2024 IEEE 100th Vehicular Technology Conference (VTC2024-Fall) | 979-8-3315-1778-6/24/$31.00 ©2024 IEEE | DOI: 10.1109/VTC2024-Fall63153.2024.10757455

On Minimizing Symbol Error Probability for Antipodal Beamforming in MIMO Gaussian Wiretap Channels

Nam Nguyen[1], An Vuong[1], Thuan Nguyen[2], and Thinh Nguyen[1]
[1]School of Electrical and Computer Engineering, Oregon State University, Corvallis, OR, 97331
[2]Department of Engineering, Engineering Technology, and Surveying, East Tennessee State University, Johnson, TN, 37604

***Abstract*—This paper investigates a beamforming scheme designed to minimize the symbol error probability (SEP) for a legitimate user while guaranteeing that the likelihood of an eavesdropper correctly recovering symbols remains below a predefined threshold. The focus is on finding an optimal beamforming vector for binary antipodal signal detection in multiple-input multiple-output (MIMO) Gaussian wiretap channels. Finding the optimal beamforming vector is a non-convex problem, and thus conventional computationally efficient algorithms for convex problems cannot be applied in this context. To that end, our proposed algorithm relies on Karush–Kuhn–Tucker (KKT) conditions and the generalized eigen-decomposition method to find an exact solution. The numerical results are presented to assess the performance of the proposed method for various scenarios.**

***Keywords*—Physical layer security, MIMO Gaussian wiretap channel, minimum symbol error probability, antipodal beamforming, KKT conditions, generalized eigen-decomposition.**

I. Introduction

The security of wireless communication has been a prominent concern. To that end, recent advancements in physical layer security, such as beamforming and artificial noise injection, have been proposed as effective strategies for enhancing wireless security [1]. These approaches leverage the information-theoretic secrecy properties of physical communication channels, initially pioneered by Wyner for the wiretap channel [2]. In this context, the transmitter, Alice, wants to transmit confidential information to the legitimate receiver, Bob, while protecting it from potential eavesdroppers like Eve. Wyner demonstrates that, it is feasible to establish a reliable and secure communication channel in the presence of eavesdroppers, particularly when the eavesdropper's signal-to-noise ratio (SNR) is lower than that of the legitimate receiver.

As high-capacity multiple-input-multiple-output (MIMO) communication systems have evolved, numerous studies have effectively characterized the secrecy capacity of such systems. Secrecy capacity is the maximum transmission rate at which the eavesdropper cannot decipher any information. In this paper, instead of secrecy capacity, a beamforming scheme is designed to minimize the symbol error probability (SEP) for a legitimate user while guaranteeing that the likelihood of an eavesdropper correctly recovering symbols remains below a predefined threshold. Specifically, this paper is focused on finding an optimal beamforming vector for binary antipodal signal detection in MIMO Gaussian wiretap channels. Finding the optimal beamforming vector is a non-convex problem, and thus conventional computationally efficient algorithms for convex problems cannot be applied in this context. To that end, our proposed algorithm relies on Karush–Kuhn–Tucker (KKT) conditions and the generalized eigen-decomposition method to find an exact solution. The numerical results are presented to assess the performance of the proposed method for various scenarios.

II. Related Work

Some representative efforts to obtain closed-form solutions for the secrecy capacity of the MIMO Gaussian wiretap channel are discussed in [3], [4]. Various approaches aiming to achieve secrecy capacity have concentrated on the determination of the transmit covariance matrix [5], [6]. These solutions employ iterative procedures to tackle the non-convexity nature of the problem. To reduce complexity, linear beamforming techniques have also been proposed to exploit transmit diversity via weighting the information stream [7], [8]. While secrecy capacity serves as a common metric, its practical realization and measurement pose challenges in real-world scenarios utilizing practical non-Gaussian codes. In contrast, we describe an optimization framework for finding an optimal beamforming vector that minimizes the symbol error rate rather than secrecy capacity. To the best of the author's knowledge, there has been no study considering the SEP minimization-based beamforming scheme for MIMO Gaussian wiretap channel.

III. MIMO beamforming in Gaussian wiretap channel

In this section, we characterize symbol error probability-based MIMO beamforming for binary antipodal signal detection and present the MIMO Gaussian wiretap channel.

A. Symbol Error Probability

Consider a MIMO communication system with N transmit antennas and K receive antennas. The MIMO received signal $\mathbf{y}$ can be expressed as:

$$\mathbf{y} = \mathbf{HWs} + \mathbf{n}, \tag{1}$$

where $\mathbf{H} \in \mathbb{C}^{K\times N}$ is the channel matrix between transmitter and receiver, $\mathbf{W} \in \mathbb{C}^{N\times M}$ is the beamforming matrix. M is

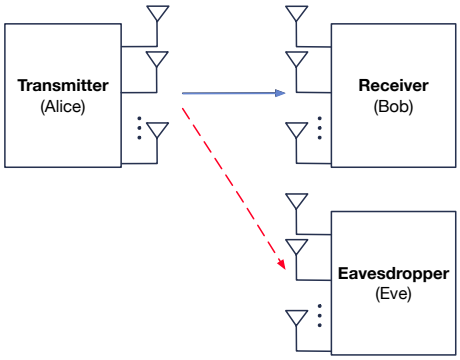


Fig. 1: MIMO Gaussian wiretap channel.

the number of information symbols and M does not exceed $\min\{N, K\}$. $\mathbf{s} = [s_1, ..., s_M]^T$ is the information intended for the receiver, $\mathbf{n} \in \mathbb{C}^K \sim \mathcal{CN}(0, N_0\mathbf{I})$ is the complex Gaussian noise. For analysis, we assume $\mathbf{H}$ is known, i.e., the full channel state information is available at both the transmitter and receiver side [9]–[11].

Binary Antipodal Signal Detection. In this paper, we limit our discussion to sending binary antipodal signals, i.e., $\mathbf{s} \in \{\mathbf{a}, -\mathbf{a}\}$, where $\mathbf{a} = [a_1, ..., a_M]^T$ is an arbitrary complex M-dimensional vector and $a_1, ..., a_M$ are discrete constellation points.

To determine whether $\mathbf{a}$ or -$\mathbf{a}$ was sent given that $\mathbf{y}$ is received, we use the following maximum a posteriori probability (MAP) test [12]:

$$\begin{cases} \dfrac{\Re\{\mathbf{y}^H(\mathbf{HWa})\}}{\|\mathbf{HWa}\|} \geq 0 \ \text{ if } \ \hat{\mathbf{s}} = \mathbf{a}, & \text{(2a)} \\ \dfrac{\Re\{\mathbf{y}^H(\mathbf{HWa})\}}{\|\mathbf{HWa}\|} < 0 \ \text{ if } \ \hat{\mathbf{s}} = -\mathbf{a}, & \text{(2b)} \end{cases}$$

where $\hat{\mathbf{s}}$ is the detected signal of $\mathbf{s}$. We assume the prior probabilities of the two signals $\mathbf{a}$ and $-\mathbf{a}$ to be equal. Thus, the error probabilities are the same whether the symbol vector $\mathbf{a}$ or $-\mathbf{a}$ was transmitted and can be derived as follows

$$\begin{aligned} P_e &= P(\hat{\mathbf{s}} = \mathbf{a}|\mathbf{s} = -\mathbf{a}) = P(\hat{\mathbf{s}} = -\mathbf{a}|\mathbf{s} = \mathbf{a}), \\ &= Q\left(\frac{\| \mathbf{HWa} \|_2}{\sqrt{N_0/2}}\right). \end{aligned} \quad (3)$$

where $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\frac{t^2}{2}} dt$ is the Gaussian Q-function.

B. MIMO Gaussian Wiretap Channel

The MIMO wiretap channel is shown in Fig. 1. The number of antennas at the transmitter (Alice), the legitimate receiver (Bob), and the eavesdropper (Eve) are N, K_B, and K_E, respectively. We call the channel between Alice and Bob the primary channel ($\mathbf{H}_B \in \mathbb{C}^{K_B \times N}$), while the channel between Alice and Eve is the eavesdropper channel ($\mathbf{H}_E \in \mathbb{C}^{K_E \times N}$). In this scenario, Alice transmits her confidential message to Bob, and Eve eavesdrops on the information being conveyed from Alice to Bob without causing any disruption to the primary channel [2]–[4].

Following the system model from Eq. (1), the received signals at Bob and Eve are:

$$\mathbf{y}_B = \mathbf{H}_B\mathbf{Ws} + \mathbf{n}_B, \quad (4)$$

$$\mathbf{y}_E = \mathbf{H}_E\mathbf{Ws} + \mathbf{n}_E, \quad (5)$$

where $\mathbf{s} \in \{\mathbf{a}, -\mathbf{a}\}$. $\mathbf{n}_B \sim \mathcal{CN}(0, N_B\mathbf{I})$ and $\mathbf{n}_E \sim \mathcal{CN}(0, N_E\mathbf{I})$ are the zero-mean complex Gaussian white noises with powers N_B and N_E for the channels of Bob and Eve, respectively. Furthermore, the input signal is subjected to a power constraint P such that $\text{Tr}(\mathbf{WW}^H) \leq P$ [13], [14].

IV. SEP Minimization for Binary Antipodal Beamforming

A. Problem Formulation

We focus on enhancing reliability and signal-to-noise ratio rather than maximizing the bit rate. Hence, we investigate a special case of binary antipodal signals, where the information symbols are $\pm a$ with $a \in \mathbb{C}$ are discrete constellation points. We can express the binary antipodal signals as $\mathbf{s} = \mathbf{w}a$ or $\mathbf{s} = \mathbf{w}(-a)$, where $\mathbf{w} \in \mathbb{C}^N$ is the beamforming vector.

Based on (3), the error probabilities of Bob and Eve are $P_e^B = Q\left(\| \mathbf{H}_B\mathbf{w}a \|_2 / \sqrt{N_B/2}\right)$ and $P_e^E = Q\left(\| \mathbf{H}_E\mathbf{w}a \|_2 / \sqrt{N_E/2}\right)$, respectively.

Our objective is to minimize Bob's error probability while ensuring that Eve's error probability exceeds a predetermined threshold, all while meeting the power constraint. Consequently, we formulate the following optimization problem:

$$\min_{\mathbf{w}} \quad Q\left(\frac{\| \mathbf{H}_B\mathbf{w}a \|_2}{\sqrt{N_B/2}}\right) \quad (6a)$$

$$\text{s.t.} \quad Q\left(\frac{\| \mathbf{H}_E\mathbf{w}a \|_2}{\sqrt{N_E/2}}\right) \geq D, \quad (6b)$$

$$\|\mathbf{w}\|_2^2 \leq P, \quad (6c)$$

where $\mathbf{H}_B \in \mathbb{C}^{K_B \times N}$, $\mathbf{H}_E \in \mathbb{C}^{K_E \times N}$, $\mathbf{w} \in \mathbb{C}^N$, $a \in \mathbb{C}$, $D \in [0, 0.5]$, and $P > 0$ is the transmitted signal power.

Let $\bar{\mathbf{w}} = \frac{\mathbf{w}}{\sqrt{P}}$, the problem (6) can be rewritten as

$$\min_{\bar{\mathbf{w}}} \quad Q\left(\sqrt{2P/N_B} \| \mathbf{H}_B\bar{\mathbf{w}}a \|_2\right) \quad (7a)$$

$$\text{s.t.} \quad Q\left(\sqrt{2P/N_E} \| \mathbf{H}_E\bar{\mathbf{w}}a \|_2\right) \geq D, \quad (7b)$$

$$\|\bar{\mathbf{w}}\|_2^2 \leq 1, \quad (7c)$$

Due to the Gaussian Q-function being a strictly decreasing function, an equivalent problem of (7) is:

$$\min_{\bar{\mathbf{w}}} \quad - \| \mathbf{H}_B\bar{\mathbf{w}} \|_2^2 \quad (8a)$$

$$\text{s.t.} \quad \| \mathbf{H}_E\bar{\mathbf{w}} \|_2^2 \leq \left(\sqrt{N_E/(2P)}Q^{-1}(D)/|a|\right)^2, \quad (8b)$$

$$\|\bar{\mathbf{w}}\|_2^2 \leq 1, \quad (8c)$$

The objective of the problem (8) is a concave function, where the feasible space of this problem is compact and convex.

Therefore, an optimal solution must lie at extreme points [15]. Finding these extreme points is challenging, hence KKT conditions are used to develop an efficient algorithm.

B. KKT Conditions

The gradient of the Lagrangian can be derived as follows

$$\nabla_{\bar{\mathbf{w}}}\mathcal{L}(\bar{\mathbf{w}},\lambda_1,\lambda_2) = 2(\lambda_1\mathbf{H}_E^H\mathbf{H}_E - \mathbf{H}_B^H\mathbf{H}_B)\bar{\mathbf{w}} + 2\lambda_2\bar{\mathbf{w}}. \quad (9)$$

Therefore, the KKT conditions of the problem (8) are:

$$\|\mathbf{H}_E\bar{\mathbf{w}}^*\|_2^2 - \left(\frac{\sqrt{N_E/(2P)}Q^{-1}(D)}{|a|}\right)^2 \leq 0, \quad (10a)$$

$$\|\bar{\mathbf{w}}^*\|_2^2 - 1 \leq 0, \quad (10b)$$

$$\lambda_1^*, \lambda_2^* \geq 0, \quad (10c)$$

$$\lambda_1^*\left(\|\mathbf{H}_E\bar{\mathbf{w}}^*\|_2^2 - \left(\frac{\sqrt{N_E/(2P)}Q^{-1}(D)}{|a|}\right)^2\right) = 0, \quad (10d)$$

$$\lambda_2^*\left(\|\bar{\mathbf{w}}^*\|_2^2 - 1\right) = 0, \quad (10e)$$

$$(\lambda_1^*\mathbf{H}_E^H\mathbf{H}_E - \mathbf{H}_B^H\mathbf{H}_B)\bar{\mathbf{w}}^* + \lambda_2^*\bar{\mathbf{w}}^* = 0. \quad (10f)$$

An optimal solution must satisfy the KKT conditions. There are 4 cases corresponding to the possibly optimal values of λ_1^* and λ_2^*.

- Case 1: For $\lambda_1^* = 0$ and $\lambda_2^* = 0$,

$$\|\mathbf{H}_E\bar{\mathbf{w}}^*\|_2^2 - \left(\sqrt{N_E/(2P)}Q^{-1}(D)/|a|\right)^2 < 0, \quad (11a)$$

$$\|\bar{\mathbf{w}}^*\|_2^2 - 1 < 0, \quad (11b)$$

$$(\mathbf{H}_B^H\mathbf{H}_B)\bar{\mathbf{w}}^* = \mathbf{0}. \quad (11c)$$

- Case 2: For $\lambda_1^* = 0$ and $\lambda_2^* > 0$,

$$\|\mathbf{H}_E\bar{\mathbf{w}}^*\|_2^2 - \left(\sqrt{N_E/(2P)}Q^{-1}(D)/|a|\right)^2 < 0, \quad (12a)$$

$$\|\bar{\mathbf{w}}^*\|_2^2 - 1 = 0, \quad (12b)$$

$$\mathbf{H}_B^H\mathbf{H}_B\bar{\mathbf{w}}^* = \lambda_2^*\bar{\mathbf{w}}^*. \quad (12c)$$

- Case 3: For $\lambda_1^* > 0$ and $\lambda_2^* = 0$,

$$\|\mathbf{H}_E\bar{\mathbf{w}}^*\|_2^2 - \left(\sqrt{N_E/(2P)}Q^{-1}(D)/|a|\right)^2 = 0, \quad (13a)$$

$$\|\bar{\mathbf{w}}^*\|_2^2 - 1 < 0, \quad (13b)$$

$$\mathbf{H}_B^H\mathbf{H}_B\bar{\mathbf{w}}^* = \lambda_1^*\mathbf{H}_E^H\mathbf{H}_E\bar{\mathbf{w}}^*. \quad (13c)$$

- Case 4: For $\lambda_1^* > 0$ and $\lambda_2^* > 0$,

$$\|\mathbf{H}_E\bar{\mathbf{w}}^*\|_2^2 - \left(\sqrt{N_E/(2P)}Q^{-1}(D)/|a|\right)^2 = 0, \quad (14a)$$

$$\|\bar{\mathbf{w}}^*\|_2^2 - 1 = 0, \quad (14b)$$

$$(\mathbf{H}_B^H\mathbf{H}_B - \lambda_1^*\mathbf{H}_E^H\mathbf{H}_E)\bar{\mathbf{w}}^* = \lambda_2^*\bar{\mathbf{w}}^*. \quad (14c)$$

C. Beamforming Design Algorithm

For our problem, the solutions should be achieved at extreme points, i.e., optimal points have to be on the boundary of constraint sets, as mentioned above. Therefore, case 1 is removed since its feasible points belong inside of constraint sets. It noted that we can find the optimal exact solution for $\bar{\mathbf{w}}$ by investigating through the cases 2, 3, and 4, separately.

For cases 2 and 3, the solutions can be obtained by solving the generalized eigenvalue problems as $\mathbf{H}_B^H\mathbf{H}_B\bar{\mathbf{w}} = \lambda_2\bar{\mathbf{w}}$ and $\mathbf{H}_B^H\mathbf{H}_B\bar{\mathbf{w}} = \lambda_1\mathbf{H}_E^H\mathbf{H}_E\bar{\mathbf{w}}$, respectively. For case 4, an exhaustive search entails a grid search through all possible values of λ_1 in the interval $[0, L]$ with a resolution of ϵ. Here, L represents the size of the search space. The optimal solution is obtained by solving the eigenvalue problem $(\mathbf{H}_B^H\mathbf{H}_B - \lambda_1\mathbf{H}_E^H\mathbf{H}_E)\bar{\mathbf{w}} = \lambda_2\bar{\mathbf{w}}$ for each λ_1. Subsequently, the solutions for $\bar{\mathbf{w}}$ are checked to ensure they meet the provided constraints. For a detailed algorithm, please refer to Algorithm 1.

Time complexity of Algorithm 1. In terms of complexity, our proposed algorithm involves finding all eigenvalues for a dense $N \times N$ matrix, which is of $O(N^3)$. Additionally, in case 4, we need to search through λ_1, adding to the complexity. Therefore, the overall complexity of our algorithm can be expressed as $O(LN^3)$, where L represents the size of the search space.

Algorithm 1 Antipodal Beamforming.

Input: $\mathbf{H}_B$, $\mathbf{H}_E$, N_B, N_E, D, P, a

Consider cases 2, 3, and 4 to determine the optimal $\bar{\mathbf{w}}^*$

Case 2:

Find eigenvector set, $\mathbb{E}_2$, corresponding to $\mathbf{H}_B^H\mathbf{H}_B\bar{\mathbf{w}} = \lambda_2\bar{\mathbf{w}}$

if $\lambda_2 > 0$ and $\bar{\mathbf{w}}_2 \in \mathbb{E}_2$ minimizes (7a) and satisfies (12a), (12b) **then**

  $P_{e_2}^B = Q\left(\sqrt{2P/N_B} \parallel \mathbf{H}_B\bar{\mathbf{w}}_2 a \parallel_2\right)$

else

  $P_{e_2}^B = +\infty$

end if

Case 3:

Find generalized eigenvector set, $\mathbb{E}_3$, corresponding to $\mathbf{H}_B^H\mathbf{H}_B\bar{\mathbf{w}} = \lambda_1\mathbf{H}_E^H\mathbf{H}_E\bar{\mathbf{w}}$

if $\lambda_1 > 0$ and $\bar{\mathbf{w}}_3 \in \mathbb{E}_3$ minimizes (7a) and satisfies (13a), (13b) **then**

  $P_{e_3}^B = Q\left(\sqrt{2P/N_B} \parallel \mathbf{H}_B\bar{\mathbf{w}}_3 a \parallel_2\right)$

else

  $P_{e_3}^B = +\infty$

end if

Case 4:

Exhaustive search with the resolution of ϵ through all values of $\lambda_1 \in [0, L]$

For each value of λ_1, find eigenvector set, $\mathbb{E}_4$, corresponding to $(\mathbf{H}_B^H\mathbf{H}_B - \lambda_1\mathbf{H}_E^H\mathbf{H}_E)\bar{\mathbf{w}} = \lambda_2\bar{\mathbf{w}}$

if $\lambda_2 > 0$ and $\bar{\mathbf{w}}_4 \in \mathbb{E}_4$ minimizes (7a) and satisfies (14a), (14b) **then**

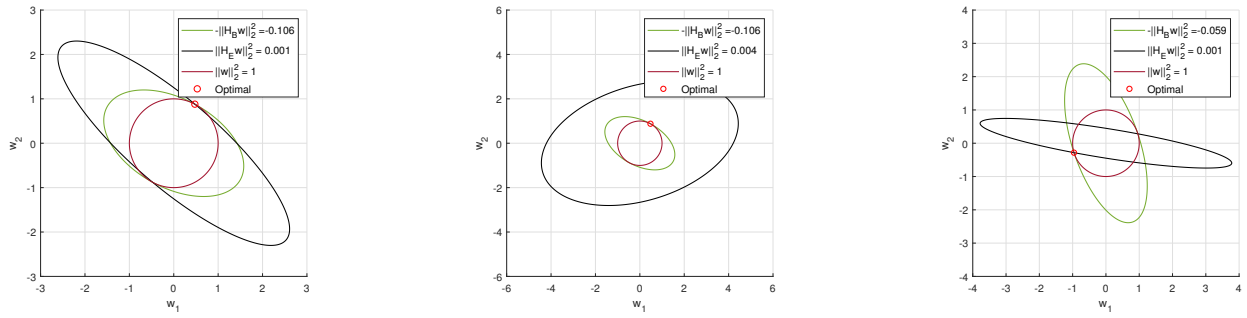
  $P_{e_4}^B = Q\left(\sqrt{2P/N_B} \parallel \mathbf{H}_B\bar{\mathbf{w}}_4 a \parallel_2\right)$

else

  $P_{e_4}^B = +\infty$

end if

Output: $\bar{\mathbf{w}}^* = \bar{\mathbf{w}}_{i^*}$ where $i^* = \min_i P_{e_i}^B = \min_i(P_{e_2}^B, P_{e_3}^B, P_{e_4}^B)$ and $\bar{\mathbf{w}}_i \in \{\bar{\mathbf{w}}_2, \bar{\mathbf{w}}_3, \bar{\mathbf{w}}_4\}$



(a) Setup 1 (b) Setup 2 (c) Setup 3

Fig. 2: Illustration of the optimal case of (a) setup 1, (b) setup 2, and setup 3 in $\mathbb{R}^2$.

D. Case Analysis

We present the analytical results based on different cases in Section IV-B. To simplify the analysis, the real-valued deterministic channel matrices are used. Figure 2 shows the objective function contours and constraint boundaries of three different setups. Note that in all three figures, the symmetry of the quadratic objective function determines two symmetric optimal points. Also, all the optimal points are the extreme points as predicted for an optimization problem with a concave objective the feasible space is compact and convex set.

Setup 1. We consider the system parameters as $\mathbf{H}_B = \begin{bmatrix} 0.21 & 0.011 \\ 0.09 & 0.3 \end{bmatrix}$, $\mathbf{H}_E = \begin{bmatrix} 0.01 & 0.02 \\ 0.017 & 0.01 \end{bmatrix}$, $D = 0.346$, $P = 1$ W, $N_B = N_E = 0.01$ W, $N = K_B = K_E = M = 2$. BPSK modulation constellations are used as $a \in \{-1, 1\}$. For case 2, $P_{e_2}^B = 0.0035$, $P_{e_2}^E = 0.4427$ (i.e., the error probability of Eve), $\bar{\mathbf{w}}_2 = \begin{bmatrix} -0.8784 & 0.4779 \end{bmatrix}^T$, and $\lambda_2 = 0.0363$. For case 3, there exists no $\bar{\mathbf{w}}_3$ that satisfies the constraint (13a). For case 4, $P_{e_4}^B = 2.0542 \times 10^{-6}$, $P_{e_2}^E = 0.346$, $\bar{\mathbf{w}}_4 = \begin{bmatrix} 0.475 & 0.88 \end{bmatrix}^T$, $\lambda_1 = 1.5$, and $\lambda_2 = 0.0361$. Overall, case 4 is selected and presented in Figure 2a. Despite similar channel matrix directions for Bob and Eve in Figure 2a, Eve's error probability worsens due to her channel's high attenuation coefficient. Case 4 is rare in practice as optimal points must be among extreme points generated by specific constraints.

Setup 2. The same setting parameters as the setup 1 are considered, except $\mathbf{H}_B = \begin{bmatrix} 0.21 & 0.011 \\ 0.09 & 0.3 \end{bmatrix}$, $\mathbf{H}_E = \begin{bmatrix} -0.01 & 0.02 \\ 0.01 & 0.01 \end{bmatrix}$, and $D = 0.2$. For case 2, $P_{e_2}^B = 2.0541 \times 10^{-6}$, $P_{e_2}^E = 0.3960$, $\bar{\mathbf{w}}_2 = \begin{bmatrix} 0.4779 & 0.8784 \end{bmatrix}^T$, and $\lambda_2 = 0.1061$. For case 3 and case 4, there exists no $\bar{\mathbf{w}}_3$ and $\bar{\mathbf{w}}_4$ that satisfies the constraint (13a) and (14a), respectively. Hence, we choose case 2 and describe in Figure 2b. In this scenario, Bob and Eve's channel matrices are highly orthogonal. Using the beamforming vector directs the signal mainly to Bob, reducing Bob's error probability but increasing Eve's.

Setup 3. We keep the same setting parameters as the setup 1, except $\mathbf{H}_B = \begin{bmatrix} 0.21 & 0.015 \\ 0.1 & 0.12 \end{bmatrix}$, $\mathbf{H}_E = \begin{bmatrix} 0.01 & 0.071 \\ 0.01 & 0.01 \end{bmatrix}$, and $D = 0.3246$. For case 2 and case 3, there exists no $\bar{\mathbf{w}}_2$ and $\bar{\mathbf{w}}_3$ that satisfies the constraint (12a) and (13a), respectively. For case 4, $P_{e_4}^B = 2.9105 \times 10^{-4}$ with respect to $\lambda_1 = 1$ and $\lambda_2 = 0.0053$. $P_{e_4}^E = 0.3246$ and $\bar{\mathbf{w}}_4 = \begin{bmatrix} -0.9592 & -0.2828 \end{bmatrix}^T$. Accordingly, case 4 is selected and represented in Figure 2c.

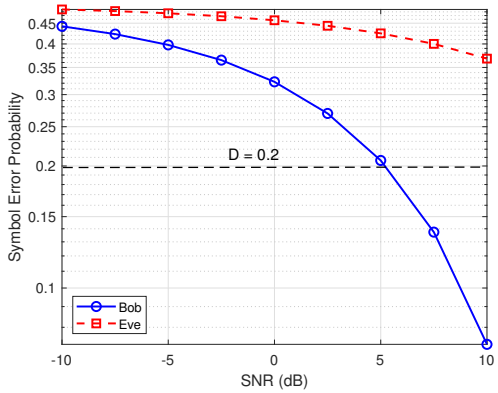


Fig. 3: Symbol error probability comparison of Bob and Eve versus SNR in deterministic real orthogonal direction channels.

V. Numerical Results

This section presents numerical results illustrating the symbol error probability of MIMO Gaussian wiretap channels. These results are obtained using the proposed antipodal beamforming scheme in Algorithm 1.

In Figure 3, we analyze Bob and Eve's symbol error probability comparison versus SNR, where $N = K_B = K_E = M = 2$. The BPSK modulation is utilized with $a \in \{-1, 1\}$, $D = 0.2$, and $N_B = N_E = 0.1$ W. Here, we consider $\mathbf{H}_B = \begin{bmatrix} 0.21 & 0.011 \\ 0.09 & 0.3 \end{bmatrix}$ and $\mathbf{H}_E = \begin{bmatrix} -0.21 & 0.011 \\ -0.09 & 0.3 \end{bmatrix}$ as deterministic orthogonal direction channels. A notable trend observed for both Bob and Eve is that their performance improves considerably with increasing SNR. Nevertheless, Bob exhibits a lower symbol error probability compared to Eve. This difference arises from the beamforming vector being optimized to direct the information signal towards Bob.

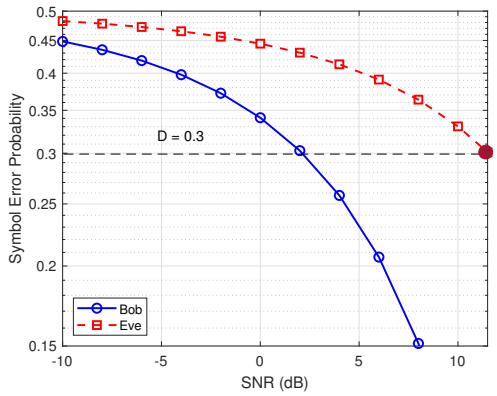


Fig. 4: Symbol error probability comparison of Bob and Eve versus SNR in deterministic real Gaussian channels.

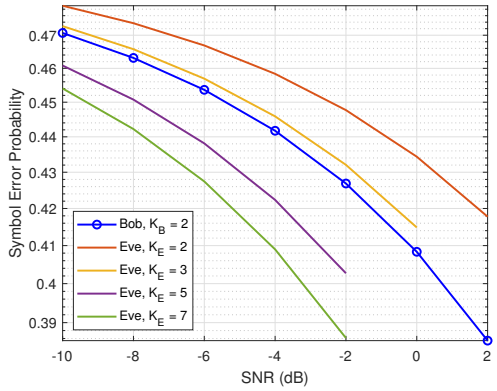


Fig. 5: Symbol error probability of Bob and Eve versus SNR with varying K_E in stochastic real Gaussian channels.

Figure 4 illustrates a comparison of symbol error probabilities for Bob and Eve as a function of SNR, using the same configuration as in Figure 3. Here, we set $D = 0.3$, $N_B = N_E = 0.01$ W, and consider $\mathbf{H}_B = \begin{bmatrix} 0.0262 & 0.0049 \\ -0.1598 & -0.2414 \end{bmatrix}$ and $\mathbf{H}_E = \begin{bmatrix} 0.0498 & 0.0194 \\ -0.0446 & -0.0758 \end{bmatrix}$ as deterministic real Gaussian channels. Consistent with the observations in Figure 3, Bob's performance significantly outperforms Eve's. It should be noted that constraints (13a) and (14a) only become active at the brown point. Furthermore, as the SNR increases, none of the scenarios under consideration yield a feasible solution.

The effect of increasing the number of antennas at the eavesdropper is illustrated in Figure 5 using the same setup as in Figure 4. This result is obtained by averaging over realizations of stochastic real Gaussian channels where $h_{ij} \in \mathcal{N}(0, 0.01)$. The symbol error probability of Eve is observed to decrease as the number of antennas increases. For $K_E \geq 5$, Eve's performance is notably high, indicating that she can intercept almost all information from Alice. This phenomenon occurs because beamforming is no longer effective at degrading the eavesdropper's reception in this scenario. Thus, the assurance of information security through physical layer techniques is not guaranteed in such circumstances.

VI. Conclusion

This paper has presented a new beamforming scheme for MIMO Gaussian wiretap channels, aiming to minimize the symbol error probability for legitimate users while limiting the eavesdropper's ability to recover symbols above a predefined threshold. The proposed algorithm, based on Karush-Kuhn-Tucker conditions and the generalized eigen-decomposition method, offers an exact solution to the non-convex optimization problem. Through extensive numerical simulations, we have demonstrated the efficacy of our approach across various scenarios.

References

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

[2] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal,* vol. 54, no. 8, pp. 1355–1387, 1975.

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

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

[5] 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 Journal on Selected Areas in Communications,* vol. 31, no. 9, pp. 1714–1727, Sep. 2013.

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

[7] S. A. A. Fakoorian and A. L. Swindlehurst, "Optimal power allocation for GSVD-based beamforming in the MIMO Gaussian wiretap channel," *2012 IEEE International Symposium on Information Theory Proceedings,* Cambridge, MA, USA, 2012, pp. 2321-2325.

[8] M. Vaezi, W. Shin and H. V. Poor, "Optimal Beamforming for Gaussian MIMO Wiretap Channels With Two Transmit Antennas," *IEEE Transactions on Wireless Communications,* vol. 16, no. 10, pp. 6726-6735, Oct. 2017.

[9] H. Sung, S.. -R. Lee and I. Lee, "Generalized Channel Inversion Methods for Multiuser MIMO Systems," *in IEEE Transactions on Communications,* vol. 57, no. 11, pp. 3489-3499, Nov. 2009.

[10] V. Stankovic and M. Haardt, "Generalized Design of Multi-User MIMO Precoding Matrices," *in IEEE Transactions on Wireless Communications,* vol. 7, no. 3, pp. 953-961, March 2008.

[11] B. M. Hochwald, C. B. Peel and A. L. Swindlehurst, "A vector-perturbation technique for near-capacity multiantenna multiuser communication-part II: perturbation," *in IEEE Transactions on Communications,* vol. 53, no. 3, pp. 537-544, March 2005.

[12] Robert G Gallager, "Principles of Digital Communication." *Cambridge University Press,* 2008.

[13] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober and I. B. Collings, "Transmit Antenna Selection for Security Enhancement in MIMO Wiretap Channels," *in IEEE Transactions on Communications,* vol. 61, no. 1, pp. 144-154, January 2013.

[14] J. Chakravarty, O. Johnson, and R. Piechocki, "A Convex Scheme for the Secrecy Capacity of a MIMO Wiretap Channel with a Single Antenna Eavesdropper," *ICC 2019 - 2019 IEEE International Conference on Communications (ICC),* Shanghai, China, 2019, pp. 1-5.

[15] Tuy, H., T. V. Thieu, and Ng. Q. Thai, "A Conical Algorithm for Globally Minimizing a Concave Function over a Closed Convex Set," *Mathematics of Operations Research,* 10, no. 3 (1985): 498–514.