Hindawi Publishing Corporation
International Journal of Antennas and Propagation
Volume 2013, Article ID 546260, 7 pages
http://dx.doi.org/10.1155/2013/546260

Research Article

Secrecy Balancing over Two-User MISO Interference Channels with Rician Fading

Jiqing Ni, Zesong Fei, Chengwen Xing, Di Zhao, Niwei Wang, and Jingming Kuang

School of Information and Electronics, Beijing Institute of Technology, Beijing 100081, China

Correspondence should be addressed to Zesong Fei; feizesong@bit.edu.cn

Received 11 January 2013; Accepted 8 July 2013

Academic Editor: Cheng-Xiang Wang

This paper considers a 2-user multiple-input single-output (MISO) interference channel with confidential messages (IFC-CM), in which the Rician channel model is assumed. The coordinated beamforming vectors at the two transmitters have the similar parameterizations as those for perfect CSI, which could be optimized jointly and achieved by agreeing on the real parameters between the two users. Our main contribution is that a quadratic relationship between the two real-valued parameters can be derived for the Rician channel to reach the ergodic secrecy rate balancing point. Simulation results present the secrecy performance over the 2-user MISO IFC-CM scenario.

1. Introduction

Security can be provided in the physical layer instead of using passwords or keys, where signal processing techniques can be adopted to degrade an eavesdropper's channel so that meaningful detection at the eavesdropper is difficult or even impossible. Information-theoretic security, widely known as physical-layer security, was first introduced in the 1970s by Wyner [1]. In particular, the notion of secrecy capacity, which is the maximum achievable rate that can be kept confidential to the eavesdropper, was defined. Later, the work was extended to the Gaussian wiretap channel in [2]. In [3], Csiszar and Korner considered a more general wiretap channel model and showed that secure communication is in fact possible without using key encryption in the presence of the eavesdropper. Recently, the advances in multiple-input multiple-output (MIMO), multicell communication and relay offer new opportunities for physical-layer security.

For MIMO wiretap channel, [4] studied the performance tradeoffs and derived upper and lower bounds on the secrecy capacity both for finite systems and in the large-system limit. Using artificial noise to confuse the eavesdropper, masked MIMO beamforming has also been considered in multicast system [5, 6]. For cooperative communication employing relays, [7] established the utility of user cooperation in facilitating secure communication and derived an outer-bound on the optimal rate-equivocation region based on a four-terminal relay-eavesdropper channel. In [8], the optimization of cooperative jamming (CJ) is examined to enhance the physical-layer security of a wiretap fading channel via distributed relays. Also, He and Yener in [9] provided an achievable secrecy rate region for the general channel with an untrusted relay. Most recently, physical layer secrecy has been also applied to other communication systems, such as two-way relay [10], satellite communications [11], and interference channel with confidential messages (IFC-CM) [12].

In [12], the achievable secrecy rate region and an outer bound for the IFC-CM were presented, while [13] derived the inner and outer bounds of a one-sided IFC-CM and analyzed the gap between them. A K-user Gaussian IFC with secrecy constraints was investigated in [14] and by using an interference alignment scheme with secrecy precoding at each transmitter, and it was revealed that a nonzero secure degree of freedom can be achieved. The scenario was extended to the K-user Gaussian many-to-one IFC in [15] where the achievable secrecy sum-rate over all users was shown to be achievable by using nested lattice codes.

From the signal-processing perspective, secure (or secret) communications has also received much attention. Literature [16] has studied the power control problem and artificial noise parameter optimization for the max-min point and the single-user point over the two-user symmetric IFC-CM without multiple antennas. For the two-user MISO IFC-CM, [17] analyzed the key points on the Pareto boundary of the secrecy rate region for the two-user IFC with multiple-input single-output (MISO) antennas. Also, the multiple-input multiple-output (MIMO) Gaussian IFC-CM was investigated in [18] where a game-theoretic approach was proposed to permit the two transmitters to compromise to an operating point that better balances the network performance.

The focus of this paper is on a two-user interference channel with confidential messages (IFC-CM) in which each receiver is to decode its own message but could eavesdrop the message intended for the other user, where the imperfect CSI with Rician fading is assumed. First, the beamforming vectors corresponding to the Pareto-optimal ergodic secrecy rate points are characterized similar to the perfect CSI case. The coordinated optimal beamforming vectors at the two transmitters could be achieved by agreeing on the real parameters between the two users. Further, a quadratic relationship between the two real valued parameters can be derived, and the ergodic secrecy-rate balancing point which provides a secrecy rate-fair operating point will be determined by searching only one real-valued parameter.

The remainder of this paper is organized as follows. In Section 2, we present the system model. In Section 3, the Pareto boundary of the secrecy rate region is characterized, and some special operating points are considered. Section 4 extends the work to the statistical CSI, and the closed-form ergodic secrecy rate expressions are derived. Section 5 presents simulation results, and conclusions are drawn in Section 6 finally.

Notations. Throughout, vectors are denoted by boldface small letters while matrices are written in boldface capital letters. We use the superscripts $(\cdot)^*$, $(\cdot)^T$, and $(\cdot)^H$ to denote, respectively, the complex conjugate, transpose and Hermitian transpose operations. An identity matrix is denoted by $\mathbf{I}$.

2. MISO IFC-CM Model

We consider a two-user MISO IFC-CM, which may arise from a downlink cellular network with two multiantenna base stations (BSs) each transmitting to one desirable mobile station (MS). The message sent by each BS is confidential and required to be kept confidential to the other unintended MS. Due to the broadcast nature of wireless channels, however, the MSs may eavesdrop on the transmitted signals not intended for them and thus be regarded as eavesdroppers to each other, as is shown in Figure 1. Note that the two BSs trust each other so that they could design the coordinated beamformers together to optimize the secrecy rates. The MS receivers are assumed to have a single antenna, and each BS is equipped with N transmit antennas.

Based on the model, the received signals at the two MSs can be written as

$$\begin{aligned} y_1 &= \mathbf{h}_{11}^T \mathbf{w}_1 s_1 + \mathbf{h}_{21}^T \mathbf{w}_2 s_2 + n_1, \\ y_2 &= \mathbf{h}_{22}^T \mathbf{w}_2 s_2 + \mathbf{h}_{12}^T \mathbf{w}_1 s_1 + n_2, \end{aligned} \tag{1}$$

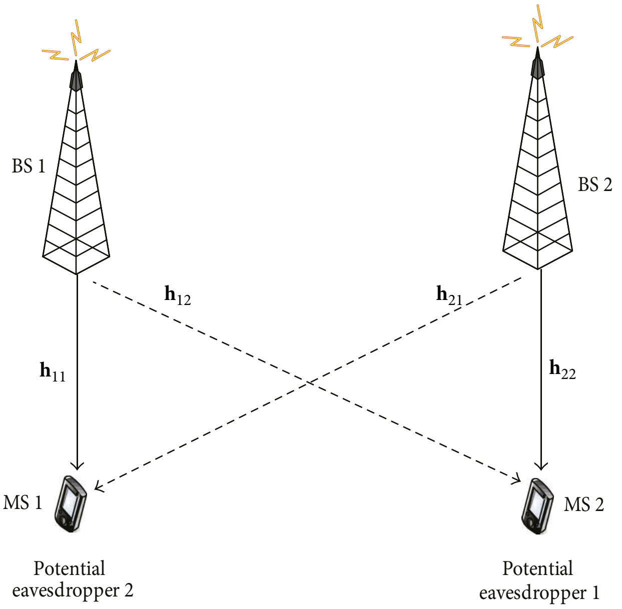


Figure 1: Coordinated beamforming with two BSs and two untrusted MSs.

where $\mathbf{h}_{ij} \in \mathbb{C}^{N\times 1}$ $(i, j = 1, 2)$ denotes the complex channel vector between BS i and MS j, s_i denotes the information symbol intended for MS i sent by BS i, n_i is the complex Gaussian noise with zero mean and variance σ^2, and $\mathbf{w}_i$ denotes the transmit beamforming vector at the ith BS and, without loss of generality, satisfies the peak power constraint $\|\mathbf{w}_i\| \le 1$. The noises and the channels are all independent to each other.

The received signal at each MS contains the desirable message and also the message intended for the other MS, and the channel can therefore be viewed as a virtual multiple-access channel (MAC) with the achievable rate already known in [19], which is given in the following lemma for completeness.

Lemma 1 (capacity for MAC [19]). *For a K-user MAC with channels $\{\mathbf{h}_k\}$ and transmit covariance matrices $\{\mathbf{\Sigma}_k\}$, for $k = 1, \ldots, K$, joint decoding with successive interference cancelation can achieve all the corner points of the capacity region. Given a decoding order $(\pi(1), \pi(2), \ldots, \pi(K))$ in which user $\pi(1)$ is decoded first, user $\pi(2)$ is decoded second, and so on, the achievable rate for user k is given by*

$$R_{\pi(k)} = \log_2 \left(1 + \frac{\mathbf{h}_{\pi(k)}^H \mathbf{\Sigma}_{\pi(k)} \mathbf{h}_{\pi(k)}}{\sigma^2 + \sum_{l=k+1}^{K} \mathbf{h}_{\pi(l)}^H \mathbf{\Sigma}_{\pi(l)} \mathbf{h}_{\pi(l)}} \right). \tag{2}$$

Lemma 1 states that the decoding order has no impact on the channel sum-rate but determines the achievable rate for each user. Specifically, the decoding order for the intended message and the eavesdropped message determines the message rate and the equivocation rate. We assume that the intended message is decoded first by treating the eavesdropped message as noise, and then the eavesdropped message is decoded without any interference. Then, the eavesdropped signals at the MSs can be equivalently expressed as

$$\begin{aligned} y_{e1} &= \mathbf{h}_{12}^{T}\mathbf{w}_1 s_1 + n_2, \\ y_{e2} &= \mathbf{h}_{21}^{T}\mathbf{w}_2 s_2 + n_1. \end{aligned} \tag{3}$$

The level of secrecy can be quantified by *secrecy rate* which is given by [3]

$$R_s = R_d - R_e, \tag{4}$$

where R_d denotes the message rate and R_e denotes the equivocation rate. With the intended message being decoded first, the secrecy rates for MS 1 and MS 2 can be, respectively, written as

$$\begin{aligned} R_{s1} &= \log_2\left(1 + \frac{|\mathbf{h}_{11}^{T}\mathbf{w}_1|^2}{\sigma^2 + |\mathbf{h}_{21}^{T}\mathbf{w}_2|^2}\right) - \log_2\left(1 + \frac{|\mathbf{h}_{12}^{T}\mathbf{w}_1|^2}{\sigma^2}\right), \\ R_{s2} &= \log_2\left(1 + \frac{|\mathbf{h}_{22}^{T}\mathbf{w}_2|^2}{\sigma^2 + |\mathbf{h}_{12}^{T}\mathbf{w}_1|^2}\right) - \log_2\left(1 + \frac{|\mathbf{h}_{21}^{T}\mathbf{w}_2|^2}{\sigma^2}\right). \end{aligned} \tag{5}$$

Based on the decoding order, the smallest R_d and the largest R_e are obtained at the MS receivers, and the achievable secrecy rates in (5) correspond to the inner bound for the secrecy rates over the general Gaussian MISO IFC-CM [12], which provides a worst-case scenario for analysis and optimization of the beamforming vectors. A similar argument has been used in [18] to justify their formulation.

We can define the *achievable secrecy rate region* to be the set of all secrecy rate pairs where the MISO beamforming vectors satisfy the power constraints at the BSs:

$$\mathscr{R}_s \triangleq \bigcup_{(\mathbf{w}_1,\mathbf{w}_2):\|\mathbf{w}_1\|,\|\mathbf{w}_2\|\le 1} (R_{s1}, R_{s2}). \tag{6}$$

The outer boundary of this region is called the *Pareto boundary*, because it consists of the operating points (R_{s1}, R_{s2}) for which it is impossible to improve one secrecy rate, without simultaneously decreasing the other secrecy rate. More precisely, we define the Pareto optimality of an operating point as follows.

Definition 2. A secrecy rate tuple (R_{s1}, R_{s2}) is Pareto optimal if there is no other tuple $(\widetilde{R}_{s1}, \widetilde{R}_{s2})$ such that $(\widetilde{R}_{s1}, \widetilde{R}_{s2}) \ge (R_{s1}, R_{s2})$ and $(\widetilde{R}_{s1}, \widetilde{R}_{s2}) \ne (R_{s1}, R_{s2})$ where the inequality operates component wisely.

It is noted that for a fixed channel, the secrecy rate region $\mathscr{R}_s$ is compact because the set $(\mathbf{w}_1, \mathbf{w}_2)$ subject to the power constraint is compact and the mapping from $(\mathbf{w}_1, \mathbf{w}_2)$ to (R_{s1}, R_{s2}) is continuous.

3. Ergodic Secrecy Rate Region with Rician Channel

3.1. Rician Channel Model. We consider that the channel vectors follow the Rician channel model, that is,

$$\mathbf{h}_{ij} = \overline{\mathbf{h}}_{ij} + \sqrt{\alpha}\Delta\mathbf{h}_{ij}, \tag{7}$$

where $\overline{\mathbf{h}}_{ij}$ is channel mean vector, $\Delta\mathbf{h}_{ij} \in \mathscr{CN}(0, I)$ denotes channel error vector and its entries are modelled as independent nonzero-mean random variables, α is the error coefficient and without losing generality, and α is assumed to be same for all the channels.

3.2. Ergodic Secrecy Rate Region. The ergodic secrecy rates are obtained by taking the expectation over the distribution of the channels, that is,

$$\begin{aligned} \overline{R}_{s1} &= \mathbb{E}_{\mathbf{h}_{11},\mathbf{h}_{12},\mathbf{h}_{21}}\left[R_{s1} \mid \mathbf{h}_{11}, \mathbf{h}_{12}, \mathbf{h}_{21}\right], \\ \overline{R}_{s2} &= \mathbb{E}_{\mathbf{h}_{22},\mathbf{h}_{21},\mathbf{h}_{12}}\left[R_{s2} \mid \mathbf{h}_{22}, \mathbf{h}_{21}, \mathbf{h}_{12}\right]. \end{aligned} \tag{8}$$

The achievable ergodic secrecy rate region can be expressed as the set of all the ergodic secrecy rates:

$$\overline{\mathscr{R}}_s \triangleq \bigcup_{(\mathbf{w}_1,\mathbf{w}_2):\|\mathbf{w}_1\|,\|\mathbf{w}_2\|\le 1} \left(\overline{R}_{s1}, \overline{R}_{s2}\right). \tag{9}$$

Consider $\overline{R}_{s1}$ first, and it has

$$\begin{aligned} \overline{R}_{s1} = {} & \mathbb{E}_{\mathbf{h}_{11},\mathbf{h}_{21}}\left[\log_2\left(1 + \left|\mathbf{h}_{11}^{T}\mathbf{w}_1\right|^2 + \left|\mathbf{h}_{21}^{T}\mathbf{w}_2\right|^2\right)\right] \\ & - \mathbb{E}_{\mathbf{h}_{21}}\left[\log_2\left(1 + \left|\mathbf{h}_{21}^{T}\mathbf{w}_2\right|^2\right)\right] \\ & - \mathbb{E}_{\mathbf{h}_{12}}\left[\log_2\left(1 + \left|\mathbf{h}_{12}^{T}\mathbf{w}_1\right|^2\right)\right], \end{aligned} \tag{10}$$

where the second and third terms could be tackled using [20]

$$\begin{aligned} & \mathbb{E}_{\mathbf{h}}\left[\log_2\left(1 + \left|\mathbf{h}^{T}\mathbf{w}\right|^2\right)\right] \\ & = \int_0^{\infty} \frac{e^{-t}}{t} \times \left(1 - \frac{1}{1+tp}\exp\left(-\frac{\alpha\left|\overline{\mathbf{h}}^{T}\mathbf{w}\right|^2 t}{1+t}\right)\right)dt, \end{aligned} \tag{11}$$

which involves a single integral which can be effectively calculated by using high-precision numerical integral methods [21]. Also note that it is monotonic increasing with $|\overline{\mathbf{h}}^{T}\mathbf{w}|^2$. While for the first term, it is more difficult to reexpress it with simpler expression, but we know that $|\mathbf{h}_{11}^{T}\mathbf{w}_1|^2 + |\mathbf{h}_{21}^{T}\mathbf{w}_2|^2$ belongs to noncentral chi-squared distribution, that is, the sum of the squares of independent Gaussian random variables having unit variance and nonzero means [22], the expectation is monotonic increasing with each mean. Although we do not present the closed form of the ergodic secrecy rate, but the monotony is very useful for us to further characterize the achievable ergodic secrecy rate region. $\overline{R}_{s2}$ has similar monotony.

3.3. Characterization of Ergodic Secrecy Rate Region. It shows that any point on the Pareto boundary should be achieved with full power and the corresponding beamforming vectors have the same characterization as perfect CSI case. To proceed, we first state the following lemma, which deals with the monotony of $\overline{R}_s$. The lemma is stated for $\overline{R}_{s1}$; similar results hold for $\overline{R}_{s2}$.

Lemma 3. *$\overline{R}_{s1}$ is monotonic increasing with $|\overline{\mathbf{h}}_{11}^T\mathbf{w}_1|$ and monotonic decreasing with $|\overline{\mathbf{h}}_{21}^T\mathbf{w}_2|$ and $|\overline{\mathbf{h}}_{12}^T\mathbf{w}_1|$.*

Proof . From discussions in the previous subsection, we know that $\mathbb{E}_{\mathbf{h}_{12}}[\log_2(1 + |\mathbf{h}_{12}^T\mathbf{w}_1|^2)]$ is monotonic increasing with $|\overline{\mathbf{h}}_{12}^T\mathbf{w}_1|$, and $\mathbb{E}_{\mathbf{h}_{11},\mathbf{h}_{21}}[\log_2(1 + |\mathbf{h}_{11}^T\mathbf{w}_1|^2 + |\mathbf{h}_{21}^T\mathbf{w}_2|^2)]$ is monotonic increasing with $|\overline{\mathbf{h}}_{11}^T\mathbf{w}_1|$ and $|\overline{\mathbf{h}}_{21}^T\mathbf{w}_2|$. Thus, it is easy to see $\overline{R}_{s1}$ is monotonic increasing with $|\overline{\mathbf{h}}_{11}^T\mathbf{w}_1|$ and decreasing with $|\overline{\mathbf{h}}_{12}^T\mathbf{w}_1|$.

Next we consider the term $|\overline{\mathbf{h}}_{21}^T\mathbf{w}_2|$, which is included in both the first term and second term in (10). We will show it using the method that for fixed $|\mathbf{h}_{11}^T\mathbf{w}_1| > 0$, it has that $\overline{R}_{s1}$ is monotonic decreasing with $|\overline{\mathbf{h}}_{21}^T\mathbf{w}_2|$. Further for any positive random variable $|\mathbf{h}_{11}^T\mathbf{w}_1| > 0$, the monotony still holds, that is, the term

$$\begin{aligned}&\mathbb{E}_{\mathbf{h}_{21}}\left[\log_2\left(1+\left|\mathbf{h}_{11}^T\mathbf{w}_1\right|^2+\left|\mathbf{h}_{21}^T\mathbf{w}_2\right|^2\right)\right]\\&\quad-\mathbb{E}_{\mathbf{h}_{21}}\left[\log_2\left(1+\left|\mathbf{h}_{21}^T\mathbf{w}_2\right|^2\right)\right]\end{aligned}\tag{12}$$

is monotonic decreasing with $|\overline{\mathbf{h}}_{21}^T\mathbf{w}_2|$. Note that since the expectation over $|\mathbf{h}_{11}^T\mathbf{w}_1|$ does not affect the monotony of this term. Thus, we have that $\overline{R}_{s1}$ is monotonic decreasing with $|\overline{\mathbf{h}}_{21}^T\mathbf{w}_2|$, which completes the proof. □

From the monotonicity of $\overline{R}_{s1}$, we see that the same conflicting situation happens as the perfect CSI case associated with the beamforming vectors. By utilizing the similar method, any beamforming vector leading to a Pareto-optimal ergodic secrecy rate tuple can be expressed as a linear combination of stochastic maximal-ratio combining (MRC) and stochastic zero-forcing (ZF) beamformers, which are defined as

$$\begin{aligned}\overline{\mathbf{w}}_1^{\mathrm{MRC}}&=\frac{\overline{\mathbf{h}}_{11}^*}{\|\overline{\mathbf{h}}_{11}\|},\qquad&\overline{\mathbf{w}}_2^{\mathrm{MRC}}&=\frac{\overline{\mathbf{h}}_{22}^*}{\|\overline{\mathbf{h}}_{22}\|},\\\overline{\mathbf{w}}_1^{\mathrm{ZF}}&=\frac{\Pi^{\perp}_{\overline{\mathbf{h}}_{12}^*}\overline{\mathbf{h}}_{12}^*}{\|\Pi^{\perp}_{\overline{\mathbf{h}}_{12}^*}\overline{\mathbf{h}}_{12}\|},\qquad&\overline{\mathbf{w}}_2^{\mathrm{ZF}}&=\frac{\Pi^{\perp}_{\overline{\mathbf{h}}_{21}^*}\overline{\mathbf{h}}_{21}^*}{\|\Pi^{\perp}_{\overline{\mathbf{h}}_{21}^*}\overline{\mathbf{h}}_{21}\|}.\end{aligned}\tag{13}$$

Theorem 4. *Any Pareto-optimal ergodic secrecy rate point is achievable with the beamforming strategy:*

$$\mathbf{w}_1=\frac{\lambda_1\overline{\mathbf{w}}_1^{MRC}+(1-\lambda_1)\overline{\mathbf{w}}_1^{ZF}}{\left\|\lambda_1\overline{\mathbf{w}}_1^{MRC}+(1-\lambda_1)\overline{\mathbf{w}}_1^{ZF}\right\|},\tag{14a}$$

$$\mathbf{w}_2=\frac{\lambda_2\overline{\mathbf{w}}_2^{MRC}+(1-\lambda_2)\overline{\mathbf{w}}_2^{ZF}}{\left\|\lambda_2\overline{\mathbf{w}}_2^{MRC}+(1-\lambda_2)\overline{\mathbf{w}}_2^{ZF}\right\|},\tag{14b}$$

where $0 \le \lambda_1,\ \lambda_2 \le 1$ are real-valued parameters.

Proof. The proof is essentially the same as that of its perfect CSI case. Hence, we only provide an outline here. The proof uses the method of contradiction.

To do so, we write any optimal beamforming vector as

$$\mathbf{w}_1' \triangleq \mathbf{w}_1 + \mathbf{u}_1,\tag{15}$$

where $\mathbf{w}_1 \in \operatorname{span}\{\overline{\mathbf{h}}_{11}^*, \overline{\mathbf{h}}_{12}^*\}$ and choosing $\mathbf{u}_1$ in the nullspace of $\operatorname{span}\{\overline{\mathbf{h}}_{11}^*, \overline{\mathbf{h}}_{12}^*\}$ such that $\|\mathbf{w}_1'\| = 1$. Clearly, $\mathbf{w}_1'$ achieves the same secrecy rate performance as $\mathbf{w}_1$. Hence, the optimal beamforming vector should lie in the space spanned by $\overline{\mathbf{h}}_{11}^*$ and $\overline{\mathbf{h}}_{12}^*$.

Next, we prove that the Pareto-optimal ergodic secrecy rate point can be obtained only when full power is used. To show this, we first consider $\overline{R}_{s1}$ and assume $\|\mathbf{w}_1\| < 1$. Construct $\mathbf{w}_1'' = \mathbf{w}_1 + \mathbf{v}_1$ such that $\|\mathbf{w}_1''\| = 1$. Based on the monotony of the associated terms, it can prove that if $\|\mathbf{w}_i\| < 1$, then it is possible to choose a new $\|\mathbf{w}_i''\| = 1$, such that $\overline{R}_{s1}$ is increased and $\overline{R}_{s2}$ is unchanged. Therefore, in order to reach the Pareto boundary, the transmitter should operate at full power. And any optimal beamformer in the space of $\operatorname{span}\{\overline{\mathbf{h}}_{11}^*, \overline{\mathbf{h}}_{12}^*\}$ could be formulated as the form in (14a). See [23] for more details regarding the proof. □

It is worth highlighting that previous Theorem 4 aligns with the result for the two-user MISO IFC-CM with perfect CSI [23]; this is because that they have the similar monotony with the terms associated with beamformers. This theorem also shows that we only need to vary the scalar real-valued parameters λ_1 and λ_2 in order to achieve any specific point on the Pareto boundary of the ergodic secrecy rate region. That is, these two BSs could achieve this specific points by setting λ_1 and λ_2 together.

4. Ergodic Secrecy Rate Balancing Point

4.1. Ergodic Secrecy Balancing. In the IFC model, user fairness is an important metric which can be achieved by balancing the user secrecy rates so that the weaker user is not overly compromised. Technically, this can be obtained by maximizing the worse-user's secrecy rate. That is,

$$\max\ \min\left\{\overline{R}_{s1}, \overline{R}_{s2}\right\}.\tag{16}$$

The secrecy rate balancing point can be realized by setting, if a solution exists,

$$\overline{R}_{s1} = \overline{R}_{s2},\tag{17}$$

which can be simplified as

$$|\overline{\mathbf{h}}_{11}^T\mathbf{w}_1|^2 + |\overline{\mathbf{h}}_{21}^T\mathbf{w}_2|^2 = |\overline{\mathbf{h}}_{22}^T\mathbf{w}_2|^2 + |\overline{\mathbf{h}}_{12}^T\mathbf{w}_1|^2.\tag{18}$$

Then, a simple relationship between λ_1 and λ_2 can be achieved.

Proposition 5. *For any given λ_2,* (18) *could be transformed into a quadratic equation:*

$$a_2\lambda_1^2 + b_2\lambda_1 + c_2 = 0, \tag{19}$$

where the coefficients are specified as (25)–(28).

Proof. We first introduce the following terms [24]:

$$\begin{aligned} p_1(\lambda_1) &\triangleq \left|\overline{\mathbf{h}}_{11}^H \mathbf{w}_1(\lambda_1)\right|^2, \\ p_2(\lambda_2) &\triangleq \left|\overline{\mathbf{h}}_{22}^H \mathbf{w}_2(\lambda_2)\right|^2, \\ q_1(\lambda_2) &\triangleq \left|\overline{\mathbf{h}}_{21}^H \mathbf{w}_2(\lambda_2)\right|^2, \\ q_2(\lambda_1) &\triangleq \left|\overline{\mathbf{h}}_{12}^H \mathbf{w}_1(\lambda_1)\right|^2. \end{aligned} \tag{20}$$

Substituting $\mathbf{w}_1$ in (14a) into $p_1(\lambda_1)$ and $q_2(\lambda_1)$, we have

$$p_1(\lambda_1) = \left\|\overline{\mathbf{h}}_{11}\right\|^2 \frac{(\alpha_1\lambda_1 + (1-\alpha_1))^2}{2\alpha_1\lambda_1^2 - 2\alpha_1\lambda_1 + 1}, \tag{21}$$

$$q_2(\lambda_1) = \frac{\beta_1^2\lambda_1^2}{2\alpha_1\lambda_1^2 - 2\alpha_1\lambda_1 + 1}, \tag{22}$$

where $\alpha_1 = 1 - (\|\Pi_{\overline{\mathbf{h}}_{12}}^{\perp}\overline{\mathbf{h}}_{11}\|/\|\overline{\mathbf{h}}_{11}\|)$ and $\beta_1 = |\overline{\mathbf{h}}_{12}^H\ \overline{\mathbf{h}}_{11}|/\|\overline{\mathbf{h}}_{11}\|$. The functions $p_2(\lambda_2)$, $q_1(\lambda_2)$ can be expressed and defined in a similar way with parameters $\alpha_2 = 1-(\|\Pi_{\overline{\mathbf{h}}_{21}}^{\perp}\overline{\mathbf{h}}_{22}\|/\|\overline{\mathbf{h}}_{22}\|)$ and $\beta_2 = |\overline{\mathbf{h}}_{21}^H\ \overline{\mathbf{h}}_{22}|/\|\overline{\mathbf{h}}_{22}\|$.

By substituting (20) into (18), we have

$$p_1(\lambda_1) - q_2(\lambda_1) = p_2(\lambda_2) - q_1(\lambda_2). \tag{23}$$

It can be easily seen that the left-hand-side (LHS) and the RHS of (23) are functions of only λ_1 and λ_2, respectively. Let the RHS of (23) be t_2. Then, we have

$$p_1(\lambda_1) - q_2(\lambda_1) = t_2. \tag{24}$$

Inserting (21) and (22) into (24) and simplifying the expression, we get the quadratic equation (19) with the coefficients as

$$a_2 = \alpha_1^2\left\|\overline{\mathbf{h}}_{11}\right\|^2 - (1+\sigma^2)\beta_1 - 2\alpha_1 t_2, \tag{25}$$

$$b_2 = 2(1-\alpha_1)\alpha_1\left\|\overline{\mathbf{h}}_{11}\right\|^2 + 2\alpha_1 t_2 + 2\alpha_1\beta_1\sigma^2, \tag{26}$$

$$c_2 = (1-\alpha_1)^2\left\|\overline{\mathbf{h}}_{11}\right\|^2 - t_2 + \beta_1\sigma^2, \tag{27}$$

$$t_2 = p_2(\lambda_2) - q_1(\lambda_2). \tag{28}$$

□

Next, we show by the method of contradiction that the secrecy rate balancing point corresponds to a unique solution in the feasible set if (19) is solvable. Assume that (19) has two solutions, λ_1 and λ_1', both corresponding to the secrecy balancing point, that is, $\overline{R}_{s1} = \overline{R}_{s2}(\lambda_1, \lambda_2) = \overline{R}_{s2}(\lambda_1', \lambda_2)$. However, from Lemma 3, $\overline{R}_{s2}(\lambda_1, \lambda_2)$ is a continuous monotonously decreasing function of λ_1 which means that for different λ_1 and λ_1', $\overline{R}_{s2}(\lambda_1, \lambda_2) \neq \overline{R}_{s2}(\lambda_1', \lambda_2)$. This contradicts the assumption which completes the proof.

For a given λ_1, λ_2 can be determined by solving a similar quadratic equation. Through Proposition 5, the secrecy rate balancing point can be determined by searching only one real-valued parameter in the feasible set. The secrecy rate balancing point achievable by $(\lambda_1^{\text{SRB}}, \lambda_2^{\text{SRB}})$ is the one that gives the maximal secrecy rate among all of the points that satisfy $\overline{R}_{s1} = \overline{R}_{s2}$. For the special case that there is no λ_1 satisfying the quadratic equation (19) for any λ_2 in the feasible set, it reduces to the single-user ergodic secrecy rate maximal point where the worse-user's secrecy rate is maximized. The single-user ergodic secrecy rate maximal point is where $\overline{R}_{s1}^{\max} < \overline{R}_{s2}^{\text{ZF}}$ or $\overline{R}_{s2}^{\max} < \overline{R}_{s1}^{\text{ZF}}$ is selected. Note that $\overline{R}_{s1}^{\max}$ denotes the maximal ergodic secrecy rate for $\overline{R}_{s1}$, and $\overline{R}_{s1}^{\text{ZF}}$ corresponds to the case that the BS 1 chooses the stochastic ZF beamforming to minimize the interference for the other link.

4.2. Single-User Maximal Ergodic Secrecy Rate.

4.2. Single-User Maximal Ergodic Secrecy Rate. At the single-user ergodic secrecy rate maximal point, one BS should choose the stochastic ZF beamforming strategy while the other BS tries to maximize the ergodic secrecy rate. In our two-user IFC-CM model, there are two single-user ergodic secrecy rate maximal points for $\overline{R}_{s1}$ and $\overline{R}_{s2}$, respectively. As the special case of secrecy balancing, the operating point is where $\overline{R}_{s1}^{\max} < \overline{R}_{s2}^{\text{ZF}}$ or $\overline{R}_{s2}^{\max} < \overline{R}_{s1}^{\text{ZF}}$ is selected.

$\overline{R}_{s1}$ can be formulated as a function of λ_1 with $\lambda_2 = 0$. In this case, there always exists an optimal λ_1, $\lambda_1^{\text{SU-opt}}$, ensuring that $\overline{R}_{s1}(\lambda_1^{\text{SU-opt}}) = \overline{R}_{s1}^{\max}$. The optimal $\lambda_1^{\text{SU-opt}}$ can be easily obtained by searching over the feasible set $0 \le \lambda_1 \le 1$. Similarly, the single-user secrecy rate maximal point for $\overline{R}_{s2}$ can be derived by setting $\lambda_1 = 0$ and $\lambda_2 = \lambda_2^{\text{SU-opt}}$. The single-user ergodic secrecy rate maximal points for $\overline{R}_{s1}$ and $\overline{R}_{s1}$ are endpoints on the Pareto boundary of the ergodic secrecy rate region. It can be also understood since there are no other operating points that could improve $\overline{R}_{s1}^{\max}$ or $\overline{R}_{s2}^{\max}$ further even sacrificing the other user's secrecy rate performance.

4.3. Other Key Points

4.3.1. Stochastic ZF. At this key point, both BSs choose the stochastic ZF beamformers, which can be achieved by simply setting $\lambda_1 = \lambda_2 = 0$. The secrecy ZF point is not on the Pareto boundary but in the interior of the ergodic secrecy rate region. Also, it is clear that at high SNR or for a large number of antennas, the secrecy ZF point will not be far away from the optimal point.

4.3.2. Nash Equilibrium. At the Nash equilibrium, the users (or BSs) selfishly optimize their beamforming vectors to maximize their own secrecy rates assuming that beamforming of

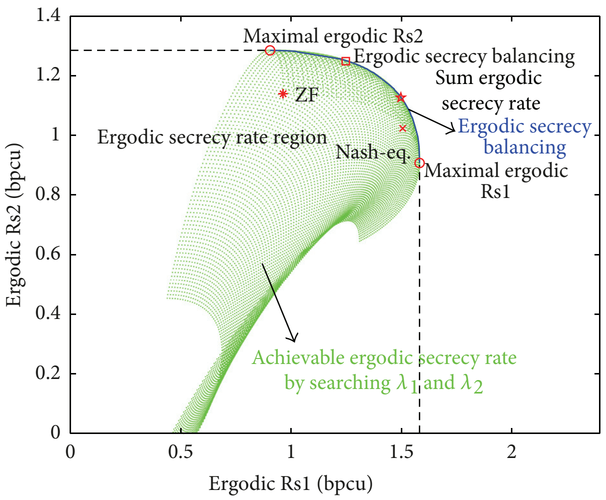


Figure 2: Ergodic secrecy rate region with 0 dB SNR for a random channel realization.

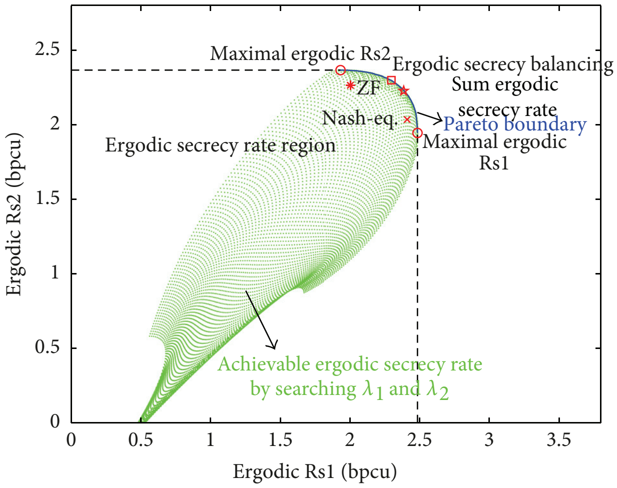


Figure 3: Ergodic secrecy rate region with 5 dB SNR for a random channel realization.

the other user is fixed [25]. We can iteratively search optimal λ_1 and λ_2 to reach the Nash-equilibrium point. This point is not optimal and thus in the interior of the ergodic secrecy rate region.

4.3.3. Sum Ergodic Secrecy Rate. The sum secrecy rate point is the point at which $\overline{R}_{s1} + \overline{R}_{s2}$ is maximized. Geometrically, this is where the Pareto boundary of the secrecy rate region, $\overline{\mathscr{R}}_s$, osculates a straight line with slope −1 [26]. It goes without saying that the sum secrecy rate point is on the Pareto boundary of $\overline{\mathscr{R}}_s$.

5. Simulation Results

Simulation results are provided to study the ergodic secrecy rate region for the two-user Gaussian MISO IFC-CM by the Pareto-boundary characterization for the cases with Rician channel. In the simulations, unless specified otherwise, we assume that the number of transmit antennas at each BS is 2 and the channel mean vector is randomly generated from an i.i.d. complex Gaussian distribution with zero mean and unit variance. Note that α is set as 0.1 in the all simulations.

Figure 2 shows an example of the ergodic secrecy rate region for a two-user Gaussian MISO IFC-CM over Rician fading with SNR at 0 dB. The achievable ergodic secrecy rate region generated from Theorem 4 by varying λ_1 and λ_2 in [0 1], and as we can see, the Pareto boundary including all the key operating points can be obtained through the parameterization. Also, the ergodic secrecy rate balancing point is on the Pareto boundary and it is where the Pareto boundary intersects the line $y = x$. In comparison, the sum secrecy rate point is the point where the Pareto boundary touches the straight line of slope −1. Results illustrate that the secrecy rate balancing point gives a lower sum secrecy rate compared to the sum secrecy rate point, but the worst-user secrecy rate is maximized. Also, the Nash-equilibrium point and the stochastic ZF point are in the interior of the secrecy rate region, that is, not Pareto optimal.

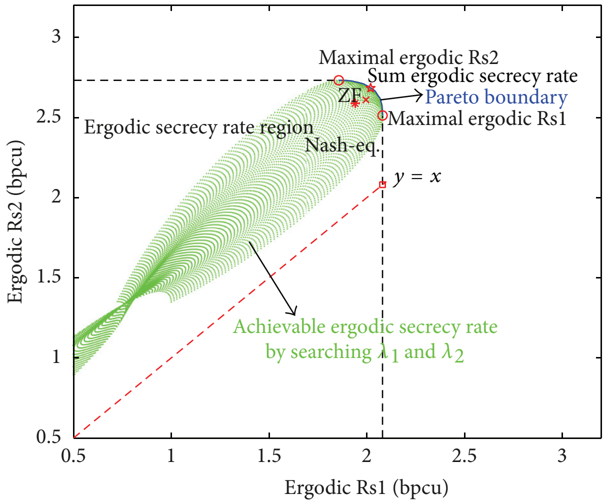


Figure 4: Ergodic secrecy rate region with 0 dB SNR for a random channel realization where the ergodic secrecy rate balancing point aligns with the single-user secrecy rate maximal point.

Figure 3 provides another example of the ergodic secrecy rate region but with SNR at 5 dB with same channel realization. As can be seen, when the SNR is increased, the corresponding ergodic secrecy rates are all improved and the stochastic ZF point in particular gets closer to the Pareto boundary.

Figure 4 considers the special case that the ergodic secrecy rate balancing point reduces to the single-user ergodic secrecy rate maximal point, which occurs when there is no solution to (18) for (λ_1, λ_2). Geometrically, the Pareto boundary of $\overline{\mathscr{R}}_s$ has no intersection point with the straight line $y = x$, which can be observed in the figure. Thus, the ergodic secrecy rate balancing point is reduced to the closest single-user ergodic secrecy rate maximal point.

6. Conclusion

In this paper, we studied the two-user MISO IFC-CM with Rician fading assumption. We revealed that the optimal beamforming vectors corresponding to the Pareto optimal point have the same parameterizations as those for perfect CSI. The secrecy rate balancing point, which provides the highest user fairness, was investigated. In particular, a quadratic relationship between the two real-valued parameters can be derived for the Rician channel to reach the ergodic secrecy rate balancing point. Simulation results show the secrecy performance of the proposed method.

Acknowledgments

This work was supported in part by China National S&T Major Project 2013ZX03003002-003, the National Natural Science Foundation of China under Grant no. 61101130, and the Excellent Young Scholar Research Funding of Beijing Institute of Technology under Grant no. 2013CX04038.

References

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

[2] S. K. Leung-Yan-Cheong and M. E. Hellman, "Gaussian wiretap channel," *IEEE Transactions on Information Theory*, vol. IT-24, no. 4, pp. 451–456, 1978.

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

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

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

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

[7] L. Lai and H. El Gamal, "The relay-eavesdropper channel: cooperation for secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, 2008.

[8] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1317–1322, 2011.

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

[10] H. Wang, Q. Yin, and X. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Transactions on Signal Processing*, vol. 60, no. 7, pp. 3532–3545, 2012.

[11] G. Zheng, P.-D. Arapoglou, and B. Ottersten, "Physical layer security in multibeam satellite systems," *IEEE Transactions on Wireless Communications*, vol. 11, no. 2, pp. 852–863, 2012.

[12] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: secrecy rate regions," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2493–2507, 2008.

[13] Z. Li, R. D. Yates, and W. Trappe, "Secrecy capacity region of a class of one-sided interference channel," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT '08)*, pp. 379–383, Toronto, Canada, July 2008.

[14] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," *IEEE Transactions on Information Theory*, vol. 57, no. 6, pp. 3323–3332, 2011.

[15] X. He and A. Yener, "The gaussian many-to-one interference channel with confidential messages," *IEEE Transactions on Information Theory*, vol. 57, no. 5, pp. 2730–2745, 2011.

[16] J. Zhu, J. Mo, and M. Tao, "Cooperative secret communication with artificial noise in symmetric interference channel," *IEEE Communications Letters*, vol. 14, no. 10, pp. 885–887, 2010.

[17] Z. Fei, J. Ni, D. Zhao, C. Xing, N. Wang, and J. Kuang, "Ergodic secrecy rate of two-user MISO interference channels with statistical CSI," submitted to *Science China Information Sciences*.

[18] S. A. A. Fakoorian and A. L. Swindlehurst, "MIMO interference channel with confidential messages: achievable secrecy rates and precoder design," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 640–649, 2011.

[19] S. Vishwanath, N. Jindal, and A. Goldsmith, "Duality, achievable rates, and sum-rate capacity of Gaussian MIMO broadcast channels," *IEEE Transactions on Information Theory*, vol. 49, no. 10, pp. 2658–2668, 2003.

[20] J. Li and A. P. Petropulu, "Ergodic secrecy rate for multiple-antenna wiretap channels with rician fading," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 861–867, 2011.

[21] D. H. Bailey, K. Jeyabalan, and X. S. Li, "A comparison of three high-precision quadrature schemes," *Experimental Mathematics*, vol. 14, no. 3, pp. 317–329, 2005.

[22] M. Alexander, F. A. Graybill, and D. C. Boes, *Introduction to the Theory of Statistics*, McGraw-Hill, 1974.

[23] E. A. Jorswieck and R. Mochaourab, "Secrecy rate region of MISO interference channel: pareto boundary and non- cooperative games," in *Proceedings of the International Workshop Smart Antennas*, Berlin, Germany, 2009.

[24] J. Lindblom, E. Karipidis, and E. G. Larsson, "Closed-form parameterization of the Pareto boundary for the two-user MISO interference channel," in *Proceedings of the 36th IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '11)*, pp. 3372–3375, Prague, Czech Republic, May 2011.

[25] P. Dubey, "Inefficiency of Nash equilibria," *Mathematics of Operations Research*, vol. 11, no. 1, pp. 1–8, 1986.

[26] E. G. Larsson and E. A. Jorswieck, "Competition versus cooperation on the MISO interference channel," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 7, pp. 1059–1069, 2008.

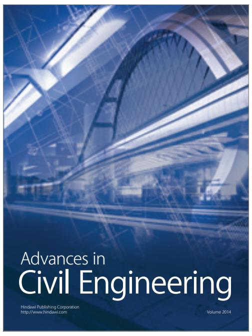
Journal of
Engineering

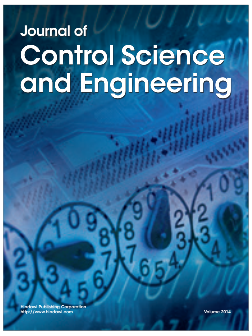
The Scientific World Journal

International Journal of
Rotating Machinery

Journal of
Sensors

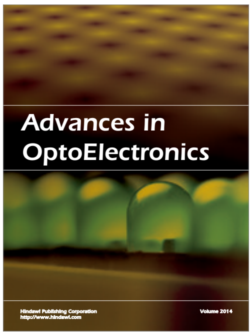
International Journal of
Distributed Sensor Networks


Advances in
Civil Engineering


Journal of
Control Science and Engineering

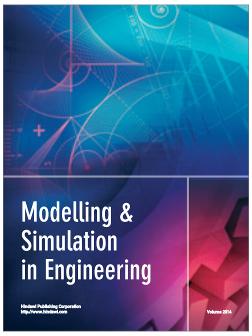
Journal of
Robotics

Journal of
Electrical and Computer Engineering

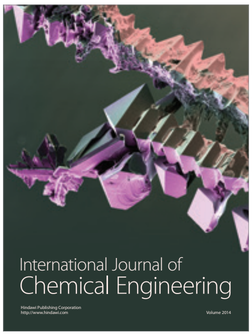

Advances in
OptoElectronics

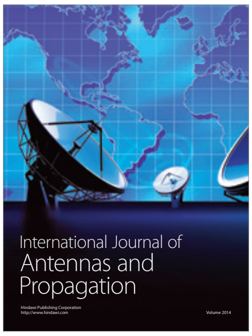
VLSI Design

International Journal of
Navigation and Observation

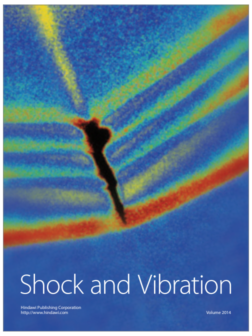

Modelling & Simulation in Engineering

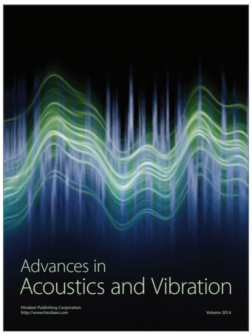
International Journal of
Aerospace Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and Propagation

Active and Passive Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration