ABSTRACT

Title of dissertation: ALIGNMENT AND COOPERATION FOR SECRECY IN MULTI-USER CHANNELS

Raef Bassily
Doctor of Philosophy, 2011

Dissertation directed by: Professor Şennur Ulukuş
Department of Electrical and Computer Engineering

The study of the physical layer has offered a new perspective to the problem of communication security. This led to the development of a vast set of ideas and techniques rooted in information theory which can be employed in practice to provide unbreakable security. The information-theoretic approach relies mainly on the physical nature of the communication medium. In a wireless medium, the unique features of the wireless communication channel, such as its fading and broadcast nature, can be exploited to achieve higher secure information rates. In this dissertation, we study the secure transmission problem in wireless channels from an information-theoretic perspective.

We first consider the fading multiple access wiretap channel. We give two new achievable schemes that use the time-varying (fading) nature of the channel to align the interference from different users at the eavesdropper perfectly in a one-dimensional space while creating a higher-dimensional space for the interfering signals at the legitimate receiver hence allowing for better chance of recovery. While we achieve

this alignment through signal scaling at the transmitters in our first scheme (scaling based alignment), we let nature provide this alignment through the ergodicity of the channel coefficients in the second scheme (ergodic secret alignment). For each scheme, we show that the achievable secrecy rates scale logarithmically with the signal-to-noise ratio (SNR).

Next, we study the security gains that can be achieved in a wireless network by employing cooperation among the nodes which is possible due to the broadcast nature of the wireless channel. We investigate the role of passive (also known as deaf) cooperation in improving the achievable secrecy rates in a Gaussian multiple relay network with an external eavesdropper. We distinguish between two modes of deaf cooperation, namely, cooperative jamming (CJ) and noise forwarding (NF). We derive the conditions in which each mode of deaf cooperation achieves secrecy rates that are higher than the secrecy capacity of the original Gaussian wiretap channel. As a result, we show that a deaf helper cannot be a useful cooperative jammer and noise forwarder at the same time. We derive the optimal power control policy for each mode. We consider the deaf helper selection problem where a fixed-size set of deaf helpers (possibly operating in different modes) are to be selected from the set of available relays so that the achievable secrecy rate is maximized. We propose a simple and efficient suboptimal strategy for selection which is shown to be optimal when only one helper is selected.

Furthermore, we study the role of a multi-antenna deaf helper. Unlike the single antenna case, we show that, in general, it is useful to split the helper's power between cooperative jamming and noise forwarding. Hence, we propose a deaf cooperation

strategy for this model and derive its optimal power control policy. We also show, for specific class of relay-eavesdropper channels, that a simple cooperative jamming strategy yields a secrecy rate that approaches the secrecy capacity as the helper's power is increased.

Finally, we consider the role of active cooperation for secrecy in the multiple relay networks. We propose several relaying strategies for secure communication and derive the achievable secrecy rate for each strategy. In our strategies the relays decode the source signal and then forward it to the destination either in a single-hop or a multi-hop fashion. Each relay scales its transmitted signal in a way that ensures that signal components from different relays are canceled out at the eavesdropper.

ALIGNMENT AND COOPERATION FOR SECRECY IN MULTI-USER CHANNELS

by

Raef Bassily

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2011

Advisory Committee:

Professor Şennur Ulukuş, Chair/Advisor
Professor Prakash Narayan
Professor Adrian Papamarcou
Professor Armand Makowski
Professor Jonathan Katz

DEDICATION

To my precious daughter, my loving parents, and my beloved sister.

ACKNOWLEDGMENTS

I would like to thank my advisor Professor Şennur Ulukuş for her support, guidance, and patience over the past five years. She has set an example for me by her diligence and tireless devotion to her work. Her continuous encouragement in both research and teaching enabled me to gain a substantial professional experience that improved and polished my skills in these two honorable endeavors. I am also grateful to her for allowing me the freedom to take a variety of courses that had a significant positive impact on my learning.

I would like to thank Professors Prakash Narayan, Armand Makowski, Adrian Papamarcou, and Jonathan Katz for serving in my PhD dissertation committee and for their valuable suggestions. I am especially thankful to Professor Prakash Narayan and Professor Armand Makowski for the helpful and insightful technical discussions in various occasions. I am also thankful to Professor Jonathan Katz for carefully designing and teaching two rich courses on the theory of cryptography and the theory of computational complexity this year. Taking these courses was not only an exciting learning experience but was also very inspiring to me from a research perspective.

I also owe a word of thanks to my friends at Communications and Signal Processing Lab (CSPL), Pritam Mukherjee, Ersen Ekrem, Ravi Tandon, Omur Ozel, Jianwei Xie, Himanshu Tyagi, Berk Gurakan, Praneeth Boda, Nan Liu, Wei Kang, and Sirin Nitinawarat for several helpful and cheerful discussions.

I give very special thanks to my dear friends with whom life is enjoyable, George Zaki, Nof AbuZainab, Gianluca Quercini, Maya Kabkab, Anthony Fanous, and George Zoto. I would also like to thank my best friend for life, Bassem Kaldas, for being such a loyal friend even though we are thousands of miles apart.

I would never forget to thank the whole University of Maryland family for setting the right standards that draw a clear path to success and self-actualization based on integrity and honesty and for creating the appropriate conditions for productivity including the long list of recreational activities and facilities offered by the University.

Finally, I owe this accomplishment to my parents, Bahi and Mona Bassily, and my sister Randa Bassily whose abundant unconditional love, support, and encouragement have always been the backbone of every success I have achieved. Their words have been and will always be the candle of hope that lights my way, the flame of inspiration that ignites my soul, and the lighthouse of assurance that tells my heart to endure the storm knowing that the shore is near.

TABLE OF CONTENTS

LIST OF FIGURES

Chapter 1

Introduction

Secure transmission of information over communication channels has become an important design criterion in almost every communication system nowadays. Modern communication systems are designed and implemented with both reliability and security of communication in mind. Consequently, the aspect of secure communications has been subjected to careful theoretical study and investigation over the last few decades. As cryptography provides us with efficient and practical solutions for the security problem that are acceptable under reasonable conjectures within the framework of the theory of computational complexity, the underlying physical model of the communication process is not exploited in the cryptographic approach. On the other hand, the study of the physical layer offers a new interesting set of ideas and methods that takes into account the aspects of how communication takes place and exploits them to achieve unconditional security. The theoretical framework of this study is rooted in information theory and is referred to as *information-theoretic security*. Information-theoretic security not only provides us with fundamental limits on secure information rates but it can also provide us with methods and techniques to achieve or approach these limits.

The first rigorous information-theoretic treatment of the security aspect of communication was presented by Shannon [17] in 1949. In his model, a private, authenticated, and error-free link is assumed to be available between the legitimate communicating pair. This link is used by the communicating pair to agree on a key which is later used by one of them to encrypt its confidential message to the other on a public error-free channel where any transmission could be perfectly intercepted by an eavesdropper with unbounded computational power. Shannon showed that, to achieve perfect security in this model, the length of the key must be at least as long as the length of the confidential message. Later, in 1975, Wyner was the first to introduce the notion of information-theoretic security to channels with imperfections in his seminal work [21]. In his model, which is known as the *wiretap channel*, the sender and the receiver of the confidential message are connected by only one imperfect communication channel which is wiretapped by a passive but informed eavesdropper with unbounded computational power. Wyner showed that one can indeed exploit the channel randomness to pay for the extra randomness required to encrypt the message and achieve secure communication without the help of a private channel between the legitimate pair. In particular, Wyner introduced a measure for security called the equivocation which is defined as the conditional entropy of the message given the eavesdropper's observation normalized by the length of the transmission duration. Accordingly, for an information rate to be secure, the normalized mutual information between the message and the eavesdropper's observation must go to zero as the length of the transmission duration goes to infinity. Wyner obtained an expression for the supremum of the set of achievable secure information rates, i.e., the *secrecy capacity*

of the wiretap channel. However, in Wyner's model it was assumed that the received signal by the eavesdropper is a degraded version of the signal received by the legitimate receiver. This constraint was later removed by Csiszar and Korner in [4] where they obtained the secrecy capacity in the general case. For a model well-suited to the wireless channels, Leung-Yan-Cheong and Hellman obtained the secrecy capacity of the Gaussian wiretap channel in [13].

Starting from Wyner's work, the basic underlying idea of these works is that it is possible to exploit the characteristics of the communication channel which are dictated by the channel's conditional probability distribution to achieve information-theoretic security. When communication takes place in a wireless medium, the properties of the wireless channel, such as its fading and broadcast nature, can be effectively utilized to attain high secure rates. For example, fading can help improve the achievable secrecy rates if the sender knows the channel state information (CSI), by utilizing the varying nature of the fading wireless channel and by adjusting its transmit power so that more information is communicated when the channel condition of the legitimate receiver is better than that of the eavesdropper. In a multi-user fading wireless channel, one can take advantage of the fading phenomenon to align the interference from different users favorably at the legitimate receiver and unfavorably at the eavesdropper and hence increase the achievable secrecy rates. On the other hand, the broadcast nature of the wireless channel gives rise to two relevant concepts, namely, interference and cooperation. These two concepts are shown to be useful in the context of secure communication. In particular, in a cooperative wireless channel, a trusted node can help increase the secure communication rate of the legitimate pair either by introducing a

useful interference to confuse the eavesdropper and hence limit its ability to obtain any information about the transmitted message, i.e., by *passive (deaf) cooperation*, or by listening to the sender's transmission and accordingly helping communicate the sender's message to the receiver, i.e., by *active cooperation*.

In this dissertation, we study the ideas of alignment and cooperation in wireless multi-user channels through the study of two different channel models, namely, the fading multiple access wiretap (MAC-WT) channel and the relay-eavesdropper channel. We introduce new schemes to achieve high secure rates in these channel models. Our work reveals several interesting aspects about the incorporation of these notions into the multi-user channels and proposes efficient techniques that utilize these aspects to boost communication security in terms of the achievable secure rates. Interestingly, the work in this dissertation shows that schemes that were not useful when the secrecy constraint is not imposed may be very useful in the secrecy context.

Our motivation is to show the role of the physical layer in providing and improving security of communication in these aforementioned channel models from an information-theoretic perspective through the efficient use of the notions of alignment and cooperation. Although the results we obtain are theoretical in nature, several practical considerations of the proposed schemes are studied to provide useful insights on the security gains attainable by these schemes when used in practice. In the models studied in this dissertation, we assume that the eavesdropper's perfect channel state information is available at all the nodes in a causal fashion which, despite of being a standard assumption in many related works in this area, is not a practical assumption. However, the problem of providing information-theoretic security in wireless channel

models where nothing is known about the eavesdropper's channel state information is a challenging task and is still being investigated in current research in this area.

The MAC-WT channel was introduced in [19]. References [19] and [20] focus on the Gaussian MAC-WT, and provide achievable schemes based on i.i.d. Gaussian signaling. Reference [20] goes further than plain Gaussian signaling and introduces a technique that uses the power of a non-transmitting node in jamming the eavesdropper with i.i.d. Gaussian noise. This technique is referred to as Gaussian signaling based *cooperative jamming* (from this point on, we will refer to this technique as simply cooperative jamming, or CJ). A notable shortcoming of these i.i.d. Gaussian signaling based achievable schemes is that rates obtained using them do not scale with the signal-to-noise ratio (SNR). Hence, the number of Degrees of Freedom (DoF) for the MAC-WT achieved using these schemes is zero. On the other hand, the results on the secure DoF of Gaussian interference networks in [12], [7], [9], [8], and [2], suggested that these schemes may be suboptimal. Fading Gaussian MAC-WT was first considered in [18] where, as in the non-fading case, the achievable ergodic secrecy rates obtained through i.i.d. Gaussian signaling do not scale with SNR.

In Chapter 2, we use the idea of *interference alignment* to introduce two new achievable schemes for secrecy in the fading MAC-WT. We derive the ergodic secrecy rates achievable by these schemes and show that, in the K-user fading MAC-WT channel, the users' sum rate achieved by each of the two schemes scales with SNR as $\frac{K-1}{K}\log(SNR)$. Our first achievable scheme, the *scaling based alignment* (SBA) scheme, is based on code repetition with proper scaling of the transmitted signals. Transmitters scale their transmit signals such that over K consecutive time instants

the equivalent channel matrix at the legitimate receiver is of full-rank whereas the equivalent channel matrix at the eavesdropper is of unit-rank. In our second achievable scheme, the *ergodic secret alignment* (ESA) scheme, we extend the idea of ergodic interference alignment in [14] to the secrecy context. In the ESA scheme, we carefully choose the time instants over which codeword symbols are repeated such that the received signals are aligned favorably at the legitimate receiver while they are aligned unfavorably at the eavesdropper. We also introduce an improved version of our second scheme in which we use cooperative jamming on top of the ESA scheme to obtain larger secrecy rates. Moreover, we obtain a power allocation policy that satisfies the necessary KKT conditions of optimality.

Next, we focus on the security problem in cooperative wireless channels. In Chapters 3 and 4, we study the concept of *deaf cooperation* to reinforce security of transmission over the Gaussian relay-eavesdropper channels. We distinguish between two main schemes of deaf cooperation based on Gaussian signaling, namely, the cooperative jamming (CJ) scheme and the noise forwarding (NF) scheme. In the CJ scheme, a helping interferer transmits white Gaussian noise when it can hurt the eavesdropper more than it can hurt the legitimate receiver and hence improve the achievable secrecy rate. The idea of introducing artificial noise in a GWT channel by a helper node was introduced in [31], [34], [19], [20]. In relay networks with secrecy constraints, the role of CJ was further investigated, e.g., in [27], [22], and [36]. References [23], [26], and [25] proposed CJ strategies for multiple-antenna relay networks. On the other hand, in the NF scheme which was introduced in [29], the relay node sends a dummy (context-free) codeword drawn at random from a codebook that is known to both the

legitimate receiver and the eavesdropper to introduce helpful interference that would hurt the eavesdropper more than the legitimate receiver.

In Chapter 3, we investigate the role of a deaf helper in improving the achievable secrecy rates of a Gaussian wiretap channel (GWT) by using either the CJ mode or the NF mode of deaf cooperation. We derive the conditions under which each mode of deaf cooperation improves over the secrecy capacity of the original wiretap channel and show that a helping node can be either a useful cooperative jammer or a useful noise forwarder but not both at the same time. We derive the optimal power allocation for both the source and the helping node to be used in each of the two modes of deaf helping. Then, we consider the deaf helper selection problem where there are N relays present in the system and it is required to select the best K deaf helpers, $K \geq 1$, that yield the maximum possible achievable secrecy rate with deaf cooperation using K relays. We give an optimal strategy for the case of $K = 1$, i.e., for the selection of a single deaf helper. The computational complexity of the optimal selection for the general case when $K > 1$ is prohibitive. We propose a suboptimal strategy for the selection problem in the general case. We discuss the complexity of the proposed single and multiple relay selection strategies and show that both of them are efficient, and verify the performance of the proposed strategies through numerical examples.

In Chapter 4, we study the CJ and the NF modes of deaf cooperation when the helper node is equipped with multiple antennas. We decompose the channel from the helper to the eavesdropper into two orthogonal components: one is aligned in the direction of the channel between the helper and the legitimate receiver (direct

component) and the other is in the orthogonal direction to the channel between the helper and the legitimate receiver (orthogonal component). We then propose a strategy in which the helper uses the orthogonal component to transmit pure Gaussian noise as in the CJ strategy while it uses the direct component for either CJ or NF depending on the given channel conditions. We explicitly derive the optimal power control policy for this strategy and give the achievable secrecy rates when the direct component is used to perform CJ or NF. We hence derive the channel conditions where CJ is better than NF over the direct component and vice versa. Next, we consider the reversely degraded multiple-antenna relay-eavesdropper channel. We show that a simple strategy in which the relay jams with full power along the orthogonal component and transmits nothing in the direct component achieves a secrecy rate that approaches the secrecy capacity of this channel as the relay's average power goes to infinity. Moreover, we show that this result is valid with probability 1 even if the relay-eavesdropper's channel state information is unavailable.

Finally, we turn our attention to the role of active cooperation for secrecy in wireless relay networks. In active cooperation, the relay listens to the source transmissions and uses its observation to improve the achievable secrecy rate. This mode is based on the well-known strategies, e.g., decode-and-forward (DF), compress-and-forward (CF), and amplify-and-forward (AF) strategies, devised originally for the cooperative models with no secrecy constraint. These strategies were first introduced in [38] for the single relay channel with no secrecy constraints. In the context of multiple relay networks with no secrecy constraints, [41] and [40] proposed multi-hop DF strategies and obtained the achievable rates by these strategies. In [29], the single

relay-eavesdropper channel was introduced and achievable secrecy rates were obtained based on extended versions of these strategies. We focus in this dissertation on the DF-based strategies. In [39] and [43], two-stage (half-duplex) cooperative secrecy protocols were proposed in which a set of multiple relays decode the source's message in the first stage, then the relays forward the source's message to the destination using beamforming. Both references investigated the role of the beamforming relays in improving secrecy.

In Chapter 5, we investigate full-duplex relaying strategies for secrecy in cooperative relay networks. We first study the DF strategy for secrecy in a single relay channel with an eavesdropper. We propose a suboptimal decode-and-forward with zero-forcing (DF/ZF) strategy for which we obtain the optimal power control policy. Next, we consider the multiple relays problem. We propose three strategies based on the DF/ZF technique. In the first strategy, all the relays decode the source message at the same time, and then perform beamforming. We give the achievable rate by this strategy and derive the optimal power control policy. We show that in this strategy the relays which are far from the source create a bottleneck and limit the achievable rate. In the second strategy, the relays are ordered with respect to their distance from the source and they perform decode-and-forward in a multi-hop fashion. We derive the achievable rate by this strategy and show that it overcomes the drawback of the first strategy. We discuss the zero-forcing technique in the second strategy and show that only half of the relays' signals can be eliminated from the eavesdropper's observation. Hence, we propose a third strategy which is also a multi-hop decode-and-forward strategy, however the number of hops is half of that required by the

second strategy. We show that in the third strategy, it is possible to fully eliminate all the relays's signals from the eavesdropper's observation. Finally, we give numerical results to illustrate the performance of each of the proposed strategies in terms of the achievable rates.

Chapter 2

Ergodic Secret Alignment

2.1 Introduction

The multiple access wiretap channel (MAC-WT) was introduced in [19]. In MAC-WT, multiple users wish to have secure communication with a single receiver, in the presence of a passive eavesdropper. The Gaussian MAC-WT was studied in [19] and [20]. In both references, achievable schemes based on Gaussian signaling (i.e., using i.i.d. Gaussian codebooks) were provided. In addition to achievable schemes based on plain Gaussian signaling, [20] introduces a scheme that can be used in conjunction with Gaussian signaling to improve the achievable secrecy rates. In this scheme, a node that does not transmit information uses its power to jam the eavesdropper. This technique is called *cooperative jamming* (CJ). Cooperative jamming is indeed a channel prefixing technique where specific choices are made for the auxiliary random variables [5]. In addition, cooperative jamming is the first significant application of channel prefixing in a multi-user Gaussian wiretap channel that improves over plain Gaussian signaling. More recently, reference [6] showed that for a certain class of Gaussian MAC-WT, one can achieve through Gaussian signaling a secrecy rate

region that is within 0.5 bits of the secrecy capacity region. Consequently, there has been some expectation that secrecy capacity may be obtained for Gaussian MAC-WT through i.i.d. Gaussian signaling, potentially with Gaussian channel prefixing.

However, a notable shortcoming of these Gaussian signaling based achievable schemes is that rates obtained using them do not scale with the signal-to-noise ratio (SNR). In other words, the schemes achieve zero Degrees of Freedom (DoF) in the MAC-WT. This observation led to the belief that these schemes, and hence Gaussian signaling (with or without channel prefixing), may be suboptimal. This belief is made certain as a direct consequence of the results on the secure DoF of Gaussian interference networks that were obtained in several papers, e.g., in [12], [7], [9], [8], and [2]. The schemes in each of [12] and [7] mainly relied on the *interference alignment* technique proposed by Cadambe and Jafar for the K-user interference channel in their pioneering work [3]. In the original interference alignment technique, the input data stream from each user is mapped using a *precoding* matrix to a longer sequence (almost twice the original length in the asymptotic sense) and then sent over the channel. Hence, the observed signal space at each receiver is of *almost* twice the size (i.e., dimensionality) of the space of the original data. By carefully designing the precoding matrices at the transmitters, the observed signal space at each receiver could be partitioned into two almost equal subspaces, one of which is meant for the desired signal and the other acts as a waste basket for the interfering signals from other users. Consequently, it was shown that one can achieve $\frac{1}{2}$ DoF per user in the K-user interference channel using this technique. Inspired by this technique in the secrecy context, it was shown in [12] and [7] that positive secure DoF is achievable

for a class of vector Gaussian interference channels. In fact, this result is also valid for time-varying channels with only causal knowledge of channel state information which in turn implies that positive secure DoF is achievable for the vector Gaussian MAC-WT in general. In [9] and [8], it was shown that through structured coding (e.g., lattice coding), it is possible to achieve positive DoF for a class of scalar (i.e., non-time-varying) Gaussian channels with interference that contains the Gaussian MAC-WT. More recently, in [2], both the Gaussian multiple input multiple output (MIMO) MAC-WT and the Gaussian scalar MAC-WT were considered. For the K-user Gaussian MIMO MAC-WT model, [2] provides an algorithm which is inspired by the original interference alignment technique [3] to separate the received signals at the legitimate receiver and at the same time align them in a low-dimensional subspace in the signal space observed by the eavesdropper. For the K-user Gaussian scalar MAC-WT, [2] proposes an achievable secure coding scheme to achieve positive secure DoF. Namely, the proposed scheme achieves total secure DoF of $\frac{K-1}{K}$ for almost all channel gains. This is done by incorporating the new alignment technique known as *real interference alignment* that was first proposed in [1] that performs on a single real line and exploits the properties of real numbers to align interference in time-invariant channels.

Fading Gaussian MAC-WT was first considered in [18] where the Gaussian signaling and cooperative jamming schemes which were originally proposed in [19] and [20] are extended to the fading MAC-WT. Using these schemes, [18] gave achievable ergodic sum secrecy rates for the fading MAC-WT. Similar to the non-fading setting, these achievable ergodic secrecy rates do not scale with the average SNRs. In this

chapter, we propose two new achievable schemes for the fading Gaussian MAC-WT. Our first achievable scheme, the *scaling based alignment* (SBA) scheme, is based on code repetition with proper scaling of transmitted signals. We first consider the two-user fading MAC-WT. The generalization of this scheme to the case of more than two users is presented subsequently. In particular, for the two-user fading MAC-WT, transmitters repeat their symbols in two *consecutive* symbol instants. Transmitters further scale their transmit signals with the goal of creating a full-rank channel matrix at the main receiver and a unit-rank channel matrix at the eavesdropper, in every two consecutive time instants. These coordinated actions create a two-dimensional space for the signal received by the legitimate receiver, while sustaining the interference in a single-dimensional space at the eavesdropper. In other words, code repetition with proper scaling of the transmit signals at each transmitter *aligns* the received signals at the eavesdropper perfectly making it difficult for the eavesdropper to decode both messages. Consequently, we obtain a new achievable secrecy rate region for the two-user fading MAC-WT. In fact, it might be useful here to compare our SBA scheme with the technique used in [2] for the Gaussian MIMO MAC-WT. In the model considered here, we could create parallel MAC channels to each of the legitimate receiver and the eavesdropper by symbol repetition and exploiting the time-varying nature of fading channels and hence by proper scaling (precoding), one can almost surely create a full-dimensional space for the received signal at the legitimate receiver and one-dimensional space for the received signal at the eavesdropper. On the other hand, in [2], the existence of multiple spatial dimensions is already imposed by the model itself (Gaussian MIMO MAC-WT) and hence the precoding technique used in [2] for

this model achieves secure DoF that eventually depends on the channel gain matrices from the transmitters to the legitimate receiver and the eavesdropper.

In another recent work [14], it was shown that in a fading interference channel, by code repetition over *properly chosen* time instants, one can perfectly cancel interference at each receiver so that the resulting individual rates scale as $\frac{1}{2}\log(\text{SNR})$. Thus, the rate reduction by a factor of $\frac{1}{2}$ comes with the benefit of perfect interference cancellation. In this chapter, we extend the ergodic interference alignment concept to a secrecy context and we propose another achievable scheme which we call *ergodic secret alignment* (ESA). We first consider the two-user fading MAC-WT, and generalize this scheme to the case of more than two users subsequently. In the SBA scheme, code repetition is done over two consecutive time instants, while in the ESA scheme, we carefully choose the time instants over which we do code repetition such that the received signals are aligned favorably at the legitimate receiver while they are aligned unfavorably at the eavesdropper. In particular, given some time instant with the vector of the main receiver channel coefficients and the vector of the eavesdropper channel coefficients given by $\mathbf{h} = [h_1 \ h_2]^T$ and $\mathbf{g} = [g_1 \ g_2]^T$, respectively, if X_1 and X_2 are the symbols transmitted in this time instant by users 1 and 2, respectively, our objective, roughly speaking, is to determine the channel gains we should wait for to transmit X_1 and X_2 again. In this chapter, we show that, in order to maximize achievable secrecy rates, we should wait for a time instant in which the main receiver channel coefficients are $[h_1 \ -h_2]^T$ and the eavesdropper channel coefficients are $[g_1 \ g_2]^T$. Consequently, we obtain another achievable secrecy rate region for the two-user fading MAC-WT.

For both proposed schemes, we show that the resulting secrecy rates scale with SNR. Specifically, the achievable secrecy sum rate scales as $\frac{1}{2}\log(\text{SNR})$. Moreover, we show that the secrecy rates achieved through i.i.d. Gaussian signaling with cooperative jamming in fading MAC-WT do not scale with SNR. The significance of these results is that, they show that indeed neither plain i.i.d. Gaussian signaling nor i.i.d. Gaussian signaling with cooperative jamming is optimal for the fading MAC-WT, and that, for high SNRs, one can achieve higher secrecy rates by aligning interference perfectly in the eavesdropper MAC while reducing, or cancelling, interference at the main receiver MAC using some coordinated actions at both transmitters that involve code repetition, i.e., a form of time-correlated (non i.i.d.) signaling.

In fact, the achievable rate region using the second scheme, the ESA scheme, involves two significant improvements over the one achieved by the SBA scheme when the channel coefficients are circularly symmetric complex Gaussian random variables. First, the expressions for achievable rates by the SBA scheme involve products of the squared magnitudes of the channel coefficients. The squared magnitudes of the channel coefficients are exponential random variables and hence multiplying them together gives a random variable that takes small values with higher probability than the original exponential random variables would take these values. This in effect reduces the achievable rates by the SBA scheme. On the other hand, the achievable secrecy rates by the ESA scheme do not have this drawback. In other words, by code repetition, the SBA scheme creates two (not perfectly) correlated MAC channels to the main receiver and two perfectly correlated MAC channels to the eavesdropper, while the ESA scheme creates an orthogonal MAC channel to the main receiver

and two perfectly correlated MAC channels to the eavesdropper. This fact leads to higher achievable secrecy rates by the ESA scheme. The second improvement of the ESA scheme with respect to the SBA scheme is that the average power constraints associated with the ESA scheme do not involve any channel coefficients whereas those associated with the SBA scheme involve the gains of the eavesdropper channel which in turn result in inefficient use of transmit powers. However, it is noteworthy that SBA scheme holds one practical advantage over the ESA scheme that actually does not appear in the achievable rates by the two schemes. Namely, in the SBA scheme, we do not wait for favorable channel conditions for alignment since repetition is done over consecutive time slots. On the other hand, in the ESA scheme, one should wait for the proper channel conditions before repetition takes place. The waiting time required to match up the channel states is an important performance factor for the ESA scheme in practice.

In addition, we introduce an improved version of our second scheme in which we use cooperative jamming on top of the ESA scheme to achieve higher secrecy rates. Moreover, since the rate expressions achieved by the ESA scheme (with and without cooperative jamming) and their associated average power constraints are simpler than their counterparts in the SBA scheme, we derive the necessary conditions on the optimal power allocations that maximize the sum secrecy rate achieved by the ESA scheme when used alone and when used together with cooperative jamming. Since the achievable secrecy sum rate, in general, is not a concave function in the power allocation policy, the solution of such optimization problem may not be unique. Hence, we obtain a power allocation policy that satisfies the necessary (but not necessarily

sufficient) KKT conditions of optimality.

We provide numerical examples that illustrate the scaling of the sum rates achieved by the proposed schemes with SNR and the saturation of the secrecy sum rate achieved by the i.i.d. Gaussian signaling scheme with cooperative jamming. We also give numerical examples for the secrecy sum rates achieved by the ESA scheme with and without cooperative jamming when power control is used.

Finally, we discuss the extension of the SBA and the ESA schemes to the case of K-user fading MAC-WT channel for $K \geq 2$. We show that each of the two schemes achieves a total of $\frac{K-1}{K}$ secure DoF which is the same total secure DoF shown in [2] to be achievable for the K-user Gaussian scalar MAC-WT for almost all channel gains using the real interference alignment technique.

2.2 System Model

We consider the two-user fading multiple access channel with an external eavesdropper. Transmitter k chooses a message W_k from a set of equally likely messages $\mathcal{W}_k = \{1, ..., 2^{2nR_k}\}$, $k = 1, 2$. Every transmitter encodes its message into a codeword of length $2n$ symbols. The channel output at the intended receiver and the eavesdropper at the symbol interval t are given by

$$Y_t = h_{1t}X_{1t} + h_{2t}X_{2t} + N_t \tag{2.1}$$

$$Z_t = g_{1t}X_{1t} + g_{2t}X_{2t} + N'_t \tag{2.2}$$

where, for $k = 1, 2$, X_{kt} is the input signal at transmitter k at channel use t, $h_{kt},\ g_{kt}$ are the channel coefficients at channel use t between transmitter k and the intended receiver and the eavesdropper, respectively. We assume a fast fading scenario where the channel coefficients randomly vary from one symbol to another in i.i.d. fashion. Also, we assume the independence of all channel coefficients h_{kt} and g_{kt} for all k, t. Each of the channel coefficients is a circularly symmetric complex Gaussian random variable with zero-mean. The variances of h_{kt} and g_{kt} are $\sigma_{h_k}^2$ and $\sigma_{g_k}^2$, respectively for all t. Hence, $|h_{kt}|^2$ and $|g_{kt}|^2$ are exponentially distributed random variables with mean $\sigma_{h_k}^2$ and $\sigma_{g_k}^2$, respectively. Moreover, we assume that all the channel coefficients are known to all the nodes in a causal fashion. In (2.1)-(2.2), N_t and N_t' are the independent Gaussian noises at the intended receiver and the eavesdropper, respectively, and are i.i.d. (in time) circularly symmetric complex Gaussian random variables with zero-mean and unit-variance. For the rest of the chapter, we will drop the time index t for notational convenience unless it is clearly stated otherwise. We have the usual average power constraints

$$E[|X_k|^2] \leq \bar{P}_k, \quad k = 1, 2. \tag{2.3}$$

A $(2^{2nR_1}, 2^{2nR_2}, 2n)$ code for this channel consists of two stochastic encoders $\varphi_k,\ k = 1, 2$ at the transmitters where φ_k maps a message $W_k \in \mathcal{W}_k$ to a sequence of complex numbers X_k^{2n}, and a decoder ψ at the main receiver which maps the received sequence at the main receiver Y^{2n} and the channel state sequences $h_1^{2n},\ h_2^{2n},\ g_1^{2n},\ g_2^{2n}$ to an

estimate of the message pair $(\hat{W}_1, \hat{W}_2) \in \mathcal{W}_1 \times \mathcal{W}_2$. The probability of error is

$$P_e^{2n} = \Pr\left((\hat{W}_1, \hat{W}_2) \neq (W_1, W_2)\right) \tag{2.4}$$

A rate pair (R_1, R_2) is said to be achievable with perfect secrecy if there is a $(2^{2nR_1}, 2^{2nR_2}, 2n)$ code satisfying

$$\lim_{n\to\infty} P_e^{2n} = 0, \qquad \text{and} \qquad \lim_{n\to\infty} \frac{1}{2n} I\left(W_1, W_2; Z^{2n} | h_1^{2n}, h_2^{2n}, g_1^{2n}, g_2^{2n}\right) = 0 \tag{2.5}$$

2.3 Previously Known Results

Here we summarize previously known results that are relevant to our development. For the general discrete-time memoryless MAC-WT, the best known achievable secrecy rate region [19], [20], [5] is given by the convex hull of all rate pairs (R_1, R_2) satisfying

$$R_1 \leq I(V_1; Y|V_2) - I(V_1; Z) \tag{2.6}$$

$$R_2 \leq I(V_2; Y|V_1) - I(V_2; Z) \tag{2.7}$$

$$R_1 + R_2 \leq I(V_1, V_2; Y) - I(V_1, V_2; Z) \tag{2.8}$$

where the distribution $p(x_1, x_2, v_1, v_2, y, z)$ factors as $p(v_1)p(x_1|v_1)p(v_2)p(x_2|v_2)$ $p(y, z|x_1, x_2)$.

Known secrecy rate regions for the Gaussian MAC-WT can be obtained from these expressions by appropriate selections for the involved random variables. For

instance, the Gaussian signaling based achievable rates proposed in [19] are obtained by choosing $X_1 = V_1$ and $X_2 = V_2$, i.e., no channel prefixing, and by choosing X_1 and X_2 to be Gaussian with full power. On the other hand, cooperative jamming based achievable rates proposed in [20] are obtained by choosing $X_1 = V_1 + T_1$ and $X_2 = V_2 + T_2$, and then by choosing V_1, V_2, T_1, T_2 to be independent Gaussian random variables [5]. Namely, for $k = 1, 2$, V_k and T_k are Gaussian random variables with zero mean and variances P_k and Q_k, respectively. Here, V_1 and V_2 carry messages, while T_1 and T_2 are jamming signals. The powers of (V_1, T_1) and (V_2, T_2) should be chosen to satisfy the power constraints of users 1 and 2, respectively. These selections yield the following achievable rate region for the Gaussian MAC-WT [20]

$$R_1 \leq \log\left(1 + \frac{|h_1|^2 P_1}{1 + |h_1|^2 Q_1 + |h_2|^2 Q_2}\right) - \log\left(1 + \frac{|g_1|^2 P_1}{1 + |g_1|^2 Q_1 + |g_2|^2 (P_2 + Q_2)}\right) \tag{2.9}$$

$$R_2 \leq \log\left(1 + \frac{|h_2|^2 P_2}{1 + |h_1|^2 Q_1 + |h_2|^2 Q_2}\right) - \log\left(1 + \frac{|g_2|^2 P_2}{1 + |g_1|^2 (P_1 + Q_1) + |g_2|^2 Q_2}\right) \tag{2.10}$$

$$R_1 + R_2 \leq \log\left(1 + \frac{|h_1|^2 P_1 + |h_2|^2 P_2}{1 + |h_1|^2 Q_1 + |h_2|^2 Q_2}\right) - \log\left(1 + \frac{|g_1|^2 P_1 + |g_2|^2 P_2}{1 + |g_1|^2 Q_1 + |g_2|^2 Q_2}\right) \tag{2.11}$$

where the powers of the signals must satisfy

$$P_k + Q_k \leq \bar{P}_k, \quad k = 1, 2 \tag{2.12}$$

where P_k and Q_k are the transmission and jamming powers, respectively, of user k.

The ergodic secrecy rate region achieved by Gaussian signaling and cooperative jamming for the fading MAC-WT can be expressed similarly by simply including expectations over fading channel states [18]

$$R_1 \leq E_{\mathbf{h},\mathbf{g}}\left\{\log\left(1+\frac{|h_1|^2P_1}{1+|h_1|^2Q_1+|h_2|^2Q_2}\right)-\log\left(1+\frac{|g_1|^2P_1}{1+|g_1|^2Q_1+|g_2|^2(P_2+Q_2)}\right)\right\} \tag{2.13}$$

$$R_2 \leq E_{\mathbf{h},\mathbf{g}}\left\{\log\left(1+\frac{|h_2|^2P_2}{1+|h_1|^2Q_1+|h_2|^2Q_2}\right)-\log\left(1+\frac{|g_2|^2P_2}{1+|g_1|^2(P_1+Q_1)+|g_2|^2Q_2}\right)\right\} \tag{2.14}$$

$$R_1+R_2 \leq E_{\mathbf{h},\mathbf{g}}\left\{\log\left(1+\frac{|h_1|^2P_1+|h_2|^2P_2}{1+|h_1|^2Q_1+|h_2|^2Q_2}\right)-\log\left(1+\frac{|g_1|^2P_1+|g_2|^2P_2}{1+|g_1|^2Q_1+|g_2|^2Q_2}\right)\right\} \tag{2.15}$$

where $\mathbf{h}=[h_1\ h_2]^T$, $\mathbf{g}=[g_1\ g_2]^T$, and the instantaneous powers P_k and Q_k, which are both functions of $\mathbf{h}$ and $\mathbf{g}$, satisfy

$$E\left[P_k+Q_k\right] \leq \bar{P}_k,\ k=1,2 \tag{2.16}$$

2.4 Scaling Based Alignment (SBA)

In this section, we introduce a new achievable scheme for the fading MAC-WT. Our achievable scheme is based on code repetition with proper scaling of the signals transmitted by each transmitter. This is done as follows. For the channel described in (2.1)-(2.2), we use a repetition code such that each transmitter repeats its channel input symbol twice over two *consecutive* time instants. Due to code repetition, we

may regard each of the MACs to the main receiver and to the eavesdropper as a vector MAC composed of two parallel scalar MACs, one for the *odd* time instants and the other for the *even* time instants. Consequently, we may describe the main receiver MAC channel by the following pair of equations

$$Y_o = h_{1o}X_1 + h_{2o}X_2 + N_o \tag{2.17}$$

$$Y_e = h_{1e}X_1 + h_{2e}X_2 + N_e \tag{2.18}$$

where, for $k = 1, 2$, h_{ko}, h_{ke} are the coefficients of the kth main receiver channel in odd and even time instants, Y_o, Y_e and N_o, N_e are the received signal and the noise at the main receiver in odd and even time instants. In the same way, we may describe the eavesdropper MAC channel by the following pair of equations

$$Z_o = g_{1o}X_1 + g_{2o}X_2 + N'_o \tag{2.19}$$

$$Z_e = g_{1e}X_1 + g_{2e}X_2 + N'_e \tag{2.20}$$

where, for $k = 1, 2$, g_{ko}, g_{ke} are the coefficients of the kth eavesdropper channel in odd and even time instants, Z_o, Z_e and N_o, N_e are the received signal and the noise at the eavesdropper in odd and even time instants.

Since all the channel gains are known to all nodes in a causal fashion, the two transmitters use this knowledge as follows. In every symbol instant, each transmitter scales its transmit signal with the gain of the other transmitter's channel to the eavesdropper. That is, in every symbol duration, the first user multiplies its channel

input with g_2, the channel gain of the second user to the eavesdropper, and the second user multiplies its channel input with g_1, the channel gain of the first user to the eavesdropper. Hence the main receiver MAC can be described as

$$Y_o = h_{1o}g_{2o}X_1 + h_{2o}g_{1o}X_2 + N_o \tag{2.21}$$

$$Y_e = h_{1e}g_{2e}X_1 + h_{2e}g_{1e}X_2 + N_e \tag{2.22}$$

and the eavesdropper MAC can be described as

$$Z_o = g_{1o}g_{2o}X_1 + g_{1o}g_{2o}X_2 + N'_o \tag{2.23}$$

$$Z_e = g_{1e}g_{2e}X_1 + g_{1e}g_{2e}X_2 + N'_e \tag{2.24}$$

It is clear from (2.21)-(2.22) that the space of the received signal (without noise, i.e., high SNR) of the main receiver over the two consecutive time instants is two-dimensional almost surely. In other words, the channel matrix of the main receiver vector MAC is full-rank almost surely. This is due to the fact that the channel coefficients are drawn from continuous bounded distributions. On the other hand, it is clear from (2.23)-(2.24) that the channel matrix of the eavesdropper vector MAC is unit-rank. That is, the two ingredients of our scheme, i.e., code repetition and signal scaling, let the interfering signals at the main receiver live in a two-dimensional space, while they *align* the interfering signals at the eavesdropper in a one-dimensional space. As we will show in the Section 2.6, these properties play a central role in achieving secrecy rates that scale with SNR.

Let $\mathbf{h}_o = (h_{1o}, h_{2o})$ and $\mathbf{h}_e = (h_{1e}, h_{2e})$. We define $\mathbf{g}_o$ and $\mathbf{g}_e$ in the same way. For $k = 1, 2$, we define the power allocation policy of transmitter k as a mapping $P_k : \mathbb{C}^4 \to \mathbb{R}_+$ which maps $(\mathbf{h}_o, \mathbf{g}_o)$ to a non-negative real number $P_k(\mathbf{h}_o, \mathbf{g}_o)$ which is the power of transmitter k in the odd time slot for which the values of channel gains are $(\mathbf{h}_o, \mathbf{g}_o)$. Note that due to symbol repetition, P_k is a function of $(\mathbf{h}_o, \mathbf{g}_o)$ only and does not depend on $(\mathbf{h}_e, \mathbf{g}_e)$. To simplify notation, we will use P_k to denote $P_k(\mathbf{h}_o, \mathbf{g}_o)$ since this dependency on channel gains is implicitly understood. We note that, due to signal scaling at the transmitters, the average power constraints become

$$E\left[\left(|g_{2o}|^2 + |g_{2e}|^2\right) P_1\right] \leq \bar{P}_1 \tag{2.25}$$

$$E\left[\left(|g_{1o}|^2 + |g_{1e}|^2\right) P_2\right] \leq \bar{P}_2 \tag{2.26}$$

Now, we evaluate the secrecy rate region achievable by our *scaling based alignment* (SBA) scheme. Given the vector channels (2.21)-(2.22) and (2.23)-(2.24), the following secrecy rates are achievable [19], [20], [5],

$$R_1 \leq \frac{1}{2}\left[I(X_1; Y_o, Y_e | X_2, \mathbf{h}, \mathbf{g}) - I(X_1; Z_o, Z_e | \mathbf{h}, \mathbf{g})\right] \tag{2.27}$$

$$R_2 \leq \frac{1}{2}\left[I(X_2; Y_o, Y_e | X_1, \mathbf{h}, \mathbf{g}) - I(X_2; Z_o, Z_e | \mathbf{h}, \mathbf{g})\right] \tag{2.28}$$

$$R_1 + R_2 \leq \frac{1}{2}\left[I(X_1, X_2; Y_o, Y_e | \mathbf{h}, \mathbf{g}) - I(X_1, X_2; Z_o, Z_e | \mathbf{h}, \mathbf{g})\right] \tag{2.29}$$

where $\mathbf{h} = (\mathbf{h}_o, \mathbf{h}_e)$ and $\mathbf{g} = (\mathbf{g}_o, \mathbf{g}_e)$. These expressions for achievable rates follow from (2.6)-(2.8) by treating channel states as outputs at the receivers, and noting the independence of channel inputs and channel states. We note that the factor of $\frac{1}{2}$ on

the right hand sides of (2.27)-(2.29) is due to repetition coding. Now, by computing (2.27)-(2.29) with Gaussian signals, we obtain the secrecy rate region given in the following theorem.

Theorem 2.1 *For the two-user fading MAC-WT, the rate region given by all rate pairs* (R_1, R_2) *satisfying the following constraints is achievable with perfect secrecy*

$$R_1 \leq \frac{1}{2} E_{\boldsymbol{h},\boldsymbol{g}} \left\{ \log\left(1 + (|h_{1o}g_{2o}|^2 + |h_{1e}g_{2e}|^2)P_1\right) - \log\left(1 + \frac{(|g_{1o}g_{2o}|^2 + |g_{1e}g_{2e}|^2)P_1}{1 + (|g_{1o}g_{2o}|^2 + |g_{1e}g_{2e}|^2)P_2}\right) \right\} \tag{2.30}$$

$$R_2 \leq \frac{1}{2} E_{\boldsymbol{h},\boldsymbol{g}} \left\{ \log\left(1 + (|h_{2o}g_{1o}|^2 + |h_{2e}g_{1e}|^2)P_2\right) - \log\left(1 + \frac{(|g_{1o}g_{2o}|^2 + |g_{1e}g_{2e}|^2)P_2}{1 + (|g_{1o}g_{2o}|^2 + |g_{1e}g_{2e}|^2)P_1}\right) \right\} \tag{2.31}$$

$$\begin{aligned} R_1 + R_2 \leq \frac{1}{2} E_{\boldsymbol{h},\boldsymbol{g}} \Bigg\{ & \log\Bigg(1 + \left(|h_{1o}g_{2o}|^2 + |h_{1e}g_{2e}|^2\right) P_1 + \left(|h_{2o}g_{1o}|^2 + |h_{2e}g_{1e}|^2\right) P_2 \\ & \qquad + |h_{1e}h_{2o}g_{1o}g_{2e} - h_{1o}h_{2e}g_{1e}g_{2o}|^2 P_1 P_2 \Bigg) \\ & - \log\left(1 + \left(|g_{1o}g_{2o}|^2 + |g_{1e}g_{2e}|^2\right)(P_1 + P_2)\right) \Bigg\} \end{aligned} \tag{2.32}$$

where P_1, P_2 *are the power allocation policies (as defined above) of users* 1 *and* 2*, respectively, that satisfy*

$$E\left[\left(|g_{2o}|^2 + |g_{2e}|^2\right) P_1\right] \leq \bar{P}_1 \tag{2.33}$$

$$E\left[\left(|g_{1o}|^2 + |g_{1e}|^2\right) P_2\right] \leq \bar{P}_2 \tag{2.34}$$

where $\bar{P}_1$ *and* $\bar{P}_2$ *are the average power constraints.*

2.5 Ergodic Secret Alignment (ESA)

After we have devised the scaling based alignment scheme, the ergodic interference alignment scheme of Nazer *et. al.* [14] inspired us to propose an improved achievable scheme. In this section, we discuss this scheme which we call *ergodic secret alignment* (ESA). The new ingredient in this scheme is to perform repetition coding at two *carefully chosen* time instances as opposed to two *consecutive* time instances as we have done in Section 2.4.

For the MAC-WT described by (2.1)-(2.2), we use a repetition code in a way similar to the one in [14]. The simple idea of the scheme is that we repeat each code symbol in the time instant that holds certain channel conditions relative to the those conditions in the time instant where this code symbol is first transmitted. Namely, given a time instant with the main receiver channel state vector $\mathbf{h} = [h_1 \ h_2]^T$ and the eavesdropper channel state vector $\mathbf{g} = [g_1 \ g_2]^T$, where the symbols X_1 and X_2 are first transmitted by the two transmitters, we will solve for the channel states $\tilde{\mathbf{h}} = [\tilde{h}_1 \ \tilde{h}_2]^T$ and $\tilde{\mathbf{g}} = [\tilde{g}_1 \ \tilde{g}_2]^T$, where these symbols should be repeated again, such that the resulting secrecy rates achieved by Gaussian signaling are maximized.

The above description is an intuitive description that gives the idea of the scheme which is based on the concept of ergodic interference alignment introduced in [14]. A rigorous description and proof follow the arguments in [14]. In particular, the idea of the proof [14] is first to quantize the channel coefficients and deal with the quantized coefficients rather than dealing with the original coefficients defined over the whole complex plane. Then, one can show that those quantized channel coefficients of

the same type (distribution) could be paired with another set of quantized channel coefficients of a *symmetric* type. Consequently, one can derive the achievable rate when such pairing between symmetric types is employed. Finally, using the continuity of the achievable rate as a function in channel coefficients, one can argue that by decreasing the quantization bin size, one can approach the desired rate for the original channel (with complex coefficients) in the limit. The detailed proof is found in [14].

Due to code repetition, we may regard each of the MACs to the main receiver and to the eavesdropper as a vector MAC composed of two parallel scalar MACs, one for each one of the two time instants over which the same code symbols X_1 and X_2 are transmitted. Consequently, we may describe the main receiver MAC channel by the following pair of equations

$$Y_1 = h_1 X_1 + h_2 X_2 + N_1 \tag{2.35}$$

$$Y_2 = \tilde{h}_1 X_1 + \tilde{h}_2 X_2 + N_2 \tag{2.36}$$

where Y_1, Y_2 and N_1, N_2 are the received symbols and the noise at the main receiver in the two time instants of code repetition. In the same way, we may describe the eavesdropper MAC channel by the following pair of equations

$$Z_1 = g_1 X_1 + g_2 X_2 + N_1' \tag{2.37}$$

$$Z_2 = \tilde{g}_1 X_1 + \tilde{g}_2 X_2 + N_2' \tag{2.38}$$

where Z_1, Z_2 and N_1', N_2' are the received symbols and the noise at the eavesdropper in

the two time instants of code repetition. For $k = 1, 2$, we define the power allocation policy P_k of transmitter k in a way similar to the way it was defined in the SBA scheme. Namely, it is defined as a mapping $P_k : \mathbb{C}^4 \to \mathbb{R}_+$ which maps the values of the channel gains $(\mathbf{h}, \mathbf{g})$ to a non-negative real number $P_k(\mathbf{h}, \mathbf{g})$ which is the power of transmitter k when the channel gains take the values $(\mathbf{h}, \mathbf{g})$. Again, to simplify notation, we will use P_k to denote $P_k(\mathbf{h}, \mathbf{g})$ since this dependency on channel gains is implicitly understood.

In the next theorem, we give another achievable secrecy rate region for the two-user fading MAC-WT. The achievable region is obtained using (2.27)-(2.29) and replacing (Y_o, Y_e) and (Z_o, Z_e) with (Y_1, Y_2) and (Z_1, Z_2), respectively, and evaluating these expressions with Gaussian signals, and by choosing optimal $\tilde{\mathbf{h}} = (\tilde{h}_1, \tilde{h}_2)$ and $\tilde{\mathbf{g}} = (\tilde{g}_1, \tilde{g}_2)$ to maximize the achievable rates. As we will show shortly as a result of Theorem 2.2, the optimal selection of $\tilde{\mathbf{h}}$ and $\tilde{\mathbf{g}}$ will yield an *orthogonal* MAC to the main receiver and a *scalar* MAC to the eavesdropper. In writing the achievable rate expressions, we will again account for code repetition by multiplying achievable rates by a factor of $\frac{1}{2}$.

Theorem 2.2 *For the two-user fading MAC-WT, the rate region given by all rate*

pairs (R_1, R_2) *satisfying the following constraints is achievable with perfect secrecy*

$$R_1 \leq \frac{1}{2} E_{\boldsymbol{h},\boldsymbol{g}} \left\{ \log\left(1 + 2|h_1|^2 P_1\right) - \log\left(1 + \frac{2|g_1|^2 P_1}{1 + 2|g_2|^2 P_2}\right) \right\} \tag{2.39}$$

$$R_2 \leq \frac{1}{2} E_{\boldsymbol{h},\boldsymbol{g}} \left\{ \log\left(1 + 2|h_2|^2 P_2\right) - \log\left(1 + \frac{2|g_2|^2 P_2}{1 + 2|g_1|^2 P_1}\right) \right\} \tag{2.40}$$

$$\begin{aligned} R_1 + R_2 \leq \frac{1}{2} E_{\boldsymbol{h},\boldsymbol{g}} \Big\{ & \log\left(1 + 2|h_1|^2 P_1\right) + \log\left(1 + 2|h_2|^2 P_2\right) \\ & - \log\left(1 + 2(|g_1|^2 P_1 + |g_2|^2 P_2)\right) \Big\} \end{aligned} \tag{2.41}$$

where P_1 *and* P_2 *are the power allocation policies of users* 1 *and* 2*, respectively, and are both functions of* $\boldsymbol{h}$ *and* $\boldsymbol{g}$ *in general (as defined above). In addition, they satisfy the average power constraints*

$$E[P_1] \leq \bar{P}_1 \tag{2.42}$$

$$E[P_2] \leq \bar{P}_2 \tag{2.43}$$

Proof: First, consider the two vector MACs given by (2.35)-(2.38). Observe that as in [14], $\tilde{\mathbf{h}}$ must be chosen such that it has the same distribution as $\mathbf{h}$ and $\tilde{\mathbf{g}}$ must be chosen such that it has the same distribution as $\mathbf{g}$. The reason for this can be understood from the idea of the proof in [14] discussed earlier in this section. Indeed, in the quantized channel, in order for the pairing between channel coefficients at two different instants to be possible, the values of the channel coefficients at the two time instants must occur with the same probability. That is why we require that $\tilde{\mathbf{h}}$ and $\tilde{\mathbf{g}}$ to have the same distributions as $\mathbf{h}$ and $\mathbf{g}$, respectively. Now, since $\mathbf{h} \sim \mathcal{CN}(\mathbf{0}, \mathbf{B}_h)$

and $\mathbf{g} \sim \mathcal{CN}(\mathbf{0}, \mathbf{B}_g)$ where $\mathbf{B}_h = \text{diag}(\sigma^2_{h_1}, \sigma^2_{h_2})$ and $\mathbf{B}_g = \text{diag}(\sigma^2_{g_1}, \sigma^2_{g_2})$, then in order to achieve the requirement above, it follows from the symmetry property of the complex Gaussian distribution that the channel realizations $\mathbf{h}$ and $\mathbf{g}$ must be paired with the channel realizations $\tilde{\mathbf{h}}$ and $\tilde{\mathbf{g}}$, respectively, that are related as $\tilde{\mathbf{h}} = \mathbf{U}\mathbf{h}$ and $\tilde{\mathbf{g}} = \mathbf{V}\mathbf{g}$ for some unitary matrices $\mathbf{U}$ and $\mathbf{V}$ (rotations in $\mathbb{C}^2$). Furthermore, for such rotations to preserve the variances of the individual components of $\mathbf{h}$ (i.e., $\sigma^2_{h_1}, \sigma^2_{h_2}$) and of $\mathbf{g}$ (i.e., $\sigma^2_{g_1}, \sigma^2_{g_2}$), we must have $\mathbf{U} = \text{diag}(\exp(j\theta_1), \exp(j\theta_2))$ and $\mathbf{V} = \text{diag}(\exp(j\omega_1), \exp(j\omega_2))$ for some $\theta_1, \theta_2, \omega_1, \omega_2 \in [0, 2\pi)$. Then, it follows that (2.35)-(2.38) can be written as

$$Y_1 = h_1 X_1 + h_2 X_2 + N_1 \tag{2.44}$$

$$Y_2 = h_1 e^{j\theta_1} X_1 + h_2 e^{j\theta_2} X_2 + N_2 \tag{2.45}$$

$$Z_1 = g_1 X_1 + g_2 X_2 + N_1' \tag{2.46}$$

$$Z_2 = g_1 e^{j\omega_1} X_1 + g_2 e^{j\omega_2} X_2 + N_2' \tag{2.47}$$

Using (2.27)-(2.29) and replacing (Y_o, Y_e) and (Z_o, Z_e) with (Y_1, Y_2) and (Z_1, Z_2),

respectively, and computing these achievable rates with Gaussian signals, we get

$$R_1 \leq \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \left\{ \log\left(1 + 2|h_1|^2 P_1\right) - \log\left(1 + \frac{2|g_1|^2 P_1 + 2(1-\cos(\omega))|g_1|^2|g_2|^2 P_1 P_2}{1 + 2|g_2|^2 P_2}\right)\right\} \tag{2.48}$$

$$R_2 \leq \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \left\{ \log\left(1 + 2|h_2|^2 P_2\right) - \log\left(1 + \frac{2|g_2|^2 P_2 + 2(1-\cos(\omega))|g_1|^2|g_2|^2 P_1 P_2}{1 + 2|g_1|^2 P_1}\right)\right\} \tag{2.49}$$

$$\begin{aligned} R_1 + R_2 \leq \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \Big\{ & \log(1 + 2|h_1|^2 P_1 + 2|h_2|^2 P_2 + 2(1-\cos(\theta))|h_1|^2|h_2|^2 P_1 P_2) \\ & - \log(1 + 2|g_1|^2 P_1 + 2|g_2|^2 P_2 + 2(1-\cos(\omega))|g_1|^2|g_2|^2 P_1 P_2) \Big\} \end{aligned} \tag{2.50}$$

where $\theta = \theta_2 - \theta_1$ and $\omega = \omega_2 - \omega_1$.

Hence, the largest achievable secrecy rate region (2.48)-(2.50) is attained by choosing $\theta = \pi$ and $\omega = 0$. This can be achieved by choosing $\theta_1 = 0$ and $\theta_2 = \pi$ and by choosing $\omega_1 = \omega_2 = 0$. Consequently, we have $\tilde{\mathbf{h}} = [h_1 \ -h_2]^T$ and $\tilde{\mathbf{g}} = [g_1 \ g_2]^T$. By substituting these values of θ and ω in (2.48)-(2.50), we obtain the region given by (2.39)-(2.41). □

Therefore, when using the ergodic secret alignment technique, the best choice for $\tilde{h}_1$ and $\tilde{h}_2$ is such that $\tilde{\mathbf{h}}$ is orthogonal to $\mathbf{h}$ and that $\|\tilde{\mathbf{h}}\| = \|\mathbf{h}\|$, and the best choice for $\tilde{g}_1$ and $\tilde{g}_2$ is such that $\tilde{\mathbf{g}}$ and $\mathbf{g}$ are linearly dependent and that $\|\tilde{\mathbf{g}}\| = \|\mathbf{g}\|$, i.e., $\tilde{\mathbf{g}} = \mathbf{g}$. This choice makes the vector MAC between the two transmitters and the main receiver equivalent to an orthogonal MAC, i.e., two independent single-user fading channels, one from each transmitter to the main receiver. This equivalent main

receiver MAC channel can be expressed as

$$\bar{Y}_1 = 2h_1X_1 + \bar{N}_1 \tag{2.51}$$

$$\bar{Y}_2 = 2h_2X_2 + \bar{N}_2 \tag{2.52}$$

where $\bar{Y}_1 = Y_1+Y_2$, $\bar{Y}_2 = Y_1-Y_2$, $\bar{N}_1 = N_1+N_2$, and $\bar{N}_2 = N_1-N_2$. Note that $\bar{N}_1$ and $\bar{N}_2$ are independent. On the other hand, this choice makes the vector MAC between the two transmitters and the eavesdropper equivalent to a single scalar MAC. This equivalent eavesdropper MAC channel can be expressed as

$$\bar{Z}_1 = 2g_1X_1 + 2g_2X_2 + \bar{N}_1' \tag{2.53}$$

$$\bar{Z}_2 = \bar{N}_2' \tag{2.54}$$

where $\bar{Z}_1 = Z_1 + Z_2$, $\bar{Z}_2 = Z_1 - Z_2$, $\bar{N}_1' = N_1' + N_2'$, and $\bar{N}_2' = N_1' - N_2'$. Note again that $\bar{N}_1$ and $\bar{N}_2$ are independent. Note that, here, the second component of the eavesdropper's vector MAC is useless for her (i.e., leaks no further information than the first component) as it contains only noise. This selection of the repetition channel state yields a most favorable setting for the main receiver and a least favorable setting for the eavesdropper.

2.6 Degrees of Freedom

In this section, we show that the secrecy sum rates achieved by our schemes scale with SNR as $\frac{1}{2}\log(\text{SNR})$ and that the secrecy sum rate achieved by the cooperative

jamming scheme given in [18] does not scale with SNR. What we give here are rigorous proofs for intuitive results. Since by looking at (2.32) and (2.41), one can note that, if we assume that $\bar{P}_1 = \bar{P}_2 = P$, then if we take $P_1 = P_2 = P$, as P becomes large, roughly speaking, in (2.32) the first term inside the expectation grows as $\log(P^2)$ while the second term grows as $\log(P)$ and hence the overall expression grows as $\frac{1}{2}\log(P)$; and similarly, in (2.41), all three terms inside the expectation grow as $\log(P)$ and hence the overall expression grows as $\frac{1}{2}\log(P)$. In the same way, by considering the secrecy sum rate achieved by the cooperative jamming scheme given in (2.15), then by referring to the power allocation policies given in [18], one can also roughly say that for all channel states, as the available average power goes to infinity, the overall expression converges to a constant.

For simplicity, we assume symmetric average power constraints for all schemes, i.e., we set $\bar{P}_1 = \bar{P}_2 = P$ in (2.33)-(2.34), (2.42)-(2.43), and (2.16). We also assume that all channel gains are drawn from continuous bounded distributions and that all channel gains have finite variances. Let R_s be the achievable secrecy sum rate, then the total number of achievable secure DoF, η, is defined as

$$\eta \triangleq \lim_{P\to\infty} \frac{R_s}{\log(P)} \tag{2.55}$$

We start by the DoF analysis of our proposed schemes, i.e., the SBA scheme and the ESA scheme, where we show that the sum secrecy rates obtained by these schemes achieve $\frac{1}{2}$ secure DoF, then we provide a rigorous proof for the fact that the scheme of [18] which is based on i.i.d. Gaussian signaling with cooperative jamming achieves

a secrecy sum rate that does not scale with SNR, i.e., achieves zero secure DoF.

2.6.1 Secure DoF with the SBA Scheme

We make the following choices for the power allocation policies P_1 and P_2 of the SBA scheme. We set $P_1 = \frac{1}{2\sigma_{g_2}^2}P$, $P_2 = \frac{1}{2\sigma_{g_1}^2}P$. It can be verified that these choices satisfy the power constraints (2.33)-(2.34). Denoting the expression inside the expectation in (2.32) by $f_P(\mathbf{h}, \mathbf{g})$, the secrecy sum rate achieved using the SBA scheme can be written as

$$R_s = \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \left\{ f_P(\mathbf{h}, \mathbf{g}) \right\} \tag{2.56}$$

Hence, the total achievable secure DoF is given by

$$\eta = \frac{1}{2} \lim_{P \to \infty} E_{\mathbf{h},\mathbf{g}} \left[\frac{f_P(\mathbf{h}, \mathbf{g})}{\log(P)} \right] \tag{2.57}$$

Now, we show that, for the two-user fading MAC-WT, a total number of secure DoF $\eta = \frac{1}{2}$ is achievable with the SBA scheme. Towards this end, it suffices to show that the order of the limit and the expectation in (2.57) can be reversed. To do this, we make use of Lebesgue dominated convergence theorem. Now, we note that for

large enough P, $\frac{f_P(\mathbf{h},\mathbf{g})}{\log(P)}$ is upper bounded by $\psi(\mathbf{h},\mathbf{g})$ where

$$\begin{aligned}\psi(\mathbf{h},\mathbf{g}) =& 4 + 2\left(\log\left(1+\frac{1}{\sigma_{g_1}^2}\right)+\log\left(1+\frac{1}{\sigma_{g_2}^2}\right)\right)+\log\left(1+\frac{\sigma_{g_1}^2+\sigma_{g_2}^2}{\sigma_{g_1}^2\sigma_{g_2}^2}\right)\\ &+3\left(\sum_{k=1}^{2}\log(1+|h_{ko}|^2)+\sum_{k=1}^{2}\log(1+|h_{ke}|^2)\right)\\ &+4\left(\sum_{k=1}^{2}\log(1+|g_{ko}|^2)+\sum_{k=1}^{2}\log(1+|g_{ke}|^2)\right)\end{aligned} \tag{2.58}$$

Hence, using the fact that all channel gains have finite variances together with Jensen's inequality, we have

$$E_{\mathbf{h},\mathbf{g}}\left[\psi(\mathbf{h},\mathbf{g})\right] < \infty \tag{2.59}$$

Thus, by the dominated convergence theorem, we have

$$\lim_{P\to\infty} E_{\mathbf{h},\mathbf{g}}\left[\frac{f_P(\mathbf{h},\mathbf{g})}{\log(P)}\right] = E_{\mathbf{h},\mathbf{g}}\left[\lim_{P\to\infty}\frac{f_P(\mathbf{h},\mathbf{g})}{\log(P)}\right] = 1 \tag{2.60}$$

Hence, from (2.57), we have $\eta = \frac{1}{2}$.

2.6.2 Secure DoF with the ESA Scheme

We show that the ESA scheme achieves $\eta = \frac{1}{2}$ secure DoF in the two-user fading MAC-WT. Here, we also use a constant power allocation policy for the ESA scheme where we set $P_1 = P_2 = P$ for all channel states. Clearly, this constant policy satisfies the average power constraints (2.42)-(2.43). Denoting the expression inside

the expectation in (2.41) by $\tilde{f}_P(\mathbf{h},\mathbf{g})$, the achievable secrecy sum rate, R_s is given by

$$R_s = \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \left\{ \tilde{f}_P(\mathbf{h},\mathbf{g}) \right\} \tag{2.61}$$

Hence, the total achievable secure DoF is given by

$$\eta = \frac{1}{2} \lim_{P\to\infty} E_{\mathbf{h},\mathbf{g}} \left[\frac{\tilde{f}_P(\mathbf{h},\mathbf{g})}{\log(P)} \right] \tag{2.62}$$

We note that for large enough P, $\frac{\tilde{f}_P(\mathbf{h},\mathbf{g})}{\log(P)} \leq \tilde{\psi}(\mathbf{h},\mathbf{g})$ where

$$\tilde{\psi}(\mathbf{h},\mathbf{g}) = 6 + \log\left(1+2|h_1|^2\right) + \log\left(1+2|h_2|^2\right) + \log\left(1+2\left(|g_1|^2+|g_2|^2\right)\right) \tag{2.63}$$

Again, using the fact that all channel gains have finite variances together with Jensen's inequality, we have

$$E_{\mathbf{h},\mathbf{g}} \left[\tilde{\psi}(\mathbf{h},\mathbf{g}) \right] < \infty \tag{2.64}$$

Then, by the dominated convergence theorem, we have

$$\lim_{P\to\infty} E_{\mathbf{h},\mathbf{g}} \left[\frac{\tilde{f}_P(\mathbf{h},\mathbf{g})}{\log(P)} \right] = E_{\mathbf{h},\mathbf{g}} \left[\lim_{P\to\infty} \frac{\tilde{f}_P(\mathbf{h},\mathbf{g})}{\log(P)} \right] = 1 \tag{2.65}$$

Hence, from (2.62), we have $\eta = \frac{1}{2}$.

2.6.3 Secure DoF with i.i.d. Gaussian Signaling with CJ

We consider the secrecy sum rate achieved by Gaussian signaling with cooperative jamming (CJ) [18] in the fading MAC-WT and show that this achievable rate does not scale with SNR. We start with the secrecy sum rate given by the right hand side of (2.15). According to the optimal power allocation policy described in [18], for $k = 1, 2$, we cannot have $P_k > 0$ and $Q_k > 0$ simultaneously. Moreover, no transmission occurs when $|h_1| \leq |g_1|$ and $|h_2| \leq |g_2|$. Consequently, according to the relative values of the channel gains $(|h_1|, |h_2|, |g_1|, |g_2|)$, there are three different cases left for the instantaneous secrecy sum rate achieved using the optimum power allocation where we omitted the case where $|h_1| \leq |g_1|$ and $|h_2| \leq |g_2|$ since no transmission is allowed.

Case 1: $(\mathbf{h}, \mathbf{g}) \in \mathcal{D}_1$ where $\mathcal{D}_1 = \big\{(\mathbf{h}, \mathbf{g}) : |h_1| > |g_1|, |h_2| > |g_2|\big\}$. Consequently, $Q_1 = Q_2 = 0$. Thus, the instantaneous secrecy sum rate, $R_s(\mathbf{h}, \mathbf{g})$, can be written as

$$R_s(\mathbf{h}, \mathbf{g}) = \log\left(\frac{1 + |h_1|^2 P_1 + |h_2|^2 P_2}{1 + |g_1|^2 P_1 + |g_2|^2 P_2}\right) \tag{2.66}$$

We can upper bound $R_s(\mathbf{h}, \mathbf{g})$ as

$$R_s(\mathbf{h}, \mathbf{g}) \leq \log\left(1 + \frac{|h_1|^2}{|g_1|^2} + \frac{|h_2|^2}{|g_2|^2}\right) \leq \log\left(1 + \frac{|h_1|^2}{|g_1|^2}\right) + \log\left(1 + \frac{|h_2|^2}{|g_2|^2}\right) \tag{2.67}$$

Case 2: $(\mathbf{h}, \mathbf{g}) \in \mathcal{D}_2$ where $\mathcal{D}_2 = \big\{(\mathbf{h}, \mathbf{g}) : |h_1| > |g_1|, |h_2| < |g_2|\big\}$. Consequently,

$Q_1 = P_2 = 0$. Thus, the instantaneous secrecy sum rate, $R_s(\mathbf{h}, \mathbf{g})$, can be written as

$$R_s(\mathbf{h}, \mathbf{g}) = \log\left(\frac{1 + |h_1|^2 P_1 + |h_2|^2 Q_2}{1 + |g_1|^2 P_1 + |g_2|^2 Q_2}\right) + \log\left(\frac{1 + |g_2|^2 Q_2}{1 + |h_2|^2 Q_2}\right) \tag{2.68}$$

We can upper bound $R_s(\mathbf{h}, \mathbf{g})$ as

$$R_s(\mathbf{h}, \mathbf{g}) \leq 1 + \log\left(1 + \frac{|h_1|^2}{|g_1|^2}\right) + \log\left(1 + \frac{|g_2|^2}{|h_2|^2}\right) \tag{2.69}$$

Case 3: $(\mathbf{h}, \mathbf{g}) \in \mathcal{D}_3$ where $\mathcal{D}_3 = \big\{(\mathbf{h}, \mathbf{g}) : |h_1| < |g_1|, |h_2| > |g_2|\big\}$. Consequently, $P_1 = Q_2 = 0$. Thus, the instantaneous secrecy sum rate, $R_s(\mathbf{h}, \mathbf{g})$, can be written as

$$R_s(\mathbf{h}, \mathbf{g}) = \log\left(\frac{1 + |h_1|^2 Q_1 + |h_2|^2 P_2}{1 + |g_1|^2 Q_1 + |g_2|^2 P_2}\right) + \log\left(\frac{1 + |g_1|^2 Q_1}{1 + |h_1|^2 Q_1}\right) \tag{2.70}$$

We can upper bound $R_s(\mathbf{h}, \mathbf{g})$ as

$$R_s(\mathbf{h}, \mathbf{g}) \leq 1 + \log\left(1 + \frac{|h_2|^2}{|g_2|^2}\right) + \log\left(1 + \frac{|g_1|^2}{|h_1|^2}\right) \tag{2.71}$$

Now, since the instantaneous sum rate is zero outside $\mathcal{D}_1 \cup \mathcal{D}_2 \cup \mathcal{D}_3$, then from (2.67), (2.69), and (2.71), the ergodic secrecy sum rate, R_s, can be upper bounded as

follows

$$
\begin{aligned}
R_s \leq & \int_{\mathcal{D}_1} \left(\log\left(1+\frac{|h_1|^2}{|g_1|^2}\right) + \log\left(1+\frac{|h_2|^2}{|g_2|^2}\right)\right) d\mathbf{F} \\
& + \int_{\mathcal{D}_2} \left(1+\log\left(1+\frac{|h_1|^2}{|g_1|^2}\right) + \log\left(1+\frac{|g_2|^2}{|h_2|^2}\right)\right) d\mathbf{F} \\
& + \int_{\mathcal{D}_3} \left(1+\log\left(1+\frac{|h_2|^2}{|g_2|^2}\right) + \log\left(1+\frac{|g_1|^2}{|h_1|^2}\right)\right) d\mathbf{F}
\end{aligned} \tag{2.72}
$$

where

$$
d\mathbf{F} = \prod_{k=1}^{2} f(|h_k|^2) f(|g_k|^2) d|h_k|^2 d|g_k|^2 \tag{2.73}
$$

where, for $k = 1, 2$, $f(|h_k|^2)$ and $f(|g_k|^2)$ are the density functions of $|h_k|^2$ and $|g_k|^2$, respectively. Now, since $E[|h_k|^2] < \infty$, $E[|g_k|^2] < \infty$ for $k = 1, 2$, $|\int_0^1 \log(x)dx| = \log(e) < \infty$, $|\int_0^1 \log(1+x)dx| = 2 - \log(e) < \infty$, and $f(|h_k|^2), f(|g_k|^2)$ are continuous and bounded for $k = 1, 2$, it follows that each of the three integrals in the above expression is finite. Hence, we have $R_s < \infty$, and that R_s is bounded from above by a constant. Thus, from definition (2.55) of the achievable secure DoF, η, we have

$$
\eta = \lim_{P\to\infty} \frac{R_s}{\log(P)} = 0 \tag{2.74}
$$

2.7 ESA Scheme with Cooperative Jamming

The result given in Theorem 2.2 can be strengthened by adding the technique of cooperative jamming to the ESA scheme of Section 2.5. We refer to the resulting

scheme as ESA/CJ. This is done through Gaussian channel prefixing as discussed in Section 2.3. In particular, we choose the channel inputs in (2.35)-(2.38) to be $X_1 = V_1 + T_1$ and $X_2 = V_2 + T_2$, and then choose V_1, V_2, T_1, T_2 to be independent Gaussian random variables. Namely, for $k = 1, 2$, V_k and T_k are Gaussian random variables with zero mean and variances P_k and Q_k, respectively. Here, V_1 and V_2 carry messages, while T_1 and T_2 are jamming signals. The powers of (V_1, T_1) and (V_2, T_2) should be chosen to satisfy the average power constraints of users 1 and 2, respectively. After these selections are made, the transmitters repeat their channel inputs X_1 and X_2 over two time instants in the same way described in the ESA scheme of Section 2.5. In particular, when transmitters 1 and 2 repeat X_1 and X_2, they repeat their selections of (V_1, T_1) and (V_2, T_2), respectively. Accordingly, the ESA scheme yield the following achievable rate region which, through an appropriate power control strategy (see Section 2.9), can be made strictly larger than the region given in Theorem 2.2,

$$R_1 \leq \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \left\{ \log\left(1 + \frac{2|h_1|^2 P_1}{1 + 2|h_1|^2 Q_1}\right) - \log\left(1 + \frac{2|g_1|^2 P_1}{1 + 2|g_1|^2 Q_1 + 2|g_2|^2 (P_2 + Q_2)}\right) \right\} \tag{2.75}$$

$$R_2 \leq \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \left\{ \log\left(1 + \frac{2|h_2|^2 P_2}{1 + 2|h_2|^2 Q_2}\right) - \log\left(1 + \frac{2|g_2|^2 P_2}{1 + 2|g_1|^2 (P_1 + Q_1) + 2|g_2|^2 Q_2}\right) \right\} \tag{2.76}$$

$$\begin{aligned} R_1 + R_2 \leq \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \Bigg\{ & \log\left(1 + \frac{2|h_1|^2 P_1}{1 + 2|h_1|^2 Q_1}\right) + \log\left(1 + \frac{2|h_2|^2 P_2}{1 + 2|h_2|^2 Q_2}\right) \\ & - \log\left(1 + \frac{2(|g_1|^2 P_1 + |g_2|^2 P_2)}{1 + 2(|g_1|^2 Q_1 + |g_2|^2 Q_2)}\right) \Bigg\} \end{aligned} \tag{2.77}$$

where, for $k = 1, 2$, P_k and Q_k are the transmission and jamming power allocation policies, respectively, of user k, and are both functions of $\mathbf{h}$ and $\mathbf{g}$ in general. In addition, they satisfy the average power constraints

$$E[P_k + Q_k] \leq \bar{P}_k, \ k = 1, 2 \tag{2.78}$$

2.8 Maximizing Secrecy Sum Rate of the ESA Scheme

In this section, we consider the problem of maximizing the secrecy sum rate achieved by the ESA scheme as a function of the power allocations P_1 and P_2 of users 1 and 2, respectively. We define $\alpha_k \triangleq 2|h_k|^2$ and $\beta_k \triangleq 2|g_k|^2$. Then, we define $\boldsymbol{\alpha} \triangleq [\alpha_1 \quad \alpha_2]^T$ and $\boldsymbol{\beta} \triangleq [\beta_1 \quad \beta_2]^T$. The achievable secrecy sum rate is given by

$$R_s = \frac{1}{2} E_{\boldsymbol{\alpha},\boldsymbol{\beta}}\{\log(1 + \alpha_1 P_1) + \log(1 + \alpha_2 P_2) - \log(1 + \beta_1 P_1 + \beta_2 P_2)\} \tag{2.79}$$

We can write the optimization problem as

$$\max \quad \frac{1}{2} E_{\boldsymbol{\alpha},\boldsymbol{\beta}}\{\log(1 + \alpha_1 P_1) + \log(1 + \alpha_2 P_2) - \log(1 + \beta_1 P_1 + \beta_2 P_2)\} \tag{2.80}$$

$$\text{s.t.} \quad E_{\boldsymbol{\alpha},\boldsymbol{\beta}}\left[P_k(\boldsymbol{\alpha}, \boldsymbol{\beta})\right] \leq \bar{P}_k, \quad k = 1, 2 \tag{2.81}$$

$$P_k(\boldsymbol{\alpha}, \boldsymbol{\beta}) \geq 0, \quad k = 1, 2, \quad \forall \boldsymbol{\alpha}, \boldsymbol{\beta} \tag{2.82}$$

The necessary KKT optimality conditions are

$$\frac{\alpha_1}{1+\alpha_1 P_1} - \frac{\beta_1}{1+\beta_1 P_1+\beta_2 P_2} - (\lambda_1 - \mu_1) = 0 \tag{2.83}$$

$$\frac{\alpha_2}{1+\alpha_2 P_2} - \frac{\beta_2}{1+\beta_1 P_1+\beta_2 P_2} - (\lambda_2 - \mu_2) = 0 \tag{2.84}$$

for some $\lambda_k, \mu_k \geq 0,\ k = 1, 2$. It should be noted here that (2.83)-(2.84) are only necessary conditions for the optimal power allocations P_1 and P_2 since the objective function, i.e., the achievable secrecy sum rate, is not concave in (P_1, P_2) in general.

For each channel state, we distinguish between three non-zero forms that the solution (P_1, P_2) of (2.83)-(2.84) may take. First, if $P_1 > 0$ and $P_2 > 0$, then $\mu_1 = \mu_2 = 0$. Hence (P_1, P_2) is the positive common root of the following two quadratic equations

$$\alpha_1 (1+\beta_2 P_2) - \beta_1 = \lambda_1 (1+\alpha_1 P_1)(1+\beta_1 P_1+\beta_2 P_2) \tag{2.85}$$

$$\alpha_2 (1+\beta_1 P_1) - \beta_2 = \lambda_2 (1+\alpha_2 P_2)(1+\beta_1 P_1+\beta_2 P_2) \tag{2.86}$$

Since it is hard to find a simple closed-form solution for the above system of equations, we solve this system numerically and obtain the positive common root (P_1, P_2). Secondly, if $P_1 > 0$ and $P_2 = 0$, then $\mu_1 = 0$. Hence, from (2.83), P_1 is given by

$$P_1 = \frac{1}{2}\left(\sqrt{\left(\frac{1}{\beta_1} - \frac{1}{\alpha_1}\right)^2 + \frac{4}{\lambda_1}\left(\frac{1}{\beta_1} - \frac{1}{\alpha_1}\right)} - \left(\frac{1}{\beta_1} + \frac{1}{\alpha_1}\right)\right) \tag{2.87}$$

Thirdly, if $P_1 = 0$ and $P_2 > 0$, then $\mu_2 = 0$. Hence, from (2.84), P_2 is given by

$$P_2 = \frac{1}{2}\left(\sqrt{\left(\frac{1}{\beta_2} - \frac{1}{\alpha_2}\right)^2 + \frac{4}{\lambda_2}\left(\frac{1}{\beta_2} - \frac{1}{\alpha_2}\right)} - \left(\frac{1}{\beta_2} + \frac{1}{\alpha_2}\right)\right) \tag{2.88}$$

From conditions (2.83)-(2.84), we can derive the following necessary and sufficient conditions for the positivity of the optimal power allocation policies:

$$P_1 > 0, \qquad \text{if and only if} \quad \alpha_1 - \frac{\beta_1}{(1+\beta_2 P_2)} > \lambda_1 \tag{2.89}$$

$$P_2 > 0, \qquad \text{if and only if} \quad \alpha_2 - \frac{\beta_2}{(1+\beta_1 P_1)} > \lambda_2 \tag{2.90}$$

Consequently, according to conditions (2.89)-(2.90), we can divide the set of all possible channel states into 7 partitions such that in each partition the solution (P_1, P_2) will either have one of the three forms stated above or will be zero. Hence, the power allocation policy (P_1, P_2) that satisfies (2.83)-(2.84) and (2.81)-(2.82) can be fully described in 7 different cases of the channel gains. The details of such cases are given in the Appendix.

2.9 Maximizing Secrecy Sum Rate of the ESA/CJ Scheme

In this section, we consider the problem of maximizing the achievable secrecy sum rate as a function in the power allocation policies P_1 and P_2 when cooperative jamming technique is used on top of the ESA scheme. Again, we define $\alpha_k \triangleq 2|h_k|^2$ and $\beta_k \triangleq 2|g_k|^2$. Then, we define $\boldsymbol{\alpha} \triangleq [\alpha_1 \quad \alpha_2]^T$ and $\boldsymbol{\beta} \triangleq [\beta_1 \quad \beta_2]^T$. In this case, the

optimization problem is described as

$$\begin{aligned}
\max \quad & \frac{1}{2}E_{\boldsymbol{\alpha},\boldsymbol{\beta}}\big\{ \log\left(1+\alpha_1(P_1+Q_1)\right)+\log\left(1+\alpha_2(P_2+Q_2)\right) \\
& \qquad -\log\left(1+\beta_1(P_1+Q_1)+\beta_2(P_2+Q_2)\right)+\log\left(1+\beta_1Q_1+\beta_2Q_2\right) \\
& \qquad -\log\left(1+\alpha_1Q_1\right)-\log\left(1+\alpha_2Q_2\right)\big\} \qquad (2.91) \\
\text{s.t.} \quad & E_{\boldsymbol{\alpha},\boldsymbol{\beta}}\left[P_k(\boldsymbol{\alpha},\boldsymbol{\beta})+Q_k(\boldsymbol{\alpha},\boldsymbol{\beta})\right]\le \bar{P}_k, \quad k=1,2 \qquad (2.92) \\
& P_k(\boldsymbol{\alpha},\boldsymbol{\beta}), Q_k(\boldsymbol{\alpha},\boldsymbol{\beta})\ge 0, \quad k=1,2,\ \forall \boldsymbol{\alpha},\boldsymbol{\beta} \qquad (2.93)
\end{aligned}$$

We first show that, at any fading state, splitting a user's power into transmission and jamming is suboptimal, i.e., an optimum power allocation policy must not have $P_k > 0$ and $Q_k > 0$ simultaneously. We note that whether we split powers or not does not affect the first three terms of the objective function since we can always convert jamming power of user k into transmission power of the same user and vice versa while keeping the sum $P_k + Q_k$ fixed. Hence, we consider the last three terms of the sum rate. For convenience, we define

$$S=\log\left(1+\beta_1Q_1+\beta_2Q_2\right)-\log\left(1+\alpha_1Q_1\right)-\log\left(1+\alpha_2Q_2\right) \qquad (2.94)$$

Consider, without loss of generality, the power allocation for user 1. We assume that P_1^*, Q_1^* is the optimum power allocation for user 1. We observe that the sign of

$$\frac{\partial S}{\partial Q_1}=\frac{\beta_1}{1+\beta_1Q_1+\beta_2Q_2}-\frac{\alpha_1}{1+\alpha_1Q_1} \qquad (2.95)$$

does not depend on Q_1. Consider a power allocation $P_1 = P_1^* - \varepsilon, Q_1 = Q_1^* + \varepsilon$. Hence, we have $P_1 + Q_1 = P_1^* + Q_1^*$ and the first three terms in the expression of the achievable sum rate do not change. On the other hand, if (2.95) is positive, any positive ε results in an increase in the achievable sum rate and jamming with the same sum power is better. While, if (2.95) is negative, then any negative ε results in an increase in the achievable sum rate and transmitting with the same sum power is better. If (2.95) is zero, then the sum rate does not depend on Q_1 and we can set it to zero, i.e., use the sum power in transmitting. Therefore, the optimum power allocation will have either $P_k > 0$ or $Q_k > 0$, but not both.

Suppose that P_1, P_2, Q_1, and Q_2 are the optimal power allocations. Then, the necessary KKT conditions satisfy

$$\frac{\alpha_1}{1+\alpha_1(P_1+Q_1)} - \frac{\beta_1}{1+\beta_1(P_1+Q_1)+\beta_2(P_2+Q_2)} - (\lambda_1 - \mu_1) = 0 \tag{2.96}$$

$$\frac{\alpha_2}{1+\alpha_2(P_2+Q_2)} - \frac{\beta_2}{1+\beta_1(P_1+Q_1)+\beta_2(P_2+Q_2)} - (\lambda_2 - \mu_2) = 0 \tag{2.97}$$

$$\frac{\alpha_1}{1+\alpha_1(P_1+Q_1)} - \frac{\beta_1}{1+\beta_1(P_1+Q_1)+\beta_2(P_2+Q_2)} + \frac{\beta_1}{1+\beta_1 Q_1+\beta_2 Q_2} - \frac{\alpha_1}{1+\alpha_1 Q_1} - (\lambda_1 - \nu_1) = 0 \tag{2.98}$$

$$\frac{\alpha_2}{1+\alpha_2(P_2+Q_2)} - \frac{\beta_2}{1+\beta_1(P_1+Q_1)+\beta_2(P_2+Q_2)} + \frac{\beta_2}{1+\beta_1 Q_1+\beta_2 Q_2} - \frac{\alpha_2}{1+\alpha_2 Q_2} - (\lambda_2 - \nu_2) = 0 \tag{2.99}$$

for some $\lambda_k, \mu_k, \nu_k \geq 0,\ k = 1, 2$. As in Section 2.8, we note that (2.96)-(2.99) are only necessary conditions for the optimal power allocations P_1, P_2, Q_1, and Q_2 since the objective function, i.e., the achievable secrecy sum rate, is not concave

in (P_1, P_2, Q_1, Q_2) in general. Therefore, we give power control policies P_1, P_2, Q_1, and Q_2 that satisfy these necessary conditions. That is, we obtain one fixed point (P_1, P_2, Q_1, Q_2) of the Lagrangian such that (P_1, P_2, Q_1, Q_2) satisfies the constraints (2.92)-(2.93). The power allocation policy (P_1, P_2, Q_1, Q_2) that satisfies (2.96)-(2.99) and (2.92)-(2.93) is described in detail in Appendix.

2.10 Numerical Results

In this section, we present some simple simulation results. We also plot the sum secrecy rate achieved using our SBA and ESA schemes, as well as the i.i.d. Gaussian signaling with cooperative jamming (GS/CJ) scheme in [18]. First, the secrecy sum rates achieved by the SBA and the ESA schemes scale with SNR. Hence, these rates exceed the one achieved by the GS/CJ scheme for high SNR. Second, the secrecy sum rate achieved by the ESA scheme is larger than the one achieved by the SBA scheme for all SNR.

In our first set of simulations, we use a rudimentary power allocation policy for our SBA and ESA schemes. For the SBA scheme, we first note, from (2.32), that the secrecy sum rate achieved can be expressed as a nested expectation as

$$\begin{aligned} R_s =& \frac{1}{2} E_{\mathbf{h}_o, \mathbf{g}_o} \Bigg\{ E_{\mathbf{h}_e, \mathbf{g}_e} \Bigg[\log \Bigg(1 + \left(|h_{1o} g_{2o}|^2 + |h_{1e} g_{2e}|^2 \right) P_1 + \left(|h_{2o} g_{1o}|^2 + |h_{2e} g_{1e}|^2 \right) P_2 \\ & \qquad + |h_{1e} h_{2o} g_{1o} g_{2e} - h_{1o} h_{2e} g_{1e} g_{2o}|^2 P_1 P_2 \Bigg) \\ & \qquad - \log \Bigg(1 + \left(|g_{1o} g_{2o}|^2 + |g_{1e} g_{2e}|^2 \right) (P_1 + P_2) \Bigg) \Bigg] \Bigg\} \end{aligned} \tag{2.100}$$

where $\mathbf{h}_o = [h_{1o}\ h_{2o}]^T$, $\mathbf{h}_e = [h_{1e}\ h_{2e}]^T$, $\mathbf{g}_o = [g_{1o}\ g_{2o}]^T$, and $\mathbf{g}_e = [g_{1e}\ g_{2e}]^T$. For those channel gains $\mathbf{h}_o, \mathbf{g}_o$ for which the inner expectation with respect to $\mathbf{h}_e, \mathbf{g}_e$ is negative, we set $P_1 = P_2 = 0$. Otherwise, we set $P_1 = \frac{1}{2\sigma_g^2}\bar{P}_1$ and $P_2 = \frac{1}{2\sigma_g^2}\bar{P}_2$. Note that turning off the powers for some values of the channel gains $\mathbf{h}_o, \mathbf{g}_o$ is possible since P_1 and P_2 are functions of $\mathbf{h}_o$ and $\mathbf{g}_o$. Secondly, note that, if a power allocation satisfies the average power constraints, then the modified power allocation where the powers are turned off at some channel states, also satisfies the power constraints. For the ESA scheme, we first note, from (2.41), that the achievable secrecy sum rate is

$$R_s = \frac{1}{2} E_{\mathbf{h},\mathbf{g}} \left\{ \log\left(1 + 2|h_1|^2 P_1\right) + \log\left(1 + 2|h_2|^2 P_2\right) - \log\left(1 + 2(|g_1|^2 P_1 + |g_2|^2 P_2)\right) \right\} \tag{2.101}$$

In this case, we set $P_1 = P_2 = 0$ for those values of channel gains for which the difference inside the expectation is negative. Otherwise, we set $P_1 = \bar{P}_1$ and $P_2 = \bar{P}_2$. Again, turning the powers off does not violate power constraints for a power allocation scheme which already satisfies the power constraints. For the GS/CJ scheme, we use the power allocation scheme described in [18].

In Figure 2.1, the secrecy sum rate achieved by each of the three schemes is plotted versus the average SNR that we define as $\frac{1}{2}(\bar{P}_1 + \bar{P}_2)$. In all simulations, we set $\sigma_{h_1}^2 = \sigma_{h_2}^2 = 1.0$, we also take $\sigma_{g_1}^2 = \sigma_{g_2}^2 = 0.75$. Clearly, the secrecy sum rate achieved by the GS/CJ scheme saturates as we increase the SNR while the secrecy sum rate achieved by the SBA and the ESA schemes grows unboundedly with the SNR. One can also notice, as discussed earlier, that the secrecy sum rate achieved by

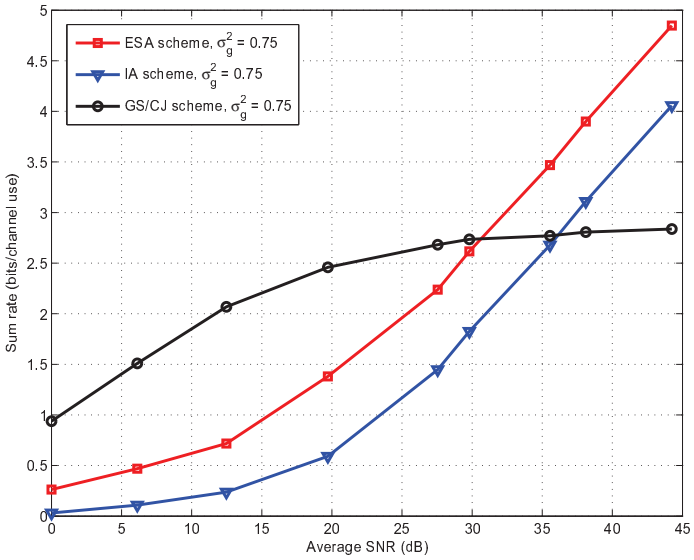

Figure 2.1: Achievable secrecy sum-rates of the SBA, the ESA, and GS/CJ schemes as function of the SNR for two different values of σ_g^2.

the ESA scheme is larger than the one achieved by the SBA scheme which is due to the fact that the ESA scheme creates two totally uncorrelated parallel MAC channels (i.e., orthogonal MAC) between the transmitters and the main receiver.

Next, in Figure 2.2, we plot secrecy sum rates achievable with constant power allocation together with secrecy sum rates achievable with power control for the ESA scheme with and without cooperative jamming. It is clear here that the secrecy sum rate achieved by the ESA/CJ scheme (with power control) is larger than the rate achieved when the ESA scheme is used solely without cooperative jamming (with or without power control). One may also note that, for low SNR, the GS/CJ scheme still gives better rates than those achieved by all the proposed schemes which is due to the factor of $\frac{1}{2}$ in the rates achieved by the proposed schemes due to code repetition.

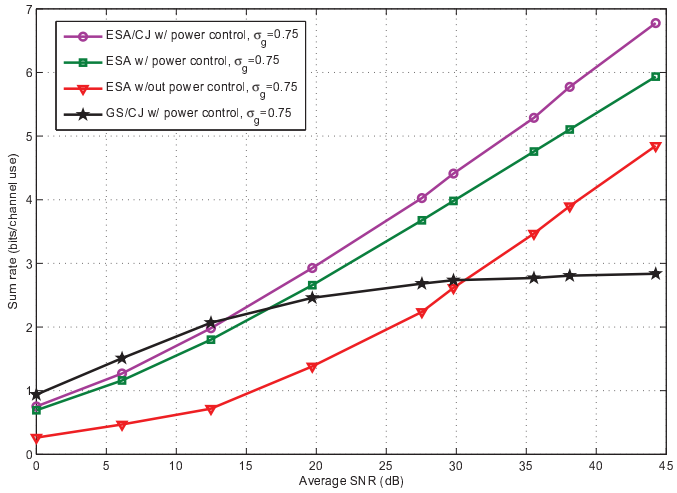

Figure 2.2: Achievable secrecy sum rates for the ESA scheme with and without power control, the ESA/CJ scheme with power control, and the GS/CJ scheme as functions of the SNR for two different values of σ_g^2.

2.11 The SBA and ESA schemes for the K-user Fading MAC-WT Channel

Let $\mathcal{K} \triangleq \{1, ..., K\}$. We consider the K-user MAC-WT for which the channel outputs at the intended receiver and the eavesdropper are given by

$$Y = \sum_{k \in \mathcal{K}} h_k X_k + N \tag{2.102}$$

$$Z = \sum_{k \in \mathcal{K}} g_k X_k + N' \tag{2.103}$$

where, for $k \in \mathcal{K}$, $h_k,\ g_k,\ X_k,\ N,\ N'$ are as defined in Section 2.2. The average power constraints are given by

$$E[|X_k|^2] \leq \bar{P}_k, \quad k \in \mathcal{K} \tag{2.104}$$

2.11.1 The SBA scheme

Here, we use a repetition code in which each transmitter repeats its channel input symbol over K consecutive time instants. Moreover, in every time instant, $\forall k \in \mathcal{K}$, transmitter k multiplies its channel input by $\prod_{i \in \mathcal{K} \setminus \{k\}} g_i$. Thus, over K consecutive time instants, the channel outputs at the main receiver and the eavesdropper are given by

$$Y_j = \sum_{k \in \mathcal{K}} h_{kj} \prod_{i \in \mathcal{K} \setminus \{k\}} g_{ij} X_k + N_j\ , \qquad 1 \leq j \leq K \tag{2.105}$$

$$Z_j = \prod_{i \in \mathcal{K}} g_{ij} \sum_{k \in \mathcal{K}} X_k + N'_j\ , \qquad 1 \leq j \leq K \tag{2.106}$$

where Y_j and Z_j denote the observations at the jth time instant at each of the main receiver and the eavesdropper, respectively, h_{ij} and g_{ij} denote the channel coefficients at the jth time instant from the ith transmitter to the main receiver and the eavesdropper, respectively. Note that due to such scaling at the transmitters, the average power constraints become

$$E\left[\sum_{j=1}^{K} \prod_{i \in \mathcal{K} \setminus \{k\}} |g_{ij}|^2 P_k\right] \leq \bar{P}_k,\ k \in \mathcal{K} \tag{2.107}$$

It is clear from (2.105)-(2.106) that the observed signal space (without noise, i.e., at high SNR) of the main receiver over the K consecutive time instants is K-dimensional almost surely whereas that of the eavesdropper is one-dimensional. Indeed, one can express (2.105)-(2.106) as

$$\mathbf{Y} = \mathbf{H}\mathbf{X} + \mathbf{N} \tag{2.108}$$

$$\mathbf{Z} = \mathbf{G}\mathbf{X} + \mathbf{N}' \tag{2.109}$$

where $\mathbf{X} = [X_1, ..., X_K]^T$,$\mathbf{Y} = [Y_1, ..., Y_K]^T$, $\mathbf{Z} = [Z_1, ..., Z_K]^T$, $\mathbf{H}$ is $K \times K$ full-rank matrix of effective channel gains from the transmitters to the main receiver, and $\mathbf{G}$ is $K \times K$ unit-rank matrix of effective channel gains from the transmitters to the eavesdropper, where the elements at the jth row and the kth column of $\mathbf{H}$ and $\mathbf{G}$ are given, respectively, by

$$H_{jk} = h_{kj} \prod_{i \in \mathcal{K} \setminus \{k\}} g_{ij} \tag{2.110}$$

$$G_{jk} = \prod_{i \in \mathcal{K}} g_{ij} \tag{2.111}$$

Hence, the achievable secrecy sum rate is given by

$$R_s = \frac{1}{K} E_{\mathbf{H},\mathbf{G}} \left\{ \log \left(\det \left(\mathbf{I} + \mathbf{H}\mathbf{S}\mathbf{H}^* \right) \right) - \log \left(\det \left(\mathbf{I} + \mathbf{G}\mathbf{S}\mathbf{G}^* \right) \right) \right\} \tag{2.112}$$

where $\mathbf{S} \triangleq \mathrm{Cov}(\mathbf{X}) = \mathrm{diag}\left(P_1, ..., P_K\right)$ and $\mathbf{A}^*$ denotes the conjugate transpose of the matrix $\mathbf{A}$.

In fact, the system given in (2.108) is equivalent to $K \times K$ MIMO channel with independent signaling across the antennas. Since $\mathbf{H}$ is full-rank, such MIMO channel possesses exactly K DoF. On the other hand, the system given in (2.109) is equivalent to $K \times K$ MIMO channel with independent signaling across the antennas and since $\mathbf{G}$ is unit-rank, such MIMO channel possesses exactly 1 DoF. Therefore, while deriving the total secure DoF achieved by the SBA scheme, conditioned on $\mathbf{H}$ and $\mathbf{G}$, the first term inside the expectation above yields K DoF whereas the second term inside the expectation yields 1 DoF. Thus, the total achievable secure DoF is $\eta = \frac{K-1}{K}$.

2.11.2 The ESA scheme

In order to extend the ESA scheme to the case of more than two users, i.e., K-user fading MAC-WT channel with $K \geq 2$, we use a repetition code, where each code symbol is repeated K times over K channel uses. However, unlike the SBA scheme, repetition is done over channel uses that hold certain conditions relative to those conditions in the channel use where this code symbol is first transmitted. For $1 \leq \ell \leq K$, let

$$\mathbf{h}_\ell \triangleq [h_{1\ell}, ..., h_{K\ell}]^T \tag{2.113}$$

$$\mathbf{g}_\ell \triangleq [g_{1\ell}, ..., g_{K\ell}]^T \tag{2.114}$$

where $h_{k\ell}$ and $g_{k\ell}$ denote the channel coefficients at the ℓth channel use from the kth transmitter to the main receiver and the eavesdropper, respectively. Following the same steps given in Section 2.5, one can easily verify that the optimal repetition

channel use $\ell,\ 2 \leq \ell \leq K$ (relative to the channel use where the first copy of the symbol is transmitted) must be chosen such that

$$\mathbf{h}_\ell = \mathbf{U}_\ell \mathbf{h}_1 \tag{2.115}$$

$$\mathbf{g}_\ell = \mathbf{g}_1 \tag{2.116}$$

where

$$\mathbf{U}_\ell \triangleq \text{diag}\left(1, e^{j\frac{2\pi}{K}(\ell-1)}, ..., e^{j\frac{2\pi}{K}(\ell-1)(K-1)}\right) \tag{2.117}$$

where $j = \sqrt{-1}$. Note that, as explained in Section 2.5, the above argument is based on the proof of the ergodic interference alignment technique given in [14]. The main idea is to quantize the channel coefficients and then group the sets of coefficients of symmetric types together. That is indeed tantamount to grouping $\{\mathbf{h}_\ell,\ \mathbf{g}_\ell : 1 \leq \ell \leq K\}$ together. Note that indeed this is possible due to the circular symmetry of the distribution of the channel coefficients. Then, using the continuity of the achievable rate as a function in channel coefficients, by decreasing the quantization bin size, one can approach the desired rate in the limit.

According to the selection given by (2.115)-(2.116), one can describe the main receiver and the eavesdropper MAC channels over such K channel uses by

$$Y_\ell = \mathbf{h}_1^T \mathbf{U}_\ell \mathbf{X} + N_\ell \tag{2.118}$$

$$Z_\ell = \mathbf{g}_1^T \mathbf{X} + N'_\ell \tag{2.119}$$

for $\ell = 1, ..., K$, where Y_ℓ and Z_ℓ are the observations at channel use ℓ at the main receiver and the eavesdropper, respectively, N_ℓ and N'_ℓ are the noise values at channel use ℓ at the main receiver and the eavesdropper, respectively, and $\mathbf{X} = [X_1, ..., X_K]$ where $X_k,\ k \in \mathcal{K}$ is the channel input of transmitter k.

Using similar argument to the one in Section 2.5, it is easy to see that the system in (2.118) is equivalent to an orthogonal K-user MAC channel where each component of such orthogonal MAC channel has unit-variance noise and channel gain $\sqrt{K}h_{k1},\ k \in \mathcal{K}$, whereas the system in (2.119) is equivalent to one-dimensional MAC channel with unit-variance noise and channel gains $\sqrt{K}g_{k1},\ k \in \mathcal{K}$. Hence, the achievable secrecy sum rate is given by

$$R_s = \frac{1}{K} E_{\mathbf{h}_1, \mathbf{g}_1} \left\{ \sum_{k \in \mathcal{K}} \log\left(1 + K|h_{k1}|^2 P_k\right) - \log\left(1 + K \sum_{k \in \mathcal{K}} |g_{k1}|^2 P_k\right) \right\} \tag{2.120}$$

Therefore, by using the same approach of Section 2.6.2, one can easily verify that the total secure DoF achievable by the ESA scheme in the K-user fading MAC-WT channel is indeed $\eta = \frac{K-1}{K}$.

2.12 Conclusions

In this chapter, we proposed two new achievable schemes for the fading multiple access wiretap channel. Our first scheme, the scaling based alignment (SBA) scheme, lets the interfering signals at the main receiver live in a two-dimensional space, while it aligns the interfering signals at the eavesdropper in a one-dimensional space. We obtained the secrecy rate region achieved by this scheme. We showed that the secrecy rates

achieved by this scheme scale with SNR as $\frac{1}{2}\log(\text{SNR})$, i.e., a total of $\frac{1}{2}$ secure DoF is achievable in the two-user fading MAC-WT. We also showed that the secrecy sum rate achieved by the i.i.d. Gaussian signaling with cooperative jamming scheme does not scale with SNR, i.e., the achievable secure DoF is zero. As a direct consequence, we showed the suboptimality of the i.i.d. Gaussian signaling based schemes with or without cooperative jamming in the fading MAC-WT.

Our second scheme, the ergodic secret alignment (ESA) scheme, is inspired by the ergodic interference alignment technique. In this scheme each transmitter repeats its symbols over carefully chosen time instants such that the interfering signals from the transmitters are aligned favorably at the main receiver while they are aligned unfavorably at the eavesdropper. We obtained the secrecy rate region achieved by this scheme and showed that, as in the scaling based alignment scheme, the secrecy sum rate achieved by the ergodic secret alignment scheme scales with SNR as $\frac{1}{2}\log(\text{SNR})$. In addition, we introduced an improved version of our ESA scheme where cooperative jamming is used as an additional ingredient to achieve higher secrecy rates. Moreover, since the rate expressions achieved with the SBA scheme seem complicated, while the rate expressions achieved with the two versions of the ESA scheme (with and without cooperative jamming) are more amenable for optimization of power allocations, we derived the necessary conditions for the optimal power allocation that maximizes the secrecy sum rate achieved by the ESA scheme when used solely and when used with cooperative jamming. Finally, we discussed the extension of our schemes to the case of more than two users and showed that, for the K-user fading MAC-WT, our schemes achieve secrecy rates that scale with SNR as $\frac{K-1}{K}\log(\text{SNR})$.

2.13 Appendix

2.13.1 Power Control for the ESA Scheme

Here, we discuss the cases of the power allocation policy of Section 2.8.

1. $\alpha_1 \leq \lambda_1, \alpha_2 - \beta_2 \leq \lambda_2$ or $\alpha_1 - \beta_1 \leq \lambda_1, \alpha_2 \leq \lambda_2$. In this case, $P_1 = P_2 = 0$. To prove this, suppose without loss of generality that $\alpha_1 \leq \lambda_1, \alpha_2 - \beta_2 \leq \lambda_2$. We note that $\alpha_1 \leq \lambda_1$ implies that $\alpha_1 - \frac{\beta_1}{(1+\beta_2 P_2)} \leq \lambda_1$ which, using (2.89), implies that $P_1 = 0$. Hence, from (2.90), we must also have $P_2 = 0$. In the same way, we can show that when $\alpha_1 - \beta_1 \leq \lambda_1, \alpha_2 \leq \lambda_2$, we also must have $P_1 = P_2 = 0$.

2. $\alpha_1 \leq \lambda_1, \alpha_2 - \beta_2 > \lambda_2$. In this case, $P_1 = 0$ and $P_2 > 0$ where P_2 is given by (2.88). As in the previous case, $\alpha_1 \leq \lambda_1$, using (2.89), implies that $P_1 = 0$. Hence, from (2.90), we must have $P_2 > 0$.

3. $\alpha_1 - \beta_1 > \lambda_1, \alpha_2 \leq \lambda_2$. In this case, $P_1 > 0$ and $P_2 = 0$ where P_1 is given by (2.87). This case is the same as the previous one with roles of users 1 and 2 interchanged.

4. $\lambda_1 < \alpha_1 \leq \lambda_1 + \beta_1, \lambda_2 < \alpha_2 \leq \lambda_2 + \beta_2$. In this case, the solution (P_1, P_2) may not be unique. Namely, we either have $P_1 > 0$ and $P_2 > 0$, or we have $P_1 = P_2 = 0$. This is due to the following facts. It is easy to see that $P_1 = P_2 = 0$ satisfies $\alpha_1 - \frac{\beta_1}{(1+\beta_2 P_2)} \leq \lambda_1$ and $\alpha_2 - \frac{\beta_2}{(1+\beta_1 P_1)} \leq \lambda_2$, i.e., satisfies conditions (2.89) and (2.90). It is also easy to see that we can find positive P_1 and P_2 such that $\alpha_1 - \frac{\beta_1}{(1+\beta_2 P_2)} > \lambda_1$ and $\alpha_2 - \frac{\beta_2}{(1+\beta_1 P_1)} > \lambda_2$, i.e., there exist positive

P_1 and P_2 that satisfy (2.89) and (2.90). Hence the solution (P_1, P_2) may not be unique. It remains to show that we cannot have $P_1 > 0, P_2 = 0$ or $P_1 = 0, P_2 > 0$. Suppose without loss of generality that $P_1 > 0, P_2 = 0$. Hence, we have $\alpha_1 - \frac{\beta_1}{(1+\beta_2 P_2)} = \alpha_1 - \beta_1 \leq \lambda_1$ which implies that $P_1 = 0$ which is a contradiction. Thus, we cannot have $P_1 > 0, P_2 = 0$. In the same way, it can be shown that we cannot have $P_1 = 0, P_2 > 0$. Hence, we obtain our power allocation policy for this case as follows. We examine the solution of equations (2.85)-(2.86), if it yields a real and non-negative solution (P_1, P_2)[1], then we take it as our solution (P_1, P_2) for this case. Otherwise, we set $P_1 = P_2 = 0$.

5. $\lambda_1 < \alpha_1 \leq \lambda_1 + \beta_1, \alpha_2 - \beta_2 > \lambda_2$. In this case, we must have $P_2 > 0$. However, we either have $P_1 > 0$ or $P_1 = 0$. This can be shown as follows. We note that $\alpha_2 - \beta_2 > \lambda_2$ implies that $\alpha_2 - \frac{\beta_2}{(1+\beta_1 P_1)} > \lambda_2$ for any $P_1 \geq 0$. Hence, by (2.90), we must have $P_2 > 0$. However, we either have $P_1 > 0$ or $P_1 = 0$ depending on whether the value of P_2 satisfies $\alpha_1 - \frac{\beta_1}{(1+\beta_2 P_2)} > \lambda_1$ or not. We obtain our power allocation policies as follows. We first solve (2.85)-(2.86), if this yields a real and non-negative solution (P_1, P_2), then we take it to be the power allocation values for this case. Otherwise, we set $P_1 = 0$ and P_2 is obtained from (2.88).

6. $\alpha_1 - \beta_1 > \lambda_1, \lambda_2 < \alpha_2 \leq \lambda_2 + \beta_2$. By the symmetry between this case and the previous case, we must have $P_1 > 0$ while we either have $P_2 > 0$ or $P_2 = 0$. We obtain our power allocation policies in a fashion similar to that of case 4 and case 5. In particular, we first solve (2.85)-(2.86), if this yields a real and

[1]Note that there is at most one such common root for these two quadratic equations.

non-negative solution (P_1, P_2), then we take it to be the power allocation values for this case. Otherwise, we set $P_2 = 0$ and P_1 is obtained from (2.87).

7. $\alpha_1 - \beta_1 > \lambda_1, \alpha_2 - \beta_2 > \lambda_2$. Here, we must have $P_1 > 0$ and $P_2 > 0$. This is due to the fact that $\alpha_1 - \beta_1 > \lambda_1$ and $\alpha_2 - \beta_2 > \lambda_2$ imply that $\alpha_1 - \frac{\beta_1}{(1+\beta_2 P_2)} > \lambda_1$ and $\alpha_2 - \frac{\beta_2}{(1+\beta_1 P_1)} > \lambda_2$, respectively. Hence, from (2.89)-(2.90), we must have $P_1 > 0$ and $P_2 > 0$. The values of P_1 and P_2 are given by the positive common root (P_1, P_2) of (2.85)-(2.86) which, in this case, have only one positive common root.

2.13.2 Power Control for the ESA/CJ Scheme

Here, we discuss the power allocation policy of Section 2.9.

For each channel state, since splitting power between transmission and jamming is sub-optimal, we can distinguish between five non-zero forms that the solution (P_1, P_2, Q_1, Q_2) of (2.96)-(2.99) may take. First, if $P_1 > 0, P_2 > 0$ and $Q_1 = Q_2 = 0$, then $\mu_1 = \mu_2 = 0$. Hence, from (2.96)-(2.97), we conclude that (P_1, P_2) is the positive common root of equations (2.85)-(2.86) which are found in Section 2.8 and are rewritten here:

$$\alpha_1 (1 + \beta_2 P_2) - \beta_1 = \lambda_1 (1 + \alpha_1 P_1) (1 + \beta_1 P_1 + \beta_2 P_2) \tag{2.121}$$

$$\alpha_2 (1 + \beta_1 P_1) - \beta_2 = \lambda_2 (1 + \alpha_2 P_2) (1 + \beta_1 P_1 + \beta_2 P_2) \tag{2.122}$$

This root can be obtained through numerical solution. Secondly, if $P_1 > 0, Q_2 > 0$ and $P_2 = Q_1 = 0$, then $\mu_1 = \nu_2 = 0$. Hence, from (2.96) and (2.98), we conclude that

(P_1, Q_2) is the positive common root of

$$\alpha_1 (1 + \beta_2 Q_2) - \beta_1 = \lambda_1 (1 + \alpha_1 P_1)(1 + \beta_1 P_1 + \beta_2 Q_2) \tag{2.123}$$

$$\beta_2 \beta_1 P_1 = \lambda_2 (1 + \beta_2 Q_2)(1 + \beta_1 P_1 + \beta_2 Q_2) \tag{2.124}$$

which can also be obtained through numerical solution. Thirdly, if $P_2 > 0, Q_1 > 0$ and $P_1 = Q_2 = 0$, then $\mu_2 = \nu_1 = 0$. Hence, from (2.97) and (2.99), we conclude that (P_2, Q_1) is the positive common root of

$$\alpha_2 (1 + \beta_1 Q_1) - \beta_2 = \lambda_2 (1 + \alpha_2 P_2)(1 + \beta_1 Q_1 + \beta_2 P_2) \tag{2.125}$$

$$\beta_1 \beta_2 P_2 = \lambda_1 (1 + \beta_1 Q_1)(1 + \beta_1 Q_1 + \beta_2 P_2) \tag{2.126}$$

which again can be obtained through numerical solution. The fourth non-zero form of (P_1, P_2, Q_1, Q_2) is when $P_1 > 0$ and $P_2 = Q_1 = Q_2 = 0$, then $\mu_1 = 0$. Hence, from (2.96), P_1 is given by (2.87) which is found in Section 2.8 and will be repeated here for convenience:

$$P_1 = \frac{1}{2}\left(\sqrt{\left(\frac{1}{\beta_1} - \frac{1}{\alpha_1}\right)^2 + \frac{4}{\lambda_1}\left(\frac{1}{\beta_1} - \frac{1}{\alpha_1}\right)} - \left(\frac{1}{\beta_1} + \frac{1}{\alpha_1}\right)\right) \tag{2.127}$$

The last non-zero form of (P_1, P_2, Q_1, Q_2) is when $P_2 > 0$ and $P_1 = Q_1 = Q_2 = 0$, then $\mu_2 = 0$. Hence, from (2.97), P_2 is given by (2.88) in Section 2.8 and is given here

again.

$$P_2 = \frac{1}{2}\left(\sqrt{\left(\frac{1}{\beta_2}-\frac{1}{\alpha_2}\right)^2+\frac{4}{\lambda_2}\left(\frac{1}{\beta_2}-\frac{1}{\alpha_2}\right)}-\left(\frac{1}{\beta_2}+\frac{1}{\alpha_2}\right)\right) \tag{2.128}$$

We obtain the following sufficient conditions on zero jamming powers Q_1 and Q_2. By subtracting (2.98) from (2.96) and subtracting (2.99) from (2.97), we get

$$\frac{\alpha_1}{1+\alpha_1 Q_1}-\frac{\beta_1}{1+\beta_1 Q_1+\beta_2 Q_2}+\mu_1-\nu_1=0 \tag{2.129}$$

$$\frac{\alpha_2}{1+\alpha_2 Q_2}-\frac{\beta_2}{1+\beta_1 Q_1+\beta_2 Q_2}+\mu_2-\nu_2=0 \tag{2.130}$$

which, by using the fact that the two users cannot be jamming together, give the following conditions

$$Q_1 = 0, \qquad \text{if} \quad \alpha_1 > \beta_1 \tag{2.131}$$

$$Q_2 = 0, \qquad \text{if} \quad \alpha_2 > \beta_2 \tag{2.132}$$

Moreover, we obtain necessary and sufficient conditions for the positivity of power allocations in the possible transmission/jamming scenarios in each channel state. First, when no user jams, i.e., $Q_1 = Q_2 = 0$, then from (2.96)-(2.97), we obtain the necessary and sufficient conditions (2.89)-(2.89) of Section 2.8 which we repeat here

for convenience.

$$P_1 > 0, \qquad \text{if and only if} \quad \alpha_1 - \frac{\beta_1}{(1+\beta_2 P_2)} > \lambda_1 \tag{2.133}$$

$$P_2 > 0, \qquad \text{if and only if} \quad \alpha_2 - \frac{\beta_2}{(1+\beta_1 P_1)} > \lambda_2 \tag{2.134}$$

Secondly, when user 1 does not jam and user 2 does not transmit, i.e., $Q_1 = P_2 = 0$, then from (2.96) and (2.98), we can easily derive the following necessary and sufficient conditions for the positivity of the transmission power P_1 of user 1 and the jamming power Q_2 of user 2.

$$P_1 > 0, \qquad \text{if and only if} \quad \alpha_1 - \frac{\beta_1}{(1+\beta_2 Q_2)} > \lambda_1 \tag{2.135}$$

$$Q_2 > 0, \qquad \text{if and only if} \quad \beta_2 - \frac{\beta_2}{(1+\beta_1 P_1)} > \lambda_2 \tag{2.136}$$

Thirdly, when user 1 does not transmit and user 2 does not jam, i.e., $P_1 = Q_2 = 0$, then from (2.97) and (2.99), we can similarly derive the following necessary and sufficient conditions for the positivity of the transmission power P_2 of user 2 and the jamming power Q_1 of user 1.

$$P_2 > 0, \qquad \text{if and only if} \quad \alpha_2 - \frac{\beta_2}{(1+\beta_1 Q_1)} > \lambda_2 \tag{2.137}$$

$$Q_1 > 0, \qquad \text{if and only if} \quad \beta_1 - \frac{\beta_1}{(1+\beta_2 P_2)} > \lambda_1 \tag{2.138}$$

Using conditions (2.131)-(2.138) given above, the power allocation policy (P_1, P_2, Q_1, Q_2) that satisfies (2.96)-(2.99) and (2.92)-(2.93) can be fully described through the fol-

lowing cases of the channel gains.

1. $\alpha_1 > \beta_1, \alpha_2 > \beta_2$. In this case, we must have $Q_1 = Q_2 = 0$. This follows directly from (2.131)-(2.132). Hence, this case reduces to one of the 7 cases given in Section 2.8 depending on the relative values of the channel gains and the values of λ_1 and λ_2. We can obtain the power allocations P_1 and P_2 in the same way described in Section 2.8.

2. $\alpha_1 > \beta_1, \alpha_2 < \beta_2$. In this case, we must have $P_2 = Q_1 = 0$. This can be shown as follows. From (2.131), we must have $Q_1 = 0$. Suppose $P_2 > 0$. Hence, $\mu_2 = 0$. Since dividing power among transmission and jamming is suboptimal, then we must have $Q_2 = 0$. Since $Q_1 = 0$, then (2.130) implies $\bar{h}_2 - \bar{g}_2 \geq 0$ which is a contradiction. Therefore, $P_2 = 0$. The power allocations P_1 and Q_2 are obtained from one of the following sub-cases:

   (a) $\alpha_1 \leq \lambda_1 \quad$ or $\quad \alpha_1 - \beta_1 \leq \lambda_1, \beta_2 \leq \lambda_2$. We have $P_1 = Q_2 = 0$. To see this, note that $\alpha_1 \leq \lambda_1$ implies that $\alpha_1 - \frac{\beta_1}{(1+\beta_2 Q_2)} \leq \lambda_1$. Hence, using (2.135), we must have $P_1 = 0$ and thus $Q_2 = 0$ since we cannot have a jamming user when the other user is not transmitting. On the other hand, if $\beta_2 \leq \lambda_2$, then it follows from (2.136) that $Q_2 = 0$. Hence, the fact that $\alpha_1 - \beta_1 \leq \lambda_1$ together with (2.135) implies that $P_1 = 0$.

   (b) $\alpha_1 - \beta_1 > \lambda_1, \beta_2 \leq \lambda_2$. We have $Q_2 = 0$ and $P_1 > 0$ where P_1 is given by (2.127). This can be shown to be true as follows. Since $\beta_2 \leq \lambda_2$, then, using (2.136), we must have $Q_2 = 0$. Hence, from (2.135) and the fact that $\alpha_1 - \beta_1 > \lambda_1$ in this case, we must have $P_1 > 0$.

(c) $\lambda_1 < \alpha_1 \leq \lambda_1 + \beta_1, \beta_2 > \lambda_2$. In this case, the solution (P_1, Q_2) may not be unique. Namely, we either have $P_1 > 0$ and $Q_2 > 0$, or we have $P_1 = Q_2 = 0$. This is due to the following facts. It is easy to see that $P_1 = Q_2 = 0$ satisfies $\alpha_1 - \frac{\beta_1}{(1+\beta_2 Q_2)} \leq \lambda_1$ and $\beta_2 - \frac{\beta_2}{(1+\beta_1 P_1)} \leq \lambda_2$, i.e. conditions (2.135) and (2.136). It is also easy to see that we can find positive P_1 and Q_2 that satisfy $\alpha_1 - \frac{\beta_1}{(1+\beta_2 Q_2)} > \lambda_1$ and $\beta_2 - \frac{\beta_2}{(1+\beta_1 P_1)} > \lambda_2$, i.e. conditions (2.135) and (2.136). Hence the solution (P_1, Q_2) may not be unique. It remains to show that we cannot have $P_1 > 0, Q_2 = 0$. Suppose that $P_1 > 0$ and $Q_2 = 0$. Hence, we have $\alpha_1 - \frac{\beta_1}{(1+\beta_2 Q_2)} = \alpha_1 - \beta_1 \leq \lambda_1$ which, by (2.135), implies that $P_1 = 0$ which is a contradiction. Thus, we cannot have $P_1 > 0$ and $Q_2 = 0$. We obtain our power allocation policies for this case as follows. We examine the solution of equations (2.123) and (2.124), if it yields a real and non-negative solution (P_1, Q_2), then we take it as our solution (P_1, Q_2) for this case. Otherwise, we set $P_1 = Q_2 = 0$.

(d) $\alpha_1 - \beta_1 > \lambda_1, \beta_2 > \lambda_2$. Here, we must have $P_1 > 0$. However, we either have $Q_2 > 0$ or $Q_2 = 0$, i.e., the solution may not be unique. To see this, we note that $\alpha_1 - \beta_1 > \lambda_1$ implies that $\alpha_1 - \frac{\beta_1}{(1+\beta_2 Q_2)} > \lambda_2$ for any $Q_2 \geq 0$. Hence, by (2.135), we must have $P_1 > 0$. However, we either have $Q_2 > 0$ or $Q_2 = 0$ depending on whether the value of P_1 satisfies $\beta_2 - \frac{\beta_2}{(1+\beta_1 P_1)} > \lambda_1$ or not. We obtain our power allocation policy as follows. We first solve (2.123) and (2.124), if this yields a real and non-negative solution (P_1, Q_2), then we take it to be the power allocation values for this case. Otherwise,

we set $Q_2 = 0$ and P_1 is obtained from (2.127).

3. $\alpha_1 < \beta_1, \alpha_2 > \beta_2$. From the symmetry between this case and the previous case, the power allocation roles can be obtained in this case by interchanging the power allocation roles of users 1 and 2 in the previous case. In particular, we must have $P_1 = Q_2 = 0$. The power allocations P_2 and Q_1 are given by one of the following sub-cases:

   (a) $\alpha_2 \leq \lambda_2 \quad \text{or} \quad \beta_1 \leq \lambda_1, \alpha_2 - \beta_2 \leq \lambda_2$. We have $P_2 = Q_1 = 0$.

   (b) $\beta_1 \leq \lambda_1, \alpha_2 - \beta_2 > \lambda_2$. We have $Q_1 = 0$ and $P_2 > 0$ where P_2 is given by (2.128).

   (c) $\beta_1 > \lambda_1, \lambda_2 < \alpha_2 \leq \lambda_2 + \beta_2$. In this case, the solution (P_2, Q_1) may not be unique as we either have $P_2 > 0$ and $Q_1 > 0$, or have $P_1 = Q_2 = 0$. Therefore, we obtain our power allocation policy for this case by numerically solving equations (2.125) and (2.126), if we have a real and non-negative solution (P_2, Q_1), then we take it as to be the power allocation values for this case. Otherwise, we set $P_2 = Q_1 = 0$.

   (d) $\beta_1 > \lambda_1, \alpha_2 - \beta_2 > \lambda_2$. Here, we must have $P_2 > 0$. However, we either have $Q_1 > 0$ or $Q_1 = 0$, i.e., the solution may not be unique. We obtain our power allocation policy as follows. We first solve (2.125)-(2.126), if this yields a real and non-negative solution (P_2, Q_1), then we take it to be the power allocation values for this case. Otherwise, we set $Q_1 = 0$ and P_2 is obtained from (2.128).

4. $\alpha_1 < \beta_1, \alpha_2 < \beta_2$. In this case, we have $P_2 = Q_1 = 0$ or $P_1 = Q_2 = 0$. In order to see this, suppose $P_1 > 0$ and $P_2 > 0$. Hence, $\mu_1 = \mu_2 = 0$. Since splitting a user's power into transmit and jamming powers is suboptimal, then we must have $Q_1 = Q_2 = 0$. Thus, from (2.129) and (2.130), we have $\bar{h}_1 \geq \bar{g}_1$ and $\bar{h}_2 \geq \bar{g}_2$ which is a contradiction. Therefore, we must have either $P_1 = 0$ or $P_2 = 0$. The power allocation policy (P_1, P_2, Q_1, Q_2) is given in the following four sub-cases of channel states:

   (a) $(\alpha_1 \leq \lambda_1 \quad \text{or} \quad \beta_2 \leq \lambda_2)$ and $(\alpha_2 \leq \lambda_2 \quad \text{or} \quad \beta_1 \leq \lambda_1)$. In this case, we have $P_1 = P_2 = Q_1 = Q_2 = 0$. To see this, first, suppose that $P_2 = Q_1 = 0$. We note that if $\alpha_1 \leq \lambda_1$ then $\alpha_1 - \frac{\beta_1}{(1+\beta_2 Q_2)} \leq \lambda_1$. Hence, using (2.135), we must have $P_1 = 0$ and thus $Q_2 = 0$ since we cannot have a jamming user when the other user is not transmitting. On the other hand, if $\beta_2 \leq \lambda_2$, then it follows from (2.136) that $Q_2 = 0$. Hence, the fact that $\alpha_1 < \beta_1$ together with (2.135) implies that $P_1 = 0$. Next, suppose that $P_1 = Q_2 = 0$. Using the fact that $\alpha_2 \leq \lambda_2$ or $\beta_1 \leq \lambda_1$ together with condition (2.137)-(2.138), we can show that $P_2 = Q_1 = 0$. Therefore, in this case, we must have $P_1 = P_2 = Q_1 = Q_2 = 0$.

   (b) $(\alpha_2 \leq \lambda_2 \quad \text{or} \quad \beta_1 \leq \lambda_1)$ and $(\alpha_1 > \lambda_1, \beta_2 > \lambda_2)$. We have $P_2 = Q_1 = 0$. The solution (P_1, Q_2) may not be unique. In particular, we may have $P_1 > 0, Q_2 > 0$ or have $P_1 = Q_2 = 0$. To see this, consider the following argument. Using the fact that $\alpha_2 \leq \lambda_2$ or $\beta_1 \leq \lambda_1$, then, as shown in case $4(a)$, we conclude that we must have $P_2 = Q_1 = 0$. Now, we consider

the power allocation policy (P_1, Q_2). We note that $P_1 = Q_2 = 0$ satisfies conditions (2.135) and (2.136). On the other hand, we can find positive P_1 and Q_2 that satisfy (2.135) and (2.135). Hence, the solution (P_1, Q_2) may not be unique as we may have $P_1 = Q_2 = 0$ or $P_1 > 0, Q_2 > 0$. It remains to show that we cannot have $P_1 > 0, Q_2 = 0$. Suppose that $P_1 > 0$ and $Q_2 = 0$. Hence, we have $\alpha_1 - \frac{\beta_1}{(1+\beta_2 Q_2)} = \alpha_1 - \beta_1 < 0 < \lambda_1$ which, by (2.135), implies that $P_1 = 0$ which is a contradiction. Thus, we cannot have $P_1 > 0$ and $Q_2 = 0$. Our power allocations P_1 and Q_2 are obtained for this case as follows. We solve (2.123) and (2.124). If the solution gives a real and non-negative common root (P_1, Q_2), we take it as our power allocation values for P_1 and Q_2. Otherwise, we set $P_1 = Q_2 = 0$.

(c) $(\alpha_1 \leq \lambda_1 \quad \text{or} \quad \beta_2 \leq \lambda_2)$ and $(\alpha_2 > \lambda_2, \beta_1 > \lambda_1)$. By the symmetry between this case and case 4(b), we have $P_1 = Q_2 = 0$. Again in this case, the solution (P_2, Q_1) may not be unique. In particular, we may have $P_2 > 0, Q_1 > 0$ or have $P_2 = Q_1 = 0$. In fact, the power allocation policy in this case, can be obtained from case 4(b) by interchanging the roles of users 1 and 2. Our power allocations P_2 and Q_1 are obtained as follows in this case. We solve (2.125)-(2.126). If the solution gives a real and non-negative common root (P_2, Q_1), we take it as our power allocation values for P_2 and Q_1. Otherwise, we set $P_2 = Q_1 = 0$.

(d) $(\alpha_1 > \lambda_1, \beta_2 > \lambda_2)$ and $(\alpha_2 > \lambda_2, \beta_1 > \lambda_1)$. Here, again the solution (P_1, P_2, Q_1, Q_2) is not unique as we may either have $P_1 > 0, Q_2 > 0, P_2 =$

$Q_1 = 0$, or $P_2 > 0, Q_1 > 0, P_1 = Q_2 = 0$, or $P_1 = P_2 = Q_1 = Q_2 = 0$. To see this, first, suppose that $P_2 = Q_1 = 0$ and consider the power allocation policy (P_1, Q_2). As in case $4(b)$, we can show that the solution (P_1, Q_2) may not be unique as we may have $P_1 = Q_2 = 0$ or $P_1 > 0, Q_2 > 0$. However, as shown in case $4(b)$, we cannot have $P_1 > 0, Q_2 = 0$. Next, suppose that $P_1 = Q_2 = 0$ and consider the power allocation policy (P_2, Q_1). As in case $4(c)$, we can show that the solution (P_2, Q_1) may not be unique as we may have $P_2 = Q_1 = 0$ or $P_2 > 0, Q_1 > 0$. However, we cannot have $P_2 > 0, Q_1 = 0$. We obtain our allocation policy (P_1, P_2, Q_1, Q_2) as follows. Let us denote the solution of (2.123) and (2.124) together by *solution A* and denote the solution of (2.125) and (2.126) together by *solution B*.

i. If solution A yields a real non-negative (P_1, Q_2) while solution B does not yield real non-negative (P_2, Q_1), then we take (P_1, Q_2) to be the power allocation values for users 1 and 2, respectively, and set $P_2 = Q_1 = 0$.

ii. If solution B yields a real non-negative (P_2, Q_1) while solution A does not yield real non-negative (P_1, Q_2), then we take (P_2, Q_1) to be the power allocation values for users 2 and 1, respectively, and set $P_1 = Q_2 = 0$.

iii. If neither solution A nor solution B gives real non-negative common root, then we set $P_1 = P_2 = Q_1 = Q_2 = 0$.

iv. If both solutions A and B yield a real non-negative common root, then

we either choose the root given by solution A, i.e., (P_1, Q_2), and set $P_2 = Q_1 = 0$, or choose the root given by solution B, i.e., (P_2, Q_1), and set $P_1 = Q_2 = 0$. We make the choice that maximizes the achievable *instantaneous* secrecy sum rate.

Chapter 3

Deaf Cooperation and Relay Selection Strategies for Secure Communication in Multiple Relay Networks

3.1 Introduction

The notion of introducing artificial noise in a Gaussian wiretap (GWT) channel by a helpful interferer to confuse the eavesdropper and improve over the secrecy capacity of the original wiretap channel was introduced in [31], [34], [19], [20]. In [34], [19], [20], this notion was called *cooperative jamming* (CJ). The term refers to the cooperation strategy in which a helping interferer transmits white Gaussian noise when it can hurt the eavesdropper more than it can hurt the legitimate receiver and hence improve the achievable secrecy rate. In [33], the idea of helping interferer was applied to the GWT channel in a scheme tantamount to the CJ scheme for the two-user multiple access wiretap channel where one of the users performs cooperative jamming. In [30], the destination carried out jamming over the feedback channel to confuse the eavesdropper.

In the context of relay networks with secrecy constraints, the role of cooperative jamming was further investigated in several works. For example, the discrete mem-

oryless relay network was investigated in [32] where achievable secrecy rates were developed when relays help increase secrecy rate by inserting noise into the network. On the other hand, the relay selection problem in the secrecy context was investigated, e.g., in [27] and [22]. In particular, reference [27] proposed a scheme that enables an opportunistic selection of two relays to increase security where one relay uses the decode-and-forward (DF) strategy while the other uses the CJ strategy to introduce useful interference and thus help increase the achievable secrecy rate. In [22], one relay node is selected to assist two source nodes to exchange messages with each other using the amplify-and-forward (AF) strategy while one or two additional relay nodes are selected to transmit jamming signals to confuse the eavesdropper. The role of cooperative jamming in the presence of multiple eavesdroppers was studied in [35] where noise generators (cooperative jammers) were employed in a multiple-relay multiple-eavesdropper network to improve security. The impact of cooperative jamming on the secrecy outage probability of a slow fading wiretap channel was studied in [36] where related security metrics, such as, jamming coverage and jamming efficiency, were introduced and different jamming strategies were proposed depending on the various levels of available channel state information. In a stochastic network model, it was shown in [37] that packet collisions caused by jamming nodes can be used to increase the level of secrecy.

Power allocation for the the source and relay nodes in cooperative jamming relay networks was studied, e.g., in [24], [23], and [25]. In [24], the communication between the source and destination occurs in two hops. Both the source and the relay are allowed to split their available power into a useful information part and a jamming

part. Reference [24] solves for the power allocation under the assumption that both the relay and the destination have the knowledge of the jamming signals. In the multiple antenna case, the power allocation and the antenna weights design problems were investigated for cooperative jamming strategies under the constraint that the jamming signals must lie in the subspace orthogonal to the channels to the legitimate receiver.

In all the references above, the role of a helping node was restricted to cooperative jamming, decode-and-forward, and amplify-and-forward. However, a helping node can also play other roles to improve secrecy. In general, in the relay-eavesdropper channel, the relay, which is assumed to be a trusted entity, can help improve secrecy either by listening to the source or by acting as a deaf helper. The role of a relay node to provide and improve secrecy in a wiretap channel was first studied in [29]. In particular, reference [29] introduced another passive (deaf) mode of cooperation, called *noise forwarding* (NF), in which the relay node sends a dummy (context-free) codeword drawn at random from a codebook that is known to both the legitimate receiver and the eavesdropper to introduce helpful interference that would hurt the eavesdropper more than the legitimate receiver. This deaf cooperation strategy was applied without power control to the Gaussian single-relay single-eavesdropper channel in [28]. The idea of such strategy is to create a virtual multiple access wiretap channel where only one user (the source) is active, i.e., sending relevant information, while the other user (the relay) is acting as an interferer that sends a signal drawn from a given codebook. In this way, the destination can perform successive decoding and cancel out the relay signal and achieve higher

secrecy rate for the intended message.

At this point, it is useful to compare the two aforementioned alternatives of deaf cooperation for secrecy introduced in the literature. Generally speaking, it is not useful to perform CJ when the helper is closer to the destination than to the eavesdropper, on the other hand, one can still introduce helpful interference in this case by transmitting a dummy codeword from a codebook that is known to the destination and the eavesdropper. The transmission of dummy codewords refers to Wyner's idea of stochastic encoding for secrecy [21] where multiple codewords are associated with a single message. Since the cost of these dummy codewords is a decrease in the transmitter's rate, if the helper takes the responsibility of sending these dummy codewords, then the secrecy rate of the transmitter may improve [5].

In this chapter, we investigate in detail the conditions under which a deaf helper performing either CJ or NF strategy would give rise to a larger achievable secrecy rate than the secrecy capacity of the original GWT channel. In particular, we give the necessary and sufficient conditions, in terms of power values and relative channel gains, for each of the two strategies to yield higher secrecy rate than the secrecy capacity of the original GWT channel. We also obtain, in terms of the channel gains solely, the necessary conditions for each of the CJ and the NF strategies to yield a secrecy rate higher than the secrecy capacity of the GWT channel. In particular, we reach the following useful conclusion. Depending on the relative location of a helping node with respect to the destination and the eavesdropper, a helping node may either be a useful jammer or a useful noise forwarder but not both at the same time, or it may not be useful at all as a deaf helper. Moreover, we derive the optimal power

allocation policy for each of the two strategies where we assume that the source, the deaf helper, the legitimate receiver, and the eavesdropper have perfect knowledge of all the relevant channel gains.

On the other hand, we consider applying both CJ and NF strategies in multiple relay networks to improve secrecy rates achievable when only CJ strategy is used. In particular, we consider a multiple relay network of N relays in addition to a source, a legitimate receiver, and an eavesdropper. The objective is to select a set of K, $K \leq N$, relays that act as the best deaf helpers, i.e., that maximize the secrecy rate achievable by deaf cooperation using K relays. We first consider the special case of $K = 1$. We propose an optimal Single Deaf Helper Selection (SDHS) strategy that identifies the optimal deaf helper node and its mode of cooperation (CJ or NF). Our strategy is simple and requires $O(N)$ computations. Second, we consider the general selection problem, i.e., the case where $K > 1$. Both the selection and the optimal power allocation problems are hard in this case. In fact, the number of computations required by the optimal selection strategy is exponential in N. Therefore, we propose a suboptimal Multiple Deaf Helper Selection (MDHS) strategy that selects K (or less) relays over K (or less) selection stages in which the source and the relays negotiate to identify the deaf helpers to be selected one by one in a greedy fashion. In terms of the computational complexity, we show that our strategy is efficient and requires $O(N)$ computations as opposed to the optimal strategy which requires a number of computations that is exponential in N. Finally, we give some numerical examples to compare our strategies, in terms of the achievable secrecy rate, with those based on only one mode of deaf cooperation. We also quantify through some numerical

examples the improvement in the achievable secrecy rate when the MDHS strategy is used instead of the SDHS strategy.

3.2 System Model

We first discuss briefly the basic discrete memoryless relay-eavesdropper channel model, then we describe our system model. The discrete memoryless relay-eavesdropper channel is a four-terminal channel consisting of alphabets $\mathcal{X}_s, \mathcal{X}_r, \mathcal{Y}, \mathcal{Y}_r, \mathcal{Z}$, and a transition probability distribution $p(y, y_r, z|x_s, x_r)$ where $\mathcal{X}_s, \mathcal{X}_r$ are the sets of the symbols of the channel inputs at the source and the relay, respectively, while $\mathcal{Y}, \mathcal{Y}_r, \mathcal{Z}$ are the sets of the symbols of the channel outputs at the destination, the relay, and the eavesdropper, respectively. The channel is memoryless, i.e., the channel outputs $(y_i, y_{r,i}, z_i)$ at time i only depend on the channel inputs $(x_{s,i}, x_{r,i})$ at time i. The source wishes to send a message $W_s \in \mathcal{W}_s = \{1, \ldots, 2^{nR_s}\}$ to the destination using a $(2^{nR_s}, n)$ code consisting of a stochastic encoder φ_s at the source that maps the message $W_s \in \mathcal{W}_s$ to a codeword $X_s^n \in \mathcal{X}_s^n$, a relay encoder that maps the received signals $(Y_{r,1}, \ldots, Y_{r,i-1})$ received at the relay before time i to the channel input $X_{r,i}$ using the mapping $\varphi_{r,i}$, and a decoder ψ at the destination that maps the received sequence Y^n to an estimate of the message $\hat{W}_s \in \mathcal{W}_s$. The probability of error is

$$P_e^n = \Pr\left(\hat{W}_s \neq W_s\right) \tag{3.1}$$

A rate R_s is said to be achievable with perfect secrecy if there is a $(2^{nR_s}, n)$ code satisfying

$$\lim_{n\to\infty} P_e^n = 0, \qquad \text{and} \qquad \lim_{n\to\infty} \frac{1}{n} I\left(W_s; Z^n\right) = 0 \tag{3.2}$$

In this chapter, we consider the following communication scenario. A source, s, sends a confidential message to a destination, d, over an AWGN channel in the presence of an informed eavesdropper, e. The communication occurs in the presence of a set of N nodes (relays), $\mathcal{N} = \{r_1, ..., r_N\}$, from which one is selected (called the helper) to help improve the achievable perfect secrecy through deaf cooperation, i.e., CJ or NF (see Figure 3.1). In other words, it is assumed that either the helper ignores what it receives from the source, i.e., Y_r, or that Y_r is too noisy to be of any use to the helper. Hence, at any time instant, the helper's channel input X_r is independent of Y_r and X_s. In this case, the helper is called deaf and is supposed to operate in one of the two aforementioned modes of deaf cooperation.

Assuming that the relay node $r \in \mathcal{N}$ is selected to be the deaf helper, the outputs of the GWT channel, with the deaf helper r, at the destination and the eavesdropper are given by

$$Y = \sqrt{\gamma_{s,d}}\tilde{X}_s + \sqrt{\gamma_{r,d}}\tilde{X}_r + N \tag{3.3}$$

$$Z = \sqrt{\gamma_{s,e}}\tilde{X}_s + \sqrt{\gamma_{r,e}}\tilde{X}_r + N' \tag{3.4}$$

where $\gamma_{k,l}$, $k \in \{s, r\}$, $l \in \{d, e\}$, is the channel gain between nodes k and l, $\tilde{X}_k$,

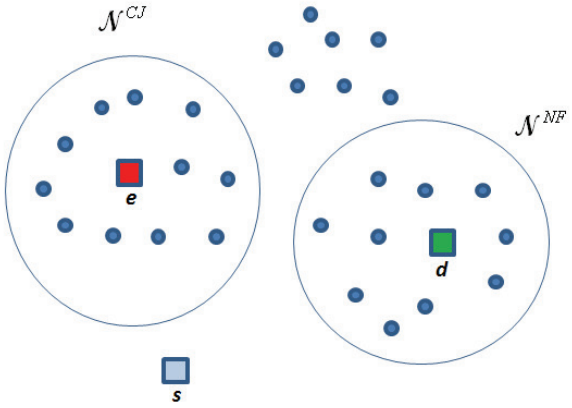

Figure 3.1: A multiple relay network.

$k \in \{s, r\}$ is the channel input at node k, and $N,\ N'$ are real-valued zero mean, unit variance AWGN at the destination and the eavesdropper, respectively. The channel inputs satisfy the following average power constraints

$$E[\tilde{X}_k^2] \leq \bar{\rho}_k, \quad k \in \{s, r\} \tag{3.5}$$

It is assumed that all channel gains in (3.3)-(3.4) are known to $s,\ d,\ r$, and e. For a fixed deaf helper node, r, the above system given by (3.3)-(3.4) and power constraints (3.5) is equivalent to

$$Y = X_s + X_r + N \tag{3.6}$$

$$Z = \sqrt{h_s} X_s + \sqrt{h_r} X_r + N' \tag{3.7}$$

with

$$E[X_k^2] \leq \bar{P}_k \triangleq \bar{\rho}_k \gamma_{k,d}, \quad k \in \{s, r\} \tag{3.8}$$

where $X_k \triangleq \sqrt{\gamma_{k,d}}\tilde{X}_k$ and $h_k \triangleq \frac{\gamma_{k,e}}{\gamma_{k,d}}$, $k \in \{s, r\}$.

3.3 Improving Secrecy through Deaf Cooperation

In this section, we consider the CJ and the NF schemes. In both schemes, the channel input at the source X_s in (4.1)-(4.2) is a symbol of the codeword that represents the encoded confidential message. Such codeword is drawn from an i.i.d. Gaussian codebook, i.e., X_s is Gaussian random variable with zero mean and variance P_s where $P_s \leq \bar{P}_s$. Also, in both schemes, the channel input at the deaf helper X_r in (4.1)-(4.2) is also Gaussian with zero mean and variance P_r where $P_r \leq \bar{P}_r$. However, the difference between the two schemes comes from the origin of X_r. In the CJ scheme, X_r is white Gaussian noise that plays the same role as the background noise at the destination and the eavesdropper except for the fact that it is generated artificially. On the other hand, in the NF scheme, X_r is a symbol of a dummy (context-free) codeword drawn from a Gaussian codebook that is assumed to be available at both the destination and the eavesdropper. Accordingly, for given power values P_s and P_r, the secrecy rate achievable by the CJ scheme [20], R^{CJ}, is given by

$$R^{CJ}(P_s, P_r) = \frac{1}{2} \log \left(\frac{(1 + P_s + P_r)(1 + h_r P_r)}{(1 + h_s P_s + h_r P_r)(1 + P_r)} \right) \tag{3.9}$$

Whereas the secrecy rate achievable by the NF scheme [29], R^{NF}, is given by

$$R^{NF}(P_s, P_r) = \min\left\{\frac{1}{2}\log\left(\frac{(1+P_s)(1+h_rP_r)}{1+h_sP_s+h_rP_r}\right), \frac{1}{2}\log\left(\frac{1+P_s+P_r}{1+h_sP_s+h_rP_r}\right)\right\} \tag{3.10}$$

On the other hand, when no helper node is involved, the secrecy capacity of the original GWT channel [13] for a given power value P_s is given by

$$C^{GWT}(P_s) = \left(\frac{1}{2}\log\left(\frac{1+P_s}{1+h_sP_s}\right)\right)^+ \tag{3.11}$$

where $(x)^+ = \max(0, x)$. In the following theorem, we give the necessary and sufficient conditions for $R^{CJ}(P_s, P_r) \geq C^{GWT}(P_s)$ and $R^{NF}(P_s, P_r) \geq C^{GWT}(P_s)$.

Theorem 3.1 *$R^{CJ}(P_s, P_r) \geq C^{GWT}(P_s)$ if and only if one of conditions (3.12) or (3.13) below is satisfied:*

$$h_s < 1 \leq h_r \quad \textit{and} \quad (h_sh_r - 1) + h_s(h_r - 1)P_s \geq h_r(1 - h_s)P_r \tag{3.12}$$

$$1 \leq h_s < h_r \quad \textit{and} \quad P_r \geq \frac{h_s - 1}{h_r - h_s} \tag{3.13}$$

On the other hand, $R^{NF}(P_s, P_r) \geq C^{GWT}(P_s)$ if and only if one of conditions (3.14),

(3.15), or (3.16) below is satisfied:

$$h_r \leq h_s \leq 1 \tag{3.14}$$

$$h_s < h_r \leq 1 \quad \textit{and} \quad P_s \leq \frac{1-h_r}{h_r - h_s} \tag{3.15}$$

$$h_r < 1 \leq h_s \quad \textit{and} \quad P_r \geq \max\left(\frac{h_s - 1}{h_r}, \frac{h_s - 1}{1-h_r} P_s\right) \tag{3.16}$$

A proof of Theorem 3.1 is given in the Appendix.

One important observation one can make in regard with Theorem 3.1 is that the CJ strategy cannot be beneficial, i.e., it cannot achieve higher secrecy rate than the secrecy capacity of the original GWT channel, if the value of the relative channel gain between the relay node and the eavesdropper h_r is less than 1 or less than the value of the relative channel gain between the source and the eavesdropper h_s. On the other hand, the NF strategy is not useful, if $h_r > 1$. This observation is stated formally in the following corollary.

Corollary 3.1 $h_r \geq \max(h_s, 1)$ *is a necessary condition for the CJ scheme to achieve higher secrecy rate than the secrecy capacity of the original GWT channel. On the other hand,* $h_r \leq 1$ *is a necessary condition for the NF scheme to achieve higher secrecy rate than the secrecy capacity of the original GWT channel.*

3.4 Maximizing the Secrecy Rates Achievable by the CJ and NF Schemes

For fixed relative channel gains h_s and h_r, we obtain the solutions of the following optimization problems.

$$\max_{P_s,P_r} R^{CJ}(P_r,P_s) \quad \text{s.t.} \quad 0 \le P_s \le \bar{P}_s,\ 0 \le P_r \le \bar{P}_r \tag{3.17}$$

$$\max_{P_s,P_r} R^{NF}(P_r,P_s) \quad \text{s.t.} \quad 0 \le P_s \le \bar{P}_s,\ 0 \le P_r \le \bar{P}_r \tag{3.18}$$

Let $(\hat{P}_s^{CJ},\hat{P}_r^{CJ})$ be the maximizer of (3.17) and $(\hat{P}_s^{NF},\hat{P}_r^{NF})$ be the maximizer of (3.18). We define $\bar{R}^{CJ} \triangleq R^{CJ}(\hat{P}_s^{CJ},\hat{P}_r^{CJ})$ and $\bar{R}^{NF} \triangleq R^{NF}(\hat{P}_s^{NF},\hat{P}_r^{NF})$.

Theorem 3.2 *The solution of (3.17) and (3.18) above is given in the following cases:*

1. $h_s < 1$*: In this case, we have the following three possibilities depending on the value of* h_r*:*

   (a) If $h_s < 1 \le h_r$*, then*

$$\hat{P}_s^{CJ} = \bar{P}_s,\ \hat{P}_r^{CJ} = \left(\min\left(\bar{P}_r, P_r^*\right)\right)^+ \tag{3.19}$$

$$\hat{P}_s^{NF} = \bar{P}_s,\ \hat{P}_r^{NF} = 0 \tag{3.20}$$

(b) If $h_s < h_r < 1$, then

$$\hat{P}_s^{CJ} = \bar{P}_s,\ \hat{P}_r^{CJ} = 0 \tag{3.21}$$

$$\hat{P}_s^{NF} = \bar{P}_s \tag{3.22}$$

$$\hat{P}_r^{NF} = \bar{P}_r,\ \textit{if } \bar{P}_s < \frac{1-h_r}{h_r-h_s} \tag{3.23}$$

$$\hat{P}_r^{NF} = 0,\ \textit{if } \bar{P}_s \geq \frac{1-h_r}{h_r-h_s} \tag{3.24}$$

(c) If $h_r \leq h_s < 1$, then

$$\hat{P}_s^{CJ} = \bar{P}_s,\ \hat{P}_r^{CJ} = 0 \tag{3.25}$$

$$\hat{P}_s^{NF} = \bar{P}_s,\ \textit{if } \bar{P}_r < \frac{1-h_s}{h_s-h_r} \tag{3.26}$$

$$\hat{P}_s^{NF} = \min\left(\bar{P}_s, \frac{1-h_r}{h_r}\right),\ \textit{if } \bar{P}_r \geq \frac{1-h_s}{h_s-h_r} \tag{3.27}$$

$$\hat{P}_r^{NF} = \bar{P}_r \tag{3.28}$$

2. $h_s \geq 1$: In this case, we have the following three possibilities depending on the value of h_r:

(a) If $1 \leq h_s < h_r$, then

$$\hat{P}_s^{CJ} = 0,\ \hat{P}_r^{CJ} = 0,\ \textit{if } \bar{P}_r \leq \frac{h_s-1}{h_r-h_s} \tag{3.29}$$

$$\hat{P}_s^{CJ} = \bar{P}_s,\ \hat{P}_r^{CJ} = \min\left(\bar{P}_r, P_r^*\right),\ \textit{if } \bar{P}_r > \frac{h_s-1}{h_r-h_s} \tag{3.30}$$

$$\hat{P}_s^{NF} = 0,\ \hat{P}_r^{NF} = 0 \tag{3.31}$$

(b) If $h_r < 1 \leq h_s$, *then*

$$\hat{P}_s^{CJ} = 0,\ \hat{P}_r^{CJ} = 0 \tag{3.32}$$

$$\hat{P}_s^{NF} = 0,\ \hat{P}_r^{NF} = 0,\ \textit{if}\ \bar{P}_r \leq \frac{h_s - 1}{h_r} \tag{3.33}$$

$$\hat{P}_s^{NF} = \min\left(\bar{P}_s, \frac{1 - h_r}{h_r}\right),\ \hat{P}_r^{NF} = \bar{P}_r,\ \textit{if}\ \bar{P}_r > \frac{h_s - 1}{h_r} \tag{3.34}$$

(c) If $1 \leq h_r \leq h_s$, *then*

$$\hat{P}_s^{CJ} = 0,\ \hat{P}_r^{CJ} = 0 \tag{3.35}$$

$$\hat{P}_s^{NF} = 0,\ \hat{P}_r^{NF} = 0 \tag{3.36}$$

where

$$P_r^* = \frac{\sqrt{(h_s(h_r - h_s)\bar{P}_s + h_s(h_r - 1))(h_r - 1)h_r} - h_r(1 - h_s)}{h_r(h_r - h_s)} \tag{3.37}$$

A proof of Theorem 3.2 is given in the Appendix.

As a consequence of Theorem 3.2, one can identify, in terms of the relative channel gains solely, the minimal set of necessary conditions for each of $\bar{R}^{CJ} > C^{GWT}$ and $\bar{R}^{NF} > C^{GWT}$ to hold. These conditions are stated formally in the following corollary.

Corollary 3.2 *If* $\bar{R}^{CJ} > C^{GWT}$, *then* $h_r > \max(1, h_s)$. *On the other hand, if* $\bar{R}^{NF} > C^{GWT}$ *then* $h_r < \min\left(1, \frac{1+h_s\bar{P}_s}{1+\bar{P}_s}\right)$.

3.5 Deaf Helper Selection Problem

3.5.1 Single Deaf Helper Selection

In this section, we are interested in selecting one relay from the set $\mathcal{N}$ of N relays that would act as the best deaf helper that maximizes the achievable secrecy rate which could be either $\bar{R}^{CJ}$ if the best deaf helper is a cooperative jammer or $\bar{R}^{NF}$ if the best deaf helper is a noise forwarder. Here, we assume that the original power constraints at the relays $\bar{\rho}_r,\ r \in \mathcal{N}$ given by (3.5) are equal. That is $\bar{\rho}_r = \bar{\rho}\ \ \forall r \in \mathcal{N}$. Consequently, the scaled power constraints at the relays $\bar{P}_r,\ r \in \mathcal{N}$, given by (3.8), have different values depending on the values of the corresponding channel gains $\gamma_{r,d},\ r \in \mathcal{N}$. Thus, in order to clarify the presentation in this section, we choose to consider the original system given by (3.3)-(3.4) together with the original power constraints (3.5). Let ρ_s and ρ_r denote the variance of $\tilde{X}_s$ and $\tilde{X}_r,\ r \in \mathcal{N}$, respectively, where $\rho_s \leq \bar{\rho}_s$ and $\rho_r \leq \bar{\rho}_r,\ r \in \mathcal{N}$.

The secrecy rates R^{CJ} and R^{NF} in (3.9) and (3.10), respectively, can be written as functions of ρ_s and ρ_r as follows

$$R^{CJ}(\rho_s, \rho_r) = \frac{1}{2}\log\left(\frac{\left(1+\gamma_{s,d}\rho_s+\gamma_{r,d}\rho_r\right)\left(1+\gamma_{r,e}\rho_r\right)}{\left(1+\gamma_{s,e}\rho_s+\gamma_{r,e}\rho_r\right)\left(1+\gamma_{r,d}\rho_r\right)}\right) \tag{3.38}$$

$$R^{NF}(\rho_s, \rho_r) = \min\left\{\frac{1}{2}\log\left(\frac{\left(1+\gamma_{s,d}\rho_s\right)\left(1+\gamma_{r,e}\rho_r\right)}{1+\gamma_{s,e}\rho_s+\gamma_{r,e}\rho_r}\right), \frac{1}{2}\log\left(\frac{1+\gamma_{s,d}\rho_s+\gamma_{r,d}\rho_r}{1+\gamma_{s,e}\rho_s+\gamma_{r,e}\rho_r}\right)\right\} \tag{3.39}$$

We note that all the results of Theorems 3.1 and 3.2 as well as Corollary 3.1 are valid here by replacing h_k with $\frac{\gamma_{k,e}}{\gamma_{k,d}}$, h_k with $\frac{\gamma_{k,e}}{\gamma_{k,d}}$, P_k with $\gamma_{k,d}\rho_k$, $\bar{P}_k$ with $\gamma_{k,d}\bar{\rho}_k$, $\hat{P}_k^{CJ}$

and $\hat{P}_k^{NF}$ with $\gamma_{k,d}\hat{\rho}_k^{CJ}$ and $\gamma_{k,d}\hat{\rho}_k^{NF}$, respectively, for $k \in \{s, r\}$ and $r \in \mathcal{N}$ where $(\hat{\rho}_s^{CJ},\ \hat{\rho}_r^{CJ})$ and $(\hat{\rho}_s^{NF},\ \hat{\rho}_r^{NF})$ are the optimal power control policies that maximize (3.38) and (3.39), respectively. Hence, using Corollary 3.2, one can find two disjoint subsets of $\mathcal{N}$ which we denote by $\mathcal{N}^{CJ}$ and $\mathcal{N}^{NF}$, where

$$\mathcal{N}^{CJ} \triangleq \left\{ r_j \in \mathcal{N} : \frac{\gamma_{r_j,e}}{\gamma_{r_j,d}} > \max\left(1, \frac{\gamma_{s,e}}{\gamma_{s,d}}\right) \right\} \tag{3.40}$$

is the set of potential cooperative jammers, and

$$\mathcal{N}^{NF} \triangleq \left\{ r_j \in \mathcal{N} : \frac{\gamma_{r_j,e}}{\gamma_{r_j,d}} < \min\left(1, \frac{1+\gamma_{s,e}\bar{\rho}_s}{1+\gamma_{s,d}\bar{\rho}_s}\right) \right\} \tag{3.41}$$

is the set of potential noise forwarders. In other words, the set $\mathcal{N}^{CJ}$ is the set that contains every relay node whose relative channel gain satisfies the condition in Corollary 3.2 necessary for the CJ scheme to achieve a secrecy rate larger than C^{GWT}. On the other hand, the set $\mathcal{N}^{NF}$ is the set that contains every relay node whose relative channel gain satisfies the condition in Corollary 3.2 necessary for the NF scheme to achieve a secrecy rate larger than C^{GWT}. Since these two subsets are disjoint, it follows that a node in $\mathcal{N}$ cannot be a useful cooperative jammer and a useful noise forwarder at the same time. It is also noteworthy that there might be some other nodes in $\mathcal{N}$ that do not fall in any of the two subsets $\mathcal{N}^{CJ}$ and $\mathcal{N}^{NF}$.

One can always regard the optimal power allocation policies $(\hat{\rho}_s^{CJ},\ \hat{\rho}_r^{CJ})$ and $(\hat{\rho}_s^{NF},\ \hat{\rho}_r^{NF})$ as functions of the channel gains $(\gamma_{r,d}, \gamma_{r,e})$ where $r \in \mathcal{N}^{CJ}$ and $r \in \mathcal{N}^{NF}$, respectively. Hence, the optimal rates $\bar{R}^{CJ}$ and $\bar{R}^{NF}$ can be also regarded as func-

tions of $(\gamma_{r,d}, \gamma_{r,e})$. Below, we describe a strategy for selecting the optimal relay node $r^* \in \mathcal{N}$ that maximizes the deaf cooperation secrecy rate.

3.5.2 Single Deaf Helper Selection (SDHS) Strategy

For each $r \in \mathcal{N}$, using its knowledge of its own channel gains and using the conditions in (3.40)-(3.41), r identifies which mode of cooperation (CJ or NF) it should target. Accordingly, r computes one of the two rates $\bar{R}^{CJ}(\gamma_{r,d}, \gamma_{r,e})$ and $\bar{R}^{NF}(\gamma_{r,d}, \gamma_{r,e})$ depending on the target mode of cooperation. We note that the rate is computed using the values of the optimal power allocations that are given by Theorem 3.2. Then r sends this information to s. Upon receiving such information from all $r \in \mathcal{N}$, s identifies the relay r^* with the maximum rate R^* and knows its mode of cooperation. Consequently, s notifies r^* that it has been selected as the optimal deaf helper which in turn notifies d of the former's selection. It is assumed that this information is also intercepted by e. By executing the SDHS strategy described above, the optimal relay r^* that achieves $\max_{r\in\mathcal{N}} \max\{\bar{R}^{CJ}(\gamma_{r,d}, \gamma_{r,e}),\ \bar{R}^{NF}(\gamma_{r,d}, \gamma_{r,e})\}$ is identified together with its mode of deaf cooperation.

Assuming that evaluating any of the rate or power functions given above requires $O(1)$ computations, since computation is done in a distributed fashion over N relays, it follows that the complexity of the above strategy in terms of the number of computations required during its execution is $O(N)$. This is due to the fact that finding the maximum of all the rates received by s from all $r \in \mathcal{N}$ requires $O(N)$ computations.

3.5.3 Multiple Deaf Helpers Selection

The system permits us to involve at most K relays, $1 \leq K \leq N$, in deaf cooperation. Each relay can be either a cooperative jammer or a noise forwarder. Let $\mathcal{K}^{CJ} \subseteq \mathcal{N}^{CJ}$ denote the set of the selected cooperative jammers and $\mathcal{K}^{NF} \subseteq \mathcal{N}^{NF}$ denote the set of the selected noise forwarders where $|\mathcal{K}^{CJ} \bigcup \mathcal{K}^{NF}| \leq K$. The achievable secrecy rate in this case for fixed power values $\rho_s,\ \rho_r,\ r \in \mathcal{K}^{CJ} \bigcup \mathcal{K}^{NF}$, is given as a function of $(\mathcal{K}^{CJ}, \mathcal{K}^{NF})$ by

$$R(\mathcal{K}^{CJ}, \mathcal{K}^{NF}) = \min_{\mathcal{M} \subseteq \mathcal{K}^{NF}} \left\{ \frac{1}{2} \log \left(\frac{1 + \gamma_{s,d}\rho_s + \sum_{r \in \mathcal{M}} \gamma_{r,d}\rho_r}{1 + \sum_{r \in \mathcal{K}^{CJ}} \gamma_{r,d}\rho_r} \right) - \frac{1}{2} \log \left(\frac{1 + \gamma_{s,e}\rho_s + \sum_{r \in \mathcal{M}} \gamma_{r,e}\rho_r}{1 + \sum_{r \in \mathcal{K}^{CJ}} \gamma_{r,e}\rho_r + \sum_{r \in \mathcal{K}^{NF} \setminus \mathcal{M}} \gamma_{r,e}\rho_r} \right) \right\} \tag{3.42}$$

In fact, the problem of finding the optimal set of deaf helpers whose size is at most K is hard for $K > 1$ in general. Not only the selection problem is hard in this case, but also even if we fix K deaf helpers, $K > 1$, then the problem of finding the optimal power allocations becomes analytically intractable in this case. Consequently, no closed-form solutions could be found and we are left with search algorithms whose running time could be unacceptably large and their convergence to the global optimum is not even guaranteed. Hence, we propose below a suboptimal strategy that builds upon the SDHS strategy presented earlier to select at most K out of the available N relays that would possibly operate in different modes of cooperation to achieve larger secrecy rate.

3.5.4 Multiple Deaf Helpers Selection (MDHS) Strategy

The strategy is carried out over at most K stages to select at most K deaf helpers. We define $\mathcal{K}_i^{CJ}$ and $\mathcal{K}_i^{NF}$ as the set of selected cooperative jammers and noise forwarders by the end of stage i, respectively. Before the first selection stage, we have $\mathcal{K}_0^{CJ} = \mathcal{K}_0^{NF} = \emptyset$. In the first stage, we run the SDHS strategy to obtain the best deaf helper $r_1^* \in \mathcal{N}$, identify its mode of cooperation (CJ or NF), and compute the corresponding achievable secrecy rate R_1^*. These are all made known to s. Moreover, the identity of r_1^* and its cooperation mode are known to $d,\ e$, and the rest of the relays by the end of the first stage. Accordingly, we either have $\mathcal{K}_1^{CJ} = \{r_1^*\}$ and $\mathcal{K}_1^{NF} = \emptyset$ or vice versa depending on the identified mode of cooperation of r_1^*. For $2 \leq i \leq K$, fix the transmission powers as $\rho_s = \bar{\rho}_s$ and $\rho_r = \bar{\rho}_r,\ r \in \mathcal{N}$. For each $r \in \mathcal{N} \setminus \{r_j^* : 1 \leq j \leq i-1\}$, r computes two secrecy rates, namely, $R\left(\mathcal{K}_{i-1}^{CJ} \cup \{r\},\ \mathcal{K}_{i-1}^{NF}\right)$ and $R\left(\mathcal{K}_{i-1}^{CJ},\ \mathcal{K}_{i-1}^{NF} \cup \{r\}\right)$ using (3.42), i.e., the secrecy rates when r plays the role of a cooperative jammer and when it plays the role of a noise forwarder. Hence, r finds the maximum of the two rates and its corresponding mode of cooperation. Then r sends this rate to s. Consequently, s finds the maximum R_i^* of all the rates it receives from all the relays involved in stage i. If $R_i^* \leq R_{i-1}^*$, then the strategy is terminated and the last selection stage would be $i-1$. Otherwise, s identifies the relay r_i^* corresponding to the rate R_i^* and its mode of cooperation. Upon termination at stage t, $1 \leq t \leq K$, the set of the selected deaf helpers $\{r_i^* : 1 \leq i \leq t\}$ and their modes of cooperation are eventually known to $s,\ d$, and e and the achievable secrecy rate in this case is R_t^*.

To derive the complexity of the MDHS strategy above, first, we note that in the ith selection stage, each relay r has to evaluate the rate in (3.42) for two choices of $\left(\mathcal{K}^{CJ}, \mathcal{K}^{NF}\right)$, namely, $\left(\mathcal{K}_{i-1}^{CJ} \cup \{r\},\ \mathcal{K}_{i-1}^{NF}\right)$ and $\left(\mathcal{K}_{i-1}^{CJ},\ \mathcal{K}_{i-1}^{NF} \cup \{r\}\right)$. For each choice, each relay $r \in \mathcal{N}$ has to find the minimum of 2^i terms. The evaluation of each of these terms is assumed to involve i computations. Thus, each relay $r \in \mathcal{N}$ performs $(i+1)2^i$ computations to evaluate the rate in (3.42). Since each relay r does this computation twice $\big($one for each choice of $\left(\mathcal{K}^{CJ}, \mathcal{K}^{NF}\right)$ $\big)$, then the total number of computation done by each relay is $(i+1)2^{i+1}$. At the source s, finding the maximum rate R_i^* requires about N computations and comparing R_i^* with R_{i-1}^* requires a single computation. Thus, the ith stage of the MDHS strategy requires $N + (i+1)2^{i+1} + 1$ computations. Note that each relay $r \in \mathcal{N}$ computes the rate in (3.42) on its own, i.e., the computation of all the rates is done in a distributed fashion over the N relays in every stage of the strategy. That is why the term $(i+1)2^{i+1}$ is not scaled by N. Since there are at most K selection stages in the MDHS strategy, in the worst case, the total number of computations required in the execution of the MDHS strategy is $K(2^{K+3} - 2^{K+2} + N + 1) + 2$ which is indeed $O(N)$ since K is assumed to be a constant that does not depend on N. Thus, our strategy is efficient. On the other hand, an optimal strategy that computes the achievable secrecy rate using every possible set of relays $\mathcal{M} \subseteq \mathcal{N}$ with $|\mathcal{M}| \leq K$, then finding the maximum rate together with the optimal relay assignment is inefficient since it requires $\sum_{i=1}^{K} \binom{N}{i} 2^{N-i} \left((i+1)2^i + 1\right)$ computations which is greater than 2^N computations.

3.6 Numerical Results

First, we consider the single deaf helper case. We compare the two modes of deaf cooperation and verify the conditions of Corollary 3.2 by plotting the optimal secrecy rate achievable by each of CJ and NF modes against the relative channel gain between the deaf helper and the eavesdropper, h_r.

In Figure 3.2, we set the scaled power constraints of the source and the deaf helper defined in (3.8) as $\bar{P}_s = \bar{P}_r = 5$. We consider two cases. In the first case, we choose $h_s < 1$, namely, we set $h_s = 0.75$. In the second case, we choose $h_s > 1$, namely, $h_s = 1.25$. For each case, we plot $\bar{R}^{CJ}$ and $\bar{R}^{NF}$ versus the relative channel gain h_r. We observe that $\bar{R}^{CJ} = C^{GWT}$ when $h_r \leq \max(1, h_s)$ and $\bar{R}^{CJ} > C^{GWT}$ otherwise. One can also see that $\lim_{h_r \to \infty} \bar{R}^{CJ}(h_r) = C^G$ where C^G is the capacity of the Gaussian channel between the source and the destination when no secrecy constraint is imposed, i.e., when the eavesdropper is not present. On the other hand, we observe that $\bar{R}^{NF} = C^{GWT}$ when $h_r \geq \min\left(1, \frac{1+h_s\bar{P}_s}{1+\bar{P}_s}\right)$ whereas $\bar{R}^{NF} > C^{GWT}$ otherwise.

Next, we consider the multiple deaf helper case. Consider a disk of radius 1 km where the source is located at the center, both the destination and the eavesdropper are located at some fixed points on the circumference. Consider N relays whose locations are chosen randomly and uniformly in this disk. Each channel gain is generated according to the formula: $\gamma = \frac{SV}{d^\alpha}$ where γ is the channel gain, S is a lognormal random variable to account for shadowing, and V is a Rayleigh random variable for fading, d is the distance, and α is the path loss [45]. We assume that

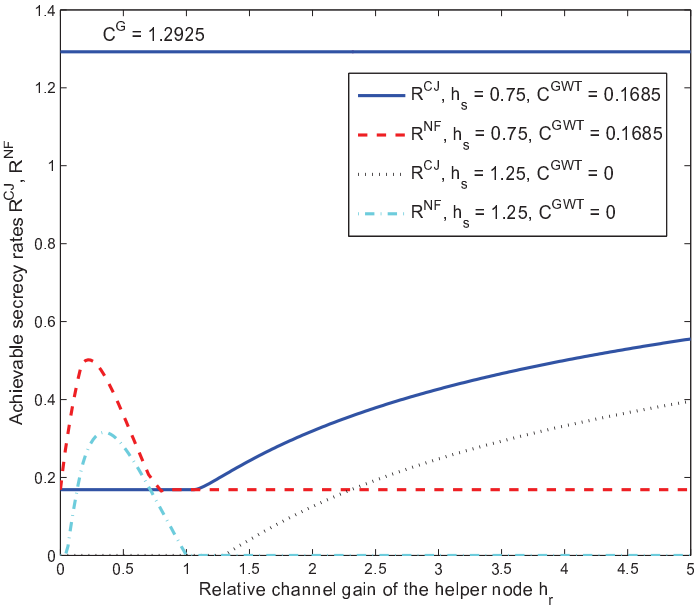

Figure 3.2: The optimal achievable rates $\bar{R}^{CJ}$ and $\bar{R}^{NF}$ as functions of h_r, for two cases of the h_s.

the underlying Gaussian random variables from which S and V are generated are independent, zero mean, and unit variance Gaussian random variables. We also take $\alpha = 3$. We set $\bar{\rho}_s = 10$ and $\bar{\rho}_r = 1$ $\forall r \in \mathcal{N}$.

In Figure 3.3, we plot the achievable secrecy rate against the maximum allowed number of helpers, K, for $N = 25$ and 50, in three different cases. In the first case, the secrecy rate is obtained using the MDHS strategy described in the previous section. In the second case, we only consider CJ as the only deaf cooperation mode, i.e., ignore all the relays that could be useful noise forwarders and use the MDHS strategy only for useful cooperative jammers. In the third case, we consider only NF as the only mode available for deaf cooperation. It is clear from Figure 3.3 that making use of the two modes (CJ/NF) together in the system could significantly increase the achievable

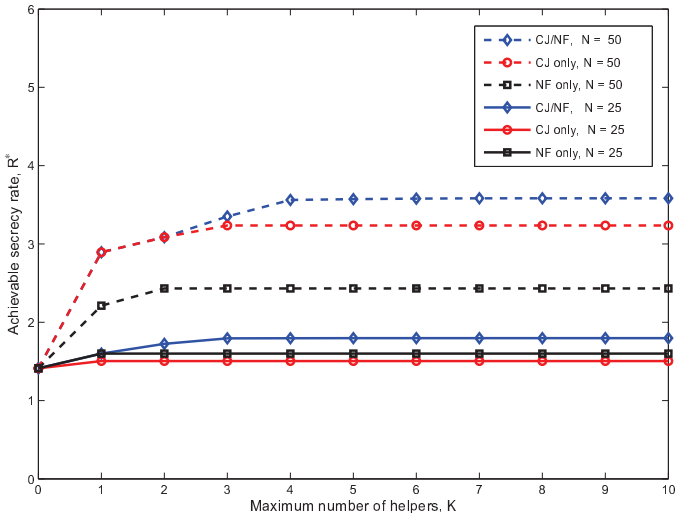

Figure 3.3: The achievable secrecy rate, R^*, versus the maximum allowed number of deaf helpers, K, for three cases: CJ/NF, NF only, and CJ only

secrecy rates. Also, we notice that one could benefit from considering a larger set of relays, i.e., larger N, as this may lead to a better selected set of helpers.

In Figure 3.4 the achievable secrecy rate, R^*, is plotted against the maximum allowed number of helpers, K, for three different realizations of the relays where $N = 50$. It can be seen that the selected helpers could be cooperative jammers (CJ) or noise forwarders (NF), or both, and that one can improve the achievable rate by selecting more than one helper. One can also see that the number of selected helpers could be less than K. Specifically, for the realizations considered here, the numbers of selected helpers are $2, 4$, and 6.

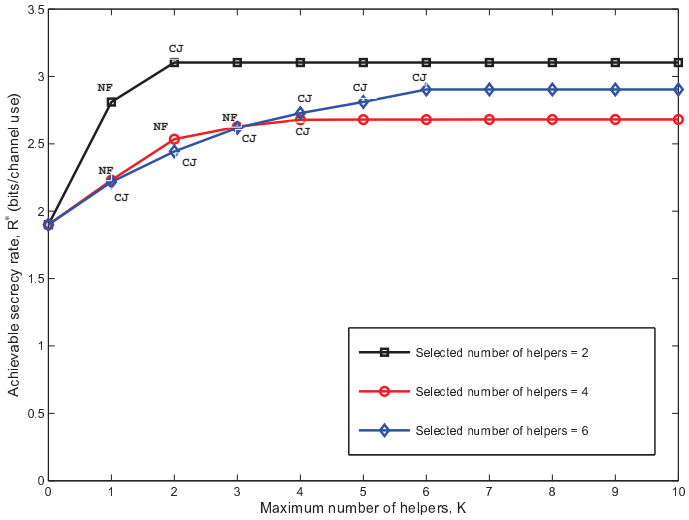

Figure 3.4: The achievable secrecy rate versus the maximum allowed number of helpers, K, for three realizations of relays locations, with $N = 50$.

3.7 Conclusions

In this chapter, we considered two modes of deaf cooperation for secrecy, CJ and NF. We gave the necessary conditions for each of the two modes to yield higher secrecy rates than the secrecy capacity of the original GWT channel. We also showed that a node cannot be both useful jammer and noise forwarder at the same time. Moreover, we derived the optimal power control policy that maximizes the secrecy rate achieved by each of the two modes. For the deaf helper selection problem, we proposed an optimal strategy to select a single deaf helper that maximizes the secrecy rate achievable by deaf cooperation with a single helper. We also proposed a suboptimal strategy for the selection of multiple deaf helpers to increase the achievable secrecy rates. We discussed the complexity of the two proposed strategies and showed that both of them are efficient. We gave numerical results to verify the derived conditions

for a useful deaf cooperation. We also presented examples to compare our strategies with those only based on one mode of cooperation. Also, through numerical examples, we showed the improvement in the secrecy rate achieved when using multiple deaf helpers instead of just one.

3.8 Appendix

3.8.1 Proof of Theorem 3.1

First, we show that $R^{CJ}(P_s, P_r) \geq C^{GWT}(P_s)$ if and only if (3.12) or (3.13) holds. It is easy to see that if any of (3.12) and (3.13) holds, then $R^{CJ}(P_s, P_r) \geq C^{GWT}(P_s)$. Now, suppose that $R^{CJ}(P_s, P_r) \geq C^{GWT}(P_s)$, then from (3.9) and (5.8), we have $R^{CJ}(P_s, P_r) \geq \frac{1}{2}\log\left(\frac{1+P_s}{1+h_s P_s}\right)$ and $R^{CJ}(P_s, P_r) \geq 0$ which imply

$$(h_s h_r - 1) + h_s(h_r - 1)P_s \geq h_r(1 - h_s)P_r \tag{3.43}$$

$$h_s - 1 \leq (h_r - h_s)P_r \tag{3.44}$$

Condition (3.44) implies $h_s \leq \max(1, h_r)$. On the other hand, we cannot have $\max(h_r, h_s) < 1$ since this contradicts (3.43). By considering the remaining possibilities, we either have

$$1 \leq h_s < h_r \tag{3.45}$$

which directly implies (3.43), or we have

$$h_s < 1 \leq h_r \tag{3.46}$$

which directly implies (3.44). Thus, if $R^{CJ}(P_s, P_r) \geq C^{GWT}(P_s)$, then we either have (3.43) and (3.46) satisfied together which is indeed condition (3.12), or we have (3.44) and (3.45) satisfied together which is condition (3.13).

Now, we prove the second part of Theorem 3.1. Again, it is easy to verify that if any of conditions (3.14)-(3.16) holds, then $R^{NF}(P_s, P_r) \geq C^{GWT}(P_s)$. Now, suppose that $R^{NF}(P_s, P_r) \geq C^{GWT}(P_s)$, then from (3.10) and (5.8), we have $R^{NF}(P_s, P_r) \geq \frac{1}{2}\log\left(\frac{1+P_s}{1+h_s P_s}\right)$ and $R^{NF}(P_s, P_r) \geq 0$ which imply

$$(h_r - h_s)P_s \leq (1 - h_r) \tag{3.47}$$

$$h_r P_r \geq h_s - 1 \tag{3.48}$$

$$(1 - h_r)P_r \geq (h_s - 1)P_s \tag{3.49}$$

Condition (3.49) implies that $\min(h_s, h_r) \leq 1$. On the other hand, we cannot have $h_s \leq 1 < h_r$ since this contradicts (3.47). Now, we consider the three remaining possible cases of relative channel gains. We either have

$$h_r \leq h_s \leq 1 \tag{3.50}$$

which directly implies all the conditions (3.47)-(3.49) above, or we have

$$h_s < h_r \leq 1 \tag{3.51}$$

which directly implies both conditions (3.48) and (3.49), or we have

$$h_r < 1 \leq h_s \tag{3.52}$$

which directly implies condition (3.47). Thus, if $R^{NF}(P_s, P_r) \geq C^{GWT}(P_s)$, we either have condition (3.50) satisfied which is indeed condition (3.14), or we have conditions (3.47) and (3.51) both satisfied which is the same as (3.15), or we have conditions (3.48), (3.49), and (3.52) satisfied together which is the same as (3.16).

3.8.2 Proof of Theorem 3.2

We define

$$f^{CJ}(P_s, P_r) \triangleq \frac{(1+P_s+P_r)(1+h_r P_r)}{(1+h_s P_s+h_r P_r)(1+P_r)} \tag{3.53}$$

$$f_1^{NF}(P_s, P_r) \triangleq \frac{(1+P_s)(1+h_r P_r)}{(1+h_s P_s+h_r P_r)} \tag{3.54}$$

$$f_2^{NF}(P_s, P_r) \triangleq \frac{(1+P_s+P_r)}{(1+h_s P_s+h_r P_r)} \tag{3.55}$$

Hence,

$$R^{CJ}(P_s, P_r) = \frac{1}{2}\log\left(f^{CJ}(P_s, P_r)\right) \tag{3.56}$$

$$R^{NF}(P_s, P_r) = \min\left(\frac{1}{2}\log\left(f_1^{NF}(P_s, P_r)\right), \frac{1}{2}\log\left(f_2^{NF}(P_s, P_r)\right)\right) \tag{3.57}$$

We first consider the case where $h_r \geq 1$. Following Corollary 3.1, the NF strategy is not useful in this case, hence, in this case if $h_s < 1$ then $\hat{P}_s^{NF} = \bar{P}_s,\ \hat{P}_r^{NF} = 0$, otherwise $\hat{P}_s^{NF} = \bar{P}_s,\ \hat{P}_r^{NF} = 0$. This proves (3.20) and (3.31). On the other hand, if $1 \leq h_r \leq h_s$, then again following Corollary 3.1, both strategies are useless and we have $\hat{P}_s^{CJ} = \hat{P}_r^{CJ} = 0$ and $\hat{P}_s^{NF} = \hat{P}_r^{NF} = 0$. This proves (3.35)-(3.36). The remaining possible cases where $h_r \geq 1$ are $h_s < 1 \leq h_r$ and $1 \leq h_s < h_r$, i.e., cases 1-(a) and 2-(a) in Theorem 3.2. Suppose that $h_s < 1 \leq h_r$. The derivatives $\frac{\partial f^{CJ}(P_s,P_r)}{\partial P_s}$ and $\frac{\partial f^{CJ}(P_s,P_r)}{\partial P_r}$ are given by

$$\frac{\partial f^{CJ}(P_s, P_r)}{\partial P_s} = \frac{(1 - h_s + (h_r - h_s)P_r)(1 + h_r P_r)}{(1 + P_r)(1 + h_s P_s + h_r P_r)^2} \tag{3.58}$$

$$\frac{\partial f^{CJ}(P_s, P_r)}{\partial P_r} = \frac{(h_r(h_s - h_r)P_r^2 + 2h_r(h_s - 1)P_r + h_s\left(h_r(1 + P_s) - P_s\right) - 1)\, P_s}{(1 + P_r)^2(1 + h_s P_s + h_r P_r)^2} \tag{3.59}$$

We note that $\frac{\partial f^{CJ}(P_s,P_r)}{\partial P_s} > 0,\ \forall P_s, P_r$. Moreover, $\frac{\partial f^{CJ}(P_s,P_r)}{\partial P_r}$ has two zeros, one of them is at $P_r = P_r^*$ where P_r^* is given by (3.37) which turns out to be the unconstrained global maximum of $f^{CJ}(\bar{P}_s, P_r)$. Thus, the optimal power values $\hat{P}_s^{CJ}$ and $\hat{P}_r^{CJ}$ are given by (3.19). Suppose now that $1 \leq h_s < h_r$. If $\bar{P}_r \leq \frac{h_s - 1}{h_r - h_s}$, then from condition (3.13) in Theorem 3.1, we must have $\hat{P}_s^{CJ} = \hat{P}_r^{CJ} = 0$ since $h_s \geq 1$. Otherwise,

suppose that $\bar{P}_r > \frac{h_s-1}{h_r-h_s}$. First, note that for all P_s, $\frac{\partial f^{CJ}(P_s,P_r)}{\partial P_s} > 0$ if $P_r > \frac{h_s-1}{h_r-h_s}$. On the other hand, $\frac{\partial f^{CJ}(P_s,P_r)}{\partial P_r}$ has two zeros, one of them is the unconstrained global maximizer of $f^{CJ}(P_s, P_r)$ with respect to P_r for any given P_s. Moreover, for all P_s, this unconstrained global maximizer is greater than $\frac{h_s-1}{h_r-h_s}$. Noting that the value of such unconstrained global maximizer at $P_s = \bar{P}_s$ is P_r^*, we conclude that $\hat{P}_r^{CJ} = \min\left(\bar{P}_r, P_r^*\right)$ and $\hat{P}_s^{CJ} = \bar{P}_s$ which proves (3.30).

Next, we consider then case where $h_r < 1$. By Corollary 3.1, the CJ strategy is not useful in this case, hence, in this case if $h_s < 1$ then $\hat{P}_s^{CJ} = \bar{P}_s,\ \hat{P}_r^{CJ} = 0$, otherwise, $\hat{P}_s^{CJ} = \hat{P}_r^{CJ} = 0$. This proves (3.21), (3.25), and (3.32). The remaining possible cases where $h_r < 1$ are $h_s < h_r < 1$, $h_r \leq h_s < 1$, and $h_r < 1 \leq h_s$, i.e., cases 1-(b), 1-(c), and 2-(b) in Theorem 3.2. First, one can easily verify that

$$f_1^{NF}(P_s, P_r) \leq f_2^{NF}(P_s, P_r) \quad \text{if and only if} \quad P_s \leq \frac{1-h_r}{h_r} \tag{3.60}$$

We also have

$$\frac{\partial f_1^{NF}(P_s, P_r)}{\partial P_s} = \frac{(1-h_s+h_rP_r)}{(1+h_sP_s+h_rP_r)^2} \tag{3.61}$$

$$\frac{\partial f_1^{NF}(P_s, P_r)}{\partial P_r} = \frac{(h_sh_rP_s(1+P_s))}{(1+h_sP_s+h_rP_r)^2} \tag{3.62}$$

$$\frac{\partial f_2^{NF}(P_s, P_r)}{\partial P_s} = \frac{(1-h_s+(h_r-h_s)P_r)}{(1+h_sP_s+h_rP_r)^2} \tag{3.63}$$

$$\frac{\partial f_2^{NF}(P_s, P_r)}{\partial P_r} = \frac{(1-h_r+(h_s-h_r)P_s)}{(1+h_sP_s+h_rP_r)^2} \tag{3.64}$$

Now, suppose first that $h_s < h_r < 1$. We note that $\frac{\partial f_1^{NF}(P_s,P_r)}{\partial P_s}$ and $\frac{\partial f_2^{NF}(P_s,P_r)}{\partial P_s}$ are positive for all $P_s,\ P_r$. Hence, we must have $\hat{P}_s^{NF} = \bar{P}_s$. On the other hand,

$\frac{\partial f_1^{NF}(P_s,P_r)}{\partial P_r} > 0$ is positive for all $P_s,\ P_r$ while $\frac{\partial f_2^{NF}(P_s,P_r)}{\partial P_r} > 0$ if and only if $\bar{P}_s < \frac{1-h_r}{h_r-h_s}$. Hence, if $\bar{P}_s < \frac{1-h_r}{h_r-h_s}$, then $\hat{P}_r^{NF} = \bar{P}_r$. If $\bar{P}_s \geq \frac{1-h_r}{h_r-h_s}$, then from (3.60), (3.10), and by noting that $\frac{1-h_r}{h_r} > \frac{1-h_r}{h_s-h_r}$, we must have $\hat{P}_r^{NF} = 0$. This proves (3.22)-(3.24). Suppose now that $h_r \leq h_s < 1$. In this case, $\frac{\partial f_1^{NF}(P_s,P_r)}{\partial P_r}$ and $\frac{\partial f_2^{NF}(P_s,P_r)}{\partial P_r}$ are positive for all $P_s,\ P_r$. Thus, both $f_1^{NF}(P_s,P_r)$ and $f_2^{NF}(P_s,P_r)$ are increasing in P_r for any given value of P_s, hence their minimum is also increasing in P_r. Thus, $\hat{P}_r^{NF} = \bar{P}_r$ which proves (3.28). Now, if $\bar{P}_r < \frac{1-h_s}{h_s-h_r}$, then $\frac{\partial f_1^{NF}(P_s,P_r)}{\partial P_s}$ and $\frac{\partial f_2^{NF}(P_s,P_r)}{\partial P_s}$ are both positive. Hence, $\hat{P}_s^{NF} = \bar{P}_s$ which proves (3.26). If $\bar{P}_r \geq \frac{1-h_s}{h_s-h_r}$, then one can verify that $f_1^{NF}(P_s,\bar{P}_r)$ is increasing in P_s while $f_2^{NF}(P_s,P_r)$ is decreasing in P_s. Thus, the unconstrained global maximizer of their minimum is the point where they are equal, i.e., $P_s = \frac{1-h_r}{h_r}$. Hence, $\hat{P}_s^{NF} = \min\left(\bar{P}_s, \frac{1-h_r}{h_r}\right)$ which proves (3.27). Finally, suppose that $h_r < 1 \leq h_s$. If $\bar{P}_r \leq \frac{h_s-1}{h_r}$, then from condition (3.16) in Theorem 3.1, we must have $\hat{P}_s^{NF} = \hat{P}_r^{NF} = 0$ since $h_s \geq 1$, which proves (3.33). If $\bar{P}_r > \frac{h_s-1}{h_r}$, then again in this case $\frac{\partial f_1^{NF}(P_s,P_r)}{\partial P_r}$ and $\frac{\partial f_2^{NF}(P_s,P_r)}{\partial P_r}$ are positive for all P_s and P_r. Thus, arguing as above, we conclude that $\hat{P}_r^{NF} = \bar{P}_r$. On the other hand, $\frac{\partial f_1^{NF}(P_s,\bar{P}_r)}{\partial P_s} > 0$ while $\frac{\partial f_2^{NF}(P_s,\bar{P}_r)}{\partial P_s} < 0$. Thus, again by arguing as above, we must have $\hat{P}_s^{NF} = \min\left(\bar{P}_s, \frac{1-h_r}{h_r}\right)$ which proves (3.34).

Chapter 4

Deaf Cooperation for Secrecy with a Multi-Antenna Helper

4.1 Introduction

In the previous chapter, we studied the notion of deaf cooperation and its application in a single antenna relay-eavesdropper channel. In this chapter, we study the application of this notion in a relay-eavesdropper channel with a multi-antenna relay. Interestingly, this study reveals new ideas that were not valid in the single-antenna relay case. This, in turn, leads to useful deaf cooperation strategies that exploit the multiple spatial dimensions available in this channel to achieve higher secure rates.

Cooperative jamming strategies in multi-antenna relay networks were investigated in [23], [26], and [25]. In [23], a cooperative jamming strategy is proposed when the relay is equipped with multiple antennas. Under the constraint that the jamming signals must lie in the subspace orthogonal to the channel vector between the relay and the destination, [23] derives the antenna weights and transmit power of the source and the relay that maximize the achievable secrecy rate subject to a total transmit power constraint. In [26], two cooperative jamming strategies were proposed for a half-duplex two-hop multi-antenna relay system where the eavesdropper's channel state

information was unknown. In the first strategy, jamming signals are only transmitted by the nodes that are also transmitting data whereas in the second strategy, the inactive nodes are used as cooperative jammers. In [25], a cooperative jamming strategy is proposed for two-hop relay networks where the eavesdropper can wiretap the transmission in both hops. In the model in [25], the source, the destination, and the eavesdropper have multiple antennas, whereas the relay has a single antenna. Under similar constraint to the one in [23], namely, that the jamming signals lie in the subspace orthogonal to the channels to the legitimate nodes, closed-form solutions were derived for jamming beamformers that maximize the achievable secrecy rate, and the optimal power allocation was obtained using numerical methods.

In all the references above, the role of a helping node was restricted to one mode of deaf cooperation, namely, cooperative jamming. However, as discussed in Chapter 3, a helping node can also improve secrecy without listening to the source by using the noise forwarding strategy which was introduced in [29] for the single antenna relay-eavesdropper channel. In this chapter, we introduce new strategies based on both CJ and NF modes of deaf cooperation. In particular, we show that having multiple antennas allows us to decompose the relay-eavesdropper channel into two orthogonal components, one in the direction of the relay-destination channel (direct component) and the other in the orthogonal direction to the relay-destination channel (orthogonal component). Accordingly, we obtain the optimal deaf cooperation strategy (CJ or NF) along each channel component. It is intuitive that the orthogonal component should be used for cooperative jamming. However, it is not clear what strategy should be used along the direct component. It is not also clear how the relay should distribute

its power over these two orthogonal directions.

In this chapter, we fully answer these two questions. We give, in terms of the model fixed parameters, the necessary conditions for each of the CJ and the NF strategy to be useful when employed along the direct component, i.e., to improve over the optimal secrecy rate achievable when the transmission from the relay is constrained only to the orthogonal component. In particular, our results show that along the direct component of the channel either CJ is useful or NF is useful but not both. Moreover, there are some cases (which are described in this chapter) in which neither CJ nor NF is useful along the direct component. We fully characterize in the closed-form the optimal power allocation policy at the source and the relay for each of the two strategies and hence show how the relay should optimally distribute its power on the two channel components.

Next, we turn our attention to a certain class of the multi-antenna relay-eavesdropper channels, namely, the reversely degraded channel. We show that the strategy in which the relay jams with full power along the orthogonal component of the channel and transmits nothing in the direct component is optimal when the relay's average power goes to infinity. In fact, we even prove a stronger result. The secrecy rate achieved by this strategy approaches the capacity of the reversely degraded multi-antenna relay channel as the relay's average power increases, and hence this strategy achieves the optimal secure degrees of freedom (DoF) of the reversely degraded multi-antenna relay-eavesdropper channel. Interestingly, this strategy is clearly suboptimal in general for a bounded relay's power. Moreover, we show that this result is valid with probability 1 even when the relay-eavesdropper's channel state information is unavail-

able.

Finally, we present numerical examples to illustrate the gains in the achievable secrecy rates by our CJ and NF strategies when the relay is equipped with multiple antennas. Our simulation results clearly show that the rates achievable by our strategies are, in general, significantly larger than those achieved when no splitting of power between CJ and NF is allowed.

4.2 System Model

We consider the following communication scenario. A single-antenna source, s, sends a confidential message to a single-antenna destination, d, over an AWGN channel in the presence of an informed eavesdropper, e, that also has a single antenna. The communication also occurs in the presence of a helper node, r, that is equipped with K antennas, $K \geq 1$. The helper node r is assumed to be a deaf relay, i.e., it can only help improving the secrecy capacity of the GWT by transmitting interfering signals that are independent of the source message. In the literature, there are two proposed strategies for useful interference introduced by a helper node [34], [19], and [29]. In the first strategy, known as cooperative jamming, one allows r to help by transmitting pure Gaussian noise whereas in the second strategy, known as noise forwarding, r sends a dummy codeword from a codebook known to both the legitimate receiver and the eavesdropper. By proper scaling of the channel inputs and accordingly modifying the power constraints at the source and the helper nodes, without loss of generality, one can express the outputs of the GWT channel, with a multi-antenna deaf helper,

at the destination and the eavesdropper as

$$Y = X_s + \mathbf{h}_r^T \mathbf{X}_r + N \tag{4.1}$$

$$Z = \sqrt{g_s} X_s + \mathbf{g}_r^T \mathbf{X}_r + N' \tag{4.2}$$

where $\mathbf{h}_r \in \mathbb{R}^K$ is the vector of the channel coefficients between the helper r and the destination d, $g_s \in \mathbb{R}$, $\mathbf{g}_r \in \mathbb{R}^K$ are the channel coefficient scalar and the channel coefficient vector from the source s and the helper r to the eavesdropper, respectively, and, N and N' are standard Gaussian random variables that denote the noise at the destination and the eavesdropper, respectively, $X_s \in \mathbb{R}$, $\mathbf{X}_r \in \mathbb{R}^K$ are the channel input scalar and the channel input vector at the source s and the helper r, respectively. The channel inputs are subjected to the following average power constraints:

$$E[|X_s|^2] \leq \bar{P}_s, \qquad \text{and} \qquad E[\| \mathbf{X}_r \|^2] \leq \bar{P}_r \tag{4.3}$$

By possibly writing $\mathbf{g}_r$ as the direct sum $\mathbf{g}_r = \sqrt{\alpha}\mathbf{h}_r + \mathbf{u}_r$ where $\mathbf{h}_r^T \mathbf{u}_r = 0$, one can write $\mathbf{X}_r$ in (4.1)-(4.2) as the sum of two orthogonal components. That is, $\mathbf{X}_r = \mathbf{X}_{r0} + \mathbf{X}_{r1}$ where

$$\mathbf{X}_{r0} = X_{r0}\mathbf{h}_r = \frac{\mathbf{h}_r^T \mathbf{X}_r^T}{\gamma_{r0}} \mathbf{h}_r \tag{4.4}$$

$$\mathbf{X}_{r1} = X_{r1}\mathbf{u}_r = \frac{\mathbf{u}_r^T \mathbf{X}_r}{\gamma_{r1}} \mathbf{u}_r \tag{4.5}$$

where $\gamma_{r0} = \| \mathbf{h}_r \|^2$ and $\gamma_{r1} = \| \mathbf{u}_r \|^2$. Thus, we can write (4.1)-(4.2) as

$$Y = X_s + \mathbf{h}_r^T \mathbf{X}_{r0} + N \tag{4.6}$$

$$Z = \sqrt{g_s} X_s + \sqrt{\alpha} \mathbf{h}_r^T \mathbf{X}_{r0} + \mathbf{u}_r^T \mathbf{X}_{r1} + N' \tag{4.7}$$

Note that X_{r0} and X_{r1} in (4.4) and (4.5), respectively, can be arbitrarily correlated. Note also that it is of no loss of generality writing $\mathbf{g}_r = \sqrt{\alpha}\mathbf{h}_r + \mathbf{u}_r$ rather than $\mathbf{g}_r = \pm\sqrt{\alpha}\mathbf{h}_r + \mathbf{u}_r$ since the sign of $\sqrt{\alpha}$ is irrelevant when it comes to expressions of the achievable secrecy rates. We call $\mathbf{X}_{r0}$ the *direct* component of the helper's signal since it is in the same direction as the channel component $\mathbf{h}_r$ from the helper to the destination while we call $\mathbf{X}_{r1}$ the *orthogonal* component of the helper's signal since it is orthogonal to the channel component $\mathbf{h}_r$. We define $\mathbf{Q}_0 \triangleq E\left[\mathbf{X}_{r0}{\mathbf{X}_{r0}}^T\right]$ and $\mathbf{Q}_1 \triangleq E\left[\mathbf{X}_{r1}{\mathbf{X}_{r1}}^T\right]$. We also define $Q_{r0} \triangleq E\left[X_{r0}^2\right]$ and $Q_{r1} \triangleq E\left[X_{r1}^2\right]$. Hence, from (4.4)-(4.5), we have $\mathrm{tr}(\mathbf{Q}_0) = \frac{Q_{r0}}{\gamma_{r0}}$ and $\mathrm{tr}(\mathbf{Q}_1) = \frac{Q_{r1}}{\gamma_{r1}}$ where $\mathrm{tr}(\mathbf{A})$ denotes the trace of the square matrix $\mathbf{A}$. Hence, it is easy to see that the second constraint in (4.3) is equivalent to

$$\frac{Q_{r0}}{\gamma_{r0}} + \frac{Q_{r1}}{\gamma_{r1}} \leq \bar{P}_r \tag{4.8}$$

Now, we consider the possible signalling $\mathbf{X}_{r0}$ and $\mathbf{X}_{r1}$ across the two orthogonal directions using either one of the two signalling strategies CJ or NF in every direction. Clearly, it would not be beneficial if the NF strategy was used for the orthogonal component $\mathbf{X}_{r1}$ (i.e., in the direction $\mathbf{u}_r$ orthogonal to the helper-destination channel

$\mathbf{h}_r$) since the destination cannot decode $\mathbf{X}_{r1}$ as it lies in the null space of its observed signal space. On the other hand, if the CJ strategy is used for $\mathbf{X}_{r1}$, the eavesdropper is the only one who is possibly harmed by the resulting noise, not the destination. Hence, we assume that the helper will use the orthogonal component $\mathbf{X}_{r1}$ for CJ. That is, $\mathbf{X}_{r1}$ is given by (4.5) where X_{r1} is a Gaussian random variable with zero mean and variance Q_{r0}. We consequently distinguish between two possible strategies depending on whether the helper uses the direct component $\mathbf{X}_{r0}$ for CJ or NF. In both strategies, the channel input at the source X_s is a symbol of the codeword that represents the encoded confidential message. Such codeword is drawn from an i.i.d. Gaussian codebook, i.e., X_s is a Gaussian random variable with zero mean and variance P_s where $P_s \leq \bar{P}_s$. Also, in both strategies, the direct component of the channel input at the helper $\mathbf{X}_{r0}$ is given by (4.4) where X_{r0} is a Gaussian random variable with zero mean and variance Q_{r1}. Moreover, X_{r0} can be arbitrarily correlated to X_{r1} and hence X_{r1} can be written as

$$X_{r1} = \tilde{X}_{r1} + \rho X_{r0} \tag{4.9}$$

where $\tilde{X}_{r1}$ is a Gaussian random variable with zero mean and variance $\tilde{Q}_{r1}$ and is independent of X_{r0} and ρ is some real number. Hence, the constraint (4.8) becomes

$$\left(\frac{1}{\gamma_{r0}} + \frac{\rho^2}{\gamma_{r1}}\right) Q_{r0} + \frac{1}{\gamma_{r1}} \tilde{Q}_{r1} \leq \bar{P}_r \tag{4.10}$$

The difference between the two strategies comes from the origin of X_{r0}. In the

CJ strategy, X_{r0} is Gaussian random variable that plays the role of background noise at both the destination and the eavesdropper except for the fact that it is generated artificially. On the other hand, in the NF strategy, X_{r0} is a symbol of a dummy (context-free) codeword drawn from an i.i.d. Gaussian codebook that is assumed to be available at both the destination and the eavesdropper. Hence, we note that in the NF strategy, it is no loss of optimality to take the two orthogonal components X_{r0} and X_{r1} to be independent since the Gaussian noise X_{r1} in the orthogonal component must not reveal any information about the codeword symbol X_{r0}. Hence, in this case, we set ρ in (4.9) and (4.10) to zero. In the CJ strategy, this is not generally the case. However, finding the optimal power control policy, i.e., the optimal values of $P_s,\ Q_{r0},\ Q_{r1}$, and ρ that maximizes the achievable secrecy rate by the CJ strategy subject to the first constraint in (4.3) and constraint (4.10) becomes analytically intractable. Hence, to obtain closed-form expressions for the power control policy of the CJ strategy, we will take both X_{r0} and X_{r1} to be independent, i.e., we set $\rho = 0$. From this point on, we will assume that the two components X_{r0} and X_{r1} are independent.

If $\mathbf{X}_{r0}$ is used for CJ, the achievable secrecy rate, denoted as R^{CJ}, is given by

$$R^{CJ}(P_s, Q_{r0}, Q_{r1}) = \frac{1}{2}\log\left(\frac{(1+P_s+Q_{r0})(1+\alpha Q_{r0}+Q_{r1})}{(1+g_s P_s+\alpha Q_{r0}+Q_{r1})(1+Q_{r0})}\right) \tag{4.11}$$

On the other hand, if $\mathbf{X}_{r0}$ is used for NF, the achievable secrecy rate, denoted as

R^{NF}, is given by

$$R^{NF}(P_s, Q_{r0}, Q_{r1}) = \min \left\{ \frac{1}{2} \log \left(\frac{(1+P_s)(1+\alpha Q_{r0}+Q_{r1})}{1+g_s P_s+\alpha Q_{r0}+Q_{r1}} \right), \right. \\ \left. \frac{1}{2} \log \left(\frac{(1+P_s+Q_{r0})(1+Q_{r1})}{1+g_s P_s+\alpha Q_{r0}+Q_{r1}} \right) \right\} \tag{4.12}$$

where, in (4.11)-(4.12), P_s, Q_{r0}, and Q_{r1} satisfy the first constraint in (4.3) and constraint (4.8). For the sake of comparison, when there is no relay involved, the secrecy capacity of the original GWT channel [13] is given by

$$C^{GWT} = \left(\frac{1}{2} \log \left(\frac{1+\bar{P}_s}{1+g_s \bar{P}_s} \right) \right)^+ \tag{4.13}$$

where $(x)^+ = \max(0, x)$.

4.3 Maximizing the Secrecy Rates Achievable by Deaf Cooperation

4.3.1 The CJ strategy

We consider the following optimization problem:

$$\max_{P_s, Q_{r0}, Q_{r1}} R^{CJ}(P_s, Q_{r0}, Q_{r1}) \tag{4.14}$$

$$\text{s.t.} \quad 0 \le P_s \le \bar{P}_s \tag{4.15}$$

$$0 \le \frac{Q_{r0}}{\gamma_{r0}} + \frac{Q_{r1}}{\gamma_{r1}} \le \bar{P}_r \tag{4.16}$$

where $R^{CJ}(P_s, Q_{r0}, Q_{r1})$ is given by (4.11). Note that

$$\frac{\partial R^{CJ}(P_s, Q_{r0}, Q_{r1})}{\partial Q_{r1}} = \frac{g_s P_s}{(1+\alpha Q_{r0}+Q_{r1})(1+g_s P_s+\alpha Q_{r0}+Q_{r1})} > 0 \tag{4.17}$$

Thus, from (4.16), it is no loss of optimality to set

$$Q_{r1} = \gamma_{r1}\bar{P}_r - \frac{\gamma_{r1}}{\gamma_{r0}} Q_{r0} \tag{4.18}$$

in (4.14). Hence, the optimization problem given by (4.14)-(4.16) reduces to

$$\max_{P_s, Q_{r0}} R^{CJ}(P_s, Q_{r0}) \triangleq \frac{1}{2}\log\left(\frac{(1+P_s+Q_{r0})(1+\tilde{\alpha}Q_{r0})}{(1+\tilde{g}_s P_s+\tilde{\alpha}Q_{r0})(1+Q_{r0})}\right) \tag{4.19}$$

$$\text{s.t.} \qquad 0 \le P_s \le \bar{P}_s \tag{4.20}$$

$$0 \le Q_{r0} \le \gamma_{r0}\bar{P}_r \tag{4.21}$$

where

$$\tilde{\alpha} \triangleq \frac{\alpha - \frac{\gamma_{r1}}{\gamma_{r0}}}{1+\gamma_{r1}\bar{P}_r} \tag{4.22}$$

$$\tilde{g}_s \triangleq \frac{g_s}{1+\gamma_{r1}\bar{P}_r} \tag{4.23}$$

Again, for the sake of comparison, let R_o denote the optimal secrecy rate achievable when no transmission is carried out along the direct component of the channel, i.e., when the transmission is constrained only to the orthogonal component of the channel.

Hence, R_o is given by

$$R_o = \left(\frac{1}{2}\log\left(\frac{1+\bar{P}_s}{1+\tilde{g}_s\bar{P}_s}\right)\right)^+ \tag{4.24}$$

Note that the optimization problem (4.19)-(4.21) may look similar to the one considered in Chapter 3 for the single-antenna case. However, a notable difference is that $\tilde{\alpha}$ could be positive or negative depending on the relative values of γ_{r0} and γ_{r1}. In particular, $\tilde{\alpha} \geq 0$ if and only if $\gamma_{r0} \geq \gamma_{r1}$, i.e., the magnitude of the direct component is greater than that of the orthogonal component.

Let $(\hat{P}_s^{CJ}, \hat{Q}_{r0}^{CJ})$ be the maximizer of (4.19) subject to (4.20)-(4.21). Note that, once $\hat{Q}_{r0}^{CJ}$ is derived, the optimal value of Q_{r1}, denoted as $\hat{Q}_{r1}^{CJ}$, can be easily found from (4.18) where Q_{r0} is set to $\hat{Q}_{r0}^{CJ}$. The optimal covariance matrices $\hat{\mathbf{Q}}_{r0}^{CJ}$ and $\hat{\mathbf{Q}}_{r1}^{CJ}$ are given by $\hat{Q}_{r0}^{CJ}\frac{\mathbf{h}_r\mathbf{h}_r^T}{{\gamma_{r0}}^2}$ and $\hat{Q}_{r1}^{CJ}\frac{\mathbf{u}_r\mathbf{u}_r^T}{{\gamma_{r1}}^2}$. In the next theorem, we fully derive the optimal power control policy $(\hat{P}_s^{CJ}, \hat{Q}_{r0}^{CJ})$ for maximizing R^{CJ}.

Theorem 4.1 *The optimal policy $(\hat{P}_s^{CJ}, \hat{Q}_{r0}^{CJ})$ is given as follows:*

1. *If $\tilde{\alpha} \leq 0$: In this case, we have*

$$\hat{P}_s^{CJ} = \bar{P}_s, \quad \textit{if } \tilde{g}_s < 1 \tag{4.25}$$

$$\hat{P}_s^{CJ} = 0, \quad \textit{if } \tilde{g}_s \geq 1 \tag{4.26}$$

$$\hat{Q}_{r0}^{CJ} = 0 \tag{4.27}$$

2. *If $\tilde{\alpha} > 0$: We have four possibilities depending on the relative values of $\tilde{\alpha}$ and $\tilde{g}_s$:*

(a) If $\tilde{g}_s \geq \max(1, \tilde{\alpha})$, *then*

$$\hat{P}_s^{CJ} = 0 \tag{4.28}$$

$$\hat{Q}_{r0}^{CJ} = 0 \tag{4.29}$$

(b) If $\tilde{g}_s < 1 \leq \tilde{\alpha}$, *then*

$$\hat{P}_s^{CJ} = \bar{P}_s \tag{4.30}$$

$$\hat{Q}_{r0}^{CJ} = \left(\min\left(\bar{P}_r, Q_{r0}^{(1)}\right)\right)^+ \tag{4.31}$$

(c) If $1 \leq \tilde{g}_s < \tilde{\alpha}$, *then*

$$\hat{P}_s^{CJ} = 0,\ \hat{Q}_{r0}^{CJ} = 0, \quad \text{if } \bar{P}_r \leq \frac{\tilde{g}_s - 1}{\tilde{\alpha} - \tilde{g}_s} \tag{4.32}$$

$$\hat{P}_s^{CJ} = \bar{P}_s,\ \hat{Q}_{r0}^{CJ} = \min\left(\bar{P}_r, Q_{r0}^{(1)}\right), \quad \text{if } \bar{P}_r > \frac{\tilde{g}_s - 1}{\tilde{\alpha} - \tilde{g}_s} \tag{4.33}$$

(d) If $\max(\tilde{g}_s, \tilde{\alpha}) < 1$, *then*

$$\hat{P}_s^{CJ} = \bar{P}_s \tag{4.34}$$

$$\hat{Q}_{r0}^{CJ} = 0 \tag{4.35}$$

where

$$Q_{r0}^{(1)} = \frac{\sqrt{\left(\tilde{g}_s\left(\tilde{\alpha} - \tilde{g}_s\right)\bar{P}_s + \tilde{g}_s\left(\tilde{\alpha} - 1\right)\right)\left(\tilde{\alpha} - 1\right)\tilde{\alpha}} - \tilde{\alpha}(1 - \tilde{g}_s)}{\tilde{\alpha}\left(\tilde{\alpha} - \tilde{g}_s\right)} \tag{4.36}$$

and, for $x \in \mathbb{R}$, $(x)^+$ *is defined as* $\max(0, x)$.

Proof: First, observe that $\frac{\partial R^{CJ}(P_s, Q_{r0})}{\partial Q_{r0}}$ is given by

$$\frac{\partial R^{CJ}(P_s, Q_{r0})}{\partial Q_{r0}} = \frac{\tilde{\alpha}(\tilde{g}_s - \tilde{\alpha}){Q_{r0}}^2 + 2Q_{r0}(\tilde{g}_s - 1)\tilde{\alpha} + \tilde{g}_s(\tilde{\alpha} - 1)P_s + \tilde{g}_s\tilde{\alpha} - 1}{(1 + Q_{r0})(1 + \tilde{g}_s P_s + \tilde{\alpha} Q_{r0})(1 + P_s + Q_{r0})(1 + \tilde{\alpha} Q_{r0})} P_s \quad (4.37)$$

It is easy to see that if $\tilde{\alpha} \leq 0$, then $\frac{\partial R^{CJ}(P_s, Q_{r0})}{\partial Q_{r0}} < 0 \ \forall P_s, Q_{r0}$. Hence, $\hat{Q}_{r0}^{CJ} = 0$ and case 1 follows. On the other hand, case 2 of this theorem is exactly the same as the case of single antenna relay given by Theorem 3.2. □

Theorem 4.1 tells us that CJ along the direct component can be useful only when the magnitude of the direct component of $\mathbf{g}_r$ is larger than that of the orthogonal component, i.e., when $\tilde{\alpha} > 0$. Otherwise, the optimal power allocation strategy at the multiple antenna deaf helper would be to jam only along the orthogonal component and transmit nothing along the direct component.

4.3.2 The NF strategy

Here, we consider the following optimization problem

$$\max_{P_s, Q_{r0}, Q_{r1}} R^{NF}(P_s, Q_{r0}, Q_{r1}) \quad (4.38)$$

$$\text{s.t.} \quad 0 \leq P_s \leq \bar{P}_s \quad (4.39)$$

$$0 \leq \frac{Q_{r0}}{\gamma_{r0}} + \frac{Q_{r1}}{\gamma_{r1}} \leq \bar{P}_r \quad (4.40)$$

where $R^{NF}(P_s, Q_{r0}, Q_{r1})$ is given by (4.12). We define

$$R_1^{NF}(P_s, Q_{r0}, Q_{r1}) = \frac{1}{2}\log\left(\frac{(1+P_s)(1+\alpha Q_{r0}+Q_{r1})}{1+g_sP_s+\alpha Q_{r0}+Q_{r1}}\right) \tag{4.41}$$

$$R_2^{NF}(P_s, Q_{r0}, Q_{r1}) = \frac{1}{2}\log\left(\frac{(1+P_s+Q_{r0})(1+Q_{r1})}{1+g_sP_s+\alpha Q_{r0}+Q_{r1}}\right) \tag{4.42}$$

Hence,

$$R^{NF}(P_s, Q_{r0}, Q_{r1}) = \min\left(R_1^{NF}(P_s, Q_{r0}, Q_{r1}), R_2^{NF}(P_s, Q_{r0}, Q_{r1})\right) \tag{4.43}$$

Note that

$$\frac{\partial R_1^{NF}(P_s, Q_{r0}, Q_{r1})}{\partial Q_{r1}} = \frac{g_sP_s}{(1+\alpha Q_{r0}+Q_{r1})(1+g_sP_s+\alpha Q_{r0}+Q_{r1})} > 0 \tag{4.44}$$

$$\frac{\partial R_2^{NF}(P_s, Q_{r0}, Q_{r1})}{\partial Q_{r1}} = \frac{g_sP_s+\alpha Q_{r0}}{(1+Q_{r1})(1+g_sP_s+\alpha Q_{r0}+Q_{r1})} > 0 \tag{4.45}$$

It follows that $\frac{\partial R^{NF}(P_s,Q_{r0},Q_{r1})}{\partial Q_{r1}} > 0$. Thus, from (4.40), again as in (4.18), it is no loss of optimality to set $Q_{r1} = \gamma_{r1}\bar{P}_r - \frac{\gamma_{r1}}{\gamma_{r0}}Q_{r0}$ in (4.38). Hence, the optimization problem given by (4.38)-(4.40) reduces to

$$\max_{P_s,Q_{r0}} R^{NF}(P_s, Q_{r0}) \triangleq \min\left(R_1^{NF}(P_s, Q_{r0}), R_2^{NF}(P_s, Q_{r0})\right) \tag{4.46}$$

$$\text{s.t.} \qquad 0 \le P_s \le \bar{P}_s \tag{4.47}$$

$$0 \le Q_{r0} \le \gamma_{r0}\bar{P}_r \tag{4.48}$$

where

$$R_1^{NF}(P_s, Q_{r0}) = \frac{1}{2}\log\left(\frac{(1+P_s)(1+\tilde{\alpha}Q_{r0})}{1+\tilde{g}_s P_s + \tilde{\alpha}Q_{r0}}\right) \tag{4.49}$$

$$R_2^{NF}(P_s, Q_{r0}) = \frac{1}{2}\log\left(\frac{(1+P_s+Q_{r0})(1-\beta Q_{r0})}{1+\tilde{g}_s P_s + \tilde{\alpha}Q_{r0}}\right) \tag{4.50}$$

where $\tilde{\alpha},\ \tilde{g}_s$ are as defined in (4.22)-(4.23) above, and

$$\beta \triangleq \frac{\gamma_{r1}}{\gamma_{r0} + \gamma_{r0}\gamma_{r1}\bar{P}_r} \tag{4.51}$$

As in the previous subsection, note that the optimal secrecy rate R_o achievable when the transmission at the relay is constrained to the orthogonal channel component is given by (4.24).

There are two main differences between the achievable secrecy rate given by (4.46) and the achievable secrecy rate by the NF strategy when the helper has a single antenna. The first difference is, as stated above, $\tilde{\alpha}$ can take a positive or negative value depending on the relative values of γ_{r0} and γ_{r1}, i.e., the magnitudes of the direct and orthogonal components of the helper-eavesdropper channel. The second difference is the factor $(1-\beta Q_{r0})$ in R_2^{NF} given by (4.50).

Let $(\hat{P}_s^{NF}, \hat{Q}_{r0}^{NF})$ be the maximizer of (4.46) subject to (4.47)-(4.48). As discussed above, once $\hat{Q}_{r0}^{NF}$ is derived, the optimal value of Q_{r1}, denoted as $\hat{Q}_{r1}^{NF}$, can be easily found from (4.18) where Q_{r0} is set to $\hat{Q}_{r0}^{NF}$. The optimal covariance matrices $\hat{\mathbf{Q}}_{r0}^{NF}$ and $\hat{\mathbf{Q}}_{r1}^{NF}$ are given by $\hat{Q}_{r0}^{NF}\frac{\mathbf{h}_r\mathbf{h}_r^T}{{\gamma_{r0}}^2}$ and $\hat{Q}_{r1}^{NF}\frac{\mathbf{u}_r\mathbf{u}_r^T}{{\gamma_{r1}}^2}$. Before we give the optimal power control policy $(\hat{P}_s^{NF}, \hat{Q}_{r0}^{NF})$, we first give the following useful lemmas.

Lemma 4.1 *A necessary condition for the NF strategy to be useful along the direct component of the channel is to have* $\tilde{\alpha} \geq 0$ *and* $\tilde{\alpha} + \beta < 1$.

Proof: First, to show that $\tilde{\alpha} \geq 0$ is necessary, suppose that $\tilde{\alpha} < 0$, one can easily verify that $\frac{\partial R_1^{NF}(P_s, Q_{r0})}{\partial Q_{r0}} \leq 0$ for all $Q_{r0} \geq 0$ which implies that achievable rate is upper bounded by $\left(R_1^{NF}(\bar{P}_s, 0)\right)^+ = R_o$ which is indeed the secrecy rate achievable when the transmission at the relay is constrained to the orthogonal component of the channel. On the other hand, suppose that $\tilde{\alpha} + \beta > 1$. Now, if $\tilde{g}_s < 1$, then we clearly have $R_2^{NF}(P_s, Q_{r0}) \leq \frac{1}{2}\log\left(\frac{1+P_s}{1+\tilde{g}_s P_s}\right) \leq \frac{1}{2}\log\left(\frac{1+\bar{P}_s}{1+\tilde{g}_s \bar{P}_s}\right)$ for all $P_s,\ Q_{r0} \geq 0$. If $\tilde{g}_s > 1$, then $R_2^{NF}(P_s, Q_{r0}) \leq 0$ for all $P_s,\ Q_{r0} \geq 0$. Thus, we have $R^{NF}(P_s, Q_{r0}) \leq R_o$ for all $P_s,\ Q_{r0} \geq 0$. $\square$

Lemma 4.2 *Let* $\phi \triangleq \tilde{g}_s \beta {P_s}^2 + (\tilde{\alpha} + \beta - \tilde{g}_s) P_s - (1 - \tilde{\alpha} - \beta)$ *and* $\psi \triangleq (\tilde{\alpha} + \beta - \tilde{g}_s)^2 - 4\tilde{g}_s\beta\,(\tilde{\alpha} + \beta - 1)$. *If the conditions of Lemma 1 hold, i.e., if*

$$\tilde{\alpha} \geq 0,\ \tilde{\alpha} + \beta < 1 \tag{4.52}$$

then, for any fixed P_s *where*

$$0 \leq P_s \leq P_s^* \triangleq \frac{\sqrt{\psi} - (\tilde{\alpha} + \beta - \tilde{g}_s)}{2\tilde{g}_s\beta}, \tag{4.53}$$

we have $\frac{\partial R_2^{NF}(P_s, Q_{r0})}{\partial Q_{r0}} \geq 0$ *if and only if*

$$0 \leq Q_{r0} \leq Q_{r0}^*(P_s) \triangleq \frac{\sqrt{\beta^2(1 + \tilde{g}_s P_s)^2 - \tilde{\alpha}\beta\phi} - \beta(1 + \tilde{g}_s P_s)}{\tilde{\alpha}\beta} \tag{4.54}$$

Consequently, if conditions (4.52)-(4.53) hold, then

$$R_2^{NF}(P_s, Q_{r0}) \leq R_2^{NF}\left(P_s, Q_{r0}^*(P_s)\right) \tag{4.55}$$

Proof: Define $f_2^{NF}(P_s, Q_{r0})$ as the numerator of $\frac{\partial R_2^{NF}(P_s,Q_{r0})}{\partial Q_{r0}}$. Note that the sign of $\frac{\partial R_2^{NF}(P_s,Q_{r0})}{\partial Q_{r0}}$ is the same as the sign of $f_2^{NF}(P_s, Q_{r0})$ for all $P_s, Q_{r0} \geq 0$. It is easy to verify that $f_2^{NF}(P_s, Q_{r0})$ is given by

$$f_2^{NF}(P_s, Q_{r0}) = -\tilde{\alpha}\beta {Q_{r0}}^2 - 2\beta(1 + \tilde{g}_s P_s)Q_{r0} - \phi \tag{4.56}$$

Fix P_s and let $q_1(P_s), q_2(P_s)$ denote the two roots of $f_2^{NF}(P_s, Q_{r0})$. Since $\tilde{\alpha} \geq 0$, then $\frac{\partial R_2^{NF}(P_s,Q_{r0})}{\partial Q_{r0}} \geq 0$ if and only if $Q_{r0} \in [q_1(P_s), q_2(P_s)]$. However, it is not hard to see that $q_1(P_s) < 0$ for any $P_s > 0$. Thus, for any $P_s, Q_{r0} \geq 0$, we have $\frac{\partial R_2^{NF}(P_s,Q_{r0})}{\partial Q_{r0}} \geq 0$ if and only if $Q_{r0} \in [0, q_2(P_s)]$ where $q_2(P_s) = Q_{r0}^*(P_s)$ where Q_{r0}^* is given in (4.54). Thus, it remains to show that $Q_{r0}^*(P_s) \geq 0$ (and hence $[0, Q_{r0}^*(P_s)]$ is not empty) whenever $0 \leq P_s \leq P_s^*$ where P_s^* is given in (4.53). We note that $Q_{r0}^*(P_s) \geq 0$ if and only if $\phi \leq 0$. Since ϕ is quadratic in P_s, it is not hard to see that $\phi \leq 0$ whenever P_s lies between the two roots of ϕ. However, one of the roots is negative and the other is positive due to the fact that $\tilde{\alpha} + \beta < 1$. Indeed, the positive root is P_s^*. Hence, $\phi < 0$ and consequently $Q_{r0}^*(P_s) > 0$ whenever $0 \leq P_s \leq P_s^*$. $\square$

In the next theorem, we fully derive the optimal power policy $(\hat{P}_s^{NF}, \hat{Q}_{r0}^{NF})$ for maximizing R^{NF}. A proof of this theorem is given in the Appendix.

Theorem 4.2 *Let $\tilde{Q}_{r0}$ be the value of Q_{r0} such that $R_1^{NF}(\bar{P}_s, Q_{r0}) = R_2^{NF}(\bar{P}_s, Q_{r0})$,*

i.e.,

$$\tilde{Q}_{r0} = \left(\frac{1 - (\tilde{\alpha} + \beta)\left(1 + \bar{P}_s\right)}{\beta} \right)^+ \tag{4.57}$$

Let Q^*_{r0} be as defined in (4.54). The optimal policy $(\hat{P}^{NF}_s, \hat{Q}^{NF}_{r0})$ is given as follows:

1. *If $\tilde{\alpha} \leq 0$: In this case, we have*

$$\hat{P}^{NF}_s = \bar{P}_s, \quad \textit{if } \tilde{g}_s < 1 \tag{4.58}$$

$$\hat{P}^{NF}_s = 0, \quad \textit{if } \tilde{g}_s \geq 1 \tag{4.59}$$

$$\hat{Q}^{NF}_{r0} = 0 \tag{4.60}$$

2. *If $\tilde{\alpha} > 0$: We have the following four possibilities depending on the values of $\tilde{\alpha}, \tilde{g}_s$, and β:*

   (a) *If $\tilde{\alpha} + \beta \geq 1$, then*

$$\hat{P}^{NF}_s = \bar{P}_s, \quad \textit{if } \tilde{g}_s < 1 \tag{4.61}$$

$$\hat{P}^{NF}_s = 0, \quad \textit{if } \tilde{g}_s \geq 1 \tag{4.62}$$

$$\hat{Q}^{NF}_{r0} = 0 \tag{4.63}$$

   (b) *If $\tilde{g}_s \leq \tilde{\alpha} < 1 - \beta$, then*

$$\hat{P}^{NF}_s = \bar{P}_s \tag{4.64}$$

$$\hat{Q}_{r0}^{NF} = \begin{cases} \min\left(\gamma_{r0}\bar{P}_r,\ \max\left(\tilde{Q}_{r0},\ Q_{r0}^{*}\left(\bar{P}_s\right)\right)\right), & \text{if } \bar{P}_s \le P_s^{*} \\ 0, & \text{if } \bar{P}_s > P_s^{*} \end{cases} \tag{4.65}$$

(c) If $\tilde{\alpha} < \min\left(1-\beta,\ \tilde{g}_s\right) < 1$, *then*

i. If $\gamma_{r0}\bar{P}_r \le \frac{1-\tilde{g}_s}{\tilde{g}_s-\tilde{\alpha}}$, *then*

$$\hat{P}_s^{NF} = \bar{P}_s \tag{4.66}$$

$$\hat{Q}_{r0}^{NF} = \begin{cases} \min\left(\gamma_{r0}\bar{P}_r,\ \max\left(\tilde{Q}_{r0},\ Q_{r0}^{*}\left(\bar{P}_s\right)\right)\right), & \text{if } \bar{P}_s \le P_s^{*} \\ 0, & \text{if } \bar{P}_s > P_s^{*} \end{cases} \tag{4.67}$$

ii. If $\gamma_{r0}\bar{P}_r > \frac{1-\tilde{g}_s}{\tilde{g}_s-\tilde{\alpha}}$, $\left[\frac{1-\tilde{g}_s}{\tilde{g}_s-\tilde{\alpha}}, \gamma_{r0}\bar{P}_r\right] \cap \left[\frac{1-(\tilde{\alpha}+\beta)(1+\bar{P}_s)}{\beta}, \frac{1-(\tilde{\alpha}+\beta)}{\beta}\right] \neq \emptyset$, *then*

$$(\hat{P}_s^{NF}, \hat{Q}_{r0}^{NF}) = \begin{cases} ({P_s}^{(a)}, {Q_{r0}}^{(a)}), \\ \qquad \text{if } R^{NF}\left({P_s}^{(a)}, {Q_{r0}}^{(a)}\right) \ge R^{NF}\left({P_s}^{(b)}, {Q_{r0}}^{(b)}\right) \\ ({P_s}^{(b)}, {Q_{r0}}^{(b)}), \\ \qquad \text{if } R^{NF}\left({P_s}^{(a)}, {Q_{r0}}^{(a)}\right) < R^{NF}\left({P_s}^{(b)}, {Q_{r0}}^{(b)}\right) \end{cases} \tag{4.68}$$

where ${P_s}^{(a)}$, ${Q_{r0}}^{(a)}$ *are the optimal values* $\hat{P}_s^{NF}$, $\hat{Q}_{r0}^{NF}$, *respectively, of*

case 2(c-ii) above, i.e.,

$$P_s{}^{(a)} = \bar{P}_s \tag{4.69}$$

$$Q_{r0}{}^{(a)} = \begin{cases} \min\left(\frac{1-\tilde{g}_s}{\tilde{g}_s-\tilde{\alpha}},\ \max\left(\tilde{Q}_{r0},\ Q^*_{r0}\left(\bar{P}_s\right)\right)\right), & \text{if } \bar{P}_s \le P^*_s \\ 0, & \text{if } \bar{P}_s > P^*_s \end{cases} \tag{4.70}$$

and

$$P_s{}^{(b)} = \frac{1-\beta Q_{r0}{}^{(b)}}{\tilde{\alpha}+\beta} - 1 \tag{4.71}$$

$$Q_{r0}{}^{(b)} = \min\left(Q^{(2)}_{r0}, \gamma_{r0}\bar{P}_r, \frac{1-(\tilde{\alpha}+\beta)}{\beta}\right) \tag{4.72}$$

where

$$Q^{(2)}_{r0} = \frac{\tilde{g}_s\left(1-(\tilde{\alpha}+\beta)+\sqrt{\tilde{\alpha}\beta}-\sqrt{(\tilde{\alpha}+\beta)\left((\tilde{\alpha}+\beta)-\tilde{g}_s\beta\right)\tilde{g}_s\left(1-\tilde{\alpha}\right)}\right)}{\sqrt{\tilde{\alpha}\beta}\left(\tilde{g}_s\beta-\tilde{\alpha}\left(\tilde{\alpha}+\beta\right)\right)} \tag{4.73}$$

iii. If $\gamma_{r0}\bar{P}_r > \frac{1-\tilde{g}_s}{\tilde{g}_s-\tilde{\alpha}} > \frac{1-(\tilde{\alpha}+\beta)}{\beta}$*, then*

$$\hat{P}^{NF}_s = \bar{P}_s \tag{4.74}$$

$$\hat{Q}^{NF}_{r0} = \begin{cases} \min\left(\frac{1-\tilde{g}_s}{\tilde{g}_s-\tilde{\alpha}},\ \max\left(\tilde{Q}_{r0},\ Q^*_{r0}\left(\bar{P}_s\right)\right)\right), & \text{if } \bar{P}_s \le P^*_s \\ 0, & \text{if } \bar{P}_s > P^*_s \end{cases} \tag{4.75}$$

iv. If $\frac{1-(\tilde{\alpha}+\beta)(1+\bar{P}_s)}{\beta} > \gamma_{r0}\bar{P}_r > \frac{1-\tilde{g}_s}{\tilde{g}_s-\tilde{\alpha}}$, *then*

$$\hat{P}_s^{NF} = \bar{P}_s \tag{4.76}$$

$$\hat{Q}_{r0}^{NF} = \gamma_{r0}\bar{P}_r \tag{4.77}$$

(d) If $\tilde{\alpha} < 1-\beta \leq 1 \leq \tilde{g}_s$, *then*

i. If $\gamma_{r0}\bar{P}_r \leq \frac{\tilde{g}_s-1}{\tilde{\alpha}}$, *then*

$$\hat{P}_s^{NF} = \hat{Q}_{r0}^{NF} = 0 \tag{4.78}$$

ii. If $\gamma_{r0}\bar{P}_r > \frac{\tilde{g}_s-1}{\tilde{\alpha}}$, $\left[\frac{\tilde{g}_s-1}{\tilde{\alpha}}, \gamma_{r0}\bar{P}_r\right] \cap \left[\frac{1-(\tilde{\alpha}+\beta)(1+\bar{P}_s)}{\beta}, \frac{1-(\tilde{\alpha}+\beta)}{\beta}\right] \neq \emptyset$, *then*

$$\hat{P}_s^{NF} = \frac{1-\beta\hat{Q}_{r0}^{NF}}{\tilde{\alpha}+\beta} - 1 \tag{4.79}$$

$$\hat{Q}_{r0}^{NF} = \min\left(Q_{r0}^{(2)}, \gamma_{r0}\bar{P}_r, \frac{1-(\tilde{\alpha}+\beta)}{\beta}\right) \tag{4.80}$$

where $Q_{r0}^{(2)}$ *is given by (4.73).*

iii. If $\gamma_{r0}\bar{P}_r > \frac{\tilde{g}_s-1}{\tilde{\alpha}} > \frac{1-(\tilde{\alpha}+\beta)}{\beta}$, *then*

$$\hat{P}_s^{NF} = \hat{Q}_{r0}^{NF} = 0 \tag{4.81}$$

iv. If $\frac{1-(\tilde{\alpha}+\beta)(1+\bar{P}_s)}{\beta} > \gamma_{r0}\bar{P}_r > \frac{\tilde{g}_s-1}{\tilde{\alpha}}$, *then*

$$\hat{P}_s^{NF} = \bar{P}_s \tag{4.82}$$

$$\hat{Q}_{r0}^{NF} = \gamma_{r0}\bar{P}_r \tag{4.83}$$

4.3.3 CJ versus NF

In the next corollary, we use the results of the above two theorems to compare the two strategies. In particular, we show in terms of the parameters of the deaf cooperation model when it is better to use CJ than NF for transmission along the direct component $\mathbf{X}_{r0}$ and vice versa. We also give the conditions for which both CJ and NF along the direct component are useless.

Corollary 4.1 *Let* $\tilde{\alpha}$, $\tilde{g}_s$, *and* β *be as defined in (4.22), (4.23), and (4.51), respectively. For the CJ along the direct channel component to be useful, it is necessary to have* $\tilde{\alpha} > \max(1, \tilde{g}_s)$. *Whereas, for the NF along the direct channel component to be useful, it is necessary to have* $0 < \tilde{\alpha} < 1 - \beta$. *In other words,*

$$\textit{If} \quad R^{CJ}\left(\hat{P}_s^{CJ}, \hat{Q}_{r0}^{CJ}\right) > R_o \quad \textit{then} \quad \tilde{\alpha} > \max(1, \tilde{g}_s) \tag{4.84}$$

$$\textit{If} \quad R^{NF}\left(\hat{P}_s^{NF}, \hat{Q}_{r0}^{NF}\right) > R_o \quad \textit{then} \quad 0 < \tilde{\alpha} < 1 - \beta \tag{4.85}$$

Hence, if

$$\tilde{\alpha} \in [1 - \beta, \max(1, \tilde{g}_s)] \cup (-\infty, 0]\,, \tag{4.86}$$

neither CJ nor NF along the direct component is useful, i.e., $\hat{Q}_{r0}^{CJ} = \hat{Q}_{r0}^{NF} = 0$. *Moreover, if, in addition to (4.86),* $\tilde{g}_s < 1$, *then* $\hat{P}_s^{CJ} = \hat{P}_s^{NF} = \bar{P}_s$ *and* $\hat{Q}_{r1} = \gamma_{r1}\bar{P}_r$, *i.e., the optimal power strategy at the relay in this case is to jam with full power along the orthogonal component and transmit nothing along the direct component. Whereas, if, in addition to (4.86),* $\tilde{g}_s \geq 1$, *then* $\hat{P}_s^{CJ} = \hat{P}_s^{NF} = \hat{Q}_{r1} = 0$, *i.e., no transmission occurs at all and hence the achievable secrecy rate is zero in this case.*

4.4 The Reversely Degraded Relay-Eavesdropper Channel with a Multi-Antenna Relay

In this section, we consider a similar model to the one described in Section 4.2 except for two differences. First, we assume that the relay receives a vector $\mathbf{Y}_r$ which is a noisy version of the source transmission and hence the relay can use this observation in one way or another to help increase the achievable secrecy rate. Second, we assume that, given the relay's channel input $\mathbf{X}_r$, the relay's observation is a degraded version of the destination's observation. In particular, we consider the system where the destination's and the eavesdropper's observations are given by (4.6) and (4.7), respectively. The relay's observation, $\mathbf{Y}_r \in \mathbb{R}^K$, is given by

$$\mathbf{Y}_r = \boldsymbol{\eta} Y + \boldsymbol{\Theta}\mathbf{X}_r + \mathbf{N}_r \tag{4.87}$$

where $\boldsymbol{\eta} \in \mathbb{R}^K$ is the vector of equivalent channel coefficients from the destination's observation Y to the relay's observation $\mathbf{Y}_r$, $\boldsymbol{\Theta} \in \mathbb{R}^{K\times K}$ is the matrix of channel

coefficients from the relay's input $\mathbf{X}_r$ to the relay's output $\mathbf{Y}_r$, and $\mathbf{N}_r \in \mathbb{R}^K$ is AWGN vector of zero mean and identity covariance matrix and is independent of $(X_s,\ \mathbf{X}_r,\ N,\ N')$. Accordingly, we have the following Markov chain $X_s \to (Y, \mathbf{X}_r) \to \mathbf{Y}_r$. We further assume that in (4.7) $\mathbf{u}_r \neq \mathbf{0}$, i.e., given the source's input X_s, neither the destination's observation Y nor the eavesdropper's observation Z is a degraded version of one another.

In the following theorem, we show that for the channel described in this section, using only the CJ strategy over the orthogonal component $\mathbf{X}_{r1}$ (no signaling over the direct component $\mathbf{X}_{r0}$) yields a secrecy rate that approaches the secrecy capacity of this channel as $\bar{P}_r \to \infty$. In other words, we show that for high SNR over the relay-destination and the relay-eavesdropper channel, the secrecy rate achieved by CJ over the orthogonal component of the relay-eavesdropper channel (and no signaling over the direct component) approaches the secrecy capacity of the channel described above, i.e., this strategy achieves the optimal secure DoF of such channel.

Theorem 4.3 *Let $C_s(\bar{P}_r)$ be the secrecy capacity of the reversely degraded relay-eavesdropper channel given by (4.6), (4.7), and (4.87) for a given value of the relay's average power constraint $\bar{P}_r$. Suppose that $\mathbf{u}_r \neq \mathbf{0}$. Let $R_o(\bar{P}_r)$ be R_o of (4.24) written as a function of $\bar{P}_r$, i.e., $R_o(\bar{P}_r)$ denote the secrecy rate achievable by using the total source's power $\bar{P}_s$ for information transmission and using the total relay's power $\bar{P}_r$ for CJ along the orthogonal component of the relay-eavesdropper channel (i.e., setting $P_s = \bar{P}_s$, $Q_{r1} = \gamma_{r1}\bar{P}_r$ and $Q_{r0} = 0$ in any one of the two strategies described in*

Section 4.3). Then, for every $\varepsilon > 0$, there is a sufficiently large value $\bar{P}_r$ such that

$$R_o(\bar{P}_r) > C_s(\bar{P}_r) - \varepsilon \tag{4.88}$$

In particular,

$$\lim_{\bar{P}_r \to \infty} R_o(\bar{P}_r) = C^G \tag{4.89}$$

where $C^G = \frac{1}{2}\log\left(1 + \bar{P}_s\right)$ is the capacity of the Gaussian channel between the source and the destination when there is no eavesdropper in the system.

In Theorem 4.3, one should note that C^G is indeed an upper bound on the secrecy capacity of the reversely degraded relay-eavesdropper channel. This is due to the fact that the relay in this case cannot increase the reliable information rate from the source to the destination and hence the capacity of the relay channel with no secrecy constraints is indeed C^G. Therefore, C^G is an upper bound on the secrecy capacity of the reversely degraded relay-eavesdropper channel. It is easy to see that

$$R_o(\bar{P}_r) = \frac{1}{2}\log\left(1 + \bar{P}_s\right) - \frac{1}{2}\log\left(\frac{1 + \gamma_{r1}\bar{P}_r + g_s\bar{P}_s}{1 + \gamma_{r1}\bar{P}_r}\right) \tag{4.90}$$

Hence, (4.89) follows. This indeed proves (4.88).

We can even make a stronger statement than the one Theorem 4.3. In fact, if the relay-eavesdropper channel $\mathbf{g}_r$ is unknown at all the nodes (except possibly the eavesdropper itself), we let the relay choose at random a signaling direction

for jamming in the subspace orthogonal to $\mathbf{h}_r$, i.e., chooses a unit vector $\mathbf{s}_r \in \mathbb{R}^K$ at random and chooses the covariance matrix $\mathbf{Q}$ of $\mathbf{X}_r$ as $\mathbf{s}_r\mathbf{s}_r^T\bar{P}_r$. In this case, conditioned on some choice of $\mathbf{s}_r$, the achievable secrecy rate by this strategy, as a function in $\bar{P}_r$, is given by

$$R_o(\bar{P}_r) = \frac{1}{2}\log\left(1+\bar{P}_s\right) - \frac{1}{2}\log\left(\frac{1+\mathbf{g}_r^T\mathbf{s}_r\bar{P}_r + g_s\bar{P}_s}{1+\mathbf{g}_r^T\mathbf{s}_r\bar{P}_r}\right) \tag{4.91}$$

It is clear that $\mathbf{g}_r^T\mathbf{s}_r \neq 0$ with probability 1. Hence, $R_o(\bar{P}_r) \to C^G$ almost surely as $\bar{P}_r \to \infty$. Thus, even if the relay-eavesdropper's channel $\mathbf{g}_r$ is unknown, the result of Theorem 4.3 would still hold with probability 1. This stronger result is stated formally in the following theorem.

Theorem 4.4 *If the relay-eavesdropper's channel information $\mathbf{g}_r$ is unavailable (except possibly at the eavesdropper), then using a simple randomized version of the relay's strategy given in Theorem 4.3, the achievable secrecy rate $R_o(\bar{P}_r)$ converges to C^G as $\bar{P}_r \to \infty$ with probability 1 where C^G is the capacity of the Gaussian channel between the source and the destination when there is no eavesdropper in the system. Hence, with probability 1, $R_o(\bar{P}_r)$ approaches the secrecy of the reversely degraded relay-eavesdropper channel with multiple antennas at the relay as the total average relay's power $\bar{P}_r$ becomes sufficiently large.*

4.5 Numerical Results

First, consider the system described in Section 4.2. We compare the optimal secrecy rates R^{CJ} and R^{NF} achievable by our CJ and NF strategies proposed in Section 4.3 with the optimal secrecy rate R_o achievable by the strategy that uses only the orthogonal component of the channel for CJ. We also compare these rates to the secrecy capacity C^{GWT} of the original Gaussian wiretap channel with no relay. In Figure 4.1, we set $\bar{P}_s = 5,\ \bar{P}_r = 2,\ g_s = 0.85,\ \gamma_{r0} = 2$, and $\gamma_{r1} = 1$. We plot $R^{CJ},\ R^{NF},\ R_o$, and C^{GWT} versus $\sqrt{\alpha}$, $0 \leq \sqrt{\alpha} \leq 4$, where, as in Section 4.2, $\sqrt{\alpha}$ is defined as $\frac{\mathbf{g}_r^T \mathbf{h}_r}{\gamma_{r0}}$. It is clear from Figure 4.1 that the necessary conditions given in Corollary 4.1 for $R^{CJ} > R_o$ and $R^{NF} > R_o$ are satisfied here. Note that the necessary condition in Corollary 4.1 for $R^{CJ} > R_o$ is equivalent to $\alpha > \frac{\gamma_{r1}}{\gamma_{r0}} + \max(g_s, 1 + \gamma_{r1}\bar{P}_r)$, i.e., $\alpha > 3.5$ (or equivalently, $\sqrt{\alpha} > 1.871$). Note also that the necessary condition in Corollary 4.1 for $R^{NF} > R_o$ is equivalent to $\frac{\gamma_{r1}}{\gamma_{r0}} < \alpha < 1 + \gamma_{r1}\bar{P}_r$, i.e., $0.5 < \alpha < 3$ (or equivalently, $0.707 < \sqrt{\alpha} < 1.732$). It is clear that, in general, our CJ and NF strategy yield greater secrecy rates than R_o and C^{GWT}.

Next, we consider the case where the relay is constrained to using only one of the two modes (CJ or NF) over all the channel components, i.e., the relay cannot split its power between CJ and NF. We denote the secrecy rate achievable in this case by either R^{SM-CJ} or R^{SM-NF} depending on the single mode of deaf cooperation that the relay is using. It is clear that $R^{SM-CJ} = R^{CJ}$ where R^{CJ} is the optimal secrecy rate achieved by our CJ strategy since in this strategy the relay jams over the two orthogonal components of the channel and hence it is indeed a single-mode strategy.

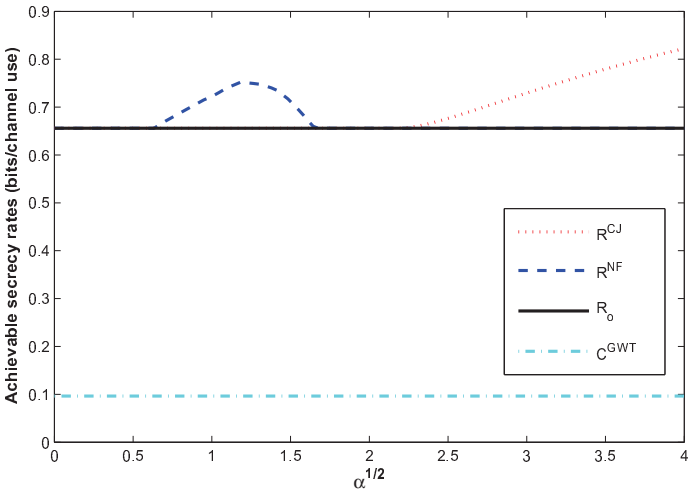

Figure 4.1: The optimal achievable secrecy rates R^{CJ} and R^{NF}, the achievable secrecy rate R_o, and the secrecy capacity of the original Gaussian wiretap channel, C^{GWT}, as functions $\sqrt{\alpha}$.

However, in our NF strategy the relay uses the orthogonal component for CJ whereas it uses the direct component for NF. Therefore, intuitively, we must have $R^{NF} > R^{SM-NF}$ in general. To illustrate this, in Figure 4.2, we plot R^{NF}, R^{SM-CJ}, R^{NF-SM}, and C^{GWT} versus $\sqrt{\alpha}$, $0 \leq \sqrt{\alpha} \leq 2$. The values of $\bar{P}_s$, $\bar{P}_r$, g_s, γ_{r0}, and γ_{r1} are fixed and chosen as in the previous example.

Finally, we consider a reversely degraded relay-eavesdropper channel with multiple antennas at the relay as the one described in Section 4.4. In Figure 4.3, we illustrate the result of Theorem 4.3. We fix $\bar{P}_s = 5, \gamma_{r1} = 1$. We plot the achievable secrecy rate R_o of Theorem 4.3 as a function of $\bar{P}_r$ for three different values of the channel gain g_s, namely, $g_s = 0.25$, 0.75, and 1.5. In this example, the capacity of the Gaussian channel between the source and the destination without secrecy constraints is $C^G = \frac{1}{2}\log(1+\bar{P}_s) = 1.292$ bits/channel use. It is clear from Figure 4.3 that $R_o(\bar{P}_r)$ converges to C^G as $\bar{P}_r$ increases and the rate of convergence increases as g_s decreases.

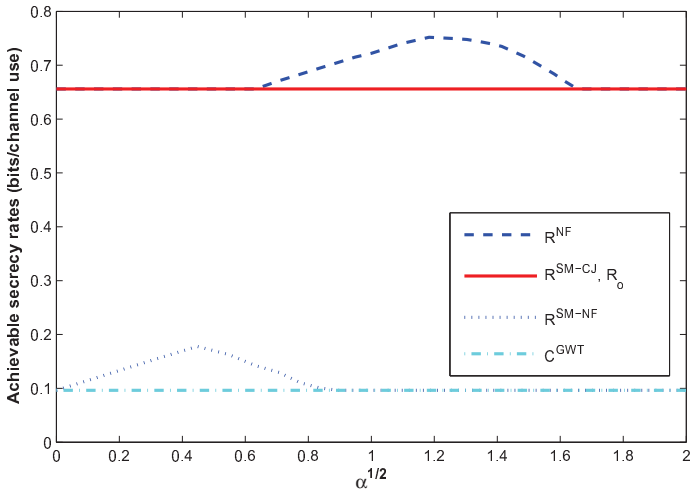

Figure 4.2: The optimal achievable secrecy rates R^{NF}, R^{SM-CJ}, R^{SM-NF}, and the secrecy capacity of the original Gaussian wiretap channel, C^{GWT}, as functions of $\sqrt{\alpha}$.

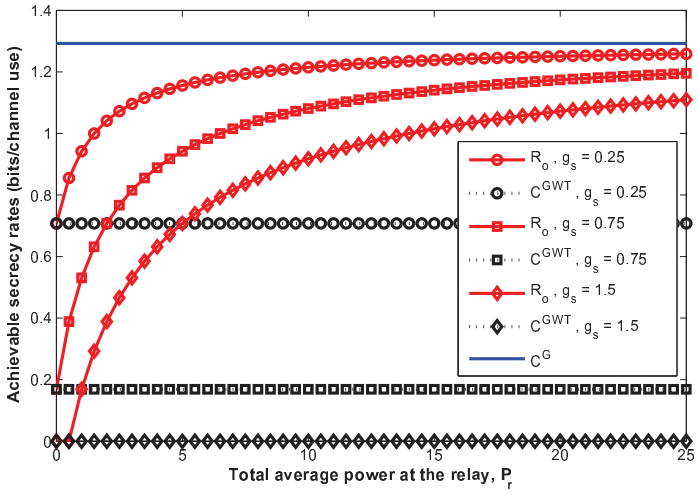

Figure 4.3: R_o as a function of $\bar{P}_r$, C^G, and C^{GWT}.

4.6 Conclusions

In this chapter, we extended the idea of deaf cooperation to the multi-antenna deaf helper model. We showed that the multiple spatial dimensions available in this model can be exploited in the deaf cooperation paradigm by possibly decomposing the relay-

eavesdropper channel into two components, a direct component in the direction of the relay-destination channel and an orthogonal component that is orthogonal to the relay-destination channel. We proposed two strategies for deaf cooperation in this model. In one strategy, the direct component is used by the relay to perform noise forwarding whereas in the other strategy, it is used for cooperative jamming. In both strategies, the orthogonal component is used for cooperative jamming. Under the assumption of independent signaling along each component, we derived the optimal power allocation for each strategy. We also found the necessary conditions for each strategy to be useful, i.e., to achieve secrecy rate higher than the secrecy capacity of the original Gaussian wiretap channel and showed that both strategies cannot be useful at the same time. Finally, we considered the reversely degraded relay channel and showed that by using a simple cooperative jamming strategy, we can approach the secrecy capacity of this reversely degraded channel as the relay's total power increases.

4.7 Appendix

4.7.1 Proof of Theorem 4.2

For cases 1 and 2(a), the proof of these cases follows easily from Lemma 1. Before we prove the rest of the cases, by simple computations, one can easily see that the

conditions below hold for the rest of the cases, i.e., whenever $\tilde{\alpha} > 0$ and $\tilde{\alpha} + \beta < 1$.

$$\forall\ P_s \geq 0, \quad \frac{\partial R_1^{NF}(P_s, Q_{r0})}{\partial P_s} \geq 0 \quad \text{if and only if} \quad Q_{r0} \geq \frac{\tilde{g}_s - 1}{\tilde{\alpha}} \tag{4.92}$$

$$\forall\ P_s \geq 0, \quad \frac{\partial R_1^{NF}(P_s, Q_{r0})}{\partial Q_{r0}} \geq 0 \quad \forall\ Q_{r0} \geq 0 \tag{4.93}$$

$$\text{If } \tilde{g}_s < \tilde{\alpha}, \quad \text{then} \quad \forall\ P_s \geq 0, \quad \frac{\partial R_2^{NF}(P_s, Q_{r0})}{\partial P_s} \geq 0 \quad \text{if and only if} \quad Q_{r0} \geq \frac{\tilde{g}_s - 1}{\tilde{\alpha} - \tilde{g}_s} \tag{4.94}$$

$$\text{If } \tilde{g}_s > \tilde{\alpha}, \quad \text{then} \quad \forall\ P_s \geq 0, \quad \frac{\partial R_2^{NF}(P_s, Q_{r0})}{\partial P_s} \geq 0 \quad \text{if and only if} \quad Q_{r0} \leq \frac{1 - \tilde{g}_s}{\tilde{g}_s - \tilde{\alpha}} \tag{4.95}$$

$$\text{If } \tilde{g}_s = \tilde{\alpha}, \quad \text{then} \quad \forall\ P_s \geq 0, \quad \frac{\partial R_2^{NF}(P_s, Q_{r0})}{\partial P_s} \geq 0 \quad \forall\ Q_{r0} \geq 0 \tag{4.96}$$

Also, from Lemma 1, we have

$$\forall\ P_s \in [0, P_s^*], \quad \frac{\partial R_2^{NF}(P_s, Q_{r0})}{\partial Q_{r0}} \geq 0 \quad \text{if and only if} \quad Q_{r0} \in [0, Q_{r0}^*(P_s)] \tag{4.97}$$

Now, we consider case 2(b). From (4.92) and (4.94), both R_1^{NF} and R_2^{NF} are increasing in P_s. Hence, $\hat{P}_s^{NF} = \bar{P}_s$. We have one of the following two cases depending on whether $\bar{P}_s \leq P_s^*$. First, if $\bar{P}_s \leq P_s^*$, then it follows from (4.97) that, $R_2^{NF}(\bar{P}_s, Q_{r0})$, as a function of Q_{r0}, attains its unconstrained maximum at $Q_{r0} = Q_{r0}^*(\bar{P}_s)$. On the other hand, from (4.92), $R_1^{NF}(\bar{P}_s, Q_{r0})$, as a function of Q_{r0}, is increasing in Q_{r0} for all $Q_{r0} \geq 0$ and hence the curves of $R_1^{NF}(\bar{P}_s, Q_{r0})$ and $R_2^{NF}(\bar{P}_s, Q_{r0})$ may intersect at some positive Q_{r0} (note that they already intersect at $Q_{r0} = 0$). It is easy to

see that such point is indeed $\tilde{Q}_{r0}$ given by (4.57). Note also that $R^{NF}(\bar{P}_s, Q_{r0}) = R_1^{NF}(\bar{P}_s, Q_{r0})$ whenever $Q_{r0} \leq \tilde{Q}_{r0}$, i.e., $R_1^{NF}(\bar{P}_s, Q_{r0}) \leq R_2^{NF}(\bar{P}_s, Q_{r0})$ whenever $Q_{r0} \leq \tilde{Q}_{r0}$. Hence, the unconstrained maximizer of $R^{NF}(\bar{P}_s, Q_{r0})$ as a function of Q_{r0} is $\max\left(Q_{r0}^*(\bar{P}_s), \tilde{Q}_{r0}\right)$. Since both $R_1^{NF}(\bar{P}_s, Q_{r0})$ and $R_2^{NF}(\bar{P}_s, Q_{r0})$ are increasing in Q_{r0} for all $0 \leq Q_{r0} \leq \max\left(Q_{r0}^*(\bar{P}_s), \tilde{Q}_{r0}\right)$, it follows that the constrained maximizer $\hat{Q}_{r0}^{NF}$ is given by $\min\left(\gamma_{r0}\bar{P}_r, \max\left(Q_{r0}^*(\bar{P}_s), \tilde{Q}_{r0}\right)\right)$. If $\bar{P}_s > P_s^*$, then from (4.97), $R_2^{NF}(\bar{P}_s, Q_{r0})$ (and consequently $R^{NF}(\bar{P}_s, Q_{r0})$) is upper bounded by $R_2^{NF}(\bar{P}_s, 0) = R_o$ which is the optimal secrecy rate achieved when there is no transmission along the direct channel component. Hence, $\hat{Q}_{r0}^{NF} = 0$.

Next, we consider case 2(c). From (4.92), $R_1^{NF}(P_s, Q_{r0})$ is increasing in P_s for all $P_s, Q_{r0} \geq 0$. In case 2(c-i), from (4.95), $R_2^{NF}(P_s, Q_{r0})$ is also increasing in P_s for all $P_s \geq 0$ and for all $0 \leq Q_{r0} \leq \gamma_{r0}\bar{P}_r$. Hence, in this case $\hat{P}_s^{NF} = \bar{P}_s$. The rest of case 2(c-i) follows using the same argument of case 2(b).

We analyze the rest of the subcases of (c) as follows. Since in these subcases $\gamma_{r0}\bar{P}_r > \frac{1-\tilde{g}_s}{\tilde{g}_s - \tilde{\alpha}}$, we solve the optimization problem in two steps. First, we find the local maximizer $({P_s}^{(a)}, {Q_{r0}}^{(a)})$ of $R^{NF}(P_s, Q_{r0})$ for $0 \leq P_s \leq \bar{P}_s$, $0 \leq Q_{r0} \leq \frac{1-\tilde{g}_s}{\tilde{g}_s - \tilde{\alpha}}$. Then, we find the local maximizer $({P_s}^{(b)}, {Q_{r0}}^{(b)})$ of $R^{NF}(P_s, Q_{r0})$ for $0 \leq P_s \bar{P}_s$, $\frac{1-\tilde{g}_s}{\tilde{g}_s - \tilde{\alpha}} \leq Q_{r0} \leq \gamma_{r0}\bar{P}_r$. Finally, we set $(\hat{P}_s^{NF}, \hat{Q}_{r0}^{NF}) = ({P_s}^{(a)}, {Q_{r0}}^{(a)})$ if $R^{NF}({P_s}^{(a)}, {Q_{r0}}^{(a)}) \geq R^{NF}({P_s}^{(b)}, {Q_{r0}}^{(b)})$ and set $(\hat{P}_s^{NF}, \hat{Q}_{r0}^{NF}) = ({P_s}^{(b)}, {Q_{r0}}^{(b)})$ otherwise.

Clearly, $({P_s}^{(a)}, {Q_{r0}}^{(a)})$ can be easily obtained in the same way the maximizer in case 2(c-i) was obtained. In particular, ${P_s}^{(a)} = \bar{P}_s$ and ${Q_{r0}}^{(a)} = \min\left(\frac{1-\tilde{g}_s}{\tilde{g}_s - \tilde{\alpha}}, \max\left(Q_{r0}^*(\bar{P}_s), \tilde{Q}_{r0}\right)\right)$ if $\bar{P}_s \leq P_s^*$ whereas ${Q_{r0}}^{(a)} = 0$ if $\bar{P}_s > P_s^*$. We

consider now the case where

$$\frac{1-\tilde{g}_s}{\tilde{g}_s-\tilde{\alpha}} \leq Q_{r0} \leq \gamma_{r0}\bar{P}_r \tag{4.98}$$

From (4.92) and (4.95), it follows that, for all Q_{r0} satisfying (4.98), $R_1^{NF}(P_s, Q_{r0})$ is increasing in P_s whereas $R_2^{NF}(P_s, Q_{r0})$ is decreasing in P_s. Let $\tilde{P}_s(Q_{r0})$ be the value of P_s such that $R_1^{NF}(P_s, Q_{r0}) = R_2^{NF}(P_s, Q_{r0})$. It is easy to see that $\tilde{P}_s(Q_{r0})$ is given by

$$\tilde{P}_s(Q_{r0}) = \frac{1-\beta Q_{r0}}{\tilde{\alpha}+\beta} - 1 \tag{4.99}$$

It follows from (4.99) that in order to have $R_1^{NF}(P_s, Q_{r0}) = R_2^{NF}(P_s, Q_{r0})$ for some $P_s \in [0, \bar{P}_s]$, we must have

$$\frac{1-(\tilde{\alpha}+\beta)(1+\bar{P}_s)}{\beta} \leq Q_{r0} \leq \frac{1-(\tilde{\alpha}+\beta)}{\beta} \tag{4.100}$$

Now, consider the maximizer of

$$R^{NF}(\tilde{P}_s(Q_{r0}), Q_{r0}) = \frac{1}{2}\log\left(\frac{(1+\tilde{\alpha}Q_{r0})(1-\beta Q_{r0})}{(\tilde{\alpha}+\beta)(1+\tilde{\alpha}Q_{r0}) + \tilde{g}_s\left(1-(\tilde{\alpha}+\beta)-\beta Q_{r0}\right)}\right) \tag{4.101}$$

subject to conditions (4.98) and (4.100), i.e., subject to

$$Q_{r0} \in \left[\frac{1-\tilde{g}_s}{\tilde{g}_s-\tilde{\alpha}}, \gamma_{r0}\bar{P}_r\right] \cap \left[\frac{1-(\tilde{\alpha}+\beta)(1+\bar{P}_s)}{\beta}, \frac{1-(\tilde{\alpha}+\beta)}{\beta}\right]$$
$$= \left[\max\left(\frac{1-\tilde{g}_s}{\tilde{g}_s-\tilde{\alpha}}, \frac{1-(\tilde{\alpha}+\beta)(1+\bar{P}_s)}{\beta}\right), \ \min\left(\gamma_{r0}\bar{P}_r, \frac{1-(\tilde{\alpha}+\beta)}{\beta}\right)\right] \quad (4.102)$$

It is not hard to check that $R^{NF}(\tilde{P}_s(Q_{r0}), Q_{r0})$ has one unconstrained maximum at $Q_{r0} = Q_{r0}^{(2)}$ where $Q_{r0}^{(2)}$ is given by (4.73). Hence, if the interval in (4.102) is not empty, then the constrained maximizer of (4.101) subject to (4.102) is given by $\min\left(Q_{r0}^{(2)}, \gamma_{r0}\bar{P}_r, \frac{1-(\tilde{\alpha}+\beta)}{\beta}\right)$. Hence, ${Q_{r0}}^{(b)} = \min\left(Q_{r0}^{(2)}, \gamma_{r0}\bar{P}_r, \frac{1-(\tilde{\alpha}+\beta)}{\beta}\right)$. Consequently, from (4.99), ${P_s}^{(b)} = \tilde{P}_s({Q_{r0}}^{(b)}) = \frac{1-\beta{Q_{r0}}^{(b)}}{\tilde{\alpha}+\beta} - 1$.

If the interval in (4.102) is empty, then we have either one of two cases. That is $\frac{1-(\tilde{\alpha}+\beta)}{\beta} < \frac{1-\tilde{g}_s}{\tilde{g}_s-\tilde{\alpha}}$ or $\frac{1-(\tilde{\alpha}+\beta)(1+\bar{P}_s)}{\beta} > \gamma_{r0}\bar{P}_r$. First, if $\frac{1-(\tilde{\alpha}+\beta)}{\beta} < \frac{1-\tilde{g}_s}{\tilde{g}_s-\tilde{\alpha}}$, then $R_2^{NF}(P_s, Q_{r0}) \leq 0$ for all $P_s \geq 0$ and all $Q_{r0} \in \left[\frac{1-\tilde{g}_s}{\tilde{g}_s-\tilde{\alpha}}, \gamma_{r0}\bar{P}_r\right]$. Hence, the choice of $({P_s}^{(b)}, {Q_{r0}}^{(b)})$ is irrelevant in this case and the maximizer of R^{NF} is given by $({P_s}^a, {Q_{r0}}^a)$. Second, if $\frac{1-(\tilde{\alpha}+\beta)(1+\bar{P}_s)}{\beta} > \gamma_{r0}\bar{P}_r$, then $R_1^{NF}(P_s, Q_{r0}) < R_2^{NF}(P_s, Q_{r0})$ for all $P_s \in [0, \bar{P}_s]$ and all $Q_{r0} \in \left[0, \gamma_{r0}\bar{P}_r\right]$. Hence, $R^{NF}(P_s, Q_{r0}) = R_1^{NF}(P_s, Q_{r0})$ for all $P_s \in [0, \bar{P}_s]$ and all $Q_{r0} \in \left[0, \gamma_{r0}\bar{P}_r\right]$. Thus, it follows from (4.92) and (4.93) that the maximizer of R^{NF} is given by $(\bar{P}_s, \gamma_{r0}\bar{P}_r)$.

Finally, we consider case 2(d). To prove the statement in case 2(d-i), we note that

$$\forall\ P_s \geq 0, \quad \text{if} \quad R_1^{NF}(P_s, Q_{r0}) > 0 \quad \text{then} \quad Q_{r0} > \frac{\tilde{g}_s - 1}{\tilde{\alpha}} \quad (4.103)$$

Hence, if $\gamma_{r0}\bar{P}_r \leq \frac{\tilde{g}_s-1}{\tilde{\alpha}}$, then we necessarily have $R^{NF}(P_s, Q_{r0}) = 0$ for all $P_s \geq 0$

and all $0 \leq Q_{r0} \leq \gamma_{r0}\bar{P}_r$. Thus, in this case, $\hat{P}_s^{NF} = \hat{Q}_{r0}^{NF} = 0$. For the rest of the subcases of 2(d), the proof follows the same steps of the proof of cases 2(c-ii), 2(c-iii), and 2(c-iv) above.

Chapter 5

Decode-and-Forward Based Strategies for Secrecy in Multiple Relay Networks

5.1 Introduction

In Chapters 3 and 4, we studied the notion of deaf cooperation in wireless relay networks with secrecy constraints. In this chapter, we turn our attention to the second type of cooperation, namely, to *active cooperation*. In general, one can distinguish between two types of cooperation in the secrecy context. The first type of cooperation for secrecy is passive (deaf) cooperation, in which the relay transmits a signal that is independent of the source message in order to confuse the eavesdropper and hence improve the achievable secrecy rate. Whereas the second type of cooperation is active cooperation in which a relay listens to the source transmissions and uses its observation to improve the achievable secrecy rate. This type is based on the well-known strategies, e.g., decode-and-forward (DF), compress-and-forward (CF), and amplify-and-forward (AF) strategies, devised originally for cooperative models with no secrecy constraint. Reference [38] was the first to introduce the basic relay channel without secrecy constraints where most of these strategies were first proposed (see

also [44]). In [29], the basic relay-eavesdropper channel was introduced and achievable secrecy rates were obtained based on extended versions of these strategies as well as new strategies that fit the secrecy model.

The role of active cooperation of beamforming relays in improving secrecy was investigated in [39] and [43]. In both [39] and [43], a two-stage cooperative secrecy protocol is proposed in which a set of multiple relays decode the source's message in the first stage, then the relays forward the source's message to the destination using beamforming. Reference [39] proposes an iterative strategy, when the global channel state information (CSI) is perfectly available, to design the beamforming coefficients either to maximize the secrecy rate for a fixed transmit power or to minimize the transmit power for a fixed secrecy rate. The same reference proposes a suboptimal zero-forcing strategy in which an additional constraint of canceling out the signals from the eavesdropper's observation is enforced. In [43], the problem of maximizing the secrecy rate achieved by the collaborative beamforming of the relays when the global CSI is perfectly available is investigated under both total and individual relay power constraints where a closed-form solution is obtained in the first case and a numerical solution is devised for the second case. The work in [39] and [43] appears to be closely related to the beamforming strategy presented in this chapter. However, there is a major difference between their model and the model presented here. In particular, both [39] and [43] assume that the communication occurs in two stages where in the first stage (source to relays) both the destination and the eavesdropper cannot hear the source at all and hence no secrecy requirement is involved in this stage whereas in the second stage only the relays (but not the source) sends the

source's message by beamforming to the destination and hence their model becomes similar to a MISO wiretap channel [16], [10], [15], [42]. This assumption is not made in the work presented here. In particular, any node in the system can hear any other transmitting node(s) at any time during the message is being communicated.

In this chapter, we study the DF scheme in the secrecy context and propose DF-based strategies for secrecy in multiple relay networks. First, we consider the single relay problem. The problem of maximizing the achievable secrecy rate under individual average power constraints at the source and the relay is, in general, analytically intractable. Hence, we propose a suboptimal DF with zero-forcing (DF/ZF) strategy for which we obtain the optimal power control policy. Next, we consider the multiple relay problem. We propose three different strategies based on DF/ZF. In the first strategy, all the relays decode the source message at the same time, then perform beamforming by transmitting scaled versions of the same signal to the destination, i.e., in this strategy each message block is transmitted to the destination in a single hop[1], i.e., all the relays decode the same message block at the same time and forward it to the destination. We give the achievable rate using this strategy and derive the optimal power control policy for both the source and the relays. Although this strategy is simple, it has an obvious drawback. In particular, we show that in this strategy the relays which are far from the source could possibly create a bottleneck that limits the achievable rate.

To overcome this drawback, we propose another strategy that is based on the

[1]Here, we define the number of hops as the number of transmission blocks required for all the relays to decode a single block of the source's message.

one proposed in [40] (see also [41]) for the case with no secrecy constraints. In this strategy, the transmission of each message block occurs in a number of hops that is equal to the number of relays. More precisely, the relays are ordered with respect to their distance from the source and they perform DF in a multi-hop fashion, i.e., the closest relay decodes the source message first, forwards it (with the help of the source) to the second closest relay and so forth till it reaches the destination. Since the encoding of the source message is done using block-Markov encoding in which the source message is divided into a sufficiently large number of blocks, the total overhead required per block becomes negligible. We show that this strategy overcomes the bottleneck drawback of the first strategy. In order to really see gains in the secrecy rate achievable by this strategy, we need to allocate power appropriately at all the relays. On the other hand, the optimal power allocation policy for the achievable rate by this strategy is analytically intractable and using numerical methods is not a practical option especially when the number of relays is large. Hence, a zero-forcing technique becomes a viable practical alternative since it guarantees that no information would leak from the relays to the eavesdropper no matter how the relays allocate their power. We discuss the zero-forcing technique in the second strategy and show that if all the relays transmit fresh information in every transmission block then only half of the signal components from different relays can be forced to zero in the eavesdropper's observation. We give the achievable secrecy rate in this case.

Although the second strategy overcomes the bottleneck drawback of the first strategy, as the optimal power allocation is not known, the inability to zero-force all the relays' signals at the eavesdropper may lead sometimes to a significant reduction in

the achievable secrecy rate. We observe that to achieve full zero-forcing in the second strategy, we need to set half of the relays' signal components (that represent the fresh information transmitted by these relays in a given transmission block) to zero. However, this is not meaningful in a T-hop strategy. Based on this observation, we propose a $\frac{T}{2}$-hop strategy that, in the Gaussian case, represents a practical realization of the second strategy with full zero-forcing and hence it combines the advantages of the two aforementioned strategies in an efficient way. That is, the achievable rate is not limited by the worst source-relay channel as in the first strategy, yet we can eliminate all the relays' signals from the eavesdropper's observation. In this strategy, the transmission of each message block takes place in a number of hops that is equal to half the number of relays. The relays form clusters of two relays per cluster. The source transmits the message to the relays in the first cluster which decode the message and forward it (with the help of the source) to the relays in the second cluster which decode it and forward it (with the help of the source and the relays in the first cluster) to the relays in the third cluster and so on so forth till the message is forwarded to the destination. The relays in each clusters are not assumed to have any kind of direct communication among them. We show that by properly adjusting the signal coefficients at the relays, we can zero-force all the relays' signals at the eavesdropper. Hence, in typical situations, the achievable secrecy rate is significantly improved with respect to the secrecy rates achieved by the first two strategies.

Finally, we give numerical results to compare the performance of the proposed strategies in terms of the achievable rates when a constant power allocation is used at all the relays. Our results show that the second (multi-hop) strategy yields higher

rates than the first (single-hop) strategy when the variation in the distance between the source and the relays is large whereas the first strategy yields higher rates when such variation is small, i.e., when the relays are at about the same distance from the source. Our simulation results also show that in a typical situation where each relay has a close neighbor relay, the third strategy outperforms the first two strategies.

5.2 Decode-and-Forward with a Single Relay

We consider the Gaussian relay-eavesdropper channel consisting of a source (node 0), a relay (node 1), a destination (node 2), and an eavesdropper (node 3); see Figure 5.1. Without loss of generality, one can normalize the channel gains from the source and the relay to the destination by proper scaling of the power constraints at the source and the relay. Hence, the outputs at the relay, the destination, and the eavesdropper are, respectively, given by

$$Y_1 = h_{01}X_0 + N_1 \tag{5.1}$$

$$Y_2 = X_0 + X_1 + N_2 \tag{5.2}$$

$$Y_3 = h_{03}X_0 + h_{13}X_1 + N_3 \tag{5.3}$$

where $h_{k\ell}$ denotes the complex channel gain from node k to node ℓ, $k \in \{0, 1\}$ and $\ell \in \{1, 3\}$, X_k denotes the channel input at node $k \in \{0, 1\}$, and N_ℓ denotes the Gaussian noise at node $\ell \in \{1, 2, 3\}$ which is circularly symmetric complex Gaussian random variable with zero mean and unit variance. We assume that all nodes have

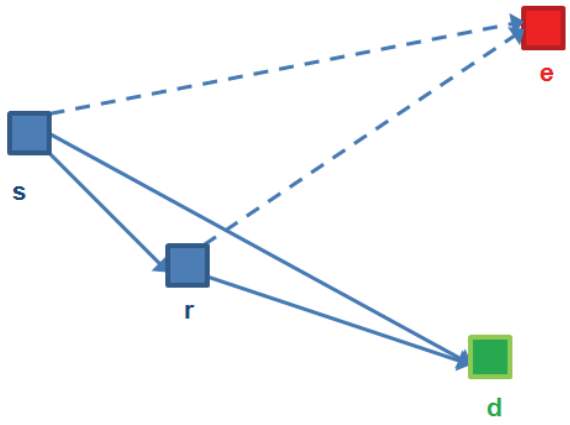

Figure 5.1: A single relay network.

perfect knowledge of all the channel gains. The average power constraints at the source and the relay are given by

$$E[|X_0|^2] \triangleq P_0 \leq \bar{P}_0, \qquad \text{and} \qquad E[|X_1|^2] \triangleq P_1 \leq \bar{P}_1 \tag{5.4}$$

We confine our attention to the DF scheme which is given in its original setting without secrecy constraints in [38] and [44] and extended in the secrecy context in [29]. The achievable secrecy rate using the DF scheme R^{DF} for any discrete memoryless relay-eavesdropper channel given by some conditional distribution $p(y_1, y_2, y_3|x_0, x_1)$ and for some input distribution $p(x_0, x_1)$ is given by (see [29])

$$R^{DF} = \min\{I(X_0; Y_1|X_1), I(X_0, X_1; Y_2)\} - I(X_0, X_1; Y_3) \tag{5.5}$$

For the Gaussian channel given by (5.1)-(5.3) above, as proposed in [38] as well as in [29], we choose X_0 and X_1 to be circularly symmetric Gaussian random variables

with zero mean and variances P_0 and P_1, respectively. Moreover, X_0 and X_1 are related as $X_0 = \tilde{X}_0 + \alpha_0 X_1$ where α_0 is some complex number to be determined later, $\tilde{X}_0$ is circularly symmetric Gaussian random variable with zero mean and variance $\tilde{P}_0$, and $\tilde{X}_0$ is independent of X_1. Hence, X_0 and X_1 are arbitrarily correlated and their covariance depends on the value of α_0. Moreover, from the average power constraints (5.4), we must have

$$\tilde{P}_0 + |\alpha_0|^2 P_1 \leq \bar{P}_0, \qquad \text{and} \qquad P_1 \leq \bar{P}_1 \tag{5.6}$$

It follows that the achievable secrecy rate by the DF strategy for such channel is given by

$$R^{DF} = \min \left\{ \log \left(\frac{1 + |h_{01}|^2 \tilde{P}_0}{1 + |h_{03}|^2 \tilde{P}_0 + |\alpha_0 h_{03} + h_{13}|^2 P_1} \right), \right. \\ \left. \log \left(\frac{1 + \tilde{P}_0 + |\alpha_0 + 1|^2 P_1}{1 + |h_{03}|^2 \tilde{P}_0 + |\alpha_0 h_{03} + h_{13}|^2 P_1} \right) \right\} \tag{5.7}$$

where α_0, $\tilde{P}_0$, and P_1 must satisfy (5.6). On the other hand, the secrecy capacity of the original Gaussian wiretap channel without a relay is given by

$$C^{GWT} = \left(\log \left(\frac{1 + \bar{P}_0}{1 + |h_{03}|^2 \bar{P}_0} \right) \right)^+ \tag{5.8}$$

where for $x \in \mathbb{R}$, $(x)^+ = \max(0, x)$. For the DF strategy to achieve strictly larger secrecy rate than the secrecy capacity of the original Gaussian wiretap channel C^{GWT}, it is clear from (5.7) and (5.8) that we must have $|h_{01}| > \max\{1, |h_{03}|\}$. In other words,

a necessary condition for the DF strategy to be useful is to have $|h_{01}| > \max\{1, |h_{03}|\}$.

The problem of finding the optimal power control policy (including finding the optimal value of α_0) is in general analytically intractable and closed form solution could not be obtained. However, we present here a suboptimal strategy for which we analytically derive the optimal power control policy. Here, we can only zero-force the relay signal X_1 but not the independent component of the source signal $\tilde{X}_0$. In particular, we set $\alpha_0 = \alpha^{ZF} \triangleq -\frac{h_{13}}{h_{03}}$. We denote the achievable rate in this case as $R^{DF/ZF}$ which, as a function of $(\tilde{P}_0, P_1)$, is given by

$$R^{DF/ZF} = \min\left\{ \log\left(\frac{1+|h_{01}|^2\tilde{P}_0}{1+|h_{03}|^2\tilde{P}_0}\right), \log\left(\frac{1+\tilde{P}_0+|\alpha^{ZF}+1|^2P_1}{1+|h_{03}|^2\tilde{P}_0}\right)\right\} \tag{5.9}$$

In the following theorem, we give the optimal power control policy $(\tilde{P}_0^\star, P_1^\star)$ that maximizes $R^{DF/ZF}$. This theorem is proved in the Appendix.

Theorem 5.1 *If $|h_{01}| \leq \max\{1, |h_{03}|\}$, then the optimal power control policy that maximizes $R^{DF/ZF}$ is given by $\tilde{P}_0^\star = P_1^\star = 0$ when $|h_{01}| \leq |h_{03}|$ whereas by $\tilde{P}_0^\star = \bar{P}_0$, $P_1^\star = 0$ when $|h_{01}| > |h_{03}|$. In this case, the DF/ZF strategy (and even the general DF strategy) becomes useless since the optimal achievable rate is equal to the secrecy capacity of the original Gaussian wiretap channel without a relay node. On the other hand, if $|h_{01}| > \max\{1, |h_{03}|\}$, then the optimal power control policy that maximizes $R^{DF/ZF}$ is given by the following cases:*

1. *If $\bar{P}_0 \leq \frac{1-|1+\frac{1}{\alpha^{ZF}}|^2-|h_{03}|^2}{|h_{03}|^2|1+\frac{1}{\alpha^{ZF}}|^2}$, $\bar{P}_1 \geq \frac{\bar{P}_0}{|\alpha^{ZF}|^2}$, then $\tilde{P}_0^\star = \bar{P}_0$, $P_1^\star = 0$.*
2. *If $\bar{P}_0 > \frac{1-|1+\frac{1}{\alpha^{ZF}}|^2-|h_{03}|^2}{|h_{03}|^2|1+\frac{1}{\alpha^{ZF}}|^2}$, $\bar{P}_1 \geq \frac{\bar{P}_0}{|\alpha^{ZF}|^2}$, then $\tilde{P}_0^\star = \frac{|1+\frac{1}{\alpha^{ZF}}|^2}{|h_{01}|^2-1+|1+\frac{1}{\alpha^{ZF}}|^2}\bar{P}_0$,*

$P_1^\star = \frac{\bar{P}_0 - \tilde{P}_0^\star}{|\alpha^{ZF}|^2}$.

3. *If* $\bar{P}_0 \leq \frac{1-|1+\frac{1}{\alpha^{ZF}}|^2-|h_{03}|^2}{|h_{03}|^2|1+\frac{1}{\alpha^{ZF}}|^2}$, $\bar{P}_1 < \frac{\bar{P}_0}{|\alpha^{ZF}|^2}$, *then* $\tilde{P}_0^\star = \bar{P}_0$, $P_1^\star = 0$.

4. *If* $\bar{P}_0 > \frac{1-|1+\frac{1}{\alpha^{ZF}}|^2-|h_{03}|^2}{|h_{03}|^2|1+\frac{1}{\alpha^{ZF}}|^2}$, $\bar{P}_1 < \frac{\bar{P}_0}{|\alpha^{ZF}|^2}$, *then we have the following subcases:*

   (a) *If* $\bar{P}_1 \leq \min\left\{\frac{1-|h_{03}|^2}{|h_{03}|^2|1+\alpha^{ZF}|^2}, \frac{|h_{01}|^2-1}{|h_{01}|^2-1+|1+\frac{1}{\alpha^{ZF}}|^2}\frac{\bar{P}_0}{|\alpha^{ZF}|^2}\right\}$, *then* $\tilde{P}_0^\star = \bar{P}_0 - |\alpha^{ZF}|^2\bar{P}_1$, $P_1^\star = \bar{P}_1$.

   (b) *If* $\frac{1-|h_{03}|^2}{|h_{03}|^2|1+\alpha^{ZF}|^2} < \bar{P}_1 \leq \frac{|h_{01}|^2-1}{|h_{01}|^2-1+|1+\frac{1}{\alpha^{ZF}}|^2}\frac{\bar{P}_0}{|\alpha^{ZF}|^2}$, *then* $\tilde{P}_0^\star = \frac{|1+\alpha^{ZF}|^2}{|h_{01}|^2-1}\bar{P}_1$, $P_1^\star = \bar{P}_1$.

   (c) *Otherwise,* $\tilde{P}_0^\star = \frac{|1+\frac{1}{\alpha^{ZF}}|^2}{|h_{01}|^2-1+|1+\frac{1}{\alpha^{ZF}}|^2}\bar{P}_0$, $P_1^\star = \frac{\bar{P}_0 - \tilde{P}_0^\star}{|\alpha^{ZF}|^2}$.

Moreover, in cases 1 and 3 above, the DF/ZF strategy is useless, i.e., it can only achieve rates as high as the secrecy capacity of the original Gaussian wiretap channel with no relay, whereas in cases 2 and 4, the DF/ZF strategy achieves a strictly larger rate than the secrecy capacity of the original Gaussian wiretap channel.

The following corollary is a direct consequence of the above theorem.

Corollary 5.1 *If at least one of the following two conditions is true, then the DF/ZF strategy is useful, i.e., it achieves a higher secrecy rate than the secrecy capacity of the original Gaussian wiretap channel without a relay:*

1. $|h_{01}| > |h_{03}| > 1$.

2. $|h_{01}| > 1 > |h_{03}|$ *and* $\bar{P}_0 > \frac{1-|1+\frac{1}{\alpha^{ZF}}|^2-|h_{03}|^2}{|h_{03}|^2|1+\frac{1}{\alpha^{ZF}}|^2}$.

5.3 Decode-and-Forward with Multiple Relays

Let $\mathcal{T} = \{1, ..., T\}$ denote the set of relays. Let the source be denoted as node 0, the destination as node $T + 1$, and the eavesdropper as node $T + 2$. The outputs at the relays, the destination, and the eavesdropper are given by

$$Y_i = h_{0i}X_0 + \sum_{j \in \mathcal{T} \setminus \{i\}} h_{ji}X_j + N_i, \ i \in \mathcal{T} \tag{5.10}$$

$$Y_{T+1} = X_0 + \sum_{i \in \mathcal{T}} X_i + N_{T+1} \tag{5.11}$$

$$Y_{T+2} = h_{0,T+2}X_0 + \sum_{i \in \mathcal{T}} h_{i,T+2}X_i + N_{T+2} \tag{5.12}$$

where, for $i, \ j \in \{0, 1, ..., T+2\}$, h_{ij} is the complex channel gain from node i to node j, X_i is the channel input at node i, and N_i is the complex circularly symmetric zero mean unit variance Gaussian noise at node i. We assume perfect knowledge of all channel gains at all the nodes. The average power constraints are given by

$$E[|X_0|^2] \triangleq P_0 \leq \bar{P}_0, \quad \text{and} \quad E[|X_i|^2] \triangleq P_i \leq \bar{P}_r, \ i \in \mathcal{T} \tag{5.13}$$

where we assume that all the relays have equal power constraints for simplicity.

5.3.1 Multiple Relay Single Hop DF (MRSH-DF) Strategy

In this strategy, all the relays decode the source message at a given block at the same time and forward it to the destination; see Figure 5.2. In the case of the general discrete memoryless multiple relay channel given by some conditional distribution

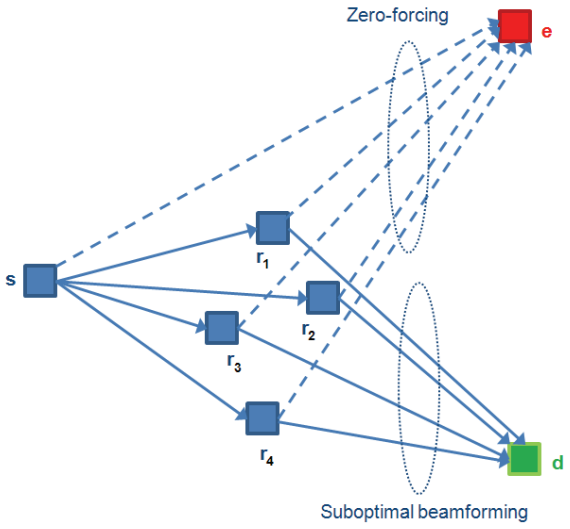

Figure 5.2: Multiple relay single hop strategy.

$p(y_1, ..., y_{T+1}, y_{T+2}|x_0, ..., x_T)$, the DF scheme of [29] can be extended to obtain an analogous scheme for the multiple relay case. It is not difficult to see that the achievable secrecy rate R^{DF} by such scheme is given by

$$R^{DF} = \min \left\{ \min_{i \in \mathcal{T}} \{I(X_0; Y_i|X_r)\}, I(X_0, X_r; Y_{T+1}) \right\} - I(X_0, X_r; Y_{T+2}) \qquad (5.14)$$

for some auxiliary random variable X_r where $p(x_r, x_0, ..., x_T)$ factors as $p(x_0|x_r)p(x_r)\prod_{j=1}^{T} p(x_j|x_r)$. For the Gaussian channel, our strategy requires that all the relays perform signal beamforming as they forward the source message to the destination. In particular, we choose $X_0 = \tilde{X}_0 + \alpha_0 X_r$ and $X_i = \alpha_i X_r,\ i \in \mathcal{T}$ where $\tilde{X}_0,\ X_r$ are independent circularly symmetric complex Gaussian random variables with zero mean and variances $\tilde{P}_0$ and P_r, respectively, and $\alpha_0, \alpha_i,\ i \in \mathcal{T}$ are some

complex numbers. From (5.13), we must have

$$\tilde{P}_0 + |\alpha_0|^2 P_r \leq \bar{P}_0, \qquad \text{and} \qquad |\alpha_i|^2 P_r \leq \bar{P}_r,\ i \in \mathcal{T} \tag{5.15}$$

Consequently, the achievable secrecy rate R^{DF} is given by

$$R^{DF} = \min \left\{ \min_{i \in \mathcal{T}} \ \log \left(\frac{1 + |h_{0i}|^2 \tilde{P}_0}{1 + |h_{0,T+2}|^2 \tilde{P}_0 + |\alpha_0 h_{0,T+2} + \sum_{j \in \mathcal{T}} \alpha_j h_{j,T+2}|^2 P_r} \right), \right.$$
$$\left. \log \left(\frac{1 + \tilde{P}_0 + |\alpha_0 + \sum_{j \in \mathcal{T}} \alpha_j|^2 P_r}{1 + |h_{0,T+2}|^2 \tilde{P}_0 + |\alpha_0 h_{0,T+2} + \sum_{j \in \mathcal{T}} \alpha_j h_{j,T+2}|^2 P_r} \right) \right\} \tag{5.16}$$

It is clear that a necessary condition for this strategy to be useful is to have $\min_{i \in \mathcal{T}} |h_{0,i}| > \max\{1, |h_{0,T+2}|\}$. Again, finding the optimal values for $\tilde{P}_0, P_r$, and $\alpha_i,\ i \in \mathcal{T} \cup \{0\}$ is analytically intractable. As in the previous section, we propose a suboptimal strategy in which α_0 is chosen to force the term of the eavesdropper's observation that depends on X_r to zero. This goal can be attained for any values of $\alpha_j,\ j \in \mathcal{T}$, by choosing $\alpha_0 = \alpha^{ZF} \triangleq -\frac{\sum_{j \in \mathcal{T}} \alpha_j h_{j,T+2}}{h_{0,T+2}}$. Hence, the achievable rate becomes

$$R^{DF/ZF} = \min \left\{ \log \left(\frac{1 + |h_{0i^\star}|^2 \tilde{P}_0}{1 + |h_{0,T+2}|^2 \tilde{P}_0} \right), \right.$$
$$\left. \log \left(\frac{1 + \tilde{P}_0 + \left| \sum_{j \in \mathcal{T}} \alpha_j \left(1 - \frac{h_{j,T+2}}{h_{0,T+2}} \right) \right|^2 P_r}{1 + |h_{0,T+2}|^2 \tilde{P}_0} \right) \right\} \tag{5.17}$$

where $i^\star = \arg\min_{i \in \mathcal{T}} |h_{0i}|$. However, the problem of maximizing (5.17) under the constraints $\tilde{P}_0 + |\alpha^{ZF}|^2 P_r \leq \bar{P}_0$ and $|\alpha_j|^2 P_r \leq \bar{P}_r,\ j \in \mathcal{T}$ is still intractable since α^{ZF}

(and hence the first constraint) depends on $\alpha_j,\ j \in \mathcal{T}$ and is not merely a constant as in the previous section. Thus, we resort to a suboptimal procedure to obtain a tractable solution. Specifically, we first find a set of suboptimal beamforming coefficients $\alpha_j,\ j \in \{T\}$, then, for this choice of coefficients, we maximize the achievable rate under the corresponding set of constraints. In particular, we ignore the constraint $\tilde{P}_0 + |\alpha^{ZF}|^2 P_r \leq \bar{P}_0$, assume $\tilde{P}_0$ to be fixed, and find $\alpha_j,\ j \in \mathcal{T}$ that maximize (5.17) for every P_r that satisfies the constraints $|\alpha_j|^2 P_r \leq \bar{P}_r,\ j \in \mathcal{T}$. For this set of coefficients, the problem of maximizing the achievable rate under the resulting set of constraints is tractable and can be solved in a way similar to that of the previous section.

Now, we claim that if $\tilde{P}_0$ is fixed, then, for every P_r that satisfies $|\alpha_j|^2 P_r \leq \bar{P}_r,\ j \in \mathcal{T}$, the rate in (5.17) is maximized by choosing $\alpha_j = \frac{\left(1-\frac{h_{j,T+2}}{h_{0,T+2}}\right)^*}{|1-\frac{h_{j,T+2}}{h_{0,T+2}}|},\ \forall j \in \mathcal{T}$, where a^* denotes the complex conjugate of the complex number a. To see this, we first note that, from the triangle inequality, we have $\left|\sum_{j\in\mathcal{T}} \alpha_j \left(1 - \frac{h_{j,T+2}}{h_{0,T+2}}\right)\right| \leq \sum_{j\in\mathcal{T}} |\alpha_j||1 - \frac{h_{j,T+2}}{h_{0,T+2}}|$. This upper bound can be attained by selecting the phase of α_j to be the negative of the phase of $\left(1 - \frac{h_{j,T+2}}{h_{0,T+2}}\right),\ j \in \mathcal{T}$. Hence, we can replace the objective function of (5.17) with

$$R^{DF/ZF} = \min \left\{ \log\left(\frac{1+|h_{0i^\star}|^2\tilde{P}_0}{1+|h_{0,T+2}|^2\tilde{P}_0}\right), \log\left(\frac{1+\tilde{P}_0+\left(\sum_{j\in\mathcal{T}}|\alpha_j|\left|1-\frac{h_{j,T+2}}{h_{0,T+2}}\right|\right)^2 P_r}{1+|h_{0,T+2}|^2\tilde{P}_0}\right) \right\} \tag{5.18}$$

Define $\hat{\beta} \triangleq \max\{|\alpha_j|,\ j \in \mathcal{T}\}$, $\beta_j \triangleq \frac{\alpha_j}{\hat{\beta}},\ j \in \mathcal{T}$, and $Q_r \triangleq \hat{\beta}^2 P_r$. Hence, the objective

function in (5.18) can be written as

$$R^{DF/ZF} = \min \left\{ \log \left(\frac{1+|h_{0i^\star}|^2 \tilde{P}_0}{1+|h_{0,T+2}|^2 \tilde{P}_0} \right), \right. \\ \left. \log \left(\frac{1+\tilde{P}_0 + \left(\sum_{j\in\mathcal{T}} |\beta_j| \left| 1 - \frac{h_{j,T+2}}{h_{0,T+2}} \right| \right)^2 Q_r}{1+|h_{0,T+2}|^2 \tilde{P}_0} \right) \right\} \tag{5.19}$$

where $|\beta_j| \leq 1,\ j \in \mathcal{T}$, and $Q_r \leq \bar{P}_r$. Finally, we note that, for every $Q_r \leq \bar{P}_r$, (5.19) is maximized by choosing $|\beta_j| = 1\ \forall j \in \mathcal{T}$.

Thus, the achievable rate by this set of coefficients $\alpha_j,\ j \in \mathcal{T}$ is given by

$$R^{DF/ZF} = \min \left\{ \log \left(\frac{1+|h_{0i^\star}|^2 \tilde{P}_0}{1+|h_{0,T+2}|^2 \tilde{P}_0} \right), \right. \\ \left. \log \left(\frac{1+\tilde{P}_0 + \left(\sum_{j\in\mathcal{T}} \left| 1 - \frac{h_{j,T+2}}{h_{0,T+2}} \right| \right)^2 P_r}{1+|h_{0,T+2}|^2 \tilde{P}_0} \right) \right\} \tag{5.20}$$

where $\tilde{P}_0,\ P_r$ satisfy

$$\tilde{P}_0 + |\alpha^{ZF}|^2 P_r \leq \bar{P}_0, \qquad \text{and} \qquad P_r \leq \bar{P}_r \tag{5.21}$$

and $\alpha^{ZF} = -\sum_{j\in\mathcal{T}} \frac{h_{j,T+2}}{h_{0,T+2}} \frac{\left(1-\frac{h_{j,T+2}}{h_{0,T+2}}\right)^*}{|1-\frac{h_{j,T+2}}{h_{0,T+2}}|}$. Indeed from the similarity between (5.20) and (5.9), we can easily modify Theorem 5.1 to obtain the optimal power control policy $(\tilde{P}_0^\star, P_r^\star)$ that maximizes (5.20) under constraints (5.21). In particular, if $|h_{0i^\star}| \leq \max\{1, |h_{0,T+2}|\}$, then this strategy is useless, i.e., it can achieve at most the secrecy capacity of the original wiretap channel with no relays. On the other hand, if $|h_{0i^\star}| > \max\{1, |h_{0,T+2}|\}$, then the optimal power control policy that maximizes (5.20) is given

by the following cases:

1. If $\bar{P}_0 \leq \frac{|\alpha^{ZF}|^2-\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2-|\alpha^{ZF}|^2|h_{0,T+2}|^2}{|h_{0,T+2}|^2\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2}$, $\bar{P}_r \geq \frac{\bar{P}_0}{|\alpha^{ZF}|^2}$, then $\tilde{P}_0^\star = \bar{P}_0$, $P_r^\star = 0$.

2. If $\bar{P}_0 > \frac{|\alpha^{ZF}|^2-\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2-|\alpha^{ZF}|^2|h_{0,T+2}|^2}{|h_{0,T+2}|^2\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2}$, $\bar{P}_r \geq \frac{\bar{P}_0}{|\alpha^{ZF}|^2}$, then
$\tilde{P}_0^\star = \frac{\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2}{|\alpha^{ZF}|^2|h_{0i^\star}|^2-|\alpha^{ZF}|^2+\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2}\bar{P}_0$, $P_r^\star = \frac{\bar{P}_0-\tilde{P}_0^\star}{|\alpha^{ZF}|^2}$.

3. If $\bar{P}_0 \leq \frac{|\alpha^{ZF}|^2-\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2-|\alpha^{ZF}|^2|h_{0,T+2}|^2}{|h_{0,T+2}|^2\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2}$, $\bar{P}_r < \frac{\bar{P}_0}{|\alpha^{ZF}|^2}$, then $\tilde{P}_0^\star = \bar{P}_0$, $P_r^\star = 0$.

4. If $\bar{P}_0 > \frac{|\alpha^{ZF}|^2-\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2-|\alpha^{ZF}|^2|h_{0,T+2}|^2}{|h_{0,T+2}|^2\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2}$, $\bar{P}_r < \frac{\bar{P}_0}{|\alpha^{ZF}|^2}$, then we have the following subcases:

   (a) If $\bar{P}_r \leq \min\left\{\frac{1-|h_{0,T+2}|^2}{|h_{0,T+2}|^2\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2}\ ,\ \frac{|h_{0i^\star}|^2-1}{|\alpha^{ZF}|^2|h_{0i^\star}|^2-|\alpha^{ZF}|^2+\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2}\bar{P}_0\right\}$,
   then $\tilde{P}_0^\star = \bar{P}_0 - |\alpha^{ZF}|^2\bar{P}_r$, $P_r^\star = \bar{P}_r$.

   (b) If $\frac{1-|h_{0,T+2}|^2}{|h_{0,T+2}|^2\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2} < \bar{P}_r \leq \frac{|h_{0i^\star}|^2-1}{|\alpha^{ZF}|^2|h_{0i^\star}|^2-|\alpha^{ZF}|^2+\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2}\bar{P}_0$,
   then $\tilde{P}_0^\star = \frac{\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2}{|h_{0i^\star}|^2-1}\bar{P}_r$, $P_r^\star = \bar{P}_r$.

   (c) Otherwise,
   then $\tilde{P}_0^\star = \frac{\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2}{|\alpha^{ZF}|^2|h_{0i^\star}|^2-|\alpha^{ZF}|^2+\left(\sum_{j\in\mathcal{T}}|1-\frac{h_{j,T+2}}{h_{0,T+2}}|\right)^2}\bar{P}_0$, $P_r^\star = \frac{\bar{P}_0-\tilde{P}_0^\star}{|\alpha^{ZF}|^2}$.

As in Theorem 5.1, cases 1 and 3 above can only achieve rates as high as the secrecy capacity of the original Gaussian wiretap channel with no relays, whereas in cases 2 and 4, the DF/ZF strategy achieves a strictly larger rate than the secrecy capacity of the original Gaussian wiretap channel.

5.3.2 Multiple Relay Multiple Hop DF (MRMH-DF) Strategy

One clear drawback of the above strategy is the requirement that all relays must decode the source message in a single hop at the same time and thus the furthest relay from the source creates a bottleneck in the achievable secrecy rate. To overcome this drawback, we propose another strategy that is based on the multi-hop DF strategy introduced in [40] for the multiple relay model without an eavesdropper. In this strategy, the relays in $\mathcal{T}$ are given a certain order. In any given transmission block b of the source message, the first relay decodes the current message block and forwards it (with the help of the source) to the second relay in the transmission block $b+1$ which decodes it and then forwards it (with the help of the source and the first relay) to the third relay in the transmission block $b+2$ and so on so forth till the last relay decodes the source message block and forwards it (with the help of the source and all the other relays) to the destination in the transmission block $b+T$. Hence, the transmission of each message block occurs over T hops before it reaches the destination; see Figure 5.3. Since the multi-hop transmission is pipelined, we only have an initial delay (overhead) of T blocks before the first message block reaches the destination, however no further delay is involved between source message blocks. Under the usual assumption that the source message is composed of sufficiently large number of blocks $B >> T$, the achievable rate loss due to such overhead is negligible. Without loss of generality, assume that the relays are ordered according to their label in $\mathcal{T}$, i.e., each relay $i \in \mathcal{T}$ is the ith relay in the multi-hop order. In the case of the general discrete memoryless multiple relay channel with external eavesdropper given by some con-

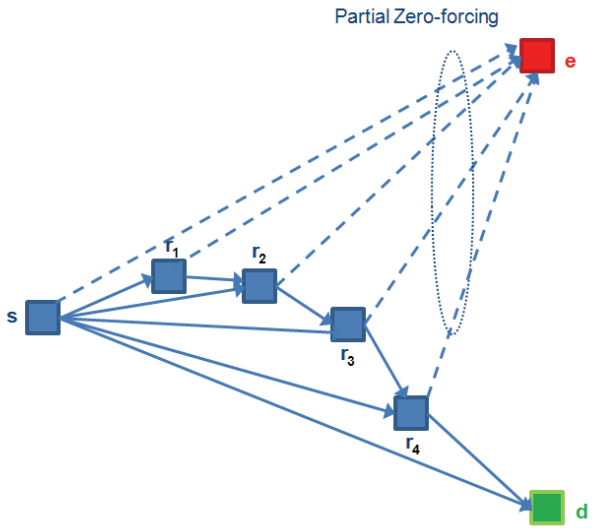

Figure 5.3: Multiple relay multiple hop strategy.

ditional distribution $p(y_1, ..., y_{T+1}, y_{T+2}|x_0, ..., x_T)$, the multi-hop DF scheme of [40] can be extended by applying stochastic encoding at the source and every relay in the usual manner to obtain an analogous secure scheme for the multiple relay with an external eavesdropper problem. By noting that the eavesdropper intercepts the signal transmitted in each of the T hops, it is not difficult to see that the achievable secrecy rate R^{DF} by such scheme for some input distribution $p(x_0, ..., x_T)$ is given by

$$R^{DF} = \min \Big\{ I(X_0; Y_1|X_1, X_2, ..., X_T), ..., I(X_0, X_1, ..., X_i; Y_{i+1}|X_{i+1}, ..., X_T), ..., I(X_0, X_1, ..., X_T; Y_{T+1}) \Big\} - I(X_0, X_1, ..., X_T; Y_{T+2}) \quad (5.22)$$

For the Gaussian channel (5.10)-(5.12), we choose the channel inputs as follows. $X_i = \tilde{X}_i + \alpha_i X_{i+1}$, $i = 0, ..., T-1$ and $X_T = \tilde{X}_T$ where all $\tilde{X}_i$, $i = 0, ..., T$ are independent circularly symmetric complex Gaussian random variables with zero mean

an variances $\tilde{P}_i,\ i = 0, ..., T$, respectively, and $\alpha_i, i = 0, ..., T-1$, are some complex numbers. Equivalently, we have $X_i = \tilde{X}_i + \sum_{j=i+1}^{T} \prod_{\ell=i}^{j-1} \alpha_\ell X_j,\ i = 0, ..., T-1$ and $X_T = \tilde{X}_T$. From (5.13), we must have

$$\tilde{P}_i + \sum_{j=i+1}^{T} \prod_{\ell=i}^{j-1} |\alpha_\ell|^2 \tilde{P}_j \le \bar{P}_i, \quad i \in \mathcal{T} \cup \{0\} \tag{5.23}$$

where $\bar{P}_i = \bar{P}_r\ \forall i \in \mathcal{T}$. Hence, the achievable rate R^{DF} is given by

$$\begin{aligned} R^{DF} = \min \Bigg\{ & \min_{j \in \mathcal{T}} \ \log \left(1 + |h_{0j}|^2 \tilde{P}_0 + \sum_{i=1}^{j-1} \left| h_{ij} + \sum_{\ell=0}^{i-1} h_{\ell j} \prod_{k=\ell}^{i-1} \alpha_k \right|^2 \tilde{P}_i \right), \\ & \log \left(1 + \tilde{P}_0 + \sum_{i \in \mathcal{T}} \left| 1 + \sum_{\ell=0}^{i-1} \prod_{k=\ell}^{i-1} \alpha_k \right|^2 \tilde{P}_i \right) \ \Bigg\} \\ & - \log \left(1 + |h_{0,T+2}|^2 \tilde{P}_0 + \sum_{i \in \mathcal{T}} \left| h_{i,T+2} + \sum_{\ell=0}^{i-1} h_{\ell,T+2} \prod_{k=\ell}^{i-1} \alpha_k \right|^2 \tilde{P}_i \right) \end{aligned} \tag{5.24}$$

For example, when $T = 3$, we have

$$\begin{aligned} R^{DF} = \min \Bigg\{ & \log \left(1 + |h_{01}|^2 \tilde{P}_0 \right), \log \left(1 + |h_{02}|^2 \tilde{P}_0 + |h_{12} + h_{02}\alpha_0|^2 \tilde{P}_1 \right), \\ & \log \left(1 + |h_{03}|^2 \tilde{P}_0 + |h_{13} + h_{03}\alpha_0|^2 \tilde{P}_1 + |h_{23} + h_{13}\alpha_1 + h_{03}\alpha_0\alpha_1|^2 \tilde{P}_2 \right), \\ & \log \big(1 + \tilde{P}_0 + |1 + \alpha_0|^2 \tilde{P}_1 + |1 + \alpha_1 + \alpha_0\alpha_1|^2 \tilde{P}_2 \\ & \quad + |1 + \alpha_2 + \alpha_1\alpha_2 + \alpha_0\alpha_1\alpha_2|^2 \tilde{P}_3 \big) \Bigg\} \\ & - \log \big(1 + |h_{0,5}|^2 \tilde{P}_0 + |h_{15} + h_{05}\alpha_0|^2 \tilde{P}_1 + |h_{25} + h_{15}\alpha_1 + h_{05}\alpha_0\alpha_1|^2 \tilde{P}_2 \\ & \quad + |h_{35} + h_{25}\alpha_2 + h_{15}\alpha_1\alpha_2 + h_{05}\alpha_0\alpha_1\alpha_2|^2 \tilde{P}_3 \big) \end{aligned} \tag{5.25}$$

Recall that this rate corresponds to the aforementioned ordering of the relays. In general, there are $T!$ of such orderings each of which gives a different rate. In this strategy, we choose to order the relays according to their distances from the source, i.e., the closer the relay to the source comes first in the multi-hop order. Hence, without loss of generality, we assume that $|h_{01}| \geq |h_{02}| \geq ... \geq |h_{0T}|$ and hence the ordering of the relays gives the rate in (5.24). Clearly, a necessary condition for this DF strategy to be useful (i.e., to give a rate higher than the secrecy capacity of the original Gaussian wiretap channel) is to have $\max_{i\in\mathcal{T}} |h_{0i}| > \max\{1, |h_{0,T+2}|\}$ which shows that the relays far from the source do not necessarily limit the achievable rate as in the MRSH-DF strategy.

Clearly, in the Gaussian case, the MRSH-DF strategy is a special case of the MRMH-DF strategy when all the relays' independent signal components $\tilde{X}_i,\ i \in \mathcal{T}$ are set to zero. This makes the MRMH-DF strategy potentially better than the MRSH-DF strategy in terms of the achievable secrecy rate if appropriate power allocation is used for the source and the relays. On the other hand, finding the optimal power allocation for the MRMH-DF strategy is analytically intractable and seeking numerical solution for this problem is not a practical choice especially if the number of relays is large. Hence, as a viable practical alternative, we may want to have some guarantees on the information rate leaked to the eavesdropper by zero-forcing the relays' signals at the eavesdropper as we did in the MRSH-DF strategy. In this case, even if the relays used a simple fixed power strategy, we would guarantee that none of the relays' signals would leak to the eavesdropper. However, unlike the MRSH-DF/ZF strategy, here we cannot eliminate all the components of the relays signals

from the eavesdropper's observation unless we set some of the relays' independent signal components $\tilde{X}_i$ to zero. More precisely, if $\tilde{P}_i > 0,\ \forall\ i \in \mathcal{T}$, then we can only eliminate half of the relays' signals from the eavesdropper's observation. In contrast, in the MRSH-DF strategy, we were able to achieve full zero-forcing because all the relays' independent signal components $\tilde{X}_i,\ i \in \mathcal{T}$ were zero in that strategy. However here if we insist that all the relays must transmit fresh information in each block, i.e., $\tilde{P}_i > 0,\ \forall\ i \in \mathcal{T}$, then only the signal components from either the odd (or the even) relays in the multi-hop ordering can be eliminated from the eavesdropper's observation but not both. Hence, we obtain a MRMH-DF strategy with partial zero-forcing (MRMH-PZF). The reason for this is that whenever we want to eliminate the signal X_i from the eavesdropper's observation, we adjust the correlation between X_i and X_{i-1} through choosing the proper value for α_{i-1}. However, this will necessarily give rise to a non-zero coefficient of X_{i-1} in the eavesdropper's observation. For example, when $T = 3$, the eavesdropper's observation Y_5 is given by

$$\begin{aligned} Y_5 =& h_{05}\tilde{X}_0 + (h_{15} + h_{05}\alpha_0)\tilde{X}_1 + (h_{25} + (h_{15} + h_{05}\alpha_0)\,\alpha_1)\,\tilde{X}_2 \\ &+ (h_{35} + (h_{25} + (h_{15} + h_{05}\alpha_0)\,\alpha_1)\,\alpha_2)\,\tilde{X}_3 + N_5 \end{aligned} \tag{5.26}$$

Here, we can either force the coefficients of $\tilde{X}_1$ and $\tilde{X}_3$ only to zero by setting $\alpha_0 = \alpha_0^{ZF} \triangleq -\frac{h_{15}}{h_{05}}$ and $\alpha_2 = \alpha_2^{ZF} \triangleq -\frac{h_{35}}{h_{25}}$, or we can force the coefficient of $\tilde{X}_2$ only to zero by setting $\alpha_1 = \alpha_1^{ZF} \triangleq -\frac{h_{25}}{h_{15}+h_{05}\alpha_0}$ where $\alpha_0 \neq \alpha_0^{ZF}$.

One can choose to force either the odd or the even terms of the relay signals in the eavesdropper's observation to zero. In general, one should make the choice such that

the coefficients with higher channel gains are forced to zero. Without loss of generality, we force the odd terms to zero by choosing $\alpha_{2i} = \alpha_{2i}^{ZF} \triangleq -\frac{h_{2i+1,T+2}}{h_{2i,T+2}},\ \forall i \in \{0, ..., \lfloor \frac{T}{2} \rfloor\}$. The rest of the coefficients must be chosen such that the power constraints (5.23) are satisfied. Hence, in this case, the achievable rate $R^{DF/PZF}$ is given by

$$\begin{aligned} R^{DF/PZF} = \min \Bigg\{ & \min_{j \in \mathcal{T}} \ \log \left(1 + |h_{0j}|^2 \tilde{P}_0 + \sum_{i=1}^{j-1} \left| h_{i,j} + \sum_{\ell=0}^{i-1} h_{\ell j} \prod_{k=\ell}^{i-1} \alpha_k \right|^2 \tilde{P}_i \right), \\ & \log \left(1 + \tilde{P}_0 + \sum_{i \in \mathcal{T}} \left| 1 + \sum_{\ell=0}^{i-1} \prod_{k=\ell}^{i-1} \alpha_k \right|^2 \tilde{P}_i \right) \Bigg\} \\ & - \log \left(1 + |h_{0,T+2}|^2 \tilde{P}_0 + \sum_{\text{even } i \in \mathcal{T}} \left| h_{i,T+2} + \sum_{\ell=0}^{i-1} h_{\ell,T+2} \prod_{k=\ell}^{i-1} \alpha_k \right|^2 \tilde{P}_i \right) \end{aligned} \tag{5.27}$$

Thus, we conclude that in order to achieve full zero-forcing in this strategy, we must set half of the independent signal components of the relays to zero, e.g., $\tilde{X}_i = 0$ (and hence $\tilde{P}_i = 0$) for all odd i in $\mathcal{T}$. However, it would be inefficient to use a DF strategy with T hops where half of the relays transmit the same signals (except for a scaling factor) that the other half of the relays transmit. Based on this observation, we propose below a multi-hop DF strategy using T relays but with only $\frac{T}{2}$ hops and show that full zero-forcing is possible in this case. Indeed, for the Gaussian model, the strategy proposed below is a practical realization of the T-hop strategy discussed here with full zero-forcing, i.e., when half of the relays independent signal components are set to zero in the T-hop strategy. It is clear now that the first MRSH-DF strategy represents one extreme case of the MRMH-DF strategy with T hops where all the relays' independent signals components $\tilde{X}_i,\ i \in \mathcal{T}$ are set to zero.

As discussed earlier, this leads to the drawback of having the achievable rate limited by the furthest relay from the source. On the other hand, the other extreme is to have a T-hop strategy where we insist that all the relays transmit fresh information (represented by the independent signals $\tilde{X}_i$) in every transmission block. In this case, although the bottleneck problem is solved, only partial zero-forcing is possible and without optimal power allocation (which is analytically intractable) there will be no guarantees on the information rate leaked to the eavesdropper. Hence, we propose next a multi-hop strategy that sits somewhere in the middle between these two extremes and provides an efficient and practical compromise where the achievable rate is not limited by the worst source-relay channel as in the MRSH-DF strategy but rather limited by the second best source-relay channel and all the relays' signals can be fully eliminated from the eavesdropper's observation.

5.3.3 Multiple Relay Multiple Hop DF with Full Zero-Forcing (MRMH-DF/FZF) Strategy

First, we discuss the general strategy without imposing the zero-forcing constraint. Then, in the Gaussian case, we show how to achieve full zero-forcing. In this strategy, we assume for simplicity that the number of relays T is even. We also take the number of the message blocks B to be even. The transmission of each message block takes place in $\frac{T}{2}$ hops; see Figure 5.4. This is done as follows. In any given transmission block b of the source message, the closest pair of relays to the source decodes the bth message block transmitted by the source and forwards it (with the help of the source)

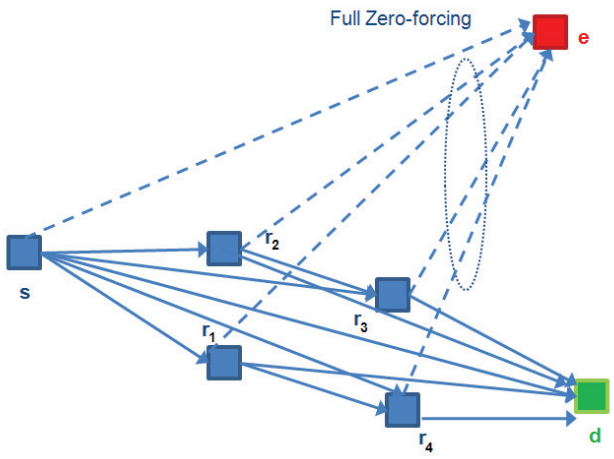

Figure 5.4: Multiple relay multiple hop strategy.

to the second closest pair of relays in the transmission block $b+1$ which decodes it and then forwards it (with the help of the source and the first pair of relays) to the third closest pair of relays[2] in the transmission block $b+2$ and so on so forth till the furthest pair of relays from the source decodes the bth message block and forwards it (with the help of the source and all the other relays) to the destination in the transmission block $b+\frac{T}{2}$. As in the previous subsection, since the multi-hop transmission is pipelined, the overhead is $\frac{T}{2}$ blocks. Hence, the loss in the achievable rate due to this overhead since $B >> T$. According to scenario described above, let the relays in the ith pair be labeled as $2i-1$ and $2i$, $1 \leq i \leq \frac{T}{2}$. In the case of the general discrete memoryless multiple relay channel with external eavesdropper given by some conditional distribution $p(y_1, ..., y_{T+1}, y_{T+2}|x_0, ..., x_T)$, by combining the results of the two previous subsections, it can be shown that the achievable secrecy

[2]Here, we mean closest to the source.

rate R^{DF} by such strategy for is given by

$$R^{DF} = \min \Bigg\{ \min_{j\in\{1,2\}} I(X_0; Y_j|X_{1,2}, ..., X_{T-1,T}), ...,$$
$$\min_{j\in\{2i-1,2i\}} I(X_0, X_{1,2}, ..., X_{2i-3,2i-2}; Y_j|X_{2i-1,2i}, ..., X_{T-1,T}), ...,$$
$$I(X_0, X_{1,2}, ..., X_{T-1,T}; Y_{T+1}) \Bigg\} - I(X_0, X_{1,2}, ..., X_{T-1,T}; Y_{T+2}) \quad (5.28)$$

for some auxiliary random variables $X_{1,2}, ..., X_{T-1,T}$ where $p(x_{1,2}, ..., x_{T-1,T}, x_0, x_1, ..., x_T)$ factors as $p(x_0|x_{1,2}, ..., x_{T-1,T}) \prod_{j=1}^{\frac{T}{2}} p(x_{2j-1}|x_{2j-1,2j}) p(x_{2j}|x_{2j-1,2j})$. For the Gaussian channel (5.10)-(5.12), we choose the channel inputs as follows. $X_0 = \tilde{X}_0 + \alpha_0 X_{1,2}$, $X_1 = X_{1,2}$, $X_2 = \beta_{1,2} X_{1,2}$, $X_{1,2} = \tilde{X}_{1,2} + \alpha_{1,2} X_{3,4}$, $X_3 = X_{3,4}$, $X_4 = \beta_{3,4} X_{3,4}$, $X_{3,4} = \tilde{X}_{3,4} + \alpha_{3,4} X_{5,6}$ and so on so forth, till $X_{T-1} = X_{T-1,T}$, $X_T = \beta_{T-1,T} X_{T-1,T}$, and $X_{T-1,T} = \tilde{X}_{T-1,T}$ where $\tilde{X}_0$ and all $\tilde{X}_{2i-1,2i}$, $i = 1, ..., \frac{T}{2}$ are independent circularly symmetric complex Gaussian random variables with zero mean an variances $\tilde{P}_0$ and $\tilde{P}_{2i-1,2i}$, $i = 1, ..., \frac{T}{2}$, respectively, and α_0, $\alpha_{2i-1,2i}$, $i = 1, ..., \frac{T}{2} - 1$, and $\beta_{2i-1,2i}$, $i = 1, ..., \frac{T}{2}$ are some complex numbers. Equivalently, we have

$$X_0 = \tilde{X}_0 + \alpha_0 \sum_{i=0}^{\frac{T}{2}-1} \left(\prod_{j=1}^{i} \alpha_{2j-1,2j} \right) \tilde{X}_{2j+1,2j+2} \quad (5.29)$$

and, for $\ell = 1, ..., \frac{T}{2}$, we have

$$X_{2\ell-1} = \sum_{i=\ell-1}^{\frac{T}{2}-1} \left(\prod_{j=1}^{i} \alpha_{2j-1,2j} \right) \tilde{X}_{2i+1,2i+2} \quad (5.30)$$

$$X_{2\ell} = \beta_{2\ell-1,2\ell} X_{2\ell-1} \quad (5.31)$$

where, whenever $i < j$, the product $\prod_{t=j}^{i}$ is set to 1 and the sum $\sum_{t=j}^{i}$ is set to 0. From (5.13), we must have

$$\tilde{P}_0 + |\alpha_0|^2 \sum_{i=0}^{\frac{T}{2}-1} \prod_{j=1}^{i} |\alpha_{2j-1,2j}|^2 \tilde{P}_{2i+1,2i+2} \leq \bar{P}_0 \tag{5.32}$$

and, for $\ell = 1, ..., \frac{T}{2}$,

$$\sum_{i=\ell-1}^{\frac{T}{2}-1} \prod_{j=1}^{i} |\alpha_{2j-1,2j}|^2 \tilde{P}_{2i+1,2i+2} \leq \bar{P}_{2\ell-1} \tag{5.33}$$

$$|\beta_{2\ell-1,2\ell}| \sum_{i=\ell-1}^{\frac{T}{2}-1} \prod_{j=1}^{i} |\alpha_{2j-1,2j}|^2 \tilde{P}_{2i+1,2i+2} \leq \bar{P}_{2\ell} \tag{5.34}$$

It follows that the achievable rate R^{DF} is given by

$$\begin{aligned}
R^{DF} = \min \Bigg\{ & \min_{t \in \{1,...,\frac{T}{2}\}} \Bigg\{ \min_{i \in \{2t-1,2t\}} \log \Big(1 + |h_{0i}|^2 \tilde{P}_0 \\
& + \sum_{\ell=1}^{t-1} \Big| \alpha_0 h_{0i} \prod_{j=1}^{\ell-1} \alpha_{2j-1,2j} + \sum_{k=1}^{\ell} (h_{2k-1,i} + \beta_{2k-1,2k} h_{2k,i}) \prod_{j=k}^{\ell-1} \alpha_{2j-1,2j} \Big|^2 \tilde{P}_{2\ell-1,2\ell} \Big) \Bigg\}, \\
& \qquad \log \Big(1 + |h_{0,T+1}|^2 \tilde{P}_0 \\
& + \sum_{\ell=1}^{\frac{T}{2}} \Big| \alpha_0 h_{0,T+1} \prod_{j=1}^{\ell-1} \alpha_{2j-1,2j} + \sum_{k=1}^{\ell} (h_{2k-1,T+1} + \beta_{2k-1,2k} h_{2k,T+1}) \prod_{j=k}^{\ell-1} \alpha_{2j-1,2j} \Big|^2 \tilde{P}_{2\ell-1,2\ell} \Big) \Bigg\} \\
& \quad - \log \Big(1 + |h_{0,T+2}|^2 \tilde{P}_0 \\
& + \sum_{\ell=1}^{\frac{T}{2}} \Big| \alpha_0 h_{0,T+2} \prod_{j=1}^{\ell-1} \alpha_{2j-1,2j} + \sum_{k=1}^{\ell} (h_{2k-1,T+2} + \beta_{2k-1,2k} h_{2k,T+2}) \prod_{j=k}^{\ell-1} \alpha_{2j-1,2j} \Big|^2 \tilde{P}_{2\ell-1,2\ell} \Big)
\end{aligned} \tag{5.35}$$

Now, we show that one can adjust the parameters in this strategy to fully eliminate

all the relays' signals from the eavesdropper observation and hence obtain a MRMH-DF strategy with full zero-forcing (MRMH-DF/FZF). First, we observe that the eavesdropper's observation is given by

$$
\begin{aligned}
Y_{T+2} &= h_{0,T+2}\tilde{X}_0 \\
&+ \sum_{\ell=1}^{\frac{T}{2}} \left(\alpha_0 h_{0,T+2} \prod_{j=1}^{\ell-1} \alpha_{2j-1,2j} + \sum_{k=1}^{\ell} (h_{2k-1,T+2} + \beta_{2k-1,2k} h_{2k,T+2}) \prod_{j=k}^{\ell-1} \alpha_{2j-1,2j} \right) \tilde{X}_{2\ell-1,2\ell} \\
&+ N_{T+2}
\end{aligned} \tag{5.36}
$$

Let ζ_ℓ denote the coefficient of $\tilde{X}_{2\ell-1,2\ell}$ in (5.36). One can verify that ζ_ℓ can be obtained recursively from $\zeta_{\ell-1}$ as follows

$$
\zeta_\ell = \alpha_{2\ell-3,2\ell-1}\zeta_{\ell-1} + h_{2\ell-1,T+2} + \beta_{2\ell-1,2\ell} h_{2\ell,T+2},\ \ell = 2, ..., \frac{T}{2} \tag{5.37}
$$

Thus, by setting $\beta_{2\ell-1,2\ell} = -\frac{h_{2\ell-1,T+2}}{h_{2\ell,T+2}}$, one can eliminate all the relays' signals from the eavesdropper observation. The rest of the parameters, i.e., $\alpha_0,\ \alpha_{2\ell-1,2\ell},\ 1 \leq \ell \leq \frac{T}{2}$ and the power values $\tilde{P}_0,\ \tilde{P}_{2\ell-1,2\ell},\ 1 \leq \ell \leq \frac{T}{2}$ should then be chosen to maximize the

achievable secrecy rate which is now given by

$$R^{DF/FZF} = \min\left\{ \min_{t\in\{1,\ldots,\frac{T}{2}\}} \left\{ \min_{i\in\{2t-1,2t\}} \log\left(1+|h_{0i}|^2\tilde{P}_0 \right.\right.\right.$$
$$\left.\left. + \sum_{\ell=1}^{t-1}\left|\alpha_0 h_{0i}\prod_{j=1}^{\ell-1}\alpha_{2j-1,2j} + \sum_{k=1}^{\ell}\left(h_{2k-1,i} - \frac{h_{2k-1,T+2}}{h_{2k,T+2}}h_{2k,i}\right)\prod_{j=k}^{\ell-1}\alpha_{2j-1,2j}\right|^2\tilde{P}_{2\ell-1,2\ell}\right)\right\},$$
$$\log\left(1+|h_{0,T+1}|^2\tilde{P}_0 \right.$$
$$\left. + \sum_{\ell=1}^{\frac{T}{2}}\left|\alpha_0 h_{0,T+1}\prod_{j=1}^{\ell-1}\alpha_{2j-1,2j} + \sum_{k=1}^{\ell}\left(h_{2k-1,T+1} - \frac{h_{2k-1,T+2}}{h_{2k,T+2}}h_{2k,T+1}\right)\prod_{j=k}^{\ell-1}\alpha_{2j-1,2j}\right|^2\tilde{P}_{2\ell-1,2\ell}\right)\right\}$$
$$- \log\left(1+|h_{0,T+2}|^2\tilde{P}_0\right) \tag{5.38}$$

5.4 Numerical Results

First, we consider the single relay DF strategy. We set $\bar{P}_1 = 10$, $h_{01} = \sqrt{2}$, and $h_{13} = h_{12} = h_{02} = 1$. In Figure 5.5, we plot both the achievable secrecy rate $R^{DF/ZF}$ by the DF/ZF strategy and the secrecy capacity C^{GWT} of the channel without a relay as functions of the source total power $\bar{P}_0$. We do this for two cases of the channel gain h_{03}, namely, $h_{03} = \sqrt{1.2}$ and $h_{03} = \sqrt{0.8}$. It is clear that, as Corollary 5.1 suggests, when $h_{01} > h_{03} > 1$, we have $R^{DF/ZF} > C^{GWT} = 0$ for all $\bar{P}_0$. On the other hand, when $h_{01} > 1 > h_{03}$, the DF/ZF strategy becomes useful when $\bar{P}_0$ is large enough.

Next, we consider the multiple relay model with T relays. We devise a simulation for the following experiment. Consider a two-dimensional coordinate system where the source (node 0) is located at the origin. The channel gain $h_{\ell k}$ between any two nodes ℓ and k is given by $h_{\ell k} = d_{\ell k}^{-\gamma} e^{j\theta_{\ell k}}$ where $d_{\ell k}$ is the distance between ℓ and k, $\gamma > 1$ is the path loss coefficient, and $\theta_{\ell k}$ accounts for independent phase fading

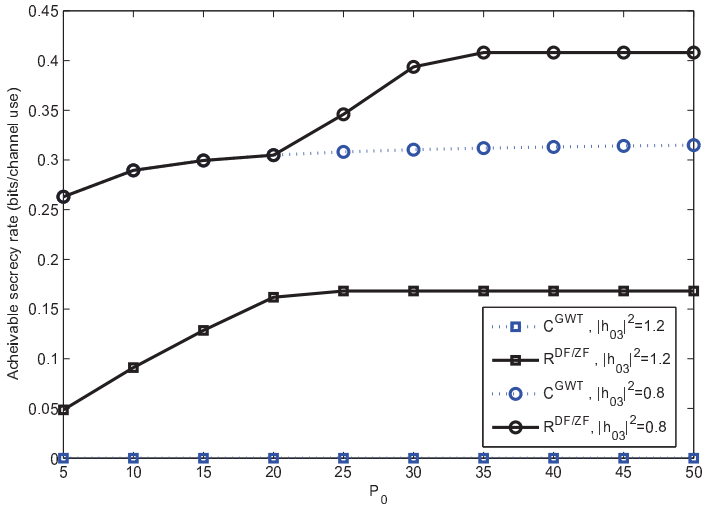

Figure 5.5: The achievable secrecy rate, $R^{DF/ZF}$, and the secrecy capacity of the original wiretap channel, C^{GWT}, versus the source's total power, $\bar{P}_0$, for two cases of h_{03}.

and is uniformly and independently distributed over $[0, 2\pi)$ for all ℓ, k. We choose $d_{0,T+1} = d_{0,T+2} = 1$ km and take $\gamma = 3$. We use a constant power allocation policy at all the relays where the transmit powers of all the relays are set to $\bar{P}_r = 10$ and accordingly power is allocated at the source to maximize the achievable rate where the total average power at the source is set to $\bar{P}_0 = 50$. We consider two scenarios. In the first scenario, all the T relays are uniformly spread over a disc of radius 0.75 km centered at the source. In the second scenario, all the T relays are at the same distance of 0.5 km from the source.

In Figure 5.6, we plot the achievable secrecy rate by each of the proposed multiple-relay strategies, the MRSH-DF/ZF, the MRMH-DF/PZF, and the MRMH-DF/FZF strategies, for $T = 1, ..., 10$. Figure 5.6 shows that the MRMH-DF/PZF strategy usually achieves higher rates than the MRSH-DF/ZF strategy when there is a noticeable

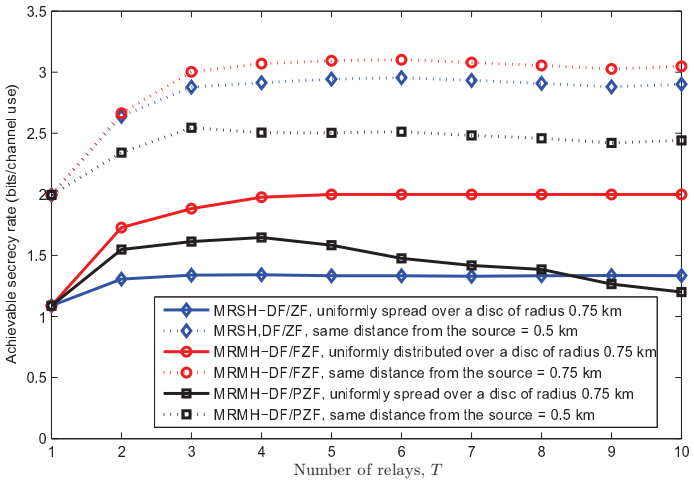

Figure 5.6: The achievable secrecy rate by the MRSH-DF, the MRMH-DF/PZF, and the MRMH-DF/FZF strategies versus the number of relays, T, for two cases.

variation in the magnitudes of the channel gains $h_{0,k},\ k \in \mathcal{T}$ between the source and the relays which is the case captured by the first scenario. However, since in the MRMH-DF/PZF strategy, we can eliminate only half of the signal terms from the eavesdropper's observation, as T increases, the MRMH-DF/PZF strategy becomes less efficient due to the increase in the number of signal components observed at the eavesdropper. One can also see that the MRSH-DF/ZF strategy is usually better than the MRMH-DF/PZF strategy when the amount of variation in the magnitudes of the channel gains between the source and the relays is small. This is clearly captured by the second scenario, where all such channel gains have the same magnitude. On the other hand, one can see the superiority of the rate achieved by the MRMH-DF/FZF strategy in both of the examples. This indeed is due to the fact that the MRMH-DF/FZF strategy enjoys the advantages of the two previous strategies with almost insignificant loss in the achievable rate in the typical situations.

5.5 Conclusions

In this chapter, we considered the notion of active cooperation in relay networks with secrecy constraint. We first studied the decode-and-forward strategy for secrecy in a single relay network. We proposed a suboptimal decode-and-forward with zero-forcing (DF/ZF) strategy for which we obtained the optimal power control policy. For the multiple relay problem, we proposed three different strategies based on decode-and-forward with zero-forcing. The first strategy is a single hop strategy. We gave the achievable rate by this strategy. We showed that all the relays' signals can be eliminated at the eavesdropper (full zero-forcing) and derived the optimal power control policy in this case. We showed that the rate achieved by this strategy suffers from a bottleneck created by the worst source-relay channel. The second strategy is a multiple hop strategy that was shown to overcome the drawback of the first strategy, however, with the disadvantage of enabling partial zero-forcing only assuming that all the relays are required to transmit fresh information in every transmission block. In the third strategy which is also a multiple hop strategy, it was shown that full zero-forcing is possible and the rate achieved does not suffer from the drawback of the first strategy. Finally, we gave numerical examples to illustrate the performance of each of the proposed strategies in terms of the achievable rates.

5.6 Appendix

5.6.1 Proof of Theorem 5.1

Define

$$R_1^{DF/ZF} = \log\left(\frac{1+|h_{01}|^2\tilde{P}_0}{1+|h_{03}|^2\tilde{P}_0}\right) \tag{5.39}$$

$$R_2^{DF/ZF} = \log\left(\frac{1+\tilde{P}_0+|\alpha^{ZF}+1|^2P_1}{1+|h_{03}|^2\tilde{P}_0}\right) \tag{5.40}$$

Hence, from (5.9), we have

$$R^{DF/ZF} = \min\left\{R_1^{DF/ZF},\ R_2^{DF/ZF}\right\} \tag{5.41}$$

Let $\bar{R}^{DF/ZF}$ denote the maximum value of $R^{DF/ZF}$ over the constraint set given by (5.6) where $\alpha_0 = \alpha^{ZF} = -\frac{h_{13}}{h_{03}}$. Recall that the secrecy capacity of the original Gaussian wiretap channel without a relay C^{GWT} is given by (5.8). First, we observe that if $|h_{01}| \leq |h_{03}|$ then the maximum value of $R_1^{DF/ZF}$ is zero and is attained at $\tilde{P}_0 = 0$. Hence, $\bar{R}^{DF/ZF} = 0 \leq C^{GWT}$ and in this case, we can set $P_1 = 0$. On the other hand, if $|h_{03}| < |h_{01}| \leq 1$, then for all $\tilde{P}_0, P_1$, we have $R^{DF/ZF} = R_1^{DF/ZF} \leq C^{GWT} = \log\left(\frac{1+\bar{P}_0}{1+|h_{03}|^2\bar{P}_0}\right)$ with equality attained if and only if $\tilde{P}_0 = \bar{P}_0$ and $P_1 = 0$.

Next, we turn to the case where $|h_{01} > \max\{1, |h_{03}|\}|$ which will be assumed in the rest of the proof. One can easily note that $R_1^{DF/ZF}$ (which does not depend on P_1) is a strictly increasing function in $\tilde{P}_0$ and that for every $\tilde{P}_0$, $R_2^{DF/ZF}$ is strictly increasing in P_1. However, the behavior of $R_2^{DF/ZF}$ as a function of $\tilde{P}_0$ for fixed P_1

depends on the power constraints $\bar{P}_0,\ \bar{P}_1$, and the channel gains $|h_{01}|,\ |h_{03}|,\ |h_{13}|$. Since both $R_1^{DF/ZF}$ and $R_2^{DF/ZF}$ are non-decreasing in P_1, then so is $R^{DF/ZF}$. Hence, from (5.6), for every $\tilde{P}_0$, one can express the optimal power P_1 as a function of $\tilde{P}_0$, namely,

$$P_1^{\star}\left(\tilde{P}_0\right) = \min\left\{\bar{P}_1, \frac{\bar{P}_0 - \tilde{P}_0}{|\alpha^{ZF}|^2}\right\} \tag{5.42}$$

Hence, $R_2^{DF/ZF}$ could be written, without loss of optimality, as a function of $\tilde{P}_0$ only as follows

$$R_2^{DF/ZF} = \log\left(\frac{1+\tilde{P}_0+|1+\alpha^{ZF}|^2\bar{P}_1}{1+|h_{03}|^2\tilde{P}_0}\right), \quad \text{if } 0 \le \tilde{P}_0 \le \left(\bar{P}_0 - |\alpha^{ZF}|^2\bar{P}_1\right)^+ \tag{5.43}$$

$$R_2^{DF/ZF} = \log\left(\frac{1+|1+\frac{1}{\alpha^{ZF}}|^2\bar{P}_0+\left(1-|1+\frac{1}{\alpha^{ZF}}|^2\right)\tilde{P}_0}{1+|h_{03}|^2\tilde{P}_0}\right),$$

$$\text{if } \left(\bar{P}_0 - |\alpha^{ZF}|^2\bar{P}_1\right)^+ \le \tilde{P}_0 \le \bar{P}_0 \tag{5.44}$$

where $(x)^+$ denotes $\max\{0, x\}$ for any real number x. Consequently, the derivative

of $R_2^{DF/ZF}$ with respect to $\tilde{P}_0$ is given by

$$\frac{\partial R_2^{DF/ZF}}{\partial \tilde{P}_0} = \frac{1-|h_{03}|^2-|h_{03}|^2|1+\alpha^{ZF}|^2\bar{P}_1}{\left(1+\tilde{P}_0+|1+\alpha^{ZF}|^2\bar{P}_1\right)\left(1+|h_{03}|^2\tilde{P}_0\right)}, \quad 0 \le \tilde{P}_0 \le \left(\bar{P}_0-|\alpha^{ZF}|^2\bar{P}_1\right)^+ \tag{5.45}$$

$$\frac{\partial R_2^{DF/ZF}}{\partial \tilde{P}_0} = \frac{1-|1+\frac{1}{\alpha^{ZF}}|^2-|h_{03}|^2-|h_{03}|^2|1+\frac{1}{\alpha^{ZF}}|^2\bar{P}_0}{\left(1+|1+\frac{1}{\alpha^{ZF}}|^2\bar{P}_0+\left(1-|1+\frac{1}{\alpha^{ZF}}|^2\right)\tilde{P}_0\right)\left(1+|h_{03}|^2\tilde{P}_0\right)}, \quad \left(\bar{P}_0-|\alpha^{ZF}|^2\bar{P}_1\right)^+ \le \tilde{P}_0 \le \bar{P}_0 \tag{5.46}$$

This leads to the four cases in Theorem 5.1 which we will prove below.

- Case (1): The second condition of this case implies that for all $0 \le \tilde{P}_0 \le \bar{P}_0$, $R_2^{DF/ZF}$ and $\frac{\partial R_2^{DF/ZF}}{\partial \tilde{P}_0}$ are given by (5.44) and (5.46), respectively. The first condition of this case implies that $\frac{\partial R_2^{DF/ZF}}{\partial \tilde{P}_0} \ge 0$. Thus, both $R_1^{DF/ZF}$ and $R_2^{DF/ZF}$ are increasing in $\tilde{P}_0$ and hence $\bar{R}^{DF/ZF}$ is attained at $\tilde{P}_0 = \tilde{P}_0^\star = \bar{P}_0$ which, by (5.42), implies that $P_1^\star = 0$. Moreover, in this case, it is clear that at the optimal power values $\bar{R}^{DF/ZF} = R_2^{DF/ZF} = C^{GWT}$.

- Case (2): Similar to case (1), the second condition of this case implies that for all $0 \le \tilde{P}_0 \le \bar{P}_0$, $R_2^{DF/ZF}$ and $\frac{\partial R_2^{DF/ZF}}{\partial \tilde{P}_0}$ are given by (5.44) and (5.46), respectively. However, the first condition of this case implies that $\frac{\partial R_2^{DF/ZF}}{\partial \tilde{P}_0} < 0$. Thus, $R_1^{DF/ZF}$ is strictly increasing in $\tilde{P}_0$ whereas $R_2^{DF/ZF}$ is strictly decreasing in $\tilde{P}_0$. Therefore, $\bar{R}^{DF/ZF}$ is attained at when $R_1^{DF/ZF} = R_2^{DF/ZF}$ which gives the optimal power values $\tilde{P}_0^\star = \frac{|1+\frac{1}{\alpha^{ZF}}|^2}{|h_{01}|^2-1+|1+\frac{1}{\alpha^{ZF}}|^2}\bar{P}_0$ and $P_1^\star = \frac{\bar{P}_0-\tilde{P}_0^\star}{|\alpha^{ZF}|^2}$. We also note that at $\tilde{P}_0 = \bar{P}_0$, we have $R_2^{DF/ZF} = C^{GWT}$. This together with the fact

that $R_2^{DF/ZF}$ is strictly decreasing in $\tilde{P}_0$ implies that $\bar{R}^{DF/ZF}$ is strictly larger than C^{GWT}.

- Case (3): In this case, one can easily verify from (5.45) and (5.46) that $\frac{\partial R_2^{DF/ZF}}{\partial \tilde{P}_0} \geq 0$ for all $0 \leq \tilde{P}_0 \leq \bar{P}_0$. Hence, both $R_1^{DF/ZF}$ and $R_2^{DF/ZF}$ are increasing in $\tilde{P}_0$. Thus, $\tilde{P}_0^{\star}$, $P_1^{\star}$, and $\bar{R}^{DF/ZF}$ are the same as in case (1).

- Case (4):

  - Case (4-a): In this case, one can verify from (5.45) and (5.46) that $\frac{\partial R_2^{DF/ZF}}{\partial \tilde{P}_0} > 0$ whenever $0 \leq \tilde{P}_0 \leq \bar{P}_0 - |\alpha^{ZF}|^2 \bar{P}_1$ and $\frac{\partial R_2^{DF/ZF}}{\partial \tilde{P}_0} < 0$ whenever $\bar{P}_0 - |\alpha^{ZF}|^2 \bar{P}_1 < \tilde{P}_0 \leq \bar{P}_0$. This implies that $R_2^{DF/ZF}$ attains its local maximum at $\tilde{P}_0 = \bar{P}_0 - |\alpha^{ZF}|^2 \bar{P}_1$. Moreover, in this case, $R_2^{DF/ZF} < R_1^{DF/ZF}$ at $\tilde{P}_0 = \bar{P}_0 - |\alpha^{ZF}|^2 \bar{P}_1$. Hence, $\bar{R}^{DF/ZF}$ is attained at $\tilde{P}_0^{\star} = \bar{P}_0 - |\alpha^{ZF}|^2 \bar{P}_1$ and at such point $R_2^{DF/ZF} = \bar{R}^{DF/ZF}$. Since $R_2^{DF/ZF}$ is strictly decreasing in $\tilde{P}_0$ for $\bar{P}_0 - |\alpha^{ZF}|^2 \bar{P}_1 < \tilde{P}_0 \leq \bar{P}_0$ and since $R_2^{DF/ZF} = C^{GWT}$ at $\tilde{P}_0 = \bar{P}_0$, then we must have $\bar{R}^{DF/ZF} > C^{GWT}$.

  - Case (4-b): In this case, from (5.45) and (5.46), we have $\frac{\partial R_2^{DF/ZF}}{\partial \tilde{P}_0} < 0$ for all $0 \leq \tilde{P}_0 \leq \bar{P}_0$. It follows that the optimal power value $\tilde{P}_0^{\star}$ is obtained by solving $R_1^{DF/ZF} = R_2^{DF/ZF}$ in $\tilde{P}_0$. In this case, we note that $R_1^{DF/ZF} = R_2^{DF/ZF}$ happens when $R_2^{DF/ZF}$ is given by (5.43), and hence $\tilde{P}_0^{\star} = \frac{|1+\alpha^{ZF}|^2}{|h_{01}|^2 - 1} \bar{P}_1$. It follows from (5.42) that $P_1^{\star} = \bar{P}_1$. At the optimal power values, we have $R_2^{DF/ZF} = \bar{R}^{DF/ZF}$. This together with the fact that $R_2^{DF/ZF}$ is strictly decreasing in $\tilde{P}_0$ for $0 \leq \tilde{P}_0 \leq \bar{P}_0$ and the fact that at $\tilde{P}_0 = \bar{P}_0$, we have $R_2^{DF/ZF} = C^{GWT}$, it follows that $\bar{R}^{DF/ZF} > C^{GWT}$.

– Case (4-c): In this case, one can easily verify that $R_2^{DF/ZF}$ is strictly decreasing in $\tilde{P}_0$ for $\bar{P}_0 - |\alpha^{ZF}|^2\bar{P}_1 < \tilde{P}_0 \leq \bar{P}_0$ and that $R_1^{DF/ZF} = R_2^{DF/ZF}$ happens when $R_2^{DF/ZF}$ is given by (5.44), i.e., the value of $\tilde{P}_0$ at which $R_1^{DF/ZF} = R_2^{DF/ZF}$ is greater than or equal to $\bar{P}_0 - |\alpha^{ZF}|^2\bar{P}_1$. Hence, this value of $\tilde{P}_0$ must be the optimal power value $\tilde{P}_0^{\star}$. As in case (2), this optimal value is given by $\tilde{P}_0^{\star} = \frac{|1+\frac{1}{\alpha^{ZF}}|^2}{|h_{01}|^2-1+|1+\frac{1}{\alpha^{ZF}}|^2}\bar{P}_0$ which, by (5.42), implies that $P_1^{\star} = \frac{\bar{P}_0-\tilde{P}_0^{\star}}{|\alpha^{ZF}|^2}$. Again, like in cases (2),(4-a), and (4-b), one can show that $\bar{R}^{DF/ZF} > C^{GWT}$.

Chapter 6

Conclusions

In this dissertation, we studied two important notions related to physical-layer security in wireless multi-user channels, namely, alignment and cooperation. Studying these two notions gives rise to a useful set of tools that exploits the physical properties of the wireless channel, e.g., its fading and broadcast nature, to achieve and reinforce information-theoretic security in wireless networks. Towards this end, we studied the fading multiple access wiretap channel and the cooperative relay channel with security constraints and proposed new schemes that efficiently exploit these notions and apply them in the physical layer to achieve high secure rates over these channels.

For the fading multiple access wiretap channel, we proposed two schemes based on signal alignment either by using code repetition and signal scaling at the transmitters (the SBA scheme), or by code repetition over carefully chosen channel uses (the ESA scheme). We showed that, unlike the schemes based only on i.i.d. Gaussian signaling, our schemes yield secure rates that scale with the signal-to-noise ratio. In particular, we showed that, in the K-user fading multiple access wiretap channel, we can achieve a total of $\frac{K-1}{K}$ degrees of freedom. We gave an improved version of our second scheme by incorporating the cooperative jamming technique. We also discussed the optimal

power control policies for our schemes.

For the cooperative Gaussian relay channel, we investigated the concept of deaf cooperation to improve the secrecy capacity of the main Gaussian wiretap channel. We studied two different modes of deaf cooperation, namely, cooperative jamming and noise forwarding. We obtained the necessary conditions for each of the two modes to improve over the secrecy capacity of the main wiretap channel. Hence, we showed that a node cannot be both a useful jammer and a useful noise forwarder at the same time. We derived the optimal power control policy for each of the two modes. For the deaf helper selection problem, we proposed a selection strategy in which multiple deaf helpers operating in different modes are selected to increase the achievable secure rate of the source. We showed that this selection strategy requires reasonable number of computations.

We studied the two modes of deaf cooperation when the relay node is equipped with multiple antennas. We gave two deaf cooperation strategies in which the relay decomposes his channel to the eavesdropper into two components and it uses the component orthogonal to the destination's channel for cooperative jamming while it uses the component in the direction of the destination's channel for either cooperative jamming or noise forwarding. We derived the necessary conditions under which cooperative jamming along the direct component is better in terms of the achievable rate than noise forwarding along the direct component and vice versa. We derived the optimal power control policy in each case. For the reversely degraded relay-eavesdropper channel, we showed that, by using a simple strategy in which the relay jams with full power along the orthogonal component, we approach the secrecy capacity of this

channel as we increase the relay's power.

Finally, we considered active cooperation in relay networks with security constraints. We focused on the decode-and-forward scheme for active cooperation. For the single relay problem, we proposed a zero-forcing strategy in which the relay signal is eliminated from the eavesdropper's observation. We derived the optimal power allocation policy for this strategy. For the multiple relay problem, we proposed three decode-and-forward based strategies. For the first strategy, which is a single hop strategy, we showed that full zero-forcing is possible, however, the rate achievable by this strategy suffers from a bottleneck caused by the worst source-relay channel. We showed that the second strategy, which is a multiple hop strategy, overcomes this drawback, however, only partial zero-forcing is possible. The third strategy, which is also a multiple hop strategy, was shown to be a good compromise since the achievable rate is not limited by the worst source-relay channel and full zero-forcing is possible.

Our results not only serve a theoretical purpose by showing that we can provide and improve security from the physical layer using the techniques of alignment and cooperation but also serve a practical purpose by studying the practical aspects of the proposed schemes and the practical considerations that should be taken into account when these schemes are implemented in a wireless communication system. However, throughout this dissertation, we made a standard assumption that is usually made in the related work in this area. Namely, we assumed that the global channel state information including the eavesdropper's channel state information is available at all the nodes in a causal fashion. Providing security when nothing is known about the eavesdropper's channel state information is a challenging task especially in scalar channels.

BIBLIOGRAPHY

[1] S. O. Gharan A. S. Motahari and A. K. Khandani. Real interference alignment with real numbers. *IEEE Trans. on Inf. Theory*, Aug. 2009. Submitted. Also available at [arXiv:0908.1208v2].

[2] G. Bagherikaram, A. S. Motahari, and A. K. Khandani. On the secure degrees of freedom of the multiple access channel. In *IEEE International Symposium on Inf. Theory ISIT, Austin, TX*, Jun. 2010. Also available at [arXiv:1003.0729].

[3] V. R. Cadambe and S. A. Jafar. Interference alignment and degrees of freedom of the k-user interference channel. *IEEE Trans. on Inf. Theory*, 54(8):3425–3441, Aug. 2008.

[4] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Trans. on Inf. Theory*, 24(3):339–348, May 1978.

[5] E. Ekrem and S. Ulukus. Cooperative secrecy in wireless communications. *Securing Wireless Communications at the Physical Layer*. W. Trappe and R. Liu, Eds., Springer-Verlag, 2009.

[6] E. Ekrem and S. Ulukus. On the secrecy of multiple access wiretap channel. In *46th Annual Allerton Conference on Communication, Control and Computing*, Sep. 2008.

[7] T. Gou and S. A. Jafar. On the secure degrees of freedom of wireless X networks. In *46th Annual Allerton Conference on Communication, Control and Computing, UIUC, IL*, pages 826–833, Sep. 2008.

[8] X. He and A. Yener. K-user interference channels: Achievable secrecy rate and degrees of freedom. In *IEEE ITW'09, Volos*, Jun. 2009.

[9] X. He and A. Yener. Secure degrees of freedom for Gaussian channels with interference: Structured codes outperform Gaussian signaling. In *IEEE Globecom*, 2009. Also available at [arXiv:0905.2638].

[10] A. Khisti and G. Wornell. Secure transmission with multiple antenna: The MISOME wiretap channel. *IEEE Trans. on Inf. Theory*, 56(7):3088–3104, July 2010.

[11] A. Khisti and G. Wornell. Secure transmission with multiple antenna: The MIMOME channel. *IEEE Trans. on Inf. Theory*, To appear. Also available at [arXiv:0710.1325].

[12] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor. Interference alignment for secrecy. *IEEE Trans. on Inf. Theory*, 57(6):3323–3332, Jun. 2011.

[13] S. Leung-Yan-Cheong and M. E. Hellman. The Gaussian wire-tap channel. *IEEE Trans. on Inf. Theory*, 24(4):451–456, Jul. 1978.

[14] B. Nazer, M. Gastpar, S. A. Jafar, and S. Vishwanath. Ergodic interference alignment. In *IEEE ISIT, Seoul, Korea*, Jun. 2009.

[15] F. Oggier and B. Hassibi. The secrecy capacity of the MIMO wiretap channel. *IEEE Trans. on Inf. Theory*, 57(8):4961–4972, August 2011.

[16] N. Liu S. Shafiee and S. Ulukus. Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel. *IEEE Trans. on Inf. Theory*, 55(9):4033–4039, Sep. 2009.

[17] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28:656–715, 1949.

[18] E. Tekin and A. Yener. Secrecy sum-rates for the multiple-access wire-tap channel with ergodic block fading. In *45th Annual Allerton Conference on Communication, Control and Computing*, pages 856–863, Sep. 2007.

[19] E. Tekin and A. Yener. The Gaussian multiple access wiretap channel. *IEEE Trans. on Inf. Theory*, 54(12):5747–5755, Dec. 2008.

[20] E. Tekin and A. Yener. The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming. *IEEE Trans. on Inf. Theory*, 54(6):2735–2751, Jun. 2008.

[21] A. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54(8):1355–1387, Jan. 1975.

[22] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao. Joint relay and jammer selection for secure two-way relay networks. In *IEEE ICC 2011, Kyoto, Japan*, Jun. 2011.

[23] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor. Cooperative jamming for wireless physical layer security. In *15th IEEE Workshop on Statistical Signal Processing*, pages 417–420, Sep. 2009.

[24] L. Dong, H. Yousefi'zadeh, and H. Jafarkhani. Cooperative jamming and power allocation for wireless relay networks in presence of eavesdropper. In *IEEE ICC 2011, Kyoto, Japan*, Jun. 2011.

[25] J. Huang and A. L. Swindlehurst. Secure communications via cooperative jamming in two-hop relay systems. In *IEEE GLOBECOM 2010, Miami, FL.*, Dec. 2010.

[26] J. Huang and A. L. Swindlehurst. Cooperation strategies for secrecy in mimo relay networks with unknown eavesdropper csi. In *ICASSP 2011, Prague, Czech Republic*, pages 3424–3427, May 2011.

[27] I. Krikidis, J. Thompson, and S. McLaughlin. Relay selection for secure cooperative networks with jamming. *IEEE Trans. on Wireless Comm.*, 8(10):5003–5011, Oct. 2009.

[28] L. Lai and H. El Gamal. Cooperation for secure communication: The relay wiretap channel. In *ICASSP 2007, Honolulu, HI*, pages III 149 – III 152, April 2007.

[29] L. Lai and H. El Gamal. Cooperation for secrecy: The relay-eavesdropper channel. *IEEE Trans. on Inf. Theory*, 54(9):4005–4019, Sep. 2008.

[30] L. Lai, H. El Gamal, and H. V. Poor. The wiretap channel with feedback: Encryption over the channel. *IEEE Trans. on Inf. Theory*, 54(11):5059–5067, Nov. 2008.

[31] R. Negi and S. Goel. Secret communication using artificial noise. In *IEEE Vehicular Technology Conference*, Sep. 2005.

[32] E. Perron, S. Diggavi, and E. Telatar. On cooperative secrecy for discrete memoryless relay networks. In *IEEE ISIT 2010, Austin, TX*, pages 2573–2577, Jun. 2010.

[33] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor. Interference-assisted secret communication. In *IEEE Information Theory Workshop*, May 2008.

[34] E. Tekin and A. Yener. Achievable rates for the general Gaussian multiple access wiretap channel with collective secrecy. In *44th Annual Allerton Conference on Communication, Control and Computing, UIUC, IL*, Sep. 2006.

[35] S. Vasudevan, S. Adams, D. Goeckel, Z. Ding, D. Towsley, and K. K. Leung. Secrecy in wireless relay channels through cooperative jamming. In *ACITA 2010*, Sep. 2010. Also available at: http://www.eecs.berkeley.edu/∼shadams/docs/SecrecyInWirelessRelayChannels.pdf.

[36] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin. Friendly jamming for wireless secrecy. In *IEEE ICC 2010, Capetown, South Africa*, May 2010.

[37] J. P. Vilela, P. C. Pinto, and J. Barros. Jammer selection policies for secure wireless networks. In *IEEE ICC 2011, Kyoto, Japan*, Jun. 2011.

[38] T. Cover and A. El Gamal. Capacity theorems for the relay channel. *IEEE Trans. on Inf. Theory*, 25:572–584, Sep. 1979.

[39] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor. Secure wireless communications via cooperation. In *46th Annual Allerton Conference on Communications, Control and Computing, Monticello, IL*, Sep. 2008.

[40] G. Kramer, M. Gastpar, and P. Gupta. Cooperative Strategies and Capacity Theorems for Relay Networks. In *IEEE Trans. on Inf. Theory*, 51(9):3037–3063, Sep. 2005.

[41] P. Gupta and P. R. Kumar. Towards an information theory of large networks: an achievable rate region. In *IEEE Trans. on Inf. Theory*, 49(8):1877–1894, Aug. 2003.

[42] T. Liu and S. Shamai. A note on the secrecy capacity of the multiple-antenna wiretap channel. *IEEE Trans. on Inf. Theory*, 55(6):2547–2553, Jun. 2009.

[43] J. Zhang and M. C. Gursoy. Collaborative relay beamforming for secrecy. *EURASIP Journal on Advances in Signal Processing*, Aug. 2010. Submitted.

[44] T. M. Cover and J. A. Thomas. Elements of Information Theory. *John Wiley and Sons*, 2nd ed., 2006.

[45] D. Tse and P. Viswanath. Fundamentals of Wireless Communication. *Cambridge University Press*, 2005.