MIMO Gaussian Wiretap Channels with Two Transmit Antennas: Optimal Precoding and Power Allocation

Mojtaba Vaezi*, Wonjae Shin†, H. Vincent Poor*, and Jungwoo Lee†
*Department of Electrical Engineering, Princeton University
†Department of Electrical and Computer Engineering, Seoul National University
Email: {mvaezi, poor}@princeton.edu {wonjae.shin, junglee}@snu.ac.kr

***Abstract*—A Gaussian multiple-input multiple-output *wiretap* channel in which the eavesdropper and legitimate receiver are equipped with arbitrary numbers of antennas and the transmitter has two antennas is studied in this paper. It is shown that the secrecy capacity of this channel can be achieved by *linear precoding*. The optimal precoding and power allocation schemes achieving the secrecy capacity are developed subsequently, and the secrecy capacity is compared with the *generalized singular value decomposition* (GSVD)-based precoding, which is the best previously proposed precoding for this problem. Numerical results show that substantial gain can be obtained in secrecy rate between the proposed and GSVD-based precodings.**

I. Introduction

Wireless security has been an important concern for many years. As a means of augmenting wireless security, *physical layer security* has attracted significant attention recently. Physical layer security is based on the information theoretic secrecy that can be provided by physical communication channels, an idea that was first proposed by Wyner [1] in the context of the *wiretap* channel. In this channel, a transmitter (Alice) wishes to transmit information to a *legitimate* receiver (Bob) while keeping the information secure from an *eavesdropper* (Eve). Wyner demonstrates that it is possible to have both *reliable* and *secure* communication between Alice and Bob in the presence of Eve under certain circumstances.

With the rapid advancement of multi-antenna techniques, security enhancement in multiple-input multiple-output (MIMO) wiretap channels has drawn significant attention. A big step toward understanding MIMO wiretap channels was taken in [2]–[4] where a closed-form expression for the capacity of this channel was established. This expression is not, however, computable because the input covariance matrix that maximizes it is unknown in general. In fact, under an average power constraint, there is no computable capacity expression and achieving the secrecy capacity would require an exhaustive search over the set of all input covariance matrices that satisfy this constraint. The complexity associated with such a search makes such an approach prohibitive and motivates the study of simpler techniques for secure communication, e.g., based on linear precoding.

Precoding is a technique for exploiting transmit diversity via weighting the information stream. *Singular value decomposition* (SVD) precoding with *water-filling* power allocation is a well-known example that achieves the capacity of the MIMO channel. Khisti and Wornell [2] proposed a generalized SVD (GSVD)-based precoding scheme, with equal power allocation, for the MIMO Gaussian wiretap channel. The optimal power allocation for GSVD precoding in the MIMO Gaussian wiretap channel was obtained in [5]. GSVD precoding gets close to the capacity in certain antenna configurations but it is not capacity-achieving in general.

Despite its importance and years of research, optimal transmit strategies to maximize the secure rate in MIMO wiretap channels remain unknown in general. Linear beamforming transmission has been proved to be optimal for the special case of $(n_t, n_r, n_e) = (2, 2, 1)$ in [6]. It is also known to be the optimal strategy for multiple-input single-output (MISO) wiretap channels [7], [8]. When all nodes have multiple antennas, capacity-achieving coding would require an exhaustive search over all input covariance matrices. Recently, a closed-form solution for the optimal covariance matrix has been found when the channel is strictly degraded [9], [10]. The combination of this result and the unit-rank solution of [7] can give the optimal covariance matrix for the case of two transmit antennas. The optimal solution is, however, still open in general.

In this paper, we characterize optimal precoding and power allocation for MIMO Gaussian wiretap channels in which the legitimate receiver and eavesdropper have arbitrary numbers of antennas but the transmitter has two antennas. A consequence of this results is to prove that linear beamforming transmission is optimal for a much broader class of MIMO Gaussian wiretap channels. Our approach in finding the optimal covariance matrix is completely different from that of [9] and [10]. It does not require the degradedness condition and thus provides the optimal solution for both full-rank and rank-deficient cases in one shot. The proposed beamforming and power allocation schemes result in a computable capacity with a reasonably low complexity, rather than a prohibitively complex exhaustive search. Also, as numerical results confirm, it can bring notably high gain over GSVD-based beamforming.

The paper is organized as follows. In Section II, we describe the system model. In Section III, we reformulate the secrecy rate problem and propose linear precoding and power allocation schemes to achieve the secrecy capacity of the MIMO wiretap channels of interest. We present numerical results in Section IV and conclude the paper in Section V.

Throughout this work, $\mathrm{tr}(\cdot)$, $(\cdot)^t$, and $(\cdot)^H$ denote the trace, transpose, and conjugate transpose of a matrix, respectively. $\mathbf{A} \succeq \mathbf{0}$ means that $\mathbf{A}$ is a positive semidefinite matrix, and $\mathbf{I}_m$ represents the identity matrix of size m.

This work was supported in part by the U. S. National Science Foundation under Grant CMMI-1435778, and in part by a Canadian NSERC fellowship.

978-1-5090-4096-4/17/$31.00 ©2017 IEEE

II. System Model and Preliminaries

Consider a MIMO Gaussian wiretap channel with n_t, n_r, and n_e antennas, respectively, at the transmitter, legitimate receiver, and eavesdropper. Let $\mathbf{H} \in \mathbb{R}^{n_r \times n_t}$ and $\mathbf{G} \in \mathbb{R}^{n_e \times n_t}$ be the real channel matrices associated with the legitimate user and eavesdropper, respectively, and assume that the channels are fixed during the transmission and are known to all terminals. The received signal at the legitimate receiver and eavesdropper are, respectively, given by

$$\mathbf{y}_r = \mathbf{H}\,\mathbf{x} + \mathbf{w}_r, \tag{1a}$$

$$\mathbf{y}_e = \mathbf{G}\,\mathbf{x} + \mathbf{w}_e, \tag{1b}$$

in which $\mathbf{x} \in \mathbb{R}^{n_t \times 1}$ is the transmitted signal and $\mathbf{w}_i \in \mathbb{R}^{n_i \times 1}$, $i \in \{r, e\}$, is an independent and identically distributed (i.i.d.) Gaussian noise vector with zero mean and identity covariance matrix. The transmitted signal is subject to an average power constraint

$$\mathrm{tr}(\mathbb{E}\{\mathbf{x}\mathbf{x}^t\}) = \mathrm{tr}(\mathbf{Q}) \le P, \tag{2}$$

where P is a scalar, and $\mathbf{Q} = \mathbb{E}\{\mathbf{x}\mathbf{x}^t\}$ is the input covariance matrix.

Khisti and Wornell [2] and Oggier and Hassibi [3] independently proved the secrecy capacity of this channel. The secrecy capacity (bits per real dimension) is the solution of [4]

$$\begin{aligned} \max_{\mathbf{Q}} \quad & \frac{1}{2}\left[\log\det(\mathbf{I}_{n_r} + \mathbf{H}\mathbf{Q}\mathbf{H}^t) - \log\det(\mathbf{I}_{n_e} + \mathbf{G}\mathbf{Q}\mathbf{G}^t)\right] \\ \text{s.t.} \quad & \mathbf{Q} \succeq \mathbf{0}, \mathbf{Q} = \mathbf{Q}^t,\ \mathrm{tr}(\mathbf{Q}) \le P, \end{aligned} \tag{3}$$

in which the first two constraints are due to the fact that $\mathbf{Q}$ is a covariance matrix and the third constraint is due to (2). The secrecy capacity is obviously nonnegative as $\mathbf{Q} = \mathbf{0}$ is a feasible solution of (3).

The above optimization problem is non-convex in general and its objective function possesses numerous local maxima. Thus, the optimum $\mathbf{Q}$ is not known, in general. There has been an active investigation into characterizing the optimal input covariance matrix. Until recently, the special cases for which the optimal $\mathbf{Q}$ was known were limited to the cases of $n_r = 1$ [7] and $n_t = 2$, $n_r = 2$, $n_e = 1$ [6]. More recently, major steps have been made in characterizing the optimal covariance matrix. Fakoorian and Swindlehurst [9] determined conditions under which the optimal input covariance matrix is full-rank or rank-deficient. They also proposed an approach for obtaining such a full-rank $\mathbf{Q}$. Very recently, Loyka and Charalambous [10] found a closed-form solution for the optimal covariance matrix when the channel is strictly degraded. Combined with the unit-rank solution of [7], this gives the optimal $\mathbf{Q}$ for the case of two transmit antennas. However, the optimal solution is yet open in general.

We consider MIMO wiretap channels where n_r and n_e are arbitrary integers while $n_t = 2$, and we show that the secrecy capacity can be achieved by linear precoding. To this end, we find a closed-form solution for the optimal covariance matrix. Our approach is completely different from that of [9] and [10]. It does not impose any conditions on the channel matrices, and explicitly finds optimal precoding and power allocation schemes. This, in turn, provides the optimal covariance matrix for both full-rank and unit-rank cases.

III. A Capacity Achieving Precoding

The secrecy capacity of the MIMO Gaussian wiretap channel can be rewritten as

$$C_s = \max_{\mathbf{Q}} \frac{1}{2}\log\frac{\det(\mathbf{I}_{n_t} + \mathbf{H}^t\mathbf{H}\mathbf{Q})}{\det(\mathbf{I}_{n_t} + \mathbf{G}^t\mathbf{G}\mathbf{Q})}, \tag{4}$$

where $\mathbf{Q} \succeq \mathbf{0}, \mathbf{Q} = \mathbf{Q}^t, \mathrm{tr}(\mathbf{Q}) \le P$. This is obtained from (3) knowing that for any $\mathbf{A} \in \mathbb{C}^{m\times n}$ and $\mathbf{B} \in \mathbb{C}^{n\times m}$ we have

$$\det(\mathbf{I}_m + \mathbf{A}\mathbf{B}) = \det(\mathbf{I}_n + \mathbf{B}\mathbf{A}). \tag{5}$$

Note that $\mathbf{H}^t\mathbf{H}$ and $\mathbf{G}^t\mathbf{G}$ are $n_t \times n_t$ symmetric matrices. Also, $\mathbf{Q}$ is an $n_t \times n_t$ symmetric matrix and its *eigendecomposition* can be written as

$$\mathbf{Q} = \mathbf{V}\mathbf{\Lambda}\mathbf{V}^t, \tag{6}$$

where $\mathbf{V} \in \mathbb{R}^{n_t \times n_t}$ is the *orthogonal matrix* whose ith column is the ith *eigenvector* of $\mathbf{Q}$ and $\mathbf{\Lambda}$ is the diagonal matrix whose diagonal elements are the corresponding eigenvalues, i.e., $\mathbf{\Lambda}_{ii} = \lambda_i$.

A. Reformulating the Problem for $n_t = 2$

We simplify the optimization problem (4) for $n_t = 2$ in this subsection. Since $\mathbf{V}$ is orthogonal its columns are orthonormal and, without loss of generality, we can write

$$\mathbf{V} = \begin{bmatrix} -\sin\theta & \cos\theta \\ \cos\theta & \sin\theta \end{bmatrix}, \tag{7}$$

for some θ. Further, let

$$\mathbf{H}^t\mathbf{H} = \begin{bmatrix} h_1 & h_2 \\ h_2 & h_3 \end{bmatrix}, \quad \mathbf{G}^t\mathbf{G} = \begin{bmatrix} g_1 & g_2 \\ g_2 & g_3 \end{bmatrix}. \tag{8}$$

The following lemma converts the optimization problem (4) into a more tractable problem.

Lemma 1. *For $n_t = 2$ but arbitrary n_r and n_e, the optimization problem in* (4) *is equivalent to*

$$C_s = \max_{\lambda_1+\lambda_2 \le P} \frac{1}{2}\log\left(\frac{a_1\sin 2\theta + b_1\cos 2\theta + c_1}{a_2\sin 2\theta + b_2\cos 2\theta + c_2}\right), \tag{9}$$

in which λ_1 and λ_2 are nonnegative, and

$$a_1 = (\lambda_2 - \lambda_1)h_2, \tag{10a}$$

$$b_1 = \frac{1}{2}(\lambda_1 - \lambda_2)(h_3 - h_1), \tag{10b}$$

$$c_1 = 1 + \frac{1}{2}(\lambda_1 + \lambda_2)(h_1 + h_3) + \lambda_1\lambda_2(h_1h_3 - h_2^2), \tag{10c}$$

$$a_2 = (\lambda_2 - \lambda_1)g_2, \tag{10d}$$

$$b_2 = \frac{1}{2}(\lambda_1 - \lambda_2)(g_3 - g_1), \tag{10e}$$

$$c_2 = 1 + \frac{1}{2}(\lambda_1 + \lambda_2)(g_1 + g_3) + \lambda_1\lambda_2(g_1g_3 - g_2^2). \tag{10f}$$

Proof. To prove this lemma, we simplify the determinants in (4). First, consider $\det(\mathbf{I}_{n_t} + \mathbf{H}^t\mathbf{H}\mathbf{Q})$. Using $\mathbf{Q}$ given in (6)

and applying (5), it is seen that $\det(\mathbf{I}_{n_t}+\mathbf{H}^t\mathbf{H}\mathbf{Q}) = \det(\mathbf{I}_{n_t}+\mathbf{V}^t\mathbf{H}^t\mathbf{H}\mathbf{V}\mathbf{\Lambda})$. Further, it is straightforward to check that

$$\mathbf{V}^t\mathbf{H}^t\mathbf{H}\mathbf{V} = \begin{bmatrix} w_1 & w_2 \\ w_2 & w_3 \end{bmatrix}, \tag{11}$$

in which

$$w_1 = h_1 \sin^2\theta + h_3\cos^2\theta - 2h_2\sin\theta\cos\theta, \tag{12a}$$
$$w_2 = h_2(\cos^2\theta - \sin^2\theta) + (h_3 - h_1)\sin\theta\cos\theta, \tag{12b}$$
$$w_3 = h_1\cos^2\theta + h_3\sin^2\theta + 2h_2\sin\theta\cos\theta. \tag{12c}$$

Consequently,

$$\begin{aligned}\det(\mathbf{I}_{n_t} + \mathbf{H}^t\mathbf{H}\mathbf{Q}) &= \det(\mathbf{I}_{n_t} + \mathbf{V}^t\mathbf{H}^t\mathbf{H}\mathbf{V}\mathbf{\Lambda}) \\ &= (1+\lambda_1 w_1)(1+\lambda_2 w_3) - \lambda_1\lambda_2 w_2^2.\end{aligned} \tag{13}$$

Next, using the trigonometric identities $\cos 2\theta = 2\cos^2\theta - 1 = 1 - 2\sin^2\theta$ and $\sin 2\theta = 2\sin\theta\cos\theta$ it is straightforward to show that

$$w_1 = \frac{h_1+h_3}{2} + \frac{h_3-h_1}{2}\cos 2\theta - h_2\sin 2\theta, \tag{14a}$$
$$w_2 = h_2\cos 2\theta + \frac{h_3-h_1}{2}\sin 2\theta, \tag{14b}$$
$$w_3 = \frac{h_1+h_3}{2} - \frac{h_3-h_1}{2}\cos 2\theta + h_2\sin 2\theta. \tag{14c}$$

Substituting (14a)-(14c) in (13), we obtain

$$\det(\mathbf{I}_{n_t} + \mathbf{H}^t\mathbf{H}\mathbf{Q}) = a_1\sin 2\theta + b_1\cos 2\theta + c_1, \tag{15}$$

in which a_1, b_1, and c_1 are given in (10a)-(10c). Following similar steps it is clear that

$$\det(\mathbf{I}_{n_t} + \mathbf{G}^t\mathbf{G}\mathbf{Q}) = a_2\sin 2\theta + b_2\cos 2\theta + c_2, \tag{16}$$

where a_2, b_2, and c_2 are given in (10d)-(10f). It should be mentioned that the constraint $\lambda_1+\lambda_2 \le P$ comes from $\mathrm{tr}(\mathbf{Q}) \le P$ since, from (6), $\mathrm{tr}(\mathbf{Q}) = \mathrm{tr}(\mathbf{V}\mathbf{\Lambda}\mathbf{V}^t) = \mathrm{tr}(\mathbf{V}^t\mathbf{V}\mathbf{\Lambda}) = \mathrm{tr}(\mathbf{\Lambda})$. Note that $\mathrm{tr}(\mathbf{A}\mathbf{B}) = \mathrm{tr}(\mathbf{B}\mathbf{A})$ and $\mathbf{V}^t\mathbf{V} = \mathbf{I}_{n_t}$. Also, $\lambda_1 \ge 0$ and $\lambda_2 \ge 0$ are due to $\mathbf{Q} \succeq \mathbf{0}$. This completes the proof of Lemma 1. □

Lemma 2. *In the optimization problem given by Lemma 1, the constraint $\lambda_1+\lambda_2 \le P$ can be replaced either by $\lambda_1+\lambda_2 = P$ or $\lambda_1+\lambda_2 = 0$; i.e., it is optimal to use either all available power or nothing.*

Proof. The proof is omitted due to space limitations [12]. □

B. Optimal Precoding

In what follows, we first find a closed-form solution for the optimization problem in Lemma 1 for a given pair of λ_1 and λ_2 that satisfy the constraints. Since $\log(x)$ is strictly increasing in x, we can instead maximize the argument of the logarithm in (9). Thus, let us define

$$W = \frac{a_1\sin 2\theta + b_1\cos 2\theta + c_1}{a_2\sin 2\theta + b_2\cos 2\theta + c_2}. \tag{17}$$

Then, $\theta^* = \arg\max W$ and is obtained by differentiating W with respect to θ and finding its critical points. It can be checked that $\frac{\partial W}{\partial\theta} = 0$ is equivalent to

$$a\sin 2\theta + b\cos 2\theta + c = 0, \tag{18}$$

in which $a = c_1b_2 - c_2b_1$, $b = a_1c_2 - a_2c_1$, and $c = a_1b_2 - a_2b_1$. Before proceeding, we note that W is periodic in θ and its period is π. Also, it can be checked that if both a and b are zero, then $\frac{a_1}{a_2} = \frac{b_1}{b_2} = \frac{c_1}{c_2}$ and W is constant; i.e., any θ is optimal. Thus, we assume $a^2+b^2 \neq 0$. Defining $\frac{b}{a} = \tan\phi$, (18) can be further simplified as

$$\sin(2\theta+\phi) + \frac{c}{\sqrt{a^2+b^2}} = 0. \tag{19}$$

The critical points of the above equation are given by

$$2\theta = \begin{cases} -\arctan\frac{b}{a} - \arcsin\frac{c}{\sqrt{a^2+b^2}} + 2k\pi \\ -\arctan\frac{b}{a} + \pi + \arcsin\frac{c}{\sqrt{a^2+b^2}} + 2k\pi \end{cases}, \tag{20}$$

where k is an integer.[1] Then, using the second derivative of W with respect to θ, it is straightforward to check that the first argument gives the minimum of W while the second one gives its maximum. Further, without loss of optimality, we let $k = 0$ in (20). Hence, the optimal θ that maximizes W is obtained by

$$\theta^* = -\frac{1}{2}\arctan\frac{b}{a} + \frac{1}{2}\arcsin\frac{c}{\sqrt{a^2+b^2}} + \frac{\pi}{2}. \tag{21}$$

Thus far, the optimal θ is obtained for given λ_1 and λ_2. To find the optimal λ_1 and λ_2, in light of Lemma 2, we can search over all $\lambda_1 \ge 0$ and $\lambda_2 \ge 0$ that satisfy $\lambda_1+\lambda_2 = P$ or $\lambda_1+\lambda_2 = 0$ and maximize (17) where θ is given in (21). We can vary λ_1 from 0 to P. Hence, we can have the following.

Theorem 1. *To achieve the secrecy capacity of the MIMO Gaussian wiretap channel (with $n_t = 2$) under the average power constraint P, it suffices to use*

$$\mathbf{V} = \begin{bmatrix} -\sin\theta & \cos\theta \\ \cos\theta & \sin\theta \end{bmatrix}, \tag{22}$$

as the transmit beamformer with the power allocation matrix $\mathbf{\Lambda} = \mathrm{diag}(\lambda_1, \lambda_2)$. An optimal θ is given by (21) *and is obtained by searching over nonnegative λ_1 and λ_2 that satisfy $\lambda_1+\lambda_2 = P$ or $\lambda_1+\lambda_2 = 0$ and maximize* (17)*.*

Once the optimal $\mathbf{V}$, λ_1, and λ_2 are determined, these can be used for precoding and power allocation as illustrated in Fig 1, very similar to the V-BLAST architecture for communicating over the MIMO channel [11]. Here, two ($n_t = 2$) independent data streams are multiplexed in the coordinate system given by the precoding matrix $\mathbf{V}$. The ith data stream is allocated a power λ_i. Each stream is encoded using a capacity-achieving Gaussian code. The data streams are decoded jointly. When the orthogonal matrix $\mathbf{V}$ and powers λ_i are chosen as described in Theorem 1, then we have the capacity-achieving architecture in Fig 1.

Lemma 3. *With a proper choice of θ, the pairs (λ_1, λ_2) and (λ_2, λ_1) result in the same maximum rate in Lemma 1.*

Proof. Suppose (λ_1, λ_2) maximizes (17) for some θ^* given by (21). Then, from (10) it is easy to check that (λ_2, λ_1) results in the same W for $\theta = \theta^* + \pi/2$. Therefore, (λ_2, λ_1) can achieve the same rate as (λ_1, λ_2) does. □

[1] It should be highlighted that we always have $|c| \le \sqrt{a^2+b^2}$, as otherwise W would be strictly increasing or strictly decreasing in θ, which is impossible because W is periodic and continuous.

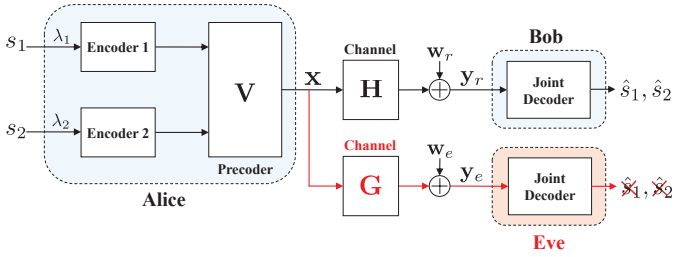


Fig. 1. Optimal architecture for communicating over the MIMO wiretap channel with $n_t = 2$ and arbitrary n_r and n_e.

C. Closed-Form Solution for Optimal Power Allocation

Finding optimal λ_1 and λ_2 in Theorem 1 requires exhaustive search. Although checking a reasonably small number of (λ_1, λ_2) is enough in practice,[2] in this subsection we find a closed-form solution for optimal (λ_1, λ_2).

We know that if $W \leq 1$ then $(\lambda_1^*, \lambda_2^*) = (0, 0)$ is the optimal solution. Thus, let us assume $W > 1$. Then, using Lemma 2, this implies that $\lambda_1 + \lambda_2 = P$ is optimal. Thus, to find optimal λ_1 and λ_2, we can solve the following problem:

$$\mathcal{C}_{\text{MIMOME}} = \max_{\lambda_1+\lambda_2=P} \frac{1}{2} \log(W), \tag{23}$$

where $W = \det(\mathbf{I}_{n_t} + \mathbf{H}^t\mathbf{H}\mathbf{Q})/\det(\mathbf{I}_{n_t} + \mathbf{G}^t\mathbf{G}\mathbf{Q})$ is given in (4). To this end, we define $a_h \triangleq \frac{h_3 - h_1}{2}$, $b_h \triangleq -h_2$, $c_h \triangleq \frac{h_1+h_3}{2}$, $d_h \triangleq \sqrt{a_h^2 + b_h^2}$, and $\frac{b_h}{a_h} \triangleq \tan\phi_h$. Then, from (14a)-(14c) we will have

$$w_1 = c_h + d_h \cos(2\theta - \phi_h), \tag{24a}$$
$$w_2 = d_h \sin(2\theta - \phi_h), \tag{24b}$$
$$w_3 = c_h - d_h \cos(2\theta - \phi_h). \tag{24c}$$

Now, we can write

$$\begin{aligned} W_h &= \det(\mathbf{I}_{n_t} + \mathbf{H}^t\mathbf{H}\mathbf{Q}) \\ &\overset{(a)}{=} (1 + \lambda_1 w_1)(1 + \lambda_2 w_3) - \lambda_1\lambda_2 w_2^2 \\ &\overset{(b)}{=} 1 + \lambda_1 w_1 + \lambda_2 w_3 + \lambda_1\lambda_2(h_1h_3 - h_2^2) \\ &\overset{(c)}{=} 1 + (\lambda_1+\lambda_2)c_h + (\lambda_1-\lambda_2)d_h\cos(2\theta - \phi_h) \\ &\quad + \lambda_1\lambda_2(h_1h_3 - h_2^2), \\ &\overset{(d)}{=} 1 + Pc_h + (2\lambda_1 - P)d_h\cos(2\theta - \phi_h) \\ &\quad + \lambda_1(P - \lambda_1)(h_1h_3 - h_2^2) \\ &\overset{(e)}{=} \alpha_h + \beta_h\lambda_1 - \delta_h\lambda_1^2, \end{aligned} \tag{25}$$

in which (a) is due to (13), (b) can be verified using (14a)-(14c), (c) is due to (24a) and (24c), (d) is due to the fact that $\lambda_1 + \lambda_2 = P$ is optimal when $W > 1$, which follows from Lemma 2, and (e) is obtained by defining

$$\alpha_h = 1 + Pc_h - Pd_h\cos(2\theta - \phi_h), \tag{26a}$$
$$\beta_h = 2d_h\cos(2\theta - \phi_h) + P\delta_h, \tag{26b}$$
$$\delta_h = h_1h_3 - h_2^2. \tag{26c}$$

[2]This is discussed in Section IV.

In a similar way, we can show that

$$W_g = \det(\mathbf{I}_{n_t} + \mathbf{G}^t\mathbf{G}\mathbf{Q}) = \alpha_g + \beta_g\lambda_1 - \delta_g\lambda_1^2, \tag{27}$$

where

$$\alpha_g = 1 + Pc_g - Pd_g\cos(2\theta - \phi_g), \tag{28a}$$
$$\beta_g = 2d_g\cos(2\theta - \phi_g) + P\delta_g, \tag{28b}$$
$$\delta_g = g_1g_3 - g_2^2, \tag{28c}$$

and c_g, d_g, and ϕ_g are defined for $\mathbf{G}$ similar to those of $\mathbf{H}$. Then, $W = W_h/W_g$ and it can be checked that

$$\frac{\partial W}{\partial \lambda_1} = \frac{\bar{c} + \bar{b}\lambda_1 + \bar{a}\lambda_1^2}{(\alpha_g + \beta_g\lambda_1 - \delta_g\lambda_1^2)^2}, \tag{29}$$

in which $\bar{a} = \delta_g\beta_h - \delta_h\beta_g, \bar{b} = 2\delta_g\alpha_h - 2\delta_h\alpha_g$, and $\bar{c} = \beta_h\alpha_g - \beta_g\alpha_h$. Let $\Delta = \bar{b}^2 - 4\bar{a}\bar{c}$, and suppose that $\Delta > 0$.[3] Then

$$\lambda_{1,1}^* = (-\bar{b} + \sqrt{\Delta})/2\bar{a}, \tag{30a}$$
$$\lambda_{1,2}^* = (-\bar{b} - \sqrt{\Delta})/2\bar{a}, \tag{30b}$$

are the roots of (29). Next, it is easy to show that, for $\lambda_{1,i}^*$, $i \in \{1, 2\}$, in (30a) and (30b) we have

$$\frac{\partial^2 W}{\partial \lambda_1^2}(\lambda_{1,i}^*) = \frac{\bar{b} + 2\bar{a}\lambda_{1,i}^*}{(\alpha_g + \beta_g\lambda_1 - \delta_g\lambda_1^2)^2} = \begin{cases} +\frac{\sqrt{\Delta}}{W_g^2}, & i = 1 \\ -\frac{\sqrt{\Delta}}{W_g^2}, & i = 2 \end{cases}.$$

That is, the second derivative is positive at $\lambda_{1,1}^*$ and negative at $\lambda_{1,2}^*$. Thus, the former corresponds to a minimum of W and the latter corresponds to a maximum of that quantity. Therefore, the following cases appear:

1) Case I ($\Delta \leq 0$): This case results in a strictly decreasing or increasing W in λ_1. Then, $\lambda_1 = 0$ or $\lambda_1 = P$ is optimal, depending on the sign of a. The optimum value of λ_1 can be inserted into (10) to find the optimal θ in (21). The optimal λ_2 is obtained from $\lambda_1 + \lambda_2 = P$.

2) Case II ($\Delta > 0$): In this case, the maximum of W is achieved by $\lambda_1 = 0$, $\lambda_1 = P$, or $\lambda_1 = \lambda_{1,2}^*$, provided that $0 \leq \lambda_{1,2}^* \leq P$. The optimal λ_2 is obtained from $\lambda_1 + \lambda_2 = P$. Hence, when $W > 1$, $(\lambda_1^*, \lambda_2^*)$ is one of the following pairs: $(0, P)$, $(P, 0)$, or $(\lambda_{1,2}^*, P - \lambda_{1,2}^*)$. But, in light of Lemma 3, it can be seen that $(0, P)$ and $(P, 0)$ result in the same optimum W and thus one of them can be omitted.

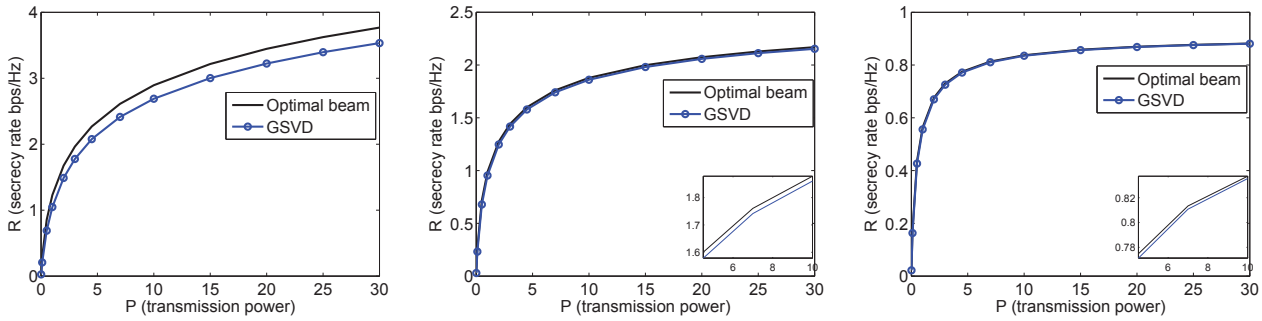
To summarize, considering all cases for $W \leq 1$ and $W > 1$, it is enough to check

$$(\lambda_1^*, \lambda_2^*) = (0, 0), \tag{31a}$$
$$(\lambda_1^*, \lambda_2^*) = (0, P), \tag{31b}$$
$$(\lambda_1^*, \lambda_2^*) = (\lambda_{1,2}^*, P - \lambda_{1,2}^*), \tag{31c}$$

in order to obtain the maximum of W. We should highlight that (31c) will be a choice only if $\lambda_{1,2}^*$, defined in (30b), is a real number between 0 and P. As a result, we have

Theorem 2. *The optimal λ_1 and λ_2 in Theorem 1 is confined to one of the cases in* (31)*, and θ is given in* (21)*.*

[3] When $\Delta \leq 0$, W is strictly decreasing or increasing in λ_1, and $\lambda_1 = 0$ or $\lambda_1 = P$ are the only critical points.



(a) $n_e = 1$ (b) $n_e = 2$ (c) $n_e = 4$

Fig. 2. Comparison of the secrecy capacity of the MIMO Gaussian wiretap channel (achieved by the proposed beamforming method) and the secrecy rate of GSVD-based beamforming for $n_t = 2$, $n_r = 4$, and (a) $n_e = 1$ (b) $n_e = 2$ (c) $n_e = 4$.

Remark 1. As can be traced from (30b), in general, the optimal λ_1 is a function of θ. On the other hand, the optimal θ, given in (21), is a function of λ_1 (and λ_2). Thus, the triplet $(\lambda_1, \lambda_2, \theta)$ can be found for any possible maximizing argument in (31). Then, by evaluating W for these points we can determine the optimal (capacity-achieving) solution. For the first two cases in (31) the solution is obtained analytically. However, the equation resulting from combining the third case in (31) and (21) is rather cumbersome and thus we solve it numerically.

IV. Numerical Results

In this section, we provide numerical examples to illustrate the secrecy capacity of Gaussian multi-antenna wiretap channels using the proposed beamforming method. We also compare our results with those of GSVD-based beamforming with optimal power allocation [5]. As proved in Section III, the proposed beamforming method is optimal and achieves the capacity. Numerical results are included here to show how much gain this optimal method brings when compared with the existing beamforming and power allocation methods.

All simulation results are for 1000 independent realizations of the channel matrices $\mathbf{H}$ and $\mathbf{G}$. The entries of these matrices are generated as i.i.d. $\mathcal{N}(0, 1)$. To get the capacity, based on the optimal beamforming scheme proposed in Theorem 1, we have searched over 50 linearly spaced values of λ_1 and λ_2. We have also used the optimal power allocation of Theorem 2. The difference between the two methods is negligible (on the order of 10^{-4}) and one curve represents both of them. We first consider the case with $n_t = 2$, $n_r = 4$, and $n_e = 1$. As can be seen from Fig. 2(a), when the eavesdropper has a single antenna the proposed capacity-achieving beamforming performs significantly better than GSVD-based beamforming. By increasing the eavesdropper's number of antennas in Fig. 2(b) and Fig. 2(c), the secrecy capacity decreases and the rate achieved by GSVD beamforming becomes very close to that of the optimal method. However, there is still a small gap between the two methods particularly when P is small. This is magnified in Fig. 2(b) and Fig. 2(c).

Figures 2(a)-2(c) also demonstrate the effect of increasing the number of antennas at the eavesdropper. As expected and can be seen from these figures, for a fixed n_t and n_r, the extent to which information can be secured over the air reduces as n_e increases. Further simulations indicate that no information can be secured via physical layer techniques for $n_e \geq 16$. This is because the eavesdropper can no longer be degraded by beamforming in this situation.

V. Conclusion

We have developed a linear precoding scheme to achieve the capacity of Gaussian multi-antenna wiretap channels in which the legitimate receiver and eavesdropper have arbitrary numbers of antennas but the transmitter has two antennas. We have reformulated the problem of determining the secrecy capacity into a tractable form and solved this new problem to find the corresponding optimal precoding and power allocation schemes. Our investigation leads to a closed-form solution for the covariance matrix and computable secrecy capacity.

References

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

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

[3] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, 2011.

[4] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, 2009.

[5] S. A. A. Fakoorian and A. L. Swindlehurst, "Optimal power allocation for GSVD-based beamforming in the MIMO Gaussian wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory*, pp. 2321–2325, 2012.

[6] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4033–4039, 2009.

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

[8] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE Int. Symp. Inf. Theory*, pp. 2466–2470, 2007.

[9] S. A. A. Fakoorian and A. L. Swindlehurst, "Full rank solutions for the MIMO Gaussian wiretap channel with an average power constraint," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2620–2631, 2013.

[10] S. Loyka and C. D. Charalambous, "Optimal signaling for secure communications over Gaussian MIMO wiretap channels," *IEEE Trans. Inf. Theory*, vol. 62, no. 12, pp. 7207–7215, 2016.

[11] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.

[12] M. Vaezi, W. Shin, and H. V. Poor, "Optimal beamforming for Gaussian MIMO wiretap channels with two transmit antennas," submitted to *IEEE Trans. Wireless Commun.*, Jan. 2017.