MIMO INTERFERENCE CHANNEL WITH CONFIDENTIAL MESSAGES: GAME THEORETIC BEAMFORMING DESIGNS

S. Ali. A. Fakoorian and A. Lee Swindlehurst

Center for Pervasive Communications and Computing
University of California, Irvine
Irvine, CA 92697-2625
afakoori@uci.edu, swindle@uci.edu

ABSTRACT

We study the achievable rate regions of the multiple-input multiple-output (MIMO) interference channel with confidential messages sent to two receivers. Under this model, each receiver is an eavesdropper for the other link and tries to decode both its own message and the message intended for the other receiver. We describe several transmission schemes for Gaussian interference channels and derive their achievable secrecy rate regions under the assumption that the transmitters use low complexity beamforming algorithms. We also consider the trade-offs associated with their need for channel state information at the transmitter (CSIT). We approach the above topics from a game-theoretic perspective.

1. INTRODUCTION

Recent information-theoretic research on secure communication focuses on implementing security at the physical layer for multi-user scenarios. The wiretap channel [1] is the most basic physical layer model that captures the problem of communication security. The Gaussian multiple access channel (MAC) with confidential messages has been studied in [2, 3], and the broadcast channel with confidential messages has been addressed in [4, 5]. A special case of the interference channel with confidential messages is addressed in [6] where the message from the cognitive transmitter to its intended receiver is the only confidential message. Interference channels with confidential messages were first studied in [5] where the authors imposed the perfect secrecy constraint and obtained inner and outer bounds for the perfect secrecy rate region. While secrecy capacity for the wiretap channel with multi-antenna nodes has been investigated extensively up to now [7]-[10], the effect of multi-antenna nodes on secrecy in multi-user scenarios has not yet been addressed extensively in the literature. In fact, all the references [2]-[6] assume single antenna nodes.

In this work, we focus on the two user MIMO interference channel (IFC) with confidential messages, where two transmitters with multiple antennas want to send independent and confidential information to their intended receivers while the receivers eavesdrop, i.e., try to decode the message of the other link. With respect to the availability of channel state information at the transmitters (CSIT), we propose several transmission schemes for Gaussian interference channels and derive their achievable secrecy rate regions. Based on the level of available CSIT, we also define cooperative and non-cooperative games with transmitters as players and secrecy rates as utility functions.

2. SYSTEM MODEL

We consider a two-user Gaussian interference channel, where transmitter 1 with N_1 antennas and transmitter 2 with N_2 antennas send independent and confidential messages W_1 and W_2 to receiver 1 with M_1 antennas and receiver 2 with M_2 antennas, respectively. Each transmitter attempts to keep its message confidential from the unintended receiver; i.e., each receiver is an eavesdropper for the respective transmitter of the other receiver. The corresponding information-theoretic secrecy constraint is given by [5]

$$I(W_j; Y_i) = 0 \quad (i \neq j \quad i, j \in \{1, 2\}) \quad (1)$$

where $I(W_j; Y_i)$ represents the mutual information between W_j and Y_i , and Y_i is the $M_i \times 1$ output vector at receiver i ($i=1, 2$) and for a specific realization is given by

$$\mathbf{y}_1 = \mathbf{H}_1 \mathbf{x}_1 + \mathbf{G}_2 \mathbf{x}_2 + \mathbf{n}_1 \quad (2)$$

$$\mathbf{y}_2 = \mathbf{H}_2 \mathbf{x}_2 + \mathbf{G}_1 \mathbf{x}_1 + \mathbf{n}_2 \quad (3)$$

In the above equations, $\mathbf{x}_i$ is a zero-mean $N_i \times 1$ random vector with the average power constraint $\text{Tr}(E\{X_i X_i^H\}) \leq q_i$, $i=1, 2$, $\mathbf{n}_i \in \mathbb{C}^{M_i \times 1}$ is an additive white Gaussian noise (AWGN) vector at receiver i with i.i.d. entries distributed as $\mathcal{CN}(0, 1)$. The channels are assumed to be quasi-static

This work was supported by the U.S. Army Research Office under the Multi-University Research Initiative (MURI) grant W911NF-07-1-0318.

flat Rayleigh fading and independent of each other. The direct channel $\mathbf{H}_i \in \mathbb{C}^{M_i \times N_i}$ has i.i.d. entries distributed as $\mathcal{CN}(0, \sigma_{di}^2)$ and the cross channel $\mathbf{G}_i$ has i.i.d. entries distributed as $\mathcal{CN}(0, \sigma_{ci}^2)$, for $i = 1, 2$.

In the following Sections, we study the MIMO IFC with confidential messages as a game with transmitters as players and secrecy rates as utility functions. The problem is a cooperative game if transmitters exchange their CSI and cooperate in choosing their transmission parameters. If such information is not shared, we refer to it as a non-cooperative game.

3. GAME THEORETIC BEAMFORMING SCHEMES

3.1. Non-cooperative Jamming (NCJ)

In this case we assume that each transmitter i only knows his own channel $\mathbf{H}_i$. Instead of attempting to maximize his secrecy rate, which is not possible without knowledge of the eavesdropper's channels, it is reasonable for each transmitter to focus on minimizing the information that the unintended receiver may obtain. The idea is to jamming or artificial noise signal to increase the interference seen by the eavesdropper in such a way that the eavesdropper's channel is degraded while the channel of the intended receiver is not. Similar problems have been considered for the wiretap channel in [7] and [8]. At each transmitter, a portion of the transmit power is used to broadcast the information signal, and the remainder of the power is used to broadcast artificial noise in order to jam the unintended receiver. The jamming signal is designed such that it is orthogonal to the space spanned by the information signal, so that it has no impact on the desired link.

The signal vector of, e.g., transmitter 1 is given by:

$$\mathbf{x}_1 = \mathbf{T}_1 \mathbf{z}_1 + \mathbf{T}'_1 \mathbf{z}'_1 \quad Z_1 \sim \mathcal{CN}(\mathbf{0}, \mathbf{Q}_1) \quad Z'_1 \sim \mathcal{CN}(\mathbf{0}, \mathbf{Q}'_1), \quad (4)$$

where each element of the $r_1 \times 1$ vector $\mathbf{z}_1$ represents an independently-encoded Gaussian codebook symbol, and $1 \leq r_1 \leq \min(N_1, M_1)$ is the number of data streams used to transmit the information-bearing symbols. Assuming that transmitter one allocates a fraction $0 \leq \lambda_1 \leq 1$ of its power to $\mathbf{z}_1$, the diagonal covariance matrix $\mathbf{Q}_1 = E\{Z_1 Z_1^H\}$ is determined by waterfilling $\lambda_1 q_1$ over the r_1 largest singular values of $\mathbf{H}_1$. The elements of the $(N_1 - r_1) \times 1$ vector $\mathbf{z}'_1$ represent artificial noise with covariance $\mathbf{Q}'_1 = \frac{(1-\lambda_1)q_1}{N_1-r_1} \mathbf{I}$. The matrix $\mathbf{T}_1$ represents the $N_1 \times r_1$ transmit beamformer matrix corresponding to $\mathbf{z}_1$ and is formed from the first r_1 dominant right singular vectors of $\mathbf{H}_1$, while $\mathbf{T}'_1$ is chosen to be the remaining $(N_1 - r_1)$ right singular vectors. This guarantees that

$$\text{span}(\mathbf{H}_1 \mathbf{T}_1) \perp \text{span}(\mathbf{H}_1 \mathbf{T}'_1). \quad (5)$$

Similar descriptions exist for transmitter 2.

By applying Theorem 2 of [5], the following secrecy rates are achievable

$$0 \leq R_1 \leq \log |\mathbf{H}_1 \mathbf{T}_1 \mathbf{Q}_1 \mathbf{T}_1^H \mathbf{H}_1^H \mathbf{E}_1 + \mathbf{I}| - \log |\mathbf{G}_1 \mathbf{T}_1 \mathbf{Q}_1 \mathbf{T}_1^H \mathbf{G}_1^H \mathbf{F}_1 + \mathbf{I}| \quad (6)$$

$$0 \leq R_2 \leq \log |\mathbf{H}_2 \mathbf{T}_2 \mathbf{Q}_2 \mathbf{T}_2^H \mathbf{H}_2^H \mathbf{E}_2 + \mathbf{I}| - \log |\mathbf{G}_2 \mathbf{T}_2 \mathbf{Q}_2 \mathbf{T}_2^H \mathbf{G}_2^H \mathbf{F}_2 + \mathbf{I}| \quad (7)$$

where $\mathbf{F}_1^{-1} = \mathbf{G}_1 \mathbf{T}'_1 \mathbf{Q}'_1 \mathbf{T}'_1{}^H \mathbf{G}_1^H + \mathbf{H}_2 \mathbf{T}'_2 \mathbf{Q}'_2 \mathbf{T}'_2{}^H \mathbf{H}_2^H + \mathbf{I}$ and $\mathbf{E}_1^{-1} = \mathbf{H}_1 \mathbf{T}'_1 \mathbf{Q}'_1 \mathbf{T}'_1{}^H \mathbf{H}_1^H + \mathbf{G}_2 (\mathbf{T}_2 \mathbf{Q}_2 \mathbf{T}_2^H + \mathbf{T}'_2 \mathbf{Q}'_2 \mathbf{T}'_2{}^H) \mathbf{G}_2^H + \mathbf{I}$. Similar expressions exist for $\mathbf{E}_2$ and $\mathbf{F}_2$.

3.2. Non-cooperative GSVD

In this case we assume that each transmitter i knows not only his direct channel $\mathbf{H}_i$, but also his cross-channel $\mathbf{G}_i$. Such information may be available in a time-division duplex (TDD) setting due to previous communication between transmitter 1 and receiver 2. With this level of CSIT, a reasonable beamforming scheme is obtained by simply treating the IFC as two parallel wiretap channels, and using the generalized singular value decomposition (GSVD) method to design the beamformers for each transmitter, as in [10].

GSVD Transform: Given two matrices $\mathbf{H}_1 \in \mathbb{C}^{M_1 \times N_1}$ and $\mathbf{G}_1 \in \mathbb{C}^{M_2 \times N_1}$, $gsvd(\mathbf{H}_1, \mathbf{G}_1)$ returns unitary matrices $\mathbf{\Psi}_{r1} \in \mathbb{C}^{M_1 \times M_1}$ and $\mathbf{\Psi}_{e1} \in \mathbb{C}^{M_2 \times M_2}$, positive semi-definite diagonal matrices $\mathbf{B}_1$ and $\mathbf{D}_1$, and a matrix $\mathbf{A}_1 \in \mathbb{C}^{N_1 \times d}$ with $d = \min(N_1, M_1 + M_2)$, such that

$$\mathbf{H}_1 \mathbf{A}_1 = \mathbf{\Psi}_{r1} \mathbf{B}_1 \quad (8)$$

$$\mathbf{G}_1 \mathbf{A}_1 = \mathbf{\Psi}_{e1} \mathbf{D}_1 \quad (9)$$

The nonzero elements of $\mathbf{B}_1$ are in ascending order while the nonzero elements of $\mathbf{D}_1$ are in decreasing order, and $\mathbf{B}_1^T \mathbf{B}_1 + \mathbf{D}_1^T \mathbf{D}_1 = \mathbf{I}$.

Transmitter 1 constructs $\mathbf{x}_1$ as

$$\mathbf{x}_1 = \mathbf{A}_1 \mathbf{s}_1, \quad S_1 \sim \mathcal{CN}(\mathbf{0}, \mathbf{P}_1) \quad (10)$$

where each nonzero element of the vector $\mathbf{s}_1$ represents an independently encoded Gaussian codebook symbol that is beamformed with the corresponding column of the matrix $\mathbf{A}_1$, and $\mathbf{P}_1$ is a positive semi-definite diagonal matrix representing the power allocated to each data stream and is given by [9]

$$p_i = \begin{cases} \max(0, \frac{-1 + \sqrt{1 - 4b_i d_i + 4(b_i - d_i)b_i d_i / (\mu a_i)}}{2b_i d_i}), & b_i > d_i \\ 0, & \text{otherwise} \end{cases} \quad (11)$$

where p_i , b_i , d_i and a_i are the i th diagonal elements of the matrices $\mathbf{P}_1$, $\mathbf{B}_1^T \mathbf{B}_1$, $\mathbf{D}_1^T \mathbf{D}_1$ and $\text{diag}(\mathbf{A}_1^H \mathbf{A}_1)$, respectively, and the Lagrange parameter $\mu > 0$ is chosen to satisfy the power constraint $\text{Tr}(\mathbf{A}_1 \mathbf{P}_1 \mathbf{A}_1^H) \leq q_1$. In [9], we proved that

the above $\mathbf{P}_1$ is the optimal power allocation policy that maximizes $I(X_1; Y_1) - I(X_1; Y_2)$ for $X_1 = \mathbf{A}_1 \mathbf{S}_1$ and $X_2 = 0$. A description similar to that above would also apply to transmitter 2.

Applying Theorem 2 of [5] yields the following rate region expressions for this technique:

$$\begin{aligned} R_1 &\leq \log |\Psi_{r1} \mathbf{C}_1 \mathbf{P}_1 \mathbf{C}_1^T \Psi_{r1}^H + \Psi_{e2} \mathbf{D}_2 \mathbf{P}_2 \mathbf{D}_2^T \Psi_{e2}^H + \mathbf{I}| \\ &\quad - \log |\Psi_{e2} \mathbf{D}_2 \mathbf{P}_2 \mathbf{D}_2^T \Psi_{e2}^H + \mathbf{I}| - \log |\Psi_{e1} \mathbf{D}_1 \mathbf{P}_1 \mathbf{D}_1^T \Psi_{e1}^H + \mathbf{I}| \\ R_2 &\leq \log |\Psi_{r2} \mathbf{C}_2 \mathbf{P}_2 \mathbf{C}_2^T \Psi_{r2}^H + \Psi_{e1} \mathbf{D}_1 \mathbf{P}_1 \mathbf{D}_1^T \Psi_{e1}^H + \mathbf{I}| \\ &\quad - \log |\Psi_{e1} \mathbf{D}_1 \mathbf{P}_1 \mathbf{D}_1^T \Psi_{e1}^H + \mathbf{I}| - \log |\Psi_{e2} \mathbf{D}_2 \mathbf{P}_2 \mathbf{D}_2^T \Psi_{e2}^H + \mathbf{I}| \end{aligned} \quad (12)$$

where $\mathbf{A}_2$, $\mathbf{B}_2$, $\mathbf{D}_2$, Ψ_{r2} , and Ψ_{e2} are given by $\text{gsvd}(\mathbf{H}_2, \mathbf{G}_2)$. While this approach will have improved secrecy over the method of Section III-A due to its more informed choice of beamformers and power levels, it cannot properly account for the interference of transmitter 1's signal with transmitter 2's signal at receiver 2, and vice versa.

3.3. Cooperative Solution: GSVD + Artificial Noise Alignment

In this case we assume that each transmitter i knows not only its own channel $\mathbf{H}_i$ and the cross-channel $\mathbf{G}_i$, but also $\text{span}(\mathbf{G}_j \mathbf{A}_j \mathbf{P}_j)$ which represents the subspace in which transmitter j 's information signal lies when it reaches receiver i . We assume that the transmitters exchange information about these subspaces with each other, and we present an approach that exploits this information in a cooperative manner in order to increase the secrecy rate performance of each link. The approach involves a combination of GSVD beamforming and the altruistic use of artificial noise to mask the information signal from the other transmitter in one's own receiver. In this sense, this scheme allows *transmitter cooperation* without exchanging confidential messages. See Fig. 1 for an illustration of the idea.

The transmitted signal vector of user i is given by:

$$\mathbf{x}_i = \mathbf{A}_i \mathbf{s}_i + \mathbf{T}_{ni} \mathbf{x}_{ni} \quad (i \in \{1, 2\}) \quad (13)$$

where $\mathbf{S}_i \sim \mathcal{CN}(\mathbf{0}, \mathbf{P}_i)$, $\mathbf{X}_{ni} \sim \mathcal{CN}(\mathbf{0}, \mathbf{Q}_{ni})$, and $\mathbf{Q}_{ni} = \frac{(1-\alpha_i)q_i}{\text{Tr}(\mathbf{T}_{ni}^H \mathbf{T}_{ni})}$. As before, $\mathbf{A}_i$ represents the beamforming matrix used to transmit confidential data from transmitter i to receiver i , and is calculated as described earlier, using $\text{gsvd}(\mathbf{H}_i, \mathbf{G}_i)$. Each non-zero element of the vector $\mathbf{s}_i$ represents an independently encoded Gaussian codebook symbol for transmitter i that is beamformed with the corresponding column of $\mathbf{A}_i$, and $\mathbf{P}_i$ is a positive semi-definite diagonal matrix representing the power allocated to the confidential data symbols using (11) with the updated power constraint

$$\text{Tr}(\mathbf{A}_i \mathbf{P}_i \mathbf{A}_i^H) \leq \alpha_i q_i.$$

The elements of the vector $\mathbf{x}_{ni}$ represent synthetic noise symbols broadcast by transmitter i along the column vectors of

Fig. 1. The idea of Artificial Noise Alignment (ANA).

the beamforming matrix $\mathbf{T}_{ni}$. In the following, we describe how the beamforming matrices $\mathbf{T}_{n1}$ and $\mathbf{T}_{n2}$ are constructed.

Let us consider, e.g., the M_1 -dimensional complex signal space of receiver 1. Let q_{12} be the number of non-zero elements of the vector $\mathbf{s}_2$ that do not lie in the nullspace of $\mathbf{G}_2$, which can be determined using (11) and the specific form of the diagonal matrix $\mathbf{D}_2$. Consequently, Ψ'_{e2} is the corresponding q_{12} columns of the unitary matrix Ψ_{e2} . At receiver 1, the information signal of transmitter 2, $\mathbf{A}_2 \mathbf{s}_2$, after spatial mixing by the channel matrix $\mathbf{G}_2$, lies in a q_{12} -dimensional subspace of $\mathbb{C}^{M_1}$, with orthonormal basis Ψ'_{e2} . Using a similar description, $\mathbf{H}_1 \mathbf{A}_1 \mathbf{s}_1$ lies in a q_{11} -dimensional subspace with orthonormal basis Ψ'_{r1} , where q_{11} is the number of non-zero elements of the vector $\mathbf{s}_1$, and Ψ'_{r1} is the corresponding q_{11} columns of the unitary matrix Ψ_{r1} in (8).

As mentioned before, the goal for transmitter 1 is to send artificial noise symbols along the column vectors of the beamforming matrix $\mathbf{T}_{n1}$ so that, after spatial mixing by $\mathbf{H}_1$, it aligns itself as much as possible with the subspace at receiver 1 in which $\mathbf{s}_2$ lies, and impacts as little as possible the subspace in which $\mathbf{s}_1$ lies at receiver 1. Define $t_1 = \min(N_1, M_1 - q_{11}, q_{12})$. More precisely, the goal of transmitter 1 is to choose the $N_1 \times t_1$ beamforming matrix such that, to the extent possible, $\mathbf{H}_1 \mathbf{T}_{n1}$ is nearly aligned with $\text{span}(\Psi'_{e2})$ and nearly orthogonal to $\text{span}(\Psi'_{r1})$. To do this, we propose the use of the following norm criterion:

$$\begin{aligned} \min_{\mathbf{T}_{n1}} & \left\| \mathbf{H}_1 \mathbf{T}_{n1} - \Psi'_{e2} \Psi_{e2}^H \mathbf{H}_1 \mathbf{T}_{n1} \right\|_F^2 \\ & + \left\| \mathbf{H}_1 \mathbf{T}_{n1} - (\mathbf{I} - \Psi'_{r1} \Psi_{r1}^H) \mathbf{H}_1 \mathbf{T}_{n1} \right\|_F^2 \end{aligned} \quad (14)$$

where we have used the fact that $\Psi_{e2}^H \Psi'_{e2} = \mathbf{I}$ and $\Psi_{r1}^H \Psi'_{r1} = \mathbf{I}$. After some straightforward computation, the above minimization problem can be written as:

$$\min_{\mathbf{T}_{n1}} \text{Tr}(\mathbf{T}_{n1}^H \mathbf{H}_1^H [\Psi'_{r1} \Psi_{r1}^H + \mathbf{I} - \Psi'_{e2} \Psi_{e2}^H] \mathbf{H}_1 \mathbf{T}_{n1}) \quad (15)$$

The solution to (15) is to set $\mathbf{T}_{n1}$ to be the eigenvectors corresponding to the t_1 minimum eigenvalues of $\mathbf{H}_1^H [\Psi'_{r1} \Psi_{r1}^H + \mathbf{I} -$

$\Psi'_{e2} \Psi'^H_{e2}] \mathbf{H}_1$. A description similar to that above also applies to transmitter 2 and $\mathbf{T}_{n2}$.

The algorithm above can be shown to yield the following secrecy rate region:

$$R_1 \leq \log |\mathbf{H}_1 \mathbf{A}_1 \mathbf{P}_1 \mathbf{A}_1^H \mathbf{H}_1^H \mathbf{K}_{r1}^{-1} + \mathbf{I}| - \log |\mathbf{G}_1 \mathbf{A}_1 \mathbf{P}_1 \mathbf{A}_1^H \mathbf{G}_1^H \mathbf{K}_{e1}^{-1} + \mathbf{I}| \quad (16)$$

$$R_2 \leq \log |\mathbf{H}_2 \mathbf{A}_2 \mathbf{P}_2 \mathbf{A}_2^H \mathbf{H}_2^H \mathbf{K}_{r2}^{-1} + \mathbf{I}| - \log |\mathbf{G}_2 \mathbf{A}_2 \mathbf{P}_2 \mathbf{A}_2^H \mathbf{G}_2^H \mathbf{K}_{e2}^{-1} + \mathbf{I}|, \quad (17)$$

where

$$\begin{aligned} \mathbf{K}_{r1} &= \mathbf{H}_1 \mathbf{T}_{n1} \mathbf{Q}_{n1} \mathbf{T}_{n1}^H \mathbf{H}_1^H + \mathbf{G}_2 (\mathbf{A}_2 \mathbf{P}_2 \mathbf{A}_2^H \\ &\quad + \mathbf{T}_{n2} \mathbf{Q}_{n2} \mathbf{T}_{n2}^H) \mathbf{G}_2^H + \mathbf{I} \\ \mathbf{K}_{e1} &= \mathbf{H}_2 \mathbf{T}_{n2} \mathbf{Q}_{n2} \mathbf{T}_{n2}^H \mathbf{H}_2^H + \mathbf{G}_1 \mathbf{T}_{n1} \mathbf{Q}_{n1} \mathbf{T}_{n1}^H \mathbf{G}_1^H + \mathbf{I} \\ \mathbf{K}_{r2} &= \mathbf{H}_2 \mathbf{T}_{n2} \mathbf{Q}_{n2} \mathbf{T}_{n2}^H \mathbf{H}_2^H + \mathbf{G}_1 (\mathbf{A}_1 \mathbf{P}_1 \mathbf{A}_1^H \\ &\quad + \mathbf{T}_{n1} \mathbf{Q}_{n1} \mathbf{T}_{n1}^H) \mathbf{G}_1^H + \mathbf{I} \\ \mathbf{K}_{e2} &= \mathbf{H}_1 \mathbf{T}_{n1} \mathbf{Q}_{n1} \mathbf{T}_{n1}^H \mathbf{H}_1^H + \mathbf{G}_2 \mathbf{T}_{n2} \mathbf{Q}_{n2} \mathbf{T}_{n2}^H \mathbf{G}_2^H + \mathbf{I}. \end{aligned}$$

In [11], we present an iterative algorithm that find the Kalai-Smorodinsky (K-S) solution for the cooperative game (GSVD+ANA) and considers the properties of the obtained operating points from the viewpoint of fairness and efficiency.

4. NUMERICAL RESULTS

In this section, we compare via simulation the achievable secrecy rate regions of the non-cooperative and cooperative transmission schemes discussed in Section III. This comparison is done for various SNR and interference conditions and also different numbers of antennas for the transmitters and receivers.

For all presented numerical results, we assume $\sigma_{d1}^2 = \sigma_{d2}^2 = \sigma_d^2$, and $\sigma_{c1}^2 = \sigma_{c2}^2 = \sigma_c^2$. In each figure, the values of σ_d^2 and σ_c^2 , as well as q_1 and q_2 , will be depicted. All displayed results are calculated based on an average of at least 100 independent channel realizations. In each trial, the achievable secrecy rate region of the non-cooperative jamming scheme (NCJ), which was proposed in Section III-A, is obtained by independently varying transmit parameters r_1, r_2, λ_1 and λ_2 , where $1 \leq r_i \leq \min(N_i, M_i)$ and $0 \leq \lambda_i \leq 1$, as described in Section III-A. Then, for each set of transmit parameters, the achievable secrecy rates in (6) and (7) are evaluated numerically. The achievable secrecy rate region of the second non-cooperative transmission scheme (GSVD), proposed in Section III-B, is obtained by varying the transmit power of each transmitter from zero to q_i , independently of the other one. Then, for a given pair of transmit powers, the achievable secrecy rates in (12) are evaluated numerically. To obtain the achievable secrecy rate region for the cooperative transmission scheme (GSVD+ANA), proposed in Section III-C, in each channel realization, α_1 and α_2 (power fractions allocated to information signal at transmitter 1 and 2, respectively), are varied from 0 to 1 independently of each other.

Fig. 2. Achievable secrecy rate regions of GSVD+ANA, GSVD and NCJ for fixed $N_1 = N_2 = 3$; M_1 and M_2 are equal but take two values, either 4 or 5.

Then, for a given pair of (α_1, α_2) , the achievable secrecy rates in (16) are evaluated numerically¹.

Fig. 2 compares the achievable secrecy rate regions of the proposed schemes for the case where the number of antennas at the receivers is greater than that of the transmitters but are equal to each other i.e., $M_1 = M_2 \geq N_1 = N_2$. The figure shows that for a given $N_1 = N_2 (= 3$ here), as M_i is increased from 4 to 5, the achievable secrecy rate regions are decreased for all three schemes. This decrease is due to the increase in the dimension of the signal space observed by the unintended receiver, which consequently increases the chance of eavesdropping. Both examples plotted in this figure illustrate that the cooperative scheme (GSVD+ANA) allows for communication over larger secrecy rates compared with the non-cooperative schemes GSVD and NCJ. In fact, as we have shown in [11], the achievable secrecy rate region of GSVD+ANA is always bigger than (or at least equal to) that of the GSVD scheme, while NCJ always has the worst performance. Note that in this figure, the achievable secrecy rate region of GSVD+ANA is bigger than that of GSVD and NCJ even with a larger number of antennas at the unintended receivers.

Fig. 3 considers the case where $N_1 = M_1 = 5$ and $N_2 = M_2 = 4$. Note that at least one of the information conveying beamformers of transmitter 1 lies in the nullspace of its eavesdropper's channel ($\mathbf{G}_1$) and of course in $\text{Range}(\mathbf{H}_1)$, but there is no non-trivial nullspace between transmitter 2

¹The secrecy rate regions are generated as the convex hull of all of the obtained rate points, assuming a standard time-sharing argument.

Fig. 3. Achievable secrecy rate regions of GSVD+ANA, GSVD and NCJ for $N_1 = M_1 = 5$ and $N_2 = M_2 = 4$.

and its eavesdropper (receiver 1). This allows user 1 to achieve considerably larger secrecy rates compared with user 2. This is especially true for the non-cooperative schemes GSVD and NCJ, while cooperation between the transmitters in GSVD+ANA scheme is seen to make a notable increase in the secrecy rate of user 2. The other interesting observation in this figure is that a portion of the boundary points of the secrecy rate regions of GSVD+ANA and GSVD almost coincide with each other. This indicates that for these points, the transmitters agree in the cooperative scheme that no artificial noise should be broadcast by transmitter 2. The reason for this is that transmitter 1's signal at receiver 2 spans almost the entire signal space of receiver 2. Thus transmitter 2 has to devote almost all of its transmit power to its information signal ($\alpha_2 \simeq 1$) to overcome the increased equivalent noise at its receiver (receiver 2). From another viewpoint, this figure shows the robustness of the GSVD scheme for cases where there is a non-trivial nullspace between transmitters and their unintended receivers.

5. CONCLUSIONS

In this paper, we have considered the problem of transmitting confidential messages in a MIMO interference channel setting. We proposed different transmission schemes for Gaussian interference channels and derived their achievable secrecy rate regions assuming the transmitters use linear beamforming. We also considered the scenario from a game-theoretic perspective with transmitters as players and secrecy rates as utility functions. Numerical results show the benefit of transmitter cooperation via the GSVD+ANA approach over the non-cooperative methods GSVD and NCJ. More-

over, the results indicate that while ordinary jamming is near optimal for the standard wiretap channel [10], its performance is far from optimal for the interference channel.

6. REFERENCES

- [1] A. Wyner, "The wire-tap channel," *Bell. Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, Jan. 1975.
- [2] Y. Liang and V. H. Poor, "Multiple access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 339-348, Mar. 2008.
- [3] R. Liu, I. Maric, R. D. Yates, P. Spasojevic, "The discrete memoryless multiple access channel with confidential messages," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Seattle, WA, July 2006, pp. 957-961.
- [4] Jin Xu, Yi Cao, and Biao Chen, "Capacity bounds for broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4529-4542, 2009.
- [5] R. Liu, I. Maric, P. Spasojevic and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493-2507, June 2008.
- [6] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai, and S. Verdú, "Capacity of cognitive interference channels with and without confidential messages," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 604-619, 2009.
- [7] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Inf. Theory*, vol. 7, no. 6, pp. 2180-2189, June 2008.
- [8] A. Mukherjee and A. L. Swindlehurst, "Fixed-rate power allocation strategies for enhanced secrecy in MIMO wiretap channels," in *Proc. 10th IEEE SPAWC*, Perugia, Italy, pp. 344-348, June, 2009.
- [9] S. Ali. A. Fakoorian and A. L. Swindlehurst, "Optimal power allocation for the GSVD based MIMO Gaussian wiretap channel," submitted to *IEEE Trans. Inf. Theory* Available: <http://arxiv.org/abs/1006.1890>
- [10] A. Khisti and G. Wornell, "Secure transmission with multiple antennas II: The MIMOME wiretap channel," to appear, *IEEE Trans. Inf. Theory*, 2010. Available: <http://allegro.mit.edu/pubs/posted/journal/2008-khisti-wornell-it.pdf>
- [11] S. A. A. Fakoorian and A. L. Swindlehurst, "MIMO interference channel with confidential messages: achievable secrecy rates and beamforming design," submitted to *IEEE Trans. on Inf. Forensics and Security*, Aug. 2010.