Robust and Secure Beamformer Design for MIMO Relaying with Imperfect Eavesdropper CSI

Nadim Badra

Department of Electrical and Computer Engineering
McGill University
Montreal, Canada
November 2016

A thesis submitted to McGill University in partial fulfillment of the requirements for the degree of Master of Engineering.

Abstract

This thesis presents a computationally efficient beamforming approach to combat wiretapping in a relay-based multiple-input multiple output (MIMO) communication system which is part of a cognitive radio (CR) network. The system operates in two stages, that is, multiple-access (MA) followed by broadcasting (BC) using physical layer network coding (PNC). The beamforming design is based on minimizing the mean square error (MSE) at the receiving node(s) while enforcing signal-to-interference-plus-noise ratio (SINR) constraints at the eavesdroppers. The constraints take into account uncertainty bounds on eavesdropper channel estimation errors. In each stage of communication, an optimization problem is devised and solved using an iterative procedure, considering two different types of eavesdropper functionality, i.e., selection combining and "blind" beamforming. Numerical results show the convergence of the MSE at the destinations and the SINR distributions at the eavesdroppers for both cases. Results are also compared to those of previously suggested solutions for blind beamforming showing improvements in MSE values in the MA stage as well as in computational efficiency in both stages.

Sommaire

Cette thèse présente une approche efficace de filtrage spatial pour lutter contre les écoutes illicites dans un système de communication basé sur un modèle de transmission ayant plusieurs entrées et plusieurs sorties (MIMO) et faisant partie d'un réseau de radio cognitive (CR). Le système opère en deux étapes, soit tout d'abord une phase d'accès multiple (MA), suivi d'une phase de radiodiffusion (BC) utilisant un encodage réseau de couche physique (PNC). La conception du filtrage spatial est basée sur une minimisation de l'erreur-quadratique-moyenne (MSE) au niveau des nœuds de réception, tout en contraignant le rapport de puissance du signal-sur-interférence-plus-bruit au niveau des oreilles indiscrètes (espionnage) (SINR). Les contraintes prennent en considération l'incertitude des erreurs d'estimations sur les bornes des canaux d'espionnage. Dans chaque étape de la communication, un problème d'optimisation est formulé puis résolu en utilisant une procédure itérative, tenant compte de deux types de fonctionnalités d'espionnage différentes, à savoir, la combinaison sélective et la séparation à l'≪ aveugle ≫ du faisceau. Les résultats numériques démontrent la convergence de la MSE aux destinataires légitimes et la distribution du SINR aux oreilles indiscrètes, et ce dans les deux cas. Les résultats sont également comparés aux solutions précédemment suggérées pour filtrage spatial aveugle et présentent des améliorations dans les valeurs de la MSE dans la phase MA et une réduction du temps de calcul dans les deux cas.

Acknowledgments

Many thanks go to my supervisors, Professors Ioannis Psaromiligkos and Benoit Champagne, for putting me in the right direction and sharing their invaluable insights. This work was accomplished due to their helpful advice in the past two years. I would also like to thank my colleague Jiaxin Yang for his much appreciated assistance. I must acknowledge Mitacs and InterDigital Canada Ltée for their financial support and my internship supervisor Mr. Benoit Pelletier for everything he taught me. Special gratitude goes to my family in Montreal and Boston who were always there for me. Last, but not least, I thank my parents for giving me the motivation I need and being my support system throughout this journey. Without them, nothing would have been possible and to them goes my sincerest love — *Dedicated to my late Grandmother and Uncle.*

Contents

List of Figures

List of Tables

Preface

The work done in this thesis led to the following publication:

N. Badra, J. Yang, I. Psaromoligkos, B. Champagne, "Robust and secure beamformer design for MIMO relaying with imperfect eavesdropper CSI, in "*Proc. of the* 2^{nd} *Int. Workshop on Cognitive Radio and Electromagnetic Spectrum Security (CRESS)*, Philadelphia, PA, USA, October 2016.

My colleague Jiaxin Yang, a PhD candidate at McGill University and a co-author of the above paper, provided valuable assistance in the application of optimization theory and in the use of various software tools for numerically solving optimization problems.

Chapter 1

Introduction

As the number of data applications for mobile users continues to expand, cognitive radio (CR) keeps gaining interest for upcoming generations of cellular networks. CR technology can improve the utility of the licensed spectrum by allowing secondary users to access spectrum holes that are unoccupied by primary users. In effect, a CR device can operate in an underlay mode where it transmits simultaneously with the primary user, as long as the interference caused to the latter is limited [1, 2].

Recently, as an extension of these concepts, device-to-device (D2D) communication has also attracted considerable attention for cellular network applications as it may increase spectral efficiency for high data rate services in addition to enhanced throughput, energy efficiency, delay and fairness [3, 4]. D2D, inspired in part by the work in [5] and references therein, allows user devices in a cellular network to communicate or relay information signals without the need to forward them to an access point or base station. D2D is currently being investigated for specific cases in the context of fourth (4G) and fifth generation (5G) of cellular networks by the 3GPP standardization body [3]. D2D is also being suggested for special applications such as multicasting, peer-to-peer communication, video dissemination, machine-to-machine (M2M) communication and cellular offloading [6–11].

Meanwhile, relay-based communication can be beneficial in extending coverage areas

and reducing transmit power consumption. Cooperative relays in CR and D2D networks offer significant advantages, as they can forward data from a source node to a destination node by using spectrum holes that they have sensed [12]. However, transmission scheduling schemes are needed to avoid interference of signals sent from different nodes to the relay. Physical layer network coding (PNC), proposed in [13], makes use of the additive nature of concurrent incoming waves for identical coding operation. PNC-based two-way relaying can achieve 100% improvement in physical layer throughput over the traditional multi-hop transmission scheduling scheme and 50% over the straightforward network coding scheme as outlined in [14].

Broadcasting signals makes them unprotected from illegitimate receivers that attempt to decode the data. The security aspects of CR systems [15, 16] have attracted increasing attention from the research community since legitimate CR devices can become exposed to eavesdroppers which can intercept confidential information. While key-based enciphering has been the conventional data transmission security scheme, physical layer security (PLS) has gained considerable interest recently. PLS avails the noise and channel randomness to prevent eavesdroppers from decoding information at the bit level with well-designed coding and transmit precoding schemes. In this way, PLS complements already existing security procedures applied in higher layers of the communication protocol stack [17].

In the literature, secrecy for multiple-input multiple-output (MIMO) systems was studied using different schemes and considering different channel state information (CSI) availability cases. When no CSI is available, waterfilling on the main channel is applied. When the statistics of the CSI are available, broadcasting artificial noise (AN) is employed [18]. Meanwhile, if full instantaneous CSI is available transmit precoding based on the generalized singular value decomposition is favored [19]. The scheme that uses more CSI produces a better secrecy rate performance [3]. Security for MIMO amplify-and-forward (AF) relaying was investigated recently in [20,21] where the relay AF matrix is optimized, subject to power constraints, in order to maximize the received signal-to-interference-

plus-noise ratio (SINR) at the destination while satisfying a set of secrecy constraints. Beamforming methods using sufficient power to ensure a certain SINR at the authorized receivers were studied in [22–28], with the remaining available power used to broadcast artificial noise (AN) orthogonal to the authorized receivers thereby degrading the quality of the eavesdropper's signal. Beamformer optimization based on the secrecy rate was studied in [29–31], while the design for quality of service discrimination in two-way relay networks was investigated in [32]. The authors in [33] presented the design of transmit and receive beamformers that minimize the mean-square-error (MSE) between authorized parties subject to the constraint that the MSE at the eavesdropper is above a threshold. Additionally, an overview of the PLS aspects of CR networks was provided in [34], where several security attacks as well as the related countermeasures were discussed. PLS for D2D MIMO relaying was examined in [35] with multiple eavesdroppers and imperfect eavesdropper CSI and a random channel estimation error model. The eavesdroppers were assumed to be blind, i.e., having no CSI available and not knowing the transmit beamformers. Since the eavesdropper channel estimation error was assumed random, the approach minimized the destination's MSE so that the mean of the SINR at the eavesdropper is kept below a threshold.

In [36], a secure beamforming design scheme was proposed for a relay-based MIMO communication system with blind eavesdroppers, where the system operates in two stages: multiple-access (MA) and broadcast (BC) using PNC. The design scheme finds transmit and receive beamforming vectors that minimize the MSE at the relay and the devices while keeping the eavesdropper SINR below a threshold. Imperfect eavesdropper CSI is considered where the post-processed channel estimation error is assumed to lie within a predefined uncertainty set characterized by a spherical bound. A semi-definite programming (SDP) approach is presented to solve this optimization problem.

In this thesis, we first propose a beamforming design scheme for a similar system model, this time having smart eavesdroppers that can process their received signal better by exploiting diversity. In particular, the eavesdroppers are assumed to apply selection

combining (SC) to their individual antenna signals. A solution to the corresponding robust design problem is presented via an SDP approach. Simulation results are provided for convergence of the MSE at the destination(s) and the SINR at the eavesdroppers for both, the MA and BC stages. Secondly, we revisit the design problem studied by [36] with blind eavesdroppers and propose a more time-efficient second-order cone (SOC) approach to this problem that can also satisfy its constraints and give optimal MSE values. Under given SINR constraints at the eavesdroppers, the SOC program finds beamforming vectors that output smaller MSE values at the destination than the approach in [36]. Additional results for the BC stage are also shown and discussed. A major advantage of our iterative approach is the time efficiency as it needs significantly shorter time to converge.

The rest of this thesis is organized as follows: Chapter 2 provides some history and background on PLS for several communication systems models. In Chapter 3, the system model is presented with the problem formulation. Chapter 4 deals with the beamforming design scheme for the case of eavesdroppers applying SC. Chapter 5 presents the efficient beamforming design for the case of blind eavesdroppers. Chapter 6 provides numerical results from simulations showing the effectiveness of the proposed solutions for both eavesdropper models. Finally, the conclusion is given in Chapter 7.

As for notation, $\mathbb{C}^{m\times n}$ denotes the set of $m \times n$ matrices with elements in the complex field. $\mathbf{1}$ is a vector of ones. $\|\cdot\|$ denotes the Euclidean norm for finite dimensional vector spaces. $\mathcal{E}\{\cdot\}$ and $\mathfrak{R}\{\cdot\}$ denote the expectation and real part respectively. $(\cdot)^T$, $(\cdot)^*$, $(\cdot)^H$ and $\mathrm{Tr}(\cdot)$ denote the transpose, complex conjugate, Hermitian and trace of a matrix respectively. Finally, $\succcurlyeq 0$ denotes positive semi-definiteness.

Chapter 2

Background

Traditionally, data transmission security has been addressed by key-based enciphering techniques at the network layer [17]. All cryptographic schemes are built on the preface that it is computationally infeasible for them to be deciphered without knowledge of the secret key. Nonetheless cryptograms that were thought to be unbreakable are now being broken due to the increase of computational power available to malicious users and/or poor hardware and software implementation of the encrypting algorithm.. Thus, secrecy at the physical layer has gained considerable interest in recent years. In this chapter, we provide some historical overview on PLS and describe selected techniques used in single and multi-antenna wiretap channels.

2.1 The Wiretap Channel

PLS was initially studied by Wyner when he defined the wiretap channel in [37]. Assuming that the eavesdropper has all the computational resources and network state knowledge that it needs, the achieved security can be quantified with information theoretic measures. Within this framework, judiciously designed PLS schemes, such as channel coding and transmit precoding that benefit from the knowledge of CSI and noise characteristics, can enable secret communication at the bit level without the usage of key-based

enciphering. Knowing that information-theoretic security characterizes strategies that allow for the exchange of encryption keys over channels seen by the eavesdropper, physical layer mechanisms can also augment already existing security procedures that are applied in higher layers of the communication protocol stack.

The most basic system in which secrecy and confidentiality issues emerge is composed of a transmitter, a legitimate receiver and a passive eavesdropper with the transmitter aiming to send private data to the receiver. Optimal transmission schemes can be devised depending on the transmitter's knowledge of the eavesdropper's CSI which may range from absence, to partial or statistical, to complete CSI knowledge. As stated previously, secret key-based encryption has been the traditional way to warrant secrecy. However, it had no mathematical basis until Claude Shannon put forward the information-theoretic foundations needed for the development of modern cryptography [38]. The fundamental idea of Shannon's work was that a non-reusable private key K_e is used to cipher the confidential message M in order to generate the cryptogram C, to be transmitted over a noiseless channel. The idea was built on the assumptions that the eavesdropper has unlimited computational power, knows the transmission coding scheme and has access to an identical copy of the signal at the intended receiver. Shannon used concepts from his own information theory, such as mutual information and entropy, to define perfect secrecy.

The mutual information $I(X;Y)$ of two random variables X and Y is a measure of the mutual dependence between the two variables. More specifically, it quantifies the "amount of information" (in units of bits) that can be obtained about one random variable, through the other. The concept of mutual information is intricately linked to the fundamental notion of entropy, $H(Z)$, of a random variable Z, which defines the "amount of information" held in Z. Using these concepts, Shannon defined the perfect secrecy condition which demands that the entropy of the secret message conditioned on the received cryptogram, $H(M|C)$, be equal to the unconditional entropy of the message,

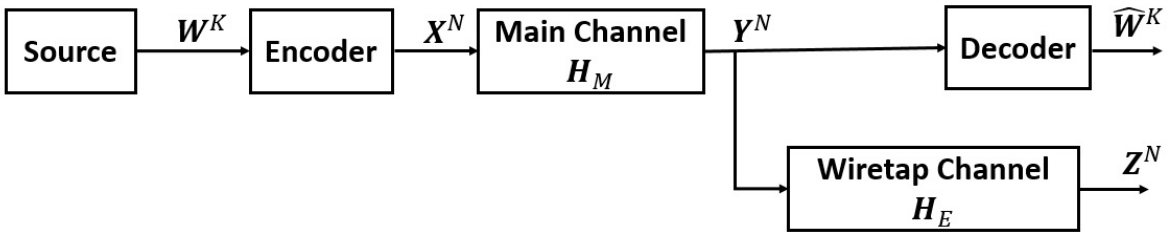

Figure 2.1: The Wiretap Channel

i.e.,

$$I(M;C) = H(M) - H(M|C) = 0 \tag{2.1}$$

In effect, perfect secrecy can be ensured if K_e has at least as much entropy as M, i.e., $H(K_e) \geq H(M)$.

Some years later, Wyner defined the wiretap channel [37] as shown in Figure 2.1, with the source-wiretapper link being a probabilistically degraded version of the main channel. The model takes into account the distortion introduced by the channel. After encoding K bits of the message $\boldsymbol{W}^K = [W_1, \ldots, W_K]$ into N bits, the information signal $\boldsymbol{X}^N$ is transmitted over the main channel, which is modeled as a discrete memoryless one. The receiver observes $\boldsymbol{Y}^N$, of length N, which also goes through the wiretap channel before the eavesdropper receives it as $\boldsymbol{Z}^N$. The receiver then decodes $\boldsymbol{Y}$ to a message $\widehat{\boldsymbol{W}}^K$ that is intended to be the same as $\boldsymbol{W}^K$.

Wyner's purpose was to maximize the intended transmission rate R in the main channel and the intended equivocation u of the data received by the wiretapper. The equivocation u is taken as a measure of the degree to which the eavesdropper is confused. In other words, the goal was to find a way to encode the data such that the eavesdropper's level of confusion is maximized. To that end, he defined a perfect secrecy notion similar to the one defined by Shannon. However, it is a weaker definition; it demands that the actual equivocation

$$\eta(N) \triangleq \frac{1}{K} H(\boldsymbol{W}^K|\boldsymbol{Z}^N) \tag{2.2}$$

approaches the source entropy in the limit, i.e.,

$$\lim_{N\to\infty} \eta(N) = H_W \tag{2.3}$$

Wyner then defined achievability of a rate-equivocation pair. With a transmission rate KH_W/N source bits per channel input symbol, H_W being the source entropy, a pair (R, u) is achievable if it is possible to find an encoder-decoder pair with arbitrarily small probability of error $P_e = \frac{1}{K}\sum_{k=1}^{K} Pr\{W_k \neq \widehat{W}_k\}$, rate KH_W/N in the vicinity of R and equivocation η in the vicinity of u. The set $\mathfrak{R}$ of achievable pairs (R, u) was then portrayed after defining the following quantity

$$\Omega(R) \triangleq \sup_{p_X \in \mathcal{P}(R)} I(X;Y|Z), \quad 0 \leq R \leq C_M \tag{2.4}$$

where $\mathcal{P}(R)$ is the set of input distributions p_X of $\boldsymbol{X}^N$ such that $I(\boldsymbol{X};\boldsymbol{Y}) \geq R$ and C_M is the main channel capacity. $\mathfrak{R}$, sketched in Figure 2.2, was found to be the following set

$$\mathfrak{R} = \{(R, u) : 0 \leq R \leq C_M \quad 0 \leq u \leq H_W \quad Ru \leq H_W\Omega(R)\} \tag{2.5}$$

The term "secrecy capacity" is the maximum achievable transmission rate that satisfies the perfect secrecy condition. Wyner eventually showed that there exists a secrecy capacity $C_W > 0$ such that (C_W, H_W) is achievable making it possible to communicate at a rate C_W with the perfect secrecy condition satisfied.

Later on, Maurer [39] developed a secrecy scheme based on a secret key joint development by the transmitter and the receiver, done through a connection over a public and error-free feedback channel. The scheme permitted a positive (non-zero) rate even when the eavesdropper channel is better than the receiver's channel. Afterwards, research in information-theoretic security split into two main branches: secret key-based secrecy such as Shannon and Maurer's work, and keyless security such as Wyner's work.

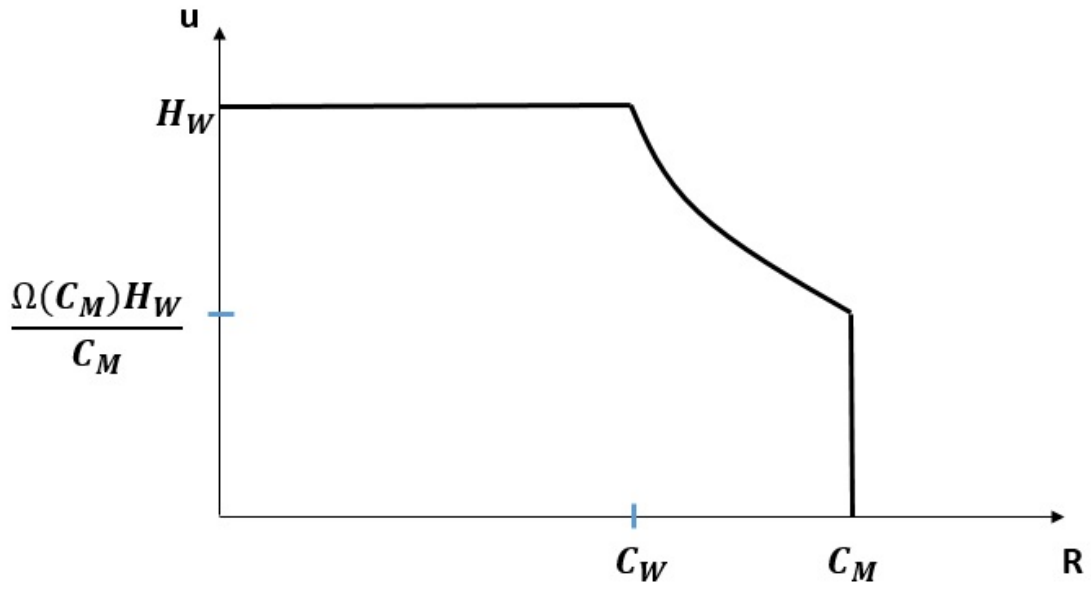

Figure 2.2: Achievable Region

2.2 Single-Antenna Wiretap Channels

2.2.1 Non-Fading Channels

As in the work by Wyner, early research in keyless security tackled non-fading channels assumed to be known at the transmitter. Wyner's wiretap channel was studied in many papers. For example, [40] established bounds on the equivocation rates, while [41] determined that by applying systematic linear codes it is possible to transmit data at capacity on the main channel and maintain secrecy on many large arbitrary portions of the message.

Wyner's work was extended to the Gaussian wiretap channel in [42] where it was shown that the secrecy capacity is the difference between the capacities of the main channel, C_M, and wiretap channel, C_E, i.e.,

$$C_W = C_M - C_E \tag{2.6}$$

It was proven that if the main channel is better than the eavesdropper's channel, a non-zero secrecy capacity can be achieved. Generalized versions of Wyner's wiretap channel were considered in [43, 44] where it was shown that non-causal side information can be beneficial in improving the achievable secrecy rate region.

Wyner introduced the type-II wiretap channel in [45] where K data bits are encoded into N bits and transmitted over a noiseless main channel. The model includes an eavesdropper which obtains an arbitrary subset of size μ of the N coded bits. The objective was to maximize the eavesdropper's equivocation under the constraint that the receiver perfectly recovers the K data bits from the N coded bits. The results presented show tradeoffs among K, N and μ and the eavesdroppers equivocation.

2.2.2 Fading Channels

Several lines of research studied fading wiretap channels. The study of secrecy in fading channels involved the use of outage probability as a performance metric, as in [46], in order to define the secrecy capacity and characterize the maximum transmission rate at which the eavesdropper cannot decode any data. The outage probability at target secrecy rate $R_W > 0$ was defined as the probability that the instantaneous secrecy capacity, C_W, is less than R_W, i.e.,

$$\mathcal{P}_{out}(R_W) = Pr(C_W < R_W) \tag{2.7}$$

Another performance measure, the ϵ-outage secrecy capacity $C_{out}(\epsilon)$, was defined as the largest rate such that the outage probability is less than ϵ, i.e.,

$$\mathcal{P}_{out}(R_W) > \epsilon, \ \forall \ R_W > C_{out}(\epsilon) \tag{2.8}$$

Using these metrics, it was found that there is no obstacle to security as long as some outage is tolerated. In other words, non-zero outage secrecy capacity is achievable even when the average signal-to-noise ratio (SNR) of the main channel is less than the average SNR of the eavesdropper's channel. This is true since there is still a small chance that

the instantaneous SNR of the main channel is greater than the one at the eavesdropper. However, a higher $\mathcal{P}_{out}$ corresponds to a higher $C_{out}(\epsilon)$.

Another channel model was studied in [47] where the main channel was an additive white Gaussian noise (AWGN) channel and the eavesdropper's channel was Rayleigh fading with additive Gaussian noise; however, the eavesdropper CSI is assumed to be unavailable to the transmitter and the receiver. The result obtained in this study was that by using Gaussian random codes, AN injection and power bursting, a non-zero secrecy rate is achievable even when the channel condition at the eavesdropper is better than that at the receiver. Power bursting means high power transmission over short periods. The works in [48, 49], assumed the unavailability of the eavesdropper CSI at the transmitter. In [48] it is assumed that both channels experience block fading where the channel gains remain constant during a time interval and change independently from one interval to the next. It is further assumed that the number of channel uses within each interval is large enough to allow invoking the use of random coding arguments. With these assumptions, an optimal power allocation strategy is established to achieve the secrecy capacity. Furthermore, an on/off power transmission scheme is proposed with variable rate allocation. This scheme achieves capacity for large average SNR thus proving that the absence of eavesdropper CSI at the transmitter does not reduce the secrecy capacity at high SNR values.

The authors of [49] proposed an approach that led to the comprehension of the information-theoretic limits of the wiretap channel with no eavesdropper CSI. The compound wiretap channel was introduced and studied under the assumption that the eavesdropper's channel is drawn from a finite, known set of states. As a performance measure, the notion of the secrecy degrees of freedom ($s.d.o.f.$) was introduced as the rate at which the secrecy capacity scales with $\log_2(\text{SNR})$, i.e.,

$$s.d.o.f. = \lim_{\text{SNR}\to\infty} \frac{C(\text{SNR})}{\frac{1}{2}\log_2(\text{SNR})} \tag{2.9}$$

A lower bound on the $s.d.o.f.$ is referred to as an achievable $s.d.o.f.$ and it was shown that the achievable $s.d.o.f.$ is determined by the geometries of the receiver and eavesdropper channel matrices, i.e.,

$$s.d.o.f. \geq \max_{\mathcal{L}} \min_{j,k} (\text{Rank}(\boldsymbol{H}_{M_j}\boldsymbol{U}_{\mathcal{L}}) - \text{Rank}(\boldsymbol{H}_{E_k}\boldsymbol{U}_{\mathcal{L}})) \tag{2.10}$$

where $\boldsymbol{H}_{M_j}$ and $\boldsymbol{H}_{E_k}$ are the j^{th} receiver and k^{th} eavesdropper's channel matrices, respectively, while $\boldsymbol{U}_{\mathcal{L}}$ is a matrix with column vectors that represent beamforming directions from a set of directions $\mathcal{L}$ for which the transmitter allocates power.

2.3 Multi-Antenna Wiretap Channels

The spatial dimensions available in MIMO systems can be exploited to boost the secrecy capabilities of wireless channels. Considering the fading MIMO channel in Figure 2.3 with a transmitter, a receiver and an eavesdropper having N_t, N_r, N_e antennas, respectively, the signals received by the receiver and the eavesdropper can be represented as

$$\boldsymbol{y}_m = \boldsymbol{H}_M\boldsymbol{x} + \boldsymbol{n}_m \tag{2.11}$$

$$\boldsymbol{y}_e = \boldsymbol{H}_E\boldsymbol{x} + \boldsymbol{n}_e \tag{2.12}$$

where $\boldsymbol{x}$ is a complex vector of length N_t representing the transmitted signal with covariance matrix $\mathcal{E}\{\boldsymbol{x}\boldsymbol{x}^H\} = \boldsymbol{Q}_x$ and average transmit power $\text{Tr}(\boldsymbol{Q}_x) \leq P$, $\boldsymbol{H}_M$ and $\boldsymbol{H}_E$ are the MIMO complex Gaussian channel matrices while $\boldsymbol{n}_m$ and $\boldsymbol{n}_e$ are zero-mean complex white Gaussian additive noise vectors. Secret communication in a MIMO setting was first studied in [50] by Hero. He designed transmission schemes based on available CSI with the goal of achieving either a low probability of intercept (LPI) or a low probability of detection (LPD). The LPI strategy aims to find a transmission scheme that can zero out the channel information rate available to the eavesdropper while maintaining high

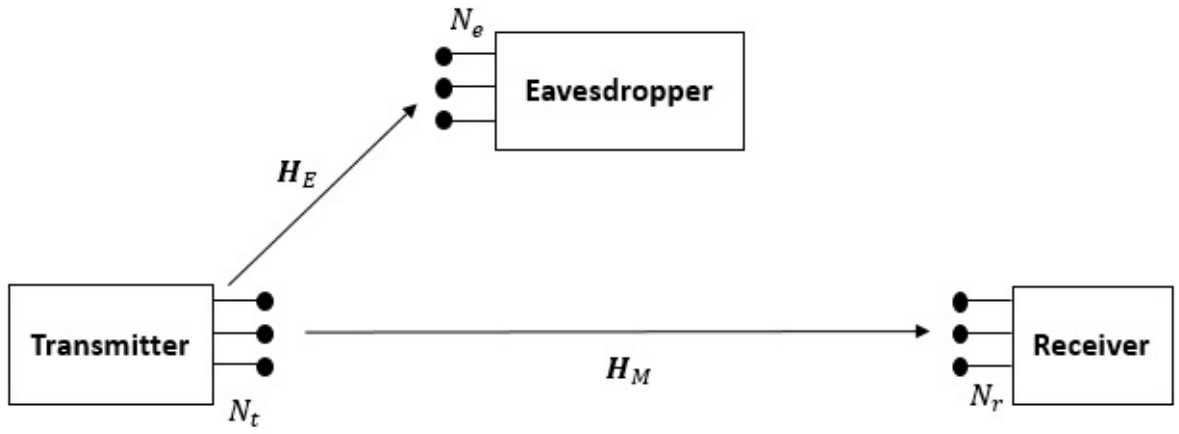

Figure 2.3: The MIMO Wiretap Channel

information rate communication to the receiver. The LPD strategy finds transmission schemes which constrain a constant ϕ to a large value or possibly a small negative value near zero and achieve highest possible information rates to the receiver. ϕ is the error rate which determines how quickly the signal presence decision error decays exponentially to zero as the number of channel output observations increases. Hero showed that significant gains are achievable when the transmitter and receiver know the main channel while the transmitter and eavesdropper do not know the eavesdropper's channel. Capacity limits are compared for various CSI availability cases with the main result being that with the eavesdropper not knowing its CSI[1], an equivocation-maximizing strategy would be employing a space-time constellation with a constant spatial inner product.

Following the study of secrecy for single-input multiple-output (SIMO) and multiple-input single-output (MISO) wiretap channels in [51–53], MIMO channels were further investigated with multiple eavesdroppers as discussed next.

2.3.1 MIMO Multi-Eavesdropper (MIMOME) Channels

Two cases of MIMO channels were considered in the literature. The first one is the deterministic case where all channels matrices are fixed and known to all nodes. A

[1]In a practical setting, an eavesdropper can hardly know its channel H_E since it cannot use pilot symbols from the transmitter to estimate the latter.

scheme that decomposes the system into parallel channels based on the GSVD of the channel matrices is proposed in [54], where it leads to a closed form expression of the secrecy rate and achieves the secrecy capacity in the high SNR limit. For the special case of the MISO channel, the secrecy capacity is characterized for any SNR by the optimal transmit precoder given by the generalized eigenvector $\boldsymbol{\psi}_m$ corresponding to the largest generalized eigenvalue λ_m of $\boldsymbol{h}_M\boldsymbol{h}_M^H - \boldsymbol{H}_E^H\boldsymbol{H}_E$ such that

$$\boldsymbol{h}_M\boldsymbol{h}_M^H\boldsymbol{\psi}_m = \lambda_m\boldsymbol{H}_E^H\boldsymbol{H}_E\boldsymbol{\psi}_m \tag{2.13}$$

where $\boldsymbol{h}_M$ is the main channel vector. It was also shown for the MISOME model [19] that not knowing $\boldsymbol{H}_E$ does not produce significant harm to performance in the high SNR regime; a secure space-time code (masked beamforming) and isotropic power radiation achieve near optimal performance. The second case is where all channels are fading. The main channel is assumed to be known by the transmitter and receiver while the statistical characterization of the eavesdropper's channel is available and the eavesdropper has access to both channels. Here, as the numbers of antennas N_r and N_e increase the secrecy capacity approaches zero whenever $N_r/N_e \geq 2$ [54].

With the statistics of $\boldsymbol{H}_E$ available to the transmitter, an AN injection strategy is employed to achieve secrecy [18,19,55,56]. AN is added to the information signal such that it does not deteriorate the receiver's channel. This strategy was devised for two distinct scenarios. The first scenario is when the transmitter has multiple transmit antennas. This provides extra degrees of freedom to be used for generating noise that degrades only the eavesdropper's channel (orthogonal to the receiver). The second scenario is when the transmitter has one antenna, but helper nodes are available. Helper nodes simulate the effect of multiple antennas and allow the transmitter to generate AN.

For the AN injection strategy, the transmit signal can be written as,

$$\boldsymbol{x} = \boldsymbol{U}_d\boldsymbol{x}_d + \boldsymbol{U}_n\boldsymbol{x}_n \tag{2.14}$$

where $\boldsymbol{U}_d$ $(N_t \times (N_t - d_{AN}))$ and $\boldsymbol{U}_n$ $(N_t \times d_{AN})$ are the complex precoding matrices corresponding to the data and AN signal vectors, $\boldsymbol{x}_d$ and $\boldsymbol{x}_n$, respectively.

When $N_t > N_r$, $\boldsymbol{U}_n$ can be formed from the nullspace of $\boldsymbol{H}_M$, otherwise $\boldsymbol{U}_n$ and $\boldsymbol{U}_d$ are chosen so that the received signals belong to orthogonal subspaces, by forming them from the right singular vectors of $\boldsymbol{H}_M$ [57]. If $\boldsymbol{H}_E$ is partially known, further enhancement can be done via optimizing the AN transmit covariance or relaxing the orthogonality constraint [58, 59].

In general, the secrecy rate gets closer to the capacity as the eavesdropper CSI knowledge increases. The GSVD method demands instantaneous knowledge of $\boldsymbol{H}_E$, the AN method demands the statistic of $\boldsymbol{H}_E$, while the waterfilling method on the main channel, i.e., amplifying each channel up to the required power level compensating for the channel impairments, demands no information about $\boldsymbol{H}_E$; these different transmission strategies have different performance levels. The authors in [60] studied the MIMO wiretap channel and used matrix optimization analysis to show that an upper bound the secrecy capacity is given as

$$C_W = \max_{\boldsymbol{Q}_x \succcurlyeq 0} \{\log\det(\boldsymbol{I} + \boldsymbol{H}_M \boldsymbol{Q}_x \boldsymbol{H}_M^H) - \log\det(\boldsymbol{I} + \boldsymbol{H}_E \boldsymbol{Q}_x \boldsymbol{H}_E^H)\} \tag{2.15}$$

Note that for the general MIMO case, a computable expression for the secrecy capacity has not been found yet under the average input power constraint, $\mathrm{Tr}(\boldsymbol{Q}_x) \leq P$, mentioned in (2.11) and (2.12). The next subsection discusses a more general input power constraint than $\mathrm{Tr}(\boldsymbol{Q}_x) \leq P$.

2.3.2 A More General Matrix Input-Power Constraint

A more general matrix input-power constraint is assumed for studying the MIMO wiretap channel, that is: $\boldsymbol{Q}_x \preceq \boldsymbol{S}$. For the special MISO case, the optimal input covariance matrix was computed in [61] while for the general MIMO case, the fundamental relationship between the MSE and the mutual information was employed to find a closed-form

expression for the capacity achieving $\boldsymbol{Q}_x$ [62]. Moreover, it was shown that

$$C_W(\boldsymbol{S}) = \sum_{i=1}^{\tau} \log_2 \kappa_i \tag{2.16}$$

where $\kappa_i, i = 1, \ldots, \tau$, are the generalized eigenvalues of the pencil $(\boldsymbol{S}^{\frac{1}{2}}\boldsymbol{H}_M^H\boldsymbol{H}_M\boldsymbol{S}^{\frac{1}{2}} + \boldsymbol{I}, \boldsymbol{S}^{\frac{1}{2}}\boldsymbol{H}_E^H\boldsymbol{H}_E\boldsymbol{S}^{\frac{1}{2}} + \boldsymbol{I})$ that are greater than 1. If there are no such eigenvalues, then the information signal at the receiver is a degraded version of that of the eavesdropper and the secrecy capacity will be zero. As mentioned earlier, the secrecy capacity is not computable under an average power constraint. It would be found via an exhaustive search over the set $\{\boldsymbol{S} : \boldsymbol{S} \succcurlyeq 0, \quad \mathrm{Tr}(\boldsymbol{S}) \leq P\}$, i.e.,

$$C_W(P) = \max_{\boldsymbol{S}\succcurlyeq 0, \mathrm{Tr}(\boldsymbol{S})\leq P} C_W(\boldsymbol{S}) \tag{2.17}$$

with $C_W(\boldsymbol{S})$ computed as in (2.16). In certain cases, it is possible to find a closed form of the capacity such as when $\boldsymbol{S}$ is full rank [63,64] or when the SNR is considered high [19].

2.4 Broadcast and Multi-Access Channels

Physical layer secrecy is also investigated for multi-user systems that include multiple transmitters and/or receivers. Two of the most common multi-user (multiple transmitter/receiver) channels are the broadcast and multi-access channels, both of which are surveyed next.

2.4.1 Broadcast Channel

From a security standpoint, a one-to-many broadcast channel (BC) occurs when one user attempts to transmit multiple messages to multiple other users. BCs can be divided into two categories, Type-I (wiretap BC) and Type–II (BC with confidential messages). Type-I is where messages are not necessarily mutually confidential among the downlink

receivers, but should be protected from eavesdroppers. For this case, the transmission schemes discussed in the previous section can be employed. Type-II is where each downlink message should be held secret from all other unintended receivers, i.e., each receiver is viewed as an eavesdropper when a message is not destined to it. This section will be dealing mainly with this category that includes multiple scenarios.

The wiretap channel introduced by Wyner is sort of a BC. Indeed, the transmitter sends confidential messages to the receiver, with the goal of keeping them secret from other receivers. An extension of Wyner's version was examined where the transmitter sends common messages to the receiver and the eavesdropper and also confidential messages only to the receiver; this is a BC with parallel independent subchannels. The secrecy capacity region was studied and the optimal source power allocation that achieves the boundary of the region was derived in [65].

The MIMO Gaussian BC with a common message to both the receiver and the eavesdropper and a confidential message to the receiver was characterized in [66, 67] under the matrix input power-covariance constraint $\boldsymbol{Q}_x \preceq \boldsymbol{S}$ and via a channel enhancement approach. Channel enhancement was used jointly with the entropy power inequality [68] to describe the capacity region .

The authors in [66] examined the problem of the discrete memoryless MIMO Gaussian broadcast channel with two confidential messages transmitted to two receivers, each receiver being an eavesdropper for the other. Under the constraint $\boldsymbol{Q}_x \preceq \boldsymbol{S}$, it was proven using dirty paper coding that both confidential messages can be transmitted simultaneously at their respected maximum secrecy rates. Moreover, it was shown that a coding scheme that employs AN and random binning achieves the secrecy capacity of the MIMO Gaussian wiretap channel. The secrecy capacity region of this model is specified by the set of non-negative rate pairs (R_1, R_2) such that

$$R_1 \leq \sum_{i=1}^{\tau} \log \kappa_i; \quad R_2 \leq \sum_{j=1}^{N_t-\tau} \log \frac{1}{\nu_j} \tag{2.18}$$

where $\kappa_i, i = 1, \ldots, \tau$, are the generalized eigenvalues of the pencil $(\boldsymbol{S}^{\frac{1}{2}}\boldsymbol{H}_M^H\boldsymbol{H}_M\boldsymbol{S}^{\frac{1}{2}} + \boldsymbol{I}, \boldsymbol{S}^{\frac{1}{2}}\boldsymbol{H}_E^H\boldsymbol{H}_E\boldsymbol{S}^{\frac{1}{2}} + \boldsymbol{I})$ that are greater than 1, and $\nu_j, j = 1, \ldots, (N_t - \tau)$, are those less than or equal to 1.

The MIMO Gaussian BC with two independent confidential messages and a confidential one being transmitted, was studied in [69] and the achievability of the secrecy capacity was obtained. Systems with more than two receivers gained attention subsequently [70, 71]. Information theoretic concepts such as mutual information, differential entropy and Fisher information were also used to characterize the secrecy capacity region of this model. Differential entropy, $h(X)$ is an extension of the discrete entropy $H(X)$, discussed in Section 2.1, to continuous random variables. It is a measure of information uncertainty of a random variable. Fisher information measures the amount of information that an observable random variable X carries about an unknown parameter θ of a distribution that models X. The likelihood function $f(X;\theta)$ is the probability mass or density of X conditional on the value of θ. The relationships between the minimum MSE and mutual information and also the relationship between Fisher information and the differential entropy were employed to characterize the capacity region in [70, 71].

To date, there is no computable secrecy capacity expression available for the general MIMO broadcast channel under the average transmit power constraint, $\mathrm{Tr}(\boldsymbol{Q}_X) \leq P$. Optimal solutions based on linear precoding have been established under the constraint $\boldsymbol{Q}_x \preceq \boldsymbol{S}$ in [72]. Using the obtained result, a closed-form sub-optimal expression was derived for an average power constraint [73–77].

2.4.2 Multi-Access Channels

The multiple-access channel (MAC) is a model that includes multiple users attempting to transmit to one receiver. In our discussion of MAC we will assume that we have single-antenna nodes. The MAC with confidential messages was investigated in [78, 79]. The setting includes two transmitters communicating with a common receiver while trying to keep their messages confidential from each other. The level of secrecy was measured

by the equivocation rate and bounds on the capacity-equivocation region and secrecy capacity region were obtained. It was also established that there is a tradeoff between the equivocation rates achieved for the two confidential messages.

The Gaussian wiretap MAC was also studied in [80, 81], where the setting includes multiple users attempting to transmit simultaneously to a base station in the presence of an eavesdropper that receives a degraded version of what the base station receives. It was proven that the secrecy sum capacity can be achieved using Gaussian inputs and stochastic encoders.

The fading cognitive MAC with confidential messages was examined in [82]. The setting involves two users trying to transmit common information to a receiver, where, however, user 1 additionally has confidential information intended only for the receiver, not for user 2. A closed-form power allocation strategy that achieves the boundary point of the secrecy capacity region was found.

2.5 Security in Relay Networks

The secure transmission problem was extended to cooperative and relay-based networks by a number of authors. Several cooperative strategies originating from conventional relay systems were adopted with a few modifications. Two broad categories characterize the security issues in relay networks, namely: untrusted relays and trusted relays. Untrusted relays are nodes whom the transmitted messages must be kept confidential from even while using them to relay those messages. Trusted relays are nodes used to relay the transmitted messages; however, these messages do not need to be kept confidential from the relays.

2.5.1 Untrusted Relays

In this category, the relay is considered to be an untrusted user acting as an eavesdropper and also a helper. The source attempts to send messages to the destination, however these

messages must be shielded from the relay. Studies in [83–86] showed that cooperation from the untrusted relay is essential for achieving a non-zero secrecy rate and under this premise, an achievable region of rate pairs was derived. [87] studies cooperative relay broadcast channels where users can help each other without decoding each other's messages. With a half-duplex AF protocol, the destination can jam the relay while it is receiving data from the source. Then, the interference can be subtracted out by the destination from the signal it receives. To maximize the secrecy rate, a joint beamforming design problem was considered through a one-way/two-way untrusted MIMO relay in [88–90]. The secrecy outage probability was considered for the AF protocol in fading channels indicating the fraction of fading realizations where a secrecy rate can be supported. In these works, outage probability is used as a metric when no eavesdropper CSI is available.

2.5.2 Trusted Relays

This scenario separates the eavesdropper and relay entities in the network. Relays can play many roles to act against eavesdroppers. They may act purely as traditional relays while utilizing help from other nodes to ensure security. Relays may also act as both relaying components as well as cooperative jamming partners to enhance the secure transmission. Additionally, relays can act as stand-alone helpers to facilitate the jamming of unintended receivers.

The two-hop MIMO-relay network, shown in Figure 2.4, with an unprotected link between the source and relay was investigated and cooperative schemes for secure transmission were suggested in [91,92]. The achievable secrecy rate was maximized by properly choosing the relay weights. Maximum secrecy rate beamforming was applied to scenarios that include multiple eavesdroppers in [93,94]. It was shown that the decode-and-forward (DF) strategy is always outperformed by the randomize and forward relaying in terms of secrecy outage probability. Ideal locations for the relay were also discussed. Techniques that included optimal precoding based on AN alignment (ANA) were designed for a MIMO relay channel [95]. Other techniques include a combination of source GSVD

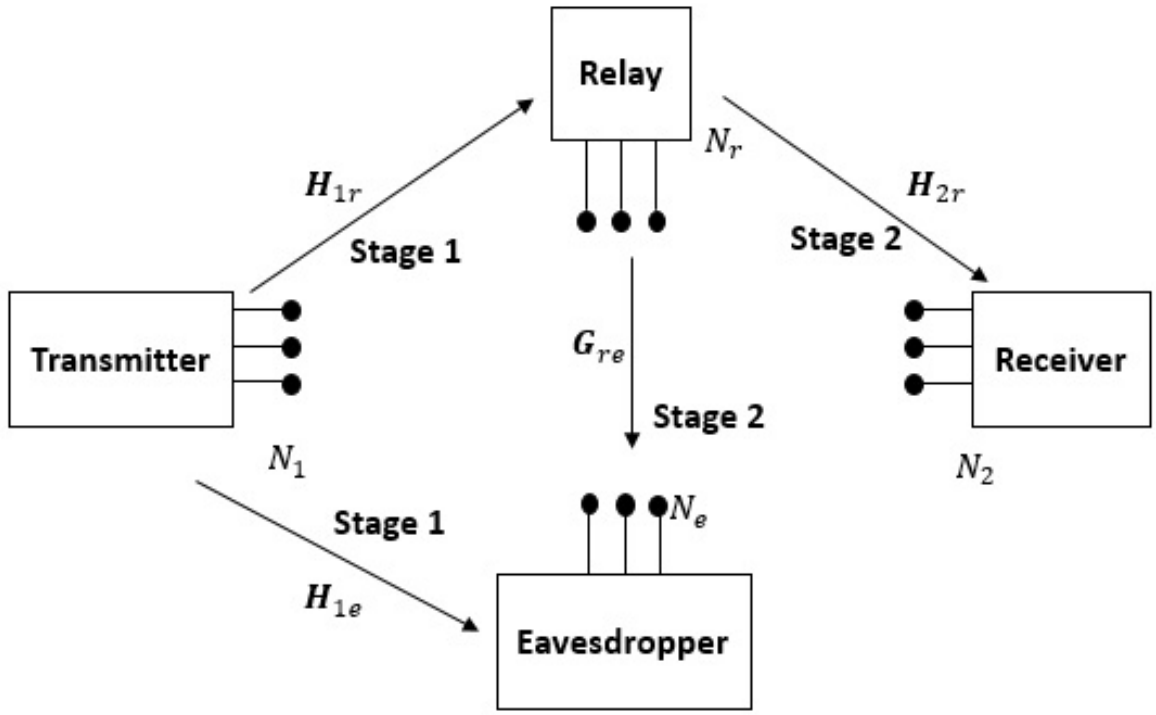

Figure 2.4: Two-hop MIMO relay network

precoding and relay SVD precoding [96].

Another issue that requires attention is relay selection. The optimal selection policy in the DF protocol was shown in [97] to be superior to conventional max-min relay selection, while an opportunistic relay selection scheme was shown to have vanishing secrecy outage probability as the number of DF relays grew.

Helpers are jammers that cooperate with authorized nodes to degrade signals intercepted by the eavesdroppers, but do not have information of their own to transmit. A helper can send random codewords at a rate that ensures that they can be decoded and subtracted from the received signal by the receiver, however not decoded by the eavesdropper. Moreover, helpers can jam signals intercepted by eavesdroppers thus interfering with their ability to decode those signals. A simple illustration is a single-antenna wiretap channel with external helpers where transmission is split into two phases. In the first phase, the transmitter and the receiver transmit independent AN to the helpers. The helpers and eavesdropper receive different weighted versions of these AN signals. In the

second phase, the helpers replay a weighted version of the received signal using a publicly available sequence of weights while the transmitter sends a message and cancels the AN at the receiver.

Multi-antenna two-way relay channels with network coding in the presence of eavesdroppers were studied and secure transmission strategied were developed in [98–101]. The end nodes exchange messages in two-time slots using the analog network-coded relaying protocol. The eavesdropper obtains two observations of the transmitted data, while the end nodes each obtain a single observation. In each of the two phases the transmitting nodes jam the eavesdropper either by optimally using any available spatial degrees of freedom or with the aid of external helpers.

2.6 Concluding Statement

In this chapter, we provided an overview of single and multi-antenna wiretap channels and the security schemes employed in them against any adversary. We also investigated special types of channels, BC and MAC, and discussed a few of the secrecy methods used to protect them. Security in relay networks was also explored with the relay being considered as a trusted node in the system or an untrusted one. The remaining chapters of this thesis deal with a system model that is very similar to the one in Figure 2.4. However, instead of having one device that transmits and once legitimate device that receives signals, we will have two devices that can both transmit and receive signals to and from each other with the aid of a trusted relay, where the aim of keeping their signals hidden from the eavesdroppers. Also, the focus will be on beamforming design, as opposed to information theoretic aspects developed in this chapter.

Chapter 3

System Model and Assumptions

In this chapter we give the formal mathematical statement of the system model under study and underlying assumptions followed by the problem statement.

We consider a system comprising two devices D_1 and D_2, a relay R and K eavesdroppers $E_1, \ldots, E_K$ which try to decode the relayed data between D_1 and D_2, as shown in Fig. 3.1 for $K = 2$. MIMO communication is considered with N_{d_i}, N_r and N_{e_k} denoting the number of antennas at D_i, R and E_k, respectively. All channels are assumed to be frequency-flat. The D_i-to-R channels, denoted as $\boldsymbol{H}_{ir} \in \mathbb{C}^{N_r \times N_{d_i}}$ for $i \in \{1, 2\}$, are assumed reciprocal and perfectly known at the devices. The D_i-to-E_k channels, $\boldsymbol{H}_{ik} \in \mathbb{C}^{N_{e_k} \times N_{d_i}}$ for $k \in \{1, \ldots, K\}$, are imperfectly known at the devices. Similarly, $\boldsymbol{G}_{rk} \in \mathbb{C}^{N_{e_k} \times N_r}$ is the R-to-E_k channel assumed to be imperfectly known at R. Note that in practice, the relative positions of the devices, eavesdroppers and relay need not follow that in Fig. 3.1, whose main purpose is to illustrate the various elements and associated channels of the relay sub-network. In particular, the eavesdroppers can be located anywhere in the given area (and not necessarily along the same line with the relay as shown here). In our approach, the network geometry (and related propagation parameters such as the pathloss) need not be explicitly specified; that is, they only affect our model through the CSI, which will be estimated by the legitimate nodes. R carries out PNC and provides bi-directional communication via time division duplexing in two

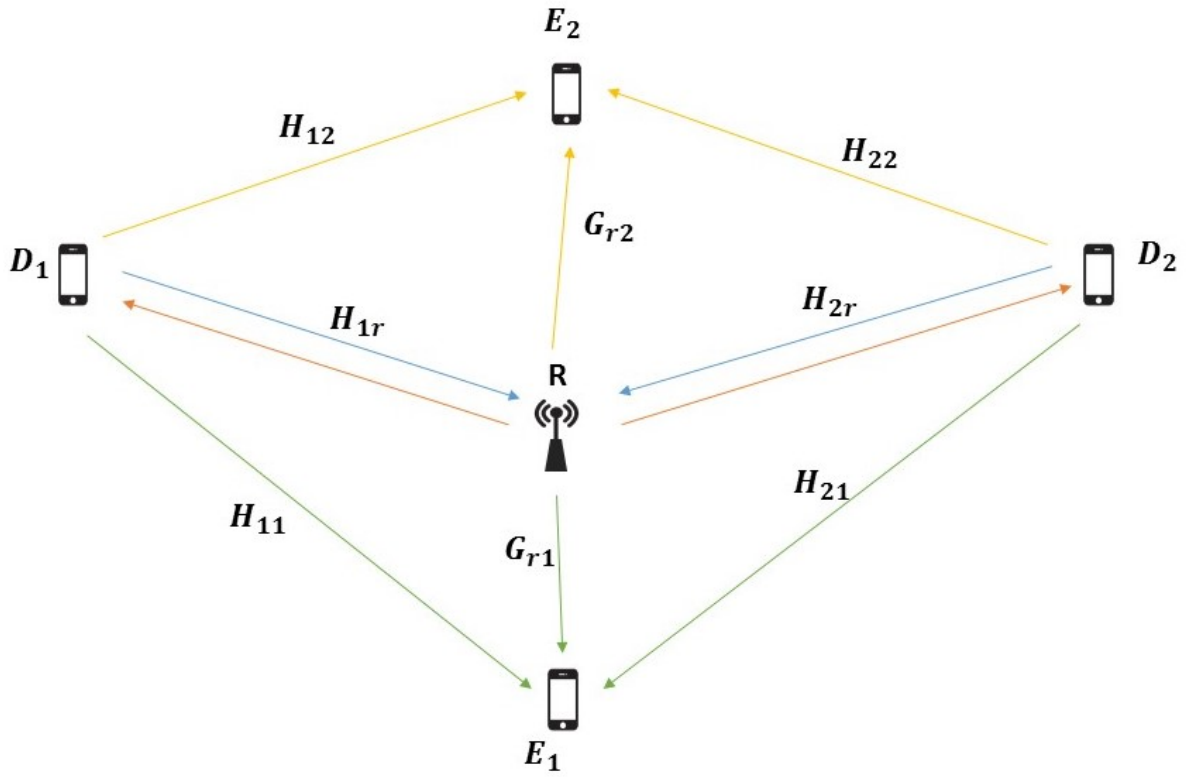

Figure 3.1: A D2D MIMO relay system wiretapped by two eavesdroppers.

stages as described next.

3.1 Multiple-Access (MA) Stage

In this stage, devices D_1 and D_2 simultaneously transmit zero-mean unit-variance uncorrelated complex random symbols s_{d_1} and s_{d_2}, respectively, where it is assumed that $\mathcal{E}\{s_{d_i}s_{d_i}^*\} = 1$ and $\mathcal{E}\{s_{d_i}s_{d_j}^*\} = 0$, $i \neq j$. At D_i, symbol s_{d_i} is beamformed by $\boldsymbol{w}_{d_i} \in \mathbb{C}^{N_{d_i}}$. At R, the superimposed signals are received and processed by a beamformer $\boldsymbol{w}_r \in \mathbb{C}^{N_r}$, resulting into

$$y_r = \boldsymbol{w}_r^H \boldsymbol{H}_{1r} \boldsymbol{w}_{d_1} s_{d_1} + \boldsymbol{w}_r^H \boldsymbol{H}_{2r} \boldsymbol{w}_{d_2} s_{d_2} + \boldsymbol{w}_r^H \boldsymbol{n}_r \tag{3.1}$$

where $\boldsymbol{n}_r$ is the zero-mean additive Gaussian noise vector at R with covariance $\mathcal{E}\{\boldsymbol{n}_r \boldsymbol{n}_r^H\} = \sigma_r^2 \boldsymbol{I}_{N_r}$ and $\mathcal{E}\{s_{d_i}\boldsymbol{n}_r^H\} = 0$. The superimposed signals from D_1 and D_2 are also received at

the K eavesdroppers. At E_k, they are beamformed by a vector $\boldsymbol{w}_{e_k} \in \mathbb{C}^{N_{e_k}}$ resulting in

$$y_{e_k} = \boldsymbol{w}_{e_k}^H \boldsymbol{H}_{1k} \boldsymbol{w}_{d_1} s_{d_1} + \boldsymbol{w}_{e_k}^H \boldsymbol{H}_{2k} \boldsymbol{w}_{d_2} s_{d_2} + \boldsymbol{w}_{e_k}^H \boldsymbol{n}_{e_k}, \forall k \tag{3.2}$$

where $\boldsymbol{n}_{e_k}$ is the zero-mean additive Gaussian noise vector at E_k with covariance $\mathcal{E}\{\boldsymbol{n}_{e_k} \boldsymbol{n}_{e_k}^H\}$ $= \sigma_{ek}^2 \boldsymbol{I}_{N_{e_k}}$.

3.2 Broadcasting (BC) Stage

The received beamformed signal y_r at R is utilized to find an estimate $s_r \in \mathbb{C}$ of $(s_{d_1} + s_{d_2})$ with the aid of PNC mapping [13]. Basically, PNC is a scheme that decides on a value of $(s_{d_1} + s_{d_2})$ using a number of decision thresholds, and then modulates the decided value into a symbol s_r The estimate s_r is then broadcast in the next time slot after being beamformed by $\boldsymbol{v}_r \in \mathbb{C}^{N_r}$. To detect the desired symbol, each device D_i estimates s_r using a beamforming vector $\boldsymbol{v}_{d_i} \in \mathbb{C}^{N_{d_i}}$, thus obtaining

$$z_{d_i} = \boldsymbol{v}_{d_i}^H \boldsymbol{H}_{ir}^T \boldsymbol{v}_r s_r + \boldsymbol{v}_{d_i}^H \boldsymbol{n}_{d_i}, \forall i \tag{3.3}$$

where $\boldsymbol{n}_{d_i}$ is the zero-mean additive Gaussian noise vector at D_i with zero-mean and covariance matrix $\mathcal{E}\{\boldsymbol{n}_{d_i} \boldsymbol{n}_{d_i}^H\} = \sigma_i^2 \boldsymbol{I}_{N_{d_i}}$. The broadcast signal by R is also beamformed at E_k by vector $\boldsymbol{v}_{e_k}$ to obtain

$$z_{ek} = \boldsymbol{v}_{e_k}^H \boldsymbol{G}_{rk} \boldsymbol{v}_r s_r + \boldsymbol{v}_{e_k}^H \boldsymbol{n}_{e_k} \tag{3.4}$$

3.3 Eavesdropper Channel Model and Error Bound

The following imperfect model for the D_i-to-E_k channel is assumed at D_i:

$$\boldsymbol{H}_{ik} = \hat{\boldsymbol{H}}_{ik} + \boldsymbol{E}_{ik}, \ \forall i, k \tag{3.5}$$

where $\hat{\boldsymbol{H}}_{ik}$ and $\boldsymbol{E}_{ik}$ are the estimated and error components of the channel, respectively. The post-processed model of the channel is represented by

$$\begin{aligned} \boldsymbol{h}_{ik} &= (\boldsymbol{w}_{e_k}^H \boldsymbol{H}_{ik})^H = (\boldsymbol{w}_{e_k}^H \hat{\boldsymbol{H}}_{ik} + \boldsymbol{w}_{e_k}^H \boldsymbol{E}_{ik})^H \\ &= \hat{\boldsymbol{h}}_{ik} + \boldsymbol{e}_{ik},\ \forall i,k \end{aligned} \tag{3.6}$$

where $\hat{\boldsymbol{h}}_{ik}$ and $\boldsymbol{e}_{ik}$ are the estimated and error components of the channel after beamforming by $\boldsymbol{w}_{e_k}$. A spherical bound on the error component $\boldsymbol{e}_{ik}$ is given as

$$\|\boldsymbol{e}_{ik}\| \leq \epsilon_i,\ \forall i,k \tag{3.7}$$

for a known $\epsilon_i > 0$.

The same model for the R-to-E_k channel is assumed at R:

$$\boldsymbol{G}_{rk} = \hat{\boldsymbol{G}}_{rk} + \boldsymbol{F}_{rk},\ \forall k \tag{3.8}$$

where $\hat{\boldsymbol{G}}_{rk}$ and $\boldsymbol{F}_{rk}$ are the estimated and error components of the channel, respectively. The post-processed model of the channel is

$$\begin{aligned} \boldsymbol{g}_{rk} &= (\boldsymbol{v}_{e_k}^H \boldsymbol{G}_{rk})^H = (\boldsymbol{v}_{e_k}^H \hat{\boldsymbol{G}}_{rk} + \boldsymbol{v}_{e_k}^H \boldsymbol{F}_{rk})^H \\ &= \hat{\boldsymbol{h}}_{rk} + \boldsymbol{f}_{rk},\ \forall k \end{aligned} \tag{3.9}$$

A spherical bound, a known $\delta_r > 0$, on the error component $\boldsymbol{f}_{rk}$ is also assumed,

$$\|\boldsymbol{f}_{rk}\| \leq \delta_r,\ \forall k \tag{3.10}$$

3.4 Problem Formulation

The objective is to find transmit and receive beamforming vectors at R, D_1 and D_2, while maintaining weak signal reception at the eavesdroppers. Special attention will be given

to the MA stage since a single message (s_{d_1} or s_{d_2}) may be sufficient to decode s_r [13]. Afterwards, we will consider the BC stage, as the secrecy in the system can be further enhanced by appropriately designing the BC transmit and receive beamforming vectors at R and D_i, respectively.

The performance metric for secrecy will be the SINR at each eavesdropper where one of the two signals transmitted from the two devices will be considered data and the other will be regarded as interference. The goal is to keep this SINR below a desired threshold. Moreover, we need to also maintain a good signal reception at the destination. To do that we chose the MSE at the destination as an indicator of reliability. Thus, the approach boils down to finding the beamforming vectors that give a minimum MSE at the destination while satisfying SINR constraints at the eavesdroppers. Factors that need to be considered are the eavesdropper channel estimation error and the beamforming mechanism at each eavesdropper. The beamforming mechanisms examined in this thesis are SC in Chapter 4, and blind beamforming in Chapter 5. As stated in the previous section, the eavesdropper channel estimation error is assumed to be a deterministic unknown, but also spherically bounded.

Chapter 4

Secrecy with Eavesdroppers Applying SC

In practice, the eavesdroppers may not be naive and may apply smart processing to enhance their ability to decode the transmitted symbols. Exploiting diversity is one way the eavesdroppers may use to improve the quality of the decoded signals. In this chapter, we focus on SC where each E_k selects the strongest signal among the ones received at each one of its N_{e_k} antennas. Since the optimization will be performed at the devices or relay, we will assume that each E_k knows $\boldsymbol{w}_{d_1}$ and $\boldsymbol{w}_{d_2}$ and use their actual values. We also assume that E_k knows imperfectly the CSI of $\boldsymbol{H}_{ik}$ and $\boldsymbol{G}_{rk}$ and use our estimates of them, $\hat{\boldsymbol{H}}_{ik}$ and $\hat{\boldsymbol{G}}_{rk}$. The next two sections of this chapter provide solutions to the secure beamforming problem for each of the two communication stages, the MA and BC stages.

4.1 Multiple-Access (MA) Stage

We find the beamforming vectors $\boldsymbol{w}_r$, $\boldsymbol{w}_{d_1}$ and $\boldsymbol{w}_{d_2}$ that minimize the MSE at R, denoted MSE_r, and given by

$$\begin{aligned}\text{MSE}_r &= \mathcal{E}\{|y_r - (s_{d_1} + s_{d_2})|^2\} \\ &= \sum_{i=1}^{2}(|\boldsymbol{w}_r^H \boldsymbol{H}_{ir}\boldsymbol{w}_{d_i}|^2 - 2\Re(\boldsymbol{w}_r^H \boldsymbol{H}_{ir}\boldsymbol{w}_{d_i})) + \sigma_r^2\|\boldsymbol{w}_r\|^2 + 2\end{aligned} \tag{4.1}$$

subject to SINR constraints at each E_k and power constraints at the devices.

Each eavesdropper E_k is assumed to apply SC and select the strongest signal among the N_{e_k} received signals by the N_{e_k} antennas. Let $\mathbb{Q} = \{\boldsymbol{q}_1, \ldots, \boldsymbol{q}_{N_{e_k}}\}$ denote the set of standard basis vectors of $\mathbb{R}^{N_{e_k}}$. Selection of the n^{th} antenna at E_k is equivalent to using $\boldsymbol{q}_n$ as the receive beamforming vector. E_k may choose $\boldsymbol{w}_{e_k}$ as follows

$$\boldsymbol{w}_{e_k} = \arg\max_{\boldsymbol{q}_n \in \mathbb{Q}} \quad (\max_{i} \quad \text{SINR}_k^{i,n}). \tag{4.2}$$

where $\text{SINR}_k^{i,n}$ is the SINR of the signal from D_i received at the n^{th} antenna of E_k, $n \in \{1, \ldots, N_{e_k}\}$ given by

$$\text{SINR}_k^{i,n} = \frac{|\boldsymbol{q}_n^H \boldsymbol{H}_{ik}\boldsymbol{w}_{d_i}|^2}{|\boldsymbol{q}_n^H \boldsymbol{H}_{jk}\boldsymbol{w}_{d_j}|^2 + \sigma_{e_k}^2} = \frac{|\boldsymbol{w}_{d_i}^H \boldsymbol{h}_{ik}^{(n)}|^2}{|\boldsymbol{w}_{d_j}^H \boldsymbol{h}_{jk}^{(n)}|^2 + \sigma_{e_k}^2} \tag{4.3}$$

where $i \neq j$, $i, j \in \{1, 2\}$, and $\boldsymbol{h}_{ik}^{(n)} = \boldsymbol{H}_{ik}^H \boldsymbol{q}_n = \hat{\boldsymbol{h}}_{ik}^{(n)} + \boldsymbol{e}_{ik}^{(n)}$.

D_1, D_2 and R should choose their transmit and receive beamforming vectors so as to minimize MSE_r while *(i)* the maximum presumed SINR_k^i at each E_k is below a predefined threshold γ_k for any possible antenna choice at E_k; *(ii)* the power at D_i satisfies the constraint $\|\boldsymbol{w}_{d_i}\|^2 \leq P_{max}$. The beamforming design should take into account the uncertainty on the post-processed channel $\boldsymbol{h}_{ik}^{(n)}$, equivalent to the one mentioned in (3.7).

A spherical bound on the error component $\boldsymbol{e}_{ik}^{(n)}$ is assumed as

$$\|\boldsymbol{e}_{ik}^{(n)}\| \leq \epsilon_i, \ \forall i, k, n \tag{4.4}$$

for a known $\epsilon_i > 0$.

The beamforming design procedure can now be formulated as the following constrained optimization problem

$$\begin{aligned} \min_{\boldsymbol{w}_r, \boldsymbol{w}_{d_1}, \boldsymbol{w}_{d_2}} \quad & \text{MSE}_r \\ \text{subject to} \quad & \|\boldsymbol{w}_{d_i}\|^2 \leq P_{max} \\ & \text{SINR}_k^{i,n} \leq \gamma_k, \\ & \|\boldsymbol{e}_{ik}^{(n)}\| \leq \epsilon_i, \ \forall i, k, n \end{aligned} \tag{4.5}$$

A practical solution to this non-convex problem can be obtained using an iterative procedure after dividing it into three sub-problems, as described next.

Sub-Problem 1: $\boldsymbol{w}_{d_1}$ and $\boldsymbol{w}_{d_2}$ are fixed to the values found in the previous iteration so that $\boldsymbol{w}_r$ is the only variable to solve for in (4.5). Since $\boldsymbol{w}_r$ only appears in the objective function $\text{MSE}_r(\boldsymbol{w}_r, \boldsymbol{w}_{d_1}, \boldsymbol{w}_{d_2})$, to find its optimal value we compute the partial derivative of MSE_r with respect to $\boldsymbol{w}_r$ and equate it to zero. This way we obtain

$$\boldsymbol{w}_r = (\sum_{i=1}^{2} (\boldsymbol{H}_{ir} \boldsymbol{w}_{d_i} \boldsymbol{w}_{d_i}^H \boldsymbol{H}_{ir}^H) + \sigma_r^2 \boldsymbol{I}_{N_r})^{-1} (\sum_{i=1}^{2} \boldsymbol{H}_{ir} \boldsymbol{w}_{d_i}) \tag{4.6}$$

Sub-Problem 2: To solve for $\boldsymbol{w}_{d_1}$, we fix $\boldsymbol{w}_{d_2}$ to the same value used in sub-problem 1 and $\boldsymbol{w}_r$ to its value computed in sub-problem 1. Using (3.6), $\text{SINR}_k^{i,n}$ can be expanded

so that (4.5) becomes

$$\begin{aligned}
\min_{\boldsymbol{w}_{d_1}} \quad & \text{MSE}_r \\
\text{subject to} \quad & \|\boldsymbol{w}_{d_i}\|^2 \leq P_{max} \\
& |\boldsymbol{w}_{d_i}^H \boldsymbol{e}_{ik}^{(n)}|^2 + 2\Re(\hat{\boldsymbol{h}}_{ik}^{(n)H} \boldsymbol{w}_{d_i} \boldsymbol{w}_{d_i}^H \boldsymbol{e}_{ik}^{(n)}) \\
& + |\boldsymbol{w}_{d_i}^H \hat{\boldsymbol{h}}_{ik}^{(n)}|^2 - \gamma_k |\boldsymbol{w}_{d_j}^H \boldsymbol{e}_{jk}^{(n)}|^2 \\
& - 2\gamma_k \Re(\hat{\boldsymbol{h}}_{jk}^{(n)H} \boldsymbol{w}_{d_j} \boldsymbol{w}_{d_j}^H \boldsymbol{e}_{jk}^{(n)}) \\
& - \gamma_k |\boldsymbol{w}_{d_j}^H \hat{\boldsymbol{h}}_{jk}^{(n)}|^2 - \gamma_k \sigma_{e_k}^2 \leq 0, \\
& \|\boldsymbol{e}_{ik}^{(n)}\| \leq \epsilon_i, \ \forall i, j, k, n, \ i \neq j
\end{aligned} \tag{4.7}$$

The SINR and error component constraints in (4.7) can be rewritten as

$$\boldsymbol{e}_k^{(n)H} \boldsymbol{B}_{ik} \boldsymbol{e}_k^{(n)} + 2\Re(\boldsymbol{d}_{ik}^{(n)H} \boldsymbol{e}_k^{(n)}) + c_{ik}^{(n)} \leq 0 \tag{4.8}$$

$$\boldsymbol{e}_k^{(n)H} \boldsymbol{e}_k^{(n)} \leq \epsilon^2, \forall i, k, n \tag{4.9}$$

where

$$\begin{aligned}
\boldsymbol{e}_k^{(n)} &= [\boldsymbol{e}_{1k}^{(n)} \quad \boldsymbol{e}_{2k}^{(n)}]^T \\
\boldsymbol{B}_{1k} &= \begin{bmatrix} \boldsymbol{w}_{d_1} \boldsymbol{w}_{d_1}^H & \boldsymbol{0}_{N_{d_1} \times N_{d_2}} \\ \boldsymbol{0}_{N_{d_2} \times N_{d_1}} & -\gamma_k \boldsymbol{w}_{d_2} \boldsymbol{w}_{d_2}^H \end{bmatrix} \\
\boldsymbol{B}_{2k} &= \begin{bmatrix} -\gamma_k \boldsymbol{w}_{d_1} \boldsymbol{w}_{d_1}^H & \boldsymbol{0}_{N_{d_1} \times N_{d_2}} \\ \boldsymbol{0}_{N_{d_2} \times N_{d_1}} & \boldsymbol{w}_{d_2} \boldsymbol{w}_{d_2}^H \end{bmatrix} \\
\boldsymbol{d}_{1k}^{(n)} &= [\boldsymbol{w}_{d_1} \boldsymbol{w}_{d_1}^H \hat{\boldsymbol{h}}_{1k}^{(n)}; -\gamma_k \boldsymbol{w}_{d_2} \boldsymbol{w}_{d_2}^H \hat{\boldsymbol{h}}_{2k}^{(n)}] \\
\boldsymbol{d}_{2k}^{(n)} &= [-\gamma_k \boldsymbol{w}_{d_1} \boldsymbol{w}_{d_1}^H \hat{\boldsymbol{h}}_{1k}^{(n)}; \boldsymbol{w}_{d_2} \boldsymbol{w}_{d_2}^H \hat{\boldsymbol{h}}_{2k}^{(n)}] \\
c_{1k}^{(n)} &= |\boldsymbol{w}_{d_1}^H \hat{\boldsymbol{h}}_{1k}^{(n)}|^2 - \gamma_k |\boldsymbol{w}_{d_2}^H \hat{\boldsymbol{h}}_{2k}^{(n)}|^2 - \sigma_{e_k}^2 \gamma_k \\
c_{2k}^{(n)} &= -\gamma_k |\boldsymbol{w}_{d_1}^H \hat{\boldsymbol{h}}_{1k}^{(n)}|^2 + |\boldsymbol{w}_{d_2}^H \hat{\boldsymbol{h}}_{2k}^{(n)}|^2 - \sigma_{e_k}^2 \gamma_k.
\end{aligned} \tag{4.10}$$

Note that ϵ is chosen such that $\epsilon_1^2 + \epsilon_2^2 \leq \epsilon^2$. Using the S-Procedure from [102], (4.8) and

(4.9) can be reformulated into a matrix inequality

$$\begin{bmatrix} \theta_{ik}^{(n)} \boldsymbol{I}_{N_{d_i}} - \boldsymbol{B}_{ik} & -\boldsymbol{d}_{ik}^{(n)} \\ -(\boldsymbol{d}_{ik}^{(n)})^H & -c_{ik}^{(n)} - \theta_{ik}^{(n)} \epsilon^2 \end{bmatrix} \succcurlyeq 0, \forall i,k,n \tag{4.11}$$

with $\theta_{ik}^{(n)} \geq 0$.

Defining $\boldsymbol{A}_i$ and $\boldsymbol{b}_i$ as follows

$$\boldsymbol{A}_i = \boldsymbol{H}_{ir}^H \boldsymbol{w}_r \boldsymbol{w}_r^H \boldsymbol{H}_{ir},\ \boldsymbol{b}_i = \boldsymbol{H}_{ir}^H \boldsymbol{w}_r, \forall i \tag{4.12}$$

we obtain the SDP relaxation of (4.7) with the modified constraints in (4.11) after replacing $\boldsymbol{w}_{d_1}\boldsymbol{w}_{d_1}^H$ with the matrix variable $\boldsymbol{W}_{d_1} \in \mathbb{C}^{N_{d_1} \times N_{d_1}}$ to get

$$\begin{aligned} &\min_{\boldsymbol{W}_{d_1}, \boldsymbol{w}_{d_1}, \theta_{ik}^{(n)}} \operatorname{Tr}(A_1 \boldsymbol{W}_{d_1}) - 2\Re(\boldsymbol{b}_1 \boldsymbol{w}_{d_1}) + \boldsymbol{w}_{d_2} \boldsymbol{A}_2 \boldsymbol{w}_{d_2} - 2\Re(\boldsymbol{b}_2 \boldsymbol{w}_{d_2}) + \sigma_r^2 \boldsymbol{w}_r^H \boldsymbol{w}_r + 2 \\ &\quad \text{subject to} \quad \operatorname{Tr}(\boldsymbol{W}_{d_1}) \leq P_{max}, \begin{bmatrix} \boldsymbol{W}_{d_1} & \boldsymbol{w}_{d_1} \\ \boldsymbol{w}_{d_1}^H & 1 \end{bmatrix} \succcurlyeq 0, \quad \forall n,k \\ &\begin{bmatrix} \theta_{1k}^{(n)} \boldsymbol{I}_{N_{d_1}} - \boldsymbol{W}_{d_1} & \boldsymbol{0}_{N_{d_1} \times N_{d_2}} & -\boldsymbol{W}_{d_1} \hat{\boldsymbol{h}}_{1k}^{(n)} \\ \boldsymbol{0}_{N_{d_2} \times N_{d_1}} & \theta_{1k}^{(n)} \boldsymbol{I}_{N_{d_2}} + \gamma_k \boldsymbol{w}_{d_2} \boldsymbol{w}_{d_2}^H & \gamma_k \boldsymbol{w}_{d_2} \boldsymbol{w}_{d_2}^H \hat{\boldsymbol{h}}_{2k}^{(n)} \\ -(\hat{\boldsymbol{h}}_{1k}^{(n)})^H \boldsymbol{W}_{d_1} & \gamma_k (\hat{\boldsymbol{h}}_{2k}^{(n)})^H \boldsymbol{w}_{d_2} \boldsymbol{w}_{d_2}^H & -\theta_{1k}^{(n)} \epsilon^2 - (\hat{\boldsymbol{h}}_{1k}^{(n)})^H \boldsymbol{W}_{d_1} \hat{\boldsymbol{h}}_{1k}^{(n)} + \gamma_k (\hat{\boldsymbol{h}}_{2k}^{(n)})^H \boldsymbol{w}_{d_2} \boldsymbol{w}_{d_2}^H \hat{\boldsymbol{h}}_{2k}^{(n)} + \sigma_{e_k}^2 \gamma_k \end{bmatrix} \succcurlyeq 0, \\ &\begin{bmatrix} \theta_{2k}^{(n)} \boldsymbol{I}_{N_{d_1}} + \gamma_k \boldsymbol{W}_{d_1} & \boldsymbol{0}_{N_{d_1} \times N_{d_2}} & \gamma_k \boldsymbol{W}_{d_1} \hat{\boldsymbol{h}}_{1k}^{(n)} \\ \boldsymbol{0}_{N_{d_2} \times N_{d_1}} & \theta_{2k}^{(n)} \boldsymbol{I}_{N_{d_2}} - \boldsymbol{w}_{d_2} \boldsymbol{w}_{d_2}^H & -\boldsymbol{w}_{d_2} \boldsymbol{w}_{d_2}^H \hat{\boldsymbol{h}}_{2k}^{(n)} \\ \gamma_k (\hat{\boldsymbol{h}}_{1k}^{(n)})^H \boldsymbol{W}_{d_1} & -(\hat{\boldsymbol{h}}_{2k}^{(n)})^H \boldsymbol{w}_{d_2} \boldsymbol{w}_{d_2}^H & -\theta_{2k}^{(n)} \epsilon^2 + \gamma_k (\hat{\boldsymbol{h}}_{1k}^{(n)})^H \boldsymbol{W}_{d_1} \hat{\boldsymbol{h}}_{1k}^{(n)} - (\hat{\boldsymbol{h}}_{2k}^{(n)})^H \boldsymbol{w}_{d_2} \boldsymbol{w}_{d_2}^H \hat{\boldsymbol{h}}_{2k}^{(n)} + \sigma_{e_k}^2 \gamma_k \end{bmatrix} \succcurlyeq 0 \end{aligned} \tag{4.13}$$

The problem in (4.13) is convex and can be solved using an SDP solver such as YALMIP.

Sub-Problem 3: To solve for $\boldsymbol{w}_{d_2}$, we fix $\boldsymbol{w}_r$ and $\boldsymbol{w}_{d_1}$ to their values found in sub-problems 1 and 2, respectively. The same approach is used here as in sub-problem 2 by applying the SDP relaxation of (4.7) with the modified constraints in (4.11) and replacing $\boldsymbol{w}_{d_2}\boldsymbol{w}_{d_2}^H$ with $\boldsymbol{W}_{d_2} \in \mathbb{C}^{N_{d_2} \times N_{d_2}}$.

After initializing $\boldsymbol{w}_{d_i} = \sqrt{P_{max}/N_{d_i}}\mathbf{1}$, all three sub-problems are solved iteratively until MSE_r converges. This procedure can be performed at D_1 and D_2. After finding the optimal $\boldsymbol{w}_r$, the devices send it to R before data transmission. This algorithm is run every time an updated value of the main channel and eavesdropper channel estimate is obtained. The frequency of obtaining a channel estimate varies from one wireless data standard to another.

4.2 Broadcasting (BC) Stage

As in the MA stage approach, the beamforming vector $\boldsymbol{v}_{e_k}$ at the n^{th} antenna of E_k is chosen from $\mathbb{Q}$ such that, e.g., it produces the highest possible symbol-to-noise ratio of s_r at E_k, SNR_k. The aim is to minimize the weighted sum of the MSEs of the received signals at D_1 and D_2 by choosing the appropriate vectors $\boldsymbol{v}_r$, $\boldsymbol{v}_{d_1}$ and $\boldsymbol{v}_{d_2}$ while also satisfying power and secrecy constraints. The MSE of the received signal s_r at D_i is denoted by MSE_{d_i}, $i = 1, 2$, and it is computed as follows,

$$\begin{aligned} \text{MSE}_{d_i} &= \mathcal{E}\{|z_{d_i} - s_r|^2\} \\ &= \rho\|\boldsymbol{v}_{d_i}^H \boldsymbol{H}_{ir}^T \boldsymbol{v}_r\|^2 - 2\rho\Re(\boldsymbol{v}_{d_i}^H \boldsymbol{H}_{ir}^T \boldsymbol{v}_r) + \rho + \sigma_i^2\|\boldsymbol{v}_{d_i}\|^2 \end{aligned} \tag{4.22}$$

where $\mathcal{E}\{s_r s_r^*\} = \rho$, with ρ representing the average normalized power of symbol s_r relative to s_{d_i}. Both MSE_{d_1} and MSE_{d_2} are considered together by taking $\overline{\text{MSE}}_d = \frac{1}{2}(\text{MSE}_{d_1} + \text{MSE}_{d_2})$ as the objective function. SNR_k^n is expressed as

$$\text{SNR}_k^n = \frac{\rho|\boldsymbol{v}_r^H \boldsymbol{g}_{rk}^{(n)}|^2}{\sigma_{e_k}^2}, \qquad \forall k, n \tag{4.23}$$

where

$$\boldsymbol{g}_{rk}^{(n)} = \boldsymbol{G}_{rk}^H \boldsymbol{q}_n = \hat{\boldsymbol{g}}_{rk}^{(n)} + \boldsymbol{f}_{rk}^{(n)}, \quad \forall k, n \tag{4.24}$$

To hinder decoding of s_r at any of the eavesdroppers, an upper bound λ_k should be enforced on SNR_k^n. Equivalently to (3.10) a spherical bound on the error component $\boldsymbol{f}_{rk}^{(n)}$ is also assumed,

$$\|\boldsymbol{f}_{rk}^{(n)}\| \leq \delta_r, \ \forall k, n \tag{4.25}$$

for a known $\delta_r > 0$. After including in the set of constraints the spherical bound on the channel error components, written in (3.10), the following optimization problem is to be

solved

$$\begin{aligned} \min_{\boldsymbol{v}_r, \boldsymbol{v}_{d_1}, \boldsymbol{v}_{d_2}} \quad & \overline{\mathrm{MSE}}_d(\boldsymbol{v}_r, \boldsymbol{v}_{d_1}, \boldsymbol{v}_{d_2}) \\ \text{subject to} \quad & \|\boldsymbol{v}_r\|^2 \leq P_{max}/\rho \\ & \mathrm{SNR}_k^n \leq \lambda_k, \\ & \|\boldsymbol{f}_{rk}^{(n)}\| \leq \delta_r, \ \forall k, n \end{aligned} \tag{4.25}$$

A practical solution to this non-convex problem can be obtained using an iterative procedure after dividing it into the following two sub-problems:

Sub-Problem 1: Here, the transmit beamforming vector $\boldsymbol{v}_r$ is fixed, leaving $\boldsymbol{v}_{d_1}$ and $\boldsymbol{v}_{d_2}$ as the optimization variables appearing only in the objective function. Therefore, the optimal value of $\boldsymbol{v}_{d_i}$ is obtained by computing the partial derivative of MSE_{d_i} with respect to $\boldsymbol{v}_{d_i}$ and equating it to zero. We thus obtain

$$\boldsymbol{v}_{d_i} = (\boldsymbol{H}_{ir}^T \boldsymbol{v}_r \boldsymbol{v}_r^H \boldsymbol{H}_{ir}^* + \sigma_i^2 \boldsymbol{I}_{N_i})^{-1} \boldsymbol{H}_{ir}^T \boldsymbol{v}_r \tag{4.26}$$

Sub-Problem 2: The receive beamforming vectors, $\boldsymbol{v}_{d_i}$ are now fixed to the values obtained in the previous iteration, so the only variable remaining would be $\boldsymbol{v}_r$. Similar to the MA stage, the SNR and error constraints are modified and the problem (4.25) is reformulated using the S-procedure and by replacing $\boldsymbol{v}_r \boldsymbol{v}_r^H$ with $\boldsymbol{V}_r$ to obtain the following convex problem, which is solved using an SDP solver:

$$\begin{aligned} \min_{\boldsymbol{V}_r, \boldsymbol{v}_r, \theta_{rk}^{(n)}} & \sum_{i=1}^{2} (\rho \ \mathrm{Tr}(A_{ri} \boldsymbol{V}_r) - 2\rho \Re(\boldsymbol{b}_{ri} \boldsymbol{v}_r) + \sigma_{d_i}^2 \boldsymbol{v}_{d_i}^H \boldsymbol{v}_{d_i} + \rho) \\ \text{subject to} \quad & \mathrm{Tr}(\boldsymbol{V}_r) \leq P_{max}/\rho, \begin{bmatrix} \boldsymbol{V}_r & \boldsymbol{v}_r \\ \boldsymbol{v}_r^H & 1 \end{bmatrix} \succcurlyeq 0, \quad \forall n, k \\ & \begin{bmatrix} \theta_{rk}^{(n)} \boldsymbol{I}_{N_r} - \rho \boldsymbol{V}_r & -\boldsymbol{V}_r \hat{\boldsymbol{h}}_{rk}^{(n)} \\ -\hat{\boldsymbol{h}}_{rk}^{(n)H} \boldsymbol{V}_r & -\theta_{rk}^{(n)} \delta_r^2 - \hat{\boldsymbol{h}}_{rk}^{(n)H} \boldsymbol{V}_r \hat{\boldsymbol{h}}_{rk}^{(n)} + \sigma_{e_k}^2 \lambda_k \end{bmatrix} \succcurlyeq 0 \end{aligned} \tag{4.27}$$

where $\boldsymbol{A}_{ri} = \boldsymbol{H}_{ir}^* \boldsymbol{v}_{d_i} \boldsymbol{v}_{d_i}^H \boldsymbol{H}_{ir}^T$ and $\boldsymbol{b}_{ri} = \boldsymbol{H}_{ir}^* \boldsymbol{v}_{d_i}$.

After initializing with $\boldsymbol{v}_r = \sqrt{P_{max}/\rho N_{d_i}}\mathbf{1}$, the two sub-problems are solved iteratively until $\overline{\text{MSE}}_d$ converges. This procedure can be performed at R, with the obtained optimal $\boldsymbol{v}_{d_i}$ sent to D_i before data transmission.

Finally, it should be noted that the beamforming coefficients in both stages are updated whenever a new CSI estimate becomes available. In practice, this means that the time interval assigned between two consecutive coefficient updates should be less than the coherence time of the channel. In LTE for example, the CSI information may be updated every 2 to 160ms, depending on system configuration and mobility parameters [103]. However, the beamforming coefficient updates need not be periodic, as the network may further request a CSI on demand.

Chapter 5

Secure Beamforming with Blind Eavesdroppers

In this chapter, we develop and solve the optimum beamformer design problem for the MA and BC stages, when the eavesdroppers do not know any of the channels nor the beamformers used at D_i and R. In this case, it is assumed that thus they combine blindly the received signals to decode each symbol separately. That is, they use [36]

$$\boldsymbol{w}_{e_k} = \boldsymbol{v}_{e_k} = (N_{e_k})^{-\frac{1}{2}}\mathbf{1},\ \forall k \tag{5.1}$$

which can be interpreted as broadside beamforming.

5.1 Multiple-Access (MA) Stage

Here using an SOC-based approach, we find the optimal beamforming vectors $\boldsymbol{w}_r$, $\boldsymbol{w}_{d_1}$ and $\boldsymbol{w}_{d_2}$ that minimize MSE_r subject to power constraints at the devices and SINR constraints at each E_k. With no changes in the assumptions on D_1, D_2 and R, the expression of MSE_r in (4.1) and the power constraint on $\boldsymbol{w}_{d_i}$ remain the same.

Given $\boldsymbol{w}_{e_k}$ in (5.1), the received SINR of s_{d_i} at E_k is given by

$$\text{SINR}_k^i = \frac{|\boldsymbol{w}_{d_i}^H \boldsymbol{h}_{ik}|^2}{|\boldsymbol{w}_{d_j}^H \boldsymbol{h}_{jk}|^2 + \sigma_{ek}^2}, \forall i, j, k,\ i \neq j \tag{5.2}$$

The SINR values at each E_k are constrained to be less than a threshold γ_k to hinder eavesdropping. By including in the set of constraints the spherical bound on the channel error components, $\|\boldsymbol{e}_{ik}\| \leq \epsilon_i$, the following optimization problem is obtained:

$$\begin{aligned} \min_{\boldsymbol{w}_r, \boldsymbol{w}_{d_1}, \boldsymbol{w}_{d_2}} \quad & \text{MSE}_r \\ \text{subject to} \quad & \|\boldsymbol{w}_{d_i}\|^2 \leq P_{max}, \quad \text{SINR}_k^i \leq \gamma_k \\ & \|\boldsymbol{e}_{ik}\| \leq \epsilon_i,\ \forall i, k \end{aligned} \tag{5.3}$$

This is a non-convex optimization problem. A solution can be obtained using an iterative procedure whose p^{th} iteration consists of the following two major steps:

Sub-Problem 1: To solve for $\boldsymbol{w}_r$, we use the same optimal solution as in [36] by fixing $\boldsymbol{w}_{d_1}$ and $\boldsymbol{w}_{d_2}$ to their values, $\boldsymbol{w}_{d_1}^{(p-1)}$ and $\boldsymbol{w}_{d_2}^{(p-1)}$, from the previous iteration. Letting $\boldsymbol{x}_i^{(p)} = \boldsymbol{H}_{ir} \boldsymbol{w}_{d_i}^{(p-1)}$, taking the derivative of the objective function with respect to $\boldsymbol{w}_r$ and setting it to zero yields

$$\boldsymbol{w}_r^{(p)} = (\sum_{i=1}^{2} (\boldsymbol{x}_i^{(p)} \boldsymbol{x}_i^{(p)H}) + \sigma_r^2 \boldsymbol{I}_{N_r})^{-1} (\sum_{i=1}^{2} \boldsymbol{x}_i^{(p)}) \tag{5.4}$$

Sub-Problem 2: To solve for $\boldsymbol{w}_{d_1}$ and $\boldsymbol{w}_{d_2}$, we fix $\boldsymbol{w}_r$ to $\boldsymbol{w}_r^{(p)}$. The SINR constraint and channel estimation error bound can be transformed into a single constraint by considering the following approach. The denominator of (5.2) is made constant by fixing $\boldsymbol{w}_{d_1}$ and $\boldsymbol{w}_{d_2}$ to the values $\boldsymbol{w}_{d_1}^{(p-1)}$ and $\boldsymbol{w}_{d_2}^{(p-1)}$ that were utilized to calculate $\boldsymbol{w}_r$ in sub-problem 1. In other words, to solve for the devices' beamforming vectors at the current p^{th} iteration $\boldsymbol{w}_{d_1}^{(p)}$ and $\boldsymbol{w}_{d_2}^{(p)}$, the SINR constraint $\text{SINR}_k^i \leq \gamma_k$ is modified into

$$|\boldsymbol{h}_{ik}^H \boldsymbol{w}_{d_i}^{(p)}|^2 \leq \gamma_k (|\boldsymbol{h}_{jk}^H \boldsymbol{w}_{d_j}^{(p-1)}|^2 + \sigma_{e_k}^2), \forall i, j, k,\ i \neq j \tag{5.5}$$

According to [102], after taking the square-root the inequality in (5.5) becomes a SOC constraint, with $\boldsymbol{w}_{d_i}^{(p)}$ the variable to solve for. The motivation behind fixing $\boldsymbol{w}_{d_j}$ to $\boldsymbol{w}_{d_j}^{(p-1)}$ is based on the idea that after each iteration $\boldsymbol{w}_{d_j}^{(p-1)}$ approaches a constant: its optimal value that minimizes MSE_r. To incorporate the channel error bound (3.7), observe that from (3.6) we can use the triangle inequality and Cauchy-Schwarz inequality to reach the following result,

$$\begin{aligned} \|\boldsymbol{h}_{ik}^H \boldsymbol{w}_{d_i}^{(p)}\| &\leq \|\hat{\boldsymbol{h}}_{ik}^H \boldsymbol{w}_{d_i}^{(p)}\| + \|\boldsymbol{e}_{ik}^H \boldsymbol{w}_{d_i}^{(p)}\| \\ &\leq \|\hat{\boldsymbol{h}}_{ik}^H \boldsymbol{w}_{d_i}^{(p)}\| + \epsilon_i \|\boldsymbol{w}_{d_i}^{(p)}\|, \forall i, k. \end{aligned} \tag{5.6}$$

Hence, the following inequality

$$\|\hat{\boldsymbol{h}}_{ik}^H \boldsymbol{w}_{d_i}^{(p)}\| + \epsilon_i \|\boldsymbol{w}_{d_i}^{(p)}\| \leq \sqrt{\gamma_k (\|\boldsymbol{h}_{jk}^H \boldsymbol{w}_{d_j}^{(p-1)}\|^2 + \sigma_{ek}^2)} \tag{5.7}$$

implies (5.5) and so it can replace it as constraint. However, it is not equivalent to (5.2) and (3.7) in (5.3), but an approximation. Now looking at the objective function MSE_r, it can be rewritten as

$$\text{MSE}_r = \sum_{i=1}^{2} (\|\boldsymbol{w}_r^{(p)H} \boldsymbol{H}_{ir} \boldsymbol{w}_{d_i}^{(p)} - 1\|^2) + \sigma_r^2 \|\boldsymbol{w}_r\|^2 \tag{5.8}$$

Since we are solving for $\boldsymbol{w}_{d_1}$ and $\boldsymbol{w}_{d_2}$, we can ignore the last term in (5.8). By transforming the two sum terms in (5.8) into epigraph form [102], minimizing (5.8) would be equivalent to

$$\begin{aligned} &\min_{t_1, t_2, \boldsymbol{w}_{d_1}^{(p)}, \boldsymbol{w}_{d_2}^{(p)}} t_1 + t_2 \\ &\text{subject to } \|\boldsymbol{w}_r^{(p)H} \boldsymbol{H}_{ir} \boldsymbol{w}_{d_i}^{(p)} - 1\|^2 \leq t_i, \forall i \end{aligned} \tag{5.9}$$

By defining the following vectors

$$\boldsymbol{u}_i = \begin{bmatrix} 2(\boldsymbol{w}_r^{(p)H} \boldsymbol{H}_{ir} \boldsymbol{w}_{d_i}^{(p)} - 1) \\ t_i - 1 \end{bmatrix}, \forall i \tag{5.10}$$

and from [equations (7) and (8) in [104]], the constraints in (5.9) can be written as SOC

constraints to get

$$\begin{aligned} &\min_{t_1,t_2,\boldsymbol{w}_{d_1}^{(p)},\boldsymbol{w}_{d_2}^{(p)}} t_1 + t_2 \\ &\text{subject to } \|\boldsymbol{u}_i\| \leq t_i + 1, \forall i \end{aligned} \tag{5.11}$$

Thus, the optimization problem (5.3) is now reformulated as

$$\begin{aligned} \min_{t_1,t_2,\boldsymbol{w}_{d_1}^{(p)},\boldsymbol{w}_{d_2}^{(p)}} \quad & t_1 + t_2 \\ \text{subject to} \quad & \|\boldsymbol{w}_{d_i}^{(p)}\|^2 \leq P_{max}, \\ & \|\hat{\boldsymbol{h}}_{ik}^H \boldsymbol{w}_{d_i}^{(p)}\| + \epsilon_i \|\boldsymbol{w}_{d_i}^{(p)}\| \leq \alpha_{jk}^{(p)} \\ & \|\boldsymbol{u}_i\| \leq t_i + 1, \ \forall i, j, k, \ i \neq j \end{aligned} \tag{5.12}$$

where $\alpha_{jk}^{(p)} = \sqrt{\gamma_k(\|\boldsymbol{h}_{jk}^H \boldsymbol{w}_{d_j}^{(p-1)}\|^2 + \sigma_{ek}^2)}$. The problem in (5.12) is convex and can be solved with an optimization solver. After initializing with $\boldsymbol{w}_{d_i} = \sqrt{P_{max}/N_{d_i}}\mathbf{1}$, both sub-problems are iteratively solved until the value of MSE_r converges. Note that the proposed method consists only of two steps per iteration, with the second one solving for two vector variables at once. Meanwhile, the solution provided in [36] consists of three steps, each one solving for one vector variable at a time. Therefore, in addition to better MSE convergence results, as will be demonstrated later, the number of steps and consequently the time needed to find the beamforming vectors is shorter. As for the algorithm of Chapter 4, this algorithm is run every time an updated value of the main channel and eavesdropper channel estimate is obtained.

5.2 Broadcasting (BC) Stage

Similar to the MA stage, we design optimal beamforming vectors $\boldsymbol{v}_r$, $\boldsymbol{v}_{d_1}$ and $\boldsymbol{v}_{d_2}$ that minimize $\overline{\text{MSE}}_d$ subject to power constraints at the relay and SNR constraints at each

E_k. Given $\boldsymbol{v}_{e_k}$ in (5.1), the received SNR of s_r at E_k is

$$\mathrm{SNR}_k = \frac{\rho|\boldsymbol{v}_r^H \boldsymbol{g}_{rk}|^2}{\sigma_{ek}^2}, \quad \forall k \tag{5.13}$$

An upper bound λ_k is enforced on SNR_k. After including in the set of constraints the spherical bound on the channel error components, $\|\boldsymbol{f}_{rk}\| \leq \delta_r$, the following optimization problem is obtained:

$$\begin{aligned} \min_{\boldsymbol{v}_r, \boldsymbol{v}_{d_1}, \boldsymbol{v}_{d_2}} \quad & \overline{\mathrm{MSE}}_d \\ \text{subject to} \quad & |\boldsymbol{v}_r|^2 \leq P_{max}/\rho \\ & \mathrm{SNR}_k \leq \lambda_k \\ & \|\boldsymbol{f}_{rk}\| \leq \delta_r, \ \forall k \end{aligned} \tag{5.14}$$

This is also a non-convex optimization problem that is solved by considering the following two sub-problems:

Sub-problem 1: Here, the transmit beamforming vector $\boldsymbol{v}_r$ is fixed, leaving $\boldsymbol{v}_{d_1}$ and $\boldsymbol{v}_{d_2}$ as the optimization variables appearing only in the objective function. Therefore, the optimal value of $\boldsymbol{v}_{d_i}$ is obtained as in (4.26).

Sub-problem 2: Now, the receive beamforming vectors, $\boldsymbol{v}_{d_1}$ and $\boldsymbol{v}_{d_2}$, are fixed to their values from the previous sub-problem. Similar to the MA stage, the constraint on SNR_k in (5.14) is an SOC constraint, after taking the square-root, with $\boldsymbol{v}_r$ the variable to solve for. To incorporate the channel error bound (3.10), observe that from (3.9) we can use the triangle and Cauchy-Schwarz inequalities to reach the following result

$$\|\boldsymbol{g}_{rk}^H \boldsymbol{v}_r\| \leq \|\hat{\boldsymbol{g}}_{rk}^H \boldsymbol{v}_r\| + \|\boldsymbol{f}_{rk}^H \boldsymbol{v}_r\| \leq \|\hat{\boldsymbol{g}}_{rk}^H \boldsymbol{v}_r\| + \delta_r \|\boldsymbol{v}_r\|. \tag{5.15}$$

Hence, using the following inequality

$$\|\hat{\boldsymbol{g}}_{rk}^H \boldsymbol{v}_r\| + \delta_r \|\boldsymbol{v}_r\| \leq \sqrt{\lambda_k \sigma_{ek}^2/\rho}, \forall k \tag{5.16}$$

as a constraint instead of the SNR and error constraints in (5.14) keeps these constraints satisfied. Hence, the optimization problem (5.14) is transformed into the following

$$\begin{aligned} \min_{\boldsymbol{v}_r} \quad & \overline{\mathrm{MSE}}_d \\ \text{subject to} \quad & \|\boldsymbol{v}_r\|^2 \leq P_{max}/\rho \\ & \|\hat{\boldsymbol{g}}_{rk}^H \boldsymbol{v}_r\| + \delta_r \|\boldsymbol{v}_r\| \leq \sqrt{\lambda_k \sigma_{ek}^2/\rho},\ \forall k \end{aligned} \tag{5.17}$$

The modified problem (5.17) is a convex one and can be transformed into a SOC program of the variable $\boldsymbol{v}_r$ and solved. After initializing with $\boldsymbol{v}_r = \sqrt{P_{max}/\rho N_{d_i}}\mathbf{1}$, the two sub-problems are solved iteratively until $\overline{\mathrm{MSE}}_d$ converges. This method needs less time to run than the one in [36], making it a preferable, more efficient, approach. Finally it should also be noted here that the beamforming coefficients in both stages are updated whenever a new CSI estimate is available. As for the model in the previous chapter, the updating scheme should be matched to the channel coherence time.

Chapter 6

Simulation Results and Discussion

In this chapter, we provide simulation results produced by our proposed solutions of the problems given in the previous two chapters. After presenting the methodology, we describe the performance measures used to discuss the reliability of our algorithms. We provide as well, a comparison of computational efficiency between our method in Chapter 5 and the one in the literature [36].

6.1 Methodology

6.1.1 System Configuration

We consider a relaying system as in Figure 3.1 with two eavesdroppers and two antennas at all nodes. The noise variances are set to 1; $\boldsymbol{e}_{ik}$ and $\boldsymbol{e}_{rk}$ follow truncated Gaussian distributions with chosen values of ϵ_i^2 and δ_r^2. We also set $P_{max} = 10$ dB, $\rho = 1$ and $\gamma_k = \gamma$ and $\lambda_k = \lambda$, $\forall k$. The main channels $\boldsymbol{H}_{ir}$ and $\boldsymbol{G}_{rk}$ are generated with the same statistics, however, this does not have to be always the case. Also note that the same experiment could be done with any number of eavesdroppers. The results shown are averaged over many realizations of the channel matrices, the elements of which are i.i.d., drawn from a standard complex Gaussian distribution.

6.1.2 Performance Measures

The results presented next are the MSE at the destination and eavesdropper SINR distribution in each of the MA and BC stages of communication, in addition to the overall bit-error-rate (BER).

6.2 Results for Eavesdroppers Applying SC

In this section we provide experimental results for the suggested solution of the problem in Chapter 4 where the eavesdroppers are assumed to be using SC to beamform their signals.

6.2.1 MA Stage

Figure 6.1 shows the convergence of MSE_r for different values γ and ϵ_i in the MA stage. As expected, the MSE increases as γ decreases due to the fact a smaller γ forces a lower SINR level at the eavesdropper. The MSE also increases when ϵ_i increases since it means that our estimate of the eavesdropper channel is far off from its actual value. For all cases, the MSE requires only a few iterations to converge. Meanwhile in Figure 6.2 we observe how the SINR at the eavesdropper is maintained below any chosen γ showing the robustness and reliability of our algorithm.

6.2.2 BC Stage

The same analysis can be provided for the convergence of the MSE in the BC stage shown in Figure 6.3. Any decrease in λ or increase in δ_r results in an increase in MSE. The robustness of the suggested algorithm is also shown in Figure 6.4 where the SNR is maintained below any chosen λ.

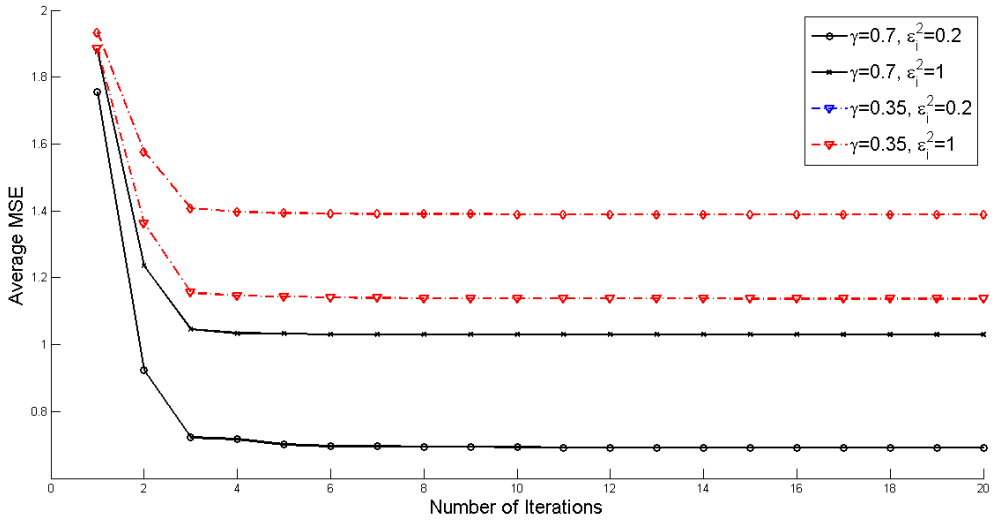

Figure 6.1: Convergence of MSE in MA stage

6.2.3 Bit-Error Rate

In Figure 6.5 we display the end-to-end BER at D_1 versus the transmit power constraint, P_{max}, for our method in Chapter 4 where the eavesdroppers apply SC using error bound values of $\epsilon_i^2 = \delta_r^2 = 0.02$. As shown, the BER increases when the SINR and SNR thresholds decrease. The reason for this is that decreasing the thresholds forces the MSE at the destination during each stage, MA and BC, to increase meaning that the PNC method makes more errors when deciding on a value of $(s_{d_1} + s_{d_2})$ which translates to more errors made at D_1. It may be argued that the BER values in Fig 6.5 are relatively high. However, depending on the system requirements and the standard, we may afford trading off reliability of the data transmission so that a robust and secure system communication is maintained between the legitimate devices. In case a high BER cannot be tolerated, we may increase the value of the transmit power constraint or obtain better eavesdropper channel estimates so that the values of ϵ_i and δ_r become smaller. Indeed, a smaller channel estimation error would improve the reliability of the beamforming scheme and the BER would decrease.

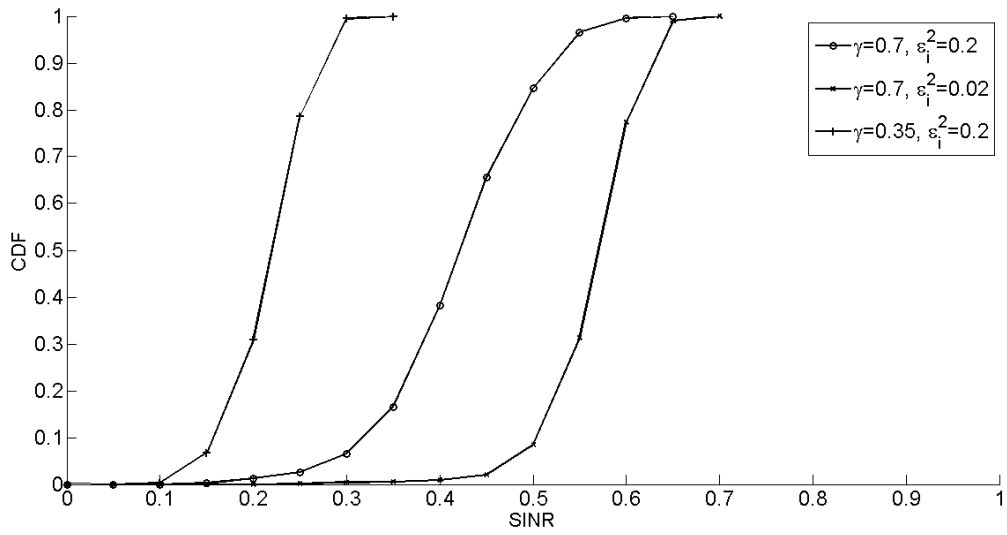

Figure 6.2: SINR distribution in MA stage

6.3 Results for Blind Eavesdroppers

Simulation results for the case of blind eavesdroppers are provided in this section and they are compared to the previously suggested solution in [36]. In the proposed SOC method for the MA stage in Chapter 5, we set $\gamma_k = 0.9\gamma \triangleq \gamma_s$. The reason for not using the same threshold is due to the different approximations made in the derivation of the methods. This empirical adjustment ensures that the SINR guarantees for both methods are the same. That is, with the adjusted γ_k, the eavesdropper SINR remains lower than the required level γ with near 100% probability.

6.3.1 MA Stage

Figures 6.6 and 6.7 provide a performance comparison between the solution we provided in Chapter 5 and the one given in [36], each for a different SINR level. As can be seen, our method results in a lower MSE_r with a few iterations required for convergence. This reliability is also shown in Figure 6.8 where we show the cumulative distribution function (CDF) of $\max\{\text{SINR}_1^{(1)}, \text{SINR}_1^{(2)}\}$ for the three methods. The SOC method produces a higher SINR due to a lower MSE, however, still satisfying the constraint.

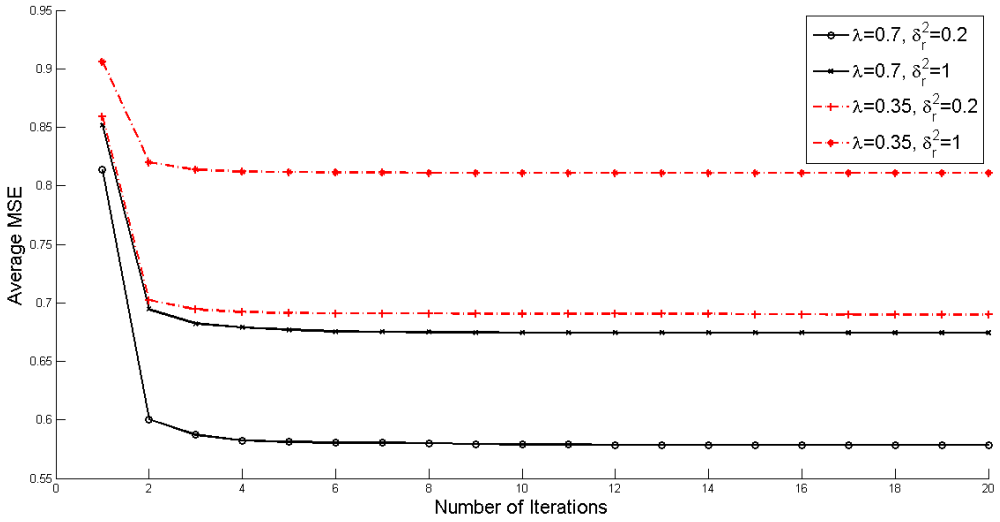

Figure 6.3: Convergence of MSE in BC Stage

6.3.2 BC Stage

Similarly, Figure 6.9 shows the MSE convergence during the BC stage. Both methods, the one in Chapter 5 and the one in [36], yield identical results, so we show only one curve for both. The main advantage of using the method in Chapter 5 is the time efficiency. The SNR CDFs for both methods in Chapter 5 and [36] are identical and the SNRs are below the threshold λ with probability 1 as seen in Figure 6.10.

6.3.3 Bit-Error Rate (BER)

In Figure 6.11 we display an end-to-end BER comparison between our method in Chapter 5 and the method in [36]. The BER at D_1 is plotted versus the maximum allowed transmit power for D_1 which is P_{max}. As shown, the BER for our SOC-based approach is lower than that of the SDP approach in the literature. This is mainly due to the fact that the SOC-based approach in the MA stage produced a lower MSE_r than the one achieved by the SDP approach.

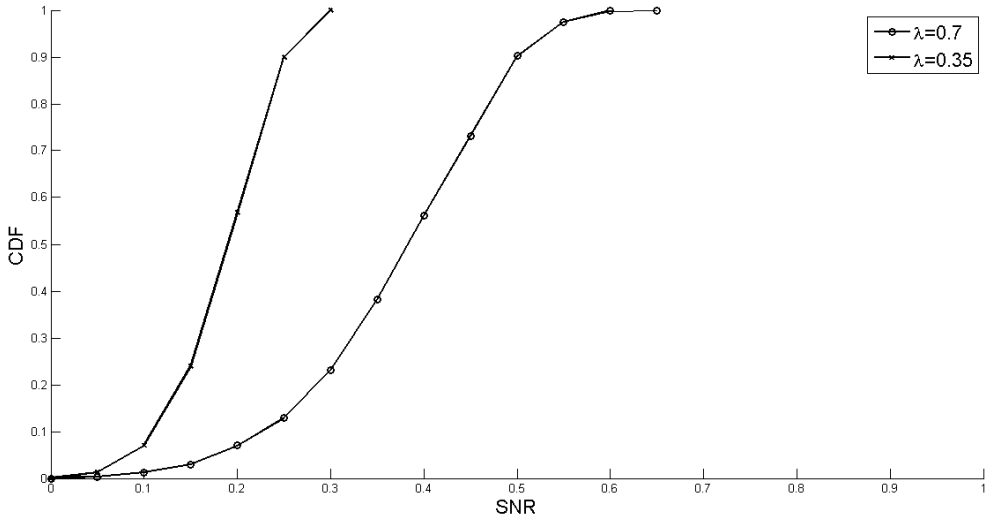

Figure 6.4: SNR distribution in BC stage for $\delta_r^2 = 0.2$

6.4 Computational Efficiency

To demonstrate the computational efficiency of our approach in Chapter 5, we show in Table 6.1 a comparison of the time needed for each algorithm to converge during the MA stage: the SC method in Chapter 4, the SOC method in Chapter 5 and the method in [36]. The comparison is done for different numbers of eavesdroppers K. The SOC method is apparently more efficient, especially as K increases. Table 6.2 shows a comparison of the time needed for the MSE to converge for each of the corresponding algorithms during the BC stage. Again, the method presented in Chapter 5 is more efficient. Looking at

MA Stage	$K = 1$	$K = 2$	$K = 4$	$K = 8$
SC	4.95	7.42	12.56	25.25
SOC	1.49	1.65	2.23	3.51
[24]	3.21	4.75	7.11	13.44

Table 6.1: Convergence time (in seconds) in MA stage

the SC case separately, the additional number of SINR constraints in (4.13) and (4.27) increase the time needed for the solver to find solutions.

In practice, the above algorithms would be run on specialized hardware, such that their running time would be much shorter than the ones given in the above tables and

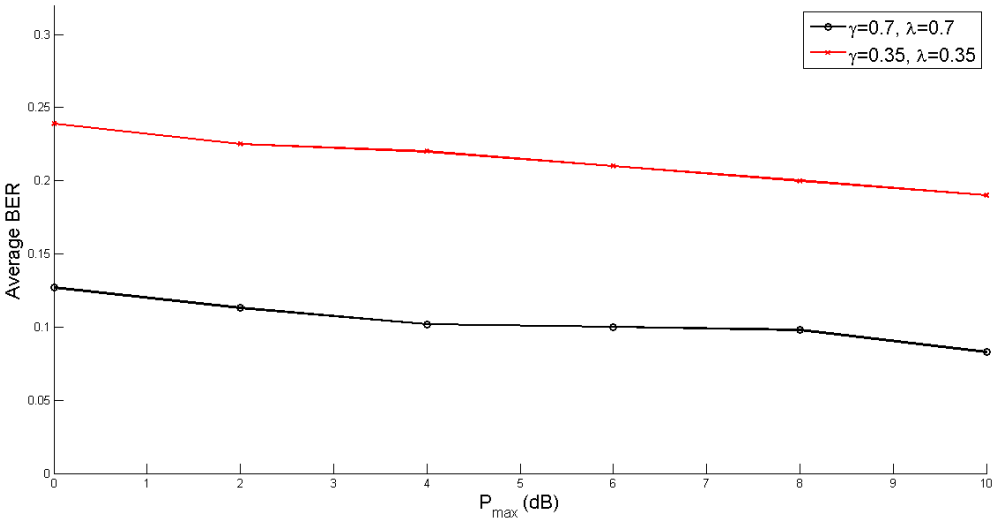

Figure 6.5: BER for $\epsilon_i^2 = \delta_r^2 = 0.02$

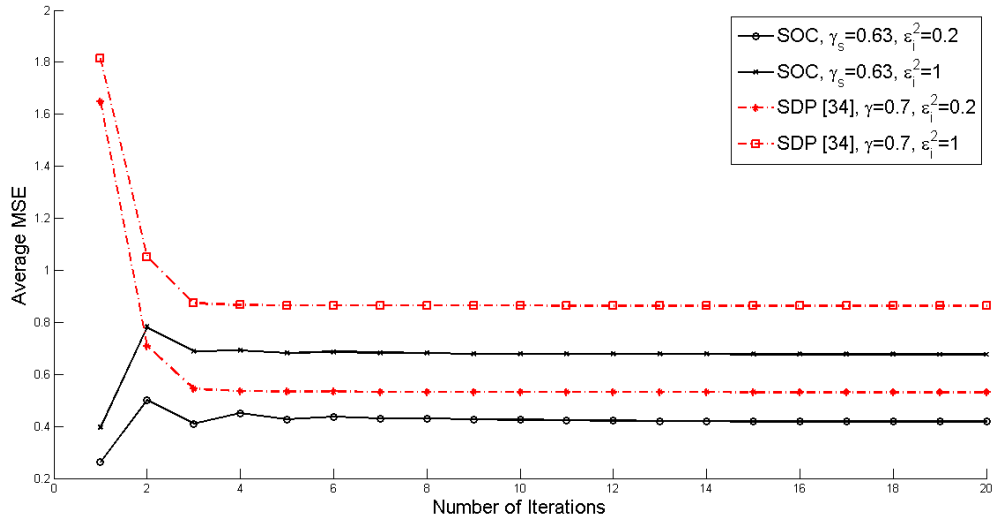

Figure 6.6: Convergence of MSE in MA stage for $\gamma = 0.7$

BC Stage	$K = 1$	$K = 2$	$K = 4$	$K = 8$
SC	1.57	2.28	3.57	5.91
SOC	1.16	1.34	1.67	2.42
[24]	1.28	1.75	2.23	3.52

Table 6.2: Convergence time (in seconds) in BC stage

also shorter than the channel coherence time. However, they would remain proportional and the same efficiency ratio would be maintained as in Tables 6.1 and 6.2.

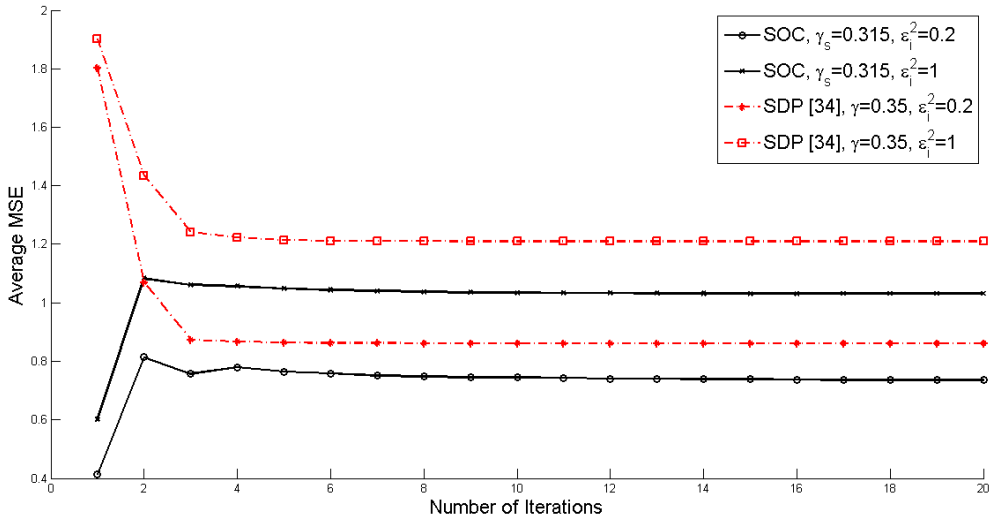

Figure 6.7: Convergence of MSE in MA stage for $\gamma = 0.35$

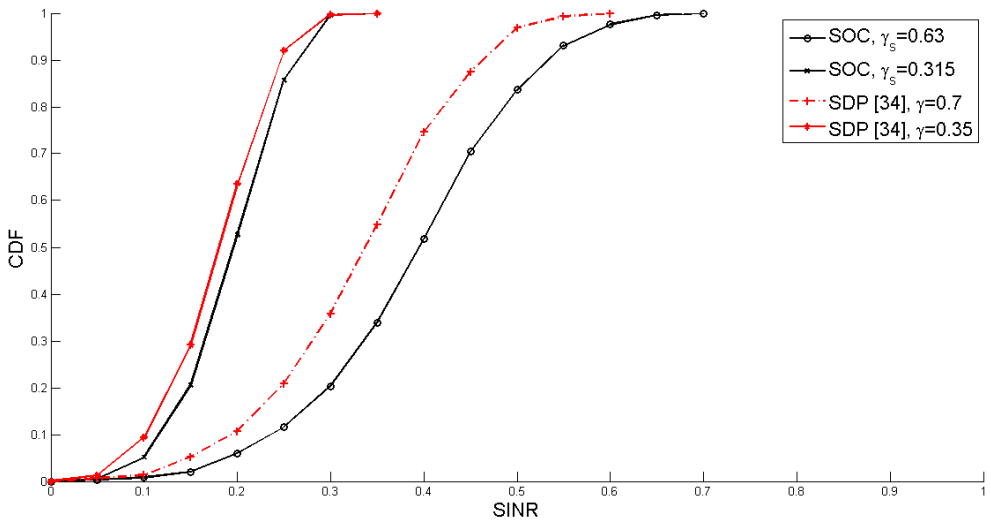

Figure 6.8: SINR distribution in MA stage for $\epsilon_i^2 = 0.02$

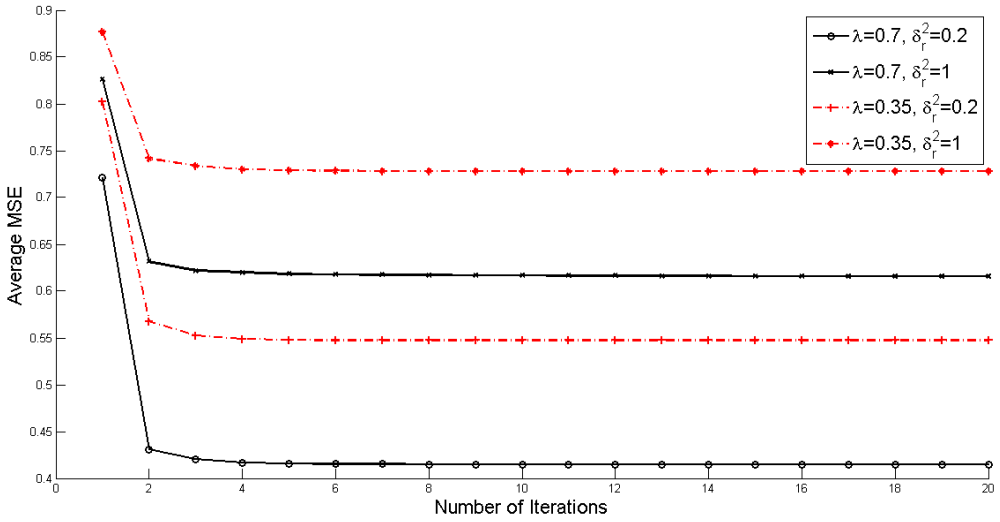

Figure 6.9: Convergence of MSE in BC Stage

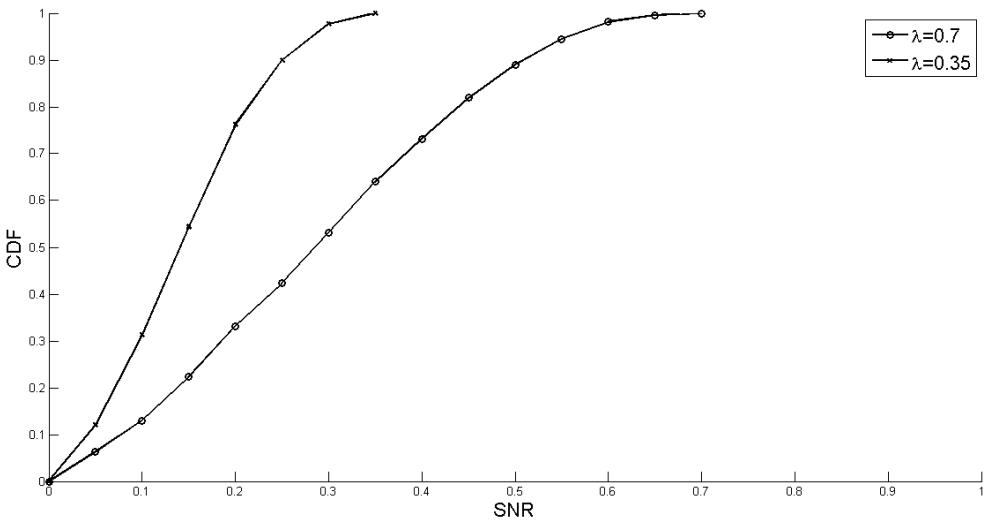

Figure 6.10: SNR distribution in BC stage for $\delta_r^2 = 0.2$

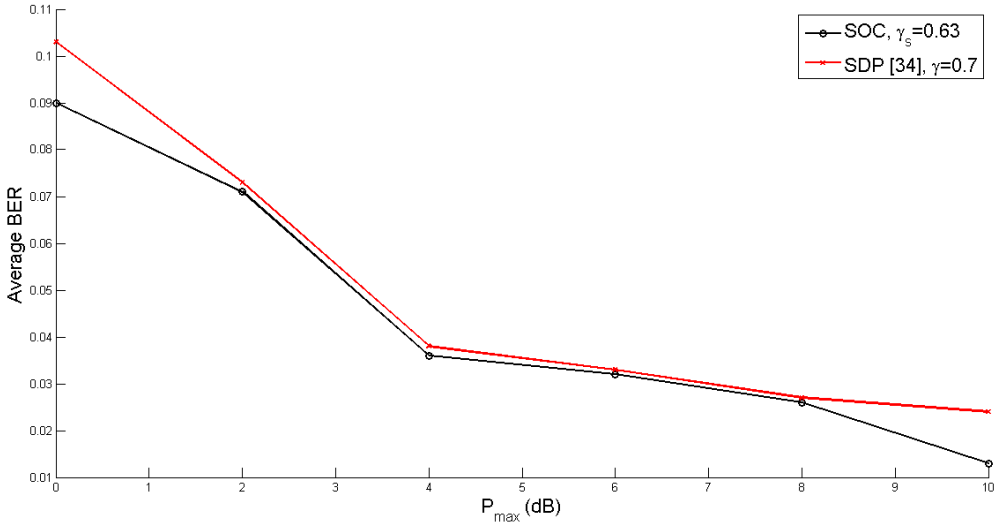

Figure 6.11: BER for $\epsilon_i^2 = \delta_r^2 = 0.2$

Chapter 7

Conclusion

In this thesis, we investigated the problem of PLS in a D2D MIMO relay network with multiple eavesdroppers. First, we presented some background and history on PLS in Chapter 2. We introduced the wiretap channel and discussed single and multi-antenna models that have been previously studied. Additionally, we discussed broadcast and muti-access channels before diving into relay-based wiretap channels.

In Chapter 3, we outlined the system model along with the problem formulation. Assuming imperfect eavesdropper CSI at the transmitting node(s), the general approach is based on choosing the beamforming vectors at the intended transmitter and receiver that minimize the MSE at the intended receiver while maintaining an eavesdropper SINR or SNR below a specified threshold and satisfying transmit power constraints. Since the transmitter uses an estimate of the eavesdropper CSI to apply this approach, errors in the estimation needed to be taken into account. A deterministic bounded error model was assumed. On the other hand, the eavesdropper can apply one of many beamforming techniques to the signals arriving using the available CSI.

In Chapter 4, we solved the beamforming problem with eavesdroppers applying SC to their incoming signals. The eavesdroppers were assumed to know their channels partially and used their channel estimates to perform SC. To account for the worst case scenario, they were also assumed to know the transmit beamforming vectors at the devices and

the relay. The results in Chapter 6 show that the SINR is always below the threshold with the MSE converging rapidly with the number of iterations.

In Chapter 5, we solved the beamforming problem with blind eavesdroppers. The eavesdroppers were assumed to not know their channels or the transmit beamforming vectors. This problem is also solved assuming the eavesdropper channel estimation error is deterministic and spherically bounded. The results in Chapter 6 show that the MSE achieved is below the value achieved by another approach given in the literature [36] and the SINR is maintained below an equivalent threshold. Furthermore, simulations showed that our approach is more computationally efficient as it needs at most one third of the time than the approach in the literature needs.

As future work, the beamforming problem with eavesdroppers applying MMSE to their signals could be investigated. Each eavesdropper in this model chooses its beamforming vectors that minimize the MSE of the signal it receives. This in turn would increase its SINR making it hard to choose low SINR constraints without suffering a large MSE at the intended destination. Furthermore, the application of the above PLS techniques to commercially deployed wireless systems is largely unexplored and remains an interesting avenue for future work. Another challenging avenue is the consideration of PLS aspects in the development of future wireless communications standards. Recently, a number of works such as [105] have appeared that address the use PLS techniques to safeguard future 5G networks.

It is anticipated that new PLS techniques will need to be devised as new questions and transmission scenario emerge, especially in the context of multi-user systems. From a secrecy aspect, cases such as massive MIMO systems, overlay cognitive radio networks and smart grid systems have not been seriously investigated. Finally, the connection and tradeoff between PLS and classic cryptography could be a major research topic in the near future.

Bibliography

[1] Y.-C. Liang, K.-C. Chen, G. Y. Li, and P. Mahonen, "Cognitive radio networking and communications: An overview," *IEEE Trans. on Vehicular Technology*, vol. 60, no. 7, pp. 3386–3407, 2011.

[2] J. Wang, M. Ghosh, and K. Challapali, "Emerging cognitive radio applications: A survey," *IEEE Communications Magazine*, vol. 49, no. 3, pp. 74–81, 2011.

[3] A. Asadi, Q. Wang, and V. Mancuso, "A survey on device-to-device communication in cellular networks," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1801–1819, 2014.

[4] D. Zhu, A. L. Swindlehurst, S. A. A. Fakoorian, W. Xu, and C. Zhao, "Device-to-device communications: The physical layer security advantage," in *Proc. IEEE ICASSP*, pp. 1606–1610, 2014.

[5] Y.-D. Lin and Y.-C. Hsu, "Multihop cellular: A new architecture for wireless communications," in *Proc. IEEE International Conference on Computer Communications (INFOCOM)*, vol. 3, pp. 1273–1282, 2000.

[6] J. Du, W. Zhu, J. Xu, Z. Li, and H. Wang, "A compressed HARQ feedback for device-to-device multicast communications," in *Proc. of IEEE Vehicular Technology Conference (VTC) Fall 2012*, pp. 1–5.

[7] B. Zhou, H. Hu, S.-Q. Huang, and H.-H. Chen, "Intracluster device-to-device relay algorithm with optimal resource utilization," *IEEE Trans. on Vehicular Technology*, vol. 62, no. 5, pp. 2315–2326, 2013.

[8] L. Lei, Z. Zhong, C. Lin, and X. Shen, "Operator controlled device-to-device communications in lte-advanced networks," *IEEE Wireless Communications*, vol. 19, no. 3, p. 96, 2012.

[9] K. Doppler, M. Rinne, C. Wijting, C. B. Ribeiro, and K. Hugl, "Device-to-device communication as an underlay to LTE-advanced networks," *IEEE Communications Magazine*, vol. 47, no. 12, pp. 42–49, 2009.

[10] N. K. Pratas and P. Popovski, "Low-rate machine-type communication via wireless device-to-device (D2D) links," *arXiv preprint, arXiv:1305.6783*, 2013.

[11] X. Bao, U. Lee, I. Rimac, and R. R. Choudhury, "Dataspotting: offloading cellular traffic via managed device-to-device data transfer at data spots," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 14, no. 3, pp. 37–39, 2010.

[12] B. Wang and K. R. Liu, "Advances in cognitive radio networks: A survey," *IEEE Journal of Selected Topics in Signal Processing*, vol. 5, no. 1, pp. 5–23, 2011.

[13] S. Zhang, S. C. Liew, and P. P. Lam, "Hot topic: physical-layer network coding," in *Proc. of the 12th annual ACM International Conference on Mobile Computing and Networking*, pp. 358–365, 2006.

[14] Y. Wu, P. A. Chou, S.-Y. Kung, *et al.*, "Information exchange in wireless networks with network coding and physical-layer broadcast," in *Proc. 39th Annual Conference on Information Systems and Sciences*, 2005.

[15] G. Baldini, T. Sturman, A. R. Biswas, R. Leschhorn, G. Godor, and M. Street, "Security aspects in software defined radio and cognitive radio networks: a survey

and a way ahead," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, pp. 355–379, 2012.

[16] J. Mitola and G. Q. Maguire, "Cognitive radio: making software radios more personal," *IEEE Personal Communications*, vol. 6, no. 4, pp. 13–18, 1999.

[17] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[18] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, 2008.

[19] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. on Information Theory*, vol. 56, no. 7, pp. 3088–3104, 2010.

[20] J. Yang, B. Champagne, Y. Zou, and L. Hanzo, "MIMO AF relaying security: Robust transceiver design in the presence of multiple eavesdroppers," in *Proc. IEEE International Conference on Communications (ICC)*, pp. 4937–4942, 2015.

[21] J. Yang, B. Champagne, Q. Li, and L. Hanzo, "Secure MIMO AF relaying design: An intercept probability constrained approach," in *Proc. IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, 2015.

[22] T. Van Nguyen and H. Shin, "Power allocation and achievable secrecy rates in MISOME wiretap channels," *IEEE Communications Letters*, vol. 15, no. 11, pp. 1196–1198, 2011.

[23] J. Xiong, K.-K. Wong, D. Ma, and J. Wei, "A closed-form power allocation for minimizing secrecy outage probability for MISO wiretap channels via masked beamforming," *IEEE Communications Letters*, vol. 16, no. 9, pp. 1496–1499, 2012.

[24] Q. Li, Y. Yang, W.-K. Ma, M. Lin, J. Ge, and J. Lin, "Robust cooperative beamforming and artificial noise design for physical-layer secrecy in AF multi-antenna multi-relay networks," *IEEE Trans. on Signal Processing*, vol. 63, no. 1, pp. 206–220, 2015.

[25] M. Pei, J. Wei, K.-K. Wong, and X. Wang, "Masked beamforming for multiuser MIMO wiretap channels with imperfect CSI," *IEEE Trans. on Wireless Communications*, vol. 11, no. 2, pp. 544–549, 2012.

[26] A. Mukherjee and A. L. Swindlehurst, "Utility of beamforming strategies for secrecy in multiuser MIMO wiretap channels," in *Proc. of 47th Annual Allerton Conf. on Communication, Control and Computing*, pp. 1134–1141, 2009.

[27] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. on Signal Processing*, vol. 59, no. 1, pp. 351–361, 2011.

[28] S. Gerbracht, A. Wolf, and E. A. Jorswieck, "Beamforming for fading wiretap channels with partial channel information," in *Proc. of Int. ITG Workshop on Smart Antennas (WSA)*, pp. 394–401, 2010.

[29] C. Wang and H.-M. Wang, "Robust joint beamforming and jamming for secure AF networks: Low-complexity design," *IEEE Trans. on Vehicular Technology*, vol. 64, no. 5, pp. 2192–2198, 2015.

[30] Q. Li and W.-K. Ma, "Optimal and robust transmit designs for MISO channel secrecy by semidefinite programming," *IEEE Trans. on Signal Processing*, vol. 59, no. 8, pp. 3799–3812, 2011.

[31] K. Cumanan, Z. Ding, B. Sharif, G. Y. Tian, and K. K. Leung, "Secrecy rate optimizations for a MIMO secrecy channel with a multiple-antenna eavesdropper," *IEEE Trans. on Vehicular Technology*, vol. 63, no. 4, pp. 1678–1690, 2014.

[32] K. Xiong, Y. Zhang, D. Li, C.-Y. Chang, and Z. Zhong, "Multiantenna relay beamforming design for QoS discrimination in two-way relay networks," *The Scientific World Journal*, 2013.

[33] H. Reboredo, J. Xavier, and M. R. Rodrigues, "Filter design with secrecy constraints: The MIMO gaussian wiretap channel," *IEEE Trans. on Signal Processing*, vol. 61, no. 15, pp. 3799–3814, 2013.

[34] Z. Shu, Y. Qian, and S. Ci, "On physical layer security for cognitive radio networks," *IEEE Network Magazine*, vol. 27, no. 3, pp. 28–33, 2013.

[35] K. Jayasinghe, P. Jayasinghe, N. Rajatheva, and M. Latva-aho, "Physical layer security for relay assisted MIMO D2D communication," in *Proc. of IEEE International Conference on Communication Workshop*, pp. 651–656, 2015.

[36] K. Jayasinghe, P. Jayasinghe, N. Rajatheva, and M. Latva-Aho, "Secure beamforming design for physical layer network coding based MIMO two-way relaying," *IEEE Communications Letters*, vol. 18, no. 7, pp. 1270–1273, 2014.

[37] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[38] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[39] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. on Information Theory*, vol. 39, no. 3, pp. 733–742, 1993.

[40] V. Korzhik and V. Yakovlev, "Nonasymptotic estimates for efficiency of code jamming in a wire-tap channel," *Problemy peredachi informatsii*, vol. 17, no. 4, pp. 11–18, 1981.

[41] A. Carleial and M. Hellman, "A note on Wyner's wiretap channel (corresp.)," *IEEE Trans. on Information Theory*, vol. 23, no. 3, pp. 387–390, 1977.

[42] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Trans. on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[43] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[44] C. Mitrpant, A. H. Vinck, and Y. Luo, "An achievable region for the gaussian wire-tap channel with side information," *IEEE Trans. on Information Theory*, vol. 52, no. 5, pp. 2181–2190, 2006.

[45] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," *AT&T Bell Laboratories Technical Journal*, vol. 63, no. 10, pp. 2135–2157, 1984.

[46] J. Barros and M. R. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE International Symposium on Information Theory*, pp. 356–360, 2006.

[47] Z. Li, R. Yates, and W. Trappe, "Secret communication with a fading eavesdropper channel," in *Proc. IEEE International Symposium on Information Theory*, pp. 1296–1300, 2007.

[48] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. on Information Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

[49] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, "Compound wiretap channels," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, pp. 1–12, 2009.

[50] A. O. Hero, "Secure space-time communication," *IEEE Trans. on Information Theory*, vol. 49, no. 12, pp. 3235–3249, 2003.

[51] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. International Symposium on Information Theory*, pp. 2152–2155, 2005.

[52] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proc. IEEE 41st Annual Conference on Information Sciences and Systems*, pp. 905–910, 2007.

[53] S. Shafiee and S. Ulukus, "Achievable rates in gaussian MISO channels with secrecy constraints," in *Proc. IEEE International Symposium on Information Theory*, pp. 2466–2470, 2007.

[54] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the gaussian MIMO wiretap channel," in *Proc. IEEE International Symposium on Information Theory*, pp. 2471–2475, 2007.

[55] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—part II: The MIMOME wiretap channel," *IEEE Trans. on Information Theory*, vol. 56, no. 11, pp. 5515–5532, 2010.

[56] R. Negi and S. Goel, "Secret communication using artificial noise," in *IEEE Vehicular Technology Conference*, vol. 62, p. 1906, Citeseer, 2005.

[57] A. Mukherjee and A. L. Swindlehurst, "Fixed-rate power allocation strategies for enhanced secrecy in MIMO wiretap channels," in *Proc. IEEE 10th Workshop on Signal Processing Advances in Wireless Communications*, pp. 344–348, 2009.

[58] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization," *IEEE Trans. on Signal Processing*, vol. 61, no. 10, pp. 2704–2717, 2013.

[59] P.-H. Lin, S.-H. Lai, S.-C. Lin, and H.-J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1728–1740, 2013.

[60] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. on Information Theory*, vol. 57, no. 8, pp. 4961–4972, 2011.

[61] J. Li and A. Petropulu, "Transmitter optimization for achieving secrecy capacity in gaussian MIMO wiretap channels," *arXiv preprint, arXiv:0909.2622*, 2009.

[62] R. Bustin, R. Liu, H. V. Poor, and S. Shamai, "An MMSE approach to the secrecy capacity of the MIMO gaussian wiretap channel," *EURASIP Journal on Wireless Communications and Networking*, no. 1, p. 1, 2009.

[63] S. A. A. Fakoorian and A. L. Swindlehurst, "Full rank solutions for the MIMO gaussian wiretap channel with an average power constraint," *IEEE Trans. on Signal Processing*, vol. 61, no. 10, pp. 2620–2631, 2013.

[64] S. Loyka and C. D. Charalambous, "On optimal signaling over secure MIMO channels," in *Proc. IEEE International Symposium on Information Theory (ISIT)*, pp. 443–447, 2012.

[65] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. on Information Theory*, vol. 54, no. 6, pp. 2470–2492, 2008.

[66] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "Multiple-input multiple-output gaussian broadcast channels with confidential messages," *IEEE Trans. on Information Theory*, vol. 56, no. 9, pp. 4215–4227, 2010.

[67] H. Weingarten, Y. Steinberg, and S. Shamai, *The Capacity Region of the Gaussian MIMO Broadcast Channel*. Department of Electrical Engineering, Technion-Israel Institute of Technology, 2004.

[68] A. Dembo, T. M. Cover, and J. A. Thomas, "Information theoretic inequalities," *IEEE Trans. on Information Theory*, vol. 37, no. 6, pp. 1501–1518, 1991.

[69] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "MIMO gaussian broadcast channels with confidential and common messages," *arXiv preprint, arXiv:1001.2806*, 2010.

[70] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "The secrecy capacity region of the gaussian MIMO broadcast channel," *IEEE Trans. on Information Theory*, vol. 59, no. 5, pp. 2673–2682, 2013.

[71] E. Ekrem and S. Ulukus, "The secrecy capacity region of the gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. on Information Theory*, vol. 57, no. 4, pp. 2083–2114, 2011.

[72] S. A. A. Fakoorian and A. L. Swindlehurst, "On the optimality of linear precoding for secrecy in the MIMO broadcast channel," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1701–1713, 2013.

[73] S. A. A. Fakoorian and A. L. Swindlehurst, "Dirty paper coding versus linear GSVD-based precoding in MIMO broadcast channel with confidential messages," in *Proc. IEEE Global Communications Conference (GLOBECOM)*, pp. 1–5, 2011.

[74] G. Geraci, M. Egan, J. Yuan, A. Razi, and I. B. Collings, "Secrecy sum-rates for multi-user MIMO regularized channel inversion precoding," *IEEE Trans. on Communications*, vol. 60, no. 11, pp. 3472–3482, 2012.

[75] G. Geraci, R. Couillet, J. Yuan, M. Debbah, and I. B. Collings, "Large system analysis of linear precoding in MISO broadcast channels with confidential messages," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1660–1671, 2013.

[76] G. Geraci, A. Y. Al-nahari, J. Yuan, and I. B. Collings, "Linear precoding for broadcast channels with confidential messages under transmit-side channel correlation," *IEEE Communications Letters*, vol. 17, no. 6, pp. 1164–1167, 2013.

[77] G. Geraci, S. Singh, J. G. Andrews, J. Yuan, and I. B. Collings, "Secrecy rates in broadcast channels with confidential messages and external eavesdroppers," *IEEE Trans. on Wireless Communications*, vol. 13, no. 5, pp. 2931–2943, 2014.

[78] R. Liu, I. Maric, R. D. Yates, and P. Spasojevic, "The discrete memoryless multiple access channel with confidential messages," *arXiv preprint, cs/0605005*, 2006.

[79] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. on Information Theory*, vol. 54, no. 3, pp. 976–1002, 2008.

[80] E. Tekin and A. Yener, "The gaussian multiple access wire-tap channel," *IEEE Trans. on Information Theory*, vol. 54, no. 12, pp. 5747–5755, 2008.

[81] E. Tekin and A. Yener, "The general gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. on Information Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.

[82] R. Liu, Y. Liang, and H. V. Poor, "Fading cognitive multiple-access channels with confidential messages," *IEEE Trans. on Information Theory*, vol. 57, no. 8, pp. 4992–5005, 2011.

[83] Y. Oohama, "Capacity theorems for relay channels with confidential messages," in *Proc. IEEE International Symposium on Information Theory*, pp. 926–930, 2007.

[84] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. on Information Theory*, vol. 56, no. 8, pp. 3807–3827, 2010.

[85] X. He and A. Yener, "Two-hop secure communication using an untrusted relay," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, p. 1, 2009.

[86] X. He and A. Yener, "The role of an untrusted relay in secret communication," in *Proc. IEEE International Symposium on Information Theory*, pp. 2212–2216, 2008.

[87] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," *IEEE Trans. on Information Theory*, vol. 57, no. 1, pp. 137–155, 2011.

[88] C. Jeong, I.-M. Kim, and D. I. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system," *IEEE Trans. on Signal Processing*, vol. 60, no. 1, pp. 310–325, 2012.

[89] J. Mo, M. Tao, Y. Liu, B. Xia, and X. Ma, "Secure beamforming for MIMO two-way transmission with an untrusted relay," in *Proc. IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 4180–4185, 2013.

[90] J. Huang and A. L. Swindlehurst, "Joint transmit design and node selection for one-way and two-way untrusted relay channels," in *Proc. IEEE Asilomar Conference on Signals, Systems and Computers*, pp. 1555–1559, 2013.

[91] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, 2010.

[92] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. on Signal Processing*, vol. 59, no. 10, pp. 4985–4997, 2011.

[93] Y. Yang, Q. Li, W.-K. Ma, J. Ge, and P. Ching, "Cooperative secure beamforming for af relay networks with multiple eavesdroppers," *IEEE Signal Processing Letters*, vol. 20, no. 1, pp. 35–38, 2013.

[94] J. Mo, M. Tao, and Y. Liu, "Relay placement for physical layer security: A secure connection perspective," *IEEE Communications Letters*, vol. 16, no. 6, pp. 878–881, 2012.

[95] X. Wang, K. Wang, and X.-D. Zhang, "Secure relay beamforming with imperfect channel side information," *IEEE Trans. on Vehicular Technology*, vol. 62, no. 5, pp. 2140–2155, 2013.

[96] M. Jilani and T. Ohtsuki, "Joint SVD-GSVD precoding technique and secrecy capacity lower bound for the MIMO relay wire-tap channel," *EURASIP Journal on Wireless Communications and Networking*, vol. 2012, no. 1, pp. 1–8, 2012.

[97] Y. Zou, X. Wang, and W. Shen, "Intercept probability analysis of cooperative wireless networks with best relay selection in the presence of eavesdropping attack," in *Proc. IEEE International Conference on Communications (ICC)*, pp. 2183–2187, 2013.

[98] A. Mukherjee and A. L. Swindlehurst, "Securing multi-antenna two-way relay channels with analog network coding against eavesdroppers," in *Proc. IEEE 11th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pp. 1–5, 2010.

[99] Z. Gao, Y.-H. Yang, and K. R. Liu, "Anti-eavesdropping space-time network coding for cooperative communications," *IEEE Trans. on Wireless Communications*, vol. 10, no. 11, pp. 3898–3908, 2011.

[100] S. Al-Sayed and A. Sezgin, "Secrecy in gaussian MIMO bidirectional broadcast wiretap channels: Transmit strategies," in *Proc. Conference Record of the Forty Fourth IEEE Asilomar Conference on Signals, Systems and Computers*, pp. 285–289, 2010.

[101] R. Zhang, L. Song, Z. Han, B. Jiao, and M. Debbah, "Physical layer security for two way relay communications with friendly jammers," in *Proc. IEEE Global Telecommunications Conference (GLOBECOM)*, pp. 1–6, 2010.

[102] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.

[103] S. Sesia, I. Toufik, and M. Baker, *LTE-the UMTS long term evolution*. Wiley Online Library, 2015.

[104] M. S. Lobo, L. Vandenberghe, S. Boyd, and H. Lebret, "Applications of second-order cone programming," *Linear Algebra and its Applications*, vol. 284, no. 1, pp. 193–228, 1998.

[105] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20–27, 2015.