Chapter 6

Physical Layer Security for Multiuser MIMO Communications

Giovanni Geraci and Jinhong Yuan

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/57130

1. Introduction

Wireless multi-user MIMO communications are used more and more often to exchange sensitive data. Because of the broadcast nature of the physical medium, unauthorized receivers located within the transmission range can observe the signals sent by the transmitter to a legitimate receiver and eavesdrop them. Therefore, security has become an extremely important issue to deal with. Multiuser MIMO communications are particularly sensitive to the problem of security, because each confidential message must be kept secret not only from external nodes, but also from all the users other than the intended one.

Traditionally, wireless security is ensured by network-layer cryptography techniques. However, these techniques may not be suitable in the case of large dynamic wireless networks, since they raise issues like key distribution and management (for symmetric cryptosystems), and high computational complexity (for asymmetric cryptosystems). Moreover, these schemes are potentially vulnerable, since they rely on the limited resources of the eavesdropper and on the unproven assumption that certain encryption algorithms are hard to invert. Methods exploiting the randomness inherent in noisy channels, known as physical layer security, have been proposed to enhance the protection of transmitted data and achieve perfect secrecy [1, 2]. Physical-layer security allows secret communications over a wireless channel without requiring an encryption key, and it works by limiting the amount of information that can be extracted at the physical level by an unintended receiver. This is performed by designing appropriate coding and precoding schemes, and by exploiting the channel state information available at the network nodes [3].

Physical layer security for communications was proposed in the 1970's by Wyner [4], who studied a three-terminal network consisting of a transmitter, an intended user and an eavesdropper, known as the wiretap channel. For this network, the secrecy capacity was defined as the maximum rate at which a message can be transmitted reliably to the intended

user while the rate of information leakage to the eavesdropper vanishes asymptotically with the code length. For the case when the eavesdropper's channel is a degraded version of the intended user's channel, Wyner showed that it is possible to have secret communication without using an encryption key. This can be achieved by a randomized coding scheme where the information is hidden in the additional noise seen by the eavesdropper. Each message is mapped to many codewords, thus inducing maximal equivocation at the eavesdropper. Csizar and Korner generalized Wyner's work by considering a nondegraded version of the wiretap channel [5].

Physical layer security was then applied to Gaussian channels [6], and it was observed that a secret transmission can be achieved only if the channel at the eavesdropper is noisier than the channel at the intended user. The presence of slow fading was shown to significantly change the situation, since it allows the transmitter to employ a variable-rate transmission, thus achieving secrecy even when the eavesdropper's channel is better than the intended receiver's channel on average [7]. Also the use of multiple antennas can enhance the secrecy capability, because it enables the transmitter to beamform in a direction as orthogonal to the eavesdropper and as close to the intended user as possible [8–10]. Even when the channel at the eavesdropper is unknown by the transmitter, artificial noise can be transmitted to degrade the eavesdropper's channel and thus reduce its signal-to-noise ratio, while being harmless to the intended receiver [11–13].

More recently, physical layer security has also been extended to multiuser MIMO channels. In this chapter, we will survey the research in the field of physical layer security for multiuser MIMO communications, especially focusing on the case when multiple malicious users are present in the network, and they can eavesdrop on each other. For these complex scenarios, we will present some suboptimal low-complexity transmission schemes, discuss their performance and quantify the sum-rate penalties imposed by the secrecy requirements and by the presence of multiple users. We will discuss the challenges that arise in networks with a large number of malicious receivers, we will identify potential ways to deal with these challenges, and present an outlook on future directions for research.

2. Physical layer security in multiuser MIMO systems

One way to extend the concept of physical layer security to multiuser systems is by considering the multiuser wiretap channel, where a transmitter wants to have confidential communication with an arbitrary number of trusted users in the presence of an external eavesdropper. For this system set-up, the secrecy capacity region in the presence of an arbitrary number of legitimate receivers was characterized in [14], by using the relationship between the minimum-mean-square-error and the mutual information. The capacity achieving coding scheme was shown to be a variant of dirty-paper coding with Gaussian signals.

Since the transmitter cannot always predict the behavior of the users, the multiuser MIMO channel with malicious users is now regarded with large interest. This is also denoted as the broadcast channel with confidential messages (BCC). Consider a broadcast channel with two independent confidential messages sent to two receivers, where each receiver acts as an eavesdropper for the other one. In other words, the first message is intended for

the first receiver but needs to be kept secret from the second receiver, and viceversa. This scenario was studied in [15] for the multiple-input single-output (MISO) Gaussian case and in [16] for general MIMO Gaussian case. In this case it was shown that both confidential messages can be simultaneously transmitted at their respective maximum secrecy rates, and the achievability was obtained using the dirty-paper coding.

Let us cosider now a larger multiuser network with more than two malicious users. For this network, it is required that the base station (BS) securely transmits each confidential message, ensuring that none of the other unintended users receive any information. Since in general the behavior of the users cannot be determined by the transmitter, a conservative worst-case scenario can be assumed for each user, where all the remaining users can cooperate to jointly eavesdrop. In this case, for each user, the alliance of the cooperating eavesdropper is equivalent to a single multi-antenna eavesdropper.

The MISO BCC with a generic number of malicious receivers was studied in [17, 18], and it consists of a BS with M antennas that simultaneously transmit independent confidential messages to K spatially dispersed single-antenna users, which can cooperate and eavesdrop on each other. Although determining the secrecy capacity region for the generic MISO BCC is still an open problem, suboptimal transmission schemes have been proposed to achieve high secrecy sum-rates by controlling the amount of crosstalk between the users [19]. These schemes are based on linear precoding, and unlike dirty-paper coding, their low complexity makes them suitable for practical implementation. In the following sections, we present some new results on the secrecy sum-rates achieved by multiuser MIMO linear precoding.

3. Physical layer security with multi-user MIMO linear precoding

Although suboptimal, linear precoding schemes are of particular interest because of their low-complexity implementations and because they can control the amount of crosstalk between the users to maintain a high sum-rate in the broadcast channel [20–27]. In the MISO BCC, linear precoding can be employed to control the amount of interference and information leakage to the unintended receivers introduced by the transmission of each confidential message [17–19].

Let the transmitted signal be denoted by $\mathbf{x}$, then the received signal is given by

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n} \tag{1}$$

where $\mathbf{H} = [\mathbf{h}_1, \ldots, \mathbf{h}_K]$ is the $K \times M$ channel matrix, $\mathbf{h}_k$ is the k-th column of $\mathbf{H}$ and it represents the channel between the BS and the k-th user, and $\mathbf{n}$ is complex Gaussian noise. In linear precoding, the transmitted vector $\mathbf{x}$ is derived from the vector containing the confidential messages $\mathbf{u} = [u_1, \ldots, u_K]^T$ through a deterministic linear transformation (precoding) [22–25]. Let $\mathbf{W} = [\mathbf{w}_1, \ldots, \mathbf{w}_K]$ be the $M \times K$ precoding matrix, where $\mathbf{w}_k$ is the k-th column of $\mathbf{W}$. Then the transmitted signal is

$$\mathbf{x} = \mathbf{W}\mathbf{u} = \sum_{k=1}^{K} \mathbf{w}_k u_k. \tag{2}$$

3.1. Achievable secrecy sum-rates with linear precoding

The secrecy sum-rates achievable by linear precoding were obtained in [18] by considering the worst-case scenario, where for each intended receiver k the remaining $K-1$ users can form an alliance $\tilde{k}$, and cooperate to jointly eavesdrop on the message u_k. By noting that each user k, along with its own eavesdropper $\tilde{k}$ and the transmitter, forms an equivalent multi-input, single-output, multi-eavesdropper (MISOME) wiretap channel [10], an achievable secrecy sum-rate R_s is given by

$$R_s = \sum_{k=1}^{K} \max\left\{\log_2\left(1+\mathrm{SINR}_k\right) - \log_2\left(1+\mathrm{SINR}_{\tilde{k}}\right), 0\right\}, \tag{3}$$

where SINR_k and $\mathrm{SINR}_{\tilde{k}}$ are the signal-to-interference-plus-noise ratios for the message u_k at the intended receiver k and the eavesdropper $\widetilde{k}$, respectively, given by

$$\mathrm{SINR}_k = \frac{\rho\left|\mathbf{h}_k^H \mathbf{w}_k\right|^2}{1+\rho\sum_{j\neq k}\left|\mathbf{h}_k^H \mathbf{w}_j\right|^2} \tag{4}$$

and

$$\mathrm{SINR}_{\tilde{k}} = \rho\left\|\mathbf{H}_k \mathbf{w}_k\right\|^2, \tag{5}$$

and where ρ is the transmit SNR, and $\mathbf{H}_k$ is the matrix obtained from $\mathbf{H}$ by removing the k-th row.

Particular attention was given to the Regularized Channel Inversion (RCI) precoder, because it achieves better performance than the plain Channel Inversion precoder, especially at low SNR [24, 25]. A linear precoder based on RCI was proposed for the MISO BCC in [19]. The RCI precoding matrix is given by

$$\mathbf{W} = \frac{1}{\sqrt{\gamma}}\mathbf{H}^H\left(\mathbf{H}\mathbf{H}^H + M\xi\mathbf{I}_K\right)^{-1}, \tag{6}$$

where γ is a long-term power normalization constant, given by

$$\gamma = \mathrm{tr}\left\{\mathbf{H}^H\mathbf{H}(\mathbf{H}^H\mathbf{H} + M\xi\mathbf{I}_M)^{-2}\right\}. \tag{7}$$

For each message, the function of the regularization parameter ξ is to achieve a tradeoff between maximizing the signal power at the intended user and minimizing the interference and information leakage at the other unintended users. In [19], the regularization parameter is optimized to maximize the secrecy sum-rate.

3.2. Large-system results

The secrecy sum-rate achievable by the RCI precoder in the MISO BCC was obtained in [19] by large-system analysis, where both the number of receivers K and the number of transmit antennas M approach infinity, with their ratio $\beta = K/M$ being held constant. Unless otherwise stated, the results presented in the following refer to the large-system regime. We note that these results are accurate even when applied to small systems with a finite number of users.

An expression for the secrecy sum-rate R_s° in the large-system regime is given by [19]

$$R_s^{\circ} = \max \left\{ K \log_2 \frac{1 + g(\beta,\xi) \frac{\rho + \frac{\rho\xi}{\beta}[1+g(\beta,\xi)]^2}{\rho + [1+g(\beta,\xi)]^2}}{1 + \frac{\rho}{(1+g(\beta,\xi))^2}}, 0 \right\} \tag{8}$$

with

$$g(\beta,\xi) = \frac{1}{2}\left[\mathrm{sgn}(\xi) \cdot \sqrt{\frac{(1-\beta)^2}{\xi^2} + \frac{2(1+\beta)}{\xi} + 1} + \frac{1-\beta}{\xi} - 1 \right]. \tag{9}$$

In [19], a closed form expression was also derived for the optimal regularization parameter $\xi^{\star\circ}$, given by

$$\xi^{\star\circ} = \frac{-2\rho^2(1-\beta)^2 + 6\rho\beta + 2\beta^2 - 2[\beta(\rho+1) - \rho] \cdot \sqrt{\beta^2[\rho^2+\rho+1] - \beta[2\rho(\rho-1)] + \rho^2}}{6\rho^2(\beta+2) + 6\rho\beta}. \tag{10}$$

For the specific case $\beta = 1$, i.e. $M = K$, the value of $\xi^{\star\circ}$ reduces to [18]

$$\xi^{\star\circ} = \frac{1}{3\rho + 1 + \sqrt{3\rho+1}}, \quad \text{for } \beta = 1. \tag{11}$$

We note that the value of the regularization parameter $\xi^{\star\circ}$ that maximizes the secrecy sum-rate differs from the value $\xi_{\mathrm{ns}}^{\star\circ} = \beta/\rho$ that maximizes the sum-rate without secrecy requirements [28].

By substituting the optimal value of the regularization parameter (10) in (8), it is possible to obtain the optimal secrecy sum-rate $R_s^{\star\circ}$ achievable by RCI precoding in the large-system regime. The secrecy sum-rate $R_s^{\star\circ}$ is a function of K, β and ρ. When $\beta = 1$, the optimal secrecy sum-rate $R_s^{\star\circ}$ has a simple expression, given by

$$R_s^{\star\circ} = K \log_2 \frac{9\rho + 2 + (6\rho + 2)\sqrt{3\rho + 1}}{4\,(4\rho + 1)}, \quad \text{for } \beta = 1. \tag{12}$$

Although the optimal value of the regularization parameter $\xi^{\star\circ}$ in (10) was derived in [19] in the large-system regime, using $\xi^{\star\circ}$ in a finite-size system does not cause a significant loss in the secrecy sum-rate compared to using a regularization parameter $\xi_{\text{fs}}(\mathbf{H})$ optimized for every channel realization.

Fig. 1 shows the complementary cumulative distribution function (CCDF) of the normalized secrecy sum-rate difference between using $\xi^{\star\circ}$ and $\xi_{\text{fs}}(\mathbf{H})$ as the regularization parameter of the RCI precoder for $K = 4, 8, 16, 32$ users, for $\beta = 1$ and at an SNR of 10dB. The difference is normalized by dividing by the secrecy sum-rate of the precoder that uses $\xi_{\text{fs}}(\mathbf{H})$. We observe that the average normalized secrecy sum-rate difference is less than 2.4 percent for all values of K. As a result, the large-system regularization parameter $\xi^{\star\circ}$ may be used instead of the finite-system regularization parameter with only a small loss of performance. Moreover, the value of $\xi^{\star\circ}$ does not need to be calculated for each channel realization.

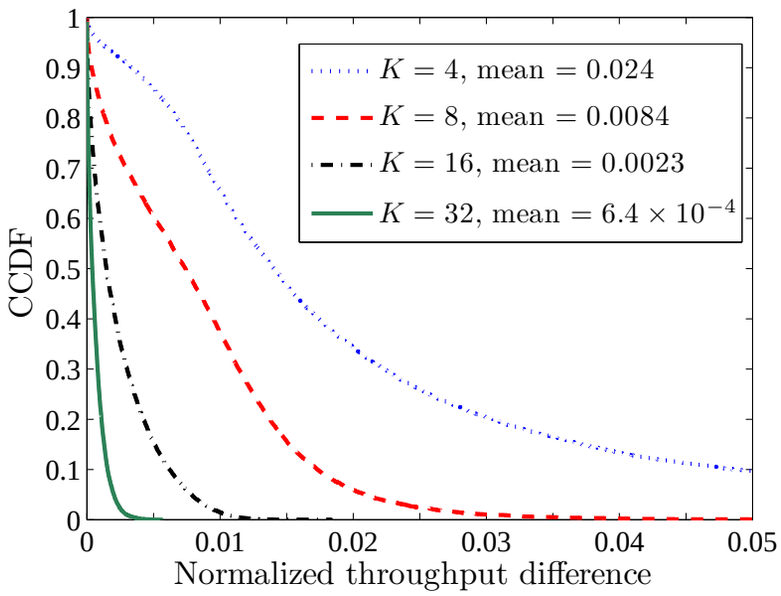

Figure 1. Complementary cumulative distribution function (CCDF) of the normalized secrecy sum-rate difference between using $\xi_{\text{fs}}(\mathbf{H})$ and $\xi^{\star\circ}$, with $\beta = 1$ and $\rho = 10$dB.

Fig. 2 compares the secrecy sum-rate $R_s^{\star\circ}$ of the RCI precoder from the large-system analysis to the simulated ergodic secrecy sum-rate R_s with a finite number of users, for different values of β. We observe that as M increases, the simulated rates approach the curves from large-system analysis. For $\beta \leq 1$, $R_s^{\star\circ}$ is always positive and monotonically increasing with the SNR ρ. However when $\beta > 1$, the secrecy sum-rate does not monotonically increase with ρ. There is an optimal value of the SNR beyond which the achievable secrecy sum-rate $R_s^{\star\circ}$ starts decreasing, until it becomes zero for large SNR. When $\beta \geq 2$ no positive secrecy sum-rate is achievable at all [19].

http://dx.doi.org/10.5772/57130

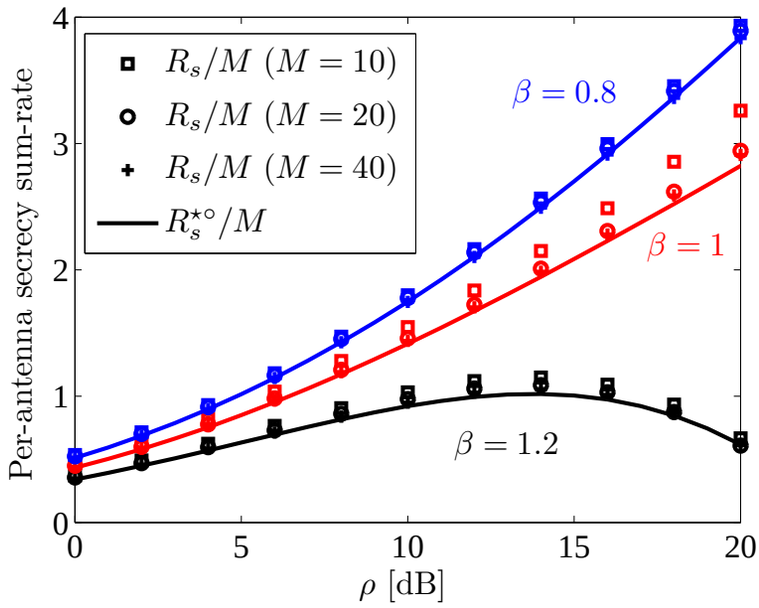

Figure 2. Comparison between the secrecy sum-rate with RCI precoding in the large-system regime (8) and the simulated ergodic secrecy sum-rate for finite M. Three sets of curves are shown, each one corresponds to a different value of β.

The expression of the secrecy sum-rate $R_s^{\star\circ}$ becomes simpler in the limit of large SNR. In fact, it can be approximated by

$$R_s^{\star\circ} \approx \begin{cases} K \log_2 \frac{1-\beta}{\beta} + K \log_2 \rho & \text{for } \beta < 1 \\ \frac{K}{2} \log_2 \frac{27}{64} + \frac{K}{2} \log_2 \rho & \text{for } \beta = 1 \\ \max\left\{ 3K \log_2 \frac{\beta}{\beta-1} - K \log_2 \rho, 0 \right\} & \text{for } \beta > 1 \end{cases}, \quad \text{as } \rho \to \infty. \tag{13}$$

We note from (13) that for high SNR, the behavior of the secrecy sum-rate significanly depends on the ratio β between the number of users K and the number of transmit antennas M. When $K < M$, the secrecy sum-rate scales linearly with the factor K. If $K = M$, the scaling factor reduces to $K/2$. When the number of users K exceeds the number of antennas M, then the secrecy sum-rate decreases with the SNR ρ, and there is a value of ρ beyond which the achievable secrecy sum-rate becomes zero.

3.3. Effect of the network load

Fig. 3 depicts the asymptotic secrecy sum-rate per transmit antenna as a function of β, for several values of the SNR. We denote by β_{opt} the value of the ratio β that maximizes the secrecy sum-rate per transmit antenna $R_s^{\star\circ}/M$. It is possible to see from Fig. 3 that β_{opt} is an increasing function of the SNR. The value of β_{opt} falls between 0 and 1, and it tends to 1 in the limit of large SNR.

We denote by $\beta_{\max}$ the maximum value of β allowed for non-zero secrecy sum-rates. The value of $\beta_{\max}$ represents the maximum number of users per transmit antenna that can be

served with non-zero secrecy sum-rate. Fig. 3 shows that $\beta_{\max}$ is a decreasing function of the SNR. The value of $\beta_{\max}$ can be found by solving the following cubic equation [19]

$$(\rho+1)\,\beta_{\max}^3-(3\rho+2)\,\beta_{\max}^2+3\rho\beta_{\max}-\rho=0. \tag{14}$$

The value of $\beta_{\max}$ falls between 1 and 2. This means that if $K \geq 2M$, i.e. if $\beta \geq 2$, then the secrecy sum-rate is zero for all SNRs. In the limit of large SNR, equation (14) reduces to

$$(\beta_{\max}-1)^3=0, \tag{15}$$

yielding to $\beta_{\max}=1$. These results can be explained as follows. In the worst-case scenario, the alliance of cooperating eavesdroppers can cancel the interference, and its received SINR is the ratio between the signal leakage and the thermal noise. In the limit of large SNR, the thermal noise vanishes, and the only means for the transmitter to limit the eavesdropper's SINR is by reducing the signal leakage to zero by inverting the channel matrix. This can only be accomplished when the number of transmit antennas is larger than or equal to the number of users, hence only if $\beta \leq 1$. When $\beta > 1$ this is not possible, and no positive secrecy sum-rate can be achieved. When $\beta \geq 2$, the eavesdroppers are able to drive the secrecy sum-rate to zero irrespective of ρ. This is consistent with the results presented in [10] for a single-user system.

4. The cost of physical layer security in multi-user MIMO

Guaranteeing secrecy and serving multiple (and potentially malicious) users at the same time both come at a cost in terms of the per-user transmission rate. In this section, we discuss the cost of achieving physical layer security in multiuser MIMO communications.

4.1. Secrecy loss

The cost due to the secrecy requirements, which we denote by *secrecy loss*, can be obtained by comparing the secrecy sum-rate $R_s^{\star\circ}$ achieved by the RCI precoder to the sum-rate $R^{\star\circ}$ achieved by an optimized RCI precoder without secrecy requirements. The gap between $R_s^{\star\circ}$ and $R^{\star\circ}$ represents how much guaranteeing secrecy costs in terms of the achievable sum-rate.

The optimal sum-rate $R^{\star\circ}$ without secrecy requirements is obtained by using the precoder in (6), and it is given by [29]

$$R^{\star\circ}=K\log_2\left[1+g\left(\beta,\xi_{\mathrm{ns}}^{\star\circ}\right)\right], \tag{16}$$

http://dx.doi.org/10.5772/57130

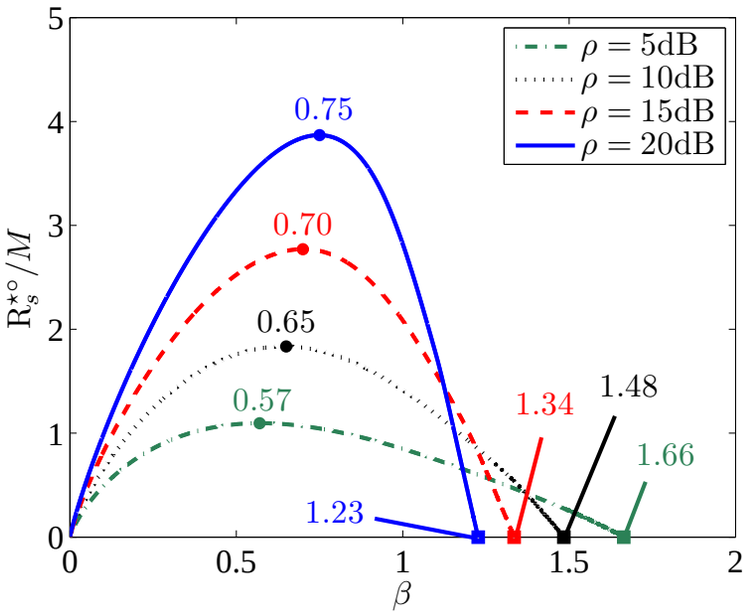

Figure 3. Asymptotic secrecy sum-rate per transmit antenna with RCI as a function of β. Circles denote β_{opt}, squares denote $\beta_{\max}$.

with $\xi_{\text{ns}}^{\star\circ} = \beta/\rho$. It is easy to show that $R^{\star\circ} \geq 0$ for all values of β and ρ, with equality only for $\rho = 0$, and that $R^{\star\circ}$ tends to zero as $\beta \to \infty$. Hence, there is no limit to the number of users per transmit antenna β that the system can accommodate with a non-zero sum-rate. However if we impose the secrecy requirements, the secrecy sum-rate $R_s^{\star\circ}$ is zero for $\beta \geq \beta_{\max}$, with $\beta_{\max}$ given by (14). Therefore, introducing the secrecy requirements will limit to $\beta_{\max}$ the number of users per transmit antenna that can be served with a non-zero sum-rate.

We now compare the secrecy sum-rate $R_s^{\star\circ}$ to the sum-rate $R^{\star\circ}$ in the limit of large SNR. Again by using the regularization parameter $\xi_{\text{ns}}^{\star\circ} = \beta/\rho$ we obtain the following large-SNR approximation for the secrecy sum-rate without secrecy requirements [19]

$$R^{\star\circ} \approx \begin{cases} K \log_2 \frac{1-\beta}{\beta} + K \log_2 \rho & \text{for } \beta < 1 \\ \frac{K}{2} \log_2 \rho & \text{for } \beta = 1 \\ K \log_2 \frac{\beta}{\beta - 1} & \text{for } \beta > 1 \end{cases}, \quad \text{as } \rho \to \infty. \tag{17}$$

By comparing (17) to (13), we can draw the following conclusions regarding the large-SNR regime. If the number of transmit antennas M is larger than the number of users K, then $\beta < 1$, $R_s^{\star\circ} = R^{\star\circ}$, and the secrecy requirements do not decrease the sum-rate of the network. Therefore, by using $\xi^{\star\circ}$ from (10) one can achieve secrecy while maintaining the same sum-rate, i.e. there is no secrecy loss. If $M = K$, then $\beta = 1$, the secrecy requirements only reduce the sum-rate by a constant value, and the scaling factor $K/2$ remains unchanged. Alternatively, one can achieve secrecy while maintaining the same sum-rate, by increasing the transmitted power by a factor $64/27 \approx 3.75$dB. If $M < K$, i.e. $\beta > 1$, then the secrecy

requirements result in a value of $R_s^{\star\circ}$ that decreases with the SNR, as opposed to a constant sum-rate $R^{\star\circ}$ without secrecy. Therefore if the SNR is too large, then the secrecy sum-rate becomes zero.

4.2. Multiuser Loss

The cost due the interference caused by the presence of multiple users in the system, which we denote by *multiuser loss*, is given by the gap between the per-user secrecy rate $R_s^{\star\circ}/K$ and the secrecy capacity $C_{s,\mathrm{SU}}$ of the single-user MISOME wiretap channel, where one user is served at a time and the remaining users can eavesdrop.

The value of $C_{s,\mathrm{SU}}$ was obtained in [10], and for large SNR it can be approximated by

$$C_{s,\mathrm{SU}} \approx \begin{cases} \log_2 \rho & \text{for } \beta < 1 \\ \frac{1}{2}\log_2 \rho & \text{for } \beta = 1 \\ \max\left\{\log_2 \frac{1}{(\beta-1)}, 0\right\} & \text{for } \beta > 1 \end{cases}, \quad \text{as } \rho \to \infty. \tag{18}$$

We compare $R_s^{\star\circ}/K$ to $C_{s,\mathrm{SU}}$ in the large-SNR regime. We note that in $C_{s,\mathrm{SU}}$ from [10] a single-user system is considered. Therefore, only one message is transmitted to one legitimate user, and the user does not experience any interference. By comparing (18) to $R_s^{\star\circ}/K$, we can conclude that for $\beta \leq 1$, the RCI precoder achieves a per-user secrecy rate which has the same linear scaling factor as the secrecy capacity of a single-user system with no interference. When $1 < \beta < 2$, the presence of interference results in a value of $R_s^{\star\circ}$ that decreases with the SNR, as opposed to a constant value for $C_{s,\mathrm{SU}}$. When $\beta \geq 2$, the secrecy rate is zero irrespective of the presence of interference.

4.3. Power allocation

In some cases, the rate loss generated by the secrecy requirements and by the interference due to the presence of multiple users can be compensated by a power allocation scheme. In [18], an iterative power allocation algorithm was proposed to obtain the maximum secrecy sum-rate for a fixed regularization parameter ξ. The algorithm was also extended to maximize the secrecy sum-rate by jointly optimizing the regularization parameter ξ and the power allocation vector. However, in many cases there is a negligible performance difference between the joint and the separate optimization. As a result, a low-complexity, near-optimal RCI precoder may be implemented by using $\xi^{\star\circ}$ from (10) and optimizing the power vector separately [18].

The RCI precoder with optimal power allocation (RCI-PA) outperforms the RCI precoder with equal power (RCI-EP), and the gain does not vanish at high SNR. The RCI-PA precoder thus reduces the rate loss due to secrecy requirements and interference, and in some cases it achieves a per-user rate which is as high as the rate achieved by the optimal RCI-EP precoder without secrecy requirements, and as high as the secrecy capacity of a single-user system [18].

4.4. Numerical results

Fig. 4 compares the simulated ergodic sum-rates R_s and R of the RCI precoder with and without secrecy requirements, respectively. These were obtained by using the regularization parameters $\xi^{\star\circ}$ and $\xi_{\text{ns}}^{\star\circ}$, respectively. For $\beta < 1$, the difference between R and R_s becomes negligible at large SNR, and secrecy can be achieved without additional costs. For $\beta = 1$, the two curves tend to have same slope at large SNR, but there is a residual gap between them. Therefore, secrecy can be achieved at a lower sum-rate. We note that in order to achieve secrecy without decreasing the sum-rate, the required additional power is less than 4dB at all SNRs. For $\beta > 1$, the sum-rate tends to saturate for large SNR, whereas the secrecy sum-rate starts decreasing. If the SNR is too large, then the secrecy requirements force the sum-rate to zero.

Fig. 4 also shows the simulated secrecy capacity $C_{s,\text{SU}}$ of the MISOME wiretap channel. For $\beta \leq 1$, the RCI precoder achieves a per-user secrecy rate which has the same linear scaling factor as $C_{s,\text{SU}}$. When $1 < \beta < 2$, $C_{s,\text{SU}}$ saturates at high SNR, while the secrecy sum-rate decreases. All these numerical results confirm the ones obtained from the large-system analysis.

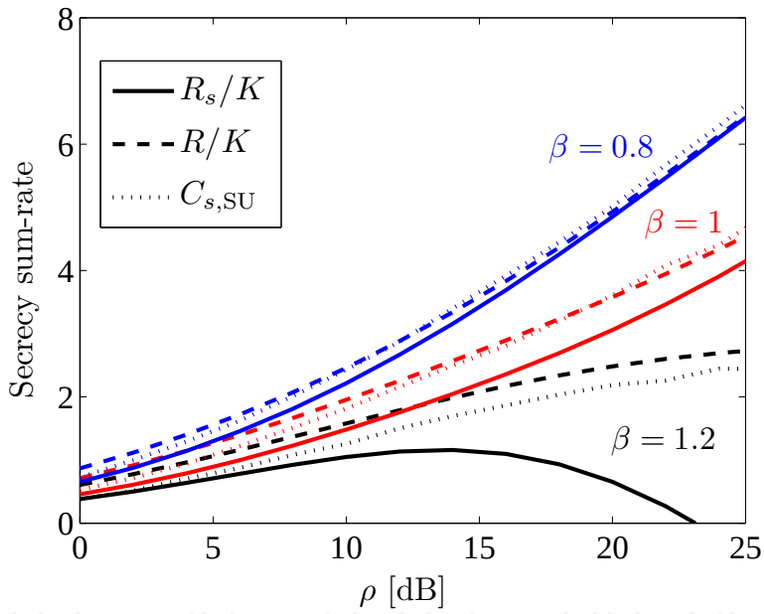

Figure 4. Comparison between the simulated ergodic per-user secrecy rate with RCI (solid) and the two upper bounds: (i) per-user rate without secrecy requirements (dashed) and (ii) MISOME secrecy capacity (dotted), for $K = 12$ users. Three values of β are considered: 0.8, 1, and 1.2, corresponding to $M = 15$, 12 and 10 antennas.

Fig. 5 shows the simulated per-user secrecy rate of the RCI-PA precoder from [18], with optimal power allocation. This is compared to the RCI-EP precoder. Fig. 5 also shows that the power allocation scheme reduces the sum-rate loss due to the secrecy requirements. For $\rho \geq 15$dB, RCI with power allocation achieves a per-user secrecy rate which is even higher than the per-user rate achieved by the optimal RCI-EP without secrecy requirements. Furthermore, Fig. 5 shows the simulated secrecy capacity $C_{s,\text{SU}}$ of a MISOME channel with the same per-message transmit power. Although $C_{s,\text{SU}}$ is obtained in a single-user and interference-free system [10], at high SNR, RCI with power allocation achieves a per-user secrecy rate as large as $C_{s,\text{SU}}$.

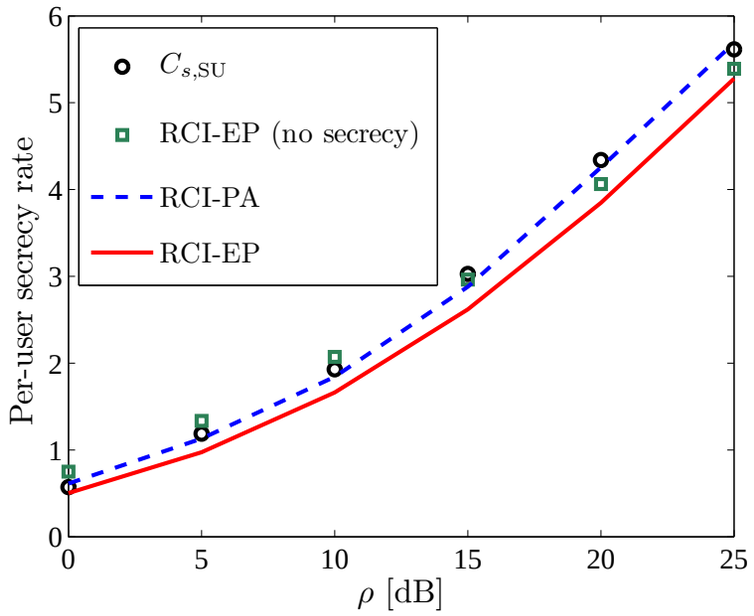

Figure 5. Per-user secrecy rate vs. ρ for $\beta = 1$ and $K = 4$ users: with equal power allocation (solid) and with optimal power allocation (dashed). The rate of the optimal RCI precoder without secrecy requirements (squares) and the secrecy capacity of the MISOME channel (circles) are also plotted.

5. Current research on multiuser MIMO physical layer security

Before concluding this chapter, we briefly discuss current research topics on physical layer security for multiuser MIMO communications, and we mention possible extensions of the results presented.

5.1. Power reduction strategy

Since for $\beta > 1$ the RCI precoder performs poorly in the high-SNR regime, a linear precoder based on RCI and power reduction could significantly increase the high-SNR secrecy sum-rate. In fact, we can observe from Fig. 2 that when $\beta > 1$ there is an optimal value of the SNR beyond which the achievable secrecy sum-rate $R_s^{\star\circ}$ starts decreasing.

A power reduction strategy would prevent the secrecy sum-rate from decreasing at high SNR by reducing the transmit power, and therefore reducing the SNR to the value that maximizes the secrecy sum-rate. For $1 < \beta < 2$ and large SNR, the RCI precoder with power reduction would thus achieve a constant nonnegative secrecy sum-rate. However, this strategy would not be effective for $\beta \geq 2$, since in this case the secrecy sum-rate is zero irrespective of the SNR.

5.2. Secrecy sum-rates in the presence of channel estimation error

In Sections 3 and 4, we discussed the secrecy rate performance of multi-user MIMO linear precoding for the case when perfect channel state information (CSI) is available at the transmitter. However, a more realistic scenario is the one where only an estimation of the channel is available at the transmitter. The relation between the true channel $\mathbf{H}$ and the estimated channel $\hat{\mathbf{H}}$ is usually modeled as

$$\mathbf{H} = \hat{\mathbf{H}} + \mathbf{E} \tag{19}$$

where the matrix $\mathbf{E}$ represents the channel estimation error, and it is independent from $\hat{\mathbf{H}}$. The knowledge of $\hat{\mathbf{H}}$ is used by the transmitter to obtain the RCI precoding matrix. The entries of $\hat{\mathbf{H}}$ and $\mathbf{E}$ are i.i.d. complex Gaussian random variables with zero mean and variances $1-\tau^2$ and τ^2, respectively. The value of $\tau \in [0,1]$ depends on the quality and technique used for channel estimation. When $\tau = 0$ the CSI is perfectly known, whereas $\tau = 1$ corresponds to the case when no CSI is available at all.

Future research could analyze the performance of linear precoding in the presence of imperfect CSI, deriving the achievable secrecy sum-rate as a function of the channel estimation error variance τ^2. This would allow to study how the CSI estimation error must scale with the SNR, in order to maintain a given high-SNR rate gap to the case with perfect CSI, so that the multiplexing gain is not affected. More specifically, the case of frequency division duplex (FDD) systems could be studied. Assuming that users quantize their channel directions by using B bits and employing random vector quantization (RVQ), and that they feed the quantization index back to the transmitter [30, 31], it would be interesting to determine how many feedback bits are required by each user in order to maintain a constant gap to the case with perfect CSI.

6. Conclusions

Throughout this chapter, we presented an up-to-date summary of the research in the field of physical layer security for multiuser MIMO communications. Unlike classical cryptography, physical layer security does not require key distribution and management, it does not rely on the limited computational power of the eavesdroppers, and it does not employ complex encryption algorithms. For these reasons, it is suitable for large dynamic wireless networks, and it has been proposed to enhance the protection of confidential messages transmitted over wireless channels. In this chapter, we especially focused on the problem of secret communication in a multiuser MIMO system. We considered the general case where a multiantenna base station transmits independent confidential messages to a generic number of users. We assumed that the users can potentially act maliciously and eavesdrop on each other. For this system set-up, we presented some transmission schemes based on linear precoding. We discussed the performance of these schemes as well as the cost of simultaneously guaranteeing secrecy to multiple users.

It has been recently shown that, in the large SNR regime, a linear precoding scheme based on regularized channel inversion can achieve secrecy without reducing the sum-rate at no additional cost when the number of transmit antennas M is larger than the number of users K. If $K = M$, secrecy can be achieved with a small rate loss or, alternatively, without reducing the sum-rate at a cost of less than 4dB in terms of the power transmitted. However, the secrecy requirements limit the maximum number of users that can be served with a non-zero rate. When $K > M$, there is an optimal value of the SNR beyond which the achievable rate starts decreasing, and at large SNR the secrecy sum-rate achievable by RCI precoding is poor. The base station could prevent the secrecy sum-rate from decreasing by reducing the transmit power, and therefore the SNR, to the value that maximizes the secrecy sum-rate. This would

result in a constant nonnegative high-SNR secrecy sum-rate. However, this strategy would not be effective if $K \geq 2M$.

Acknowledgements

The work of G. Geraci was supported in part by the Australian Government under International Postgraduate Research Scholarship, and in part by the Wireless Technologies Laboratory, CSIRO ICT Centre, Sydney, Australia. The work of J. Yuan was supported in part by the Australian Research Council Discovery Project (Grant DP120102607).

Author details

Giovanni Geraci[1,2,⋆] and Jinhong Yuan[1]

⋆ Address all correspondence to: giovanni.geraci@yahoo.it

1 School of Electrical Eng. & Telecommunications, The University of New South Wales, Australia
2 Wireless and Networking Technologies Laboratory, CSIRO ICT Centre, Sydney, Australia

References

[1] Y. Liang, H. V. Poor, and S. Shamai (Shitz). *Information Theoretic Security*. Dordrecht, The Netherlands: Now Publisher, 2009.

[2] R. Liu and W. Trappe. Eds, *Securing Wireless Communications at the Physical Layer*. New York: Springer Verlag, 2010.

[3] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst. Principles of physical-layer security in multiuser wireless networks: Survey. 2010. arXiv:1011.3754.

[4] A. D. Wyner. The wire-tap channel. *Bell System Tech. J.*, 54:1355–1387, 1975.

[5] I. Csiszár and J. Körner. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 24(3):339–348, May 1978.

[6] S. Leung-Yan-Cheong and M. Hellman. The Gaussian wire-tap channel. *IEEE Trans. Inf. Theory*, 24(4):451–456, July 1978.

[7] J. Barros and M.R.D. Rodrigues. Secrecy capacity of wireless channels. In *Proc. IEEE Int. Symp. on Inform. Theory (ISIT)*, pages 356–360, july 2006.

[8] Z. Li, W. Trappe, and R. Yates. Secret communication via multi-antenna transmission. In *Proc. CISS*, March 2007.

[9] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar. On the Gaussian MIMO wiretap channel. In *Proc. IEEE Int. Symp. on Inform. Theory (ISIT)*, pages 2471–2475, 2007.

[10] A. Khisti and G.W. Wornell. Secure transmission with multiple antennas I: The MISOME wiretap channel. *IEEE Trans. Inf. Theory*, 56(7):3088–3104, July 2010.

[11] S. Goel and R. Negi. Guaranteeing secrecy using artificial noise. *IEEE Trans. Wireless Commun.*, 7(6):2180–2189, 2008.

[12] X. Zhou and M.R. McKay. Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation. *IEEE Trans. Veh. Technol.*, 59(8):3831–3842, Oct. 2010.

[13] A. Mukherjee and A.L. Swindlehurst. Robust beamforming for security in MIMO wiretap channels with imperfect CSI. *IEEE Trans. Signal Process.*, 59(1):351–361, Jan. 2011.

[14] E. Ekrem and S. Ulukus. The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel. *IEEE Trans. Inf. Theory*, 57(4):2083–2114, April 2011.

[15] R. Liu and H.V. Poor. Secrecy capacity region of a multiple-antenna Gaussian broadcast channel with confidential messages. *IEEE Trans. Inf. Theory*, 55(3):1235–1249, 2009.

[16] R. Liu, T. Liu, H.V. Poor, and S. Shamai. Multiple-input multiple-output Gaussian broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 56(9):4215–4227, 2010.

[17] G. Geraci, J. Yuan, A. Razi, and I. B. Collings. Secrecy sum-rates for multi-user MIMO linear precoding. In *Proc. IEEE Int. Symp. on Wireless Commun. Systems (ISWCS)*, Nov. 2011.

[18] 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. Commun.*, 2012. to appear. Available: http://arxiv.org/abs/1207.5063.

[19] G. Geraci, J. Yuan, and I. B. Collings. Large system analysis of the secrecy sum-rates with regularized channel inversion precoding. In *Proc. IEEE Wireless Commun. Networking Conference (WCNC)*, Apr. 2012.

[20] Q.H. Spencer, C.B. Peel, A.L. Swindlehurst, and M. Haardt. An introduction to the multi-user MIMO downlink. *IEEE Comms. Mag.*, 42(10):60–67, Oct. 2004.

[21] Qinghua Li, Guangjie Li, Wookbong Lee, Moon Lee, D. Mazzarese, B. Clerckx, and Zexian Li. MIMO techniques in WiMAX and LTE: a feature overview. *IEEE Comms. Mag.*, 48(5):86–92, May 2010.

[22] Q.H. Spencer, A.L. Swindlehurst, and M. Haardt. Zero-forcing methods for downlink spatial multiplexing in multiuser MIMO channels. *IEEE Trans. Signal Process.*, 52(2):461–471, 2004.

[23] T. Yoo and A. Goldsmith. On the optimality of multiantenna broadcast scheduling using zero-forcing beamforming. *IEEE J. Sel. Areas Commun.*, 24(3):528–541, March 2006.

[24] C. B. Peel, B. M. Hochwald, and A. L. Swindlehurst. A vector-perturbation technique for near-capacity multiantenna multiuser communication - Part I: Channel inversion and regularization. *IEEE Trans. Commun.*, 53(1):195–202, January 2005.

[25] M. Joham, W. Utschick, and J.A. Nossek. Linear transmit processing in MIMO communications systems. *IEEE Trans. Signal Process.*, 53(8):2700–2712, August 2005.

[26] L. Sun and M.R. McKay. Eigen-based transceivers for the MIMO broadcast channel with semi-orthogonal user selection. *IEEE Trans. Signal Process.*, 58(10):5246–5261, Oct. 2010.

[27] S. Jin, M. R. McKay, X. Gao, and I. B. Collings. MIMO multichannel beamforming: SER and outage using new eigenvalue distributions of complex noncentral wishart matrices. *IEEE Trans. Commun.*, 56(3):424–434, 2008.

[28] V.K. Nguyen and J.S. Evans. Multiuser transmit beamforming via regularized channel inversion: A large system analysis. In *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, pages 1–4, Dec. 2008.

[29] V. K. Nguyen, R. Muharar, and J. S. Evans. Multiuser transmit beamforming via regularized channel inversion: A large system analysis. *Technical Report*, Nov. 2009. Available: http://cubinlab.ee.unimelb.edu.au/ rmuharar/doc/manuscriptrevRusdha22- 11.pdf.

[30] N. Jindal. MIMO broadcast channels with finite-rate feedback. *IEEE Trans. Inf. Theory*, 52(11):5045–5060, November 2006.

[31] D. Ryan, I. B. Collings, I. V. L. Clarkson, and R. W. Heath Jr. Performance of vector perturbation multiuser MIMO systems with limited feedback. *IEEE Trans. Commun.*, 57(9):2633–2644, 2008.