Summer 8-2011

COOPERATIVE WIRELESS COMMUNICATIONS: THE IMPACT OF CHANNEL UNCERTAINTY AND PHYSICAL-LAYER SECURITY CONSIDERATIONS

Junwei Zhang
University of Nebraska - Lincoln., junweizhang2006@gmail.com

COOPERATIVE WIRELESS COMMUNICATIONS: THE IMPACT OF CHANNEL UNCERTAINTY AND PHYSICAL-LAYER SECURITY CONSIDERATIONS

by

Junwei Zhang

A DISSERTATION

Presented to the Faculty of

The Graduate College at the University of Nebraska

In Partial Fulfilment of Requirements

For the Degree of Doctor of Philosophy

Major: Engineering

Under the Supervision of Professor Mustafa Cenk Gursoy

Lincoln, Nebraska

August, 2011

COOPERATIVE WIRELESS COMMUNICATIONS: THE IMPACT OF CHANNEL UNCERTAINTY AND PHYSICAL-LAYER SECURITY CONSIDERATIONS

Junwei Zhang, Ph. D.

University of Nebraska, 2011

Adviser: Mustafa Cenk Gursoy

In this thesis, cooperative wireless communication strategies are studied in the presence of channel uncertainty and physical-layer security considerations. Initially, achievable rates and resource allocation strategies for imperfectly-known fading relay channels are investigated. Amplify-and-forward (AF) and decode-and-forward (DF) relaying schemes with different degrees of cooperation are considered. The corresponding achievable rate expressions are obtained and efficient resource allocation strategies are identified. Then, the analysis is extended to two-way decode-and-forward (DF) fading relay channels. In the second part of the thesis, the concentration is on wireless information-theoretic security. First, collaborative beamforming schemes for both DF and AF relaying are studied under secrecy constraints. The optimal selection of the beamforming vector is formulated as a semidefinite programming problem and an iterative algorithm is proposed to numerically obtain the optimal beamforming structure and maximize the secrecy rates. In addition, for DF relaying, the worst-case robust beamforming design is identified when channel state information (CSI) is imperfect but bounded, and the statistical robust beamforming design based upon minimum non-outage probability criterion is analyzed. Collaborative relay beamforming for secure broadcasting is subsequently investigated. Novel DF-based null space

beamforming schemes are proposed and the optimality of these schemes is investigated by comparing them with the outer bound secrecy rate region. Then, information-theoretic security in cognitive radios is explored. AF relay beamforming designs in the presence of an eavesdropper and a primary user are studied and compared with sub-optimal null space beamforming schemes. Secrecy capacity limits and optimal power allocation of opportunistic spectrum-sharing channels in fading environments are investigated. Finally, secrecy rates are analyzed over weak Gaussian interference channels for different transmission schemes.

ACKNOWLEDGMENTS

First, I would like to thank my advisor, Professor Mustafa Cenk Gursoy for his guidance throughout my graduate program. I thank him for always encouraging me to work on theoretically challenging problems. I also thank him for always being patient and cheering me up no matter how stuck I got or even failed after months or years of efforts. I highly appreciate the environment he fosters in our group, which I believe is very healthy and helpful for theoretical and creative research.

I also would like to thank Professors Lance C. Pérez, Michael W. Hoffman, and Mehmet Can Vuran for serving on my Ph.D. dissertation committee and providing many valuable comments and suggestions. Their input has strengthened my thesis and brought insightful perspectives of other fields into my research.

Throughout my graduate program, I have been surrounded by an amazing group of colleagues at UNL. My countless conversations with them have been invaluable to my research and to learning about other fields. I especially thank my fellow students from both the Wireless Communications and Networking Laboratory as well as the Smart Vision Systems Laboratory. The discussions, chats and laughters with them made my life in Nebraska much more fun.

Lastly, and most importantly, I would like to thank my parents Xinqiao Zhang and Songru Zhou for always being loving, caring and encouraging. Even in the most difficult times, they never lost their confidence and belief in me. I can always rely on their advices and support. Without them, I could not reach this far.

Contents

List of Figures

Chapter 1

Introduction

1.1 Cooperative Wireless Communications

In wireless communications, deterioration in performance is experienced due to various impediments such as interference, fluctuations in power due to reflections and attenuation, and randomly-varying channel conditions caused by mobility and changing environment. Recently, cooperative wireless communications has attracted much interest as a technique that can mitigate these degradations and provide higher rates or improve the reliability through diversity gains. The relay channel was first introduced by van der Meulen in [68], and initial research was primarily conducted to understand the rates achieved in relay channels [13] [19]. More recently, diversity gains of cooperative transmission techniques have been studied in [62] [40][39]. In [40], several cooperative protocols have been proposed, with amplify-and-forward (AF) and decode-and-forward (DF) being the two basic relaying schemes. The performance of these protocols are characterized in terms of outage events and outage probabilities. In [55], three different time-division AF and DF cooperative protocols with different degrees of broadcasting and receive

collision are studied. Resource allocation for relay channel and networks has been addressed in several studies (see e.g., [31][25][74][44][43][57]). In [31], upper and lower bounds on the outage and ergodic capacities of relay channels are obtained under the assumption that the channel side information (CSI) is available at both the transmitter and receiver. Power allocation strategies are explored in the presence of a total power constraint on the source and relay. In [25], under again the assumption of the availability of CSI at the receiver and transmitter, optimal dynamic resource allocation methods in relay channels are identified under total average power constraints and delay limitations by considering delay-limited capacities and outage probabilities as performance metrics.

Another important concern in wireless communications is the efficient use of limited energy resources. Hence, the energy required to reliably send one bit is a metric that can be adopted to measure the performance. Generally, energy-per-bit requirement is minimized, and hence the energy efficiency is maximized, if the system operates in the low-SNR regime. In [69], Verdu has analyzed the trade-off between the spectral efficiency and bit energy in the low-SNR regime for a general class of channels. As argued in [69], two key performance measures in the low-power regime are the minimum energy per bit $\frac{E_b}{N_0}_{\min}$ required for reliable communication and the slope of the spectral efficiency versus $\frac{E_b}{N_0}$ curve at $\frac{E_b}{N_0}_{\min}$. Caire *et al.* in [9] employed these two measures to study the multiple access, broadcast, and interference channels in the low-power regime. By comparing the performance of TDMA and superposition schemes, they concluded that the growth of TDMA-achievable rates with energy per bit is suboptimal except in some special cases. In [74], resource allocation schemes in relay channels are studied in the low-power regime when only the receiver has perfect CSI. Liang *et al.* in [44] investigated resource allocation strategies under separate power con-

straints at the source and relay nodes, and showed that the optimal strategies differ depending on the channel statics and the values of the power constraints.

A spectrally efficient relaying technique named two-way relaying has been proposed in [61] and [41], in which two nodes are able to exchange information via the help of a relay node. Two-way relaying method consists of two phases: the multiple access (MAC) phase in which the source nodes simultaneously transmit their data to the relay, and the broadcast (BC) phase in which the relay forwards the received signal to the sources. One key technique in two-way relaying is interference cancelation in which the source nodes subtract their own forwarded signals from the received signal. However, perfect interference cancelation requires perfect knowledge of the channel conditions and most work on two-way relay channels have assumed the availability of perfect channel side information at the receivers.

1.2 Imperfectly-Known Channel Conditions

As noted above, studies on relaying and cooperation are numerous. However, most work has assumed that the channel conditions are perfectly known at the receiver and/or transmitter sides. Especially in mobile applications, this assumption is unwarranted as randomly-varying channel conditions can be learned by the receivers only imperfectly. Moreover, the performance analysis of cooperative schemes in such scenarios is especially interesting and called for because relaying introduces additional channels and hence increases the uncertainty in the model if the channels are known only imperfectly. Recently, Wang *et al.* in [71] considered pilot-assisted transmission over wireless sensory relay networks, and analyzed scaling laws achieved by the amplify-and-forward scheme in the

asymptotic regimes of large nodes, large block length, and small signal-to-noise ratio (SNR) values. In this study, the channel conditions are being learned only by the relay nodes. In [20] and [58], estimation of the overall source-relay-destination channel is addressed for amplify-and-forward relay channels. In [20], Gao *et al.* considered both the least squares (LS) and minimum-mean-square error (MMSE) estimators, and provided optimization formulations and guidelines for the design of training sequences and linear precoding matrices. In [58], under the assumption of fixed power allocation between data transmission and training, Patel and Stüber analyzed the performance of linear MMSE estimation in relay channels. In both [20] and [58], the training design is studied in an estimation-theoretic framework, and mean-square errors and bit error rates, rather than the achievable rates, are considered as performance metrics. Performance analysis and resource allocation strategies have not been sufficiently addressed for imperfectly-known relay channels in an information-theoretic context by considering rate expressions. We note that Avestimehr and Tse in [5] studied the outage capacity of slow fading relay channels. They showed that Bursty Amplify-Forward strategy achieves the outage capacity in the low SNR and low outage probability regime. Interestingly, they further proved that the optimality of Bursty AF is preserved even if the receivers do not have prior knowledge of the channels. The training design for the two-way amplify-and-forward (AF) relaying was recently studied in [33] and [32]. In [32], the authors derived lower bounds on the training-based individual rates and sum-rate. Given the total transmit power constraint, they investigated the optimal power allocation between the two terminals and the relay.

1.3 Physical-Layer Security

The broadcast nature of wireless transmissions allows for the signals to be received by all users within the communication range, making wireless communications vulnerable to eavesdropping. The problem of secure transmission in the presence of an eavesdropper was first studied from an information-theoretic perspective in [73] where Wyner considered a wiretap channel model. Wyner showed that secure communication is possible without sharing a secret key if the eavesdropper's channel is a degraded version of the main channel, and identified the rate-equivocation region and established the secrecy capacity of the degraded discrete memoryless wiretap channel. The secrecy capacity is defined as the maximum achievable rate from the transmitter to the legitimate receiver, which can be attained while keeping the eavesdropper completely ignorant of the transmitted messages. Later, Wyner's result was extended to the Gaussian channel in [42] and recently to fading channels in [43] and [24]. In addition to the single antenna case, secrecy in multi-antenna models is addressed in [64] and [36]. One particular result in [64] and [36] that is related to our study is that for the multiple-input single-output (MISO) secrecy channel, the optimal transmitting strategy is beamforming based on the generalized eigenvector of two matrices that depend on the channel coefficients. Regarding multiuser models, Liu *et al.* [45] presented inner and outer bounds on secrecy capacity regions for broadcast and interference channels. The secrecy capacity of the multi-antenna broadcast channel is obtained in [46]. Bloch *et al.* in [7] discussed the theoretical aspects and practical schemes for wireless information-theoretic security.

Having multiple antennas at the transmitter and receiver has multitude of benefits in terms of increasing the performance, and provides the potential to

improve the physical-layer security as well. Additionally, it is well known that even if they are equipped with single-antennas individually, users can cooperate to form a distributed multi-antenna system by performing relaying [40][55][37]. When channel side information (CSI) is exploited, relay nodes can collaboratively work similarly as in a multiple-input multiple-output (MIMO) system to build a virtual beam towards the receiver. Relay beamforming research has attracted much interest recently (see e.g., [35][86][34][56][87] and references therein). The optimal power allocation at the relays has been addressed in [86] and [34] when instantaneous CSI is known. In [56], the problem of distributed beamforming in a relay network is considered with the availability of second-order statistics of CSI. Most recently, Zheng *et al.* [87] have addressed the robust collaborative relay beamforming design by optimizing the weights of amplify-and-forward (AF) relays. They maximize the worst-case signal-to-noise ratio (SNR) assuming that CSI is imperfect but bounded. Transmit beamforming and receive beamforming strategies have been studied extensively for over a decade. A recent tutorial paper [21] provides an overview of advanced convex optimization approaches to both transmit, receive and network beamforming problems, and includes a comprehensive list of references in this area.

Cooperative relaying under secrecy constraints was also recently studied in [17][18][16][3] . In [17], a decode-and-forward (DF) based cooperative protocol is considered, and a beamforming system is designed for secrecy capacity maximization or transmit power minimization. For amplify-and-forward (AF), suboptimal closed-form solutions that optimize bounds on secrecy capacity are proposed in [18]. However, in those studies, the analysis is conducted only under total relay power constraints and perfect CSI assumption.

1.4 Cognitive Radio

The need for the efficient use of the scarce spectrum in wireless applications has led to significant interest in the analysis of cognitive radio systems. One possible scheme for the operation of the cognitive radio network is to allow the secondary users to transmit concurrently on the same frequency band with the primary users as long as the resulting interference power at the primary receivers is kept below the interference temperature limit [29]. Note that interference to the primary users is caused due to the broadcast nature of wireless transmissions, which allows the signals to be received by all users within the communication range. A significant amount of work has been done to study the transmitter design under such interference constraints, e.g., in [22] and [54] for the fading channel, in [85] for the multiple-input multiple-output (MIMO) channel, in [51] for the relay channel. Although cognitive radio networks are also susceptible to eavesdropping, the combination of cognitive radio channels and information-theoretic security has received little attention. Very recently, Pei *et al.* in [59] studied secure communication over multiple input, single output (MISO) cognitive radio channels. In this work, finding the secrecy-capacity-achieving transmit covariance matrix under joint transmit and interference power constraints is formulated as a quasiconvex optimization problem.

1.5 Overview of the Thesis and Contributions

In this thesis, we initially explore achievable rates and resource allocation strategies for imperfectly-known fading relay channels. Then, we focus on secure communication at the physical layer. Specially, we investigate the collaborative

use of relays to form a beamforming system and provide physical-layer security.

The organization of the rest of the thesis is as follows:

In Chapter 2, achievable rates and resource allocation strategies for imperfectly-known fading relay channels are studied. It is assumed that communication starts with the network training phase in which the receivers estimate the fading coefficients of the channels. In the data transmission phase, amplify-and-forward and decode-and-forward relaying schemes with different degrees of cooperation are considered, and the corresponding achievable rate expressions are obtained. Three resource allocation problems are addressed: 1) power allocation between data and training symbols; 2) time/bandwidth allocation to the relay; 3) power allocation between the source and relay in the presence of total power constraints. The achievable rate expressions are employed to identify efficient resource allocation strategies. Several observations with important practical implications are made. It is noted that unless the source-relay channel quality is high, cooperation is not beneficial and noncooperative direct transmission should be preferred at high signal-to-noise ratio (SNR) values when amplify-and-forward or decode-and-forward with repetition coding is employed as the cooperation strategy. On the other hand, relaying is shown to generally improve the performance at low SNRs. Additionally, transmission schemes in which the relay and source transmit in non-overlapping intervals are seen to perform better in the low-SNR regime. Finally, through a bit energy analysis, it is noted that care should be exercised when operating at very low SNR levels, as energy efficiency significantly degrades below a certain SNR threshold value. This chapter, as a journal paper, appeared in EURASIP Journal on Wireless Communications and Networking in 2009 [75], and, as conference papers, appeared in the Proceedings of Annual Allerton Conference on Communication, Control and Computing in 2007 [76] and IEEE International

Workshop on Signal Processing Advances in Wireless Communications (SPAWC) in 2008 [77].

In Chapter 3, achievable rates and resource allocation strategies for imperfectly known two-way relay fading channels are studied. Decode-and-forward (DF) relaying is considered. It is assumed that communication starts with the network training phase in which the users and the relay estimate the fading coefficients, albeit imperfectly. Subsequently, data transmission is performed in multiple-access and broadcast phases. In both phases, achievable rate regions are identified by treating the terms that arise due to channel estimation errors and imperfect interference cancelation as Gaussian distributed noise components. The achievable rate region of the two-way relay channel is given by the intersection of the achievable rate regions of multiple-access and broadcast phases. The impact of several training and transmission parameters (such as training power levels, time/bandwidth allocated to the multiple access and broadcast phases, and relay power allocation parameter) on the achievable rate regions and sum rates is investigated. This chapter, as a conference paper, appeared in the Proceedings of IEEE International Symposium on Information Theory (ISIT) in 2011 [81].

In Chapter 4, collaborative use of relays to form a beamforming system and provide physical-layer security is investigated. In particular, decode-and-forward (DF) and amplify-and-forward (AF) relay beamforming designs under total and individual relay power constraints are studied with the goal of maximizing the secrecy rates when perfect channel state information (CSI) is available. In the DF scheme, the total power constraint leads to a closed-form solution, and in this case, the optimal beamforming structure is identified in the low and high signal-to-noise ratio (SNR) regimes. The beamforming design under individual relay power constraints is formulated as an optimization problem which is shown to be

easily solved using two different approaches, namely semidefinite programming and second-order cone programming. A simplified and suboptimal technique which reduces the computational complexity under individual power constraints is also presented. In the AF scheme, not having analytical solutions for the optimal beamforming design under both total and individual power constraints, an iterative algorithm is proposed to numerically obtain the optimal beamforming structure and maximize the secrecy rates. Finally, robust beamforming designs in the presence of imperfect CSI are investigated for DF-based relay beamforming, and optimization frameworks are provided. This chapter, as conference papers, appeared in the Proceedings of the IEEE International Conference on Communication (ICC) in 2010 [78] and the 44th Annual Conference on Information Sciences and Systems in 2010. [80]

In Chapter 5, collaborative use of relays to form a beamforming system with the aid of perfect channel state information (CSI) and to provide secure communication between a transmitter and two receivers is investigated. In particular, we describe decode-and-forward based null space beamforming schemes and optimize the relay weights jointly to obtain the largest secrecy rate region. Furthermore, the optimality of the proposed schemes is investigated by comparing them with the outer bound secrecy rate region. This chapter, as a conference paper, appeared in the Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC) in 2010 [79].

In Chapter 6, a cognitive relay channel is considered, and amplify-and-forward (AF) relay beamforming designs in the presence of an eavesdropper and a primary user are studied. Our objective is to optimize the performance of the cognitive relay beamforming system while limiting the interference in the direction of the primary receiver and keeping the transmitted signal secret from the eavesdropper.

We show that under both total and individual power constraints, the problem becomes a quasiconvex optimization problem which can be solved by interior point methods. We also propose two sub-optimal null space beamforming schemes which are obtained in a more computationally efficient way. This chapter, as a conference paper, appeared in the Proceedings of the 45th Annual Conference on Information Sciences and Systems (CISS) in 2011 [82].

In Chapter 7, we consider a scenario in which a secondary user is operating in the presence of both a primary user and an eavesdropper. Hence, the secondary user has both interference limitations and security considerations. In such a scenario, we study the secrecy capacity limits of opportunistic spectrum-sharing channels in fading environments and investigate the optimal power allocation for the secondary user under average and peak received power constraints at the primary user with global channel side information (CSI). Also, in the absence of the eavesdropper's CSI, we study optimal power allocation under an average power constraint and propose a suboptimal on/off power control method.

In Chapter 8, we study the secrecy rates over weak Gaussian interference channels for different transmission schemes. We focus on the low-SNR regime and obtain the minimum bit energy $\frac{E_b}{N_0}_{\min}$ values, and the wideband slope regions for both TDMA and multiplexed transmission schemes. We show that secrecy constraints introduce a penalty in both the minimum bit energy and the slope regions. Additionally, we identify under what conditions TDMA or multiplexed transmission is optimal. Finally, we show that TDMA is more likely to be optimal in the presence of secrecy constraints.

Chapter 2

Achievable Rates and Resource Allocation Strategies for Imperfectly-Known Fading Relay Channels

In this chapter, we study the imperfectly-known fading relay channels. We assume that transmission takes place in two phases: *network training phase* and *data transmission phase*. In the network training phase, a-priori unknown fading coefficients are estimated at the receivers with the assistance of pilot symbols. Following the training phase, AF and DF relaying techniques are employed in the data transmission. Our contributions in this chapter are the following:

1. We obtain achievable rate expressions for AF and DF relaying protocols with different degrees of cooperation, ranging from noncooperative communications to full cooperation. We provide a unified analysis that applies to both

overlapped and non-overlapped transmissions of the source and relay. We note that achievable rates are obtained by considering the ergodic scenario in which the transmitted codewords are assumed to be sufficiently long to span many fading realizations.

2. We identify resource allocation strategies that maximize the achievable rates. We consider three types of resource allocation problems:

   a) power allocation between data and training symbols;

   b) time/bandwidth allocation to the relay;

   c) power allocation between the source and relay if there is a total power constraint in the system.

3. We investigate the energy efficiency in imperfectly-known relay channels by finding the bit energy requirements in the low-SNR regime.

The organization of the rest of the chapter is as follows. In Section 2.1, we describe the channel model. Network training and data transmission phases are explained in Section 2.2. We obtain the achievable rate expressions in Section 2.3 and study the resource allocation strategies in Section 2.4. We discuss the energy efficiency in the low-SNR regime in Section 2.5. Finally, we provide conclusions in Section 2.6. The proofs of the achievable rate expressions are relegated to the Appendix.

2.1 Channel Model

We consider a three-node relay network which consists of a source, destination, and a relay node. This relay network model is depicted in Figure 2.1.

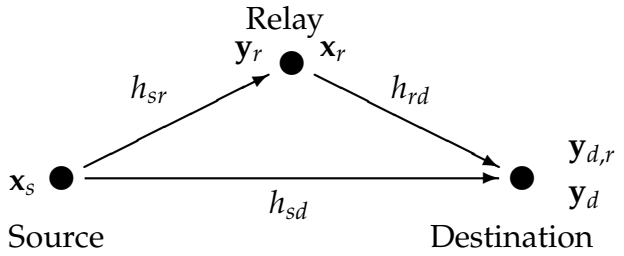

Figure 2.1: Three-node relay network model

Source-destination, source-relay, and relay-destination channels are modeled as Rayleigh block-fading channels with fading coefficients denoted by h_{sd}, h_{sr}, and h_{rd}, respectively for each channel. Due to the block-fading assumption, the fading coefficients $h_{sr} \sim \mathcal{CN}(0, {\sigma_{sr}}^2)$, $h_{sd} \sim \mathcal{CN}(0, {\sigma_{sd}}^2)$, and $h_{rd} \sim \mathcal{CN}(0, {\sigma_{rd}}^2)$ stay constant for a block of m symbols before they assume independent realizations for the following block[1]. In this system, the source node tries to send information to the destination node with the help of the intermediate relay node. It is assumed that the source, relay, and destination nodes do not have prior knowledge of the realizations of the fading coefficients. The transmission is conducted in two phases: *network training phase* in which the fading coefficients are estimated at the receivers, and *data transmission phase*. Overall, the source and relay are subject to the following power constraints in one block:

$$|x_{s,t}|^2 + E\{\|\mathbf{x}_s\|^2\} \leq mP_s, \tag{2.1}$$

$$|x_{r,t}|^2 + E\{\|\mathbf{x}_r\|^2\} \leq mP_r, \tag{2.2}$$

[1] $x \sim \mathcal{CN}(d, \sigma^2)$ is used to denote a proper complex Gaussian random variable with mean d and variance σ^2.

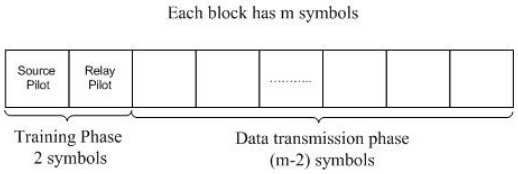

Figure 2.2: Transmission structure in a block of m symbols.

where $x_{s,t}$ and $x_{r,t}$ are the training symbols sent by the source and relay, respectively, and $\mathbf{x}_s$ and $\mathbf{x}_r$ are the corresponding source and relay data vectors. The pilot symbols enable the receivers to obtain the minimum mean-square error (MMSE) estimates of the fading coefficients. Since MMSE estimates depend only on the total training power but not on the training duration, transmission of a single pilot symbol is optimal for average-power limited channels. The transmission structure in each block is shown in Fig. 2.2. As observed immediately, the first two symbols are dedicated to training while data transmission occurs in the remaining duration of $m-2$ symbols. Detailed description of the network training and data transmission phases is provided in the following section.

2.2 Network Training and Data Transmission

2.2.1 Network Training Phase

Each block transmission starts with the training phase. In the first symbol period, source transmits the pilot symbol $x_{s,t}$ to enable the relay and destination to estimate the channel coefficients h_{sr} and h_{sd}, respectively. The signals received by the relay and destination are

$$y_{r,t} = h_{sr}x_{s,t} + n_r, \quad \text{and} \quad y_{d,t} = h_{sd}x_{s,t} + n_d, \tag{2.3}$$

respectively. Similarly, in the second symbol period, relay transmits the pilot symbol $x_{r,t}$ to enable the destination to estimate the channel coefficient h_{rd}. The signal received by the destination is

$$y_{d,r,t} = h_{rd}x_{r,t} + n_{d,r}. \tag{2.4}$$

In the above formulations, $n_r \sim \mathcal{CN}(0, N_0)$, $n_d \sim \mathcal{CN}(0, N_0)$, and $n_{d,r} \sim \mathcal{CN}(0, N_0)$ represent independent Gaussian random variables. Note that n_d and $n_{d,r}$ are Gaussian noise samples at the destination in different time intervals, while n_r is the Gaussian noise at the relay.

In the training process, it is assumed that the receivers employ minimum mean-square-error (MMSE) estimation. We assume that the source allocates δ_s fraction of its total power mP_s for training while the relay allocates δ_r fraction of its total power mP_r for training. As described in [26], the MMSE estimate of h_{sr} is given by

$$\hat{h}_{sr} = \frac{\sigma_{sr}^2\sqrt{\delta_s m P_s}}{\sigma_{sr}^2\delta_s m P_s + N_0} y_{r,t}, \tag{2.5}$$

where $y_{r,t} \sim \mathcal{CN}(0, \sigma_{sr}^2\delta_s m P_s + N_0)$. We denote by $\tilde{h}_{sr}$ the estimate error which is a zero-mean complex Gaussian random variable with variance $var(\tilde{h}_{sr}) = \frac{\sigma_{sr}^2 N_0}{\sigma_{sr}^2\delta_s m P_s + N_0}$. Similarly, for the fading coefficients h_{sd} and h_{rd}, we have the following estimates

and estimate error variances:

$$\hat{h}_{sd} = \frac{\sigma_{sd}^2\sqrt{\delta_s m P_s}}{\sigma_{sd}^2\delta_s m P_s + N_0} y_{d,t}, \quad y_{d,t} \sim \mathcal{CN}(0, \sigma_{sd}^2\delta_s m P_s + N_0), \quad var(\tilde{h}_{sd}) = \frac{\sigma_{sd}^2 N_0}{\sigma_{sd}^2\delta_s m P_s + N_0}, \tag{2.6}$$

$$\hat{h}_{rd} = \frac{\sigma_{rd}^2\sqrt{\delta_r m P_r}}{\sigma_{rd}^2\delta_r m P_r + N_0} y_{d,r,t}, \quad y_{d,r,t} \sim \mathcal{CN}(0, \sigma_{rd}^2\delta_r m P_r + N_0), \quad var(\tilde{h}_{rd}) = \frac{\sigma_{rd}^2 N_0}{\sigma_{rd}^2\delta_r m P_r + N_0}. \tag{2.7}$$

With these estimates, the fading coefficients can now be expressed as

$$h_{sr} = \hat{h}_{sr} + \tilde{h}_{sr}, \quad h_{sd} = \hat{h}_{sd} + \tilde{h}_{sd}, \quad h_{rd} = \hat{h}_{rd} + \tilde{h}_{rd}. \tag{2.8}$$

2.2.2 Data Transmission Phase

As discussed in the previous section, within a block of m symbols, the first two symbols are allocated to network training. In the remaining duration of $m-2$ symbols, data transmission takes place. Throughout the chapter, we consider several transmission protocols which can be classified into two categories depending on whether or not the source and relay simultaneously transmit information: *non-overlapped* and *overlapped transmissions*. Since the practical relay node usually cannot transmit and receive data simultaneously, we assume that the relay works under half-duplex constraint. Hence, the relay first listens and then transmits. We introduce the relay transmission parameter α and assume that $\alpha(m-2)$ symbols are allocated for relay transmission. Hence, α can be seen as the fraction of total time or bandwidth allocated to the relay. Note that the parameter α enables us to control the degree of cooperation. In non-overlapped transmission protocol, source and relay transmit over non-overlapping intervals. Therefore, source

transmits over a duration of $(1-\alpha)(m-2)$ symbols and becomes silent as the relay transmits. On the other hand, in overlapped transmission protocol, source transmits all the time and sends $m-2$ symbols in each block.

We assume that the source transmits at a per-symbol power level of P_{s1} when the relay is silent, and P_{s2} when the relay is in transmission. Clearly, in non-overlapped mode, $P_{s2} = 0$. On the other hand, in overlapped transmission, we assume $P_{s1} = P_{s2}$. Noting that the total power available after the transmission of the pilot symbol is $(1-\delta_s)mP_s$, we can write

$$(1-\alpha)(m-2)P_{s1} + \alpha(m-2)P_{s2} = (1-\delta_s)mP_s. \tag{2.9}$$

The above assumptions imply that power for data transmission is equally distributed over the symbols during the transmission periods. Hence, in non-overlapped and overlapped modes, the symbol powers are $P_{s1} = \frac{(1-\delta_s)mP_s}{(1-\alpha)(m-2)}$ and $P_{s1} = P_{s2} = \frac{(1-\delta_s)mP_s}{(m-2)}$, respectively. Furthermore, we assume that the power of each symbol transmitted by the relay node is P_{r1}, which satisfies, similarly as above,

$$\alpha(m-2)P_{r1} = (1-\delta_r)mP_r. \tag{2.10}$$

Next, we provide detailed descriptions of non-overlapped and overlapped cooperative transmission schemes.

2.2.2.1 Non-overlapped transmission

We first consider the two simplest cooperative protocols: *non-overlapped AF* where the relay amplifies the received signal and forwards it to the destination, and *non-overlapped DF with repetition coding* where the relay decodes the message,

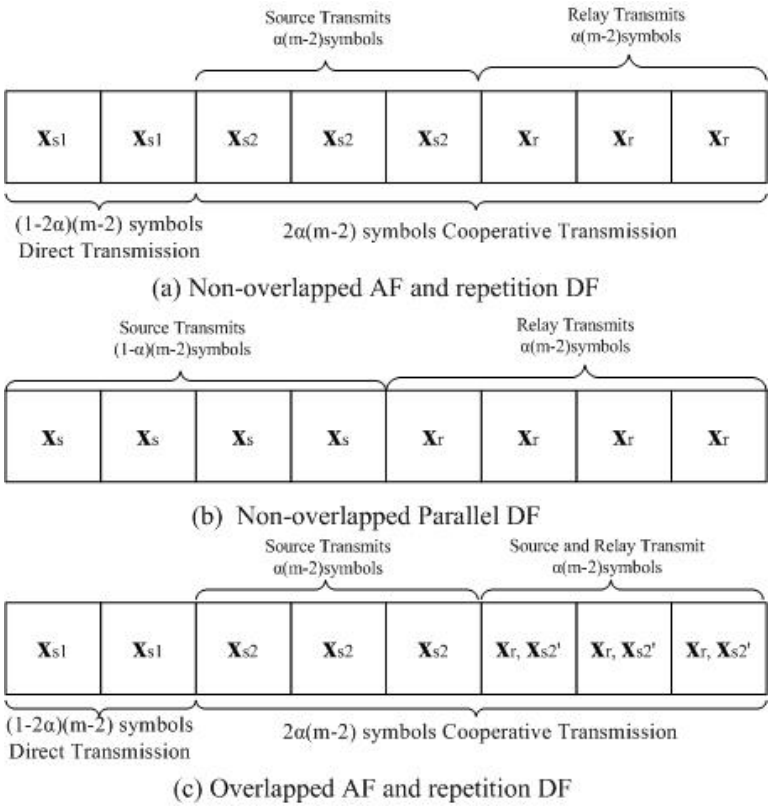

Figure 2.3: Transmission structure and order in the data transmission phase for different cooperation schemes.

re-encodes it using the same codebook as the source, and forwards it. In these protocols, since the relay either amplifies the received signal, or decodes it but uses the same codebook as the source when forwarding, source and relay should be allocated equal time slots in the cooperation phase. Therefore, before cooperation starts, we initially have direct transmission from the source to the destination without any aid from the relay over a duration of $(1-2\alpha)(m-2)$ symbols. In this phase, source sends the $(1-2\alpha)(m-2)$-dimensional data vector $\mathbf{x}_{s1}$ and the

received signal at the destination is given by

$$\mathbf{y}_{d1} = h_{sd}\mathbf{x}_{s1} + \mathbf{n}_{d1}. \tag{2.11}$$

Subsequently, cooperative transmission starts. At first, the source transmits the $\alpha(m-2)$-dimensional data vector $\mathbf{x}_{s2}$ which is received at the relay and the destination, respectively, as

$$\mathbf{y}_r = h_{sr}\mathbf{x}_{s2} + \mathbf{n}_r, \quad \text{and} \quad \mathbf{y}_{d2} = h_{sd}\mathbf{x}_{s2} + \mathbf{n}_{d2}. \tag{2.12}$$

In (2.11) and (2.12), $\mathbf{n}_{d1}$ and $\mathbf{n}_{d2}$ are independent Gaussian noise vectors composed of independent and identically distributed (i.i.d.), circularly symmetric, zero-mean complex Gaussian random variables with variance N_0, modeling the additive background noise at the transmitter in different transmission phases. Similarly, $\mathbf{n}_r$ is a Gaussian noise vector at the relay, whose components are i.i.d. zero-mean Gaussian random variables with variance N_0. For compact representation, we denote the overall source data vector by $\mathbf{x}_s = [\mathbf{x}_{s1}^T \ \mathbf{x}_{s2}^T]^T$, and the signal received at the destination directly from the source by $\mathbf{y}_d = [\mathbf{y}_{d1}^T \ \mathbf{y}_{d2}^T]^T$ where T denotes the transpose operation. After completing its transmission, the source becomes silent, and the relay transmits an $\alpha(m-2)$-dimensional symbol vector $\mathbf{x}_r$ which is generated from the previously received $\mathbf{y}_r$ [40] [39]. Now, the destination receives

$$\mathbf{y}_{d,r} = h_{rd}\mathbf{x}_r + \mathbf{n}_{d,r}. \tag{2.13}$$

After substituting the estimate expressions in (2.8) into (2.11)–(2.13), we have

$$\mathbf{y}_{d1} = \hat{h}_{sd}\mathbf{x}_{s1} + \tilde{h}_{sd}\mathbf{x}_{s1} + \mathbf{n}_{d1}, \quad \mathbf{y}_r = \hat{h}_{sr}\mathbf{x}_{s2} + \tilde{h}_{sr}\mathbf{x}_{s2} + \mathbf{n}_r, \quad \mathbf{y}_{d2} = \hat{h}_{sd}\mathbf{x}_{s2} + \tilde{h}_{sd}\mathbf{x}_{s2} + \mathbf{n}_{d2}, \tag{2.14}$$

$$\mathbf{y}_{d,r} = \hat{h}_{rd}\mathbf{x}_r + \tilde{h}_{rd}\mathbf{x}_r + \mathbf{n}_{d,r}. \tag{2.15}$$

Note that we have $0 < \alpha \leq 1/2$ for AF and repetition coding DF. Therefore, $\alpha = 1/2$ models full cooperation while we have noncooperative communications as $\alpha \to 0$. It should also be noted that α should in general be chosen such that $\alpha(m-2)$ is an integer. The transmission structure and order in the data transmission phase of non-overlapped AF and repetition DF are depicted Fig. 2.3.a, together with the notation used for the data symbols sent by the source and relay.

For non-overlapped transmission, we also consider *DF with parallel channel coding*, in which the relay uses a different codebook to encode the message. In this case, the source and relay do not have to be allocated the same duration in the cooperation phase. Therefore, source transmits over a duration of $(1-\alpha)(m-2)$ symbols while the relay transmits in the remaining duration of $\alpha(m-2)$ symbols. Clearly, the range of α is now $0 < \alpha < 1$. In this case, the input-output relations are given by (2.12) and (2.13). Since there is no separate direct transmission, $\mathbf{x}_{s2} = \mathbf{x}_s$ and $\mathbf{y}_{d2} = \mathbf{y}_d$ in (2.12). Moreover, the dimensions of the vectors $\mathbf{x}_s, \mathbf{y}_d, \mathbf{y}_r$ are now $(1-\alpha)(m-2)$, while $\mathbf{x}_r$ and $\mathbf{y}_{d,r}$ are vectors of dimension $\alpha(m-2)$. Fig. 2.3.b provides a graphical description of the transmission order for non-overlapped parallel DF scheme.

2.2.2.2 Overlapped transmission

In this category, we consider a more general and complicated scenario in which the source transmits all the time. We study AF and repetition DF, in which we, similarly as in the non-overlapped model, have unaided direct transmission from the source to the destination in the initial duration of $(1-2\alpha)(m-2)$ symbols. Cooperative transmission takes place in the remaining duration of $2\alpha(m-2)$ symbols. Again, we have $0 < \alpha \leq 1/2$ in this setting. In these protocols, the input-output relations are expressed as follows:

$$\mathbf{y}_{d1} = h_{sd}\mathbf{x}_{s1} + \mathbf{n}_{d1}, \quad \mathbf{y}_r = h_{sr}\mathbf{x}_{s2} + \mathbf{n}_r, \quad \mathbf{y}_{d2} = h_{sd}\mathbf{x}_{s2} + \mathbf{n}_{d2},$$
$$\text{and} \quad \mathbf{y}_{d,r} = h_{sd}\mathbf{x}'_{s2} + h_{rd}\mathbf{x}_r + \mathbf{n}_{d,r}. \tag{2.16}$$

Above, $\mathbf{x}_{s1}, \mathbf{x}_{s2}, \mathbf{x}'_{s2}$, which have respective dimensions of $(1-2\alpha)(m-2)$, $\alpha(m-2)$ and $\alpha(m-2)$, represent the source data vectors sent in direct transmission, cooperative transmission when relay is listening, and cooperative transmission when relay is transmitting, respectively. Note again that the source transmits all the time. $\mathbf{x}_r$ is the relay's data vector with dimension $\alpha(m-2)$. $\mathbf{y}_{d1}, \mathbf{y}_{d2}, \mathbf{y}_{d,r}$ are the corresponding received vectors at the destination, and $\mathbf{y}_r$ is the received vector at the relay. The input vector $\mathbf{x}_s$ now is defined as $\mathbf{x}_s = [\mathbf{x}_{s1}^T, \mathbf{x}_{s2}^T, \mathbf{x}_{s2}'^T]^T$ and we again denote $\mathbf{y}_d = [\mathbf{y}_{d1}^T \ \mathbf{y}_{d2}^T]^T$. If we express the fading coefficients as $h = \hat{h} + \tilde{h}$ in (2.16), we obtain the following input-output relations:

$$\mathbf{y}_{d1} = \hat{h}_{sd}\mathbf{x}_{s1} + \tilde{h}_{sd}\mathbf{x}_{s1} + \mathbf{n}_{d1}, \quad \mathbf{y}_r = \hat{h}_{sr}\mathbf{x}_{s2} + \tilde{h}_{sr}\mathbf{x}_{s2} + \mathbf{n}_r, \quad \mathbf{y}_{d2} = \hat{h}_{sd}\mathbf{x}_{s2} + \tilde{h}_{sd}\mathbf{x}_{s2} + \mathbf{n}_{d2}, \tag{2.17}$$

$$\text{and} \quad \mathbf{y}_{d,r} = \hat{h}_{sd}\mathbf{x}'_{s2} + \hat{h}_{rd}\mathbf{x}_r + \tilde{h}_{sd}\mathbf{x}'_{s2} + \tilde{h}_{rd}\mathbf{x}_r + \mathbf{n}_{d,r}. \tag{2.18}$$

A graphical depiction of the transmission order for overlapped AF and repetition DF is given in Fig. 2.3.c.

Finally, the list of notations used throughout the chapter is given in Table 2.1. and 2.2

Table 2.1: List of Notations

h_{sd}	source-destination channel fading coefficient
h_{sr}	relay-destination channel fading coefficient
h_{rd}	relay-destination channel fading coefficient
$\hat{h}_{.}$	estimate of the fading coefficient $h_{.}$
$\tilde{h}_{.}$	error in the estimate of the fading coefficient $h_{.}$
σ^2	variance of random variables
N_0	variance of Gaussian random variables due to thermal noise
m	number of symbols in each block
mP_s	total average power of the source in each block of m symbols
mP_r	total average power of the relay in each block of m symbols
δ_s	fraction of total power allocated to training by the source
δ_r	fraction of total power allocated to training by the relay
$x_{s,t}$	pilot symbol sent by the source
$x_{r,t}$	pilot symbol sent by the relay
n_d	additive Gaussian noise at the destination in the interval in which the source pilot symbol is sent
n_r	additive Gaussian noise at the relay in the interval in which the source pilot symbol is sent
$n_{d,r}$	Gaussian noise at the destination in the interval in which the relay pilot symbol is sent
$y_{d,t}$	received signal at the destination in the interval in which the source pilot symbol is sent
$y_{d,t}$	received signal at the relay in the interval in which the source pilot symbol is sent
$y_{d,r,t}$	received signal at the destination in the interval in which the relay pilot symbol is sent
P_{s1}	power of each source symbol sent in the interval in which the relay is not transmitting
P_{s2}	power of each source symbol sent in the interval in which the relay is transmitting
P_{r1}	power of each relay symbol
α	fraction of time/bandwidth allocated to the relay

Table 2.2: List of Notations continued

$\mathbf{x}_{s1}$	$(1-2\alpha)(m-2)$-dimensional data vector sent by the source in the noncooperative transmission mode
$\mathbf{x}_{s2}$	data vector sent by the source when the relay is listening. The dimension is $\alpha(m-2)$ for AF and repetition DF, and $(1-\alpha)(m-2)$ for parallel DF
$\mathbf{x}'_{s2}$	$\alpha(m-2)$-dimensional data vector sent by the source when the relay is transmitting
$\mathbf{x}_r$	$\alpha(m-2)$-dimensional data vector sent by the relay
$\mathbf{n}_{d1}$	$(1-2\alpha)(m-2)$-dimensional noise vector at the destination in the noncooperative transmission mode
$\mathbf{n}_{d2}$	noise vector at the destination in the interval when the relay is listening. The dimension is $\alpha(m-2)$ for AF and repetition DF, and $(1-\alpha)(m-2)$ for parallel DF
$\mathbf{n}_{d,r}$	$\alpha(m-2)$-dimensional noise vector at the destination in the interval when the relay is transmitting
$\mathbf{n}_r$	noise vector at the relay. The dimension is $\alpha(m-2)$ for AF and repetition DF, and $(1-\alpha)(m-2)$ for parallel DF
$\mathbf{y}_{d1}$	$(1-2\alpha)(m-2)$-dimensional received vector at the destination in the noncooperative transmission mode
$\mathbf{y}_{d2}$	received vector at the destination in the interval when the relay is listening. The dimension is $\alpha(m-2)$ for AF and repetition DF, and $(1-\alpha)(m-2)$ for parallel DF
$\mathbf{y}_{d,r}$	$\alpha(m-2)$-dimensional received vector at the destination in the interval when the relay is transmitting
$\mathbf{y}_r$	received vector at the relay. The dimension is $\alpha(m-2)$ for AF and repetition DF, and $(1-\alpha)(m-2)$ for parallel DF

2.3 Achievable Rates

In this section, we provide achievable rate expressions for AF and DF relaying in both non-overlapped and overlapped transmission scenarios in a unified fashion. Achievable rate expressions are obtained by considering the estimate errors as additional sources of Gaussian noise. Since Gaussian noise is the worst uncorrelated additive noise for a Gaussian model [28, Appendix] [67], achievable rates given in this section can be regarded as worst-case rates.

We first consider AF relaying scheme. The capacity of the AF relay channel is

the maximum mutual information between the transmitted signal $\mathbf{x}_s$ and received signals $\mathbf{y}_d$ and $\mathbf{y}_{d,r}$ given the estimates $\hat{h}_{sr}, \hat{h}_{sd}, \hat{h}_{rd}$:

$$C_{AF} = \sup_{p_{x_s}(\cdot)} \frac{1}{m} I(\mathbf{x}_s; \mathbf{y}_d, \mathbf{y}_{d,r} | \hat{h}_{sr}, \hat{h}_{sd}, \hat{h}_{rd}). \tag{2.19}$$

Note that this formulation presupposes that the destination has the knowledge of $\hat{h}_{sr}$. Hence, we assume that the value of $\hat{h}_{sr}$ is forwarded reliably from the relay to the

destination over low-rate control links. In general, solving the optimization problem in (2.19) and obtaining the AF capacity is a difficult task. Therefore, we concentrate on finding a lower bound on the capacity. A lower bound is obtained by replacing the product of the estimate error and the transmitted signal in the input-output relations with the worst-case noise with the same correlation. Therefore, we consider in the overlapped AF scheme

$$\mathbf{z}_{d1} = \tilde{h}_{sd}\mathbf{x}_{s1} + \mathbf{n}_{d1}, \quad \mathbf{z}_r = \tilde{h}_{sr}\mathbf{x}_{s2} + \mathbf{n}_r, \quad \mathbf{z}_{d2} = \tilde{h}_{sd}\mathbf{x}_{s2} + \mathbf{n}_{d2}, \quad \mathbf{z}_{d,r} = \tilde{h}_{sd}\mathbf{x}'_{s2} + \tilde{h}_{rd}\mathbf{x}_r + \mathbf{n}_{d,r}, \tag{2.20}$$

as noise vectors with covariance matrices

$$E\{\mathbf{z}_{d1}\mathbf{z}_{d1}^\dagger\} = \sigma^2_{z_{d1}}\mathbf{I} = \sigma^2_{\tilde{h}_{sd}} E\{\mathbf{x}_{s1}\mathbf{x}_{s1}^\dagger\} + N_0\mathbf{I}, \quad E\{\mathbf{z}_r\mathbf{z}_r^\dagger\} = \sigma^2_{z_r}\mathbf{I} = \sigma^2_{\tilde{h}_{sr}} E\{\mathbf{x}_{s2}\mathbf{x}_{s2}^\dagger\} + N_0\mathbf{I}, \tag{2.21}$$

$$\begin{aligned} E\{\mathbf{z}_{d2}\mathbf{z}_{d2}^\dagger\} &= \sigma^2_{z_{d2}}\mathbf{I} = \sigma^2_{\tilde{h}_{sd}} E\{\mathbf{x}_{s2}\mathbf{x}_{s2}^\dagger\} + N_0\mathbf{I}, \\ E\{\mathbf{z}_{d,r}\mathbf{z}_{d,r}{}^\dagger\} &= \sigma^2_{z_{d,r}}\mathbf{I} = \sigma^2_{\tilde{h}_{sd}} E\{\mathbf{x}'_{s2}\mathbf{x}'^\dagger_{s2}\} + \sigma^2_{\tilde{h}_{rd}} E\{\mathbf{x}_r\mathbf{x}_r^\dagger\} + N_0\mathbf{I}. \end{aligned} \tag{2.22}$$

Above, $\mathbf{x}^\dagger$ denotes the conjugate transpose of the vector $\mathbf{x}$. Note that the expressions for the non-overlapped AF scheme can be obtained as a special case of

(2.20)–(2.22) by setting $\mathbf{x}'_{s2} = 0$.

An achievable rate expression R_{AF} is obtained by solving the following optimization problem which requires finding the worst-case noise:

$$C_{AF} \geqslant R_{AF} = \inf_{p_{z_{d1}}(\cdot), p_{z_r}(\cdot), p_{z_{d2}}(\cdot), p_{z_{d,r}}(\cdot)} \sup_{p_{x_s}(\cdot)} \frac{1}{m} I(\mathbf{x}_s; \mathbf{y}_d, \mathbf{y}_{d,r} | \hat{h}_{sr}, \hat{h}_{sd}, \hat{h}_{rd}). \tag{2.23}$$

The following results provides a general formula for R_{AF}, which applies to both non-overlapped and overlapped transmission scenarios.

Theorem 1 *An achievable rate for AF transmission scheme is given by*

$$\begin{aligned} R_{AF} =& \frac{1}{m} E_{w_{sd}, w_{rd}, w_{sr}} \Bigg\{ (1-2\alpha)(m-2) \log\left(1 + \frac{P_{s1}|\hat{h}_{sd}|^2}{\sigma^2_{z_{d1}}}\right) + (m-2)\alpha \log\Bigg(1 + \frac{P_{s1}|\hat{h}_{sd}|^2}{\sigma^2_{z_{d2}}} \\ &+ f\left(\frac{P_{s1}|\hat{h}_{sr}|^2}{\sigma^2_{z_r}}, \frac{P_{r1}|\hat{h}_{rd}|^2}{\sigma^2_{z_{d,r}}}\right) + q\left(\frac{P_{s1}|\hat{h}_{sd}|^2}{\sigma^2_{z_{d2}}}, \frac{P_{s2}|\hat{h}_{sd}|^2}{\sigma^2_{z_{d,r}}}, \frac{P_{s1}|\hat{h}_{sr}|^2}{\sigma^2_{z_r}}, \frac{P_{r1}|\hat{h}_{rd}|^2}{\sigma^2_{z_{d,r}}}\right)\Bigg)\Bigg\} \end{aligned} \tag{2.24}$$

where $f(.)$ *and* $q(.)$ *are defined as* $f(x,y) = \frac{xy}{1+x+y}$ *and* $q(a,b,c,d) = \frac{(1+a)b(1+c)}{1+c+d}$. *Furthermore,*

$$\frac{P_{s1}|\hat{h}_{sd}|^2}{\sigma^2_{z_{d1}}} = \frac{P_{s1}|\hat{h}_{sd}|^2}{\sigma^2_{z_{d2}}} = \frac{P_{s1}\delta_s m P_s \sigma^4_{sd}}{P_{s1}\sigma^2_{sd}N_0 + (\sigma^2_{sd}\delta_s m P_s + N_0)N_0}|w_{sd}|^2 \tag{2.25}$$

$$\frac{P_{s1}|\hat{h}_{sr}|^2}{\sigma^2_{z_r}} = \frac{P_{s1}\delta_s m P_s \sigma^4_{sr}}{P_{s1}\sigma^2_{sr}N_0 + (\sigma^2_{sr}\delta_s m P_s + N_0)N_0}|w_{sr}|^2 \tag{2.26}$$

$$\frac{P_{r1}|\hat{h}^2_{rd}|}{\sigma^2_{z_{d,r}}} = \frac{P_{r1}\delta_r m P_r \sigma^4_{rd}(\sigma^2_{sd}\delta_s m P_s + N_0)|w_{rd}|^2}{\mathbb{A}} \tag{2.27}$$

$$\frac{P_{s2}|\hat{h}^2_{sd}|}{\sigma^2_{z_{d,r}}} = \frac{P_{s2}\delta_s m P_s \sigma^4_{sd}(\sigma^2_{rd}\delta_r m P_r + N_0)|w_{sd}|^2}{\mathbb{A}} \tag{2.28}$$

where $\mathbb{A} = P_{s2}\sigma^2_{sd}N_0(\sigma^2_{rd}\delta_r m P_r + N_0) + P_{r1}\sigma^2_{rd}N_0(\sigma^2_{sd}\delta_s m P_s + N_0) + N_0(\sigma^2_{sd}\delta_s m P_s +$

$N_0)(\sigma_{rd}^2\delta_r mP_r + N_0)$. *In the above equations and henceforth,* $w_{sr} \sim \mathcal{CN}(0,1)$, $w_{sd} \sim \mathcal{CN}(0,1)$, $w_{rd} \sim \mathcal{CN}(0,1)$ *denote independent, standard Gaussian random variables. The above formulation applies to both overlapped and non-overlapped cases. Recalling (2.9), if we assume in (2.24)–(2.28) that*

$$P_{s1} = \frac{(1-\delta_s)mP_s}{(m-2)(1-\alpha)} \quad \textit{and} \quad P_{s2} = 0, \tag{2.29}$$

we obtain the achievable rate expression for the non-overlapped AF scheme. Note that if $P_{s2} = 0$, *the function* $q(\cdot,\cdot,\cdot,\cdot) = 0$ *in (2.24). For overlapped AF, we have*

$$P_{s1} = P_{s2} = \frac{(1-\delta_s)mP_s}{m-2}. \tag{2.30}$$

Moreover, we know from (2.10) that

$$P_{r1} = \frac{(1-\delta_r)mP_r}{(m-2)\alpha}. \tag{2.31}$$

Proof: See Appendix A.

Next, we consider DF relaying scheme. In DF, there are two different coding approaches [39], namely repetition coding and parallel channel coding. We first consider repetition channel coding scheme. The following result provides achievable rate expressions for both non-overlapped and overlapped transmission scenarios.

Theorem 2 *An achievable rate expression for DF with repetition channel coding transmission scheme is given by*

$$R_{DFr} = \frac{(1-2\alpha)(m-2)}{m} E_{w_{sd}}\left\{\log\left(1 + \frac{P_{s1}|\hat{h}_{sd}|^2}{\sigma_{z_{d1}}^2}\right)\right\} + \frac{(m-2)\alpha}{m}\min\{I_1, I_2\} \tag{2.32}$$

where

$$I_1 = E_{w_{sr}}\left\{ \log\left(1 + \frac{P_{s1}|\hat{h}_{sr}|^2}{\sigma_{z_r}^2}\right)\right\}, \text{ and} \tag{2.33}$$

$$I_2 = E_{w_{sd},w_{rd}}\left\{ \log\left(1 + \frac{P_{s1}|\hat{h}_{sd}|^2}{\sigma_{z_{d2}}^2} + \frac{P_{r1}|\hat{h}_{rd}|^2}{\sigma_{z_{d,r}}^2} + \frac{P_{s2}|\hat{h}_{sd}|^2}{\sigma_{z_{d,r}}^2} + \frac{P_{s1}|\hat{h}_{sd}|^2}{\sigma_{z_{d2}}^2}\frac{P_{s2}|\hat{h}_{sd}|^2}{\sigma_{z_{d,r}}^2}\right)\right\}. \tag{2.34}$$

$\frac{P_{s1}|\hat{h}_{sd}|^2}{\sigma_{z_{d1}}^2}, \frac{P_{s1}|\hat{h}_{sd}|^2}{\sigma_{z_{d2}}^2}, \frac{P_{s1}|\hat{h}_{sr}|^2}{\sigma_{z_r}^2}, \frac{P_{s2}|\hat{h}_{sd}|^2}{\sigma_{z_{d,r}}^2}, \frac{P_{r1}|\hat{h}_{rd}|^2}{\sigma_{z_{d,r}}^2}$ *have the same expressions as in (2.25)–(2.28).* P_{s1}, P_{s2} *and* P_{r1} *are given in (2.29)–(2.31).*

Proof: See Appendix B.

Finally, we consider DF with parallel channel coding and assume that non-overlapped transmission scheme is adopted. From [43, Equation (6)], we note that an achievable rate expression is given by

$$\min\{(1-\alpha)I(\mathbf{x}_s;\mathbf{y}_r|\hat{h}_{sr}), (1-\alpha)I(\mathbf{x}_s;\mathbf{y}_d|\hat{h}_{sd}) + \alpha I(\mathbf{x}_r;\mathbf{y}_{d,r}|\hat{h}_{rd})\}.$$

Note that we do not have separate direct transmission in this relaying scheme. Using similar methods as in the proofs of Theorems 1 and 2, we obtain the following result. The proof is omitted to avoid repetition.

Theorem 3 *An achievable rate of non-overlapped DF with parallel channel coding scheme is given by*

$$R_{DFp} = \min\left\{ \frac{(1-\alpha)(m-2)}{m} E_{w_{sr}}\left\{\log\left(1 + \frac{P_{s1}|\hat{h}_{sr}|^2}{\sigma_{z_r}^2}\right)\right\}, \frac{(1-\alpha)(m-2)}{m} E_{w_{sd}}\left\{\log\left(1 + \frac{P_{s1}|\hat{h}_{sd}|^2}{\sigma_{z_{d2}}^2}\right)\right\} + \frac{\alpha(m-2)}{m} E_{w_{rd}}\left\{\log\left(1 + \frac{P_{r1}|\hat{h}_{rd}|^2}{\sigma_{z_{d,r}}^2}\right)\right\}\right\} \tag{2.35}$$

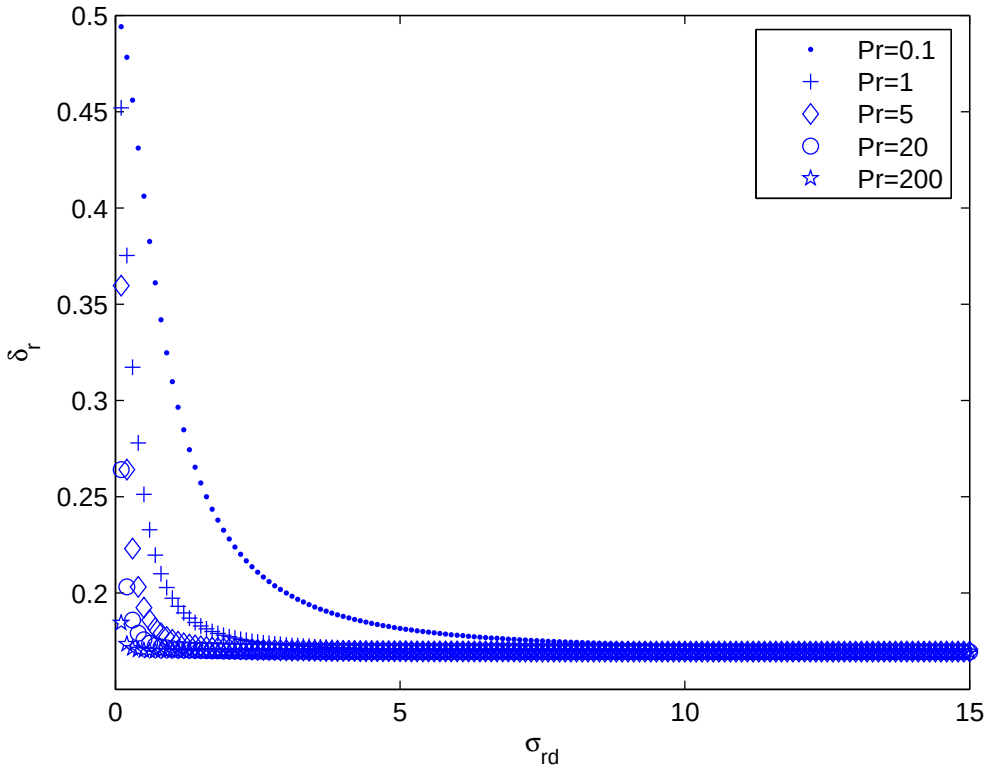

Figure 2.4: δ_r vs. σ_{rd} for different values of P_r when $m = 50$.

where $\frac{P_{s1}|\hat{h}_{sd}|^2}{\sigma^2_{z_{d2}}}$, $\frac{P_{s1}|\hat{h}_{sr}|^2}{\sigma^2_{z_r}}$, *and* $\frac{P_{r1}|\hat{h}_{rd}|^2}{\sigma^2_{z_{d,r}}}$ *are given in (2.25)-(2.27) with* P_{s1} *and* P_{r1} *defined in (2.29) and (2.31).* □

2.4 Resource Allocation Strategies

Having obtained achievable rate expressions in Section 2.3, we now identify resource allocation strategies that maximize these rates. We consider three resource allocation problems: 1) power allocation between training and data symbols; 2) time/bandwidth allocation to the relay; 3) power allocation between the source and relay under a total power constraint.

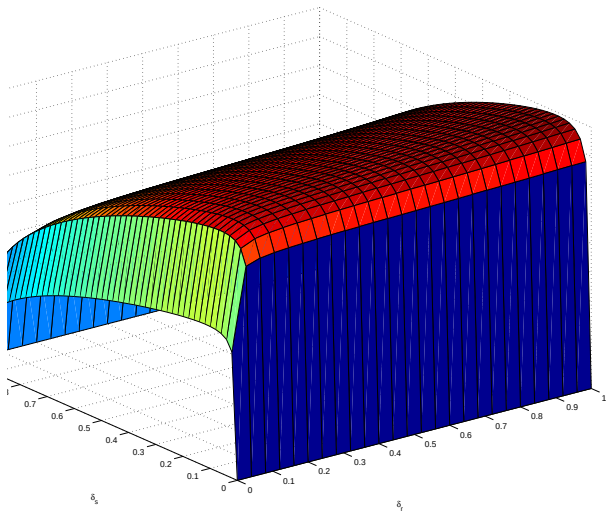

Figure 2.5: Overlapped AF achievable rates vs. δ_s and δ_r when $P_s = P_r = 50$

We first study how much power should be allocated for channel training. In non-overlapped AF, it can be seen that δ_r appears only in $\frac{P_{r1}|\hat{h}_{rd}|^2}{\sigma^2_{z_{d,r}}}$ in the achievable rate expression (2.24). Since $f(x,y) = \frac{xy}{1+x+y}$ is a monotonically increasing function of y for fixed x, (2.24) is maximized by maximizing $\frac{P_{r1}|\hat{h}_{rd}|^2}{\sigma^2_{z_{d,r}}}$. We can maximize $\frac{P_{r1}|\hat{h}_{rd}|^2}{\sigma^2_{z_{d,r}}}$ by maximizing the coefficient of the random variable $|w_{rd}|^2$ in (2.27), and the optimal δ_r is given below:

$$\delta_r^{opt} = \frac{-mP_r\sigma^2_{rd} - \alpha mN_0 + 2\alpha N_0 + \sqrt{\mathbb{B}}}{mP_r\sigma^2_{rd}(-1+\alpha m - 2\alpha)}. \tag{2.36}$$

Where $\mathbb{B} = \alpha(m-2)(m^2P_r\sigma^2_{rd}\alpha N_0 + m^2P_r^2\sigma^4_{rd} + \alpha mN_0^2 + mP_r\sigma^2_{rd}N_0 - 2mP_r\sigma^2_{rd}\alpha N_0 - 2N_0\alpha)$. Optimizing δ_s in non-overlapped AF is more complicated as it is related to all the terms in (2.24), and hence obtaining an analytical solution is unlikely. A suboptimal solution is to maximize $\frac{P_{s1}|\hat{h}_{sd}|^2}{\sigma^2_{z_{d1}}}$ and $\frac{P_{s1}|\hat{h}_{sr}|^2}{\sigma^2_{z_r}}$ separately, and obtain two solutions $\delta_{s,1}^{subopt}$ and $\delta_{s,2}^{subopt}$, respectively. Note that expressions for $\delta_{s,1}^{subopt}$ and

$\delta_{s,2}^{subopt}$ are exactly the same as that in (2.36) with P_r and α replaced by P_s and $(1-\alpha)$, and σ_{rd} replaced by σ_{sd} in $\delta_{s,1}^{subopt}$ and replaced by σ_{sr} in $\delta_{s,2}^{subopt}$. When the source-relay channel is better than the source-destination channel and the fraction of time over which direct transmission is performed is small, $\frac{P_{s1}|\hat{h}_{sr}|^2}{\sigma_{z_r}^2}$ is a more dominant factor and $\delta_{s,2}^{subopt}$ is a good choice for training power allocation. Otherwise, $\delta_{s,1}^{subopt}$ might be preferred. Note that in non-overlapped DF with repetition and parallel coding, $\frac{P_{r1}|\hat{h}_{rd}|^2}{\sigma_{z_{d,r}}^2}$ is the only term that includes δ_r. Therefore, similar results and discussions apply. For instance, the optimal δ_r has the same expression as that in (2.36). Figure 2.4 plots the optimal δ_r as a function of σ_{rd} for different relay power constraints P_r when $m = 50$ and $\alpha = 0.5$. It is observed in all cases that the allocated training power monotonically decreases with improving channel quality and converges to $\frac{\sqrt{\alpha(m-2)}-1}{\alpha m-2\alpha-1} \approx 0.169$ which is independent of P_r.

In overlapped transmission schemes, both δ_s and δ_r appear in more than one term in the achievable rate expressions. Therefore, we resort to numerical results to identify the optimal values. Figures 2.5 and 2.6 plot the achievable rates as a function of δ_s and δ_r for overlapped AF. In both figures, we have assumed that $\sigma_{sd} = 1, \sigma_{sr} = 2, \sigma_{rd} = 1$ and $m = 50, N_0 = 1, \alpha = 0.5$. While Fig. 2.5 considers high SNRs ($P_s = 50$ and $P_r = 50$), we assume that $P_s = 0.5$ and $P_r = 0.5$ in Fig. 2.6. In Fig. 2.5, we observe that increasing δ_s will increase achievable rate until $\delta_s \approx 0.1$. Further increase in δ_s decreases the achievable rates. On the other hand, rates always increase with increasing δ_r, leaving less and less power for data transmission by the relay. This indicates that cooperation is not beneficial in terms of achievable rates and direct transmission should be preferred. On the other hand, in the low-power regime considered in Fig. 2.6, the optimal values of δ_s and δ_r are approximately 0.18 and 0.32, respectively. Hence, the relay in this case helps to improve the rates.

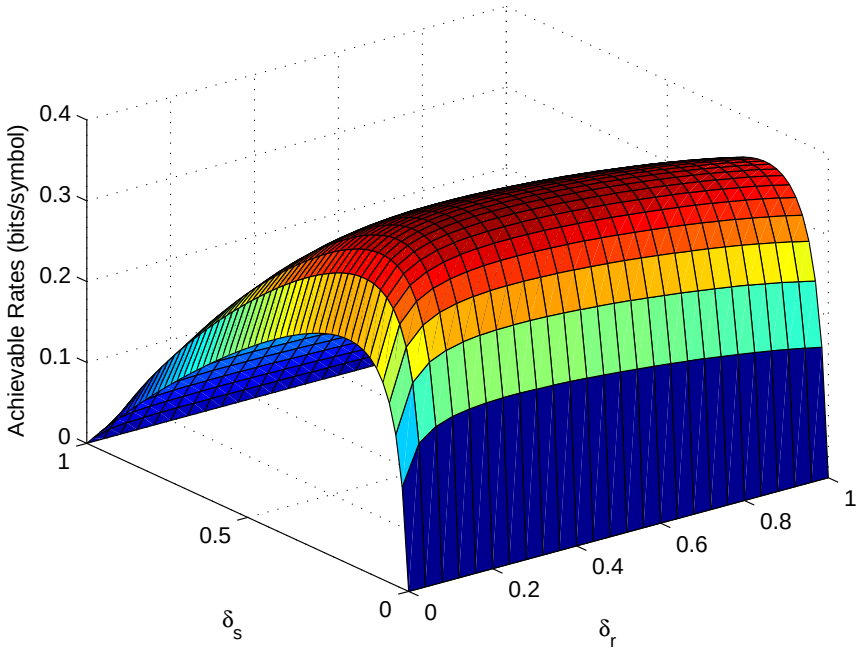

Figure 2.6: Overlapped AF achievable rates vs. δ_s and δ_r when $P_s = P_r = 0.5$

Next, we analyze the effect of the degree of cooperation on the performance in AF and repetition DF. Figures 2.7 and 2.8 plot the achievable rates as a function of α which gives the fraction of total time/bandwidth allocated to the relay. Achievable rates are obtained for different channel qualities given by the standard deviations σ_{sd}, σ_{sr}, and σ_{rd} of the fading coefficients. We observe that if the input power is high, α should be either 0.5 or close to zero depending on the channel qualities. On the other hand, $\alpha = 0.5$ always gives us the best performance at low SNR levels regardless of the channel qualities. Hence, while cooperation is beneficial in the low-SNR regime, noncooperative transmissions might be optimal at high SNRs. We note from Fig. 2.7 in which $P_s = P_r = 50$ that cooperation starts

being useful as the source-relay channel variance σ_{sr}^2 increases. Similar results are also observed if overlapped DF with repetition coding is considered. Hence, the source-relay channel quality is one of the key factors in determining the usefulness of cooperation in the high SNR regime. At the same time, additional numerical analysis has indicated that if SNR is further increased, noncooperative direct transmission tends to outperform cooperative schemes even in the case in which $\sigma_{sr} = 10$. Hence, there is a certain relation between the SNR level and the required source-relay channel quality for cooperation to be beneficial. The above conclusions apply to overlapped AF and DF with repetition coding. In contrast, numerical analysis of non-overlapped DF with parallel coding in the high-SNR regime has shown that cooperative transmission with this technique provides improvements over noncooperative direct transmission. A similar result will be discussed later in this section when the performance is analyzed under total power constraints.

In Fig. 2.8 in which SNR is low ($P_s = P_r = 0.5$), we see that the highest achievable rates are attained when there is full cooperation (i.e., when $\alpha = 0.5$). Note that in this figure, overlapped DF with repetition coding is considered. If overlapped AF is employed as the cooperation strategy, we have similar conclusions but it should also be noted that overlapped AF achieves smaller rates than those attained by overlapped DF with repetition coding.

In Fig. 2.9, we plot the achievable rates of DF with parallel channel coding, derived in Theorem 3, when $P_s = P_r = 0.5$. We can see from the figure that the highest rate is obtained when both the source-relay and relay-destination channel qualities are higher than that of the source-destination channel (i.e., when $\sigma_{sd} = 1, \sigma_{sr} = 4, \sigma_{rd} = 4$). Additionally, we observe that as the source-relay channel improves, more resources need to be allocated to the relay to achieve

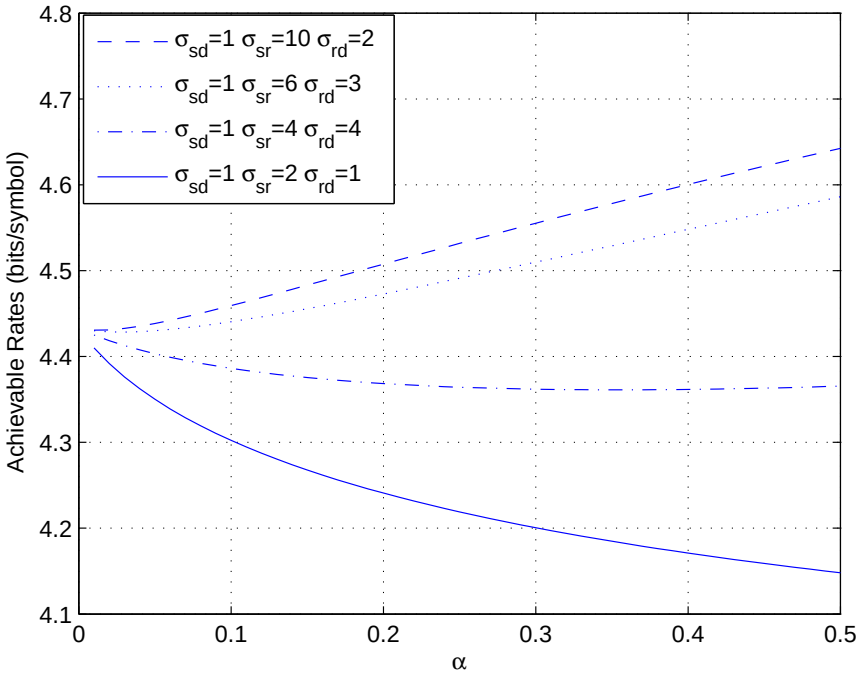

Figure 2.7: Overlapped AF achievable rate vs. α when $P_s = P_r = 50, \delta_s = \delta_r = 0.1$, $m = 50$.

the maximum rate. We note that significant improvements with respect to direct transmission (i.e., the case when $\alpha \to 0$) are obtained. Finally, we can see that when compared to AF and DF with repetition coding, DF with parallel channel coding achieves higher rates. On the other hand, AF and repetition coding DF have advantages in the implementation. Obviously, the relay, which amplifies and forwards, has a simpler task than that which decodes and forwards. Moreover, as pointed out in [38], if AF or repetition coding DF is employed in the system, the architecture of the destination node is simplified because the data arriving from the source and relay can be combined rather than stored separately.

In certain cases, source and relay are subject to a total power constraint. Here,

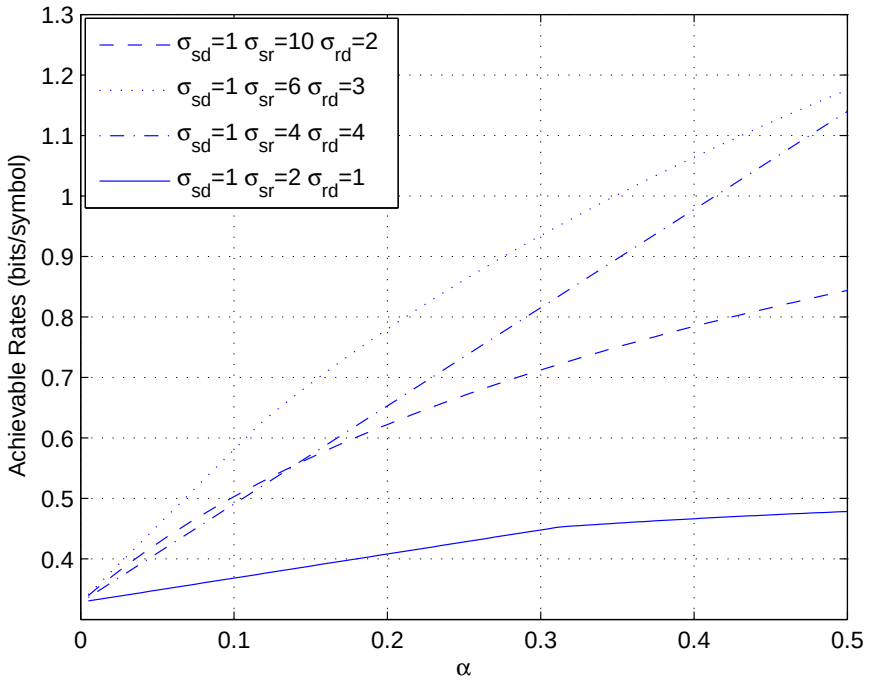

Figure 2.8: Overlapped DF with repetition coding achievable rate vs. α when $P_s = P_r = 0.5, \delta_s = \delta_r = 0.1$, $m = 50$.

we introduce the power allocation coefficient θ, and total power constraint P. P_s and P_r have the following relations: $P_s = \theta P$, $P_r = (1-\theta)P$, and hence $P_s + P_r = P$. Next, we investigate how different values of θ, and hence different power allocation strategies, affect the achievable rates. Analytical results for θ that maximizes the achievable rates are difficult to obtain. Therefore, we again resort to numerical analysis. In all numerical results, we assume that $\alpha = 0.5$ which provides the maximum of degree of cooperation. First, we consider the AF. The fixed parameters we choose are $P = 100, N_0 = 1, \delta_s = 0.1, \delta_r = 0.1$. Fig. 2.10 plots the achievable rates in the overlapped AF transmission scenario as a function of θ for different channel conditions, i.e., different values of σ_{sr}, σ_{rd}, and σ_{sd}. We observe that the best performance is achieved as $\theta \to 1$. Hence, even in the overlapped scenario,

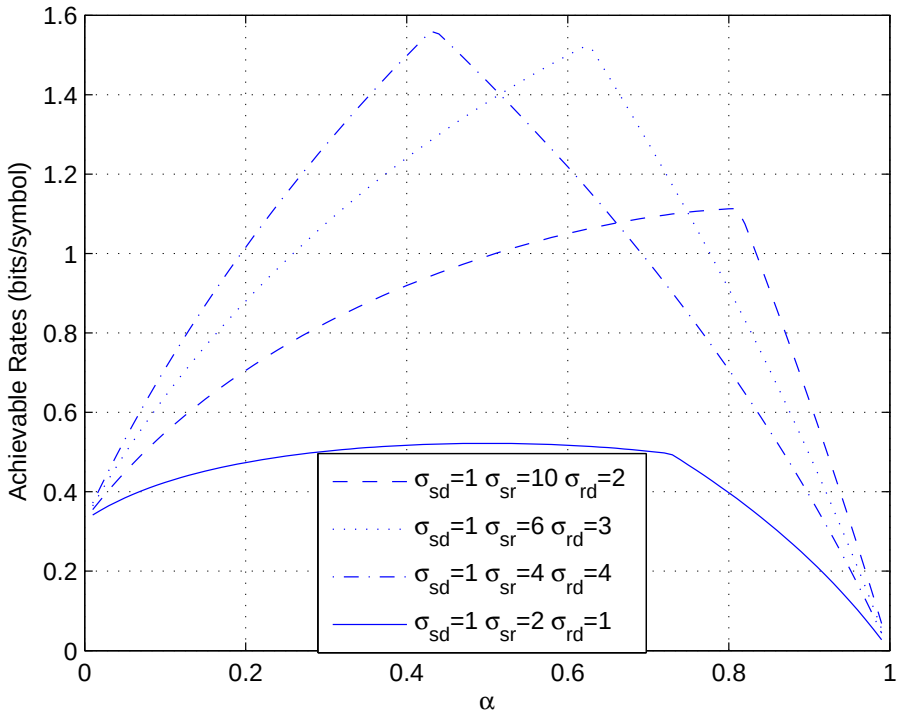

Figure 2.9: Non-overlapped DF parallel coding achievable rate vs. α when $P_s = P_r = 0.5, \delta_s = \delta_r = 0.1$, $m = 50$.

all the power should be allocated to the source and direct transmission should be preferred at these high SNR levels. Note that if direct transmission is performed, there is no need to learn the relay-destination channel. Since the time allocated to the training for this channel should be allocated to data transmission, the real rate of direct transmission is slightly higher than the point that the cooperative rates converge as $\theta \to 1$. For this reason, we also provide the direct transmission rate separately in Fig. 2.10. Further numerical analysis has indicated that direct transmission outperforms non-overlapped AF, overlapped and non-overlapped DF with repetition coding as well at this level of input power. On the other hand, in Fig. 2.11 which plots the achievable rates of non-overlapped DF with parallel

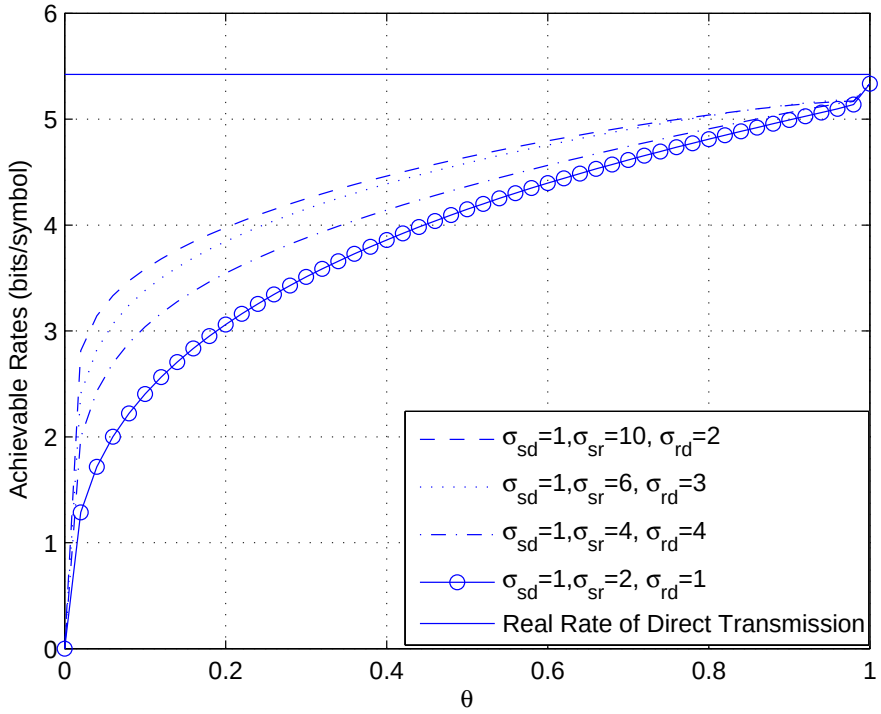

Figure 2.10: Overlapped AF achievable rate vs. θ. $P = 100$, $m = 50$.

coding as a function of θ, we observe that direct transmission rate, which is the same as that given in Fig. 2.10, is exceeded if $\sigma_{sr} = 10$ and hence the source-relay channel is very strong. The best performance is achieved when $\theta \approx 0.7$ and therefore 70% of the power is allocated to the source.

Figs. 2.12 and 2.13 plot the non-overlapped achievable rates when $P = 1$. In all cases, we observe that performance levels higher than that of direct transmission are achieved unless the qualities of the source-relay and relay-destination channels are comparable to that of the source-destination channel (e.g., $\sigma_{sd} = 1, \sigma_{sr} = 2, \sigma_{rd} = 1$). Moreover, we note that the best performances are attained when the source-relay and relay-destination channels are both considerably better than the source-destination channel (i.e., when $\sigma_{sd} = 1, \sigma_{sr} = 4, \sigma_{rd} = 4$). As expected, high-

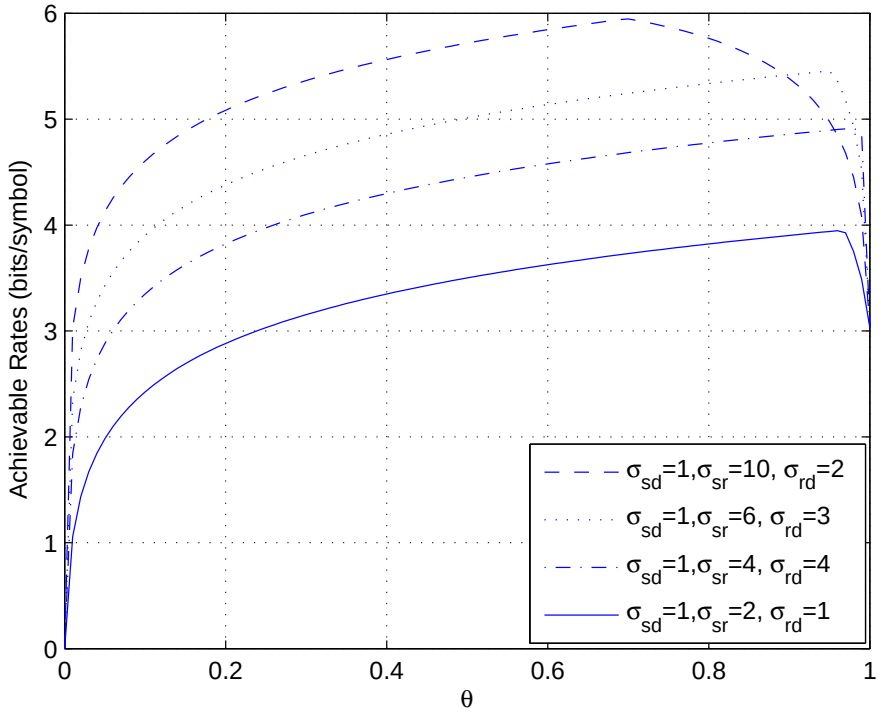

Figure 2.11: Non-overlapped Parallel coding DF rate vs. θ. $P = 100$, $m = 50$.

est gains are obtained with parallel coding DF although further numerical analysis has shown that repetition coding incur only small losses. Finally, Fig. 2.14 plot the achievable rates of overlapped AF when $P = 1$. Similar conclusions apply also here. However, it is interesting to note that overlapped AF rates are smaller than those achieved by non-overlapped AF. This behavior is also observed when DF with repetition coding is considered. Note that in non-overlapped transmission, source transmits in a shorter duration of time with higher power. This signaling scheme provides better performance as expected because it is well-known that flash signaling achieves the capacity in the low-SNR regime in imperfectly known channels [69].

Table 2.3 below summarizes the conclusions drawn and insights gained in

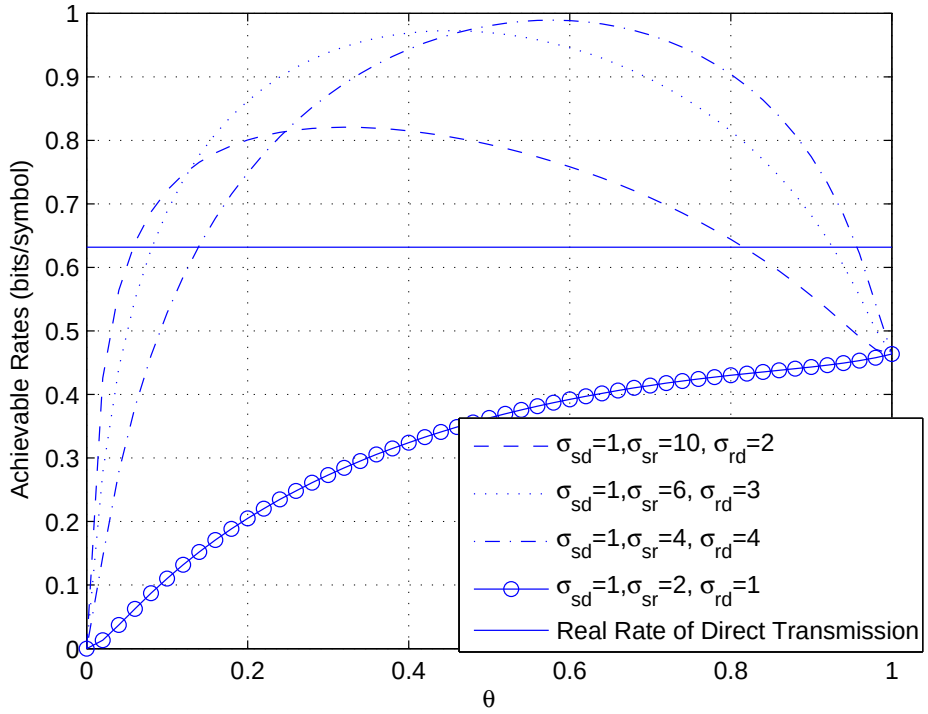

Figure 2.12: Non-overlapped AF achievable rate vs. θ. $P = 1$, $m = 50$.

this section on the performance of different cooperation strategies and resource allocation schemes in the high- and low-SNR regimes.

2.5 Energy Efficiency

Our analysis has shown that cooperative relaying is generally beneficial in the low-power regime, resulting in higher achievable rates when compared to direct transmission. In this section, we provide an energy efficiency perspective and remark that care should be exercised when operating at very low SNR values. The least amount of energy required to send one information bit reliably is given

Table 2.3:

High-SNR Regime	• Cooperation employing *overlapped AF* or *DF with repetition coding* is beneficial only if the source-relay channel quality is high enough. If this is not the case or SNR is very high, noncooperative direct transmission should be employed. • Cooperation using *non-overlapped DF with parallel coding* provides improvements over the performance of noncooperative direct transmission, and achieves higher rates than those attained by *overlapped AF* and *DF with repetition coding*. • If the system is operating under total power constraints, all the power should be allocated to the source and hence direct transmission should be preferred over *overlapped* and *non-overlapped AF*, and *overlapped and non-overlapped DF with repetition coding*. • Under total power constraints, only *non-overlapped DF with parallel coding* outperforms noncooperative direct transmission when the source-relay channel is strong.
Low-SNR Regime	• Cooperation is generally beneficial. • The strengths of both the source-relay and relay-destination channels are important factors. • *Non-overlapped DF with parallel coding* achieves the highest performance levels. In general, non-overlapped transmission methods should be preferred. Also, *DF* provides higher gains over *AF*. • Under total power constraints, highest gains over noncooperative direct transmission are attained when both the source-relay and relay-destination channels are considerably stronger than the source-destination channel. • Under total power constraints, noncooperative direct transmission should be preferred if the qualities of both the source-relay and relay-destination channels are comparable to that of the source-destination channel.

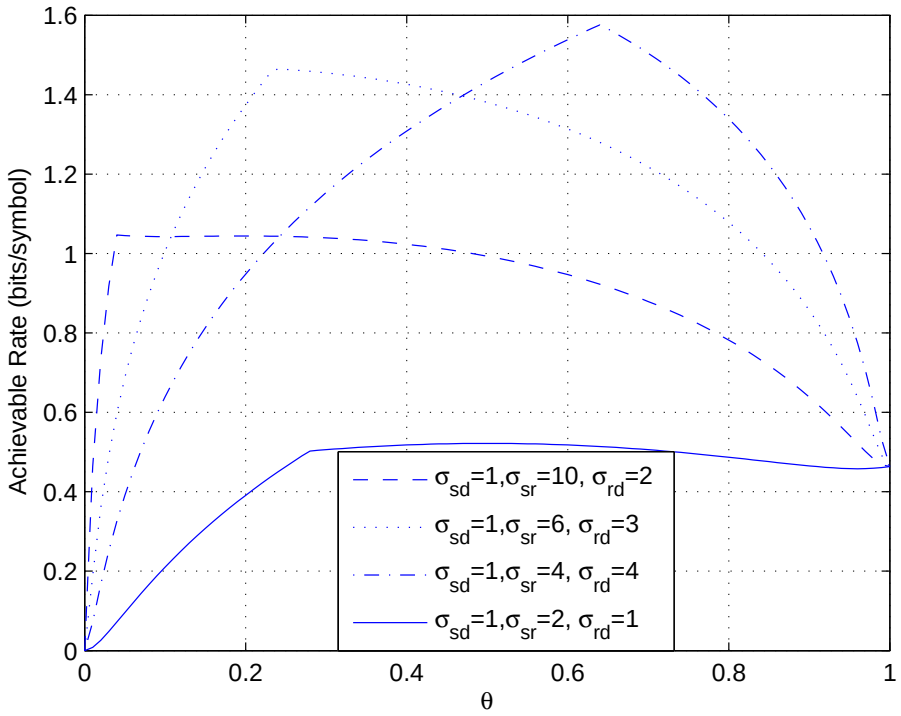

Figure 2.13: Non-overlapped Parallel coding DF rate vs. θ. $P = 1$, $m = 50$.

by[2] $\frac{E_b}{N_0} = \frac{\text{SNR}}{C(\text{SNR})}$ where $C(\text{SNR})$ is the channel capacity in bits/symbol. In our setting, the capacity will be replaced by the achievable rate expressions and hence the resulting bit energy, denoted by $\frac{E_{b,U}}{N_0}$, provides the least amount of normalized bit energy values in the worst-case scenario and also serves as an upper bound on the achievable bit energy levels in the channel.

We note that in finding the bit energy values, we assume that $\text{SNR} = P/N_0$ where $P = P_r + P_s$ is the total power. The next result provides the asymptotic behavior of the bit energy as SNR decreases to zero.

Theorem 4 *The normalized bit energy in all relaying schemes grows without bound as*

[2]Note that $\frac{E_b}{N_0}$ is the bit energy normalized by the noise power spectral level N_0.

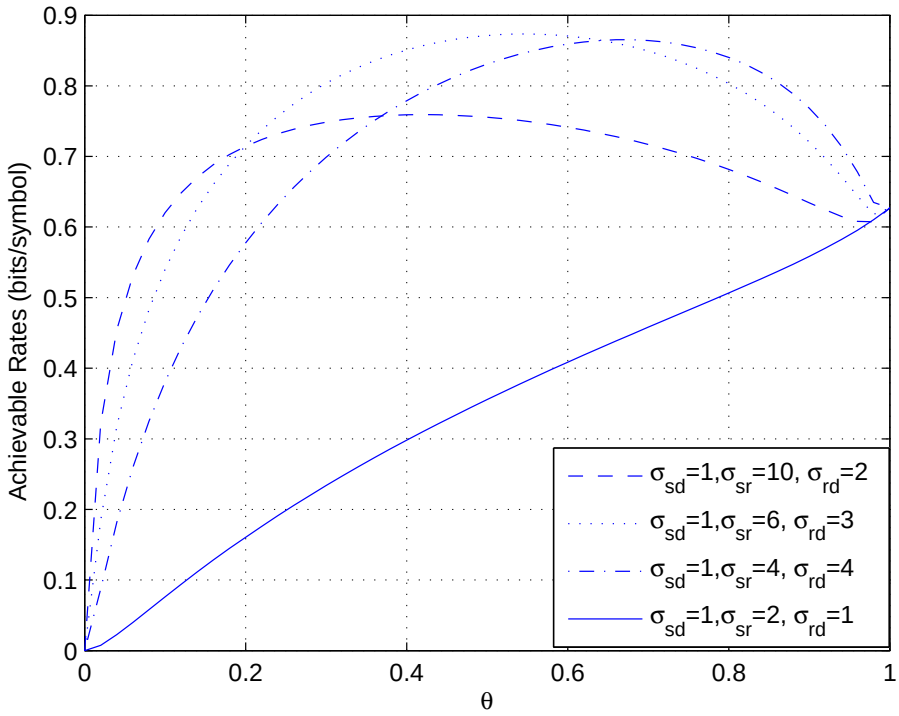

Figure 2.14: Overlapped AF achievable rate vs. θ. $P = 1$, $m = 50$.

the signal-to-noise ratio decreases to zero, i.e.,

$$\left.\frac{E_{b,U}}{N_0}\right|_{R=0} = \lim_{SNR\to 0} \frac{SNR}{R(SNR)} = \frac{1}{\dot{R}(0)} = \infty. \tag{2.37}$$

Proof: $\dot{R}(0)$ is the derivative of R with respect to SNR as SNR $\to$ 0. The key point to prove this theorem is to show that when SNR $\to$ 0, the mutual information decreases as SNR^2, and hence $\dot{R}(0) = 0$. This can be easily shown because when $P \to 0$, in all the terms ,$\frac{P_{s1}|\hat{h}_{sd}|^2}{\sigma^2_{z_{d1}}}$,$\frac{P_{s1}|\hat{h}_{sd}|^2}{\sigma^2_{z_{d2}}}$, $\frac{P_{s1}|\hat{h}_{sr}|^2}{\sigma^2_{z_r}}$,$\frac{P_{s2}|\hat{h}_{sd}|^2}{\sigma^2_{z_{d,r}}}$ and $\frac{P_{r1}|\hat{h}_{rd}|^2}{\sigma^2_{z_{d,r}}}$ in Theorems 1-3, the denominator goes to a constant while the numerator decreases as P^2. Hence, these terms diminish as SNR^2. Since $\log(1+x) = x + o(x)$ for small x, where $o(x)$ satisfies $\lim_{x\to 0} \frac{o(x)}{x} = 0$, we conclude that the achievable rate expressions

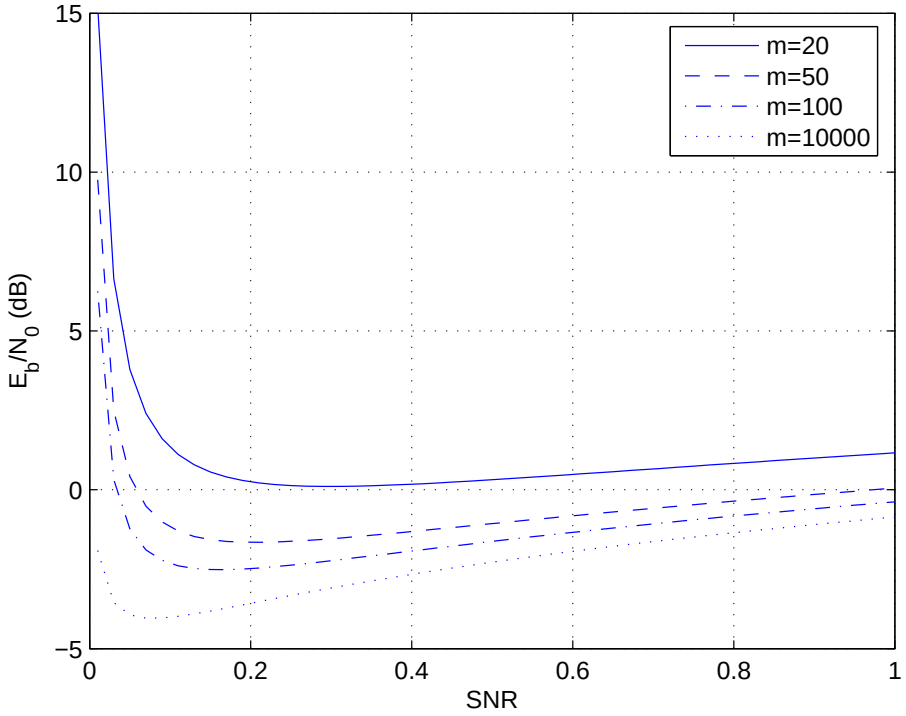

Figure 2.15: Non-overlapped AF $E_{b,U}/N_0$ vs. SNR

also decrease as SNR^2 as SNR vanishes. □

Theorem 4 indicates that it is extremely energy-inefficient to operate at very low SNR values. We identify the most energy-efficient operating points in numerical results. We choose the following numerical values for the fixed parameters: $\delta_s = \delta_r = 0.1$, $\sigma_{sd} = 1$, $\sigma_{sr} = 4$, $\sigma_{rd} = 4$, $\alpha = 0.5$, and $\theta = 0.6$. Fig. 2.15 plots the bit energy curves as a function of SNR for different values of m in the non-overlapped AF case. We can see from the figure that the minimum bit energy, which is achieved at a nonzero value of SNR, decreases with increasing m and is achieved at a lower SNR value. Fig. 2.16 shows the minimum bit energy for different relaying schemes with overlapped or non-overlapped transmission techniques. We observe that the minimum bit energy decreases with increasing m in

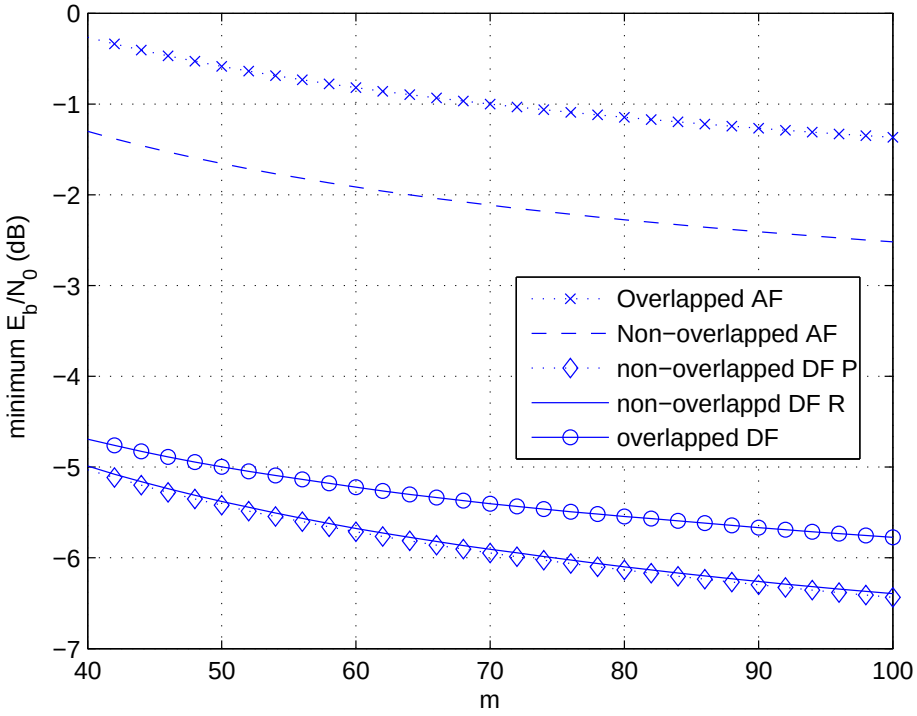

Figure 2.16: $E_{b,U}/N_0$ vs. m for different transmission scheme

all cases . We realize that DF is in general much more energy-efficient than AF. Moreover, we note that employing non-overlapped rather than overlapped transmission improves the energy efficiency. We further remark that the performances of non-overlapped DF with repetition coding and parallel coding are very close.

2.6 Conclusion

In this chapter, we have studied the imperfectly-known fading relay channels. We have assumed that the source-destination, source-relay, and relay-destination channels are not known by the corresponding receivers a priori, and transmission starts with the training phase in which the channel fading coefficients are

learned with the assistance of pilot symbols, albeit imperfectly. Hence, in this setting, relaying increases the channel uncertainty in the system, and there is increased estimation cost associated with cooperation. We have investigated the performance of relaying by obtaining achievable rates for AF and DF relaying schemes. We have considered both non-overlapped and overlapped transmission scenarios. We have controlled the degree of cooperation by varying the parameter α. We have identified resource allocation strategies that maximize the achievable rate expressions. We have observed that if the source-relay channel quality is low, then cooperation is not beneficial and direct transmission should be preferred at high SNRs when amplify-and-forward or decode-and-forward with repetition coding is employed as the cooperation strategy. On the other hand, we have seen that relaying generally improves the performance at low SNRs. We have noted that DF with parallel coding provides the highest rates. Additionally, under total power constraints, we have studied power allocation between the source and relay. We have again pointed out that relaying degrades the performance at high SNRs unless DF with parallel channel coding is used and the source-relay channel quality is high. The benefits of relaying is again demonstrated at low SNRs. We have noted that non-overlapped transmission is superior compared to overlapped one in this regime. Finally, we have considered the energy efficiency in the low-power regime, and proved that the bit energy increases without bound as SNR diminishes. Hence, operation at very low SNR levels should be avoided. From the energy efficiency perspective, we have again observed that non-overlapped transmission provides better performance. We have also noted that DF is more energy efficient than AF.

Chapter 3

An Achievable Rate Region for Imperfectly-Known Two-Way Relay Fading Channels

In this chapter, we investigate the training-based achievable rate region of the decode-and-forward (DF) two-way relaying scheme. We note that the DF strategy has certain advantages over AF. In AF, due to the need to estimate the cascade of the channels in non-Gaussian noise, performing minimum mean-square-error (MMSE) estimation is often not feasible and suboptimal linear MMSE estimates are employed. In addition, noise forwarding in AF is a factor that can lead to losses in performance unless the signal-to-noise ratio is high enough. Moreover, degrees of freedom in transmission might be limited in AF schemes since the MAC and BC phases of the transmission are necessarily of equal duration. At the same time, it should be noted that DF requires a more complicated operation at the relay, and training in DF mode takes a duration of three symbols instead of two as required in AF.

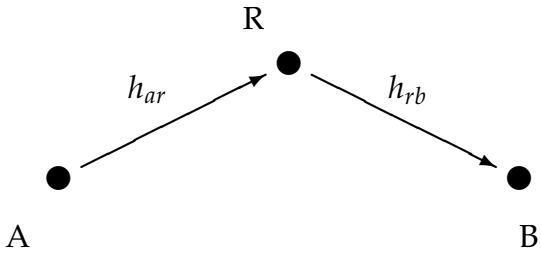

Figure 3.1: three-node two-way relay network which consists of user nodes A and B

3.1 Channel Model

We consider a three-node two-way relay network which consists of user nodes A and B, and a relay node R. Channels between A and R , R and B are modeled as Rayleigh block-fading channels with fading coefficients denoted by h_{ar} and h_{rb}, respectively. We further assume that there is no direct link between user A and user B. Due to the block-fading assumption, the fading coefficients[1] $h_{ar} \sim \mathcal{CN}(0, \sigma_{ar}^2)$, and $h_{br} \sim \mathcal{CN}(0, \sigma_{br}^2)$ stay constant for a block of m symbols before they assume independent realizations for the following block. In this system, user nodes A and B send data to each other with the assistance of the intermediate relay node. It is assumed that none of the nodes has prior knowledge of the instantaneous realizations of the fading coefficients, and the transmission is conducted in two phases: network training phase in which pilot symbols are transmitted and the fading coefficients are estimated at the receivers, and data transmission phase. Over these phases, the source and relay nodes are subject to the following average power

[1] $x \sim \mathcal{CN}(d, \sigma^2)$ is used to denote a proper complex Gaussian random variable with mean d and variance σ^2.

constraints:

$$\|\mathbf{x}_{a,t}\|^2 + E\{\|\mathbf{x}_a\|^2\} \leq mP_a, \tag{3.1}$$

$$\|\mathbf{x}_{b,t}\|^2 + E\{\|\mathbf{x}_b\|^2\} \leq mP_b, \tag{3.2}$$

$$\|\mathbf{x}_{r,t}\|^2 + E\{\|\mathbf{x}_r\|^2\} \leq mP_r, \tag{3.3}$$

where $\mathbf{x}_{a,t}$, $\mathbf{x}_{b,t}$ and $\mathbf{x}_{r,t}$ are the training signal vectors of users A and B, and the relay R, respectively, and $\mathbf{x}_a$, $\mathbf{x}_b$ and $\mathbf{x}_r$ are the corresponding data transmission vectors.

3.2 Training and Data Transmission Phases and Achievable Rate Regions

3.2.1 Network Training Phase

Each block transmission starts with the training phase. In the first symbol period, user A transmits a pilot symbol to enable the relay to estimate channel coefficient h_{ar}. In the average power limited case, sending a single pilot is optimal because instead of increasing the number of pilot symbols, a single pilot with higher power can be used. The signal received by the relay is

$$y_{ar,t,} = h_{ar}x_{a,t} + n_r. \tag{3.4}$$

Similarly, in the second symbol period, user B transmits a pilot symbol to enable the relay to estimate channel coefficient h_{br}. The signal received by the relay is

$$y_{br,t,} = h_{br}x_{b,t} + n_r. \tag{3.5}$$

In the third symbol period, relay transmits a pilot symbol to enable user A to estimate the fading coefficient h_{ra} and user B to estimate h_{rb}. The signals received at A and B, respectively, are

$$y_{a,t} = h_{ra}x_{r,t} + n_a, \text{ and} \tag{3.6}$$

$$y_{b,t} = h_{rb}x_{r,t} + n_b. \tag{3.7}$$

In the above formulations, $n_r \sim \mathcal{CN}(0, N_0)$, $n_a \sim \mathcal{CN}(0, N_0)$ and $n_b \sim \mathcal{CN}(0, N_0)$ represent independent Gaussian noise samples at the relay and the user nodes. Notice also in (3.6) and (3.7) that we have denoted the fading coefficients experienced when the relay transmits to the users as h_{ra} and h_{rb} rather than h_{ar} and h_{br}, which are the fading coefficients when the users transmit to the relay. It is important to note that although we implicitly assume channel reciprocity and consider that statistically the same fading is experienced in the uplink (user-to-relay) and downlink (relay-to-user) transmissions, this assumption is not required in the analysis and different fading conditions can be considered in the downlink and uplink. Hence, for more generality, we opted to choose different notations for the fading coefficients.

In the training process, it is assumed that the receivers employ minimum mean-square error (MMSE) estimation. Let us assume that the user A allocates δ_a of its total power for training, user B allocates δ_b of its total power for training while the relay allocates δ_r of its total power for training. As described in [26], the MMSE estimate of h_{ar} is given by

$$\hat{h}_{ar} = \frac{\sigma_{ar}^2\sqrt{\delta_a m P_a}}{\sigma_{ar}^2\delta_a m P_a + N_0}y_{ar,t}, \tag{3.8}$$

where $y_{ar,t} \sim \mathcal{CN}(0, \sigma_{ar}^2 \delta_a m P_a + N_0)$. We denote by $\tilde{h}_{ar}$ the estimate error which is a zero-mean complex Gaussian random variable with variance

$$var(\tilde{h}_{ar}) = \frac{\sigma_{ar}^2 N_0}{\sigma_{ar}^2 \delta_a m P_a + N_0}. \tag{3.9}$$

Similarly, we have

$$\begin{aligned} \hat{h}_{br} &= \frac{\sigma_{br}^2 \sqrt{\delta_b m P_b}}{\sigma_{br}^2 \delta_b m P_b + N_0} y_{br,t}, \\ y_{br,t} &\sim \mathcal{CN}(0, \sigma_{br}^2 \delta_b m P_b + N_0), \end{aligned} \tag{3.10}$$

$$var(\tilde{h}_{br}) = \frac{\sigma_{br}^2 N_0}{\sigma_{br}^2 \delta_b m P_b + N_0}. \tag{3.11}$$

$$\begin{aligned} \hat{h}_{ra} &= \frac{\sigma_{ra}^2 \sqrt{\delta_r m P_r}}{\sigma_{ra}^2 \delta_r m P_r + N_0} y_{a,t}, \\ y_{a,t} &\sim \mathcal{CN}(0, \sigma_{ra}^2 \delta_r m P_r + N_0), \end{aligned} \tag{3.12}$$

$$var(\tilde{h}_{ra}) = \frac{\sigma_{ra}^2 N_0}{\sigma_{ra}^2 \delta_r m P_r + N_0}, \tag{3.13}$$

$$\begin{aligned} \hat{h}_{rb} &= \frac{\sigma_{rb}^2 \sqrt{\delta_r m P_r}}{\sigma_{rb}^2 \delta_r m P_r + N_0} y_{b,t}, \\ y_{b,t} &\sim \mathcal{CN}(0, \sigma_{rb}^2 \delta_r m P_r + N_0), \end{aligned} \tag{3.14}$$

$$var(\tilde{h}_{rb}) = \frac{\sigma_{rb}^2 N_0}{\sigma_{rb}^2 \delta_r m P_r + N_0}. \tag{3.15}$$

With these estimates, the fading coefficients can now be expressed as

$$h_{ar} = \hat{h}_{ar} + \tilde{h}_{ar}, \tag{3.16}$$

$$h_{br} = \hat{h}_{br} + \tilde{h}_{br}, \tag{3.17}$$

$$h_{ra} = \hat{h}_{ra} + \tilde{h}_{ra}. \tag{3.18}$$

$$h_{rb} = \hat{h}_{rb} + \tilde{h}_{rb}. \tag{3.19}$$

3.2.2 Data Transmission Phase

The practical relay node usually cannot transmit and receive data simultaneously. Thus, we assume that the relay works under half-duplex constraint. As discussed in the previous section, within a block of m symbols, the first three symbols are allocated for channel training. In the remaining duration of $m-3$ symbols, data transmission takes place. As usual, two-way relaying can be divided into two phases. The first one is usually called the multiple access (MAC) phase in which the users simultaneously transmit their messages to the relay. The second phase is called the broadcast phase (BC) in which the relay transmits to both users. We introduce the MAC transmission parameter α and assume that a duration of $\alpha(m-3)$ symbols is allocated for users' transmission to the relay. Hence, α can be seen as the fraction of total time (or bandwidth) dedicated to the MAC phase. The remaining duration of $(1-\alpha)(m-3)$ symbols is to be used in the broadcast phase.

3.2.2.1 Multiple Access Phase

In the multiple access phase of the bidirectional relaying protocol, nodes A and B simultaneously transmit independent messages m_a and m_b with rates R_a and R_b to the relay node. Thereby, the message m_a from node A is intended for node B and vice versa for message m_b. Then, the input-output relation in the multiple

access channel is given by

$$\mathbf{y}_r = h_{ar}\mathbf{x}_a + h_{br}\mathbf{x}_b + \mathbf{n}_r \tag{3.20}$$

$$= \hat{h}_{ar}\mathbf{x}_a + \hat{h}_{br}\mathbf{x}_b + \tilde{h}_{ar}\mathbf{x}_a + \tilde{h}_{br}\mathbf{x}_b + \mathbf{n}_r \tag{3.21}$$

where the data transmission vectors $\mathbf{x}_a$ and $\mathbf{x}_b$ are assumed to be composed of independent random variables with equal energy. Hence, the corresponding covariance matrices are

$$E\{\mathbf{x}_a\mathbf{x}_a^\dagger\} = P_a' \ \mathbf{I} = \frac{(1-\delta_a)mP_a}{(m-3)\alpha} \ \mathbf{I}, \tag{3.22}$$

$$E\{\mathbf{x}_b\mathbf{x}_b^\dagger\} = P_b' \ \mathbf{I} = \frac{(1-\delta_b)mP_b}{(m-3)\alpha} \ \mathbf{I}. \tag{3.23}$$

Using the same techniques described in [75], we can show that capacity lower bounds can be obtained when the channel estimation error is assumed to be another source of Gaussian noise. This is due to the fact that Gaussian noise is the worst uncorrelated noise for the Gaussian model. Now, we can write the new noise vector as

$$\mathbf{z}_r = \tilde{h}_{ar}\mathbf{x}_a + \tilde{h}_{br}\mathbf{x}_b + \mathbf{n}_r. \tag{3.24}$$

The covariance matrix of this noise vector can be expressed as

$$E\{\mathbf{z}_r{\mathbf{z}_r}^\dagger\} = \sigma_{z_r}^2\mathbf{I} = \sigma_{\tilde{h}_{ar}}^2 E\{\mathbf{x}_a\mathbf{x}_a^\dagger\} + \sigma_{\tilde{h}_{br}}^2 E\{\mathbf{x}_b\mathbf{x}_b^\dagger\} + N_0\mathbf{I}. \tag{3.25}$$

Using the approach employed in [75], we can obtain the worst-case achievable

rate region of the MAC phase as follows:

$$\mathbb{R}_{MAC} := \{[R_a, R_b] \in \mathcal{R}_+^2 : R_a \leq R_a^m, R_b \leq R_b^m, \\ R_a + R_b \leq R_\Sigma^{MAC}\} \tag{3.26}$$

with the individual and sum-rate upper bounds given by

$$R_a^m = E\left[\frac{\alpha(m-3)}{m}\log\left(1+\frac{P_a'|\hat{h}_{ar}|^2}{\sigma_{z_r}^2}\right)\right] \tag{3.27}$$

$$R_b^m = E\left[\frac{\alpha(m-3)}{m}\log\left(1+\frac{P_b'|\hat{h}_{br}|^2}{\sigma_{z_r}^2}\right)\right] \tag{3.28}$$

$$R_\Sigma^{MAC} = E\left[\frac{\alpha(m-3)}{m}\log\left(1+\frac{P_a'|\hat{h}_{ar}|^2}{\sigma_{z_r}^2}+\frac{P_b'|\hat{h}_{br}|^2}{\sigma_{z_r}^2}\right)\right] \tag{3.29}$$

where $\frac{P_a'|\hat{h}_{ar}|^2}{\sigma_{z_r}^2}$ and $\frac{P_b'|\hat{h}_{br}|^2}{\sigma_{z_r}^2}$ are given on the next page in (3.30) and (3.31)

$$\frac{P_a'|\hat{h}_{ar}|^2}{\sigma_{z_r}^2} = \frac{\delta_a(1-\delta_a)\sigma_{ar}^4 m^2 P_a^2(\sigma_{br}^2\delta_b m P_b + N_0)|w_{ar}^2|}{\mathbb{C}} \tag{3.30}$$

$$\frac{P_b'|\hat{h}_{br}|^2}{\sigma_{z_r}^2} = \frac{\delta_b(1-\delta_b)\sigma_{br}^4 m^2 P_b^2(\sigma_{ar}^2\delta_a m P_a + N_0)|w_{br}^2|}{\mathbb{C}} \tag{3.31}$$

Where $\mathbb{C} = \sigma_{ar}^2 N_0(1-\delta_a)mP_a(\sigma_{br}^2\delta_b mP_b + N_0) + +\sigma_{br}^2 N_0(1-\delta_b)mP_b(\sigma_{ar}^2\delta_a mP_a + N_0) + N_0(m-3)\alpha(\sigma_{ar}^2\delta_a mP_a + N_0)(\sigma_{br}^2\delta_b mP_b + N_0)$ in which we have defined $w_{ar} \sim$

$\mathcal{CN}(0,1)$ and $w_{br} \sim \mathcal{CN}(0,1)$. Since $\mathbb{R}_{MAC}$ is a pentagon, it can be completely described by five vertices. The two vertices where the individual rate constraints intersect with the sum-rate constraint are

$$v_{a\sum} := [R_a^m, R_b^{a\sum}] \text{ and } v_{b\sum} := [R_a^{b\sum}, R_b^m] \tag{3.32}$$

where

$$R_b^{a\sum} = R_{\sum}^{MAC} - R_a^m \tag{3.33}$$

$$= E\left[\frac{\alpha(m-3)}{m}\log\left(1+\frac{P_b'|\hat{h}_{br}|^2}{\sigma_{z_r}^2+P_a'|\hat{h}_{ar}|^2}\right)\right], \tag{3.34}$$

$$R_a^{b\sum} = R_{\sum}^{MAC} - R_b^m \tag{3.35}$$

$$= E\left[\frac{\alpha(m-3)}{m}\log\left(1+\frac{P_a'|\hat{h}_{ar}|^2}{\sigma_{z_r}^2+P_b'|\hat{h}_{br}|^2}\right)\right]. \tag{3.36}$$

3.2.2.2 Broadcast Phase

In the succeeding BC phase of duration $(1-\alpha)(m-3)$ symbols, the relay forwards the previously received message m_a to node B and message m_b to node A. Similarly as for the source transmission vectors, we assume that the relay vector $\mathbf{x}_r$ has independent components with equal energy. Hence, the covariance matrix of the relay transmission vector is

$$E\{\mathbf{x}_r\mathbf{x}_r^\dagger\} = P_r'\ \mathbf{I} = \frac{(1-\delta_r)mP_r}{(m-3)(1-\alpha)}\ \mathbf{I}. \tag{3.37}$$

In this chapter, we consider the superposition encoding strategy. Therefore, the messages m_a and m_b are separately encoded as for the point-to-point Gaussian channel. Then, the vector transmitted from the relay node obtained with superpo-

sition encoding can be expressed as

$$\mathbf{x}_r = \mathbf{w}_a + \mathbf{w}_b, \tag{3.38}$$

where the vectors $\mathbf{w}_a$ and $\mathbf{w}_b$ correspond to the codewords of the messages m_a and m_b, respectively. Note that $E\{\|\mathbf{x}_r\|^2\} = E\{\|\mathbf{w}_a\|^2\} + E\{\|\mathbf{w}_b\|^2\}$. Let β_1 and β_2 denote the proportion of relay transmit power P_r' used for the codewords w_a and w_b, respectively. Hence, $E\{\|\mathbf{w}_a\|^2\} = \beta_1 P_r'$ and $E\{\|\mathbf{w}_b\|^2\} = \beta_2 P_r'$. Then, the simplex

$$[\beta_1, \beta_2] \in [0,1] \times [0,1] : \beta_1 + \beta_2 \leq 1 \tag{3.39}$$

characterizes the set of feasible relay power distributions that satisfy the relay transmit power constraint.

Now, the signals received at nodes A and B can be expressed as

$$\mathbf{y}_k = h_{rk}\mathbf{x}_r + \mathbf{n}_k \qquad \text{for } k = a, b \tag{3.40}$$

$$= \hat{h}_{rk}\mathbf{w}_a + \hat{h}_{rk}\mathbf{w}_b + \tilde{h}_{rk}\mathbf{x}_r + \mathbf{n}_k. \tag{3.41}$$

$$= \hat{h}_{rk}\mathbf{w}_a + \hat{h}_{rk}\mathbf{w}_b + \mathbf{z}_k \tag{3.42}$$

where we have defined

$$\mathbf{z}_k = \tilde{h}_{rk}\mathbf{x}_r + \mathbf{n}_k \tag{3.43}$$

as the effective noise vector with covariance matrix

$$E\{\mathbf{z}_k {\mathbf{z}_k}^\dagger\} = \sigma_{z_k}^2 \mathbf{I} = \sigma_{\tilde{h}_{rk}}^2 E\{\mathbf{x}_r \mathbf{x}_r^\dagger\} + N_0 \mathbf{I}. \tag{3.44}$$

Note that the user nodes A and B know their own transmitted codewords $\mathbf{w}_a$ and $\mathbf{w}_b$, respectively. Moreover, through the network training phase, they are equipped with the channel estimate $\hat{h}_{rk}$. Hence, they can suppress the interference due to their own messages, and the signals at nodes A and B can now be expressed, respectively, as

$$\mathbf{y}_a = \hat{h}_{rk}\mathbf{w}_b + \mathbf{z}_k, \text{ and} \tag{3.45}$$

$$\mathbf{y}_b = \hat{h}_{ra}\mathbf{w}_a + \mathbf{z}_k. \tag{3.46}$$

It should also be noticed that due to the presence of channel estimation errors, self-interference cannot be canceled perfectly. The residual interference components $\tilde{h}_{rk}\mathbf{w}_a$ at node A and $\tilde{h}_{rk}\mathbf{w}_b$ at node B are incorporated into the noise term $\mathbf{z}_k$.

Now, assuming superposition encoding at the relay and self-interference suppression at the receiver nodes, and regarding the noise component, which includes the residual interference terms and the background noise, as Gaussian distributed, we can easily see that the worst-case achievable rate region of the BC phase is given by

$$\mathbb{R}_{BC} := \{[R_a, R_b] \in \mathcal{R}_+^2 : R_a \leq R_a^b(\beta_1), R_b \leq R_b^b(\beta_2)\} \tag{3.47}$$

where

$$R_a^b = E\left[\frac{(1-\alpha)(m-3)}{m}\log\left(1 + \frac{P_r'\beta_1|\hat{h}_{rb}|^2}{\sigma_{z_b}^2}\right)\right] \tag{3.48}$$

$$R_b^b = E\left[\frac{(1-\alpha)(m-3)}{m}\log\left(1 + \frac{P_r'\beta_2|\hat{h}_{ra}|^2}{\sigma_{z_a}^2}\right)\right] \tag{3.49}$$

with

$$\frac{P_r'|\hat{h}_{rb}|^2}{\sigma_{z_b}^2} = \frac{\delta_r(1-\delta_r)\sigma_{rb}^4 m^2 P_r^2 |w_{rb}^2|}{\sigma_{rb}^2 N_0(1-\delta_r)mP_r + N_0(m-3)(1-\alpha)(\sigma_{rb}^2\delta_r mP_r + N_0)}$$

$$\frac{P_r'|\hat{h}_{ra}|^2}{\sigma_{z_a}^2} = \frac{\delta_r(1-\delta_r)\sigma_{ra}^4 m^2 P_r^2 |w_{ra}^2|}{\sigma_{ra}^2 N_0(1-\delta_r)mP_r + N_0(m-3)(1-\alpha)(\sigma_{ra}^2\delta_r mP_r + N_0)}.$$

Above, $w_{ra} \sim \mathcal{CN}(0,1)$ and $w_{rb} \sim \mathcal{CN}(0,1)$.

On the boundary of the BC achievable region $\mathbb{R}_{BC}$, we have $\beta_1 + \beta_2 = 1$. Let us set $\beta_1 = \beta$ and $\beta_2 = 1-\beta$. Now, any point on the boundary can be achieved by varying β from 0 to 1. Of particular interest is the value of β that achieves the maximum sum rate $R_{\sum}^b := \max_{[R_a,R_b]\in\mathbb{R}_{BC}} R_a + R_b$ in the broadcast phase. In general, it is difficult to analytically determine the sum-rate-maximizing value of β for the cases in which β is kept fixed by the relay for different channel realizations. On the other hand, if the relay knows the channel estimates $\hat{h}_{ra}$ and $\hat{h}_{rb}$ of the source nodes, then it can adapt β to these estimates in each block. For this case, we can find the optimal β^* value, which maximizes the sum rate, in closed-form as follows:

$$\beta^* = \begin{cases} 0 & \text{if } \frac{1}{2} + \frac{1}{2P_r'}\left(\frac{\sigma_{z_a}^2}{|\hat{h}_{ra}|^2} - \frac{\sigma_{z_b}^2}{|\hat{h}_{rb}|^2}\right) < 0 \\ \frac{1}{2} + \frac{1}{2P_r'}\left(\frac{\sigma_{z_a}^2}{|\hat{h}_{ra}|^2} - \frac{\sigma_{z_b}^2}{|\hat{h}_{rb}|^2}\right) & \text{if } 0 \le \frac{1}{2} + \frac{1}{2P_r'}\left(\frac{\sigma_{z_a}^2}{|\hat{h}_{ra}|^2} - \frac{\sigma_{z_b}^2}{|\hat{h}_{rb}|^2}\right) \le 1 \\ 1 & \text{if } \frac{1}{2} + \frac{1}{2P_r'}\left(\frac{\sigma_{z_a}^2}{|\hat{h}_{ra}|^2} - \frac{\sigma_{z_b}^2}{|\hat{h}_{rb}|^2}\right) > 1 \end{cases}$$

3.2.2.3 Achievable Rate Region for Two-Way Relay Channel

The worst-case achievable rate region of the two-way decode-and-forward relaying scheme considered in this chapter is given by the intersection of the rate regions of the multiple-access and broadcast phases:

$$\mathbb{R}(\alpha) := \mathbb{R}_{MAC} \bigcap \mathbb{R}_{BC}. \tag{3.50}$$

3.3 Numerical Results and Discussions

The achievable rate regions obtained in the previous section depend on several parameters, such as the fractions of power allocated to training δ_a, δ_b, and δ_r; the fraction of time allocated to the MAC phase α; the relay power allocation parameter β; the coherence block length m; and the fading variances σ^2. Other than some special cases as seen in the discussion of the sum-rate-maximizing value of β above, finding closed-form expressions for the optimized values of training and data transmission parameters seems unlikely in general scenarios. For this reason, we resort to numerical methods in order to identify the impact of these parameters.

In Figure 3.2, we plot the achievable rate regions of the multiple access and broadcast phases of two-way relaying for different values of α when the other parameters are $P_a = P_b = P_r = 1, m = 50, \sigma_{ra} = \sigma_{ar} = \sigma_{br} = \sigma_{rb} = 1, \delta_a = \delta_b = \delta_r = 0.1$. It can be easily seen that the MAC region expands and BC region shrinks, as expected, as the value of α is increased. Hence, for small values of α, MAC region dictates the achievable rate region of two-way relaying while BC region does so for larger α. In Figs. 3.3 and 3.4, we plot the sum rate of users A and B as a function of α for high and lower SNR values, respectively. In both cases,

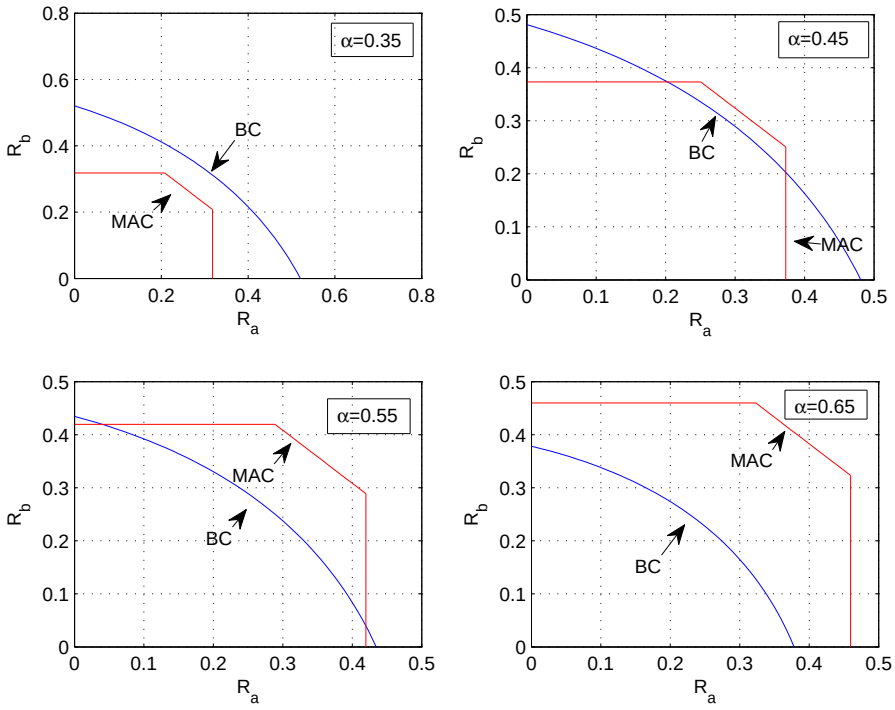

Figure 3.2: Achievable Rate Region for different values of α when $P_a = P_b = P_r = 1, m = 50, \sigma_{ra} = \sigma_{ar} = \sigma_{br} = \sigma_{rb} = 1, \delta_a = \delta_b = \delta_r = 0.1$.

the optimal α value is around 0.55, indicating that when sum rate is concerned, equal time/bandwidth allocation between multiple access and broadcast phases is not necessarily optimal.

Next, we investigate how much power needs to be spent on training to maximize the sum rate. For simplification, we assume all nodes spend the same ratio of power for training, i.,e. $\delta_a = \delta_b = \delta_r = \delta$. In Fig. 3.5, sum rate is plotted as a function of this common δ value. We observe that the optimal fraction of power allocated for training is around 0.2. Further increase in training power leads to a decrease in the overall throughput as it diminishes the available power for data transmission.

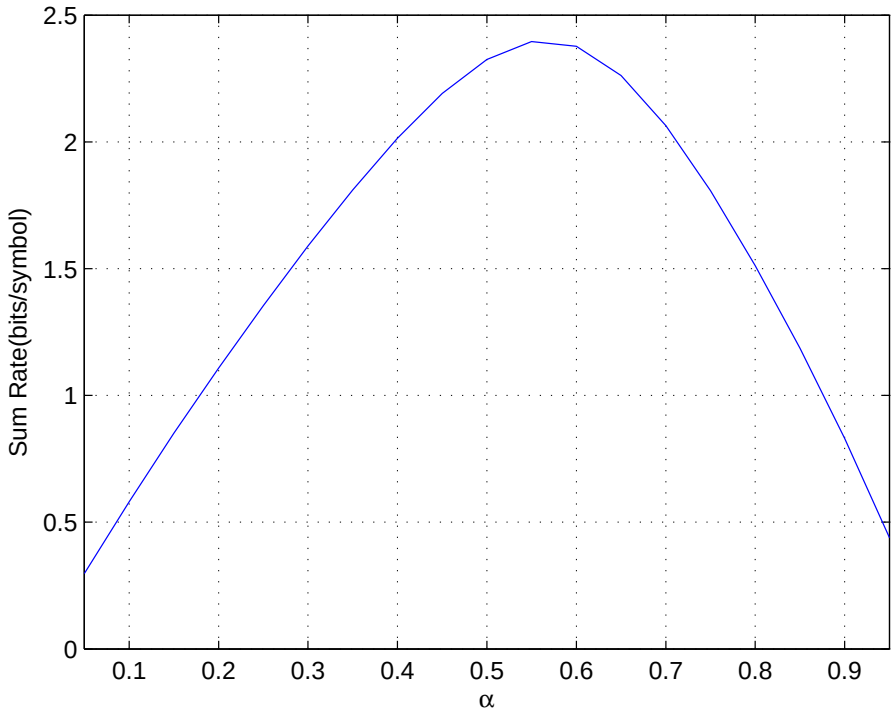

Figure 3.3: Sum rate vs. α with $P_a = P_b = P_r = 10, m = 50, \sigma_{ra} = \sigma_{ar} = 1, \sigma_{br} = \sigma_{rb} = 2, \delta_a = \delta_b = \delta_r = 0.1$.

Finally, in Fig.3.6, we provide the sum rate curve as a function of the relay power P_r. We see that the sum rate saturates as the relay power is increased beyond some threshold. This is mainly because of the fact that MAC phase becomes the bottleneck of the whole system for large relay power levels.

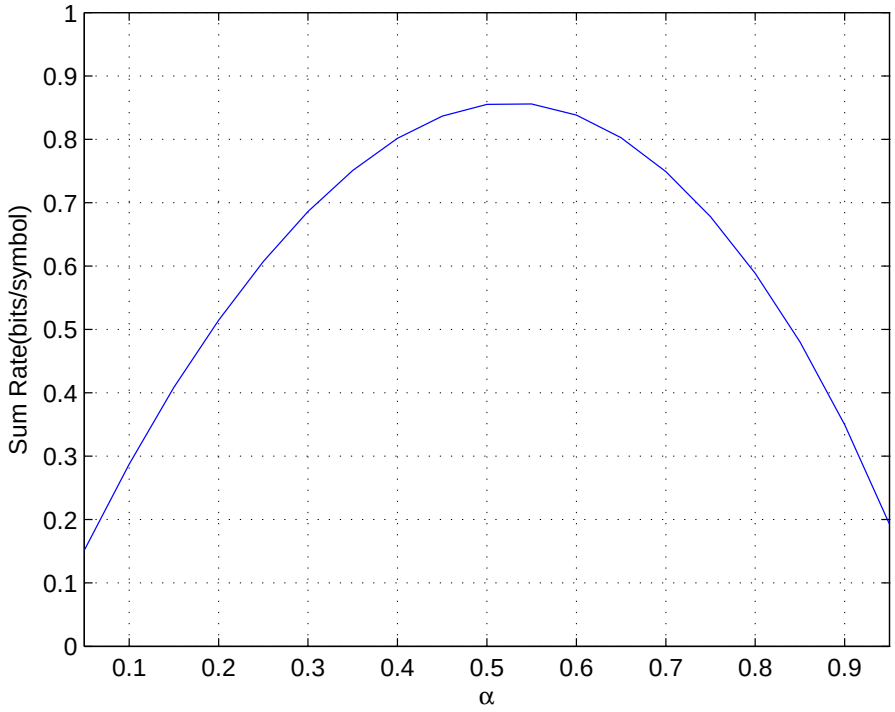

Figure 3.4: Sum rate vs. α with $P_a = P_b = P_r = 1, m = 50, \sigma_{ra} = \sigma_{ar} = 1, \sigma_{br} = \sigma_{rb} = 2, \delta_a = \delta_b = \delta_r = 0.1$.

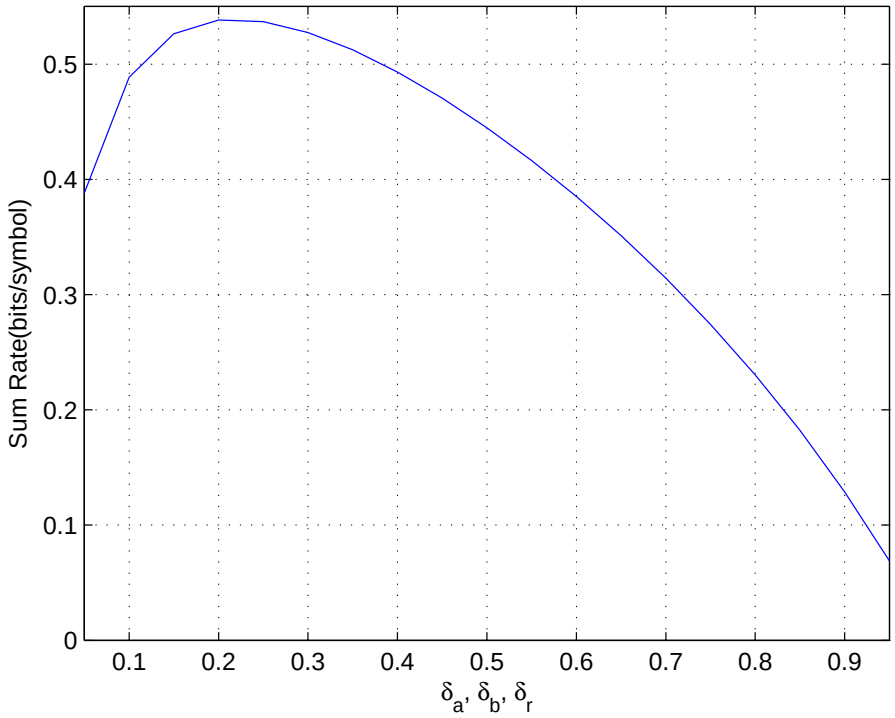

Figure 3.5: Sum rate vs. $\delta_a, \delta_b, \delta_r$ with $P_a = P_b = P_r = 1, m = 50, \sigma_{ra} = \sigma_{ar} = \sigma_{br} = \sigma_{rb} = 1, \alpha = 0.55$.

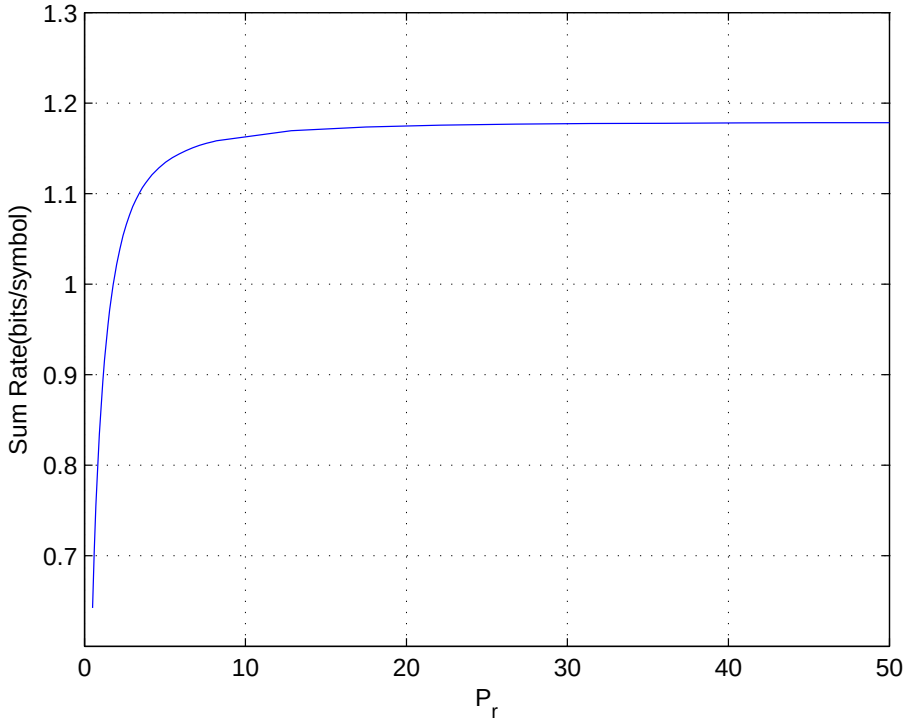

Figure 3.6: Sum rate vs. P_r with $P_a = P_b = 1, m = 50, \sigma_{ra} = \sigma_{ar} = 1, \sigma_{br} = \sigma_{rb} = 2, \delta_a = \delta_b = \delta_r = 0.1, \alpha = 0.55$.

Chapter 4

Collaborative Relay Beamforming for Secrecy

In this chapter, we investigate the collaborative relay beamforming under secrecy constraints in the presence of both total and individual power constraints with the assumptions of perfect and imperfect channel knowledge.

More specifically, our contributions in this chapter are as follows:

1. In DF, under total power constraints, we analytically determine the beamforming structure in the high- and low-SNR regimes.

2. In DF, under individual power constraints, not having analytical solutions available, we provide an optimization framework to obtain the optimal beamforming that maximizes the secrecy rate. We use the semidefinite relaxation (SDR) approach to approximate the problem as a convex semidefinite programming (SDP) problem which can be solved efficiently. We also provide an alternative method by formatting the original optimization problem as a convex second-order cone programming (SOCP) problem that can be ef-

ficiently solved by interior point methods. Also, we describe a simplified suboptimal beamformer design under individual power constraints.

3. In AF, we first obtain an expression for the achievable secrecy rate, and then we show that the optimal beamforming solution that maximizes the secrecy rate can be obtained by semidefinite programming with a two dimensional search for both total and individual power constraints.

4. Two robust beamforming design methods for DF relaying are described in the case of imperfect CSI.

The organization of the rest of the chapter is as follows. In Section 4.1, we describe the channel model and study the beamforming design for DF relaying under secrecy constraints. Beamforming for AF relaying is investigated in Section 4.2. In Section 4.3, robust beamforming design in the case of imperfect CSI is studied. Numerical results for the performance of different beamforming schemes are provided in Section 4.4. Finally, we conclude in Section 4.5.

4.1 Decode-and-Forward Relaying

We consider a communication channel with a source S, a destination D, an eavesdropper E, and M relays $\{R_m\}_{m=1}^{M}$ as depicted in Figure 4.1. In this model, the source S tries to transmit confidential messages to destination D with the help of the relays while keeping the eavesdropper E ignorant of the information. We assume that there is no direct link between S and D, and S and E. Hence, initially messages transmitted by the source are received only by the relays. Subsequently, relays work synchronously and multiply the signals with complex weights $\{w_m\}$ and produce a virtual beam point to the destination. We denote the channel coeffi-

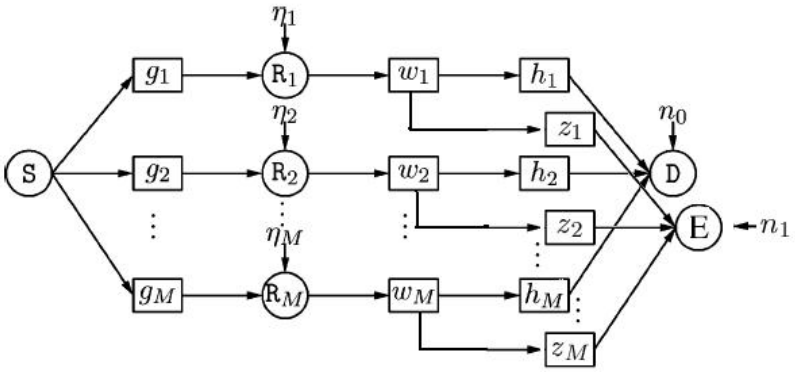

Figure 4.1: Channel Model

cient between the source S and the m^{th} relay R_m as $g_m \in \mathbb{C}$, the channel coefficient between R_m and the destination D as $h_m \in \mathbb{C}$, and the channel coefficient between R_m and eavesdropper E as $z_m \in \mathbb{C}$.

It is obvious that our channel is a two-hop relay network. In the first hop, the source S transmits x_s to the relays with power $E[|x_s|^2] = P_s$. The received signal at R_m is given by

$$y_{r,m} = g_m x_s + \eta_m \tag{4.1}$$

where η_m is the background noise that has a complex, circularly symmetric Gaussian distribution with zero mean and variance of N_m.

In the second hop, we employ decode-and-forward transmission scheme. In this scheme, each relay first decodes the message x_s and normalizes it as $x'_s = x_s/\sqrt{P_s}$. Subsequently, the normalized message is multiplied by the weight factor w_m by the m^{th} relay to generate the transmitted signal $x_r = w_m x'_s$. The output

power of the m^{th} relay R_m is given by

$$E[|x_r|^2] = E[|w_m x_s'|^2] = |w_m|^2. \tag{4.2}$$

The received signals at the destination D and eavesdropper E are the superpositions of the signals transmitted from the relays. These signals can be expressed, respectively, as

$$y_d = \sum_{m=1}^{M} h_m w_m x_s' + n_0 = \mathbf{h}^\dagger \mathbf{W} x_s' + n_0, \quad \text{and} \tag{4.3}$$

$$y_e = \sum_{m=1}^{M} z_m w_m x_s' + n_1 = \mathbf{z}^\dagger \mathbf{W} x_s' + n_1 \tag{4.4}$$

where n_0 and n_1 are the Gaussian background noise components at D and E, respectively, with zero mean and variance N_0. Additionally, we have defined $\mathbf{h} = [h_1^*, ...h_M^*]^T, \mathbf{z} = [z_1^*, ...z_M^*]^T$, and $\mathbf{W} = [w_1, ...w_M]^T$ where superscript $*$ denotes conjugate operation, and $(\cdot)^T$ and $(\cdot)^\dagger$ denote the transpose and conjugate transpose, respectively, of a matrix or vector. The metrics of interest are the received SNR levels at D and E, which are given, respectively, by

$$\Gamma_d = \frac{|\sum_{m=1}^{M} h_m w_m|^2}{N_0} \text{ and } \Gamma_e = \frac{|\sum_{m=1}^{M} z_m w_m|^2}{N_0}. \tag{4.5}$$

It is well-known that given the channel coefficients, the secrecy rate R_s over the channel between the relays and destination is (see e.g., [42])

$$R_s = I(x_s'; y_d) - I(x_s'; y_e) \tag{4.6}$$

$$= \log(1 + \Gamma_d) - \log(1 + \Gamma_e) \tag{4.7}$$

$$= \log\left(\frac{N_0 + |\sum_{m=1}^{M} h_m w_m|^2}{N_0 + |\sum_{m=1}^{M} z_m w_m|^2}\right) \tag{4.8}$$

where $I(\cdot;\cdot)$ denotes the mutual information, and x_s' is Gaussian distributed with zero-mean and $E[|x_s'|^2] = 1$. Coding strategies that achieve the secrecy rates involve randomization at the encoder to introduce uncertainty to the eavesdropper. Secrecy coding techniques are discussed in detail in [73][42][15][24]. Practical coding schemes for secure communications have been studied in [49] and [66] for certain special cases of the wiretap channel. It is important to note that we assume in the decode-and-forward scenario that the relays use the same secrecy codebook and transmit the same signal x_s' simultaneously. We further note that we throughout the text are interested in beamforming vectors that satisfy for given channel coefficients the inequality, $N_0 + |\sum_{m=1}^{M} h_m w_m|^2 > N_0 + |\sum_{m=1}^{M} z_m w_m|^2$. If there are no such beamforming vectors and the ratio inside the logarithm in (4.8) is less than 1, then the secrecy rate, by definition, is zero meaning that secure transmission cannot be established. The beamforming vectors which lead to zero secrecy capacity are not of interest.

In this section, we address the joint optimization of $\{w_m\}$ and hence identify the optimum collaborative relay beamforming (CRB) direction that maximizes the secrecy rate given in (4.8). Initially, we assume that the perfect knowledge of the channel coefficients is available. Later, in Section 4.3, we address the case in which the channel coefficients are only imperfectly known. We would like to also remark that the secrecy rate expression in (4.8) in a fading environment represents the instantaneous secrecy rate for given instantaneous values of the channel fading coefficients. Hence, in such a case, our formulation considers the optimization of $\{w_m\}$ in order to maximize the instantaneous secrecy rates.

4.1.1 Optimal Beamforming under Total Power Constraints

In this section, we consider a total relay power constraint in the following form: $||\mathbf{W}||^2 = \mathbf{W}^\dagger\mathbf{W} \leq P_T$. The optimization problem can now be formulated as follows:

$$\begin{aligned} R_s(\mathbf{h},\mathbf{z},P_T) &= \max_{\mathbf{W}^\dagger\mathbf{W}\leq P_T} \log\left(\frac{N_0+|\sum_{m=1}^{M} h_m w_m|^2}{N_0+|\sum_{m=1}^{M} z_m w_m|^2}\right) \\ &= \log \max_{\mathbf{W}^\dagger\mathbf{W}\leq P_T} \frac{N_0+|\sum_{m=1}^{M} h_m w_m|^2}{N_0+|\sum_{m=1}^{M} z_m w_m|^2} \qquad (4.9) \\ &= \log \max_{\mathbf{W}^\dagger\mathbf{W}\leq P_T} \frac{\mathbf{W}^\dagger(\frac{N_0}{P_T}\mathbf{I}+\mathbf{h}\mathbf{h}^\dagger)\mathbf{W}}{\mathbf{W}^\dagger(\frac{N_0}{P_T}\mathbf{I}+\mathbf{z}\mathbf{z}^\dagger)\mathbf{W}} \qquad (4.10) \\ &= \log \max_{\mathbf{W}^\dagger\mathbf{W}\leq P_T} \frac{\mathbf{W}^\dagger(N_0\mathbf{I}+P_T\mathbf{h}\mathbf{h}^\dagger)\mathbf{W}}{\mathbf{W}^\dagger(N_0\mathbf{I}+P_T\mathbf{z}\mathbf{z}^\dagger)\mathbf{W}} \qquad (4.11) \\ &= \log \lambda_{\max}(N_0\mathbf{I}+P_T\mathbf{h}\mathbf{h}^\dagger, N_0\mathbf{I}+P_T\mathbf{z}\mathbf{z}^\dagger) \qquad (4.12) \end{aligned}$$

where $\lambda_{\max}(\mathbf{A},\mathbf{B})$ is the largest generalized eigenvalue of the matrix pair $(\mathbf{A},\mathbf{B})$ [1]. Hence, the maximum secrecy rate in (4.12) is achieved by the optimal beamforming vector

$$\mathbf{W}_{opt} = \varsigma\mathbf{u} \qquad (4.13)$$

where $\mathbf{u}$ is the eigenvector that corresponds to $\lambda_{\max}(N_0\mathbf{I}+P_T\mathbf{h}\mathbf{h}^\dagger, N_0\mathbf{I}+P_T\mathbf{z}\mathbf{z}^\dagger)$ and ς is chosen to ensure $\mathbf{W}_{opt}^\dagger\mathbf{W}_{opt} = P_T$. Note that in the first-hop of the channel model, the maximum rate we can achieve is

$$R_1 = \min_{m=1,\ldots,M} \log\left(1+\frac{|g_m|^2 P_s}{N_m}\right). \qquad (4.14)$$

[1] For a Hermitian matrix $\mathbf{A}\in\mathbb{C}^{n\times n}$ and positive definite matrix $\mathbf{B}\in\mathbb{C}^{n\times n}$, (λ,ψ) is referred to as a generalized eigenvalue – eigenvector pair of $(\mathbf{A},\mathbf{B})$ if (λ,ψ) satisfy $\mathbf{A}\psi = \lambda\mathbf{B}\psi$ [23].

Since we want all relays to successfully decode the signal transmitted from the source in the DF scenario, the rate expression in (4.14) is equal to the minimum of the rates required for reliable decoding at the relays. Hence, the first-hop rate is dictated by the worst channel among the channels between the source and the relays.

The overall secrecy rate is

$$R_{dof,s} = \min(R_1, R_s). \tag{4.15}$$

Above, we observe that having a severely weak source-relay channel can significantly degrade the performance. In these cases, other forwarding techniques (e.g., amplify-and-forward) can be preferred. Throughout the analysis of the DF scenario, we will not explicitly address these considerations and we will concentrate on the secure communication between the relays and the destination. Hence, we will have the implicit assumption that the source-relay links do not constitute a bottleneck for communication.

Next, we provide some remarks on the performance of collaborative relay beamforming in the high- and low-SNR regimes. Optimal beamforming under total power constraints is studied in detail in [17] and [18]. However, these studies have not identified the beamforming structure at low and high SNR levels. For simplicity, we assume in the following that the noise variances at the destination and eavesdropper are $N_0 = 1$.

4.1.1.1 High-SNR Regime

In the high SNR scenario, where both $P_s, P_T \to \infty$, we can easily see that

$$\lim_{P_s \to \infty} (R_1 - \log P_s) = \min_{m=1,\ldots,M} \log(|g_m|^2 / N_m). \tag{4.16}$$

From the Corollary 4 in Chapter 4 of [36], we can see that

$$\lim_{P_T \to \infty} (R_s - \log(P_T)) = \log(\max_{\tilde{\psi}} |\mathbf{h}^\dagger \tilde{\psi}|^2) \tag{4.17}$$

where $\tilde{\psi}$ is a unit vector on the null space of $\mathbf{z}^\dagger$. This result implies that choosing the beamforming vectors to lie in the null spaces of the eavesdropper's channel vector, i.e., having $|\sum_{m=1}^{M} z_m w_m|^2 = \mathbf{z}^\dagger \mathbf{W} = 0$, is asymptotically optimal in the high-SNR regime. In this case, the eavesdropper cannot receive any data from the relays, and secrecy is automatically guarantied. No secrecy coding is needed at the relays. This asymptotic optimality can be seen from the following discussion. Assume that we impose the constraint $\mathbf{z}^\dagger \mathbf{W} = 0$. Now, the optimization problem

(under the assumption $N_0 = 1$) becomes

$$\max_{\substack{\mathbf{W}^\dagger\mathbf{W}\leq P_T \\ \mathbf{z}^\dagger\mathbf{W}=0}} \log\left(\frac{1+\left|\sum_{m=1}^{M} h_m w_m\right|^2}{1+\left|\sum_{m=1}^{M} z_m w_m\right|^2}\right) = \max_{\substack{\mathbf{W}^\dagger\mathbf{W}\leq P_T \\ \mathbf{z}^\dagger\mathbf{W}=0}} \log\left(1+\left|\sum_{m=1}^{M} h_m w_m\right|^2\right) \tag{4.18}$$

$$= \max_{\substack{\hat{\mathbf{W}}^\dagger\hat{\mathbf{W}}\leq 1 \\ \mathbf{z}^\dagger\hat{\mathbf{W}}=0}} \log\left(1+\left|\sum_{m=1}^{M} h_m \hat{w}_m \sqrt{P_T}\right|^2\right) \tag{4.19}$$

$$= \log(P_T) + \max_{\substack{\hat{\mathbf{W}}^\dagger\hat{\mathbf{W}}\leq 1 \\ \mathbf{z}^\dagger\hat{\mathbf{W}}=0}} \log\left(\sqrt{\frac{1}{P_T}}+\left|\sum_{m=1}^{M} h_m \hat{w}_m\right|^2\right) \tag{4.20}$$

$$\approx \log(P_T) + \log\left(\max_{\substack{\hat{\mathbf{W}}^\dagger\hat{\mathbf{W}}\leq 1 \\ \mathbf{z}^\dagger\hat{\mathbf{W}}=0}} \left|\sum_{m=1}^{M} h_m \hat{w}_m\right|^2\right) \tag{4.21}$$

$$= \log(P_T) + \log(\max_{\tilde{\psi}} |\mathbf{h}^\dagger \tilde{\psi}|^2) \tag{4.22}$$

such that $\mathbf{z}^\dagger\psi = 0$ and $\|\psi\|^2 = 1$. Above in (4.19), we have defined $\hat{\mathbf{W}} = \mathbf{W}/\sqrt{P_T}$ for which the constraint becomes $\hat{\mathbf{W}}^\dagger\hat{\mathbf{W}} \leq 1$. The approximation in (4.21) is due to the fact that $\frac{1}{\sqrt{P_T}}$ becomes negligible for large P_T. Hence, null space beamforming provides the same asymptotic performance as in (4.17) and is optimal in the high-SNR regime.

Furthermore, the optimal null space beamforming vector can be obtained explicitly. Due to the null space constraint, we can write $\mathbf{W} = \mathbf{H}_z^\perp \mathbf{v}$, where $\mathbf{H}_z^\perp$ denotes the projection matrix onto the null space of $\mathbf{z}^\dagger$. Specifically, the columns of $\mathbf{H}_z^\perp$ are orthonormal vectors that form the basis of the null space of $\mathbf{z}^\dagger$. In our case, $\mathbf{H}_z^\perp$ is an $M \times (M-1)$ matrix. The power constraint $\mathbf{W}^\dagger\mathbf{W} = \mathbf{v}^\dagger {\mathbf{H}_z^\perp}^\dagger \mathbf{H}_z^\perp \mathbf{v} =$

$\mathbf{v}^\dagger\mathbf{v} \leq P_T$. Then, the optimization problem can be recast as

$$\max_{\mathbf{W}^\dagger\mathbf{W}\leq P_T} \log\left(1+\left|\sum_{m=1}^{M} h_m w_m\right|^2\right) = \log\left(1+\max_{\mathbf{W}^\dagger\mathbf{W}\leq P_T}(\mathbf{W}^\dagger\mathbf{h}\mathbf{h}^\dagger\mathbf{W})\right) \tag{4.23}$$

$$= \log\left(1+\max_{\mathbf{v}^\dagger\mathbf{v}\leq P_T}(\mathbf{v}^\dagger{\mathbf{H}_z^\perp}^\dagger\mathbf{h}\mathbf{h}^\dagger\mathbf{H}_z^\perp\mathbf{v})\right) \tag{4.24}$$

$$= \log\left(1+P_T\lambda_{\max}({\mathbf{H}_z^\perp}^\dagger\mathbf{h}\mathbf{h}^\dagger\mathbf{H}_z^\perp)\right) \tag{4.25}$$

$$= \log\left(1+P_T\mathbf{h}^\dagger\mathbf{H}_z^\perp{\mathbf{H}_z^\perp}^\dagger\mathbf{h}\right). \tag{4.26}$$

Therefore, the optimum null space beamforming vector $\mathbf{W}$ is

$$\mathbf{W}_{opt,n} = \mathbf{H}_z^\perp\mathbf{v} = \varsigma_1\mathbf{H}_z^\perp{\mathbf{H}_z^\perp}^\dagger\mathbf{h} \tag{4.27}$$

where ς_1 is a constant that is introduced to satisfy the power constraint.

4.1.1.2 Low-SNR Regime

In the low SNR regime, in which both $P_s, P_T \to 0$, we can see that

$$\lim_{P_s\to 0}\frac{R_1}{P_s} = \min_{m=1,\ldots,M}\frac{|g_m|^2}{N_m}, \text{ and} \tag{4.28}$$

$$\lim_{P_s\to 0}\frac{R_s}{P_T} = \lambda_{\max}(\mathbf{h}\mathbf{h}^\dagger - \mathbf{z}\mathbf{z}^\dagger). \tag{4.29}$$

Thus, in the low SNR regime, the direction of the optimal beamforming vector approaches that of the eigenvector that corresponds to the largest eigenvalue of $\mathbf{h}\mathbf{h}^\dagger - \mathbf{z}\mathbf{z}^\dagger$. A similar result is shown in a multiple-antenna setting in [26].

4.1.2 Optimal Beamforming under Individual Power Constraints

In a multiuser network such as the relay system we study in this chapter, it is practically more relevant to consider individual power constraints as wireless nodes generally operate under such limitations. Motivated by this, we now impose $|w_m|^2 \leq p_m \ \forall m$ or equivalently $|\mathbf{W}|^2 \leq \mathbf{p}$ where $|\cdot|^2$ denotes the element-wise norm-square operation and $\mathbf{p}$ is a column vector that contains the components $\{p_m\}$. In what follows, the problem of interest will be again be the maximization of the secrecy rate or equivalently the maximization of the term inside logarithm function of R_s (4.8) but now under individual power constraints:

$$\max_{|\mathbf{W}|^2 \leq \mathbf{p}} \frac{N_0 + |\sum_{m=1}^{M} h_m w_m|^2}{N_0 + |\sum_{m=1}^{M} z_m w_m|^2} \tag{4.30}$$

$$= \max_{|\mathbf{W}|^2 \leq \mathbf{p}} \frac{N_0 + \mathbf{W}^\dagger \mathbf{h}\mathbf{h}^\dagger \mathbf{W}}{N_0 + \mathbf{W}^\dagger \mathbf{z}\mathbf{z}^\dagger \mathbf{W}}. \tag{4.31}$$

In the following, we solve the optimization problem using two methods: one is semidefinite relaxation (SDR) based semidefinite programming (SDP) and the other one is the second-order cone programming (SOCP). We note that SOCP method is more efficient in general. However, the SDR method with bisection search technique described here will later be employed in the analysis of the amplify-and-forward (AF) relaying and in robust beamforming design. Since the formulations are more complicated in those cases, we believe it is more instructive to clearly explain the SDR approach here in the DF case.

4.1.2.1 Semidefinite Relaxation (SDR) Approach

We first consider a semidefinite programming method similar to that in [56]. Using the definition $\mathbf{X} \triangleq \mathbf{W}\mathbf{W}^{\dagger}$, we can rewrite the optimization problem in (4.31) as

$$\begin{aligned} \max_{\mathbf{X}} \quad & \frac{N_0 + tr(\mathbf{h}\mathbf{h}^{\dagger}\mathbf{X})}{N_0 + tr(\mathbf{z}\mathbf{z}^{\dagger}\mathbf{X})} \\ s.t \quad & diag(\mathbf{X}) \leq \mathbf{p} \\ & rank \ \mathbf{X} = 1, \quad and \quad \mathbf{X} \succeq 0 \end{aligned} \tag{4.32}$$

or equivalently as

$$\begin{aligned} \max_{\mathbf{X},t} \quad & t \\ s.t \quad & tr(\mathbf{X}(\mathbf{h}\mathbf{h}^{\dagger} - t\mathbf{z}\mathbf{z}^{\dagger})) \geq N_0(t-1), \\ & diag(\mathbf{X}) \leq \mathbf{p}, \\ & rank \ \mathbf{X} = 1, \quad and \quad \mathbf{X} \succeq 0 \end{aligned} \tag{4.33}$$

where $tr(\cdot)$ represents the trace of a matrix, $diag(\mathbf{X})$ denotes the vector whose components are the diagonal elements of $\mathbf{X}$, and $\mathbf{X} \succeq 0$ means that $\mathbf{X}$ is a symmetric positive semi-definite matrix. The optimization problem in (4.33) is not convex and may not be easily solved. Let us now ignore the rank constraint in (4.33). That is, using a semidefinite relaxation (SDR), we aim to solve the following

optimization problem:

$$\begin{aligned} &\max_{\mathbf{X},t} \quad t \\ &s.t \;\; tr(\mathbf{X}(\mathbf{h}\mathbf{h}^{\dagger} - t\mathbf{z}\mathbf{z}^{\dagger})) \geq N_0(t-1), \\ &and \;\; diag(\mathbf{X}) \leq \mathbf{p}, \quad and \quad \mathbf{X} \succeq 0. \end{aligned} \tag{4.34}$$

If the matrix $\mathbf{X}_{opt}$ obtained by solving the optimization problem in (4.34) happens to be rank one, then its principal component will be the optimal solution to the original problem. Note that the optimization problem in (4.34) is quasiconvex. In fact, for any value of t, the feasible set in (4.34) is convex. Let $t_{\max}$ be the maximum value of t obtained by solving the optimization problem (4.34). If, for any given t, the convex feasibility problem

$$\begin{aligned} &find \quad \mathbf{X} \\ &such \;\; that \; tr(\mathbf{X}(\mathbf{h}\mathbf{h}^{\dagger} - t\mathbf{z}\mathbf{z}^{\dagger})) \geq N_0(t-1), \\ &and \;\; diag(\mathbf{X}) \leq \mathbf{p}, \quad and \quad \mathbf{X} \succeq 0 \end{aligned} \tag{4.35}$$

is feasible, then we have $t_{\max} \geq t$. Conversely, if the convex feasibility optimization problem (4.35) is not feasible, then we conclude $t_{\max} < t$. Therefore, we can check whether the optimal value $t_{\max}$ of the quasiconvex optimization problem in (4.34) is smaller than or greater than a given value t by solving the convex feasibility problem (4.35). If the convex feasibility problem (4.35) is feasible then we know $t_{\max} \geq t$. If the convex feasibility problem (4.35) is infeasible, then we know that $t_{\max} < t$. Based on this observation, we can use a simple bisection algorithm to solve the quasiconvex optimization problem (4.34) by solving a convex feasibility problem (4.35) at each step. We assume that the problem is feasible, and start with an interval $[l, u]$ known to contain the optimal value $t_{\max}$. We then solve the

convex feasibility problem at its midpoint $t = (l + u)/2$ to determine whether the optimal value is larger or smaller than t. We update the interval accordingly to obtain a new interval. That is, if t is feasible, then we set $l = t$, otherwise, we choose $u = t$ and solve the convex feasibility problem again. This procedure is repeated until the width of the interval is smaller than the given threshold. Note that the technique of using bisection search to solve the SDP feasibility problem is also given in [84]. Once the maximum feasible value for $t_{\max}$ is obtained, one can solve

$$\begin{aligned} &\min_{\mathbf{X}} \quad tr(\mathbf{X}) \\ &s.t \;\; tr(\mathbf{X}(\mathbf{h}\mathbf{h}^{\dagger} - t_{\max}\mathbf{z}\mathbf{z}^{\dagger})) \geq N_0(t_{\max} - 1), \\ &and \;\; diag(\mathbf{X}) \leq \mathbf{p}, \quad and \quad \mathbf{X} \succeq 0 \end{aligned} \tag{4.36}$$

to get the solution $\mathbf{X}_{opt}$. (4.36) is a convex problem which can be solved efficiently using interior-point based methods.

To solve the convex feasibility problem, one can use the well-studied interior-point based methods as well. We use the well-developed interior point method based package SeDuMi [65], which produces a feasibility certificate if the problem is feasible, and its popular interface Yalmip [47]. In semidefinite relaxation, the solution may not be rank one in general. Interestingly, in our extensive simulation results, we have never encountered a case where the solution $\mathbf{X}_{opt}$ to the SDP problem has a rank higher than one. In fact, there is always a rank one optimal solution for our problem as will be explained later. Therefore, we can obtain our optimal beamforming vector from the principal component of the optimal solution $\mathbf{X}_{opt}$.

4.1.2.2 Second-order Cone Program (SOCP) Approach

The reason that the SDR method is optimal for the above problem is that we can reformulate it as a second order cone problem [72] [12] by ignoring the phase in which we optimize $\mathbf{W}$ directly rather than performing the optimization over $\mathbf{X} = \mathbf{W}\mathbf{W}^{\dagger}$. This provides us with another way of solving the optimization. The optimization problem (4.30) is equivalent to

$$\max_{\mathbf{W},t} \quad t \tag{4.37}$$

$$s.t \ \frac{N_0 + |\mathbf{h}^{\dagger}\mathbf{W}|^2}{N_0 + |\mathbf{z}^{\dagger}\mathbf{W}|^2} \geq t \tag{4.38}$$

$$and \quad |\mathbf{W}|^2 \leq \mathbf{p}.$$

Note that (4.38) can be written as

$$\frac{1}{t}|\mathbf{h}^{\dagger}\mathbf{W}|^2 \geq \left\| \begin{pmatrix} \mathbf{z}^{\dagger}\mathbf{W} \\ \sqrt{\left(1 - \frac{1}{t}\right) N_0} \end{pmatrix} \right\|^2 = |\mathbf{z}^{\dagger}\mathbf{W}|^2 + \left(1 - \frac{1}{t}\right) N_0. \tag{4.39}$$

where the equality on the right hand side of (4.39) follows from the definition of the magnitude-square of a vector. The equivalence of (4.38) and (4.39) can easily be seen by rearranging the terms in (4.39). In the above formulation, we have implicitly assumed that $t \geq 1$. Note that this assumption does not lead to loss of generality as we are interested in cases in which $\frac{N_0+|\mathbf{h}^{\dagger}\mathbf{W}|^2}{N_0+|\mathbf{z}^{\dagger}\mathbf{W}|^2} > 1$. If this ratio is less than 1, the secrecy rate, as discussed before, is zero.

Observe that an arbitrary phase rotation can be added to the beamforming vector without affecting the constraint in (4.38). Thus, $\mathbf{h}^{\dagger}\mathbf{W}$ can be chosen to be real without loss of generality. We can take the square root of both sides of (4.39).

The constraint becomes a second-order cone constraint, which is convex. The optimization problem now becomes

$$\begin{aligned} &\max_{\mathbf{W},t} \quad t \\ &s.t \quad \sqrt{\frac{1}{t}}\mathbf{h}^{\dagger}\mathbf{W} \geq \left\| \begin{pmatrix} \mathbf{z}^{\dagger}\mathbf{W} \\ \sqrt{\left(1-\frac{1}{t}\right)N_0} \end{pmatrix} \right\| \text{ and } \ |\mathbf{W}|^2 \leq \mathbf{p}. \end{aligned} \tag{4.40}$$

As described in the SDR approach, the optimal solution of (4.40) can be obtained by repeatedly checking the feasibility and using a bisection search over t with the aid of interior point methods for second order cone program. Again, we use SeduMi together with Yalmip in our simulations. Once the maximum feasible value $t_{\max}$ is obtained, we can then solve the following second order cone problem (SOCP) to obtain the optimal beamforming vector:

$$\begin{aligned} &\min_{\mathbf{W}} \quad ||\mathbf{W}||^2 \\ &s.t \quad \sqrt{\frac{1}{t_{\max}}}\mathbf{h}^{\dagger}\mathbf{W} \geq \left\| \begin{pmatrix} \mathbf{z}^{\dagger}\mathbf{W} \\ \sqrt{\left(1-\frac{1}{t_{\max}}\right)N_0} \end{pmatrix} \right\| \text{ and } \ |\mathbf{W}|^2 \leq \mathbf{p}. \end{aligned} \tag{4.41}$$

Thus, we can get the secrecy rate $R_{s,ind}$ for the second-hop relay beamforming system under individual power constraints employing the above two numerical optimization methods. Then, combined with the first-hop source relay link rate R_1, secrecy rate of the decode and forward collaborative relay beamforming system becomes $R_{dof,ind} = \min(R_1, R_{s,ind})$.

4.1.2.3 Simplified Suboptimal Design

As shown above, the design of the beamformer under individual relay power constraints requires an iterative procedure in which, at each step, a convex feasibility problem is solved. We now propose a suboptimal beamforming vector that can be obtained without significant computational complexity.

We choose a simplified beamformer as $\mathbf{W}_{sim} = \theta \mathbf{W}_{opt}$ where $\mathbf{W}_{opt}$ is given by (5.20) with $||\mathbf{W}_{opt}||^2 = P_T = \sum p_i$ where p_i is the individual power constraint for the i^{th} relay, and we choose

$$\theta = \frac{1}{|w_{opt,k}|/\sqrt{p_k}} \tag{4.42}$$

where $w_{opt,k}$ and p_k are the kth entries of $\mathbf{W}_{opt}$ and $\mathbf{p}$ respectively, and we choose k as

$$k = \arg \max_{1 \leq i \leq M} \frac{|w_{opt,i}|^2}{p_i} \tag{4.43}$$

Substituting this beamformer $\mathbf{w}_{sim}$ into (4.8), we get the achievable suboptimal rate under individual power constraints.

4.2 Amplify-and-Forward Relaying

Another common relaying scheme in practice is amplify-and-forward relaying. In this scenario, the received signal at the m^{th} relay R_m is directly multiplied by $l_m w_m$ without decoding, and forwarded to D. The relay output can be written as

$$x_{r,m} = w_m l_m (g_m x_s + \eta_m). \tag{4.44}$$

The scaling factor,

$$l_m = \frac{1}{\sqrt{|g_m|^2 P_s + N_m}}, \tag{4.45}$$

is used to ensure $E[|x_{r,m}|^2] = |w_m|^2$. The received signals at the destination D and eavesdropper E are the superposition of the messages sent by the relays. These received signals are expressed, respectively, as

$$y_d = \sum_{m=1}^{M} h_m w_m l_m (g_m x_s + \eta_m) + n_0, \text{ and} \tag{4.46}$$

$$y_e = \sum_{m=1}^{M} z_m w_m l_m (g_m x_s + \eta_m) + n_1. \tag{4.47}$$

Now, it is easy to compute the received SNR at D and E as

$$\Gamma_d = \frac{|\sum_{m=1}^{M} h_m g_m l_m w_m|^2 P_s}{\sum_{m=1}^{M} |h_m|^2 l_m^2 |w_m|^2 N_m + N_0}, \text{ and} \tag{4.48}$$

$$\Gamma_e = \frac{|\sum_{m=1}^{M} z_m g_m l_m w_m|^2 P_s}{\sum_{m=1}^{M} |z_m|^2 l_m^2 |w_m|^2 N_m + N_0}. \tag{4.49}$$

The secrecy rate is now given by

$$R_s = I(x_s; y_d) - I(x_s; y_e) \tag{4.50}$$

$$= \log(1 + \Gamma_d) - \log(1 + \Gamma_e) \tag{4.51}$$

$$= \log \left(\frac{|\sum_{m=1}^{M} h_m g_m l_m w_m|^2 P_s + \sum_{m=1}^{M} |h_m|^2 l_m^2 |w_m|^2 N_m + N_0}{|\sum_{m=1}^{M} z_m g_m l_m w_m|^2 P_s + \sum_{m=1}^{M} |z_m|^2 l_m^2 |w_m|^2 N_m + N_0} \right.$$
$$\left. \times \frac{\sum_{m=1}^{M} |z_m|^2 l_m^2 |w_m|^2 N_m + N_0}{\sum_{m=1}^{M} |h_m|^2 l_m^2 |w_m|^2 N_m + N_0} \right). \tag{4.52}$$

Again, we maximize this term by optimizing $\{w_m\}$ jointly with the aid of perfect CSI. It is obvious that we only have to maximize the term inside the logarithm

function. Let us define

$$\mathbf{h_g} = [h_1^* g_1^* l_1, ..., h_M^* g_M^* l_M]^T, \tag{4.53}$$

$$\mathbf{h_z} = [z_1^* g_1^* l_1, ..., z_M^* g_M^* l_M]^T, \tag{4.54}$$

$$\mathbf{D_h} = \text{Diag}(|h_1|^2 l_1^2 N_1, ..., |h_M|^2 l_M^2 N_M), \text{ and} \tag{4.55}$$

$$\mathbf{D_z} = \text{Diag}(|z_1|^2 l_1^2 N_1, ..., |z_M|^2 l_M^2 N_M). \tag{4.56}$$

Then, the received SNR at the destination and eavesdropper can be reformulated, respectively, as

$$\Gamma_d = \frac{P_s \mathbf{W}^\dagger \mathbf{h_g} \mathbf{h_g}^\dagger \mathbf{W}}{\mathbf{W}^\dagger \mathbf{D_h} \mathbf{W} + N_0} = \frac{P_s tr(\mathbf{h_g} \mathbf{h_g}^\dagger \mathbf{W} \mathbf{W}^\dagger)}{tr(\mathbf{D_h} \mathbf{W} \mathbf{W}^\dagger) + N_0}, \text{ and} \tag{4.57}$$

$$\Gamma_e = \frac{P_s \mathbf{W}^\dagger \mathbf{h_z} \mathbf{h_z}^\dagger \mathbf{W}}{\mathbf{W}^\dagger \mathbf{D_z} \mathbf{W} + N_0} = \frac{P_s tr(\mathbf{h_z} \mathbf{h_z}^\dagger \mathbf{W} \mathbf{W}^\dagger)}{tr(\mathbf{D_z} \mathbf{W} \mathbf{W}^\dagger) + N_0}. \tag{4.58}$$

With these notations, we can write the objective function of the optimization problem as

$$\frac{1+\Gamma_d}{1+\Gamma_e} = \frac{1 + \frac{P_s \mathbf{W}^\dagger \mathbf{h_g} \mathbf{h_g}^\dagger \mathbf{W}}{\mathbf{W}^\dagger \mathbf{D_h} \mathbf{W} + N_0}}{1 + \frac{P_s \mathbf{W}^\dagger \mathbf{h_z} \mathbf{h_z}^\dagger \mathbf{W}}{\mathbf{W}^\dagger \mathbf{D_z} \mathbf{W} + N_0}} \tag{4.59}$$

$$= \frac{\mathbf{W}^\dagger \mathbf{D_h} \mathbf{W} + N_0 + P_s \mathbf{W}^\dagger \mathbf{h_g} \mathbf{h_g}^\dagger \mathbf{W}}{\mathbf{W}^\dagger \mathbf{D_z} \mathbf{W} + N_0 + P_s \mathbf{W}^\dagger \mathbf{h_z} \mathbf{h_z}^\dagger \mathbf{W}} \times \frac{\mathbf{W}^\dagger \mathbf{D_z} \mathbf{W} + N_0}{\mathbf{W}^\dagger \mathbf{D_h} \mathbf{W} + N_0} \tag{4.60}$$

$$= \frac{N_0 + tr((\mathbf{D_h} + P_s \mathbf{h_g} \mathbf{h_g}^\dagger) \mathbf{W} \mathbf{W}^\dagger)}{N_0 + tr((\mathbf{D_z} + P_s \mathbf{h_z} \mathbf{h_z}^\dagger) \mathbf{W} \mathbf{W}^\dagger)} \times \frac{N_0 + tr(\mathbf{D_z} \mathbf{W} \mathbf{W}^\dagger)}{N_0 + tr(\mathbf{D_h} \mathbf{W} \mathbf{W}^\dagger)}. \tag{4.61}$$

If we denote $t_1 = \frac{N_0 + tr((\mathbf{D_h} + P_s \mathbf{h_g} \mathbf{h_g}^\dagger) \mathbf{W} \mathbf{W}^\dagger)}{N_0 + tr((\mathbf{D_z} + P_s \mathbf{h_z} \mathbf{h_z}^\dagger) \mathbf{W} \mathbf{W}^\dagger)}$, $t_2 = \frac{N_0 + tr(\mathbf{D_z} \mathbf{W} \mathbf{W}^\dagger)}{N_0 + tr(\mathbf{D_h} \mathbf{W} \mathbf{W}^\dagger)}$, and use the similar SDR approach as described in the DF case, we can express the optimization

problem as

$$\begin{aligned}
&\max_{\mathbf{X},t_1,t_2} \quad t_1 t_2 \\
&s.t \;\; tr\left(\mathbf{X}\left(\mathbf{D_z} - t_2\mathbf{D_h}\right)\right) \geq N_0(t_2-1) \\
&\quad tr\left(\mathbf{X}\left(\mathbf{D_h} + P_s\mathbf{h_g}\mathbf{h_g}^\dagger - t_1\left(\mathbf{D_z} + P_s\mathbf{h_z}\mathbf{h_z}^\dagger\right)\right)\right) \geq N_0(t_1-1) \\
&and \;\; diag(\mathbf{X}) \leq \mathbf{p}, \;\; (and/or \;\; tr(\mathbf{X}) \leq P_T) \;\; and \;\; \mathbf{X} \succeq 0.
\end{aligned} \tag{4.62}$$

Notice that this formulation is applied to both total relay power constraint and individual relay power constraint which are represented by $tr(\mathbf{X}) \leq P_T$ and $diag(\mathbf{X}) \leq \mathbf{p}$, respectively. When there is only total power constraint, we can easily compute the maximum values of t_1 and t_2 separately since now we have Rayleigh quotient problems. These maximum values are

$$t_{1,u} = \lambda_{max}\left(\mathbf{D_h} + \frac{N_0}{P_T}\mathbf{I} + P_s\mathbf{h_g}\mathbf{h_g}^\dagger, \mathbf{D_z} + \frac{N_0}{P_T}\mathbf{I} + P_s\mathbf{h_z}\mathbf{h_z}^\dagger\right), \tag{4.63}$$

$$t_{2,u} = \lambda_{max}\left(\mathbf{D_z} + \frac{N_0}{P_T}\mathbf{I}, \mathbf{D_h} + \frac{N_0}{P_T}\mathbf{I}\right). \tag{4.64}$$

When there are individual power constraints imposed on the relays, we can use the bisection algorithm similarly as in the DF case to get the maximum values $t_{1,i,u}$ and $t_{2,i,u}$ [2] for t_1 and t_2 by repeatedly solving the following two feasibility problems:

[2]Subscripts i in $t_{1,i,u}$ and $t_{2,i,u}$ are used to denote that these are the maximum values in the presence of individual power constraints.

$$
\begin{aligned}
&find \;\; \mathbf{X} \\
&s.t \;\; tr\left(\mathbf{X}\left(\mathbf{D_h} + P_s\mathbf{h_g}\mathbf{h_g}^\dagger - t_1\left(\mathbf{D_z} + P_s\mathbf{h_z}\mathbf{h_z}^\dagger\right)\right)\right) \geq N_0(t_1 - 1) \\
&and \;\; diag(\mathbf{X}) \leq \mathbf{p}, \quad and \quad \mathbf{X} \succeq 0,
\end{aligned} \tag{4.65}
$$

and

$$
\begin{aligned}
&find \;\; \mathbf{X} \\
&s.t \;\; tr\left(\mathbf{X}\left(\mathbf{D_z} - t_2\mathbf{D_h}\right)\right) \geq N_0(t_2 - 1) \\
&and \;\; diag(\mathbf{X}) \leq \mathbf{p}, \quad and \quad \mathbf{X} \succeq 0.
\end{aligned} \tag{4.66}
$$

Note that for both total and individual power constraints, the maximum values of t_1 and t_2 are obtained separately above, and these values are in general attained by different $\mathbf{X} = \mathbf{W}\mathbf{W}^\dagger$. Now, the following strategy can be used to obtain achievable secrecy rates. For those $\mathbf{X}$ values that correspond to $t_{1,i,u}$ and $t_{1,u}$ (i.e., the maximum t_1 values under individual and total power constraints, respectively), we can compute the corresponding $t_2 = \frac{N_0 + tr(\mathbf{D_z}\mathbf{W}\mathbf{W}^\dagger)}{N_0 + tr(\mathbf{D_h}\mathbf{W}\mathbf{W}^\dagger)}$ and denote them as $t_{2,i,l}$ and $t_{2,l}$ for individual and total power constraints, respectively. Then, $\log(t_{1,i,u}t_{2,i,l})$ and $\log(t_{1,u}t_{2,l})$ will serve as our amplify-and-forward achievable rates for individual and total power constraints, respectively. With the achievable rates, we propose the following algorithm to iteratively search over t_1 and t_2 to get the optimal $t_{1,o}$ and $t_{2,o}$ that maximize the product t_1t_2 by checking following

feasibility problem.

$$
\begin{aligned}
&find \quad \mathbf{X} \succeq 0 \\
&s.t\ tr\left(\mathbf{X}\left(\mathbf{D_z} - t_2\mathbf{D_h}\right)\right) \geq N_0(t_2 - 1) \\
&\ tr\left(\mathbf{X}\left(\mathbf{D_h} + P_s\mathbf{h_g}\mathbf{h_g}^\dagger - t_1\left(\mathbf{D_z} + P_s\mathbf{h_z}\mathbf{h_z}^\dagger\right)\right)\right) \geq N_0(t_1 - 1) \qquad (4.67) \\
&and\ \ tr(\mathbf{X}) \leq P_T \quad \text{if there is total power constraint,} \\
&or\ \ diag(\mathbf{X}) \leq \mathbf{p} \ \text{ if there is individual power constraint.}
\end{aligned}
$$

4.2.1 Proposed Algorithm

Define the resolution $\Delta t = \frac{t_{1,u}}{N}$ or $\Delta t = \frac{t_{1,i,u}}{N}$ for some large N for total and individual power constraints, respectively.

1. Initialize $t_{1,o} = t_{1,u}$, $t_{2,o} = t_{2,l}$ when total power constraint is imposed, and $t_{1,o} = t_{1,i,u}$, $t_{2,o} = t_{2,i,l}$ when individual power constraint is imposed. Initialize the iteration index $i = N$.

2. Set $t_1 = i\Delta t$. If $t_1 t_{2,u} < t_{1,o}t_{2,o}$ (total power constraint) or $t_1 t_{2,i,u} < t_{1,o}t_{2,o}$ (individual power constraint), then go to Step (3). Otherwise,

   a) Let $t_2 = \frac{t_{1,o}t_{2,o}}{t_1}$. Check the feasibility problem (4.67). If it is infeasible, $i = i - 1$ go to step (2). If it is feasible, use the bisection algorithm in (4.67) with t_1 to get the maximum possible values of t_2 and denote this maximum as $t_{2,m}$. The initial interval in the above bisection algorithm can be chosen as $[\frac{t_{1,o}t_{2,o}}{t_1}, t_{2,u}]$ or $[\frac{t_{1,o}t_{2,o}}{t_1}, t_{2,i,u}]$ depending on the power constraints.

   b) Update $t_{1,o} = t_1$, $t_{2,o} = t_{2,m}$, $i = i - 1$. Go back to step (2).

3. Solve the following problem to get the optimal $\mathbf{X}$

$$\begin{aligned}
&\min_{\mathbf{X}} \quad tr(\mathbf{X}) \\
&s.t\ tr\left(\mathbf{X}\left(\mathbf{D_z} - t_{2,o}\mathbf{D_h}\right)\right) \geq N_0(t_{2,o}-1) \\
&\quad tr\left(\mathbf{X}\left(\mathbf{D_h} + P_s\mathbf{h_g}\mathbf{h_g}^{\dagger} - t_{1,o}\left(\mathbf{D_z} + P_s\mathbf{h_z}\mathbf{h_z}^{\dagger}\right)\right)\right) \geq N_0(t_{1,o}-1) \\
&\quad \mathbf{X} \succeq 0 \ \ and \\
&\quad tr(\mathbf{X}) \leq P_T \quad \text{if there is total power constraint,} \\
&\quad diag(\mathbf{X}) \leq \mathbf{p} \ \ \text{if there is individual power constraint.}
\end{aligned} \tag{4.68}$$

4.2.2 Discussion of the Algorithm

Our algorithm is a two-dimensional search over all possible pairs (t_1, t_2), which can produce the greatest product t_1t_2, whose logarithm will be the global maximum value of the secrecy rate. In the following, we will illustrate how our algorithm works for individual power constraints. Similar discussion applies to the total power constraint case as well. The algorithm initiates with the achievable pair $(t_{1,i,u}, t_{2,i,l})$, in which $t_{1,i,u}$ is the maximum feasible value for t_1. Thus, all t_1 values in our search lie in $[0, t_{1,i,u}]$. We chose the resolution parameter N to equally pick N points in this interval. We then use a brute force strategy to check each point iteratively starting from $t_{1,i,u}$ down to 0. In each iteration, the feasibility problem (4.67) is quasi-convex. Thus, we can use the bisection search over t_2 to get the greatest value of t_2. Note that our initial bisection interval for t_2 is $[\frac{t_{1,o}t_{2,o}}{t_1}, t_{2,i,u}]$ where $t_{2,i,u}$ is the maximum feasible value for t_2, and $\frac{t_{1,o}t_{2,o}}{t_1}$ is chosen so that the optimal t_2 we find at the end of the bisection search will produce a product t_1t_2 that is greater than our currently saved optimal $t_{1,o}t_{2,o}$. With this approach, after each iteration, if a t_2 value is found, the new optimal $t_{1,o}t_{2,o}$

will be greater than the previous one. Note that our iteration's stop criterion is $t_1 t_{2,i,u} < t_{1,o} t_{2,o}$. This means that further decrease in the value of t_1 will not produce a product $t_1 t_2$ that is greater than our current $t_{1,o} t_{2,o}$. Thus, the value $t_{1,o} t_{2,o}$ at the end of this algorithm will be the global maximum since we have already checked all possible pairs t_1, t_2 that are candidates for the optimal value.

Again, the optimal $\mathbf{X}$ needs to be of rank-one to determine the beamforming vector. Since we in general have more than two linear constraints depending on the number of relay nodes and since we cannot assume that we have channels with real and positive coefficients, the techniques used in other studies (e.g., [86], [48], and reference therein) are not directly applicable to our setting. Although, we can not prove the rank-one solution analytically, we would like to emphasize that the solutions are rank-one in our simulations. Thus, our numerical result are tight. Also, even when we encounter a solution with rank higher than one, the Gaussian randomization technique is practically proven to be effective in finding a feasible, rank-one approximate solution of the original problem. Details can be found in [48].

4.3 Robust Beamforming Design

All of the beamforming methods discussed heretofore rely on the assumption that the exact knowledge of the channel state information is available for design. However, when the exact CSI is unavailable, the performance of these beamforming techniques may degrade severely. Motivated by this, the problem of robust beamforming design is addressed in [6] and [10]. The robust beamforming for MISO secrecy communications was studied in [83] where the duality between the cognitive radio MISO channel and secrecy MISO channel is exploited to trans-

form the robust design of the transmission strategy over the secrecy channel into a robust cognitive radio beamforming design problem.

We additionally remark that, beside the assumption of perfect channel state information, our previous analysis is applicable only when the relays are fully synchronized at the symbol level. When the time synchronization between the relays is poor, the signal replicas passed through different relays will arrive to the destination node with different delays. This will result in inter-symbol-interference (ISI). To combat such ISI, the authors of [2] view an asynchronous flat-fading relay network as an artificial multipath channel (where each channel path corresponds to one particular relay), and use the orthogonal frequency division multiplexing (OFDM) scheme at the source and destination nodes to deal with this artificial multipath channel. In [11], a filter-and-forward protocol has been introduced for frequency selective relay networks, and several related network beamforming techniques have been developed. In these techniques, the relays deploy finite impulse response (FIR) filters to compensate for the effect of source-to-relay and relay-to-destination channels. Since the relay synchronization problem is out of the scope of this chapter, we will mainly focus on combatting the effect of imperfect channel state information in the following discussion.

Systems robust against channel mismatches can be obtained by two approaches. In most of robust beamforming methods, the perturbation is modeled as a deterministic one with bounded norm which lead to a worst cast optimization. The other approach applied to the case in which the CSI error is unbounded is the statistical approach which provides the robustness in the form of confidence level measured by probability.

Let us consider the DF case. We define $\hat{\mathbf{H}} = \hat{\mathbf{h}}\hat{\mathbf{h}}^{\dagger}$ and $\hat{\mathbf{Z}} = \hat{\mathbf{z}}\hat{\mathbf{z}}^{\dagger}$ as the channel estimators, and $\tilde{\mathbf{H}} = \mathbf{H} - \hat{\mathbf{H}}$ and $\tilde{\mathbf{Z}} = \mathbf{Z} - \hat{\mathbf{Z}}$ as the estimation errors. First, consider

the worst case optimization. In the worst case assumption, $\tilde{\mathbf{H}}$ and $\tilde{\mathbf{Z}}$ are bounded in their Frobenius norm as $||\tilde{\mathbf{H}}|| \leq \epsilon_H$, $||\tilde{\mathbf{Z}}|| \leq \epsilon_Z$, where ϵ_H, ϵ_Z are assumed to be upper bounds of the channel uncertainty. Based on the result of [6], the robust counterpart of previously discussed SDR-based optimization problem can be written as

$$\begin{aligned} &\max_{\mathbf{X},t} \quad t \\ &s.t \;\; tr(\mathbf{X}((\hat{\mathbf{H}} - \epsilon_H \mathbf{I}) - t(\hat{\mathbf{Z}} + \epsilon_Z \mathbf{I})) \geq N_0(t-1), \\ &and \;\; diag(\mathbf{X}) \leq \mathbf{p}, \quad and \quad \mathbf{X} \succeq 0. \end{aligned} \tag{4.69}$$

Note that the total power constraint $tr(\mathbf{X}) \leq P_T$ can be added into the formulation or substituted for the individual power constraint in (4.69). This problem can be solved the same way as discussed before.

However, the worst-case approach requires the norms to be bounded, which is usually not satisfied in practice. Also, this approach is too pessimistic since the probability of the worst-case may be extremely low. Hence, statistical approach is a good alternative in certain scenarios. In our case, we require the probability of the non-outage for secrecy transmission is greater than the predefined threshold ε by imposing

$$Pr\left(\frac{N_0 + tr((\hat{\mathbf{H}} + \tilde{\mathbf{H}})\mathbf{X})}{N_0 + tr((\hat{\mathbf{Z}} + \tilde{\mathbf{Z}})\mathbf{X})} \geq t\right) = Pr\left(tr\left(\mathbf{X}(\hat{\mathbf{H}} + \tilde{\mathbf{H}} - t(\hat{\mathbf{Z}} + \tilde{\mathbf{Z}})\right) \geq N_0(t-1))\right) \geq \varepsilon. \tag{4.70}$$

Now, the optimization problem under imperfect CSI can be expressed as

$$\begin{aligned} &\max_{\mathbf{X},t} \quad t \\ &s.t \;\; Pr\left(tr\left(\mathbf{X}(\hat{\mathbf{H}}+\tilde{\mathbf{H}}-t(\hat{\mathbf{Z}}+\tilde{\mathbf{Z}})\right)\geq N_0(t-1)\right)\right)\geq \varepsilon, \\ &and \;\; diag(\mathbf{X})\leq \mathbf{p} \;\; (or \;\; tr(\mathbf{X})\leq P_T), \quad and \quad \mathbf{X}\succeq 0. \end{aligned} \tag{4.71}$$

If relays are under individual power constraints, we use $diag(\mathbf{X}) \leq \mathbf{p}$. Otherwise, for the case of total power constraint, we use $tr(\mathbf{X}) \leq P_T$. We can also impose both constraints in the optimization.

Note that the distribution of the components of the error matrices $\tilde{\mathbf{H}}$ and $\tilde{\mathbf{Z}}$ depend on the channel estimation technique and distribution of the channel coefficients. In order to simplify the analysis and provide an analytically and numerically tractable approach, we assume that the components of the Hermitian channel estimation error matrices $\tilde{\mathbf{H}}$ and $\tilde{\mathbf{Z}}$ are independent, zero-mean, circularly symmetric, complex Gaussian random variables with variances $\sigma^2_{\tilde{H}}$ and $\sigma^2_{\tilde{Z}}$. Such an assumption is also used in [10]. Now, we can rearrange the probability in the constraint as

$$Pr\left(tr\left((\hat{\mathbf{H}}-t\hat{\mathbf{Z}}+\tilde{\mathbf{H}}-t\tilde{\mathbf{Z}})\mathbf{X}\right)\geq (t-1)N_0)\right). \tag{4.72}$$

Let us define $y = tr\left((\hat{\mathbf{H}}-t\hat{\mathbf{Z}}+\tilde{\mathbf{H}}-t\tilde{\mathbf{Z}})\mathbf{X}\right)$. For given $\mathbf{X}$, $\hat{\mathbf{H}}$, and $\hat{\mathbf{Z}}$, we know from the results of [10] that y is a Gaussian distributed random variable with mean $\mu = tr\left((\hat{\mathbf{H}}-t\hat{\mathbf{Z}})\mathbf{X}\right)$ and variance $\sigma^2_y = (\sigma^2_{\tilde{H}}+t^2\sigma^2_{\tilde{Z}})\,tr(\mathbf{X}\mathbf{X}^{\dagger})$. Then, the non-outage

probability can be written as

$$Pr(y \geq (t-1)N_0) = \int_{(t-1)N_0}^{\infty} \frac{1}{\sqrt{2\pi}\sigma_y} \exp\left(-\frac{(y-\mu)^2}{2\sigma_y^2}\right) \tag{4.73}$$

$$= \frac{1}{2} - \frac{1}{2}\text{erf}\left(\frac{(t-1)N_0 - \mu}{\sqrt{2}\sigma_y}\right) \geq \varepsilon, \tag{4.74}$$

or equivalently as,

$$\frac{(t-1)N_0 - \mu}{\sqrt{2}\sigma_y} \leq \text{erf}^{-1}(-2\varepsilon + 1). \tag{4.75}$$

Note that ε should be close to one for good performance. Thus, both $-2\varepsilon + 1$ and $\frac{(t-1)N_0-\mu}{\sqrt{2}\sigma_y}$ should be negative valued. Note further that we have $tr(\mathbf{X}\mathbf{X}^\dagger) = \|\mathbf{X}\|^2$, and hence $\sigma_y = \sqrt{\sigma_{\tilde{H}}^2 + t^2\sigma_{\tilde{Z}}^2}\|\mathbf{X}\|$. Then, this constraint can be written as

$$\|\mathbf{X}\| \leq \frac{(t-1)N_0 - \mu}{\sqrt{2(\sigma_{\tilde{H}}^2 + t^2\sigma_{\tilde{Z}}^2)}\text{erf}^{-1}(-2\varepsilon + 1)}. \tag{4.76}$$

As a result, the optimization problem becomes

$$\begin{aligned} &\max_{\mathbf{X},t} \quad t \\ &s.t \;\; ||\mathbf{X}|| \leq \frac{(t-1)N_0 - \mu}{\sqrt{2(\sigma_{\tilde{H}}^2 + t^2\sigma_{\tilde{Z}}^2)}\text{erf}^{-1}(-2\varepsilon + 1)}, \\ &and \;\; diag(\mathbf{X}) \leq \mathbf{p}(or \;\; tr(\mathbf{X}) \leq P_T), \quad and \quad \mathbf{X} \succeq 0. \end{aligned} \tag{4.77}$$

Using the same bisection search, we can solve this optimization numerically.

4.4 Numerical Results

We assume that $\{g_m\}$, $\{h_m\}$, $\{z_m\}$ are complex, circularly symmetric Gaussian random variables with zero mean and variances σ_g^2, σ_h^2, and σ_z^2 respectively. We first provide numerical results for decode-and-forward beamforming schemes. In our numerical results, we focus on the performance of second-hop secrecy rate since the main emphasis of this chapter is on the design of the beamforming system in the second-hop. Moreover, each figure is plotted for fixed realizations of the Gaussian channel coefficients. Hence, the secrecy rates in the plots are instantaneous secrecy rates.

In Figures 4.2 and 4.3, we plot the second-hop secrecy rate, which is the maximum secrecy rate that our collaborative relay beamforming system can support under both total and individual relay power constraints. For the case of individual relay power constraints, we assume that the relays have the same power budgets: $p_i = \frac{P_T}{M}$. Specifically, in Fig. 4.2, we have $\sigma_h = 3$, $\sigma_z = 1$, $N_0 = 1$ and $M = 5$. In this case, the legitimate user has a stronger channel. In Fig. 4.3, the only changes are $\sigma_h = 1$ and $\sigma_z = 2$, which imply that the eavesdropper has a stronger channel. Our CRB system can achieve secure transmission even when the eavesdropper has more favorable channel conditions. As can be seen from the figures, the highest secrecy rate is achieved, as expected, under a total transmit power constraint. On the other hand, we observe that only a relatively small rate loss is experienced under individual relay power constraints. Moreover, we note that our two different optimization approaches give nearly the same result. It also can be seen that under individual power constraint, the simple suboptimal method suffers a constant loss as compared to SDR or SOCP based optimal value.

In Fig. 4.4, we fix the relay total transmitting power as $P_T = 10dB$, and vary the

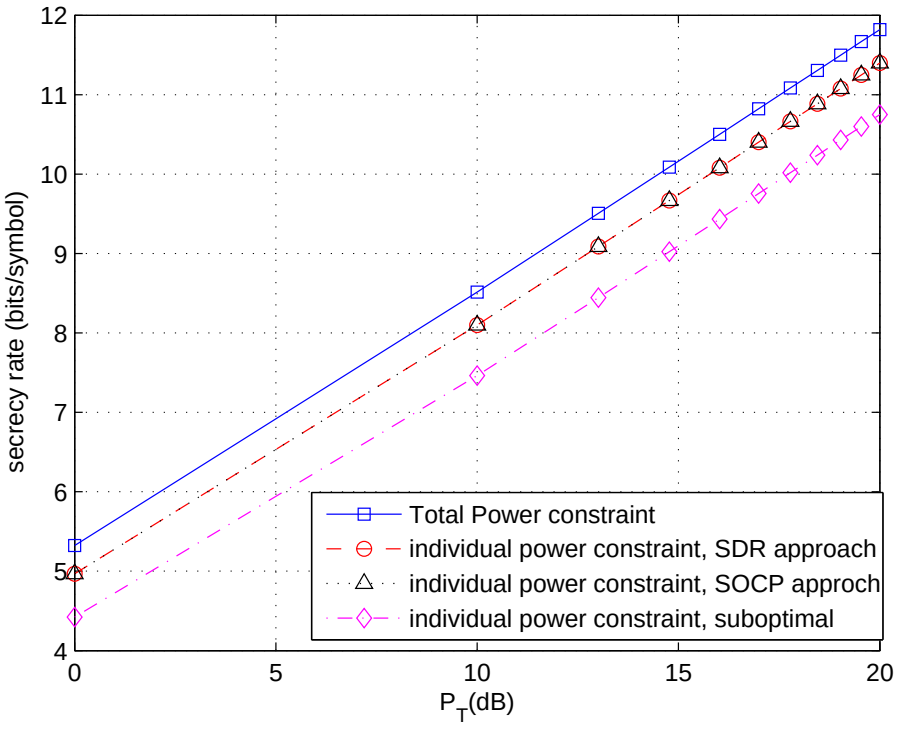

Figure 4.2: DF Second-hop secrecy rate vs. the total relay transmit power P_T for different cases. Eavesdropper has a weaker channel.

number of collaborative relays. Other parameters are the same as those used in Fig. 4.3. We can see that increasing M, increases the secrecy rate under both total and individual power constraints. We also observe that in some cases, increasing M can degrade the performance when our simplified suboptimal beamformer is used.

In Fig. 4.5, we plot the secrecy rate for amplify-and-forward collaborative relay beamforming system for both individual and total power constraints. We also provide the result of suboptimal achievable secrecy rate for comparison. The fixed parameters are $\sigma_g = 10, \sigma_h = 2, \sigma_z = 2$, and $M = 10$. Since the AF secrecy rates depend on both the source and relay powers, the rate curves are plotted as

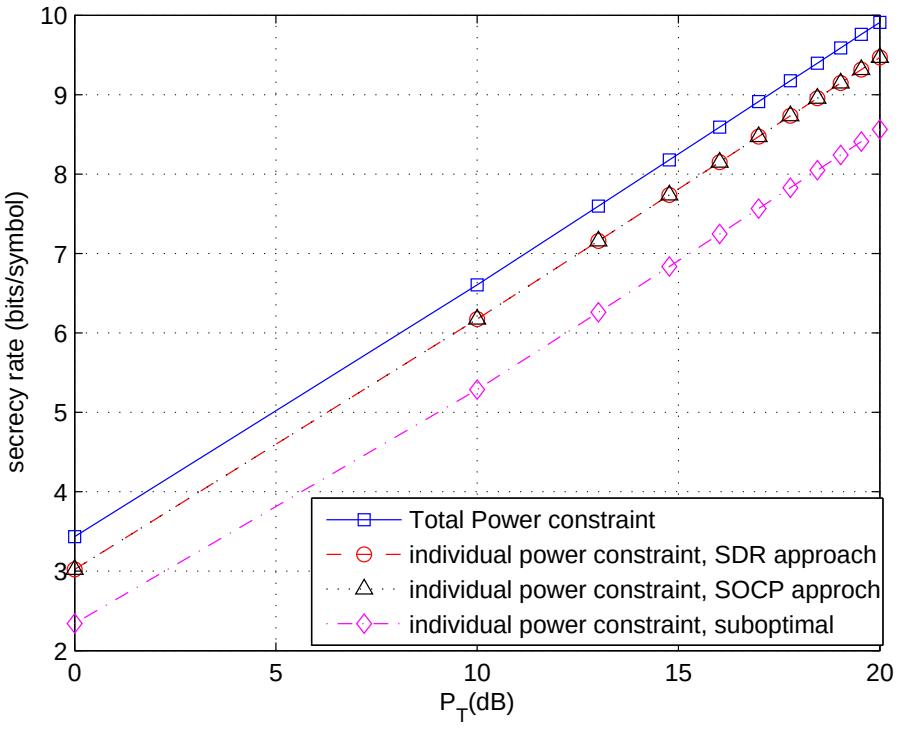

Figure 4.3: DF Second-hop secrecy rate vs. the total relay transmit power P_T for different cases. Eavesdropper has a stronger channel.

a function of P_T/P_s. As before, we assume that the relays have equal powers in the case in which individual power constraints are imposed, i.e., $p_i = P_T/M$. It is immediately seen from the figure that the achievable rates for both total and individual power constraints are very close to the corresponding optimal ones. Thus, the achievable beamforming scheme is a good alternative in the amplify-and-forward relaying case due to the fact that it has much less computational burden. Moreover, we interestingly observe that imposing individual relay power constraints leads to only small losses in the secrecy rates with respect to the case in which we have total relay power constraints.

In Fig. 4.6, we plot the maximum second hop secrecy rate of decode-and-

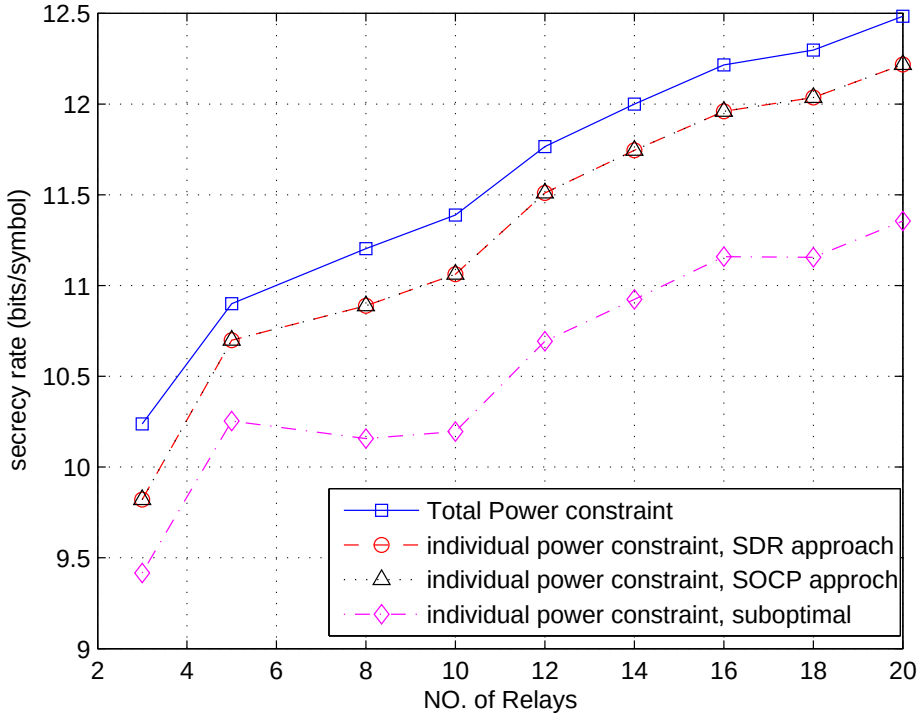

Figure 4.4: DF second-hop secrecy rate vs. number of relays for different cases.

forward that we can achieve for different power P_T and non-outage probability ε values. In this figure, we fix $M = 5$. $\hat{\mathbf{h}}$ and $\hat{\mathbf{z}}$ are randomly picked from Rayleigh fading with $\sigma_{\hat{h}} = 1$ and $\sigma_{\hat{z}} = 2$, and we assume that estimation errors are inversely proportional to P_T. More specifically, in our simulation, we have $\sigma^2_{\tilde{H}} = 0.1/P_T$ and $\sigma^2_{\tilde{Z}} = 0.2/P_T$. We also assume the relays are operating under equal individual power constraints, i.e., $p_i = \frac{P_T}{M}$. It is immediately observed in Fig. 4.6 that smaller rates are supported under higher non-outage probability requirements. In particular, this figure illustrates that our formulation and the proposed optimization framework can be used to determine how much secrecy rate can be supported at what percentage of the time. For instance, at $P_T = 20dB$, we see that approximately 7.4 bits/symbol secrecy rate can be attained 70

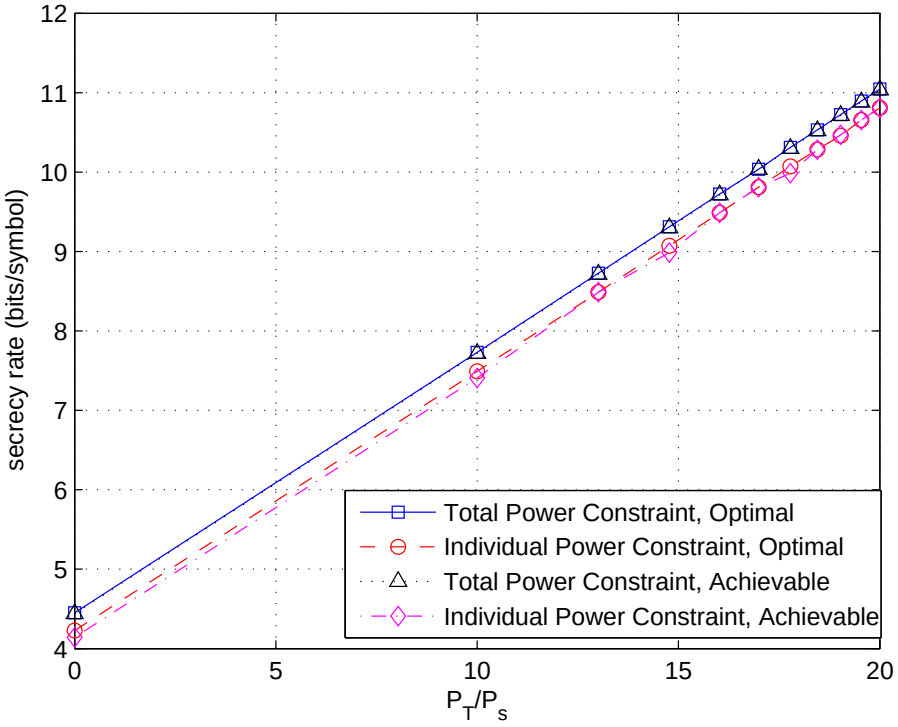

Figure 4.5: AF secrecy rate vs. P_T/P_s. $\sigma_g = 10, \sigma_h = 2, \sigma_z = 2, M = 10$.

percent of the time (i.e., $\varepsilon = 0.7$) while supported secrecy rate drops to about 6.2 bits/symbol when $\varepsilon = 0.95$.

4.5 Conclusion

In this chapter, collaborative beamforming for both DF and AF relaying is studied under secrecy constraints. Optimal beamforming designs that maximize secrecy rates are provided under both total and individual relay power constraints. For DF with total power constraint, we have remarked that the optimal beamforming vector is the solution of a Rayleigh quotient problem. We have further identified the beamforming structure in the high- and low-SNR regimes. For DF with

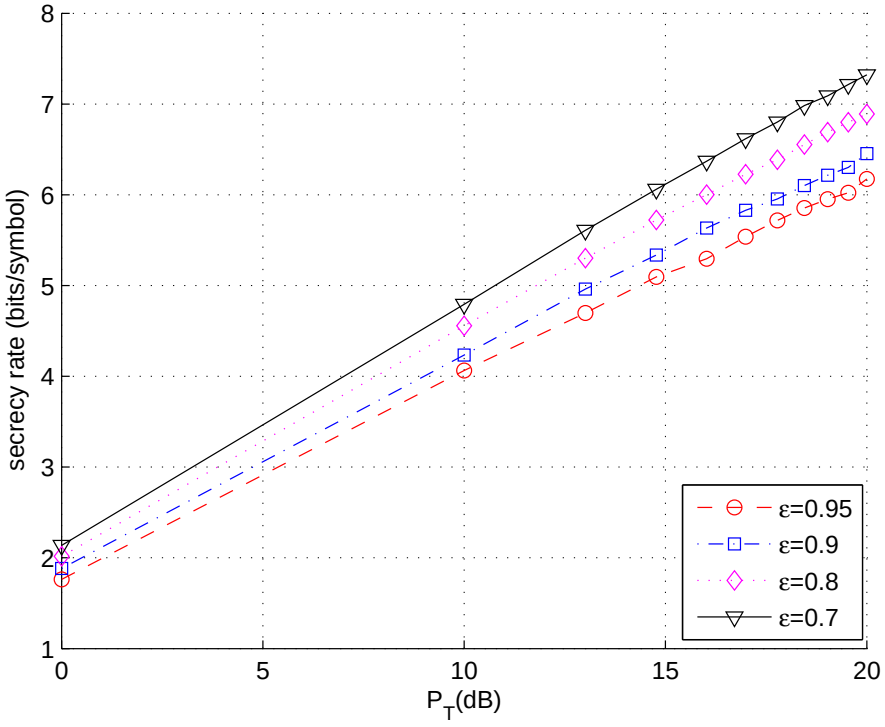

Figure 4.6: DF second secrecy rate vs. P_T under different ε.

individual relay power constraints and AF with both total and individual relay power constraints, we have formulated the problem as a semidefinite programming problem and provided an optimization framework. We have also provided an alternative SOCP method to solve the DF relaying with individual power constraints. In addition, for DF relaying, we have described the worst-case robust beamforming design when CSI is imperfect but bounded, and the statistical robust beamforming design based upon minimum non-outage probability criterion. Finally, we have provided numerical results to illustrate the performance of beamforming techniques under different assumptions, e.g., DF and AF relaying, total and individual relay power constraints, perfect and imperfect channel information.

Chapter 5

Collaborative Relay Beamforming for Secure Broadcasting

In this chapter, we study the relay-aided secure broadcasting scenario. We assume that the source has two independent messages, each of which is intended for one of the receivers but needs to be kept asymptotically perfectly secret from the other. This is achieved via relay node cooperation in decode and forward fashion to produce virtual beam points to two receivers. The problem is formulated as a problem of designing the relay node weights in order to maximize the secrecy rate for both receivers for a fixed total relay power. We assume that the global channel state information (CSI) is available for weight design. Due to the difficulty of the general optimization problem, we propose null space beamforming transmission schemes and compare their performance with the outer bound secrecy rate region.

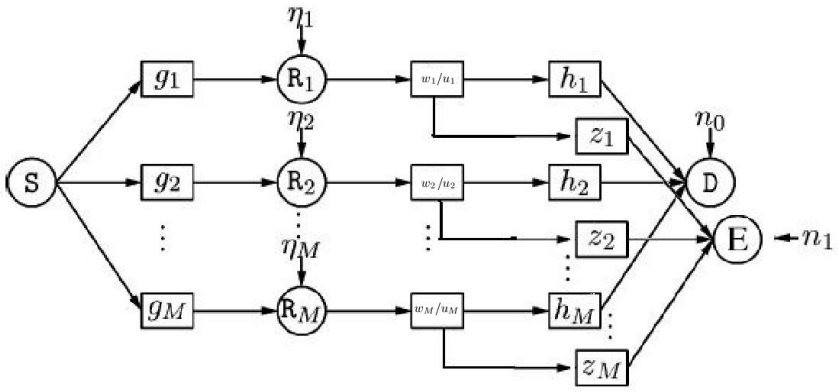

Figure 5.1: Channel Model

5.1 Channel

We consider a communication channel with a source S, two destination nodes D and E, and M relays $\{R_m\}_{m=1}^{M}$ as depicted in Figure 5.1. We assume that there is no direct link between S and D, and S and E. We also assume that relays work synchronously and multiply the signals to be transmitted by complex weights to produce virtual beam points to D and E. We denote the channel fading coefficient between S and R_m as $g_m \in \mathbb{C}$, the channel fading coefficient between R_m and D as $h_m \in \mathbb{C}$, and the channel coefficient between R_m and E as $z_m \in \mathbb{C}$. In this model, the source S tries to transmit confidential messages to D and E with the help of the relays . It is obvious that our channel is a two hop relay network. In the first hop, the source S transmits x_s which contains the confidential messages intended for both D and E to the relays with power $E[|x_s|^2] = P_s$. The received signal at

relay R_m is given by

$$y_{r,m} = g_m x_s + \eta_m \tag{5.1}$$

where η_m is the background noise that has a Gaussian distribution with zero mean and a variance of N_m.

In the first hop, the secrecy rates for destination D and E lie in the following triangle region.

$$R_d \geq 0 \text{ and } R_e \geq 0 \tag{5.2}$$

$$R_d + R_e \leq \min_{m=1,\ldots,M} \log\left(1 + \frac{|g_m|^2 P_s}{N_m}\right) \tag{5.3}$$

where R_d and R_e denote the secrecy rates for destination D and E, respectively.

5.2 Relay Beamforming

We consider the scenario in which relays are much more closer to the source than the destinations, and hence, the first-hop rate does not become a bottleneck of the whole system. Due to this assumption, we in the following focus on characterizing the secrecy rate region of the second-hop. We consider the decode-and-forward relaying protocol in which each relay R_m first decodes the message x_s,and subsequently scales the decoded messages to obtain $x_r = w_m x_d + u_m x_e$, where w_m and u_m are the weight values. x_d and x_e are independent, zero-mean, unit-variance Gaussian signals which include the confidential messages to D and

E, respectively. Under these assumptions, the output power of relay R_m is

$$E[|x_r|^2] = E[|w_m x_d + u_m x_e|^2] = |w_m|^2 + |u_m|^2 \tag{5.4}$$

The received signals at the destination nodes D and E are the superpositions of the signals transmitted from the relays. These signals can be expressed, respectively, as

$$\begin{aligned} y_d &= \sum_{m=1}^{M} h_m w_m x_d + \sum_{m=1}^{M} h_m u_m x_e + n_0 \\ &= \mathbf{h}^\dagger \mathbf{W} x_d + \mathbf{h}^\dagger \mathbf{u} x_e + n_0 \end{aligned} \tag{5.5}$$

$$\begin{aligned} y_e &= \sum_{m=1}^{M} z_m w_m x_d + \sum_{m=1}^{M} z_m u_m x_e + n_1 \\ &= \mathbf{z}^\dagger \mathbf{W} x_d + \mathbf{z}^\dagger \mathbf{u} x_e + n_1 \end{aligned} \tag{5.6}$$

where n_0 and n_1 are the Gaussian background noise components at D and E, respectively, with zero mean and variance N_0. Additionally, we have above defined $\mathbf{h} = [h_1^*, ...h_M^*]^T, \mathbf{z} = [z_1^*, ...z_M^*]^T$, $\mathbf{W} = [w_1, ...w_M]^T$, and $\mathbf{u} = [u_1, ...u_M]^T$. In these notations, while superscript $*$ denotes the conjugate operation, $(\cdot)^T$ and $(\cdot)^\dagger$ denote the transpose and conjugate transpose , respectively, of a matrix or vector. From the transmitting and receiving relationship in (5.5) and (5.6), we can see that the channel we consider can be treated as an interference channel with secrecy constraints studied in [45]. The achievable secrecy rate region is shown to

be

$$0 \leq R_d \leq \log\left(1 + \frac{|\sum_{m=1}^{M} h_m w_m|^2}{N_0 + |\sum_{m=1}^{M} h_m u_m|^2}\right) - \log\left(1 + \frac{|\sum_{m=1}^{M} z_m w_m|^2}{N_0}\right) \tag{5.7}$$

$$0 \leq R_e \leq \log\left(1 + \frac{|\sum_{m=1}^{M} z_m u_m|^2}{N_0 + |\sum_{m=1}^{M} z_m w_m|^2}\right) - \log\left(1 + \frac{|\sum_{m=1}^{M} h_m u_m|^2}{N_0}\right). \tag{5.8}$$

In this chapter, we address the joint optimization $\{w_m\}$ and $\{u_m\}$ with the aid of perfect CSI, and hence identify the optimal collaborative relay beamforming (CRB) direction that maximizes the secrecy rate region given by (5.7) and (5.8). Since the optimization problem above is in general intractable, we investigate suboptimal schemes.

5.2.1 Single Null Space Beamforming

In this scheme, we choose one user's (e.g., E) beamforming vector (e.g., $\mathbf{u}$) to lie in the null space of the other user's channel. With this assumption, we eliminate the user E's interference on D and hence D's capability of eavesdropping on E. Mathematically, this is equivalent to $|\sum_{m=1}^{M} h_m u_m|^2 = \mathbf{h}^\dagger \mathbf{u} = 0$, which means $\mathbf{u}$ is in the null space of $\mathbf{h}^\dagger$.

We further assume α fraction of total relay transmitting power P_r is used for sending confidential message to D. Under these assumptions, we can solve the optimization problem to get maximum R_d . The maximum R_d can be computed

as

$$
\begin{aligned}
& R_{d,m}(\mathbf{h}, \mathbf{z}, P_r, \alpha) \\
&= \max_{\mathbf{W}^\dagger \mathbf{W} \leq \alpha P_r} \log \frac{N_0 + |\sum_{m=1}^{M} h_m w_m|^2}{N_0 + |\sum_{m=1}^{M} z_m w_m|^2} && (5.9) \\
&= \log \max_{\mathbf{W}^\dagger \mathbf{W} \leq \alpha P_R} \frac{N_0 + |\sum_{m=1}^{M} h_m w_m|^2}{N_0 + |\sum_{m=1}^{M} z_m w_m|^2} && (5.10) \\
&= \log \max \frac{\mathbf{W}^\dagger (\frac{N_0}{\alpha P_r} \mathbf{I} + \mathbf{h}\mathbf{h}^\dagger) \mathbf{W}}{\mathbf{W}^\dagger (\frac{N_0}{\alpha P_r} \mathbf{I} + \mathbf{z}\mathbf{z}^\dagger) \mathbf{W}} && (5.11) \\
&= \log \max \frac{\mathbf{W}^\dagger (N_0 \mathbf{I} + \alpha P_r \mathbf{h}\mathbf{h}^\dagger) \mathbf{W}}{\mathbf{W}^\dagger (N_0 \mathbf{I} + \alpha P_r \mathbf{z}\mathbf{z}^\dagger) \mathbf{W}} && (5.12) \\
&= \log \lambda_{max}(N_0 \mathbf{I} + \alpha P_r \mathbf{h}\mathbf{h}^\dagger, N_0 \mathbf{I} + \alpha P_r \mathbf{z}\mathbf{z}^\dagger) && (5.13)
\end{aligned}
$$

Here, we use the fact that (5.12) is the Rayleigh quotient problem, and its maximum value is as given in (5.13) where $\lambda_{max}(\mathbf{A}, \mathbf{B})$ is the largest generalized eigenvalue of the matrix pair $(\mathbf{A}, \mathbf{B})$. Note that we will also use $\lambda_{max}(\cdot)$ to denote largest eigenvalue of the matrix in later discussion. The optimum beamforming weights $\mathbf{W}$ is

$$\mathbf{W}_{opt} = \varsigma \psi_w \tag{5.14}$$

where ψ_w is the eigenvector that corresponds to $\lambda_{max}(N_0 \mathbf{I} + \alpha P_r \mathbf{h}\mathbf{h}^\dagger, N_0 \mathbf{I} + \alpha P_r \mathbf{z}\mathbf{z}^\dagger)$ and ς is chosen to ensure $\mathbf{W}_{opt}^\dagger \mathbf{W}_{opt} = \alpha P_r$.

Now we turn our attention to the maximization of R_e when $\mathbf{W} = \mathbf{W}_{opt}$. Note that $N_0 + |\sum_{m=1}^{M} z_m w_m|^2$ is a constant denoted by N_t, due to the null space constraint, we can write $\mathbf{u} = \mathbf{H}_h^\perp \mathbf{v}$, where $\mathbf{H}_h^\perp$ denotes the projection matrix onto the null space of $\mathbf{h}^\dagger$. Specifically, the columns of $\mathbf{H}_h^\perp$ are orthonormal vectors which form the basis of the null space of $\mathbf{h}^\dagger$. In our case, $\mathbf{H}_h^\perp$ is an $M \times (M-1)$ matrix.

The power constraint $\mathbf{u}^\dagger\mathbf{u} = \mathbf{v}^\dagger{\mathbf{H}_h^\perp}^\dagger\mathbf{H}_h^\perp\mathbf{v} = \mathbf{v}^\dagger\mathbf{v} \leq (1-\alpha)P_r$.

The maximum R_e under this condition can be computed as

$$
\begin{aligned}
& R_{e,m}(\mathbf{h}, \mathbf{z}, P_r, \alpha) \\
&= \max_{\mathbf{u}^\dagger\mathbf{u} \leq (1-\alpha)P_r} \log\left(1 + \frac{|\sum_{m=1}^{M} z_m u_m|^2}{N_t}\right) && (5.15) \\
&= \log\left(1 + \frac{\max_{\mathbf{u}^\dagger\mathbf{u} \leq (1-\alpha)P_r}(\mathbf{u}^\dagger\mathbf{z}\mathbf{z}^\dagger\mathbf{u})}{N_t}\right) && (5.16) \\
&= \log\left(1 + \frac{\max_{\mathbf{v}^\dagger\mathbf{v} \leq (1-\alpha)P_r}(\mathbf{v}^\dagger{\mathbf{H}_h^\perp}^\dagger\mathbf{z}\mathbf{z}^\dagger\mathbf{H}_h^\perp\mathbf{v})}{N_t}\right) && (5.17) \\
&= \log\left(1 + \frac{(1-\alpha)P_r\lambda_{max}({\mathbf{H}_h^\perp}^\dagger\mathbf{z}\mathbf{z}^\dagger\mathbf{H}_h^\perp)}{N_t}\right) && (5.18) \\
&= \log\left(1 + \frac{(1-\alpha)P_r\mathbf{z}^\dagger\mathbf{H}_h^\perp{\mathbf{H}_h^\perp}^\dagger\mathbf{z}}{N_t}\right) && (5.19)
\end{aligned}
$$

The optimum beamforming vector $\mathbf{u}$ is

$$
\mathbf{u}_{opt} = \mathbf{H}_h^\perp\mathbf{v} = \varsigma_1\mathbf{H}_h^\perp{\mathbf{H}_h^\perp}^\dagger\mathbf{z} \tag{5.20}
$$

where ς_1 is a constant introduced to satisfy the power constraint. Hence, secrecy rate region $\mathbb{R}_{s,b}$ achieved with this strategy is

$$
\begin{aligned}
0 \leq R_d &\leq R_{d,m}(\mathbf{h}, \mathbf{z}, P_r, \alpha) \\
0 \leq R_e &\leq R_{e,m}(\mathbf{h}, \mathbf{z}, P_r, \alpha)
\end{aligned} \tag{5.21}
$$

Note that we can switch the role of D and E, and choose $\mathbf{W}$ to be in the null space of $\mathbf{z}^\dagger$. In general, the union of region described in (5.21) and its switched counterpart is the secrecy rate region of single null space beamforming strategy.

5.2.2 Double Null Space Beamforming

In this scheme, we simultaneously choose the beamforming vectors for D and E to lie in the null space of each other's channel vector. That is $|\sum_{m=1}^{M} h_m u_m|^2 = \mathbf{h}^\dagger \mathbf{u} = 0$, and $|\sum_{m=1}^{M} z_m w_m|^2 = \mathbf{z}^\dagger \mathbf{W} = 0$. In this case, the channel reduces to two parallel channels. Since interference is completely eliminated, the secrecy constraint is automatically satisfied. Coding for secrecy is not needed at the relays. The channel input-output relations are

$$y_d = \mathbf{h}^\dagger \mathbf{W} x_d + n_0 \tag{5.22}$$

$$y_e = \mathbf{z}^\dagger \mathbf{u} x_e + n_1 \tag{5.23}$$

Now, we only need to solve the following problems:

$$\max_{\mathbf{W}^\dagger \mathbf{W} \leq \alpha P_r} \log\left(1 + \frac{|\sum_{m=1}^{M} h_m w_m|^2}{N_0}\right) \quad s.t \;\; \mathbf{z}^\dagger \mathbf{W} = 0 \tag{5.24}$$

$$\max_{\mathbf{u}^\dagger \mathbf{u} \leq (1-\alpha) P_r} \log\left(1 + \frac{|\sum_{m=1}^{M} z_m u_m|^2}{N_0}\right) \quad s.t \;\; \mathbf{h}^\dagger \mathbf{u} = 0. \tag{5.25}$$

Similarly as in Section 5.2.1, we can easily find the secrecy rate region $\mathbb{R}_{d,b}$ for double null space beamforming as

$$0 \leq R_d \leq \log\left(1 + \frac{\alpha P_r \mathbf{h}^\dagger \mathbf{H}_z^\perp {\mathbf{H}_z^\perp}^\dagger \mathbf{h}}{N_0}\right) \tag{5.26}$$

$$0 \leq R_e \leq \log\left(1 + \frac{(1-\alpha) P_r \mathbf{z}^\dagger \mathbf{H}_h^\perp {\mathbf{H}_h^\perp}^\dagger \mathbf{z}}{N_0}\right) \tag{5.27}$$

where $\mathbf{H}_z^\perp$ denote the projection matrix onto the null space of $\mathbf{z}^\dagger$ and is defined similarly as $\mathbf{H}_h^\perp$.

5.2.3 TDMA

For comparison, we consider in the second-hop that the relay only transmits secret information to one user at a time and treat the other user as the eavesdropper. We assume that relay uses α fraction of time to transmit x_d where $(1-\alpha)$ fraction of the time is used to transmit x_e. The channel now is the standard Gaussian wiretap channel instead of an interference channel. It can be easily shown that the rate region $\mathbb{R}_{tdma}$ is

$$0 \leq R_d \leq \alpha \log \lambda_{max}(N_0\mathbf{I} + P_r\mathbf{h}\mathbf{h}^\dagger, N_0\mathbf{I} + P_r\mathbf{z}\mathbf{z}^\dagger) \tag{5.28}$$

$$0 \leq R_e \leq (1-\alpha) \log \lambda_{max}(N_0\mathbf{I} + P_r\mathbf{z}\mathbf{z}^\dagger, N_0\mathbf{I} + P_r\mathbf{h}\mathbf{h}^\dagger) \tag{5.29}$$

5.3 Optimality

In this section, we investigate the optimality of our proposed null space beamforming techniques. Although the optimal values of $\mathbf{W}$ and $\mathbf{u}$ that maximize the rate region (5.7) and (5.8) is unknown, we can easily see that the following rate region is an outer bound region of our original achievable secrecy rate region.

$$0 \leq R_d \leq \log\left(1 + \frac{|\sum_{m=1}^{M} h_m w_m|^2}{N_0}\right) - \log\left(1 + \frac{|\sum_{m=1}^{M} z_m w_m|^2}{N_0}\right) \tag{5.30}$$

$$0 \leq R_e \leq \log\left(1 + \frac{|\sum_{m=1}^{M} z_m u_m|^2}{N_0}\right) - \log\left(1 + \frac{|\sum_{m=1}^{M} h_m u_m|^2}{N_0}\right). \tag{5.31}$$

Again, this rate region should be maximized with all possible $\mathbf{W}$ and $\mathbf{u}$ satisfying $||\mathbf{W}||^2 + ||\mathbf{u}||^2 \leq P_r$. From the above expressions, we can see that this outer bound can be interpreted as two simultaneously transmitting wire-tap channels. Fortunately, the optimization problem in this case can be solved analytically. With

the same assumptions as before that $||\mathbf{W}||^2 = \alpha P_r$, $||\mathbf{u}||^2 = (1-\alpha)P_r$, we can easily show that the outer bound secrecy rate region $\mathbb{R}_{outer}$ of our collaborative relay beamforming system is

$$0 \leq R_d \leq \log \lambda_{max}(N_0\mathbf{I} + \alpha P_r \mathbf{h}\mathbf{h}^\dagger, N_0\mathbf{I} + \alpha P_r \mathbf{z}\mathbf{z}^\dagger) \tag{5.32}$$

$$0 \leq R_e \leq \log \lambda_{max}(N_0\mathbf{I} + (1-\alpha) P_r \mathbf{z}\mathbf{z}^\dagger, N_0\mathbf{I} + (1-\alpha) P_r \mathbf{h}\mathbf{h}^\dagger) \tag{5.33}$$

The expression for R_d and R_e here coincide with the secrecy capacity of Gaussian MISO wiretap channel [64] [36] with transmit power levels αP and $(1-\alpha)P$.

5.3.1 Optimality in the High-SNR Regime

In this section, we show that the outer bound region $\mathbb{R}_{outer}$ converges to the proposed null space beamforming regions at high SNR. For the single null space beamforming scheme, the maximum R_d in (5.13) has the same expression as in (5.32), and thus it is automatically optimal. R_e in single null space beamforming has basically the same expression as that of R_e in double null space beamforming with N_0 replaced by N_t. This difference is negligible as P goes infinity. Hence, we focus on double null space beamforming and show that in the high-SNR regime, the $\mathbb{R}_{outer}$ coincide with the double null space region described by (5.26) and (5.27). In the following analysis, for simplicity and without loss of generality, we assume $N_0 = 1$. From the Corollary 4 in Chapter 4 of [36], we can see that

$$\lim_{P_r \to \infty} \frac{1}{P_r} \lambda_{max}(\mathbf{I} + P_r \mathbf{h}\mathbf{h}^\dagger, \mathbf{I} + P_r \mathbf{z}\mathbf{z}^\dagger) = \max_{\tilde{\psi}} |\mathbf{h}^\dagger \tilde{\psi}|^2 \tag{5.34}$$

where $\tilde{\psi}$ is a unit vector on the null space of $\mathbf{z}^\dagger$. Similarly, we can define $\tilde{\psi}_1$ as a unit vector on the null space of $\mathbf{h}^\dagger$. Combining this result with (5.32) and (5.33),

we can express the region $\mathbb{R}_{outer}$ at high SNRs as

$$0 \leq R_d \leq \log(\alpha P_r) + \log(\max_{\tilde{\psi}} |\mathbf{h}^\dagger \tilde{\psi}|^2) + o(1) \tag{5.35}$$

$$0 \leq R_e \leq \log((1-\alpha) P_r) + \log(\max_{\tilde{\psi}_1} |\mathbf{z}^\dagger \tilde{\psi}_1|^2) + o(1) \tag{5.36}$$

where $o(1) \to 0$ as $P_r \to \infty$. On the other hand, double null space beamforming region satisfies

$$0 \leq R_d \leq \max_{\mathbf{W}^\dagger \mathbf{W} \leq \alpha P_r} \log \left(1 + |\sum_{m=1}^{M} h_m w_m|^2\right) \tag{5.37}$$

$$= \log(\alpha P_r) + \log(\max_{\tilde{\psi}} |\mathbf{h}^\dagger \tilde{\psi}|^2) + o(1) \tag{5.38}$$

$$0 \leq R_e \leq \max_{\mathbf{u}^\dagger \mathbf{u} \leq (1-\alpha) P_r} \log \left(1 + |\sum_{m=1}^{M} z_m u_m|^2\right) \tag{5.39}$$

$$= \log((1-\alpha) P_r) + \log(\max_{\tilde{\psi}_1} |\mathbf{z}^\dagger \tilde{\psi}_1|^2) + o(1). \tag{5.40}$$

Above, (5.38) follows from the observation that

$$\lim_{P_r \to \infty} \log \left(1 + |\sum_{m=1}^{M} h_m w_m|^2\right) - \log(\alpha P_r) \tag{5.41}$$

$$= \lim_{P_r \to \infty} \log \left(\frac{1}{\alpha P_r} + \left|\sum_{m=1}^{M} h_m \frac{w_m}{\sqrt{\alpha P_r}}\right|^2\right) \tag{5.42}$$

$$= \log |\mathbf{h}^\dagger \tilde{\psi}|^2 \tag{5.43}$$

where $\tilde{\psi}$ is a unit vector and is in the null space of $\mathbf{z}^\dagger$ because $\mathbf{W}$ is in the null space of $\mathbf{z}^\dagger$. (5.40) follows similarly. Thus, the outer bound secrecy rate region converges to the double null space beamforming region in the high-SNR regime, showing that the null space beamforming strategies are optimal in this regime.

5.3.2 Optimality of TDMA in the Low-SNR Regime

In this section, we consider the limit $P_r \to 0$. In the following steps, the order notation $o(P_r)$ means that $o(P_r)/P_r \to 0$ as $P_r \to 0$.

$$\lambda_{max}(\mathbf{I} + P_r\mathbf{h}\mathbf{h}^\dagger, \mathbf{I} + P_r\mathbf{z}\mathbf{z}^\dagger) \tag{5.44}$$

$$= \lambda_{max}\left((\mathbf{I} + P_r\mathbf{z}\mathbf{z}^\dagger)^{-1}(\mathbf{I} + P_r\mathbf{h}\mathbf{h}^\dagger)\right) \tag{5.45}$$

$$= \lambda_{max}\left((\mathbf{I} - P_r\mathbf{z}\mathbf{z}^\dagger + o(P_r))(\mathbf{I} + P_r\mathbf{h}\mathbf{h}^\dagger)\right) \tag{5.46}$$

$$= \lambda_{max}\left((\mathbf{I} - P_r\mathbf{z}^\dagger\mathbf{z})(\mathbf{I} + P_r\mathbf{h}\mathbf{h}^\dagger)\right) + o(P_r) \tag{5.47}$$

$$= \lambda_{max}\left(\mathbf{I} + P_r(\mathbf{h}\mathbf{h}^\dagger - \mathbf{z}\mathbf{z}^\dagger)\right) + o(P_r) \tag{5.48}$$

$$= 1 + P_r\lambda_{max}(\mathbf{h}\mathbf{h}^\dagger - \mathbf{z}\mathbf{z}^\dagger) + o(P_r) \tag{5.49}$$

Combining this low-SNR approximation with (5.32) and (5.33), we can see that the $\mathbb{R}_{outer}$ at low SNRs is

$$\begin{aligned} 0 \le R_d &\le \log \lambda_{max}(\mathbf{I} + \alpha P_r\mathbf{h}\mathbf{h}^\dagger, \mathbf{I} + \alpha P_r\mathbf{z}\mathbf{z}^\dagger) \\ &= \alpha P_r\lambda_{max}(\mathbf{h}\mathbf{h}^\dagger - \mathbf{z}\mathbf{z}^\dagger) + o(P_r) \end{aligned} \tag{5.50}$$

$$\begin{aligned} 0 \le R_e &\le \log \lambda_{max}(\mathbf{I} + (1-\alpha)P_r\mathbf{z}\mathbf{z}^\dagger, \mathbf{I} + (1 - \alpha P_r)\mathbf{h}\mathbf{h}^\dagger) \\ &= (1-\alpha)P_r\lambda_{max}(\mathbf{z}\mathbf{z}^\dagger - \mathbf{h}\mathbf{h}^\dagger) + o(P_r) \end{aligned} \tag{5.51}$$

Note that (5.50) and (5.51) are also the low-SNR approximations for the TDMA approach. Thus, the TDMA scheme can achieve the optimal rate region in the low-SNR regime. For the completeness, we give the lower SNR approximations for single and double null space beamforming as well. For single null space

beamforming scheme, the low-SNR approximation of (5.21) is

$$0 \leq R_d \leq \alpha P_r \lambda_{max}(\mathbf{h}\mathbf{h}^\dagger - \mathbf{z}\mathbf{z}^\dagger) + o(P_r) \tag{5.52}$$

$$0 \leq R_e \leq (1-\alpha) P_r / N_t \mathbf{z}^\dagger \mathbf{H}_z^\perp \mathbf{H}_z^{\perp\dagger} \mathbf{z} + o(P_r) \tag{5.53}$$

while for the double null space beamforming scheme, low-SNR approximations of (5.26) and (5.27) are

$$0 \leq R_d \leq \alpha P_r \mathbf{h}^\dagger \mathbf{H}_z^\perp \mathbf{H}_z^{\perp\dagger} \mathbf{h} + o(P_r) \tag{5.54}$$

$$0 \leq R_e \leq (1-\alpha) P_r \mathbf{z}^\dagger \mathbf{H}_h^\perp \mathbf{H}_h^{\perp\dagger} \mathbf{z} + o(P_r) \tag{5.55}$$

5.3.3 Optimality when the Number of Relays is Large

It is easy to show that

$$\begin{aligned} \lambda_{max}(\mathbf{I} + \alpha P_r \mathbf{h}\mathbf{h}^\dagger, \mathbf{I} + \alpha P_r \mathbf{z}\mathbf{z}^\dagger) &\leq \lambda_{max}(\mathbf{I} + \alpha P_r \mathbf{h}\mathbf{h}^\dagger) \\ &= 1 + \alpha P_r \mathbf{h}^\dagger \mathbf{h} \end{aligned} \tag{5.56}$$

Now, consider the function

$$1 + \alpha P_r \mathbf{h}^\dagger \mathbf{H}_z^\perp \mathbf{H}_z^{\perp\dagger} \mathbf{h} \tag{5.57}$$

which is inside the log function in the double null space beamforming R_d boundary rate (5.26). In our numerical results, we observe that when M is large and $\mathbf{h}$ and $\mathbf{z}$ are Gaussian distributed (Rayleigh fading environment), (5.56) and (5.57) converge to the same value. Similar results are also noted when R_e in (5.27) is considered. These numerical observations indicate the optimality of null space

beamforming strategies in the regime in which the number of relays, M, is large.

5.4 Simulation Results

In our simulations, we assume $N_m = N_0 = 1$, and $\{g_m\}$, $\{h_m\}$,$\{z_m\}$ are complex, circularly symmetric Gaussian random variables with zero mean and variances σ_g^2, σ_h^2, and σ_z^2 respectively.

In Figures 5.2 and 5.3, we plot the second-hop secrecy rate region of different schemes in which we see $\mathbb{R}_{outer} \supset \mathbb{R}_{s,b} \supset \mathbb{R}_{d,b} \supset \mathbb{R}_{tdma}$. We notice that our proposed suboptimal beamforming region is very close to outer bound secrecy region $\mathbb{R}_{outer}$. Furthermore, the larger the M, the smaller the rate gap between $\mathbb{R}_{outer}$ and our proposed null space beamforming schemes. Also, we note that increasing the number of relays,M, enlarges the rate region. Moreover, we can see that $M = 15$ is sufficient for the null space beamforming schemes to coincide with the $\mathbb{R}_{outer}$.

Next, we examine the null space beamforming's optimality in the high-SNR regime in Fig. 5.4. In this simulation, we can see that when the relay power is large enough, $\mathbb{R}_{outer}$ coincides with the regions of our proposed null space beamforming schemes as expected even M is very small. Finally, in Fig. 5.5 where relay power small, we observe that $\mathbb{R}_{outer}$ coincides with the rate region of the TDMA transmission scheme. Also, we note that the double null space beamforming has better performance than single null space beamforming at some operation points. This is mainly because N_t is no longer negligible at very low SNR values.

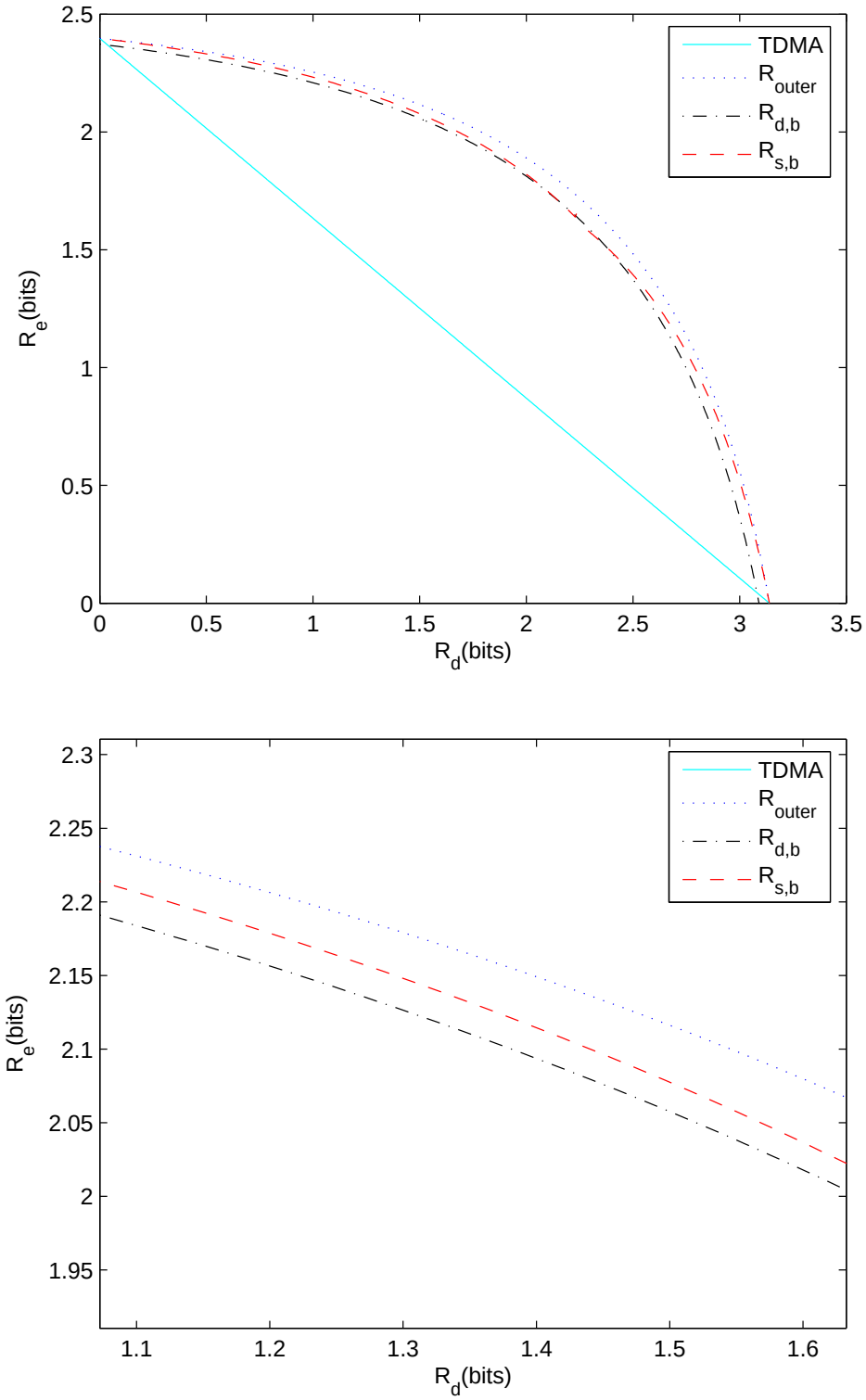

Figure 5.2: Second-hop secrecy rate region $\sigma_h = 2, \sigma_z = 2, P_r = 1, M = 5$. Lower figure provides a zoomed version.

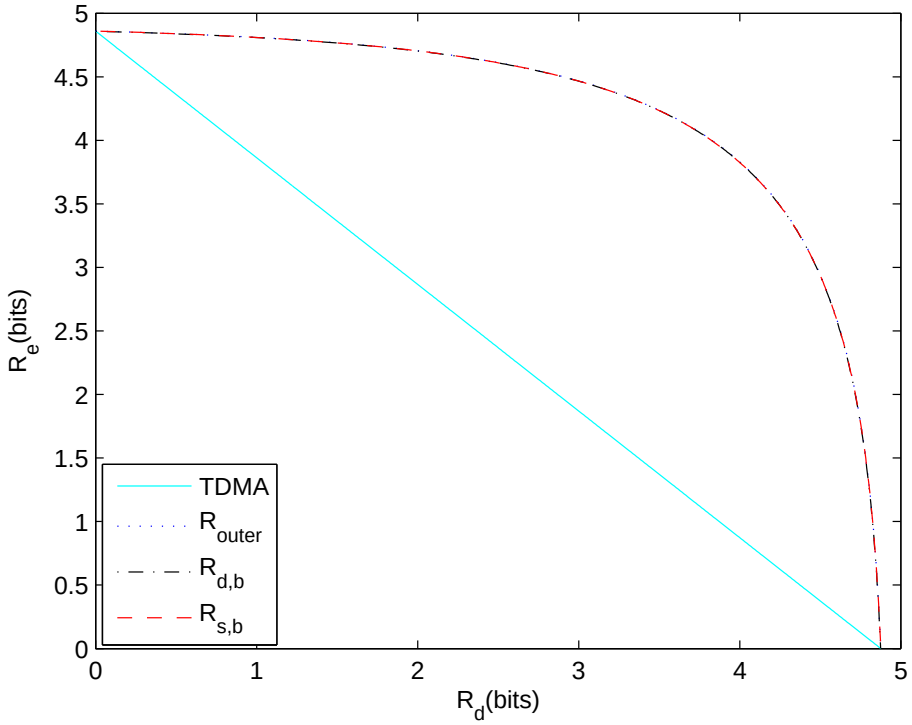

Figure 5.3: Second-hop secrecy rate region $\sigma_h = 2, \sigma_z = 2, P_r = 1, M = 15$

5.5 Conclusion

In this chapter, we have considered a DF-based collaborative relay beamforming protocol to achieve secure broadcasting to two users. As the general optimization of relay weights is a difficult task, we have proposed single and double null space beamforming schemes. We have compared the rate regions of these two schemes and the TDMA scheme with the outer bound secrecy rate region of the original the relay beamforming system. We have analytically shown that null space beamforming schemes are optimal in the high-SNR regime, and TDMA scheme is optimal in the low-SNR regime. In our numerical results, we have seen that our proposed null space beamforming schemes perform in general very close to outer

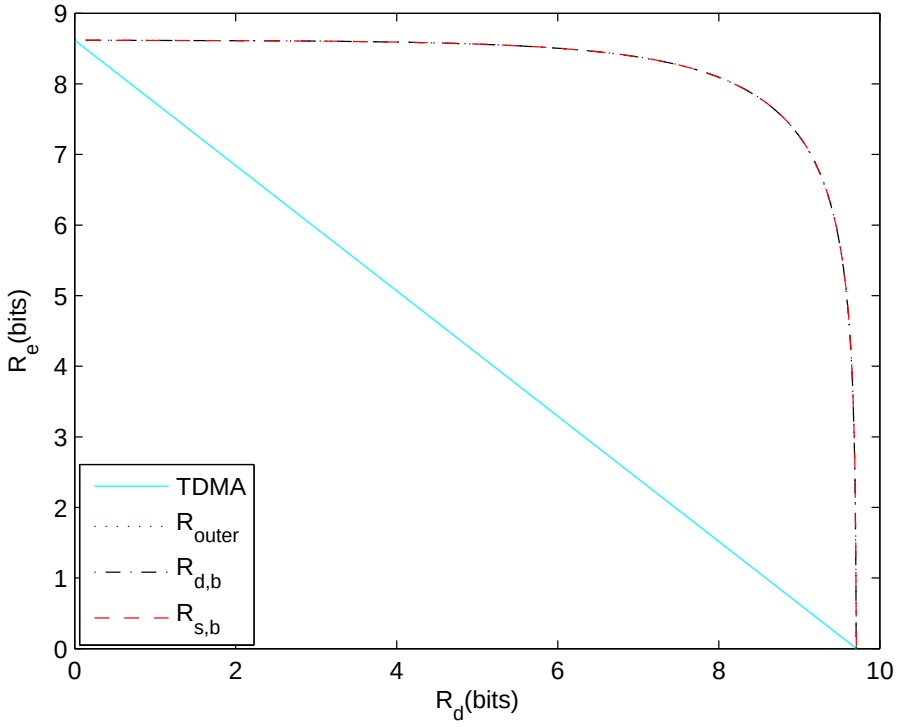

Figure 5.4: Second hop secrecy rate region $\sigma_h = 2, \sigma_z = 2, P_r = 100, M = 3$

bound secrecy rate region. We have numerically shown that when the number of relays is large, the null space beamforming schemes are optimal.

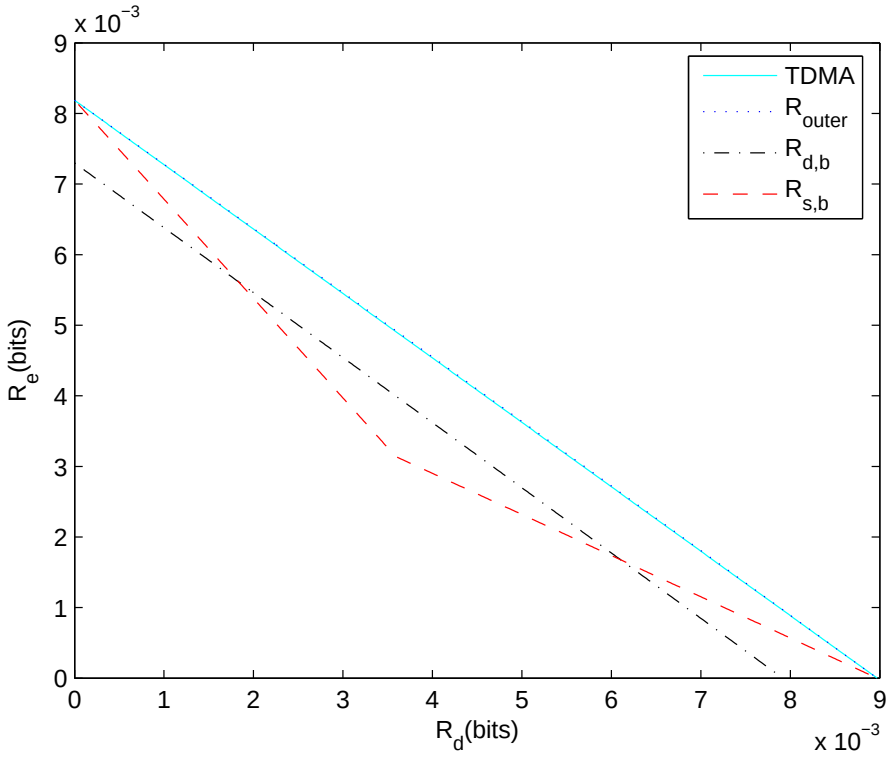

Figure 5.5: Second hop secrecy rate region $\sigma_h = 2, \sigma_z = 2, P_r = 0.001, M = 10$

Chapter 6

Secure Relay Beamforming over Cognitive Radio Channels

In this chapter, we investigate the collaborative relay beamforming under secrecy constraints in the cognitive radio network. We first characterize the secrecy rate of the amplify-and-forward (AF) cognitive relay channel. Then, we formulate the beamforming optimization as a quasiconvex optimization problem which can be solved through convex semidefinite programming (SDP). Furthermore, we propose two sub-optimal null space beamforming schemes to reduce the computational complexity.

6.1 Channel Model

We consider a cognitive relay channel with a secondary user source S, a primary user P, a secondary user destination D, an eavesdropper E, and M relays $\{R_m\}_{m=1}^{M}$, as depicted in Figure 6.1. We assume that there is no direct link between S and D, S and P, and S and E. We also assume that relays work synchronously

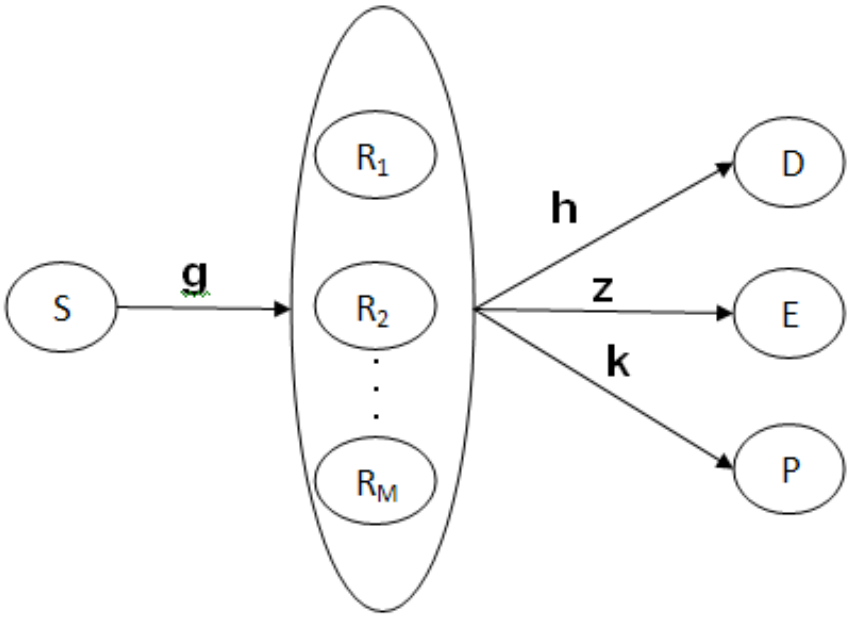

Figure 6.1: Channel Model

to perform beamforming by multiplying the signals to be transmitted with complex weights $\{w_m\}$. We denote the channel fading coefficient between S and R_m by $g_m \in \mathbb{C}$, the fading coefficient between R_m and D by $h_m \in \mathbb{C}$, R_m and P by $k_m \in \mathbb{C}$ and the fading coefficient between R_m and E by $z_m \in \mathbb{C}$. In this model, the source S tries to transmit confidential messages to D with the help of the relays on the same band as the primary user's while keeping the interference on the primary user below some predefined interference temperature limit and keeping the eavesdropper E ignorant of the information. It's obvious that our channel is a two-hop relay network. In the first hop, the source S transmits x_s to relays with

power $E[|x_s|^2] = P_s$. The received signal at the m^{th} relay R_m is given by

$$y_{r,m} = g_m x_s + \eta_m \tag{6.1}$$

where η_m is the background noise that has a Gaussian distribution with zero mean and variance of N_m.

In the AF scenario, the received signal at R_m is directly multiplied by $l_m w_m$ without decoding, and forwarded to D. The relay output can be written as

$$x_{r,m} = w_m l_m (g_m x_s + \eta_m). \tag{6.2}$$

The scaling factor,

$$l_m = \frac{1}{\sqrt{|g_m|^2 P_s + N_m}}, \tag{6.3}$$

is used to ensure $E[|x_{r,m}|^2] = |w_m|^2$. There are two kinds of power constraints for relays. First one is a total relay power constraint in the following form: $||\mathbf{W}||^2 = \mathbf{W}^\dagger \mathbf{W} \leq P_T$ where $\mathbf{W} = [w_1, ...w_M]^T$ and P_T is the maximum total power. $(\cdot)^T$ and $(\cdot)^\dagger$ denote the transpose and conjugate transpose, respectively, of a matrix or vector. In a multiuser network such as the relay system we study in this chapter, it is practically more relevant to consider individual power constraints as wireless nodes generally operate under such limitations. Motivated by this, we can impose $|w_m|^2 \leq p_m \forall m$ or equivalently $|\mathbf{W}|^2 \leq \mathbf{p}$ where $|\cdot|^2$ denotes the element-wise norm-square operation and $\mathbf{p}$ is a column vector that contains the components $\{p_m\}$. p_m is the maximum power for the m^{th} relay node.

The received signals at the destination D and eavesdropper E are the superposition of the messages sent by the relays. These received signals are expressed,

respectively, as

$$y_d = \sum_{m=1}^{M} h_m w_m l_m (g_m x_s + \eta_m) + n_0, \text{ and} \tag{6.4}$$

$$y_e = \sum_{m=1}^{M} z_m w_m l_m (g_m x_s + \eta_m) + n_1 \tag{6.5}$$

where n_0 and n_1 are the Gaussian background noise components with zero mean and variance N_0, at D and E, respectively. It is easy to compute the received SNR at D and E as

$$\Gamma_d = \frac{|\sum_{m=1}^{M} h_m g_m l_m w_m|^2 P_s}{\sum_{m=1}^{M} |h_m|^2 l_m^2 |w_m|^2 N_m + N_0}, \text{ and} \tag{6.6}$$

$$\Gamma_e = \frac{|\sum_{m=1}^{M} z_m g_m l_m w_m|^2 P_s}{\sum_{m=1}^{M} |z_m|^2 l_m^2 |w_m|^2 N_m + N_0}. \tag{6.7}$$

The secrecy rate is now given by

$$R_s = I(x_s; y_d) - I(x_s; y_e) \tag{6.8}$$

$$= \log(1 + \Gamma_d) - \log(1 + \Gamma_e) \tag{6.9}$$

$$= \log \left(\frac{\sum_{m=1}^{M} |z_m|^2 l_m^2 |w_m|^2 N_m + N_0}{\sum_{m=1}^{M} |h_m|^2 l_m^2 |w_m|^2 N_m + N_0} \times \right.$$
$$\left. \frac{|\sum_{m=1}^{M} h_m g_m l_m w_m|^2 P_s + \sum_{m=1}^{M} |h_m|^2 l_m^2 |w_m|^2 N_m + N_0}{|\sum_{m=1}^{M} z_m g_m l_m w_m|^2 P_s + \sum_{m=1}^{M} |z_m|^2 l_m^2 |w_m|^2 N_m + N_0} \right) \tag{6.10}$$

where $I(\cdot;\cdot)$ denotes the mutual information. The interference at the primary user is

$$\Lambda = |\sum_{m=1}^{M} k_m g_m l_m w_m|^2 P_s + \sum_{m=1}^{M} |k_m|^2 l_m^2 |w_m|^2 N_m. \tag{6.11}$$

In this chapter, under the assumption that the relays have perfect channel side

information (CSI), we address the joint optimization of $\{w_m\}$ and hence identify the optimum collaborative relay beamforming (CRB) direction that maximizes the secrecy rate in (6.10) while maintaining the interference on the primary user under a certain threshold, i.e,. $\Lambda \leq \gamma$, where γ is the interference temperature limit.

6.2 Optimal Beamforming

Let us define

$$\mathbf{h_g} = [h_1^* g_1^* l_1, ..., h_M^* g_M^* l_M]^T, \tag{6.12}$$

$$\mathbf{h_z} = [z_1^* g_1^* l_1, ..., z_M^* g_M^* l_M]^T, \tag{6.13}$$

$$\mathbf{h_k} = [k_1^* g_1^* l_1, ..., k_M^* g_M^* l_M]^T, \tag{6.14}$$

$$\mathbf{D_h} = \text{Diag}(|h_1|^2 l_1^2 N_1, ..., |h_M|^2 l_M^2 N_M), \tag{6.15}$$

$$\mathbf{D_z} = \text{Diag}(|z_1|^2 l_1^2 N_1, ..., |z_M|^2 l_M^2 N_M), \text{ and} \tag{6.16}$$

$$\mathbf{D_k} = \text{Diag}(|k_1|^2 l_1^2 N_1, ..., |k_M|^2 l_M^2 N_M) \tag{6.17}$$

where superscript $*$ denotes conjugate operation. Then, the received SNR at the destination and eavesdropper, and the interference on primary user can be written, respectively, as

$$\Gamma_d = \frac{P_s \mathbf{W}^\dagger \mathbf{h_g} \mathbf{h_g}^\dagger \mathbf{W}}{\mathbf{W}^\dagger \mathbf{D_h} \mathbf{W} + N_0}, \tag{6.18}$$

$$\Gamma_e = \frac{P_s \mathbf{W}^\dagger \mathbf{h_z} \mathbf{h_z}^\dagger \mathbf{W}}{\mathbf{W}^\dagger \mathbf{D_z} \mathbf{W} + N_0}, \tag{6.19}$$

$$\Lambda = P_s \mathbf{W}^\dagger \mathbf{h_k} \mathbf{h_k}^\dagger \mathbf{W} + \mathbf{W}^\dagger \mathbf{D_k} \mathbf{W}. \tag{6.20}$$

With these notations, we can write the objective function of the optimization problem (i.e., the term inside the logarithm in (6.10)) as

$$\begin{aligned}\frac{1+\Gamma_d}{1+\Gamma_e} &= \frac{1+\frac{P_s\mathbf{W}^\dagger\mathbf{h_g}\mathbf{h_g}^\dagger\mathbf{W}}{\mathbf{W}^\dagger\mathbf{D_h}\mathbf{W}+N_0}}{1+\frac{P_s\mathbf{W}^\dagger\mathbf{h_z}\mathbf{h_z}^\dagger\mathbf{W}}{\mathbf{W}^\dagger\mathbf{D_z}\mathbf{W}+N_0}} \\ &= \frac{\mathbf{W}^\dagger\mathbf{D_h}\mathbf{W}+N_0+P_s\mathbf{W}^\dagger\mathbf{h_g}\mathbf{h_g}^\dagger\mathbf{W}}{\mathbf{W}^\dagger\mathbf{D_z}\mathbf{W}+N_0+P_s\mathbf{W}^\dagger\mathbf{h_z}\mathbf{h_z}^\dagger\mathbf{W}} \times \frac{\mathbf{W}^\dagger\mathbf{D_z}\mathbf{W}+N_0}{\mathbf{W}^\dagger\mathbf{D_h}\mathbf{W}+N_0} \\ &= \frac{N_0+tr((\mathbf{D_h}+P_s\mathbf{h_g}\mathbf{h_g}^\dagger)\mathbf{W}\mathbf{W}^\dagger)}{N_0+tr((\mathbf{D_z}+P_s\mathbf{h_z}\mathbf{h_z}^\dagger)\mathbf{W}\mathbf{W}^\dagger)} \times \frac{N_0+tr(\mathbf{D_z}\mathbf{W}\mathbf{W}^\dagger)}{N_0+tr(\mathbf{D_h}\mathbf{W}\mathbf{W}^\dagger)}.\end{aligned} \tag{6.21}$$

If we denote $t_1 = \frac{N_0+tr((\mathbf{D_h}+P_s\mathbf{h_g}\mathbf{h_g}^\dagger)\mathbf{W}\mathbf{W}^\dagger)}{N_0+tr((\mathbf{D_z}+P_s\mathbf{h_z}\mathbf{h_z}^\dagger)\mathbf{W}\mathbf{W}^\dagger)}$, $t_2 = \frac{N_0+tr(\mathbf{D_z}\mathbf{W}\mathbf{W}^\dagger)}{N_0+tr(\mathbf{D_h}\mathbf{W}\mathbf{W}^\dagger)}$, define $\mathbf{X} \triangleq \mathbf{W}\mathbf{W}^\dagger$, and employ the semidefinite relaxation approach, we can express the beamforming optimization problem as

$$\begin{aligned}&\max_{\mathbf{X},t_1,t_2} \quad t_1t_2 \\ &s.t \;\; tr\left(\mathbf{X}\left(\mathbf{D_h}+P_s\mathbf{h_g}\mathbf{h_g}^\dagger - t_1\left(\mathbf{D_z}+P_s\mathbf{h_z}\mathbf{h_z}^\dagger\right)\right)\right) \geq N_0(t_1-1) \\ &\quad tr\left(\mathbf{X}\left(\mathbf{D_z}-t_2\mathbf{D_h}\right)\right) \geq N_0(t_2-1) \\ &\quad tr\left(\mathbf{X}\left(\mathbf{D_k}+P_s\mathbf{h_k}\mathbf{h_k}^\dagger\right)\right) \leq \gamma \\ &and \;\; diag(\mathbf{X}) \leq \mathbf{p}, \;\; (and/or \;\; tr(\mathbf{X}) \leq P_T) \;\; and \;\; \mathbf{X} \succeq 0.\end{aligned} \tag{6.22}$$

The optimization problem here is similar to that in [80]. The only difference is that we have an additional constraint due to the interference limitation. Thus, we can use the same optimization framework. The optimal beamforming solution that maximizes the secrecy rate in the cognitive relay channel can be obtained by using semidefinite programming with a two dimensional search for both total and individual power constraints. For simulation, one can use the well-developed interior point method based package SeDuMi [65], which produces a feasibility

certificate if the problem is feasible, and its popular interface Yalmip [47]. It is important to note that we should have the optimal $\mathbf{X}$ to be of rank-one to determine the beamforming vector. While proving analytically the existence of a rank-one solution for the above optimization problem seems to be a difficult task[1], we would like to emphasize that the solutions are rank-one in our simulations. Thus, our numerical result are tight. Also, even in the case we encounter a solution with rank higher than one, the Gaussian randomization technique is practically proven to be effective in finding a feasible, rank-one approximate solution of the original problem. Details can be found in [48].

6.3 Sub-Optimal Null Space Beamforming

Obtaining the optimal solution requires significant computation. To simplify the analysis, we propose suboptimal null space beamforming techniques in this section .

6.3.1 Beamforming in the Null Space of Eavesdropper's Channel (BNE)

We choose $\mathbf{W}$ to lie in the null space of $\mathbf{h_z}$. With this assumption, we eliminate E's capability of eavesdropping on D. Mathematically, this is equivalent to $|\sum_{m=1}^{M} z_m g_m l_m w_m|^2 = |\mathbf{h_z}^\dagger \mathbf{W}|^2 = 0$, which means $\mathbf{W}$ is in the null space of $\mathbf{h_z}^\dagger$. We can write $\mathbf{W} = \mathbf{H}_z^\perp \mathbf{v}$, where $\mathbf{H}_z^\perp$ denotes the projection matrix onto the null space of $\mathbf{h_z}^\dagger$. Specifically, the columns of $\mathbf{H}_z^\perp$ are orthonormal vectors which form

[1]Since we in general have more than two linear constraints depending on the number of relay nodes and since we cannot assume that we have channels with real and positive coefficients, the techniques that are used in several studies to prove the existence of a rank-one solution (see e.g., [86], [48],and references therein) are not directly applicable to our setting.

the basis of the null space of $\mathbf{h_z}^\dagger$. In our case, $\mathbf{H}_z^\perp$ is an $M \times (M-1)$ matrix. The total power constraint becomes $\mathbf{W}^\dagger\mathbf{W} = \mathbf{v}^\dagger{\mathbf{H}_z^\perp}^\dagger\mathbf{H}_z^\perp\mathbf{v} = \mathbf{v}^\dagger\mathbf{v} \leq P_T$. The individual power constraint becomes $|\mathbf{H}_z^\perp\mathbf{v}|^2 \leq \mathbf{p}$

Under the above null space beamforming assumption, Γ_e is zero. Hence, we only need to maximize Γ_d to get the highest achievable secrecy rate. Γ_d is now expressed as

$$\Gamma_d = \frac{P_s\mathbf{v}^\dagger{\mathbf{H}_z^\perp}^\dagger\mathbf{h_g}\mathbf{h_g}^\dagger\mathbf{H}_z^\perp\mathbf{v}}{\mathbf{v}^\dagger{\mathbf{H}_z^\perp}^\dagger\mathbf{D_h}\mathbf{H}_z^\perp\mathbf{v} + N_0}. \tag{6.23}$$

The interference on the primary user can be written as

$$\Lambda = P_s\mathbf{v}^\dagger{\mathbf{H}_z^\perp}^\dagger\mathbf{h_k}\mathbf{h_k}^\dagger\mathbf{H}_z^\perp\mathbf{v} + \mathbf{v}^\dagger{\mathbf{H}_z^\perp}^\dagger\mathbf{D_k}\mathbf{H}_z^\perp\mathbf{v}. \tag{6.24}$$

Defining $\mathbf{X} \triangleq \mathbf{vv}$, we can express the optimization problem as

$$\begin{aligned}
&\max_{\mathbf{X},t} \quad t \\
&\text{s.t} \;\; \text{tr}\left(\mathbf{X}\left(P_s{\mathbf{H}_z^\perp}^\dagger\mathbf{h_g}\mathbf{h_g}^\dagger\mathbf{H}_z^\perp - t{\mathbf{H}_z^\perp}^\dagger\mathbf{D_h}\mathbf{H}_z^\perp\right)\right) \geq N_0 t \\
&\quad tr\left(\mathbf{X}\left({\mathbf{H}_z^\perp}^\dagger\mathbf{D_k}\mathbf{H}_z^\perp + P_s{\mathbf{H}_z^\perp}^\dagger\mathbf{h_k}\mathbf{h_k}^\dagger\mathbf{H}_z^\perp\right)\right) \leq \gamma \\
&\text{and} \;\; \text{diag}(\mathbf{H}_z^\perp\mathbf{X}{\mathbf{H}_z^\perp}^\dagger) \leq \mathbf{p}, (and/or \;\; tr(\mathbf{X}) \leq P_T) \quad and \quad \mathbf{X} \succeq 0.
\end{aligned} \tag{6.25}$$

This problem can be easily solved by semidefinite programming with bisection search [78].

6.3.2 Beamforming in the Null Space of Eavesdropper's and Primary User's Channels (BNEP)

In this section, we choose $\mathbf{W}$ to lie in the null space of $\mathbf{h_z}$ and $\mathbf{h_k}$. Mathematically, this is equivalent to requiring $|\sum_{m=1}^{M} z_m g_m l_m w_m|^2 = |\mathbf{h_z}^\dagger \mathbf{W}|^2 = 0$, and $|\sum_{m=1}^{M} k_m g_m l_m w_m|^2 = |\mathbf{h_k}^\dagger \mathbf{W}|^2 = 0$. We can write $\mathbf{W} = \mathbf{H}_{z,k}^{\perp}\mathbf{v}$, where $\mathbf{H}_{z,k}^{\perp}$ denotes the projection matrix onto the null space of $\mathbf{h_z}^\dagger$ and $\mathbf{h_k}^\dagger$. Specifically, the columns of $\mathbf{H}_{z,k}^{\perp}$ are orthonormal vectors which form the basis of the null space. In our case, $\mathbf{H}_{z,k}^{\perp}$ is an $M \times (M-2)$ matrix. The total power constraint becomes $\mathbf{W}^\dagger\mathbf{W} = \mathbf{v}^\dagger {\mathbf{H}_{z,k}^{\perp}}^\dagger \mathbf{H}_{z,k}^{\perp}\mathbf{v} = \mathbf{v}^\dagger\mathbf{v} \leq P_T$. The individual power constraint becomes $|\mathbf{H}_{z,k}^{\perp}\mathbf{v}|^2 \leq \mathbf{p}$.

With this beamforming strategy, we again have $\Gamma_e = 0$. Moreover, the interference on the primary user is now reduced to

$$\Lambda = \sum_{m=1}^{M} |k_m|^2 l_m^2 |w_m|^2 N_m = \mathbf{v}^\dagger {\mathbf{H}_{z,k}^{\perp}}^\dagger \mathbf{D_k} \mathbf{H}_{z,k}^{\perp}\mathbf{v} \tag{6.26}$$

which is the sum of the forwarded additive noise components present at the relays. Now, the optimization problem becomes

$$\begin{aligned}
&\max_{\mathbf{X},t} \quad t \\
&\text{s.t} \;\; \text{tr}\left(\mathbf{X}\left(P_s {\mathbf{H}_{z,k}^{\perp}}^\dagger \mathbf{h_g}\mathbf{h_g}^\dagger \mathbf{H}_{z,k}^{\perp} - t{\mathbf{H}_{z,k}^{\perp}}^\dagger \mathbf{D_h} \mathbf{H}_{z,k}^{\perp}\right)\right) \geq N_0 t \\
&\quad tr\left(\mathbf{X}\left({\mathbf{H}_{z,k}^{\perp}}^\dagger \mathbf{D_k} \mathbf{H}_{z,k}^{\perp}\right)\right) \leq \gamma \\
&\text{and} \;\; \text{diag}(\mathbf{H}_{z,k}^{\perp}\mathbf{X}{\mathbf{H}_{z,k}^{\perp}}^\dagger) \leq \mathbf{p}, (and/or \;\; tr(\mathbf{X}) \leq P_T) \\
&\text{and} \quad \mathbf{X} \succeq 0.
\end{aligned} \tag{6.27}$$

Again, this problem can be solved through semidefinite programming. With the

following assumptions, we can also obtain a closed-form characterization of the beamforming structure. Since the interference experienced by the primary user consists of the forwarded noise components, we can assume that the interference constraint $\Lambda \leq \gamma$ is inactive unless γ is very small. With this assumption, we can drop this constraint. If we further assume that the relays operate under the total power constraint expressed as $\mathbf{v}^\dagger \mathbf{v} \leq P_T$, we can get the following closed-form solution:

$$\begin{aligned}
&\max_{\mathbf{v}^\dagger \mathbf{v} \leq P_t} \Gamma_d \\
&= \max_{\mathbf{v}^\dagger \mathbf{v} \leq P_t} \frac{P_s \mathbf{v}^\dagger {\mathbf{H}_{z,k}^\perp}^\dagger \mathbf{h_g} \mathbf{h_g}^\dagger \mathbf{H}_{z,k}^\perp \mathbf{v}}{\mathbf{v}^\dagger {\mathbf{H}_{z,k}^\perp}^\dagger \mathbf{D_h} \mathbf{H}_{z,k}^\perp \mathbf{v} + N_0} \\
&= \max_{\mathbf{v}^\dagger \mathbf{v} \leq P_t} \frac{P_s \mathbf{v}^\dagger {\mathbf{H}_{z,k}^\perp}^\dagger \mathbf{h_g} \mathbf{h_g}^\dagger \mathbf{H}_{z,k}^\perp \mathbf{v}}{\mathbf{v}^\dagger \left({\mathbf{H}_{z,k}^\perp}^\dagger \mathbf{D_h} \mathbf{H}_{z,k}^\perp + \frac{N_0}{P_T} \mathbf{I} \right) \mathbf{v}} \\
&= P_s \lambda_{max} \left({\mathbf{H}_{z,k}^\perp}^\dagger \mathbf{h_g} \mathbf{h_g}^\dagger \mathbf{H}_{z,k}^\perp, {\mathbf{H}_{z,k}^\perp}^\dagger \mathbf{D_h} \mathbf{H}_{z,k}^\perp + \frac{N_0}{P_T} \mathbf{I} \right)
\end{aligned}$$

where $\lambda_{\max}(\mathbf{A}, \mathbf{B})$ is the largest generalized eigenvalue of the matrix pair $(\mathbf{A}, \mathbf{B})$ [2]. Hence, the maximum secrecy rate is achieved by the beamforming vector

6.4 Multiple Primary Users and Eavesdroppers

The discussion in Section 6.2 can be easily extended to the case of more than one primary user in the network. Each primary user will introduce an interference constraint $\Gamma_i \leq \gamma_i$ which can be straightforwardly included into (6.22). The beamforming optimization is still a semidefinite programming problem. On the other hand, the results in Section 6.2 cannot be easily extended to

[2] For a Hermitian matrix $\mathbf{A} \in \mathbb{C}^{n \times n}$ and positive definite matrix $\mathbf{B} \in \mathbb{C}^{n \times n}$, (λ, ψ) is referred to as a generalized eigenvalue – eigenvector pair of $(\mathbf{A}, \mathbf{B})$ if (λ, ψ) satisfy $\mathbf{A}\psi = \lambda \mathbf{B}\psi$ [23].

the multiple-eavesdropper scenario. In this case, the secrecy rate for AF relaying is $R_s = I(x_s; y_d) - \max_i I(x_s; y_{e,i})$, where the maximization is over the rates achieved over the links between the relays and different eavesdroppers. Hence, we have to consider the eavesdropper with the strongest channel. In this scenario, the objective function cannot be expressed in the form given in (6.10) and the optimization framework provided in Section 6.2 does not directly apply to the multi-eavesdropper model.

However, the null space beamforming schemes discussed in Section 6.3 can be extended to the case of multiple primary users and eavesdroppers under the condition that the number of relay nodes is greater than the number of eavesdroppers or the total number of eavesdroppers and primary users depending on which null space beamforming is used. The reason for this condition is to make sure the projection matrix $\mathbf{H}^{\perp}$ exists. Note that the null space of i channels in general has the dimension $M \times (M - i)$ where M is the number of relays.

6.5 Numerical Results and Discussion

We assume that $\{g_m\}, \{h_m\}, \{z_m\}, \{k_m\}$ are complex, circularly symmetric Gaussian random variables with zero mean and variances σ_g^2, σ_h^2, σ_z^2 and σ_k^2 respectively. In this section, each figure is plotted for fixed realizations of the Gaussian channel coefficients. Hence, the secrecy rates in the plots are instantaneous secrecy rates.

In Fig. 6.2, we plot the optimal secrecy rates for the amplify-and-forward collaborative relay beamforming system under both individual and total power constraints. We also provide, for comparison, the secrecy rates attained by using the suboptimal beamforming schemes. The fixed parameters are $\sigma_g = 10, \sigma_h = 1, \sigma_z = 1, \sigma_k = 1, \gamma = 0dB$, and $M = 10$. Since AF secrecy rates depend on both the

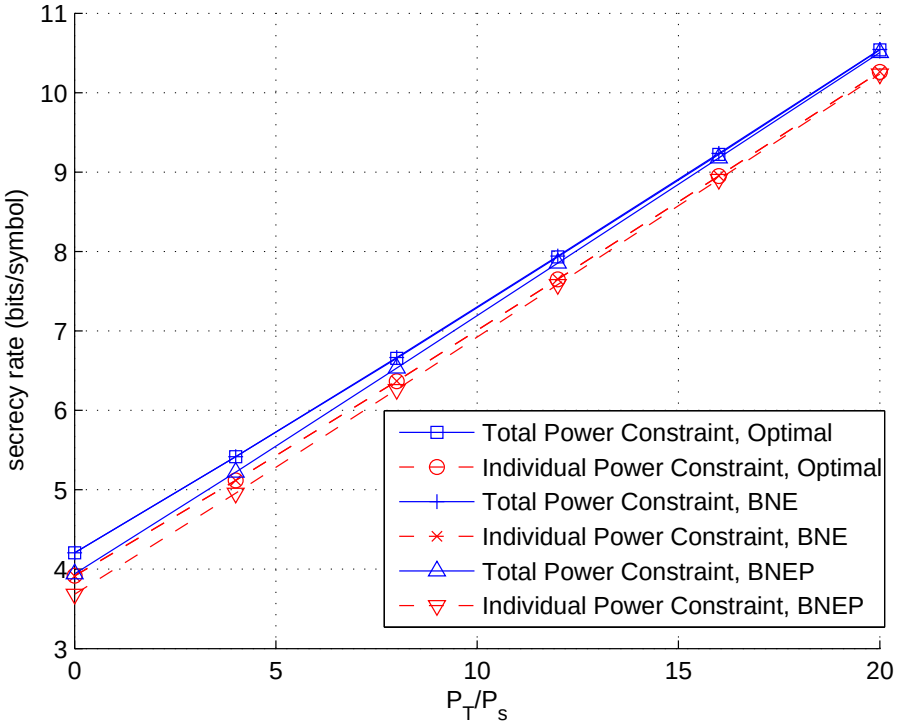

Figure 6.2: AF secrecy rate vs. P_T/P_s. $\sigma_g = 10, \sigma_h =, \sigma_z = 1, \sigma_k = 1, M = 10, \gamma = 0dB$.

source and relay powers, the rate curves are plotted as a function of P_T/P_s. We assume that the relays have equal powers in the case in which individual power constraints are imposed, i.e., $p_i = P_T/M$. It is immediately seen from the figure that the suboptimal null space beamforming achievable rates under both total and individual power constraints are very close to the corresponding optimal ones. Especially, they are nearly identical in the high SNR regime, which suggests that null space beamforming is optimal at high SNRs. Thus, null space beamforming schemes are good alternatives as they are obtained with much less computational burden. Moreover, we interestingly observe that imposing individual relay power constraints leads to small losses in the secrecy rates.

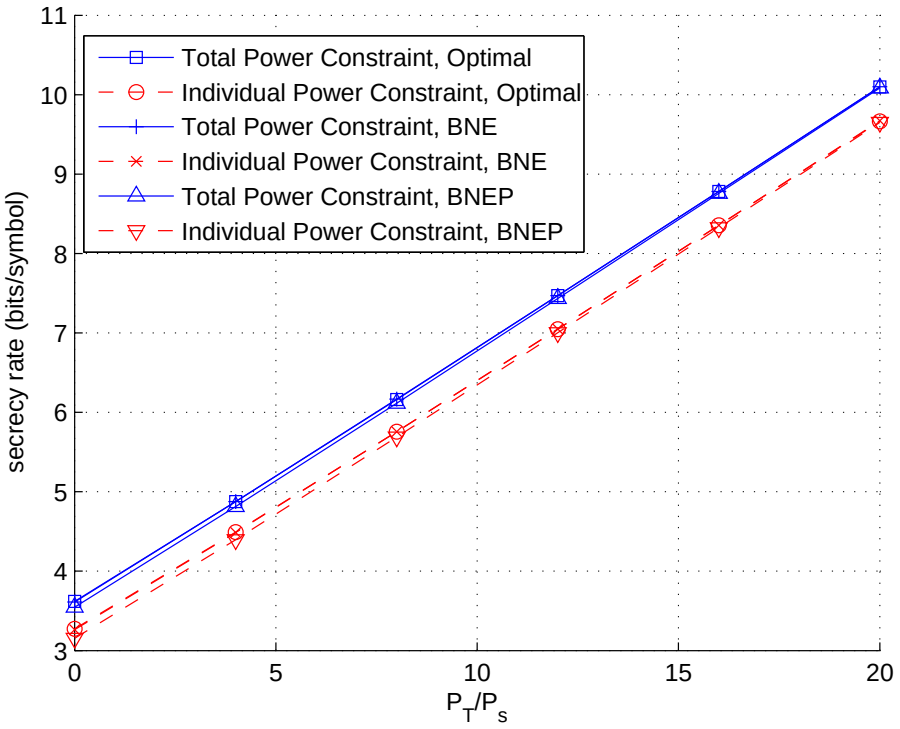

Figure 6.3: AF secrecy rate vs. P_T/P_s. $\sigma_g = 10, \sigma_h = 1, \sigma_z = 2, \sigma_k = 4, M = 10, \gamma = 10dB$.

In Fig. 6.3, we change the parameters to $\sigma_g = 10, \sigma_h = 1, \sigma_z = 2, \sigma_k = 4$, $\gamma = 10dB$ and $M = 10$. In this case, channels between the relays and the eavesdropper and between the relays and the primary-user are on average stronger than the channels between the relays and the destination. We note that beamforming schemes can still attain good performance and we observe similar trends as before.

In Fig. 6.4, we plot the optimal secrecy rate and the secrecy rates of the two suboptimal null space beamforming schemes (under both total and individual power constraints) as a function of the interference temperature limit γ. We assume that $P_T = P_s = 0dB$. It is observed that the secrecy rate achieved by beamforming in

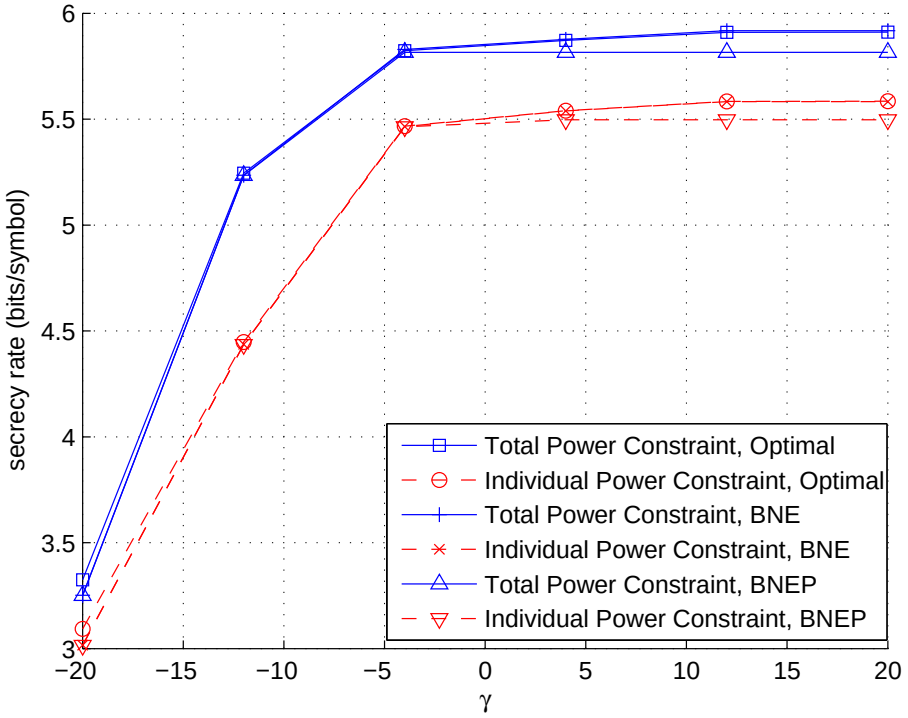

Figure 6.4: AF secrecy rate vs. interference temperature γ. $\sigma_g = 10, \sigma_h = 2, \sigma_z = 2, \sigma_k = 4, M = 10, P_s = P_T = 0dB$.

the null space of both the eavesdropper's and primary user's channels (BNEP) is almost insensitive to different interference temperature limits when $\gamma \geq -4dB$ since it always forces the signal interference to be zero regardless of the value of γ. It is further observed that beamforming in the null space of the eavesdropper's channel (BNE) always achieves near optimal performance regardless the value of γ under both total and individual power constraints.

6.6 Conclusion

In this chapter, collaborative relay beamforming in cognitive radio networks is studied under secrecy constraints. Optimal beamforming designs that maximize secrecy rates are investigated under both total and individual relay power constraints. We have formulated the problem as a semidefinite programming problem and provided an optimization framework. In addition, we have proposed two sub-optimal null space beamforming schemes to simplify the computation. Finally, we have provided numerical results to illustrate the performances of different beamforming schemes.

Chapter 7

Optimal Power Allocation for Secrecy Fading Channels Under Spectrum-Sharing Constraints

In this chapter, we consider a scenario in which second users communicate in the presence of a primary user and an eavesdropper. Hence, secondary users need to both control the interference levels on the primary user and send the information securely. Hence, we combine the challenges seen in studies of cognitive radio networks and information-theoretic security. Our contributions in this chapter are as follows. We initially assume that the transmitter has global channel side information (CSI), i.e., perfectly knows the fading coefficients of all channels, and we study the secrecy capacity limits of opportunistic spectrum-sharing channels in fading environments and identify the optimal power allocation for the secondary user under average and peak received power constraints at the primary user. Subsequently, we consider the case in which the eavesdropper's CSI is unavailable at the source. In this scenario, we study the optimal power allocation under average

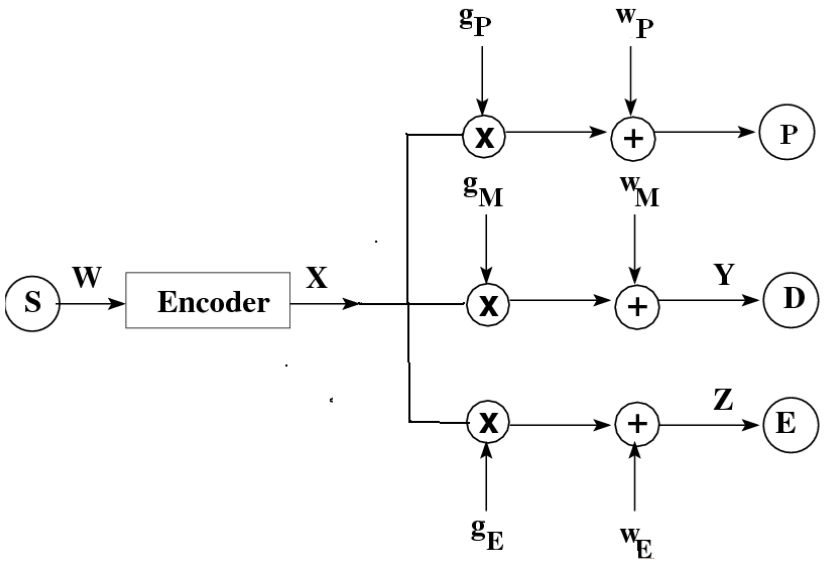

Figure 7.1: Channel Model

power constraints, and propose a simplified on/off power control method.

7.1 Channel Model

As depicted in Fig.7.1, we consider a cognitive radio channel model with a secondary user source S, a primary user P, a secondary user destination D, and an eavesdropper E. In this model, the source S tries to transmit confidential messages to destination D on the same band as the primary user's while keeping the interference on the primary user below some predefined interference temperature limit and keeping the eavesdropper E ignorant of the information. During any coherence interval i, the signal received by the destination and the eavesdropper

are given, respectively, by

$$y(i) = g_M(i)x(i) + w_M(i), \tag{7.1}$$

$$z(i) = g_E(i)x(i) + w_E(i), \tag{7.2}$$

where $g_M(i), g_E(i)$ are the channel gains from the secondary source to the secondary receiver (main channel) and from the secondary source to the eavesdropper (eavesdropper channel), respectively, and $w_M(i), w_E(i)$ represent the i.i.d additive Gaussian noise with zero-mean and unit-variance at the destination and the eavesdropper, respectively. We denote the fading power gains of the main and eavesdropper channels by $h_M(i) = |g_M(i)|^2$ and $h_E(i) = |g_E(i)|^2$, respectively. Similarly, we denote the channel gain from the secondary source to the primary receiver by $g_P(i)$ and its fading power gain by $h_P(i) = |g_P(i)|^2$. We assume that both channels experience block fading, i.e., the channel gains remain constant during each coherence interval and change independently from one coherence interval to the next. The fading process is assumed to be ergodic with a bounded continuous distribution. Moreover, the fading coefficients of the destination and the eavesdropper in any coherence interval are assumed to be independent of each other.

Since transmissions pertaining to the secondary user should not harm the signal quality at the receiver of the primary user, we impose constraints on the received-power at the primary user P. Hence, denoting the average and peak received-power values by Q_{avg} and Q_{peak}, respectively, we define the corresponding constraints as:

$$\mathcal{E}_{h_M,h_E,h_P}\{P(h_M, h_E, h_P)h_P\} \leq Q_{avg} \tag{7.3}$$

and

$$P(h_M, h_E, h_P)h_P \leq Q_{peak}, \quad \forall h_M, h_E, h_P. \tag{7.4}$$

Note that Q_{avg} can be seen as a long-term average received power constraint. Additionally, although we call Q_{peak} as the peak received-power constraint, it is actually a peak constraint on the average instantaneous received power and can be regarded as a short-term constraint.

7.2 Power Allocation under Average Received-Power Constraints

In a fading environment, following the same line of development as in [24], it is straightforward but tedious to show that the channel capacity is achieved by optimally distributing the transmitted power over time such that the primary user received power constraint is met. By assuming that h_M, h_E, and h_P are independent of each other and global CSI is available, the secrecy capacity under an average received power constraint is the solution to the following optimization problem,

$$\begin{aligned}
\max_{P(h_M,h_E,h_P)\geq 0} \int\int\int \Big[& \log\left(1 + h_M P(h_M, h_E, h_P)\right) \\
& - \log\left(1 + h_E P(h_M, h_E, h_P)\right) \Big]^+ \\
& \times f(h_M) f(h_E) f(h_P) \mathrm{d}h_M \mathrm{d}h_E \mathrm{d}h_P \\
s.t \quad & \int\int\int h_P P(h_M, h_E, h_P) \\
& \times f(h_M) f(h_E) f(h_P) \mathrm{d}h_M \mathrm{d}h_E \mathrm{d}h_P \leq Q_{avg}
\end{aligned} \tag{7.5}$$

where $[x]^+ = \max\{0, x\}$. To find the optimal power allocation $P(h_M, h_E, h_P)$, we form the Lagrangian:

$$\begin{aligned} L(P,\lambda) = &\int\int\int \Big[\log\left(1 + h_M P(h_M,h_E,h_P)\right) \\ &- \log\left(1 + h_E P(h_M,h_E,h_P)\right)\Big]^+ f(h_M)f(h_E)f(h_P)\mathrm{d}h_M\mathrm{d}h_E\mathrm{d}h_P \\ &- \lambda\Big(\int\int\int h_P P(h_M,h_E,h_P) \\ &\quad \times f(h_M)f(h_E)f(h_P)\mathrm{d}h_M\mathrm{d}h_E\mathrm{d}h_P - Q_{avg}\Big). \end{aligned} \tag{7.6}$$

By using the Lagrangian maximization approach, we get the following optimality condition:

$$\begin{aligned} &\frac{\partial L(P,\lambda)}{\partial P(h_M,h_E,h_P)} \\ &= \Big(\frac{h_M}{1 + h_M P(h_M,h_E,h_P)} - \frac{h_E}{1 + h_E P(h_M,h_E,h_P)} - \lambda h_P\Big) \\ &\quad \times f(h_M)f(h_E)f(h_P) \;=\; 0. \end{aligned} \tag{7.7}$$

Solving (7.7) with the constraint $P(h_M, h_E, h_P) \geq 0$ yields the optimal power allocation policy at the transmitter as

$$\begin{aligned} P(h_M,h_E,h_P) = \frac{1}{2}\Bigg[\sqrt{\left(\frac{1}{h_E} - \frac{1}{h_M}\right)^2 + \frac{4}{\lambda h_P}\left(\frac{1}{h_E} - \frac{1}{h_M}\right)} \\ - \left(\frac{1}{h_M} + \frac{1}{h_E}\right)\Bigg]^+, \end{aligned} \tag{7.8}$$

where λ is a constant that is introduced to satisfy the receive power constraint (7.5) at the primary user.

Remark 1 *It is easy to see that when $h_E > h_M$, $P(h_M, h_E, h_P) = 0$, which is in accor-*

dance with our intuition. Transmitter only spends power for transmission when the main channel is better than the eavesdropper's channel. With little calculation, we can also see that when $h_P > \frac{h_M - h_E}{\lambda}$*, we have* $P(h_M, h_E, h_P) = 0$*. Thus, the power allocation can be rewritten as*

$$P(h_M, h_E, h_P) = \begin{cases} \frac{1}{2}\left[\sqrt{\left(\frac{1}{h_E} - \frac{1}{h_M}\right)^2 + \frac{4}{\lambda h_P}\left(\frac{1}{h_E} - \frac{1}{h_M}\right)} \right. \\ \left. - \left(\frac{1}{h_M} + \frac{1}{h_E}\right)\right] & \frac{h_M - h_E}{h_P} > \lambda \\ 0 & \frac{h_M - h_E}{h_P} \leq \lambda \end{cases} . \tag{7.9}$$

Remark 2 *From the expression of the optimal power allocation obtained in (7.8), we can easily see that more transmission power is used when either* h_M *increases or* h_P *decreases. Also the derivative of (7.8) with regard to* h_E *is*

$$-\frac{1}{2h_E^2}\left[\frac{\frac{1}{h_E} - \frac{1}{h_M} + \frac{2}{\lambda h_P}}{\sqrt{\left(\frac{1}{h_E} - \frac{1}{h_M}\right)^2 + \frac{4}{\lambda h_P}\left(\frac{1}{h_E} - \frac{1}{h_M}\right)}} - 1\right]. \tag{7.10}$$

We can see that the derivative is negative, so $P(h_M, h_E, h_P)$ *decreases when* h_E *increases. These observations are also intuitively appealing. The secondary user takes advantage of the weak link between its transmitter and the primary receiver, and the stronger main channel. Also, a weaker eavesdropper's channel is preferred for secure message transmission.*

Remark 3 *When there is no eavesdropper, the channel is the standard cognitive radio channel. By letting* $h_E = 0$ *in (7.7) and solving the problem, we can obtain the optimal power allocation as* $(\frac{1}{\lambda h_P} - \frac{1}{h_M})^+$*, which has also been shown in [22] and [54].*

Remark 4 *When there is no primary user, the channel is the standard secrecy fading*

channel. By replacing h_P with 1 in (7.5) and correspondingly replacing h_P with 1 in (7.8), we get the optimal power allocation for the fading secrecy channel given in [24].

7.3 Power Allocation under both Average and Peak Received-Power Constraints

The average received power constraint is reasonable when the primary user's QoS is determined by the average long-term interference. However, we note that in many cases, the primary user's QoS is also limited by the instantaneous interference at the primary receiver. With this motivation, we in this section study the power allocation under both average and peak received power constraints.

We first introduce a real-valued function β which is defined as

$$\beta^2 \triangleq \frac{Q_{peak}}{h_P} - P(h_M, h_E, h_P). \tag{7.11}$$

To satisfy the peak power constraint, the right-hand side of (7.11) must be non-negative over all the possible values of the channel gain. Using (7.11), we form an equivalent problem of (7.5), which contains an equality constraint for the peak power.

$$\max_{P(h_M,h_E,h_P)\geq 0,\beta} \int\int\int \Big[\log\left(1+h_M P(h_M,h_E,h_P)\right) - \log\left(1+h_E P(h_M,h_E,h_P)\right)\Big]^+ \times f(h_M)f(h_E)f(h_P)\mathrm{d}h_M\mathrm{d}h_E\mathrm{d}h_P \tag{7.12}$$

$$s.t \quad \int\int\int h_P P(h_M,h_E,h_P) \times f(h_M)f(h_E)f(h_P)\mathrm{d}h_M\mathrm{d}h_E\mathrm{d}h_P \leq Q_{avg} \tag{7.13}$$

$$\text{and} \qquad \beta^2 + P(h_M,h_E,h_P) = \frac{Q_{peak}}{h_P}. \tag{7.14}$$

Now, the Lagrangian becomes

$$\begin{aligned} L(P,\lambda) = &\int\int\int \Big[\log\left(1+h_M P(h_M,h_E,h_P)\right) \\ &- \log\left(1+h_E P(h_M,h_E,h_P)\right)\Big]^+ f(h_M)f(h_E)f(h_P)\mathrm{d}h_M\mathrm{d}h_E\mathrm{d}h_P \\ &- \lambda\Big(\int\int\int h_P P(h_M,h_E,h_P) \\ &\quad \times f(h_M)f(h_E)f(h_P)\mathrm{d}h_M\mathrm{d}h_E\mathrm{d}h_P - Q_{avg}\Big) \\ &- \lambda_0\Big(\beta^2 + P(h_M,h_E,h_P) - \frac{Q_{peak}}{h_P}\Big). \end{aligned} \tag{7.15}$$

Setting each of the partial derivatives of the Lagrangian with respect to P and β to zero, we obtain, respectively, the necessary conditions for the optimal solution to problem (7.14) as

$$\frac{h_M}{1+h_M P(h_M,h_E,h_P)} - \frac{h_E}{1+h_E P(h_M,h_E,h_P)} - \lambda h_P - \lambda_0 = 0 \tag{7.16}$$

$$2\beta\lambda_0 = 0. \tag{7.17}$$

Note that (7.17) implies either $\beta = 0$ or $\lambda_0 = 0$. $\beta = 0$ means that the peak power constraint is active and hence, the optimal transmission power in this case is given by (7.18)

$$P(h_M, h_E, h_P) = \frac{Q_{peak}}{h_P}. \tag{7.18}$$

On the other hand, $\lambda_0 = 0$ in (7.17) means that the peak transmission power constraint is inactive and it can be ignored. Solving (7.16) with $\lambda_0 = 0$, we get the expression for the optimal transmitter power as

$$\frac{1}{2}\left[\sqrt{\left(\frac{1}{h_E} - \frac{1}{h_M}\right)^2 + \frac{4}{\lambda h_P}\left(\frac{1}{h_E} - \frac{1}{h_M}\right)} - \left(\frac{1}{h_M} + \frac{1}{h_E}\right)\right]^+,$$

which is the same expression as in (7.8) obtained when there is only an average received power constraint. Combining the two cases, the optimal power allocation under both average and peak power constraints becomes

$$P(h_M, h_E, h_P) = \min\left(\frac{Q_{peak}}{h_P}, \right.$$
$$\left.\frac{1}{2}\left[\sqrt{\left(\frac{1}{h_E} - \frac{1}{h_M}\right)^2 + \frac{4}{\lambda h_P}\left(\frac{1}{h_E} - \frac{1}{h_M}\right)} - \left(\frac{1}{h_M} + \frac{1}{h_E}\right)\right]^+\right) \tag{7.19}$$

where λ is a constant with which the average power constraint is satisfied. We should note that λ here is generally not the same as λ in the optimal power allocation in (7.8).

Remark 5 *We can see from (7.19) with little computation that when the condition*

$$\frac{1}{\frac{h_E}{h_P} + 1/Q_{peak}} - \frac{1}{\frac{h_M}{h_P} + 1/Q_{peak}} > \lambda Q_{peak}^2 \tag{7.20}$$

is satisfied, we have $P(h_M, h_E, h_P) = \frac{Q_{peak}}{h_P}$

7.4 Power Allocation without Eavesdropper's CSI

Since eavesdropping is a passive operation (i.e., does not involve any transmission), the source may not be able to get the CSI of the eavesdropper's channel in certain circumstances. With this motivation, we in this section study the optimal power allocation when the source knows only h_M and h_P. To simplify the analysis, we consider only average receive power constraints here.

7.4.1 Optimal Power Allocation

Based on the results of [24], the secrecy capacity in this case is the solution of the following optimization problem:

$$\begin{aligned}\max_{P(h_M,h_P)\geq 0} \int\int\int \Big[&\log\left(1+h_M P(h_M,h_P)\right) \\ &- \log\left(1+h_E P(h_M,h_P)\right)\Big]^+ \\ &\times f(h_M)f(h_E)f(h_P)\mathrm{d}h_M\mathrm{d}h_E\mathrm{d}h_P \\ s.t \quad \int\int\int & h_P P(h_M,h_P) \\ &\times f(h_M)f(h_E)f(h_P)\mathrm{d}h_M\mathrm{d}h_E\mathrm{d}h_P \leq Q_{avg}. \end{aligned} \tag{7.21}$$

Similarly, using the Lagrangian approach, we get the optimal condition as

$$\begin{aligned}&\frac{h_M \Pr\left(h_E \leq h_M\right)}{1+h_M P(h_M,h_P)} \\ -&\int_0^{h_M} \left(\frac{h_E}{1+h_E P(h_M,h_P)}\right) f(h_E)\mathrm{d}h_E - \lambda h_P \;=\; 0, \end{aligned} \tag{7.22}$$

where λ is a constant that satisfies the power constraints in (7.21) with equality. By solving (7.22), we can get the optimal transmit power allocation $P(h_M, h_P)$. If the obtained value turns out to be negative, then the optimal value of $P(h_M, h_P)$ is equal to 0. The exact solution to this optimization problem depends on the fading distributions.

If Rayleigh fading scenario is considered with $\mathbb{E}\{h_M\} = \overline{\gamma}_M$, $\mathbb{E}\{h_E\} = \overline{\gamma}_E$ and $\mathbb{E}\{h_P\} = \overline{\gamma}_P$, then the optimal power allocation is the solution of the following equation:

$$\begin{aligned}
&\left(1 - e^{-(h_M/\overline{\gamma}_E)}\right)\left(\frac{h_M}{1 + h_M P(h_M, h_P)}\right)\lambda h_P \\
&- \frac{\left(1 - e^{-(h_M/\overline{\gamma}_E)}\right)}{P(h_M, h_P)} + \frac{\exp\left(\frac{1}{\overline{\gamma}_E P(h_M, h_P)}\right)}{\overline{\gamma}_E (P(h_M, h_P))^2}\left[\mathrm{Ei}\left(\frac{1}{\overline{\gamma}_E P(h_M, h_P)}\right)\right. \\
&\left. - \mathrm{Ei}\left(\frac{h_M}{\overline{\gamma}_E} + \frac{1}{\overline{\gamma}_E P(h_M, h_P)}\right)\right] \;=\; 0
\end{aligned} \tag{7.23}$$

where $\mathrm{Ei}(x) = \int_x^\infty \frac{e^{-t}}{t}\,\mathrm{d}t$ is the exponential integral function. Again, if there is no positive solution to (7.23), the optimal $P(h_M, h_P) = 0$.

7.4.2 On/Off power control

As seen above, the computation of the optimal power allocation is in general complicated. In this section, we use a simplified suboptimal on/off power control method [24]. That is, the source sends information only when the channel gain h_M exceeds a pre-determined constant threshold $\tau > 0$. Moreover, when $h_M > \tau$, the transmitter always uses the same power level P . It is easy to compute that

the constant power level used for transmission should be

$$P = \frac{Q_{avg}}{\overline{\gamma}_P \Pr(h_M > \tau)}. \tag{7.24}$$

For the Rayleigh fading scenario for which $f(h_M) = \frac{1}{\overline{\gamma}_M} e^{-(h_M/\overline{\gamma}_M)}$, we get

$$P = \frac{Q_{avg}}{\overline{\gamma}_P} e^{(\tau/\overline{\gamma}_M)}. \tag{7.25}$$

Then, the secrecy rate can be computed as

$$\begin{aligned}
R_s &= \int_0^\infty \int_\tau^\infty \left[\log\left(1 + h_M P\right) - \log\left(1 + h_E P\right)\right]^+ \\
&\qquad \times f(h_M) f(h_E) \mathrm{d}h_M \mathrm{d}h_E \\
&= e^{-(\tau/\overline{\gamma}_M)} \log\left(1 + \tau \frac{Q_{avg}}{\overline{\gamma}_P} e^{(\tau/\overline{\gamma}_M)}\right) + \exp\left(\frac{1}{\overline{\gamma}_M \frac{Q_{avg}}{\overline{\gamma}_P} e^{(\tau/\overline{\gamma}_M)}}\right) \\
&\quad \mathrm{Ei}\left(\frac{\tau}{\overline{\gamma}_M} + \frac{1}{\overline{\gamma}_M \frac{Q_{avg}}{\overline{\gamma}_P} e^{(\tau/\overline{\gamma}_M)}}\right) + \exp\left(\frac{1}{\overline{\gamma}_E \frac{Q_{avg}}{\overline{\gamma}_P} e^{(\tau/\overline{\gamma}_M)}} - \frac{\tau}{\overline{\gamma}_M}\right) \\
&\quad \left[\mathrm{Ei}\left(\frac{\tau}{\overline{\gamma}_E} + \frac{1}{\overline{\gamma}_E \frac{Q_{avg}}{\overline{\gamma}_P} e^{(\tau/\overline{\gamma}_M)}}\right) - \mathrm{Ei}\left(\frac{1}{\overline{\gamma}_E \frac{Q_{avg}}{\overline{\gamma}_P} e^{(\tau/\overline{\gamma}_M)}}\right)\right] \\
&\quad - \exp\left(\frac{\left[\frac{1}{\overline{\gamma}_M} + \frac{1}{\overline{\gamma}_E}\right]}{\frac{Q_{avg}}{\overline{\gamma}_P} e^{(\tau/\overline{\gamma}_M)}}\right) \mathrm{Ei}\left(\left[\frac{1}{\overline{\gamma}_M} + \frac{1}{\overline{\gamma}_E}\right]\left[\tau + \frac{1}{\frac{Q_{avg}}{\overline{\gamma}_P} e^{(\tau/\overline{\gamma}_M)}}\right]\right).
\end{aligned} \tag{7.26}$$

Note that the secrecy rate depends on the threshold τ. Hence, we can get the maximum achievable secrecy rate under the on/off power control policy by optimizing the threshold τ.

7.5 Numerical Results

In this section, we numerically illustrate the secrecy rate studied in this chapter. In all simulations, we assume that the fading is Rayleigh distributed.

We first consider the case in which the global CSI is available. In Fig. 7.2, we plot the secrecy rate versus Q_{avg} for different values of the peak received power constraint Q_{peak}. We can see from the figure that, as expected, the larger the Q_{peak}, the closer the rate is to the case of no peak power constraint. We also observe that the constraint on the peak received power does not have much impact on the secrecy rate for low values of Q_{avg}. On the other hand, as the value of the average received power limit approaches the peak received power constraint, the rate plots become flat and the performance gets essentially limited by the peak received-power constraint.

In Fig. 7.3, we plot the ergodic secrecy rate as a function of Q_{avg} while keeping the ratio $\frac{Q_{peak}}{Q_{avg}}$ fixed. We should point out that eavesdropper's channel is stronger than the main channel on average (i.e., $\overline{\gamma}_M = 1 < \overline{\gamma}_E = 2$) in this figure. Note that positive secrecy rate can not achieved without fading in such a case. In the figure, we again see that the higher the ratio $\frac{Q_{peak}}{Q_{avg}}$, the closer the curve is to the no peak power constraint case. Also, since the peak power constraint becomes more relaxed with increasing Q_{avg}, we do not see the flattening of the rate curve in contrast to what is observed in Fig. 7.2.

Next, we consider the case in which the eavesdropper's CSI is not available. In Fig.7.4, we plot the ergodic secrecy rate vs. Q_{avg} curves achieved with optimal power allocation and with the on/off power control method. The fading variances $\bar{\lambda}$ are the same as in Fig. 7.3. By comparing the secrecy rates in Fig. 7.4 with the secrecy rate in Fig. 7.3 obtained in the absence of peak constraints, we observe

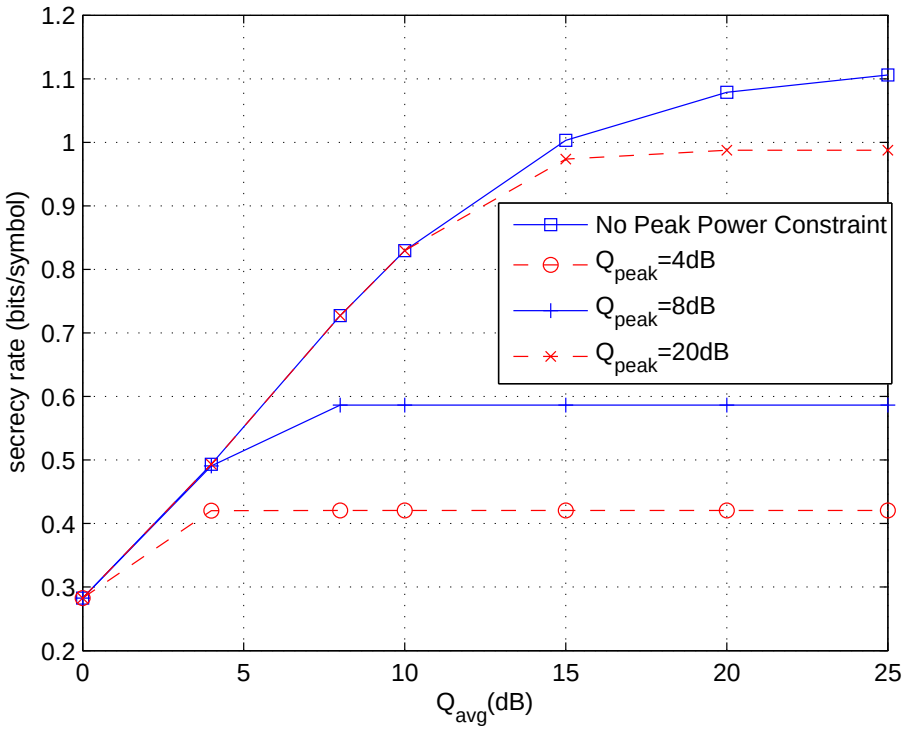

Figure 7.2: secrecy rate vs. Q_{avg} for different peak power constraint with global CSI available, $\overline{\gamma}_M = \overline{\gamma}_E = 1, \overline{\gamma}_P = 2$.

that not having the eavesdropper's channel information result in a certain loss in the secrecy rate. We also see that the performance of the on/off power control scheme is very close to the optimal secrecy capacity (when only the main channel and primary channel CSI is available) for a wide range of SNRs, and approach the optimal rate when SNR is high. Note that the optimality of the on/off power control scheme at high SNRs has been proved in [24] for the secrecy fading channel. Thus, the on/off power control method has great utility in practical systems due to its advantage of simple implementation.

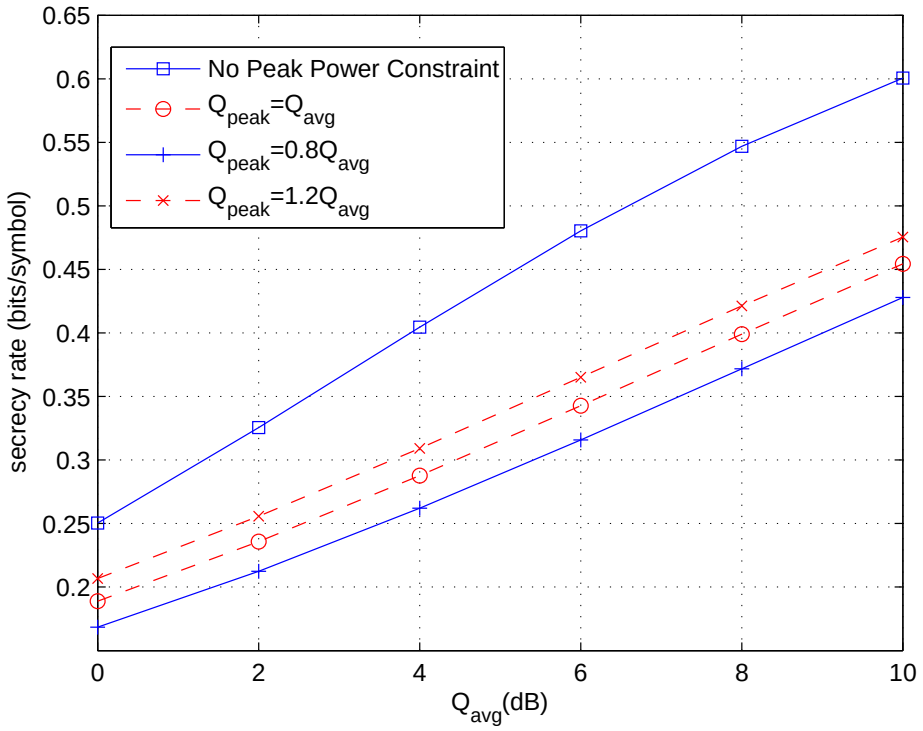

Figure 7.3: secrecy rate vs. Q_{avg} for different peak power constraint with global CSI available, $\overline{\gamma}_M = 1, \overline{\gamma}_E = 2, \overline{\gamma}_P = 2$.

7.6 Conclusion

In this chapter, we have considered a spectrum-sharing system subject to security considerations and studied the optimal power allocation strategies for the secrecy fading channel under average and peak received power constraints at the primary user. In particular, we have considered two scenarios regarding the availability of the CSI. When global CSI is available, we have obtained analytical expressions for the optimal power allocation under average and peak received power constraints. When only main channel's and primary channel's CSI is available, we have characterized the optimal power allocation as the solution to a certain equation. We have also derived the analytical secrecy rate expression for

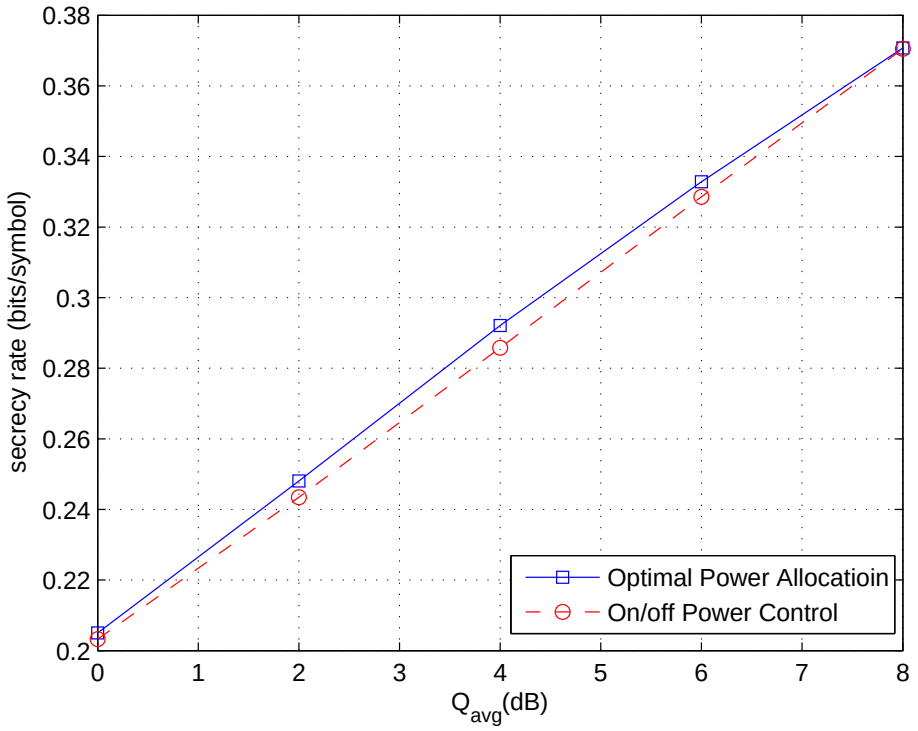

Figure 7.4: secrecy rate vs. Q_{avg} without eavesdropper's CSI, $\overline{\gamma}_M = 1, \overline{\gamma}_E = 2, \overline{\gamma}_P = 2$.

the simplified on/off power control scheme in this scenario. Numerical results corroborating our theoretical analysis have also been provided. Specially, it is shown that the constraint on the peak received power does not have much impact on the secrecy rate for low values of Q_{avg} as long as the average power constraints remain active, and that the performance of the suboptimal on/off power control scheme approaches the optimal performance when the eavesdropper's CSI is not available.

Chapter 8

Low-SNR Analysis of Interference Channels under Secrecy Constraints

In this chapter, we study secure transmission over Gaussian weak interference channels in the low-power regime. The organization of the rest of the chapter is as follows. In Section 8.1, we describe the channel model and obtain the secrecy achievable rate regions for TDMA, multiplexed transmission schemes and artificial noise schemes, and compare their performances in terms of the achievable rates. In Section 8.2, we compute the minimum energy per bit and slope at $\frac{E_b}{N_0}_{\min}$ for TDMA and multiplexed transmission schemes. In Section 8.3, we use results in Section 8.2 to evaluate how secrecy constraints affect the performance in the low-power regime and identify optimal transmission schemes. Finally, we provide conclusions in Section 8.4.

8.1 Gaussian Interference Channels with Confidential Messages

We consider secure communication over a two-transmitter, two-receiver Gaussian interference channel. The input-output relations for this channel model are given by

$$y_1 = c_{11}x_1 + c_{12}x_2 + n_1, \text{ and} \tag{8.1}$$

$$y_2 = c_{21}x_1 + c_{22}x_2 + n_2 \tag{8.2}$$

where x_1 and x_2 are the channel inputs of the transmitters, the coefficients $\{c_{ij}\}$ denote the channel gains and are deterministic scalars, and n_1 and n_2 are independent, circularly symmetric, complex Gaussian random variables with zero mean and common variance σ^2. It is assumed that the transmitters are subject to the following average power constraint:

$$E[|x_i|^2] \leqslant P_i = \text{SNR}_i\, \sigma^2, \quad i = 1, 2. \tag{8.3}$$

We focus on the weak interference channel i.e., we assume that $\frac{|c_{12}|^2}{|c_{11}|^2} < 1$ and $\frac{|c_{21}|^2}{|c_{22}|^2} < 1$. Over this channel, transmitter i for $i = 1, 2$ intends to send an confidential message by transmitting x_i to the desired receiver i, which receives y_i, while ensuring that the other receiver does not obtain any information by listening the transmission. Following [45], we next consider three transmission schemes and their corresponding achievable secrecy rate regions.

8.1.1 Time Division Multiple Access

In TDMA, the transmission period is divided into two nonoverlapping time slots. Transmitters 1 and 2 transmit using α and $1-\alpha$ fractions of time, respectively. We note that under this assumption, the channel in each time slot reduces to a Gaussian wiretap channel [42], and the following rate region can be achieved with perfect secrecy [45]:

$$\begin{aligned}
&R_1 \geqslant 0 \\
&R_2 \geqslant 0 \\
&R_1 \leqslant \alpha \left[\log\left(1+\frac{|c_{11}|^2\mathrm{SNR}_1}{\alpha}\right) - \log\left(1+\frac{|c_{21}|^2\mathrm{SNR}_1}{\alpha}\right)\right] \\
&R_2 \leqslant (1-\alpha)\left[\log\left(1+\frac{|c_{22}|^2\mathrm{SNR}_2}{1-\alpha}\right) - \log\left(1+\frac{|c_{12}|^2\mathrm{SNR}_2}{1-\alpha}\right)\right]
\end{aligned} \tag{8.4}$$

over all possible transmitting signal-to-noise-ratio pairs $\mathrm{SNR}_1 \in [0, P_1/\sigma^2], \mathrm{SNR}_2 \in [0, P_2/\sigma^2]$ and time allocation parameter α.

8.1.2 Multiplexed Transmission

In the multiplexed transmission scheme, transmitters are allowed to share the same degrees of freedom. By the constraint of information-theoretic security, no partial decoding of the other transmitter's message is allowed at a receiver. Hence, the interference results in an increase of the noise floor. Thus, the following rate

region can be achieved with perfect secrecy [45]:

$$
\begin{aligned}
&R_1 \geqslant 0 \\
&R_2 \geqslant 0 \\
&R_1 \leqslant \log\left(1+\frac{|c_{11}|^2\mathrm{SNR}_1}{1+|c_{12}|^2\mathrm{SNR}_2}\right)-\log\left(1+|c_{21}|^2\mathrm{SNR}_1\right) \\
&R_2 \leqslant \log\left(1+\frac{|c_{22}|^2\mathrm{SNR}_2}{1+|c_{21}|^2\mathrm{SNR}_1}\right)-\log(1+|c_{12}|^2\mathrm{SNR}_2)
\end{aligned} \tag{8.5}
$$

over all possible transmitting signal-to-noise-ratio pairs $\mathrm{SNR}_1 \in [0, P_1/\sigma^2], \mathrm{SNR}_2 \in [0, P_2/\sigma^2]$.

8.1.3 Artificial Noise

This scheme allows one of the transmitters (e.g transmitter 2) to generate artificial noise. This scheme will split the power of transmitter 2 into two parts: λP_2 for generating artificial noise and the remaining $(1-\lambda)P_2$ for encoding the confidential message. As detailed in [45], the achievable rate region is

$$
\begin{aligned}
&R_1 \geqslant 0 \\
&R_2 \geqslant 0 \\
&R_1 \leqslant \log\left(1+\frac{|c_{11}|^2\mathrm{SNR}_1}{1+|c_{12}|^2\mathrm{SNR}_2}\right)-\log\left(1+\frac{|c_{21}|^2\mathrm{SNR}_1}{1+|c_{22}|^2\lambda\mathrm{SNR}_2}\right) \\
&R_2 \leqslant \log\left(1+\frac{|c_{22}|^2(1-\lambda)\mathrm{SNR}_2}{1+|c_{21}|^2\mathrm{SNR}_1+|c_{22}|^2\lambda\mathrm{SNR}_2}\right) \\
&\qquad -\log\left(1+\frac{|c_{12}|^2(1-\lambda)\mathrm{SNR}_2}{1+|c_{12}|^2\lambda\mathrm{SNR}_2}\right)
\end{aligned} \tag{8.6}
$$

over all possible transmitting signal-to-noise-ratio pairs $\mathrm{SNR}_1 \in [0, P_1/\sigma^2], \mathrm{SNR}_2 \in [0, P_2/\sigma^2]$ and power splitting parameter λ. We can further enlarge the rate region

by reversing the roles of transmitters 1 and 2.

When the transmitting power is moderate, neither too high nor too small, as demonstrated in [45], transmission strategy with artificial noise provides the largest achievable rate region while TDMA gives the smallest rate region.

On the other hand, when we consider the two extreme cases of high- and low-SNR regimes, the picture changes. In the high-SNR regime, when we let $\mathrm{SNR}_1 \to \infty, \mathrm{SNR}_2 \to \infty$ and $\lim \frac{\mathrm{SNR}_1}{\mathrm{SNR}_2} = q$ in (8.4), (8.5), and (8.6), we can see that multiplexed transmission can not achieve any positive secrecy rate, while TDMA rates are bounded by $R_1 < \alpha \log(\frac{|c_{11}|^2}{|c_{21}|^2})$, and $R_2 < (1-\alpha)\log(\frac{|c_{22}|^2}{|c_{12}|^2})$. For the strategy with the artificial noise, rate R_1 is bounded by $R_1 < \log(\frac{1+\frac{|c_{11}|^2 q}{|c_{12}|^2}}{1+\frac{|c_{21}|^2 q}{|c_{22}|^2 \lambda}})$, but we can not achieve any secrecy rate for R_2. Thus, TDMA is the best choice when we want both users to have secure communication in the high-SNR regime.

In the low-SNR regime (as SNR approaches zero), TDMA and multiplexed transmission achievable regions become identical. They converge to the following rectangular rate region, as illustrated in Fig.8.1:

$$\begin{aligned} R_1 &\geqslant 0 \\ R_2 &\geqslant 0 \\ R_1 &\leqslant |c_{11}|^2 \mathrm{SNR}_1 - |c_{21}|^2 \mathrm{SNR}_1 + o(\mathrm{SNR}_1) \\ R_2 &\leqslant |c_{22}|^2 \mathrm{SNR}_2 - |c_{12}|^2 \mathrm{SNR}_2 + o(\mathrm{SNR}_2) \end{aligned} \tag{8.7}$$

Thus, these schemes have similar performances at vanishing SNR levels in terms of the asymptotic rates. However, a finer analysis in the next section will provide more insight. We note that in the case of transmission with artificial noise, we have $R_1 \leqslant |c_{11}|^2 \mathrm{SNR}_1 - |c_{21}|^2 \mathrm{SNR}_1 + o(\mathrm{SNR}_1)$ and $R_2 \leqslant (1-\lambda)(|c_{22}|^2 \mathrm{SNR}_2 -$

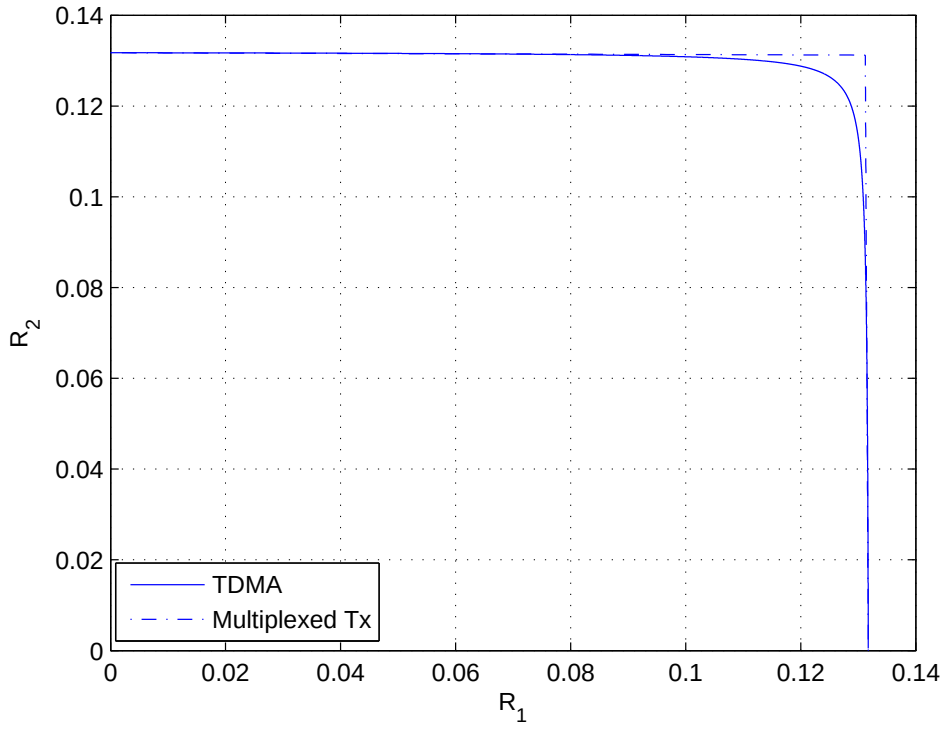

Figure 8.1: Gaussian Interference Channel secrecy rate achievable Region $P_1 = P_2 = 0.1, c_{11} = c_{22} = 1, c_{12} = c_{21} = 0.2$

$|c_{12}|^2 \mathrm{SNR}_2) + o(\mathrm{SNR}_2)$ which is strictly smaller than that in (8.7). This lets us to conclude that introducing artificial noise is not preferable in the low-SNR regime.

8.2 Energy Efficiency in the Low-SNR Regime

The tradeoff of spectral efficiency versus energy per information bit is the key measure of performance in the low-SNR regime. The two major analysis tools in this regime are the minimum value of the energy per bit $\frac{E_b}{N_0}_{\min}$, and the slope S of

the spectral efficiency versus $\frac{E_b}{N_0}$ curve at $\frac{E_b}{N_{0\,\min}}$ [69]. These can be obtained from

$$\frac{E_b}{N_{0\,\min}} = \frac{\log_e 2}{\dot{C}(0)} \tag{8.8}$$

and

$$S = \frac{2[\dot{C}(0)^2]}{-\ddot{C}(0)} \tag{8.9}$$

where $\dot{C}(0)$ and $\ddot{C}(0)$ denote the first and second derivatives of the channel capacity with respect to SNR at SNR = 0.

In this section, using these tools, we analyze the performance in interference channels with confidential messages, following an approach similar to that in [9]. Note that in interference channels, we have the achievable rate pairs (R_1, R_2). As the SNRs of both users approach zero in the low-SNR regime, it can be easily seen that $R_1 \to 0$ and $R_2 \to 0$. In this regime, we introduce the parameter θ, and assume that the ratio of the rates is $R_1/R_2 = \theta$ as R_1 and R_2 both vanish. In both TDMA and multiplexed transmissions, we have

$$\theta = \frac{R_1}{R_2} = \frac{\mathrm{SNR}_1(|c_{11}|^2 - |c_{21}|^2)}{\mathrm{SNR}_2(|c_{22}|^2 - |c_{12}|^2)}. \tag{8.10}$$

By fixing θ, we can rewrite the achievable rate region of multiplexed transmission

in (8.5) as

$$
\begin{aligned}
R_1 &\geqslant 0 \\
R_2 &\geqslant 0 \\
R_1 &\leqslant \log\left(1+\frac{|c_{11}|^2\mathrm{SNR}_1}{1+|c_{12}|^2\frac{(|c_{11}|^2-|c_{21}|^2)}{\theta(|c_{22}|^2-|c_{12}|^2)}\mathrm{SNR}_1}\right)-\log(1+|c_{21}|^2\mathrm{SNR}_1) \\
R_2 &\leqslant \log\left(1+\frac{|c_{22}|^2\mathrm{SNR}_2}{1+|c_{21}|^2\frac{\theta(|c_{22}|^2-|c_{12}|^2)}{(|c_{11}|^2-|c_{21}|^2)}\mathrm{SNR}_2}\right)-\log(1+|c_{12}|^2\mathrm{SNR}_2). \qquad (8.11)
\end{aligned}
$$

From (8.4) and (8.11), we can see that when SNR diminishes, the bit energy $\frac{E_b}{N_0} = \frac{\mathrm{SNR}}{R(\mathrm{SNR})}$ for both TDMA and multiplexed transmission schemes monotonically decreases. Furthermore, it can be shown that the rates are concave functions of SNR in the low-SNR regime. Thus, the minimum energy per bit is achieved as $\mathrm{SNR} \to 0$. The following theorems provide the minimum energy per bit and the slope at the minimum energy per bit.

Theorem 5 *For all $\theta = R_1/R_2$, the minimum bit energies in the Gaussian interference channel with confidential messages for both TDMA and multiplexed transmissions are*

$$\frac{E_1}{N_{0\,\min}} = \frac{\log_e 2}{|c_{11}|^2-|c_{21}|^2}, \qquad (8.12)$$

$$\frac{E_2}{N_{0\,\min}} = \frac{\log_e 2}{|c_{22}|^2-|c_{12}|^2}. \qquad (8.13)$$

Proof: From (8.4) and (8.11), we can for both cases easily compute the derivatives of the achievable rates with respect to SNR as

$$\dot{R}_1(0) = |c_{11}|^2-|c_{21}|^2 \qquad (8.14)$$

$$\dot{R}_2(0) = |c_{22}|^2-|c_{12}|^2. \qquad (8.15)$$

Using (8.8), we get the minimum bit energy expressions. □

From the result of Theorem 5, we see that TDMA and multiplexed transmission achieve the same minimum energy per bit. Next, we consider the wideband slope regions.

Theorem 6 *Let the rates vanish while keeping* $R_1/R_2 = \theta$. *Then, for the Gaussian interference channel with confidential messages, the slope region achieved by TDMA is*

$$\begin{aligned} 0 \leqslant S_1 < 2 \\ 0 \leqslant S_2 < 2 \\ \frac{S_1}{2A} + \frac{S_2}{2B} = 1 \end{aligned} \tag{8.16}$$

and the slope region achieved by multiplexed transmission is

$$\begin{aligned} 0 \leqslant S_1 < 2 \\ 0 \leqslant S_2 < 2 \\ \left(\frac{2A}{S_1} - 1\right)\left(\frac{2B}{S_2} - 1\right) = \frac{4|c_{11}|^2|c_{12}|^2|c_{22}|^2|c_{21}|^2}{(|c_{11}|^4 - |c_{21}|^4)(|c_{22}|^4 - |c_{12}|^4)} \end{aligned} \tag{8.17}$$

where

$$A = \frac{|c_{11}|^2 - |c_{21}|^2}{|c_{11}|^2 + |c_{21}|^2}, \tag{8.18}$$

$$B = \frac{|c_{22}|^2 - |c_{12}|^2}{|c_{22}|^2 + |c_{12}|^2}. \tag{8.19}$$

Proof: Note again that for both transmission schemes, we have

$$\dot{R}_1(0) = |c_{11}|^2 - |c_{21}|^2, \tag{8.20}$$

$$\dot{R}_2(0) = |c_{22}|^2 - |c_{12}|^2. \tag{8.21}$$

In TDMA, we also have

$$-\ddot{R}_1(0) = \frac{|c_{11}|^4 - |c_{21}|^4}{\alpha}, \tag{8.22}$$

$$-\ddot{R}_2(0) = \frac{|c_{22}|^4 - |c_{12}|^4}{(1-\alpha)}. \tag{8.23}$$

Then, using (8.9), we get

$$S_1 = \frac{2\alpha(|c_{11}|^2 - |c_{21}|^2)}{|c_{11}|^2 + |c_{21}|^2}, \tag{8.24}$$

$$S_2 = \frac{2(1-\alpha)(|c_{22}|^2 - |c_{12}|^2)}{|c_{22}|^2 + |c_{12}|^2}. \tag{8.25}$$

Considering different values of α leads to the region in (8.16). Similarly, for multiplexed transmission, we can obtain

$$-\ddot{R}_1(0) = |c_{11}|^4 - |c_{21}|^4 + \frac{2|c_{11}|^2|c_{12}|^2(|c_{11}|^2 - |c_{21}|^2)}{\theta(|c_{22}|^2 - |c_{12}|^2)}, \tag{8.26}$$

$$-\ddot{R}_2(0) = |c_{22}|^4 - |c_{12}|^4 + \frac{2|c_{22}|^2|c_{21}|^2\theta(|c_{22}|^2 - |c_{12}|^2)}{|c_{11}|^2 - |c_{21}|^2}. \tag{8.27}$$

From the above expression, we can easily see that

$$S_1 = \frac{2(|c_{11}|^2 - |c_{21}|^2)}{|c_{11}|^2 + |c_{21}|^2 + \frac{2|c_{11}|^2|c_{12}|^2}{\theta(|c_{22}|^2 - |c_{12}|^2)}}, \tag{8.28}$$

$$S_2 = \frac{2(|c_{22}|^2 - |c_{12}|^2)}{|c_{22}|^2 + |c_{12}|^2 + \frac{2|c_{22}|^2|c_{21}|^2\theta}{|c_{11}|^2 - |c_{21}|^2}}. \tag{8.29}$$

Considering different values of θ leads to the slope region given in (8.17). □

8.3 the Impact of Secrecy on Energy Efficiency

For comparison, we provide below the minimum energy per bit and slope region when there are no secrecy constraints [9]. The minimum bit energies for both TDMA and multiplexed transmission are

$$\frac{E_1}{N_0}_{\min} = \frac{\log_e 2}{|c_{11}|^2}, \tag{8.30}$$

$$\frac{E_2}{N_0}_{\min} = \frac{\log_e 2}{|c_{22}|^2}. \tag{8.31}$$

The achievable slope region for TDMA is

$$\begin{aligned} 0 &\leqslant S_1 < 2 \\ 0 &\leqslant S_2 < 2 \\ S_1 + S_2 &= 2, \end{aligned} \tag{8.32}$$

while for multiplexed transmission, we have

$$\begin{aligned} 0 &\leqslant S_1 < 2 \\ 0 &\leqslant S_2 < 2 \\ (\frac{2}{S_1} - 1)(\frac{2}{S_2} - 1) &= 4\frac{|c_{12}|^2}{|c_{22}|^2}\frac{|c_{21}|^2}{|c_{11}|^2}. \end{aligned} \tag{8.33}$$

We can immediately note that the minimum bit energies in (8.30) and (8.31) are strictly smaller than those given in (8.12) and (8.13). Thus, there is an energy penalty associated with secrecy. Moreover, comparing the slope regions in (8.16) and (8.17) with those in (8.32) and (8.33), and noting that

$$\begin{aligned} A &< 1 \\ B &< 1 \\ 4\frac{|c_{12}|^2}{|c_{22}|^2}\frac{|c_{21}|^2}{|c_{11}|^2} &< \frac{4|c_{11}|^2|c_{12}|^2|c_{22}|^2|c_{21}|^2}{(|c_{11}|^4 - |c_{21}|^4)(|c_{22}|^4 - |c_{12}|^4)}, \end{aligned} \tag{8.34}$$

we can easily verify that the slope region of Gaussian weak interference channel is strictly larger than the slope region of Gaussian weak interference channel with confidential messages for both TDMA and multiplexed transmission schemes. Thus, in addition to the increase in the minimum energy per bit, secrecy introduces a penalty in terms of the achievable wideband slope values. In Figs. 8.2 and 8.3, we plot the slope regions for TDMA and multiplexed transmissions, respectively, under secrecy constraints. We note that regions become smaller as $|c_{12}|^2$ and $|c_{21}|^2$ increase. This is due to the fact that for fixed $|c_{11}|^2$ and $|c_{22}|^2$, the larger values of $|c_{12}|^2$ and $|c_{21}|^2$ mean that channel of the unintended receiver gets stronger and we have to use more energy to achieve the same secrecy transmission rate.

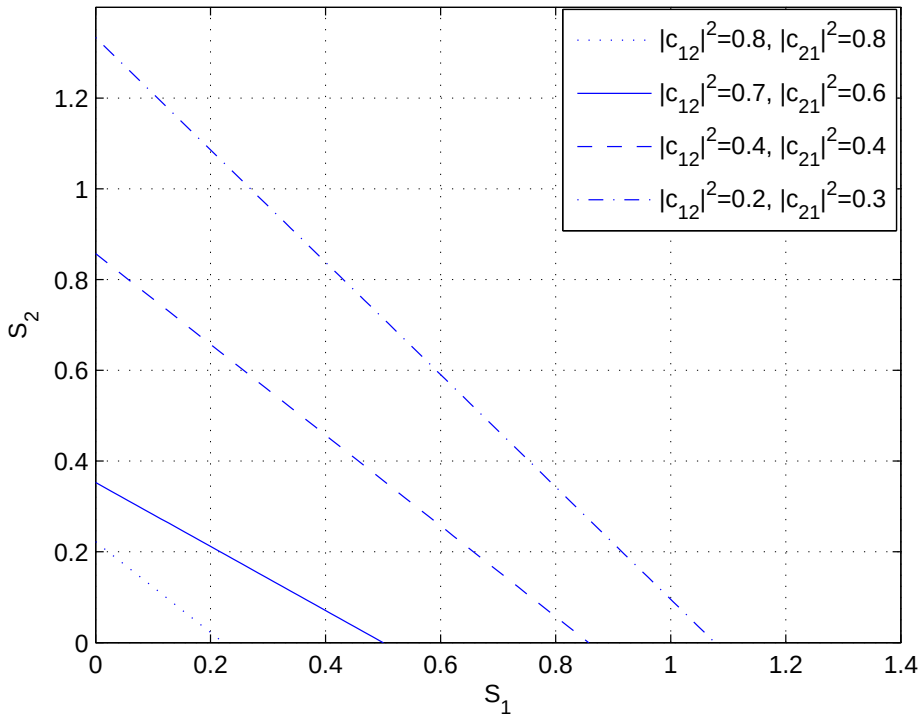

Figure 8.2: Slope regions in the Gaussian interference channel with confidential messages for the TDMA scheme with $|c_{11}|^2 = |c_{22}|^2 = 1$ and various values of $|c_{12}|^2, |c_{21}|^2$

.

We are also interested in determining which transmission scheme performs better in the low-SNR regime. TDMA achievable rate regions converge to those of multiplexed transmission scheme as power decreases. Furthermore, TDMA and multiplexed transmission has the same minimum energy per bit values. Therefore, we should consider the slope regions. From Theorem 6, we know that when

$$\frac{4|c_{11}|^2|c_{12}|^2|c_{22}|^2|c_{21}|^2}{(|c_{11}|^4 - |c_{21}|^4)(|c_{22}|^4 - |c_{12}|^4)} < 1, \tag{8.35}$$

the slope region of multiplexed transmission is strictly larger than the slope region

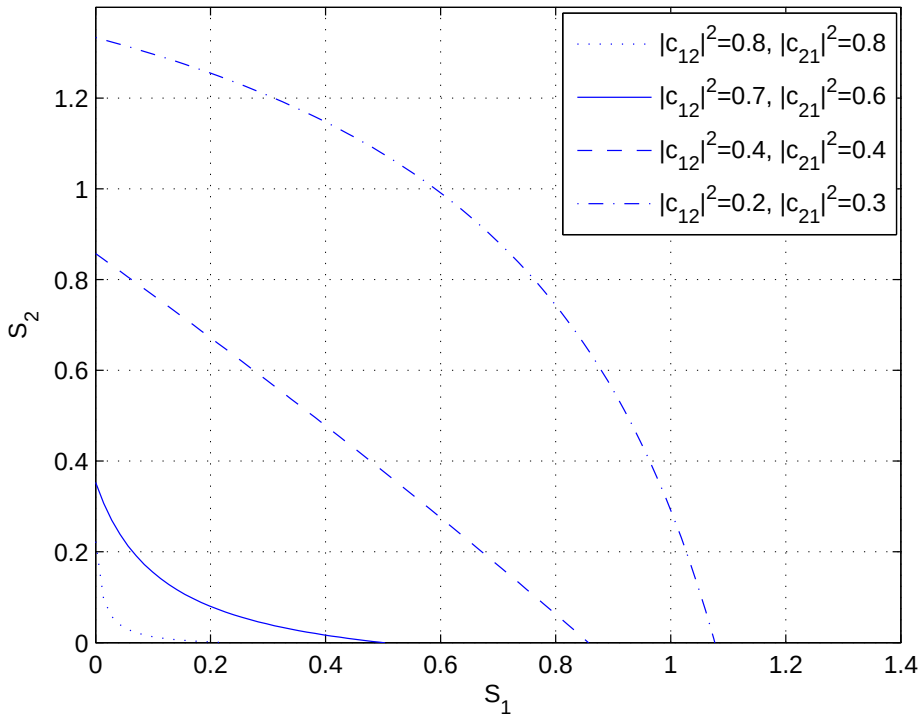

Figure 8.3: Slope regions in the Gaussian interference channel with confidential messages for multiplexed transmission scheme with $|c_{11}|^2 = |c_{22}|^2 = 1$ and various values of $|c_{12}|^2, |c_{21}|^2$

.

of TDMA, thus in this case, multiplexed transmission is preferred. On the other hand, when

$$\frac{4|c_{11}|^2|c_{12}|^2|c_{22}|^2|c_{21}|^2}{(|c_{11}|^4 - |c_{21}|^4)(|c_{22}|^4 - |c_{12}|^4)} > 1, \tag{8.36}$$

the slope region of TDMA is larger than the slope region of multiplexed transmission. Hence, TDMA should be used in this scenario. Finally, when

$$\frac{4|c_{11}|^2|c_{12}|^2|c_{22}|^2|c_{21}|^2}{(|c_{11}|^4 - |c_{21}|^4)(|c_{22}|^4 - |c_{12}|^4)} = 1, \tag{8.37}$$

the slope regions of TDMA and multiplexed transmission converge to the same triangular region. In this case, TDMA should still be preferred due to its representational advantages. These results show parallels to those obtained in [9] in the absence of secrecy constraints. In [9], the function that is compared with one is $4\frac{|c_{12}|^2}{|c_{22}|^2}\frac{|c_{21}|^2}{|c_{11}|^2}$. From (8.34), we see that when we vary the channel parameters, $\frac{4|c_{11}|^2|c_{12}|^2|c_{22}|^2|c_{21}|^2}{(|c_{11}|^4-|c_{21}|^4)(|c_{22}|^4-|c_{12}|^4)}$ is more likely to be greater than one than $4\frac{|c_{12}|^2}{|c_{22}|^2}\frac{|c_{21}|^2}{|c_{11}|^2}$ is. This observation lets us conclude that under secrecy constraints, TDMA is more likely to be the optimal transmission scheme. In particular, when

$$\left(\frac{|c_{11}|^2}{|c_{21}|^2}-\frac{|c_{21}|^2}{|c_{11}|^2}\right)\left(\frac{|c_{22}|^2}{|c_{12}|^2}-\frac{|c_{12}|^2}{|c_{22}|^2}\right)<4<\frac{|c_{11}|^2}{|c_{21}|^2}\frac{|c_{22}|^2}{|c_{12}|^2} \tag{8.38}$$

TDMA is preferred in secure transmissions while multiplexed transmission is preferred when there are no secrecy limitations. In Fig.8.4, we plot the slope regions when the channel parameters are $|c_{11}|^2=|c_{22}|^2=1, |c_{12}|^2=0.4, |c_{21}|^2=0.5$. As explained above, secrecy slope regions are inside the slope regions of Gaussian interference channel with no secrecy constraints. For secure transmissions, the region of TDMA is larger than that of multiplexed transmission while for transmissions without secrecy, the region of multiplexed transmission is larger. In Fig. 8.5, we plot the slope regions when the channel parameters are $|c_{11}|^2=|c_{22}|^2=1, |c_{12}|^2=0.1, |c_{21}|^2=0.2$. Here, we note that multiplexed transmission scheme is superior to TDMA scheme with and without secrecy constraints.

8.4 Conclusion

In this chapter, we have studied the achievable secrecy rates over Gaussian interference channel for TDMA, multiplexed and artificial noise schemes.

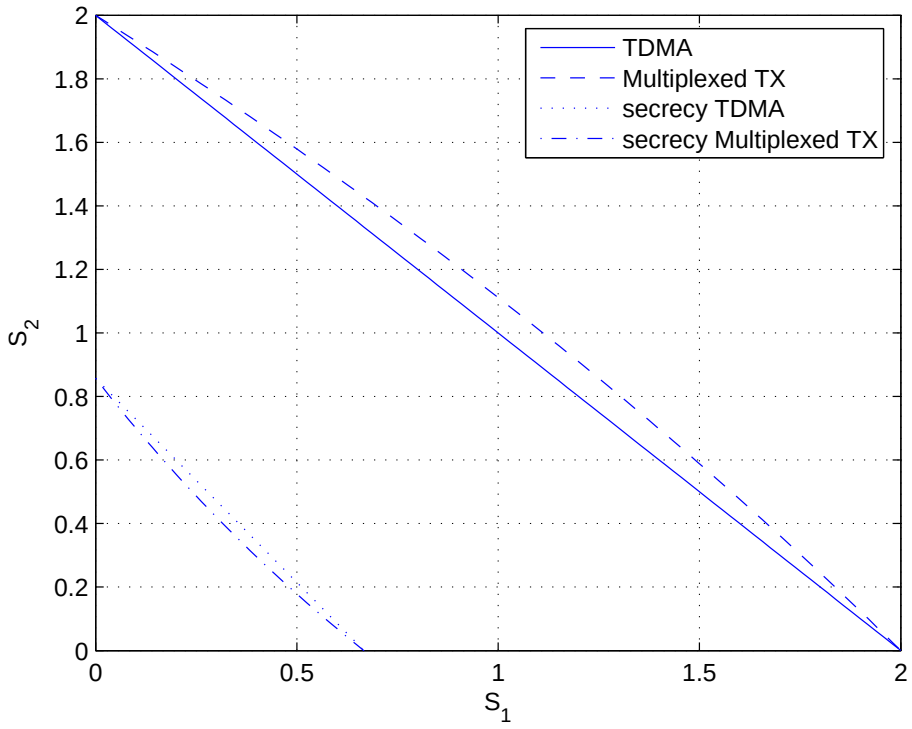

Figure 8.4: Slope regions in the Gaussian interference channel. $|c_{11}|^2 = |c_{22}|^2 = 1, |c_{12}|^2 = 0.4, |c_{21}|^2 = 0.5$

Although usually TDMA has the worst performance [45], we have noted that only TDMA can achieve positive secrecy rates for both users in the high-SNR regime. In the low-power regime, we have shown that TDMA is optimal when $\frac{4|c_{11}|^2|c_{12}|^2|c_{22}|^2|c_{21}|^2}{(|c_{11}|^4-|c_{21}|^4)(|c_{22}|^4-|c_{12}|^4)} \geqslant 1$. We have also shown that secrecy constraints introduce penalty in both the minimum bit energy and slope. Finally, we have shown that TDMA is more likely to be optimal in the presence of secrecy limitations.

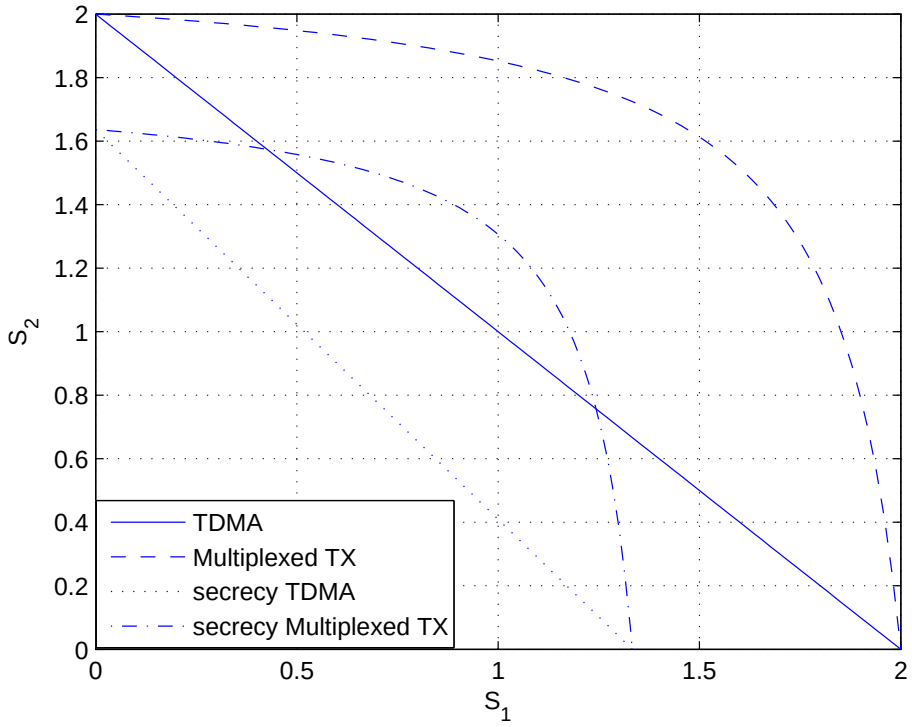

Figure 8.5: Slope regions in the Gaussian interference channel. $|c_{11}|^2 = |c_{22}|^2 = 1, |c_{12}|^2 = 0.1, |c_{21}|^2 = 0.2$

Appendix A

Proof of Theorem 1

Note that in AF relaying,

$$I(\mathbf{x}_s; \mathbf{y}_d, \mathbf{y}_{d,r} | \hat{h}_{sr}, \hat{h}_{sd}, \hat{h}_{rd}) = I(\mathbf{x}_{s1}; \mathbf{y}_{d1} | \hat{h}_{sd}) + I(\mathbf{x}_{s2}; \mathbf{y}_{d2}, \mathbf{y}_{d,r} | \hat{h}_{sr}, \hat{h}_{sd}, \hat{h}_{rd}) \tag{A.1}$$

where the first mutual expression on the right-hand side of (A.1) is for the direct transmission and the second is for the cooperative transmission. In the direct transmission, we have

$$\mathbf{y}_{d1} = \hat{h}_{sd}\mathbf{x}_{s1} + \mathbf{z}_{d1}. \tag{A.2}$$

In this setting, it is well-known that the worst-case noise $\mathbf{z}_{d1}$ is Gaussian [28, Appendix] and $\mathbf{x}_{s1}$ with independent Gaussian components achieves

$$\inf_{p_{z_{d1}}(\cdot)} \sup_{p_{x_{s1}}(\cdot)} I(\mathbf{x}_{s1}; \mathbf{y}_{d1} | \hat{h}_{sd}) = E\left\{(1-2\alpha)(m-2)\log\left(1 + \frac{P'_{s1}|\hat{h}_{sd}|^2}{\sigma^2_{z_{d1}}}\right)\right\}. \tag{A.3}$$

We now investigate the cooperative phase. Comparing (2.14) and (2.15) with (2.17) and (2.18), we see that non-overlapped can be obtained as a special case of over-

lapped AF scheme by letting $x'_{s2} = 0$. Therefore, we concentrate on the more general case of overlapped transmission. For better illustration, we rewrite the symbol-wise channel input-output relationships in the following:

$$y_r[i] = \hat{h}_{sr} x_{s2}[i] + z_r[i], \quad y_{d2}[i] = \hat{h}_{sd} x_{s2}[i] + z_{d2}[i], \tag{A.4}$$

for $i = 1 + (1-2\alpha)(m-2), ..., (1-\alpha)(m-2)$, and

$$y_{d,r}[i] = \hat{h}_{sd} x'_{s2}[i] + \hat{h}_{rd} x_r[i] + z_{d,r}[i], \tag{A.5}$$

for $i = (1-\alpha)(m-2)+1, ..., m-2$. In AF, the signals received and transmitted by the relay have following relation:

$$x_r[i] = \beta y_r[i - \alpha(m-2)], \quad \text{where} \quad \beta \leqslant \sqrt{\frac{E\{|x_r|^2\}}{|\hat{h}_{sr}|^2 E\{|x_{s2}|^2\} + E\{|z_r|^2\}}}. \tag{A.6}$$

Now, we can write the channel in the vector form

$$\underbrace{\begin{pmatrix} y_{d2}[i] \\ y_{d,r}[i+\alpha(m-2)] \end{pmatrix}}_{\check{\mathbf{y}}_d[i]} = \underbrace{\begin{pmatrix} \hat{h}_{sd} & 0 \\ \hat{h}_{rd}\beta\hat{h}_{sr} & \hat{h}_{sd} \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} x_s[i] \\ x_s[i+\alpha(m-2)] \end{pmatrix}}_{\check{\mathbf{x}}_s[i]} + \underbrace{\begin{pmatrix} 0 & 1 & 0 \\ \hat{h}_{rd}\beta & 0 & 1 \end{pmatrix}}_{B} \underbrace{\begin{pmatrix} z_r[i] \\ z_{d2}[i] \\ z_{d,r}[i+\alpha(m-2)] \end{pmatrix}}_{\mathbf{z}[i]} \tag{A.7}$$

where $i = 1 + (1-2\alpha)(m-2), ..., (1-\alpha)(m-2)$ and $\beta \leqslant \sqrt{\frac{E\{|x_r|^2\}}{|\hat{h}_{sr}|^2 E\{|x_s|^2\} + E\{|z_r|^2\}}}$. Note that we have defined $\mathbf{x}_s = [\mathbf{x}_{s1}^T, \mathbf{x}_{s2}^T, \mathbf{x}_{s2}'^T]^T$, and the expression in (A.7) uses the property that $x_{s2}(j) = x_s(j + (1-2\alpha)(m-2))$ and $x'_{s2}(j) = x_s(j + (1-\alpha)(m-2))$

for $j = 1, \ldots, \alpha(m-2)$. The input-output mutual information in the cooperative phase can now be expressed as

$$I(\mathbf{x}_{s2}, \mathbf{x}'_{s2}; \mathbf{y}_{d2}, \mathbf{y}_{d,r} | \hat{h}_{sr}, \hat{h}_{sd}, \hat{h}_{rd}) = \sum_{i=1+(1-2\alpha)(m-2)}^{(1-\alpha)(m-2)} I(\check{\mathbf{x}}_s[i]; \check{\mathbf{y}}_d[i] | \hat{h}_{sr}, \hat{h}_{sd}, \hat{h}_{rd}) = \alpha(m-2) I(\check{\mathbf{x}}_\mathbf{s}; \check{\mathbf{y}}_d | \hat{h}_{sr} \hat{h}_{sd}, \hat{h}_{rd}) \tag{A.8}$$

where in (A.8) we removed the dependence on i without loss of generality. Note that $\check{\mathbf{x}}_s$ and $\check{\mathbf{y}}_d$ are defined in (A.7). Now, we can calculate the worst-case capacity by proving that Gaussian distribution for z_r, z_{d2}, and $z_{d,r}$ provides the worst case. We employ techniques similar to that in [28, Appendix]. Any set of particular distributions for z_r, z_{d2}, and $z_{d,r}$ yields an upper bound on the worst case. Let us choose z_r, z_{d2}, and $z_{d,r}$ to be zero mean complex Gaussian distributed. Then as in [40, Appendix II],

$$\inf_{p_{z_r}(\cdot), p_{z_{d2}}(\cdot), p_{z_{d,r}}(\cdot)} \sup_{p_{x_{s2}}(\cdot), p_{x'_{s2}}(\cdot)} I(\check{\mathbf{x}}_\mathbf{s}; \check{\mathbf{y}}_d | \hat{h}_{sr}, \hat{h}_{sd}, \hat{h}_{rd}) \leq E \log\det \left(\mathbf{I} + (AE\{\check{\mathbf{x}}_\mathbf{s} \check{\mathbf{x}}_\mathbf{s}^\dagger\} A^\dagger)(BE\{\mathbf{z}\mathbf{z}^\dagger\} B^\dagger)^{-1} \right) \tag{A.9}$$

where the expectation is with respect to the fading estimates. To obtain a lower bound, we compute the mutual information for the channel in (A.7) assuming that $\check{x}_s$ is a zero-mean complex Gaussian with variance $E\{\check{\mathbf{x}}_\mathbf{s} \check{\mathbf{x}}_\mathbf{s}^\dagger\}$, but the distributions of noise components z_r, z_{d2}, and $z_{d,r}$ are arbitrary. In this case, we have

$$\begin{aligned} I(\check{\mathbf{x}}_\mathbf{s}; \check{\mathbf{y}}_d; | \hat{h}_{sr}, \hat{h}_{sd}, \hat{h}_{rd}) &= h(\check{\mathbf{x}}_\mathbf{s} | \hat{h}_{sr}, \hat{h}_{sd}, \hat{h}_{rd}) - h(\check{\mathbf{x}}_\mathbf{s} | \check{\mathbf{y}}_d, \hat{h}_{sr}, \hat{h}_{sd}, \hat{h}_{rd}) \\ &\geqslant \log \pi e E\{\check{\mathbf{x}}_\mathbf{s} \check{\mathbf{x}}_\mathbf{s}^\dagger\} - \log \pi e \, var(\check{\mathbf{x}}_\mathbf{s} | \check{\mathbf{y}}_d, \hat{h}_{sr}, \hat{h}_{sd}, \hat{h}_{rd}) \end{aligned} \tag{A.10}$$

where the inequality is due to the fact that Gaussian distribution provides the largest entropy and hence [14, Chap. 9]

$$h(\check{\mathbf{x}}_\mathbf{s}|\check{\mathbf{y}}_d, \hat{h}_{sr}, \hat{h}_{sd}, \hat{h}_{rd}) \leq \log \pi e \, var(\check{\mathbf{x}}_\mathbf{s}|\check{\mathbf{y}}_d, \hat{h}_{sr}, \hat{h}_{sd}, \hat{h}_{rd}).$$

Above, $h()$ denotes the differential entropy functional. From [28, Lemma 1, Appendix], we know that

$$var(\check{\mathbf{x}}_\mathbf{s}|\check{\mathbf{y}}_d, \hat{h}_{sr}, \hat{h}_{sd}, \hat{h}_{rd}) \leqslant E\left\{(\check{\mathbf{x}}_\mathbf{s} - \hat{\check{\mathbf{x}}}_s)(\check{\mathbf{x}}_\mathbf{s} - \hat{\check{\mathbf{x}}}_s)^\dagger | \hat{h}_{sr}, \hat{h}_{sd}, \hat{h}_{rd}\right\} \tag{A.11}$$

for any estimate $\hat{\check{\mathbf{x}}}_s$ given $\check{\mathbf{y}}_d, \hat{h}_{sr}, \hat{h}_{sd}$, and $\hat{h}_{rd}$. If we substitute the linear minimum mean-square-error (LMMSE) estimate $\hat{\check{\mathbf{x}}}_s = R_{\check{\mathbf{x}}\check{\mathbf{y}}} R_{\check{\mathbf{y}}}^{-1} \check{\mathbf{y}}_d$, where $R_{\check{\mathbf{x}}\check{\mathbf{y}}}$ and $R_{\check{\mathbf{y}}}$ are cross-covariance and covariance matrices respectively, into (A.10) and (A.11), we obtain[1]

$$I(\check{\mathbf{x}}_\mathbf{s}; \check{\mathbf{y}}_d | \hat{h}_{sr}, \hat{h}_{sd}, \hat{h}_{rd}) \geq E \log\det\left(\mathbf{I} + (E\{|x_s|^2\} A A^\dagger)(BE\{\mathbf{z}\mathbf{z}^\dagger\}B^\dagger)^{-1}\right). \tag{A.12}$$

Since the lower bound (A.12) applies for any noise distribution, we can easily see that

$$\inf_{p_{z_r}(\cdot), p_{z_{d2}}(\cdot), p_{z_{d,r}}(\cdot)} \sup_{p_{x_{s2}}(\cdot), p_{x'_{s2}}(\cdot)} I(x_s; \check{\mathbf{y}}_d | \hat{h}_{sr}, \hat{h}_{sd}, \hat{h}_{rd}) \geqslant E \log\det\left(\mathbf{I} + (AE\{\check{\mathbf{x}}_\mathbf{s}\check{\mathbf{x}}_\mathbf{s}^\dagger\}A^\dagger)(BE\{\mathbf{z}\mathbf{z}^\dagger\}B^\dagger)^{-1}\right). \tag{A.13}$$

[1]Here, we use the property that $\det(\mathbf{I} + \mathbf{AB}) = \det(\mathbf{I} + \mathbf{BA})$.

From (A.9) and (A.13), we conclude that

$$\inf_{p_{z_r}(\cdot),p_{z_{d2}}(\cdot),p_{z_{d,r}}(\cdot)} \sup_{p_{x_{s2}}(\cdot),p_{x'_{s2}}(\cdot)} I(x_s;\check{\mathbf{y}}_d|\hat{h}_{sr},\hat{h}_{sd},\hat{h}_{rd})$$

$$= E\log\det\left(\mathbf{I}+(AE\{\check{\mathbf{x}}_\mathbf{s}\check{\mathbf{x}}_\mathbf{s}^\dagger\}A^\dagger)(BE\{\mathbf{z}\mathbf{z}^\dagger\}B^\dagger)^{-1}\right) \tag{A.14}$$

$$= E\log\left\{1+\frac{P_{s1}|\hat{h}_{sd}|^2}{\sigma^2_{z_{d2}}}+f\left(\frac{P_{s1}|\hat{h}_{sr}|^2}{\sigma^2_{z_r}},\frac{P_{r1}|\hat{h}_{rd}|^2}{\sigma^2_{z_{d,r}}}\right)\right.$$
$$\left.+\,q\left(\frac{P_{s1}|\hat{h}_{sd}|^2}{\sigma^2_{z_{d2}}},\frac{P_{s2}|\hat{h}_{sd}|^2}{\sigma^2_{z_{d,r}}},\frac{P_{s1}|\hat{h}_{sr}|^2}{\sigma^2_{z_r}},\frac{P_{r1}|\hat{h}_{rd}|^2}{\sigma^2_{z_{d,r}}}\right)\right\} \tag{A.15}$$

In obtaining (A.15), we have used the fact that $E\{\check{\mathbf{x}}_\mathbf{s}\check{\mathbf{x}}_\mathbf{s}^\dagger\} = \begin{pmatrix} P_{s1} & 0 \\ 0 & P_{s2} \end{pmatrix}$. Note also that in (A.15), P_{s1}, P_{s2} and P_{r1} are the powers of source and relay symbols and are given in (2.29)–(2.31). Moreover, $\sigma^2_{z_{d2}}, \sigma^2_{z_r}, \sigma^2_{z_{d,r}}$ are the variances of the noise components defined in (2.20). Now, combining (2.23), (A.1), (A.3), and (A.15), we obtain the achievable rate expression in (2.24). Note that (2.25)–(2.28) are obtained by using the expressions for the channel estimates in (3.8)–(2.7) and noise variances in (2.21) and (2.22). □

Appendix B

Proof of Theorem 2

For DF with repetition coding in overlapped transmission, an achievable rate expression is

$$I(\mathbf{x}_{s1};\mathbf{y}_{d1}|\hat{h}_{sd}) + \min\left\{I(\mathbf{x}_{s2};\mathbf{y}_r|\hat{h}_{sr}), I(\mathbf{x}_{s2},\mathbf{x}'_{s2};\mathbf{y}_d,\mathbf{y}_{d,r}|\hat{h}_{sd},\hat{h}_{rd})\right\}. \tag{B.1}$$

Note that the first and second mutual information expressions in (B.1) are for the direct transmission between the source and destination, and direct transmission between the source and relay, respectively. Therefore, as in the proof of Theorem 1, the worst-case achievable rates can be immediately seen to be equal to the first term on the right-hand side of (2.32) and I_1, respectively.

In repetition coding, after successfully decoding the source information, the relay transmits the same codeword as the source. As a result, the input-output

relation in the cooperative phase can be expressed as

$$\underbrace{\begin{pmatrix} y_{d2}[i] \\ y_{d,r}[i+\alpha(m-2)] \end{pmatrix}}_{\check{\mathbf{y}}_d[i]} = \underbrace{\begin{pmatrix} \hat{h}_{sd} & 0 \\ \hat{h}_{rd}\beta & \hat{h}_{sd} \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} x_s[i] \\ x_s[i+\alpha(m-2)] \end{pmatrix}}_{\check{\mathbf{x}}_s[i]} + \underbrace{\begin{pmatrix} z_{d2}[i] \\ z_{d,r}[i+\alpha(m-2)] \end{pmatrix}}_{\mathbf{z}[i]}. \tag{B.2}$$

where $\beta \leq \sqrt{\frac{E\{|x_r|^2\}}{E\{|x_s|^2\}}}$. From (B.2), it is clear that the knowledge of $\hat{h}_{sr}$ is not required at the destination. We can easily see that (B.2) is a simpler expression than (A.7) in the AF case, therefore we can adopt the same methods as employed in the proof of Theorem 1 to show that Gaussian noise is the worst noise and I_2 is the worst-case rate. □

Bibliography

[1] Special issue on models, theory, and codes for relaying and cooperation in communication networks. *IEEE Trans. Inform. Theory*, 53(9).

[2] A. Abdelkader, S. Shahbazpanahi, and A. B. Gershman. Joint subcarrier power loading and distributed beamforming in ofdm-based asynchronous relay networks. In *IEEE CAMSAP*, Aruba, Dec 2009. 4.3

[3] V. Aggarwal, L. Sankar, A. R. Calderbank, and H. V. Poor. Secrecy capacity of a class of orthogonal relay eavesdropper channels. *Available: http://arxiv.org/abs/0812.2275*. 1.3

[4] S. Akin and M. C. Gursoy. Achievable rates and training optimization for fading relay channels with memory. In *the 42nd Annual Conference on Information Sciences and Systems (CISS)*, Princeton University, Mar. 2008.

[5] A. S. Avestimehr and D. N. C. Tse. Outage capacity of the fading relay channel in the low-snr regime. *IEEE Trans. Inform. Theory*, 53(4):1401 – 1415. 1.2

[6] M. Bengtsson and B. Ottersten. Optimal downlink beamforming using semidefinite optimization. In *Proc. 37th Annual Allerton Conference on Communication, Control and Computing*, Sep 1999. 4.3

[7] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin. Wireless information-theoretic security. *IEEE Trans. Inform. Theory*, 54(6):2515–2534. 1.3

[8] S. Boyd and L. Vandenberghe. *Convex optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[9] G. Caire, D. Tuninetti, and S. Verdú. Suboptimality of tdma in the low-power regime. *IEEE Trans. Inform. Theory*, 50(4). 1.1, 8.2, 8.3, 8.3

[10] B. K. Chalise and A. Czylwik. Robust uplink beamforming based upon minimum outage probability criterion. In *IEEE Globecomm*, Sep 2004. 4.3, 4.3, 4.3

[11] H. Chen, A. B. Gershman, and S. Shahbazpanahi. Filter-and-forward distributed beamforming in relay networks with frequency selective fading. *IEEE Trans. on Signal Proc.*, 58(3). 4.3

[12] H. Chen, A. B. Gershman, and S. Shahbazpanahi. Distributed peer-to-peer beamforming for multiuser relay networks. In *Proc. IEEE Intl Conf. Acoust. Speech Signal Proc.*, Taipei, Taiwan, Apr. 2009. 4.1.2.2

[13] T. M. Cover and A. A. El Gamal. Capacity theorems for the relay channel. *IEEE Trans. Inf. Theory*, (5):572–584. 1.1

[14] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. New York: Wiley, 1991. A

[15] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Trans. Inform. Theory*, (3):339–348. 4.1

[16] L. Dong, Z. Han, A. Petropulu, and H. V. Poor. Improving wireless physical layer security via cooperating relays. *IEEE Trans. on Signal Proc.*, 58(3). 1.3

[17] L. Dong, Z. Han, A. Petropulu, and H. V. Poor. Secure wireless communications via cooperation. In *Proc. 46th Annual Allerton Conf. Commun., Control, and Computing*, Monticello, IL, Sept. 2008. 1.3, 4.1.1

[18] L. Dong, Z. Han, A. Petropulu, and H. V. Poor. Amplify-and-forward based cooperation for secure wireless communications. In *Proc. IEEE Intl Conf. Acoust. Speech Signal Proc.*, Taipei, Taiwan, Apr. 2009. 1.3, 4.1.1

[19] A. A. El Gamal and M. Aref. The capacity of the semideterministic relay channel. *IEEE Trans. Inf. Theory*, (3):536–536. 1.1

[20] F. Gao, T. Cui, and A. Nallanathan. On channel estimation and optimal training design for amplify and forward relay networks. *IEEE Trans. Wireless. Commun.*, 7(5):1907 – 1916. 1.2

[21] A. B. Gershman, N. D. Sidiropoulos, S. Shahbazpanahi, M. Bengtsson, and B. Ottersten. Convex optimization-based beamforming: from receive to transmit and network designs. *IEEE Signal Proc. Mag.*, 27(3). 1.3

[22] A. Ghasemi and E. S. Sousa. Fundamental limits of spectrum-sharing in fading environments. *IEEE Trans. Wireless. Comunication*, 6(2):649–658. 1.4, 3

[23] G. Golub and C. F. Van Loan. *Matrix Computations*. Johns Hopkins University Press, third edition, 1996. 1, 2

[24] P. K. Gopala, L. Lai, , and H. E. Gamal. On the secrecy capacity of fading channels. *IEEE Trans. Inform. Theory*, 54(10):4687–4698. 1.3, 4.1, 7.2, 4, 7.4.1, 7.4.2, 7.5

[25] D. Gunduz and E. Erkip. Opportunistic cooperation by dynamic resource allocation. *IEEE Trans. Wireless. Commun.*, 6(4):1446–1454. 1.1

[26] M. C. Gursoy. An energy efficiency perspective on training for fading channels. In *IEEE Intl Symp. on Inform. Theory*, Nice ,France, July 2007. 2.2.1, 3.2.1, 4.1.1.2

[27] M. C. Gursoy. Secure communication in the low-snr regime: A characterization of the energy-secrecy tradeoff. In *Proc. of the IEEE International Symposium on Information Theory (ISIT)*, Seoul, Korea, July. 2009.

[28] B. Hassibi and B. M. Hochwald. How much training is needed in multiple-antenna wireless link? *IEEE Trans. Inform. Theory*, 49(4):951–964. 2.3, A, A, A

[29] S. Haykin. Cognitive radio: brain-empowered wireless communicatioins. *IEEE J. Sel. Areas Commun*, 23(2):201–220. 1.4

[30] A. Host-Madsen. Capacity bounds for cooperative diversity. *IEEE Trans. Inform. Theory*, 52(4):1522–1544.

[31] A. Host-Madsen and J. Zhang. Capacity bounds and power allocation for wireless relay channels. *IEEE Trans. Inform. Theory*, 51(6):2020–2040. 1.1

[32] Y. Jia and A. Vosoughi. Impact of channel estimation error upon sum-rate in amplify-and-forward two-way relaying systems. In *Proceedings of the IEEE SPAWC*, 2010. 1.2

[33] B. Jiang, F. Gao, X. Gao, and A. Nallanathan. Channel estimation and training design for two-way relay networks with power allocation. *IEEE Trans. Wireless. Comunication*, 9(6). 1.2

[34] Y. Jing and H. Jafarkhani. Network beamforming using relays with perfect channel information. *IEEE Trans. Inf. Theory.*, 55(6):2499–2517. 1.3

[35] Y. Jing and H. Jafarkhani. Network beamforming using relays with perfect channel information. In *IEEE International Conference on Acoustics, Speech, and Signal Processing*, Honolulu, Hawaii, Apr 2007. 1.3

[36] A. Khisti. Algorithms and architectures for multiuser, multiterminal, and multilayer information-theoretic security. *Doctoral Thesis, MIT*. 1.3, 4.1.1.1, 5.3, 5.3.1

[37] G. Kramer, M. Gastpar, and P. Gupta. Cooperative strategies and capacity theorems for relay networks. *IEEE Trans. Inform. Theory*, 51(9):3037–3063. 1.3

[38] G. Kramer, I. Mari'c, and R. D. Yates. Cooperative communications. *Foundations and Trends in Networking. Hanover, MA: NOW Publishers*, 1(3). 2.4

[39] J. N. Laneman. *ch.1 Cooperative Diversity: Models, Algorithms, and Architectures, Cooperation in wireless networks: Principles and applications*. Springer, 2006. 1.1, 2.2.2.1, 2.3

[40] J. N. Laneman, D. N. C. Tse, and G. W. Wornel. Cooperative diversity in wireless networks: Efficient protocols and outage behavior. *IEEE Trans. Inf. Theory*, 50. 1.1, 1.3, 2.2.2.1, A

[41] P. Larsson, N. Johansson, , and K.-E. Sunell. Coded bidirectional relaying. In *Proc. IEEE Veh. Tech. Conf., vol. 2.*, Melbourne, Australia, May 2006. 1.1

[42] S. K. Leung-Yan-Cheong and M. E. Hellman. The gaussian wire-tap channel. *IEEE Trans. Inform. Theory*, (4):451–456. 1.3, 4.1, 4.1, 8.1.1

[43] Y. Liang and V. V. Veeravalli. Gaussian orthogonal relay channels: Optimal resource allocation and capacity. *IEEE Trans. Inform. Theory*, 51(9):3284–3289. 1.1, 1.3, 2.3

[44] Y. Liang, V. V. Veeravalli, and H. Vincent Poor. Resource allocation for wireless fading relay channels: Max-min solution. *IEEE Trans. Inform. Theory*, 53(10):3432–3453. 1.1

[45] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates. Discrete memoryless interference and broadcast channels with confidential messages: Secrecy capacity regions. *IEEE Trans. Inform. Theory*, 54(6):2493–2507. 1.3, 5.2, 8.1, 8.1.1, 8.1.2, 8.1.3, 8.1.3, 8.4

[46] R. Liu and H. V. Poor. Secrecy capacity region of a multi-antenna gaussian broadcast channel with confidential messages. *IEEE Trans. Inform. Theory*, 55(3):1235–1249. 1.3

[47] J. Lofberg. Yalmip: A toolbox for modeling and optimization in matlab. In *Proc. the CACSD Conf.*, Taipei, Taiwan, 2004. 4.1.2.1, 6.2

[48] Z-Q Luo, Wing kin Ma, A.M.-C. So, Yinyu Ye, and Shuzhong Zhang. Semidefinite relaxation of quadratic optimization problems. *IEEE Signal Proc. Mag..*, 27(3). 4.2.2, 6.2, 1

[49] H. Mahdavifar and A. Vardy. Achieving the secrecy capacity of wiretap channels using polar codes. In *IEEE Intl Symp. on Inform. Theory*, Austin, Tx, June 2010. 4.1

[50] M. Medard. The effect upon channel capacity in wireless communication of perfect and imperfect knowledge of the channel. *IEEE Trans. Inform. Theory*, 46(5):933–946.

[51] J. Mietzner, L. Lampe, and R. Schober. Distributed transmit power allocation for multihop cognitive-radio systems. *IEEE Trans. Wireless. Commun*, 8(10):5187–5201. 1.4

[52] P. Mitran, H. Ochiai, and V. Tarokh. Space-time diversity enhancements using collaborative communications. *IEEE Trans. Inform. Theory*, 51(6):2041–2057.

[53] T. Muharemovic and B. Aazhang. Robust slope region for wideband cdma with multiple antennas. In *Proc. 2003 IEEE Information Theory Workshop*, Paris, France, Mar. 2003.

[54] L. Musavian and S. Aissa. Capacity and power allocation for spectrum-sharing communications in fading channels. *IEEE Trans. Wireless. Comunication*, 8(1):148–156. 1.4, 3

[55] R. U. Nabar, H. Bolcskei, and F. W. Kneubuhler. Fading relay channels:performance limits and space-time signal design. *IEEE J.Select. Areas Commun.*, 22(6):1099–1109. 1.1, 1.3

[56] V. Nassab, S. Shahbazpanahi, A. Grami, and Z.-Q. Luo. Distributed beamforming for relay networks based on second order statistics of the channel state information. *IEEE Trans. on Signal Proc.*, 56(9):4306–4316. 1.3, 4.1.2.1

[57] C. T. K. Ng and A. Goldsmith. The impact of csi and power allocation on relay channel capacity and cooperation strategies. *IEEE Trans. Wireless Commun.*, 7(12):5380–5389. 1.1

[58] C. S. Patel and G. L. Stüber. Channel estimation for amplify and forward relay based cooperation diversity systems. *IEEE Trans. Wireless. Commun.*, 6(6):2348–2356. 1.2

[59] Y. Pei, Y-C. Liang, L. Zhang, K. C. Teh, and K. H. Li. Secure communication over miso cognitive radio channel. *IEEE Trans. Wireless. Commun*, 9(4):1494–1502. 1.4

[60] H. V. Poor. *An Introduction to Signal Detection and Estimation*. Springer-Verlag, second edition, March 1994.

[61] B. Rankov and A. Wittneben. Spectral efficient protocols for half-duplex fading relay channels. *IEEE J. Select. Areas Commun*, 25. 1.1

[62] A. Sendonaris, E. Erkip, and B. Aazhang. User cooperation diversity-part i: System description. *IEEE Trans. Commun.*, 51(11):1927–1938. 1.1

[63] A. Sendonaris, E. Erkip, and B. Aazhang. User cooperation diversity-part ii: Implementation aspects and performance analysis. *IEEE Trans. Commun.*, 51(11):1939–1948.

[64] S. Shafiee and S. Ulukus. Achievable rates in gaussian miso channels with secrecy constraint. In *IEEE Intl Symp. on Inform. Theory*, Nice ,France, July 2007. 1.3, 5.3

[65] J. Sturm. Using sedumi 1.02: A matlab toolbox for optimization over symmetric cones. *Opt. Methods and Software, Special issue on Interior Point Methods (CD supplement with software)*, 11. 4.1.2.1, 6.2

[66] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.Merolla. Applications of ldpc codes to the wiretap channel. *IEEE Trans. Inform. Theory*, 53(8):2933–2945. 4.1

[67] L. Tong, B. M. Sadler, and M. Dong. Pilot-assisted wireless transmission. *IEEE Signal Processing Mag.* 2.3

[68] E. C. van der Meulen. 'three-terminal communication channels. *Adv. Appl. Probab.*, 3. 1.1

[69] S. Verdú. Spectral efficiency in the wideband regime. *IEEE Trans. Inform. Theory*, 48(6). 1.1, 2.4, 8.2

[70] S. Verdú, G. Caire, and D. Tuninetti. Is tdma optimal in the low power regime? In *IEEE ISIT*, Lausanne, Switzerland, June/July 2002.

[71] B. Wang, J. Zhang, and L. Zheng. Achievable rates and scaling laws of power-constrained wireless sensory relay networks. *IEEE Trans. Inform. Theory*, 52(9). 1.2

[72] A. Wiesel, Y. C. Eldar, and S. Shamai. Linear precoding via conic optimization for fixed mimo receivers. *IEEE Trans. on Signal Proc.*, 54(3). 4.1.2.2

[73] A. Wyner. The wire-tap channel. *Bell. Syst Tech. J*, 54(8):1355–1387. 1.3, 4.1

[74] Y. Yao, X. Cai, and G. B. Giannakis. On energy efficiency and optimum resource allocation of relay tranmissions in the low-power regime. *IEEE Trans. Wireless Commun.*, 4(6):2917–2927. 1.1

[75] J. Zhang and M. C. Gursoy. Achievable rates and resource allocation strategies for imperfectly known fading relay channels. *EURASIP Journal on Wireless Communications and Networking*, 2009. 1.5, 3.2.2.1, 3.2.2.1

[76] J. Zhang and M. C. Gursoy. Achievable rates and optimal resource allocation for imperfectly-known relay channels. In *the 45th Annual Allerton Conference on Communication, Control and Computing*, University of Illinois at Urbana-Champaign, Sep. 2007. 1.5

[77] J. Zhang and M. C. Gursoy. To cooperate, or not to cooperate in imperfectly known fading channels. In *the 9th IEEE International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Recife, Brazil, July 2008. 1.5

[78] J. Zhang and M. C. Gursoy. Collaborative relay beamforming for secrecy. In *Proc. of the IEEE International Conference on Communication (ICC)*, Cape Town,South Africa, May 2010. 1.5, 6.3.1

[79] J. Zhang and M. C. Gursoy. Collaborative relay beamforming for secure broadcasting. In *Proc of Ithe IEEE Wireless Communications and Networking Conference (WCNC)*, Sydney, Austria, Apr. 2010. 1.5

[80] J. Zhang and M. C. Gursoy. Relay beamforming strategies for physical-layer security. In *Proc. of the 44th Annual Conference on Information Sciences and Systems*, Princeton,NJ, Mar. 2010. 1.5, 6.2

[81] J. Zhang and M. C. Gursoy. An achievable rate region for imperfectly-known two-way relay fading channels. In *Proc of IEEE International Symposium on Information Theory(ISIT)*, Saint Petersburg, Russia, July-August 2011. 1.5

[82] J. Zhang and M. C. Gursoy. Secure relay beamforming over cognitive radio channels. In *Proc. of the 45th Annual Conference on Information Sciences and Systems*, Baltimore,MD, Mar. 2011. 1.5

[83] L. Zhang, Y.-C. Liang, Y. Pei, and R. Zhang. Robust beamforming design: from cognitive radio miso channels to secrecy miso channels. In *IEEE Globecomm*, 2009. 4.3

[84] L. Zhang, R. Zhang, Y.-C. Liang, Y. Xin, and S. Cui. On the relationship between the multi-antenna secrecy communications and cognitive radio communications. In *Proc. 47th Annual Allerton Conf. Commun., Control, and Computing*, Monticello, IL, Sept. 2009. 4.1.2.1

[85] R. Zhang and Y-C. Liang. Exploiting multi-antenna for opportunistic spectrum sharing in cognitive radio networks. *IEEE J. Sel. Topics Signal Process.*, 2(2):88 – 102. 1.4

[86] G. Zheng, K. Wong, A. Paulraj, and B. Ottersten. Collaborative-relay beamforming with perfect csi: Optimum and distributed implementation. *IEEE Signal Process Letters*, 16(4). 1.3, 4.2.2, 1

[87] G. Zheng, K. K. Wong, A. Paulraj, and B. Ottersten. Robust collaborative-relay beamforming. *IEEE Trans. on Signal Proc.*, 57(9). 1.3