Chapter 6

MIMO Signal Processing Algorithms for Enhanced Physical Layer Security

Amitav Mukherjee
Hitachi America Ltd.

S. Ali A. Fakoorian
University of California Irvine

Jing Huang
University of California Irvine

Lee Swindlehurst
University of California Irvine

The use of physical layer methods for improving the security of wireless links has recently become the focus of a considerable research effort. Such methods can be used in combination with cryptography to enhance the exchange of confidential messages over a wireless medium in the presence of unauthorized eavesdroppers, or they can be used to enable secrecy in the absence of shared secret keys through the use of coding strategies, jamming or beamforming. Indeed, one of the driving forces behind the recent emergence of physical layer techniques for security is the push toward adding extra degrees of freedom in the form of multiple antennas at the transmitter and receiver of the link. Multiple-input multiple-output (MIMO) wireless systems have been extensively studied during the past two decades, and their potential gains in throughput, diversity, and range have been well quantified. MIMO approaches are now an integral part of the WiFi and 4G standards in use today. It is not surprising that MIMO architectures are useful in improving wireless security as well, since they can provide focused transmit selectivity of both information and noise toward desired and undesired receivers. In this chapter, we discuss a number of different ways that physical layer security can be achieved in wireless networks with MIMO links. We will focus primarily on signal processing related issues (e.g., beamforming, power control, resource allocation) that enable reliable reception at intended recipients and minimize data leakage to eavesdroppers, and we will consider a variety of different MIMO settings including point-to-point, broadcast, interference, and multi-hop networks. We cannot offer an exhaustive survey of such methods in just a single chapter; instead, we present a few representative approaches that illustrate
the gains that multiple antennas provide. Additional and more complete treatments of the physical layer security problem can be found in [1–4] as well as other chapters in this book.

6.1 Introduction

The availability of multiple antennas in multiuser networks is akin to a double-edged sword from the security point of view: the enhanced transmission quality of the legitimate users is offset by the increased interception capabilities of unauthorized receivers. Consequently, MIMO signal processing techniques must be carefully designed in order to ensure both the reliability of the desired communication links and the degradation of those for the eavesdroppers. The chapter commences with a description of transceiver optimization algorithms for the conventional three-user MIMO wiretap channel with perfect channel state information (CSI). As with MIMO techniques in general, the availability and accuracy of CSI is crucial to success, and plays a major role in achieving secure communications. Thus, we subsequently examine robust techniques that compensate for partial or inaccurate CSI in the MIMO wiretap channel. A key secrecy-enhancing technique in scenarios with partial CSI is the embedding of “artificial noise” or jamming signals together with the confidential message, the objective being to selectively degrade the signal quality at any unintended receiver.

Generalizing to multiuser wiretap scenarios opens new avenues for study, since resource allocation among multiple legitimate users must be balanced with potentially limited cooperation between them. Two prime examples are the MIMO wiretap channel with external cooperative jammers or helpers, and the broadcast MIMO wiretap network with multiple receivers. For the former example, we describe the optimal precoding and power allocation operations at the helping jammer in order to maximally suppress the information decodable at the eavesdroppers, without information being exchanged with the transmitter. In the latter example, we present linear and non-linear MIMO downlink precoding algorithms that are categorized by the level of eavesdropper CSI assumed. Subsequently, we study MIMO interference networks with secrecy constraints as a more involved wiretap network scenario, since in this application the design of MIMO precoders requires that the confidential information exchanged between pairs is suppressed at cochannel terminals without causing excessive degradation to the secrecy sum rate or secure degrees of freedom.

Finally, we examine MIMO multi-hop networks where intermediary relays play a pivotal role in establishing secure one-way or two-way links. In some cases, the relay(s) acts as an enabler in enhancing secrecy, for example by acting as an external jammer if a direct source-to-destination link is available. Alternatively, the relay itself may be an unauthenticated node from which the exchanged messages must be kept secret. For each case, we examine MIMO relay optimization procedures and their robust counterparts, depending upon the CSI assumed to be known.

6.2 Physical Layer Security

6.2.1 Signal Processing Aspects

An early information-theoretic treatment of physical layer security by Wyner [5] in 1975 demonstrated that perfect secrecy is achievable in the wiretap channel without the use of encryption keys, provided that the eavesdropper’s channel is of lower quality than the desired receiver. In general, approaches to physical layer security in the information theory literature have primarily focused on code design and bounds for achievable secrecy capacities/regions. Such analyses frequently involve idealized assumptions of perfectly known
global CSI, random coding arguments, Gaussian inputs, and so on. The signal processing perspective on physical layer security then naturally pertains to optimal and near-optimal transceiver design in situations where these assumptions may or may not hold. As a result, the optimization of power allocation algorithms together with the design of spatial transmit/receive filters under perfect and imperfect channel state information form the major thrust of signal processing research in this area.

6.2.2 Secrecy Performance Metrics

Secret communication problems arise in multi-terminal networks comprising a minimum of three nodes: the legitimate transmitter and its intended receiver, and an unauthorized interloper commonly referred to as an eavesdropper. This three-terminal system is referred to as the wiretap channel [1]. Several of the most frequently used secrecy metrics are introduced below, while their formal descriptions are relegated to subsequent sections.

- **Secrecy Rate**—In the wiretap channel, the secrecy rate is a transmission rate that can be reliably supported on the primary channel, but which is undecodable on the eavesdropper’s channel. For Gaussian channels, it is calculated as the difference between the mutual information on the primary and eavesdropper’s channels. Secrecy capacity is achieved when the secrecy rate is maximized. When multiple communication links are present, for example as in broadcast or interference channels, then one is typically interested in defining the achievable secrecy rate or secrecy capacity regions or the aggregate secrecy sum rate or sum capacity.

- **Secrecy Outage Probability**—The secrecy outage probability (SOP) represents the probability that a certain target secrecy rate is not achieved for a given communication link. The SOP characterizes the likelihood of simultaneously reliable and secure data transmission, and is most often employed in situations where only statistical CSI about the eavesdropper is available.

- **Secret Diversity/Multiplexing Gain**—Secret diversity and multiplexing gains for wiretap channels can be defined similarly to their counterparts in conventional MIMO systems [6]. The secret diversity gain is the asymptotic rate of decrease with signal-to-noise ratio (SNR) in probability of error at the desired receiver when subject to secrecy constraints, while the secret multiplexing gain (or degrees of freedom) is the asymptotic rate of increase with SNR in the secrecy rate. The secret diversity/multiplexing trade-off (DMT) captures the interplay between these competing metrics.

- **Secret Key Rate**—The secret key rate quantifies the rate at which legitimate users can agree upon a shared key sequence by exchanging messages over a public channel that is observable to eavesdroppers.

6.2.3 The Role of CSI

Realization of the gains promised by multiple antenna transceivers hinges in large part on the ability of the system to obtain and exploit accurate CSI. In the wiretap channel, this includes not only CSI for the primary link, but also possibly CSI for the eavesdroppers.

- **Complete CSI**—Intuitively, the greatest level of security can be achieved when the legitimate transmitters have complete knowledge of the wireless channels to all receivers, including the eavesdroppers. Such information may be available if the potential eavesdropper is an active network node, and has previously communicated with the transmitter. The knowledge of global CSI can be exploited to design MIMO transmit precoders that minimize the information leaked into eavesdropper channels, or to accurately direct jamming signals toward the eavesdroppers, as described in the following sections.
Partial CSI—In many cases of practical interest, the eavesdroppers may be passive and their instantaneous channels are not known at the transmitters. If the statistical distribution of the eavesdropper’s channel is known, then the transmit signals can be designed to optimize an ergodic secrecy metric. If nothing is known about the eavesdropper, measures can still be taken to improve secrecy, although in such cases the benefits of such measures are difficult to quantify. Going one step further, the CSI of the intended receiver itself may only be known partially due to estimation error or limited feedback, in which case robust or worst-case secrecy optimization methods must be developed.

6.3 MIMO Wiretap Channels

A MIMO wiretap channel consists of a transmitter (Alice), a legitimate receiver (Bob), and an eavesdropper (Eve) equipped with $N_T$, $N_R$, and $N_E$ antennas, respectively. A general representation for the signal received by the legitimate receiver is

$$y_b = H_b x_a + n_b,$$

while the received signal at the eavesdropper is

$$y_e = H_e x_a + n_e,$$

where $x_a \in \mathbb{C}^{N_T \times 1}$ is the transmitted signal with covariance $E\{x_a x_a^H\} = Q_x$, $H_b \in \mathbb{C}^{N_R \times N_T}$, $H_e \in \mathbb{C}^{N_E \times N_T}$ are the complex MIMO channel matrices associated with Bob and Eve, respectively, and $n_b, n_e$ represent additive noise at the two receivers. The above scenario with multiple antennas at all nodes is occasionally referred to as the MIMOME (multiple-input multiple-output multiple-eavesdropper) channel [7].

When the additive noise is Gaussian, a Gaussian input $x_a$ is the optimal choice for achieving the secrecy capacity under an average power constraint on the transmit covariance matrix [8]–[11]:

$$C_s = \max_{Q_x, \operatorname{Tr}(Q_x) \leq P} \left[ I(X_a; Y_b) - I(X_a; Y_e) \right]$$

where $I(\cdot; \cdot)$ denotes mutual information, and $X_a, Y_a, Y_e$ are the random variables whose realizations follow the system model in (6.1)–(6.2). For Gaussian input signaling, this is equivalent to

$$C_s = \max_{Q_x, \operatorname{Tr}(Q_x) \leq P} \log \det \left( I + H_b Q_x H_b^H \right) - \log \det \left( I + H_e Q_x H_e^H \right),$$

assuming for simplicity that the noise is spatially white and unit-variance at both receivers.

Secret-key agreement over wireless channels is another promising application of physical layer security since the noise, interference, and fading affecting wireless communications provide a convenient source of randomness. A secret-key rate is informally defined as the ratio between the number of key bits $k$ obtained at the end of a key-distillation strategy and the number of noisy channel uses $n$ required to obtain it. Assuming the eavesdropper and receiver observe independent signals and are under an average power constraint, the MIMO secret-key capacity is [12, 13]

$$C_k = \max_{Q_x, \operatorname{Tr}(Q_x) \leq P} I(X_a; Y_b | Y_e).$$

For Gaussian input signaling, $C_k$ has a form similar to (6.4) with an equivalent channel $\tilde{H}_b^H \tilde{H}_b = H_b^H H_b + H_e^H H_e$ introduced into the first log-determinant term on the RHS.
6.3.1 Complete CSI

For the case where the transmitter possesses instantaneous CSI for both the desired receiver and the eavesdropper, a precise characterization of the secrecy capacity and the corresponding transmit covariance \( Q_x \) for the MIMO wiretap channel under an average power constraint is unknown. Solutions can be found in special cases; for example, in the so-called MISOME case where \( N_R = 1, N_T, N_E > 1 \), the optimal solution is based on transmit beamforming: \( Q_x = P \psi_m \psi_m^H \), where \( \psi_m \) is the unit-norm generalized eigenvector corresponding to the largest generalized eigenvalue \( \lambda_m \) of

\[
(I + P h_b^H h_b) \psi_m = \lambda_m (I + P H_e^H H_e) \psi_m.
\]

(6.6)

Other special cases have been investigated, but the general solution remains an open problem.

An alternative power constraint was considered by Bustin et al. [14], who reexamined the MIMO wiretap channel by exploiting the derivative relationship between mutual information and mean-squared error to provide a closed-form expression for the capacity-achieving \( Q_x \) under a matrix power covariance \( Q_x \preceq S \). For this constraint, the MIMO secrecy capacity was shown to be given by

\[
C_{\text{sec}}(S) = \sum_{i=1}^{\lambda} \log \alpha_i
\]

(6.7)

where \( \alpha_i \) are the generalized eigenvalues of the pencil

\[
(S^{\frac{1}{2}} H_b^H H_b S^{\frac{1}{2}} + I, S^{\frac{1}{2}} H_e^H H_e S^{\frac{1}{2}} + I)
\]

(6.8)

that are greater than one. The matrix power constraint is a more narrow constraint that places considerable limits on the per-antenna power and transmit correlation structure [44]. The average power constraint is a much less restrictive constraint that provides considerable additional flexibility in increasing the secrecy rate of the MIMO wiretap channel. In principle, at least, the secrecy capacity of the MIMO wiretap channel under the average power constraint could be found via an exhaustive search over the set \( \{ S : S \succeq 0, \text{Tr}(S) \leq P \} \) [41, Lemma 1], [44]:

\[
C_{\text{sec}}(P_t) = \max_{S \succeq 0, \text{Tr}(S) \leq P_t} C_{\text{sec}}(S),
\]

(6.9)

where for any given semidefinite \( S \), \( C_{\text{sec}}(S) \) should be computed as in (6.7).

A closed-form solution is possible in certain special cases, for example when \( Q_x \) is known to be full rank [15, 16], or in the high-SNR regime [7]. In the latter case, it was shown that the asymptotically optimal solution for high SNR can be found by decomposing the system into parallel channels based upon the generalized singular value decomposition (GSVD) of the matrix pair \((H_b, H_e)\). The optimal power allocation for GSVD precoding was derived in [17], and is shown to empirically achieve the MIMO secrecy capacity in (6.4). The GSVD precoding approach is also applicable to MIMO secret-key establishment due to the close similarity between \( C_s \) and \( C_k \).

An example of the secrecy rate performance of various transmission strategies for the MIMO wiretap channel is shown in Figure 6.1. The GSVD scheme assumes instantaneous knowledge of the eavesdropper channel \( H_e \), the artificial noise scheme requires the statistics of \( H_e \), and the relatively poor performance of waterfilling on the main channel is also shown for the case where no information is available regarding \( H_e \). In this example, the power allocation given in [17] is observed to essentially achieve the secrecy capacity of the wiretap channel.
6.3.2 Partial CSI

When only CSI for the primary channel is available at the transmitter, an alternative scheme for the MIMO wiretap channel is to transmit an artificial or synthetic noise signal \( z' \) in conjunction with the information signal. The artificial noise signal is generally designed to be orthogonal to the intended receiver such that only the eavesdropper is jammed \([7–9]\), although in certain cases secrecy rates can be improved by allowing some noise leakage to the receiver \([18]\). An example of an artificial noise transmission strategy is

\[
x_a = Tz + T'z',
\]

(6.10)

where \( T, T' \) are the \( N_T \times d, N_T \times (N_T - d) \) precoding matrices for the \( d \times 1 \) information vector \( z \) and uncorrelated \( (N_T - d) \times 1 \) jamming signal \( z' \), respectively. These signals can be made orthogonal at the intended receiver by choosing \( T \) and \( T' \) as disjoint sets of the right singular vectors of \( H_b \) \([9, 22]\).

A frequent assumption in the literature is that only the statistical distribution of \( H_e \) is known to the transmitter, along with perfect knowledge of \( H_b \). In such scenarios, the artificial noise injection strategy as first suggested by Goel and Negi \([9]\) remains the best known secure transmission strategy, with approaches for optimizing the number of spatial dimensions and power allocated to the artificial noise ranging from an exhaustive search to optimizing an approximate expression for the ergodic secrecy rate. For the MISOME channel in this scenario, rank-1 beamforming without artificial noise has been shown to be the optimal strategy \([19]\). An alternative assumption regarding imperfect eavesdropper CSI is that the error in knowledge of \( H_e \) is norm-bounded \([20, 21]\). In \([20]\), the authors studied the optimal transmit strategy by exploiting the relationship between the secrecy MISO channel and the cognitive radio MISO channel. The authors in \([21]\) considered the MISO channel with and without an external helper, and obtained robust beamforming/jamming solutions via numerical methods.
The use of artificial noise can be problematic when the channel to the intended receiver is also not known perfectly, since the noise can leak into the desired receiver's signal. The imperfect CSI at the transmitter can be written as
\[ \hat{H}_b = H_b + \Delta H_b \]
where \( \Delta H_b \) is the unknown channel perturbation matrix. The two common approaches for modeling \( \Delta H_b \) are (1) to assume it follows a zero-mean complex Gaussian matrix distribution with a known covariance matrix \( C_\Delta \) [22], and (2) a deterministic model where the “size” of the perturbation lies within known bounds, e.g., \( \| \Delta H_b \|_F \leq \varepsilon \) [23]. In [22], the Gaussian perturbation model is considered. The authors propose a rank-1 beamforming strategy, compute the degradation in receiver SINR due to noise leakage based on SVD perturbation theory, and construct robust transmit/receive beamformers to recover the loss in SINR. In [23] on the other hand, the deterministic perturbation case is investigated, and the nonconvex secrecy rate maximization problem is numerically solved by applying a semidefinite relaxation based on a worst-case channel perturbation. The authors of [24] consider the case where \( \Delta H_b \) arises due to limited feedback from the receiver, and devise optimal power allocation and feedback rules to constrain the level of artificial noise leakage.

As an extreme case of partial CSI, consider the scenario where neither the realization nor the distribution of the eavesdropper channel is known to the legitimate parties. Information-theoretic solutions have been focused on the design of robust coding schemes that guarantee a minimum secrecy rate irrespective of the eavesdropper’s channel state. A far simpler method, albeit without such a guarantee, is to devote just enough resources to achieve a desired signal-to-interference-and-noise ratio (SINR) or rate to the intended receiver, and allocate any unused power/spatial resources to the generation of orthogonal artificial noise [22, 25]. Interestingly, the conventional waterfilling strategy is not necessarily the optimal approach for achieving a desired rate on the main channel, and can be outperformed by rank-minimization methods that yield greater unused spatial dimensions for artificial noise [25].

MIMO secret-key rates under assumptions of partial CSI are comparatively less well studied. In [26], the transmitter knows \( H_b \) but assumes \( H_e \) is drawn arbitrarily from a known finite set of possible matrices. This scenario naturally leads to a max–min approach to optimize the worst-case secret-key rate; it is shown that a saddlepoint exists and the optimal transmit covariance matrix is subsequently characterized.

It is important to note in closing that the vast majority of prior work on the MIMO wiretap channel assumes the use of Gaussian input signals for analytical simplicity. Moving to a model with inputs drawn from a finite alphabet immediately renders analyses more intractable due to the lack of simple closed-form expressions for mutual information. In most cases with discrete inputs, we must resort to numerical methods for MIMO transceiver optimization [28].

### 6.4 MIMO Wiretap Channel with an External Helper

It was shown in [29] that for a wiretap channel without feedback, a nonzero secrecy capacity can only be obtained if the eavesdropper’s channel is of lower quality than that of the intended recipient. If such a situation does not exist endogenously, one solution is to solicit the assistance of external nodes such as relays or helpers in facilitating the transmission of confidential messages from the source to the destination. While the helper could in principle assist with the transmission of the confidential messages themselves, the computational cost associated with this approach may be prohibitive and there are difficulties associated with
the coding and decoding schemes at both the helper and the intended receiver. Alternatively, the helper can simply transmit noise-like jamming signals independent of the source message, to confuse the eavesdropper and increase the range of channel conditions under which secure communications can take place [30,32,33]. This so-called cooperative jamming (CJ) or noise-forwarding approach is analogous to the artificial noise strategy described previously for the MIMOME channel.

Prior work on CJ assuming single-antenna nodes includes [30], which considers multiple single-antenna users communicating with a common receiver (i.e., the multiple access channel) in the presence of an eavesdropper, and the optimal transmit power allocation that achieves the maximum secrecy sum-rate is obtained. The work of [30] shows that any user prevented from transmitting based on the obtained power allocation can help increase the secrecy rate for other users by transmitting artificial noise to the eavesdropper via cooperative jamming. In [32], a MISO source–destination system in the presence of multiple helpers and multiple eavesdroppers is considered, where the helpers can transmit weighted jamming signals to degrade the eavesdropper’s ability to decode the source. While the objective is to select the weights so as to maximize the secrecy rate under a total power constraint, or to minimize the total power under a secrecy rate constraint, the results in [32] yield suboptimal weights for both single and multiple eavesdroppers, due to the assumption that the jamming signal must be nulled at the destination. The noise-forwarding scheme of [33] requires that the interferer’s codewords be decoded by the intended receiver. A generalization of [30,32] and [33] is proposed in [34], in which the helper’s codewords do not have to be decoded by the receiver. In [35], a CJ scenario is considered with an arbitrary number of antennas at the transmitters but with only single-antenna receivers, and it is shown that beamforming is the optimal strategy at both the main transmitter and the helper. A closed-from solution is obtained for the optimal channel input at the transmitter side based on the CJ signal chosen by the helper. Also, [35] analytically shows that sending CJ in the null space of $G_b$ is a near-optimal solution.

While all the previous work considers SISO or MISO scenarios, [36] and [37] propose solutions for the MIMO case. In [36], multiple cooperative jammers were studied, wherein the jammers aligned their interference to lie within a prespecified “jamming subspace” at the receiver, but the dimensions of the subspace and the power allocation were not optimized. In [37], necessary and sufficient conditions are obtained to have a jamming signal which does not reduce the mutual information between the source and the legitimate receiver. Thus the jamming signal only degrades the mutual information between the main transmitter and the eavesdropper, and as a result, the achievable secrecy rate improves.

Figure 6.2 shows the maximum achievable secrecy rate for the proposed algorithm in [37] versus the helper’s transmit power $P_h$. In this figure, it is assumed that the total average power $P_t + P_h = 110$, where $P_t$ is the power assigned to the source. While channels are assumed to be quasistatic flat Rayleigh fading and independent of each other, direct and cross channels have i.i.d. entries distributed as $CN(0, \sigma_d^2)$ and $CN(0, \sigma_c^2)$, respectively. The figure considers a situation in which $\sigma_c > \sigma_d$, or in other words where the channel between the transmitter and the intended receiver is weaker than the channel between the transmitter and the eavesdropper, and the channel between the helper and the intended receiver is weaker than the channel between the helper and the eavesdropper. The arrow in the figure shows the secrecy capacity without the helper ($P_h = 0$). The figure shows that a helper with just a single antenna can provide a dramatic improvement in secrecy rate with very little power allocated to the jamming signal; in fact, the optimal rate is obtained when $P_h$ is less than $2\%$ of the total available transmit power. If the number of antennas at the helper increases, a much higher secrecy rate can be obtained, but at the expense of allocating more power to the helper and less to the signal for the desired user.

While many cases assume the external helper knows the CSI of the eavesdropper, in some
scenarios perfect CSI may be difficult to obtain due to the nature of the eavesdropper, and thus robust beamforming/precoding strategies are needed to guarantee efficient cooperative jamming. The authors in [21] considered optimizing the worst-case secrecy performance for a MISO wiretap channel with a helper where the source and the helper only possess imperfect CSI for the eavesdropper and the channel error is norm-bounded by some known constraints. By converting the resulting nonconvex maximin problem into a quasiconvex problem, [21] derived optimal transmit covariance matrices for both the source and the helper under the zero-forcing constraint that the jamming signals are nulled at the legitimate receivers, and a Quality-of-Service constraint that a minimum receive SINR at the legitimate receiver is imposed.

6.5 MIMO Broadcast Channel

The original wiretap channel, as proposed by Wyner [5], is a form of broadcast channel (BC) where the source sends confidential messages to the destination while the messages should be kept as secret as possible from the other receiver(s)/eavesdropper(s). Csiszar and Körner extended this work to the case where the source sends common information to both the destination and the eavesdropper, and confidential messages are sent only to the destination [29]. The secrecy capacity region for the case of a BC with parallel independent subchannels is considered in [39] and the optimal source power allocation that achieves the boundary of the secrecy capacity region is derived. A special case of the MIMO Gaussian broadcast channel with common and confidential messages is considered in [40], where the common message is intended for both receivers but the confidential message is intended only
for receiver 1, and must be kept secret from receiver 2. A matrix characterization of the secrecy capacity region is established by first splitting receiver 1 into two virtual receivers and then enhancing only the virtual receiver that decodes the confidential message. It should be noted that the notion of an enhanced broadcast channel was first introduced in [41] to characterize the capacity region of the conventional Gaussian MIMO broadcast channel without secrecy constraints.

Prior work has considered the discrete memoryless broadcast channel with two confidential messages sent to two receivers, where each receiver acts as an eavesdropper for the other. This problem has been addressed in [42], where inner and outer bounds for the secrecy capacity region were established. Further work in [43] studied the MISO Gaussian case under the average power constraint, and [44] considered the general MIMO Gaussian case under the matrix power constraint.

For the two-user BC where each user is to receive own confidential message, it was shown in [44] that, under a matrix input power-covariance constraint, both confidential messages can be simultaneously communicated at their respective maximum secrecy rates as if over two separate MIMO Gaussian wiretap channels. In other words, under the matrix power constraint $S$, the secrecy capacity region $\{R_1, R_2\}$ is rectangular. This interesting result is obtained using secret dirty-paper coding (S-DPC), and the corner point rate $(R_1^*, R_2^*)$ of the secrecy capacity region under the matrix constraint $S$ can be calculated as [44, Theorem 3],

\[
\begin{align*}
R_1^* &= \log |A_1| \\
R_2^* &= -\log |A_2|
\end{align*}
\]

where the diagonal matrices $A_1$ and $A_2$ contain the generalized eigenvalues of

\[
\left( S^2 H_1^H H_2 S^2 + I, \quad S^2 H_1^H H_1 S^2 + I \right)
\]

that are respectively greater than or less than one.

The secrecy capacity region of the MIMO Gaussian broadcast channels with both confidential and common messages under the matrix power constraint is characterized in [45] and [46], where the transmitter has two independent confidential messages and a common message. The achievability is obtained using secret dirty-paper coding, while the converse is proved by using the notion of channel splitting [45]. Secure broadcasting with more than two receivers has been considered in [47–50] and references therein. The secrecy capacity region for the two-legitimate receiver case is characterized by Khandani et al. [48] using enhanced channels, and for an arbitrary number of legitimate receivers by Ekrem and Ulukus [49] who use relationships between the minimum mean square error and mutual information, and between the Fisher information and the differential entropy to provide the converse proof. Liu et al. [50] considered the secrecy capacity regions of the degraded vector Gaussian MIMO broadcast channel with layered confidential messages, and presented a vector generalization of Costa’s entropy power inequality to provide the converse proof. The role of artificial noise for jamming unintended receivers in multiuser downlink channels was investigated, for example, in [51, 52].

It should be noted that, under the average power constraint, there is not a computable secrecy capacity expression for the general MIMO broadcast channel case. However, optimal solutions based on linear precoding have been found. For example, in [53], a linear precoding scheme is proposed for a general MIMO BC under the matrix covariance constraint $S$. Conditions are derived under which the proposed linear precoding approach is optimal and achieves the same secrecy rate region as S-DPC. Then this result is used to derive a closed-form suboptimal algorithm based on linear precoding for an average power constraint. In [54], GSVD-based beamforming is used for the MIMO Gaussian BC to simultaneously diagonalize the channels. The GSVD creates a set of parallel independent
subchannels between the transmitter and the receivers, and it suffices for the transmitter to use independent Gaussian codebooks across these subchannels. In particular, the confidential message $W_1$ for receiver 1 is sent only over the subchannels for which the output at receiver 2 is a degraded version of the output at receiver 1. These subchannels correspond to the generalized singular values that are larger than one. On the other hand, the confidential message $W_2$ for receiver 2 is sent only over those subchannels for which the output at receiver 1 is a degraded version of the output at receiver 2. These subchannels correspond to the generalized singular values that are less than one. The optimal power allocation for these subchannels is derived in [54] to maximize the sum-secrecy rate for a given fraction $\alpha$ and $1 - \alpha$ of the total power allocated to $W_1$ and $W_2$, respectively. The Pareto boundary of the suboptimal secrecy rate region is then achieved by sweeping through all values of $\alpha \in \{0, 1\}$.

Figure 6.3 compares the average over 1,000 channel realizations of the sum-secrecy rate of the GSVD-based beamforming approach and the optimal S-DPC methods, when $N_T$ varies from two to six and for different numbers of antennas at the receivers. As the figure shows, the performance of the proposed GSVD-based beamforming approach is essentially identical to that of the optimal S-DPC, while requiring considerably less computation.

### 6.6 MIMO Interference Channel

The interference channel (IFC) refers to the case where multiple communication links are simultaneously active in the same time and frequency slot, and hence potentially interfere
with each other. A two-user IFC is depicted in Figure 6.4. A special application of the IFC with secrecy constraints is addressed in [55], where the message from only one of the transmitters is considered confidential. The more general case was studied in [42] where, in the absence of a common message, the authors imposed a perfect secrecy constraint and obtained inner and outer bounds for the perfect secrecy capacity region of a two-user discrete memoryless IFC.

For multiuser networks, a useful metric that captures the scaling behavior of the sum secrecy rate $R_\Sigma$ as the transmit SNR, $\rho$, goes to infinity is secret multiplexing gain or degrees of freedom (DoF), which can be defined as

$$\eta = \lim_{\rho \to \infty} \frac{R_\Sigma(\rho)}{\log(\rho)}. \quad (6.12)$$

Calculation of the number of secure DoF for the $K$-user Gaussian IFC ($K \geq 3$) has been addressed in [56] and [57], where it was shown that under very strong interference, positive secure DoFs are achievable for each user in the network. For the case of a $K$-user SISO Gaussian interference channel with confidential messages, where each node has one antenna and each transmitter needs to ensure the confidentiality of its message from all nonintended receivers, a secure DoF of

$$\eta = \frac{K - 2}{2K - 2} \quad (6.13)$$

is almost surely achievable for each user [56]. The achievability of this result is obtained by interference alignment and channel extension. Moreover, for the case of a $K$-user SISO Gaussian interference channel with an external eavesdropper, each user can achieve

$$\eta = \frac{K - 2}{2K}. \quad (6.14)$$

While the above references [55] through [57] assume single-antenna nodes, it should be noted that the secrecy capacity region of a two-user multiple antenna Gaussian interference channel, even for the MISO case, is still unknown. Indeed, from [42, Theorem 2], any rate pair

$$0 \leq R_1 \leq I(V_1; Y_1) - I(V_1; Y_2 | V_2)$$

$$0 \leq R_2 \leq I(V_2; Y_2) - I(V_2; Y_1 | V_1) \quad (6.15)$$
over all \( p(V_1, V_2, X_1, X_2, Y_1, Y_2) = p(V_1)p(V_2)p(X_1|V_1)p(X_2|V_2)p(Y_1, Y_2|X_1, X_2) \) is achievable, where the independent precoding auxiliary random variables \( V_1 \) and \( V_2 \) represent two independent stochastic encoders. To ensure information-theoretic secrecy, the bound for the achievable rate \( R_1 \) includes a penalty term \( I(V_1; Y_2|V_2) \), which is the conditional mutual information of receiver 2’s eavesdropper channel assuming that receiver 2 can first decode its own information. Thus, the achievable rates in (6.15) correspond to the worst-case scenario, i.e., where the intended messages are decoded treating the interference as noise, but the eavesdropped message is decoded without any interference (which is assumed to be subtracted before) [42, 58].

In Jorswieck et al. [58], studied the achievable secrecy rates of a two-user MISO interference channel, where each single-antenna receiver acts as an eavesdropper for the other link, and each transmitter only sends its information signal. In [60] and [61], a two-user MIMO Gaussian IFC is investigated where each node has arbitrary number of antennas:

\[
y_1 = H_1 x_1 + G_2 x_2 + n_1 \\
y_2 = H_2 x_2 + G_1 x_1 + n_2.
\] (6.16)

Based on different assumptions about the CSI available at the transmitter, several cooperative and noncooperative transmission schemes are described, and their achievable secrecy rate regions are derived.

In one noncooperative game, it is assumed that each transmitter \( i \) knows not only its own direct channel \( H_i \), but also the cross-channel \( G_i \) to the potential eavesdropper. When both \( H_i \) and \( G_i \) are available to transmitter \( i \), a reasonable precoding scheme is obtained by simply treating the IFC as two parallel wiretap channels and using the GSVD method to design the precoders for each transmitter. Thus, transmitter 1 constructs \( x_1 \) as

\[
x_1 = A_1 s_1, \quad s_1 \sim \mathcal{CN}(0, P_1)
\] (6.17)

where \( A_1 \) is obtained from the GSVD of the pair \((H_1, G_1)\), each nonzero element of the vector \( s_1 \) represents an independently encoded Gaussian codebook symbol that is beamformed with the corresponding column of the matrix \( A_1 \), and \( P_1 \) is a positive semidefinite diagonal matrix representing the power allocated to each data stream [61]. A similar description applies for transmitter 2.

In the cooperative solution, [61] assumes that each transmitter \( i \) knows not only its own channel \( H_i \) and the cross-channel \( G_i \), but also the subspaces \( \text{span}(G_jA_jP_j) \) and \( \text{span}(H_jA_jP_j) \), which represent the subspaces in which transmitter \( j \)’s information signal lies when it reaches receiver \( i \) and \( j \), respectively. It is assumed that the transmitters exchange information about these subspaces with each other. For the cooperative scheme, transmitter \( i \) devotes a fraction \( 1 - \alpha_i \) of its power \( (0 \leq \alpha_i \leq 1) \) to transmit artificial noise. Mathematically, the transmitted signal vector for user \( i \) is given by:

\[
x_i = A_is_i + T_iz_i \quad (i \neq j \quad i,j \in \{1,2\})
\] (6.18)

where \( s_i \sim \mathcal{CN}(0, P_i) \), \( z_i \sim \mathcal{CN}(0, Q_{zi}) \), and

\[
Q_{zi} = \frac{(1 - \alpha_i)p_i}{\text{Tr}(T_iT_i^H)}.
\] (6.19)

The elements of the vector \( z_i \) represent synthetic noise symbols broadcast by transmitter \( i \) along the column vectors of the beamforming matrix \( T_i \). Again, \( A_i \), the precoder for the information signal, is determined using the GSVD of the pair \((H_i, G_i)\) as in the noncooperative GSVD approach, with power loading matrix \( P_{zi} \), but with the updated power constraint \( \text{Tr}(A_iP_iA_i^H) \leq \alpha_i P_i \).
In [61], a closed-form solution is proposed to construct $T_1$, by considering the fact that there are three possible goals that, for example, transmitter 1 could consider when cooperatively designing $T_1$ to broadcast artificial noise:

1. Eliminate the impact of the artificial noise on its own information signal at Rx1: $\text{span}(H_1 A_1 P_1) \perp \text{span}(H_1 T_1)$,

2. Eliminate the impact of the artificial noise on the information signal from Tx2 at Rx2: $\text{span}(H_2 A_2 P_2) \perp \text{span}(G_1 T_1)$, and

3. Align the artificial noise with Tx2’s information signal at Rx1: $\text{span}(G_2 A_2 P_2) \cong \text{span}(H_1 T_1)$.

The last two goals are entirely altruistic, and aid Tx2 in improving its secrecy rate. A subspace fitting method that minimizes a weighted sum of the errors in achieving goals 1 through 3 is explained in [61].

Two-user IFC scenarios with confidential messages are also interesting to consider from game-theoretic perspective. In [62], a cognitive radio scenario is considered where only the message from the primary transmitter is considered confidential and must be kept secret at the cognitive receiver. While the primary transmitter and receiver employ a single-user wire-tap channel encoder and decoder, respectively, the strategy of the cognitive transmitter is power allocation on the nonsecure cognitive message and the noise signal. For this scenario, the Nash Equilibrium (NE) is established for the case that all nodes have a single antenna.

\footnote{Note that we do not include the goal of using the artificial noise to hide its own information signal at Rx2; this is because we are using GSVD precoding for this purpose, which is known to be more effective than artificial noise [7].}
In [63], a two-user one-sided interference channel with confidential messages is considered, in which one transmitter/receiver pair is interference-free. For this scenario, the NE for the binary deterministic channel is determined. In [58], an iterative algorithm is proposed to compute the NE point for the MISO Gaussian IFC, where each transmitter wishes to maximize its own utility function. The authors of [59] obtain a closed-form solution for the NE point where each multiantenna transmitter desires to maximize the difference between its secrecy rate and the secrecy rate of the other link. In [61], a game-theoretic formulation is adopted for an arbitrary two-user MIMO Gaussian interference channel, where the transmitters find an operating point that balances network performance and fairness using the so-called Kalai-Smorodinsky (K-S) bargaining solution [61]. Figure 6.5 shows the achievable secrecy rate regions of the proposed schemes in [61], along with the NE from the noncooperative GSVD approach, and the K-S rate point for the cooperative GSVD and artificial noise alignment method. In this figure, $n_i$ is the number of antennas at transmitter $i$ and $m_i$ is the number of antennas at receiver $i$. The benefit of transmitter cooperation in the IFC network is clearly evident from the secrecy point of view.

6.7 MIMO Relay Wiretap Networks

Physical layer security in relay networks can be considered as a natural extension to methods for secure transmission in MIMO networks. The scenarios considered in MIMO relay wiretap networks can be classified into two main categories: trusted and untrusted relay wiretap networks. The trusted relay network refers to a traditional scenario where the relays and destinations are all legitimate users. However, in an untrusted relay wiretap network, the relay itself is a potential eavesdropper, although it may still be able to offer assistance for cooperative transmission. For these models, the secrecy capacity and achievable secrecy rate bounds have been investigated for various types of relay-eavesdropper channels, and many cooperative strategies, based on those for conventional relay systems, have been proposed.

6.7.1 Relay-aided Cooperation

In trusted relay wiretap networks, the relays can play various roles with external eavesdroppers. They may act purely as traditional relays while utilizing help from other nodes to ensure security, they may also act as both relaying components as well as cooperative jamming partners to enhance the secure transmission, or they can assume the role of stand-alone helpers to facilitate jamming unintended receivers.

One-way Relays

A typical model of a one-way relay channel with an external eavesdropper is investigated in [33], where the four-terminal network is introduced and an outer bound on the optimal rate-equivocation region is derived. The authors also propose a noise-forwarding strategy where the full-duplex relay sends codewords independent of the secret message to confuse the eavesdropper. A more practical two-hop half-duplex relay wiretap channel is studied in [32], where several cooperative schemes are proposed for a two-hop multiple-relay network, and the corresponding relay weights are derived aiming to maximize the achievable secrecy rate, under the constraint that the link between the source and the relay is not protected from eavesdropping.

A more general case where cooperative jamming strategies guarantee secure communication in both hops without using external helpers is studied in [64], as illustrated in Figure 6.6. In the proposed cooperative jamming strategies, the source and destination nodes act as temporary helpers to transmit jamming signals during transmission phases in
which they are normally inactive. In general, the signals transmitted by Alice in the first phase may contain both information and jamming signals, and Bob may also transmit jamming signals at the same time. Thus the signals received by the relay and Eve in the first phase will be given by (the expressions for the second phase are similar in form)

\[ y_r = H_{ar}(T_a z_a + T'_a z'_a) + H_{br} T'_b z'_b + n_r \]  
\[ y_{e1} = H_{ae}(T_a z_a + T'_a z'_a) + H_{be} T'_b z'_b + n_{e1} \]

where \( z_a \) is the data signal vector, \( z'_a \) and \( z'_b \) are jamming signal vectors transmitted by Alice and Bob, respectively, and \( T'_a \) and \( T'_b \) are the corresponding transmit beamformers. The case where both \( z'_a \neq 0 \) and \( z'_b \neq 0 \) is defined as fully cooperative jamming (FCJ), while if either of them is zero, it is referred to as partially cooperative jamming (PCJ). One possible example of PCJ is for Alice to utilize the conventional GSVD transmit strategy, while Bob implements jamming in a reverse GSVD fashion, i.e., Bob in phase 1 considers Eve as the intended receiver of the jamming and wants to avoid leaking interference signals to the relay. The performance in terms of secrecy rate of this approach is depicted in Figure 6.7.

For the case where the relay acts as a helper, an interesting approach is to split the transmission time into two phases. In the first phase, the transmitter and the intended receiver both transmit independent artificial noise signals to the helper nodes. The helper nodes and the eavesdropper receive different weighted versions of these two signals. In the second stage, the helper nodes simply replay a weighted version of the received signal, using a publicly available sequence of weights. At the same time, the transmitter sends its secret message, while also canceling the artificial noise at the intended receiver [9].

**Two-way Relays**

In [30], a two-way wiretap channel is considered, in which both the source and the receiver transmit information over the channel to each other in the presence of a wiretapper. Achievable rates for the two-way Gaussian channel are derived. In addition, a cooperative jamming scheme that utilizes the potential jammers is shown to be able to further increase the secrecy sum rate. In [65], it is shown that using feedback for encoding is essential in Gaussian full-duplex two-way wiretap channels, while feedback can be ignored in the Gaussian half-duplex two-way relay channel with untrusted relays. More recently, secure transmission strategies
Figure 6.7: Secrecy rate vs. transmit SNR. Each node has four antennas. The distance between the source and destination is 800m with target rate $R_t = 2$bps/Hz.

have been studied for multiantenna two-way relay channels with network coding in the presence of eavesdroppers [66], [67]. By applying the analog network-coded relaying protocol, the end nodes exchange messages in two time slots. In this scenario, the eavesdropper has a significant advantage since it obtains two observations of the transmitted data compared to a single observation at each of the end nodes. As a countermeasure, in each of the two communication phases the transmitting nodes jam the eavesdropper, either by optimally using any available spatial degrees of freedom, or with the aid of external helpers.

6.7.2 Untrusted Relaying

For the untrusted relay case, the relay node acts both as an eavesdropper and an intermediate helper, i.e., the eavesdropper is colocated with the relay node. This type of relay may belong to a heterogeneous network without the same security clearance as the source and destination nodes. The source desires to use the relay to communicate with the destination, but at the same time intends to shield the message from the relay. This type of model was first studied in [68] for the general relay channel. Coding problems of the relay-wiretap channel are studied under the assumption that some transmitted messages are confidential to the relay, and deterministic and stochastic rate regions are explicitly derived in [69–71], which show that cooperation from the untrusted relay is still essential for achieving a nonzero secrecy rate. A more symmetric case is discussed in [72], where both the source and the relay send their own private messages while keeping them secret from the destination. Assuming a half-duplex amplify-and-forward (AF) protocol, another effective countermeasure in this case is to have the destination jam the relay while it is receiving data from the source. This intentional interference can then be subtracted out by the destination from the signal it receives via the relay.
In [73], the authors consider the joint source/relay beamforming design problem for secrecy rate maximization, through a one-way untrusted MIMO relay. For the two-way untrusted relay case, [74] proposes an iterative algorithm to solve for the joint beamformer optimization problem. In realistic fading channels, the secrecy outage probability (SOP) is more meaningful compared with the ergodic secrecy rate, which is ill-defined under finite delay constraints. Thus [75] focuses on the SOP of the AF relaying protocol, which is chosen due to its increased security vis-à-vis decode-and-forward relaying and has lower complexity compared to compress-and-forward approaches. The SOP is a criterion that indicates the fraction of fading realizations where a secrecy rate $R$ can be supported, and also provides a security metric when the source and destination have no CSI for the eavesdropper [76].

In general for untrusted AF relaying, when the number of antennas at the source and the destination is fixed, more antennas at the unauthenticated relay will facilitate a more powerful wiretapping ability and thus the secrecy performance will be degraded. Therefore, an alternative scenario is to consider implementing antenna selection at the relay (e.g., when the relay has only one RF chain) combined with cooperative jamming, in order to suppress the relay’s wiretapping ability while still providing diversity gain for the legitimate destination. One example is the case where the relay has no knowledge of the channel to Bob, which applies to the case where Bob transmits no training data to the relay, and jams only when Alice is transmitting so the relay cannot collect interference information [75]. In such cases, the relay selects the receive antenna with the largest channel gain during the first hop, and then uses either the same or some random antenna for transmission during the second hop. Note that the first hop antenna selection uses the same scheme as in traditional AF relaying where the best antenna pair is chosen for the first hop. With this scheme, the SOP is shown to be a nonincreasing function of the number of antennas at the relay, which indicates a possible solution for using multiple antennas at an untrusted relay.

6.8 Conclusions

We have surveyed a number of different methods that have been used to exploit the availability of multiple antennas in enhancing the security of wireless networks at the physical layer. Several different applications were considered, including MIMO wiretap, broadcast, and interference networks, as well as the use of external helpers for cooperative jamming. We have seen that multiple antennas provide considerable flexibility in the form of spatial degrees of freedom that can be exploited for steering signals of interest away from eavesdroppers and toward desired users, and doing the opposite for jamming signals. While performance limits (e.g., secrecy capacity regions, optimal solutions, etc.) have been derived for certain special cases, we have highlighted a number of open problems that require additional attention by researchers in the field. We hope that this chapter can serve as a helpful “jumping-off” point for those interested in investigating some of these problems.

References

MIMO Signal Processing Algorithms for Enhanced Physical Layer Security


Physical Layer Security in Wireless Communications


Physical Layer Security in Wireless Communications

Antennas (WSA), 2009.


