \right] \right\}^{\frac{1}{\mathfrak{m}(\mathscr{M}')}} c^{\frac{1}{\mathfrak{m}(\mathscr{M}')}} - \frac{1}{h} - \mu = 0 \text{ for } h \in \mathscr{M}'', \tag{2.20}$$

$$\mathbf{E}_{h \in \mathscr{M}''} x(h) = J_M + \sigma_N^2 \mathfrak{m}(\mathscr{M}''), \tag{2.21}$$

$$\mu \geq 0, \tag{2.22}$$

where $\mathscr{M}''$ is the set of channel coefficients on which the jammer transmits non-zero power.

For fixed $\mathscr{M}'$ and $\mathscr{M}''$, the jammer's optimal strategy has to satisfy these KKT conditions. The resulting optimal strategy is

$$x(h) = \frac{h}{1 + \mu h} \left\{ c \exp\left[\mathbf{E}_{h \in \mathscr{M}'} \left(\log \frac{x(h)}{h} \right) \right] \right\}^{\frac{1}{\mathfrak{m}(\mathscr{M}')}}. \tag{2.23}$$

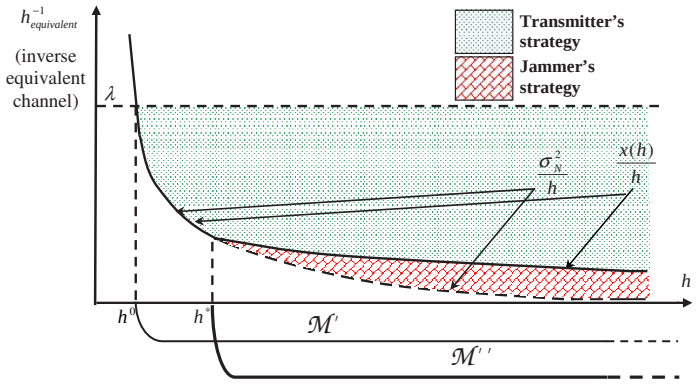

FIGURE 2.2. Optimal second level power control strategies

The expression above states that for any two channel realizations with coefficients $h_i,\ h_j$ belonging to $\mathscr{M}''$, we have

$$\frac{x(h_i)}{h_i} \geq \frac{x(h_j)}{h_j} \Leftrightarrow h_i \leq h_j \Leftrightarrow x(h_i) \leq x(h_j). \tag{2.24}$$

Note that for any two channel realizations $h_i,\ h_j \notin \mathscr{M}''$ (i.e. $x(h_i) = x(h_j) = \sigma_N^2$) we also have

$$\frac{x(h_i)}{h_i} \geq \frac{x(h_j)}{h_j} \Leftrightarrow h_i \leq h_j. \tag{2.25}$$

The following proposition brings more insight into the optimal jamming strategy. Its proof is deferred to Section 2.8.2.

Proposition 2.4. *The optimal jamming strategy is such that $x(h)/h$ is a continuous decreasing function of h over all of $\mathbb{R}_+$, and $\mathscr{M}''$ is of the form $\mathscr{M}'' = [h^*, \infty)$. Moreover, this implies that $\mathscr{M}'$ is of the form $\mathscr{M}' = [h^0, \infty)$.*

The optimal transmitter/jammer strategies for allocating power over a frame are described in Figure 2.2.

Substituting (2.23) into (2.16), we get a new expression for λ:

$$\lambda = \frac{x(h)}{h}(1 + \mu h), \text{ for } h \in \mathscr{M}'' \tag{2.26}$$

which together with (2.15) yields

$$P(h) = \mu x(h), \text{ for } h \in \mathscr{M}''. \tag{2.27}$$

An interesting remark which supports the results of the next subsection is that, for the optimal solution of *Problem 1*, μ has to be strictly greater than zero, hence eliminating the possibility that the jammer allocates positive power to frames where the transmitter, although "non-absent", could allocate zero power. In Section 2.8.2 it is shown how this remark follows from Proposition 2.4.

Taking expectation over $h \in \mathscr{M}''$ in (2.23), and using the constraint (2.21), we get

$$x(h) = \frac{J_M + \mathfrak{m}(\mathscr{M}'')\sigma_N^2}{\frac{1+\mu h}{h}\mathbf{E}_{h\in\mathscr{M}''}\frac{h}{1+\mu h}}, \tag{2.28}$$

for $h \in \mathscr{M}''$ and $x(h) = \sigma_N^2$ for $h \notin \mathscr{M}''$.

To solve for μ, substitute (2.28) into (2.23):

$$\left[\frac{J_M + \mathfrak{m}(\mathscr{M}'')\sigma_N^2}{\mathbf{E}_{h\in\mathscr{M}''}\frac{h}{1+\mu h}}\right]^{\mathfrak{m}(\mathscr{M}')-\mathfrak{m}(\mathscr{M}'')} =$$
$$= c\exp\left[\mathbf{E}_{h\in\mathscr{M}''}\left(\log\frac{1}{1+\mu h}\right)\right]\cdot\exp\left[\mathbf{E}_{h\in\mathscr{M}'-\mathscr{M}''}\left(\log\frac{\sigma_N^2}{h}\right)\right]. \tag{2.29}$$

The second level power allocation solution for the maximin problem is thus completely determined by the triple $(\mathscr{M}', \mathscr{M}'', \mu)$, or equivalently by (h^0, h^*, μ). By Proposition 2.4 above, $x(h^*) = \sigma_N^2$ (by continuity in h^*), and $\lambda = \sigma_N^2/h^0$. Rearranging these two relations, along with (2.29) in a more convenient form, we obtain the following system of equations, which has to hold for any solution to our problem:

$$h^0 = \frac{h^*}{1+\mu h^*}, \tag{2.30}$$

$$\frac{J_M}{\sigma_N^2} = \int_{h^*}^{\infty}\left(\frac{\frac{h}{1+\mu h}}{\frac{h^*}{1+\mu h^*}} - 1\right)p(h)dh, \tag{2.31}$$

$$R = \int_{\frac{h^*}{1+\mu h^*}}^{h^*}\log\left(h\frac{1+\mu h^*}{h^*}\right)p(h)dh - \int_{h^*}^{\infty}\log\left(\frac{1}{1+\mu h}\right)p(h)dh. \tag{2.32}$$

The equations above lead to the following result:

Proposition 2.5. *The solution of the maximin second level power allocation problem is unique.*

Proof. It is easy to see that the right hand side of (2.31) is a strictly decreasing function of h^*, for fixed μ, and a strictly decreasing function of μ, for fixed h^*, while being equal to a constant. Hence, for given J_M, (2.31) yields μ as a strictly decreasing function of h^*.

Similarly, the right hand side of (2.32) is a strictly decreasing function of h^*, for fixed μ, and a strictly increasing function of μ, for fixed h^*, while being equal to a constant. Hence, (2.32) yields μ as a strictly increasing function of h^*.

Since (2.31) and (2.32) have to be satisfied simultaneously by any solution, the solution has to be unique. □

Another insightful remark that follows from (2.30)–(2.32) is that as J_M increases, both μ and h^* should be decreasing.

The following proposition, characterizing the $P_M(J_M)$ function, is necessary for deriving the optimal power allocation between frames in the next section. The proof is deferred to Section 2.8.3.

Proposition 2.6. *Under the optimal maximin second level power control strategies, the "required" transmitter power P_M over a frame is a strictly increasing, unbounded and concave function of the power J_M that the jammer invests in that frame.*

Throughout the remainder of this chapter, we shall denote by $\mathscr{P}_M(J_M)$ the function that characterizes the "required" transmitter power over a frame where the jammer invests power J_M, in the maximin case.

Solution of Problem 2

To solve the minimax intra-frame power allocation problem by using the same techniques as in *Problem 1* turns out to be more difficult. Instead we use the above solution of *Problem 1* and show that for both problems, the second level power allocation follows the same rules.

Theorem 2.7. *If $J_{M,1}$ is the value used for the second constraint in* Problem 1 *above, and $P_{M,1}$ is the resulting value of the cost/reward function, then solving* Problem 2 *with $P_M = P_{M,1}$ yields the cost/reward function $J_M = J_{M,1}$. Moreover, any pair of second level power allocation strategies that makes an optimal solution of* Problem 1, *should also make an optimal solution of* Problem 2, *and this also holds conversely.*

Proof. The result is a direct consequence of Theorem 2.21 in Section 2.8.4, if we denote $x = P(h)$, $y = J(h)$, $f(x) = \mathbf{E}_h[P(h)]$, $g(y) = \mathbf{E}_h[J(h)]$ and $h(x, y) = C(P(h), J(h))$. □

We shall denote by $\mathscr{J}_M(P_M)$ the function that characterizes the "required" jamming power over a frame where the transmitter invests power P_M, in the minimax case. By Theorem 2.7, we have that $\mathscr{J}_M(\mathscr{P}_M(J_M)) = J_M$ and $\mathscr{P}_M(\mathscr{J}_M(P_M)) = P_M$.

Further comments on the power control within frames

Although the second level optimal power allocation strategies for the maximin and minimax problems coincide, this result should not be associated to the notion of Nash equilibrium, since the two problems solved above do not form a zero-sum game, while for the game of (2.9) and (2.10), first level power control strategies are yet to be investigated.

Instead, the result should be interpreted as a form of duality. In fact, a much stronger result can be observed as a consequence of Theorem 2.21. Namely, a similar "duality" property links *Problem 1* and *Problem 2* above to the auxiliary problem of (2.3) and (2.4) appearing in the peak power constraints scenario. This explains the resemblance between the solution of the peak power constraints auxiliary problem (2.6) and the solution of *Problem1* (2.26), (2.27).

Also, this common solution implies that $P(h) = \mu(J(h) + \sigma_N^2)$ over the set $\mathscr{M}''$ of channel realizations where both jammer and transmitter are present. Although the transmitter is also active over the set of nonzero measure $\mathscr{M}' \setminus \mathscr{M}''$ as in Figure 2.2, under practical conditions the measure $\mathfrak{m}(\mathscr{M}' \setminus \mathscr{M}'')$ of this set is relatively small. This is the reason why the $\mathscr{P}_M(J_M)$ curve appears to be linear (although it is not) in Figure 2.3 of the numerical results section.

2.3.2 Power Allocation between Frames

The Maximin Solution

In this subsection we present the first level optimal power allocation strategies for the maximin problem. Recall that all frames are equivalent in the sense that they are all characterized by the same channel realizations (although not necessarily occurring in the same chronological order).

The maximin scenario assumes that the transmitter is completely aware of the jammer's power control strategy (only pure strategies are considered in this section). Given a jammer's strategy that allocates different jamming powers to different frames, the optimal way of allocating the transmitter's power is always to ensure that reliable communication is obtained on the frames that require the least amount of transmitter power. The jammer's optimal strategy (which is based solely on this knowledge about the transmitter's strategy) is presented in the following theorem.

Theorem 2.8. *Under the maximin scenario it is optimal for the jammer to allocate the same amount of power $J_M = \mathcal{J}$ to all frames.*

Proof. The proof relies on the concavity of $\mathscr{P}_M(J_M)$. Consider the optimal maximin inter-frame power allocation strategies. Let $\mathscr{S}, \mathscr{X}$ denote the sets of frames over which the transmitter and the jammer are present, respectively. Note that the jammer can itself compute the optimal transmitter strategy in response to its own, and hence is fully informed of the transmitter's response.

We first look at the set of frames $\mathscr{S}$ where the transmitter is active. Denote the power invested by the jammer in this set by $\mathcal{J}_{\mathscr{S}}$. Note that $\mathcal{P}$ is the average "required" transmitter power over $\mathscr{S}$.

If the two players' strategies are both optimal, then by modifying the allocation of $\mathcal{J}_{\mathscr{S}}$ over the frames of $\mathscr{S}$, the new average "required" transmitter power over $\mathscr{S}$ can only be less than or equal to $\mathcal{P}$. In other words, if we denote by j_M the generic power level allocated by the jammer to a frame in $\mathscr{S}$, then

$$\mathcal{P} = \max_{j_M} \int_{\mathscr{S}} \mathscr{P}_M(j_M) dj_M \tag{2.33}$$

subject to

$$\int_{\mathscr{S}} j_M dj_M = \mathcal{J}_{\mathscr{S}}. \tag{2.34}$$

By writing the KKT conditions for the maximization problem in (2.33) and (2.34) above, it is straightforward to see that, at an optimum, $\frac{d\mathscr{P}_M(j_M)}{dj_M}$ should be constant all over $\mathscr{S}$. Taking into account the fact that $\mathscr{P}_M(j_M)$ is concave, we have that a uniform jamming power allocation of $\mathcal{J}_{\mathscr{S}}$ over $\mathscr{S}$ achieves this optimum.

We next look at the set of frames $\mathscr{X} \setminus \mathscr{S}$ where the transmitter cannot afford to be active. This means that the "required" transmitter power over $\mathscr{X} \setminus \mathscr{S}$ is greater than or equal to $\mathscr{P}_M(\mathcal{J}_{\mathscr{S}})$, or equivalently, the power invested by the jammer is greater than or equal to $\mathcal{J}_{\mathscr{S}}$. But since the jammer already knows the transmitter's strategy, investing more than $\mathcal{J}_{\mathscr{S}}$ in any of the frames of $\mathscr{X} \setminus \mathscr{S}$ would be a waste. Therefore, under the optimal maximin inter-frame power allocation strategies, the jammer can invest the same amount of power into all the frames of $\mathscr{X} \bigcup \mathscr{S}$ (which means $\mathscr{S} \subset \mathscr{X}$). But since the transmitter decides to match the required transmitter power on $\mathscr{S}$, there can be no frames where the jammer is not active, and hence $\mathscr{X}$ is the set of all frames. □

The jamming power allocated to each frame is $J_M = \mathcal{J}$. In this case the transmitter faces an indifferent choice space. The power required for the transmitter to achieve reliable communication is $P_M(J_M)$. Hence, the transmitter's optimal strategy is to randomly pick as many frames as possible and allocate power $P_M(J_M)$ to each of them. This is equivalent to saying the transmitter is present over a frame with probability p_t, given by $p_t = \frac{\mathcal{P}}{P_M(\mathcal{J})}$. The resulting probability of outage is now $P_{out} = 1 - p_t$. Note that if $\mathcal{P} \geq P_M(\mathcal{J})$, the probability of outage can be reduced to zero. This corresponds to the case when the ergodic capacity of the channel, computed in the conventional way, with peak power constraints, is larger than the rate R.

The Minimax Solution

Theorem 2.7 showed that for the minimax problem the power allocation within a frame, as well as the relationship between the total powers used by transmitter and receiver over a particular

frame, are identical to the maximin problem. Hence, by rotating the $\mathscr{P}_M(J_M)$ plane, we get the characteristic $\mathscr{J}_M(P_M)$ curve for the minimax problem.

The minimax scenario assumes that the jammer knows exactly when and with what power level the transmitter transmits. Given a transmitter's strategy that allocates different powers to different (equivalent) frames, the optimal way of allocating the jammer's power is such that outage is first induced on the frames that require the least amount of jamming power. Under these conditions, the transmitter's optimal strategy is presented in the following theorem.

Theorem 2.9. *Under the minimax scenario it is optimal for the transmitter to transmit over a maximum number of frames, with the same power P_M that minimizes the probability of outage.*

Proof. The proof relies on the convexity of $\mathscr{J}_M(P_M)$. Consider the optimal minimax inter-frame power allocation strategies, and let $\mathscr{S}, \mathscr{X}$ denote the sets of frames over which the transmitter and the jammer are present, respectively. It is clear in this scenario that $\mathscr{X} \subset \mathscr{S}$.

We first look at the set of frames $\mathscr{X}$ where the jammer is active. Denote the power invested by the jammer in this set by $\mathcal{J}_{\mathscr{X}}$, and the power invested by the transmitter by $\mathcal{P}_{\mathscr{X}}$. Note that $\mathcal{J}_{\mathscr{X}}$ is the average "required" jamming power over $\mathscr{X}$.

If the two players' strategies are both optimal, then by modifying the allocation of $\mathcal{P}_{\mathscr{X}}$ over the frames of $\mathscr{X}$, the new average "required" jamming power over $\mathscr{X}$ can only be less than or equal to $\mathcal{J}_{\mathscr{X}}$. In other words, if we denote by p_M the generic power level allocated by the transmitter to a frame in $\mathscr{X}$, then

$$\mathcal{J}_{\mathscr{X}} = \max_{p_M} \int_{\mathscr{X}} \mathscr{J}_M(p_M) dp_M \tag{2.35}$$

subject to

$$\int_{\mathscr{X}} p_M dp_M = \mathcal{P}_{\mathscr{X}}. \tag{2.36}$$

From the KKT conditions for the maximization problem in (2.35) and (2.36) above, we see that, at an optimum, $\frac{d\mathscr{J}_M(p_M)}{dp_M}$ should be constant all over $\mathscr{X}$. Taking into account the fact that

$\mathscr{J}_M(p_M)$ is convex, we have that a uniform transmitter power allocation of $\mathcal{P}_{\mathscr{X}}$ over $\mathscr{X}$ achieves this optimum.

We should emphasize here that the above arguments hold *under the assumption that the jammer is active over the whole set* $\mathscr{X}$, i.e. when $\mathscr{J}_M(p_M) > 0$ over $\mathscr{X}$. Of course, the overall required jamming power is increased by increasing the transmitter power over some frames of $\mathscr{X}$, while neglecting the others. But this action modifies the set $\mathscr{X}$ itself, and thus the initial assumptions.

We next look at the set of frames $\mathscr{S} \setminus \mathscr{X}$ where the jammer cannot afford to be active. This means that the "required" jamming power over $\mathscr{S} \setminus \mathscr{X}$ is greater than or equal to $\mathscr{J}_M(\mathcal{P}_{\mathscr{X}})$, or equivalently, the power invested by the transmitter is greater than or equal to $\mathcal{P}_{\mathscr{X}}$. But since the transmitter already knows the jammer's strategy, investing more than $\mathcal{P}_{\mathscr{X}}$ in any of the frames of $\mathscr{S} \setminus \mathscr{X}$ would be a waste.

Therefore, under the optimal maximin inter-frame power allocation strategies, the transmitter can invest the same amount of power into all the frames of $\mathscr{S}$. □

The frames over which the transmitter allocates the optimal P_M can be chosen at random. This is equivalent to the transmitter being active over a frame with probability p_t given by $p_t = \frac{\mathcal{P}}{P_M}$. Searching for the optimal P_M is equivalent to searching for the optimal p_t.

The jammer's strategy is to attack as many of the frames where the transmitter is present as possible. In order to induce outage over these frames, the jammer needs to allocate $\mathscr{J}_M(P_M)$ to each of them. This is equivalent to the jammer transmitting $\mathscr{J}_M(P_M)$ on a frame on which the transmitter is present, with probability p_j given by $p_j = \frac{\mathcal{J}}{p_t \mathscr{J}_M(P_M)}$. Note that p_j represents the conditional probability that the jammer transmits over a frame, given that the transmitter is present over that frame. Outage over a frame occurs in two circumstances: either the transmitter (and consequently also the jammer) decides to ignore the frame, or the transmitter attempts to transmit the corresponding codeword, but the jammer is present (and since this is the minimax scenario, it is also successful).

The resulting probability of outage is $P_{out} = (1 - p_t) + p_j p_t$ or, only as a function of P_M:

$$P_{out} = (1 - \frac{\mathcal{P}}{P_M}) + \frac{\mathcal{J}}{\mathscr{J}_M(P_M)}. \tag{2.37}$$

The transmitter finds the optimal value of P_M as the argument that minimizes P_{out} above. A numerical approach should perform exhaustive search with the desired resolution in the interval $[\mathcal{P}, P_{M,max}]$, where $P_{M,max}$ can be set such that $\forall P_M > P_{M,max}$ we have $P_{out}(P_M) > 1 - \epsilon$ for a fixed ϵ. Since $P_{out} \to 1$ as $P_M \to \infty$ independently of the $\mathscr{J}_M(P_M)$ curve, such a finite bound $P_{M,max}$ exists for any ϵ.

Note that if the $\mathscr{P}_M(J_M)$ curve is strictly concave, the jammer can never achieve an outage probability $P_{out} = 1$. This is because the transmitter can invest all its power over a small enough set of frames, such that the jamming power required to jam all the frames in this set exceeds the jammer's power budget. If however the probability measure $\mathfrak{m}$ is chosen such that $\mathscr{P}_M(J_M)$ is an affine function of the form $P_M = P_{M,0} + 1/\theta J_M$, and furthermore if $\mathcal{J} \geq \theta(\mathcal{P} - P_{M,0})$, then $\frac{\mathcal{J}}{\mathscr{J}_M(P_M)} \geq \frac{\mathcal{P} - P_{M,0}}{P_M - P_{M,0}} \geq \frac{\mathcal{P}}{P_M}$ for all values of P_M, and the probability of outage becomes $P_{out} = 1$.

2.3.3 Some Numerical Results

An example of the $\mathscr{P}_M(J_M)$ curve is given in Figure 2.3 for a fixed rate $R = 2$, noise power $\sigma_N^2 = 10$ and a channel coefficient distributed exponentially, with parameter $\lambda = 1/6$.

For the same parameters used to generate Figure 2.3, the probability of outage was computed for a jammer power constraint $\mathcal{J} = 10$ and different values of the transmitter power constraint $\mathcal{P}$. The results were plotted in Figure 2.4. For comparison, the same figure shows $P_{out}(\mathcal{P})$ for the case when the jammer does not use any power control strategy (non-intelligent jammer). Since the jammer's first level of power control for the maximin scenario reduces to uniformly distributing the available power to all frames, the only difference between the maximin scenario and the non-intelligent jammer scenario is in the power allocation within frames. However, as seen from Figure 2.4, this difference is almost negligible.

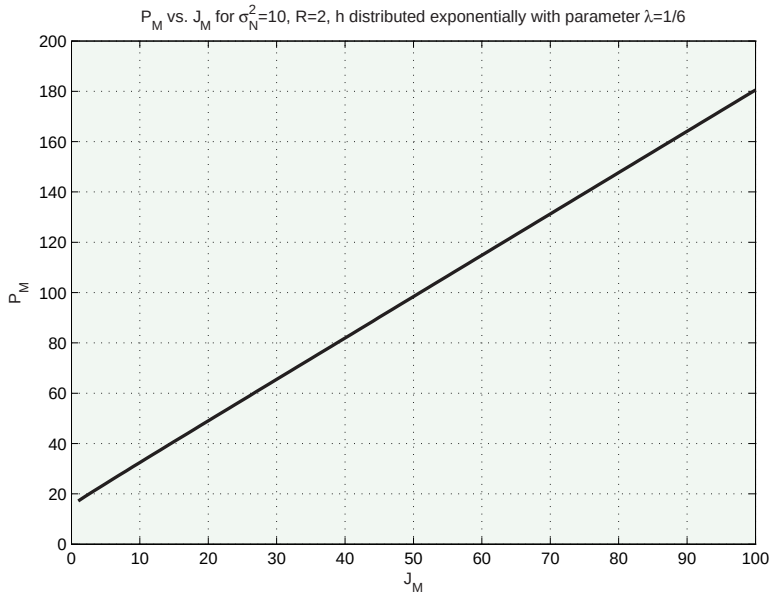

FIGURE 2.3. P_M vs. J_M curve when $R = 2$, $\sigma_N^2 = 10$ and h is distributed exponentially, with parameter $\lambda = 1/6$.

Figure 2.5 shows how the outage probability varies with the rate R, for fixed power constraints $\mathcal{P} = 30$ and $\mathcal{J} = 10$. The $P_{out}(R)$ curves delimitate the achievable capacity vs. outage regions for both peak power constraints and average power constraints (minimax and maximin cases).

Note that even for the minimax solution of the average power constraints problem, there exist values of $\mathcal{P}$ (Figure 2.4), or of the rate R (Figure 2.5) for which the outage probability is less than that achievable under peak power constraints.

Also note that the maximin curve coincides with the peak power constraints curve at large transmitter power (in Figure 2.4) or at small rates (in Figure 2.5). Recall that the jammer's strategy in the maximin scenario is the same as in the peak power constraints scenario (i.e. the jammer allocates the same amount of power $\mathcal{J}$ to each frame). Due to the favorable conditions in the regions characterized by large $\mathcal{P}$ or small R, the transmitter can also spread its power uniformly over all frames (just like in the peak power constraints scenario), overcoming the jammer completely (hence the resulting zero probability of outage).

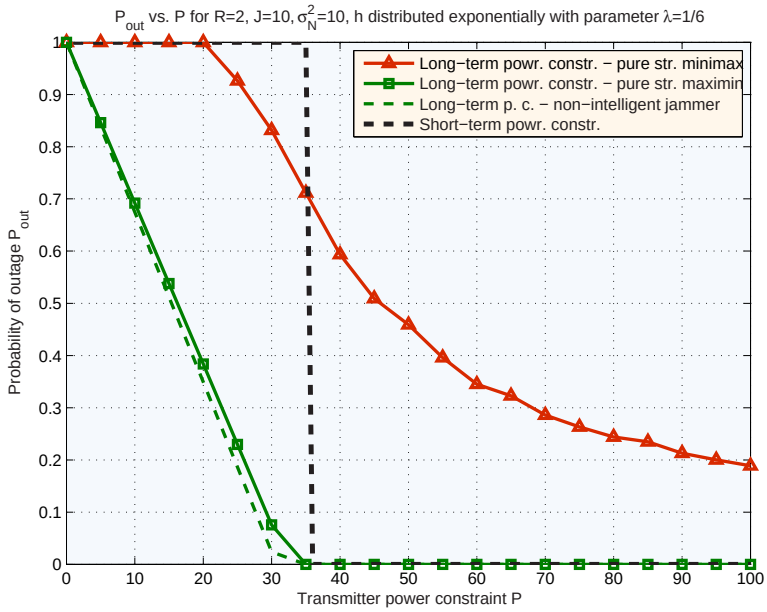

FIGURE 2.4. Outage probability vs. transmitter power constraint $\mathcal{P}$ when $\mathcal{J} = 10$, $R = 2$, $\sigma_N^2 = 10$ and h is distributed exponentially, with parameter $\lambda = 1/6$.

2.4 CSI Available to All Parties. Jamming Game with Average Power Constraints: Mixed Strategies

In the previous section we studied the maximin and minimax solutions of the jamming game when only pure strategies were allowed. Implicitly, we assumed that the power control strategies employed by the first player are perfectly known to the second player, even if they include a form of ON/OFF randomization. We made a case that such a situation as the minimax case can emerge when the jammer does not transmit unless it senses that the transmitter is on (and it can always serve as a pessimistic scenario for the transmitter).

However,our previous assumption may sometimes be inappropriate from a practical point of view. For example, if the transmitter does not stick with the optimal minimax solution, the jammer may have a hard time following the transmitter's behavior. The reason for this is that, as we have already mentioned, the jammer would find it much harder to correctly estimate the amount of power that the transmitter invests in a given frame, than to just detect the presence of the transmitter.

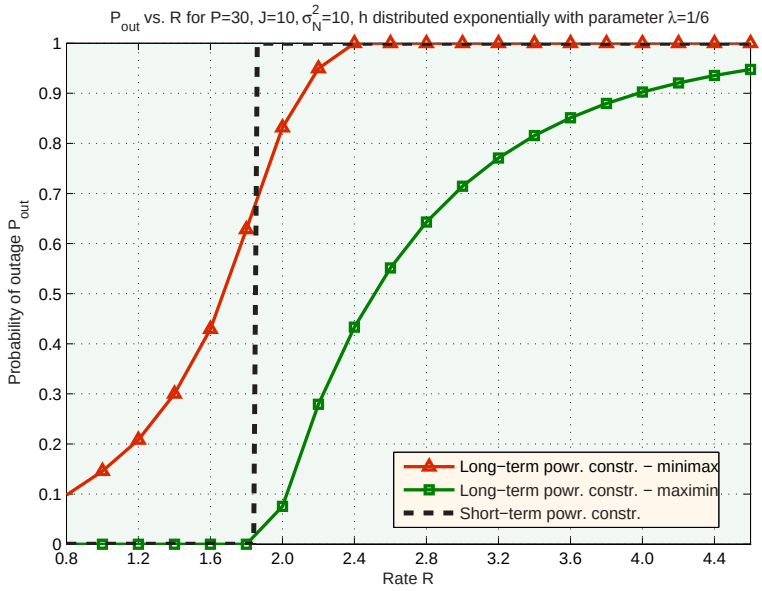

FIGURE 2.5. Outage probability vs. rate for $\mathcal{P} = 30$, $\mathcal{J} = 10$, $\sigma_N^2 = 10$ and h is distributed exponentially, with parameter $\lambda = 1/6$.

In this section we investigate the jamming game with average power constraints when mixed (probabilistic) strategies are considered. Similarly to the pure strategies scenario of the previous section, this game is played on two levels, with the first (coarser) level dealing with power allocation between frames. Its cost/reward function is the probability of outage. We assume that the jammer's and transmitter's randomized strategies consist of picking the power values to be invested over a frame in a random manner. In our previous notation, P_M and J_M are now random variables, and each frame is characterized by a realization (p_M, j_M) of the pair (P_M, J_M).

Given this realization, each player has to distribute its power over the frame in an optimal way. This is the purpose of the second (finer) level of power control. The objective of each player at this level is to make the best of the available resources (i.e. the powers (p_M, j_M)). This means maximizing (or minimizing, respectively) the average rate supported by the frame, in the hope that the resulting average rate will be above (or below, respectively) the system's fixed rate R.

2.4.1 Power Allocation within a Frame

We can formulate the second level of power control similarly to the two-player, zero-sum game of (2.3) and (2.4) having the ergodic capacity calculated over a frame $C(P(h), J(h))$ as cost function. The difference is that under the current scenario, none of the players knows the other player's constraints, because (P_M, J_M) is a random event. Theorem 2.10 below provides the optimal transmitter/jammer strategies for power allocation within a frame.

Theorem 2.10. *Given a realization (p_M, j_M) of (P_M, J_M), let $\mathscr{P}_M(j_M)$ denote the solution of* Problem 1 *in Section 2.3 with $J_M = j_M$, and $\mathscr{J}_M(p_M)$ denote the solution of* Problem 2 *in Section 2.3 with $P_M = p_M$.*

The transmitter's optimal strategy is the solution of the game in (2.3) and (2.4), where the jammer is constrained to $\mathbf{E}_h[J(h)] \leq \mathscr{J}_M(p_M)$ and the transmitter is constrained to $\mathbf{E}_h[P(h)] \leq p_M$. The jammer's optimal strategy is the solution of the game in (2.3) and (2.4), where the transmitter is constrained to $\mathbf{E}_h[P(h)] \leq \mathscr{P}_M(j_M)$ and the jammer is constrained to $\mathbf{E}_h[J(h)] \leq j_M$.

Note that each of the two players deploys the strategy that results from the most pessimistic scenario that it can handle successfully.

Proof. Denote the solution of the game in (2.3) and (2.4), where the jammer is constrained to $\mathbf{E}_h[J(h)] \leq \mathscr{J}_M(p_M)$ and the transmitter is constrained to $\mathbf{E}_h[P(h)] \leq p_M$ by $(P_1(h), J_1(h))$, and the solution of the game in (2.3) and (2.4), where the transmitter is constrained to $\mathbf{E}_h[P(h)] \leq \mathscr{P}_M(j_M)$ and the jammer is constrained to $\mathbf{E}_h[J(h)] \leq j_M$ by $(P_2(h), J_2(h))$.

Denote the solution of the game in (2.3) and (2.4), where the jammer is constrained to $\mathbf{E}_h[J(h)] \leq j_M$ and the transmitter is constrained to $\mathbf{E}_h[P(h)] \leq p_M$ by $(P_0(h), J_0(h))$..

By the duality property of Theorem 2.21 in Section 2.8.4, we must have $C(P_1(h), J_1(h)) = R$ and $C(P_2(h), J_2(h)) = R$.

We will show that (i) even if mixed strategies are considered for the game in (2.3) and (2.4), any Nash equilibrium has the same value as the Nash equilibrium of pure strategies; (ii) even if the

jammer's power j_M is different from $\mathscr{J}_M(p_M)$, the transmitter's strategy is still optimal; (iii) even if the transmitter's power p_M is different from $\mathscr{P}_M(j_M)$, the jammer's strategy is still optimal.

(i): Since the game of (2.3) and (2.4) is a two-person zero-sum game, all Nash equilibria of mixed strategies yield the same value of the cost/reward function [33]. Moreover, the two players are indifferent between all equilibria. It was shown in [9] that this game has a Nash equilibrium of pure strategies. But any equilibrium of pure strategies is also an equilibrium of mixed strategies [33] and hence it is enough to consider the equilibrium of pure strategies found in [9].

(ii),(iii): Assume the transmitter plays the strategy given by $P_1(h)$.

If $j_M = \mathscr{J}_M(p_M)$, it is clear that the optimal solution for both transmitter and jammer is the solution of the game in (2.3) and (2.4), where the jammer is constrained to $\mathbf{E}_h[J(h)] \leq j_M$ and the transmitter is constrained to $\mathbf{E}_h[P(h)] \leq p_M$. In this case, it is as if each player knows the other player's power constraint.

If $j_M < \mathscr{J}_M(p_M)$, then by Lemma 2.16 in Section 2.8.3 we have that $J_0(h) < J_1(h)$. Since $C(P(h), J(h))$ is a strictly decreasing function of $J(h)$ (under the order relation defined in Section 2.8.4), this implies that $C(P_1(h), J_0(h)) > R$. Note that $J_0(h)$ is the jammer's strategy when the jammer knows the transmitter's power constraint p_M. Thus we have shown that when the transmitter plays $P_1(h)$ and $j_M < \mathscr{J}_M(p_M)$, the jammer cannot induce outage over the frame even if it knew the value of p_M.

The condition $j_M > \mathscr{J}_M(p_M)$ is equivalent to $p_M < \mathscr{P}_M(j_M)$ (by Theorem 2.21). In this case, since the jammer plays the strategy given by $J_2(h)$, a similar argument as above (but this time applied to the transmitter's strategy) shows that the transmitter cannot achieve reliable communication over the frame even if it knew the exact value of j_M.

This accomplishes the proof and shows that $(P_1(h), J_2(h))$ is a Bayes equilibrium [33] for the game with incomplete information describing the power allocation within a frame. □

2.4.2 Power Allocation between Frames

Due to the form of the optimal second level power allocation strategies described in the previous subsection, the outage probability can be expressed as

$$P_{out} = Pr\{J_M \geq \mathscr{J}_M(P_M)\} = 1 - Pr\{P_M \geq \mathscr{P}_M(J_M)\}, \tag{2.38}$$

where $\mathscr{P}_M(J_M)$ is the strictly increasing, unbounded and concave function of Proposition 2.6. The optimal mixed strategies for power allocation between frames are presented in the following theorem.

Theorem 2.11. *The unique Nash equilibrium of mixed strategies of the two-player, zero-sum game with average power constraints described in (2.9) and (2.10) is attained by the pair of strategies* $(F_P(p_M), F_J(j_M))$ *satisfying:*

$$F_P(\mathscr{P}_M(y)) \sim k_p \mathbb{U}([0, 2v])(y) + (1 - k_p)\Delta_0(y), \tag{2.39}$$

$$F_J(\mathscr{J}_M(x)) \sim k_j \mathbb{U}([0, J_M(2v)])(x) + (1 - k_j)\Delta_0(x), \tag{2.40}$$

where $\mathbb{U}([r, t])(\cdot)$ *denotes the CDF of a uniform distribution over the interval* $[r, t]$*, and* $\Delta_0(\cdot)$ *denotes the CDF of a Dirac distribution (i.e. a step function), and the parameters* $k_p, k_j \in [0, 1]$ *and* $v \in [\max\{\mathcal{J}, \mathscr{J}_M(\mathcal{P})/2\}, \infty)$ *are uniquely determined from the following steps:*

1. *Find the unique value* v_0 *which satisfies:*

$$\mathcal{P}\mathcal{J} = [\mathscr{P}_M(2v_0) - \mathcal{P}](2v_0 - \mathcal{J}). \tag{2.41}$$

2. *Compute* $S(v_0) = \int_0^{2v_0} \mathscr{P}_M(y)dy - 2v_0\mathcal{P}$.

3. *If* $S(v_0) < 0$*, then* v *is the unique solution of*

$$\int_0^{2v} \mathscr{P}_M(y)dy - 2v\mathcal{P} = 0, \tag{2.42}$$

$$k_p = 1 \tag{2.43}$$

and

$$k_j = \frac{\mathcal{J}\mathscr{P}_M(2v)}{2v[\mathscr{P}_M(2v) - \mathcal{P}]}. \tag{2.44}$$

4. *If* $S(v_0) = 0$ *then* $v = v_0$, $k_p = k_j = 1$.

5. *If* $S(v_0) > 0$, *then* v *is the unique solution of*

$$\int_0^{2v} \mathscr{P}_M(y)dy - \mathscr{P}_M(2v)(2v - \mathcal{J}) = 0, \tag{2.45}$$

$$k_p = \frac{2v\mathcal{P}}{\mathscr{P}_M(2v)[2v - \mathcal{J}]} \tag{2.46}$$

and

$$k_j = 1. \tag{2.47}$$

Proof. The proof follows directly from Theorem 2.22 in Section 2.9, by substituting $x = P_M$, $y = J_M$, $g(y) = \mathscr{P}_M(y)$, $g^{-1}(x) = \mathscr{J}_M(x)$, $a = \mathcal{P}$ and $b = \mathcal{J}$. It is also interesting to note that the condition $\int_0^b g(y)dy < \lim_{z\to\infty} \int_{g(b)}^{g(z)} g^{-1}(x)dx - b[g(z) - g(b)]$ is satisfied because $\mathscr{P}_M(y)$ is unbounded (Proposition 2.6). □

2.4.3 Numerical Results

For the same parameters as in subsection 2.3.3 we evaluated numerically the optimal probabilistic power control strategies. Figure 2.6 shows the probability of outage obtained under the mixed strategies Nash equilibrium, versus the transmitter power constraint $\mathcal{P}$, for a fixed rate $R = 2$, noise power $\sigma_N^2 = 10$, a jammer power constraint $\mathcal{J} = 10$ and a channel coefficient distributed exponentially, with parameter $\lambda = 1/6$. All the previously obtained curves are shown for comparison.

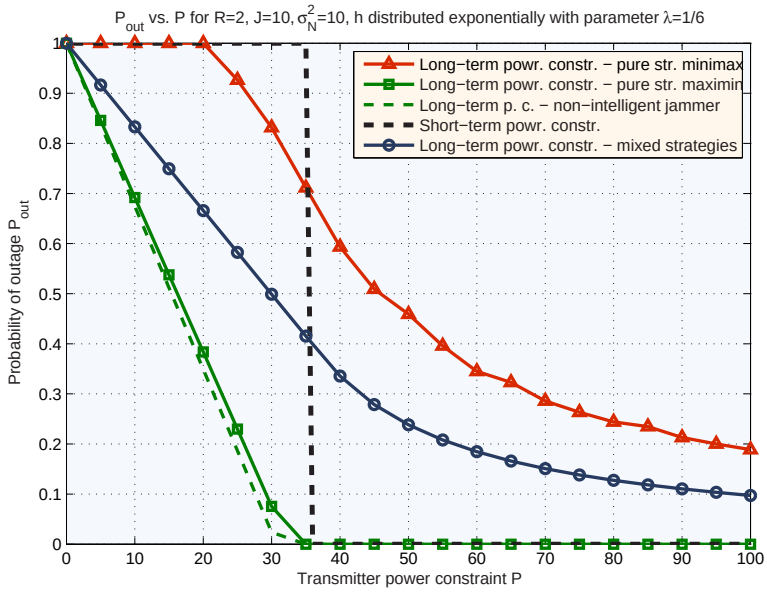

FIGURE 2.6. Outage probability vs. transmitter power constraint $\mathcal{P}$ when $\mathcal{J} = 10$, $R = 2$, $\sigma_N^2 = 10$ and h is distributed exponentially, with parameter $\lambda = 1/6$.

Figure 2.7 shows the same probability of outage when $\mathcal{P} = 30$ and the system rate R is varied. In both figures it can be seen that the system performance under the Nash equilibrium of mixed strategies is better (from the transmitter's point of view) than the minimax and worse than the maximin solutions of the pure strategies game. This is expected since the pure strategies solutions assume that the second player (the "follower") is constantly at a disadvantage with the first player (the "leader").

2.5 CSI Available to Receiver Only. Jamming Game with Average Power Constraints: Mixed Strategies

In this section we investigate the scenario when the receiver does not feed back any channel state information. Since we have already shown that the long term power constraints problem is the more interesting and challenging one, we further focus only on the scenario of average power constraints and mixed strategies. As in the previous sections, we have to discuss two levels of power control: within a frame and between frames.

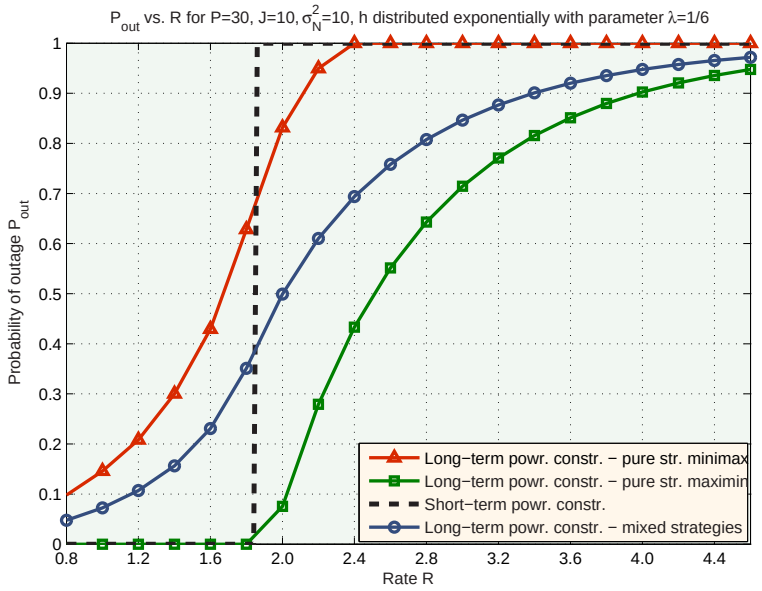

FIGURE 2.7. Outage probability vs. rate for $\mathcal{P} = 30$, $\mathcal{J} = 10$, $\sigma_N^2 = 10$ and h is distributed exponentially, with parameter $\lambda = 1/6$.

2.5.1 Power Allocation within a Frame

The jammer and transmitter powers allocated to each frame will be established in the next subsection. For now we are concerned with the optimal power allocation within a frame, given the amounts of power invested in that frame by each one of the players. For a given frame, denote these powers by P_M and J_M, to be consistent with our previous notation. Both the transmitter and the jammer will choose a probability distribution for the randomly variable power levels P and J, respectively, such that $\mathbf{E}_P P \leq P_M$ and $\mathbf{E}_J J \leq J_M$, where the notations $\mathbf{E}_P$ and $\mathbf{E}_J$ denote the expectations with respect to these probability distributions. For the generic channel use, the channel coefficient h, the transmitter's power P and the jammer's power J are all independent random variables, which yield the randomly variable instantaneous mutual information $\log\left(1 + \frac{hP}{J+\sigma_N^2}\right)$. For a frame, this results in the ergodic capacity $\mathbf{E}_{h,P,J} \log\left(1 + \frac{hP}{J+\sigma_N^2}\right)$, where $\mathbf{E}_h$ denotes expectation with respect to the channel coefficient.

The transmitter's purpose is to use the allocated power P_M in an attempt to make this ergodic capacity larger than the rate R. Similarly, the jammer is concerned with using J_M for making the

ergodic capacity fall below R. The problem of allocating the power within the frame can be written as:

$$\max_{P:\mathbf{E}_P P\le P_M}\ \min_{J:\mathbf{E}_J J\le J_M} \mathbf{E}_{h,P,J}\log\left(1+\frac{hP}{J+\sigma_N^2}\right). \tag{2.48}$$

Denote $L(P,J)=\mathbf{E}_h\log\left(1+\frac{hP}{J+\sigma_N^2}\right)$ and let us observe that

$$\frac{dL}{dP}=\mathbf{E}_h\frac{h}{Ph+J+\sigma_N^2}>0, \tag{2.49}$$

$$\frac{dL}{dJ}=-\mathbf{E}_h\frac{Ph}{(Ph+J+\sigma_N^2)(J+\sigma_N^2)}<0, \tag{2.50}$$

$$\frac{d^2L}{dP^2}=-\mathbf{E}_h\left(\frac{h}{Ph+J+\sigma_N^2}\right)^2<0, \tag{2.51}$$

$$\frac{d^2L}{dJ^2}=\mathbf{E}_h\frac{Ph(Ph+2J+2\sigma_N^2)}{[J^2+J(Ph+2\sigma_N^2)+\sigma_N^2(Ph+\sigma_N^2)]^2}>0, \tag{2.52}$$

which implies that $L(P,J)$ is a strictly increasing, concave function of P for fixed J, and a strictly decreasing, convex function of J for fixed P.

Thus, we can write

$$\mathbf{E}_{h,P}\log\left(1+\frac{hP}{J_M+\sigma_N^2}\right)\le\mathbf{E}_h\log\left(1+\frac{hP_M}{J_M+\sigma_N^2}\right)\le\mathbf{E}_{h,J}\log\left(1+\frac{hP_M}{J+\sigma_N^2}\right), \tag{2.53}$$

and hence the uniform distribution of P_M and J_M over the frame achieves a Nash equilibrium. A frame to which the transmitter allocates power P_M and the jammer allocates power J_M is in outage if and only if

$$\mathbf{E}_h\log\left(1+\frac{hP_M}{J_M+\sigma_N^2}\right)\le R. \tag{2.54}$$

The probability of this event depends on the power allocation between frames and is the subject of the first level of power control treated in the next subsection.

But before we get to that, we need to make several comments. Note that if we force equality in (2.54) above, we obtain a $\mathscr{P}'_M(J_M)$ curve as in Section 2.3. It is straightforward to see that the

$\mathscr{P}'_M(J_M)$ curve is affine, because solving (2.54) with equality yields $P_M = \mu'(J_M + \sigma_N^2)$ where μ' is the (unique) solution of $\mathbf{E}_h \log(1 + \mu' h) = R$. Recall that the curve $\mathscr{P}_M(J_M)$ of Section 2.3 (with full CSI) is *almost* affine due to the fact that the measure of the set of channel realizations, within a frame, over which the transmitter is present but the jammer is not, is often quite small. For this reason, we expect the $\mathscr{P}'_M(J_M)$ and the $\mathscr{P}_M(J_M)$ curves to be very close to each other.

Although the two curves are still different in general, they have the same physical interpretation: if the jammer invests power j_M over a frame, and the power p_M invested by the transmitter satisfies $p_M < \mathscr{P}'_M(j_M)$, then the frame is in outage. Otherwise, if $p_M > \mathscr{P}'_M(j_M)$, the frame supports the asymptotically error-free decoding of the transmitted codeword.

As in Section 2.3, we shall denote by $\mathscr{J}'_M(P_M)$ the "inverse" of the $\mathscr{P}'_M(J_M)$ function, or the symmetric of the $\mathscr{P}'_M(J_M)$ curve with respect to the first bisector.

2.5.2 Power Allocation between Frames

The arguments of this subsection are very similar to those of Subsection 2.4.2 and will not be discussed in great detail. We have seen that the outage probability can be expressed as

$$P_{out} = Pr\{J_M \geq \mathscr{J}'_M(P_M)\} = 1 - Pr\{P_M \geq \mathscr{P}'_M(J_M)\}, \tag{2.55}$$

where $\mathscr{P}'_M(J_M)$ is an affine, and hence strictly increasing and unbounded function of the form $\mathscr{P}'_M(J_M) = \mu' J_M + \mu' \sigma_N^2$. The optimal mixed strategies for power allocation between frames are presented in the following theorem.

Theorem 2.12. *The unique Nash equilibrium of mixed strategies of our two-player, zero-sum game with average power constraints is attained by the pair of strategies* $(F_P(p_M), F_J(j_M))$ *satisfying:*

$$F_P(x) \sim k_p \mathbb{U}([\mu' \sigma_N^2, 2v\mu' + \mu' \sigma_N^2])(x) + (1 - k_p)\Delta_0(x),$$

$$F_J(y) \sim \frac{2v}{2v + \sigma_N^2} k_j \mathbb{U}([0, 2v])(y) + (1 - \frac{2v}{2v + \sigma_N^2} k_j)\Delta_0(y),$$

where $\mathbb{U}([r,t])(\cdot)$ *denotes the CDF of a uniform distribution over the interval* $[r,t]$*, and* $\Delta_0(\cdot)$ *denotes the CDF of a Dirac distribution (i.e. a step function), and the parameters* $k_p, k_j \in [0,1]$ *and* $v \in [\max\{\mathcal{J}, \mathscr{J}'_M(\mathcal{P})/2\}, \infty)$ *are uniquely determined from the following steps:*

1. *If*

$$\mathcal{P} \geq \mu'\sigma_N^2 + \frac{1}{2}\mu'\mathcal{J}\left[1 + \sqrt{1 + \frac{2\sigma_N^2}{\mathcal{J}}}\right], \tag{2.56}$$

then

$$v = \frac{\mathcal{P} - \mu'\sigma_N^2}{\mu'}, \tag{2.57}$$

$$k_p = 1 \tag{2.58}$$

and

$$k_j = \frac{\mu'\mathcal{J}(2\mathcal{P} - \mu'\sigma_N^2)}{2(\mathcal{P} - \mu'\sigma_N^2)^2}. \tag{2.59}$$

2. *If*

$$\mathcal{P} < \mu'\sigma_N^2 + \frac{1}{2}\mu'\mathcal{J}\left[1 + \sqrt{1 + \frac{2\sigma_N^2}{\mathcal{J}}}\right], \tag{2.60}$$

then

$$v = \frac{1}{2}\mathcal{J}\left[1 + \sqrt{1 + \frac{2\sigma_N^2}{\mathcal{J}}}\right], \tag{2.61}$$

$$k_p = \frac{2v\mathcal{P}}{\mu'(2v + \sigma_N^2)(2v - \mathcal{J})} \tag{2.62}$$

and

$$k_j = 1. \tag{2.63}$$

Proof. The proof follows directly from Theorem 2.22 in Section 2.9, by substituting $x = P_M$, $y = J_M$, $g(y) = \mathscr{P}'_M(y)$, $g^{-1}(x) = \mathscr{J}'_M(x)$, $a = \mathcal{P}$ and $b = \mathcal{J}$. It is also interesting to note that the condition $\int_0^b g(y)dy < \lim_{z\to\infty}\int_{g(b)}^{g(z)} g^{-1}(x)dx - b[g(z) - g(b)]$ is satisfied because $\mathscr{P}'_M(y)$ is unbounded. □

2.5.3 Numerical Results

In this subsection we provide the numerical evaluation of our system's performance when no channel state information is fed back by the receiver. The parameters are identical to those used in the numerical evaluation of the previous sections.

The new $\mathscr{P}_M(J_M)$ curve is given in Figure 2.8. It can be seen that for a given jamming power allocated to a frame, the transmitter power required to ensure asymptotically error-free transmission over that frame is only slightly larger if no CSI is fed back than when full CSI is available to all parties.

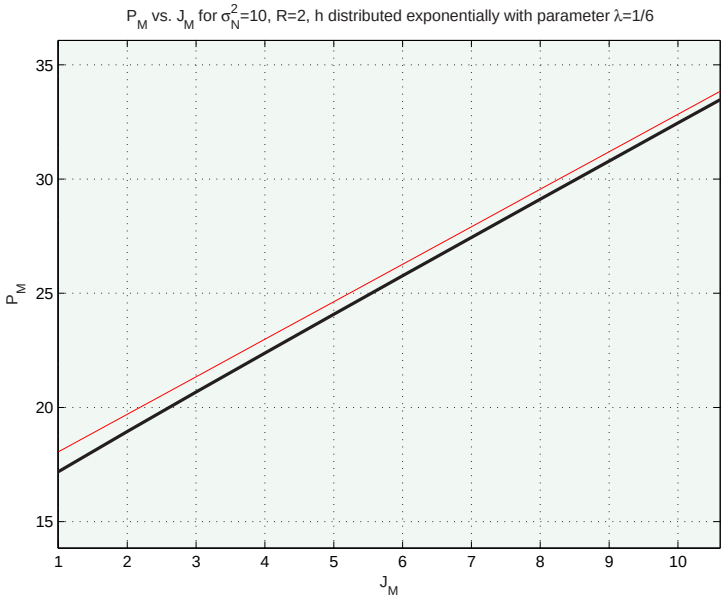

FIGURE 2.8. P_M vs. J_M curve with and without CSI feedback when $R = 2$, $\sigma_N^2 = 10$ and h is distributed exponentially, with parameter $\lambda = 1/6$.

This observation explains the very small difference in achievable outage probabilities that can be observed in Figures 2.9 and 2.10.

2.6 Conclusions

We have shown that for a high transmission rate R the jammer could have enough power to keep the ergodic capacity below R. In this scenario, if the transmitter imposes average power constraints

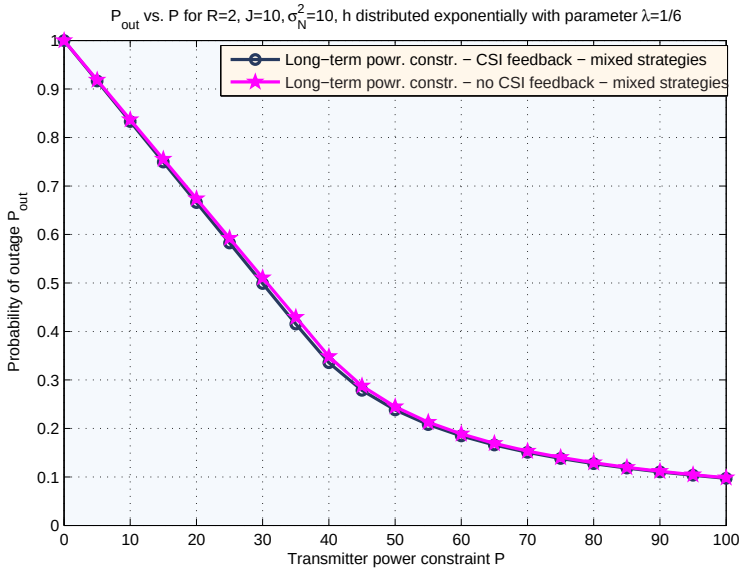

FIGURE 2.9. Outage probability vs. transmitter power constraint $\mathcal{P}$ with and without CSI feedback when $\mathcal{J} = 10$, $R = 2$, $\sigma_N^2 = 10$ and h is distributed exponentially, with parameter $\lambda = 1/6$. (Mixed strategies.)

rather than peak power constraints, reliable communication is possible at the cost of a non-zero probability of outage.

If both transmitter and jammer use average power constraints, their optimal strategies result as solutions of a two-person zero-sum game. This game is played on two levels of power control. The second level (power control within a frame) exhibits similar strategies for the pure (maximin and minimax cases) and mixed strategies scenarios. However in the pure strategies scenario, maximin and minimax first level power control (between frames) is generally done differently, implying the non-existence of a Nash equilibrium. A Nash equilibrium was derived for the mixed strategies scenario, placing the value of the objective function between those of the minimax and maximin pure strategies solutions.

Although it may seem that the mixed strategies game makes more sense from a practical point of view, the pure strategies minimax scenario may be a more appropriate model for the case when the jammer does not attempt to jam unless it senses that the transmitter is on. In any circumstances, the minimax scenario with pure strategies serves as a lower bound (the pessimistic approach) to the system's performance.

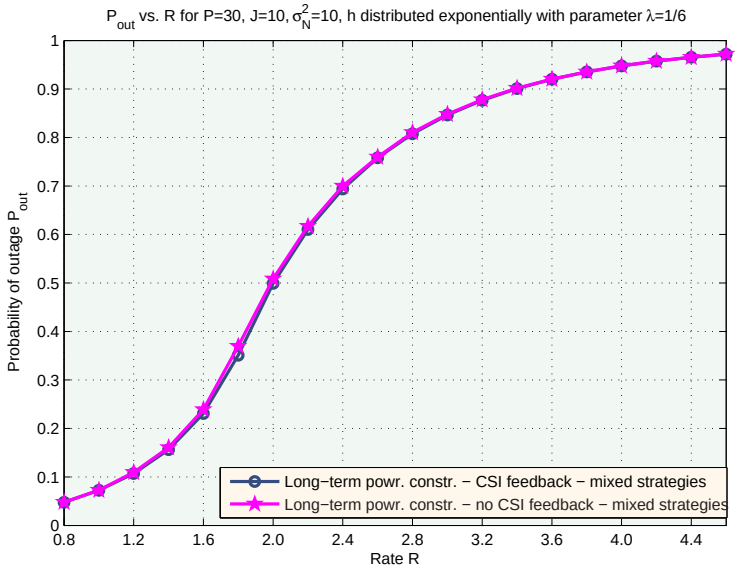

FIGURE 2.10. Outage probability vs. rate with and without CSI feedback for $\mathcal{P} = 30$, $\mathcal{J} = 10$, $\sigma_N^2 = 10$ and h is distributed exponentially, with parameter $\lambda = 1/6$.(Mixed strategies.)

The feedback of CSI by the legitimate receiver is known to bring benefits (in terms of achievable transmission rate) when nobody attempts to jam the transmission. However, for a fast fading AWGN channel, these improvements are shown to be marginal [35]. We have shown that a similar conclusion holds (this time in terms of outage probability) for the case when the parties that communicate over the fast fading AWGN channel are under attack from a jammer. The CSI fed back can easily be intercepted by the jammer, which can then use this information to the transmitter's disadvantage. If one should also take into account the loss of bandwidth and the complexity required for CSI feedback and processing, keeping the transmitter (and jammer) ignorant of the channel coefficients may seem a better choice.

The same remark cannot be made for a parallel slow fading AWGN channel. It was shown in [32] that when CSI is fed back and no jamming is present, the improvements in terms of probability of outage are significant. In Chapter 3 we show that this conclusion also holds if we consider the jamming scenario. In doing this we exploit the similarities that the parallel slow fading channel bears to the fast fading channel, and develop new and even more interesting techniques to make up for the additional complexity incurred by this new model.

2.7 Additional Results for Peak Power Constraints - Proof of Theorem 2.2

This proof follows the one described in the Appendix B of [32]. The probability of outage can be written as:

$$Pr(C(P(h), J(h)) < R) = E[\chi_{\{C(P(h),J(h))<R\}}], \tag{2.64}$$

where $\chi_{\{\mathscr{A}\}}$ denotes the indicator function of the set $\mathscr{A}$. Replacing the power allocations by the solutions of the game described by (2.3) and (2.4), we define

$$\chi^* = \chi_{\{C(P^*(h),J^*(h))<R\}}. \tag{2.65}$$

We next use the fact that the pair $(P^*(h), J^*(h))$ determines an equilibrium of the game (2.3), (2.4). Thus, for any random power allocation $P(h)$ satisfying the power constraint, we can write:

$$\chi^* \leq \chi_{\{C(P(h),J^*(h))<R\}}, \text{with probability } 1. \tag{2.66}$$

Similarly, for any random $J(h)$, we have

$$\chi^* \geq \chi_{\{C(P^*(h),J(h))<R\}}, \text{with probability } 1. \tag{2.67}$$

Now pick some arbitrary power allocation functions $P_a(h)$ and $J_a(h)$, which satisfy the peak power constraints, and set

$$\widehat{P}(h) = (1 - \chi^*)P^*(h) + \chi^* P_a(h), \tag{2.68}$$

and

$$\widehat{J}(h) = (1 - \chi^*)J_a(h) + \chi^* J^*(h), \tag{2.69}$$

It is easy to see that $\mathbf{E}_h\widehat{P}(h) \leq \mathcal{P}$ with probability 1 , $\mathbf{E}_h\widehat{J}(h) \leq \mathcal{J}$ with probability 1, and moreover that

$$\chi^* = \chi_{\{C(\widehat{P}(h),\widehat{J}(h))<R\}}. \tag{2.70}$$

Note that transmitter and jammer could pick $P_a(h) = 0$ and $J_a(h) = 0$ respectively, but this strategy would not improve their performances (power cannot be saved), since the only power constraints are set over frames.

Now, using (2.64), (2.66) and (2.67), we get:

$$Pr(C(P(h), \widehat{J}(h)) < R) \geq Pr(C(\widehat{P}(h), \widehat{J}(h)) < R) \geq Pr(C(\widehat{P}(h), J(h)) < R), \qquad (2.71)$$

which proves the existence of a Nash equilibrium of the original game.

2.8 Additional Results for Average Power Constraints: Pure Strategies

2.8.1 Proof of Proposition 2.3

In proving the proposition, we take a contradictory approach. It suffices to show that the situation $J(h) > 0$ and $\lambda < x(h)/h$ cannot be part of the solution of *Problem 1*.

Assume that $J(h) > 0$ and $\lambda < x(h)/h$ for h in some set $\mathscr{S} \subset \mathbb{R}_+$. If the jammer decreases the value of $J(h)$ on $\mathscr{S}$, two situations are possible. In the first one, $J(h)$ is reduced to zero on $\mathscr{S}$, and the transmitter is still "absent". This happens if $\sigma_N^2 > \lambda h$. In this case, modifying the value of $J(h)$ has no impact upon the value of λ, and hence neither upon the outcome.

In the second case $J(h)$ is reduced to some positive value $J'(h)$, such that the transmitter decides to be "non-absent" over $\mathscr{S}$. This happens if $J'(h) + \sigma_N^2 = \lambda' h$. Note that the value of λ might be changed to some λ'. However, as we shall see briefly, if we consider $J'(h)$ that satisfies $J'(h) + \sigma_N^2 = \lambda' h$, then we have $\lambda' = \lambda$.

To prove this, let λ be given by (2.16), and assume that $\lambda - x(h)/h \geq 0$ for $h \in \mathscr{M}'$, and $\lambda - x(h)/h < 0$ for $h \in \mathscr{S}$. Now modify $x(h)$ by decreasing $J(h)$ as above. We have

$$\lambda' = c^{\frac{1}{\mathfrak{m}(\mathscr{M}' \cup \mathscr{S})}} \left\{ \exp\left[\mathbf{E}_{h \in \mathscr{M}' \cup \mathscr{S}} \left(\log \frac{x(h)}{h} \right) \right] \right\}^{\frac{1}{\mathfrak{m}(\mathscr{M}' \cup \mathscr{S})}} = \frac{x(h)}{h}, \text{ for } h \in \mathscr{S}. \qquad (2.72)$$

Note that for $h \in \mathscr{S}$ we have $\frac{x(h)}{h} = \lambda'$, so

$$\mathbf{E}_{h \in \mathscr{S}} \log \frac{x(h)}{h} = \log \lambda' \mathfrak{m}(\mathscr{S}). \qquad (2.73)$$

Taking logarithm of (2.72):

$$\frac{1}{\mathfrak{m}(\mathscr{M}')+\mathfrak{m}(\mathscr{S})}\left[\log c+\mathbf{E}_{h\in\mathscr{M}'}\left(\log\frac{x(h)}{h}\right)+\mathbf{E}_{h\in\mathscr{S}}\left(\log\frac{x(h)}{h}\right)\right]=\log\frac{x(h)}{h},\ \text{for } h\in\mathscr{S}, \tag{2.74}$$

and noting that the left hand side of (2.74) is independent of the actual realizations of h, we can compute the expectation over $h\in\mathscr{S}$, and get:

$$\frac{\mathfrak{m}(\mathscr{S})}{\mathfrak{m}(\mathscr{M}')+\mathfrak{m}(\mathscr{S})}\left[R+\mathbf{E}_{h\in\mathscr{M}'}\left(\log\frac{x(h)}{h}\right)\right]=\frac{\mathfrak{m}(\mathscr{M}')}{\mathfrak{m}(\mathscr{M}')+\mathfrak{m}(\mathscr{S})}\mathbf{E}_{h\in\mathscr{S}}\left(\log\frac{x(h)}{h}\right). \tag{2.75}$$

Using (2.73), this leads to

$$\log\lambda=\frac{1}{\mathfrak{m}(\mathscr{M}')}\left[R+\mathbf{E}_{h\in\mathscr{M}'}\left(\log\frac{x(h)}{h}\right)\right]=\frac{1}{\mathfrak{m}(\mathscr{S})}\mathbf{E}_{h\in\mathscr{S}}\left(\log\frac{x(h)}{h}\right)=\log\lambda'. \tag{2.76}$$

Therefore the outcome is maintained because, although "non-absent", the transmitter still invests zero power on $\mathscr{S}$.

Hence if such a situation where the jammer transmits on a set of channel coefficient values over which the transmitter is "absent" occurs, the jammer can save power and maintain the same outcome. Meanwhile the new set over which jammer transmits becomes a subset of the new set over which the transmitter is "non-absent".

2.8.2 Proof of Proposition 2.4

We already know that the optimal $x(h)$ is a continuous function of $h\in\mathscr{M}''$ if $\mathscr{M}'$ and $\mathscr{M}''$ are fixed.

The following lemma shows that under this scenario the optimal $x(h)$ is also unique.

Lemma 2.13. *For fixed $\mathscr{M}'$ and $\mathscr{M}''$, the KKT conditions (2.20)–(2.22) admit a unique solution.*

Proof. Consider $\mathscr{M}'$ and $\mathscr{M}''$ to be fixed. The constant μ resulting from (2.20)–(2.22) can be computed as in (2.29). This implies that $J_M(\mu)$ is a strictly decreasing function, hence an injection.

Thus, for a given J_M there exists a unique corresponding value of μ, and since $x(h)$ is a deterministic function of μ, a unique solution $x(h)$. □

Suppose the jammer's optimal power distribution $x^*(h)$ is not continuous over the whole $\mathbb{R}_+$.

Note that an optimal power distribution $x^*(h)$ obtained for fixed $\mathscr{M}'$ and $\mathscr{M}''$ can only be a globally optimal solution (i.e. over all possible choices of $\mathscr{M}'$ and $\mathscr{M}''$), if by keeping the same $\mathscr{M}'$ and extending $\mathscr{M}''$ to a set ${\mathscr{M}''}_n$ that contains a discontinuity point , the new optimal strategy is either the same as $x^*(h)$, or violates the constraint $x(h) \geq \sigma_N^2$. But an optimal strategy has to be continuous over ${\mathscr{M}''}_n$, and hence the constraint $x(h) \geq \sigma_N^2$ has to be violated on the left-most side of ${\mathscr{M}''}_n$ (according to (2.28)).

Also note that if under the optimal strategy the jammer allocates some power J_x over a set $\mathscr{M} \subset \mathbb{R}_+$, then the distribution of J_x over $\mathscr{M}$ should be done optimally, according to (2.28), (2.29). This implies that by extending the set $\mathscr{M}$ by a set $\mathscr{N}$ disjoint from $\mathscr{M}''$, and re-allocating J_x over $\mathscr{M}_x \bigcup \mathscr{N}$, the constraint $x(h) \geq \sigma_N^2$ will be violated on the left-most side of $\mathscr{M}_x \bigcup \mathscr{N}$.

The arguments above imply the following:

1. The optimal jamming power allocation should be such that $x(h) = \sigma_N^2$ on the left-most point of $\mathscr{M}''$: otherwise extend $\mathscr{M}''$ by an arbitrarily small set to the left and increase J_M until $x(h) = \sigma_N^2$ on the left-most point of the new set ${\mathscr{M}''}_n$; by continuity of $x(h)$, the left-most point of $\mathscr{M}''$ should be arbitrarily close to σ_N^2.

2. The optimal jamming power allocation should be such that $\mathscr{M}'' = [h^*, \infty)$: otherwise take a subset $\mathscr{M}_x \subset \mathscr{M}''$, such that there exists a set $\mathscr{N}$ situated to the right of $\mathscr{M}_x$, and denote by J_x the jamming power originally allocated to $\mathscr{M}_x$. By re-allocating J_x over $\mathscr{M}_x \bigcup \mathscr{N}$, the constraint $x(h) \geq \sigma_N^2$ will be violated on the left-most side of $\mathscr{M}_x$. If $\mathscr{N}$ is picked of arbitrarily small $\mathfrak{m}$-measure, by the previous arguments we should have $x(h)$ arbitrarily close to σ_N^2 at the left-most point of $\mathscr{M}_x$. But since $\mathscr{M}_x$ is arbitrary, this yields the contradiction that $x(h) = \sigma_N^2$ for any h to the left of $\mathscr{N}$.

This proves Proposition 2.4.

Note that if $\mu = 0$, then $P(h) = 0$ over $\mathscr{M}''$, and since $x(h)/h$ is decreasing over the whole $\mathbb{R}_+$, and $\mathscr{M}'' = [h^*, \infty)$, this implies that the transmitter does not transmit at all. However, this strategy does not achieve an ergodic capacity larger than the rate R, and hence it results in a contradiction.

2.8.3 Proof of Proposition 2.6

Recall Proposition 2.6: *Under the optimal maximin second level power control strategies, the "required" transmitter power P_M over a frame is a strictly increasing, unbounded and concave function of the power J_M that the jammer invests in that frame.*

The fact that $\mathscr{P}_M(J_M)$ is strictly increasing follows from Proposition 2.5 and Proposition 2.20. If $J_{M,1} < J_{M,2}$ existed such that $P_M(J_{M,1}) = P_M(J_{M,2})$, then when the jammer's power constraint is $J_{M,2}$, *Problem 1* would either have two different solutions, or the solution would satisfy the constraint with strict inequality.

If $J_M \to \infty$ then (2.28) implies that $J(h) \to \infty$ for any h. If P_M was finite, this would imply $C(P(h), J(h)) \to 0$, which violates the constraints of *Problem 1*. Hence $\mathscr{J}_M(P_M)$ has to be unbounded.

In proving concavity of the $\mathscr{P}_M(J_M)$ function for the case when the channel coefficient h belongs to a continuous alphabet, we first show that the solution of the discretized problem (i.e. when h belongs to a discrete alphabet, obtained by some discretization of the original continuous alphabet) is unique and converges point-wise to the solution of the continuous problem as the discrete alphabet converges to the original continuous alphabet.

This approach also serves the purpose of legitimizing numerical evaluations.

Next, we prove that for the discretized problem $\mathscr{P}_M(J_M)$ is concave. Finally, we show that point-wise convergence of a sequence of concave functions is enough for the concavity of its limit function.

Consider the uniformly spaced discretization $q\mathbb{Z}_+$ of the interval $[0, \infty)$, and a p.m.f. of the channel coefficient $h \in q\mathbb{Z}_+$ that converges to the original p.d.f. as q goes to zero.

The maximin second level power allocation problem can still be written as in (2.11), even though the integrals representing the expectations can now be written as sums. Moreover, Propositions 2.3–2.4 and relations (2.15)–(2.29) hold with the only modification that the term "continuous" should be crossed out.

The second level power allocation solution for the discretized maximin problem is completely determined by the triple $(\mathscr{M}', \mathscr{M}'', \mu)$, or equivalently by (h^0, h^*, μ). Instead of (2.30)–(2.32) we can now write

$$\frac{\sigma_N^2}{h^0} \leq \lambda < \frac{\sigma_N^2}{h^0 - q}, \tag{2.77}$$

$$\sigma_N^2 \frac{1+\mu h^*}{h^*} \leq \lambda < \sigma_N^2 \frac{1+\mu(h^*-q)}{h^*-q}, \tag{2.78}$$

$$R = \sum_{h_0}^{h^*-q} \log\left(\frac{\lambda h}{\sigma_N^2}\right) p(h) - \sum_{h^*}^{\infty} \log\left(\frac{1}{1+\mu h}\right) p(h), \tag{2.79}$$

or equivalently

$$Q_U\left[\frac{h^*-q}{1-\mu(h^*-q)}\right] \leq h^0 \leq Q_D\left[\frac{h^*}{1-\mu h^*} + q\right], \tag{2.80}$$

$$\sum_{h=h^*}^{\infty} \left[\frac{\frac{h}{1+\mu h}}{\frac{h^*}{1+\mu h^*}} - 1\right] p(h) \leq \frac{J_M}{\sigma_N^2} \leq \sum_{h=h^*}^{\infty} \left[\frac{\frac{h}{1+\mu h}}{\frac{h^*-q}{1+\mu(h^*-q)}} - 1\right] p(h), \tag{2.81}$$

$$\begin{aligned} \sum_{h=Q_D\left[\frac{h^*}{1+\mu h^*}+q\right]}^{h^*-q} \log\left(h\frac{1+\mu h^*}{h^*}\right) p(h) - \sum_{h^*}^{\infty} \log\left(\frac{1}{1+\mu h}\right) p(h) \leq R \leq \\ \leq \sum_{h=Q_U\left[\frac{h^*-q}{1+\mu(h^*-q)}\right]}^{h^*-q} \log\left(h\frac{1+\mu(h^*-q)}{h^*-q}\right) p(h) - \sum_{h^*}^{\infty} \log\left(\frac{1}{1+\mu h}\right) p(h), \end{aligned} \tag{2.82}$$

where $Q_D[h]$ denotes the largest element of $q\mathbb{Z}_+$ that is less than h and $Q_U[h]$ denotes the smallest element of $q\mathbb{Z}_+$ that is larger than h.

Lemma 2.14. *For a given J_M the solution of the discretized maximin second level power allocation problem is unique.*

Proof. It is straightforward to show that for fixed h^* the left-most and the right-most terms of inequality (2.81) (which upper-bound and lower-bound J_M/σ_N^2) are strictly decreasing functions of μ, and similarly the left-most and the right-most terms of inequality (2.82) are strictly increasing functions of μ.

Note that

$$\sum_{h=h^*}^{\infty}\left[\frac{\frac{h}{1+\mu h}}{\frac{h^*}{1+\mu h^*}}-1\right]p(h)=\sum_{h=h^*+q}^{\infty}\left[\frac{\frac{h}{1+\mu h}}{\frac{h^*}{1+\mu h^*}}-1\right]p(h), \tag{2.83}$$

$$Q_D\left[\frac{h^*-q}{1+\mu(h^*-q)}+q\right]=Q_U\left[\frac{h^*-q}{1+\mu(h^*-q)}\right], \tag{2.84}$$

and

$$\begin{aligned}&\sum_{h=Q_D\left[\frac{h^*}{1+\mu h^*}+q\right]}^{h^*-q}\log\left(h\frac{1+\mu h^*}{h^*}\right)p(h)-\sum_{h^*}^{\infty}\log\left(\frac{1}{1+\mu h}\right)p(h)=\\ &=\sum_{h=Q_D\left[\frac{h^*}{1+\mu h^*}+q\right]}^{h^*}\log\left(h\frac{1+\mu h^*}{h^*}\right)p(h)-\sum_{h^*+q}^{\infty}\log\left(\frac{1}{1+\mu h}\right)p(h).\end{aligned} \tag{2.85}$$

These arguments imply that by keeping μ constant and replacing h^* by h^*-q in both first terms of (2.81) and (2.82), we get exactly the last terms of (2.81) and (2.82), respectively. Thus, if (h^*,μ) satisfy both (2.81) and (2.82), then decreasing h^* (by more than one step) and maintaining the same μ violates both (2.81) and (2.82). In order for (2.81) to still hold, μ should be increased, while in order for (2.82) to still hold, μ should be decreased. But once h^* and μ are given, λ and hence h^0 are uniquely determined. Therefore there cannot exist more than one solution to the discretized problem. □

The following lemma deals with the convergence of this solution as $q\to 0$.

Lemma 2.15. *For a given J_M, the solution of the discretized maximin second level power allocation problem converges to the solution of the continuous problem as $q \to 0$.*

Proof. This follows by noticing that as $q \to 0$ (2.77)–(2.79) become arbitrarily close to (2.30)–(2.32), and the sums involved in the expectations converge to integrals (by the definition of the Riemann integral). □

Next we prove that for the discretized problem, the resulting $\mathscr{P}_M(J_M)$ function is concave. We first show in Lemma 2.16 that the optimal jammer strategy $\{x^*(h)\}_{h=0}^{\infty}$ is a continuous function of the given jamming power J_M. Lemma 2.17 proves that $P_M(\{x(h)\})$ is continuous and has continuous first order derivatives. This implies that $\mathscr{P}_M(J_M)$ is in fact continuous and has a continuous first order derivative. Finally, Lemma 2.18 shows that for any fixed M' and M'' the function $\mathscr{P}_M(J_M)$ is concave.

Lemma 2.16. *The optimal jammer power allocation $\{x^*(h)\}_{h\in q\mathbb{Z}_+}$ within a frame is a continuous increasing function of the given jamming power J_M invested over that frame.*

Proof. It is clear that $x(h)$ is continuous and increasing as a function of J_M if h^* and h^0 are fixed. At any point where either h^* or h^0 change as a result of a change in J_M, the optimal jamming strategy $\{x^*(h)\}_{h\in q\mathbb{Z}_+}$ maintains continuity as a result of the uniqueness of the solution (Lemma 2.14). □

Lemma 2.17. *Both $P_M(\{x(h)\})$ and the derivatives $\frac{dP_M}{dx(h)}$, for $h \in q\mathbb{Z}_+$ are continuous functions of $\{x(h)\}_{h\in q\mathbb{Z}_+}$.*

Proof. Consider any two points $\{x_1(h)\}_{h\in q\mathbb{Z}_+}$ and $\{x_2(h)\}_{h\in q\mathbb{Z}_+}$ and any trajectory $\mathfrak{T}$ that connects them.

Without loss of generality, assume that the channel coefficients are always indexed in decreasing order of the quantities $\frac{x(h)}{h}$.

For a given vector $\{x(h)\}_{h\in q\mathbb{Z}_+}$, the required transmitter power is

$$P_M = \lambda \sum_{h\in\mathscr{M}'} p(h) - \sum_{h\in\mathscr{M}'} \frac{x(h)}{h} p(h), \tag{2.86}$$

while the derivatives are given by

$$\frac{dP_M}{dx(h)} = \left[\frac{\lambda}{x(h)} - \frac{1}{h}\right] p(h) \tag{2.87}$$

for $h \in \mathscr{M}'$, with λ given by

$$\lambda(\mathscr{M}') = \left[c \prod_{h\in\mathscr{M}'} \left(\frac{x(h)}{h}\right)^{p(h)}\right]^{\frac{1}{\sum_{h\in\mathscr{M}'} p(h)}}. \tag{2.88}$$

Note that $\mathscr{M}'$ depends upon the choice of $\{x(h)\}$. For fixed $\mathscr{M}'$, the continuity and differentiability of $P_M(\{x(h)\})$ are obvious. Thus, it suffices to show that these properties also hold in a point of $\mathfrak{T}$ where $\mathscr{M}'$ changes.

If we can show continuity and differentiability when $\mathscr{M}'$ is increased by including one channel coefficient h_0, then larger variations of $\mathscr{M}'$ can be treated as multiple changes by one channel coefficient, and continuity still holds.

Let $\{x_k(h)\}_{h\in q\mathbb{Z}_+}$ be a point of $\mathfrak{T}$ where the transmitter increases the number of frames over which it transmits as above, and denote by $\mathfrak{T}_1$ the part of the trajectory $\mathfrak{T}$ that is between $\{x_1(h)\}$ and $\{x_k(h)\}$, and $\mathfrak{T}_2 = \mathfrak{T} \setminus \mathfrak{T}_1$.

Since $P(h_0) = 0$ (i.e. $\lambda = \frac{x(h_0)}{h_0}$), we have $\lambda(\mathscr{M}') = \lambda(\mathscr{M}' \bigcup \{h_0\})$, because they both satisfy

$$\sum_{h\in\mathscr{M}'} \left[\lambda - \frac{x(h)}{h}\right] p(h) = P_M. \tag{2.89}$$

Define the "left" and "right" limits $P_M(\{x_k(h)\}-)$ and $P_M(\{x_k(h)\}+)$ as:

$$P_M(\{x_k(h)\}-) = \lim_{\substack{\{x(h)\}\to\{x_k(h)\} \\ \{x(h)\}\in\mathfrak{T}_1}} P_M(\{x(h)\}), \tag{2.90}$$

$$P_M(\{x_k(h)\}+) = \lim_{\substack{\{x(h)\}\to\{x_k(h)\} \\ \{x(h)\}\in\mathfrak{T}_2}} P_M(\{x(h)\}). \tag{2.91}$$

We can now write:

$$P_M(\{x(h)\}+) = \lambda \sum_{h\in\mathscr{M}'\bigcup\{h_0\}} p(h) - \sum_{h\in\mathscr{M}'\bigcup\{h_0\}} \frac{x(h)}{h}p(h) =$$

$$= \lambda \sum_{h\in\mathscr{M}'} p(h) - \sum_{h\in\mathscr{M}'} \frac{x(h)}{h}p(h) + \lambda p(h_0) - \frac{x(h_0)}{h_0}p(h_0) = P_M(\{x(h)\}-) \tag{2.92}$$

where the last equality follows since $\lambda = \frac{x(h_0)}{h_0}$. This proves continuity.

Similar arguments can be used to show the continuity of the derivatives in (2.87). □

Lemma 2.18. *In the discretized case, for fixed h^0 and h^*, the function $\mathscr{P}_M(J_M)$ is concave.*

Proof. Write (2.29) explicitly for the discretized problem:

$$MJ_M + \sigma_N^2 \sum_{h=h^*}^{\infty} p(h) = \left[c \prod_{h=h^*}^{\infty} \left(\frac{1}{1+\mu h} \right)^{p(h)} \cdot \right.$$
$$\left. \cdot \prod_{h=h^0}^{h^*-q} \left(\frac{\sigma_N^2}{h} \right)^{p(h)} \right]^{\frac{1}{\sum_{h=h^0}^{h^*-q} p(h)}} \sum_{h=h^*}^{\infty} \frac{h}{1+\mu h} p(h), \tag{2.93}$$

and denote

$$g(\mu) = \prod_{h=h^*}^{\infty} \left(\frac{1}{1+\mu h} \right)^{\frac{p(h)}{\sum_{h=h^0}^{h^*-q} p(h)}} \cdot \sum_{h=h^*}^{\infty} \frac{h}{1+\mu h} p(h). \tag{2.94}$$

Note that for fixed h^0 and h^*, J_M is a linear function of g.

From (2.15), (2.16) and (2.28) a similar relation can be found for the required transmitter power P_M:

$$MP_M + \sum_{h=h^0}^{h^*-q} \frac{\sigma_N^2}{h_m} p(h) = \left[c \prod_{h=h^*}^{\infty} \left(\frac{1}{1+\mu h} \right)^{p(h)} \cdot \prod_{h=h^0}^{h^*-q} \left(\frac{\sigma_N^2}{h} \right)^{p(h)} \right]^{\frac{1}{\sum_{h=h^0}^{h^*-q} p(h)}} \cdot$$
$$\cdot \left[\sum_{h=h^0}^{h^*-q} p(h) - \sum_{h=h^*}^{\infty} \frac{1}{1+\mu h} p(h) \right]. \tag{2.95}$$

Denote

$$f(\mu) = \prod_{h=h^*}^{\infty} \left(\frac{1}{1+\mu h} \right)^{\frac{p(h)}{\sum_{h=h^0}^{h^*-q} p(h)}} \cdot \left[\sum_{h=h^0}^{\infty} p(h) - \sum_{h=h^*}^{\infty} \frac{1}{1+\mu h} p(h) \right], \tag{2.96}$$

and note that for fixed h^0 and h^*, P_M is a linear function of f.

It suffices to show that $f(g)$ is concave. For this purpose, the derivative $\frac{df}{dg} = \frac{df}{d\mu}(\frac{d\mu}{dg})^{-1}$ should be a decreasing function of g, and hence an increasing function of μ.

Computing the derivatives from (2.94) and (2.96) we obtain

$$\frac{df}{dg} = \frac{\frac{df}{d\mu}}{\frac{dg}{d\mu}} = \frac{\frac{1}{\sum_{h=h^0}^{h^*-q} p(h)} \left(\sum_{h=h^0}^{\infty} p(h) - \sum_{h=h^*}^{\infty} \frac{1}{1+\mu h} p(h) \right) - \frac{\sum_{h=h^*}^{\infty} \frac{h}{(1+\mu h)^2} p(h)}{\sum_{h=h^*}^{\infty} \frac{h}{1+\mu h} p(h)}}{\frac{1}{\sum_{h=h^0}^{h^*-q} p(h)} \sum_{h=h^*}^{\infty} \frac{h}{(1+\mu h)^2} p(h) + \frac{\sum_{h=h^*}^{\infty} \frac{h^2}{(1+\mu h)^2} p(h)}{\sum_{h=h^*}^{\infty} \frac{h}{1+\mu h} p(h)}} \tag{2.97}$$

Looking at the right hand side of (2.97) (the "large fraction"), we notice that the first term in the numerator increases with μ. For the second term in the numerator, it is clear that as μ increases, its numerator decreases faster than its denominator. This implies that the whole numerator of the "large fraction" is an increasing function of μ. Similarly, the first term in the denominator is clearly a decreasing function of μ. The only thing left is the second term of the denominator. It is straightforward to show that its derivative with respect to μ can be written as

$$\frac{d}{d\mu} \frac{\sum_{h=h^*}^{\infty} \frac{h^2}{(1+\mu h)^2} p(h)}{\sum_{h=h^*}^{\infty} \frac{h}{1+\mu h} p(h)} = \frac{1}{\left[\sum_{h=h^*}^{\infty} \frac{h}{1+\mu h} p(h) \right]^2} \cdot$$
$$\cdot \left\{ \left[\sum_{h=h^*}^{\infty} \frac{h^2}{(1+\mu h)^2} p(h) \right]^2 - \sum_{h=h^*}^{\infty} \frac{h^3}{(1+\mu h)^3} p(h) \cdot \sum_{h=h^*}^{\infty} \frac{h}{(1+\mu h)} p(h) \right\} \tag{2.98}$$

If we consider the fact that for any two real numbers a and b we have

$$(a^2+b^2)^2 - (a+b)(a^3+b^3) = -ab(a-b)^2 \tag{2.99}$$

and the summations in (2.98) are positive, it is easy to see that the second term of the denominator of the "large fraction" is decreasing with μ. Hence overall the derivative in (2.97) increases with μ. □

Lemma 2.19. *The limit of a point-wise convergent sequence of concave functions is concave.*

Proof. Denote the sequence by $(f_n(x))_{n=1}^{\infty}$ and its limit by $f(x)$. Point-wise convergence implies that for any x and $\forall \epsilon > 0$, $\exists N(x)$ such that $|f(x) - f_n(x)| < \epsilon$, $\forall n \geq N(x)$. Take two arbitrary points x and y, and pick some arbitrary $\alpha \in [0, 1]$. Denote $N = \max\{N(x), N(y), N(\alpha x + (1 - \alpha)y)\}$. Then for $n \geq N$ and any $\epsilon > 0$ we have

$$\begin{aligned} f(\alpha x + (1-\alpha)y) > f_n(\alpha x + (1-\alpha)y) - \epsilon \geq \\ \geq \alpha f_n(x) + (1-\alpha) f_n(y) - \epsilon > \alpha f(x) + (1-\alpha) f(y) - 2\epsilon, \end{aligned} \tag{2.100}$$

where the second inequality follows from the concavity of f_n. This implies that f is also concave.

□

2.8.4 On a Special Kind of Duality

Take $x, y \in L^2[\mathbb{R}]$ and define the order relation $x > y$ if and only if $x(t) > y(t)\ \forall t \in \mathbb{R}$. Consider the continuous real functions $f(x)$, $g(y)$ and $h(x, y)$ over $L^2[\mathbb{R}]$, such that f is a strictly increasing function of x, g is a strictly increasing function of y, and h is a strictly increasing function of x for fixed y and a strictly decreasing function of y for fixed x.

Define the following minimax and maximin problems:

$$\max_{y \geq 0} \left[\min_{x \geq 0} f(x) \text{ s.t. } h(x, y) \geq H \right] \text{ s.t.} g(y) \leq G, \tag{2.101}$$

$$\max_{x \geq 0} \left[\min_{y \geq 0} g(y) \text{ s.t. } h(x, y) \leq H \right] \text{ s.t.} f(x) \leq F, \tag{2.102}$$

$$\min_{y \geq 0} \left[\max_{x \geq 0} h(x, y) \text{ s.t. } f(x) \leq F \right] \text{ s.t.} g(y) \leq G. \tag{2.103}$$

The following result is important in the proof of Theorem 2.21 below.

Proposition 2.20. *For any of the three problems above, the optimal solution satisfies both constraints with equality.*

Proof. Take problem (2.101). Let (x_1, y_1) be a solution such that $f(x_1) = F$, and assume that $h(x_1, y_1) > H$. Since h is a continuous, strictly increasing function of x for a fixed y, we can find $x_n < x_1$ such that $h(x_n, y_1) = H$. But then $f(x_n) < f(x_1)$, which means that there exists a better value of x if $y = y_1$, and hence that (x_1, y_1) is not a solution.

Therefore, the first constraint has to be satisfied with equality.

Now assume that $g(y_1) < G$. Then we can find $y_0 > y_1$, such that $g(y_0) = G$. However, since $h(x_1, y_1) = H$, we have $h(x_1, y_0) < H$. In order for the first constraint to be satisfied, we need to replace x_1 by some other value x_0. We prove next that the value x_0 resulting from this modification will be such that $f(x_0) > f(x_1)$, which makes the pair (x_1, y_1) suboptimal, thus contradicting the hypothesis that it is a solution, and proving that the second constraint should hold with equality.

Assume that the value of x_0 is such that

$$f(x_0) = F_0 \leq F. \tag{2.104}$$

Then, replacing y_0 by y_1, we have that (x_0, y_1) is either a second solution of Problem 1 (if the inequality in (2.104) holds with equality), or a better choice (if the inequality in (2.104) holds with strict inequality). We can readily dismiss the latter case, since (x_1, y_1) was assumed to be an optimal solution. For the former case, h is a strictly decreasing function of y, thus $h(x_0, y_1) > R$, which contradicts the first part of this proof. The same arguments work for the problem in (2.102).

Take problem (2.103), and denote by (x_3, y_3) one of its optimal solutions. If $g(y_3) < G$, we can increase y up to a value y_m such that $g(y_m) = G$. But in turn, this yields $h(x_3, y_m) < h(x_3, y_3)$, making y_3 suboptimal. Therefore, the first constraint has to hold with equality.

Similarly, if $f(x_3) < F$, we can increase x up to a value x_m such that $f(f_m) = F$, yielding $h(x_m, y_3) > h(x_3, y_3)$, and thus resulting in a contradiction. Thus the second constraint also holds with equality. □

The main result of this section is the following theorem, which introduces a special kind of duality between the three problems in (2.101), (2.102) and (2.103).

Theorem 2.21. *(I) Choose any real values for G and H. Take problem (2.101) under these constraints and let the pair (x_1, y_1) denote one of its optimal solutions, yielding a value of the objective function $f(x_1) = F_1$. If we set the value of the corresponding constraints in problems (2.102) and (2.103) to $F = F_1$, then the values of the objective functions of problems (2.102) and (2.103) under their optimal solutions are $g(y) = G$ and $h(x, y) = H$, respectively. Moreover, (x_1, y_1) is also an optimal solution of all problems.*

(II) Choose any real values for F and H. Take problem (2.102) under these constraints and let the pair (x_2, y_2) denote one of its optimal solutions, yielding a value of the objective function $g(y_2) = G_2$. If we set the value of the corresponding constraints in problems (2.101) and (2.103) to $G = G_2$, then the values of the objective functions of problems (2.101) and (2.103) under their optimal solutions are $f(x) = F$ and $h(x, y) = H$, respectively. Moreover, (x_2, y_2) is an optimal solution of all problems.

(III) Choose any real values for F and G. Take problem (2.103) under these constraints and let the pair (x_3, y_3) denote one of its optimal solutions, yielding a value of the objective function $h(x_3, y_3) = H_3$. If we set the value of the corresponding constraints in problems (2.101) and (2.102) to $H = H_3$, then the values of the objective functions of problems (2.101) and (2.102) under their optimal solutions are $f(x) = F$ and $g(y) = G$, respectively. Moreover, (x_3, y_3) is an optimal solution of all problems.

Proof. (I) Take problem (2.101) and let (x_1, y_1) be an optimal solution, such that $f(x_1) = F$. We need to show that (x_1, y_1) is also an optimal solution of problems (2.102) and (2.103). Since x_1 and y_1 are a solution of problem (2.101), by Proposition 2.20, they satisfy the first constraint in problem (2.101) with equality, and so they also satisfy the first constraint in problem (2.102).

Since the second constraint of problem (2.102) reads $f(x) \leq F$, we note that x_1 and y_1 are in the feasible set. If we evaluate the cost function at this point, we get $g(y_1) = G$. Thus, keeping $x = x_1$, in problem (2.102), we can only obtain $g(y) \leq G$, by minimizing the cost function over y.

Now take any different value $x_0 \neq x_1$, satisfying $f(x_0) = F$. If the pair (x_0, y_1) satisfies the first constraint in problem (2.101), then it is a solution of problem (2.101), and hence the constraints should hold with equality. This implies that (x_0, y_1) also satisfies the first constraint of problem (2.102). If (x_0, y_1) does not satisfy the first constraint in problem (2.101), then it certainly satisfies the first constraint of problem (2.102). Either way, the pair (x_0, y_1) makes a feasible solution of problem (2.102) (although possibly not optimal) and, by evaluating the cost function at this point, we get $g(y_1) = G$.

Thus, for any value x_0 we pick, we should always obtain an optimal solution of problem (2.102) for which $g(y) \leq G$. But any such optimal solution has to satisfy the first constraint with equality, hence is also a solution of problem (2.101). In turn, this implies $g(y) = G$. But then the original pair (x_1, y_1) is a solution of problem (2.102), since it is feasible and yields the same cost/reward function.

Take problem (2.103), and denote by (x_3, y_3) one of its optimal solutions. By Proposition 2.20 we have $f(x_3) = F$ and $g(y_3) = G$. Then either $h(x_3, y_3) \leq H$, which implies that (x_3, y_3) is an optimal solution of problem (2.102), or $h(x_3, y_3) \geq H$ and then (x_3, y_3) is an optimal solution of problem (2.101). Either way, the inequality should hold with equality, and hence (x_3, y_3) is an optimal solution of both problem (2.101) and problem (2.102), with $h(x_3, y_3) = H$. But this also implies that (x_1, y_1) is an optimal solution of problem (2.103).

(II) A similar argument can be made if we consider an optimal solution (x_2, y_2) of problem (2.102), such that $g(y_2) = G$.

(III) Consider an optimal solution (x_3, y_3) of problem (2.103), such that $h(x_3, y_3) = H$, and suppose there exists an optimal solution (x_2, y_2) of problem (2.102) is such that $g(y_2) \neq G$. By Proposition 2.20, (x_2, y_2) satisfies $f(x_2) = F$ and $h(x_2, y_2) = H$. If $g(y_2) < G$, then (x_2, y_2) is an optimal solution of problem (2.103) which does not satisfy the constraints with equality, and thus Proposition 2.20 is contradicted. If $g(y_2) = G_2 > G$, then if we construct a modified version of problem (2.103), where the constraint $g(y) \leq G$ is replaced by $g(y) \leq G_2$, we know by the first

part of this proof that (x_2, y_2) is an optimal solution of this new problem, yielding $h(x_2, y_2) = H$. But the same objective is attained by (x_3, y_3), and moreover (x_3, y_3) satisfies the new problem's constraints since $g(y_3) = G < G_3$, and thus is an optimal solution. However, one of the constraints is satisfied with strict inequality, thus contradicting Proposition 2.20. Therefore, (x_3, y_3) has to be a solution of problem (2.102). A similar argument can be made to prove it is also a solution of problem (2.101). □

2.9 Additional Results for Average Power Constraints: Mixed Strategies - A Special Two-Player, Zero-Sum Game with Mixed Strategies

In this section, we present a general form of a special two-player, zero-sum game with mixed strategies. Particular forms of this game have been investigated by other authors over the last three decades. The first simplified version was presented by Bell and Cover [31], and a slightly more general form was later solved by Hughes and Narayan [11].

Problem Statement

Let $g(y) : \mathbb{R}_+ \to \mathbb{R}_+$ be a monotone increasing, almost everywhere (a.e.) continuous function such that $g(0) = 0$. For any point of discontinuity y_0 such that $g(y_0^-) = x_1$ and $g(y_0^+) = x_2 > x_1$, we define $g(y_0) = x_1$ (g is left-continuous) and $g^{-1}(x) = y_1$ for all $x \in [x_1, x_2]$. For any interval of non-zero measure (y_1, y_2) where g is constant, i.e. $g(y) = x_0$ for all $y \in (y_1, y_2)$, we define $g^{-1}(x_0) = y_1$ (g^{-1} is also left-continuous). On the rest of $\mathbb{R}_+$, where g is continuous and strictly increasing, g^{-1} is defined as the usual inverse function of g. Note that g^{-1} is a monotone increasing, a.e. continuous function.

Consider the two-player, zero-sum game with mixed strategies defined as follows. The allowable strategies for Player 1 are all non-negative, real-valued random variables X satisfying $\mathbf{E}[X] \leq a$. The allowable strategies for Player 2 are all non-negative, real-valued random variables Y satisfying $\mathbf{E}[Y] \leq b$. The payoff function is $Pr\{X \geq g(Y)\}$, which Player 1 seeks to maximize,

while Player 2 seeks to minimize, by properly picking the probability distributions of X and Y respectively. Throughout the sequel, these probability distributions will be represented by their corresponding cumulative distribution functions (CDFs) $F_X^0(x)$ and $F_Y^0(y)$.

Problem Solution

Theorem 2.22. *(I) If there exists a solution with $k_x, k_y \in [0,1]$ and $v \in [\max\{b/2, g^{-1}(a)/2\}, \infty)$ of the following three equations:*

$$k_x\left(1-\frac{b}{2v}\right) = 1 - k_y\left(1-\frac{a}{g(2v)}\right), \tag{2.105}$$

$$k_x = \frac{2va}{\int_0^{2v} g(y)dy}, \tag{2.106}$$

$$k_y = \frac{g(2v)b}{\int_0^{g(2v)} g^{-1}(x)dx}. \tag{2.107}$$

then this solution is unique and the unique Nash equilibrium of the two-player, zero-sum game described above is attained by the pair of strategies $(F_X^0(x), F_Y^0(y))$ satisfying:

$$F_X^0(g(y)) \sim k_x\mathbb{U}([0,2v])(y) + (1-k_x)\Delta_0(y), \tag{2.108}$$

$$F_Y^0(g^{-1}(x)) \sim k_y\mathbb{U}([0,g(2v)])(x) + (1-k_y)\Delta_0(x), \tag{2.109}$$

where $\mathbb{U}([r,t])(\cdot)$ denotes the CDF of a uniform distribution over the interval $[r,t]$, and $\Delta_0(\cdot)$ denotes the CDF of a Dirac distribution (i.e. a step function).

(II) If g is strictly increasing and continuous on $[\max\{b/2, g^{-1}(a)/2\}, \infty)$, and $\int_0^b g(y)dy < \lim_{z\to\infty}\int_{g(b)}^{g(z)} g^{-1}(x)dx - b[g(z)-g(b)]$, then the system in (2.105), (2.106) and (2.107) has a unique solution such that $k_x, k_y \in [0,1]$ and $v \in [\max\{b/2, g^{-1}(a)/2\}, \infty)$. Moreover, the parameters k_x, k_y and v are uniquely determined from the following steps:

1. *Find the unique value v_0 which satisfies:*

$$ab = [g(2v_0) - a](2v_0 - b). \tag{2.110}$$

2. *Compute* $S(v_0) = \int_0^{2v_0} g(y)dy - 2v_0 a$.

3. *If* $S(v_0) < 0$, *then* v *is the unique solution of*

$$\int_0^{2v} g(y)dy - 2va = 0, \tag{2.111}$$

$$k_x = 1 \tag{2.112}$$

and

$$k_y = \frac{bg(2v)}{2v[g(2v) - a]}. \tag{2.113}$$

4. *If* $S(v_0) = 0$ *then* $v = v_0$, $k_x = k_y = 1$.

5. *If* $S(v_0) > 0$, *then* v *is the unique solution of*

$$\int_0^{2v} g(y)dy - g(2v)(2v - b) = 0, \tag{2.114}$$

$$k_x = \frac{2va}{g(2v)(2v - b)} \tag{2.115}$$

and

$$k_y = 1. \tag{2.116}$$

Proof. Before starting the actual proof, several remarks are in order. First, $F_X^0(x)$ can be computed from $F_X^0(g(y))$ by writing $x = g(g^{-1}(x))$, and thus by evaluating $F_X^0(g(y))$ in $y = g^{-1}(x)$. A similar algorithm works for computing $F_Y^0(y)$ from $F_Y^0(g^{-1}(x))$.

Second, note that by following this algorithm, for any point of discontinuity y_0 of g such that $g(y_0^-) = x_1$ and $g(y_0^+) = x_2 > x_1$, we have:

$$F_X^0(x_1) = F_X^0(g(g^{-1}(x_1))) = F_X^0(g(y_0)) = F_X^0(g(g^{-1}(x_2))) = F_X^0(x_2), \tag{2.117}$$

i.e. Player 1 does not allow X to take values in (x_1, x_2), and

$$F_Y^0(y_0) = F_Y^0(y_0^+) = F_Y^0(g^{-1}(g(y_0^+))) = F_Y^0(g^{-1}(x_2)), \tag{2.118}$$

while by the same rational $F_Y^0(y_0^-) = F_Y^0(g^{-1}(x_1))$, meaning that Player 2 uses a probability mass point in y_0.

Third, for an interval of non-zero measure (y_1, y_2) where g is constant, i.e. $g(y) = x_0$ for all $y \in (y_1, y_2)$, we have:

$$F_Y^0(y_1) = F_Y^0(g^{-1}(g(y_1))) = F_Y^0(g^{-1}(x_0)) = F_Y^0(g^{-1}(g(y_2))) = F_Y^0(y_2), \tag{2.119}$$

i.e. Player 2 does not allow Y to take values in (y_1, y_2), and

$$F_X^0(x_0) = F_X^0(x_0^+) = F_X^0(g(g^{-1}(x_0^+))) = F_X^0(g(y_2)), \tag{2.120}$$

while by the same rational $F_X^0(x_0^-) = F_X^0(g(y_1))$, meaning that Player 1 uses a probability mass point in x_0. We now proceed with the proof of the first part of the theorem.

(I) Since this is a two-player, zero-sum game with mixed strategies, it has a unique Nash equilibrium. Let $X_0 \sim F_X^0$ and $Y_0 \sim F_Y^0$ denote the random variables with the CDFs in (2.108) and (2.109), and $X \sim F_X$ and $Y \sim F_Y$ be any arbitrary random variables.

Note that $Pr\{X \geq g(Y)\} = \int_0^\infty [1 - F_X(g(y))] dF_Y(y) = \int_0^\infty F_Y(g^{-1}(x)) dF_X(x)$. We can write

$$\begin{aligned} Pr\{X_0 \geq g(Y)\} &= \int_0^\infty [1 - F_X^0(g(y))] dF_Y(y) = \\ = 1 - k_x \int_0^\infty \mathbb{U}([0, 2v])(y) dF_Y(y) &- (1 - k_x) \int_0^\infty \Delta_0(y) dF_Y(y) \geq \\ &\geq k_x \left(1 - \frac{1}{2v} \int_0^\infty y dF_Y(y)\right) \geq k_x \left(1 - \frac{b}{2v}\right), \end{aligned} \tag{2.121}$$

and

$$Pr\{X \geq g(Y_0)\} = \int_0^\infty F_Y^0(g^{-1}(x))dF_X(x) =$$
$$= k_y \int_0^\infty \mathbb{U}([0, g(2v)])(x)dF_X(x) + (1-k_y)\int_0^\infty \Delta_0(x)dF_X(x) \leq$$
$$\leq 1 - k_y\left(1 - \frac{1}{g(2v)}\int_0^\infty xdF_X(x)\right) \leq 1 - k_y\left(1 - \frac{a}{g(2v)}\right). \tag{2.122}$$

Note that equality holds in the first inequality of (2.121) if $F_Y(2v) = 1$, and in the second inequality of (2.121) if $\mathbf{E}[Y] = b$. Similarly, equality holds in the first inequality of (2.122) if $F_X(g(2v)) = 1$, and in the second inequality of (2.122) if $\mathbf{E}[X] = a$.

Since $F_Y^0(2v) = F_Y^0(g^{-1}(g(2v))) = 1$ and $F_X^0(g(2v)) = 1$ (see (2.108), (2.109)), equalities hold in (2.121) and (2.122) when $F_X = F_X^0$ and $F_Y = F_Y^0$ if and only if

$$a = \int_0^\infty xdF_X^0(x) \tag{2.123}$$

and

$$b = \int_0^\infty ydF_Y^0(y). \tag{2.124}$$

Although the two CDFs $F_X^0(x)$ and $F_Y^0(y)$ may not be continuous as functions in $\mathscr{L}_1$, they admit derivatives in the distribution space $\mathscr{D}'$ [36], and thus we can write

$$\int_0^\infty xdF_X^0(x) = \int_0^\infty x\frac{dF_X^0(x)}{dx}dx = \int_0^\infty g(y)\frac{dF_X^0(g(y))}{dg(y)}\frac{dg(y)}{dy}dy =$$
$$= \int_0^\infty g(y)\frac{dF_X^0(g(y))}{dy}dy = (1-k_x)\int_0^\infty \delta_0(y)g(y)dy + \frac{k_x}{2v}\int_0^\infty g(y)dy, \tag{2.125}$$

which along with (2.123) results in (2.106), and similarly

$$\int_0^\infty ydF_Y^0(y) = \int_0^\infty g^{-1}(x)\frac{dF_Y^0(g^{-1}(x))}{dx}dx =$$
$$= (1-k_y)\int_0^\infty \delta_0(x)g^{-1}(x)dx + \frac{k_y}{g(2v)}\int_0^\infty g^{-1}(x)dx, \tag{2.126}$$

which together (2.124) yields (2.107). The conditions for $(F_X^0(x), F_Y^0(y))$ to achieve a saddle-point is that equality holds between the bounds in (2.121) and (2.122), which translates to (2.105), and that there always exists a solution of the system given by (2.105), (2.106) and (2.107).

(II) This part of the theorem provides a general (although not necessary) condition for such a solution to exist and states that under this condition no more than one such a solution can exist (although the uniqueness already follows as a consequence of the uniqueness of a Nash equilibrium). By substituting (2.106) and (2.107) in (2.105) we get

$$\frac{a(2v-b)}{\int_0^{2v} g(y)dy} = 1 - \frac{b(g(2v)-a)}{\int_0^{g(2v)} g^{-1}(x)dx}. \tag{2.127}$$

Denote the left hand side of (2.127) by $L(v)$ and the right hand side by $R(v)$ for simplicity. Note that for any function g that satisfies the conditions set in the problem formulation we have

$$\int_0^{2v} g(y)dy = 2vg(2v) - \int_0^{g(2v)} g^{-1}(x)dx. \tag{2.128}$$

This relation is best observed graphically in Figure 2.11.

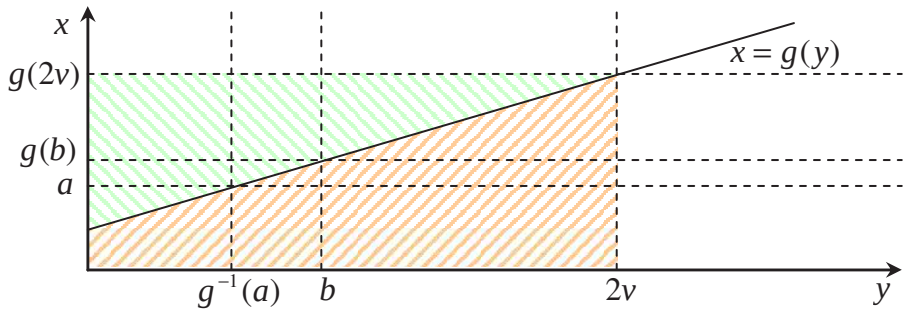

FIGURE 2.11. The relationship between the integrals of $g(y)$ and $g^{-1}(x)$.

Computing the derivatives of $L(v)$ and $R(v)$ with respect to v (these derivatives always exist for $v \geq \max\{b/2, g^{-1}(a)/2\}$) we get

$$\frac{dL(v)}{dv} = \frac{2a}{\left[\int_0^{2v} g(y)dy\right]^2} \cdot \left[\int_0^{2v} g(y)dy - g(2v)(2v-b)\right], \tag{2.129}$$

and

$$\begin{aligned}\frac{dR(v)}{dv} &= \frac{2g'(v)b}{\left[\int_0^{g(2v)} g^{-1}(x)dx\right]^2} \cdot \left[2v(g(2v)-a) - \int_0^{g(2v)} g^{-1}(x)dx\right] = \\ &= \frac{2g'(v)b}{\left[\int_0^{g(2v)} g^{-1}(x)dx\right]^2} \left[\int_0^{2v} g(y)dy - 2va\right],\end{aligned} \tag{2.130}$$

where $g'(v) > 0$ denotes the first derivative $dg(y)/dy$, evaluated in $y = v$, and the second equality in (2.130) follows from (2.128).

Note that $L(v)$ and $R(v)$ are both probabilities, hence belong to $[0, 1]$. Therefore, any possible solution of the system in (2.105), (2.106) and (2.107) should satisfy $2v \geq b$ and $g(2v) \geq a$, or equivalently:

$$v \geq \max\{b/2, g^{-1}(a)/2\}. \tag{2.131}$$

Therefore, in the sequel of this proof we shall implicitly assume that (2.131) holds true.

Denote $S_L(v) = \int_0^{2v} g(y)dy - g(2v)(2v - b)$ and $S_R(v) = \int_0^{2v} g(y)dy - 2va$. Since

$$\frac{d}{dv}\int_0^{2v} g(y)dy = 2g(2v), \tag{2.132}$$

we observe that

$$\frac{d}{dv}S_L(v) = -2g'(v)(2v - b) < 0 \tag{2.133}$$

and

$$\frac{d}{dv}S_R(v) = 2(g(2v) - a) > 0, \tag{2.134}$$

which imply that $S_L(v)$ is a strictly decreasing function of v, while $S_R(v)$ is a strictly increasing function of v, for the domain of interest $v \in [\max\{b/2, g^{-1}(a)/2\}, \infty)$.

Note that $\frac{d}{dv}S_R(v)$ is strictly positive even in the limit as $v \to \infty$, and thus $\lim_{v\to\infty} S_R(v) = \infty$. By writing $S_L(v) = \int_0^b g(y)dy - \int_{g(b)}^{g(2v)} g^{-1}(x)dx$, we also have $\lim_{v\to\infty} S_L(v) = -\infty$.

A first possible solution:

An extremum of $L(v)$ is obtained by setting $\frac{dL(v)}{dv} = 0$, or equivalently

$$\int_0^{2v_l} g(y)dy = g(2v_l)(2v_l - b). \tag{2.135}$$

In our previously introduced notation, this writes $S_L(v_l) = 0$. But since $S_L(v)$ is strictly decreasing on the domain of interest, the extremum is unique and is a maximum.

The values of $L(v)$ and $R(v)$ at this point are given by

$$L(v_l) = R(v_l) = \frac{a}{g(2v_l)}. \tag{2.136}$$

Moreover, substituting (2.135) and (2.128) back in (2.106) and (2.107) we get

$$k_{x,l} = \frac{2v_l a}{g(2v_l)(2v_l - b)} \tag{2.137}$$

and

$$k_{y,l} = 1. \tag{2.138}$$

Therefore $(v_l, k_{x,l}, k_{y,l})$ are a solution of the system given by (2.105), (2.106) and (2.107) if and only if $k_{x,l} \in [0, 1]$. From (2.131) it is implied that $2v_l \geq b$, and hence that $k_{x,l} \geq 0$. The condition $k_{x,l} \leq 1$ yields

$$2v_l a \leq g(2v_l)(2v_l - b). \tag{2.139}$$

A second possible solution:

An extremum of $R(v)$ is obtained by setting $\frac{dR(v)}{dv} = 0$, or equivalently

$$\int_0^{2v_r} g(y)dy = 2v_r a. \tag{2.140}$$

In our previously introduced notation, this writes $S_R(v_r) = 0$. When this extremum of $R(v)$ exists, it is also unique and is a minimum, since $S_R(v)$ is strictly increasing on the domain of interest.

The values of $L(v)$ and $R(v)$ at this point are given by

$$L(v_r) = R(v_r) = 1 - \frac{b}{2v_r}. \tag{2.141}$$

Moreover, substituting (2.140) back in (2.106) and (2.107) we get

$$k_{x,r} = 1 \tag{2.142}$$

and

$$k_{y,r} = \frac{bg(2v_r)}{2v_r(g(2v_r) - a)}. \tag{2.143}$$

Therefore $(v_r, k_{x,r}, k_{y,r})$ are a solution of the system given by (2.105), (2.106) and (2.107) if and only if $k_{y,r} \in [0, 1]$. From (2.131) it is implied that $g(2v_r) \geq a$, and hence that $k_{y,r} \geq 0$. The condition $k_{y,r} \leq 1$ yields the same inequality as before:

$$2v_r a \leq g(2v_r)(2v_r - b). \tag{2.144}$$

Recall that $L(v)$ has a unique maximum, while $R(v)$ has a unique minimum. The immediate implication of this is that the equation $L(v) = R(v)$ can have a maximum of two solutions. These are the possible solutions discussed above.

To summarize, we have two sets of relations:

$$\begin{aligned} \int_0^{2v_l} g(y)dy &= g(2v_l)(2v_l - b), \\ 2v_l a &\leq g(2v_l)(2v_l - b) \end{aligned} \tag{2.145}$$

and

$$\begin{aligned} \int_0^{2v_r} g(y)dy &= 2v_r a, \\ 2v_r a &\leq g(2v_r)(2v_r - b) \end{aligned} \tag{2.146}$$

that could each yield a solution of the system in (2.105), (2.106) and (2.107).

In the remainder of this proof, we show that at least one of the sets (2.145) and (2.146) has a solution and the sets (2.145) and (2.146) cannot both have different solutions.

Let v_0 denote the value of v in $[\max\{b/2, g^{-1}(a)/2\}, \infty)$ for which

$$2v_0 a = g(2v_0)(2v_0 - b), \tag{2.147}$$

as in Figure 2.12.

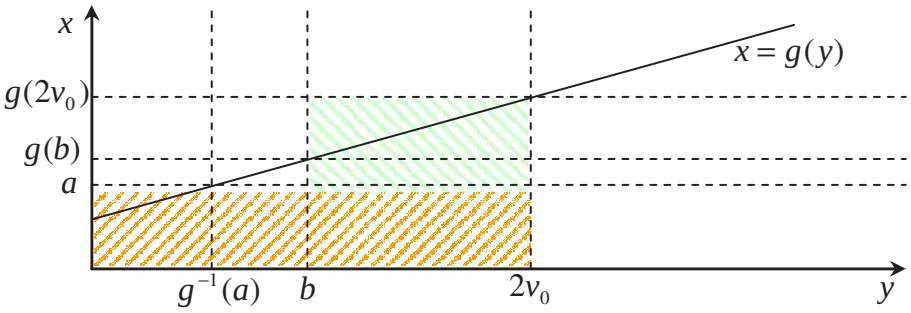

FIGURE 2.12. Finding v_0.

Such a value exists and is unique since (2.147) is equivalent to $ab = (g(2v_0)-a)(2v_0-b)$, where the term on the right hand side is a strictly increasing function of v_0 on $[\max\{b/2, g^{-1}(a)/2\}, \infty)$, with a minimum in $v_0 = \max\{b/2, g^{-1}(a)/2\}$ which is 0 and $\lim_{v\to\infty}(g(2v) - a)(2v - b) = \infty$. Note that this also implies that $2va \leq g(2v)(2v - b)$ can only be satisfied if $v > v_0$.

Denote $S = S_L(v_0) = S_R(v_0)$ the common value of S_L and S_R in v_0. If $S = 0$, then $v_l = v_r = v_0$. If $S < 0$ or $S > 0$, since $S_L(v)$ is decreasing with v and $S_R(v)$ is increasing with v for the domain of interest, it is not possible to obtain solutions larger than v_0 to both equations $S_L(v) = 0$ and $S_R(v) = 0$.

However, a solution always exists. If $S < 0$, the solution is guaranteed by the continuity of $S_R(v)$ on the domain of interest, and by the fact that $\lim_{v\to\infty} S_R(v) = \infty$. If $S > 0$, the solution is guaranteed by the continuity of $S_L(v)$ on the domain of interest, and by the fact that $\lim_{v\to\infty} S_L(v) < 0$, which follows from the condition $\int_0^b g(y)dy < \lim_{z\to\infty} \int_{g(b)}^{g(z)} g^{-1}(x)dx - b[g(z) - g(b)]$. Note that this condition is only necessary if $S > 0$ and is illustrated in Figure 2.13.

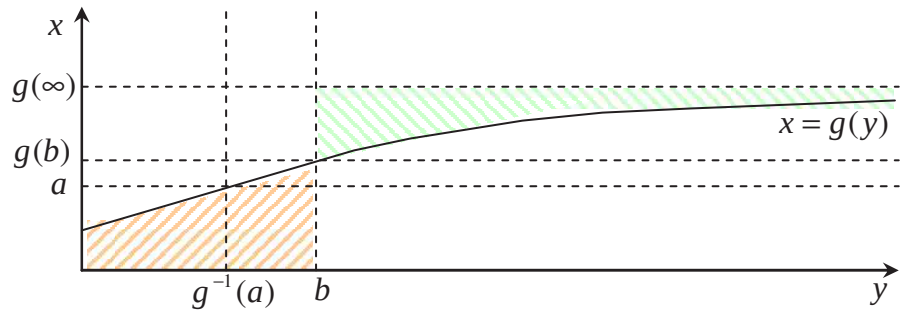

FIGURE 2.13. The necessary condition for the existence of a solution when $S > 0$.

A similar condition can be written for the case when $S < 0$, that is $\lim_{v\to\infty} S_R(v) > 0$ if and only if $\int_0^a g^{-1}(x)dx < \int_{g^{-1}(a)}^{\infty} g(y)dy$. However, since g is a function and is defined over $\mathbb{R}_+$, this latter condition can only be violated if g is constant on $[g^{-1}(a), \infty)$. But this is impossible under the former condition.

We have thus shown that under the condition that g is strictly increasing and continuous on $[\max\{b/2, g^{-1}(a)/2\}, \infty)$, and $\int_0^b g(y)dy < \lim_{z\to\infty} \int_{g(b)}^{g(z)} g^{-1}(x)dx - b[g(z) - g(b)]$, the system given by (2.105), (2.106) and (2.107) always has a solution, and that this solution is unique. □

Several additional remarks

Bell and Cover [31] found the solution of our game for the particular case when $a = b = 1$ and $g(y) = y$. In the context of Gaussian arbitrarily varying channels, Hughes and Narayan [11] extended the previous result to the case where a and b are any positive constants, and $g(y) = y + c$, with $c \geq 0$. In the remainder of this section we show that our results can be easily particularized to obtain the same results as in [11].

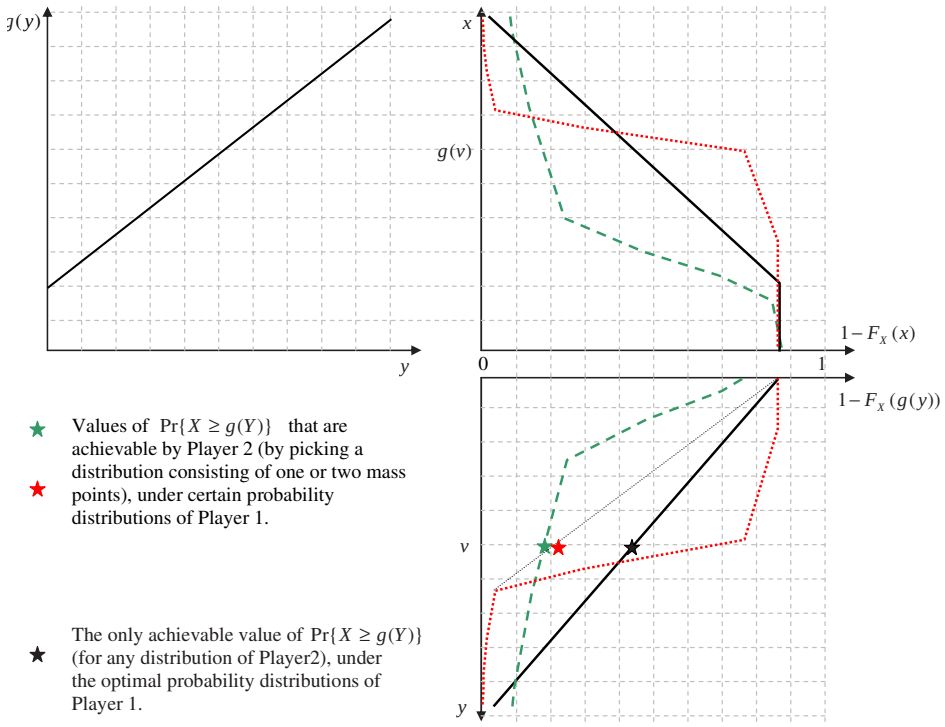

FIGURE 2.14. Intuitive explanation for the optimality of the strategy in (2.108).

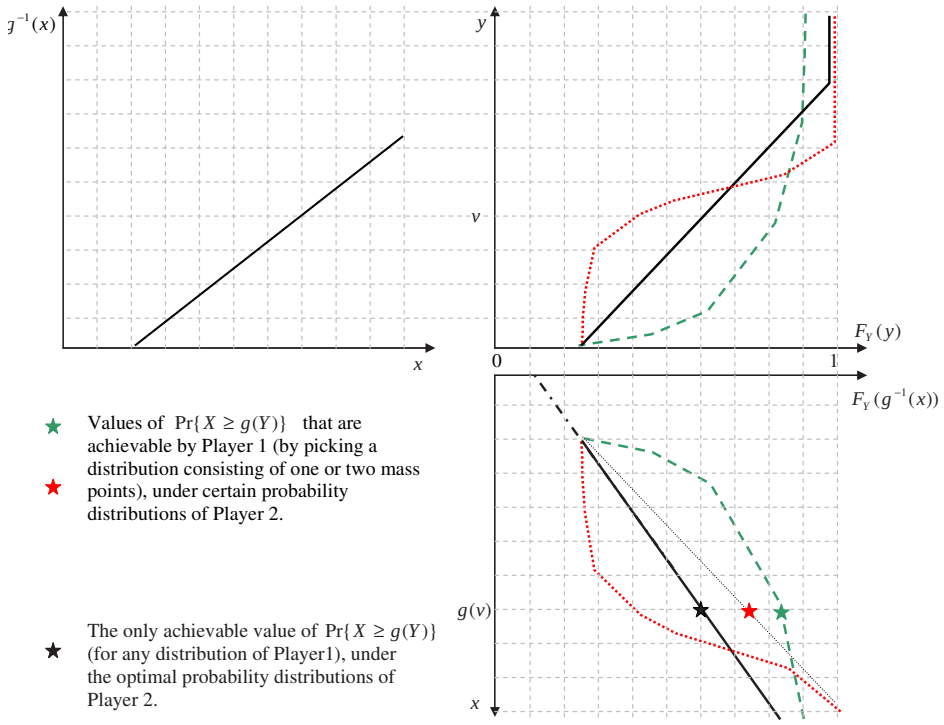

FIGURE 2.15. Intuitive explanation for the optimality of the strategy in (2.109).

If we force $g(0) = g(0^-) = 0$, the function $g(y) = y + c,\ \forall y > 0$ is unbounded, linear, strictly increasing, and has only one discontinuity in $y = 0$. Hence, it satisfies all the conditions set in the problem formulation, as well as those of part (II) of our Theorem 2.22.

Substituting $g(y) = y + c$ in (2.145), we get (Case 1):

$$2v_l^2 - 2v_l b - bc = 0 \tag{2.148}$$

and

$$a \leq v_l + c, \tag{2.149}$$

resulting in

$$v_l = \frac{b}{2}\left[1 + \sqrt{1 + \frac{2c}{b}}\right] \tag{2.150}$$

under the condition that

$$a \leq c + \frac{b}{2}\left[1 + \sqrt{1 + \frac{2c}{b}}\right]. \tag{2.151}$$

The cost function for this case results from (2.136) as

$$Pr\{X \geq g(Y)\} = \frac{a}{c + b\left[1 + \sqrt{1 + \frac{2c}{b}}\right]} = \frac{a}{c}\left[1 + \frac{b}{c}\left(1 - \sqrt{1 + \frac{2c}{b}}\right)\right], \tag{2.152}$$

and is also consistent with [11]. Note that although $k_y = 1$ for this case, this does not mean that Player 2 is always on. Recall that a discontinuity of g is translated into a mass point for the probability distribution of Y. In this case, the discontinuity in $y = 0$ means that $Y = 0$ with probability $\frac{c}{g(2v_l)} = 1 - \frac{b}{v_l}$, which is the same as in [11].

Similarly, substituting $g(y) = y + c$ in (2.146), we get (Case 2):

$$v_l = \frac{b}{2}\left[1 + \sqrt{1 + \frac{2c}{b}}\right] \tag{2.153}$$

under the condition that

$$a \geq c + \frac{b}{2}\left[1 + \sqrt{1 + \frac{2c}{b}}\right]. \tag{2.154}$$

Note that the two conditions (2.151) and (2.154) are mutually exclusive. The cost function for this case is

$$Pr\{X \geq g(Y)\} = 1 - \frac{b}{2(a - c)}, \tag{2.155}$$

and is consistent with [11].

In Figure 2.14 we offer an intuitive explanation of why $F_X^0(g(y))$ should be uniform over $[0, 2v]$, from a maximin point of view. The function $g(y)$ is taken to be linear, with a discontinuity in 0, similar to [11]. Assuming that Player 1 plays first (maximin), we note that if $F_X^0(g(y))$ is not uniform, the second player can pick a strategy that decreases the value of the objective $Pr\{X \geq g(Y)\}$. Therefore, in order to provide the second player with an indifferent choice space (the strategy of Player 2 can be any probability distribution over $[0, 2v]$), Player 1 should pick $F_X^0(x)$ such that $F_X^0(g(y))$ is uniform over $[0, 2v]$.

Similarly, in Figure 2.15 we offer an intuitive explanation of why $F_Y^0(g^{-1}(x))$ should be uniform over $[0, g(2v)]$, from a minimax point of view. Assuming that Player 2 plays first (minimax), note

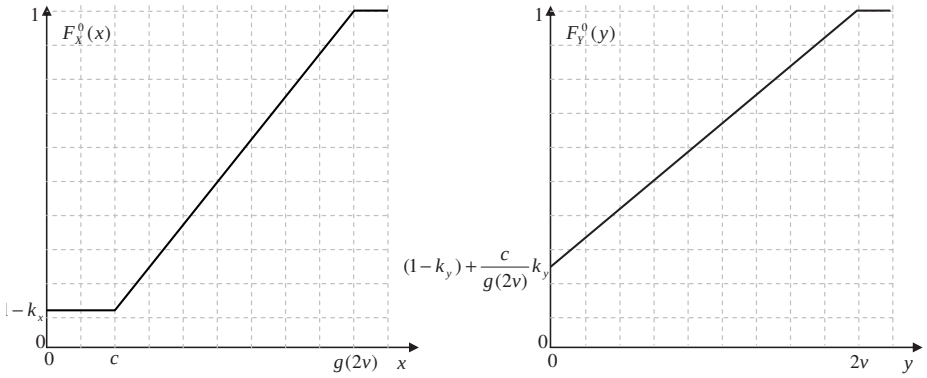

FIGURE 2.16. The resulting strategies $F_X^0(x)$ and $F_Y^0(y)$ for a linear $g(y)$ with a discontinuity in 0.

that if $F_Y^0(g^{-1}(x))$ is not uniform, the first player can pick a strategy that increases the value of the objective $Pr\{X \geq g(Y)\}$.

The optimal distributions resulting from Figures 2.14 and 2.15 are shown in Figure 2.16. They are consistent with our theoretical results (and the results of [11]) for $g(y) = y + c$.

Chapter 3

Jamming in Fixed-Rate Wireless Systems with Power Constraints - Part II: Parallel Slow Fading Channels

3.1 Introduction

The concept of jamming plays an extremely important role in ensuring the quality and security of wireless communications, especially at this moment when wireless networks are quickly becoming ubiquitous. Although the recent literature covers a wide variety of jamming problems [3–5, 9, 11, 37, 38], the investigation of optimal jamming and anti-jamming strategies for the parallel slow-fading channel is missing.

The parallel slow-fading channel is a widely used model for OFDM transmission [28]. Since the usual definition of capacity does not provide a positive performance indicator for this model, a more adequate performance measure is the probability of outage [28], defined as the probability that the instantaneous mutual information characterizing the parallel channel, under a given channel realization, is below a fixed transmission rate R. Under the optimal diversity-multiplexing tradeoff, the parallel slow-fading channel with M subchannels is known [28] to yield an M-fold diversity gain over the scalar single antenna channel. However the diversity-multiplexing tradeoff only gives an approximative analytical evaluation of the probability of outage for a given rate R and a signal-to-noise ratio (SNR), and this approximation is usually accurate only in the high SNR region. Thus, for evaluating a system which functions at a moderate SNR, the exact probability-of-outage vs. transmission-rate curve is often computed numerically. Moreover, the high SNR assumption is clearly not adequate for studying a practical uncorrelated jamming situation, where the jammer's power should be considered at least comparable to the legitimate transmitter's.

Therefore, we aim at deriving the exact probability of outage achievable in the presence of a jammer, over our parallel slow fading channel, for a fixed transmission rate R. Our channel model is depicted in Figure 3.1. The span of a codeword is denoted by "frame". To model our parallel

slow fading channel, each frame is divided into M "blocks" (corresponding to the M subchannels), each of which consists of N channel uses, like in Figure 3.2.

The channel fading is slow, such that the corresponding channel coefficients remain constant over each block and vary independently across different blocks. The channel coefficients are complex numbers, and their squared absolute values are denoted as h_m. The vector $\mathbf{h} = [h_0, h_1, \ldots, h_{M-1}]$ of channel coefficients over a whole frame is assumed to be perfectly known to the receiver, and can be made available by feedback (if the receiver wishes) to the transmitter (Tx), and jammer (Jx) before the transmission begins. It was shown in [32] that the feedback of channel state information (CSI) (i.e. the M coefficients of a frame) brings moderate benefits for the parallel slow-fading channel without jamming. Thus, by employing optimal power control strategies, the transmitter can lower the probability of outage for fixed transmission rate and SNR. In this chapter, we study both the scenarios when the CSI is fed back by the legitimate receiver – and hence all M channel coefficients characterizing a frame are available to both transmitter and jammer in a non-causal fashion (it is only natural to assume that if the transmitter has full CSI, the jammer can get the same information by eavesdropping) – and the scenario when no feedback takes place and thus the CSI is only available to the receiver.

In addition to fading, the transmission is affected by additive white complex Gaussian noise (AWGN), and by a jammer. The jammer has no knowledge about the transmitter's output, or even

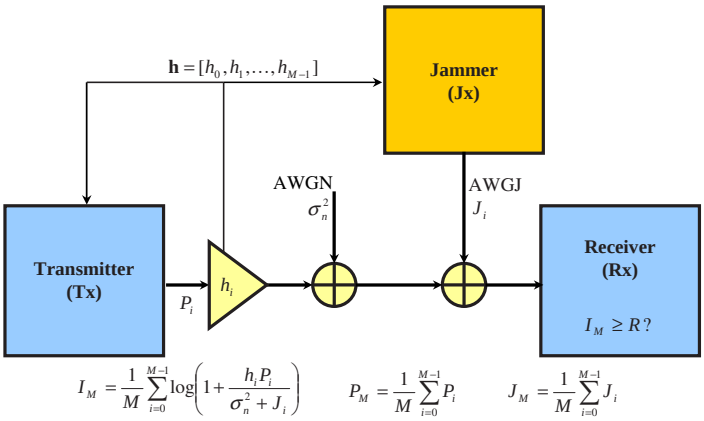

FIGURE 3.1. Channel model

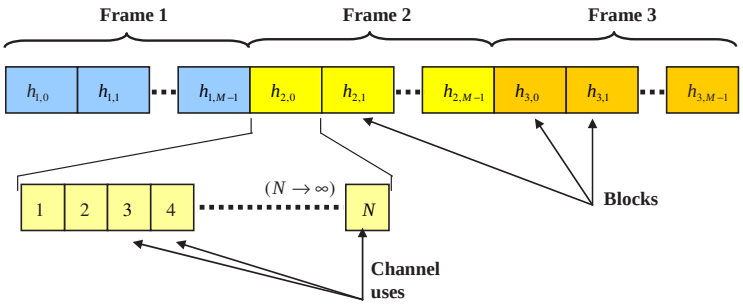

FIGURE 3.2. Frames, blocks and channel uses

the codebook that the transmitter is using, and hence it deploys its most harmful strategy: it transmits white complex Gaussian noise [30] (AWGJ in Figure 3.1).

The transmitter (Tx) uses a complex Gaussian codebook. Over a given frame, it allocates power P_m to block m, $0 \leq m \leq M-1$, while the jammer (Jx) invests power J_m in jamming the same block with noise. As assumed in [32], the number of channel uses per block is large $N \to \infty$ in order to average out the impact of the Gaussian noise. Under these assumptions, the instantaneous mutual information characterizing a subchannel m is given by $I(h_m, P_m, J_m) = \log(1 + \frac{h_m P_m}{\sigma_N^2 + J_m})$, where σ_N^2 is the variance of the ambient AWGN. The following denotations will be repeatedly used in the sequel:

- Power allocated by the transmitter over a frame:
  $P_M = \frac{1}{M} \sum_{m=0}^{M-1} P_m$;
- Power allocated by the jammer over a frame:
  $J_M = \frac{1}{M} \sum_{m=0}^{M-1} J_m$;
- Instantaneous mutual information between the transmitter and the receiver over a frame:
  $I_M = \frac{1}{M} \sum_{m=0}^{M-1} I(h_m, P_m, J_m)$.

Note that P_M is a function of the channel realization $\mathbf{h}$, so we often write $P_M(\mathbf{h})$ when this relation needs to be explicitly emphasized. $P_M(\mathbf{h})$ can also be interpreted as the function giving the power distribution across different frames. We also use $P_M(h)$ and $J_M(h)$ to denote inter-frame

power allocation for the case $M = 1$, since in this case a frame only contains one block. Like in Chapter 2, throughout this chapter we shall also use the notation $c = \exp(MR)$ for simplicity.

As depicted in Figure 3.1, our channel model is similar to that of [9]. The difference, however, is that we investigate the jamming problem in slow-fading channels and hence the probability of outage, defined as the probability that the instantaneous mutual information I_M of the channel is lower than the fixed transmission rate R [32] is considered as an objective function $P_{out} = Pr(I_M < R)$ (while [9] assumes fast fading and uses the ergodic capacity as objective). Our problem is still formulated as a two-player, zero-sum game. The transmitter wants to achieve reliable communication and hence minimize the outage probability, while the jammer wants to induce outage and maximize the outage probability. Strategies consist of varying transmission powers based on the CSI (i.e. the perfect knowledge of $\mathbf{h}$) if available, or solely on the channel's statistics if CSI is not available. The properties of our different objective function make our new jamming and anti-jamming problem much more challenging to solve.

It is easy to find similarities to the fixed rate system with fast fading which was studied in Chapter 2. In fact, the fast fading scenario of Chapter 2 can be obtained as a particular case of the current setup, by allowing a large number of blocks per frame $M \to \infty$ (corresponding to an infinite number of subchannels). In doing so, the different frames are no longer characterized by their respective channel realizations, but instead they become long enough to display the statistical properties of the channel coefficient and thus become equivalent. This is why our present parallel slow fading scenario is more involved than the fast fading model of Chapter 2, especially when it comes to resolving the optimal power allocation between different frames. Sometimes this additional complexity leads to an additional level of power control, as we shall see in Section 3.4.

Our contributions are summarized below:

- We first investigate the case where the receiver feeds back the channel state information (CSI) which becomes available to both transmitter and jammer. For the short-term power

constraints case we show the existence of and find a Nash equilibrium of pure strategies. Note that for a two-person, zero-sum game, all Nash equilibria have the same value [33]. Since an equilibrium of pure strategies is also an equilibrium of mixed strategies, our Nash equilibrium of pure strategies provides the complete solution of the game.

- For the case with long-term power constraints we find the maximin and minimax solutions of pure strategies, and show they do not coincide (hence the non-existence of a Nash equilibrium of pure strategies). Traditional methods of optimization, such as the KKT conditions, cannot be applied to solve for these solutions completely. Therefore we provide a new, more intuitive approach based on the special duality property discussed in Section 2.8.4 of Chapter 2. As argued in Chapter 2, Nash equilibria of mixed strategies may not always be the best solutions to jamming problems. A smart jammer could eavesdrop the channel and detect both the legitimate transmitter's presence and its power level. Therefore, we believe that the maximin and minimax problem formulations with pure strategies are of great importance in understanding and resolving the practical jamming situations (in the worst case, they provide upper and lower bounds on the system's performance).

- The optimal pure strategies of allocating power between frames, for the maximin and minimax formulations, are found as the solutions of two simple numerical algorithms. These algorithms function according to two different techniques which we explain in the sequel and we dub as "the vase water filling problems".

- Mixed strategies are discussed next. We show that for completely characterizing this scenario we need three different levels of power control. We then particularize and obtain numerical results for the special simple case with only one block per frame ($M = 1$).

- Finally, we compare our results to the case when the channel state information is only available to the receiver. We derive a Nash equilibrium for $M = 1$, and show that unlike in the

fast fading scenario (where CSI feedback brings negligible improvements), under our current parallel slow fading channel model, perfect knowledge about the CSI at all parties can substantially improve performance.

The chapter is organized as follows. Section 3.2 deals with the short term power constrained problem when full CSI is available to all parties. Section 3.3 studies the scenario with long term power constraints and pure strategies under the same assumption of available CSI. Mixed strategies are discussed in Section 3.4. For comparison purposes, Section 3.5 presents results for the case with no CSI feedback. Finally, conclusions are drawn in Section 3.6.

3.2 CSI Available to All Parties. Jamming Game with Short-Term Power Constraints

The game with short-term power constraints is the less complex of the two games we discuss in the sequel. In this game, the transmitter's goal is to:

$$\begin{cases} \text{Minimize} & \Pr(I_M(\mathbf{h}, P(h), J(h)) < R) \\ \text{Subject to} & P_M(\mathbf{h}) \leq \mathcal{P}, \text{with prob. 1} \end{cases} \tag{3.1}$$

while the jammer's goal is to:

$$\begin{cases} \text{Maximize} & \Pr(I_M(\mathbf{h}, P(h), J(h)) < R) \\ \text{Subject to} & J_M(\mathbf{h}) \leq \mathcal{J}, \text{with prob. 1.} \end{cases} \tag{3.2}$$

We shall prove that this game is closely related to a different two player, zero-sum game, which has the mutual information between Tx and Rx as a cost/reward function:

$$\text{Tx} \begin{cases} \text{Maximize} & I_M(\mathbf{h}, P(h), J(h)) \\ \text{Subject to} & P_M(\mathbf{h}) \leq \mathcal{P}, \end{cases} \tag{3.3}$$

$$\text{Jx} \begin{cases} \text{Minimize} & I_M(\mathbf{h}, P(h), J(h)) \\ \text{Subject to} & J_M(\mathbf{h}) \leq \mathcal{J}. \end{cases} \tag{3.4}$$

This latter game is characterized by the following proposition:

Proposition 3.1. *The game of (3.3) and (3.4) has a Nash equilibrium point given by the following strategies:*

$$P^*(h_m) = \begin{cases} (\frac{1}{\eta} - \frac{\sigma_N^2}{h_m})^+ & \textit{if} \quad h_m < \frac{\sigma_N^2 \eta}{1-\sigma_N^2 \nu} \\ \frac{h_m}{\eta(h_m + \frac{\eta}{\nu})} & \textit{if} \quad h_m \geq \frac{\sigma_N^2 \eta}{1-\sigma_N^2 \nu} \end{cases} \tag{3.5}$$

$$J^*(h_m) = \begin{cases} 0 & \textit{if} \quad h_m < \frac{\sigma_N^2 \eta}{1-\sigma_N^2 \nu} \\ \frac{h_m}{\nu(h_m + \frac{\eta}{\nu})} - \sigma_N^2 & \textit{if} \quad h_m \geq \frac{\sigma_N^2 \eta}{1-\sigma_N^2 \nu} \end{cases} \tag{3.6}$$

where η and ν are constants that can be determined from the power constraints.

Proof. The proof is a straightforward adaptation of Section IV.B in [9], and is outlined in Section 3.7. □

The connection between the two games above is made clear in the following theorem, the proof of which follows in the footsteps of [32] and is given in Section 3.7.

Theorem 3.2. *Let $P^*(h)$ and $J^*(h)$ denote the Nash equilibrium solutions of the game described by (3.3) and (3.4). Then the original game of (3.1), (3.2) has a Nash equilibrium point, which is given by the following pair of strategies:*

$$\widehat{P}(h_m) = \begin{cases} P^*(h_m) & \textit{if} \quad \mathbf{h} \in \mathcal{U}(R, \mathcal{P}, \mathcal{J}) \\ P_a(h_m) & \textit{if} \quad \mathbf{h} \notin \mathcal{U}(R, \mathcal{P}, \mathcal{J}) \end{cases} \tag{3.7}$$

$$\widehat{J}(h_m) = \begin{cases} J_a(h_m) & \textit{if} \quad \mathbf{h} \in \mathcal{U}(R, \mathcal{P}, \mathcal{J}) \\ J^*(h_m) & \textit{if} \quad \mathbf{h} \notin \mathcal{U}(R, \mathcal{P}, \mathcal{J}) \end{cases} \tag{3.8}$$

where $\mathcal{U}(R, \mathcal{P}, \mathcal{J}) = \{\mathbf{h} \in \mathbb{R}_+^M : I_M(\mathbf{h}, P^*(h), J^*(h)) \geq R\}$, and where $P_a(h)$ and $J_a(h)$ are some arbitrary power allocations satisfying the power constraints respectively.

3.3 CSI Available to All Parties. Jamming Game with Long-Term Power Constraints: Pure Strategies

The long-term power constrained jamming game can be formulated as:

$$\text{Tx} \begin{cases} \text{Minimize} & \Pr(I_M(\mathbf{h}, \{P_m\}, \{J_m\}) < R) \\ \text{Subject to} & E[P_M(\mathbf{h})] \leq \mathcal{P} \end{cases} \tag{3.9}$$

$$\text{Jx} \begin{cases} \text{Maximize} & \Pr(I_M(\mathbf{h}, \{P_m\}, \{J_m\}) < R) \\ \text{Subject to} & E[J_M(\mathbf{h})] \leq \mathcal{J} \end{cases} \tag{3.10}$$

where the expectation is taken with respect to the vector of channel coefficients $\mathbf{h} = (h_0, h_1, \ldots, h_{M-1}) \in \mathbb{R}_+^M$, and $\mathcal{P}$ and $\mathcal{J}$ are the upper-bounds on average transmission power of the source and jammer, respectively.

Contrary to the previous short-term power constraints scenario, if long-term power constraints are used it is possible to have $P_M(\mathbf{h}) > \mathcal{P}$ for a particular channel realization $\mathbf{h}$, as long as the average of $P_M(\mathbf{h})$ over all possible channel realizations is less than $\mathcal{P}$.

Let $\mathfrak{m}$ denote the probability measure introduced by the probability density function (p.d.f.) of $\mathbf{h}$, i.e., for a set $\mathscr{A} \subseteq \mathbb{R}_+^M$, we have $\mathfrak{m}(\mathscr{A}) = \int_{\mathscr{A}} f(\mathbf{h}) d\mathbf{h}$. Integrating with respect to this measure is equivalent to computing an average with respect to the p.d.f. given by $f(\mathbf{h})$, i.e., $d\mathfrak{m}(\mathbf{h}) = f(\mathbf{h})d\mathbf{h}$.

Both transmitter and jammer have to plan in terms of power allocation, considering both the instantaneous realization and the probability distribution of the channel coefficient vector, as well as their opponent's strategy.

If the number of blocks M in each frame is larger than 1, the game between transmitter and jammer has two levels. The first (coarser) level is about power allocation between frames, and has the probability of outage as a cost/reward function. This is the only level that shows up in the case of $M = 1$. The second (finer) level is that of power allocation between the blocks within a frame.

An important comment similar to that in Chapter 2 needs to be made. We should point out that decomposing the problem into several (two or three) levels of power control, each of which

is solved separately, does not restrict the generality of our solution. In proving our main results we take a contradictory approach. That is, instead of directly deriving each optimal strategy, we assume an optimal solution has already been reached and show it has to satisfy a set of properties. We do this by first assuming that the properties are not satisfied, and then showing that under this assumption at least one of the players can improve its strategy (and hence the original solution cannot be optimal). The properties are selected such that they are not only necessary, but also sufficient for the completely characterizing the optimal solution (i.e. there exists a unique pair of strategies that satisfy these properties).

3.3.1 Power Allocation between the Blocks in a Frame

In this subsection we only deal with the second (intra-frame) level of power allocation for the maximin and minimax problems. The first (inter-frame) level will be investigated in detail in the following two subsections.

The probability of outage is determined by the $\mathfrak{m}$-measure of the set over which the transmitter is not present or the jammer is successful in inducing outage. This set is established in the first level of power control. Note that the first level power allocation strategies cannot be derived before the second level strategies are available.

In the maximin case (when the jammer plays first), assume that the jammer has already allocated some power J_M to a given frame. Naturally, the transmitter knows J_M (the maximin problem assumes that the transmitter is fully aware of the jammer's strategy). Depending on the channel realization, the value of J_M, and its own power constraints, the transmitter decides whether it wants to achieve reliable communication over that frame. If it decides to transmit, it needs to spend as little power as possible (the transmitter will be able to use the saved power for achieving reliable communication over another set of positive $\mathfrak{m}$-measure, and thus to decrease the probability of outage). Therefore, the transmitter's objective is to minimize the power P_M spent for achieving reliable communication. The transmitter will adopt this strategy whether the jammer is present

over the frame, or not. The jammer's objective is then to allocate J_M between the blocks such that the required P_M is maximized.

In the minimax scenario (when transmitter plays first) the jammer's objective is to minimize the power J_M used for jamming the transmission over a given frame. The jammer will only transmit if the transmitter is present with some P_M. The transmitter's objective is to distribute P_M between blocks such that the power required for jamming is maximized.

The two problems can be formulated as:

Problem 1 (for the maximin solution - jammer plays first)

$$\max_{\{J_m \geq 0\}} \Big[\min_{\{P_m \geq 0\}} P_M = \frac{1}{M} \sum_{m=0}^{M-1} P_m, \text{ s.t. } I_M(\{P_m\}, \{J_m\}) \geq R \Big] \text{ s.t.} \frac{1}{M} \sum_{m=0}^{M-1} J_m \leq J_M; \quad (3.11)$$

Problem 2 (for the minimax solution - transmitter plays first)

$$\max_{\{P_m \geq 0\}} \Big[\min_{\{J_m \geq 0\}} J_M = \frac{1}{M} \sum_{m=0}^{M-1} J_m, \text{ s.t. } I_M(\{P_m\}, \{J_m\}) \leq R \Big] \text{ s.t.} \frac{1}{M} \sum_{m=0}^{M-1} P_m \leq P_M. \quad (3.12)$$

These problems can be solved by methods very similar to those presented in Chapter 2. For the brevity of this presentation, we shall only point out the main results, and defer all proofs to the Section 3.8. The following propositions fully characterize the solutions.

Proposition 3.3. *The optimal solution of either of the two problems above satisfies both constraints with equality.*

Proposition 3.4. *(I) Take the game given by (3.3) and (3.4) and set the constraints to* $P_M(\mathbf{h}) \leq P_{M,1}$ *and* $J_M(\mathbf{h}) \leq J_{M,1}$. *Denote the resulting value of the objective by* $I_M(\mathbf{h}, P(h), J(h)) = R_1$. *Then solving* Problem 1 *above with the constraints* $\frac{1}{M} \sum_{m=0}^{M-1} J_m \leq J_{M,1}$ *and* $I_M(\{P_m\}, \{J_m\}) \geq R_1$ *yields the objective* $P_M = P_{M,1}$. *Moreover, any pair of power allocations across blocks that makes an optimal solution of the game in (3.3) and (3.4) is also an optimal solution of* Problem 1, *and conversely.*

(II)Take the game given by (3.3) and (3.4) and set the constraints to $P_M(\mathbf{h}) \leq P_{M,1}$ *and* $J_M(\mathbf{h}) \leq J_{M,1}$. *Denote the resulting value of the objective by* $I_M(\mathbf{h}, P(h), J(h)) = R_1$. *Then solving* Problem 2 *above with the constraints* $\frac{1}{M}\sum_{m=0}^{M-1} P_m \leq P_{M,1}$ *and* $I_M(\{P_m\}, \{J_m\}) \leq R_1$ *yields the objective* $J_M = J_{M,1}$. *Moreover, any pair of power allocations across blocks that makes an optimal solution of the game in (3.3) and (3.4) is also an optimal solution of* Problem 2, *and conversely.*

(III) If $J_{M,1}$ *is the value used for the second constraint in* Problem 1 *above, and* $P_{M,1}$ *is the resulting value of the cost/reward function, then solving* Problem 2 *with* $P_M = P_{M,1}$ *yields the cost/reward function* $J_M = J_{M,1}$. *Moreover, any pair of power allocations across blocks that makes an optimal solution of* Problem 1, *should also make an optimal solution of* Problem 2, *and conversely.*

Proposition 3.5. *The optimal solutions of* Problem 1 *and* Problem 2 *above are unique.*

Proposition 3.6. *(I) Under the optimal maximin second level power control strategies (*Problem 1*), the "required" transmitter power* P_M *over a frame is a strictly increasing, continuous, concave and unbounded function of the power* J_M *that the jammer invests in that frame.*

*(II) Under the optimal minimax second level power control strategies (*Problem 2*), the "required" jamming power* J_M *over a frame is a strictly increasing, continuous, convex and unbounded function of the power* P_M *that the transmitter invests in that frame.*

Although under the same transmitter/jammer frame power constraints P_M and J_M the second level optimal power allocation strategies for the maximin and minimax problems coincide, this result should not be associated with the notion of Nash equilibrium, since the two problems solved above do not form a zero-sum game, while for the game of (3.9) and (3.10), first level power control strategies are yet to be investigated.

As in Chapter 2, we shall henceforth denote the function that gives the "required" transmitter power P_M over a frame where the jammer invests power J_M by $\mathscr{P}_M(J_M, \mathbf{h})$ and its "inverse", i.e.

the function that gives the "required" jamming power over a frame where the transmitter invests P_M by $\mathscr{J}_M(P_M, \mathbf{h})$. Note that unlike in Chapter 2, these functions are now also dependent on the channel realization $\mathbf{h}$. A particular channel realization can be characterized in terms of the second level power allocation technique. For instance, considering the maximin problem, we can map each channel vector $\mathbf{h}$ to a unique curve $\mathscr{P}_M(J_M)$ in the plane. That is, for fixed $\mathbf{h}$, we increase the jamming power allocated to the frame from 0 to ∞, and compute the transmitter power $\mathscr{P}_M(J_M, \mathbf{h})$ required for achieving reliable communication. We have already mentioned that, for any fixed $\mathbf{h}$, $\mathscr{P}_M(J_M)$ is a strictly increasing, continuous, concave and unbounded function.

Next we take a closer look at the $\mathscr{P}_M(J_M, \mathbf{h})$ curves. By inspecting the proofs of Propositions 3.3 - 3.6, we notice that j denotes the index of the first block on which the jammer allocates nonzero power, while p is the index of the first block on which the transmitter allocates nonzero power (the blocks are indexed in increasing order of their squared channel coefficients h_m, and both transmitter and jammer allocate more power to blocks with larger values of h_m). Note also that $p \leq j$. If for a given $\mathbf{h}$ we have $p = j$ over an interval of J_M, then the $\mathscr{P}_M(J_M)$ curve is linear over that interval. However, if $p < j$, the curve is strictly concave.

We can think of the $\mathscr{P}_M(J_M)$ curve that characterizes a given channel realization $\mathbf{h}$ as being "built" in the following manner. We increase the jamming power allocated to the corresponding frame, starting from $J_M = 0$. We already know that without the jammer's presence the transmitter transmits over the "best" blocks , i.e. the ones having the largest channel coefficients. Even as the jammer starts interfering, its optimal strategy is such that the blocks with the largest coefficients remain the most attractive for the transmitter. However, they do become worse than before. Hence, if without the presence of the jammer the transmitter would normally ignore some of the blocks, as the jammer's power increases, those blocks may slowly become more attractive. At some point, the transmitter will choose to increase the number of blocks over which it allocates non-zero power (i.e. decrease p). Similarly, as the jammer's power J_M increases, the jammer moves from the best block to the best two blocks, and so on (i.e. the jammer decreases j).

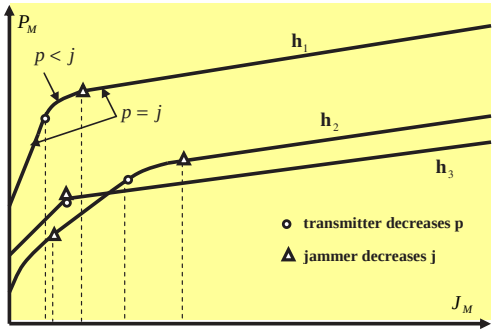

FIGURE 3.3. Typical $P_M(J_M)$ curves, for different channel realizations

The transmitter's and the jammer's transitions do not have to be simultaneous. Recall that the relationship between the values of p and j decide whether the $\mathscr{P}_M(J_M)$ curve is linear or strictly concave over an interval of J_M. Therefore, we expect the $\mathscr{P}_M(J_M)$ curves to look like a concatenation of linear and strictly concave segments, as in Figure 3.3. As J_M increases, the transmitter decreases the value of p whenever the slope of the $\mathscr{P}_M(J_M)$ curve can be decreased by this move and similarly, the jammer decreases the value of j whenever the slope can be increased. In other words, as J_M increases, the transitions from linear portions to nonlinear portions are caused by the transmitter, while the transitions from nonlinear to linear ones are caused by the jammer.

In the remainder of this subsection we provide the simplest example of optimal power allocation between the blocks of a frame. Namely, we look at the case when $M = 2$ – only two blocks per frame.

Particular case: $M = 2$

The case of $M = 2$ is the simplest and most intuitive illustration of the second-level power control strategy. Since we have already discussed the nice dual property between the second level minimax and maximin strategies, the following considerations refer to the maximin scenario only. The jamming power J_M has to be allocated between the two blocks in a way that maximizes the transmitter's expense, should it decide to achieve reliable communication over the frame. The jammer and the transmitter can each transmit over either one or both blocks. All possible situations are considered next.

Let the two channel coefficients be $h_0 \leq h_1$, and denote the transmitter's and jammer's powers allocated to the blocks by P_0, P_1 and J_0, J_1 respectively. Also denote $x_i = J_i + \sigma_N^2$, for $i \in \{0, 1\}$, and $c = \exp(2R)$. If we take a closer look at the solutions (3.5) and (3.6) of the game in (3.3) and (3.4), and if we recall that the solutions of either of our maximin and minimax second layer power allocation strategies have a similar form (up to the constants η and ν), it is easy to observe that $x_0 \leq x_1$ and $\frac{x_0}{h_0} \geq \frac{x_1}{h_1}$. This fact is also noted in Section 3.8.3, where the solution of *Problem 1* is given again, with the new notation $\lambda = 1/\eta$ and $\mu = \nu/\eta$. Throughout the rest of this subsection we shall refer to the notation in Section 3.8.3 and the solution in (3.100) and (3.101).

If the transmitter is active over both blocks, then the constraint $I_M = R$ yields

$$\left(1 + \frac{h_0}{x_0} P_0\right)\left(1 + \frac{h_1}{x_1} P_1\right) = c, \tag{3.13}$$

and with (3.102) in Section 3.8.3 we obtain $\lambda = \sqrt{c\frac{x_0}{h_0}\frac{x_1}{h_1}}$.

Suppose that the jammer is only present on one block of the frame, then that is the block with coefficient h_1. This implies $x_0 = \sigma_N^2$, and $x_1 = (2J_M + \sigma_N^2)$. Under these assumptions, the transmitter will only transmit on the first block, (that is $P_0 = 2P_M$ and $P_1 = 0$) if and only if

$$\lambda = \sqrt{c\frac{x_0}{h_0}\frac{x_1}{h_1}} < \frac{x_0}{h_0}, \tag{3.14}$$

which translates to $c\frac{(2J_M + \sigma_N^2)}{h_1} < \frac{\sigma_N^2}{h_0}$.

Otherwise, the transmitter is present over both blocks, performing water-pouring as in (3.102), with

$$\lambda = \sqrt{c\frac{(2J_M + \sigma_N^2)\sigma_N^2}{h_0 h_1}}. \tag{3.15}$$

Note that the transmitter cannot be present only on the second block.

If the jammer decides to allocate non-zero power over both blocks, its optimal strategy is such that $x_0/h_0 \geq x_1/h_1$. If we also have $x_0/h_0 \leq c(x_1/h_1)$ (corresponding to $\lambda \geq x_0/h_0$), then the transmitter is present over both blocks. In this case, we can particularize (3.102) to $M = 2$ and

obtain:

$$P_m = \sqrt{c\frac{x_0}{h_0}\frac{x_1}{h_1}} - \frac{x_m}{h_m}, \text{ for } m \in \{0, 1\}. \tag{3.16}$$

Define the ratio $r = \frac{x_0/h_0}{x_1/h_1}$. Since $x_0 + x_1 = 2(J_M + \sigma_N^2)$, we can write

$$P_M = \frac{(J_M + \sigma_N^2)(2\sqrt{cr} - r - 1)}{h_0 r + h_1}, \text{ if } c\frac{x_1}{h_1} \geq \frac{x_0}{h_0}. \tag{3.17}$$

Setting the derivative of P_M with respect to r equal to zero, we get the unique solution

$$r_{opt} = \left(\frac{\sqrt{(h_1 - h_0)^2 + 4h_0h_1c} - (h_1 - h_0)}{2h_0\sqrt{c}} \right)^2, \tag{3.18}$$

which provides the optimal allocation of the jamming power J_M between the two blocks. The value of r_{opt} is between 1 (for $h_0 = h_1$) and c (for $h_0 = 0$). Furthermore, $P_M(r)$ is strictly increasing for $r \in [1, r_{opt})$ and strictly decreasing for $r \in (r_{opt}, c]$, hence r_{opt} is the maximizing argument in (3.17).

This also implies that if $r_{opt}\frac{(2J_M+\sigma_N^2)}{h_1} < \frac{\sigma_N^2}{h_1}$, the jammer's optimal strategy is to allocate all of its power to the second block. If, on the other hand, $r_{opt}\frac{(2J_M+\sigma_N^2)}{h_1} \geq \frac{\sigma_N^2}{h_1}$, then the jammer's best strategy is to allocate the power J_M such that the ratio $r = (x_0/h_0)/(x_1/h_1)$ equals the optimal ratio r_{opt}.

The remarks above conclude in the following algorithm:

- If $c\frac{(2J_M+\sigma_N^2)}{h_1} \leq \frac{\sigma_N^2}{h_0}$, both transmitter and jammer will only transmit on the second block.
- If $c\frac{(2J_M+\sigma_N^2)}{h_1} > \frac{\sigma_N^2}{h_0}$ but $r_{opt}\frac{(2J_M+\sigma_N^2)}{h_1} \leq \frac{\sigma_N^2}{h_1}$, the jammer will allocate all its power to the second block, while the transmitter will transmit on both blocks.
- If $r_{opt}\frac{(2J_M+\sigma_N^2)}{h_1} > \frac{\sigma_N^2}{h_1}$, the jammer will transmit over both blocks such that $(x_0/h_0)/(x_1/h_1) = r_{opt}$, and the transmitter will also be present on both blocks.

3.3.2 Inter-Frame Power Allocation

In this subsection we present the first level optimal power allocation strategies.

The Maximin Solution

Under our full CSI, average power constraints scenario, the jammer needs to find the best choice of the set $\mathscr{X} \subset \mathbb{R}_+^M$ of channel realizations over which it should be present, and the optimal way $J_M(\mathbf{h})$ to distribute its power over $\mathscr{X}$, such that when the transmitter employs its optimal strategy, the probability of outage is maximized.

We already know that given the jammer's strategy, the optimal way of allocating the transmitter's power is such that reliable communication is first obtained on the frames that require the least amount of transmitter power. The jammer's optimal strategy is presented in Theorem 3.7 below.

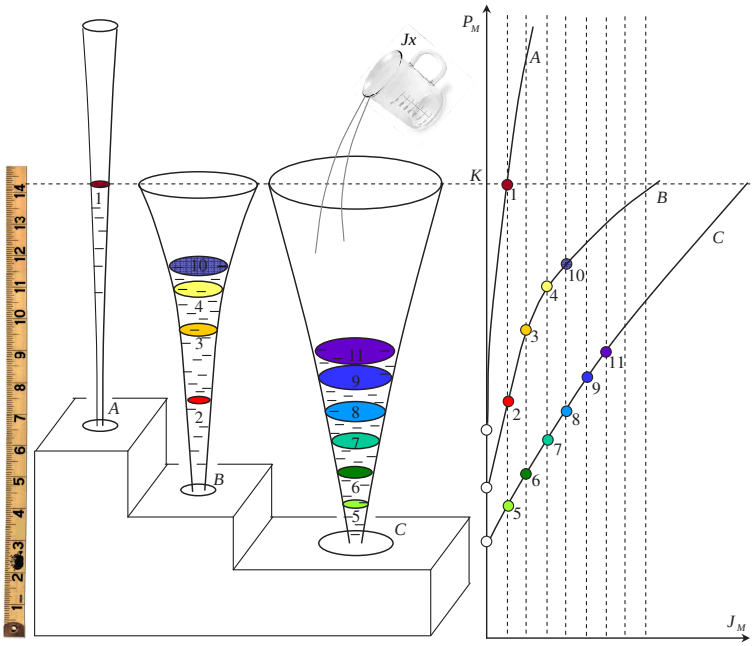

FIGURE 3.4. Maximin vase filling.

The theorem is complemented by the numerical algorithm and the intuition-building analogy that follows its proof.

Theorem 3.7. *It is optimal for the jammer to make* $J_M(\mathbf{h})$ *satisfy the power constraint with equality. The optimal jammer strategy for allocating power across frames is to increase the* required

transmitter power, starting with those frames whose channel realizations exhibit the steepest instantaneous slope of the characteristic $\mathscr{P}_M(J_M)$ curve. The jamming power should be allocated such that the required *transmitter power over each channel realization where the jammer is present does not exceed a pre-defined level K. The optimal value for K that maximizes the outage probability can be found numerically, by exhaustive search in a compact interval of the positive real line.*

Proof. Our proof takes a contradictory approach. Instead of deriving the optimal strategy defined above in a direct manner, we show instead that any other strategy not satisfying the theorem's requirements is suboptimal. Let $\mathscr{S}, \mathscr{X} \subset \mathbb{R}_+^M$ denote the sets of channel realizations over which the transmitter and the jammer are present, respectively.

Suppose the jammer picks a certain strategy $J_M(\mathbf{h})$. Since the transmitter's strategy is predictable, the jammer already knows the transmitter's optimal strategy. Under this optimal strategy, the transmitter picks a set of frames $\mathscr{S}$ over which it will invest non-zero power. This choice also results in a maximum level of *required* transmitter power that will actually be matched by the transmitter. Denote this level by K. Since the transmitter's strategy is the optimal response to the jammer's strategy, the *required* transmitter power should be larger than or equal to K over the set of frames $\mathscr{X} \setminus \mathscr{S}$ where the jammer jams, but the transmitter does not afford to transmit. Otherwise, the transmitter would be wasting power and its strategy would not be optimal.

But since the jammer knows the transmitter's strategy, and knows that the transmitter will not transmit over $\mathscr{X} \setminus \mathscr{S}$, its optimal strategy should make the *required* transmitter power over $\mathscr{X} \setminus \mathscr{S}$ at most equal to K. Otherwise the jammer would be wasting power.

We have seen how the jammer's power should be distributed over $\mathscr{X} \setminus \mathscr{S}$. Next we show that if the jammer's power allocation over $\mathscr{S} \bigcap \mathscr{X}$ is not done according to the theorem, the jammer's strategy is not optimal. For this, we assume that the jammer's strategy does not satisfy the theorem's requirements, and provide a method of improvement (i.e. we prove sub-optimality).

If the theorem is not satisfied, than there exist two sets $\mathscr{A}, \mathscr{B} \subset \mathscr{S} \bigcap \mathscr{X}$ of non-zero $\mathfrak{m}$-measure such that $\frac{dP_M(\mathbf{h}_1)}{dJ_M} > \frac{dP_M(\mathbf{h}_2)}{dJ_M}$ $\forall$ $\mathbf{h}_1 \in \mathscr{A}$ and $\mathbf{h}_2 \in \mathscr{B}$, and such that the required P_M is less than K on $\mathscr{A}$ and $J_M > 0$ on $\mathscr{B}$.

Consider a small enough amount of jamming power δJ_M, such that, for any channel realization $\mathbf{h} \in \mathscr{A} \bigcup \mathscr{B}$, we can modify the jamming power by δJ_M without changing the slope of the $\mathscr{P}_M(J_M)$ curve. Subtracting δJ_M from all frames in $\mathscr{B}$, the jammer obtains the excess power $\delta J_M m(\mathscr{B})$, which it can allocate uniformly over $\mathscr{A}$. The jammer's total average power remains unchanged. However, the required transmitter power over $\mathscr{A} \bigcup \mathscr{B}$ is increased (because the slopes of the $\mathscr{P}_M(J_M)$ curves corresponding to $\mathscr{A}$ are all larger than the slopes of the $\mathscr{P}_M(J_M)$ curves corresponding to $\mathscr{B}$), and thus the modification results in a larger probability of outage.

There exists a closed interval $[0, K_{max}] \in \mathbb{R}_+$ which includes the optimal value of K. This observation is vital to the existence of a numerical algorithm that searches for the optimal K. Once such an interval has been set, we can fix the desired resolution and calculate the numerical complexity of the algorithm. We next show how the upper limit K_{max} of this interval can be found. Consider the set of channel realizations $\mathscr{S}_0$ where the transmitter is active when the jammer does not interfere with the transmission. Next, find the value K_{max} for which, when the jammer allocates its power $\mathcal{J}$ according to the rules of the theorem, we obtain a set $\mathscr{X}_0 \subset \mathbb{R}_+^M \setminus \mathscr{S}_0$. This means that the jammer's strategy under any $K \geq K_{max}$ has no influence upon the transmitter's strategy. Note that such a finite K_{max} can be found whenever $\mathbb{R}_+^M \setminus \mathscr{S}_0$ has non-zero $\mathfrak{m}$-measure. $\square$

The algorithm in Table 3.1 which we used in generating our numerical results in Subsection 3.3.3 helps shed more light into the practicality of Theorem 3.7. In the description of the algorithm, we assume discrete jamming power levels J_M^k with $k = 0, 1, \ldots$ and $J_M^0 = 0$, as well as a discrete and finite channel coefficient space. As a consequence, there exists a finite number of $\mathscr{P}_M(J_M)$ curves, each characterizing one possible channel realization, and each completely determined by a finite vector whose components are the values of $\mathscr{P}_M(J_M^k)$ for that particular channel realization.

An intuitive description of the technique is given in Figure 3.4. Consider the problem where the jammer has to pour water in a number of vases (a vase for each possible channel realization). The shape of each vase is such that the vertical section of its wall produces a concave curve similar to the corresponding $\mathscr{P}_M(J_M)$ curve. The jammer can afford to spend a certain volume of water. The jammer wants to "annoy" the transmitter, which is deeply concerned with *the sum of the heights* that the water levels reach in the vases. Hence, the jammer tries to use its available volume of water, such that the sum of the water levels' heights is maximized. However, the jammer cannot pour all the water in the thinnest vase, because then the transmitter might just ignore that vase. Instead, the jammer has to set a height limit K which it should not exceed. The jammer pours the water a cup at a time, starting with the vase in which a cup of water rises the water level the quickest. In Figure 3.4, the order of adding cups to the vases is shown by numerals from 1 to 11. The first cup is poured into the thinnest vase (vase A) and incidentally reaches the level K. Thus, no more water should be added to vase A. The next three cups are added to vase B, and then the next five cups to vase C. Then the jammer returns to vase B, and adds another cup, for this increases the water level more than it would increase the level in vase C. Finally, the last available cup is added to vase C. The way the numerical algorithm works is illustrated in the right part of Figure 3.4.

The Minimax Solution

In Theorem 3.4 we showed that given the transmitter's and the jammer's powers P_M and J_M allocated to a frame, the optimal strategies for distributing these powers inside the frame are identical for the minimax and the maximin problems. Hence, by rotating the $\mathscr{P}_M(J_M)$ plane, we get the characteristic $\mathscr{J}_M(P_M)$ curves for the minimax problem. We already know that given the transmitter's strategy, the optimal way of allocating the jammer's power is such that outage is first induced on the frames that require the least amount of jamming power.

The transmitter's optimal strategy is presented in the following theorem, which is complemented by the numerical algorithm and the analogy that follows its proof.

TABLE 3.1. Numerical algorithm for deriving the maximin solution.

Let $\mathbf{P}$ denote a matrix with each row representing one of the vectors $\mathscr{P}_M(J_M^k)$, for different channel realizations $\mathbf{h}$. Let P_{req} be the vector of required powers for the different frames. The initial P_{req} is set equal to the first column of $\mathbf{P}$. Let K_{max} be the upper limit when searching for the optimal K.
Initialize $K = 0$.
while $K \leq K_{max}$
    $p_T = 0$.
    Let L be an index vector, the same size as P_{req}.
    Initialize all components of L to be equal to 1.
    We have the relationship $P_{req}(j) = \mathbf{P}(j, L(j))$.
% Jx strategy:
The amount of jamming power spent at each step is accumulated into the variable J_c.
    while Jx power constraint is satisfied ($J_c \leq \mathcal{J}$)
        Find row j of $\mathbf{P}$ with the largest difference between components $L(j)+1$ and $L(j)$, and such that $\mathbf{P}(j, L(j)+1) \leq K$.
        $P_{req}(j) = \mathbf{P}(j, L(j)+1)$.
        $L(j) = L(j) + 1$.
        Weigh J_M^j by probability of row j and add to J_c.
    end
% Tx strategy (Tx picks frames where required power is minimum first)
The amount of transmitter power spent at each step is simulated into the variable P_c.
    while Tx power constraint is satisfied ($P_c \leq \mathcal{P}$)
        Pick the least component of P_{req}.
          Add probability of corresponding frame to p_T.
        Add value of component, weighted by probability above, to P_c.
        Delete component from P_{req}.
    end
    $P_{out}(K) = 1 - p_T$
    Increment K.
end
Select K that produces the largest P_{out}.

Theorem 3.8. *It is optimal for transmitter to make $P_M(\mathbf{h})$ satisfy the long-term power constraint with equality. The optimal transmitter power allocation across frames is to increase the* required *jamming power up to some pre-defined level K, starting with those frames on which the required transmitter power to achieve this goal is least.*

The optimal value for K that minimizes the outage probability can be found numerically by exhaustive search.

Proof. As in the case of Theorem 3.7, we take a contradictory approach. Instead of directly deriving the optimal strategy defined above, we show that any other strategy not satisfying the theorem's requirements is suboptimal. Recall that $\mathscr{S}$ and $\mathscr{X} \subset \mathbb{R}_+^M$ denote the sets of channel realizations over which the transmitter and the jammer are present, respectively.

Suppose the transmitter picks a certain strategy $P_M(\mathbf{h})$. Since the jammer's strategy is predictable, the transmitter already knows the jammer's optimal strategy. Under this optimal strategy, the jammer should pick a set of frames $\mathscr{X}$ over which it will invest non-zero power. This choice also results in a maximum level of *required* jamming power that will actually be matched by the jammer. Denote this level by K. Since the jammer's strategy is optimal, the *required* jamming power outside the set $\mathscr{X}$ should be larger than or equal to K. Otherwise, the jammer would be wasting power and hence its strategy would not be optimal. But since the transmitter knows the jammer's strategy, it also knows that the jammer will not be present over $\mathscr{S} \setminus \mathscr{X}$, so the transmitter should make the *required* jamming power over $\mathscr{S} \setminus \mathscr{X}$ at most equal to K. Otherwise the transmitter would be wasting power. Hence, over $\mathscr{S} \setminus \mathscr{X}$ the transmitter should allocate power such that the required jamming power is equal to K.

Next we show that if the transmitter's power allocation over $\mathscr{S} \bigcap \mathscr{X}$ is not done according to the theorem, the transmitter's strategy is not optimal. For this, we assume that the transmitter's strategy does not satisfy the theorem's requirements, and provide a method of improvement (i.e. we prove sub-optimality).

If the theorem is not satisfied, than there exist two sets $\mathscr{A}, \mathscr{B} \subset \mathscr{S} \bigcap \mathscr{X}$ of non-zero $\mathfrak{m}$-measure such that $P_M(\mathbf{h}_1, K) < P_M(\mathbf{h}_2, K)\ \forall\ \mathbf{h}_1 \in \mathscr{A}$ and $\mathbf{h}_2 \in \mathscr{B}$, and such that the required J_M is less than K on $\mathscr{A}$ and $J_M > 0$ on $\mathscr{B}$ cannot be part of the minimax solution. Denote the original transmitter power allocation functions over $\mathscr{A}$ and $\mathscr{B}$ by $P^A_{M,0}(\mathbf{h})$ and $P^B_{M,0}(\mathbf{h})$ respectively.

For any $\mathbf{h}_1 \in \mathscr{A},\ \mathbf{h}_2 \in \mathscr{B}$ and $J_{M,1}, J_{M,2} < K$, we have:

$$\frac{K - J_{M,1}}{P_M(\mathbf{h}_1, K) - P_M(\mathbf{h}_1, J_{M,1})} \overset{a)}{\geq} \frac{K}{P_M(\mathbf{h}_1, K)} \overset{b)}{>} \frac{K}{P_M(\mathbf{h}_2, K)} \overset{c)}{\geq} \frac{J_{M,2}}{P_M(\mathbf{h}_2, J_{M,2})}, \tag{3.19}$$

where both $a)$ and $c)$ follow from the convexity of $\mathscr{J}_M(P_M)$ – Proposition 3.6 – and $b)$ follows from the assumption in the beginning of this proof.

If the transmitter cuts off transmission over a subset $\mathscr{B}' \subset \mathscr{B}$, it obtains the excess power $\int_{\mathscr{B}'} P_M(\mathbf{h}) dm(\mathbf{h})$, which it can allocate to a subset $\mathscr{A}' \subset \mathscr{A}$ such that the required J_M is equal to K over $\mathscr{A}'$, i.e.

$$\int_{\mathscr{B}'} P^B_{M,0}(\mathbf{h}) dm(\mathbf{h}) = \int_{\mathscr{A}'} \left[P_M(\mathbf{h}, K) - P^A_{M,0}(\mathbf{h})\right] dm(\mathbf{h}) \tag{3.20}$$

Replacing $P_M(\mathbf{h}_1, J_{M,1})$ by $P^A_{M,0}(\mathbf{h})$ and $P_M(\mathbf{h}_2, J_{M,2})$ by $P^B_{M,0}(\mathbf{h})$ in (3.19), we see the transmitter improves its strategy by forcing the jammer to allocate more power to the set $\mathscr{A} \bigcup \mathscr{B}$, and hence decreases the probability of outage. Note that since $\mathscr{B}' \subset \mathscr{S} \bigcap \mathscr{X}$, the set $\mathscr{B}'$ is in outage, regardless of whether the transmitter is present or not. Thus, transmitter does not increase P_{out} by cutting off transmission on $\mathscr{B}'$.

There exists a closed interval $[0, K_{max}] \in \mathbb{R}_+$ which includes the optimal value of K. As in the maximin case, the existence of such a closed interval is required for constructing a numerical algorithm that searches for the optimal K. The upper limit K_{max} of this interval can be found and updated as follows. First solve the problem for an arbitrarily chosen K_0, and determine the set $\mathscr{S}_0 \setminus \mathscr{X}_0$ over which the transmitter achieves reliable communication. We can set K_{max} equal to the value of K that yields a set $\mathscr{S}$ of the same $\mathfrak{m}$-measure as the set $\mathscr{S}_0 \setminus \mathscr{X}_0$. Note that if K is increased over this K_{max}, the outage probability is at least as large as that obtained for $K = K_0$ (and hence K_0 is a better choice). $\square$

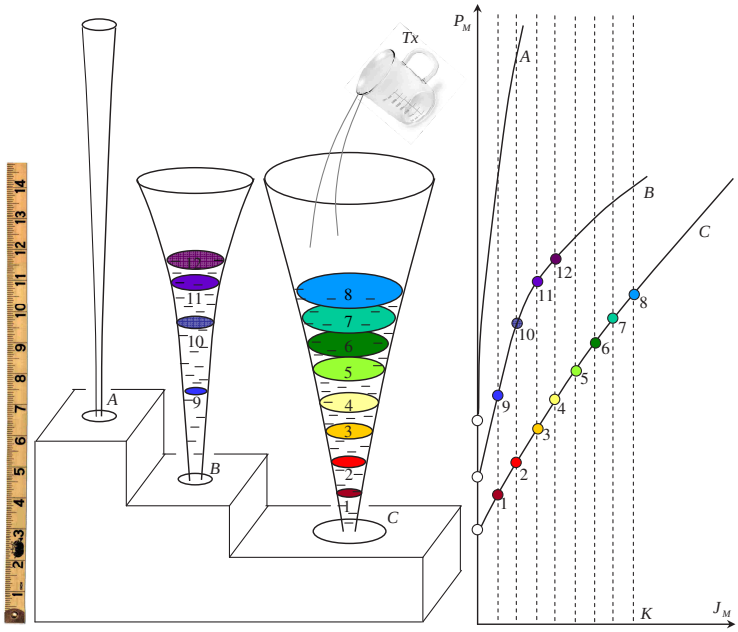

FIGURE 3.5. Minimax vase filling.

The algorithm in Table 3.2 which we used for our numerical results in Subsection 3.3.3 illustrates the application of Theorem 3.8. In the description of the algorithm, we assume discrete jamming power levels J_M^k with $k = 0, 1, \ldots$ and $J_M^0 = 0$, as well as a discrete and finite channel coefficient space. As a consequence, there exists a finite number of $\mathscr{P}_M(J_M)$ curves, each characterizing one possible channel realization, and each completely determined by a finite vector whose components are the values of $\mathscr{P}_M(J_M^k)$ for that particular channel realization.

A description of the technique is given in Figure 3.5, using the same vase analogy as in the maximin case. This time, the transmitter does the pouring. Its obsession with the sum of the heights of the water levels imposes a constraint on this sum. Under this constraint, the transmitter wants to use as much of the jammer's water as possible. That is, the transmitter attempts to maximize the volume of water that can be accommodated by the vases, under the constraint that the sum of the water levels' heights is less than some given value. Moreover, if the transmitter pours water only in the thickest vase, it might not feel that it did enough damage to the jammer. Thus, the transmitter needs to set a limit K. The optimal strategy is to fill (up to volume level K) the thickest vase first

TABLE 3.2. Numerical algorithm for deriving the minimax solution.

Let $\mathbf{P}$ denote the matrix with rows representing the $\mathscr{P}_M(J_M^k)$ vectors for different channel realizations $\mathbf{h}$. Let K_{max} be value where searching for the optimal K stops.
Initialize $K = 0$.
while $K \leq K_{max}$
% Tx strategy:
The amount of transmitter power spent at each step is accumulated into the variable P_c.
    Initialize $K = J_M^k$.
    Initialize $P_c = 0,\ p_T = 0$.
    while Tx power constraint is satisfied ($P_c \leq \mathcal{P}$)
        Find row j of $\mathbf{P}$ with least k-th component.
        Add probability of row j to p_T.
        Add value of the k-th component, weighted by the probability above, to P_c.
        Delete row j from matrix $\mathbf{P}$.
    end
% Jx strategy (Jx jams frames where Tx is present, randomly, until it reaches its power constraints):
    $p_J = \frac{\mathcal{J}}{K}$.
    $P_{out}(K) = p_T - p_J$.
    Increment K.
end
Select K that produces the least P_{out}.

(note that "thickest" refers to the fact that when filled up to volume level K, the vase displays the lowest water level height, thus "thickest" is defined with respect to K). The order in which the transmitter adds cups of water to the vases is depicted in Figure 3.5 by numerals from 1 to 12. The way the numerical algorithm works is illustrated in the right part of Figure 3.5.

Particular case: $M = 1$

For this simple scenario, there is no second level of power allocation. All frames consist of only one block, and the $P_M(J_M)$ curves have the particular affine form with parameter h (the squared channel coefficient corresponding to this block):

$$P_M = \frac{\exp(R) - 1}{h}(J_M + \sigma_N^2). \tag{3.21}$$

Since the slopes of the $P_M(J_M)$ curves are constant with J_M and the frames with smaller values of the channel coefficients have larger characteristic slopes, we can easily particularize Theorems 3.7 and 3.8. With the same notation $\mathscr{X} \subset \mathbb{R}_+$ for the set of channel realizations over which the jammer invests non-zero power and $\mathscr{S} \subset \mathbb{R}_+$ for the set of channel realizations over which the transmitter uses non-zero power, we can now define the optimal power allocation strategies. For the maximin scenario, The jammer should deploy some $J_M(h)$ over $\mathscr{X}$ such that the *required* $P_M(h)$ is constant over the whole interval $\mathscr{X}$. The purpose of the jammer being active over $\mathscr{X} \setminus \mathscr{S}$ is to "intimidate" the transmitter. The transmitter plays second, and hence takes advantage of the jammer's weaknesses. It always chooses to be active on the subset of $\mathscr{X}$ on which the *required* $P_M(h)$ is least. This is why the optimal jammer strategy is to display no weakness, i.e. to make $P_M(h)$ constant over $\mathscr{X}$. These considerations are formalized in Proposition 3.9 below.

Proposition 3.9. *In the maximin scenario, the jammer should adopt such a strategy as to make the transmitter's best choice of $\mathscr{S}$ intersect $\mathscr{X}$ on the the left-most part of $\mathscr{S}$, and the required transmitter power equal to some constant K on $\mathscr{X} \bigcap \mathscr{S}$ and to $(c-1)\sigma_N^2/h$ on $\mathscr{S} \setminus \mathscr{X}$. Transmitting $J_M(h)$, satisfying the power constraint with equality, such that the transmitter power required for reliable communication is $P_M(h) = K, \forall h \in [h_1^*, h_2^*]$, and $P_M(h) = (c-1)\sigma_N^2/h, \forall h \in [0,\infty) \setminus (h_1^*, h_2^*]$, for some $h_1^* < h_2^* \in \mathbb{R}_+$ and some constant $K \in \mathbb{R}_+ \bigcup \{\infty\}$ is an optimal jammer strategy for the maximin problem. (Note that $P_M(h)$ should be continuous at h_1^*.) The values $K,\ h_1^*$ and h_2^* that maximize the outage probability can be found by solving the following problem:*

$$\textit{Find } \min_K \int_{h_0}^{\infty} f(h)dh, \textit{ where}$$

$$h_0 \textit{ is given by } \int_{h_0}^{h_2} K f(h)dh + \int_{h_2}^{\infty} \frac{c-1}{h}\sigma_N^2 f(h)dh = \mathcal{P}, \tag{3.22}$$

$$h_1 \textit{ is given by } h_1 = \frac{c-1}{K}\sigma_N^2, \tag{3.23}$$

$$\textit{and } h_2 \textit{ is given by } \int_{h_1}^{h_2} \left(\frac{hK}{c-1} - \sigma_N^2\right) f(h)dh = \mathcal{J}. \tag{3.24}$$

■

The power allocation is depicted in Figure 3.6. The convex decreasing curve represents the original required transmitter power, without the presence of a jammer and satisfies the equation $P_M = (c-1)\sigma_N^2/h$. Notice how by picking some K, we can determine h_1, h_2 and h_0 (in this order), and then find the probability of outage as $P_{out}(h_1) = 1 - \mathfrak{m}[(h_0, \infty)]$. The optimal K, resulting in h_1^*, h_2^* and h_0^*, is the one minimizing the $\mathfrak{m}$-measure of the set (h_0, ∞).

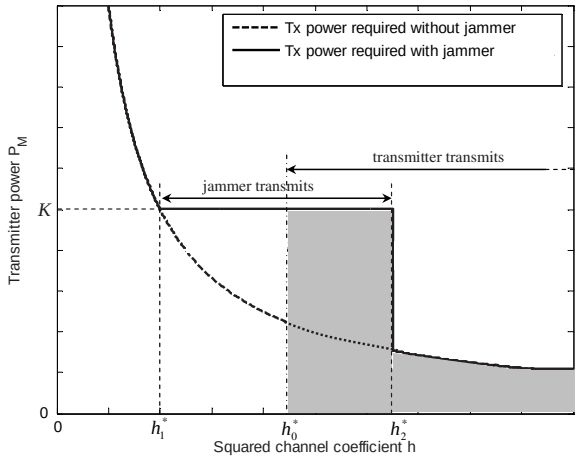

FIGURE 3.6. Maximin solution for $M = 1$ - power distribution between frames

For the minimax scenario the jammer will not transmit any power over a frame if outage is not going to be induced or if the transmitter is not present, i.e. $\mathscr{X} \subset \mathscr{S}$. The jammer will start allocating power to the frames over which an outage is easiest to induce, and go on with this technique until the average power reaches the limit set by its power constraint. Obviously, the jammer prefers the frames for which the required $J_M(h)$ is less. The optimal transmitter's strategy is to allocate its power such that the required $J_M(h)$ is constant on the whole set $\mathscr{S}$, and hence to display no weakness.

These considerations are formalized in Proposition 3.10 below.

Proposition 3.10. *For the minimax scenario, the transmitter's optimal way to allocate its power is to make the required jamming power remain equal to some constant K on all of $\mathscr{X}$. Transmitting $P_M(h)$, satisfying the power constraint with equality, such that the required $J_M(h)$ equals K for*

$h \in [h_x^*, \infty)$, *and* $J_M(h) = 0 \; \forall h \in [0, h_x^*)$, *for some* $h_x^* \in \mathbb{R}_+$, *is an optimal transmitter strategy for the minimax problem. The values* K *and* h_x^* *that minimize the outage probability can be found by solving the following problem numerically:*

$$\textit{Find} \max_K \int_{h_0}^{\infty} f(h)dh, \textit{ where}$$

$$h_0 \textit{ is given by } \int_{h_x}^{h_0} K f(h)dh = \mathcal{J}, \tag{3.25}$$

$$h_x \textit{ is given by } \int_{h_x}^{\infty} \frac{(c-1)(K+\sigma_N^2)}{h} f(h)dh = \mathcal{P}. \tag{3.26}$$

■

The numerical problem is described in Figure 3.7. Notice how by picking some K, we can determine h_x and h_0 (in this order), and then find the probability of outage as $P_{out}(h_1) = 1 - \mathfrak{m}[(h_0, \infty)]$. The optimal K, resulting in h_x^* and h_0^*, is the one maximizing the $\mathfrak{m}$-measure of the set (h_0, ∞). Note that the jammer does not necessarily have to jam on an interval of the form $[h_x, h_0]$. The jammer's choice space (the set of frames out of which the jammer picks its set $\mathscr{X}$) is an indifferent one, i.e. the jammer can randomly pick $\mathscr{X} \subset [h_x, \infty)$ as long as its measure satisfies $K\mathfrak{m}(\mathscr{X}) = \mathcal{J}$. However, for the purpose of computing the outage probability, the representation of $\mathscr{X}$ as an interval is convenient and incurs no loss of generality.

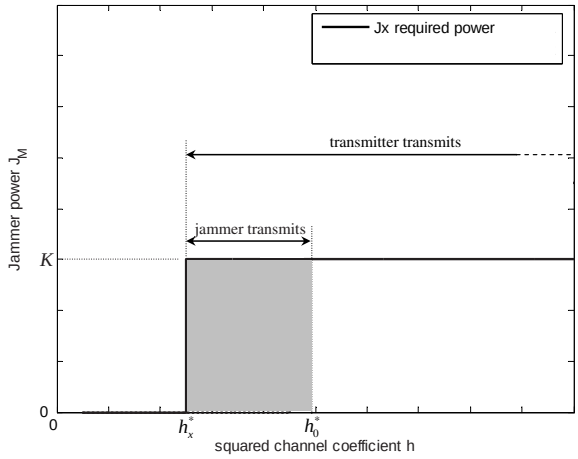

FIGURE 3.7. Minimax solution for $M = 1$ - power distribution between frames

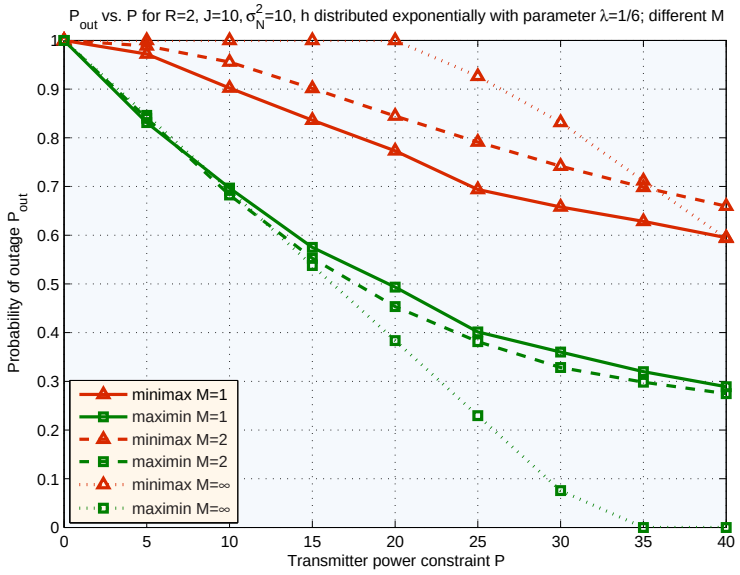

FIGURE 3.8. Outage probability vs. $\mathcal{P}$ for $M = 1$ and $M = 2$ and $M \to \infty$ when $\mathcal{J} = 10$ – minimax and maximin cases. We take $R = 2$.

3.3.3 Numerical Results

We have computed the outage probabilities for both minimax and maximin problems when $M = 1$ and $M = 2$. The channel coefficients are assumed i.i.d. exponentially distributed with parameter $\lambda = 1/6$. Figure 3.8 shows the outage probability vs. the maximum allowable average transmitter power $\mathcal{P}$ for fixed $\mathcal{J} = 10$ when $R = 1$. For comparison purposes, we also plotted the results for the case when $M = \infty$, which are readily available from Chapter 2.

Numerical results demonstrate a sharp difference between the minimax solutions and the maxmin solutions, which demonstrates the non-existence of Nash-equilibria of pure strategies for our two-person zero-sum game with full CSI. Note the behavior of the outage probability when the number of blocks per frame M is increased. At low transmitter powers, the increase of M produces an increase in the outage probability for both the minimax, and the maximin scenarios.

On the contrary, at higher transmitter powers a lower outage probability is obtained for both the minimax and the maximin cases when M is larger. This behavior can be summarized as follows: the more powerful player will use the available diversity to its own advantage.

3.4 CSI Available to All Parties. Jamming Game with Long-Term Power Constraints: Mixed Strategies

We have already seen that the maximin and minimax solutions of the jamming game when only pure strategies are allowed do not agree, and thus our game has no Nash equilibrium of pure strategies. However, recall that the solution of the minimax problem with pure strategies can often be a good characterization of a practical jamming situation (e.g. when the jammer does not transmit unless it senses that the transmitter is on) and can always serve as a lower bound on the system's performance.

This aside, a Nash equilibrium is still the preferred characterization of jamming games, and since such an equilibrium exists for our problem only when mixed strategies are allowed, the current section is dedicated to the derivation of such a saddlepoint.

Unlike the fast fading scenario of Chapter 2, the frames in our slow-fading parallel-channels model are not equivalent. Each frame is characterized by a different realization of the channel vector $\mathbf{h}$. This is why our present scenario is even more involved than the one in Chapter 2, and requires three levels of power control instead of two.

As before, our approach to the problem is a contradictory one. We study the power control levels starting with the "finest" one, and show that if our conditions for power allocations are not satisfied, then the strategy is suboptimal. The reason why an additional (third) level of power control appears here is a combination of the facts that we study mixed strategies and the frames are not all equivalent as in Chapter 2. Namely, to cover all possible probabilistic strategies, we need to dedicate a level of power control to the power allocation between frames with the same channel realizations (i.e. equivalent frames) and an additional level of power control for the power allocation between frames with different channel realizations. Along with the power allocation within frames, these problems cover all possible cases.

3.4.1 Power Allocation within a Frame

The third level of power control deals with the optimal power allocation between the blocks in a frame, once the transmitter is given the channel vector $\mathbf{h}$ characterizing the frame and allocated power P_M, and the jammer is given the channel vector and its allocated power J_M.

At this point, the third level of power control resembles the two-player, zero-sum game of (3.3) and (3.4) having the mutual information calculated over a frame I_M as cost function. However, none of the players knows the other player's constraints, because (P_M, J_M) is a random event. Theorem 3.11 below provides the optimal transmitter/jammer strategies for power allocation within a frame.

Theorem 3.11. *Given a frame with channel vector* $\mathbf{h}$ *and a realization* (p_M, j_M) *of* (P_M, J_M)*, let* $\mathscr{P}_M(j_M)$ *denote the solution of* Problem 1 *in Section 3.3 with* $J_M = j_M$*, and* $\mathscr{J}_M(p_M)$ *denote the solution of* Problem 2 *in Section 3.3 with* $P_M = p_M$*.*

The transmitter's optimal strategy is the solution of the game in (3.3) and (3.4), where the jammer is constrained to $\frac{1}{M}\sum_{m=1}^{M-1} J_m \leq \mathscr{J}_M(p_M)$ *and the transmitter is constrained to* $\frac{1}{M}\sum_{m=1}^{M-1} P_m \leq p_M$*. The jammer's optimal strategy is the solution of the game in (3.3) and (3.4), where the transmitter is constrained to* $\frac{1}{M}\sum_{m=1}^{M-1} P_m \leq \mathscr{P}_M(j_M)$ *and the jammer is constrained to* $\frac{1}{M}\sum_{m=1}^{M-1} J_m \leq j_M$*.*

Proof. The proof is very similar to the proof of Theorem 5 of Chapter 2 and is deferred to Section 3.9. □

3.4.2 Power Allocation between Frames with the Same Channel Vector

Due to the form of the optimal second level power allocation strategies described in the previous subsection, the probability that a given frame is in outage can be expressed as

$$P_{out,\mathbf{h}} = Pr\{J_M \geq \mathscr{J}_M(P_M)\} = 1 - Pr\{P_M \geq \mathscr{P}_M(J_M)\}, \tag{3.27}$$

where $P_M(j_M)$ is the strictly increasing, unbounded and concave function (see Proposition 3.6) that characterizes the frame. Note that a pair of strategies can only be optimal if $P_{out,\mathbf{h}}$ above is the Nash equilibrium of a jamming game played over the frames characterized by the same channel vector $\mathbf{h}$. This means that if the transmitter and jammer decide to allocate powers $P_{M,\mathbf{h}}$ and $J_{M,\mathbf{h}}$ respectively to frames with channel vector $\mathbf{h}$, they should not allocate the same amount of power to each of these frames. Instead, they should use power levels given by the realizations of two random variables P_M and J_M with distribution functions $(F_P(p_M), F_J(j_M))$ given in the following theorem.

Theorem 3.12. *The unique Nash equilibrium of mixed strategies of the two-player, zero-sum game with average power constraints described by*

$$\min_{F_P(p_M):\mathbf{E}_{F_P}P_M\leq P_M(\mathbf{h})} \max_{F_J(j_M):\mathbf{E}_{F_J}J_M\leq J_M(\mathbf{h})} P_{out,\mathbf{h}}, \tag{3.28}$$

where $\mathbf{E}_{F_P}$ and $\mathbf{E}_{F_J}$ denote expectations with respect to the distributions $F_P(p_M)$ and $F_J(j_M)$, is attained by the pair of strategies $(F_P(p_M), F_J(j_M))$ satisfying:

$$F_P(\mathscr{P}_M(y)) \sim k_p\mathbb{U}([0,2v])(y) + (1-k_p)\Delta_0(y), \tag{3.29}$$

$$F_J(\mathscr{J}_M(x)) \sim k_j\mathbb{U}([0,J_M(2v)])(x) + (1-k_j)\Delta_0(x), \tag{3.30}$$

where $\mathbb{U}([r,t])(\cdot)$ denotes the CDF of a uniform distribution over the interval $[r,t]$, and $\Delta_0(\cdot)$ denotes the CDF of a Dirac distribution (i.e. a step function), and the parameters $k_p, k_j \in [0,1]$ and $v \in [\max\{J_{M,\mathbf{h}}, \mathscr{J}_M(P_{M,\mathbf{h}})/2\}, \infty)$ are uniquely determined from the following steps:

1. *Find the unique value v_0 which satisfies:*

$$P_{M,\mathbf{h}}J_{M,\mathbf{h}} = [\mathscr{P}_M(2v_0) - P_{M,\mathbf{h}}](2v_0 - J_{M,\mathbf{h}}). \tag{3.31}$$

2. *Compute $S(v_0) = \int_0^{2v_0} \mathscr{P}_M(y)dy - 2v_0P_{M,\mathbf{h}}$.*

3. *If $S(v_0) < 0$, then v is the unique solution of*

$$\int_0^{2v} \mathscr{P}_M(y)dy - 2vP_{M,\mathbf{h}} = 0, \tag{3.32}$$

$$k_p = 1 \tag{3.33}$$

and

$$k_j = \frac{J_{M,\mathbf{h}}\mathscr{P}_M(2v)}{2v[\mathscr{P}_M(2v) - P_{M,\mathbf{h}}]}. \tag{3.34}$$

4. *If $S(v_0) = 0$ then $v = v_0$, $k_p = k_j = 1$.*

5. *If $S(v_0) > 0$, then v is the unique solution of*

$$\int_0^{2v} \mathscr{P}_M(y)dy - \mathscr{P}_M(2v)(2v - J_{M,\mathbf{h}}) = 0, \tag{3.35}$$

$$k_p = \frac{2vP_{M,\mathbf{h}}}{\mathscr{P}_M(2v)[2v - J_{M,\mathbf{h}}]} \tag{3.36}$$

and

$$k_j = 1. \tag{3.37}$$

Proof. The proof follows directly from Theorem 2.22 in Section 2.9 of Chapter 2, by substituting $x = P_M$, $y = J_M$, $g(y) = \mathscr{P}_M(y)$, $g^{-1}(x) = \mathscr{J}_M(x)$, $a = P_{M,\mathbf{h}}$ and $b = J_{M,\mathbf{h}}$. It is also interesting to note that the condition $\int_0^b g(y)dy < \lim_{z\to\infty} \int_{g(b)}^{g(z)} g^{-1}(x)dx - b[g(z) - g(b)]$ is satisfied because $\mathscr{P}_M(y)$ is unbounded. □

Particular case: $M = 1$

For $M = 1$ the first (intra-frame) level of power control is inexistent. For a given channel realization h we can readily derive the *affine* function $P_M(j_M)$ in (3.27) as

$$P_M(j_M) = \frac{c-1}{h}(j_M + \sigma_N^2) \tag{3.38}$$

where $c = \exp(R)$. If we use the particularization of the general solution of Theorem 3.12 to affine functions, as in the last part of Section 2.9 of Chapter 2, we obtain the outage probability as

$$P_{out,h} = 1 - \frac{\frac{hP_M(h)}{c-1}}{J_M(h)\left[1+\sqrt{1+2\frac{\sigma_N^2}{J_M(h)}}\right]+\sigma_N^2}$$
$$\text{if } \frac{hP_M(h)}{c-1} \leq \frac{1}{2}J_M(h)\left[1+\sqrt{1+2\frac{\sigma_N^2}{J_M(h)}}\right]+\sigma_N^2, \tag{3.39}$$

and

$$P_{out,h} = \frac{\frac{1}{2}J_M(h)}{\frac{hP_M(h)}{c-1}-\sigma_N^2}$$
$$\text{if } \frac{hP_M(h)}{c-1} > \frac{1}{2}J_M(h)\left[1+\sqrt{1+2\frac{\sigma_N^2}{J_M(h)}}\right]+\sigma_N^2. \tag{3.40}$$

The transmitter and jammer strategies that achieve these payoffs are such that

$$F_P(x) \sim k_p \mathbb{U}([\frac{c-1}{h}\sigma_N^2, 2v\frac{c-1}{h}+\frac{c-1}{h}\sigma_N^2])(x) + (1-k_p)\Delta_0(x),$$

$$F_J(y) \sim \frac{2v}{2v+\sigma_N^2}k_j\mathbb{U}([0,2v])(y) + (1-\frac{2v}{2v+\sigma_N^2}k_j)\Delta_0(y).$$

The parameters $k_p, k_j \in [0,1]$ and $v \in [\max\{J_M(h), \mathscr{J}'_M(P_M(h))/2\}, \infty)$ are uniquely determined from the following steps:

1. If

$$\frac{hP_M(h)}{c-1} \leq \frac{1}{2}J_M(h)\left[1+\sqrt{1+2\frac{\sigma_N^2}{J_M(h)}}\right]+\sigma_N^2, \tag{3.41}$$

then

$$v = \frac{1}{2}J_M(h)\left[1+\sqrt{1+\frac{2\sigma_N^2}{J_M(h)}}\right], \tag{3.42}$$

$$k_p = \frac{2vP_M(h)}{\frac{c-1}{h}(2v+\sigma_N^2)(2v-J_M(h))} \tag{3.43}$$

and

$$k_j = 1. \tag{3.44}$$

2. If

$$\frac{hP_M(h)}{c-1} > \frac{1}{2}J_M(h)\left[1+\sqrt{1+2\frac{\sigma_N^2}{J_M(h)}}\right]+\sigma_N^2, \tag{3.45}$$

then

$$v = \frac{P_M(h) - \frac{c-1}{h}\sigma_N^2}{\frac{c-1}{h}}, \tag{3.46}$$

$$k_p = 1 \tag{3.47}$$

and

$$k_j = \frac{\frac{c-1}{h}J_M(h)(2P_M(h) - \frac{c-1}{h}\sigma_N^2)}{2(P_M(h) - \frac{c-1}{h}\sigma_N^2)^2}. \tag{3.48}$$

The special form of this solution will be used in the next subsection to derive the overall Nash equilibrium of the mixed strategies game for $M = 1$.

3.4.3 Power Allocation between Frames with Different Channel Vectors

In the previous subsections we have described the optimal power control strategies for given particular channel realization $\mathbf{h}$, and transmitter and jammer power levels $P_{M,\mathbf{h}}$ and $J_{M,\mathbf{h}}$ respectively. The first level of power control,which is the subject of this subsection, deals with allocating the powers specified by the transmitter and jammer average power constraints $\mathcal{P}$ and $\mathcal{J}$ between different channel vectors. In other words, we are now concerned with solving the problem

$$\min_{P_M(\mathbf{h}):\mathbf{E_h}P_M(\mathbf{h})\leq\mathcal{P}} \max_{J_M(\mathbf{h}):\mathbf{E_h}J_M(\mathbf{h})\leq\mathcal{J}} \mathbf{E_h}[P_{out,\mathbf{h},P_M(\mathbf{h}),J_M(\mathbf{h})}] \tag{3.49}$$

where $P_{out,\mathbf{h},P_M(\mathbf{h}),J_M(\mathbf{h})}$ (also denoted as $P_{out,\mathbf{h}}$) is the outage probability of a frame characterized by the channel vector $\mathbf{h}$ and to which the transmitter allocates power $P_M(\mathbf{h})$, and the jammer

allocates power $J_M(\mathbf{h})$. Note that $P_{out,\mathbf{h},P_M(\mathbf{h}),J_M(\mathbf{h})}$ can be easily computed according to the second and third levels of power control already presented.

However, the Nash equilibrium of the game in (3.49) above is highly dependent on the result of the second level of power control. Since finding a closed form solution for the second level is still an open problem, a general solution for the first level of power control is not available at this time.

However, we next provide a Nash equilibrium for the particular case when $M = 1$.

Particular case: $M = 1$

We start by pointing out the following important property of the second-level power control strategies for $M = 1$.

Proposition 3.13. *The outage probability $P_{out,h}$ given in (3.39) and (3.40) above is a continuous function of both arguments. Moreover, $P_{out,h}$ is a strictly decreasing, convex function of $P_M(h)$ for fixed $J_M(h)$ and a strictly increasing, concave function of $J_M(h)$ for fixed $P_M(h)$.*

Proof. In the remainder of this section we shall denote the case when $\frac{hP_M(h)}{c-1} \leq \frac{1}{2}J_M(h)\left[1+\sqrt{1+2\frac{\sigma_N^2}{J_M(h)}}\right]+\sigma_N^2$ by *Case 1* and the case when $\frac{hP_M(h)}{c-1} > \frac{1}{2}J_M(h)\left[1+\sqrt{1+2\frac{\sigma_N^2}{J_M(h)}}\right]+\sigma_N^2$ by *Case 2*.

It is straightforward to check that when $\frac{hP_M(h)}{c-1} = \frac{1}{2}J_M(h)\left[1+\sqrt{1+2\frac{\sigma_N^2}{J_M(h)}}\right]+\sigma_N^2$ we get $P_{out,h} = \frac{1}{1+\sqrt{1+2\frac{\sigma_N^2}{J_M(h)}}}$ by using either of the relations in (3.39) or (3.40). Thus, the continuity of $P_{out,h}$ follows immediately.

If we evaluate the derivatives for *Case 1*

$$\frac{dP_{out,h}}{dP_M(h)} = -\frac{\frac{h}{c-1}}{J_M(h)\left[1+\sqrt{1+2\frac{\sigma_N^2}{J_M(h)}}\right]+\sigma_N^2} \tag{3.50}$$

and for *Case 2*

$$\frac{dP_{out,h}}{dP_M(h)} = -\frac{\frac{c-1}{h}J_M(h)}{2(P_M(h)-\frac{c-1}{h}\sigma_N^2)^2} \tag{3.51}$$

we note that when $J_M(h)$ is fixed, $P_{out,h}$ is a strictly decreasing function of $P_M(h)$, affine in *Case 1* and strictly convex in *Case 2*. Moreover, $\frac{dP_{out,h}}{dP_M(h)}$ is continuous, which makes $P_{out,h}$ an overall strictly decreasing, convex function of $P_M(h)$.

Similar (but symmetric) properties hold for the derivatives

$$\frac{dP_{out,h}}{dJ_M(h)} = \frac{\frac{h}{c-1}}{J_M(h)\left[1+\sqrt{1+2\frac{\sigma_N^2}{J_M(h)}}\right]+\sigma_N^2} \cdot \frac{P_M(h)}{J_M(h)\sqrt{1+2\frac{\sigma_N^2}{J_M(h)}}}, \tag{3.52}$$

for *Case 1* and

$$\frac{dP_{out,h}}{dJ_M(h)} = \frac{1}{2}\frac{1}{\frac{h}{c-1}P_M(h)-\sigma_N^2} \tag{3.53}$$

for *Case 2*, yielding $P_{out,h}$ an overall strictly increasing, concave function of $J_M(h)$ (strictly concave in *Case 1* and affine in *Case 2*). □

The result of Proposition 3.13 implies that the overall outage probability $\mathbf{E}_h P_{out,h}$ is a convex function of $\{P_M(h)\}$ for fixed $\{J_M(h)\}$ and a concave function of $\{J_M(h)\}$ for fixed $\{P_M(h)\}$. Since the set of strategies $\{P_M(h), J_M(h)\}$ is convex, there always exists a saddlepoint of the game in (3.49) [39]. The importance of this result should be noted, since it implies that a Nash equilibrium of mixed strategies of the two-person, zero-sum game in (3.49) can be achieved by only looking for pure strategies. Recall that any Nash equilibrium of pure strategies is also a Nash equilibrium of mixed strategies, and that for a two-person, zero-sum game all Nash equilibria share the same value of the cost function [33].

Any saddlepoint of (3.49) has to satisfy the KKT conditions associated with the maximization and minimization problems of (3.49) simultaneously. The next Proposition shows these KKT conditions are not only necessary, but also sufficient for determining a saddlepoint. The proof is deferred to Section 3.9.

Proposition 3.14. *For our two-player, zero-sum game of (3.49), any solution of the joint system of KKT conditions associated with the maximization and minimization problems yields a Nash equilibrium.*

We can now solve the KKT conditions associated with the maximization and minimization problems of (3.49) simultaneously. For *Case 1*, these are

$$-\frac{\frac{h}{c-1}}{J_M(h)\left[1+\sqrt{1+2\frac{\sigma_N^2}{J_M(h)}}\right]+\sigma_N^2}+\lambda-\gamma(h)=0 \tag{3.54}$$

and

$$-\frac{\frac{h}{c-1}}{J_M(h)\left[1+\sqrt{1+2\frac{\sigma_N^2}{J_M(h)}}\right]+\sigma_N^2}\cdot\frac{P_M(h)}{J_M(h)\sqrt{1+2\frac{\sigma_N^2}{J_M(h)}}}+\mu-\delta(h)=0, \tag{3.55}$$

where $\gamma(h)$ and $\delta(h)$ are the complementary slackness conditions satisfying $\gamma(h)P_M(h)=0$ and $\delta(h)J_M(h)=0$, and where $\mu,\ \lambda\ \geq 0$. From (3.55) we get

$$P_M(h)=\frac{\mu}{\lambda}J_M(h)\sqrt{1+2\frac{\sigma_N^2}{J_M(h)}}, \tag{3.56}$$

resulting in

$$J_M(h)=\left[\sqrt{\left(\frac{\lambda}{\mu}\right)^2 P_M(h)^2+\sigma_N^4}-\sigma_N^2\right]_+, \tag{3.57}$$

which in combination with (3.54) yields

$$P_M(h)=\left[\frac{h}{c-1}\frac{\mu}{2\lambda^2}-\frac{\mu(c-1)}{2h}\sigma_N^4\right]_+, \tag{3.58}$$

where we denote $[x]_+=\max\{x,0\}$. Under this solution, the condition for being under *Case 1*,

$$\frac{hP_M(h)}{c-1}\leq\frac{1}{2}J_M(h)\left[1+\sqrt{1+2\frac{\sigma_N^2}{J_M(h)}}\right]+\sigma_N^2 \tag{3.59}$$

translates to

$$\frac{2\mu h}{\lambda(c-1)}\leq 1+\sqrt{1+4\sigma_N^2\mu^2\left(\sigma_N^2+\frac{1}{\mu}\right)}=2(1+\sigma_N^2\mu). \tag{3.60}$$

Note that $P_M(h)=0$ if and only if $J_M(h)=0$, and this happens when $h\leq h_{0/1}$, where

$$h_{0/1}=\lambda(c-1)\sigma_N^2. \tag{3.61}$$

Writing the KKT conditions for *Case 2* under the assumption that $P_M(h),\ J_M(h) \geq 0$ we obtain

$$-\frac{\frac{h}{c-1}J_M(h)}{2\left(\frac{h}{c-1}P_M(h)-\sigma_N^2\right)^2}+\lambda-\gamma(h)=0 \tag{3.62}$$

and

$$-\frac{1}{2\left(\frac{h}{c-1}P_M(h)-\sigma_N^2\right)}+\mu-\delta(h)=0, \tag{3.63}$$

which yield

$$J_M(h)=\frac{c-1}{h}\frac{\lambda}{2\mu^2} \tag{3.64}$$

and

$$P_M(h)=\frac{c-1}{h}\left(\frac{1}{2\mu}+\sigma_N^2\right). \tag{3.65}$$

Note that in this case both $P_M(h)$ and $J_M(h)$ are strictly positive for finite h. Under this solution, the condition for being under *Case 2*,

$$\frac{hP_M(h)}{c-1}>\frac{1}{2}J_M(h)\left[1+\sqrt{1+2\frac{\sigma_N^2}{J_M(h)}}\right]+\sigma_N^2 \tag{3.66}$$

translates to

$$\frac{2\mu h}{\lambda(c-1)}>1+\sqrt{1+4\sigma_N^2\mu^2\frac{h}{\lambda(c-1)}}. \tag{3.67}$$

Forcing the right-hand side of (3.60) to equal the right-hand side of (3.67) we get the value of h which is at the boundary between *Case 1* and *Case 2*:

$$h_{1/2}=\lambda(c-1)(\frac{1}{\mu}+\sigma_N^2). \tag{3.68}$$

A close inspection of the expressions of $P_M(h)$ and $J_M(h)$ for the two cases shows that they are both increasing functions of h under *Case 1* and decreasing functions of h under *Case 2*, and moreover, they are both continuous in $h_{1/2}$. To summarize the results above, the optimal transmitter/jammer first level power control strategies are given in (3.69) and (3.70) below, respectively. The constants λ and μ can be obtained from the power constraints $\mathbf{E}_h P_M(h)=\mathcal{P}$ and $\mathbf{E}_h J_M(h)=\mathcal{J}$.

$$P_M(h) = \begin{cases} 0, & \text{if} \quad h \leq h_{0/1} \\ \frac{h}{c-1}\frac{\mu}{2\lambda^2} - \frac{\mu(c-1)}{2h}\sigma_N^2, & \text{if} \quad h_{0/1} < h \leq h_{1/2} \\ \frac{c-1}{h}\left(\frac{1}{2\mu} + \sigma_N^2\right), & \text{if} \quad h > h_{1/2} \end{cases} \tag{3.69}$$

$$J_M(h) = \begin{cases} 0, & \text{if} \quad h \leq h_{0/1} \\ \sqrt{\left(\frac{\lambda}{\mu}\right)^2 (\frac{h}{c-1}\frac{\mu}{2\lambda^2} - \frac{\mu(c-1)}{2h}\sigma_N^2)^2 + \sigma_N^4} - \sigma_N^2, & \text{if} \quad h_{0/1} < h \leq h_{1/2} \\ \frac{c-1}{h}\frac{\lambda}{2\mu^2}, & \text{if} \quad h > h_{1/2} \end{cases} \tag{3.70}$$

3.4.4 Numerical Results

Figure 3.9 shows the probability of outage obtained under the mixed strategies Nash equilibrium, versus the transmitter power constraint $\mathcal{P}$, when $M = 1$, for a fixed rate $R = 1$, noise power $\sigma_N^2 = 10$, a jammer power constraint $\mathcal{J} = 10$ and a channel coefficient distributed exponentially, with parameter $\lambda = 1/6$. The maximin and minimax solutions of the pure strategies game are shown for comparison.

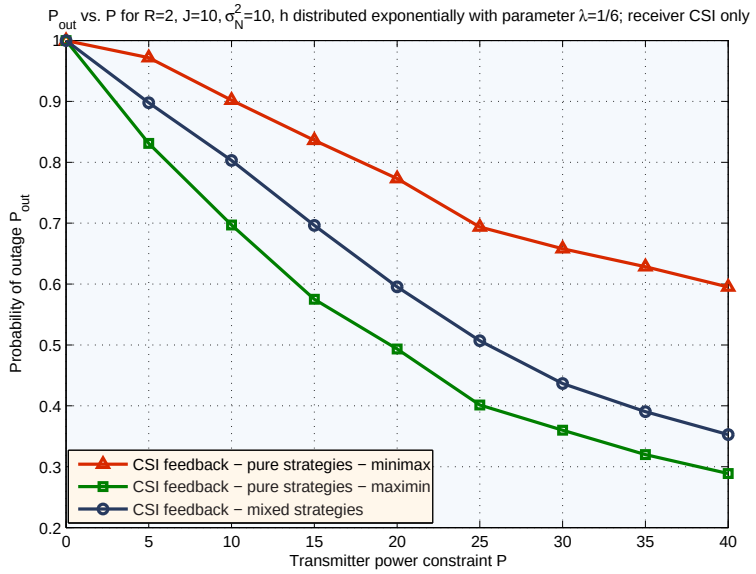

FIGURE 3.9. Outage probability vs. transmitter power constraint $\mathcal{P}$ for $M = 1$ when $\mathcal{J} = 10$, $R = 2$, $\sigma_N^2 = 10$ and h is distributed exponentially, with parameter $\lambda = 1/6$.

As expected, the solution of the of mixed strategies game is better (from the transmitter's point of view) than the minimax and worse than the maximin solutions of the pure strategies game.

3.5 CSI Available Receiver Only. Jamming Game with Long-Term Power Constraints: Mixed Strategies

In this section we investigate the scenario when the receiver does not feed back any channel state information. Since we have already shown that the problem with long-term power constraints is the more interesting and challenging one, and since the purpose of this section is to offer a comparison with previous results, we further focus only on the scenario of average power constraints and mixed strategies.

Unlike in the corresponding Section 2.5 of Chapter 2, where all frames were equivalent because of the fast fading channel, in our present scenario each frame is characterized by a particular channel realization. Since this channel realization is not known to either the transmitter or the jammer, they both have to allocate some power over each frame, in a random fashion, such that the transmitter minimizes and the jammer maximizes the probability that the mutual information over the frame is less than the transmission rate R. In its most general form, the game can be written as

$$\min_{P_M:\mathbf{E}P_M\leq\mathcal{P}}\max_{J_M:\mathbf{E}J_M\leq\mathcal{J}}\mathbf{E}_{P_M,J_M}$$
$$\left[\min_{P_m:\sum P_m\leq MP_M}\max_{J_m:\sum J_m\leq J_M} Pr\{\sum_{m=0}^{M-1}\log\left(1+\frac{P_m h_m}{J_m+\sigma_N^2}\right)\leq MR\}\right], \tag{3.71}$$

where $\mathbf{E}_{P_M,J_M}$ denotes statistical expectation with respect to the probability distribution of P_M and J_M. The form of (3.71) suggests two levels of power control: a first one which deals with the allocation of power between different frames, and a second one which allocates the powers within each frame.

In solving the game, we start as before with the second level of power control. However, this level requires an exact expression of $Pr\{\sum_{m=0}^{M-1}\log\left(1+\frac{P_m h_m}{J_m+\sigma_N^2}\right)\leq MR\}$. Note that this probability

depends upon the probability distribution of the channel vector $\mathbf{h}$. A practical way of solving the problem is the following.

Denote $S_m = \log\left(1+\frac{P_m h_m}{J_m+\sigma_N^2}\right)$ the random variable (depending on h_m) which characterizes the instant mutual information over the m-th block of the frame. We can write the cumulative distribution function (c.d.f.) of S_m as

$$F_{S_m}(x) = Pr\{S_m \leq x\} = Pr\{h_m \leq (e^x-1)\frac{J_m+\sigma_N^2}{P_m}\} = F_h\left((e^x-1)\frac{J_i+\sigma_N^2}{P_i}\right) \quad (3.72)$$

where $F_h(x)$ is the c.d.f. of the channel coefficient h_m and we assume that the channel coefficients over all the blocks of a frame are independent and identically distributed random variables.

We can now compute the p.d.f. (assuming it exists) of S_m as

$$f_{S_m}(x) = \frac{dF_{S_m}(x)}{dx} = \frac{dF_h\left((e^x-1)\frac{J_m+\sigma_N^2}{P_m}\right)}{dx}. \quad (3.73)$$

Finally, our probability can be written as

$$Pr\{\sum_{m=0}^{M-1}\log\left(1+\frac{P_m h_m}{J_m+\sigma_N^2}\right) \leq MR\} = \left(F_{S_0} * f_{S_1} * \ldots * f_{S_{M-1}}\right)(MR) \quad (3.74)$$

where $*$ denotes regular convolution. Due to the intricate expression of this probability, as well as its dependence on the statistical properties of the channel, we next focus exclusively on the simple case when $M=1$.

Particular case: $M=1$

For $M=1$, we are only concerned with the first level of power control. The game can be written as

$$\min_{P_M:\mathbf{E}P_M\leq\mathcal{P}}\max_{J_M:\mathbf{E}J_M\leq\mathcal{J}} \mathbf{E}_{P_M,J_M} Pr\{P \leq (c-1)\frac{J_M+\sigma_N^2}{h}\} \quad (3.75)$$

or equivalently,

$$\min_{P_M:\mathbf{E}P_M\leq\mathcal{P}}\max_{J_M:\mathbf{E}J_M\leq\mathcal{J}} \mathbf{E}_{P_M,J_M} Pr\{h \leq (c-1)\frac{J_M+\sigma_N^2}{P_M}\}. \quad (3.76)$$

In order to provide a good numerical comparison with the results of the previous sections, assume that the channel coefficient h has an exponential probability distribution with parameter λ. Its cumulative distribution function can thus be written as $F(h) = 1 - e^{-\lambda h}$, which enables us to write

$$Pr\{h \leq (c-1)\frac{J_M + \sigma_N^2}{P_M}\} = 1 - \exp\left[-\lambda(c-1)\frac{J_M + \sigma_N^2}{P_M}\right]. \tag{3.77}$$

Denote $H(P_M, J_M) = 1 - \exp\left[-\lambda(c-1)\frac{J_M+\sigma_N^2}{P_M}\right]$.

By computing the derivatives

$$\frac{dH}{dP_M} = -\lambda(c-1)\frac{J_M + \sigma_N^2}{P_M^2}\exp\left[-\lambda(c-1)\frac{J_M + \sigma_N^2}{P_M}\right] < 0, \tag{3.78}$$

$$\frac{d^2H}{dP_M^2} = \lambda(c-1)\frac{J_M + \sigma_N^2}{P_M^3}\left[\lambda(c-1)\frac{J_M + \sigma_N^2}{P_M} + 2\right]\exp\left[-\lambda(c-1)\frac{J_M + \sigma_N^2}{P_M}\right] > 0, \tag{3.79}$$

$$\frac{dH}{dJ_M} = \lambda(c-1)\frac{1}{P_M}\exp\left[-\lambda(c-1)\frac{J_M + \sigma_N^2}{P_M}\right] > 0, \tag{3.80}$$

and

$$\frac{d^2H}{dJ_M^2} = -(\lambda(c-1)\frac{1}{P_M})^2\exp\left[-\lambda(c-1)\frac{J_M + \sigma_N^2}{P_M}\right] < 0, \tag{3.81}$$

we notice that H is a strictly decreasing, convex function of P_M for a fixed J_M, and a strictly increasing, concave function of J_M for a fixed P_M. Hence, a Nash equilibrium is achieved by uniformly distributing the transmitter's and jammer's powers between the frames:

$$\begin{aligned}\mathbf{E}_{P_M:\mathbf{E}P_M\leq\mathcal{P}}\left\{1 - \exp\left[-\lambda(c-1)\frac{\mathcal{J} + \sigma_N^2}{P_M}\right]\right\} &\leq 1 - \exp\left[-\lambda(c-1)\frac{\mathcal{J} + \sigma_N^2}{\mathcal{P}}\right] \leq \\ &\leq \mathbf{E}_{J_M:\mathbf{E}J_M\leq\mathcal{J}}\left\{1 - \exp\left[-\lambda(c-1)\frac{J_M + \sigma_N^2}{\mathcal{P}}\right]\right\}\end{aligned} \tag{3.82}$$

This saddlepoint is an equilibrium of pure strategies, and hence also an equilibrium of mixed strategies. Note that the existence of such an equilibrium of pure strategies might no longer hold

for different probability distributions of h, and this would demand a search for purely probabilistic strategies. For example, when the c.d.f. of the channel coefficient $F(h)$ is not concave, then $F((c-1)\frac{J_M+\sigma_N^2}{P_M})$ is no longer a concave function of J_M, and hence the optimal jammer strategy is not deterministic.

Numerical evaluations of the system's performance under the present scenario are presented in the next subsection.

3.5.1 Numerical Results

The probability of outage as a function of the transmitter's power constraint $\mathcal{P}$ is shown in Figure 3.10 for $M = 1$, and under the assumption that both the transmitter and the jammer distribute their powers uniformly over the frames.

For comparison, the maximin and minimax solutions of the pure strategies game and the mixed strategies Nash equilibrium, all under the scenario that channel state information is fed back by the receiver, are also shown in the figure.

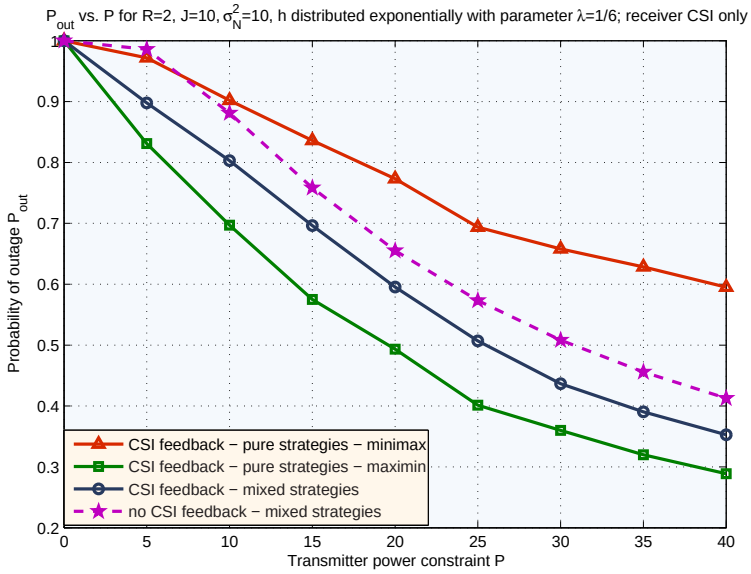

FIGURE 3.10. Outage probability vs. transmitter power constraint $\mathcal{P}$ for $M = 1$, with and without CSI feedback when $\mathcal{J} = 10$, $R = 2$, $\sigma_N^2 = 10$ and h is distributed exponentially, with parameter $\lambda = 1/6$. (Mixed strategies.)

Note that when the receiver does not feed back the CSI, the system performance suffers degradation. Unlike in the fast fading scenario of Chapter 2, in the present slow fading scenario the increase in the outage probability is significant. The difference is most visible at low transmitter powers, when not feeding back the channel state information amounts to worse performance than the pessimistic (minimax) scenario with full CSI.

3.6 Conclusions

We have studied the jamming game over slow fading channels, with the outage probability as objective. Similarly to the fast fading scenario, the game with full CSI and average (or long term) power constraints does not have a Nash equilibrium of pure strategies. Nevertheless, we derived the minimax and maximin solutions of pure strategies, which provide lower and upper bounds on the system performance, respectively.

In addition, we investigated the Nash equilibrium of mixed strategies. Compared to the fast fading scenario Chapter 2, the Nash equilibrium for the slow fading, full CSI game is much more involved. The difference comes from the fact that frames are not equivalent. In fact, instead of being characterized by the channel statistics as in Chapter 2, the frames are now characterized by different channel realizations. This results in the existence of an additional third level of power control.

We also showed that for parallel slow fading channels, the CSI feedback helps in the battle against jamming, since if the receiver does not feed back the channel state information, the system's performance suffers a significant degradation. We expect this degradation to decrease as the number of parallel channels M increases, until it becomes marginal for $M \to \infty$ (which can be considered as the case in Chapter 2).

These results, along with our conclusions from Chapter 2, reveal an interesting duality between the ways that different communication models behave with and without jamming. As remarked in Chapter 2, under a fast fading channel with jamming, the feedback of channel state information

brings little benefits in terms of the overall probability of outage. The same tendency is observed for the fast fading channel without jamming in [35] (although the performance measure therein is the ergodic capacity). However, [32] shows that for a parallel slow fading channel, the CSI feedback is quite important. The improvement of the probability of outage when the channel coefficients are perfectly known to the transmitter is no longer negligible. The results of this chapter demonstrate that even in the presence of a jammer (which can eavesdrop the feedback channel and hence obtain the same CSI as the transmitter), CSI feedback improves the transmission considerably.

3.7 Additional Results for Short-Term Power Constraints - Proofs of Main Results

3.7.1 Proof of Proposition 3.1

The proof is an adaptation of the results in Section IV.B of [9], regarding uncorrelated jamming with CSI at the transmitter. The only difference is that in our case, the power constraints and cost function involve short-term, temporal averages, while in [9], they are expressed in terms of statistical averages. Nevertheless, the same techniques can be applied.

The set of all pairs $(P(h), J(h))$ satisfying the power constraints is convex, since the power constraints are linear functions of $P(h)$ and $J(h)$, respectively. Moreover, the cost function

$$I_M(\mathbf{h}, P(h), J(h)) = \frac{1}{M}\sum_{m=0}^{M-1}\log(1+\frac{h_m P_m}{\sigma_N^2 + J_m})$$

is a convex function of $J(h)$ for fixed $P(h)$, and a concave function of $P(h)$ for fixed $J(h)$. These properties imply that there exists at least one saddle point of the game.

Writing the KKT conditions for both optimization problems we get [9]:

$$-\frac{h}{\sigma_N^2 + J(h) + hP(h)} + \lambda - \gamma(h) = 0 \tag{3.83}$$

and

$$-\frac{hP(h)}{(\sigma_N^2 + J(h))(\sigma_N^2 + J(h) + hP(h))} + \nu - \delta(h) = 0, \tag{3.84}$$

where $\gamma(h)$ and $\delta(h)$ are the complementary slackness variables for $P(h)$ and $J(h)$, respectively.

The three possible cases are [9]: Case 1: $P(h) > 0$, $J(h) > 0$; Case 2: $P(h) > 0$, $J(h) = 0$ and Case 3: $P(h) = J(h) = 0$.

For Case 1 both complementary slackness variables are 0, and solving (3.83) and (3.84) together we get

$$\frac{\lambda}{\mu} = \frac{J(h) + \sigma_N^2}{P(h)}, \tag{3.85}$$

and

$$P(h) = \frac{h}{\lambda(h + \lambda/\mu)}, \tag{3.86}$$

while for Cases 2 and 3, the solution is plain water-filling [9].

These considerations result in the solutions (3.5) and (3.6).

3.7.2 Proof of Theorem 3.2

This proof follows the one described in the Appendix B of [32]. The probability of outage can be written as:

$$Pr(I_M(\mathbf{h}, P(h), J(h)) < R) = E[\chi_{\{I_M(\mathbf{h}, P(h), J(h)) < R\}}], \tag{3.87}$$

where $\chi_{\{\mathscr{A}\}}$ denotes the indicator function of the set $\mathscr{A}$. Replacing the power allocations by the solutions of the game described by (3.3) and (3.4), we define

$$\chi^*(\mathbf{h}) = \chi_{\{I_M(\mathbf{h}, P^*(h), J^*(h)) < R\}}. \tag{3.88}$$

Then the region $\mathcal{U}(R, \mathcal{P}, \mathcal{J})$ can be written as:

$$\mathcal{U}(R, \mathcal{P}, \mathcal{J}) = \{\mathbf{h} \in \mathbb{R}_+^M : \chi^*(\mathbf{h}) = 0\}. \tag{3.89}$$

We next use the fact that the pair $(P^*(h), J^*(h))$ determines an equilibrium of the game (3.3), (3.4). Thus, for any random power allocation $P(h)$ satisfying the power constraint, we can write:

$$\chi^*(\mathbf{h}) \leq \chi_{\{I_M(\mathbf{h}, P(h), J^*(h)) < R\}}, \text{ with probability } 1. \tag{3.90}$$

Similarly, for any random $J(h)$, we have

$$\chi^*(\mathbf{h}) \geq \chi_{\{I_M(\mathbf{h},P^*(h),J(h))<R\}}, \text{ with probability } 1. \tag{3.91}$$

Now pick some arbitrary power allocation functions $P_a(h)$ and $J_a(h)$, which satisfy the short-term power constraints, and set

$$\widehat{P}(h) = (1-\chi^*(\mathbf{h}))P^*(h) + \chi^*(\mathbf{h})P_a(h), \tag{3.92}$$

and

$$\widehat{J}(h) = (1-\chi^*(\mathbf{h}))J_a(h) + \chi^*(\mathbf{h})J^*(h), \tag{3.93}$$

It is easy to see that $1/M\sum_{m=0}^{M-1}\widehat{P}(h_m) \leq \mathcal{P}$ with probability 1 , $1/M\sum_{m=0}^{M-1}\widehat{J}(h_m) \leq \mathcal{J}$ with probability 1, and moreover that

$$\chi^*(\mathbf{h}) = \chi_{\{I_M(\mathbf{h},\widehat{P}(h),\widehat{J}(h))<R\}}. \tag{3.94}$$

Note that transmitter and jammer could pick $P_a(h) = 0$ and $J_a(h) = 0$ respectively, but this strategy would not improve their performances (power cannot be saved), since the only power constraints are set over frames.

Now, using (3.87), (3.90) and (3.91), we get:

$$Pr(I_M(\mathbf{h},P(h),\widehat{J}(h)) < R) \geq Pr(I_M(\mathbf{h},\widehat{P}(h),\widehat{J}(h)) < R) \geq Pr(I_M(\mathbf{h},\widehat{P}(h),J(h)) < R), \tag{3.95}$$

which proves the existence of a Nash equilibrium of the original game.

3.8 Additional Results for Long-Term Power Constraints: Pure Strategies

3.8.1 Proof of Proposition 3.3

Take *Problem 1*. Let $(\mathfrak{P}^*,\mathfrak{J}^*) = \big((P_0^*,P_1^*,\ldots,P_{M-1}^*),(J_0^*,J_1^*,\ldots,J_{M-1}^*)\big)$ be a solution such that $\sum_{m=0}^{M-1}P_m^* = P_{M,1}$ and $\sum_{m=0}^{M-1}J_m^* = J_{M,1}$, and assume that $I_M(\mathfrak{P}^*,\mathfrak{J}^*) > R$. Since I_M is a

continuous, strictly increasing function of P_0, without loss of generality, we can find $P_0' < P_0^*$ such that $I_M((P_0', P_1^*, \ldots, P_{M-1}^*), \mathfrak{J}^*) = R$.

But then $P_0' + \sum_{m=1}^{M-1} P_m^* < MP_{M,1}$, which means that $(\mathfrak{P}^*, \mathfrak{J}^*)$ is suboptimal (from the transmitter's point of view), and hence not a solution.

Therefore, the first constraint $I_M \geq R$ has to be satisfied with equality, i.e. $I_M = R$.

Now take the solution $(\mathfrak{P}^*, \mathfrak{J}^*)$, and assume that $\frac{1}{M}\sum_{m=0}^{M-1} J_m^* < J_M$. Then we can find $J_0' > J_0^*$, such that $J_0' + \sum_{m=1}^{M-1} J_m^* = MJ_M$. In order for the first constraint $I_M = R$ to be satisfied, the value and distribution of P_M will have to be modified.

We prove next that the value of P_M should be increased, which makes the pair $(\mathfrak{P}^*, \mathfrak{J}^*)$ suboptimal (from the jammer's point of view), thus contradicting the hypothesis that it is a solution, and proving that the second constraint should hold with equality.

Assume there is a distribution $\mathfrak{P}'' = (P_0'', P_1'', \ldots, P_{M-1}'')$ that minimizes P_M, under the constraint $I_M(\{P_m\}, (J_0', J_1^*, \ldots, J_{M-1}^*)) = R$, such that

$$\sum_{m=0}^{M-1} P_m'' \leq P_{M,1}. \tag{3.96}$$

Then, replacing J_0 by its old value J_0^*, we have that $(\mathfrak{P}'', \mathfrak{J}^*)$ is either a second solution of Problem 1 (if (3.96) is satisfied with equality), or a better choice (if (3.96) is satisfied with strict inequality). We can readily dismiss the latter case. For the former case, I_M is a strictly decreasing function of J_0, thus $I_M(\mathfrak{P}'', \mathfrak{J}^*) > R$, which contradicts the first part of this proof. The same arguments work for *Problem 2*.

3.8.2 Proof of Proposition 3.4

Proposition 3.4 is a direct consequence of Theorem 2.21 in the Section 2.8.4 of Chapter 2. We restate the theorem here for completeness. For a complete proof, see Chapter 2.

Theorem 3.15. *Take $x, y \in L^2[\mathbb{R}]$ and define the order relation $x > y$ if and only if $x(t) > y(t)\ \forall t \in \mathbb{R}$. Consider the continuous real functions $f(x)$, $g(y)$ and $h(x, y)$ over $L^2[\mathbb{R}]$, such that*

f is a strictly increasing function of x, g is a strictly increasing function of y, and h is a strictly increasing function of x for fixed y and a strictly decreasing function of y for fixed x.

Define the following minimax and maximin problems:

$$\max_{y\geq 0}\left[\min_{x\geq 0} f(x) \text{ s.t. } h(x,y)\geq H\right] \text{ s.t.} g(y)\leq G, \tag{3.97}$$

$$\max_{x\geq 0}\left[\min_{y\geq 0} g(y) \text{ s.t. } h(x,y)\leq H\right] \text{ s.t.} f(x)\leq F, \tag{3.98}$$

$$\min_{y\geq 0}\left[\max_{x\geq 0} h(x,y) \text{ s.t. } f(x)\leq F\right] \text{ s.t.} g(y)\leq G. \tag{3.99}$$

(I) Choose any real values for G and H. Take problem (3.97) under these constraints and let the pair (x_1, y_1) denote one of its optimal solutions, yielding a value of the objective function $f(x_1) = F_1$. If we set the value of the corresponding constraints in problems (3.98) and (3.99) to $F = F_1$, then the values of the objective functions of problems (3.98) and (3.99) under their optimal solutions are $g(y) = G$ and $h(x, y) = H$, respectively. Moreover, (x_1, y_1) is also an optimal solution of all problems.

(II) Choose any real values for F and H. Take problem (3.98) under these constraints and let the pair (x_2, y_2) denote one of its optimal solutions, yielding a value of the objective function $g(y_2) = G_2$. If we set the value of the corresponding constraints in problems (3.97) and (3.99) to $G = G_2$, then the values of the objective functions of problems (3.97) and (3.99) under their optimal solutions are $f(x) = F$ and $h(x, y) = H$, respectively. Moreover, (x_2, y_2) is an optimal solution of all problems.

(III) Choose any real values for F and G. Take problem (3.99) under these constraints and let the pair (x_3, y_3) denote one of its optimal solutions, yielding a value of the objective function $h(x_3, y_3) = H_3$. If we set the value of the corresponding constraints in problems (3.97) and (3.98)

to $H = H_3$, then the values of the objective functions of problems (3.97) and (3.98) under their optimal solutions are $f(x) = F$ and $g(y) = G$, respectively. Moreover, (x_3, y_3) is an optimal solution of all problems.

3.8.3 Proof of Proposition 3.5

Take *Problem 1*. By Proposition 3.4, if there exists $P_{M,1}$ such that solving the game in (3.3) and (3.4) with the constraint $\sum_{m=1}^{M-1} P_m \leq M P_{M,1}$ yields the objective $I_M(\mathbf{h}, \{P_m\}, \{J_m\}) = R$, then the solution of *Problem 1* coincides with the solution of the game in (3.3) and (3.4).

We write this solution as in (3.5) and (3.6), but we denote $\lambda = 1/\eta$ and $\mu = \nu/\eta$:

$$P_m^* = \begin{cases} (\lambda - \frac{\sigma_N^2}{h_m})^+ & \text{if} \quad h_m < \frac{\sigma_N^2}{\lambda - \sigma_N^2 \mu} \\ \mu \frac{\lambda h_m}{1+\mu h_m} & \text{if} \quad h_m \geq \frac{\sigma_N^2}{\lambda - \sigma_N^2 \mu} \end{cases} \tag{3.100}$$

$$J_m^* = \begin{cases} 0 & \text{if} \quad h_m < \frac{\sigma_N^2}{\lambda - \sigma_N^2 \mu} \\ \frac{\lambda h_m}{1+\mu h_m} - \sigma_N^2 & \text{if} \quad h_m \geq \frac{\sigma_N^2}{\lambda - \sigma_N^2 \mu} \end{cases} \tag{3.101}$$

where λ and μ are constants that can be determined from the constraints $\sum_{m=1}^{M-1} J_m = M J_M$ and $\sum_{m=1}^{M-1} I(h_m, P_m, J_m) = MR$.

We shall use the following conventions and denotations:

- Without loss of generality, we shall assume that the blocks in a frame are indexed in increasing order of their channel coefficients. That is, $h_0 \leq h_1 \leq \ldots, \leq h_{M-1}$.
- Denote $x_m = J_m + \sigma_N^2$ and $x_m^* = J_m^* + \sigma_N^2$. Note that $\frac{x_0^*}{h_0} \geq \frac{x_1^*}{h_1} \geq \ldots, \geq \frac{x_{M-1}^*}{h_{M-1}}$.
- Denote by h_p the first block on which the transmitter's power is strictly positive, and by h_j the first block on which the jammer's power is strictly positive. Note that $h_p \leq h_j$.

Note that

$$P_m^* = \left[\lambda - \frac{x_m^*}{h_m}\right]_+ \tag{3.102}$$

for all $m \in \{0, 1, \ldots, M-1\}$, where $[z]_+ = \max\{z, 0\}$.

Given these and (3.100) and (3.101) above, we can write:

$$\frac{\sigma_N^2}{h_p} \leq \lambda < \frac{\sigma_N^2}{h_{p-1}}, \tag{3.103}$$

$$\sigma_N^2 \frac{1+\mu h_j}{h_j} \leq \lambda < \sigma_N^2 \frac{1+\mu(h_{j-1})}{h_{j-1}}, \tag{3.104}$$

$$MR = \sum_{m=p}^{j-1} \log\left(\frac{\lambda h_m}{\sigma_N^2}\right) - \sum_{m=j}^{M-1} \log\left(\frac{1}{1+\mu h_m}\right), \tag{3.105}$$

Denote by $Q_U[h]$ denotes the index of the smallest channel coefficient in the frame that is larger than h. With this notation, we can write

$$p \geq Q_U\left[\frac{h_{j-1}}{1+\mu h_{j-1}}\right] \tag{3.106}$$

$$h_{p-1} < \frac{h_j}{1+\mu h_j} \tag{3.107}$$

$$\frac{1}{M}\sum_{m=j}^{M-1}\left[\frac{\frac{h_m}{1+\mu h_m}}{\frac{h_j}{1+\mu h_j}} - 1\right] \leq \frac{J_M}{\sigma_N^2} \leq \frac{1}{M}\sum_{m=j}^{M-1}\left[\frac{\frac{h_m}{1+\mu h_m}}{\frac{h_{j-1}}{1+\mu h_{j-1}}} - 1\right], \tag{3.108}$$

$$\sum_{m=Q_U\ \frac{h_j}{1+\mu h_j}}^{j-1} \log\left(h_m \frac{1+\mu h_j}{h_j}\right) - \sum_{m=j}^{M-1} \log\left(\frac{1}{1+\mu h_m}\right) \leq MR \leq$$

$$\leq \sum_{m=Q_U\ \frac{h_{j-1}}{1+\mu h_{j-1}}}^{j-1} \log\left(h_m \frac{1+\mu(h_{j-1})}{h_{j-1}}\right) - \sum_{j}^{M-1} \log\left(\frac{1}{1+\mu h_m}\right), \tag{3.109}$$

where (3.108) follows from $J_M = \sum_{m=j}^{M-1} \left[\frac{\lambda h_m}{1+\mu h_m} - \sigma_N^2 \right]$, and the first inequality in (3.109) follows since $h_{p-1} < \frac{h_j}{1+\mu h_j}$ implies $p \leq Q_U \left[\frac{h_j}{1+\mu h_j} \right]$ because there is no other channel coefficient between h_{p-1} and h_p.

It is straightforward to show that for fixed h_j the left-most and the right-most terms of inequality (3.108) are strictly decreasing functions of μ, while the left-most and the right-most terms of inequality (3.109) are strictly increasing functions of μ.

Note that

$$\sum_{m=j}^{M-1} \left[\frac{\frac{h_m}{1+\mu h_m}}{\frac{h_j}{1+\mu h_j}} - 1 \right] = \sum_{m=j+1}^{M-1} \left[\frac{\frac{h_m}{1+\mu h_m}}{\frac{h_j}{1+\mu h_j}} - 1 \right], \tag{3.110}$$

and

$$\begin{aligned} \sum_{m=Q_U \frac{h_j}{1+\mu h_j}}^{j-1} \log\left(h_m \frac{1+\mu h_j}{h_j} \right) - \sum_{m=j}^{M-1} \log\left(\frac{1}{1+\mu h_m} \right) = \\ = \sum_{m=Q_U \frac{h_j}{1+\mu h_j}}^{j} \log\left(h_m \frac{1+\mu h_j}{h_j} \right) - \sum_{m=j+1}^{M-1} \log\left(\frac{1}{1+\mu h_m} \right). \end{aligned} \tag{3.111}$$

That is, by keeping μ constant and replacing h_j by h_{j-1} in both first terms of (3.108) and (3.109), we get exactly the last terms of (3.108) and (3.109), respectively.

Finally, we take a contradictory approach. Suppose there exist two different pairs (h_{j1}, μ_1) and (h_{j2}, μ_2) that satisfy both (3.108) and (3.109) and assume, without loss of generality that $h_{j1} < h_{j2}$. Then, in order for (h_{j2}, μ_2) to satisfy (3.108) we need $\mu_2 > \mu_1$, while in order for (h_{j2}, μ_2) to satisfy (3.109) we need $\mu_< \mu_1$. Thus h_j is unique. Note however that the relations above do not guarantee the uniqueness of μ.

For the optimal h_j, the constraint $\sum_{m=1}^{M-1} J_m = M J_M$ translates to

$$\sum_{m=j}^{M-1} \frac{\lambda h_m}{1+\mu h_m} = M J_M + (M-j)\sigma_N^2. \tag{3.112}$$

while the constraint $I_M(\mathbf{h}, \{P_m\}, \{J_m\}) = R$ is already given in (3.105). The left hand side of (3.112) is a strictly increasing function of λ for fixed μ and a strictly decreasing function of μ for fixed λ, while being equal to a constant.

Again, for a contradictory approach, suppose there exist two different pairs of (μ_1, λ_1) and (μ_2, λ_2) that can generate different solutions. If we assume, without loss of generality that $\mu_1 > \mu_2$, then, in order for (3.112) to be satisfied by both pairs, we need $\lambda_1 > \lambda_2$. But this can only mean that under (μ_2, λ_2) the transmitter allocates non-zero power to more channel coefficients than under (μ_1, λ_1). This remark simply says that the index p at which the transmitter starts transmitting is a decreasing function of λ, and can easily be verified by (3.102). Looking now at (3.105), we observe that its right hand side is a strictly increasing function of λ for fixed μ and a strictly increasing function of μ for fixed λ, while being equal to a constant. In other words, if (3.105) is satisfied by the pair (μ_1, λ_1), then it cannot also be satisfied by (μ_2, λ_2). Thus, the pair (λ, μ) that satisfies both (3.105) and (3.112) is also unique. But once h_j, λ and μ are given, h^p is uniquely determined. Therefore there cannot exist more than one solution to *Problem1*. Similar arguments can be applied to show that the solution of *Problem2* is unique.

3.8.4 Proof of Proposition 3.6

Since the solution is unique, it follows that $\mathscr{P}_M(J_M)$ is a strictly increasing function. By closely inspecting the form of the solution in (3.100) and (3.101), it is straightforward to see that if $J_M \to \infty$, then $J_m \to \infty$ for all $m \in \{0, 1, \ldots, M-1\}$. If the required P_M were finite, this would imply $I_M \to 0$, which violates the power constraints of *Problem 1*. For *Problem 1* we prove that the resulting $\mathscr{P}_M(J_M)$ function is continuous and concave in several steps. We first show in Lemma 3.16 that the optimal jammer strategy $\{x_m^*\}_{m=0}^{M-1}$ is a continuous function of the given jamming power J_M. Lemma 3.17 proves that $P_M(\{x_m\})$ is continuous and has continuous first order derivatives. This implies that $P_M(J_M)$ is in fact continuous and has a continuous first order derivative. Finally, Lemma 3.18 shows that for any fixed h_p and h_j the function $P_M(J_M)$ is concave.

Lemma 3.16. *The optimal jammer power allocation $\{x_m^*\}_{m=0}^{M-1}$ within a frame is a continuous increasing function of the given jamming power J_M invested over that frame.*

Proof. It is clear that x_m^* is continuous and increasing as a function of J_M if h_p and h_j are fixed. At any point where either h_p or h_j change as a result of a change in J_M, the optimal jamming strategy $\{x_m^*\}_{m=0}^{M-1}$ maintains continuity as a result of the uniqueness of the solution (Proposition 3.5). □

Lemma 3.17. *Both $P_M(\{x_m\})$ and the derivatives $\frac{dP_M}{dx_m}$ are continuous functions of $\{x_m\}_{m=0}^{M-1}$.*

Proof. Consider any two points $\mathfrak{X}_1 = (x_{1,m})_{m=0}^{M-1}$ and $\mathfrak{X}_2 = (x_{2,m})_{m=0}^{M-1}$ and any trajectory $\mathfrak{T}$ that connects them.

For a given vector $\mathfrak{X} = (x_m)_{m=0}^{M-1}$, the required transmitter power is

$$P_M = \frac{M-p}{M}\left(\frac{c}{\left(\prod_{m=p}^{M-1} h_m\right)}\right)^{\frac{1}{M}}\left(\prod_{m=p}^{M-1} x_m\right)^{\frac{1}{M}} - \frac{1}{M}\sum_{m=p}^{M-1}\frac{x_m}{h_m}. \tag{3.113}$$

Note that p depends upon the choice of $\mathfrak{X}$. For fixed p, the continuity and differentiability of $P_M(\mathfrak{X})$ are obvious. Thus, it suffices to show that these properties also hold in a point of $\mathfrak{T}$ where p changes.

If we can show continuity and differentiability when p is decreased by 1, then larger variations of p can be treated as multiple changes by 1, and continuity still holds.

Recall the assumption that the channel coefficients are always indexed in decreasing order of the quantities $\frac{x_m}{h_m}$. Let $\mathfrak{X}_k = (x_{k,m})_{m=0}^{M-1}$ be a point of $\mathfrak{T}$ where the transmitter decreases the index of the block over which it starts to transmit from p_k to $p_k - 1$, and denote by $\mathfrak{T}_1$ the part of the trajectory $\mathfrak{T}$ that is between $\mathfrak{X}_1$ and $\mathfrak{X}_k$, and $\mathfrak{T}_2 = \mathfrak{T} \setminus \mathfrak{T}_1$.

Since $P_{p_k-1} = 0$, we know that λ does not change in this point, since

$$\frac{1}{M}\sum_{m=p}^{M-1}\left[\lambda - \frac{x_m}{h_m}\right] = \frac{1}{M}\sum_{m=p-1}^{M-1}\left[\lambda - \frac{x_m}{h_m}\right] = P_M. \tag{3.114}$$

Define the "left" and "right" limits $P_M(\mathfrak{X}_k-)$ and $P_M(\mathfrak{X}_k+)$ as:

$$P_M(\mathfrak{X}_k-) = \lim_{\substack{\mathfrak{X}\to\mathfrak{X}^k \\ \mathfrak{X}\in\mathfrak{T}_1}} P_M(\mathfrak{X}), \tag{3.115}$$

$$P_M(\mathfrak{X}_k+) = \lim_{\substack{\mathfrak{X}\to\mathfrak{X}^k \\ \mathfrak{X}\in\mathfrak{T}_2}} P_M(\mathfrak{X}). \tag{3.116}$$

Since $\mathbb{R}_+^M$ is Hausdorff [40], there exists a small enough neighborhood $\mathfrak{U} \subset \mathbb{R}_+^M$ of $\mathfrak{X}_k$, such that $p(\mathfrak{X}) = p_k$ to the "left" and $p(\mathfrak{X}) = p_k - 1$ to the "right" of $\mathfrak{X}_k$ on $\mathfrak{U}$. We can now write:

$$P_M(\mathfrak{X}_k+) = \lambda\frac{M-p_k+1}{M} - \frac{1}{M}\sum_{m=p_k-1}^{M-1}\frac{x_{k,m}}{h_m} =$$

$$= \lambda\frac{M-p_k}{M} - \frac{1}{M}\sum_{m=p_k}^{M-1}\frac{x_{k,m}}{h_m} + \frac{1}{M}(\lambda - \frac{x_{k,p_k-1}}{h_{p_k-1}}) = P_M(\mathfrak{X}_k-), \tag{3.117}$$

where the last equality follows because $\lambda = \frac{x_{k,p_k-1}}{h_{p_k-1}}$. This proves continuity.

Similar arguments can be used to show the continuity of the derivatives

$$\frac{dP_M}{dx_n} = \frac{1}{M}\left(\frac{\lambda}{x_n} - \frac{1}{h_n}\right) \tag{3.118}$$

in $\mathfrak{X}_k$ (note that $\frac{\lambda}{x_{k,p_k-1}} = \frac{1}{h_{p_k-1}}$).

Therefore, $P_M(\mathfrak{X})$ is continuous and has first-order derivatives that are continuous along any trajectory $\mathfrak{T}$ between any two points $\mathfrak{X}_1$ and $\mathfrak{X}_2$. □

Finally, for the last part of our proof:

Lemma 3.18. *For fixed p and j, the function $P_M(J_M)$ is concave.*

Proof. We can write

$$MJ_M + (M-j)\sigma_N^2 = \left[c\prod_{m=p}^{j-1}\left(\frac{\sigma_N^2}{h_m}\right)^{\frac{1}{M}} \cdot \prod_{m=j}^{M-1}\left(\frac{1}{1+\mu h_m}\right)^{\frac{1}{M}}\right]^{\frac{M}{j-p}} \sum_{m=j}^{M-1}\frac{h_m}{1+\mu h_m}, \tag{3.119}$$

and denote

$$g(\mu) = \prod_{m=j}^{M-1}\left(\frac{1}{1+\mu h_m}\right)^{\frac{1}{j-p}} \sum_{m=j}^{M-1}\frac{h_m}{1+\mu h_m} \tag{3.120}$$

Note that for fixed p and j, J_M is a linear function of g.

A similar relation can be found for the required transmitter power P_M:

$$MP_M + \frac{1}{M}\sum_{m=p}^{j-1}\frac{\sigma_N^2}{h_m} = \left[c\prod_{m=p}^{j-1}\left(\frac{\sigma_N^2}{h_m}\right)^{\frac{1}{M}}\cdot\prod_{m=j}^{M-1}\left(\frac{1}{1+\mu h_m}\right)^{\frac{1}{M}}\right]^{\frac{M}{j-p}}\cdot \cdot\left[\frac{M-p}{M}-\frac{1}{M}\sum_{m=j}^{M-1}\frac{1}{1+\mu h_m}\right]. \tag{3.121}$$

Denote

$$f(\mu)=\prod_{m=j}^{M-1}\left(\frac{1}{1+\mu h_m}\right)^{\frac{1}{j-p}}\cdot\left[(M-p)-\sum_{m=j}^{M-1}\frac{1}{1+\mu h_m}\right] \tag{3.122}$$

and note that for fixed p and j, P_M is a linear function of f.

It suffices to show that $f(g)$ is concave. For this purpose, the derivative $\frac{df}{dg}=\frac{df}{d\mu}(\frac{d\mu}{dg})^{-1}$ should be a decreasing function of g, and hence an increasing function of μ.

Computing the derivatives from (3.119) and (3.121) we get:

$$\frac{df}{dg}=\frac{\frac{df}{d\mu}}{\frac{dg}{d\mu}}=\frac{\frac{1}{j-p}\left((M-p)-\sum_{m=j}^{M-1}\frac{1}{1+\mu h_m}\right)-\frac{\sum_{m=j}^{M-1}\frac{h_m}{(1+\mu h_m)^2}}{\sum_{m=j}^{M-1}\frac{h_m}{1+\mu h_m}}}{\frac{1}{j-p}\sum_{m=j}^{M-1}\frac{h_m}{(1+\mu h_m)^2}+\frac{\sum_{m=j}^{M-1}\frac{h_m^2}{(1+\mu h_m)^2}}{\sum_{m=j}^{M-1}\frac{h_m}{1+\mu h_m}}} \tag{3.123}$$

Arguments similar to those in Chapter 2 apply in proving that above the derivative increases with μ. Looking at the right hand side of (3.123) (the "large fraction"), we notice that the first term in the numerator increases with μ. For the second term in the numerator, it is clear that as μ increases, its numerator decreases faster than its denominator. This implies that the whole numerator of the "large fraction" is an increasing function of μ. Similarly, the first term in the denominator is clearly a decreasing function of μ. The only thing left is the second term of the denominator. It is straightforward to show that its derivative with respect to μ can be written as

$$\frac{d}{d\mu}\frac{\sum_{m=j}^{M-1}\frac{h_m^2}{(1+\mu h_m)^2}}{\sum_{m=j}^{M-1}\frac{h_m}{1+\mu h_m}}=\frac{1}{\left[\sum_{m=j}^{M-1}\frac{h_m}{1+\mu h_m}\right]^2}\cdot \cdot\left\{\left[\sum_{m=j}^{M-1}\frac{h_m^2}{(1+\mu h_m)^2}\right]^2-\sum_{m=j}^{M-1}\frac{h_m^3}{(1+\mu h_m)^3}\cdot\sum_{m=j}^{M-1}\frac{h_m}{(1+\mu h_m)}\right\} \tag{3.124}$$

If we consider the fact that for any two real numbers a and b we have

$$(a^2+b^2)^2-(a+b)(a^3+b^3)=-ab(a-b)^2 \tag{3.125}$$

and the summations in (3.124) are positive, it is easy to see that the second term of the denominator of the "large fraction" is decreasing with μ. Hence overall the derivative in (3.123) increases with μ. □

3.9 Additional Results for Long Term Power Constraints: Mixed Strategies

3.9.1 Proof of Theorem 3.11

Denote the solution of the game in (3.3) and (3.4), where the jammer is constrained to $\frac{1}{M}\sum_{m=1}^{M-1} J_m \leq J_M(p_M)$ and the transmitter is constrained to $\frac{1}{M}\sum_{m=1}^{M-1} P_m \leq p_M$ by $(\{P_{m,1}\},\{J_{m,1}\})$, and the solution of the game in (3.3) and (3.4), where the transmitter is constrained to $\frac{1}{M}\sum_{m=1}^{M-1} P_m \leq P_M(j_M)$ and the jammer is constrained to $\frac{1}{M}\sum_{m=1}^{M-1} J_m \leq j_M$ by $(\{P_{m,2}\},\{J_{m,2}\})$.

Denote the solution of the game in (3.3) and (3.4), where the jammer is constrained to $\frac{1}{M}\sum_{m=1}^{M-1} J_m \leq j_M$ and the transmitter is constrained to $\frac{1}{M}\sum_{m=1}^{M-1} P_m \leq p_M$ by $(\{P_{m,0}\},\{J_{m,0}\})$..

By the Proposition 3.3, we must have $I_M(\{P_{m,1}\},\{J_{m,1}\})=R$ and $I_M(\{P_{m,2}\},\{J_{m,2}\})=R$, where $I_M(\{P_m\},\{J_m\})=\frac{1}{M}\sum_{m=0}^{M-1}\log(1+\frac{P_m h_m}{J_m+\sigma_N^2})$.

We will show that (i) even if the jammer's power j_M is different from $J_M(p_M)$, the transmitter's strategy is still optimal; (ii) even if the transmitter's power p_M is different from $P_M(j_M)$, the jammer's strategy is still optimal.

Assume the transmitter plays the strategy given by $\{P_{m,1}\}$.

If $j_M = J_M(p_M)$, it is clear that the optimal solution for both transmitter and jammer is the solution of the game in (3.3) and (3.4), where the jammer is constrained to $\frac{1}{M}\sum_{m=1}^{M-1} J_m \leq j_M$ and the transmitter is constrained to $\frac{1}{M}\sum_{m=1}^{M-1} P_m \leq p_M$. In this case, it is as if each player knows the other player's power constraint.

If $j_M < J_M(p_M)$, then by Lemma 3.16 we have that $J_{m,0} < J_{m,1}\ \forall m$. Since $I_M(\{P_m\},\{J_m\})$ is a strictly decreasing function of $\{J_m\}$ (under the order relation defined in the Section 2.8.4 of Chapter 2), this implies that $I_M(\{P_{m,1}\},\{J_{m,1}\}) > R$. Note that $\{J_{m,0}\}$ is the jammer's strategy when the jammer knows the transmitter's power constraint p_M. Thus we have shown that when the transmitter plays $\{P_{m,1}\}$ and $j_M < J_M(p_M)$, the jammer cannot induce outage over the frame even if it knew the value of p_M.

Assume that the jammer plays the strategy given by $\{J_{m,2}\}$. A similar argument shows that if $p_M < P_M(j_M)$, or equivalently $j_M > J_M(p_M)$, the transmitter cannot achieve reliable communication over the frame even if it knew the exact value of j_M.

This shows that $(\{P_{m,1}\},\{J_{m,2}\})$ is a Bayes equilibrium [33] for the game with incomplete information describing the power allocation within a frame.

3.9.2 Proof of Proposition 3.14

Take any solution $\{P_M(h)^*\},\{J_M(h)^*\}$ of the KKT conditions and denote by P^*_{out} the outage probability obtained under these strategies. By maintaining $\{J_M(h)^*\}$ constant and changing $\{P_M(h)^*\}$, the resulting probability of outage can only be greater than or equal to P^*_{out}, since the original $\{P_M(h)^*\}$ is the solution of a minimization problem with convex cost function and linear constraints.

Similarly, by maintaining $\{P_M(h)^*\}$ constant and changing $\{J_M(h)^*\}$, the resulting probability of outage can only be less than or equal to P^*_{out}, since the original $\{J_M(h)^*\}$ is the solution of a maximization problem with concave cost function and linear constraints.

These arguments imply that $\{P_M(h)^*\},\{J_M(h)^*\}$ is a Nash equilibrium of the game.

Chapter 4

Feedback-Based Collaborative Secrecy Encoding over Binary Symmetric Channels

4.1 Introduction

In the context of a broadcast channel with confidential messages, it was shown in [13] that a strictly positive secrecy capacity cannot be achieved for any arbitrary pair of receiver/eavesdropper channels. In particular, [14] proves that whenever the eavesdropper's channel is *less noisy* than the receiver's channel, no secret messages can be exchanged between the legitimate transmitter and receiver by the conventional method of [12].

This motivated several works [41], [20], [21], [42], [1] to focus on alternative methods of achieving positive secrecy rates even when the legitimate receiver has a worse channel than the eavesdropper. All these works exploit the idea of feedback channels.

The simple and interesting method of [41] is based on making the receiver jam the eavesdropper. The receiver can subtract its own jamming signal from the received signal, while the wiretapper is kept totally ignorant of the confidential information flowing between the legitimate users. The drawback of this approach is that the receiver has to function in full duplex mode. Although an extension to half-duplex mode is presented in [41] for binary symmetric channels, it relies on the assumption that the transmission of symbol 0 is equivalent to the absence of a physical signal. We believe that under this assumption, the binary symmetric channel is no longer valid as a simplified model for a physical wireless channel.

More recently, [42], [1] both use a secret key to enhance the secrecy throughput of Wyner's scheme. In [42] the secret key is communicated through an error-free secure channel, while in [1] it is transmitted using Wyner's scheme on the feedback channels (and thus its secrecy is subject to Alice's feedback channel being better than Eve's). An interesting idea of [1] is to use time-sharing on the feedback link. Part of the feedback transmission is used to generate the secret key, while

the remaining channel uses transmit random symbols with the purpose of providing the "common randomness" necessary for our secrecy encoding scheme described in this chapter. A mixed secrecy encoding strategy is proposed in [1]. The main idea behind this strategy is to simultaneously transmit a combination of secret messages, encoded by different methods. However, while a message encrypted by a secret key can be transmitted at the same time as a secret message encoded by Wyner's scheme, the additional secret message encrypted with the use of a random feedback sequence does not maintain secrecy. The exact reasons why the proposed scheme of [1] is incorrect will be revealed in Section 4.4. None of the previously mentioned works considers the impact of feedback transmission on the overall bandwidth use. This drawback becomes critical in [1], where it results in the "secrecy rates" bearing no physical meaning, as will be shown in Section 4.7.

The concept of *common randomness* is introduced in [20, 21]. Such randomness can be acquired if all terminals attempt to decode (note that a necessary condition is that the eavesdropper cannot decode perfectly) a sequence of random bits, as for example a data stream transmitted by a satellite at very low signal to noise ratio (SNR) [20]. Both [20] and [21] study the case when the legitimate users agree on a secret key by employing repetitive protocols, which are not efficient for regular data transmission.

The idea developed in this chapter is inspired by a particular case in [20]. As an example and motivation for the feedback approach to secrecy in the classical Alice (transmitter) - Bob (receiver) - Eve (eavesdropper) scenario, [20] develops a scheme where the common randomness is not received from some external source (like a satellite), but introduced by Alice herself, and functions as a secret key which allows Bob to share a secret message with Alice over a public, error free channel. Our model changes the roles of Alice and Bob. Although at some point we make use of the same concept of public error free channel, we show how the techniques that create such a channel impact the overall secrecy rate. Our results explicitly count the loss in the total rate due to the transmission of feedback.

While sharing functional similarities with the well-known *one-time pad* [43] encryption scheme, our approach is radically different in that it requires no secret key to be shared by the legitimate parties before the initiation of the transmission protocol (except maybe a small secret key that guarantees authenticity as in [20]). Instead it exploits the channel randomness as means of confusing the eavesdropper.

Our contributions can be summarized as follows:

- We show how an adaptation of Maurer's scheme [20] can be used to achieve a non-empty rate-equivocation region and hence a strictly positive secrecy rate over binary symmetric channels (BSCs) even when the forward channel between Alice and Eve is *less noisy* than the forward channel between Alice and Bob, regardless of the feedback channel quality between Bob and Alice or Bob and Eve.

- Our results also indicate how the forward channel capacities scale the overall secrecy rate and what penalties are incurred by the transmission of feedback sequences.

- We show that even if the forward channel from Alice to Bob is less noisy than the channel from Alice to Eve, feedback can sometimes further improve the achievable rate-equivocation region obtained using Wyner's classical method [12]. This is done by dividing the transmission over the forward channel into two parts, as in [13]. Thus, we transmit a secret message at a rate less than the secrecy capacity [12], and allow room for an additional common message, which carries information "encrypted" with the help of the feedback sequence. The optimal way of splitting the forward message rate is found numerically.

- We prove that, for a two-user broadcast channel with both channels binary and symmetric, the optimal auxiliary channel of [13], needed to encode both a secret and a common message into the transmitted sequence is a binary symmetric one, and its optimal input distribution is uniform.

- Finally, we take our scheme a step further and implement it on the reverse channel (from Bob to Alice, rather than from Alice to Bob), in order to generate a secret key. Alice uses this key as a one-time pad for the transmission of a secret message.

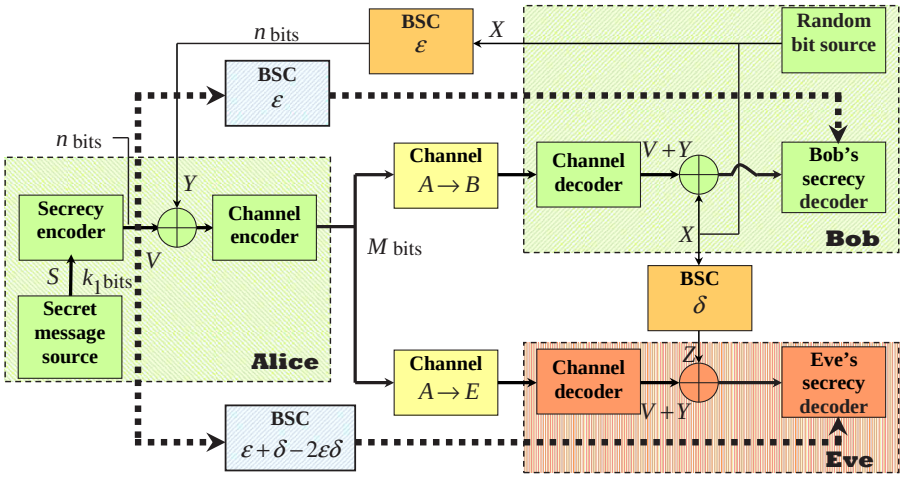

FIGURE 4.1. System model.

The sequel is organized into seven sections. Sections 4.2.1 and 4.2.2 describe the kernel of our scheme. Our adaptation of Maurer's idea [20], including the channel model and the transmission protocol are presented in Section 4.2.1 under the assumption that the forward channels are error free. The public error free channel and the overall rate-equivocation region are discussed in Section 4.2.2 for a general value of the forwarding rate. Section 4.3 deals with the special case when the eavesdropper's forward channel is less noisy than the legitimate receiver's forward channel, while section 4.4 extends the model to the case when the eavesdropper's forward channel is worse than the legitimate receiver's. An alternative scheme, which reverses our protocol to generate a secret key, is provided in Section 4.5. Finally, conclusions are drawn in Section 4.6.

4.2 The Kernel

4.2.1 The Unscaled Rates

Consider the classical Alice (transmitter) - Bob (receiver) - Eve (eavesdropper) scenario with binary symmetric channels (BSCs) between any pair of users. We assume that Eve's only form of

interfering with the transmission is eavesdropping. Although our present treatment is restrictive to binary channels, the principles and results therein can be easily extended to more complex models. A simple extension to additive white Gaussian noise (AWGN) channels is provided in Section 4.9.

The proposed model is depicted in Figure 4.1. The transmitter (Alice) wants to communicate the outputs of a source $\mathscr{S}$ of entropy H_s to the legitimate receiver (Bob), and maintain some level of secrecy towards the wiretapper (Eve). The channel $A \rightarrow B$ from Alice to Bob is a BSC characterized by its crossover probability ϵ_f, while the binary symmetric channel $A \rightarrow E$ from Alice to Eve is characterized by the crossover probability δ_f. Similarly, the feedback BSCs $B \rightarrow A$ (Bob to Alice) and $B \rightarrow E$ (Bob to Eve) are characterized by their crossover probabilities ϵ_b and δ_b, respectively.

The transmission protocol associated with the channel model in Figure 4.1 is an adaptation of Maurer's scheme [20] and is described as follows. Bob feeds back a sequence $\mathbf{x}$ of n bits representing the independent realizations of a Bernoulli random variable X with expectation $\mathbf{E}[X] = 0.5$. Since the bits are independent and identically distributed (i.i.d), Alice's and Eve's estimate of each bit should be based solely on the corresponding received bit. Therefore, the bit error probabilities that affect Alice's and Eve's decoding are ϵ_b and δ_b respectively. Denote the feedback sequences received by Alice and Eve as $\mathbf{y}$ and $\mathbf{z}$, respectively.

At this point, our feedback-based protocol assumes that Alice can share information with both Bob and Eve through an error free public channel, just like in [20]. The implications of achieving such an error free channel are discussed in Section 4.2.2.

Since an error free public channel cannot protect Alice's information from the eavesdropper Eve, the protocol has to artificially create a pair of channels that are adequate for the transmission of secret messages.

For this purpose, if Alice needs to send an n-dimensional sequence $\mathbf{v}$ to Bob, she first computes $\mathbf{v} \oplus \mathbf{y}$, where $\oplus$ denotes addition $\mod 2$, and feeds this signal through the error free channel.

Since $\mathbf{x}$ is a sequence of i.i.d. symbols with a uniform distribution over $\{0, 1\}$, the same property holds for the BSC output $\mathbf{y}$ and, by the *Crypto lemma*[1] [44], [41], for $\mathbf{v} \oplus \mathbf{y}$.

Both Bob and Eve receive $\mathbf{v} \oplus \mathbf{y}$ with no errors. In order to obtain the original message $\mathbf{v}$, the optimal strategy for Bob is to compute $\mathbf{v} \oplus \mathbf{y} \oplus \mathbf{x}$, while Eve's best strategy is to compute $\mathbf{v} \oplus \mathbf{y} \oplus \mathbf{z}$ [20].

As a consequence, a bit error probability of $\epsilon_B = \epsilon_b$ will affect Bob's estimate of $\mathbf{v}$, while a bit error probability of $\epsilon_E = \epsilon_b + \delta_b - 2\epsilon_b\delta_b$ will affect Eve's estimate [20]. The result is an equivalent system in which Eve's channel is a degraded version of Bob's channel, and which is therefore adequate for the transmission of secret messages from Alice to Bob. In other words, standard secrecy encoding can be performed for this equivalent system so that the n-sequence $\mathbf{v}$ carries a secret message $\mathbf{s}^{k_1}$ (which will hence forth be represented as a sequence of k_1 source symbols). A total transmission rate arbitrarily close to

$$R_{t,u} = 1 - h(\epsilon_b) \tag{4.1}$$

can be achieved as $n \to \infty$, where $h(\cdot)$ represents the binary entropy function $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$.

We shall now restate some of the definitions in [12] and then show how Theorem 2 of [12] can be readily applied to our scenario.

Definition 4.1. *The equivocation of the source $\mathscr{S}$ of entropy H_s at Eve is defined as:*

$$\Delta = \frac{1}{k} H(\mathbf{s}^k | \mathbf{w}_{\mathbf{E}}^{\mathbf{M}}), \tag{4.2}$$

where the sequence $\mathbf{s}^k$ of k source symbols are encoded into a codeword $\mathbf{w}_{\mathbf{A}}^{\mathbf{M}}$ of length M which is transmitted over the broadcast channel, and received by Eve as $\mathbf{w}_{\mathbf{E}}^{\mathbf{M}}$.

[1] Special care should be applied when using the Crypto lemma [44]. For instance, if $\mathcal{C}$ is a compact Abelian group and X and E are random variables over $\mathcal{C}$ such that X is *independent of* E and uniformly distributed over $\mathcal{C}$, then $X + E$ is uniform and *independent of* E. However, E is not independent of $(X, X + E)$.

Definition 4.2. *The rate-equivocation pair (R, d) is achievable if for any $\nu > 0$ there exists an $(M, k, \Delta, \overline{P_e})$ code as defined in [12] such that:*

$$\frac{kH_s}{M} \geq R - \nu, \quad \Delta \geq d - \nu, \quad \overline{P_e} \leq \nu \tag{4.3}$$

where $\overline{P_e}$ is the average error probability in decoding for $\mathbf{s}^k$ at Bob.

Theorem 4.3. *(*Theorem 2 from [12]*) A rate-equivocation pair (R, d) is achievable for Wyner's scheme with* discrete memoryless symmetric channels *if and only if*

$$0 \leq R \leq C_M, \quad 0 \leq d \leq H_s, \quad Rd \leq H_s C_s, \tag{4.4}$$

where $C_s = C_M - C_{MW}$ is the secrecy capacity (representing the maximum rate at which the outputs of the source $\mathscr{S}$ can be conveyed from Alice to Bob, while remaining perfectly secret to Eve) achievable by Wyner's scheme in this case, C_M is the capacity of Bob's channel, and C_{MW} is the capacity of Eve's channel.

The following corollary, which will prove useful in the sequel, follows directly from Theorem 4.3 and Definition 4.2.

Corollary 4.4. *If (R, d) is an achievable rate-equivocation pair, then the number of secret source symbols k that can be encoded into the M-sequence $\mathbf{w}_{\mathbf{A}}^{\mathbf{M}}$ has to satisfy:*

$$k \leq \frac{MC_s}{d}. \tag{4.5}$$

Proof. Take an achievable rate-equivocation pair (R, d) such that $Rd = H_s C_s$. If $k > \frac{MC_s}{d}$, then there exists $R' > R$ such that the same code that achieves the (R, d) pair satisfies $\frac{H_s k}{M} \geq R' - \nu$, for any $\nu > 0$. This implies that (R', d) is an achievable rate. But then $R'd > H_s C_s$, and this violates Theorem 4.3. □

If we apply Theorem 4.3 to the pair of equivalent channels derived above, we can conclude that there exists a $(n, k_1, \Delta_1, \overline{P_{e,1}})$ code satisfying $\frac{k_1 H_s}{n} \geq R - \nu$, $\Delta_1 \geq d - \nu$, and $\overline{P_{e,1}} \leq \nu$ if and only

if $0 \leq R \leq R_{t,u}$, $0 \leq d \leq H_s$, $Rd \leq H_s R_{s,u}$, where $R_{s,u}$ is the maximum achievable *secrecy rate* [13, 20]

$$R_{s,u} = h(\epsilon_b + \delta_b - 2\epsilon_b\delta_b) - h(\epsilon_b). \tag{4.6}$$

Several comments are in order. First, note that $R_{s,u} > 0$ – and therefore the rate-equivocation region as defined in [12] is non-empty – unless $\delta_b \in \{0, 1\}$ (the assumption that feedback channels exist implies $\epsilon_b \neq 0.5$)

Second, the rates $R_{t,u}$ and $R_{s,u}$ do not represent the *overall* transmission and secrecy rates of our model, since a pair of binary symmetric channels such as the forward $A \rightarrow B$ and $A \rightarrow E$ channels cannot provide error free transmission at infinite rates. The information encoded in the sequence $\mathbf{v}$ mentioned above has to be passed through one of these channels in order to be available at the other two terminals. While this "correction" will be considered in Section 4.2.2, we shall denote the rates $R_{t,u}$ and $R_{s,u}$ as *the unscaled transmission and secrecy rates*, respectively.

Third, note that under the above protocol, an independent feedback sequence $\mathbf{x}$ is transmitted every time for each new information-carrying sequence $\mathbf{v}$. Eve's resulting error sequence is always different and independent, and acts like a *one-time pad* [43]. As is the case with a one-time pad, the feedback sequence cannot be recycled. If only one feedback sequence is transmitted and used for a set of several messages, Eve's equivocation about the whole set will be the same as her equivocation about any one message in the set.

Therefore, an additional rate penalty has to address the channel uses required for the feedback of $\mathbf{x}$, as will be shown in Section 4.2.2.

4.2.2 The Overall Rate-Equivocation Region and Secrecy Rate

This section shows how the overall transmission rates of our model depend on the *unscaled* rates of the equivalent system presented in Section 4.2.1 and on the transmission rates used over the forward binary symmetric channels.

In Section 4.2.1 we showed that, if feedback is allowed, we can artificially form an equivalent system that allows encoding by Wyner's scheme [12]. All that is needed is an error free public channel to support the transmission of the n-sequence $\mathbf{v} \oplus \mathbf{y}$. By the channel coding theorem, this channel is readily available if $\mathbf{v} \oplus \mathbf{y}$ is transmitted at a rate $R_{AB,fb}$ (the notation stands for the rate at which the feedback processed signal is transmitted from Alice to Bob) less than the capacity of the $A \rightarrow B$ channel $C_{AB} = 1 - h(\epsilon_f)$.

For a more formal proof, denote the error sequences introduced by the feedback channels by $\mathbf{e_{bA}}$ – for Alice – and $\mathbf{e_{bE}}$ – for Eve. According to [12] if the rate of the secret message is less than $R_{s,u}$, then there exists an encoding/decoding technique such that for any $\nu > 0$ there exists $N_0 > 0$ such that the average probability of correctly decoding for the secret message $\mathbf{s}^{k_1}$ is

$$\sum_{\mathbf{s}} Pr\{\mathbf{s}^{k_1}\} \sum_{\mathbf{v},\mathbf{e_{bA}}} Pr\{\mathbf{e_{bA}}\} Pr\{\mathbf{v}|\mathbf{s}^{k_1}\} \cdot Pr\{\psi(\mathbf{v} \oplus \mathbf{e_{bA}}) = \mathbf{s}^{k_1}\} \geq 1 - \nu \tag{4.7}$$

for $n > N_0$, where $\psi(\cdot)$ is Bob's secrecy decoder.

Moreover, according to Gallager's second corollary of Theorem 5.6.2. [45], there exists a code for Bob's forward channel with the property that if the transmission rate is $R_{AB,fb} < C_{AB}$, then for any $\nu > 0$ there exists $N_1 > 0$ such that the average probability of correctly decoding a given transmitted message $\mathbf{t}$ is

$$\sum_{\mathbf{w_B},\mathbf{t}} Pr\{\mathbf{t}\} Pr\{\mathbf{w_B}|\mathbf{t}\} Pr\{\phi(\mathbf{w_B}) = \mathbf{t}\} \geq 1 - \nu \tag{4.8}$$

for $n > N_1$, where $\phi(\cdot)$ is Bob's channel decoder and $\mathbf{w_B}$ is Bob's received sequence over the forward channel (when $\mathbf{w_A}$ is transmitted by Alice). Note that our decoding method consists of separate channel and secrecy decoding. That is, Bob estimates the secret message s, as $\widehat{s} = \psi(\phi(\mathbf{w_B}) \oplus \mathbf{x})$. There is no guarantee that this separate decoding method is optimal. We define Bob's optimal (joint) decoder $\xi(\cdot)$, yielding the optimal estimate $\widetilde{s} = \xi(w_B)$. Given the feedback sequence $\mathbf{x}$, we can lower bound

$$Pr\{\xi(\mathbf{w_B}) = \mathbf{s}^{k_1}\} \geq \sum_{\mathbf{t}} Pr\{\phi(\mathbf{w_B}) = \mathbf{t}\} Pr\{\psi(\mathbf{t} \oplus \mathbf{x}) = \mathbf{s}^{k_1}\}. \tag{4.9}$$

Thus given the feedback sequence $\mathbf{x}$, Bob's average probability of correctly decoding for the secret message $\mathbf{s}^{k_1}$ can be lower bounded as

$$\sum_{\mathbf{s}^{k_1}} Pr\{\mathbf{s}^{k_1}\} \sum_{\mathbf{v},\mathbf{e_{bA}}} Pr\{\mathbf{e_{bA}}\} Pr\{\mathbf{v}|\mathbf{s}^{k_1}\} \sum_{\mathbf{x}} Pr\{\mathbf{x}\} \cdot$$

$$\cdot \sum_{\mathbf{w_B}} Pr\{\mathbf{w_B}|\mathbf{v} \oplus \mathbf{e_{bA}} \oplus \mathbf{x}\} Pr\{\xi(\mathbf{w_B}) = \mathbf{s}^{k_1}\} \overset{(a)}{\geq}$$

$$\geq \sum_{\mathbf{s}^{k_1}} Pr\{\mathbf{s}^{k_1}\} \sum_{\mathbf{v},\mathbf{e_{bA}}} Pr\{\mathbf{e_{bA}}\} Pr\{\mathbf{v}|\mathbf{s}^{k_1}\} \sum_{\mathbf{x}} Pr\{\mathbf{x}\} \cdot$$

$$\cdot \sum_{\mathbf{w_B}} Pr\{\mathbf{w_B}|\mathbf{v} \oplus \mathbf{e_{bA}} \oplus \mathbf{x}\} \sum_{\mathbf{t}} Pr\{\phi(\mathbf{w_B}) = \mathbf{t}\} \cdot Pr\{\psi(\mathbf{t} \oplus \mathbf{x}) = \mathbf{s}^{k_1}\} \overset{(b)}{\geq}$$

$$\geq \sum_{\mathbf{s}^{k_1}} Pr\{\mathbf{s}^{k_1}\} \sum_{\mathbf{v},\mathbf{e_{bA}}} Pr\{\mathbf{e_{bA}}\} Pr\{\mathbf{v}|\mathbf{s}^{k_1}\} \sum_{\mathbf{x}} Pr\{\mathbf{x}\} \cdot \sum_{\mathbf{w_B}} Pr\{\mathbf{w_B}|\mathbf{v} \oplus \mathbf{e_{bA}} \oplus \mathbf{x}\} \cdot$$

$$\cdot Pr\{\phi(\mathbf{w_B}) = \mathbf{v} \oplus \mathbf{e_{bA}} \oplus \mathbf{x}\} \cdot Pr\{\psi(\mathbf{v} \oplus \mathbf{e_{bA}})\} = \mathbf{s}^{k_1}\} \overset{(c)}{=}$$

$$= \sum_{\mathbf{s}^{k_1}} Pr\{\mathbf{s}^{k_1}\} \sum_{\mathbf{v},\mathbf{e_{bA}}} Pr\{\mathbf{e_{bA}}\} Pr\{\mathbf{v}|\mathbf{s}^{k_1}\} \cdot Pr\{\psi(\mathbf{v} \oplus \mathbf{e_{bA}})\} = \mathbf{s}^{k_1}\} \cdot$$

$$\cdot \sum_{\mathbf{x}} Pr\{\mathbf{x}\} \sum_{\mathbf{w_B}} Pr\{\mathbf{w_B}|\mathbf{v} \oplus \mathbf{e_{bA}} \oplus \mathbf{x}\} \cdot Pr\{\phi(\mathbf{w_B}) = \mathbf{v} \oplus \mathbf{e_{bA}} \oplus \mathbf{x}\} \overset{(d)}{\geq}$$

$$\geq (1-\nu) \sum_{\mathbf{s}^{k_1}} Pr\{\mathbf{s}^{k_1}\} \sum_{\mathbf{v},\mathbf{e_{bA}}} Pr\{\mathbf{e_{bA}}\} Pr\{\mathbf{v}|\mathbf{s}^{k_1}\} \cdot Pr\{\psi(\mathbf{v} \oplus \mathbf{e_{bA}})\} = \mathbf{s}^{k_1}\} \overset{(e)}{\geq} (1-\nu)^2. \quad (4.10)$$

Inequality (a) follows from (4.9), inequality (b) from the fact that $\sum_t F(\mathbf{t}) \geq F(\mathbf{t})|_{\mathbf{t}=\mathbf{v}\oplus\mathbf{e_{bA}}\oplus\mathbf{x}}$ for any positive function F, while the equality (c) from simply re-arranging the terms. In inequality (d) we used (4.8) and the fact that $Pr\{\mathbf{v} \oplus \mathbf{e_{bA}} \oplus \mathbf{x}\} = Pr\{\mathbf{x}\}$ (due to the Crypto lemma [44]), while inequality (e) follows directly from (4.7). The resulting average error probability at Bob is thus

$$\overline{P_e} < 2\nu - \nu^2, \quad (4.11)$$

which goes to zero as $\nu \to 0$.

Denote $C_{AE} = 1 - h(\delta_f)$ the capacity of Eve's forward channel. Note that if $C_{AE} \geq C_{AB}$, Eve will also be able to decode the sequence $\mathbf{v} \oplus \mathbf{y}$ with no errors asymptotically. However, Eve's equivocation about the secret message $\mathbf{s}^{k_1}$ is maintained due to the feedback processing. On the

other hand, if $C_{AE} < C_{AB}$, Eve cannot decode for the message $\mathbf{v} \oplus \mathbf{y}$. Under this scenario, a secret message can be transmitted from Alice to Bob by Wyner's scheme, without using any feedback. The optimal tradeoff between the rate of encoding a secret message directly through Wyner's scheme and the rate $R_{AB,fb}$ at which a feedback-processed secret message should be forwarded to Bob will be discussed in Section 4.4. In what follows, we prove that Eve's equivocation about the feedback-processed secret message $\mathbf{s}^{k_1}$ is maintained regardless of the forwarding rate $R_{AB,fb}$.

Let $\mathbf{w_E}$ denote Eve's received signal over the forward channel and $\mathbf{s}^{k_1}$ denote the secret message. Also, recall the error sequences corresponding to the feedback channels were denoted by $\mathbf{e_{bA}}$ (for Alice's feedback channel) and $\mathbf{e_{bE}}$ (for Eve's feedback channel).

Eve's equivocation about the secret message is

$$H(\mathbf{s}^{k_1}|\mathbf{w_E}, \mathbf{x} \oplus \mathbf{e_{bE}}) \geq H(\mathbf{s}^{k_1}|\mathbf{v} \oplus \mathbf{y}, \mathbf{x} \oplus \mathbf{e_{bE}}) = H(\mathbf{s}^{k_1}|\mathbf{v} \oplus \mathbf{e_{bE}} \oplus \mathbf{e_{bA}}), \tag{4.12}$$

where the inequality follows since $\mathbf{s}^{k_1} \rightarrow \mathbf{v} \oplus \mathbf{y} \rightarrow \mathbf{w_E}$ form a Markov chain, and the equality is due to the Crypto lemma [44] and the fact that the probability distribution of $\mathbf{x}$ is uniform over $\{0,1\}^n$ (implying that $\mathbf{x} \oplus \mathbf{e_{bE}}$ is independent of $(\mathbf{s}^{k_1},\ \mathbf{v} \oplus \mathbf{e_{bE}} \oplus \mathbf{e_{bA}})$). Hence Eve's equivocation can only increase because of the imperfect forward channels.

The impact of the forward channel finite transmission rate on the overall achievable rates is reflected in a scaling of the *unscaled* rates by the rate used over the forward link $R_{AB,fb}$. That is, a sequence of m_1 bits carrying $k_1 = nR_{s,u}/H_s$ secret symbols is mapped to an n-sequence $\mathbf{v}$ by Alice's secrecy encoder, such that $\frac{m_1}{n} \approx R_{t,u}$. Next, Alice computes $\mathbf{v} \oplus \mathbf{y}$, and feeds this signal to the channel encoder. Since $\mathbf{v} \oplus \mathbf{y}$ is a sequence of i.i.d. uniform bits (as shown in Section 4.2.1), its error free transmission requires an approximate number of $M = \frac{n}{R_{AB,fb}}$ channel uses. Hence, the m_1 source bits are transmitted in M channel uses.

An additional number of n channel uses have to be considered for the transmission of the required feedback sequence $\mathbf{x}$. Noting that $\frac{n}{M+n} = \frac{R_{AB,fb}}{R_{AB,fb}+1}$, we can state the following result.

Theorem 4.5. *For any ν_0, by choosing ν such that $\nu_0 > \max\{\nu, 2\nu - \nu^2\}$, we can find a code comprising the original $(n, k_1, d, \overline{P_{e,1}})$ secrecy code, the forward channel code and the feedback, which encodes the k_1-sequence $\mathbf{s}^{k_1}$ into the M-sequence $\mathbf{w}_\mathbf{A}^\mathbf{M}$, such that if Bob receives $\mathbf{w}_\mathbf{B}^\mathbf{M}$ and Eve receives $\mathbf{w}_\mathbf{E}^\mathbf{M}$, we have $\frac{k_1 H_s}{M+n} \geq \frac{n}{M+n} R - \nu_0$, $\Delta_1 \geq d - \nu_0$, and $\overline{P_{e,1}} \leq \nu_0$, as long as*

$$0 \leq \frac{n}{M+n} R \leq \frac{R_{AB,fb}}{R_{AB,fb}+1} R_{t,u}, \tag{4.13}$$

$$0 \leq d \leq H_s, \tag{4.14}$$

$$\frac{n}{M+n} Rd \leq H_s \frac{R_{AB,fb}}{R_{AB,fb}+1} R_{s,u}. \tag{4.15}$$

This yields an overall secrecy rate of

$$R_{s,0} = R_{s,u} \frac{R_{AB,fb}}{R_{AB,fb}+1}. \tag{4.16}$$

4.3 The First Approach: Eavesdropper's Forward Channel Less Noisy than Legitimate Receiver's Channel

In this section we show a first approach to increasing the secrecy rate by using our feedback-based scheme. We prove that it can achieve a strictly positive secrecy rate and a non-empty rate-equivocation region even if the eavesdropper's forward channel $A \rightarrow E$ is less noisy than the legitimate receiver's channel $A \rightarrow B$. The case when $A \rightarrow B$ is less noisy than $A \rightarrow E$ is studied in Section 4.4.

If Eve's forward channel is less noisy than Bob's forward channel, or equivalently $\delta_f \leq \epsilon_f$, then no messages can be transmitted at any level of secrecy over the $A \rightarrow B$ channel by Wyner's method [12]. If we take the forwarding rate $R_{AB,fb}$ arbitrarily close to Bob's forward channel capacity C_{AB}, we obtain the following result which is a straightforward adaptation of Theorem 4.5.

Corollary 4.6. *For any $\nu_0 > 0$ there exists a code which encodes the k-sequence $\mathbf{s}^{k_1}$ into the M-sequence $\mathbf{w}_\mathbf{A}^\mathbf{M}$, such that if Bob receives $\mathbf{w}_\mathbf{B}^\mathbf{M}$ and Eve receives $\mathbf{w}_\mathbf{E}^\mathbf{M}$, we have $\frac{k_1 H_s}{M+n} \geq \frac{n}{M+n} R - \nu_0$,*

$\Delta_1 \geq d - \nu_0$, *and* $\overline{P_e} \leq \nu_0$, *as long as*

$$0 \leq \frac{n}{M+n} R \leq \frac{C_{AB}}{C_{AB}+1} R_{t,u}, \tag{4.17}$$

$$0 \leq d \leq H_s, \tag{4.18}$$

$$\frac{n}{M+n} Rd \leq H_s \frac{C_{AB}}{C_{AB}+1} R_{s,u}. \tag{4.19}$$

This yields an overall secrecy rate of

$$R_{s,0} = R_{s,u} \frac{C_{AB}}{C_{AB}+1}. \tag{4.20}$$

The following remark is in order. Maurer's "secrecy capacity with public discussion" [20] is upper-bounded as follows:

$$\widehat{C}_s(P_{YZ|X}) \leq \max_{P_X} I(X;Y|Z) \tag{4.21}$$

where X, Y and Z denote the input and the outputs of the non-perfect channel (in our case the input to feedback channel at Bob and the outputs at Alice and Eve, respectively), and P_X denotes the probability distribution of X input. It is also noted in [20] that in the case of binary symmetric channels, the upper-bound is achieved. For our case, this means that the *unscaled* secrecy rate $R_{s,u} = h(\epsilon_b + \delta_b - 2\epsilon_b\delta_b) - h(\epsilon_b)$ can be increased no further.

However, for a practical system with imperfect forward channels, the objective should be to maximize the *overall* secrecy rate rather than the *unscaled* secrecy rate. In the remainder of this section we provide a simple example to prove that by altering the feedback sequence we can increase the overall secrecy rate of the system over the value

$$R_{s,0} = \left[h(\epsilon_b + \delta_b - 2\epsilon_b\delta_b) - h(\epsilon_b)\right] \frac{C_{AB}}{C_{AB}+1} \tag{4.22}$$

provided by the maximization of the unscaled secrecy rate.

Processing the feedback sequence improves performance

So far we assumed that the feedback i.i.d. uniform sequence of bits $\mathbf{x}$ is transmitted by Bob with no further processing.

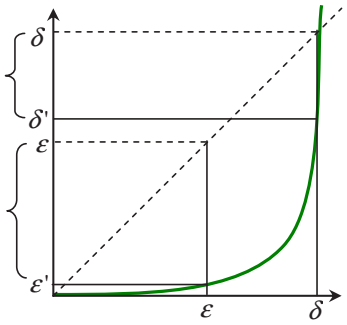

FIGURE 4.2. The operator corresponding to the repetition coding preprocessing.

Further processing of the feedback sequence results in equivalent feedback channels with altered error probabilities. Although the overall achievable secrecy rate depends on the rate at which the feedback is transmitted, an error and rate reducing encoding/decoding scheme for the feedback sequence implemented among the three parties can improve the system's performance. One such simple scheme, which preserves the independence between the symbols of $\mathbf{y}$ after decoding, is obtained if Bob encodes the feedback sequence $\mathbf{x}$ using repetition coding of rate $1/N$, and Alice and Eve employ the optimal decoding scheme, which is majority decoding. The scheme results in equivalent BSCs with crossover probabilities

$$\epsilon_b' = \sum_{i=K+1}^{2K+1} \begin{pmatrix} 2K+1 \\ i \end{pmatrix} \epsilon_b^i (1-\epsilon_b)^{2K+1-i} \tag{4.23}$$

and

$$\delta_b' = \sum_{i=k+1}^{2K+1} \begin{pmatrix} 2K+1 \\ i \end{pmatrix} \delta_b^i (1-\delta_b)^{2K+1-i}, \tag{4.24}$$

where $N = 2K+1$ if N is odd and $N = 2K+2$ if N is even, and $K \geq 0$.

The optimum N that maximizes the overall secrecy rate can be obtained numerically. The improvement in the overall secrecy rate due to repetition coding, as well as the optimal choice of N will be shown in Figure 4.4 and 4.5 of Section 4.4. However at this point we note that a processing method that decreases equivalent crossover probabilities is better when ϵ_b is decreased more than δ_b, i.e. when the strength of Bob's channel is increased relative to that of Eve's. By inspecting

(4.23) and (4.24), we notice that the operator corresponding to our preprocessing method is exponential. It is therefore expected that the method gives better results when $\epsilon_b < \delta_b$, as can be seen from Figure 4.2 (this phenomenon is indeed observed in our numerical results of Section 4.4) .

Although the above result may seem counter-intuitive (in light of Maurer's Theorem 4 [20]), the improvement in our case results exactly from the imperfection of the forward channels, which translates to scaling coefficients for all achievable rates, as shown in Section 4.2.2.

Note that if a rate $1/N$ repetition coding is used for the transmission of the feedback sequence, the total number of channel uses needed for feedback is Nn, leading to the overall secrecy rate

$$R_{s,c} = \frac{nR_{s,u}}{n/R_{AB,fb} + nN} = R_{s,u}\frac{R_{AB,fb}}{NR_{AB,fb}+1}. \tag{4.25}$$

The unscaled secrecy rate $R_{s,u}$ increases with N, while the correction factor $\frac{C_{AB}}{NC_{AB}+1}$ decreases with N, hence the need to find the optimal value of N that maximizes $R_{s,c}$.

Some numerical results

Since the secrecy rate is simpler to represent than the rate-equivocation region, throughout this chapter we focus on illustrating the improvements in the achievable secrecy rate due to feedback. We first consider a model in which the forward channels have crossover probabilities $\epsilon_f = 0.02$ and $\delta_f = 0.01$, respectively. In this scenario, Wyner's scheme cannot deliver a secret message from Alice to Bob at any positive rate. However, the secrecy rates achievable by our feedback based scheme (in Figure 4.3) are strictly positive (except in the pathological cases when $\delta_b = 0$ or $\epsilon_b = 0.5$).

In Figures 4.4 and 4.5 we show the additional improvement in the overall achievable secrecy rate obtained if we use repetition coding for the transmission of the feedback sequence, and the optimal repetition order N. Although the improvement is marginal, it proves that Maurer's upper bound on the secrecy capacity with public discussion [20] does not hold if the forward channels are imperfect.

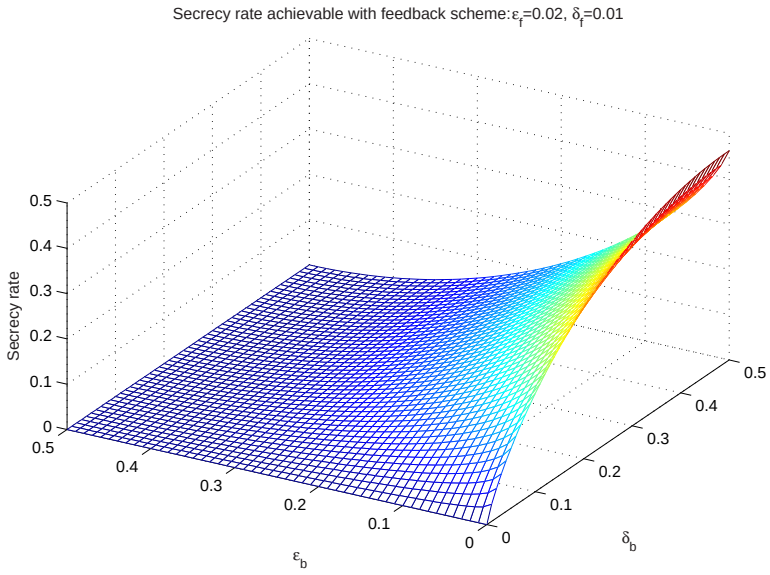

FIGURE 4.3. Overall secrecy rate achievable by our feedback scheme for $\epsilon_f = 0.02$ and $\delta_f = 0.01$.

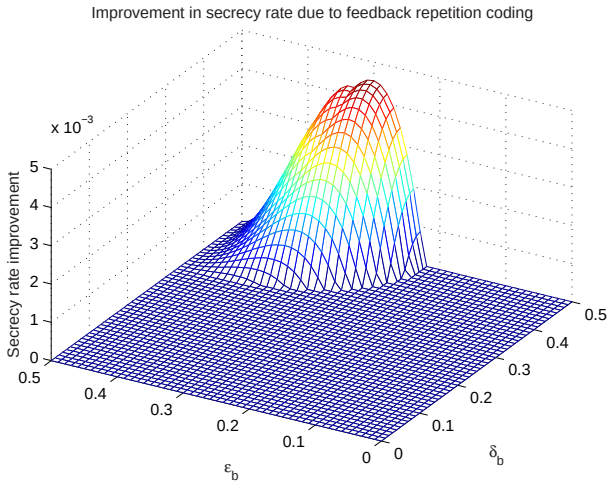

FIGURE 4.4. Secrecy rate improvement due to feedback repetition coding.

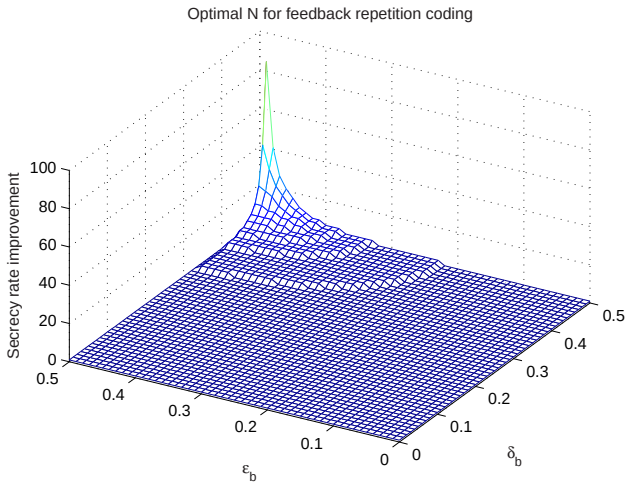

FIGURE 4.5. The optimal value of N for feedback repetition coding.

4.4 The Second Approach: Legitimate Receiver's Forward Channel Less Noisy than Eavesdropper's Channel

If $\epsilon_f < \delta_f$, a non-empty rate-equivocation region and a strictly positive secrecy rate less than $C_s = C_{AB} - C_{AE}$ are asymptotically achievable without feedback [12]. In this section we show that even under this scenario, sometimes feedback can improve the achievable secrecy rate. For example, when C_s is small compared to C_{AB},and the unscaled secrecy rate achievable with feedback $R_{s,u}$ is relatively large (i.e. when the channel $B \to A$ is significantly better than the channel $B \to E$, while the channel $A \to B$ is only slightly better than the channel $A \to E$) , we can have $C_s < R_{s,u}\frac{C_{AB}}{C_{AB}+1}$.

However, in general, neither Wyner's original scheme, nor our feedback based scheme is optimal. Instead, as we shall see shortly, encoding a combination of a secret message and a feedback-processed message into the forwarded sequence $\mathbf{w_A}$ can achieve a higher overall secrecy rate.

The method behind the direct part of Wyner's Theorem 2 [12] assumes the transmission of m_2 bits, containing $k_2 = n_2 C_s$ secret bits, by mapping the k_2-bit secret message $\mathbf{s}^{k_2}$ to a specific coset. The rest of $m_2 - k_2$ bits correspond to the index of the randomly picked coset representative which is transmitted. Since Bob can decode the transmitted codeword perfectly, he has access to all m_2 bits. The $m_2 - k_2$ non-secret bits are neither secret to, nor can they be decoded by Eve without errors [13]. It was assumed in [12] that these bits are picked randomly (according to a uniform

distribution) and carry no information. In their extension of Wyner's work, Csiszar and Korner [13] observe that these bits can actually be picked according to the output message of a uniform source of entropy $H_x = m_2 - k_2$, which can carry useful information for Bob [13].

At a first glance, it would appear that by encoding the message $\mathbf{v} \oplus \mathbf{y}$ into the $m_2 - k_2$ non-secret bits, we could transmit it asymptotically error free to Bob, at a rate arbitrarily close to $C_{AB} - C_s = C_{AE}$, in addition to the original secret message $\mathbf{s}^{k_2}$. In this case, even if Eve had perfect access to these bits (which she has not), the equivocation of both secret messages would be preserved. This argument is the starting point of the proposed mixed secrecy scheme of [1] (see Section 4.7 for more remarks on [1]). Unfortunately, the argument above is false. By using the sequence $\mathbf{v} \oplus \mathbf{y} = \mathbf{v} \oplus \mathbf{x} \oplus \mathbf{e_{bA}}$ to pick the coset representative to be transmitted over the forward channel, the equivocation of the secret message $\mathbf{s}^{k_2}$ encoded into the other k_2 bits is compromised. As shown in Section 4.7, this happens because Eve has access to a distorted version of the feedback sequence $\mathbf{x} \oplus \mathbf{e_{bE}}$, which is correlated with $\mathbf{v} \oplus \mathbf{y}$.

Therefore we need an encoding technique in which Eve's information about the message $\mathbf{v} \oplus \mathbf{y}$, obtained through $\mathbf{x} \oplus \mathbf{e_{bE}}$, does not influence the secrecy of $\mathbf{s}^{k_2}$. Such a technique is readily provided by [13]: we can treat the sequence $\mathbf{v} \oplus \mathbf{y}$ as a common message, intended for both Bob and Eve. In addition to the common message, a secret message $\mathbf{s}^{k_2}$ can be transmitted to Bob. Since the common message is designed to be perfectly decoded by Eve, the additional information contained in $\mathbf{x} \oplus \mathbf{e_{bE}}$ cannot compromise the secrecy of $\mathbf{s}^{k_2}$. The drawback is that the transmission of a common message decreases the rate at which the secret message $\mathbf{s}^{k_2}$ can be conveyed to Bob [13]. However, the transmission of an additional secret message $\mathbf{s}^{k_1}$, encoded in the sequence $\mathbf{v}$, can make up for this loss and, in many circumstances, bring noticeable improvements over Wyner's scheme [12].

In order to pursue this path, we first need to establish what is the optimal tradeoff between the common message rate and the secret message rate. Denote by W_A, W_B and W_E the input to the forward channel and the outputs at Bob and Eve, respectively. According to Theorem 1 of [13], the

two rates have to satisfy:

$$R_e \leq I(V;W_B|U) - I(V;W_E|U), \tag{4.26}$$

$$R_c \leq \min[I(U;W_B), I(U;W_E)], \tag{4.27}$$

where R_e is the secret message rate, R_c is the common message rate, and U and V are two auxiliary random variables such that $U \rightarrow V \rightarrow W_A \rightarrow W_B, W_E$ form a Markov chain.

For our special BSC case, and under the scenario where $\epsilon_f < \delta_f$, we can further simplify (4.27):

$$R_c \leq I(U;W_E). \tag{4.28}$$

Following the proof of Corollary 3 in [13], we can write (4.26) as:

$$\begin{aligned} R_e &\leq I(V;W_B|U) - I(V;W_E|U) = \\ &= I(V;W_B) - I(V;W_E) - [I(U;W_B) - I(U;W_E)] = \\ &= [I(W_A;W_B) - I(W_A;W_E)] - [I(W_A;W_B|V) - I(W_A;W_E|V)] - \\ &\quad -[I(U;W_B) - I(U;W_E)], \end{aligned} \tag{4.29}$$

where the equalities follow from the fact that if $X \rightarrow Y \rightarrow Z$ form a Markov chain, then $I(Y;Z) = I(X;Z) + I(Y;Z|X)$ (Lemma 1 in [13]). Note that the term $[I(W_A;W_B|V) - I(W_A;W_E|V)]$ is always positive [13], and is minimized for $V = W_A$. The condition in (4.29) is thus reduced to

$$R_e \leq [I(W_A;W_B) - I(W_A;W_E)] - [I(U;W_B) - I(U;W_E)], \tag{4.30}$$

or equivalently

$$R_e \leq I(W_A;W_B|U) - I(W_A;W_E|U). \tag{4.31}$$

At this point we are looking for the auxiliary random variable U, and its relationship with the channel input random variable W_A, that achieve the points on the boundary of the (R_e, R_c) region

described above. The only information about U that is provided in [13], is that its alphabet size may, without loss of generality, be assumed to be at most three letters larger than the alphabet of W_A (in our binary case, the alphabet of U would have at most five letters). In Theorem 4.7 below, which is a straightforward adaptation of Theorem 4.8 in the Section 4.8, we present an interesting result, namely that the optimal U is in fact a binary, uniformly distributed random variable, and moreover, it is linked to W_A through a simple binary symmetric channel.

Theorem 4.7. *Any point on the boundary of the (R_e, R_c) region described above can be achieved by a binary random variable U with a uniform distribution over $\{0, 1\}$. Moreover, the channel input random variable W_A can be obtained by passing U through a binary symmetric channel of crossover probability γ that satisfies $1 - h(\gamma + \delta_f - 2\gamma\delta_f) = R_c^*$ (where $h(\cdot)$ is the binary entropy function).*

As a consequence of Theorem 4.7, once we pick the auxiliary channel crossover probability γ we can compute

$$R_c^* = 1 - h(\gamma + \delta_f - 2\gamma\delta_f) \tag{4.32}$$

and

$$R_e^* = [h(\delta_f) - h(\epsilon_f)] - [h(\gamma + \delta_f - 2\gamma\delta_f) - h(\gamma + \epsilon_f - 2\gamma\epsilon_f)]. \tag{4.33}$$

Similar arguments to those in the previous section apply to show that the messages $\mathbf{v} \oplus \mathbf{y}$, containing the secret message $\mathbf{s}^{k_1}$, can now be transmitted to Bob asymptotically error free at a rate arbitrarily close to R_c^*, in the form of a common message. In addition, another secret message $\mathbf{s}^{k_2}$ can be transmitted simultaneously to Bob at rate close to R_e^*. In the remainder of this section we calculate the resulting overall secrecy rate.

Define the equivocations $\Delta_1 = \frac{1}{k_1} H(\mathbf{s}^{k_1} | \mathbf{w}_{\mathbf{E}}^{\mathbf{M}}, \mathbf{x}^n + \mathbf{e_{bE}}^n)$ and $\Delta_2 = \frac{1}{k_2} H(\mathbf{s}^{k_2} | \mathbf{w}_{\mathbf{E}}^{\mathbf{M}})$, where $\mathbf{s}^{k_2}$ is the k_2-sequence of secret source symbols that are encoded in the codeword $\mathbf{w}_{\mathbf{A}}^{\mathbf{M}}$ as a secret message, and $\mathbf{s}^{k_1}$ is a distinct k_1-sequence of secret source symbols that are encoded in the sequence $\mathbf{v} \oplus \mathbf{y}$

by our feedback scheme. The sequence $\mathbf{v} \oplus \mathbf{y}$ is in turn mapped into the same codeword $\mathbf{w_A^M}$ as a common message. The transmitted codeword $\mathbf{w_A^M}$ is received by Eve as $\mathbf{w_E^M}$. We know that for any $\nu > 0$ there exists such an encoding technique which satisfies

$$\tfrac{k_2 H_s}{M} \geq R_2 - \nu, \quad \Delta_2 \geq d_2 - \nu, \quad \overline{P_{e,2}} \leq \nu, \tag{4.34}$$

as long as

$$0 \leq R_2 \leq C_{AB}, \quad 0 \leq d_2 \leq H_s, \quad R_2 d_2 \leq H_s R_e^*, \tag{4.35}$$

and

$$\tfrac{k_1 H_s}{M+n} \geq R_1 - \nu, \quad \Delta_1 \geq d_1 - \nu, \quad \overline{P_{e,1}} \leq \nu, \tag{4.36}$$

as long as

$$0 \leq R_1 \leq C_{AB} R_{t,u}, \quad 0 \leq d_1 \leq H_s, \quad R_1 d_1 \leq H_s R_{s,u} \tfrac{R_c^*}{R_c^*+1}. \tag{4.37}$$

The equivocation of the secret message at Eve is now defined as:

$$\Delta = \frac{1}{k_1 + k_2} H(\mathbf{s}^{k_1}, \mathbf{s}^{k_2} | \mathbf{w_E^M}, \mathbf{x}^n + \mathbf{e_{be}}^n). \tag{4.38}$$

Since $\mathbf{s}^{k_1}$ and $\mathbf{s}^{k_2}$ are independent, we can write

$$\Delta = \frac{k_1}{k_1 + k_2} \Delta_1 + \frac{k_2}{k_1 + k_2} \Delta_2. \tag{4.39}$$

Note that the overall rate at which the secret source is transmitted is now $\frac{(k_1+k_2)H_s}{M+n}$. Therefore, a correction of $\frac{M}{M+n}$ has to be applied to the rate R_2. As a result, the rate-equivocation pair (R, d) is achievable if $R = \min\{\frac{M}{M+n} R_2 + R_1, C_{AB}\}$ and $d = \frac{k_1}{k_1+k_2} d_1 + \frac{k_2}{k_1+k_2} d_2$. Note that this implies $R < C_{AB}$ and $d < H_s$. Also, due to Corollary 4.4 we have $k_2 d_2 \leq M R_e^*$ and $k_2 d_2 \leq (M+n) \frac{R_c^*}{R_c^*+1} R_{s,u}$. Due to (4.34) and (4.36) we have $k_1 + k_2 \geq \frac{M+n}{H_s} (\frac{M}{M+n} R_2 + R_1 - \nu(1 + \frac{M}{M+n}))$, so we can upper-bound

$$d = \frac{k_1 d_1 + k_2 d_2}{k_1 + k_2} \leq H_s \frac{1}{R - \nu(1 + \frac{M}{M+n})} \frac{(R_e^* + R_c^* R_{s,u})}{R_c^* + 1}, \tag{4.40}$$

and

$$Rd \leq H_s \frac{R}{R - \nu(1 + \frac{M}{M+n})} \frac{(R_e^* + R_c^* R_{s,u})}{R_c^* + 1}, \tag{4.41}$$

If we take $\nu \to 0$, we get

$$Rd \leq H_s \frac{(R_e^* + R_c^* R_{s,u})}{R_c^* + 1}. \tag{4.42}$$

Equality can be asymptotically achieved (as $\nu \to 0$) in (4.42) above if the two levels of secrecy operate at $R_2 d_2 = H_s C_e^*$ and $R_1 d_1 = H_s \frac{R_c^*}{R_c^*+1} R_{s,u}$ respectively.

To conclude, our scheme yields an overall asymptotically achievable secrecy rate

$$R_{s,0} = \max \left[\max_{\gamma} \frac{(R_e^* + R_c^* R_{s,u})}{R_c^* + 1}, \frac{C_{AB} R_{s,u}}{C_{AB} + 1} \right], \tag{4.43}$$

where R_e^* and R_c^* are given by (4.32) and (4.33), respectively.

Several comments are in order. If $\gamma = 0$, we obtain $R_c^* = C_{AE}$, and $R_e^* = 0$. However in this case, since no secret message is transmitted directly by Wyner's scheme, we can safely transmit the feedback-processed message at a rate $R_{AB,fb} = C_{AB}$ just like in (Subsection 4.3). This discontinuity in $\gamma = 0$ is why in (4.43) we have to compare the result of the maximization over γ (corresponding to the mixed scheme) with the rate achieved by the pure feedback scheme. If $\gamma = 0.5$, we have $R_c^* = 0$, and $R_e^* = C_{AB} - C_{AE} = C_s$, resulting in Wyner's original scheme [12] – hence no discontinuity in $\gamma = 0.5$. Any value of γ in the open interval $(0, 0.5)$ results in a combination of the two schemes.

Some more numerical results

To illustrate the performance of our second approach to implementing the feedback-based secrecy scheme, we consider a model in which the forward channels have crossover probabilities $\epsilon_f = 0.01$ and $\delta_f = 0.02$, respectively. The secrecy rate achievable by Wyner's original scheme is $C_s = 0.06$.

In Figure 4.6 we show the overall achievable secrecy rate when we use our feedback scheme, for different values of the crossover probabilities characterizing the feedback channels. The corre-

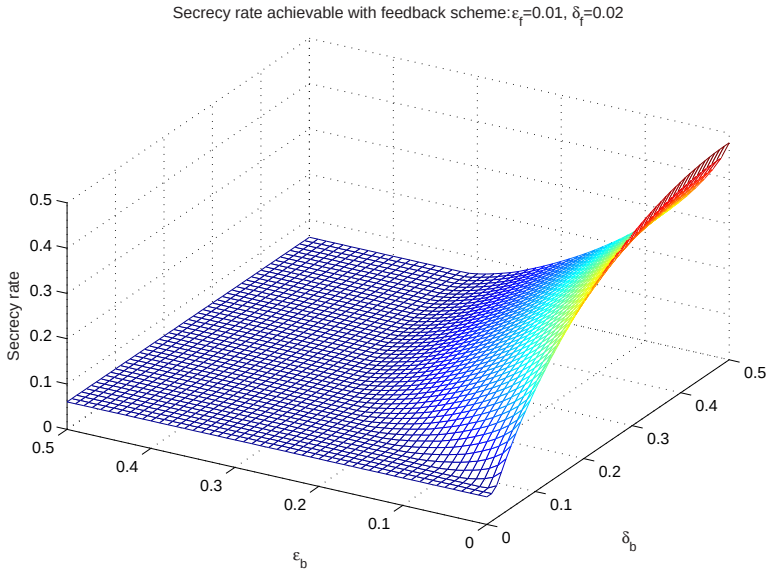

FIGURE 4.6. Secrecy rate achievable by the feedback scheme for $\epsilon_f = 0.01$ and $\delta_f = 0.02$.

sponding optimal value of the parameter γ is given in Figure 4.7. Recall that whenever $\gamma = 0.5$, our feedback scheme reduces to Wyner's scheme, and hence the achievable secrecy rate is C_s. Also, when $\gamma = 0$, our scheme uses the whole capacity C_{AB} of Bob's forward channel to convey a secret message encoded with the help of the feedback sequence (no additional directly encoded secret message is present). The improvements are significant.

4.5 The Third Approach: The Reversed Feedback Scheme

The feedback-based scheme discussed in the previous section encodes two secret messages into the sequence transmitted over the forward channel. The main idea behind this construction is based on the capability of the legitimate transmitter (Alice) to transmit two types of messages simultaneously [13]: a first secret message to Bob, and a common message to both Bob and Eve. In our case, the common message carries a second secret message, the encoding of which is based on artificially degrading Eve's equivalent channel by the use of a feedback sequence. But on a deeper level, the encoding of both secret messages uses the same principle developed in [12], and none of them uses an explicit secret key.

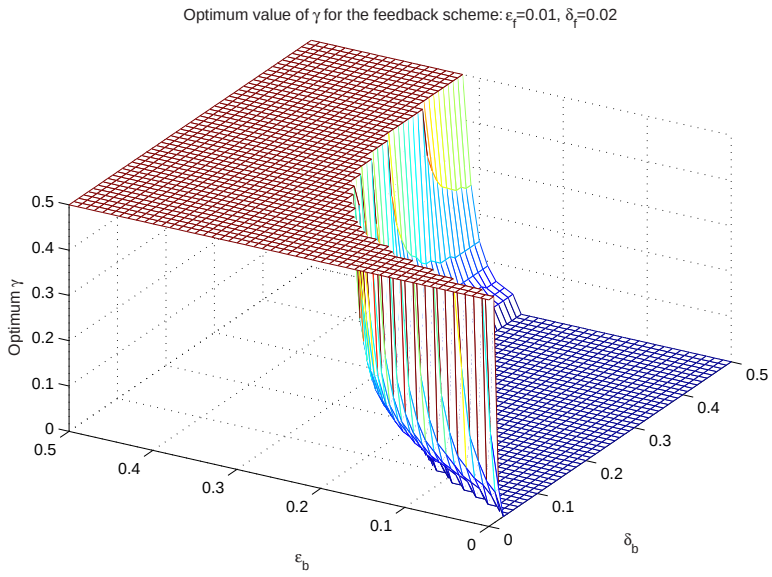

FIGURE 4.7. The optimal value of γ for the feedback scheme when $\epsilon_f = 0.01$ and $\delta_f = 0.02$.

In this section, we discuss another approach to increasing the secrecy rate, namely when the feedback-based scheme is used on the reversed channel (in the sense that the secret message encoded with the help of our feedback-based scheme is now transmitted from Bob to Alice instead of from Alice to Bob) to send a secret key from Bob to Alice, much like in [42] and [1] (in fact the scenarios of [42] and the correct part of [1] can be considered as special cases of our reversed mixed feedback scheme.). Alice can subsequently use this secret key as a one-time pad, for transmitting a secret message of the same entropy [43] to Bob.

Although this new protocol requires more bandwidth than the previous one, it can sometimes achieve better overall performance in terms of rate-equivocation region and secrecy rate. However, this can only happen under the (necessary but not sufficient) condition that the rate at which the secret key is transmitted from Bob to Alice exceeds the secrecy rates achievable by the original feedback scheme.

Denote by $R_{s,p}$ the supremum of the rates at which Bob can transmit a secret key (or a one-time pad) to Alice by using the feedback scheme developed in the previous section on the reversed

channel. Note that $R_{s,p}$ can be obtained from the expression of $R_{s,0}$ in (4.43) by replacing ϵ_f by ϵ_b, δ_f by δ_b, and vice versa.

To acquire this secret key, Alice and Bob engage in a protocol which is the reversed version of the one described in the previous sections. Alice broadcasts a random feedback sequence of n bits. Bob can then encode k_1 secret bits into an n-sequence, which is added $\mod 2$ to Bob's received feedback sequence, and then the result is further encoded into an M-sequence for asymptotically error free transmission over the $B \to A$ and $B \to E$ channels.

If $C_{BA} > C_{BE}$, the same M-sequence can carry an additional secret message of k_2 bits. A number of $M + n$ channel uses are thus required for the transmission of a $k_r = k_1 + k_2$-bit secret key $\mathbf{r}^{k_r}$, and are accounted for in the expression of $R_{s,p}$ (that is, $R_{s,p} = \frac{k_r}{M+n}$).

After adding the secret key $\mathbf{r}^{k_r}$ to a secret message $\mathbf{s_r}^{k_r}$ of her own (also a k_r-bit sequence), Alice encodes the result into an M'-sequence for the forward channel. Note here that because Alice uses a secret key, the secrecy of $\mathbf{s_r}^{k_r}$ is preserved (by the Crypto lemma [44]) even if Eve has perfect access to the resulting k_r-bit sum sequence $\mathbf{r}^{k_r} \oplus \mathbf{s_r}^{k_r}$.

At this point, Alice could choose to encrypt everything she transmits to Bob. However, that strategy would require the generation of a long secret key, and hence cause a large rate loss due to feedback – recall that in our results we count the bandwidth expenditure due to feedback. Instead, a mixed secrecy encoding strategy on the forward link may be optimal. For example, a special adaptation of our reversed feedback scheme is possible when $C_{AB} > C_{AE}$. Recall that in Section 4.4 we made a comment about the possibility to transmit a secret message, encoded in the cosets of a code, at a rate arbitrarily close to the secrecy capacity $C_s = \max\{C_{AB} - C_{AE}, 0\}$, while using the feedback-processed sequence $\mathbf{v} \oplus \mathbf{y}$ (that was carrying a separate secret message) for selecting the exact coset representative to be transmitted. In Section 4.4 this was not possible due to the fact that Eve had some information about $\mathbf{v} \oplus \mathbf{y}$, from its received feedback sequence $\mathbf{x} \oplus \mathbf{e_{bE}}$. In the present scenario, however, the message $\mathbf{r}^{k_r} \oplus \mathbf{s}^{k_r}$ is totally unknown to Eve, and can be safely used for selecting the coset representative.

Thus, a first k_0-bit secret message – denote it by $\mathbf{s_0}^{k_0}$ – can be transmitted from Alice to Bob using Wyner's original scheme [12], at a rate $\frac{k_0}{M'} \simeq C_s$. A second secret message $\mathbf{s_r}^{k_r}$ can be transmitted at a rate $\frac{k_r}{M'} \simeq C_F$ (we denoted $C_F = \min\{C_{AB}, C_{AE}\}$) by using the secret key $\mathbf{r}^{k_r}$ generated through a reversed feedback scheme.

With this notation, and taking into account all $n+M+M'$ channel uses involved in the protocol (i.e. n for the reversed feedback sequence from Alice to Bob, M for the transmission of the secret key from Bob to Alice, and M' for the transmission of the secret message from Alice to Bob), we can write the overall achievable secrecy rate as

$$R_{s,rf} = \frac{k_0 + k_r}{n + M + M'} = \frac{M'}{n + M + M'}(C_s + C_F) = C_{AB}\frac{R_{s,p}}{C_F + R_{s,p}}, \tag{4.44}$$

where in the second equality we used the fact that $C_F + C_s = C_{AB}$ and that

$$\frac{M'}{n + M + M'} = \frac{k_r/(n+M)}{k_r/M' + k_r/(n+M)} = \frac{R_{s,p}}{C_F + R_{s,p}}. \tag{4.45}$$

An observation is now in order. Note that employing Wyner's original scheme, when possible, in addition to the encryption by the secret key generated by the reversed feedback-based scheme, is always optimal. Indeed, Wyner's scheme guarantees the transmission of a secret message without wasting any resources other than the M' bits of the forward channel sequence, while encrypting a message by a secret key generated as above requires additional resources that grow linearly with the size of the secret key. Therefore, for instance, generating a secret key long enough to encrypt the whole secret message (of size $M'C_{AB}$ bits) yields an achievable secrecy rate equal to $C_{AB}\frac{R_{s,p}}{C_{AB}+R_{s,p}}$, thus is always outperformed by our combination of encryption and Wyner's scheme.

Numerical Results

For the first data set, of Section 4.3, ($\epsilon_f = 0.02$ and $\delta_f = 0.01$), the achievable secrecy rate and the optimal γ for the reversed feedback scheme are given in Figures 4.8 and 4.9.

The improvement in the overall secrecy rate when using the reversed feedback scheme instead of the regular feedback scheme, i.e. the function $\max\{0, R_{s,rf} - R_0\}$, is shown in Figure 4.10. Note

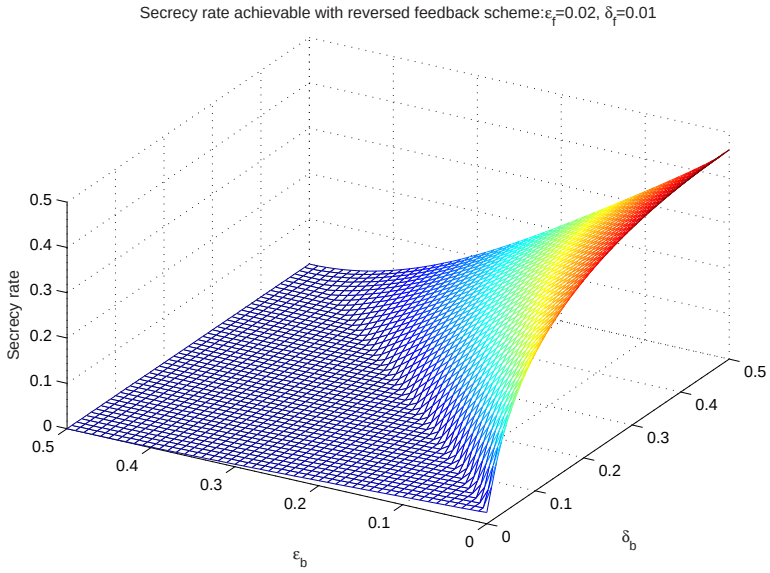

FIGURE 4.8. Overall secrecy rate achievable by the reversed feedback scheme for $\epsilon_f = 0.02$ and $\delta_f = 0.01$.

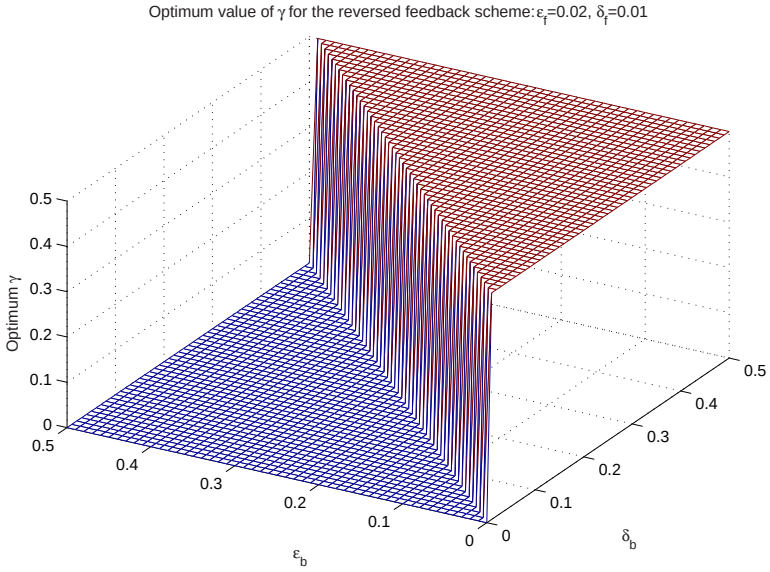

FIGURE 4.9. The optimal value of γ for the reversed feedback scheme when $\epsilon_f = 0.01$ and $\delta_f = 0.02$.

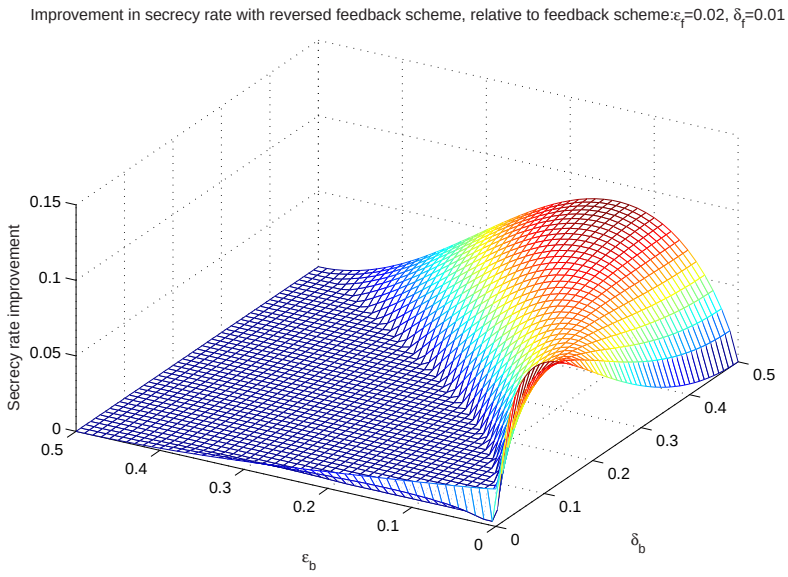

FIGURE 4.10. Improvement in overall secrecy rate when using the reversed feedback scheme instead of the regular feedback scheme: $\epsilon_f = 0.02$ and $\delta_f = 0.01$. Represented is the function $\max\{0, R_{s,rf} - R_0\}$.

that the reversed mixed feedback scheme is usually a better choice when Eve's feedback channel is worse than Alice's (i.e. $\delta_b > \epsilon_b$).

For the second data set, of Section 4.4, ($\epsilon_f = 0.01$ and $\delta_f = 0.02$), the secrecy rate $R_{s,f}$ achievable by the reversed mixed feedback scheme is given in Figure 4.11, and the improvement over the regular mixed feedback scheme is depicted in Figure 4.9. Once again, the reversed feedback scheme performs better when $\delta_b > \epsilon_b$. It is also interesting to note the existence of a region in the (ϵ_b, δ_b) plane (around the diagonal $\epsilon_b = \delta_b$), where our regular mixed feedback scheme beats Wyner's scheme even when $\epsilon_b > \delta_b$, and it also beats the reversed mixed feedback scheme even when $\epsilon_b < \delta_b$.

4.6 Conclusions

We presented a scheme that achieves a strictly positive secrecy rate even if the eavesdropper's channel is better than the legitimate receiver's channel, and improves the achievable secrecy rate if the eavesdropper's channel is worse.

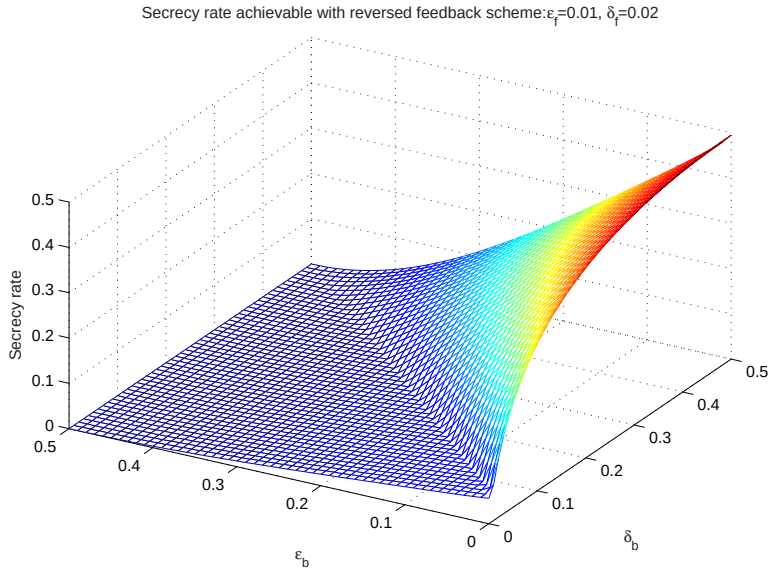

FIGURE 4.11. Secrecy rate achievable by the reversed feedback scheme for $\epsilon_f = 0.01$ and $\delta_f = 0.02$.

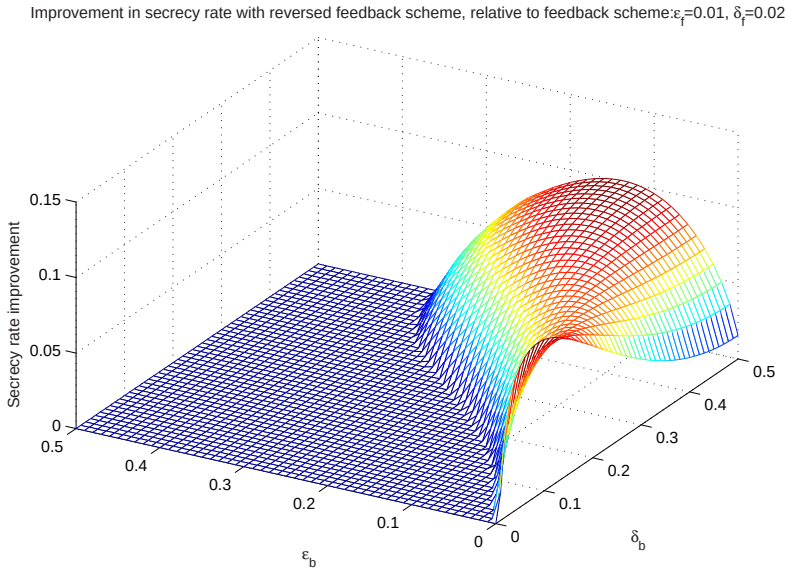

FIGURE 4.12. Improvement in secrecy rate when using the reversed feedback scheme instead of the regular feedback scheme: $\epsilon_f = 0.01$ and $\delta_f = 0.02$. Represented is the function $\max\{0, R_{s,rf} - R_0\}$.

TABLE 4.1. Possible implementation of our feedback-based secrecy scheme.

Channel conditions	Possible implementation
$C_{BA} \leq C_{BE}$ $C_{AB} \leq C_{AE}$	Pure feedback scheme
$C_{BA} > C_{BE}$ $C_{AB} \leq C_{AE}$	Pure feedback scheme OR Reversed mixed feedback scheme
$C_{BA} \leq C_{BE}$ $C_{AB} > C_{AE}$	Mixed feedback scheme OR Reversed pure feedback scheme
$C_{BA} > C_{BE}$ $C_{AB} > C_{AE}$	Mixed feedback scheme OR Reversed mixed feedback scheme

We proposed several collaborative secrecy encoding methods, all of which use our feedback scheme. Depending on the channel conditions, the possible ways in which the feedback-based scheme can be used are summarized in Table 4.1. The term *pure feedback scheme* in Table 4.1 denotes the feedback scheme as implemented in Section 4.3, i.e. without being mixed with Wyner's scheme, while *mixed feedback scheme* refers to the implementation of Section 4.4, under the optimal mixture between the pure feedback scheme and Wyner's scheme. Similar considerations hold for the *reversed pure/mixed feedback scheme* (see Section 4.5).

Our scheme requires a new random sequence to be fed back from Bob, for each codeword that Alice wants to send over the forward channel, in a manner similar to the one-time pad. We have shown that Theorem 4 in [20], which provides an upper bound on the achievable secrecy rate when the public channel is error free, does not hold if this condition is not satisfied. The derivation of such an upper bound for the more realistic scenario with imperfect public channels is still under our investigation.

The main advantage of our scheme is that it makes physical layer security protocols implementable with only minor restrictions imposed on the eavesdropper's channel, restrictions which can be easily ensured by perimeter defense (transmission power is low enough to guarantee a minimum error probability for any terminal situated outside a safe perimeter).

4.7 Additional Results. Why the Approach of [1] Is Wrong

Since the ideas of [1] are closely related to our feedback secrecy encoding scheme, and since [1] suffers from several subtle flaws, we dedicate this section to pointing out the following three.

First, all the rates of [1] are expressed without considering the expense of channel uses due to feedback. While this may seem like a minor inconvenience as far as the forward channel rates are involved, it becomes a problem when the forward channel rates are mixed with orthogonal feedback channel rates, as in sections 3 and 4 of [1]. More specifically, the secrecy rate achievable by Wyner's scheme on the forward channel cannot be added to the rate at which the secret key is generated over the orthogonal feedback channel unless both channels use the exact same codeword length.

Second, even if both the feedback and forward channels used the same codeword length, the time sharing idea of [1] is meaningless. It is claimed in [1] that time sharing is performed between two modes of operation on the feedback channel: Wyner's regular scheme, and our feedback secrecy scheme. With the notation of [1], the two modes of operation would normally yield secrecy rates $C_s^b = [h(\delta_b) - h(\epsilon_b)]^+$ (Wyner's scheme) and $R_{fbs} = h(\epsilon_b + \delta_b - 2\epsilon_b\delta_b) - h(\epsilon_b)$ (our feedback scheme). Thus, the optimal time sharing between these schemes is to always use our feedback secrecy scheme (i.e. $\alpha = 0$ always in [1]) since $R_{fbs} > C_s^b$ regardless of the channel parameters.

Third, our secrecy feedback scheme cannot be mixed with Wyner's secrecy scheme the way that was claimed in section 4 of [1]. If mixing is desired, special care should be taken to ensure that Eve's information about the random feedback sequence, obtained on the feedback channel, does not compromise the secrecy of Wyner's scheme. We have already mentioned this in Section 4.4. In the following, we give a more detailed explanation of this account. With the notation on Section 4.4, consider the secret message encoded by Wyner's scheme $\mathbf{s}^{k_2}$, Alice's transmitted sequence $\mathbf{w}_{\mathbf{A}}^{\mathbf{M}}$, and Eve's received sequence $\mathbf{w}_{\mathbf{E}}^{\mathbf{M}}$. The key to Wyner's secrecy scheme is to employ an encoding scheme that guarantees that $H(\mathbf{w}_{\mathbf{A}}^{\mathbf{M}}|\mathbf{w}_{\mathbf{E}}^{\mathbf{M}}, \mathbf{s}^{k_2})$ is arbitrarily small, and that $H(\mathbf{w}_{\mathbf{A}}^{\mathbf{M}}|\mathbf{s}^{k_2})$ is arbitrarily close to $I(\mathbf{w}_{\mathbf{A}}^{\mathbf{M}}; \mathbf{w}_{\mathbf{E}}^{\mathbf{M}})$ [12]. Indeed, this is how the encoding in [1] is performed.

However, recall that due to the feedback scheme, Eve also has access to a distorted version $\mathbf{z}$ of Bob's feedback sequence $\mathbf{x}$. Although $H(\mathbf{w}_{\mathbf{A}}^{\mathbf{M}}|\mathbf{w}_{\mathbf{E}}^{\mathbf{M}}, \mathbf{z}, \mathbf{s}^{k_2})$ remains arbitrarily small, $H(\mathbf{w}_{\mathbf{A}}^{\mathbf{M}}|\mathbf{s}^{k_2})$ is not arbitrarily close to $I(\mathbf{w}_{\mathbf{A}}^{\mathbf{M}}; \mathbf{w}_{\mathbf{E}}^{\mathbf{M}}, \mathbf{z})$. This is because

$$I(\mathbf{w}_{\mathbf{A}}^{\mathbf{M}}; \mathbf{w}_{\mathbf{E}}^{\mathbf{M}}, \mathbf{z}) > I(\mathbf{w}_{\mathbf{A}}^{\mathbf{M}}; \mathbf{w}_{\mathbf{E}}^{\mathbf{M}}) \Leftrightarrow H(\mathbf{w}_{\mathbf{A}}^{\mathbf{M}}|\mathbf{w}_{\mathbf{E}}^{\mathbf{M}}, \mathbf{z}) < H(\mathbf{w}_{\mathbf{A}}^{\mathbf{M}}|\mathbf{w}_{\mathbf{E}}^{\mathbf{M}}).$$

Note that if we had $H(\mathbf{w}_{\mathbf{A}}^{\mathbf{M}}|\mathbf{w}_{\mathbf{E}}^{\mathbf{M}}, \mathbf{z}) = H(\mathbf{w}_{\mathbf{A}}^{\mathbf{M}}|\mathbf{w}_{\mathbf{E}}^{\mathbf{M}})$, then $\mathbf{z} \rightarrow \mathbf{w}_{\mathbf{E}}^{\mathbf{M}} \rightarrow \mathbf{w}_{\mathbf{A}}^{\mathbf{M}}$ would form a Markov chain. But by the very construction of the feedback scheme, we have that $\mathbf{z} \rightarrow \mathbf{w}_{\mathbf{A}}^{\mathbf{M}} \rightarrow \mathbf{w}_{\mathbf{E}}^{\mathbf{M}}$ form a Markov chain, and hence $H(\mathbf{z}|\mathbf{w}_{\mathbf{A}}^{\mathbf{M}}) = H(\mathbf{z}|\mathbf{w}_{\mathbf{E}}^{\mathbf{M}})$, which would imply that no information about $\mathbf{z}$, or equivalently about $\mathbf{x}$ is lost over the forward channel. In other words, Eve has perfect access to the auxiliary message that picks the exact bin representative to be transmitted by Wyner's scheme [12], and this contradicts the results of [13].

4.8 Additional Results. The Optimal Tradeoff between the Secret Rate and the Common Rate

In Section 4.4 we have already shown that for an eavesdropper channel with input (at Alice) X and outputs Y at the legitimate receiver (Bob) and Z at the eavesdropper (Eve), for which the Bob's channel is less noisy than Eve's channel, a pair of one secret and one common messages can be transmitted with asymptotically zero average error probability if and only if the rate R_e of the secret message and the rate R_c of the common message satisfy

$$R_e \leq I(X;Y|U) - I(X;Z|U) \tag{4.46}$$

and

$$R_c \leq I(U;Z), \tag{4.47}$$

where U is an auxiliary random variable such that $U \rightarrow X \rightarrow YZ$ form a Markov chain. This result is a straightforward particularization of Theorem 1 in [13], for the case when Bob's channel is less noisy and we are only concerned with common and secret messages. From an application

point of view, an efficient communications system that uses the framework in [13] to transmit two such messages should operate on the boundary of the (R_e, R_c) rate region. For example, once R_c is set to a fixed value R_c^*, the system should aim to use the maximum secrecy rate R_e available under these circumstances. This is equivalent to finding the optimal auxiliary random variable U, and the optimal relation (we shall henceforth denote this relation by the term "channel") between U and X, that maximize R_e for a given value of R_c.

To the best of our knowledge, at present there exist no studies that solve the above problem, even for the simplest of cases. In this section, we do just that: we prove that when all channels are binary and symmetric (BSC), the boundary of the (R_e, R_c) rate region is achieved by a binary auxiliary random variable U, which is connected to the channel input random variable X through a BSC. Theorem 4.8 below formalizes our results.

Theorem 4.8. *Consider a main channel and an eavesdropper channel modeled as BSCs with crossover probabilities ϵ and δ, respectively, such that $\epsilon < \delta$ and $\epsilon, \delta \in [0, 0.5]$. Any point on the boundary of the (secret message rate, common message rate) rate region can be written as (R_e^*, R_c^*), where*

$$R_c^* = 1 - h(\gamma + \delta - 2\gamma\delta), \tag{4.48}$$

$$R_e^* = [h(\delta) - h(\epsilon)] - [h(\gamma + \delta - 2\gamma\delta) - h(\gamma + \epsilon - 2\gamma\epsilon)], \tag{4.49}$$

γ is a parameter that can take values in $[0, 0.5]$, and $h(\cdot)$ is the binary entropy function.

Proof. We prove the theorem in two steps. First we show that no generality is lost by taking U to be a binary random variable in (4.46) and (4.47). Next we prove that only a uniform distribution

of U, combined with a binary symmetric channel between U and X can achieve a point on the boundary of our rate region.

Step I: The random variable U can be considered binary

Following the proof of the admissibility of the size constraints in [13], we make the following denotations:

$$f_x(\mathbf{p}) = Pr(X = 0|\mathbf{p}) = \mathbf{p}(0) = p, \tag{4.50}$$

$$f_y(\mathbf{p}) = H(Y|\mathbf{p}) = h(\epsilon + p - 2\epsilon p), \tag{4.51}$$

$$f_z(\mathbf{p}) = H(Z|\mathbf{p}) = h(\delta + p - 2\delta p), \tag{4.52}$$

where $\mathbf{p}$ denotes the probability mass function (p.m.f.) of X, while $f_y(\mathbf{p})$ and $f_z(\mathbf{p})$ are the respective entropies of Y and Z, when X has the p.m.f. given by $\mathbf{p}$. In the remainder of this section we shall denote $a \to b = a + b - 2ab$, as the formula is the same as that of the crossover probability of a concatenation of two BSCs with respective crossover probabilities a and b.

Think of $\mathbf{p}$ as a function under the control of the random variable U. Thus, for any u in the alphabet of U, if $U = u$, then the p.m.f. of X becomes $\mathbf{p}_u$. We can now write, as in [13],

$$Pr(X = 0) = \sum_u Pr(U = u) f_x(\mathbf{p}_u), \tag{4.53}$$

$$I(U;Z) = H(Z) - H(Z|U) = H(Z) - \sum_u Pr(U = u) f_z(\mathbf{p}_u), \tag{4.54}$$

$$I(X;Y|U) = H(Y|U) - H(Y|X) = \sum_u Pr(U = u) \left[f_y(\mathbf{p}_u) - h(\epsilon) \right], \tag{4.55}$$

and

$$I(X;Z|U) = H(Z|U) - H(Z|X) = \sum_u Pr(U = u) \left[f_z(\mathbf{p}_u) - h(\delta) \right], \tag{4.56}$$

where we used the fact that $U \rightarrow X \rightarrow YZ$ form a Markov chain and that $H(Z|X)$ and $H(Y|X)$ are independent of the actual probability distribution of X (the variables are related through BSCs). Note that $H(Z)$ is completely determined by the channel coefficients ϵ and δ and by $Pr(X = 0)$ defined in (4.53).

Consider the triple $(f_x(\mathbf{p}), f_y(\mathbf{p}), f_z(\mathbf{p})) = (p, h(\epsilon + p - 2\epsilon p), h(\delta + p - 2\delta p))$ and note that all of the quantities in (4.53) - (4.56) above are expressed in terms of the same convex combination of one of the members of our triple. In other words, any set of feasible values for the quantities in (4.53) - (4.56) is uniquely determined by a point in the convex hull of the set $\mathscr{C} = \{(p, h(\epsilon + p - 2\epsilon p), h(\delta + p - 2\delta p))|p \in [0, 0.5]\}$, which is a 3D space curve. Note here that for any $p \in [0.5, 1]$ we can find a $p' \in [0, 0.5]$ that yields the same values for $I(U; Z)$, $I(X; Y|U)$ and $I(X; Z|U)$.

By Caratheodory's theorem, since $\mathscr{C} \subset \mathbb{R}^3$, any point in the convex hull of $\mathscr{C}$ can be expressed as a convex combination of only four points belonging to $\mathscr{C}$. Using the same strengthened version of Caratheodory's theorem, due to Eggleston (Theorem 18 (ii) on page 35 of [46]), as in [13], we can state that, since $\mathscr{C}$ is a *connected* subset of $\mathbb{R}^3$, any point in its convex hull can be expressed as a convex combination of only three points belonging to $\mathscr{C}$. In Lemma 4.9 following this proof we conjecture that, due to the special form of the set $\mathscr{C}$, we can actually express any point in its convex hull as the convex combination of only two of its points.

This implies that it is enough to consider only two values of p to be able to produce any triple of feasible values for the quantities in (4.55) - (4.56). But since p is controlled by the value of the auxiliary random variable U, we can therefore let U be binary. This completes the first step of our proof.

Step II: The optimal distribution of U is uniform and the optimal channel from U to X is a BSC

We have established that the auxiliary random variable U can be considered binary. Let U belong to $\{0, 1\}$, and denote $q = Pr(U = 0)$. Since X is also binary, the channel between U and X can

be completely characterized by two transition probabilities. Denote $\alpha = Pr(X = 1|U = 0)$ (this implies $Pr(X = 0|U = 0) = 1 - \alpha$), and $\beta = Pr(X = 0|U = 1)$ (this implies $Pr(X = 1|U = 1) = 1 - \beta$).

Note that (4.46) and (4.47) can be rewritten as:

$$R_e \leq [H(Z|X) - H(Y|X)] - [q(H(Z|U = 0) - H(Y|U = 0)) + \\ +(1 - q)(H(Z|U = 1) - H(Y|U = 1))] \tag{4.57}$$

and

$$R_c \leq H(Z) - [qH(Z|U = 0) + (1 - q)H(Z|U = 1)], \tag{4.58}$$

With the notation above, the upper bounds can be written as

$$R_{e,u}(q, \alpha, \beta) = [h(\delta) - h(\epsilon)] - [q(h(\alpha \to \delta) - h(\alpha \to \epsilon)) + \\ +(1 - q)(h(\beta \to \delta) - h(\beta \to \epsilon))] \tag{4.59}$$

and

$$R_{c,u}(q, \alpha, \beta) = h([q\alpha + (1 - q)(1 - \beta)] \to \delta) - [qh(\alpha \to \delta) + (1 - q)h(\beta \to \delta)], \tag{4.60}$$

where $a \to b$ stands for $a(1 - b) + b(1 - a) = a + b - 2ab$ as before, and we emphasized the dependence of the upper bounds upon the triple (q, α, β).

In what follows we take a contradictory approach. Consider any triple (q, α, β) and denote

$$R_x(q, \alpha, \beta) = 1 - [qh(\alpha \to \delta) + (1 - q)h(\beta \to \delta)]. \tag{4.61}$$

We show that if we replace this triple by the triple $(0.5, \gamma, \gamma)$ (corresponding to a uniform distribution of U over $\{0, 1\}$ and a BSC between U and X), such that

$$R_x(q, \alpha, \beta) = R_x(0.5, \gamma, \gamma) \tag{4.62}$$

(we also prove that such a γ exists always), we have $R_{e,u}(q,\alpha,\beta) \leq R_{e,u}(0.5,\gamma,\gamma)$ and $R_{c,u}(q,\alpha,\beta) \leq R_{c,u}(0.5,\gamma,\gamma)$. Therefore, a triple (q,α,β) for which either $q \neq 0.5$ or $\alpha \neq \beta$ holds cannot be optimal, and hence the last part of our theorem is proved.

Note that $R_x(q,\alpha,\beta) = R_x(0.5,\gamma,\gamma)$ translates to

$$qh(\alpha \to \delta) + (1-q)h(\beta \to \delta) = h(\gamma \to \delta), \tag{4.63}$$

Since $qh(\alpha \to \delta) + (1-q)h(\beta \to \delta) \in [0,1]$, the binary entropy function is a bijection over $[0,0.5]$ and $f(\gamma) = \gamma \to \delta$ with $\delta \in (0,0.5)$ is also a bijection over $[0,0.5]$, we can always find a γ that satisfies (4.63). Since $h([q\alpha + (1-q)(1-\beta)] \to \delta) \leq 1$ and $h([0.5\gamma + 0.5(1-\gamma)] \to \delta) = h(0.5 \to \delta) = 0$ it is straightforward to see that

$$R_{c,u}(q,\alpha,\beta) \leq R_x(q,\alpha,\beta) = R_x(0.5,\gamma,\gamma) = R_{c,u}(0.5,\gamma,\gamma). \tag{4.64}$$

We can now write

$$R_{e,u}(0.5,\gamma,\gamma) - R_{e,u}(q,\alpha,\beta) = h(\gamma \to \epsilon) - qh(\alpha \to \epsilon) + (1-q)h(\beta \to \epsilon). \tag{4.65}$$

Define $g(x) = h(\gamma \to x) - qh(\alpha \to x) + (1-q)h(\beta \to x)$. From (4.62) we have that $g(\delta) = 0$, and it is straightforward to see that $g(0.5) = 0$. Since we only discuss the case when $\delta < 0.5$, we now know that $g(x)$ has two different zeros over the interval $[0,0.5]$. We need to show that for any $\epsilon < \delta$ we have $g(\epsilon) > 0$.

Denote $g'(x) = \frac{dg(x)}{dx}$ and $g''(x) = \frac{d^2g(x)}{dx^2}$ the first and second order derivatives of g. With the notation $\mu(x) = \frac{x(1-x)}{(1-2x)^2}$, we can write g'' as in (4.66) below.

$$\begin{aligned} g''(x) &= \frac{q}{x(1-x)+\mu(\alpha)} + \frac{1-q}{x(1-x)+\mu(\beta)} - \frac{1}{x(1-x)+\mu(\gamma)} = \\ &= \frac{x(1-x)[\mu(\gamma) - q\mu(\alpha) - (1-q)\mu(\beta)] + \mu(\gamma)(q\mu(\beta) + (1-q)\mu(\alpha)) - \mu(\alpha)\mu(\beta)}{(x(1-x)+\mu(\alpha))(x(1-x)+\mu(\beta))(x(1-x)+\mu(\gamma))} \end{aligned} \tag{4.66}$$

Since the denominator of g'' is always positive, the equation $g''(x) = 0$ reduces to a second degree equation in x. Thus g'' has at most two real zeros, which are symmetric with respect to

the point 0.5, and hence at most one zero (denote it by z'') in the interval $[0, 0.5]$. Moreover, since $\mu(x)$ is a strictly convex function of x, the coefficient $-[\mu(\gamma) - q\mu(\alpha) - (1-q)\mu(\beta)]$ of x^2 in the numerator of g'' is strictly positive. This implies that $g''(x) > 0$ for $x \in [0, z'']$.

Now suppose that $g(x)$ had more than two zeros on the interval $[0, 0.5]$. Then $g'(x)$ would have at least two zeros on the open interval $(0, 0.5)$, and hence a total of three zeros in $[0, 0.5]$ (it is straightforward to check that $g'(0.5) = 0$). Thus g'' would need to have at least two zeros in $(0, 0.5)$. But we have already shown that this is impossible. Therefore, $g(x)$ has only two zeros in the interval $[0, 0.5]$ (these are δ and 0.5).

As a consequence, g' has at least one zero in $(\delta, 0.5)$ – denote this zero by z'. Since g' has a zero in 0.5, this implies that the zero z'' of g'' is in the interval $(z', 0.5)$. We can now write $\delta < z' < z''$. We already know that $g''(x) > 0$ on $[0, z'')$, thus $g'(x)$ is strictly increasing on $[0, z']$, and since $g'(z') = 0$, this means that $g'(x) < 0$ on $[0, \delta]$. But since $g(\delta) = 0$, this means that for any $\epsilon < \delta$ we have $g(\epsilon) > 0$.

Our proof is now complete. □

At this point, the following lemma remains a conjecture. However, it is stated as a lemma due to the fact that its proof reduces the problem tackled therein to the much simpler problem stated in Remark 4.10 below. Although we currently do not have a sound theoretical proof of Remark 4.10, its validity has been proved numerically for an extensive number of parameters.

Lemma 4.9. *Consider the 3D space curve given by* $\mathscr{C} = \{(p, h(\epsilon + p - 2\epsilon p), h(\delta + p - 2\delta p)) | p \in [0, 0.5]\}$. *Any point in the convex hull of* $\mathscr{C}$ *can be expressed as the convex combination of only two points belonging to* $\mathscr{C}$.

Proof. Recall the denotation $x \to p = x + p - 2xp$. The space curve $\mathscr{C}$, along with its projections onto the $(p, h(\epsilon \to p))$ and $(p, h(\delta \to p))$ planes, is represented in Figure 4.13. We shall henceforth call the p axis the "abscissa" axis, because it is the common abscissa axis of both $(p, h(\epsilon \to p))$ and $(p, h(\delta \to p))$ planes. Also represented in the figure is a random point M in the convex hull of

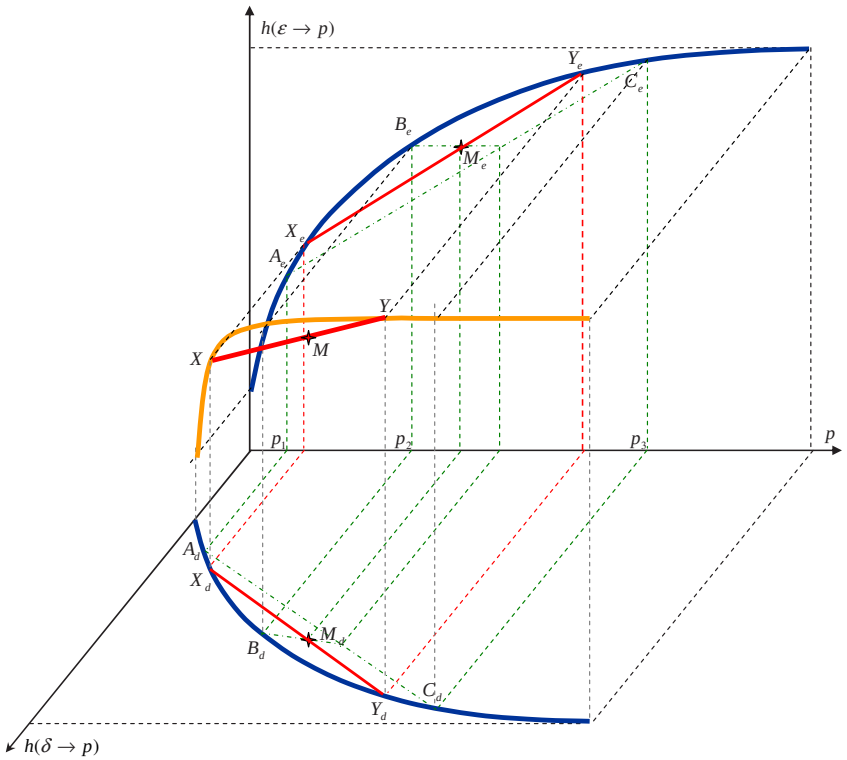

FIGURE 4.13. The space curve and its projections onto the $(p, h(\epsilon \to p))$ and $(p, h(\delta \to p))$ planes.

$\mathscr{C}$, which was obtained as the convex combination of three points A, B and C belonging to $\mathscr{C}$. Due to Eggleston's extension of Caratheodory's theorem [46], we know that any point in the convex hull of $\mathscr{C}$ can be obtained in this manner. Note that throughout this proof, we shall denote by P_d the projection of the point P onto the $(p, h(\delta \to p))$ plane, and by P_e the projection of the point P onto the $(p, h(\epsilon \to p))$ plane, for any point $P \in \{A, B, C, D, E, F, G, M, X, Y\}$. Moreover, we denote by $\mathscr{C}_d$ and $\mathscr{C}_e$ the projections of the space curve $\mathscr{C}$ on the two planes, respectively.

The present lemma shows that in fact the point M can be obtained as the convex combination of only two points of $\mathscr{C}$ - in Figure 4.13 these points were denoted by X and Y.

This is equivalent to showing that there exist two values p_x and p_y of p, such that if we denote the points $X_e = (p_x, h(\epsilon \to p_x))$, $X_d = (p_x, h(\delta \to p_x))$, $Y_e = (p_y, h(\epsilon \to p_y))$ and $Y_d = (p_y, h(\delta \to p_y))$, then M_e belongs to the line segment connecting X_e and Y_e, and simultaneously M_d belongs to the line segment connecting X_d and Y_d. At this point, assume that the following remark is true.

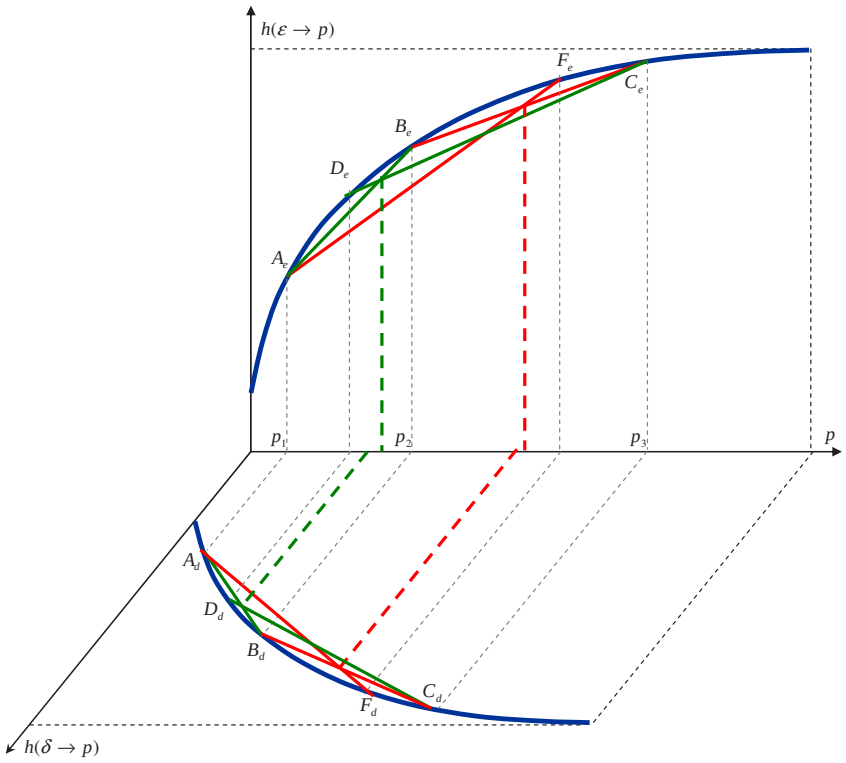

FIGURE 4.14. Projections of the space curve: simplified problem.

Remark 4.10. *(This remark has been checked numerically. However, we currently do not have a theoretical proof.) Consider four random points A, D, B, C on the space curve $\mathscr{C}$, such that their respective abscissae p_1, p_4, p_2, p_3 satisfy $p_1 < p_4 < p_2 < p_3$, and construct their projections A_e, D_e, B_e, C_e and A_d, D_d, B_d, C_d on the planes $(p, h(\epsilon \to p))$ and $(p, h(\delta \to p))$, respectively. Then the abscissa of the intersection of the segments A_eB_e and D_eC_e is greater than the abscissa of the intersection of the segments A_dB_d and D_dC_d. The result is illustrated in Figure 4.14 for two tuples of points, namely (A, D, B, C) and (A, B, F, C).*

Recall that the points A, B and C determine our point of interest M, that is $M = aA + bB + cC$, where $a, b, c \in [0, 1]$ and $a + b + c = 1$. This implies that the intersection between the segments A_eB_e and C_eM_e, and the intersection between A_dB_d and C_dM_d have the same abscissa, namely $\frac{ap_1+bp_2}{a+b}$. Due to Remark 4.10 above, this means that the segment C_eM_e intersects the curve $\mathscr{C}_e$ at a point E_e which has an abscissa $p_{1,e}$ which is less than the abscissa $p_{1,d}$ of the intersection D_d between C_dM_d and $\mathscr{C}_d$, as illustrated in Figure 4.15.

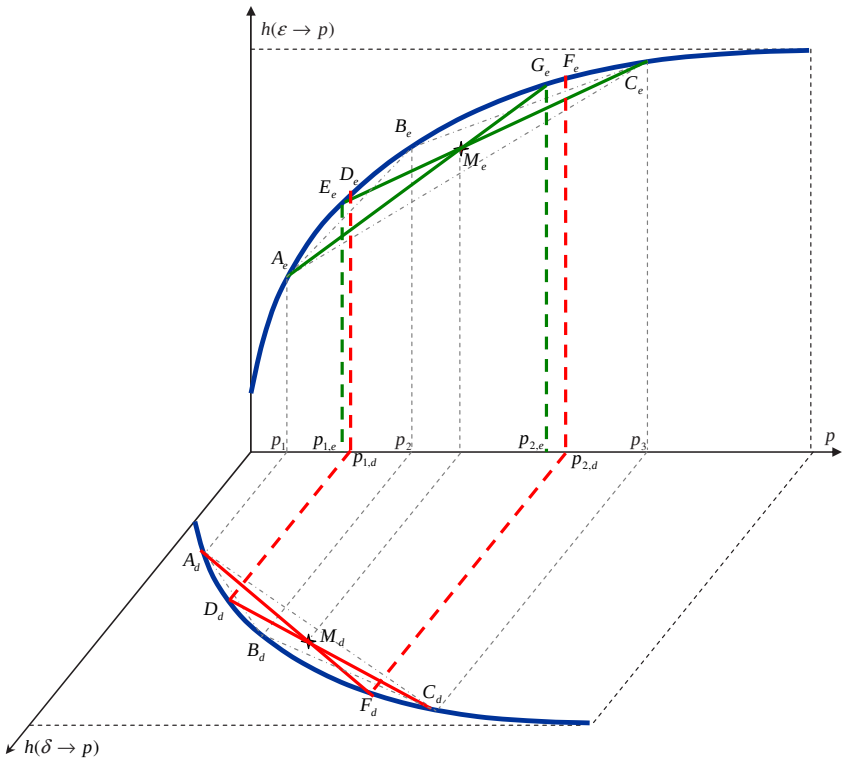

FIGURE 4.15. Projections of the space curve: existence of a solution.

Denote by D_e the point of $\mathscr{C}_e$ with the same abscissa $p_{1,d}$ as D_d. It is clear that the segment D_eC_e passes above the point M_e, while D_dC_d passes through M_d.

By a similar rationale, the intersection between the segments A_eM_e and B_eC_e, and the intersection between A_dM_d and B_dC_d have the same abscissa, namely $\frac{bp_2+cp_3}{b+c}$. Due to Remark 4.10, this means that the segment A_eM_e intersects the curve $\mathscr{C}_e$ at a point G_e which has an abscissa $p_{2,e}$ which is less than the abscissa $p_{2,d}$ of the intersection F_d between A_dM_d and $\mathscr{C}_d$ (see Figure 4.15). Denote by F_e the point of $\mathscr{C}_e$ with the same abscissa $p_{2,d}$ as F_d. It is clear that the segment A_eF_e passes below the point M_e, while A_dF_d passes through M_d.

This implies that there exists a value $p_x \in [p_1, p_{1,d}]$ of p such that, if we denote $X_e = (p_x, h(\epsilon \to p_x))$ and $X_d = (p_x, h(\delta \to p_x))$, then the segments X_eM_e and X_dM_d intersect the curves $\mathscr{C}_e$ and $\mathscr{C}_d$, respectively, at points Y_e and Y_d with the same abscissa $p_y \in [p_{2,d}, p_3]$. Hence X_e and X_d are the projections of a point $X \in \mathscr{C}$, and Y_e and Y_d are the projections of a point $Y \in \mathscr{C}$, and the segment XY goes through M. □

4.9 Additional Results. Extension to AWGN Channels – Binary Feedback

In this section we provide a simple (although not optimal) way to extend our previous results to the case where all channels are modeled as AWGN channels. Note that most of our arguments hold true for any type of forward $A \rightarrow B$ and $A \rightarrow E$ channels. Therefore, since the only difference is in the feedback $B \rightarrow A$ and $B \rightarrow E$ channels, we shall assume that the forward channels are error-free, as in Section 4.2.1.

Although modeled as AWGN channels, the actual behavior of the feedback channels depends on the feedback signal constellation. For simplicity, and as a first step toward an optimal scheme, we assume that Bob transmits a sequence of independent uniformly distributed bits, via a BPSK signal constellation. Denote by $\mathbf{x}_b$ the sequence of random bits transmitted by Bob, and by $\mathbf{x}$ the corresponding BPSK signal.[2]

Since the transmitted symbols are not correlated, and since Alice needs discrete alphabet sequences that act as input messages to her channel encoder, her best strategy is to perform hard decision on each symbol. Equivalently, the $B \rightarrow A$ AWGN channel is artificially transformed into a BSC with crossover probability $\epsilon_b = Q(\sqrt{\frac{P_b}{N_{BA}}})$, where $Q(x) = 1/\sqrt{2\pi}\int_x^\infty e^{-x^2/2}dx$, P_b is Bob's transmission power and N_{BA} is the variance of the white Gaussian noise characterizing the $B \rightarrow A$ channel. We denote $\mathbf{y}_b = \mathbf{x}_b \oplus \mathbf{e}_{BA,b}$, where $\mathbf{e}_{BA,b}$ is the error sequence, the components of which are independent realizations of the binary random variable E_{BA}, having $Pr(E_{BA} = 1) = \epsilon_f$. The rest of Alice's secrecy encoding works similarly to the binary case.

The actual difference from the all-BSC scenario however is that the hard decision decoding of the feedback signal is not optimal for Eve. Instead, Eve wants to use both her received feedback sequence $\mathbf{z} \in \mathbb{R}^n$ (recall Eve's feedback channel remains an AWGN channel) and her received

[2]Throughout this section, bold letters will denote sequences, capital letters will denote random variables, and the subscript $_b$ will be used to emphasize that the sequence or the random variable is binary. For example, $\mathbf{x}$ is a continuous waveform, $\mathbf{x}_b$ is its discrete, binary version, X is a random variable with an arbitrary alphabet, and X_b is a binary random variable.

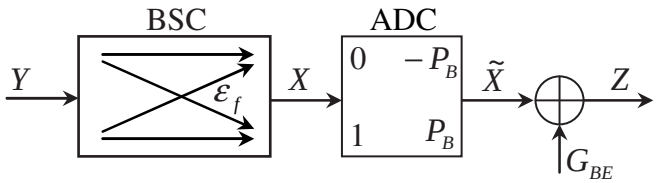

FIGURE 4.16. Eve's hybrid channel.

forward sequence $\mathbf{y}_b \oplus \mathbf{v}_b \in \{0,1\}^n$ (which is correlated with $\mathbf{z}$ through the term $\mathbf{y}_b$), for a soft detection of $\mathbf{v}_b$.

After performing the $\mod 2$ addition $\mathbf{y}_b \oplus \mathbf{v}_b \oplus \mathbf{x}_b$, Bob's equivalent forward channel yields $\widehat{\mathbf{v}}_\mathbf{b} = \mathbf{v}_b \oplus \mathbf{e}_{BA,b}$. A more subtle approach will be used to derive Eve's equivalent forward channel. Consider Eve's received forward sequence $\mathbf{y}_b \oplus \mathbf{v}_b$. Given $\mathbf{y}_b \oplus \mathbf{v}_b$, decoding for the data sequence $\mathbf{v}_b$ is equivalent to decoding for the noise-distorted feedback sequence $\mathbf{y}_b$, since any one of them is a deterministic function of the other when $\mathbf{y}_b \oplus \mathbf{v}_b$ is known. The number of messages that can be transmitted from Alice to Bob with asymptotically zero probability of error is given by the number of binary n-sequences $\mathbf{y}_b$ that can be supported by Bob's equivalent BSC. In other words, Bob estimates the sequence $\mathbf{y}_b$ based on the output $\mathbf{x}_b$ of his equivalent forward channel and the BSC crossover probability ϵ_f (we can write $\mathbf{x}_b = \mathbf{y}_b \oplus \mathbf{e}_{BA,b}$).

Since Eve does not have perfect access to $\mathbf{x}$, she first needs to estimate it from her received sequence $\mathbf{z}$. Thus, Eve's equivalent forward channel with input Y_b and output Z can be written as $Z = X + G_{BE}$ where

$$X = \begin{cases} P_B, & \text{if } X_b = 1 \\ -P_B, & \text{if } X_b = 0, \end{cases} , \tag{4.67}$$

$X_b = Y_b \oplus E_{BA,b}$ and G_{BE} is the $B \to E$ additive white Gaussian noise with probability distribution $p_G(q)$ of zero mean and variance N_{BE}. In other words, Eve's equivalent channel is a degraded version of Bob's equivalent channel, formed by concatenating Bob's BSC with an AWGN channel with noise variance N_{BE}, as in Figure 4.16

For this "hybrid" channel we can write the conditional probability densities:

$$p(z|Y_b = 0) = (1 - \epsilon_f)p_G(z + P_B) + \epsilon_f p_G(z - P_B), \tag{4.68}$$

$$p(z|Y_b = 1) = \epsilon_f p_G(z + P_B) + (1 - \epsilon_f)p_G(z - P_B), \tag{4.69}$$

and denoting $\alpha = P(Y_b = 0)$, the entropies:

$$\begin{aligned} H(Z|Y) = -\int_{-\infty}^{\infty} \Big[& \alpha p(z|Y_b = 0) \log p(z|Y_b = 0) + \\ & + (1 - \alpha)p(z|Y_b = 1) \log p(z|Y_b = 1) \Big] dz, \end{aligned} \tag{4.70}$$

$$\begin{aligned} H(Z) = -\int_{-\infty}^{\infty} \Big[& \alpha p(z|Y_b = 0) \log[\alpha p(z|Y_b = 0)] + \\ & + (1 - \alpha)p(z|Y_b = 1) \log[(1 - \alpha)p(z|Y_b = 1)] \Big] dz \end{aligned} \tag{4.71}$$

At this point we assume that the conjecture in [13] regarding the extension of all results to infinite alphabets holds true. This implies that the secrecy capacity of this system of degraded equivalent channels equals the maximum of the difference of mutual informations:

$$C_{s,u} = \max_{p_{Y_b}(y)} \left[I(Y_b; X_b) - I(Y_b; Z) \right]. \tag{4.72}$$

Chapter 5

Active Eavesdropping in Fast Fading Channels. A Block-Markov Wyner Secrecy Encoding Scheme

5.1 Introduction

A great number of recent works have been fueled by the still growing interest in physical layer secrecy. Most of them attempt to overcome the limitations of the classical wiretapper/eavesdropper scenarios of [12] or [13] (namely that no secret message can be successfully transmitted if the eavesdropper's channel is less noisy than the legitimate receiver's channel) by using some form of diversity.

The benefits of the ergodic-fading diversity upon the achievable secrecy rates have been exposed by works like [22], [23], [24] or [25]. A fast-fading eavesdropper channel is studied in [22] under the assumption that the main channel is a fixed-SNR additive white Gaussian noise (AWGN) channel. Although the secrecy capacity for fast-fading eavesdropper channels is still unknown, [22] provides achievable secrecy rates and shows that sometimes noise injection at the transmitter can improve these rates.

The different approach of [23] models both the main and the eavesdropper channels as ergodicly-fading AWGN channels. However, the fading is assumed to be slow enough to be considered constant for infinitely long blocks of transmitted symbols. The secrecy capacity is derived for this model, and the achievability part is proved by using separate channel encoding for each of the blocks. A similar approach is taken in [24] and [25], where the fading broadcast channel with confidential messages (BCC) is considered equivalent to a parallel AWGN BCC.

However, the slow fading ergodic channel model is quite restrictive. Although the model can be artificially created by a multiplexing/demultiplexing architecture as in [35], it still requires either coarse quantization or long delays (e.g. under fine quantization, for a channel state with low

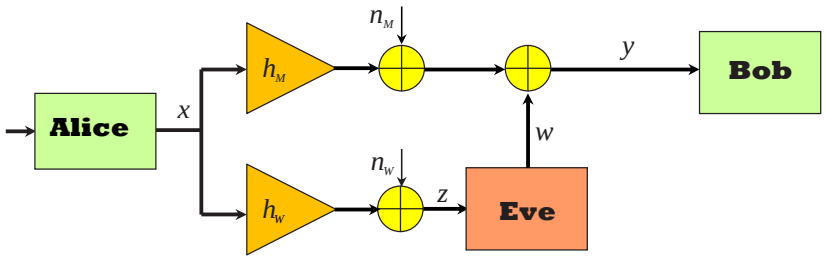

FIGURE 5.1. Channel model

probability it may take forever to gather a large enough number of transmitted symbols to enable almost-error-free decoding).

With these considerations, we focus instead on the more practical scenario where both the main and the eavesdropper's channel are affected by *fast* stationary fading. However, unlike [22], we are concerned with a much stronger adversary: an *active eavesdropper*.

In our channel model, depicted in Figure 5.1, the eavesdropper (Eve) has two options: either to jam the conversation between the legitimate transmitter (Alice) and the legitimate receiver (Bob) – Jx mode – or to eavesdrop – Ex mode – (our eavesdropper cannot function in full duplex mode, i.e. she cannot transmit and receive on the same frequency slot, at the same time). Both Alice and Eve (in Jx mode) are constrained by average (over each codeword) power budgets $\mathscr{P}$ and $\mathscr{J}$, respectively.

Eve's purpose is to minimize the secrecy rate achievable by Alice, and to that extent she has to decide on the optimal alternation between the jamming mode and the eavesdropping mode. The state of each of the main and eavesdropper channels, i.e. the absolute squared channel coefficients (or simply "the channel coefficients" hence forth), which we denote by h_M and h_W, respectively, are assumed to be available to the respective receivers. However, Bob does not know the exact state of Eve's channel, nor does Eve have any information about Bob's channel, except its statistics. In addition to fading, each channel is further distorted by an independent additive white complex Gaussian noise of variance σ_N^2. There exists a low-rate, unprotected feedback channel between Bob and Alice.

The present chapter is limited to the following simplifying (although not uncommon) assumptions: i) Rayleigh fading: h_M and h_W are exponentially distributed, with parameters λ_M and λ_W respectively; ii) the channel that links Eve (when in Jx mode) and Bob is error free and does not experience fading [10],[7]; iii) Eve only uses white Gaussian noise for jamming [38], [10], since this is the most harmful uncorrelated jamming strategy [30]; iv) Eve's exact jamming strategy (i.e. when and with what power she jams) is perfectly known to Bob (a posteriori) so that Bob can employ coherent detection and communicate Eve's strategy to Alice, via the low-rate feedback link; v) the instantaneous state of the main channel cannot be known to the transmitter Alice non-causally; vi) the codewords are long enough such that not only the channel fading, but also the combination of channel fluctuation and Eve's alternation between jamming and eavesdropping display ergodic properties over the duration of a codeword; vii) Eve employs an ergodic strategy, i.e. she uses the same statistics for alternating between Jx mode and Ex mode for every codeword. Our contributions can be stated as follows:

- In Section 5.2 we study the minimax scenario (where the objective – to be minimized by Eve and maximized by Alice and Bob – is the achievable secrecy rate), or *the best-case scenario*, when Eve's strategy is known to both Alice and Bob, in advance.

- We show that, even for this scenario, depending on how Eve uses her channel state information (about the exact values of h_W) in elaborating her strategy, the active eavesdropper can induce moderate to severe degradation of the achievable secrecy rate.

- The maximin scenario, or *the worst-case scenario*, when Alice and Bob have to plan for the situation where Eve can find out their transmission strategy, is studied in Section 5.3.

- We show that Wyner's scheme [12] performs poorly (if at all) in these conditions, and we provide a novel block-Markov Wyner secrecy encoding scheme, which requires a low-rate, unprotected feedback from Bob to Alice and can improve the secrecy rate significantly.

5.2 The Best-Case Scenario

In this section we study the scenario where the legitimate transmitter (Alice) and the legitimate receiver (Bob) know Eve's strategy in advance, i.e. they have access to the exact statistical description of how Eve alternates between jamming and eavesdropping (note that the statistical description is enough to fully characterize Eve's strategy under our channel model). Although this is not the most practical assumption, the present scenario is significant for both comparison purposes and demonstrating the devastating effect of an active eavesdropper upon the achievable secrecy rate.

The fact that Eve can alternate between jamming and eavesdropping causes a modification of the channel statistics. In other words, we can view the active eavesdropper's interference as a change of the channel coefficients. Indeed, whenever Eve is in Ex mode, the main channel instantaneous SNR is $\frac{h_M P}{\sigma_N^2}$, while the SNR of Eve's channel is $\frac{h_W P}{\sigma_N^2}$ – no change here. However, when Eve is in Jx mode, the main channel instantaneous SNR is $\frac{h_M P}{\sigma_N^2+J}$, where J is the instantaneous jamming power, while the SNR of Eve's channel is zero (recall that whenever Eve jams, she cannot simultaneously listen on the same frequency slot). We denote the *equivalent* channel coefficients as

$$\widetilde{h_M} = \begin{cases} h_M & \text{if Ex mode} \\ \frac{h_M \sigma_N^2}{\sigma_N^2+J} & \text{if Jx mode} \end{cases} \tag{5.1}$$

and

$$\widetilde{h_W} = \begin{cases} h_W & \text{if Ex mode} \\ 0 & \text{if Jx mode.} \end{cases} \tag{5.2}$$

Note that our equivalent channel coefficient approach is similar to the one in [29] which shows that a fixed codebook can achieve the power-control ergodic capacity of the fast-fading channel. Also, our equivalent channel coefficients display ergodic properties over a frame, according to assumptions vi) and vii) of the previous section.

Denote by X the random variable at the input of the two channels, and by Y and Z the corresponding random variables received by Bob and Eve, respectively. According to [13], the secrecy

capacity of our model (if the realizations of the random variables representing the equivalent channel coefficients $\widetilde{H_M}$ and $\widetilde{H_W}$ are known to Bob and Eve respectively, and hence can be considered as outputs of the channel) is given by

$$\begin{aligned} C_s &= \max_{V \to X \to YZ} \left[I(V; Y, \widetilde{H_M}) - I(V; Z, \widetilde{H_W}) \right] \geq \\ &\geq \max_{V \to X \to YZ} \left[I(V; Y|\widetilde{H_M}) - I(V; Z|\widetilde{H_W}) \right], \end{aligned} \tag{5.3}$$

where the maximization is over all joint probability distributions of V and X such that $V \to X \to YZ$ form a Markov chain. The inequality in (5.3) follows from the independence between V and H_W, and holds with equality if V is also independent of H_M (i.e. Alice has no channel state information – CSI). Since the optimal choice of V and X is presently unknown, we shall henceforth concentrate on the *achievable secrecy rate* (instead of secrecy capacity) obtained by setting $V = X$ and picking a complex Gaussian distribution for X, with zero mean and variance P. Under these constraints, the achievable secrecy rate becomes:

$$R_s = \mathbf{E}_{\widetilde{h_M}, \widetilde{h_W}, P} \left[\log(1 + \frac{\widetilde{h_M} P}{\sigma_N^2}) - \log(1 + \frac{\widetilde{h_W} P}{\sigma_N^2}) \right], \tag{5.4}$$

where P is the instantaneous transmitter scaling power [29] and is subject to the constraint $\mathbf{E}P \leq \mathscr{P}$. Note that the statistical information about Eve's strategy allows Alice and Bob to design a codebook, based on Wyner's encoding scheme [12], tailored to this strategy. We have already mentioned that the only party that has any control upon the actual equivalent channel coefficients is Eve. Since Alice has no CSI, her only option of being active against the eavesdropper is to randomize the scaling power P. However, as we shall see shortly, a constant power allocation is the optimal strategy for Alice. Eve's strategy consists of choosing when to eavesdrop and when to jam, and for the latter case picking a proper distribution (over the channel uses within a codeword) of her power budget $\mathscr{J}$. Depending on whether Eve can use the knowledge about her own channel coefficient h_W for employing her strategy, we have two different cases.

5.2.1 Channel Coefficients Available to Eve after Decision on Jx or Ex Mode

In this first case, Eve can know the exact value of h_W only after she made her decision to eavesdrop (Ex mode), and has no information about the value(s) that h_W might take while she is in Jx mode. This scenario models a situation where the training sequences, which are transmitted by Alice at a low rate, and are used by Bob to estimate the channel coefficient before the transmission of a block of symbols, is protected against eavesdropping (for instance, by using some form of secrecy encoding designed for non-coherent reception). Under these circumstances, Eve has to take the decision on whether to jam or eavesdrop in the absence of any non-causal channel state information (i.e. randomly).

Denote $q = Pr\{\text{Ex mode}\}$ the probability that Eve is in Ex mode. The equivalent channel coefficients become

$$\widetilde{h_M} = \begin{cases} h_M & \text{with probability } q \\ \frac{h_M \sigma_N^2}{\sigma_N^2 + J} & \text{with probability } (1-q) \end{cases} \tag{5.5}$$

and

$$\widetilde{h_W} = \begin{cases} h_W & \text{with probability } q \\ 0 & \text{with probability } (1-q), \end{cases} \tag{5.6}$$

resulting in the achievable secrecy rate

$$R_s = \mathbf{E}_{h_M, h_W, P, J} \left[q \log(1 + \frac{h_M P}{\sigma_N^2}) - q \log(1 + \frac{h_W P}{\sigma_N^2}) + (1-q) \log(1 + \frac{h_M P}{\sigma_N^2 + J}) \right]. \tag{5.7}$$

At this point we prove our first result regarding the optimal choice of the instantaneous scaling power P:

Proposition 5.1. *When no channel state information is available to the transmitter, the optimal transmitter strategy is to allocate constant power $P = \mathscr{P}$ to each symbol.*

Proof. Recall our assumption that both h_M and h_W are exponentially distributed, with parameters λ_M and λ_W, respectively. Denote the probability distributions by $f_M(x) = \lambda_M e^{-\lambda_M x}$ and $f_W(x) = \lambda_W e^{-\lambda_W x}$.

If $\lambda_M \geq \lambda_W$ (Eve's channel is statistically "better"), then by letting $q = 1$, Eve can reduce the achievable secrecy rate to zero. In this case the way Alice distributes her power (without knowledge of the exact channel coefficients) is irrelevant, and a constant power allocation is as good as any. Hence we shall concentrate on the case when $\lambda_M < \lambda_W$.

We need to prove that whenever $\lambda_M < \lambda_W$ (Bob's channel is statistically "better"), the function

$$R_s(P) = q\mathbf{E}_{h_M} \log(1 + \frac{h_M P}{\sigma_N^2}) - q\mathbf{E}_{h_W} \log(1 + \frac{h_W P}{\sigma_N^2}) + (1-q)\mathbf{E}_{h_M,J} \log(1 + \frac{h_M P}{\sigma_N^2 + J}) \quad (5.8)$$

is a concave $\bigcap$ function of P. It is easy to see that the third term in the right-hand side of (5.8) is concave in P. Since both q and $1-q$ are non-negative, it is enough to show that

$$F(P) = \mathbf{E}_{h_M} \log(1 + \frac{h_M P}{\sigma_N^2}) - \mathbf{E}_{h_W} \log(1 + \frac{h_W P}{\sigma_N^2}) \quad (5.9)$$

is also concave in P. We can write

$$F(P) = \int_0^\infty \log(1 + \frac{xP}{\sigma_N^2})(f_M(x) - f_W(x))dx. \quad (5.10)$$

Note that $f_M(x) - f_W(x)$ is negative for $x \in [0, x_0)$ and positive for $x \in [x_0, \infty)$, where x_0 is the (unique) solution of $f_M(x) = f_W(x)$. Moreover, $\int_0^\infty f_M(x)dx = \int_0^\infty f_W(x)dx = 1$, which results in

$$\int_0^{x_0} [f_W(x) - f_M(x)]dx = \int_{x_0}^\infty [f_M(x) - f_W(x)]dx. \quad (5.11)$$

A graphical representation of these functions is given in Figure 5.2, where we used the notation $f_1 = f_M$ and $f_2 = f_W$. Take an *increasing function* $G(x)$. We can write

$$\begin{aligned} &\int_0^{x_0} G(x)[f_W(x) - f_M(x)]dx \leq \int_0^{x_0} G(x_0)[f_W(x) - f_M(x)]dx = \\ &= \int_{x_0}^\infty G(x_0)[f_M(x) - f_W(x)]dx \leq \int_{x_0}^\infty G(x)[f_M(x) - f_W(x)]dx. \end{aligned} \quad (5.12)$$

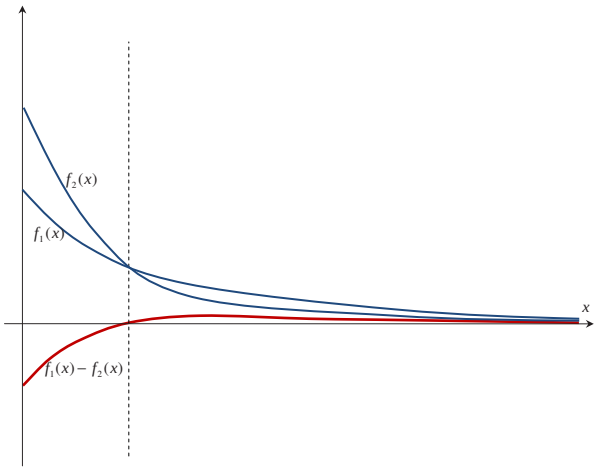

FIGURE 5.2. Exponential distributions and their difference.

Now, taking $G(x) = \log(1 + \frac{xP}{\sigma_N^2})$ we see that $F(P)$ is a positive function of P, taking $G(x) = \frac{dF(P)}{dP} = \frac{x}{\sigma_N^2 + xP}$ we see $F(P)$ is increasing, and taking $G(x) = \frac{d^2F(P)}{dP^2} = -\left(\frac{x}{\sigma_N^2 + xP}\right)^2$ we see that $F(P)$ is concave. □

Note that unlike in [22], where noise injection can increase the achievable secrecy rate, in our scenario (with both main and eavesdropper channels affected by fading) the injection of additive white Gaussian noise at Alice – which is equivalent to a proportional reduction of both Bob's and Eve's SNRs – would only make things worse. This is because the achievable secrecy rate $R_s(P)$ is a positive, increasing function of P and a decreasing function of σ_N^2. Noise injection may only increase the secrecy rate if $f_M(x) - f_W(x)$ does not have the particular form of our scenario (i.e. negative on $[0, x_0]$ and positive on $[x_0, \infty)$ for some x_0, as seen in Figure 5.2). This property is quite restrictive. In fact, in Section 5.2.2 below we study a scenario where the property does not hold anymore, and we provide an intuitive description of the conditions under which noise injection can improve the secrecy rate.

A statement similar to Proposition 5.1 can be proved for the distribution of the jamming power $\mathscr{J}$ by Eve:

Proposition 5.2. *When in jamming (Jx) mode, Eve's optimal strategy is to use the same jamming power $J = \frac{\mathscr{J}}{1-q}$ across all channel realizations involved.*

Proof. Recall that Eve adopts the Jx mode with probability $1-q$. From (5.7) we notice that only the last term in the expectation depends on J, and that term is a convex function of J. In the remainder of this proof we take a contradictory approach. Suppose that an optimal strategy is reached, and J is not constant over all channel realizations over which Eve is in Jx mode. Since the probability of the Jx mode $(1-q)$ is fixed, and for fixed q we have that R_s is a convex function of J, Eve can improve her strategy (i.e. decrease R_s) by using a constant jamming power $J = \frac{\mathscr{J}}{1-q}$ whenever in Jx mode. Thus, the original strategy is not optimal, which creates a contradiction. □

The achievable secrecy rate is now simply

$$R_s = \mathbf{E}_{h_M,h_W}\Bigg[q_{opt}\log(1+\frac{h_M\mathscr{P}}{\sigma_N^2}) - q_{opt}\log(1+\frac{h_W\mathscr{P}}{\sigma_N^2}) + \\ +(1-q_{opt})\log(1+\frac{h_M\mathscr{P}}{\sigma_N^2+\frac{\mathscr{J}}{1-q_{opt}}})\Bigg], \tag{5.13}$$

where q_{opt} is the the optimal value of q that minimizes R_s. Due to Lemma 5.9 of Section 5.5 it is easy to see that R_s in (5.13) is a convex function of q (we only need to replace $x = \frac{h_M\mathscr{P}}{\sigma_N^2}$ and $y = \frac{\mathscr{J}}{\sigma_N^2}$ and notice that the middle term of the expectation in (5.13) is a linear function of q). Therefore, q_{opt} can be found as the solution of the equation $\frac{dR_s(q)}{d_q} = 0$.

Note that the fact that $R_s(q)$ is convex supports our innitial assumption that Eve uses a fixed value of q, instead of picking random values for q, for each new channel use, according to some probability distribution over $[0,1]$.

5.2.2 Channel Coefficients Available to Eve before Decision on Jx or Ex Mode

This second scenario assumes that the eavesdropper channel coefficient is available to Eve before she makes her decision about jamming or listening to the corresponding time slot. This assumption is justified if the transmission protocol requires that an unprotected training sequence be transmitted periodically, to give the legitimate receiver the opportunity to estimate its own channel state. Although this new scenario brings no benefits to either Alice or Bob, it creates a new opportunity

for Eve. The eavesdropper can now select the better channel realizations for listening (Ex mode) and use the worse channel realizations for jamming (Jx mode).

Instead of selecting an optimal q and switch to Ex mode with probability q randomly (as when she did not have access to the value of h_W), Eve can now select a threshold v and switch to Jx mode if and only if $h_W < v$. Note that under our current assumptions, i.e. when Eve does not know Bob's instantaneous channel coefficient, and when the channel from Eve to Bob does not experience fading, Eve's threshold approach is optimal. Denote by $q = e^{-\lambda_W v}$ the probability that $h_W > v$ (the probability that Eve is in Ex mode). Note that this new attack strategy is completely transparent to Alice, since she has no way of finding out the exact value of h_W. Nevertheless, the statistics of the new equivalent eavesdropper channel coefficient:

$$\widetilde{h_W} = \begin{cases} h_W & \text{if } h_W \geq v \text{ i.e. with probability } q \\ 0 & \text{if } h_W < v \text{ i.e. w. p. } (1-q), \end{cases} \tag{5.14}$$

are known to Alice. The new achievable secrecy rate becomes

$$R_s = \mathbf{E}_{h_M,P,J}\left[q\log(1+\frac{h_M P}{\sigma_N^2}) + (1-q)\log(1+\frac{h_M P}{\sigma_N^2+J})\right] - \\ -\mathbf{E}_P\left[\int_{\frac{1}{\lambda_W}\log\frac{1}{q}}^{\infty} \log(1+\frac{h_W P}{\sigma_N^2}) f_W(h_W) dh_W\right]. \tag{5.15}$$

In order to characterize the optimal transmitter and active eavesdropper strategies we need to prove results similar to those in Subsection 5.2.1. We begin with the most evident of these.

Proposition 5.3. *When in jamming (Jx) mode, Eve's optimal strategy is to use the same jamming power $J = \frac{\mathscr{J}}{1-q}$ across all channel realizations involved.*

Proof. The proof is very similar to that of Proposition 5.2 and will be omitted here for brevity. □

As far as the optimal distribution of Alice's power is concerned, this is no longer uniform in general. With the notation

$$f_1(x) = q f_M(x) \tag{5.16}$$

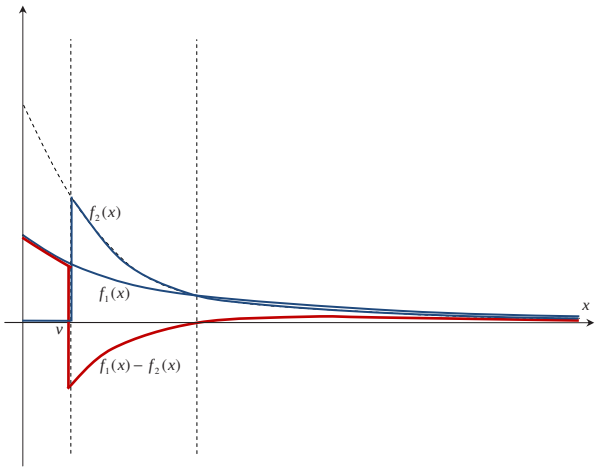

FIGURE 5.3. Modified exponential distributions and their difference – Eve uses threshold v.

and

$$f_2(x) = \begin{cases} 0 & \text{if } x \leq v \\ f_W(x) & \text{if } x > v \end{cases} \tag{5.17}$$

we can write the difference between the first and the last term in the right-hand side of (5.15) as $F(P) = \int_0^\infty \log(1 + \frac{xP}{\sigma_N^2})(f_1(x) - f_2(x))dx$. The shapes of f_1, f_2 and $f_1 - f_2$ are given in Figure 5.3.

At this point, we can no longer state that for any increasing function $G(x)$ we have a positive $\int_0^\infty G(x)(f_1(x) - f_2(x))dx$. In fact, in general, the function $F(P)$ can be negative, decreasing and/or convex on certain intervals. Note that the middle term of (5.15) is still a concave, increasing function of P, and does not affect our observations. For many situations, including the one in which Eve's channel is statistically better (i.e. $\lambda_W < \lambda_M$), the shape of $R_s(P)$ (where $R_s(P)$ is defined in (5.15)) is that of Figure 5.4 (the black lower curve). As a matter of fact, a similar shape is noticed for some situations in [22].

It now becomes clear how noise injection can improve the achievable secrecy rate. As shown in [22], if a part N of the total transmitter power P is used for injecting white Gaussian noise, the

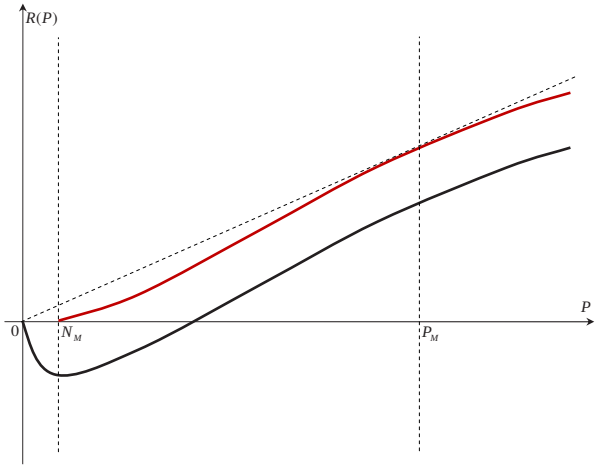

FIGURE 5.4. General form of $R_s(P)$ and improvement by noise injection.

secrecy rate becomes $R'_s(P,N) = R_s(P) - R_s(N)$. To see this,

$$\begin{aligned} R'_s(P,N) = \mathbf{E}_{h_M,P,J,N}\left[q\log(1+\frac{h_M(P-N)}{\sigma_N^2+h_MN}) + (1-q)\log(1+\frac{h_M(P-N)}{\sigma_N^2+J+h_MN})\right] - \\ -\mathbf{E}_{P,N}\left[\int_{\frac{1}{\lambda_W}\log\frac{1}{q}}^{\infty}\log(1+\frac{h_W(P-N)}{\sigma_N^2+h_WN})f_W(h_W)dh_W\right] = \\ = \mathbf{E}_{h_M,P,J}\left[q\log(1+\frac{h_MP}{\sigma_N^2}) + (1-q)\log(1+\frac{h_MP}{\sigma_N^2+J})\right] - \\ -\mathbf{E}_{P}\left[\int_{\frac{1}{\lambda_W}\log\frac{1}{q}}^{\infty}\log(1+\frac{h_WP}{\sigma_N^2})f_W(h_W)dh_W\right] - \\ -\mathbf{E}_{h_M,N,J}\left[q\log(1+\frac{h_MN}{\sigma_N^2}) + (1-q)\log(1+\frac{h_MN}{\sigma_N^2+J})\right] - \\ -\mathbf{E}_{N}\left[\int_{\frac{1}{\lambda_W}\log\frac{1}{q}}^{\infty}\log(1+\frac{h_WN}{\sigma_N^2})f_W(h_W)dh_W\right]. \quad (5.18) \end{aligned}$$

Thus, for example, if P is large enough and we choose N such that $R_s(N)$ is minimized ($N = N_M$ in Figure 5.4), then $R'_s(P,N_M) > R_s(P)$, as represented in the red upper curve of Figure 5.4. Note that even after this improvement, the $R'_s(P,N_M)$ curve is not concave. Therefore, an additional improvement would be to randomize the transmitted power between zero and P_M whenever Alice's power budget satisfies $\mathscr{P} \in [N_M, P_M]$, where P_M is chosen such that the straight line through the origin and the point $(P_M, R_s(P_M))$ is tangent to the curve $R'_s(P,N_M)$, as in Figure 5.4. Although the curve in Figure 5.4 is the most general representation of $R_s(P)$,

for many practical scenarios the actual $R_s(P)$ can be strictly positive, and even concave (see the two numerical examples in Figures 5.5 and 5.6). Hence, noise injection cannot always improve the achievable secrecy rates.

The optimal value of $q \in [0, 1]$ that minimizes the achievable secrecy rate in (5.18) can be found by a numerical algorithm involving exhaustive searching over the interval $[0, 1]$. However, it would be helpful if we knew that a unique solution exists, and this solution were reachable by a less complex algorithm. Although at this point we are not able to prove it, the following conjecture, which, if true, guarantees the uniqueness of the solution, and the fact that the solution is given by the equation $\frac{dR'_s(P,N,q)}{d_q} = 0$, is supported by our simulation results.

Conjecture 5.4. *The achievable secrecy rate in (5.18) is a quasiconvex function of q. By definition, a real scalar function $f : X \to \mathbb{R}$ is quasiconvex if its level set $[S^c, f] = \{x : x \in X, f(x) \leq c\}$ is a convex set for any $c \in \mathbb{R}$ [47].*

Two remarks are in order. First, note that the conjecture above also supports our innitial assumption that Eve uses a fixed threshold, instead of changing the threshold for every new channel realization, according to some probability distribution of v over $[0, \infty)$. Second, although the conjecture is not proved at this time, our results still function as an upper-bound on the achievable secrecy rate (note that if the conjecture were false, this upper bound would just be looser, but an upper bound nevertheless).

5.2.3 Numerical Results

In Figure 5.5 we show the achievable secrecy rates vs. transmitter power budget, in the two scenarios outlined in this section: when the channel coefficients are available to Eve before deciding whether to jam or eavesdrop, and when they are not. The main channel coefficient h_M is considerably better than Eve's channel coefficient h_W ($\lambda_M = 0.2$ and $\lambda_W = 0.8$). For comparison, we also show the achievable secrecy rates when Eve employs either the Jx mode or the Ex mode exclusively.

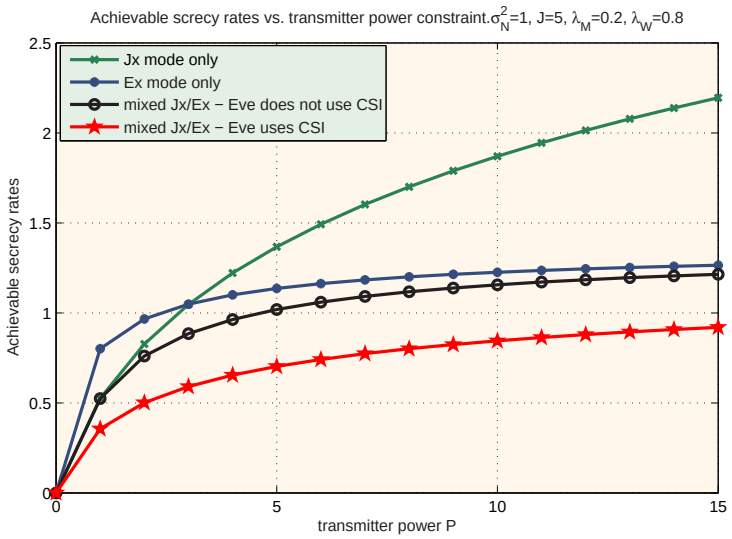

FIGURE 5.5. Achievable secrecy rates with an active eavesdropper. Exponentially distributed channel coefficients with $\lambda_M = 0.2$, $\lambda_W = 0.8$, $J = 5$, $\sigma_N^2 = 1$.

It can be noticed that, in the presence of an active eavesdropper who uses the information about its own channel to put up a more efficient fight against the transmission of secret messages, the achievable secrecy rate is seriously reduced. This reduction is even more serious in Figure 5.6, where the two channel coefficients h_M and h_W are statistically closer to each other – their parameters are $\lambda_M = 0.2$ and $\lambda_W = 0.27$. The benefits of noise injection are also illustrated in Figure 5.6.

5.3 The Worst-Case Scenario and the Block-Markov Wyner Secrecy Encoding Scheme

In the previous section we considered the scenario when the active eavesdropper "plays first". Taking advantage of her a priori knowledge about Eve's strategy, Alice was able to construct a codebook for conveying a secret message to Bob. The problem with this approach is that the codebook used by Alice and Bob (which is a simple Wyner secrecy encoding scheme [12]) needs to be tailored to Eve's exact jamming/eavesdropping strategy.

Therefore, under the more practical scenario when Eve's strategy is not known in advance, the codebook designed for a specific parameter $q_0 = Pr\{\text{Ex mode}\}$ will fail if Eve decides to use any

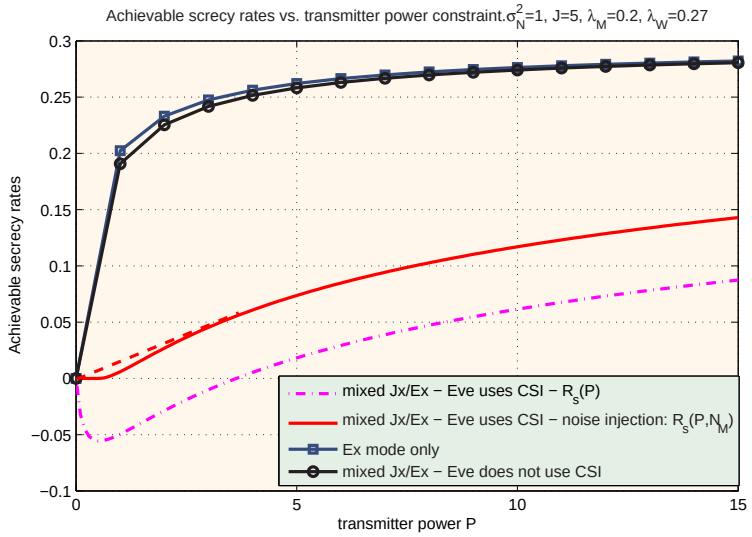

FIGURE 5.6. Achievable secrecy rates with an active eavesdropper – benefits of noise injection. Exponentially distributed channel coefficients with $\lambda_M = 0.2$, $\lambda_W = 0.27$, $J = 5$, $\sigma_N^2 = 1$.

different strategy. More precisely, if Eve uses $q_1 > q_0$, the perfect secrecy of the message will be compromised (we call this *secrecy outage*), while if Eve uses $q_2 < q_0$, the secret message becomes unintelligible to Bob (we call this *intelligibility outage*).

As a result, the legitimate parties have to use a transmission strategy that can protect both the secrecy and the intelligibility of the secret message, under any strategy that Eve might use. This problem is best modeled by the *maximin* scenario, which uses the assumption that Eve knows Alice's strategy in advance.

The simplest encoding scheme that may offer this kind of protection is a Wyner-type encoding strategy, with a forwarding rate low enough to protect the message against the most powerful attempt to induce intelligibility outage (i.e. when Eve is in Jx mode all the time), and with a secrecy rate low enough to offer protection against the most powerful attempt to induce secrecy outage (i.e. when Eve is in Ex mode all the time). The achievable secrecy rate for this kind of scheme is

$$R_{s,wcs} = \left[\mathbf{E}_{h_M} \left[\log(1 + \frac{h_M \mathscr{P}}{\sigma_N^2 + \mathscr{J}}) \right] - q \mathbf{E}_{h_W} \left[\log(1 + \frac{h_W \mathscr{P}}{\sigma_N^2}) \right] \right]^+ \tag{5.19}$$

(the subscript "wcs" stands for "worst-case scenario"), where we assumed for simplicity that Eve does not use the information about her own channel coefficient to decide when to jam and when to

eavesdrop as in Subsection 5.2.2, but rather takes that decision in a random fashion as in Subsection 5.2.1. This simplifying assumption will be maintained throughout this section for its relative ease of manipulation. All our results can be easily extended to the more complex model of Subsection 5.2.2.

Note that under the limiting assumptions above, Eve's optimal strategy is to pick $q = 1$, i.e. to remain in Ex mode all the time. In this case, the achievable secrecy rate in (5.19) is rarely strictly positive. Recalling that the channel coefficients h_M and h_W are exponentially distributed, with parameters λ_M and λ_W, respectively, the condition $R_{s,wcs} > 0$ holds if and only if $\lambda_W > \lambda_M(1 + \frac{\mathscr{J}}{\sigma_N^2})$. For a large jamming-power-to-noise ratio $\mathscr{J}/\sigma_N^2$, this implies that Eve's channel needs to be impractically worse than Bob's.

However, the above scheme does not take full advantage of the model characteristics. Recall the original assumption that Eve can function only as a half-duplex terminal. Therefore, whenever Eve is in Jx mode, she cannot eavesdrop – so the whole transmission remains perfectly secret to Eve – and conversely, if she is in Ex mode, Eve cannot simultaneously jam the transmission. In the remainder of this section we develop an alternative transmission scheme, which greatly improves the achievable secrecy rate, and is tuned to specifically exploit the active eavesdropper's limitations.

5.3.1 The Block-Markov Wyner (BMW) Encoding Scheme for the Active Eavesdropper Channel

There are two main reasons why Wyner's scheme [12] does not work in our model. First, Alice does not know the statistics of Bob's channel in advance – Eve has control over the signal-to-noise ratio of this channel. Therefore, the main channel can be modeled as a compound channel. In order to reliably transmit a message to Bob, Alice should use a special kind of encoding. It was shown in [16] that the same layered encoding technique that achieves the points on the boundary of the capacity region for broadcast channels can also be used for transmission over compound channels. Our scheme uses the broadcast layered encoding of [16] to ensure that reliable transmission is

possible between Alice and Bob even in the most unfavorable conditions. However, even if such a scheme is used, Alice cannot know in advance which messages will actually be decodable by Bob.

The second reason is that Alice does not know the statistics of Eve's channel in advance – due to the alternation between jamming and eavesdropping Eve's equivalent channel is actually weaker than her physical channel. Therefore, Alice cannot directly transmit a secret message at a rate larger than $R_{s,wcs}$ in (5.19), because she is not sure whether the secrecy would be compromised or not.

Our novel BMW secrecy encoding scheme solves both of these problems: it guarantees both the intelligibility and the secrecy of the message, for a transmission rate much larger than $R_{s,wcs}$. Our approach is a sequential one, and requires that Bob should be actively involved in the secrecy encoding process. Bob's involvement consists of estimating and feeding back to Alice the exact value of Eve's strategy q. The detailed description is given below. However, before we get to that, we first make a brief comment on Wyner's original encoding scheme [12], which will help build some intuition regarding the principle of our own scheme.

A short comment on Wyner's secrecy encoding scheme

We begin this comment by studying a scenario where, before the transmission takes place, Alice and Bob already share a secret key. Then in addition to the secret message that can be encoded by Wyner's scheme, another secret message can be transmitted over the channel. This latter message is encrypted using the secret key. We provide two encoding schemes that can both achieve the simultaneous transmission of the two secret messages.

Denote the capacities of the channels from Alice to Bob and from Alice to Eve by C_M and C_E, respectively, the achievable secrecy rate (under Wyner's original scheme) by R_k, the rate of the encrypted message by R_s and the codeword length by N.

Scheme 1: Wyner's scheme with an encrypted message. Alice bins the codebook (containing 2^{NC_M} codewords) into 2^{NR_k} "super-bins", such that $R_k \leq C_M - C_E$. The first secret message

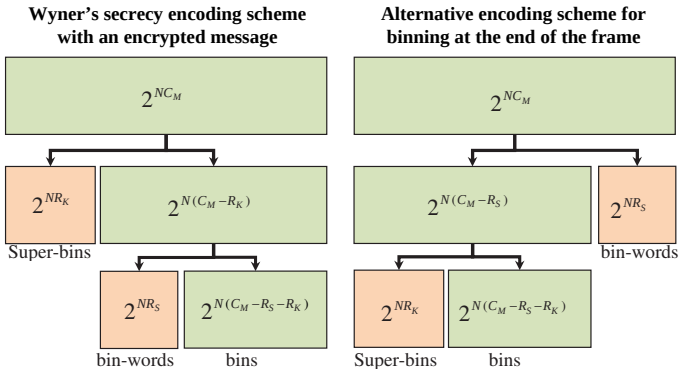

FIGURE 5.7. Alternative binning: Wyner's secrecy encoding scheme with an additional encrypted message, and the basis of our block-Markov Wyner encoding scheme.

picks the index of a super-bin. The super-bin is then binned again into $2^{N(C_M-R_s-R_k)}$ bins (each containing 2^{NR_s} bin-words). One of the bins is picked randomly, while a specific codeword in that bin is picked according to the encrypted message.

Scheme 2: An alternative encoding scheme. The codebook is randomly binned into $2^{N(C_M-R_s)}$ bins – let us denote these as "pre-bins". Each pre-bin consists of 2^{NR_s} bin-words. The bins are then randomly grouped into 2^{NR_k} "super-bins", such that each super-bin consists of $2^{N(C_M-R_s-R_k)}$ bins, and where R_k is picked to satisfy $R_k \leq C_M - C_E$. The first secret message picks the index of a super-bin. A bin inside that super-bin is randomly picked, and the transmitted codeword is the picked by the encrypted message inside this bin.

The two schemes are equivalent, and they are described in Figure 5.7. However, as we shall see shortly, the applicability of *Scheme 2* is larger. We should recall here that Wyner's original encoding scheme [12] involves a random binning of the codebook into bins which are, each of them, good codes for Eve's channel. The actual transmission does not contain any information about the binning itself. Hence, the same "random" binning needs to be done separately at Alice (before the transmission takes place) and at Bob (before he can begin decoding). The reason why Alice performs the binning of the codebook before transmitting is because she needs to send a *meaningful* secret message over the coming frame. Therefore, the transmitted codeword needs to belong to the particular bin indexed by the secret message.

This suggests that if the "secret message" transmitted by Alice had no meaning (i.e. if Alice picked this message in a random fashion), both Alice and Bob could perform the binning of the codebook after the transmission ends. The "secret message" generated this way could be thought of as a *secret key* for encrypting a meaningful message over the next frame.

Suppose that Eve's channel is unknown to Alice and Bob until the transmission of the current codeword ends. The first transmitted codeword is randomly selected from the whole un-binned codebook. After the transmission ends, Alice and Bob realize that the secrecy capacity was R_s. Both Bob and Alice can now proceed to the (same) binning of the codebook. As a result, the same single bin will be identified by both legitimate parties as containing the transmitted message, and its index will be secret to Eve. Clearly, the secret message conveyed by the index of this bin has no meaning. Nevertheless, it can be used over the next frame, as a secret key. Over the second frame, Alice and Bob use *Scheme 2* above. The codebook is randomly binned before transmission, into $2^{N(C_M-R_s)}$ bins that could each be regarded as a code for carrying the encrypted message. One of the bins will be selected randomly, and the encrypted message will select the exact codeword to be transmitted. This method of transmission ensures that the encrypted message does not overlap with the secret key that needs to be generated at the end of the frame – the encrypted message has nothing to do with how the bins are ultimately chosen, as seen in Figure 5.7. The encrypted message may be *decodable, but not decryptable* by Eve. After the transmission of the second frame takes place, Alice and Bob realize that the secrecy capacity was R_k. The indices of the bins are "randomly" grouped by both Alice and Bob into 2^{NR_k} super-bins , and a new secret key is agreed upon by the legitimate parties. The protocol continues in the same manner.

Three observations are in order. First, the secret key (decided upon at the end of the frame) and the encrypted message (carried by the frame) cannot overlap and maintain the same equivocation at Eve – see the *one-time pad* [43]. Hence, in the above description of the protocol, it is required that $R_s + R_k \leq C_M$. Second, if the secrecy capacity is the same $R_s = R_k = C_s$ over each frame, and our previous condition holds in the form $R_s < C_M/2$, the transmission of the meaningful secret

message can be done at almost the secrecy capacity, with a small initial penalty (due to the fact that the first frame does not carry an encrypted message) which becomes negligible as the number of transmitted frames increases.[1] Third, our new protocol can be used whenever Alice does not have a good description of Eve's channel over a frame until the transmission of the corresponding codeword ends, which is precisely the case with our current model.

Detailed description of the BMW encoding scheme

Eve's strategy consists of choosing the parameter $q = Pr\{\text{Ex mode}\}$. Once the transmission of a codeword (we shall denote the span of a codeword by "frame") is finished, Bob can accurately evaluate the parameter q used by Eve over that frame. Bob can then feed this value back to Alice. Note that the knowledge of q provides Alice with the statistical description of both the main channel – determined by the jamming probability $(1 - q)$ – and the eavesdropper's channel – determined by the eavesdropping probability q. Before learning Eve's strategy, the channel between Alice and Bob appears like a compound channel to the legitimate parties. The possible states of this channel are given by Eve's strategy q, which takes values in the interval $[0, 1]$. To transform this uncountable set of possible channel states into a finite set, we divide the interval $[0, 1]$ to which q belongs into n subintervals such that

$$[0, 1] = [q_0, q_1) \cup [q_1, q_2) \ldots \cup [q_{n-1}, q_n] \tag{5.20}$$

where $q_0 = 0$ and $q_n = 1$.

For conveying a message to Bob, Alice uses an n-level broadcast-channel-type codebook, as in [16]. Level i is designed to deal with a jammer which is on with probability $1 - q_{i-1}$ over each channel use. Note that $q_0 < q_1 < \ldots < q_n$. In the remainder of this chapter, we shall say that level

[1] Assume that Eve's channel conditions are always the same. As an example, consider a codebook with 10000 codewords, which is used for transmitting a secret message of length $\log(50)$ bits, according to our protocol. Take any random frame. For transmitting the encrypted message, the codebook is binned into 200 bins, each containing 50 codewords. One of the bins is picked randomly, and the encrypted message picks one of the 50 codewords in the bin. After the transmission takes place, Alice and Bob both group the original 200 bins into 50 "super-bins" (each containing 4 original bins), using the same "recipe". The secret key is the index of the super-bin to which the transmitted codeword belongs. Note that the actual codeword that was transmitted inside this super-bin is picked independently of the choice of the super-bin.

i is "stronger" than level j if $i < j$, i.e. if level i can deal with a jammer which is on more often. The notation is fully justified by Lemma 5.5 below.

Denote the rates of the different encoding levels as:

$$R_1 = \mathbf{E}_{h_M}\Big[\log\big(1 + \frac{(1-\alpha_1)Ph_M}{\sigma_N^2 + \alpha_1 Ph_M + \mathscr{J}}\big)\Big] \tag{5.21}$$

for the strongest level, which can deal with the case when Eve is always in Jx mode, i.e. $q = q_0 = 0$,

$$R_i = \mathbf{E}_{h_M}\Bigg[q_{i-1}\log\left(1 + \frac{(1-\alpha_i)\alpha_{i-1}\ldots\alpha_1 Ph_M}{\sigma_N^2 + \alpha_i\ldots\alpha_1 Ph_M}\right) + \\ +(1-q_{i-1})\log\left(1 + \frac{(1-\alpha_i)\alpha_{i-1}\ldots\alpha_1 Ph_M}{\sigma_N^2 + \alpha_i\ldots\alpha_1 Ph_M + \frac{\mathscr{J}}{1-q_{i-1}}}\right)\Bigg], \tag{5.22}$$

for $i = 2, 3\ldots n-1$, and finally

$$R_n = \mathbf{E}_{h_M}\left[q_{n-1}\log\left(1 + \frac{\alpha_{n-1}\ldots\alpha_1 Ph_M}{\sigma_N^2}\right) + (1-q_{n-1})\log\left(1 + \frac{\alpha_{n-1}\ldots\alpha_1 Ph_M}{\sigma_N^2 + \frac{\mathscr{J}}{1-q_{n-1}}}\right)\right] \tag{5.23}$$

for the weakest level, corresponding to the case when Eve is in Jx mode with probability $1 - q_{n-1}$. Note that the encoding levels are designed such that Bob decodes the stronger levels first, and treats the remaining un-decoded messages as white noise. The codebook for level i contains 2^{NR_i} codewords of length N, generated such that each component of each codeword represents an independent realization of a Gaussian random variable of mean 0 and variance $(1-\alpha_i)\alpha_{i-1}\ldots\alpha_1 P$, where $\alpha_n = 0$ for compatibility.

The relative strength of the encoding levels is established by the following lemma.

Lemma 5.5. *If Eve uses a parameter $q \in [q_{i-1}, q_i)$ over a frame, then the messages encoded in levels $1, 2, \ldots, i$ are intelligible by Bob at the end of the frame. Thus the forwarding rate from Alice to Bob is $R_{M,i} = R_1 + R_2 + \ldots + R_i$.*

Proof. In order to prove that the encoding levels with lower indices are stronger in the sense that they can deal with a worse jamming situation, it is enough to show that R_i as defined in 5.22 is an increasing function of q. In other words, encoding level i, transmitting at a rate R_i, is intelligible

by Bob whenever Eve is in jamming mode with a probability less than $(1 - q_{i-1})$. But this is a direct consequence of Lemma 5.9 in Section 5.5, if we simply replace x by $\frac{(1-\alpha_i)\alpha_{i-1}...\alpha_1 Ph_M}{\sigma_N^2+\alpha_i...\alpha_1 Ph_M}$ and y by $\frac{\mathscr{J}}{\sigma_N^2+\alpha_i...\alpha_1 Ph_M}$. (see Section 5.5). □

Consider a first frame, for which the transmitted message carries no useful information, but rather its symbols are selected in a random, i.i.d. fashion. Once Alice receives the feedback sequence from Bob at the end of the frame, describing Eve's strategy (i.e. the value of q – actually, as we shall see shortly, only the interval $[q_{i-1}, q_i)$ that contains q is enough information for Alice, thus the length of the feedback sequence need not be larger than $log(n)$), Alice and Bob can separately agree on the same secret message, as described in the protocol above. This message will function as a secret key for encrypting a meaningful secret message over the next frame. In turn, the secret message agreed upon at the end of the second frame can function as a secret key for the third frame, and so on.

To formalize the intuitive description above, we begin by stating several definitions:

- The "encrypted message" is a meaningful secret message, encrypted with the help of a secret key that was generated in the previous frame.
- The "secret key" is a meaningless random message, which is perfectly secret to Eve, is agreed upon by both Alice and Bob at the end of the frame, and can be used for the encryption of a secret message (of at most the same length) over the next frame.
- The term "secret key rate" refers to the rate at which a secret key is generated at the end of a frame – the correspondent of Wyner's "secrecy capacity".
- The term "achievable secrecy rate" refers to the rate of transmission of the encrypted message.

Our encoding scheme works as follows. First, the n codebooks, indexed by i, with $i \in \{1, 2, \ldots, n\}$ are generated as described above, and are made available to all parties. On a given frame, Alice

transmits an encrypted message, at a rate

$$R_s \leq 0.5R_1 \tag{5.24}$$

(we show in Theorem 5.7 below that this constraint does not incur any loss of performance) – note that the *encrypted message* is encrypted with the help of a secret key generated over a previous frame. To transmit the encrypted message, Alice randomly bins codebook 1 into $2^{N(R_1-R_s)}$ bins. One of the bins (each containing 2^{NR_s} codewords) will be picked randomly (uniformly), and the encrypted message will pick a codeword from this bin for transmission. Recall that the reason why Alice cannot directly bin the codebook for generating the secret key is because Eve's strategy (hence her equivalent channel) is unknown until the end of the frame. An additional $n-1$ codewords are also chosen randomly, one from each of the remaining $n-1$ codebooks of rates $R_2, R_3, \ldots, R_n$. Alice's transmitted sequence is the sum of the n codewords.

At the end of the frame, Bob feeds back to Alice the exact value of Eve's strategy q over that frame. In order to agree on a secret key, Alice and Bob first need to know which encoding levels are decodable by Bob, and which are decodable by Eve. Only the information encoded in those levels that are decodable by Bob, but are not perfectly decodable by Eve, can contribute to the generation of the secret key.

Due to the construction of the code (see Lemma 5.5), it is clear that under any jamming/ eavesdropping strategy, Bob will be able to decode the strongest level first, treating the other levels as white noise, and then perform successive interference cancellation to decode increasingly weaker levels. However, the same statement cannot be made for Eve. Note that Eve's channel is quite different from Bob's. In the general case, it is therefore possible that the order of strength of the encoding levels, from Eve's perspective, is not the same as that given by Bob's perspective. For example, for a code with 7 levels Bob might be able to decode only levels $1, 2, 3, 4$, while Eve may be able to perfectly decode only levels $1, 4, 6, 7$. In this case, we can re-order the levels from Eve's perspective, as $1, 4, 6, 7, 2, 3, 5$. The first four levels are decodable by Eve perfectly, the next two

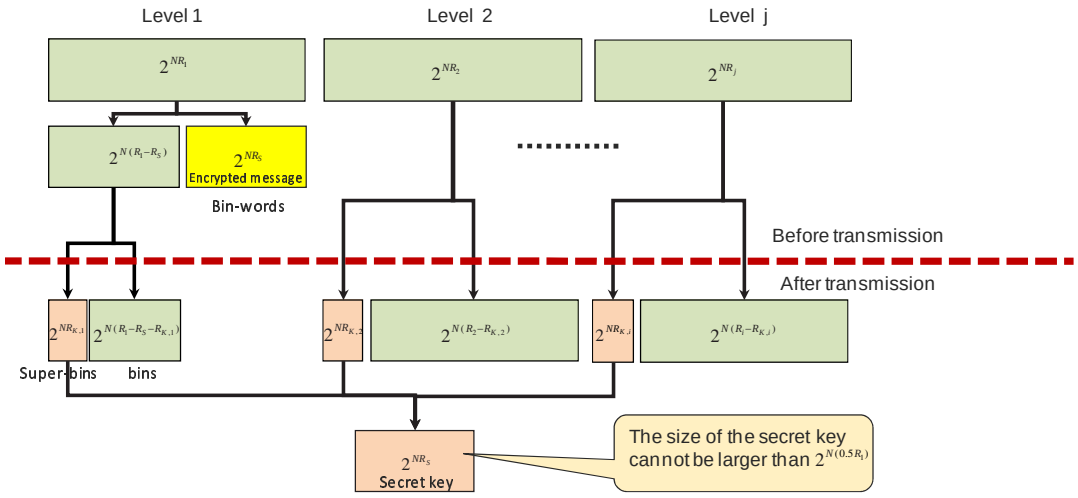

FIGURE 5.8. BMW encoding method – most general case, when $1 \in \mathscr{I}_{ne}$.

are decodable by Bob, but not by Eve, and the last level is decodable by neither. Hence, only levels 2 and 3 can be used for generating the secret key.

For the general case, we shall denote the ordered set of indices corresponding to the encoding levels specified by their rates in (5.21)-(5.23) by $\mathscr{I}$, and the set of indices corresponding to the order of strength of the encoding levels from Eve's perspective by $\widehat{\mathscr{I}}$. There exists a bijection (i.e. a re-ordering) $\mathbb{B} : \mathscr{I} \rightarrow \widehat{\mathscr{I}}$, defined as follows: (1) the set of indices (in arbitrary order) corresponding to levels that are perfectly decodable by Eve is denoted $\mathscr{I}_e$; (2) the set of indices (in arbitrary order) corresponding to levels that are not perfectly decodable by Eve, but perfectly decodable by Bob is denoted $\mathscr{I}_k$; (3) the set of indices (in arbitrary order) corresponding to levels that are not perfectly decodable by either Eve or Bob is denoted $\mathscr{I}_n$; (4) the ordered set $\widehat{\mathscr{I}}$ is defined as

$$\widehat{\mathscr{I}} = \{\mathscr{I}_e, \mathscr{I}_k, \mathscr{I}_n\}. \tag{5.25}$$

Furthermore, we define $\mathscr{I}_{ne} = \{\mathscr{I}_k, \mathscr{I}_n\}$ as the set of indices corresponding to encoding levels which are not perfectly decodable by Eve. The method of encoding is described in Figure 5.8. Theorem 5.6 below provides the achievable secret key rate for the general case.

Theorem 5.6. *Suppose that Eve picks a strategy $q \in [q_{i-1}, q_i)$ over a frame. Then an achievable secret key rate is*

$$R_{k,i} = \sum_{j \in \mathscr{I}_k} [R_j - R_{E,j}], \tag{5.26}$$

where:

- *R_j are defined as in (5.21)-(5.23) for $j = 1, 2, \ldots, n$,*
- *$R_{E,j},\ j \in \mathscr{I}_{ne}$ are selected such that they satisfy the following set of conditions:*

$$R_{E,1} \geq 0.5 R_1 \tag{5.27}$$

if $1 \in \mathscr{I}_{ne}$,

$$R_{E,j} \leq R_j, \tag{5.28}$$

$$\sum_{j \in \mathscr{S}} R_{E,j} \leq q \mathbf{E}_{h_W} \Big[\log \big(1 + \frac{\sum_{j \in \mathscr{S}} (1-\alpha_j)\alpha_{j-1} \ldots \alpha_1 P h_W}{\sigma_N^2}\big)\Big], \tag{5.29}$$

for any subset $\mathscr{S}$ of $\mathscr{I}_{ne}$, and

$$\sum_{j \in \mathscr{I}_{ne}} R_{E,j} = q \mathbf{E}_{h_W} \Big[\log \big(1 + \frac{\sum_{j \in \mathscr{I}_{ne}} (1-\alpha_j)\alpha_{j-1} \ldots \alpha_1 P h_W}{\sigma_N^2}\big)\Big] - \epsilon, \tag{5.30}$$

with ϵ positive and arbitrarily close to zero.

The expressions in (5.29) and (5.30) use the convention $\alpha_n = 0$. Note that the bijection $\mathbb{B}$ defined above also depends on Eve's strategy q, and hence on the interval i to which q belongs. Therefore, the set of indices $\mathscr{I}_k$ depends on i.

Proof. The proof is based on two observations. First, we have already shown that if the secret message is not a meaningful one, the binning of Wyner's scheme can be done at the end of the transmission, when the statistical properties of Eve's channel are known to both Bob and (through

feedback) to Alice. To accomplish this, both Alice and Bob will have to memorize a set of "binning recipes", one for each possible value of Eve's strategy (actually only the interval $[q_{i-1}, q_i)$ to which q belongs, and not the exact value of q, matters in our case). This is a bit different from Wyner's original scheme [12] where only one such recipe needed to be memorized. Therefore, in the remainder of the proof, we can and shall treat the encoding as if Eve's channel were known to all parties in advance, without losing any generality.

Second, we shall "encode" a secret key $\mathbf{K} = \bigcup_{j \in \mathscr{I}_{ne}} \mathbf{K}_j$ into all encoding levels j belonging to $\mathscr{I}_{ne}$, i.e. over both $\mathscr{I}_k$ and $\mathscr{I}_n$, although Bob cannot decode the levels of $\mathscr{I}_n$. We shall prove that the whole key $\mathbf{K}$ is secret to Eve. Then, following a simple argument in [2], it is straightforward to see that this also implies the secrecy of $\bigcup_{j \in \mathscr{I}_k} \mathbf{K}_j$, which can actually be decoded and used by Bob.

We use a separate secret key encoding for each of Alice's encoding levels in $\mathscr{I}_{ne}$. As a consequence, Eve sees a fast fading multiple access channel, where the transmitters have different power constraints, but the same channel coefficient. In this context, we note that the conditions set forth for the rates $R_{j,E}$ in (5.29) and (5.30) are exactly the conditions necessary for these rates to belong to the boundary of the capacity region of Eve's equivalent multiple access channel. The problem of a multiple access eavesdropper AWGN channel was discussed in [2]. However, neither the main results, nor the method of encoding of [2] are correct. We provide a simple explanation of this assertion in Section 5.6. Therefore, we continue with describing a correct encoding method which yields an achievable secret key rate.

For any level of encoding $j \in \mathscr{I}_{ne}$, we encode a secret key $\mathbf{K}_j$ according to Wyner's scheme [12], [15]. That is, if $j \neq 1$, we randomly bin the randomly generated N-dimensional codebook of 2^{NR_j} codewords into $2^{N(R_j - R_{E,j})}$ bins. The secret message corresponds to the index of the bin, while the exact codeword in the bin is randomly picked. The rates $R_{E,j}$ are selected as in the statement of the theorem. If $j = 1 \in \mathscr{I}_{ne}$ (recall that codebook 1 was already binned once), Bob generates the bins in two steps: first he identifies the $2^{N(R_1 - R_s)}$ bins used for transmitting Alice's

encrypted message, and then he randomly *groups* these bins into $2^{N(R_1-R_{E,1})}$ larger bins. A secret message is encoded into the indices of the resulting larger bins.

Denote the resulting N-dimensional output sequence of level j by $\mathbf{X}_j$, and denote the p-the component of $\mathbf{X}_j$ by $\mathbf{X}_j(p)$. Also denote the union of the N-sequences from all levels (including those from $\mathscr{I}_e$ which do not carry a secret key) by $\mathbf{X} = \bigcup_{j\in\hat{\mathscr{I}}}\mathbf{X}_j$. The notation $\mathbf{X}(p)$ now denotes the n-dimensional set consisting of the p-th components of the output sequences from every encoding level, that is $\mathbf{X}(p) = \bigcup_{j\in\hat{\mathscr{I}}}\mathbf{X}_j(p)$. Eve's received sequence is now $\mathbf{Z} = \mathbf{H}_W \cdot \sum_{j\in\hat{\mathscr{I}}}\mathbf{X}_j + \mathbf{Q}$, where $\mathbf{H}_W$ is the N-dimensional vector of channel realizations corresponding to the N symbols, $\mathbf{Q}$ is Eve's N-dimensional additive white Gaussian noise sequence , and $(\cdot)$ denotes component-wise multiplication. The p-th scalar components of these vectors will be denoted by $\mathbf{Z}(p)$, $\mathbf{H}_W(p)$ and $\mathbf{Q}(p)$, respectively. The notation $\mathbf{X}_{\mathscr{S}}$ will be used for the union of the output sequences corresponding to levels with indices in $\mathscr{S}$, i.e. $\mathbf{X}_{\mathscr{S}} = \bigcup_{j\in\mathscr{S}}\mathbf{X}_j$, and the notation for the p-th components is extended correspondingly.

Eve's equivocation about the secret key can be written as follows

$$\begin{aligned}\Delta = \frac{H(\mathbf{K}|\mathbf{Z},\mathbf{H}_W)}{H(\mathbf{K})} = \frac{H(\mathbf{K},\mathbf{Z},\mathbf{H}_W) - H(\mathbf{Z},\mathbf{H}_W)}{H(\mathbf{K})} \overset{(a)}{=} \\ = \frac{H(\mathbf{K}) + H(\mathbf{Z},\mathbf{H}_W,\mathbf{X}|\mathbf{K}) - H(\mathbf{X}|\mathbf{Z},\mathbf{H}_W,\mathbf{K}) - H(\mathbf{Z},\mathbf{H}_W)}{H(\mathbf{K})} \overset{(b)}{=} \\ = \frac{H(\mathbf{K}) + H(\mathbf{Z},\mathbf{H}_W|\mathbf{X},\mathbf{K}) + H(\mathbf{X}|\mathbf{K}) - H(\mathbf{X}|\mathbf{Z},\mathbf{H}_W,\mathbf{K}) - H(\mathbf{Z},\mathbf{H}_W)}{H(\mathbf{K})} = \\ = 1 - \frac{I(\mathbf{X};\mathbf{Z},\mathbf{H}_W) - I(\mathbf{X};\mathbf{Z},\mathbf{H}_W|\mathbf{K})}{H(\mathbf{K})},\end{aligned} \tag{5.31}$$

where both (a) and (b) result from the chain rule for entropy.

Denote $\mathcal{D} = I(\mathbf{X};\mathbf{Z},\mathbf{H}_W) - I(\mathbf{X};\mathbf{Z},\mathbf{H}_W|\mathbf{K})$. We can now write

$$I(\mathbf{X};\mathbf{Z},\mathbf{H}_W) = H(\mathbf{X}_{\mathscr{I}_e}) + H(\mathbf{X}_{\mathscr{I}_{ne}}) - H(\mathbf{X}_{\mathscr{I}_e}|\mathbf{Z},\mathbf{H}_W) - H(\mathbf{X}_{\mathscr{I}_{ne}}|\mathbf{X}_{\mathscr{I}_e},\mathbf{Z},\mathbf{H}_W), \tag{5.32}$$

$$H(\mathbf{X}|\mathbf{K}) = H(\mathbf{X}_{\mathscr{I}_e}) + H(\mathbf{X}_{\mathscr{I}_{ne}}|\mathbf{K}), \tag{5.33}$$

and

$$H(\mathbf{X}|\mathbf{Z},\mathbf{H}_W,\mathbf{K}) = H(\mathbf{X}_{\mathscr{I}_e}|\mathbf{Z},\mathbf{H}_W,\mathbf{K}) + H(\mathbf{X}_{\mathscr{I}_{ne}}|\mathbf{X}_{\mathscr{I}_e},\mathbf{Z},\mathbf{H}_W,\mathbf{K}) \leq$$
$$\leq H(\mathbf{X}_{\mathscr{I}_e}|\mathbf{Z},\mathbf{H}_W) + H(\mathbf{X}_{\mathscr{I}_{ne}}|\mathbf{X}_{\mathscr{I}_e},\mathbf{Z},\mathbf{H}_W,\mathbf{K}), \tag{5.34}$$

where we used the fact that $\{\mathbf{X}_j : j \in \mathscr{I}\}$ are all independent of each other, and that conditioning reduces entropy. Substituting (5.32)-(5.34) in the expression of $\mathcal{D}$ above, and noting that $H(\mathbf{X}_{\mathscr{I}_{ne}}) = H(\mathbf{X}_{\mathscr{I}_{ne}}|\mathbf{X}_{\mathscr{I}_e})$, we obtain

$$\mathcal{D} \leq I(\mathbf{X}_{\mathscr{I}_{ne}};\mathbf{Z},\mathbf{H}_W|\mathbf{X}_{\mathscr{I}_e}) - H(\mathbf{X}_{\mathscr{I}_{ne}}|\mathbf{K}) + H(\mathbf{X}_{\mathscr{I}_{ne}}|\mathbf{X}_{\mathscr{I}_e},\mathbf{Z},\mathbf{H}_W,\mathbf{K}). \tag{5.35}$$

By the code construction, and recalling that the rates $R_{j,E}$ in the statement of the theorem are picked such that they belong to the boundary of the capacity region of Eve's equivalent multiple access channel, we can use Fano's inequality and the arguments of [12], to upper bound

$$H(\mathbf{X}_{\mathscr{I}_{ne}}|\mathbf{X}_{\mathscr{I}_e},\mathbf{Z},\mathbf{H}_W,\mathbf{K}) \leq |\mathscr{I}_{ne}|N\delta_N, \tag{5.36}$$

where $|\mathscr{I}_{ne}| \leq n < \infty$ is the cardinality of $\mathscr{I}_{ne}$, and $\delta_N \to 0$ as $N \to \infty$. This is quite intuitive, since given the secret key, the other information is transmitted by Alice using codes which are good for Eve's multiple access channel. In fact δ_N is an upper bound on the probabilities of error for any of these individual codes. Since the random, complementary-to-the-secret-key information is carried by these codes at a total rate almost equal to the capacity of the virtual MAC between Alice and Eve, corresponding to the encoding levels in $\mathscr{I}_{ne}$, we also have

$$H(\mathbf{X}_{\mathscr{I}_{ne}}|\mathbf{K}) = Nq\mathbf{E}_{h_W}\Big[\log\big(1 + \frac{\sum_{j\in\mathscr{I}_{ne}}(1-\alpha_j)\alpha_{j-1}\ldots\alpha_1 Ph_W}{\sigma_N^2}\Big] - N\epsilon. \tag{5.37}$$

To upper bound the first term on the right hand side of (5.35), we write

$$\begin{aligned} I(\mathbf{X}_{\mathscr{I}_{ne}}; \mathbf{Z}, \mathbf{H}_W | \mathbf{X}_{\mathscr{I}_e}) = H(\mathbf{Z}, \mathbf{H}_W | \mathbf{X}_{\mathscr{I}_e}) - H(\mathbf{Z}, \mathbf{H}_W | \mathbf{X}_{\mathscr{I}}) \stackrel{(a)}{=} \\ = H(\mathbf{Z}, \mathbf{H}_W | \mathbf{X}_{\mathscr{I}_e}) - NH(\mathbf{Z}(p), \mathbf{H}_W(p) | \mathbf{X}_{\mathscr{I}}(p)) \stackrel{(b)}{\leq} \\ \leq NH(\mathbf{Z}(p), \mathbf{H}_W(p) | \mathbf{X}_{\mathscr{I}_e}(p)) - NH(\mathbf{Z}(p), \mathbf{H}_W(p) | \mathbf{X}_{\mathscr{I}}(p)) = \\ = NI(\mathbf{X}_{\mathscr{I}_{ne}}(p); \mathbf{Z}(p), \mathbf{H}_W(p) | \mathbf{X}_{\mathscr{I}_e}(p)) \stackrel{(c)}{\leq} \\ \leq Nq\mathbf{E}_{h_W}\Big[\log\big(1 + \frac{\sum_{j \in \mathscr{I}_{ne}} (1-\alpha_j)\alpha_{j-1} \ldots \alpha_1 P h_W}{\sigma_N^2}\Big]. \end{aligned} \tag{5.38}$$

Equality in (a) follows from the fact that the channel is memoryless, (b) follows from the chain rule for entropy and the fact that conditioning does not increase entropy, and (c) is obtained by using Jensen's inequality, as in the proof of the converse to the AWGN channel coding theorem in Section 9.2. of [48].

Putting together (5.36), (5.37) and (5.38), we obtain

$$\mathcal{D} \leq N(\epsilon + |\mathscr{I}_{ne}|\delta_N), \tag{5.39}$$

which in turn implies

$$\Delta \geq 1 - N\frac{\epsilon + |\mathscr{I}_{ne}|\delta_N}{H(\mathbf{K})}. \tag{5.40}$$

We have thus proved that the key $\mathbf{K}$ remains secret from Eve as long as the codeword length N goes to infinity. However, note that the entire key $\mathbf{K}$ cannot be understood by Bob. In fact, Bob and Alice can only agree on the part $\mathbf{K}_{\mathscr{I}_k}$ of the key. But the secrecy of the entire key guarantees the secrecy of any part of the key [2]. For the sake of completeness, we restate the following proof from [2].

$$\begin{aligned} H(\mathbf{K}_{\mathscr{I}_k} | \mathbf{Z}, \mathbf{H}_W) \stackrel{(a)}{=} H(\mathbf{K}_{\mathscr{I}_{ne}} | \mathbf{Z}, \mathbf{H}_W) - H(\mathbf{K}_{\mathscr{I}_n} | \mathbf{K}_{\mathscr{I}_k}, \mathbf{Z}, \mathbf{H}_W) \stackrel{(b)}{\geq} \\ \geq H(\mathbf{K}) - N(\epsilon + |\mathscr{I}_{ne}|\delta_N) - H(\mathbf{K}_{\mathscr{I}_n} | \mathbf{K}_{\mathscr{I}_k}, \mathbf{Z}, \mathbf{H}_W) \stackrel{(c)}{\geq} \\ \geq H(\mathbf{K}_{\mathscr{I}_k}) + H(\mathbf{K}_{\mathscr{I}_n}) - N(\epsilon + |\mathscr{I}_{ne}|\delta_N) - H(\mathbf{K}_{\mathscr{I}_n} | \mathbf{K}_{\mathscr{I}_k}, \mathbf{Z}, \mathbf{H}_W) \stackrel{(d)}{\geq} \\ \geq H(\mathbf{K}_{\mathscr{I}_k}) - N(\epsilon + |\mathscr{I}_{ne}|\delta_N), \end{aligned} \tag{5.41}$$

where (a) follows from the chain rule, (b) from (5.40) and the definition of Δ, (c) from the independence of the keys from different encoding levels, and (d) from the fact that conditioning does not increase entropy.

This results in

$$\frac{H(\mathbf{K}_{\mathscr{I}_k}|\mathbf{Z},\mathbf{H}_W)}{H(\mathbf{K}_{\mathscr{I}_k})} \geq 1 - N\frac{\epsilon + |\mathscr{I}_{ne}|\delta_N}{H(\mathbf{K}_{\mathscr{I}_k})} \to 1 \text{ as } N \to \infty. \tag{5.42}$$

□

We have seen the best achievable secret key rate if $q \in [q_{i-1}, q_i)$. The next theorem provides Eve's optimal strategy under the maximin scenario, and also Alice's best achievable secrecy rate.

Theorem 5.7. *(1) If Eve chooses a strategy $q \in [q_{i-1}, q_i)$, then it is optimal for her to choose q arbitrarily close to q_i.*

(2) Eve's optimal strategy under the maximin scenario is the same over all frames.

(3) Denote the achievable secret key rates by $\{R_{k,i} : i = 1, 2, \ldots, n\}$, where $R_{k,i}$ is the best achievable secret key rate given by Theorem 5.6, under $q = q_i$. Then Eve's optimal strategy is $q_{i_{opt}} = \arg\min_{q_i}\{R_{k,i}\}$, if $\min_{q_i}\{R_{k,i}\} < 0.5R_1$, and $q_{i_{opt}} = q_1$, otherwise.

(4) Under Eve's optimal strategy, the maximum achievable secrecy rate (under the current setup) is

$$R_s = \min\{0.5R_1, R_{k,i_{opt}}\}. \tag{5.43}$$

(5) There is no loss of performance incurred by restricting the rate of the encrypted message to $R_s \leq 0.5R_1$ in (5.24).

Proof. (1) Using Theorem 5.6, it is easy to check that, given $q \in [q_{i-1}, q_i)$, the achievable secret key rate is a decreasing function of q. Therefore, if $q \in [q_{i-1}, q_i)$, Eve's optimal strategy is to pick q arbitrarily close to q_i.

(2),(3),(4) We have already seen that the rate at which the encrypted message is transmitted is restricted to $R_s \leq 0.5R_1$. If $\min_{q_i}\{R_{k,i}\}$ is achieved by $q_{i_{opt}}$ and is less than $0.5R_1$, then switching

to a different Eve's strategy q_d will only increase the rate of generation of the secret key, and hence the rate of transmission of the encrypted message. On the other hand, if $\min_{q_i}\{R_{k,i}\} \geq 0.5R_1$, then no matter what Eve's strategy is, the secrecy rate will always equal $0.5R_1$.

(5) Alice has to protect the encrypted message against jamming. But if Eve chooses to constantly play a strategy $q \in [0, q_1)$, Bob will only be able to decode level 1 of the code. This message, transmitted at a maximum rate of R_1, has to carry an encrypted message and generate a secret key, simultaneously. But if Eve's strategy remains in $[0, q_1)$ over the next frames, the rate of the encrypted message cannot exceed $0.5R_1$ – there would not be enough secret key bits to encrypt it. Therefore, the strategy $q \in [0, q_1)$ can function as a "default" state for Eve, where she could take refuge if the achievable secrecy rate under any other strategy exceeded $0.5R_1$. □

Theorems 5.6 and 5.7 above offer a good description of the achievable secrecy rates. However, in Theorem 5.6 we assumed that the set $\mathscr{I}_{ne}$ of indices corresponding to the levels that are *not perfectly decodable by Eve* is readily available. However, the characterization of the set $\mathscr{I}_{ne}$ and its complement $\mathscr{I}_e$ is not straightforward. At this time, we conjecture that these sets can be found as follows. The reasons behind our conjecture, as well as the reasons why it remains just a conjecture, are presented in Section 5.7.

Conjecture 5.8. *The maximal set of indices $\mathscr{I}_e$ corresponding to the levels that are perfectly decodable by Eve is the largest of the sets $\mathscr{V}_e$ for which*

$$\sum_{j\in\mathscr{S}} R_j \leq q\mathbf{E}_{h_W}\Big[\log\big(1+\frac{\sum_{j\in\mathscr{S}}(1-\alpha_j)\alpha_{j-1}\ldots\alpha_1 Ph_W}{\sigma_N^2+\sum_{i\in\mathscr{V}_e^c}(1-\alpha_i)\alpha_{i-1}\ldots\alpha_1 Ph_W}\big)\Big],\ \forall\mathscr{S}\subseteq\mathscr{V}_e, \tag{5.44}$$

where $\mathscr{V}_e^c$ is the complement of $\mathscr{V}_e$ with respect to $\widehat{\mathscr{I}}$

On the complexity of the algorithm

Our results so far facilitate the computation of an achievable secrecy rate, given a partition of the interval $[0, 1]$ expressed in terms of the parameters $\{q_1, q_2, \ldots, q_{n-1}\}$, and a power allocation between the encoding levels, given by the parameters $\{\alpha_1, \alpha_2, \ldots, \alpha_{n-1}\}$. If Alice and Bob wish

to exploit the full secrecy capabilities of the model, they should first perform a maximization of the achievable secrecy rate with respect to the parameters $\{(q_i, \alpha_i) : i = 1, 2, \ldots, n-1\}$.

Although the optimization problem requires a high complexity numerical algorithm (recall that for each value of the parameter vector $\{(q_i, \alpha_i) : i = 1, 2, \ldots, n-1\}$ we need to find the set $\mathscr{I}_{ne}$ as in the above Conjecture, which involves combinatorial complexity), it needs to be solved only once for the desired value of n. The optimal parameters may then be stored at both legitimate parties.

In an effort to reduce the complexity of the algorithm, we propose to pick the parameters $\{(q_i) : i = 1, \ldots, n-1\}$ such that $\{q_0, q_1, q_2, \ldots, q_{n-1}, q_n\}$ are all equally spaced, which corresponds to a uniform partition (or "quantization") of the interval $[0, 1]$. With this rule in place, the optimization needs to be performed only over the $(n-1)$ parameters $\alpha_1, \ldots, \alpha_{n-1}$, hence the complexity is reduced by half.

From our numerical results for $n = 2$ and $n = 3$ (see Figure 5.11), the loss of optimality due to the uniform partition of $[0, 1]$ is not very significant. We believe that, as n increases, this loss of performance should become negligible. Our remark is based on the fact that as $n \to \infty$ the optimal partition of the interval $[0, 1]$ approaches a uniform partition (with a vanishing step).

5.3.2 Numerical Results

In Figures 5.9 and 5.10 we show the improvement of our BMW secrecy encoding scheme over the worst-case scenario approach of (5.19). Note that if Eve's channel coefficient is close (statistically) to Bob's – the case of Figure 5.9 – the worst-case approach of (5.19) – or equivalently the case $n = 1$ – cannot achieve a positive secrecy rate.

However, even by Wyner's pure scheme (5.19) in Figure5.10 can achieve a positive secrecy rate if $\lambda_W > \lambda_M(1 + \frac{\mathscr{J}}{\sigma_N^2})$, as discussed in Section 5.3. The merit of our novel encoding scheme is significant. The minimax solution of Section 5.2 is given in both Figures 5.9 and 5.10 for comparison.

Figure 5.11 depicts the performance of the BMW secrecy encoding scheme when the partition of the interval $[0, 1]$ into intervals of the form $[q_{i-1}, q_1)$ is done uniformly, i.e. the parameters

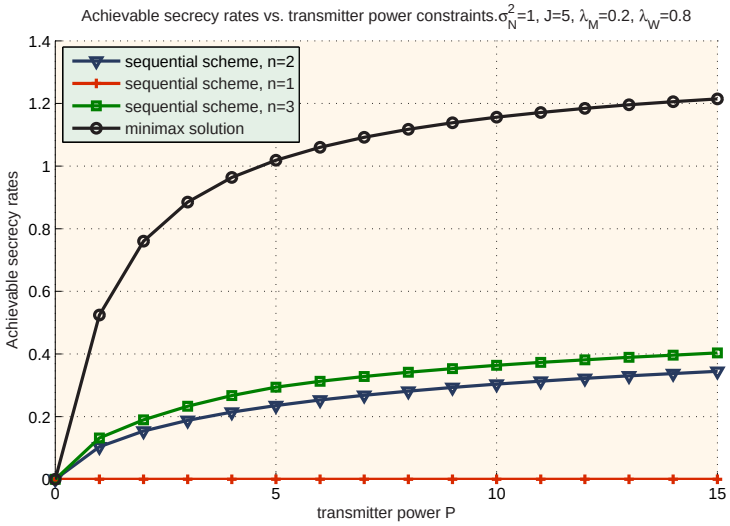

FIGURE 5.9. Achievable secrecy rates with our BMW secrecy encoding scheme. Exponentially distributed channel coefficients with $\lambda_M = 0.3$, $\lambda_W = 0.8$, $J = 5$, $\sigma_N^2 = 1$.

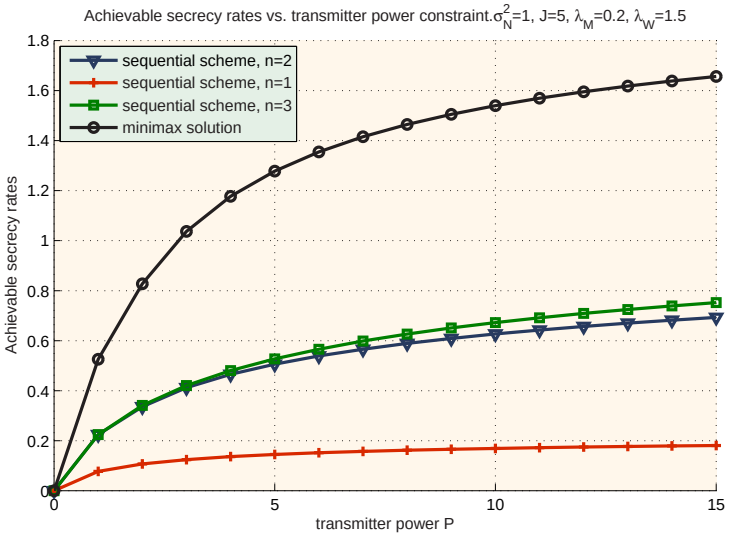

FIGURE 5.10. Achievable secrecy rates with our BMW secrecy encoding scheme. Exponentially distributed channel coefficients with $\lambda_M = 0.2$, $\lambda_W = 1.5$, $J = 5$, $\sigma_N^2 = 1$.

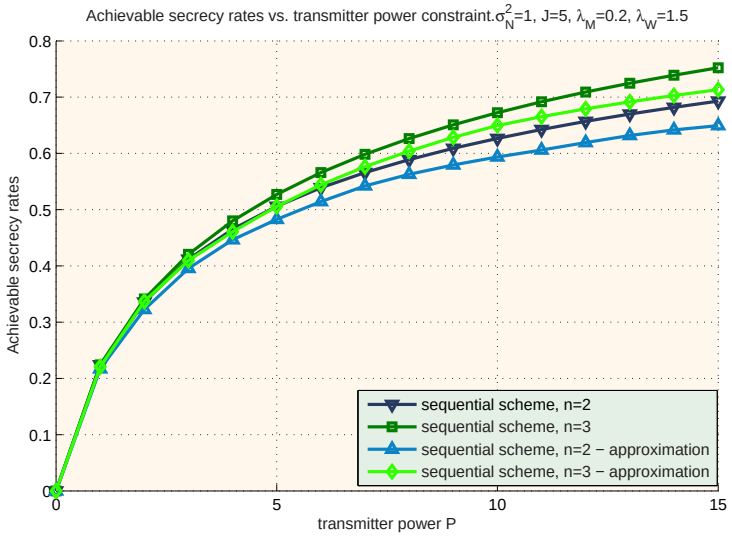

FIGURE 5.11. Achievable secrecy rates with our BMW secrecy encoding scheme, with uniform and with optimized partition of the interval $[0, 1]$. Exponentially distributed channel coefficients with $\lambda_M = 0.2$, $\lambda_W = 1.5$, $J = 5$, $\sigma_N^2 = 1$.

$q_0, q_1, q_2, \ldots, q_n$ are equally spaced, instead of being picked in an optimal way. We note that the degradation of the achievable secrecy rates is quite small and decreasing as n increases. Figures 5.12 and 5.13 show the design parameters used for obtaining the results of Figure 5.11.

5.4 Conclusions

We have seen how an active eavesdropper can seriously decrease the achievable secrecy rate in a classical scenario of a fast-fading AWGN channel with an eavesdropper. We have described both the best-case and the worst-case scenario formulations of the problem in which the objective is the achievable secrecy rate.

While the best-case scenario formulation is given mostly for completeness and comparison purposes, the importance of the worst-case scenario scenario should not be underestimated. This scenario models the most conservative and most practical approach to the active eavesdropper.

We have seen that, in order to take advantage of the non-duplex nature of the eavesdropper's terminal, we need a more elaborate, block-Markov Wyner encoding scheme. While in the classical eavesdropper scenario the legitimate receiver is completely passive, our scheme relies heavily on

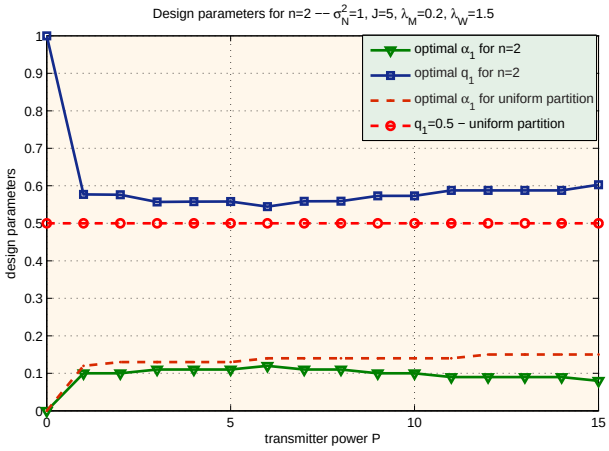

FIGURE 5.12. The encoding parameters q_1 and α_1 for the case $n = 2$: optimal and uniform partition of the interval [0,1]. Exponentially distributed channel coefficients with $\lambda_M = 0.2$, $\lambda_W = 1.5$, $J = 5$, $\sigma_N^2 = 1$.

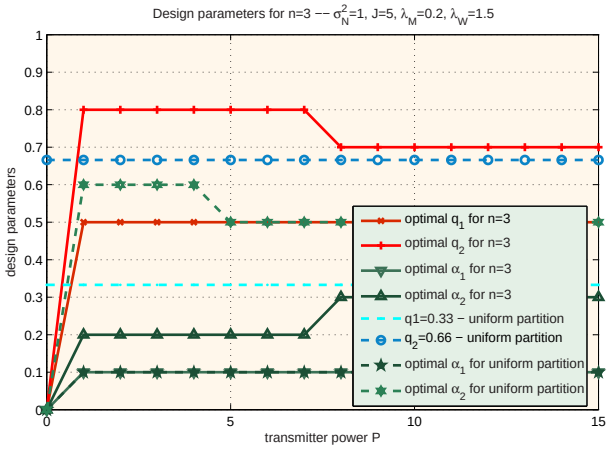

FIGURE 5.13. The encoding parameters q_1, q_2, α_1 and α_2 for the case $n = 3$: optimal and uniform partition of the interval [0,1]. Exponentially distributed channel coefficients with $\lambda_M = 0.2$, $\lambda_W = 1.5$, $J = 5$, $\sigma_N^2 = 1$.

the cooperation of the receiver. That means that at the end of each frame, Bob is required to feed back to Alice information about Eve's strategy, and then, based on this information, replicate Alice's efforts to distill a secret key.

The improvement of our BMW scheme over the passive-receiver solution to the maximin scenario is significant.

5.5 Additional Results. A Useful Lemma

The following lemma is used several times in this chapter.

Lemma 5.9. *The function*

$$f(q) = q\log(1+x) + (1-q)\log\left(1 + \frac{x}{1+\frac{y}{1-q}}\right), \tag{5.45}$$

where $x, y > 0$, is strictly increasing and strictly convex as a function of q.

Proof. It is straightforward to compute

$$\frac{df(q)}{dq} = \log\left((1+x)\frac{1+\frac{y}{1-q}}{1+x+\frac{y}{1-q}}\right) - \frac{xy}{1-q}\cdot\frac{1}{(1+\frac{y}{1-q})(1+x+\frac{y}{1-q})}, \tag{5.46}$$

and

$$\frac{d^2f(q)}{dq^2} = \frac{\frac{xy}{(1-q)^2}}{(1+\frac{y}{1-q})(1+x+\frac{y}{1-q})}\cdot\left[1 - \frac{1+x-(\frac{y}{(1-q)})^2}{(1+\frac{y}{1-q})(1+x+\frac{y}{1-q})}\right]. \tag{5.47}$$

Since $1+\frac{y}{1-q} > 1$ and $1+x-(\frac{y}{(1-q)})^2 < 1+x+\frac{y}{1-q}$, we can state that $\frac{d^2f(q)}{dq^2} > 0$. Therefore, $\frac{df(q)}{dq}$ is a strictly increasing function of q. But evaluating the first derivative in $q=0$ we get

$$\begin{aligned}\frac{df}{dq}(0) &= \log\left(\frac{(1+x)(1+y)}{1+x+y}\right) - \frac{xy}{(1+y)(1+x+y)} = \\ &= \log\left(1+\frac{xy}{1+x+y}\right) - \frac{xy}{(1+x+y)(1+y)} \overset{(a)}{\geq} \\ &\geq \frac{xy}{(1+x)(1+y)} - \frac{xy}{(1+x+y)(1+y)} \overset{(b)}{>} 0,\end{aligned} \tag{5.48}$$

where inequality (a) follows from $\log(1+\beta) > \frac{\beta}{1+\beta}$ for any $\beta > -1,\ \beta \neq 0$, if we replace $\beta = \frac{xy}{1+x+y}$, while inequality (b) follows since $x > 0$. Therefore $\frac{df(q)}{dq}$ is always strictly positive and strictly increasing, which implies that $f(q)$ is strictly increasing and strictly convex. □

5.6 Additional Results. Why the Encoding Method of [2] Is Incorrect

The encoding method of [2] uses a separate secret message encoding for each user, much like our own encoding scheme. However, unlike the present chapter, the secrecy encoding of [2] employs a "superposition encoding scheme" (see Section III of [2]). In the following paragraphs, we provide a brief description of this technique.

Take one user with power constraint P. The user generates two independent codebooks, in the following manner: the first codebook contains 2^{NR_s} N-dimensional codewords, and each letter of each codeword is independently generated, according to the realization of a Gaussian random variable of zero mean and variance αP; the second codebook contains 2^{NR_0} N-dimensional codewords, and each letter of each codeword is independently generated, according to the realization of a Gaussian random variable of zero mean and variance $(1-\alpha)P$. The secret message – transmitted at rate R_s – picks a codeword from the first codebook, while another codeword is randomly picked from the second codebook. The message transmitted by this user is the summation of the two codewords.

At a first glance, it appears that the transmitted message belongs to a codebook of $2^{N(R_s+R_0)}$ N-dimensional codewords, in which each letter of each codeword is the realization of a Gaussian random variable of variance P. Moreover, the codebook is already binned, like in Wyner's scheme [12].

However, if the transmitted message is completely decodable by Bob, the rates R_s and R_0 should be situated within the corresponding MAC rate region. For example, if we had a Gaussian eavesdropper channel where the AWGN variances were 1 for both channels, while the absolute squared channel coefficients are 1 for the main channel and h_k for the eavesdropper's channel, the rates should satisfy $R_s \leq \log\left[1+\alpha P\right]$, $R_0 \leq \log\left[1+(1-\alpha)P\right]$, and $R_s + R_0 \leq \log\left[1+P\right]$. But the first two conditions do not appear in [2].

Even if these conditions were satisfied, the "superposition encoding scheme" of [2] is not equivalent to Wyner's scheme. The key to Wyner's scheme is that each bin makes a "good" codebook for the eavesdropper. That is, given the secret key and the eavesdropper's received message, the bin chosen by the secret key conveys information to the eavesdropper at a rate arbitrarily close to the eavesdropper's channel capacity.

For the same toy model as above, the rate of each bin should be arbitrarily close to $\log[1+Ph_k]$. However, under the "superposition encoding scheme" of [2], this rate cannot exceed $\log[1+\alpha Ph_k]$[2]. To achieve the capacity of the eavesdropper's channel, α would need to be arbitrarily close to 1. But then the codebook associated with the secret message would be generated with arbitrarily small power. If a positive secrecy rate R_s is still desired, the intelligibility of the secret message at the legitimate receiver is compromised. Therefore, the "superposition encoding scheme" of [2] cannot work for secrecy encoding.

Also, we believe that the specification of the achievable rate region for the GGMAC-WT of [2] is too restrictive. This is because a subset $\mathscr{S}$ – the complement of which is denoted by $\mathscr{S}^c$ – of users with powers P_k and transmitting at rates R_k is not necessarily *decodable* by Eve if

$$\sum_{k\in\mathscr{S}} R_k < \log\left[1+\frac{\sum_{k\in\mathscr{S}} P_k h_k}{1+\sum_{j\in\mathscr{S}^c} P_j h_j}\right], \tag{5.49}$$

as suggested by condition (28) of [2]. In fact, it is possible to transmit a secret message over the GGMAC-WT of [2] even if $\sum_{k\in\mathscr{K}} P_k < \sum_{k\in\mathscr{K}} P_k h_k$, where $\mathscr{K}$ denotes the set of all users, as in [2]. E.g., imagine a two-user scenario, where user 1 has a large channel coefficient $h_1 >> 1$ to the eavesdropper, while user 2 has a channel coefficient $h_2 < 1$. It is intuitive that under these circumstances a secret message may still be transmitted by user 2, since the eavesdropper's extremely good channel from user 1 cannot yield any additional information about user 2.

[2]Note that although the second codebook has a rate equal to $\log[1+Ph_k]$ in [2], this rate is not sustainable by the eavesdropper's channel with power constraint αP.

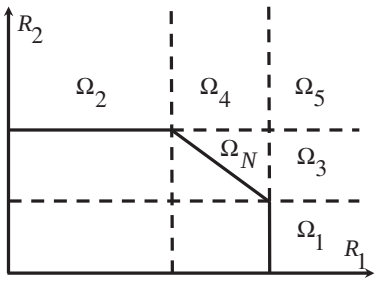

FIGURE 5.14. The capacity region of a MAC.

5.7 Additional Results. About Our Conjecture on the Maximal Set of Perfectly Decodable Encoding Levels

As we stated earlier, from Eve's point of view, the different encoding levels are very similar to different users. Therefore, Eve's channel can be seen as a multiple access channel (MAC), with n users, each with a different power, but all sharing the same channel coefficient. However, to the best of our knowledge, in the current literature there is no treatment of the achievable rate region for a set of users when the other users are not decodable.

As an example, we look at the two-user Gaussian MAC, the capacity region of which is given in Figure 5.14. Denote the two user's N-dimensional transmitted sequences by $\mathbf{X}_1$ and $\mathbf{X}_2$, respectively, and the received sequence by $\mathbf{Z} = \mathbf{X}_1 + \mathbf{X}_2 + \mathbf{Q}$, where $\mathbf{Q}$ is a sequence of i.i.d. realizations of a Gaussian random variable of variance σ_N^2.

Let the capacity of the first user's channel (when user 2 is absent) be $C_1 = \log(1 + P_1/\sigma_N^2)$, and the capacity of the second user's channel (when user 1 is absent) be $C_2 = \log(1 + P_2/\sigma_N^2)$. We know that the achievable rate region is given by all pairs (R_1, R_2) that satisfy

$$R_1 \leq C_1, \tag{5.50}$$

$$R_2 \leq C_2, \tag{5.51}$$

and

$$R_1 + R_2 \leq \log(1 + (P_1 + P_2)/\sigma_N^2). \tag{5.52}$$

This implies that when user 2 transmits at a rate $R_2 = C_2$, user 1 should be decoded by treating the second user as white Gaussian noise, and by performing successive interference cancellation. Hence, under this scenario, the first user's maximum decodable transmission rate is $R_1 = \log(1 + P_1/(\sigma_N^2 + P_2))$.

We know that user 1 can always be decoded if the pair of rates (R_1, R_2) falls within region Ω_2 of Figure 5.14, and similarly, user 2 can be decoded if (R_1, R_2) is in Ω_1. It is also clear that no user is decodable in region Ω_5. We are now concerned with the regions Ω_3 and Ω_4 in Figure 5.14.

For example, when user 2 cannot be decoded because $R_2 > C_2$, but it still uses a randomly generated Gaussian codebook, the first user's maximum decodable transmission rate may be larger than $\log(1 + P_1/(\sigma_N^2 + P_2))$. To justify this statement, consider the following "decoding" method. First, a *list* of possible codewords is computed for user 2, by treating user 1 as interference, and selecting only those codewords of the second user's codebook that have a non-zero a posteriori probability. This list may be shorter than the second user's whole codebook, and the a posteriori probability of the codewords therein may be non-uniform. Then, using this information about user 2, we attempt decoding for user 1. At this moment, we cannot state that this method is no better than the one which treats user 2 as interference.

However, our conjecture is equivalent to stating that the optimal strategy for user 1 is to treat user 2 as interference. We base our conjecture on the following arguments. It is clear that if $R_2 = C_2 - \epsilon$, even if we do not aim at decoding user 2, the maximum achievable rate of user 1 is still $\log(1 + P_1/(\sigma_N^2 + P_2))$. To see this, suppose user 1 were decodable at a rate $R_1 > \log(1 + P_1/(\sigma_N^2 + P_2))$. Then the receiver could subtract the first user's signal from the received sequence, and decode for user 2. Note that decoding for user 2 is possible with high probability, since this user employs a randomly generated Gaussian codebook, with a rate less than the capacity C_2. Hence, we would obtain a pair of rates outside the capacity region [48]. (This comment can also serve to prove that no user is decodable if (R_1, R_2) is in Ω_N of Figure 5.14.) On the other hand, as R_2 increases, the size of the "list" we might be able to compute for user 2 grows (exponentially with R_2). Hence, we

expect that at some point this list will become useless for decoding the first user. Eventually this will result in user 1 treating user 2 as interference.

Chapter 6
Future Work

While working on the problems treated in the previous chapters, we ran across many intriguing questions. Although some were answered and presented in this dissertation, several more remain on our open-problem list. In this final chapter we briefly discuss those which will most probably become the focus of our research in the near future.

6.1 The Converse to the Channel Coding Theorem and Transmission at Rates Larger than the Channel Capacity

Due to the nature of the physical layer secrecy problem, transmission has to take place at a rate larger than the eavesdropper's channel capacity. In the eavesdropper channel model the emerging uncertainty phenomenon is studied in the context of Wyner's special encoding scheme [12]. However, we have often faced the problem of quantifying the receiver's uncertainty about the transmitted message under a general (non-secrecy) channel encoding scheme with rate exceeding the channel capacity.

The problem is usually avoided in the related literature. Although sharing similarities with the concept of *list decoding* [49], the implications of this problem are quite deeper. For example, a simple study of the bounds on the error probability [45], [48] shows that for a random code with rate larger than capacity, both upper and lower bounds approach 1 as the codeword length approaches infinity. As a consequence, we believe that transmission might be possible at rates higher than capacity, with acceptable (but non-vanishing) codeword error probability, as long as the codeword length is not infinitely large.

One of our most recent encounters with this problem is the specification of the achievable rates under a multiple access channel (MAC) scenario, when not all of the users are perfectly decodable (see Appendix 5.7 in Chapter 5).

6.2 Multiuser Extensions of the Active Eavesdropper Channel Model

As a continuation of our work in Chapter 5, we are planning to extend the active eavesdropper channel model to multiuser scenarios. These extensions would eventually drive our research towards cooperative jamming and eavesdropping strategies, as we have already mentioned when we described “the big picture” in Chapter 1.

6.3 Optimal Transmitter-Receiver Collaboration for Secrecy

Although our results in Chapters 4 and 5 describe novel techniques to improve the achievable secrecy rates by allowing the legitimate parties to work together, we have not yet formulated any optimality statements. Both the feedback-based secrecy encoding scheme of Chapter 4 and our BMW scheme in Chapter 5 are suboptimal for several reasons described therein. One common reson is that the secrecy capacity of an eavesdropper channel with feedback is currently unknown. We are planning to investigate the optimal collaborative strategies that maximize the secrecy rate. We believe this might be related to the notion of physical layer secrecy in two-way channels.

6.4 Secrecy and the Rate of Convergence

In the treatment of channel coding [45], the *random coding exponent* describes the speed at which the average error probability of random codes approaches zero as the codeword length increases. The practical importance of this concept is obvious: in a practical scenario, where the codeword length can be large, but not infinite, the *random coding exponent* provides an indication of what an “acceptable” codeword length is, with respect to the achievable average error probability. We intend to define and formalize a similar concept for physical layer secrecy. Our “secrecy exponent” would show how fast the conditional entropy of the secret message, given the eavesdropper’s received sequence, approaches the unconditioned entropy of the secret message, as the codeword length increases. We believe that this kind of framework will bring the physical layer secrecy one step closer to practical implementation.

6.5 Secrecy in Slow-Fading Channels

To the best of our knowledge, the current literature deals with secrecy in slow-fading channels in two ways. The first direction, represented by papers like [23], [25] or [24], assumes that, although the fading is slow, the application exhibits enough delay tolerance to consider the channel ergodic. In other words, piece-wise encoding is performed on the sub-blocks of a codeword, such that fading is slow over each such sub-block. Moreover, it is assumed that there are enough sub-blocks in a codeword to exhibit the ergodic properties of the channel. The drawbacks of this direction have been clearly specified in Chapter 5.

A second, more natural direction is represented by papers like [26] and [27], where the slow fading channel is also delay constrained. Under these assumptions, there is no way to guarantee either the secrecy or the intelligibility (by the legitimate receiver) of a secret message under Wyner's encoding scheme [12]. Therefore, [26] and [27] both introduce the notion of *secrecy outage*. However, we see this notion as an oxymoron. Sticking to the notion of "perfect secrecy", under the scenario where some secret messages will inevitably be compromised, seems somewhat artificial.

We believe that a more appropriate objective for the scenario of slow-fading, delay-constrained channels would be a *secrecy mask*. We define a secrecy mask as a pair of ordered sets: a set $\mathscr{P} = \{p_1, p_2, \ldots, p_n\}$ of probabilities, such that $\sum_{i=1}^{n} p_i = 1$, and a set $\mathscr{D} = \{d_1, d_2, \ldots, d_n\}$ of equivocation values, such that $0 < d_1 < d_2 < \ldots < d_n < 1$. To meet the specifications of the *mask* means to make sure that $Pr\{\Delta \leq d_i\} \leq p_i \; \forall i = 1, 2, \ldots, n$, where Δ is the equivocation of a secret message, defined as the ratio between the conditional entropy of the secret message, given the eavesdropper's received sequence, and the unconditioned entropy of the secret message.

We see this as the most practical approach to secrecy in slow-fading channels so far. However, our *secrecy mask* approach raises some more questions, which remain open at this time. One of them is *what are the actual implications of non-perfect secrecy on the intelligibility of the secret message*.

6.6 Non-Perfect Secrecy

In the early '90s, [50] notes for the first time that Wyner's notion of secrecy [12] may not be the strongest. Indeed, as [50] points out, Wyner's secrecy definition reduces to $\frac{1}{k}H(\mathbf{K}^k|\mathbf{Z}^n) > H(K) - \epsilon$, for an arbitrarily small ϵ, as $n, k \to \infty$, where k is the length of the secret message $\mathbf{K}^k$, and n is the length of the eavesdropper's received codeword $\mathbf{Z}^n$. Here, the secret message is a sequence of i.i.d. symbols, each distributed according to the random variable K. The argument in [50] states that as $n, k \to \infty$, the amount of information about the secret message that leaks to the eavesdropper may be *significant* – note that $H(\mathbf{K}^k) - H(\mathbf{K}^k|\mathbf{Z}^n) < k\epsilon$. Therefore, they propose the notion of "strong secrecy", defined as $H(\mathbf{K}^k|\mathbf{Z}^n) > H(\mathbf{K}^k) - \epsilon$ as $n, k \to \infty$.

Our questions about the argument in [50] are *what does significant leakage mean* in the first place and *how can the eavesdropper use this information*. These two questions also hold for the previously discussed slow-fading channel scenario.

We believe that non-perfect secrecy, for example an equivocation $\Delta = \frac{H(\mathbf{K}^k|\mathbf{Z}^n)}{H(\mathbf{K}^k)} = 0.9$, may lead to the eavesdropper's ability to generate a list of messages (perhaps smaller than the whole codebook that the legitimate parties use), with different (a posteriori) probabilities of having been transmitted. This would be related to the problem of *list decoding* in [49].

Even if the eavesdropper could perfectly decode part of the secret message, this information might not be enough to understand the meaning of the overall secret message. For example, if the secure transmission of a page of text through multiple channel codewords is desired, and if a simple interleaving procedure is performed before channel encoding, compromising the secrecy of the message over only one codeword may reveal several letters randomly spread on the page. But this would by no means render the content of the page intelligible to the eavesdropper.

We believe that some light needs to be shed on the link between the imperfect secrecy and the eavesdropper's intelligibility of the message, and this subject is on our immediate research agenda. In this short section we talked about the *meaning* and the *intelligibility* of the message. We believe that in order to explore these notions, we first need to link our information theoretical problem to

a different area, which is strongly connected to the field of communications as part of electrical engineering: human communication, or *semantics*.

6.7 On Semantics and Its Implications in Communications Engineering

By definition, "semantics" is *the study of the meaning or relationship of meanings of a sign or set of signs*. Since the objective of communications – as part of electrical engineering – is to facilitate the transmission of meaningful messages at long distance, the composition and structure of those messages can be used to develop a better understanding of the concepts we use regularly in engineering.

This fact has been understood from the first mathematical formulation of the theory behind source and channel coding. Source coding itself is concerned with reducing the redundancy in a message, such that the size of that message is minimized for efficient storage or transmission over a channel [48]. The extent to which the size of a message can be reduced by source coding, such that it can be reproduced from its encoded version, up to some distortion constraint, is studied by the *rate distortion theory* [48].

However, the rate distortion theory, and the measures of distortion used therein for a particular type of message, are primarily concerned with the *quality* of the reproduction. At the other end, when looking at source coding from the security point of view, we are more interested in the converse problem: *what is the minimum distortion necessary to render the reproduction unintelligible*. We believe that the concept of "unintelligibility" is vital to leading the field of information-theoretic secrecy towards practical implementation. Until this concept is defined, the only notion of secrecy that makes sense is that of "perfect strong secrecy" [49].

This is the motivation behind our goal to extend the applicability of physical-layer secrecy by launching our own cross-disciplinary research, and incorporating concepts from *semantics* and *hermeneutics* (the study of interpretation theory) into the already-existing engineering framework.

Bibliography

[1] D. Gunduz, D. R. Brown, and H. V. Poor, "Secret communication with feedback," *Int. Symp. on Inform. Theory and its Applications (ISITA)*, Dec. 2008.

[2] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way channels: achievable rates and cooperative jamming," *IEEE Trans. Inform. Theory*, vol. 54, pp. 2735–2751, June 2008.

[3] T. Basar, "The Gaussian test channel with an intelligent jammer," *IEEE Trans. Inform. Theory*, vol. 29, pp. 152–157, Jan. 1983.

[4] T. Basar and Y.-W. WU, "A complete characterization of minimax and maximin encoder-decoder policies for communication channels with incomplete statistical description," *IEEE Trans. Inform. Theory*, vol. 31, pp. 482–489, July 1985.

[5] M. Medard, "Capacity of correlated jamming channels," *Allerton Annual Conf. on Comm., Control and Computing*, 1997.

[6] A. Bayesteh, M. Ansari, and A. K. Khandani, "Effect of jamming on the capacity of MIMO channels," *Allerton Annual Conf. on Comm., Control and Computing*, 2004.

[7] A. Kashyap, T. Basar, and R. Srikant, "Correlated jamming on mimo Gaussian fading channels," *IEEE Trans. Inform. Theory*, vol. 50, pp. 2119–2123, Sept. 2004.

[8] M. H. Brady, M. Mohseni, and J. M. Cioffi, "Spatially-correlated jamming in Gaussian multiple access and broadcast channels," *Proc. Confe. on Inform., Science, and Systems, Princeton*, March 2006.

[9] S. Shafiee and S. Ulukus, "Correlated jamming in multiple access channels," *Conference on Information Sciences and Systems*, March 2005.

[10] ——, "Capacity of multiple access channels with correlated jamming," *Military Communications Conference, MILCOM*, vol. 1, pp. 218–224, Oct. 2005.

[11] B. Hughes and P. Narayan, "Gaussian arbitrarily varying channels," *IEEE Trans. Inform. Theory*, vol. 33, pp. 267–284, March 1987.

[12] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, pp. 1355–1387, Oct. 1975.

[13] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, pp. 339–348, May 1978.

[14] M. van Dijk, "On a special class of broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 43, pp. 712–714, March 1997.

[15] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inform. Theory*, vol. 24, pp. 451–456, July 1978.

[16] T. M. Cover, "Broadcast channels," *IEEE Trans. Inform. Theory*, vol. 18, pp. 2–14, Jan. 1972.

[17] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel: Wireless secrecy and cooperative jamming," *Information Theory and Applications Workshop*, pp. 404–413, Jan. 2007.

[18] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inform. Theory*, vol. 54, pp. 4005–4019, Sept. 2008.

[19] Y. Oohama, "Relay channels with confidential messages," *arXiv:cs.IT/0611125v3*, Dec. 2006.

[20] U. E. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, pp. 733–742, May. 1993.

[21] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography – part I: Secret sharing," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1121–1132, July 1993.

[22] Z. Li, R. Yates, and W. Trappe, "Secret communication with a fading eavesdropper channel," *Proc. IEEE Int. Symp. on Inform. Theory (ISIT)*, June 2007.

[23] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inform. Theory*, vol. 54, pp. 4687–4698, Oct. 2008.

[24] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inform. Theory*, vol. 54, pp. 2470–2492, June 2008.

[25] A. Khisti, A. Tchamkerten, and G. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inform. Theory*, vol. 54, pp. 2453–2469, June 2008.

[26] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," *Proc. IEEE Int. Symp. on Inform. Theory (ISIT)*, July 2006.

[27] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels," *IEEE Trans. Inform. Theory*, vol. 55, pp. 1575–1591, Apr. 2009.

[28] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.

[29] G. Caire and S. Shamai, "On the capacity of some channels with channel state information," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2007–2019, Sept. 1999.

[30] S. N. Diggavi and T. Cover, "The worst additive noise under a covariance constraint," *IEEE Trans. Inform. Theory*, vol. 47, pp. 3072–3081, Nov. 2001.

[31] R. M. Bell and T. M. Cover, "Competitive optimality of logarithmic investment," *Math. Oper. Res.*, vol. 5, pp. 161–166, 1980.

[32] G. Caire, G. Taricco, and E. Biglieri, "Optimum power control over fading channels," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1468–1489, July 1999.

[33] R. B. Meyerson, *Game Theory (Analysis of Conflict)*. Harvard University Press, 1997.

[34] D. P. Bertsekas, A. Nedic, and A. E. Ozdaglar, *Convex Analysis and Optimization*. Athena Scientific, 2003.

[35] A. J. Goldsmith and P. P. Varaiya, "Capacity of fading channels with channel state information," *IEEE Trans. Inform. Theory*, vol. 43, pp. 1986–1992, Nov. 1997.

[36] A. H. Zemanian, *Distribution theory and transform analysis: an introduction to generalized functions, with applications*. Dover Pubns., 1987.

[37] R. K. Mallik, R. A. Scholtz, and G. P. Papavassilopuolos, "Analysis of an On-Off jamming situation as a dynamic game," *IEEE Trans. Commun.*, vol. 48, pp. 1360–1373, Aug. 2000.

[38] E. Altman, K. Avrachenkov, and A. Garnaev, "A jamming game in wireless networks with transmission cost," *Proceedings of Net-Coop, Avignon, France*, June 2007.

[39] J.-P. Aubin, *Optima and Equilibria*. Springer-Verlag, 1993.

[40] J. R. Munkres, *Topology*. Prentice-Hall, 2004.

[41] L. Lai, H. E. Gamal, and V. Poor, "The wiretap channel with feedback: Encryption over the channel," *IEEE Trans. Inform. Theory*, vol. 54, pp. 5059–5067, Nov. 2008.

[42] E. Ardetsanizadeh, M. Franceschetti, T. Javidi, and Y.-H. Kim, "Wiretap channel with rate-limited feedback," *Proc. IEEE Int. Symp. on Inform. Theory (ISIT)*, July 2008.

[43] B. Schneier, *Applied cryptography*. John Wiley & Sons, 1996.

[44] U. Erez and R. Zamir, "Achieving $\frac{1}{2}\log(1+SNR)$ on the AWGN channel with lattice encoding and decoding," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1121–1132, July 1993.

[45] R. G. Gallager, *Information Theory and Reliable Communication*. John Wiley and Sons, Inc., 1968.

[46] H. G. Eggleston, *Convexity*. Cambridge University Press, 1958.

[47] H. J. Greenberg and W. P. Pierskalla, "A review of quasiconvex functions," *Operations Research*, vol. 19, pp. 1553–1570, Nov.-Dec. 1971.

[48] T. M. Cover and J. A. Thomas, *Elements of information theory (second ed.)*. Hoboken, New Jersey: John Wiley & Sons, Inc., 2006.

[49] J. Wolfowitz, "On list codes," *Journal of Combinatorics, Information & System Sciences*, vol. 4, pp. 117–122, 1979.

[50] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1915–1923, Nov. 1995.

Vita

George T. Amariucai was born in December 1979, in Piatra Neamt, Romania. He finished his undergraduate studies at the University Politehnica of Bucharest in June 2003. He earned a master of science degree in electrical engineering from the University Politehnica of Bucharest in June 2004. In August 2004 he came to Louisiana State University to pursue graduate studies. He is currently a candidate for the degree of Doctor of Philosophy in the Department of Electrical and Computer Engineering. In August 2009 he will join the Department of Electrical and Computer Engineering at Iowa State University, as an Adjunct Assistant Professor.