Optimal Beamforming for Gaussian MIMO Wiretap Channels With Two Transmit Antennas

Mojtaba Vaezi, *Member, IEEE*, Wonjae Shin, *Student Member, IEEE*, and H. Vincent Poor, *Fellow, IEEE*

***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. The input covariance matrix that achieves the secrecy capacity is determined. In particular, it is shown that the secrecy capacity of this channel can be achieved by *linear precoding*. Precoding and power allocation schemes that maximize the achievable secrecy rate, and thus achieve the secrecy capacity, are developed. The secrecy capacity is then compared with the achievable secrecy rate of *generalized singular value decomposition* (GSVD)-based precoding, which is the best previously proposed technique for this problem. Numerical results demonstrate that substantial gain can be obtained in secrecy rate between the proposed and GSVD-based precodings.**

***Index Terms*— Physical layer security, MIMO wiretap channel, secrecy rate, beamforming, linear precoding.**

I. Introduction

Wireless networks have become an indispensable part of our daily lives and security/privacy of information transfer via these networks is crucial. Unfortunately, wireless communication systems are inherently insecure due to the broadcast nature of the medium. Hence, wireless security has been an important concern for many years. Traditionally, security is provided at the upper layers of wireless networks via *cryptographic* techniques, wherein the legitimate recipient of a message has a secret key to decode its message. Security can be also offered at the lowest layer (physical layer), e.g., via beamforming or artificial noise injection [2], to support and supplement existing cryptographic protocols.

Physical layer security has attracted widespread attention as a means of augmenting wireless security [2]. 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 [3], in the context of the *wiretap* channel. In this channel, a transmitter wishes to transmit information to a *legitimate* receiver while keeping the information secure from an *eavesdropper*. Wyner demonstrated that it is possible to have both *reliable* and *secure* communication between the transmitter and legitimate receiver in the presence of an eavesdropper under certain circumstances. The basic principle is that the channel of the legitimate receiver should be stronger in some sense than that of the eavesdropper.

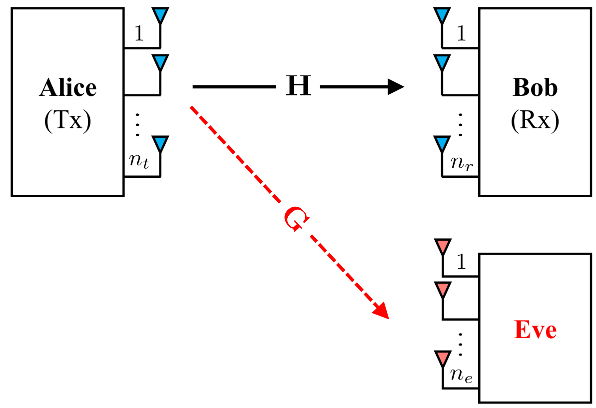


Fig. 1. MIMO Gaussian wiretap channel with n_t, n_r, and n_e antennas, respectively, at the transmitter (Alice), legitimate receiver (Bob), and eavesdropper (Eve).

With the rapid advancement of multi-antenna techniques, security enhancement in multiple-input multiple-output (MIMO) wiretap channels, see Fig. 1, has drawn significant attention. A big step toward understanding the MIMO Gaussian wiretap channel was taken in [4]–[6] where a closed-form expression for the secrecy capacity of this channel was established. However, to compute this expression, the input covariance matrix that maximizes it needs to be determined. Under an average power constraint, such a matrix is unknown in general.[1] Recently, numerical solutions have been proposed to compute a transmit covariance matrix for this channel [8]–[10]. These numerical approaches solve the underlying non-convex optimization problem iteratively. Despite their efficiency, there is still motivation to find an analytical solution for this problem and study simpler techniques for secure communication, e.g., based on linear precoding.

Precoding is a technique for exploiting transmit diversity via weighting of the information stream. *Singular value decomposition* (SVD) precoding with *water-filling* power allocation is a well-known example that achieves the capacity

Manuscript received January 16, 2017; revised May 5, 2017 and July 12, 2017; accepted July 16, 2017. Date of publication July 25, 2017; date of current version October 9, 2017. 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. This paper was presented in part at the IEEE International Symposium on Information Theory, Aachen, Germany, June 2017 [1]. The associate editor coordinating the review of this paper and approving it for publication was L. Lai. *(Corresponding author: Mojtaba Vaezi.)*

M. Vaezi and H. V. Poor are with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA (e-mail: mvaezi@princeton.edu; poor@princeton.edu).

W. Shin is with the Department of Electrical and Computer Engineering, Seoul National University, Seoul 08826, South Korea (e-mail: wonjae.shin@snu.ac.kr).

Digital Object Identifier 10.1109/TWC.2017.2729541

[1] Under a power-covariance constraint, the capacity expression and corresponding covariance matrix are found in [6] and [7], respectively.

1536-1276 © 2017 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

of the MIMO channel. Khisti and Wornell [4] proposed a *generalized SVD* (GSVD)-based precoding scheme with equal power allocation for the MIMO Gaussian wiretap channel. The optimal power allocation scheme for GSVD precoding in the MIMO Gaussian wiretap channel was obtained in [11]. Although GSVD precoding gets close to the secrecy capacity in certain antenna configurations, it is neither capacity-achieving nor very close to capacity, in general. Despite its importance and years of research, transmit/receive strategies that maximize the secure rate in MIMO wiretap channels remain unknown, in general. Linear beamforming transmission has, however, been proved to be optimal for the special case of $n_t = 2$, $n_r = 2$, and $n_e = 1$ in [12]. It is also known to be the optimal communication strategy for multiple-input single-output (MISO) wiretap channels [13], [14].

Recently, a closed-form solution for the optimal covariance matrix has been found when the channel is strictly degraded and another condition on the channel matrices, which is equivalent to a lower threshold on the transmitted power, holds [15]–[17]. The combination of this result and the unit-rank solution of [14] gives the optimal covariance matrix for the case of two transmit antennas [17]. 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. This proves that linear beamforming transmission can be 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 [16] and [17]. 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. It requires searching over two scalars (i.e., the power allocation) at most. In addition, the proposed beamforming and power allocation schemes can bring notably high gain over GSVD-based beamforming, as confirmed by simulation results.

It is worth highlighting that the new precoding and power allocation techniques are applicable to and optimal for MIMO channels without secrecy, simply by setting the eavesdropper's channel gain to zero. In such cases, power allocation is even simpler and does not require a search.

Secure transmission strategies in multi-antenna networks with various constraints and/or in different settings, e.g., with energy-efficiency [18], finite memory [19], joint source-relay precoding [20], game-theoretic precoding [21], and varying eavesdropper channel states [22], have been considered recently.

The rest of 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/MISO wiretap channels. In Section IV, we show that the proposed precoding and power allocation schemes are also optimal for MIMO/MISO channels without an eavesdropper and we discuss possible extensions of the proposed precoding method. We present numerical results in Section V before concluding the paper in Section VI.

Throughout this work, we use $\mathrm{tr}(\cdot)$, $\det(\cdot)$, $(\cdot)^t$, and $(\cdot)^H$ to denote the trace, determinant, transpose, and conjugate transpose of a matrix, respectively. Matrices are written in bold capital letters and vectors are written in bold small letters. $\mathbf{A} \succeq \mathbf{0}$ means that $\mathbf{A}$ is a positive semidefinite matrix, and $\mathbf{I}_m$ represents the identity matrix of size m.

II. System Model and Preliminaries

Consider a MIMO Gaussian wiretap channel, in which a transmitter (Alice) wishes to communicate with a legitimate receiver (Bob) in the presence of an eavesdropper (Eve), as shown in Fig. 1. The nodes are equipped with n_t, n_r, and n_e antennas, respectively. Let $\mathbf{H} \in \mathbb{R}^{n_r \times n_t}$ and $\mathbf{G} \in \mathbb{R}^{n_e \times n_t}$ be the channel matrices for the legitimate user and eavesdropper. Both channels are assumed to undergo independent and identically distributed (i.i.d.) Rayleigh fading, where the channel gains are real Gaussian random variables.[2] The received signals 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 $\mathbf{w}_i \in \mathbb{R}^{n_i \times 1}$, $i \in \{r, e\}$, represents an i.i.d. Gaussian noise vector with zero mean and identity covariance matrix. As will be seen later, $\mathbf{x} = \mathbf{V}\mathbf{s}$ where $\mathbf{V} \in \mathbb{R}^{n_t \times n_t}$ is the *precoding matrix* to transmit a secrete data symbol vector $\mathbf{s}$. The transmitted signal is subject to an average power constraint

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

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

A single-letter expression for the secrecy capacity of the general *discrete memoryless* wiretap channel with transition probability $p(y_r, y_e|x)$ is given by [24]

$$C_s = \max_{p(u,x)} \left[I(U; Y_r) - I(U; Y_e) \right], \tag{2}$$

in which the auxiliary random variable U satisfies the Markov relation $U \to X \to (Y_r, Y_e)$.

With this, the problem of characterizing the secrecy capacity of the multiple-antenna wiretap channel reduces to evaluating (2) for the channel model given in (1). This was, however, open until the works of Khisti and Wornell [4] and Oggier and Hassibi [5], in which it was proven that $U = X$ is optimal in (2). Then, the secrecy capacity (bits per real dimension) is the solution of the following optimization problem[3] [4]–[6]:

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

[2]The results of this paper are easily extendable to the case in which the channel gains and noises are complex Gaussian random variables and the input is real. This is due to the fact that each use of the complex channel can be thought of as two independent uses of a real additive white Gaussian noise channel, noting that the noise is independent in the I and Q components [23].

[3]For a complex channel, the factor $\frac{1}{2}$ is dropped because the capacity per complex dimension is twice the capacity per real dimension.

in which the first two constraints are due to the fact that $\mathbf{Q}$ is a covariance matrix and the third constraint is the aforementioned average power constraint. The secrecy capacity is obviously nonnegative as $\mathbf{Q} = \mathbf{0}$ is a feasible point of (3). The above optimization problem is non-convex (except for $n_r = n_e = 1$ [25]) and its objective function possesses numerous local maxima [8], [10], [26]. As such, a closed-form solution for the optimum $\mathbf{Q}$ is not known, in general.

The problem of characterizing the input covariance matrix that achieves the secrecy capacity subject to a power constraint has been under active investigation [15]–[17], [27]. Until recently, the special cases for which the optimal $\mathbf{Q}$ was known were limited to the cases of $n_r = 1$ [14] and $n_t = 2$, $n_r = 2$, $n_e = 1$ [12].[4] More recently, major steps have been made in characterizing the optimal covariance matrix. Fakoorian and Swindlehurst [16] determined conditions under which the optimal input covariance matrix is full-rank or rank-deficient. They also fully characterized the optimal $\mathbf{Q}$ when it is full-rank. Very recently, Loyka and Charalambous [17] found a closed-form solution for the optimal covariance matrix when the channel is strictly degraded ($\mathbf{H}^H\mathbf{H} \succ \mathbf{G}^H\mathbf{G}$) and transmission power is greater than a certain value. The combination of this result and the unit-rank solution of [4] gives the optimal $\mathbf{Q}$ for the rank-2 case [17]. The optimal solution is, however, still open in general.

In this paper, we study the MIMO wiretap channel with $n_t = 2$ while n_r and n_e are arbitrary integers. We derive a closed-form solution for the optimal covariance matrix in this case. Our approach is completely different from that of [16] and [17]. In addition, unlike [16] and [17], our approach does not require finding the rank of the optimal covariance matrix before fully characterizing the solution. It gives the optimal solution for both full-rank and rank-deficient cases in one shot. This is in contrast to the results in [17], from which it is not clear when the rank of the optimal solution switches from one to two (i.e., the paper does not clarify at what power threshold this change of rank happens); thus, it is not known from [17] whether a rank-one solution or full-rank solution should be applied.

III. A Capacity Achieving Precoding

Based on the optimization problem in (3), a characterization of the secrecy capacity of the MIMO Gaussian wiretap channel is given by non-negative R such that

$$\begin{aligned} R &\le \max_{\mathbf{Q}} \frac{1}{2}\left[\log\det(\mathbf{I}_{n_r}+\mathbf{H}\mathbf{Q}\mathbf{H}^t) - \log\det(\mathbf{I}_{n_e}+\mathbf{G}\mathbf{Q}\mathbf{G}^t)\right] \\ &= \max_{\mathbf{Q}} \frac{1}{2}\log\frac{\det(\mathbf{I}_{n_t}+\mathbf{H}^t\mathbf{H}\mathbf{Q})}{\det(\mathbf{I}_{n_t}+\mathbf{G}^t\mathbf{G}\mathbf{Q})}, \end{aligned} \tag{4}$$

where $\mathbf{Q} \succeq \mathbf{0}, \mathbf{Q} = \mathbf{Q}^t, \mathrm{tr}(\mathbf{Q}) \le P$. The equality in (4) is due to the fact 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

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

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 Λ is the diagonal matrix whose diagonal elements are the corresponding eigenvalues, i.e., $\Lambda_{ii} = \lambda_i$. In this paper, we study the case in which $n_t = 2$ while n_r and n_e are arbitrary integers.

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*

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

in which λ_1 and λ_2 are nonnegative, and

$$a_1 = (\lambda_2 - \lambda_1)h_2, \tag{10a}$$
$$b_1 = \frac{1}{2}(\lambda_1 - \lambda_2)(h_3 - h_1), \tag{10b}$$
$$c_1 = 1 + \frac{1}{2}(\lambda_1 + \lambda_2)(h_1 + h_3) + \lambda_1\lambda_2(h_1h_3 - h_2^2), \tag{10c}$$

and

$$a_2 = (\lambda_2 - \lambda_1)g_2, \tag{11a}$$
$$b_2 = \frac{1}{2}(\lambda_1 - \lambda_2)(g_3 - g_1), \tag{11b}$$
$$c_2 = 1 + \frac{1}{2}(\lambda_1 + \lambda_2)(g_1 + g_3) + \lambda_1\lambda_2(g_1g_3 - g_2^2). \tag{11c}$$

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

$$\mathbf{V}^t\mathbf{H}^t\mathbf{H}\mathbf{V} = \begin{bmatrix} w_1 & w_2 \\ w_2 & w_3 \end{bmatrix}, \tag{12}$$

in which

$$w_1 = h_1\sin^2\theta + h_3\cos^2\theta - 2h_2\sin\theta\cos\theta, \tag{13a}$$
$$w_2 = h_2(\cos^2\theta - \sin^2\theta) + (h_3 - h_1)\sin\theta\cos\theta, \tag{13b}$$
$$w_3 = h_1\cos^2\theta + h_3\sin^2\theta + 2h_2\sin\theta\cos\theta. \tag{13c}$$

Consequently,

$$\begin{aligned} \det(\mathbf{I}_{n_t} + \mathbf{H}^t\mathbf{H}\mathbf{Q}) &= \det(\mathbf{I}_{n_t} + \mathbf{V}^t\mathbf{H}^t\mathbf{H}\mathbf{V}\Lambda) \\ &= (1 + \lambda_1 w_1)(1 + \lambda_2 w_3) - \lambda_1\lambda_2 w_2^2. \end{aligned} \tag{14}$$

[4]In these cases, the capacity is obtained by beamforming (i.e., signaling with a rank one covariance) along the direction of the generalized eigenvector of $\mathbf{H}$ and $\mathbf{G}$ corresponding to the maximum eigenvalue of that pair.

Next, using the basic trigonometric identities

$$\cos 2\theta = 2\cos^2\theta - 1 = 1 - 2\sin^2\theta, \tag{15a}$$
$$\sin 2\theta = 2\sin\theta\cos\theta, \tag{15b}$$

it is straightforward to show that

$$w_1 = \frac{h_1+h_3}{2} + \frac{h_3-h_1}{2}\cos 2\theta - h_2\sin 2\theta, \tag{16a}$$
$$w_2 = h_2\cos 2\theta + \frac{h_3-h_1}{2}\sin 2\theta, \tag{16b}$$
$$w_3 = \frac{h_1+h_3}{2} - \frac{h_3-h_1}{2}\cos 2\theta + h_2\sin 2\theta. \tag{16c}$$

Substituting (16a)-(16c) in (14), we obtain

$$\det(\mathbf{I}_{n_t} + \mathbf{H}^t\mathbf{H}\mathbf{Q}) = a_1\sin 2\theta + b_1\cos 2\theta + c_1, \tag{17}$$

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

$$\det(\mathbf{I}_{n_t} + \mathbf{G}^t\mathbf{G}\mathbf{Q}) = a_2\sin 2\theta + b_2\cos 2\theta + c_2, \tag{18}$$

where a_2, b_2, and c_2 are given in (11). It should be mentioned that the constraint $\lambda_1 + \lambda_2 \le P$ comes from $\mathrm{tr}(\mathbf{Q}) \le P$ since, from (6), $\mathrm{tr}(\mathbf{Q}) = \mathrm{tr}(\mathbf{V}\Lambda\mathbf{V}^t) = \mathrm{tr}(\mathbf{V}^t\mathbf{V}\Lambda) = \mathrm{tr}(\Lambda)$. Note that $\mathrm{tr}(\mathbf{AB}) = \mathrm{tr}(\mathbf{BA})$ 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: See Appendix A. □

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

$$W = \frac{a_1\sin 2\theta + b_1\cos 2\theta + c_1}{a_2\sin 2\theta + b_2\cos 2\theta + c_2}. \tag{19}$$

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

$$a\sin 2\theta + b\cos 2\theta + c = 0, \tag{20}$$

in which

$$a = c_1b_2 - c_2b_1, \tag{21a}$$
$$b = a_1c_2 - a_2c_1, \tag{21b}$$
$$c = a_1b_2 - a_2b_1. \tag{21c}$$

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 $a^2 + b^2 \ne 0$. Defining $\frac{b}{a} = \tan\phi$, (20) can be further simplified as

$$\sin(2\theta + \phi) + \frac{c}{\sqrt{a^2+b^2}} = 0. \tag{22}$$

The critical points of the above equation are given by

$$2\theta = \begin{cases} -\arctan\dfrac{b}{a} - \arcsin\dfrac{c}{\sqrt{a^2+b^2}} + 2k\pi \\ -\arctan\dfrac{b}{a} + \pi + \arcsin\dfrac{c}{\sqrt{a^2+b^2}} + 2k\pi \end{cases}, \tag{23}$$

where k is an integer.[5] Then, using the second derivative of W with respect to θ, we can verify that the first argument gives the minimum of W while the second one gives its maximum. For completeness, this is proved in Appendix B. Further, without loss of optimality, we let $k = 0$ in (23). Hence, the θ that maximizes W is obtained as

$$\theta^* = -\frac{1}{2}\arctan\frac{b}{a} + \frac{1}{2}\arcsin\frac{c}{\sqrt{a^2+b^2}} + \frac{\pi}{2}. \tag{24}$$

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 (19) where θ is given in (24). We can vary λ_1 from 0 to P. Therefore, we 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

$$\mathbf{V} = \begin{bmatrix} -\sin\theta & \cos\theta \\ \cos\theta & \sin\theta \end{bmatrix}, \tag{25}$$

as the transmit beamformer with the power allocation matrix

$$\Lambda = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}. \tag{26}$$

An optimal θ is given by (24) *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* (19).

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 2, similarly to the V-BLAST architecture for communicating over the MIMO channel [23]. 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, we have the capacity-achieving architecture in Fig 2.[6]

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: See Appendix C. □

This lemma implies that to find optimal (λ_1, λ_2) in Theorem 1, it suffices to search for λ_1 in $[0, \frac{P}{2}]$ rather than $[0, P]$.

[5]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.

[6]It is worth mentioning that we can determine another orthogonal matrix $\mathbf{U}$, to express the output in terms of its columns, such that the input/output relationship is very simple and independent decoding is optimal.

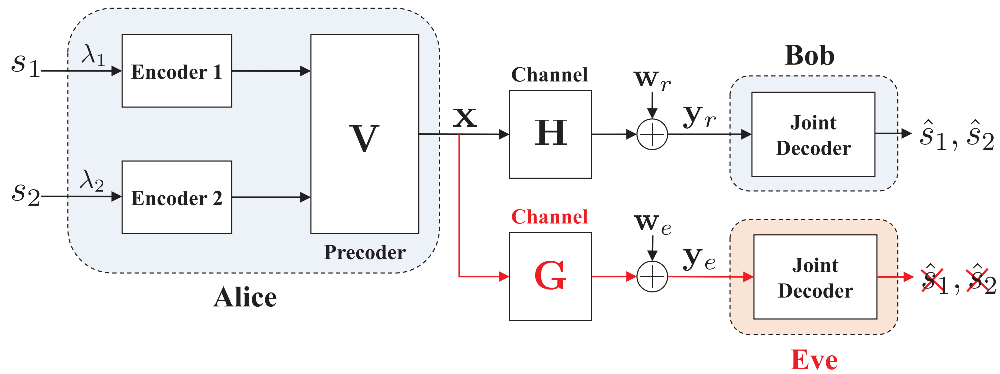


Fig. 2. Optimal architecture for communicating over the MIMO Gaussian wiretap channel with $n_t = 2$ and arbitrary n_r and n_e.

C. Special Cases

The first special case of the MIMO Gaussian wiretap channel we consider is the MISO Gaussian wiretap channel. In the following corollary, we prove that a positive capacity for the MISO case is obtained by signaling with a rank one covariance. This has already been shown in [14] using a different argument.

Corollary 1: For the MISO Gaussian wiretap channel, Theorem 1 significantly simplifies and $(\lambda_1, \lambda_2) = (0, P)$ or $(\lambda_1, \lambda_2) = (0, 0)$ is the optimal solution. The optimal θ is then obtained from (24).

Proof: In the case of the MISO multi-eavesdropper wiretap channel it is known that the rank of the covariance matrix is either one or zero (see [14, Theorem 2] or [17]). In the latter case, it is trivial that $(\lambda_1, \lambda_2) = (0, 0)$ is an optimal solution. In the former case, from Theorem 1 we can see that a rank-one solution implies that either λ_1 or λ_2 is equal to zero. Then, from Lemma 2 we conclude that $(\lambda_1, \lambda_2) = (P, 0)$ or $(\lambda_1, \lambda_2) = (0, P)$. But, in view of Lemma 3, we know that with proper choice of θ these two cases result in the same maximum rates; thus, one of them can be removed. □

Another special case of the MIMO Gaussian wiretap channel is the case in which the eavesdropper has only one antenna. Specifically, by setting $n_e = 1$ in Theorem 1 we get the following.

Corollary 2: For the 2-n_r-1 Gaussian wiretap channel, the optimal transmit covariance matrix is at most unit-rank. In particular, either $(\lambda_1, \lambda_2) = (0, P)$ or $(\lambda_1, \lambda_2) = (0, 0)$ gives the optimal solution in Theorem 1.

Proof: The proof is very similar to that of Corollary 1 and is omitted. Note that the objective function, in this case, is in the form of the inverse of that of Corollary 1. □

Note that Corollary 1 gives the secrecy capacity of 2-n_r-1 channels and thus generalizes the result of [12] for the 2-2-1 channel.

D. Closed-Form Solution for Optimal Power Allocation

Finding optimal λ_1 and λ_2 in Theorem 1 requires an exhaustive search. Although checking a reasonably small number of (λ_1, λ_2) is enough in practice,[7] 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:

$$C_{\text{MIMOME}} = \max_{\lambda_1+\lambda_2=P} \frac{1}{2}\log(W), \tag{27}$$

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 (16a)-(16c) we will have

$$w_1 = c_h + d_h \cos(2\theta - \phi_h), \tag{28a}$$
$$w_2 = d_h \sin(2\theta - \phi_h), \tag{28b}$$
$$w_3 = c_h - d_h \cos(2\theta - \phi_h). \tag{28c}$$

Now, we can write

$$\begin{aligned} W_h &= \det(\mathbf{I}_{n_t} + \mathbf{H}^t\mathbf{H}\mathbf{Q}) \\ &\overset{(a)}{=} (1 + \lambda_1 w_1)(1 + \lambda_2 w_3) - \lambda_1\lambda_2 w_2^2 \\ &= 1 + \lambda_1 w_1 + \lambda_2 w_3 + \lambda_1\lambda_2(w_1 w_3 - w_2^2) \\ &\overset{(b)}{=} 1 + \lambda_1 w_1 + \lambda_2 w_3 + \lambda_1\lambda_2(h_1 h_3 - h_2^2) \\ &\overset{(c)}{=} 1 + (\lambda_1 + \lambda_2)c_h + (\lambda_1 - \lambda_2)d_h\cos(2\theta - \phi_h) \\ &\quad + \lambda_1\lambda_2(h_1 h_3 - h_2^2), \\ &\overset{(d)}{=} 1 + Pc_h + (2\lambda_1 - P)d_h\cos(2\theta - \phi_h) \\ &\quad + \lambda_1(P - \lambda_1)(h_1 h_3 - h_2^2) \\ &\overset{(e)}{=} \alpha_h + \beta_h\lambda_1 - \delta_h\lambda_1^2, \end{aligned} \tag{29}$$

in which (a) is due to (14), (b) can be verified using (16a)-(16c), (c) is due to (28a) and (28c), (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

$$\alpha_h = 1 + Pc_h - Pd_h\cos(2\theta - \phi_h), \tag{30a}$$
$$\beta_h = 2d_h\cos(2\theta - \phi_h) + P\delta_h, \tag{30b}$$
$$\delta_h = h_1 h_3 - h_2^2. \tag{30c}$$

In a similar way, we can show that

$$W_g = \det(\mathbf{I}_{n_t} + \mathbf{G}^t\mathbf{G}\mathbf{Q}) = \alpha_g + \beta_g\lambda_1 - \delta_g\lambda_1^2, \tag{31}$$

[7] This is discussed in Section V.

where

$$\alpha_g = 1 + Pc_g - Pd_g \cos(2\theta - \phi_g), \tag{32a}$$

$$\beta_g = 2d_g \cos(2\theta - \phi_g) + P\delta_g, \tag{32b}$$

$$\delta_g = g_1 g_3 - g_2^2, \tag{32c}$$

and c_g, d_g, and ϕ_g are defined for $\mathbf{G}$ similarly to those of $\mathbf{H}$. Hence, we can write

$$W = \frac{W_h}{W_g} = \frac{\alpha_h + \beta_h \lambda_1 - \delta_h \lambda_1^2}{\alpha_g + \beta_g \lambda_1 - \delta_g \lambda_1^2}. \tag{33}$$

Next, it can be checked that

$$\frac{\partial W}{\partial \lambda_1} = \frac{\bar{c} + \bar{b}\lambda_1 + \bar{a}\lambda_1^2}{(\alpha_g + \beta_g \lambda_1 - \delta_g \lambda_1^2)^2}, \tag{34}$$

in which

$$\bar{a} = \delta_g \beta_h - \delta_h \beta_g, \tag{35a}$$

$$\bar{b} = 2\delta_g \alpha_h - 2\delta_h \alpha_g, \tag{35b}$$

$$\bar{c} = \beta_h \alpha_g - \beta_g \alpha_h. \tag{35c}$$

Let $\Delta = \bar{b}^2 - 4\bar{a}\bar{c}$, and suppose that $\Delta > 0$.[8] Then

$$\lambda_{1,1}^* = (-\bar{b} + \sqrt{\Delta})/2\bar{a}, \tag{36a}$$

$$\lambda_{1,2}^* = (-\bar{b} - \sqrt{\Delta})/2\bar{a}, \tag{36b}$$

are the roots of (34). Next, it is easy to show that, for $\lambda_{1,i}^*$, $i \in \{1, 2\}$, in (36a) and (36b) we have

$$\frac{\partial^2 W}{\partial \lambda_1^2}(\lambda_{1,i}^*) = \frac{\bar{b}+2\bar{a}\lambda_{1,i}^*}{(\alpha_g+\beta_g\lambda_1-\delta_g\lambda_1^2)^2} = \begin{cases} +\dfrac{\sqrt{\Delta}}{W_g^2}, & i = 1 \\ -\dfrac{\sqrt{\Delta}}{W_g^2}, & i = 2. \end{cases} \tag{37}$$

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) and (11) to find the optimal θ. 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

$$(\lambda_1^*, \lambda_2^*) = (0, 0), \tag{38a}$$

$$(\lambda_1^*, \lambda_2^*) = (0, P), \tag{38b}$$

$$(\lambda_1^*, \lambda_2^*) = (\lambda_{1,2}^*, P - \lambda_{1,2}^*), \tag{38c}$$

in order to obtain the maximum of W. We should highlight that (38c) will be a choice only if $\lambda_{1,2}^*$, defined in (36b), is a real number between 0 and P. As a result, we have the following.

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

Theorem 2: The optimal λ_1 and λ_2 in Theorem 1 are confined to one of the following cases:

$$(\lambda_1, \lambda_2) = \begin{cases} (0, 0), \\ (0, P), \\ (\lambda^*, P - \lambda^*), \end{cases} , \tag{39}$$

in which $\lambda^* \triangleq \lambda_{1,2}^*$ is defined in (36b)*, and θ is given in* (24)*.*

Remark 1: As can be traced from (36b), in general, the optimal λ_1 is a function of θ. On the other hand, the optimal θ, given in (24), 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 (39). Then, by evaluating W for these points we can determine which one is the optimal (capacity-achieving) solution. For the first two cases in (39) the solution is obtained analytically. However, the equation resulting from combining the third case in (39) and (24) is rather cumbersome and thus we solve it numerically.

IV. Special Cases and Possible Extensions

In this section, we briefly consider some special cases of the proposed precoding as well as possible extensions of this work.

A. Beamforming for MISO and MIMO Channels

The optimal beamforming provided in the previous section achieves the capacity of MISO and MIMO channels without an eavesdropper ($\mathbf{G} = \mathbf{0}$), as shown below.

1) Capacity of MISO Channels: We know that the capacity of a MISO channel is given by [23]

$$C_{\text{MISO}} = \frac{1}{2} \log \; (1 + \|\mathbf{h}\|^2 P), \tag{40}$$

where $\mathbf{h}$ is the channel vector. On the other hand, using (14), it is straightforward to check that the above rate is achieved by letting $\lambda_1 = P$, $\lambda_2 = 0$, and $\theta = \frac{\pi}{2} + \alpha$, where $\tan\alpha \triangleq \frac{\sqrt{h_3}}{\sqrt{h_1}}$.

2) Capacity of MIMO Channels: It can be also checked that the proposed beamforming and power allocation is equal to SVD-based beamforming with water-filling for $\theta = \frac{1}{2}\tan^{-1}\frac{b_h}{a_h}$ and

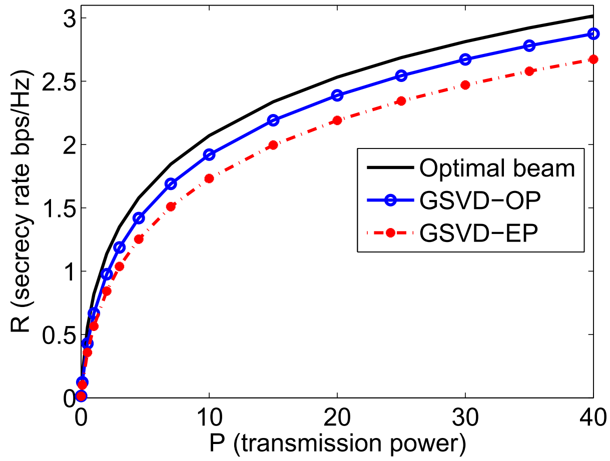
$$\lambda_1 = \min\left\{\frac{P}{2} + \frac{c_h}{\delta_h}, P\right\}, \tag{41a}$$

$$\lambda_2 = \max\left\{\frac{P}{2} - \frac{c_h}{\delta_h}, 0\right\}, \tag{41b}$$

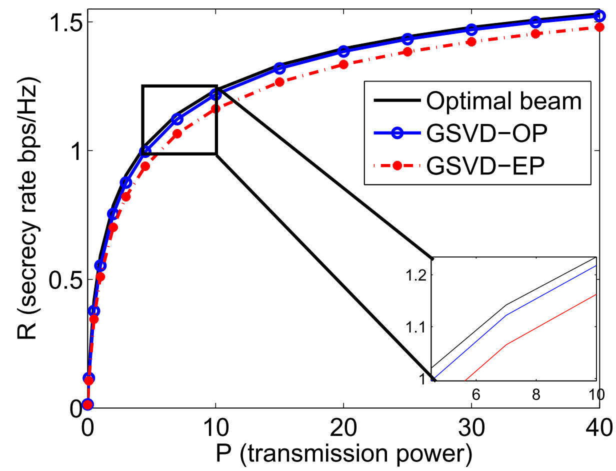
where $a_h = \frac{h_1 - h_3}{2}$, $b_h = h_2$, $c_h = \sqrt{a_h^2 + b_h^2}$, and $\delta_h = h_1 h_1 - h_2^2$.

B. Extension to $n_t > 2$

The key idea in this paper is to use the fact that any orthogonal matrix $\mathbf{V}$ is parametrized by a single parameter θ, as shown in (7). Considering this, in (4), we rewrite the capacity expression in a way that for any n_r and n_e (with $n_t = 2$) the terms $\mathbf{H}^t\mathbf{H}$ and $\mathbf{G}^t\mathbf{G}$ are 2×2 matrices. Hence, the capacity expression can be represented by three parameters, two nonnegative powers (λ_1 and λ_2) and one



(a) $n_e = 1$



(b) $n_e = 2$

Fig. 3. Comparison of the secrecy capacity of the MIMO Gaussian wiretap channel (achieved by the proposed beamforming method) and the secrecy rates of GSVD-based beamforming with equal and optimal power allocations for (a) $n_t = 2$, $n_r = 2$, $n_e = 1$ (b) $n_t = 2$, $n_r = 2$, $n_e = 2$.

angle θ.[9] Then, the covariance matrix can be optimized with elementary trigonometric equations, as shown in Section III. In the case of $n_t = 3$, the main difficulty is to parametrize the 3×3 orthogonal matrix $\mathbf{V}$ with two parameters. Even with this, it is not guaranteed that we will get a tractable optimization problem. We have made some progress towards this goal, but the resulting optimization problem is rather cumbersome and needs further simplification. This issue becomes more challenging as n_t increases.

C. Construction of Practical Codes

Although the capacity of the MIMO wiretap channel is well-studied, construction of practical codes is still a challenging issue for this channel. Recently, it has been shown in [28] that a good wiretap code, e.g., a scalar random-binning code [29], is applicable to the MIMO wiretap channel in conjunction with a linear encoder and a successive interference cancellation (SIC) decoder to achieve a rate close to the MIMO wiretap capacity. However, this approach gives rise to several practical issues in terms of implementation, such as dithering in the SIC decoder. Considering this, one direction for future work would be to find a more practical code construction for MIMO wiretap channels based on our new design of closed-form optimal beamforming and power allocation solutions.

V. 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 equal power (GSVD-EP) and optimal power (GSVD-OP) allocation proposed in [4] and [11], respectively. As proved in Section III, the proposed beamforming method is optimal and gives 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. It should be highlighted that the rate achieved by GSVD-OP is equal to or better than that of GSVD-EP, for any $\mathbf{H}$ and $\mathbf{G}$.

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, we use the optimal power allocation of Theorem 2. We plot the secrecy rates versus total average power.

We first consider the case with $n_t = 2$, $n_r = 2$, and $n_e = 1$, i.e., in which the eavesdropper has only one antenna. As can be seen from Fig. 3(a), the capacity-achieving beamforming performs significantly better than both versions of GSVD-based beamforming. By doubling the eavesdropper's number of antennas in Fig. 3(b), the secrecy capacity nearly halves. Moreover, the rate achieved by GSVD-OP becomes very close to that of the optimal method. However, as can be seen in Fig. 3(b), there is still a small gap between the two methods particularly when P is small.

We next consider the MISO wiretap channel in Fig. 4. It can be seen that there is a visible gap between the proposed beamforming and GSVD-based beamforming. Note that GSVD-EP and GSVD-OP have exactly the same performance for MISO wiretap channels. This is because there is only one beam and all power is allocated to that. A general trend seen both for MISO and MIMO wiretap channels is that as SNR increases the performance of GSVD-EP, and thus GSVD-OP, get closer to that of the optimal beamforming scheme derived in this paper. This is not surprising knowing that GSVD-EP is asymptotically optimal; i.e., it is capacity-achieving as $P \to \infty$ [4].

Figure 5 demonstrates the effect of increasing the number of antennas at the eavesdropper. All curves in this figure are for $n_t = 2$ and $n_r = 4$ but a different number of eavesdropper antennas, as denoted on each curve. Note that $n_e = 0$ refers to the case in which there is no eavesdropper; this curve is thus

[9]Excluding the case $\mathbf{H}^H\mathbf{H} - \mathbf{G}^H\mathbf{G} \preceq 0$ which results in the trivial solution $(\lambda_1, \lambda_2) = (0, 0)$, from Lemma 2 we can see that $\lambda_1 + \lambda_2 = P$. This implies that the capacity region can be expressed in terms of only two parameters, i.e., λ_1 and θ.

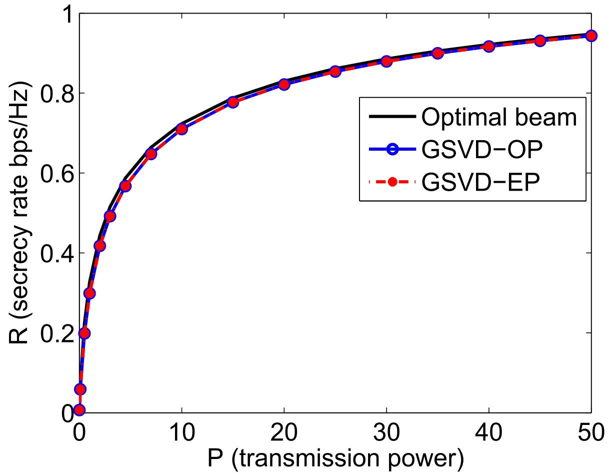


Fig. 4. The secrecy capacity of the MISO wiretap channel and the secrecy rates of GSVD-based beamforming for $n_t = 2$, $n_r = 1$, and $n_e = 2$.

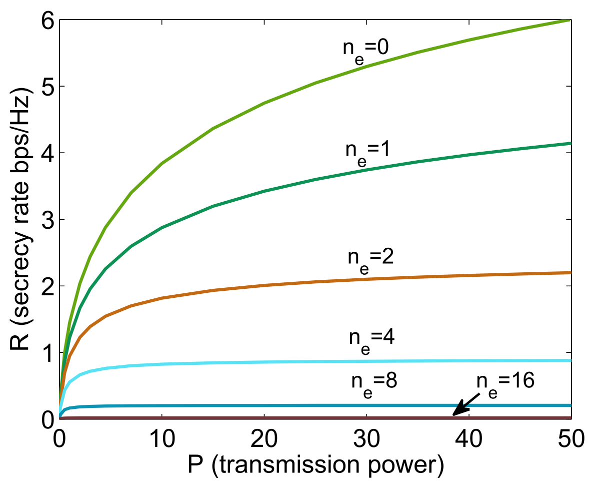


Fig. 5. The secrecy capacity of the MIMO Gaussian wiretap channel for various values of n_e, with $n_t = 2$ and $n_r = 4$.

the capacity of the MIMO channel.[10] Once the eavesdropper comes into play ($n_e \geq 1$), the extent to which information can be secured over the air reduces. The gap between each curve and the curve corresponding to $n_e = 0$ is the amount of unsecured information. Unfortunately, for $n_e = 16$, and thus $n_e > 16$, almost no information can be secured via physical layer techniques. This is because the eavesdropper can no longer be degraded by beamforming in this situation.

VI. Conclusion

We have developed a linear precoding scheme to achieve the secrecy 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 computable capacity with reasonably small complexity. The gap between the secrecy rates achieved by the proposed precoding and GSVD-based beamforming can be remarkably high depending on the antenna configurations. When the legitimate receiver or eavesdropper has a single antenna, the optimal transmission scheme is unit-rank, i.e., beamforming is optimal. Further, in the absence of the eavesdropper, the proposed precoding reduces to the capacity-achieving scheme for MIMO/MISO channels. Hence, it can be used for these channels with/without an eavesdropper.

[10]Recall from Section IV-A.2 that the proposed precoding for the MIMO Gaussian wiretap channel reduces to the well-known SVD precoding of the MIMO channel ($\mathbf{G} = \mathbf{0}$), and is capacity-achieving.

Appendix A: Proof of Lemma 2

Proof: Consider the optimization problem in (3). The secrecy capacity is zero if $\mathbf{H}^t\mathbf{H} - \mathbf{G}^t\mathbf{G} \preceq 0$ [5]. In this case, it is clear that $(\lambda_1, \lambda_2) = (0, 0)$ is optimal. Otherwise, the secrecy capacity is strictly positive [5] and $\lambda_1 + \lambda_2 = P$ is optimal. This completes the proof since the optimization problem in Lemma 1 is a different representation of (3). □

Appendix B

To prove that the first (second) argument in (23) corresponds to the minimum (maximum), it suffices to show that the second derivative of W is positive for the first argument and negative for the second one. Let $\beta \triangleq \arcsin \frac{c}{\sqrt{a^2+b^2}}$ and recall that $\beta \in [-\frac{\pi}{2}, \frac{\pi}{2}]$. Then, from (23), the critical points are given by θ_1 and θ_2 where

$$\theta_1 \triangleq -\frac{1}{2}\phi - \frac{1}{2}\beta + k\pi, \tag{42a}$$

$$\theta_2 \triangleq -\frac{1}{2}\phi + \frac{1}{2}\pi + \frac{1}{2}\beta + k\pi. \tag{42b}$$

Further, from (19)-(22), we know that

$$\frac{\partial W}{\partial \theta} = \frac{\sin(2\theta + \phi) + \sin\beta}{(a_2 \sin 2\theta + b_2 \cos 2\theta + c_2)^2}. \tag{43}$$

Then, at θ_2 we have

$$\begin{aligned} \frac{\partial^2 W}{\partial \theta^2}(\theta = \theta_2) &= \frac{2\cos(2\theta_2 + \phi)}{(a_2 \sin 2\theta_2 + b_2 \cos 2\theta_2 + c_2)^2} \\ &= \frac{-2\cos\beta}{(a_2 \sin 2\theta_2 + b_2 \cos 2\theta_2 + c_2)^2} \\ &\leq 0, \end{aligned} \tag{44}$$

since $\beta \in [-\frac{\pi}{2}, \frac{\pi}{2}]$. Similarly, we can prove that $\frac{\partial^2 W}{\partial \theta^2}(\theta_1) \geq 0$. Thus, θ_1 and θ_2 minimize and maximize W, respectively.

Appendix C: Proof of Lemma 3

To prove this, suppose (λ_1, λ_2) maximizes (19) for some θ^* given by (24). Then, from (10) and (11), 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.

Acknowledgement

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions that have significantly improved the quality of this paper.

REFERENCES

[1] M. Vaezi, W. Shin, H. V. Poor, and J. Lee, "MIMO Gaussian wiretap channels with two transmit antennas: Optimal precoding and power allocation," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2017, pp. 1708–1712.

[2] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 2014.

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

[4] 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, Nov. 2010.

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

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

[7] R. Bustin, R. Liu, H. V. Poor, and S. Shamai (Shitz), "An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel," *EURASIP J. Wireless Commun. Netw.*, Dec. 2009.

[8] Q. Li, M. Hong, H.-T. Wai, Y.-F. Liu, W.-K. Ma, and Z.-Q. Luo, "Transmit solutions for MIMO wiretap channels using alternating optimization," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1714–1727, Sep. 2013.

[9] J. Steinwandt, S. A. Vorobyov, and M. Haardt, "Secrecy rate maximization for MIMO Gaussian wiretap channels with multiple eavesdroppers via alternating matrix POTDC," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, May 2014, pp. 5686–5690.

[10] S. Loyka and C. D. Charalambous, "An algorithm for global maximization of secrecy rates in Gaussian MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 63, no. 6, pp. 2288–2299, Jun. 2015.

[11] 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*, Jul. 2012, pp. 2321–2325.

[12] 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, Sep. 2009.

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

[14] 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, Jul. 2010.

[15] S. Loyka and C. D. Charalambous, "On optimal signaling over secure MIMO channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2012, pp. 443–447.

[16] 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, May 2013.

[17] 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, Dec. 2016.

[18] H. Zhang, Y. Huang, S. Li, and L. Yang, "Energy-efficient precoder design for MIMO wiretap channels," *IEEE Commun. Lett.*, vol. 18, no. 9, pp. 1559–1562, Sep. 2014.

[19] N. Shlezinger, D. Zahavi, Y. Murin, and R. Dabora, "The secrecy capacity of Gaussian MIMO channels with finite memory," *IEEE Trans. Inf. Theory*, vol. 63, no. 3, pp. 1874–1897, Mar. 2017.

[20] H.-M. Wang, F. Liu, and X.-G. Xia, "Joint source-relay precoding and power allocation for secure amplify-and-forward MIMO relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 8, pp. 1240–1250, Aug. 2014.

[21] B. Fang, Z. Qian, W. Shao, W. Zhong, and T. Yin, "Game-theoretic precoding for cooperative MIMO SWIPT systems with secrecy consideration," in *Proc. IEEE Global Commun. Conf.*, Dec. 2015, pp. 1–5.

[22] X. He and A. Yener, "MIMO wiretap channels with unknown and varying eavesdropper channel states," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6844–6869, Nov. 2014.

[23] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[24] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[25] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proc. 41st Annu. Conf. Inf. Sci. Syst.*, Mar. 2007, pp. 905–910.

[26] S. Bashar, Z. Ding, and C. Xiao, "On secrecy rate analysis of MIMO wiretap channels driven by finite-alphabet input," *IEEE Trans. Commun.*, vol. 60, no. 12, pp. 3816–3825, Dec. 2012.

[27] J. Li and A. Petropulu. (Sep. 2009). "Transmitter optimization for achieving secrecy capacity in Gaussian MIMO wiretap channels." [Online]. Available: https://arxiv.org/abs/0909.2622

[28] A. Khina, Y. Kochman, and A. Khisti, "From ordinary AWGN codes to optimal MIMO wiretap schemes," in *Proc. IEEE Inf. Theory Workshop*, Nov. 2014, pp. 631–635.

[29] H. Tyagi and A. Vardy, "Explicit capacity-achieving coding scheme for the Gaussian wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun./Jul. 2014, pp. 956–960.

Mojtaba Vaezi (S'09–M'14) is an Associate Research Scholar in the Department of Electrical Engineering at Princeton University. He received the Ph.D. degree from McGill University, Montreal, in 2014, and the B.Sc. and M.Sc. degrees from Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran, all in Electrical Engineering. Before joining Princeton, he was a researcher at Ericsson Research in Montreal, Canada. His research interests include the broad areas of information theory, wireless communications, and signal processing, with an emphasis on physical layer security, fifth generation (5G) radio access technologies, and internet of things (IoT).

Dr. Vaezi has served as the president of McGill IEEE Student Branch during 2012–2013. Before joining McGill, he was the Head of Mobile Radio Network Design and Optimization Department at Ericsson Iran. He has been an Associate Technical Editor of *IEEE Communication Magazine* since 2014 and a TPC Chair of NOMA workshops at VTC-Spring'17 and Globecom'17. He is a recipient of several academic, leadership, and research awards, including McGill Engineering Doctoral Award, IEEE Larry K. Wilson Regional Student Activities Award in 2013, and the Natural Sciences and Engineering Research Council of Canada (NSERC) Postdoctoral Fellowship in 2014.

Wonjae Shin (S'14) received the B.S. and M.S. degrees from the Korea Advanced Institute of Science and Technology in 2005 and 2007, respectively. He is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, Seoul National University, South Korea. He has been a Visiting Student Research Collaborator with Princeton University, Princeton, NJ, USA, from 2016 to 2017. From 2007 to 2014, he was a Member of Technical Staff, Samsung Advanced Institute of Technology (SAIT) and Samsung Electronics Co., Ltd., South Korea, where he contributed to next generation wireless communication networks, especially for 3GPP LTE/LTE-Advanced standardizations. His research interests are in the design and analysis of future wireless communications, such as interference-limited networks. He received the SNU Best Ph.D. Dissertation Award in 2017, and the Gold Prize in the 2014 IEEE Student Paper Contest. He was a co-recipient of the SAIT Patent Award (2010), *Samsung Journal of Innovative Technology* (2010), Samsung Humantech Paper Contest (2010), and the Samsung CEO Award (2013). He was recognized as an Exemplary Reviewer by the IEEE WIRELESS COMMUNICATIONS LETTERS in 2014. He also received several fellowships, including the Samsung Fellowship Program in 2014 and the SNU Long-term Overseas Study Scholarship in 2016. He has been a Program Co-Chair for the IEEE VTC 2017-Spring Workshop.

H. Vincent Poor (S'72–M'77–SM'82–F'87) received the Ph.D. degree in EECS from Princeton University in 1977. From 1977 to 1990, he was on the faculty of the University of Illinois at Urbana–Champaign. Since 1990, he has been on the faculty at Princeton, where he is currently the Michael Henry Strater University Professor of Electrical Engineering. From 2006 to 2016, he served as the Dean of Princeton's School of Engineering and Applied Science. His research interests are in the areas of information theory and signal processing, and their applications in wireless networks and related fields such as smart grid and social networks. Among his publications in these areas is the book *Information Theoretic Security and Privacy of Information Systems* (Cambridge University Press, 2017).

Dr. Poor is a member of the National Academy of Engineering and the National Academy of Sciences, and is a foreign member of the Royal Society. He is also a fellow of the American Academy of Arts and Sciences, the National Academy of Inventors, and other national and international academies. He received the Marconi and Armstrong Awards of the IEEE Communications Society in 2007 and 2009, respectively. Recent recognition of his work includes the 2016 John Fritz Medal, the 2017 IEEE Alexander Graham Bell Medal, Honorary Professorships at Peking University and Tsinghua University, both conferred in 2016, and a D.Sc. *honoris causa* from Syracuse University awarded in 2017.