A Rotation-Based Precoding for MIMO Broadcast Channels With Integrated Services

Mojtaba Vaezi, *Senior Member, IEEE*, Yue Qi, and Xinliang Zhang, *Student Member, IEEE*

***Abstract*—The problem of merging multiple services over multiple-input multiple-output Gaussian broadcast channels with two receivers is studied. The transmitter provides two independent services: a public (multicast) service with a common message for both users, and a private service with a confidential message intended only for one of the users which is to be kept secret from the other. Under this scenario, a new linear precoding scheme is developed to maximize secrecy-multicast rate region. This scheme decomposes input covariance matrix using rotation matrices and results in a reformulation of the secrecy-multicast capacity region which is easier to be optimized. Next, by finding the distributions to which eigenvalues and rotation angles fit in, a search algorithm is proposed to solve the new capacity expression to find precoding and power allocation matrices. Numerical results illustrate that the proposed precoding method significantly increases the rate region compared to the existing methods.**

***Index Terms*—MIMO broadcast channel, physical layer service integration, secrecy capacity region, multicast, precoding.**

I. Introduction

THERE has been an ever-increasing demand for secure, reliable, and efficient implementation of communication services. Integration of different services, such as *multicast* and *confidential* services, is traditionally addressed by higher-layer policies (e.g., by allocating different *logical channels* to each service) and cryptographic techniques. As an alternative approach, *physical-layer service integration* (PHY-SI) offers these services on the same wireless resources in the lowest layer [1], [2]. Unlike conventional service integrations, the PHY-SI can flexibly merge multiple services which results in more advantageous utilization of the spectral and physical nature of wireless channels.

The basic idea of the PHY-SI can be dated back to Csiszár and Körner's seminal work on *broadcast channel* (BC) with confidential messages [3]. This idea has then been extended to multiple-input multiple-output (MIMO) channels. Particularly, the capacity region of the Gaussian MIMO-BC with one common message and one confidential message is established in [4]. In this model, the sender not only transmits an individual message to one receiver, which is to be kept secret from the other receiver, but also integrates an additional multicast service to both receivers. Although capacity expression for the above channel is known, optimal signaling (covariance matrix) to achieve the capacity region is not known to date.

Manuscript received July 3, 2019; revised September 9, 2019; accepted October 3, 2019. Date of publication October 7, 2019; date of current version October 24, 2019. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Yunlong Cai. *(Corresponding author: Mojtaba Vaezi.)*

The authors are with Villanova University, Villanova, PA 19085 USA (e-mail: mvaezi@villanova.edu; yqi@villanova.edu; xzhang4@villanova.edu).

Digital Object Identifier 10.1109/LSP.2019.2946088

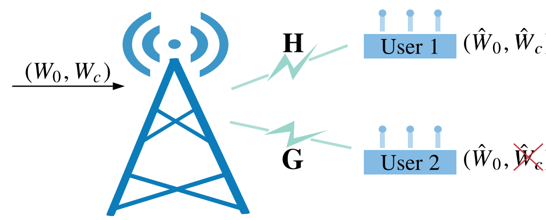


Fig. 1. MIMO-BC with common and confidential messages.

Secret dirty paper coding is the technique used to obtain the capacity regions in the above and other related settings [4]–[6]. The complexity of dirty-paper encoding and decoding is, however, very high and, in practice, linear precoding based transmit strategies are popular for their simplicity. A precoding scheme based on the *generalized singular value decomposition* (GSVD) was proposed in [7] which decouples the channels between the transmitter and receivers into several parallel subchannels where common and confidential messages are transmitted via different subchannels without interfering with each other. This method is, however, suboptimal and results in a solution far from the capacity region as shown in [7]. GSVD has also been applied in various related problems [8]–[11].

In this letter, we propose a new transmission strategy for the MIMO-BC in which a base station (BS) offers two types of services to two users: a public service (common, or multicast, message for both users), and a confidential service (private message merely for one of the users). To achieve the largest rate region promised by information theory, we propose a new *linear precoding* method based on basic *rotation* matrices. This method decomposes the covariance matrix into the product of a set of rotation matrices (for precoding) and a diagonal power-allocation matrix. With this parameterization, the original optimization problem is converted to a new problem which is easier to solve. In particular, it removes the positive semi-definiteness constraint of the covariance matrix. We also show that, with a judicious parameter generation, this method can reach the boundary of the capacity region in a more efficient manner. Numerical results show that the proposed transmission strategy achieves a significantly better rate region than GSVD-based precoding. It improves the achievable rates for both public and private services.

II. System Model and Background

Consider the communication over a Gaussian MIMO-BC with one BS and two users as shown in Fig. 1. The transmitter provides two kinds of services: 1) both users are served with the common message W_0; 2) one of the users is served with a confidential message W_c, which is to be kept perfectly secret from the other user. For $W_c = \emptyset$ this system reduces to a *multicast channel*, transmitting one common message to both users, and for $W_0 = \emptyset$ the system becomes a *wiretap channel* [10]–[13].

The transmitter, user 1, and user 2 are equipped with n_t, n_r, and n_e antennas, respectively. User 1 orders both common and confidential messages whereas user 2 orders only a common message. In this model, user 2 can be seen as an eavesdropper to the confidential message of user 1. The received signals at user 1 and user 2 at time m are given by

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

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

in which $\mathbf{x} \in \mathbb{R}^{n_t \times 1}$ is the channel input, $\mathbf{H} \in \mathbb{R}^{n_r \times n_t}$ and $\mathbf{G} \in \mathbb{R}^{n_e \times n_t}$ are the channel matrices for user 1 and user 2, respectively, and $\mathbf{w}_r \in \mathbb{R}^{n_r \times 1}$ and $\mathbf{w}_e \in \mathbb{R}^{n_e \times 1}$ are independent and identically distributed (i.i.d) Gaussian noise vectors with means zero and identity covariance matrices. The channel input $\mathbf{x}$ is composed of two independent parts: $\mathbf{x}_0$, the multicast (common) message, and $\mathbf{x}_c$, the confidential message. Specifically, $\mathbf{x} = \mathbf{x}_0 + \mathbf{x}_c$ and the input $\mathbf{x}$ is subject to the average total power constraint $\frac{1}{n}\sum_{m=1}^{n}(\mathbf{x}[m]^T\mathbf{x}[m]) = \frac{1}{n}\sum_{m=1}^{n}(||\mathbf{x}[m]||^2) \leq P$, where n is the codeword length [4].

Corollary 3 in [4] characterizes the capacity region of the PHY-SI (MIMO-BC with common and confidential messages) under the above power constraint. The capacity region is given by a set of common-confidential pairs (R_0, R_c) that satisfy

$$R_0 \leq \min\left\{\frac{1}{2}\log\left|\mathbf{I}_{n_r} + \frac{\mathbf{H}\mathbf{Q}_0\mathbf{H}^T}{\mathbf{I}_{n_r} + \mathbf{H}\mathbf{Q}_c\mathbf{H}^T}\right|, \frac{1}{2}\log\left|\mathbf{I}_{n_e} + \frac{\mathbf{G}\mathbf{Q}_0\mathbf{G}^T}{\mathbf{I}_{n_e} + \mathbf{G}\mathbf{Q}_c\mathbf{G}^T}\right|\right\}, \tag{2a}$$

$$R_c \leq \frac{1}{2}\log|\mathbf{I}_{n_r} + \mathbf{H}\mathbf{Q}_c\mathbf{H}^T| - \frac{1}{2}\log|\mathbf{I}_{n_e} + \mathbf{G}\mathbf{Q}_c\mathbf{G}^T|, \tag{2b}$$

$$\text{s.t.} \quad \mathrm{tr}(\mathbf{Q}_0 + \mathbf{Q}_c) \leq P, \tag{2c}$$

$$\mathbf{Q}_0 \succeq \mathbf{0},\ \mathbf{Q}_c \succeq \mathbf{0}, \tag{2d}$$

"$\succeq$" represents "great than or equal to" in the positive semidefinite order between matrices, $\mathbf{I}_n$ denotes the identity matrix of size n, and $\mathrm{tr}(\mathbf{A})$ denotes the trace of matrix $\mathbf{A}$. This capacity region is obtained when $\mathbf{x}_0 \sim \mathcal{N}(\mathbf{0}, \mathbf{Q}_0)$ and $\mathbf{x}_c \sim \mathcal{N}(\mathbf{0}, \mathbf{Q}_c)$ [4] where $\mathbf{Q}_0$ and $\mathbf{Q}_c$ are the covariance matrices of common and confidential messages, respectively.

While the capacity region of the PHY-SI is known in (2), it is unknown how to optimize the capacity-achieving covariance matrices $\mathbf{Q}_0$ and $\mathbf{Q}_c$. These are commonly obtained via an exhaustive search over $\{(\mathbf{Q}_0, \mathbf{Q}_c)|\mathbf{Q}_0 \succeq \mathbf{0}, \mathbf{Q}_c \succeq \mathbf{0}, \mathrm{tr}(\mathbf{Q}_0 + \mathbf{Q}_c) \leq P\}$ whose complexity is extremely high. It is worth noting that when there is no multicast message ($W_0 = \emptyset$), R_0 is zero and $\mathbf{Q}_0 = \mathbf{0}$ is optimal. In this case, a MIMO wiretap channel is obtained. On the other hand, $W_c = \emptyset$ implies $R_c = 0$ which results in $\mathbf{Q}_c = \mathbf{0}$. In this case, a MIMO multicast channel is obtained. Even in these special cases, the problem is challenging and optimal precoding is unknown, in general.

Mei *et al.* [7] proposed a GSVD-based precoding which produces several virtual orthogonal subchannels and transmits multicast and confidential messages in different subchannels. This scheme is suboptimal as orthogonalization does not result in an equivalent problem and is used for its simplicity. It may also not utilize the whole channel since certain subchannels (e.g., private subchannels of the eavesdropper) cannot be used for any of the messages and thus need to be discarded [7].

III. Rotation-Based Precoding

In this section, we reformulate the problem as an equivalent problem by applying a rotation-based parameterization to the covariance matrices $\mathbf{Q}_0$ and $\mathbf{Q}_c$. The idea of parameterization of the covariance matrix using a rotation matrix first appeared in the context of the MIMO wiretap channel [11], [13]. The covariance matrices $\mathbf{Q}_0$ and $\mathbf{Q}_c$ can be eigendecomposed as

$$\mathbf{Q}_0 = \mathbf{V}_0\mathbf{\Lambda}_0\mathbf{V}_0^T,\ \mathbf{Q}_c = \mathbf{V}_c\mathbf{\Lambda}_c\mathbf{V}_c^T, \tag{3}$$

in which $\mathbf{\Lambda}_0$ and $\mathbf{\Lambda}_c$ are diagonal matrices and their diagonal elements are eigenvalues of the corresponding covariance matrices and $\mathbf{V}_0$ and $\mathbf{V}_c$ are the eigenvectors matrices corresponding to $\mathbf{Q}_0$ and $\mathbf{Q}_c$, respectively. In [11], it is proposed that, without loss of generality, a rotation matrix can be used to parameterize the eigenvalue matrix for $n_t = 2$. The proposed solution has recently been generalized into an arbitrary n_t in [14]. Here, we apply this method to (2). We consider the cases with $n_t = 2$ and $n_t = 3$.

A. Parameterization of Covariance Matrices for $n_t = 2$

The eigenvalue matrices $\mathbf{\Lambda}_0$ and $\mathbf{\Lambda}_c$ can be written as

$$\mathbf{\Lambda}_0 = \begin{bmatrix}\lambda_{01} & 0\\ 0 & \lambda_{02}\end{bmatrix},\ \mathbf{\Lambda}_c = \begin{bmatrix}\lambda_{c1} & 0\\ 0 & \lambda_{c2}\end{bmatrix}, \tag{4}$$

in which the eigenvalues λ_{0j} and $\lambda_{cj}, j \in \{1, 2\}$, denote power allocation coefficients for common and confidential messages, respectively. The eigenvector matrices are orthonormal matrices and, without loss of generality, can be defined as [11]

$$\mathbf{V}_0 = \begin{bmatrix}\cos\alpha_0 & -\sin\alpha_0\\ \sin\alpha_0 & \cos\alpha_0\end{bmatrix},\ \mathbf{V}_c = \begin{bmatrix}\cos\alpha_c & -\sin\alpha_c\\ \sin\alpha_c & \cos\alpha_c\end{bmatrix}. \tag{5}$$

$\mathbf{V}_0$ and $\mathbf{V}_c$ are rotation matrices with parameters α_0 and α_c.

B. Parameterization of Covariance Matrices for $n_t = 3$

For $n_t = 3$, the power allocation matrices are given as

$$\mathbf{\Lambda}_0 = \begin{bmatrix}\lambda_{01} & 0 & 0\\ 0 & \lambda_{02} & 0\\ 0 & 0 & \lambda_{03}\end{bmatrix},\ \mathbf{\Lambda}_c = \begin{bmatrix}\lambda_{c1} & 0 & 0\\ 0 & \lambda_{c2} & 0\\ 0 & 0 & \lambda_{c3}\end{bmatrix}, \tag{6}$$

in which λ_{0j} and $\lambda_{cj}, j \in \{1, 2, 3\}$, are the power allocation of common and confidential messages respectively. The eigenvector matrices can be represented by rotation matrices $\mathbf{V}_0$ and $\mathbf{V}_c$ which are defined by

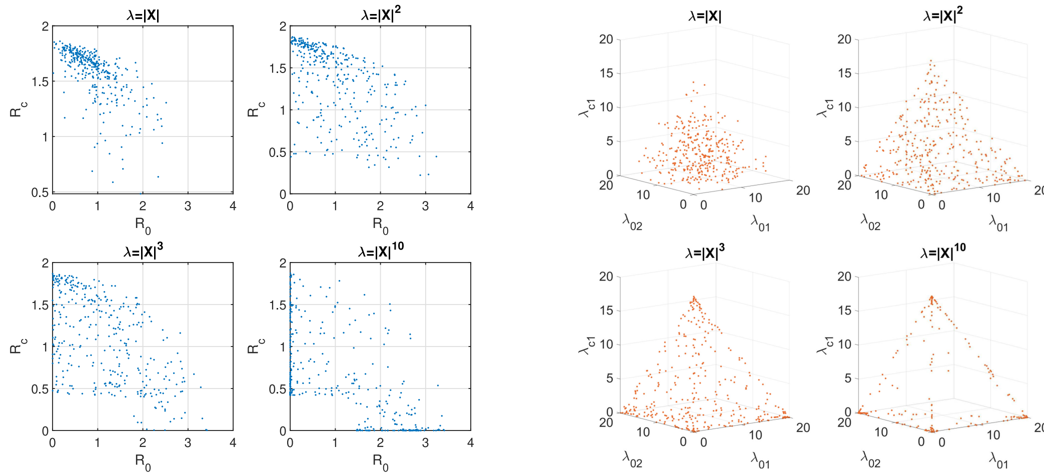
$$\mathbf{V}_0 = \mathbf{V}_{01}\mathbf{V}_{02}\mathbf{V}_{03},\ \mathbf{V}_c = \mathbf{V}_{c1}\mathbf{V}_{c2}\mathbf{V}_{c3}, \tag{7a}$$

and

$$\mathbf{V}_{i1} = \begin{bmatrix}\cos\alpha_{i1} & -\sin\alpha_{i1} & 0\\ \sin\alpha_{i1} & \cos\alpha_{i1} & 0\\ 0 & 0 & 1\end{bmatrix},$$

$$\mathbf{V}_{i2} = \begin{bmatrix}\cos\alpha_{i2} & 0 & -\sin\alpha_{i2}\\ 0 & 1 & 0\\ \sin\alpha_{i2} & 0 & \cos\alpha_{i2}\end{bmatrix},$$

$$\mathbf{V}_{i3} = \begin{bmatrix}1 & 0 & 0\\ 0 & \cos\alpha_{i3} & -\sin\alpha_{i3}\\ 0 & \sin\alpha_{i3} & \cos\alpha_{i3}\end{bmatrix}, \tag{7b}$$



(a) The achievable rate pairs (b) Dispersion of the eigenvalues

Fig. 2. The effect of different distributions of the eigenvalues (λ_{ij}s) on the rate region with $n_t = 2$, $P = 20$, and $X \sim \mathcal{N}(0,1)$.

in which α_{ij}, $i \in \{0, c\}$ and $j \in \{1, 2, 3\}$, is the rotation angle corresponding to $\mathbf{V}_{ij}$.

C. Reformulated Optimization Problem

Replacing $\mathbf{Q}_0$ and $\mathbf{Q}_c$ of (3) in (2), the following expression of the capacity region, which is equivalent to the original one in (2), is obtained.

$$R_0 \leq \min\left\{\frac{1}{2}\log\left|\mathbf{I}_{n_r} + \frac{\mathbf{H}\mathbf{V}_0\mathbf{\Lambda}_0\mathbf{V}_0^T\mathbf{H}^T}{\mathbf{I}_{n_r} + \mathbf{H}\mathbf{V}_c\mathbf{\Lambda}_c\mathbf{V}_c^T\mathbf{H}^T}\right|,\right.$$

$$\left.\frac{1}{2}\log\left|\mathbf{I}_{n_e} + \frac{\mathbf{G}\mathbf{V}_0\mathbf{\Lambda}_0\mathbf{V}_0^T\mathbf{G}^T}{\mathbf{I}_{n_e} + \mathbf{G}\mathbf{V}_c\mathbf{\Lambda}_c\mathbf{V}_c^T\mathbf{G}^T}\right|\right\}, \tag{8a}$$

$$R_c \leq \frac{1}{2}\log\left|\mathbf{I}_{n_r} + \mathbf{H}\mathbf{V}_c\mathbf{\Lambda}_c\mathbf{V}_c^T\mathbf{H}^T\right|$$

$$- \frac{1}{2}\log\left|\mathbf{I}_{n_e} + \mathbf{G}\mathbf{V}_c\mathbf{\Lambda}_c\mathbf{V}_c^T\mathbf{G}^T\right|, \tag{8b}$$

$$\text{s.t.} \quad \sum_{j=1}^{n_t}(\lambda_{0j} + \lambda_{cj}) \leq P, \tag{8c}$$

$$\lambda_{0j} \geq 0,\ \lambda_{cj} \geq 0,\ j = 1, 2, \ldots, n_t. \tag{8d}$$

This alternative optimization problem, which is on variables λ_{0j} and $\lambda_{cj}, j \in \{1, 2, \ldots, n_t\}$, has two advantages: 1) it has removed positive semidefinite constrains of (2d), since $\mathbf{Q}_0$ and $\mathbf{Q}_c$ now satisfy those conditions by construction; 2) it has parameterized $\mathbf{Q}_0$ and $\mathbf{Q}_c$ with scalar parameters described in Section III-A (for $n_t = 2$) and Section III-B (for $n_t = 3$). Next, we can optimize power parameters and rotating angles instead of exhaustively searching for optimal $\mathbf{Q}_0$ and $\mathbf{Q}_c$.

IV. Solving the New Optimization Problem

With the new optimization problem (8), to find the capacity region we need to find the parameters (eigenvalues and angles) that optimize (8). To this end, different methods such as linear search [15] and evolutionary algorithm [16] can be used to find globally optimal parameters.[1] Such a method can, however, be time-consuming particularly when n_t is high. To increase the speed, we develop a nonlinear random search algorithm to find the parameters. Random search can be found in various optimization problems, e.g., genetic algorithm [18], gradient descent [19], deep neural networks [20], etc.

This algorithm generates power and angle parameters following specific distributions and then optimizes the rate pairs (R_0, R_c). Specifically, all angles are generated using independent uniform distribution between $[0, 2\pi)$. The power parameters λ_{ij}, $i \in \{0, c\}$ and $j \in \{1, \ldots, n_t\}$, are also generated independently and normalized to satisfy (8c). While it is intuitive to use uniform distribution for the angles, it is not clear what distribution best fits λ_{ij}s. We find this distribution empirically by running experiments with different distributions including $\lambda_{ij} \sim |X|^q$, $q \in \{1, \ldots, 10\}$, where X is the standard Gaussian distribution, i.e., $X \sim \mathcal{N}(0,1)$. It then appears that $q \in \{3, 4, 5\}$ rapidly produces diverse rate pairs (different points) close to the boundary of the capacity region, as visualized in Fig. 2(a) for some values of q. Very small and very large values of q, e.g., $q = 1$ and $q = 10$, do not provide as big region as $q = 3$. This is because the probability of reaching some power allocation in those cases is too low. For example, $q = 1$ (half-normal distribution) rarely reaches $[\lambda_{01}, \lambda_{02}, \lambda_{c1}, \lambda_{c2}] = [0, 0, 0, P]$ whereas $q = 10$ rarely reaches the central part of the region shown in Fig. 2(b).

The nonlinear search based on the fitted distributions results in a larger rate region than linear search because the regular searching step usually cannot come close to some boundary points, while randomly generated parameters will increase the diversity of the solution space. So, bringing in randomness in a judicious manner provides a higher chance to find points close to the boundary of the capacity in a faster way.

Algorithm 1 summarizes the evaluation of $\mathbf{Q}_0$ and $\mathbf{Q}_c$ and corresponding rate region for the PHY-SI. M is the number

[1] One may also use *semidefinite relaxation* (SDR) technique to solve (8) in the multiple-input single-output (MISO) case [17]. Our numerical evaluations, however, show that the performance of the SDR-based solution is comparable to that of the proposed method for a higher complexity.

Algorithm 1: Nonlinear Random Search Algorithm.

inputs: P, n_t, n_r, n_e, M, and N;
initialize: $m = 1$ and $n = 1$;
while $n \leq N$ **do**
  generate $\mathbf{H}$ and $\mathbf{G}$;
  while $m \leq M$ **do**
    generate $\lambda_{ij} = |X|^3$ where $X \sim \mathcal{N}(0, 1)$, $i \in \{0, c\}$, and $j \in \{1, \ldots, n_t\}$;
    if (8c) is true **then**
      generate rotation angles using $\mathrm{Uniform}[0, 2\pi)$;
      calculate $\mathbf{Q}_0$ and $\mathbf{Q}_c$ using (3);
      evaluate (8a) and (8b) to find (R_0, R_c);
      $m = m + 1$;
    end if
    smooth nth rate region via linear interpolation;
    $n = n + 1$;
  end while
  average the rate regions;
end while

of times $\mathbf{Q}_0$ and $\mathbf{Q}_c$ are generated, and N is the number of realizations of $\mathbf{H}$ and $\mathbf{G}$. We get closer to the capacity region as M increases. Also, as N increases, a more accurate statistical average of the capacity region is obtained. It is worth pointing out that averaging two different rate curves, corresponding to two sets of $\mathbf{H}$ and $\mathbf{G}$, in the rectangular coordinate system is challenging. Thus, we complete averaging (R_0, R_c) pairs in the polar system.

V. Numerical Results

In this section, we illustrate the performance of the proposed precoding scheme by numerical evaluation. We randomly generate 100 independent $\mathbf{H}$ and $\mathbf{G}$ whose entries are generated by i.i.d. $\mathcal{N}(0, 1)$. We consider two cases: Case I with $n_t = 2$; Case II with $n_t = 3$. Total power P in both cases is 20 W. We set $M = 10^3$ and $M = 10^4$ for the rotation-based precoding (both for the proposed and linear search) in Case I and Case II, respectively. For linear search, the eigenvalues steps are 1.2 (Case I) and 5 (Case II), and the angles steps are $\pi/8$ (Case I) and $\pi/3$ (Case II). Also, $M = 10^5$ (Case I) and $M = 10^6$ (Case II) are large enough to achieve the capacity region with the proposed search, and thus are referred to exhaustive search.

Figs. 3 and 4 show the secrecy rate region achieved by different strategies for $n_t = 2$ and $n_t = 3$, respectively. The gap between our rotation-based precoding (both with the proposed random search and linear search) and the capacity region is significantly smaller than that in GSVD-based precoding, particularly when $n_t = 2$. This is due to the fact that the rotation-based method is solving (8) which is equivalent representation of the capacity region in (2) whereas GSVD-based method developed in [7] is based on a simplification of the capacity region which is suboptimal.

Time consumption of different methods is listed in Table I. It is seen that the exhaustive and linear searches are much more time-consuming than GSVD-based precoding. Our proposed precoding scheme strikes a balance between complexity and performance. Further, it gives a systematic way of obtaining the capacity region as $M \to \infty$.

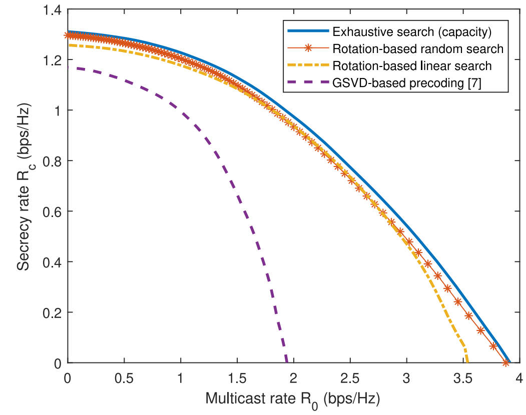


Fig. 3. Achievable secrecy and multicast rates with different precoding methods for $n_t = 2, n_r = 4$, and $n_e = 3$.

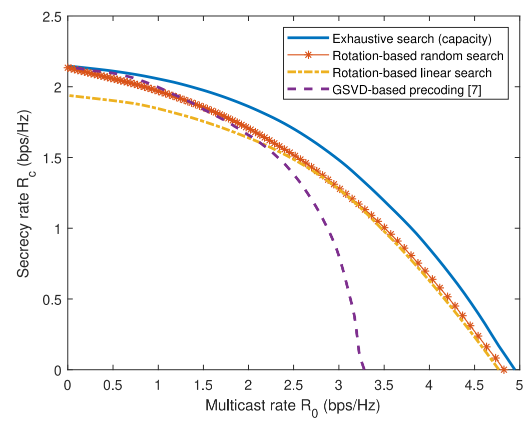


Fig. 4. Achievable secrecy and multicast rates with different precoding methods for $n_t = 3, n_r = 4$, and $n_e = 3$.

TABLE I
Average Execution Time for Different Precoding and Search Methods

	GSVD	**Rotation (proposed)**	**Rotation (linear)**	**Rotation (exhaustive)**
Case I	0.0121 s	0.06 s	3.41 s	5.92 s ($M = 10^5$)
Case II	0.0128 s	3.11 s	26.96 s	30.33 s ($M = 10^6$)

VI. Conclusion

We have developed a new method for precoding and power allocation for the MIMO-BC with multicast and confidential messages where the input covariance matrix is parameterized based on the rotation matrices and eigenvalues. To efficiently find the parameters, a nonlinear search algorithm exploiting the empirical distributions of the rotation angles and eigenvalues is developed. The proposed precoding significantly outperforms GSVD-based precoding in satisfying different users demand.

REFERENCES

[1] R. F. Schaefer and H. Boche, "Physical layer service integration in wireless networks: Signal processing challenges," *IEEE Signal Process. Mag.*, vol. 31, no. 3, pp. 147–156, May 2014.

[2] W. Mei, Z. Chen, J. Fang, and S. Li, "Physical layer service integration in 5G: Potentials and challenges," *IEEE Access*, vol. 6, pp. 16563–16575, 2018.

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

[4] H. Ly, T. Liu, and Y. Liang, "Multiple-input multiple-output Gaussian broadcast channels with common and confidential messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5477–5487, Nov. 2010.

[5] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2083–2114, Apr. 2011.

[6] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "MIMO Gaussian broadcast channels with confidential and common messages," in *Proc. IEEE Int. Symp. Inf. Theory*, 2010, pp. 2578–2582.

[7] W. Mei, Z. Chen, and J. Fang, "GSVD-based precoding in MIMO systems with integrated services," *IEEE Signal Process. Lett.*, vol. 23, no. 11, pp. 1528–1532, Nov. 2016.

[8] S. A. A. Fakoorian and A. L. Swindlehurst, "On the optimality of linear precoding for secrecy in the MIMO broadcast channel," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1701–1713, Sep. 2013.

[9] 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*, 2012, pp. 2321–2325.

[10] 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.

[11] M. Vaezi, W. Shin, and H. V. Poor, "Optimal beamforming for Gaussian MIMO wiretap channels with two transmit antennas," *IEEE Trans. Wireless Commun.*, vol. 16, no. 10, pp. 6726–6735, Oct. 2017.

[12] 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, Jun. 2009.

[13] 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*, 2017, pp. 1708–1712.

[14] X. Zhang, Y. Qi, and M. Vaezi, "A rotation-based method for precoding in Gaussian MIMOME channels," 2019, *arXiv:1908.00994*.

[15] S. S. Skiena, *The Algorithm Design Manual*, vol. 1. London, U.K.: Springer-Verlag, 1998.

[16] D. E. Goldberg, *Genetic Algorithms in Search, Optimization and Machine Learning.* Reading, MA, USA: Addison-Wesley, 1989.

[17] W. Mei, Z. Chen, and J. Fang, "Secrecy capacity region maximization in Gaussian MISO channels with integrated services," *IEEE Signal Process. Lett.*, vol. 23, no. 8, pp. 1146–1150, Aug. 2016.

[18] C. Ergun and K. Hacioglu, "Multiuser detection using a genetic algorithm in CDMA communications systems," *IEEE Trans. Commun.*, vol. 48, no. 8, pp. 1374–1383, Aug. 2000.

[19] M. Andrychowicz *et al.*, "Learning to learn by gradient descent by gradient descent," in *Proc. Adv. Neural Inf. Process. Syst.*, 2016, pp. 3981–3989.

[20] J. Bergstra and Y. Bengio, "Random search for hyper-parameter optimization," *J. Mach. Learn. Res.*, vol. 13, pp. 281–305, 2012.