This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2011 proceedings.

Dirty Paper Coding Versus Linear GSVD-Based Precoding in MIMO Broadcast Channel with Confidential Messages

S. Ali. A. Fakoorian and A. Lee Swindlehurst
Electrical Engineering and Computer Science
University of California, Irvine, CA 92697
Email: {afakoori, swindle}@uci.edu

***Abstract*—This paper studies linear beamforming based on the generalized singular value decomposition (GSVD) for the two-receiver multiple-input multiple-output (MIMO) Gaussian broadcast channel with confidential messages. The transmitter has two independent messages, each of which is intended for one of the receivers but needs to be kept as secret as possible from the other. Recently, it has been proved that, under an input power-covariance constraint, the secret dirty paper coding (S-DPC) scheme is optimal, but under the average power constraint, there is not a computable secrecy capacity expression for the general MIMO case. In fact, for this case, the secrecy capacity region must in general be found through an exhaustive search over the set of all possible matrix power constraints. Clearly, this exhaustive search, as well as the complexity of dirty-paper encoding and decoding, motivates us to consider low complexity linear beamforming technique whose performance is close to the optimal S-DPC scheme. In this paper, we propose a GSVD-based beamforming scheme for the general MIMO broadcast channel with confidential messages. Moreover, an optimal power allocation is obtained to maximize the sum-secrecy rates for the GSVD-based beamforming technique, under the average power constraint. Numerical results are presented to illustrate that the secrecy rate region of the linear precoding approach is nearly identical to that of the optimal S-DPC scheme.**

***Index Terms*—MIMO, physical-layer secrecy, broadcast channel, wiretap channel.**

I. Introduction

Due to its broadcast nature, wireless communication is particularly susceptible to eavesdropping, where the transmitted message is decoded by unintended receiver(s). The problem of broadcasting confidential messages in an information-theoretic setting was formulated by Wyner [1]. The so-called wiretap channel model introduced by Wyner in his work is the most basic physical layer model that captures the problem of communication security. In the wiretap channel, the transmitter broadcasts its confidential messages to the legitimate receiver, in the presence of an eavesdropper. This work led to the development of the notion of perfect secrecy capacity, which quantifies the maximum rate at which a transmitter can reliably send a secret message to the receiver, without the eavesdropper being able to decode it.

Prior work has considered the discrete memoryless broadcast channel with two confidential messages sent to two receivers, where each receiver acts as an eavesdropper for the other one. This problem has been addressed in [2], where inner and outer bounds for the secrecy capacity region were established. Further work in [3] studied the multiple-input single-output (MISO) Gaussian case, and [4] considered the general MIMO Gaussian case. It was shown in [4] that, under a matrix input power-covariance constraint, both confidential messages can be simultaneously communicated at their respective maximum secrecy rates, where the achievability is obtained using secret dirty-paper coding (S-DPC). However, under an average power constraint, there is not a computable secrecy capacity expression for the general MIMO case. In fact, for the average power constraint, the secrecy capacity region must in general be found through an exhaustive search over the set of all covariance matrices that satisfy the average power constraint. Clearly, this exhaustive search, as well as the complexity of dirty-paper encoding and decoding, are the main drawbacks of implementing of the optimal S-DPC scheme in achieving the boundary points of the secrecy capacity region. This makes linear precoding techniques (*e.g.,* beamforming) an attractive alternative because of their simplicity.

Note that, while low-complexity linear transmission techniques have been extensively investigated for the broadcast channel (BC) without secrecy constraints, e.g., [7]-[10], there has been relatively little effort on considering the effect of secrecy in the design of linear precoders for the BC case. In this paper, we consider a linear transmission technique for the MIMO Gaussian broadcast channel with confidential messages where the transmitter performs beamforming based on the generalized singular value decomposition (GSVD) [5], [6]. The optimal allocation of power for the GSVD-based precoder that maximizes the sum-secrecy rates, under the average power constraint, is obtained. Numerical results illustrate the close performance, in terms of secrecy rate region, of the proposed linear precoding scheme and the optimal S-DPC scheme.

The remainder of the paper is organized as follows. In Section II, we describe the system model for the MIMO Gaussian broadcast channel with confidential messages and the optimal S-DPC scheme, proposed in [4]. In Sections III, we propose the GSVD-based beamforming scheme for BC and derive the optimal power allocation that maximizes the sum-secrecy rates, under the average power constraint. Numerical

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

978-1-4244-9268-8/11/$26.00 ©2011 IEEE

results in Section IV are presented to illustrate the proposed solution. Finally, Section V concludes the paper.

II. System Model

We consider a two-receiver multiple-antenna Gaussian broadcast channel with confidential messages, where the transmitter, receiver 1 and receiver 2 possess n_t, n_1, and n_2 antennas, respectively. The transmitter has two independent confidential messages, W_1 and W_2, where message W_1 is intended for receiver 1 but needs to be kept secret from receiver 2, and message W_2 is intended for receiver 2 but needs to be kept secret from receiver 1 [4].

The signals at each receiver can be written as:

$$\mathbf{y}_1 = \mathbf{H}_1\mathbf{x} + \mathbf{z}_1 \tag{1}$$

$$\mathbf{y}_2 = \mathbf{H}_2\mathbf{x} + \mathbf{z}_2 \tag{2}$$

where $\mathbf{x}$ is the $n_t \times 1$ transmitted signal vector, and $\mathbf{z}_i \in \mathbb{C}^{n_i \times 1}$ is an additive white Gaussian noise (AWGN) vector at receiver i, $i = 1, 2$, with i.i.d. entries distributed as $\mathcal{CN}(0, 1)$. The channel matrices $\mathbf{H}_i \in \mathbb{C}^{n_i \times n_t}$ are assumed to be unrelated to each other, and known at all three nodes.

The channel input $\mathbf{x}$ is subject to the average total power constraint as

$$\text{Tr}(E\{XX^H\}) \leq P \tag{3}$$

where Tr(.) is the matrix trace, $E\{.\}$ denotes expectation, $(\cdot)^H$ denotes the Hermitian transpose, X is the random variable counterpart to the specific realization $\mathbf{x}$ and P is a scalar. The corresponding information-theoretic secrecy constraints are given by [1], [2], [4]

$$\lim_{n\to\infty} I(W_1; \mathbf{y}_2^n) = 0 \quad \text{and} \quad \lim_{n\to\infty} I(W_2; \mathbf{y}_1^n) = 0$$

where $I(a; b)$ represents mutual information between a and b, and $\mathbf{y}_1^n$ and $\mathbf{y}_2^n$ are the received signals at receiver 1 and 2, respectively, after n channel uses.

It was shown in [2] that for any jointly distributed (V_1, V_2, X) such that $(V_1, V_2) \to X \to (Y_1, Y_2)$ forms a Markov chain and the power constraint over X is satisfied, the secrecy rate pair (R_1, R_2) given by

$$\begin{aligned} R_1 &= I(V_1; Y_1) - I(V_1; V_2, Y_2) \\ R_2 &= I(V_2; Y_2) - I(V_2; V_1, Y_1) \end{aligned} \tag{4}$$

is achievable for the MIMO Gaussian broadcast channel given by (1) and (2). In [2], the achievability of the rate pair (4) was proved using a double-binning scheme. Specifically, the auxiliary variables V_1 and V_2 represent the precoding signals for the confidential messages W_1 and W_2, respectively [4].

Liu *et al.* [4] analyzed the above secret communication problem under a matrix power-covariance constraint, defined as

$$E\{XX^H\} = \mathbf{K}_x \preceq \mathbf{S} \tag{5}$$

where $\mathbf{K}_x$ is the transmitter covariance matrix, $\mathbf{S}$ is a positive semidefinite matrix, and "$\preceq$" denotes "less than or equal to" in the positive semidefinite ordering between Hermitian matrices. They showed that, under the matrix power constraint (5), the secrecy capacity region $\mathcal{C}_s(\mathbf{H}_1, \mathbf{H}_2, \mathbf{S}) = \{R_1, R_2\}$ is rectangular. This interesting result implies that under the matrix power constraint, both confidential messages W_1 and W_2 can be *simultaneously* transmitted at their respective maximal secrecy rates (as if over two separate MIMO Gaussian wiretap channels). To prove this result, Liu *et al.* revisited the MIMO Gaussian wiretap channel and showed that a coding scheme that uses artificial noise and random binning achieves the secrecy capacity of the MIMO Gaussian wiretap channel as well [4, Theorem 2].

Under the matrix power constraint (5), the achievablity of the corner point (R_1^*, R_2^*) given by [4, Theorem 1]

$$R_1^* = \max_{0 \preceq \mathbf{K}_x \preceq \mathbf{S}} \log\left|\mathbf{H}_1\mathbf{K}_x\mathbf{H}_1^H + \mathbf{I}\right| - \log\left|\mathbf{H}_2\mathbf{K}_x\mathbf{H}_2^H + \mathbf{I}\right| \tag{6}$$

$$R_2^* = \log\left|\frac{\mathbf{H}_2\mathbf{S}\mathbf{H}_2^H + \mathbf{I}}{\mathbf{H}_1\mathbf{S}\mathbf{H}_1^H + \mathbf{I}}\right| + R_1^* \tag{7}$$

is obtained using dirty-paper coding based on double binning, or as referred to in [4], secret dirty paper coding (S-DPC). More precisely, let $\mathbf{K}_x$ be a positive semidefinite matrix that maximizes (6) and (7), and let

$$\begin{aligned} V_1 &= U_1 + \mathbf{F}U_2 \\ V_2 &= U_2 \\ X &= U_1 + U_2 \end{aligned} \tag{8}$$

where U_1 and U_2 are two independent Gaussian vectors with zero means and covariance matrices $\mathbf{K}_x$ and $\mathbf{S} - \mathbf{K}_x$, respectively, and where the precoding matrix $\mathbf{F}$ is chosen as

$$\mathbf{F} = \mathbf{K}_x\mathbf{H}_1^H\left(\mathbf{H}_1\mathbf{K}_x\mathbf{H}_1^H + \mathbf{I}\right)^{-1}\mathbf{H}_1. \tag{9}$$

One can easily confirm the achievablity of the corner point (R_1^*, R_2^*) by evaluating (4) for the above random variables and noting that $Y_i = \mathbf{H}_i(U_1 + U_2) + \mathbf{z}_i$, $i = 1, 2$.

The matrix $\mathbf{K}_x$ that maximizes (6) and (7) is given by [4], [11]

$$\mathbf{K}_x = \mathbf{S}^{\frac{1}{2}}\mathbf{C}\begin{bmatrix} (\mathbf{C}_1^H\mathbf{C}_1)^{-1} & 0 \\ 0 & 0 \end{bmatrix}\mathbf{C}^H\mathbf{S}^{\frac{1}{2}} \tag{10}$$

where $\mathbf{C}$ is an invertible generalized eigenvector matrix of the pencil

$$\left(\mathbf{S}^{\frac{1}{2}}\mathbf{H}_1^H\mathbf{H}_1\mathbf{S}^{\frac{1}{2}} + \mathbf{I}, \quad \mathbf{S}^{\frac{1}{2}}\mathbf{H}_2^H\mathbf{H}_2\mathbf{S}^{\frac{1}{2}} + \mathbf{I}\right)$$

such that [12]

$$\begin{aligned} \mathbf{C}^H\left[\mathbf{S}^{\frac{1}{2}}\mathbf{H}_1^H\mathbf{H}_1\mathbf{S}^{\frac{1}{2}} + \mathbf{I}\right]\mathbf{C} &= \mathbf{\Lambda} \\ \mathbf{C}^H\left[\mathbf{S}^{\frac{1}{2}}\mathbf{H}_2^H\mathbf{H}_2\mathbf{S}^{\frac{1}{2}} + \mathbf{I}\right]\mathbf{C} &= \mathbf{I} \end{aligned}$$

where $\mathbf{\Lambda} = \text{diag}\{\lambda_1, ..., \lambda_{n_t}\}$ is a positive definite diagonal matrix and $\lambda_1, ..., \lambda_{n_t}$ represent the generalized eigenvalues. Without loss of generality, we may assume that these generalized eigenvalues are ordered as

$$\lambda_1 \geq ... \geq \lambda_b > 1 \geq \lambda_{b+1} \geq ... \geq \lambda_{n_t} > 0$$

i.e., a total of b $(0 \leq b \leq n_t)$ of them are assumed to be greater than 1. Hence, we can write $\mathbf{\Lambda}$ as

$$\mathbf{\Lambda} = \begin{bmatrix} \mathbf{\Lambda}_1 & 0 \\ 0 & \mathbf{\Lambda}_2 \end{bmatrix}$$

where $\mathbf{\Lambda}_1 = \text{diag}\{\lambda_1, ..., \lambda_b\}$ and $\mathbf{\Lambda}_2 = \text{diag}\{\lambda_{b+1}, ..., \lambda_{n_t}\}$. Also, we can write $\mathbf{C}$ as

$$\mathbf{C} = [\mathbf{C}_1 \mathbf{C}_2]$$

where $\mathbf{C}_1$ is the $n_t \times b$ submatrix representing the generalized eigenvectors corresponding to $\{\lambda_1, ..., \lambda_b\}$ and $\mathbf{C}_2$ is the $n_t \times (n_t - b)$ submatrix representing the generalized eigenvectors corresponding to $\{\lambda_{b+1}, ..., \lambda_{n_t}\}$. Now, by applying (10) in (6) and (7), the corner rate pair (R_1^*, R_2^*) can be calculated as ([4, Teorem 3])

$$\begin{aligned} R_1^* &= \log|\mathbf{\Lambda}_1| \\ R_2^* &= -\log|\mathbf{\Lambda}_2| \end{aligned} \tag{11}$$

It should be noted that, under the average power constraint (3), there is not a computable secrecy capacity expression for the general MIMO case. In fact, for the average power constraint, the secrecy capacity region is found through an exhaustive search over the set $\{\mathbf{S} : \mathbf{S} \succeq 0, \text{Tr}(\mathbf{S}) \leq P\}$. More precisely, the secrecy capacity region under the average power constraint (3), $\mathcal{C}_s(\mathbf{H}_1, \mathbf{H}_2, P) = \{R_1, R_2\}$, can be written as [4], [13, Lemma 1]

$$\mathcal{C}_s(\mathbf{H}_1, \mathbf{H}_2, P) = \bigcup_{\mathbf{S} \succeq 0, \text{Tr}(\mathbf{S}) \leq P} \mathcal{C}_s(\mathbf{H}_1, \mathbf{H}_2, \mathbf{S}) \, . \tag{12}$$

For any given semidefinite $\mathbf{S}$, $\mathcal{C}_s(\mathbf{H}_1, \mathbf{H}_2, \mathbf{S})$ can be computed as given by (11). Then, the secrecy capacity region $\mathcal{C}_s(\mathbf{H}_1, \mathbf{H}_2, P)$ is the convex hull of all of the obtained corner points using (11).

Clearly, this exhaustive search, as well as the complexity of dirty-paper encoding and decoding, are the main drawbacks of implementing the optimal S-DPC scheme in achieving the boundary points of the secrecy capacity region $\mathcal{C}_s(\mathbf{H}_1, \mathbf{H}_2, P)$. This makes linear precoding (beamforming) techniques an attractive alternative because of their simplicity. In the following, we describe an approach using GSVD-based beamforming for the MIMO Gaussian BC with confidential messages.

III. GSVD-Based Beamforming Scheme

The idea of beamforming based on the generalized singular value decomposition (GSVD) for secret communication problems, was first used in [5]. They studied a single source-destination communication link being eavesdropped upon by a wiretapper, and showed that GSVD-based beamforming achieved the secrecy capacity in the high SNR regime. However, the optimal input covariance matrix that achieves the secrecy capacity at high SNR was not fully characterized, especially for the case where there is a non-trivial nullspace for the channel between the transmitter and eavesdropper. In [6], we derived an optimal power allocation that achieves the secrecy capacity of the GSVD-based MIMO Gaussian wiretap channel for any SNR. In this section, we extend our previous work in [6] for a two-receiver MIMO Gaussian BC with confidential messages. To begin, we first define the GSVD transform below.

Definition 1 *(GSVD Transform)*: Given two matrices $\mathbf{H}_1 \in \mathbb{C}^{n_1 \times n_t}$ and $\mathbf{H}_2 \in \mathbb{C}^{n_2 \times n_t}$, $gsvd(\mathbf{H}_1, \mathbf{H}_2)$ returns unitary matrices $\mathbf{\Psi}_1 \in \mathbb{C}^{n_1 \times n_1}$ and $\mathbf{\Psi}_2 \in \mathbb{C}^{n_2 \times n_2}$, non-negative diagonal matrices $\mathbf{B}$ and $\mathbf{D}$, and a matrix $\mathbf{A} \in \mathbb{C}^{n_t \times q}$ with q=min$(n_t, n_1 + n_2)$, such that

$$\mathbf{H}_1 \mathbf{A} = \mathbf{\Psi}_1 \mathbf{B} \tag{13}$$

$$\mathbf{H}_2 \mathbf{A} = \mathbf{\Psi}_2 \mathbf{D} \tag{14}$$

The nonzero elements of $\mathbf{B}$ are in ascending order while the nonzero elements of $\mathbf{D}$ are in descending order. Moreover, $\mathbf{B}^T\mathbf{B} + \mathbf{D}^T\mathbf{D} = \mathbf{I}$. Hence, letting b_i and d_i represent the i^{th} diagonal elements of $\mathbf{B}^T\mathbf{B}$ and $\mathbf{D}^T\mathbf{D}$, respectively, the generalized singular values $\sigma_i = \frac{b_i}{d_i}$, $i = 1...q$, are in ascending order.

Eqs. (13) and (14) show that applying the GSVD transform to $\mathbf{H}_1$ and $\mathbf{H}_2$ simultaneously diagonalizes them. Thus, the GSVD transform creates a set of parallel independent subchannels between the transmitter and the receivers, and it suffices for the transmitter to use independent Gaussian codebooks across these subchannels. As we will show mathematically, it is optimal, from the viewpoint of maximizing the sum-secrecy rate, that the confidential message W_1 for receiver 1 is sent only over those subchannels for which the output at receiver 2 is a degraded version of the output at receiver 1. These subchannels correspond to the condition $b_i > d_i$, or the generalized singular values of $gsvd(\mathbf{H}_1, \mathbf{H}_2)$ that are larger than 1. On the other hand, the confidential message W_2 for receiver 2 should be sent only over those subchannels for which the output at receiver 1 is a degraded version of the output at receiver 2. These subchannels correspond to the condition $d_i > b_i$, or the generalized singular values of $gsvd(\mathbf{H}_1, \mathbf{H}_2)$ that are less than 1.

Recall from the definition of the GSVD transform that the generalized singular values are in ascending order. Assume a total of ρ of them to be greater than 1 and the rest of them $(q - \rho)$ to be less than 1. The transmitted signal vector $\mathbf{x}$ is constructed as

$$\mathbf{x} = \mathbf{A} \begin{bmatrix} \mathbf{v}_2 \\ \mathbf{v}_1 \end{bmatrix}, \quad \begin{bmatrix} V_2 \\ V_1 \end{bmatrix} \sim \mathcal{CN}(\mathbf{0}, \mathbf{P}) \tag{15}$$

where $\mathbf{A}$ is obtained from $gsvd(\mathbf{H}_1, \mathbf{H}_2)$, $V_1 \sim \mathcal{CN}(\mathbf{0}, \mathbf{P}_1)$ and $V_2 \sim \mathcal{CN}(\mathbf{0}, \mathbf{P}_2)$, representing the precoding signals for the confidential messages W_1 and W_2, are two *independent* Gaussian vectors with zero means and diagonal covariance matrices $\mathbf{P}_1$ and $\mathbf{P}_2$, respectively. The vectors $\mathbf{v}_1$ and $\mathbf{v}_2$ are specific realizations of V_1 and V_2, respectively. Hence, each element of the $\rho \times 1$ vector $\mathbf{v}_1$ represents an independently encoded Gaussian codebook symbol corresponding to the confidential message W_1, while each element of the $(q - \rho) \times 1$ vector $\mathbf{v}_2$ represents an independently encoded Gaussian codebook symbol corresponding to the confidential message W_2. $\mathbf{P}$ is a positive semi-definite diagonal matrix

representing the power allocated by the transmitter among its data symbols and can be written as

$$\mathbf{P} = \begin{bmatrix} \mathbf{P}_2 & 0 \\ 0 & \mathbf{P}_1 \end{bmatrix}$$

$\mathbf{P}$ is such that the average power constraint (3) is satisfied, i.e., we have:

$$\text{Tr}(E\{XX^H\}) = \text{Tr}(\mathbf{APA}^H) = \text{Tr}(\mathbf{PA}^H\mathbf{A}) \leq P\ . \quad (16)$$

In the following, we derive an optimal source power allocation which maximizes the sum-secrecy rate for the GSVD-based MIMO Gaussian BC with confidential messages, under the average power constraint (3). Substituting (15) into the channel model (1)-(2) and using (13)-(14) yields

$$\mathbf{y}_1 = \mathbf{\Psi}_1\mathbf{B}\begin{bmatrix} \mathbf{v}_2 \\ \mathbf{v}_1 \end{bmatrix} + \mathbf{z}_1 \quad (17)$$

$$\mathbf{y}_2 = \mathbf{\Psi}_2\mathbf{D}\begin{bmatrix} \mathbf{v}_2 \\ \mathbf{v}_1 \end{bmatrix} + \mathbf{z}_2 \quad (18)$$

Now, by evaluating the mutual information expressions in (4), for the precoding signals V_1 and V_2 above, the following secrecy rate pair is achievable:

$$R_1 = \log\left|\begin{bmatrix} 0 & 0 \\ 0 & \mathbf{P}_1 \end{bmatrix}\mathbf{B}^T\mathbf{B} + \mathbf{I}\right| - \log\left|\begin{bmatrix} 0 & 0 \\ 0 & \mathbf{P}_1 \end{bmatrix}\mathbf{D}^T\mathbf{D} + \mathbf{I}\right| \quad (19)$$

$$R_2 = \log\left|\begin{bmatrix} \mathbf{P}_2 & 0 \\ 0 & 0 \end{bmatrix}\mathbf{D}^T\mathbf{D} + \mathbf{I}\right| - \log\left|\begin{bmatrix} \mathbf{P}_2 & 0 \\ 0 & 0 \end{bmatrix}\mathbf{B}^T\mathbf{B} + \mathbf{I}\right| \quad (20)$$

where we have used the fact that V_1 and V_2 are independent, ($I(V_1;V_2) = 0$), $\mathbf{\Psi}_1$ and $\mathbf{\Psi}_2$ are unitary matrices ($\mathbf{\Psi}_1^H\mathbf{\Psi}_1 = \mathbf{\Psi}_1\mathbf{\Psi}_1^H = \mathbf{I}, \mathbf{\Psi}_2^H\mathbf{\Psi}_2 = \mathbf{\Psi}_2\mathbf{\Psi}_2^H = \mathbf{I}$), and $|\mathbf{EG} + \mathbf{I}| = |\mathbf{GE} + \mathbf{I}|$.

Considering the above equations, the maximum sum-secrecy rate for the GSVD-based beamforming is represented by:

$$\max_{\mathbf{P}\succeq 0, \text{diagonal}} R_1 + R_2\ . \quad (21)$$

In [6], we considered the above problem for the case of $\mathbf{P}_2 = 0$ ($R_2 = 0$), where an optimal power allocation was derived for the MIMO Gaussian wiretap channel as follows:

$$p_i = \begin{cases} 0, & \text{if} \quad b_i < d_i \\ \max(0, \frac{-1+\sqrt{1-4b_id_i+4(b_i-d_i)b_id_i/(\mu a_i)}}{2b_id_i}), & \text{if} \quad b_i > d_i \end{cases} \quad (22)$$

where p_i, b_i, d_i and a_i are the ith diagonal elements of the matrices $\mathbf{P}$, $\mathbf{B}^T\mathbf{B}$, $\mathbf{D}^T\mathbf{D}$ and $\text{diag}(\mathbf{A}^H\mathbf{A})$, respectively.

Following the same footsteps as in the proof of (22) in [6], the optimal $\mathbf{P}$ in the sum-secrecy rate maximization problem (21) is given by

$$p_i^* = \begin{cases} \max(0, \frac{-1+\sqrt{1-4b_id_i+4(d_i-b_i)b_id_i/(\mu a_i)}}{2b_id_i}), & \text{if} \quad b_i < d_i \\ \max(0, \frac{-1+\sqrt{1-4b_id_i+4(b_i-d_i)b_id_i/(\mu a_i)}}{2b_id_i}), & \text{if} \quad b_i > d_i \end{cases} \quad (23)$$

The Lagrange parameter $\mu > 0$ is chosen to satisfy the average power constraint (3), or (16).

Note that, for the optimal $\mathbf{P}$ obtained in (23), the first $(q-\rho)$ diagonal elements characterize $\mathbf{P}_2$, while the last ρ diagonal elements characterize $\mathbf{P}_1$. By replacing the obtained $\mathbf{P}_1$ and $\mathbf{P}_2$ in (20), we obtain a secrecy rate pair for which $R_1 + R_2$ is maximized. However, this corner point is not the only critical point that can be achieved using the above GSVD-based beamforming. Clearly, $\max R_1$ and $\max R_2$ are other critical points which can be obtained by allocating the entire average power P to only one receiver. In this case, the other receiver is just an eavesdropper and the problem is reduced from a BC with confidential messages to a wiretap channel. Hence, e.g., $\max R_1$ is simply obtained using (22). A description similar to this would also apply to $\max R_2$. The secrecy rate region is generated as the convex hull of all of the obtained rate points, as well as $(0, 0)$, assuming a standard time-sharing argument [14].

IV. Numerical Results

In this section, we compare via simulation the achievable secrecy *rate* region of the proposed GSVD-based beamforming with the secrecy *capacity* region obtained by the optimal S-DPC as described in Section II. This comparison is done for randomly generated $\mathbf{H}_1$ and $\mathbf{H}_2$ channel matrices, with i.i.d. entries distributed as $\mathcal{CN}(0, 1)$. The average transmit power P is assumed to be 100.

In the first example we assume $n_t = 2$ and $n_1 = n_2 = 3$. The two randomly generated $\mathbf{H}_1$ and $\mathbf{H}_2$ matrices in this case are:

$$\mathbf{H}_1 = \begin{bmatrix} 0.74 - 0.97i & -0.01 + 0.14i \\ -0.42 + 0.42i & 0.15 - 0.61i \\ -0.43 - 0.97i & 1.04 + 0.39i \end{bmatrix}$$

$$\mathbf{H}_2 = \begin{bmatrix} -0.42 - 0.95i & -0.88 + 1.14i \\ 0.13 + 0.13i & -0.33 + 0.98i \\ -0.34 + 0.55i & 0.46 + 0.79i \end{bmatrix}$$

As Fig. 1 shows, the performance of the proposed optimal GSVD-based beamforming approach is essentially identical to that of the optimal S-DPC, while not requiring an exhaustive search as with S-DPC based on (12).

Fig. 2 gives another example when $n_t = n_1 = n_2 = 3$ and the randomly generated $\mathbf{H}_1$ and $\mathbf{H}_2$ are:

$$\mathbf{H}_1 = \begin{bmatrix} 0.77 - 0.62i & 0.12 + 0.25i & 0.19 + 0.62i \\ -0.80 + 0.26i & -0.28 - 0.19i & -0.41 + 0.97i \\ 0.24 - 1.11i & -0.11 - 0.28i & 0.66 - 0.66i \end{bmatrix}$$

$$\mathbf{H}_2 = \begin{bmatrix} 0.36 - 0.78i & 0.47 - 0.10i & 0.54 - 0.17i \\ -1.27 - 0.84i & 0.01 - 0.01i & 0.67 - 0.41i \\ -0.47 + 0.70i & -0.49 + 1.7i & -0.52 - 0.15i \end{bmatrix}$$

Fig. 3 compares the average (over 1000 channel realizations) sum-secrecy rate of the GSVD-based beamforming and the optimal S-DPC methods, when n_t varies from 2-6 and for different numbers of antennas at the receivers.

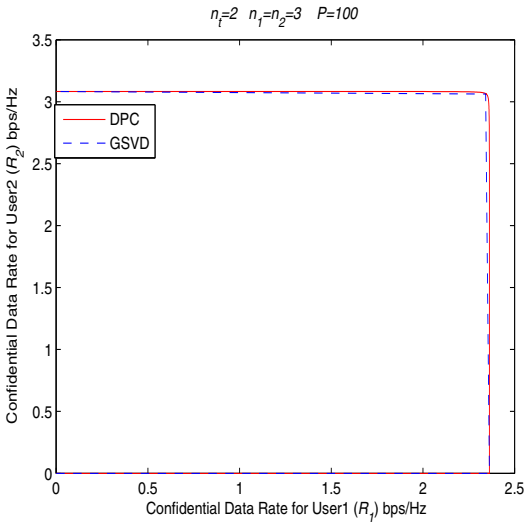

Fig. 1. Comparison of the achievable secrecy rate region of GSVD and the secrecy capacity region of S-DPC for $n_t = 2$, $n_1 = n_2 = 3$ and $P = 100$.

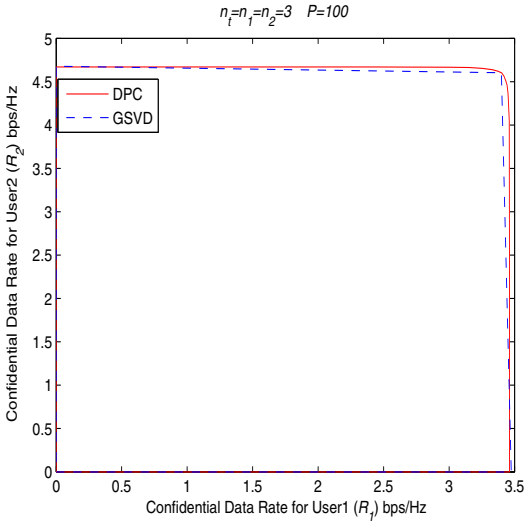

Fig. 2. Comparison of the achievable secrecy rate region of GSVD and the secrecy capacity region of S-DPC for $n_t = n_1 = n_2 = 3$ and $P = 100$.

V. Conclusions

In this paper, we have considered the problem of linear beamforming for a two-receiver MIMO Gaussian broadcast channel with confidential messages. We proposed an optimal power allocation for GSVD-based beamforming that maximized the sum-secrecy rate. Next we considered the achievable secrecy rate region of the GSVD-based beamforming scheme and the secrecy capacity region of the secret dirty paper coding method which is obtained using an exhaustive search. While there are difficulties in implementing dirty paper encoding and decoding, our numerical results show the benefit of the proposed linear precoding scheme in finding the boundary points of the secrecy capacity region.

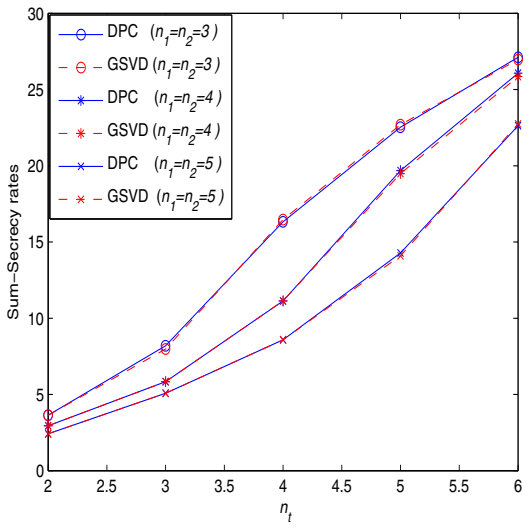

Fig. 3. Comparison of the sum-secrecy rate of GSVD and S-DPC versus n_t, and for different $n_1 = n_2$ values.

References

[1] A. Wyner, "The wire-tap channel," *Bell. Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, Jan. 1975.

[2] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493-2512, June 2008.

[3] R. Liu and H. V. Poor, "Secrecy capacity region of a multiple-antenna Gaussian broadcast channel with confidential messages," *IEEE Trans. Inf. Theory*, vol. 55, no. 3, pp. 1235-1249, Mar. 2009.

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

[5] A. Khisti and G. Wornell, "Secure transmission with multiple antennas II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515-5532, 2010.

[6] 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

[7] Q. H. Spencer, A. L. Swindlehurst, and M. Haardt, "Zero-forcing methods for downlink spatial multiplexing in multiuser MIMO channels," *IEEE Trans. Signal Processing*, vol. 52, no. 2, pp. 461471, Feb. 2004.

[8] T. Yoo and A. Goldsmith, "On the optimality of multi-antenna broadcast scheduling using zero-forcing beamforming," *IEEE J. Select. Areas Commun.*, special issue on 4G wireless systems, vol. 24, no. 3, pp.528541, Mar. 2006.

[9] A. Wiesel, Y. Eldar, and S. Shamai, "Linear precoding via conic optimization for fixed mimo receivers," *IEEE Trans. Signal Processing*, vol. 54, no. 1, pp. 161176, Jan. 2006.

[10] S. S. Christensen, R. Agarwal, E. d. Carvalho, and J. M. Cioffi, "Weighted sum-rate maximization using weighted MMSE for MIMO-BC beamforming design," *IEEE Trans. Wireless Comm.*, vol. 7, no. 12, Dec. 2008

[11] R. Bustin, R. Liu, H. V. Poor, and S. Shamai (Shitz), "A MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, Article ID 370970, 8 pages, 2009.

[12] R. A. Horn and C. R. Johnson, *Matrix Analysis*, University Press, Cambridge, UK, 1985.

[13] H. Weingarten, Y. Steinberg, and S. Shamai (Shitz), "The capacity region of the Gaussian multiple-input multiple-output broadcast channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3936-3964, 2006

[14] E. Larsson and E. Jorswieck, "Competition versus collaboration on the MISO interference channel," *IEEE Journal on selected areas in Communications*, vol. 26, no. 7, pp. 1059-1069, Sep. 2008.