Frontiers of Information Technology & Electronic Engineering
www.zju.edu.cn/jzus; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

Correlated channel model-based secure communications in dual-hop wireless communication networks*

Zhen-hua YUAN†1, Chen CHEN†1, Xiang CHENG1, Guo-cheng LV1,
Liu-qing YANG†2, Ye JIN1

(1State Key Laboratory of Advanced Optical Communication Systems and Networks,
Peking University, Beijing 100871, China)

(2Department of Electrical & Computer Engineering, Colorado State University, Fort Collins, CO 80523, USA)

†E-mail: yuanzhenhua@pku.edu.cn; c.chen@pku.edu.cn; lqyang@engr.colostate.edu

Received Jan. 9, 2017; Revision accepted Mar. 14, 2017; Crosschecked June 1, 2017

Abstract: This article is focused on secure relay beamformer design with a correlated channel model in the relay-eavesdropper network. In this network, a single-antenna source-destination pair transmits secure information with the help of an amplify-and-forward (AF) relay equipped with multiple antennas, and the legitimate and eavesdropping channels are correlated. The relay cannot obtain the instantaneous channel state information (CSI) of the eavesdropper, and has only the knowledge of correlation information between the legitimate and eavesdropping channels. Depending on this information, we derive the conditional distribution of the eavesdropping channel. Two beamformers at the relay are studied for the approximate ergodic secrecy rate: (1) the generalized match-and-forward (GMF) beamformer to maximize the legitimate channel rate, and (2) the general-rank beamformer (GRBF). In addition, one lower-bound-maximizing (LBM) beamformer at the relay is discussed for maximizing the lower bound of the ergodic secrecy rate. We find that the GMF beamformer is the optimal rank-one beamformer, that the GRBF is the iteratively optimal beamformer, and that the performance of the LBM beamformer for the ergodic secrecy rate gets close to that of the GRBF for the approximate secrecy rate. It can also be observed that when the relay has lower power or the channel gain of the second hop is low, the performance of the GMF beamformer surpasses that of the GRBF. Numerical results are presented to illustrate the beamformers' performance.

Key words: Physical layer security; Relay beamforming; Correlated channels; Ergodic secrecy rate
http://dx.doi.org/10.1631/FITEE.1700023 **CLC number:** TN925.1

1 Introduction

Security is an important aspect of a wireless communication system due to the broadcast nature of radio propagation. In the past, secure communication in wireless networks was typically guaranteed by using cryptographic algorithms implemented at higher network layers. Recently, physical layer security has drawn much attention, because it can protect wireless communications from eavesdropping by exploiting the physical characteristics of wireless channels.

Wyner (1975) proposed the wiretap channel model, and proved that when the wiretap channel is a degraded version of the main source-destination channel, the source could send secret messages to the destination without leaking any information to the eavesdropper, by exploiting the physical properties of the channel. Leung-Yan-Cheong and Hellman (1978) and Csiszár and Korner (1978) generalized Wyner's approach to scenarios with Gaussian

* Project supported by the National Natural Science Foundation of China (Nos. 61471008, 61571020, and 61622101) and the National Key Research and Development Project of China (No. 2016YFE0123100)

ORCID: Zhen-hua YUAN, http://orcid.org/0000-0003-3619-4831 channels and broadcast channels, respectively.

However, physical layer security was not really attractive to researchers during the 1980s and 1990s. In a single-antenna system, the secrecy rate is typically zero when the legitimate channel is worse than the eavesdropping channel. To avoid this limitation, in recent years, many studies have been conducted by taking advantage of cooperative communications (Dong *et al.*, 2010; Krikidis, 2010; Chen, 2011; Li *et al.*, 2011; Lee, 2015; Wang *et al.*, 2015; Zhang M *et al.*, 2016; Zhang R *et al.*, 2016a; 2016b). Cooperative issues via spectrum sharing in device-to-device networks were analyzed in a few reports (Zhang R *et al.*, 2016a; 2016b). Four cooperative schemes, decode-and-forward (DF), amplify-and-forward (AF), compress-and-forward (CF), and cooperative jamming (CJ), have been studied by Li *et al.* (2011), Dong *et al.* (2010), Chen (2011), and Lee (2015), respectively. Optimal relay weights have been derived for maximizing the secrecy rate or minimizing the power consumption of the relays. Krikidis (2010) studied the opportunistic relay selection techniques when an instantaneous knowledge or an average knowledge of the eavesdropper channels is known to the relays. Wang *et al.* (2015) designed the optimal and suboptimal relay selection algorithms for backscatter wireless communication systems under the information security constraint.

Most of the previous works on relay wireless networks assumed that the legitimate channel and the wiretap channel are independent. However, in practical scenarios, correlations between channels usually exist (McKay and Collings, 2005; Tulino *et al.*, 2005; Cheng *et al.*, 2012; Geraci *et al.*, 2013; Ghose and Bose, 2013; Ferdinand *et al.*, 2014; Yin and Cheng, 2016), depending on antenna deployments, scatters around the legitimate receiver and eavesdropper, and so on. Tulino *et al.* (2005) studied the impact of antenna correlation on the trade-offs among power, bandwidth, and channel capacity. Using transmit antenna selection (TAS), Ferdinand *et al.* (2014) investigated the secrecy performance of multiple-input single-output (MISO) wiretap channels when the eavesdropper channel is correlated with the main one. The issue of transmit power minimization under the correlated Rayleigh fading model was addressed by Ghose and Bose (2013). Geraci *et al.* (2013) studied the precoding schemes for broadcast channels under transmit side channel correlation.

In this study, for the first time, we have investigated the beamforming schemes to maximize the secrecy capacity of a wireless dual-hop AF relay network in which the legitimate channel is correlated with the eavesdropper's channel. We suppose that the relay with multiple antennas cannot obtain the instantaneous channel state information (CSI) of the eavesdropper's channel. The legitimate receiver estimates the correlation information between the two channels and then feeds it back to the relay.

In our previous work (Yuan *et al.*, 2016), only the approximate ergodic secrecy rate was adopted as the performance metric. The approximate ergodic secrecy rate $\bar{R}$ is not absolutely greater or smaller than the ergodic secrecy rate R_{eg}. In this study, we derive another performance metric, i.e., the lower bound of the ergodic secrecy rate R_{lb}. Along with the increase in R_{lb}, the ergodic secrecy rate increases. By comparing the performances using these two metrics, it can be seen that both metrics are efficient and the performance with R_{lb} is close to that with $\bar{R}$. Actually, a positive and clear lower bound is more useful in practical scenarios. In addition, in this article, we present the analysis of computation complexity for the two iterative optimization algorithms.

The main contributions of this study are summarized as follows:

1. For the first time, a more practical scenario of the dual relay network has been considered, in which the legitimate channels of the second hop are correlated with the eavesdropping channels. By exploiting the channel correlation matrix, we derive the statistical distribution of the eavesdropping channels based on the instantaneous legitimate channel states.

2. The analytical expression of the generalized match-and-forward (GMF) beamformer at the relay is presented based on the maximal-ratio-transmitting (MRT) strategy. It can be observed that the GMF beamformer is of low computation complexity, while it is the optimal rank-one beamformer to guarantee the transmission security from the transmitter to the legitimate receiver.

3. The approximate ergodic secrecy rate maximization problem is re-transformed into a semi-definite programming (SDP) problem, and the general rank beamformer (GRBF) is proposed to obtain the iteratively optimal relay beamformer. The computation complexity for the GRBF is presented and compared with that of the GMF beamformer.

4. The study also derives the iteratively optimal beamformer for the lower bound of the ergodic secrecy rate, to make a comparison with the beamformers mentioned herein in terms of the approximate secrecy rate.

Notations: We use upper-case and lower-case boldface letters to denote matrices and vectors, respectively. $\boldsymbol{I}_M$ denotes the $M \times M$ identity matrix, $(\cdot)^{\mathrm{T}}$ and $(\cdot)^{\mathrm{H}}$ are the transpose and conjugate transpose of matrices or vectors, respectively, $(\cdot)^*$ is the complex conjugate operator, $\mathbb{E}[\cdot]$ is the statistical expectation, and $\mathrm{tr}(\cdot)$ denotes the trace of a matrix. The Kronecker product is denoted as $\otimes$. $\mathrm{vec}(\cdot)$ represents the column vectorizing operator which stacks the columns of a matrix to a column vector, while $\mathrm{unvec}\,(\cdot)$ is the corresponding inverse-transforming operator. $\lambda_{\min}(\cdot)$ and $\lambda_{\max}(\cdot)$ denote the minimum and maximum eigenvalues of a matrix, respectively.

2 System model and problem formulation

2.1 System model

We consider a four-node wireless communication system as shown in Fig. 1, which consists of a source (Alice), a destination (Bob), a relay, and an eavesdropper (Eve). The relay helps secure transmissions from Alice to Bob. There are no direct channels from Alice to Bob and Eve. Eve aims to eavesdrop on the signals from the relay to Bob. We consider the following scenarios:

Scenario 1 The relay is equipped with M antennas for secure and reliable transmissions to Bob, while Alice, Bob, and Eve are all equipped with a single antenna.

Scenario 2 Bob can assume that Eve might be close to him for better eavesdropping and deduce a potential Eve's channel, which might be correlated with Bob's channel.

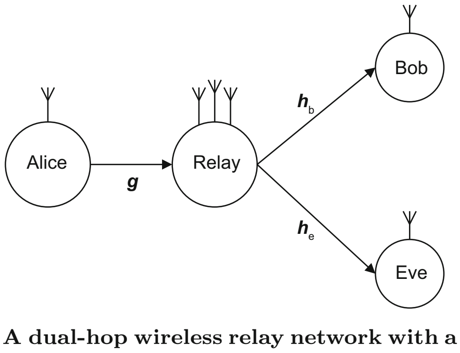

Fig. 1 A dual-hop wireless relay network with a single antenna eavesdropper

Let $\boldsymbol{h}_{\mathrm{b}}$ denote the channel vector to Bob from the relay. In addition, the channel vector to Eve from the relay is denoted by $\boldsymbol{h}_{\mathrm{e}}$. According to Scenario 2, $\boldsymbol{h}_{\mathrm{b}}$ and $\boldsymbol{h}_{\mathrm{e}}$ could be correlated and this correlation can be observed by Bob (the same assumption was adopted in Choi (2016)). Note that if Eve is not close to Bob, the two channel vectors are uncorrelated and Bob is unable to know their correlations. Assuming Rayleigh fading, $\boldsymbol{h}_{\mathrm{b}}$ and $\boldsymbol{h}_{\mathrm{e}}$ can be modeled as jointly circularly symmetric complex Gaussian (CSCG) random vectors:

$$\boldsymbol{h} = [\boldsymbol{h}_{\mathrm{b}}^{\mathrm{T}}\ \boldsymbol{h}_{\mathrm{e}}^{\mathrm{T}}]^{\mathrm{T}} \sim \mathcal{CN}\left(\begin{bmatrix} \boldsymbol{0} \\ \boldsymbol{0} \end{bmatrix}, \begin{bmatrix} \boldsymbol{R}_{11} & \boldsymbol{R}_{12} \\ \boldsymbol{R}_{21} & \boldsymbol{R}_{22} \end{bmatrix}\right), \tag{1}$$

where $\boldsymbol{R}_{11} = \mathbb{E}[\boldsymbol{h}_{\mathrm{b}}\boldsymbol{h}_{\mathrm{b}}^{\mathrm{H}}]$, $\boldsymbol{R}_{12} = \mathbb{E}[\boldsymbol{h}_{\mathrm{b}}\boldsymbol{h}_{\mathrm{e}}^{\mathrm{H}}]$, $\boldsymbol{R}_{21} = \mathbb{E}[\boldsymbol{h}_{\mathrm{e}}\boldsymbol{h}_{\mathrm{b}}^{\mathrm{H}}]$, and $\boldsymbol{R}_{22} = \mathbb{E}[\boldsymbol{h}_{\mathrm{e}}\boldsymbol{h}_{\mathrm{e}}^{\mathrm{H}}]$.

Because of the correlation between $\boldsymbol{h}_{\mathrm{b}}$ and $\boldsymbol{h}_{\mathrm{e}}$, $\boldsymbol{h}$ can be represented using a CSCG random vector $\boldsymbol{h}_1 \sim \mathcal{CN}\left(\boldsymbol{0}, \sigma^2\boldsymbol{I}\right)$ as

$$\boldsymbol{h} = \boldsymbol{R}^{1/2}\boldsymbol{h}_1, \tag{2}$$

where $\boldsymbol{R}$ denotes the channel correlation matrix and is Hermitian and positive definite, and σ^2 is the variance for each correspondingly independent channel. According to this discussion, it is easily obtained that

$$\begin{bmatrix} \boldsymbol{R}_{11} & \boldsymbol{R}_{12} \\ \boldsymbol{R}_{21} & \boldsymbol{R}_{22} \end{bmatrix} = \sigma^2\boldsymbol{R}.$$

At Bob's position, with knowing its channel vector $\boldsymbol{h}_{\mathrm{b}}$, the conditional distribution of $\boldsymbol{h}_{\mathrm{e}}$ can be found as follows (Barkat, 2005):

$$\boldsymbol{h}_{\mathrm{e}}|\boldsymbol{h}_{\mathrm{b}} \sim \mathcal{CN}\left(\bar{\boldsymbol{h}}_{\mathrm{e}}, \bar{\boldsymbol{R}}_{\mathrm{e}}\right), \tag{3}$$

where $\bar{\boldsymbol{h}}_{\mathrm{e}} = \boldsymbol{R}_{21}\boldsymbol{R}_{11}^{-1}\boldsymbol{h}_{\mathrm{b}}$ and $\bar{\boldsymbol{R}}_{\mathrm{e}} = \boldsymbol{R}_{22} - \boldsymbol{R}_{21}\boldsymbol{R}_{11}^{-1}\boldsymbol{R}_{12}$. The proof of Eq. (3) can be seen in Appendix A.

According to Kim *et al.* (2009), the channel correlation matrix can be divided into two parts, i.e., $\boldsymbol{R} = \boldsymbol{R}_{\mathrm{r}} \otimes \boldsymbol{R}_{\mathrm{s}}$, where $\boldsymbol{R}_{\mathrm{r}}$ and $\boldsymbol{R}_{\mathrm{s}}$ are 2×2 and $M \times M$ Hermitian matrices, denoting the receive and transmit correlation matrices, respectively.

We denote $\boldsymbol{R}_{\mathrm{r}} = \begin{bmatrix} 1 & \varepsilon \\ \varepsilon^* & 1 \end{bmatrix}$, where ε is the receive correlation coefficient between the receive antennas $(0 < \varepsilon \leq 1)$. Thus, $\boldsymbol{R}_{11} = \boldsymbol{R}_{22} = \sigma^2\boldsymbol{R}_{\mathrm{s}}$, and $\boldsymbol{R}_{12} = \boldsymbol{R}_{21}^{\mathrm{H}} = \varepsilon\sigma^2\boldsymbol{R}_{\mathrm{s}}$.

2.2 Signal transmitting procedure

The transmitting procedure is divided into two stages. In the first stage, Alice sends the source signal s with distribution $\mathcal{CN}(0,1)$ to the relay. The received signal vector at the relay is given by

$$\boldsymbol{y}_{\mathrm{r}} = \boldsymbol{g}s + \boldsymbol{n}, \tag{4}$$

where $\boldsymbol{g}$ is the channel vector from Alice to the relay, and $\boldsymbol{n}$ is the background complex Gaussian noise vector. In the second stage, the relay retransmits $\boldsymbol{y}_r$ via AF protocols. The beamforming matrix at the relay for AF relaying is denoted by $\boldsymbol{F}$. Then, the received signals at Bob and Eve, denoted by y_{b} and y_{e}, respectively, are given by

$$y_{\mathrm{b}} = \boldsymbol{h}_{\mathrm{b}}^{\mathrm{H}}\boldsymbol{F}\left(\boldsymbol{g}s + \boldsymbol{n}\right) + n_{\mathrm{b}}, \tag{5}$$

$$y_{\mathrm{e}} = \boldsymbol{h}_{\mathrm{e}}^{\mathrm{H}}\boldsymbol{F}\left(\boldsymbol{g}s + \boldsymbol{n}\right) + n_{\mathrm{e}}, \tag{6}$$

where n_{b} and n_{e} are the background complex Gaussian noise variables at Bob and Eve, respectively.

The power consumed at the relay for transmitting signals can be rewritten as

$$\begin{aligned} p(\boldsymbol{F}) &= \mathrm{tr}\left(\boldsymbol{F}\boldsymbol{g}\boldsymbol{g}^{\mathrm{H}}\boldsymbol{F}^{\mathrm{H}}\right) + \mathrm{tr}\left(\boldsymbol{F}\boldsymbol{F}^{\mathrm{H}}\right) \\ &= \mathrm{tr}\left(\boldsymbol{F}\hat{\boldsymbol{G}}\boldsymbol{F}^{\mathrm{H}}\right) \\ &\le p_{\mathrm{r}}, \end{aligned} \tag{7}$$

where $\hat{\boldsymbol{G}} = \boldsymbol{G} + \boldsymbol{I}_M$, $\boldsymbol{G} = \boldsymbol{g}\boldsymbol{g}^{\mathrm{H}}$, and p_{r} is the relay power constraint in the second stage.

Remark 1 In this study, we assume that all noise variances are one, i.e., $\boldsymbol{n} \sim \mathcal{CN}(\boldsymbol{0}, \boldsymbol{I})$, $n_{\mathrm{b}} \sim \mathcal{CN}(0,1)$, and $n_{\mathrm{e}} \sim \mathcal{CN}(0,1)$. Generally, we assume that $\boldsymbol{n} \sim \mathcal{CN}\left(\boldsymbol{0}, \sigma^2\boldsymbol{I}\right)$, $n_{\mathrm{b}} \sim \mathcal{CN}(0, \sigma_{\mathrm{b}})$, and $n_{\mathrm{e}} \sim \mathcal{CN}(0, \sigma_{\mathrm{e}})$, where σ, σ_{b}, and σ_{e} are the variances. We can easily normalize the noise variances to one by the following transforms: $\boldsymbol{y}_{\mathrm{r}} \to \boldsymbol{y}_{\mathrm{r}}/\sigma$, $\boldsymbol{y}_{\mathrm{b}} \to \boldsymbol{y}_{\mathrm{b}}/\sigma_{\mathrm{b}}$, $\boldsymbol{y}_{\mathrm{e}} \to \boldsymbol{y}_{\mathrm{e}}/\sigma_{\mathrm{e}}$, $\boldsymbol{g} \to \boldsymbol{g}/\sigma$, $\boldsymbol{h}_{\mathrm{b}} \to \sigma\boldsymbol{h}_{\mathrm{b}}/\sigma_{\mathrm{b}}$, and $\boldsymbol{h}_{\mathrm{e}} \to \sigma\boldsymbol{h}_{\mathrm{e}}/\sigma_{\mathrm{e}}$. Thus, the general case always fits into our assumptions.

2.3 Problem formulation

In this article, we focus on the relay beamforming problems. We first define several quantities prior to presenting the optimization criteria. The signal-to-noise ratio (SNR) at Bob, γ_{b}, as a function of $\boldsymbol{F}$, is defined as

$$\gamma_{\mathrm{b}}(\boldsymbol{F}) = \frac{|\boldsymbol{h}_{\mathrm{b}}^{\mathrm{H}}\boldsymbol{F}\boldsymbol{g}|^2}{1 + \|\boldsymbol{h}_{\mathrm{b}}^{\mathrm{H}}\boldsymbol{F}\|^2}, \tag{8}$$

and the SNR at Eve, γ_{e}, as a function of $\boldsymbol{h}_{\mathrm{e}}$ and $\boldsymbol{F}$, is defined as

$$\gamma_{\mathrm{e}}(\boldsymbol{F}, \boldsymbol{h}_{\mathrm{e}}) = \frac{|\boldsymbol{h}_{\mathrm{e}}^{\mathrm{H}}\boldsymbol{F}\boldsymbol{g}|^2}{1 + \|\boldsymbol{h}_{\mathrm{e}}^{\mathrm{H}}\boldsymbol{F}\|^2}. \tag{9}$$

For fast fading channels, with $\gamma_{\mathrm{b}}(\boldsymbol{F})$ and $\gamma_{\mathrm{e}}(\boldsymbol{F}, \boldsymbol{h}_{\mathrm{e}})$ in Eqs. (8) and (9), for a given $\boldsymbol{h}_{\mathrm{b}}$, the performance metric can be the ergodic secrecy rate:

$$\begin{aligned} R_{\mathrm{eg}}(\boldsymbol{F}) = \frac{1}{2}\Big(&\log_2(1 + \gamma_{\mathrm{b}}(\boldsymbol{F})) \\ &- \mathbb{E}_{\boldsymbol{h}_{\mathrm{e}}|\boldsymbol{h}_{\mathrm{b}}}\left[\log_2(1 + \gamma_{\mathrm{e}}(\boldsymbol{F}, \boldsymbol{h}_{\mathrm{e}}))\right]\Big)^{+}. \end{aligned} \tag{10}$$

As the ergodic secrecy rate R_{eg}, which is expressed in the integral form, is difficult for computation and optimization, we use the following approximation to simplify the optimization problem:

$$\bar{R}(\boldsymbol{F}) = \frac{1}{2}\left(\log_2(1 + \gamma_{\mathrm{b}}(\boldsymbol{F})) - \log_2(1 + \bar{\gamma}_{\mathrm{e}}(\boldsymbol{F}))\right)^{+}, \tag{11}$$

where the approximate average SNR at Eve is

$$\begin{aligned} \bar{\gamma}_{\mathrm{e}}(\boldsymbol{F}) &= \frac{\mathbb{E}_{\boldsymbol{h}_{\mathrm{e}}|\boldsymbol{h}_{\mathrm{b}}}\left[|\boldsymbol{h}_{\mathrm{e}}^{\mathrm{H}}\boldsymbol{F}\boldsymbol{g}|^2\right]}{1 + \mathbb{E}_{\boldsymbol{h}_{\mathrm{e}}|\boldsymbol{h}_{\mathrm{b}}}\left[\|\boldsymbol{h}_{\mathrm{e}}^{\mathrm{H}}\boldsymbol{F}\|^2\right]} \\ &= \frac{|\bar{\boldsymbol{h}}_{\mathrm{e}}^{\mathrm{H}}\boldsymbol{F}\boldsymbol{g}|^2 + \boldsymbol{g}^{\mathrm{H}}\boldsymbol{F}^{\mathrm{H}}\bar{\boldsymbol{R}}_{\mathrm{e}}\boldsymbol{F}\boldsymbol{g}}{1 + \left\|\bar{\boldsymbol{h}}_{\mathrm{e}}^{\mathrm{H}}\boldsymbol{F}\right\|^2 + \mathrm{tr}\left(\boldsymbol{F}^{\mathrm{H}}\bar{\boldsymbol{R}}_{\mathrm{e}}\boldsymbol{F}\right)} \\ &= \frac{\boldsymbol{g}^{\mathrm{H}}\boldsymbol{F}^{\mathrm{H}}\hat{\boldsymbol{H}}_{\mathrm{e}}\boldsymbol{F}\boldsymbol{g}}{1 + \mathrm{tr}\left(\boldsymbol{F}^{\mathrm{H}}\hat{\boldsymbol{H}}_{\mathrm{e}}\boldsymbol{F}\right)}, \end{aligned} \tag{12}$$

$\hat{\boldsymbol{H}}_{\mathrm{e}} = \bar{\boldsymbol{H}}_{\mathrm{e}} + \bar{\boldsymbol{R}}_{\mathrm{e}}$, and $\bar{\boldsymbol{H}}_{\mathrm{e}} = \bar{\boldsymbol{h}}_{\mathrm{e}}\bar{\boldsymbol{h}}_{\mathrm{e}}^{\mathrm{H}}$.

Note that the same approximation method has been adopted in Wang *et al.* (2013) and Kobayashi and Caire (2007) to maximize the average secrecy rate with imperfect CSI at the transmitter. The beamforming matrix is used to maximize the secrecy rate for a given $\boldsymbol{h}_{\mathrm{b}}$.

In addition to the approximate ergodic secrecy rate $\bar{R}(\boldsymbol{F})$, the other performance metric used is the lower bound on the ergodic secrecy rate. If we can maximize the lower bound, we can also increase the result of Eq. (10). The following expression is the lower bound that we have derived:

$$\begin{aligned}
R_{\mathrm{eg}}(\boldsymbol{F}) &\overset{\mathrm{a}}{\geq} \frac{\log_2 \mathrm{e}}{2}\left(\ln(1+\gamma_{\mathrm{b}}(\boldsymbol{F}))-\mathbb{E}_{\boldsymbol{h}_{\mathrm{e}}|\boldsymbol{h}_{\mathrm{b}}}\left[\gamma_{\mathrm{e}}(\boldsymbol{F},\boldsymbol{h}_{\mathrm{e}})\right]\right)\\
&= \frac{\log_2 \mathrm{e}}{2}\left(\ln(1+\gamma_{\mathrm{b}}(\boldsymbol{F}))-\mathbb{E}_{\boldsymbol{h}_{\mathrm{e}}|\boldsymbol{h}_{\mathrm{b}}}\left[\frac{\left|\boldsymbol{h}_{\mathrm{e}}^{\mathrm{H}}\boldsymbol{F}\boldsymbol{g}\right|^2}{1+\left\|\boldsymbol{h}_{\mathrm{e}}^{\mathrm{H}}\boldsymbol{F}\right\|^2}\right]\right)\\
&\overset{\mathrm{b}}{\geq} \frac{\log_2 \mathrm{e}}{2}\left(\ln(1+\gamma_{\mathrm{b}}(\boldsymbol{F}))-\frac{\mathbb{E}_{\boldsymbol{h}_{\mathrm{e}}|\boldsymbol{h}_{\mathrm{b}}}\left[\left|\boldsymbol{h}_{\mathrm{e}}^{\mathrm{H}}\boldsymbol{F}\boldsymbol{g}\right|^2\right]}{1+\mathbb{E}_{\boldsymbol{h}_{\mathrm{e}}|\boldsymbol{h}_{\mathrm{b}}}\left[\left\|\boldsymbol{h}_{\mathrm{e}}^{\mathrm{H}}\boldsymbol{F}\right\|^2\right]}\right)\\
&= \frac{\log_2 \mathrm{e}}{2}\left(\ln(1+\gamma_{\mathrm{b}}(\boldsymbol{F}))-\bar{\gamma}_{\mathrm{e}}(\boldsymbol{F})\right)\\
&\triangleq R_{\mathrm{lb}}(\boldsymbol{F}),
\end{aligned} \tag{13}$$

where the derivation (a) is due to $x > \ln(1+x)$ for $x > 0$, and the derivation (b) depends on Jensen's inequality.

For convenience, we drop the operator $(\cdot)^+$ and the constant coefficient 1/2. Mathematically, the beamforming optimization problem for Eq. (11) can be expressed as

$$\begin{aligned}
&\max_{\boldsymbol{F}} \ \log_2(1+\gamma_{\mathrm{b}}(\boldsymbol{F}))-\log_2(1+\bar{\gamma}_{\mathrm{e}}(\boldsymbol{F}))\\
&\text{s.t. } \operatorname{tr}(\boldsymbol{F}\hat{\boldsymbol{G}}\boldsymbol{F}^{\mathrm{H}}) \leq p_{\mathrm{r}}.
\end{aligned} \tag{14}$$

In the same way, by dropping the term $\log_2 \mathrm{e}/2$ in Eq. (13), the beamforming problem that maximizes the lower bound of R_{eg} can be formulated as follows:

$$\begin{aligned}
&\max_{\boldsymbol{F}} \ \ln(1+\gamma_{\mathrm{b}}(\boldsymbol{F}))-\bar{\gamma}_{\mathrm{e}}(\boldsymbol{F})\\
&\text{s.t. } \operatorname{tr}(\boldsymbol{F}\hat{\boldsymbol{G}}\boldsymbol{F}^{\mathrm{H}}) \leq p_{\mathrm{r}}.
\end{aligned} \tag{15}$$

3 Relay beamformer design

In this section, we design the beamforming matrices to obtain the maximal approximate ergodic secrecy rate $\bar{R}$.

According to Eq. (8), γ_{b} can be rewritten as

$$\begin{aligned}
\gamma_{\mathrm{b}}(\boldsymbol{F}) &= \frac{\boldsymbol{g}^{\mathrm{H}}\boldsymbol{F}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{b}}\boldsymbol{F}\boldsymbol{g}}{1+\operatorname{tr}(\boldsymbol{F}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{b}}\boldsymbol{F})}\\
&\overset{\mathrm{a}}{=} \frac{\operatorname{vec}(\boldsymbol{F})^{\mathrm{H}}\operatorname{vec}(\boldsymbol{H}_{\mathrm{b}}\boldsymbol{F}\boldsymbol{G})}{1+\operatorname{vec}(\boldsymbol{F})^{\mathrm{H}}\operatorname{vec}(\boldsymbol{H}_{\mathrm{b}}\boldsymbol{F})}\\
&\overset{\mathrm{b}}{=} \frac{\operatorname{vec}(\boldsymbol{F})^{\mathrm{H}}\left(\boldsymbol{G}^{\mathrm{T}}\otimes\boldsymbol{H}_{\mathrm{b}}\right)\operatorname{vec}(\boldsymbol{F})}{1+\operatorname{vec}(\boldsymbol{F})^{\mathrm{H}}\left(\boldsymbol{I}_M\otimes\boldsymbol{H}_{\mathrm{b}}\right)\operatorname{vec}(\boldsymbol{F})},
\end{aligned} \tag{16}$$

where $\boldsymbol{H}_{\mathrm{b}} = \boldsymbol{h}_{\mathrm{b}}\boldsymbol{h}_{\mathrm{b}}^{\mathrm{H}}$. The derivations (a) and (b) come from the theorems $\operatorname{tr}(\boldsymbol{A}^{\mathrm{H}}\boldsymbol{B}) = \operatorname{vec}(\boldsymbol{A})^{\mathrm{H}}\operatorname{vec}(\boldsymbol{B})$ and $\operatorname{vec}(\boldsymbol{ABC}) = (\boldsymbol{C}^{\mathrm{T}}\otimes\boldsymbol{A})\operatorname{vec}(\boldsymbol{B})$, respectively (Magnus and Neudecker, 1988).

Let $\boldsymbol{w} = \operatorname{vec}(\boldsymbol{F})$. Then

$$\gamma_{\mathrm{b}}(\boldsymbol{w}) = \frac{\boldsymbol{w}^{\mathrm{H}}\left(\boldsymbol{G}^{\mathrm{T}}\otimes\boldsymbol{H}_{\mathrm{b}}\right)\boldsymbol{w}}{1+\boldsymbol{w}^{\mathrm{H}}\left(\boldsymbol{I}_M\otimes\boldsymbol{H}_{\mathrm{b}}\right)\boldsymbol{w}}. \tag{17}$$

In a similar way, $\bar{\gamma}_{\mathrm{e}}$ can be rewritten as

$$\bar{\gamma}_{\mathrm{e}}(\boldsymbol{w}) = \frac{\boldsymbol{w}^{\mathrm{H}}\left(\boldsymbol{G}^{\mathrm{T}}\otimes\hat{\boldsymbol{H}}_{\mathrm{e}}\right)\boldsymbol{w}}{1+\boldsymbol{w}^{\mathrm{H}}\left(\boldsymbol{I}_M\otimes\hat{\boldsymbol{H}}_{\mathrm{e}}\right)\boldsymbol{w}}, \tag{18}$$

and the relay power constraint (7) can be rewritten as

$$p(\boldsymbol{w}) = \boldsymbol{w}^{\mathrm{H}}\left(\hat{\boldsymbol{G}}^{\mathrm{T}}\otimes\boldsymbol{I}_M\right)\boldsymbol{w} \leq p_{\mathrm{r}}. \tag{19}$$

Let $\boldsymbol{H}_{\mathrm{gb}} = \boldsymbol{G}^{\mathrm{T}}\otimes\boldsymbol{H}_{\mathrm{b}}$, $\boldsymbol{H}_{\mathrm{ib}} = \boldsymbol{I}_M\otimes\boldsymbol{H}_{\mathrm{b}}$, $\boldsymbol{H}_{\mathrm{ge}} = \boldsymbol{G}^{\mathrm{T}}\otimes\hat{\boldsymbol{H}}_{\mathrm{e}}$, $\boldsymbol{H}_{\mathrm{ie}} = \boldsymbol{I}_M\otimes\hat{\boldsymbol{H}}_{\mathrm{e}}$, and $\boldsymbol{H}_{\mathrm{gi}} = \hat{\boldsymbol{G}}^{\mathrm{T}}\otimes\boldsymbol{I}_M$. After plugging Eqs. (17), (18), and (19) into problem (14), the optimization problem can be rewritten as

$$\begin{aligned}
&\max_{\boldsymbol{w}} \log_2\left(1+\frac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{gb}}\boldsymbol{w}}{1+\boldsymbol{w}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{ib}}\boldsymbol{w}}\right)-\log_2\left(1+\frac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{ge}}\boldsymbol{w}}{1+\boldsymbol{w}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{ie}}\boldsymbol{w}}\right)\\
&\text{s.t. } \boldsymbol{w}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{gi}}\boldsymbol{w} \leq p_{\mathrm{r}}.
\end{aligned} \tag{20}$$

Since $\boldsymbol{w} = \operatorname{vec}(\boldsymbol{F})$, when we obtain the optimal $\boldsymbol{w}$, we can obtain the optimal $\boldsymbol{F}$ by solving $\boldsymbol{F} = \operatorname{unvec}(\boldsymbol{w})$.

3.1 GMF beamformer design

The GMF beamformer is designed to use the MRT strategy to make Bob obtain the largest channel capacity.

Using Eq. (5), we can see

$$\begin{aligned}
y_{\mathrm{b}} &= \boldsymbol{h}_{\mathrm{b}}^{\mathrm{H}}\boldsymbol{F}\boldsymbol{g}s+\boldsymbol{h}_{\mathrm{b}}^{\mathrm{H}}\boldsymbol{F}\boldsymbol{n}+n_{\mathrm{b}}\\
&= \left(\boldsymbol{g}^{\mathrm{T}}\otimes\boldsymbol{h}_{\mathrm{b}}^{\mathrm{H}}\right)\boldsymbol{w}s+\boldsymbol{h}_{\mathrm{b}}^{\mathrm{H}}\boldsymbol{F}\boldsymbol{n}+n_{\mathrm{b}}.
\end{aligned} \tag{21}$$

According to the MRT strategy, we can derive that the optimal $\boldsymbol{w}$ of the GMF beamformer is

$$\boldsymbol{w} = \mu_2\boldsymbol{q}_{\mathrm{gb}}, \tag{22}$$

where $\boldsymbol{q}_{\mathrm{gb}} = \boldsymbol{g}^*\otimes\boldsymbol{h}_{\mathrm{b}}$, and μ_2 is a scale number that ensures that $\boldsymbol{w}$ satisfies the power constraint.

After plugging Eq. (22) into problem (20), the problem becomes a single variable optimization problem. According to Appendix B, the optimal μ_2 can be obtained as follows:

$$\mu_2 = \begin{cases} 0, & m \geq h_{\mathrm{b}}^4,\\ \sqrt{x_0}, & m < \min\left(h_{\mathrm{b}}^4, \dfrac{g^2+1}{p_{\mathrm{r}}^2}\right),\\ \sqrt{x_1}, & \text{otherwise,} \end{cases} \tag{23}$$

where $h_{\rm b} = \|\boldsymbol{h}_{\rm b}\|$, $g = \|\boldsymbol{g}\|$, $m = \boldsymbol{h}_{\rm b}^{\rm H}\hat{\boldsymbol{H}}_{\rm e}\boldsymbol{h}_{\rm b}$, $x_0 = p_{\rm r}/(g^2h_{\rm b}^2(g^2+1))$, and $x_1 = \sqrt{1/((g^2+1)g^4h_{\rm b}^4m)}$.

As $\boldsymbol{F} = {\rm unvec}(\boldsymbol{w})$, the GMF beamformer can be rewritten as $\boldsymbol{F}_{\rm GMF} = \mu_2\boldsymbol{h}_{\rm b}\boldsymbol{g}^{\rm H}$. Compared with the MF beamformer in Wang *et al.* (2013), it is easily obtained that the GMF beamformer is essentially the MF beamformer proposed by Wang *et al.* (2013), i.e., the optimal rank-one beamformer. The proof is omitted here.

3.2 GRBF design

In this subsection, we do not impose any other constraints to the beamforming matrices. By dropping the $\log_2$ constraint, problem (20) can be formulated as follows:

$$\begin{aligned}&\max_{\boldsymbol{w}}\ \frac{1+\boldsymbol{w}^{\rm H}(\boldsymbol{H}_{\rm gb}+\boldsymbol{H}_{\rm ib})\boldsymbol{w}}{1+\boldsymbol{w}^{\rm H}\boldsymbol{H}_{\rm ib}\boldsymbol{w}}\frac{1+\boldsymbol{w}^{\rm H}\boldsymbol{H}_{\rm ie}\boldsymbol{w}}{1+\boldsymbol{w}^{\rm H}(\boldsymbol{H}_{\rm ie}+\boldsymbol{H}_{\rm ge})\boldsymbol{w}}\\&\text{s.t. }\ \boldsymbol{w}^{\rm H}\boldsymbol{H}_{\rm gi}\boldsymbol{w}\le p_{\rm r}.\end{aligned}\tag{24}$$

We introduce a slacking variable τ which satisfies the following relationship:

$$\tau = \frac{1+\boldsymbol{w}^{\rm H}\boldsymbol{H}_{\rm ie}\boldsymbol{w}}{1+\boldsymbol{w}^{\rm H}\left(\boldsymbol{H}_{\rm ie}+\boldsymbol{H}_{\rm ge}\right)\boldsymbol{w}}.\tag{25}$$

By plugging Eq. (25) into Eq. (24), for each given τ, problem (24) can be rewritten as follows:

$$\begin{aligned}&\max_{\boldsymbol{w}}\ \tau\frac{1+\boldsymbol{w}^{\rm H}\left(\boldsymbol{H}_{\rm gb}+\boldsymbol{H}_{\rm ib}\right)\boldsymbol{w}}{1+\boldsymbol{w}^{\rm H}\boldsymbol{H}_{\rm ib}\boldsymbol{w}}\\&\text{s.t. }\ \boldsymbol{w}^{\rm H}\boldsymbol{H}_{\rm gi}\boldsymbol{w}\le p_{\rm r},\\&\qquad \boldsymbol{w}^{\rm H}(\tau\boldsymbol{H}_{\rm ge}+(\tau-1)\boldsymbol{H}_{\rm ie})\boldsymbol{w} = 1-\tau.\end{aligned}\tag{26}$$

To solve this problem, semi-definite relaxation (SDR) is used. We define a matrix $\boldsymbol{W}$ that satisfies $\boldsymbol{W} = \boldsymbol{w}\boldsymbol{w}^{\rm H}$. By dropping the non-convex rank-one constraint of $\boldsymbol{W}$, problem (26) can be reformulated as follows:

$$\begin{aligned}&\max_{\boldsymbol{W}}\ \tau\frac{1+{\rm tr}((\boldsymbol{H}_{\rm gb}+\boldsymbol{H}_{\rm ib})\boldsymbol{W})}{1+{\rm tr}(\boldsymbol{H}_{\rm ib}\boldsymbol{W})}\\&\text{s.t. }\ {\rm tr}(\boldsymbol{H}_{\rm gi}\boldsymbol{W})\le p_{\rm r},\\&\qquad {\rm tr}((\tau\boldsymbol{H}_{\rm ge}+(\tau-1)\boldsymbol{H}_{\rm ie})\boldsymbol{W}) = 1-\tau,\\&\qquad \boldsymbol{W}\succcurlyeq 0.\end{aligned}\tag{27}$$

Problem (27) is quasi-convex. To solve it, we adopt the Charnes-Cooper transformation. We introduce two variables $\boldsymbol{Z}\succcurlyeq 0$ and $\eta > 0$, and further define that $\boldsymbol{W} = \boldsymbol{Z}/\eta$. Then problem (27) can be rewritten as follows:

$$\begin{aligned}&\max_{\boldsymbol{Z},\eta}\ \tau\left(\eta+{\rm tr}\left(\left(\boldsymbol{H}_{\rm gb}+\boldsymbol{H}_{\rm ib}\right)\boldsymbol{Z}\right)\right)\\&\text{s.t. }\ {\rm tr}\left(\boldsymbol{H}_{gi}\boldsymbol{Z}\right)\le\eta p_{\rm r},\\&\qquad {\rm tr}\left(\left(\tau\boldsymbol{H}_{\rm ge}+\left(\tau-1\right)\boldsymbol{H}_{\rm ie}\right)\boldsymbol{Z}\right) = \eta\left(1-\tau\right),\\&\qquad \eta+{\rm tr}\left(\boldsymbol{H}_{\rm ib}\boldsymbol{Z}\right) = 1, \boldsymbol{Z}\succcurlyeq 0, \eta > 0.\end{aligned}\tag{28}$$

Problem (28) is an SDP problem that is convex, and it can be solved by many convex optimization tools, such as CVX.

We assume that the optimal result of problem (28) is denoted by $\phi(\tau)$, as it is calculated with a given τ. To obtain the optimal solution of problem (24), the single-variable optimization problem represented as

$$\begin{aligned}&\max_{\tau}\ \phi(\tau)\\&\text{s.t. }\ \tau_{\rm lb}\le\tau\le\tau_{\rm ub}\end{aligned}\tag{29}$$

needs to be solved, where $\tau_{\rm lb}$ and $\tau_{\rm ub}$ are the lower and upper bounds, respectively. According to Eq. (25), we can see that

$$\begin{aligned}\tau &= \frac{1+\boldsymbol{w}^{\rm H}\boldsymbol{H}_{\rm ie}\boldsymbol{w}}{1+\boldsymbol{w}^{\rm H}\left(\boldsymbol{H}_{\rm ie}+\boldsymbol{H}_{\rm ge}\right)\boldsymbol{w}}\\&\ge\frac{\boldsymbol{w}^{\rm H}\left(\boldsymbol{H}_{\rm ie}+\dfrac{\boldsymbol{H}_{\rm gi}}{p_{\rm r}}\right)\boldsymbol{w}}{\boldsymbol{w}^{\rm H}\left(\boldsymbol{H}_{\rm ie}+\boldsymbol{H}_{\rm ge}+\dfrac{\boldsymbol{H}_{\rm gi}}{p_{\rm r}}\right)\boldsymbol{w}}\\&\ge\lambda_{\min}\left(\left(\boldsymbol{H}_{\rm ie}+\boldsymbol{H}_{\rm ge}+\frac{\boldsymbol{H}_{\rm gi}}{p_{\rm r}}\right)^{-1}\left(\boldsymbol{H}_{\rm ie}+\frac{\boldsymbol{H}_{\rm gi}}{p_{\rm r}}\right)\right)\\&\triangleq\tau_{\rm lb},\end{aligned}\tag{30}$$

and

$$\tau = \frac{1+\boldsymbol{w}^{\rm H}\boldsymbol{H}_{\rm ie}\boldsymbol{w}}{1+\boldsymbol{w}^{\rm H}\left(\boldsymbol{H}_{\rm ie}+\boldsymbol{H}_{\rm ge}\right)\boldsymbol{w}}\le 1\triangleq\tau_{\rm ub}.\tag{31}$$

From Eqs. (30) and (31), we can see that $\tau = \tau_{\rm lb}$ denotes that Eve's approximate wiretapping channel capacity reaches the best, while $\tau = \tau_{\rm ub}$ denotes that Eve cannot obtain any information from the channel.

Problem (29) is a one-variable optimization problem. Its optimal solution can be obtained by the one-dimensional exhaustive search algorithm.

3.3 Lower-bound-maximizing beamformer design

Next, we study the approximate ergodic secrecy rate for the system. However, the approximate ergodic secrecy rate is not strictly greater or smaller than the ergodic secrecy rate. In this subsection, we discuss the lower bound of the ergodic secrecy rate, and derive the iteratively optimal relay beamformer for the system.

After plugging Eqs. (17), (18), and (19) into problem (15), the optimization problem can be rewritten as

$$\begin{aligned} &\max_{\boldsymbol{w}} \ \ln\left(1+\frac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{gb}}\boldsymbol{w}}{1+\boldsymbol{w}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{ib}}\boldsymbol{w}}\right)-\frac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{ge}}\boldsymbol{w}}{1+\boldsymbol{w}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{ie}}\boldsymbol{w}} \\ &\text{s.t.} \ \ \boldsymbol{w}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{gi}}\boldsymbol{w}\le p_{\mathrm{r}}. \end{aligned} \tag{32}$$

A slacking parameter τ is introduced which satisfies

$$\tau=\frac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{ge}}\boldsymbol{w}}{1+\boldsymbol{w}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{ie}}\boldsymbol{w}}. \tag{33}$$

After substituting Eq. (33) into problem (32), the optimization problem can be rewritten as

$$\begin{aligned} &\max_{\boldsymbol{w}} \ \frac{1+\boldsymbol{w}^{\mathrm{H}}\left(\boldsymbol{H}_{\mathrm{gb}}+\boldsymbol{H}_{\mathrm{ib}}\right)\boldsymbol{w}}{1+\boldsymbol{w}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{ib}}\boldsymbol{w}} \\ &\text{s.t.} \ \ \boldsymbol{w}^{\mathrm{H}}\left(\boldsymbol{H}_{\mathrm{ge}}-\tau\boldsymbol{H}_{\mathrm{ie}}\right)\boldsymbol{w}=\tau, \\ &\qquad \boldsymbol{w}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{gi}}\boldsymbol{w}\le p_{\mathrm{r}}. \end{aligned} \tag{34}$$

To solve this problem, the SDR approach is used. We define a matrix $\boldsymbol{W}$ which satisfies $\boldsymbol{W}=\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}}$. By dropping the non-convex rank-one constraint of $\boldsymbol{W}$, problem (34) can be reformulated as

$$\begin{aligned} &\max_{\boldsymbol{W}} \ \frac{1+\mathrm{tr}\left(\left(\boldsymbol{H}_{\mathrm{gb}}+\boldsymbol{H}_{\mathrm{ib}}\right)\boldsymbol{W}\right)}{1+\mathrm{tr}\left(\boldsymbol{H}_{\mathrm{ib}}\boldsymbol{W}\right)} \\ &\text{s.t.} \ \ \mathrm{tr}\left(\left(\boldsymbol{H}_{\mathrm{ge}}-\tau\boldsymbol{H}_{\mathrm{ie}}\right)\boldsymbol{W}\right)=\tau, \\ &\qquad \mathrm{tr}\left(\boldsymbol{H}_{\mathrm{gi}}\boldsymbol{W}\right)\le p_{\mathrm{r}}, \boldsymbol{W}\succcurlyeq 0. \end{aligned} \tag{35}$$

Problem (35) is a quasi-convex problem; to solve this problem, we adopt the Charnes-Cooper transformation. We introduce two variables $\boldsymbol{Z}\succcurlyeq 0$ and $\eta>0$, and further define $\boldsymbol{W}=\boldsymbol{Z}/\eta$. Then problem (35) can be rewritten as

$$\begin{aligned} &\max_{\eta,\boldsymbol{Z}} \ \eta+\mathrm{tr}\left(\left(\boldsymbol{H}_{\mathrm{gb}}+\boldsymbol{H}_{\mathrm{ib}}\right)\boldsymbol{Z}\right) \\ &\text{s.t.} \ \ \mathrm{tr}\left(\left(\boldsymbol{H}_{\mathrm{ge}}-\tau\boldsymbol{H}_{\mathrm{ie}}\right)\boldsymbol{Z}\right)=\tau\eta, \\ &\qquad \mathrm{tr}\left(\boldsymbol{H}_{\mathrm{gi}}\boldsymbol{Z}\right)\le \eta p_{\mathrm{r}}, \\ &\qquad \eta+\mathrm{tr}\left(\boldsymbol{H}_{\mathrm{ib}}\boldsymbol{Z}\right)=1, \\ &\qquad \boldsymbol{Z}\succcurlyeq 0, \eta>0. \end{aligned} \tag{36}$$

Problem (36) is an SDP problem and is convex. It can also be solved by CVX tools.

We assume that the result of problem (36) is denoted by $\phi\left(\tau\right)$, as it is calculated with a given τ. To obtain the solution of problem (32), the single-variable optimization problem, represented as

$$\begin{aligned} &\max_{\tau} \ \ln\left(\phi\left(\tau\right)\right)-\tau \\ &\text{s.t.} \ \ \tau_{\mathrm{lb}}\le\tau\le\tau_{\mathrm{ub}}, \end{aligned} \tag{37}$$

needs to be solved, where τ_{lb} and τ_{ub} are the lower and upper bounds, respectively. According to constraint (33), it can be observed that

$$\begin{aligned} \tau&=\frac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{ge}}\boldsymbol{w}}{1+\boldsymbol{w}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{ie}}\boldsymbol{w}} \\ &\le\frac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{ge}}\boldsymbol{w}}{\boldsymbol{w}^{\mathrm{H}}\left(\frac{\boldsymbol{H}_{\mathrm{gi}}}{p_{\mathrm{r}}}+\boldsymbol{H}_{\mathrm{ie}}\right)\boldsymbol{w}} \\ &\le\lambda_{\max}\left(\left(\frac{\boldsymbol{H}_{\mathrm{gi}}}{p_{\mathrm{r}}}+\boldsymbol{H}_{\mathrm{ie}}\right)^{-1}\boldsymbol{H}_{\mathrm{ge}}\right) \\ &\triangleq\tau_{\mathrm{ub}}, \end{aligned} \tag{38}$$

and

$$\tau=\frac{\boldsymbol{w}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{ge}}\boldsymbol{w}}{1+\boldsymbol{w}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{ie}}\boldsymbol{w}}\ge 0\triangleq\tau_{\mathrm{lb}}. \tag{39}$$

Problem (37) is a one-variable optimization problem. Its optimal solution can be obtained by the one-dimensional exhaustive search algorithm.

Notations: Problems (27) and (34) are solved by dropping the rank-one constraint of $\boldsymbol{W}$. We assume that $(\boldsymbol{Z}^*,\eta^*)$ is the optimal solution of problem (28), and that $\boldsymbol{W}^*=\boldsymbol{Z}^*/\eta^*$. If $\boldsymbol{W}^*$ is of rank-one, we can obtain the optimal $\boldsymbol{w}^*$ via the eigenvalue decomposition of $\boldsymbol{W}^*$. If the rank of $\boldsymbol{W}^*$ is larger than one, we can extract an approximate solution $\boldsymbol{w}^*$ by the Gaussian randomization procedure (Luo *et al.*, 2010). The procedure for problem (34) is the same as that for problem (27), so it is omitted for clarity and simplicity.

According to Luo *et al.* (2010), the SDP problems represented in problems (28) and (36) can be numerically tackled through interior-point methods with the worst case complexity

$$\mathcal{O}\left(\max\left(4,M^2+1\right)^4\left(M^2+1\right)^{1/2}\lg\left(1/\delta\right)\right), \tag{40}$$

where $\delta>0$ is a given solution accuracy. Meanwhile, the computation complexity of the GMF beamformer is $\mathcal{O}\left(1\right)$, irrespective of the number of antennas in the relay.

4 Numerical results

In this section, simulation results are shown to present the performance of the proposed relay beamformers. The values for $R_{\rm eg}$ in Eq. (10) for the proposed relay beamformers are also given with high precision numerical methods, and the results of the MF beamformer (Wang *et al.*, 2013) are presented for comparison. In the simulation, we set $g^2 = \|\boldsymbol{g}\|^2 = 10$ dB.

Because the receive correlation matrix is more complex for the situation in which Bob and Eve have multiple antennas, we consider only that Bob and Eve are both equipped with a single antenna for simplicity. We assume that the receive correlation matrix satisfies

$$\boldsymbol{R}_{\rm r} = \begin{bmatrix} 1 & \varepsilon \\ \varepsilon^* & 1 \end{bmatrix},$$

where $\varepsilon = 0$ means that the receive channel states of Bob and Eve are independent, and $|\varepsilon| = 1$ means that the receive channel states of Bob and Eve are completely correlated. The transmit correlation matrix can be assumed as an $M \times M$ identity matrix, because the relative positions among the relay's antennas could be well designed to reduce their correlations. For simulations, $\boldsymbol{g}$ and $\boldsymbol{h}_{\rm b}$ are generated randomly for each run, and the average values of 1000 runs are presented.

Figs. 2 and 3 show the impact of the receive correlation coefficient on the secrecy rate for different numbers of antennas in the relay (M). As observed, the performance of the GRBF surpasses that of the GMF beamformer, while the performance of the LBM beamformer gets close to that of the GRBF. When the correlation between Bob's and Eve's channels, i.e., $|\varepsilon|$, increases, the secrecy rates deteriorate for all the beamformers. Specifically, when $|\varepsilon| = 0$ (i.e., Bob's and Eve's channels are independent), the secrecy rates for all the beamformers reach the largest value; when $|\varepsilon| = 1$ (i.e., Bob's and Eve's channels are fully correlated), the secrecy rates of all the channels become zero. In this condition, extra jammers are needed to guarantee the security of information transmission, which is another topic different from that in this study. Along with the increase in the correlation, it becomes harder to exploit the difference between the channels to transmit secure information. $\bar{R}$ for the MF beamformer is coincident with $\bar{R}$ for the GMF beamformer, proving that the GMF beamformer is the optimal rank-one beamformer. $R_{\rm eg}$ for the LBM beamformer gets closer to that obtained by the GRBF when $M = 4$ than it does when $M = 2$.

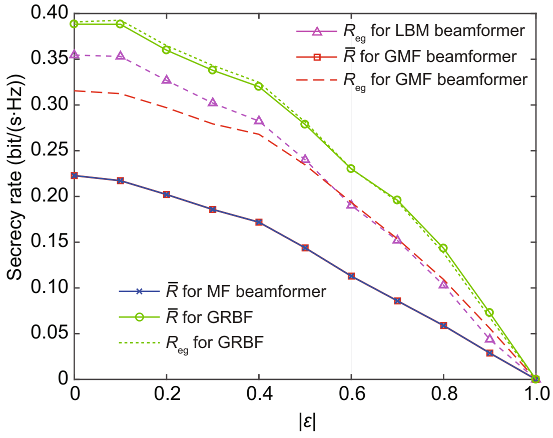

Fig. 2 Approximate ergodic secrecy rate $\bar{R}$ and ergodic secrecy rate $R_{\rm eg}$ versus the receive correlation coefficient between receiving antennas, $|\varepsilon|$ ($M = 2$, $p_{\rm r} = 10$ dB, and $\sigma^2 = 1$)

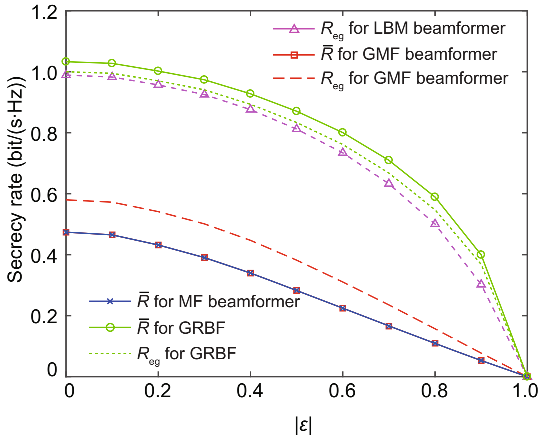

Fig. 3 Approximate ergodic secrecy rate $\bar{R}$ and ergodic secrecy rate $R_{\rm eg}$ versus the receive correlation coefficient between receiving antennas, $|\varepsilon|$ ($M = 4$, $p_{\rm r} = 10$ dB, and $\sigma^2 = 1$)

Fig. 4 depicts the curves of system performance versus the relay power $p_{\rm r}$. When $p_{\rm r}$ increases, $\bar{R}$ for the GRBF increases fast, and $\bar{R}$ for the GMF beamformer increases at the beginning, but then the curve becomes flat. When $p_{\rm r}$ is in the lower region, the performance of the GMF beamformer for $R_{\rm eg}$ surpasses that of the GRBF and the LBM beamformer. According to Eq. (23), we can see that when $p_{\rm r}$ is low, the performance of the GMF beamformer improves with the increase of $p_{\rm r}$; when $p_{\rm r}$ is in the high region, the performance of the GMF beamformer is irrelevant to $p_{\rm r}$.

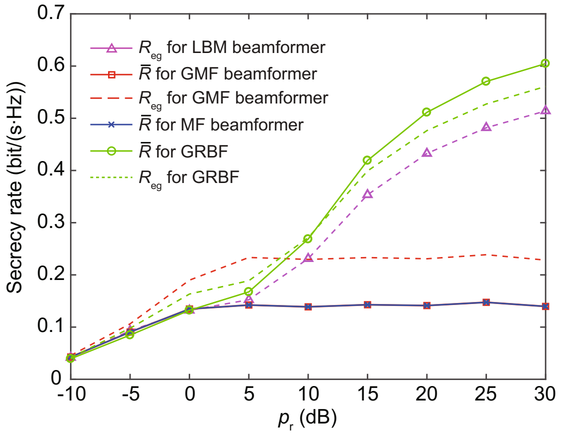

Fig. 4 Approximate ergodic secrecy rate $\bar{R}$ and ergodic secrecy rate R_{eg} versus the relay power, p_r ($M = 2$, $|\varepsilon| = 0.5$, and $\sigma^2 = 1$)

In Fig. 5, we discuss the impact of the channel gain of the second hop σ^2 on the secrecy rate. The terms σ^2 and p_r have the same impact on the performance of the system, because they both affect the signal strength at Bob's and Eve's locations. When σ^2 increases, the value of $\bar{R}$ for the GRBF increases, and the value of $\bar{R}$ for the GMF beamformer remains constant because p_r is large enough.

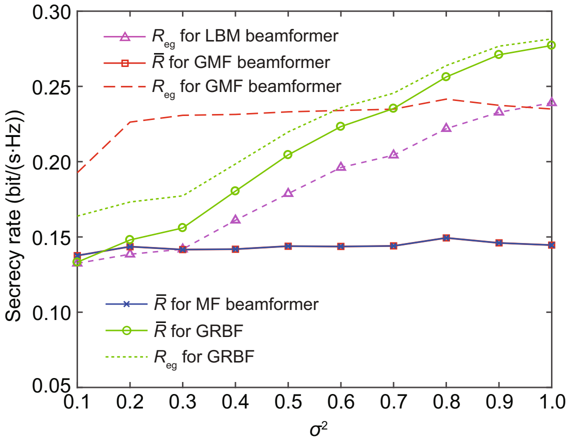

Fig. 5 Approximate ergodic secrecy rate $\bar{R}$ and ergodic secrecy rate R_{eg} versus the channel gain of the second hop, σ^2 ($M = 2$, $|\varepsilon| = 0.5$, and $p_r = 10$ dB)

Fig. 6 presents the curves of the secrecy rates versus the number of antennas in the relay (M). When M increases, the performance for both the GMF beamformer and the GRBF is improved; however, the improvement rate becomes lower, because we assume that the channel gain between Alice and the relay g^2 is constant. When M increases, the average signal strength for each antenna degrades.

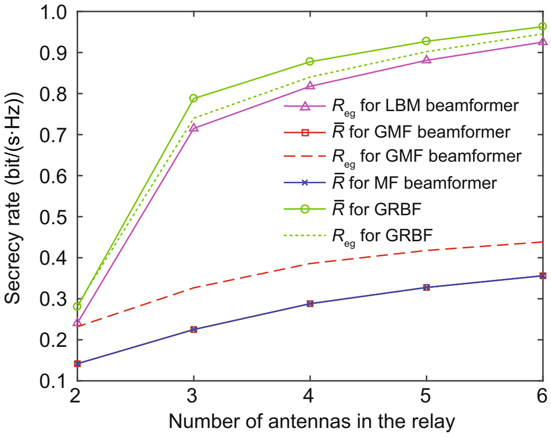

Fig. 6 Approximate ergodic secrecy rate $\bar{R}$ and ergodic secrecy rate R_{eg} versus the number of antennas in the relay, M ($\sigma^2 = 1$, $|\varepsilon| = 0.5$, and $p_r = 10$ dB)

From all the results presented herein, we observe that R_{eg} always changes the same as $\bar{R}$ for each kind of beamformer. R_{eg} for the LBM beamformer follows the same change trend as R_{eg} for the GRBF, and gets closer to R_{eg} while M increases.

5 Conclusions

In this study, a dual-hop wireless communication system was studied. In this system, the relay is equipped with multiple antennas, and the legitimate channel is correlated with the eavesdropping one. Three different beamformers at the relay were studied: the GMF beamformer, the GRBF for the approximate ergodic secrecy rate, and the LBM beamformer for the lower bound of the ergodic secrecy rate. It could be found that: the performance of the GRBF was the best, the performance of the LBM beamformer was the second, and the GMF had the lowest computation complexity. When the relay had lower power or the channel of the second hop was weak, the performance of the GMF beamformer surpassed that of the other two beamformers. In addition, the performance of the LBM beamformer for the ergodic secrecy rate got close to that of the GRBF for the approximate ergodic secrecy rate of the system. It should be noted that the study considered only the simple situation in which the legitimate receiver was equipped with a single antenna, as was the eavesdropping receiver. In the future, more research would be carried out on systems with more complex correlated channels, for instance, cases of multiple relays with multiple antennas.

References

Barkat, M., 2005. Signal Detection and Estimation. Artech House.

Chen, L., 2011. Physical layer security for cooperative relaying in broadcast networks. Military Communications Conf., p.91-96. http://dx.doi.org/10.1109/MILCOM.2011.6127796

Cheng, X., Wang, C., Wang, H., *et al.*, 2012. Cooperative MIMO channel modeling and multi-link spatial correlation properties. *IEEE J. Sel. Areas Commun.*, **30**(2):388-396. http://dx.doi.org/10.1109/JSAC.2012.120218

Choi, J., 2016. A robust beamforming approach to guarantee instantaneous secrecy rate. *IEEE Trans. Wirel. Commun.*, **15**(2):1076-1085. http://dx.doi.org/10.1109/TWC.2015.2482494

Csiszár, I., Korner, J., 1978. Broadcast channels with confidential messages. *IEEE Trans. Inform. Theory*, **24**(3):339-348. http://dx.doi.org/10.1109/TIT.1978.1055892

Dong, L., Han, Z., Petropulu, A.P., *et al.*, 2010. Improving wireless physical layer security via cooperating relays. *IEEE Trans. Signal Process.*, **58**(3):1875-1888. http://dx.doi.org/10.1109/TSP.2009.2038412

Ferdinand, N.S., da Costa, D.B., de Almeida, A.L.F., *et al.*, 2014. Physical layer secrecy performance of TAS wiretap channels with correlated main and eavesdropper channels. *IEEE Wirel. Commun. Lett.*, **3**(1):86-89. http://dx.doi.org/10.1109/WCL.2013.112313.130733

Geraci, G., Al-Nahari, A.Y., Yuan, J., *et al.*, 2013. Linear precoding for broadcast channels with confidential messages under transmit-side channel correlation. *IEEE Commun. Lett.*, **17**(6):1164-1167. http://dx.doi.org/10.1109/LCOMM.2013.050313.130353

Ghose, S., Bose, R., 2013. Power allocation strategy using node cooperation for transmit power minimization under correlated fading. National Conf. on Communications, p.1-5. http://dx.doi.org/10.1109/NCC.2013.6487960

Kim, A.Y., Cho, H.N., Lee, J.W., *et al.*, 2009. Allocation of transmit power in spatially-correlated dual-hop MIMO relay channels. 9th Int. Symp. on Communications and Information Technology, p.332-336. http://dx.doi.org/10.1109/ISCIT.2009.5341231

Kobayashi, M., Caire, G., 2007. Joint beamforming and scheduling for a multi-antenna downlink with imperfect transmitter channel knowledge. *IEEE J. Sel. Areas Commun.*, **25**(7):1468-1477. http://dx.doi.org/10.1109/JSAC.2007.070919

Krikidis, I., 2010. Opportunistic relay selection for cooperative networks with secrecy constraints. *IET Commun.*, **4**(15):1787-1791. http://dx.doi.org/10.1049/iet-com.2009.0634

Lee, J.H., 2015. Cooperative relaying protocol for improving physical layer security in wireless decode-and-forward relaying networks. *Wirel. Pers. Commun.*, **83**(4):3033-3044. http://dx.doi.org/10.1007/s11277-015-2580-2

Leung-Yan-Cheong, S., Hellman, M.E., 1978. The Gaussian wire-tap channel. *IEEE Trans. Inform. Theory*, **24**(4):451-456. http://dx.doi.org/10.1109/TIT.1978.1055917

Li, J., Petropulu, A.P., Weber, S., 2011. On cooperative relaying schemes for wireless physical layer security. *IEEE Trans. Signal Process.*, **59**(10):4985-4997. http://dx.doi.org/10.1109/TSP.2011.2159598

Luo, Z., Ma, W.K., So, A.M.C., *et al.*, 2010. Semidefinite relaxation of quadratic optimization problems. *IEEE Signal Process. Mag.*, **27**(3):20-34. http://dx.doi.org/10.1109/MSP.2010.936019

Magnus, J.R., Neudecker, H., 1988. Matrix Differential Calculus with Applications in Statistics and Econometrics. Wiley.

McKay, M.R., Collings, I.B., 2005. General capacity bounds for spatially correlated Rician MIMO channels. *IEEE Trans. Inform. Theory*, **51**(9):3121-3145. http://dx.doi.org/10.1109/TIT.2005.853325

Tulino, A.M., Lozano, A., Verdu, S., 2005. Impact of antenna correlation on the capacity of multiantenna channels. *IEEE Trans. Inform. Theory*, **51**(7):2491-2509. http://dx.doi.org/10.1109/TIT.2005.850094

Wang, X., Wang, K., Zhang, X., 2013. Secure relay beamforming with imperfect channel side information. *IEEE Trans. Veh. Technol.*, **62**(5):2140-2155. http://dx.doi.org/10.1109/TVT.2012.2230657

Wang, X., Su, Z., Wang, G., 2015. Relay selection for secure backscatter wireless communications. *Electron. Lett.*, **51**(12):951-952. http://dx.doi.org/10.1049/el.2014.4401

Wyner, A.D., 1975. The wire-tap channel. *Bell Syst. Techn. J.*, **54**(8):1355-1387. http://dx.doi.org/10.1002/j.1538-7305.1975.tb02040.x

Yin, X., Cheng, X., 2016. Propagation Channel Characterization, Parameter Estimation, and Modeling for Wireless Communications. Wiley-IEEE Press.

Yuan, Z., Chen, C., Bai, L., *et al.*, 2016. Secure relay beamforming with correlated channel models in dual-hop wireless communication networks. IEEE GLOBECOM, p.1-6. http://dx.doi.org/10.1109/GLOCOM.2016.7842252

Zhang, M., Wen, M., Cheng, X., *et al.*, 2016. A dual-hop virtual MIMO architecture based on hybrid differential spatial modulation. *IEEE Trans. Wirel. Commun.*, **15**(9):6356-6370. http://dx.doi.org/10.1109/TWC.2016.2583423

Zhang, R., Cheng, X., Yang, L., 2016a. Cooperation via spectrum sharing for physical layer security in device-to-device communications underlaying cellular networks. *IEEE Trans. Wirel. Commun.*, **15**(8):5651-5663. http://dx.doi.org/10.1109/GLOCOM.2015.7417724

Zhang, R., Cheng, X., Yang, L., 2016b. Joint power and access control for physical layer security in D2D communications underlaying cellular networks. IEEE Int. Conf. on Communications, p.1-6. http://dx.doi.org/10.1109/ICC.2016.7511531

Appendix A: Derivation of the conditional distribution of $\boldsymbol{h}_{\mathrm{e}}$

It is known that $\boldsymbol{h} = [\boldsymbol{h}_{\mathrm{b}}^{\mathrm{T}} \;\; \boldsymbol{h}_{\mathrm{e}}^{\mathrm{T}}]^{\mathrm{T}}$ is a CSCG random vector. The probability density function (PDF) of $\boldsymbol{h}$ can be expressed as

$$f(\boldsymbol{h})=\frac{1}{\pi^{2M}\det\left[\begin{array}{cc}\boldsymbol{R}_{11}&\boldsymbol{R}_{12}\\\boldsymbol{R}_{21}&\boldsymbol{R}_{22}\end{array}\right]}\cdot\exp\left[\left[\boldsymbol{h}_{\mathrm{b}}^{\mathrm{H}},\boldsymbol{h}_{\mathrm{e}}^{\mathrm{H}}\right]\left[\begin{array}{cc}\boldsymbol{R}_{11}&\boldsymbol{R}_{12}\\\boldsymbol{R}_{21}&\boldsymbol{R}_{22}\end{array}\right]^{-1}\left[\begin{array}{c}\boldsymbol{h}_{\mathrm{b}}\\\boldsymbol{h}_{\mathrm{e}}\end{array}\right]\right]. \tag{A1}$$

$\boldsymbol{h}_{\mathrm{b}}$ is a CSCG random vector. The PDF of $\boldsymbol{h}_{\mathrm{b}}$ can be expressed as

$$f(\boldsymbol{h}_{\mathrm{b}})=\frac{1}{\pi^{M}\det\boldsymbol{R}_{11}}\exp\left[\boldsymbol{h}_{\mathrm{b}}^{\mathrm{H}}\boldsymbol{R}_{11}^{-1}\boldsymbol{h}_{\mathrm{b}}\right]. \tag{A2}$$

Because $\boldsymbol{R}_{ij}$ $(i=1,2;j=1,2)$ are full-rank matrices, transformations in Eqs. (A3) and (A4) are satisfied:

$$\det\left[\begin{array}{cc}\boldsymbol{R}_{11}&\boldsymbol{R}_{12}\\\boldsymbol{R}_{21}&\boldsymbol{R}_{22}\end{array}\right]=\det\left[\boldsymbol{R}_{11}\right]\det\left[\hat{\boldsymbol{R}}_{11}\right], \tag{A3}$$

$$\left[\begin{array}{cc}\boldsymbol{R}_{11}&\boldsymbol{R}_{12}\\\boldsymbol{R}_{21}&\boldsymbol{R}_{22}\end{array}\right]^{-1}=\left[\begin{array}{cc}\left(\boldsymbol{R}_{11}-\boldsymbol{R}_{12}\boldsymbol{R}_{22}^{-1}\boldsymbol{R}_{21}\right)^{-1}&-\hat{\boldsymbol{R}}_{12}^{-1}\\\left(\boldsymbol{R}_{12}-\boldsymbol{R}_{11}\boldsymbol{R}_{21}^{-1}\boldsymbol{R}_{22}\right)^{-1}&\hat{\boldsymbol{R}}_{11}^{-1}\end{array}\right], \tag{A4}$$

where $\hat{\boldsymbol{R}}_{11}=\boldsymbol{R}_{22}-\boldsymbol{R}_{21}\boldsymbol{R}_{11}^{-1}\boldsymbol{R}_{12}$ and $\hat{\boldsymbol{R}}_{12}=\boldsymbol{R}_{21}-\boldsymbol{R}_{22}\boldsymbol{R}_{12}^{-1}\boldsymbol{R}_{11}$.

According to the probability theory, the conditional PDF can be rewritten as

$$f(\boldsymbol{h}_{\mathrm{e}}|\boldsymbol{h}_{\mathrm{b}})=\frac{f(\boldsymbol{h})}{f(\boldsymbol{h}_{\mathrm{b}})}=\frac{1}{\pi^{M}\det\left(\boldsymbol{R}_{22}-\boldsymbol{R}_{21}\boldsymbol{R}_{11}^{-1}\boldsymbol{R}_{12}\right)}\cdot\exp\left[\left[\boldsymbol{h}_{\mathrm{b}}^{\mathrm{H}}\ \ \boldsymbol{h}_{\mathrm{e}}^{\mathrm{H}}\right]\begin{bmatrix}\boldsymbol{R}_{11}&\boldsymbol{R}_{12}\\\boldsymbol{R}_{21}&\boldsymbol{R}_{22}\end{bmatrix}^{-1}\begin{bmatrix}\boldsymbol{h}_{\mathrm{b}}\\\boldsymbol{h}_{\mathrm{e}}\end{bmatrix}-\boldsymbol{h}_{\mathrm{b}}^{\mathrm{H}}\boldsymbol{R}_{\mathrm{bb}}^{-1}\boldsymbol{h}_{\mathrm{b}}\right]. \tag{A5}$$

According to the properties of the Gaussian random process, the statistical distribution of the conditional probability $\boldsymbol{h}_{\mathrm{e}}|\boldsymbol{h}_{\mathrm{b}}$ is still a Gaussian random process, i.e., $\boldsymbol{y}=\boldsymbol{h}_{\mathrm{e}}|\boldsymbol{h}_{\mathrm{b}}\sim\mathcal{CN}\left(\bar{\boldsymbol{h}}_{\mathrm{e}},\bar{\boldsymbol{R}}_{\mathrm{e}}\right)$. Then, the PDF of $\boldsymbol{y}$ can be rewritten as

$$f(\boldsymbol{y})=\frac{1}{\pi^{M}\det\bar{\boldsymbol{R}}_{\mathrm{e}}}\exp\left[\left(\boldsymbol{y}-\bar{\boldsymbol{h}}_{\mathrm{e}}\right)^{\mathrm{H}}\bar{\boldsymbol{R}}_{\mathrm{e}}^{-1}\left(\boldsymbol{y}-\bar{\boldsymbol{h}}_{\mathrm{e}}\right)\right]. \tag{A6}$$

By plugging Eq. (A4) into Eq. (A5) and comparing Eqs. (A5) and (A6), we can easily obtain

$$\begin{cases}\bar{\boldsymbol{R}}_{\mathrm{e}}=\boldsymbol{R}_{22}-\boldsymbol{R}_{21}\boldsymbol{R}_{11}^{-\mathbf{1}}\boldsymbol{R}_{12},\\-(\hat{\boldsymbol{R}}_{11})^{-1}\bar{\boldsymbol{h}}_{\mathrm{e}}=\left(\boldsymbol{R}_{12}-\boldsymbol{R}_{11}\boldsymbol{R}_{21}{}^{-1}\boldsymbol{R}_{22}\right)^{-1}\boldsymbol{h}_{\mathrm{b}}.\end{cases}$$

That is,

$$\bar{\boldsymbol{h}}_{\mathrm{e}}=\boldsymbol{R}_{21}\boldsymbol{R}_{11}^{-1}\boldsymbol{h}_{\mathrm{b}}, \tag{A7}$$

$$\bar{\boldsymbol{R}}_{\mathrm{e}}=\boldsymbol{R}_{22}-\boldsymbol{R}_{21}\boldsymbol{R}_{11}^{-1}\boldsymbol{R}_{12}. \tag{A8}$$

The proof is completed.

Appendix B: Procedure for obtaining the optimal $\boldsymbol{\mu_2}$

Substituting Eq. (22) into Eq. (17), then we have

$$\begin{aligned}&\gamma_{\mathrm{b}}(\mu_2)\\&=\frac{\mu_2^2(\boldsymbol{g}^*\otimes\boldsymbol{h}_{\mathrm{b}})^{\mathrm{H}}((\boldsymbol{g}\boldsymbol{g}^{\mathrm{H}})^{\mathrm{T}}\otimes(\boldsymbol{h}_{\mathrm{b}}\boldsymbol{h}_{\mathrm{b}}^{\mathrm{H}}))(\boldsymbol{g}^*\otimes\boldsymbol{h}_{\mathrm{b}})}{1+\mu_2^2(\boldsymbol{g}^*\otimes\boldsymbol{h}_{\mathrm{b}})^{\mathrm{H}}(\boldsymbol{I}_M\otimes(\boldsymbol{h}_{\mathrm{b}}\boldsymbol{h}_{\mathrm{b}}^{\mathrm{H}}))(\boldsymbol{g}^*\otimes\boldsymbol{h}_{\mathrm{b}})}\\&\overset{\mathrm{a}}{=}\frac{\mu_2^2\left(\boldsymbol{g}^{\mathrm{T}}\boldsymbol{g}^*\boldsymbol{g}^{\mathrm{T}}\boldsymbol{g}^*\right)\otimes\left(\boldsymbol{h}_{\mathrm{b}}^{\mathrm{H}}\boldsymbol{h}_{\mathrm{b}}\boldsymbol{h}_{\mathrm{b}}^{\mathrm{H}}\boldsymbol{h}_{\mathrm{b}}\right)}{1+\mu_2^2\left(\boldsymbol{g}^{\mathrm{T}}\boldsymbol{I}_M\boldsymbol{g}^*\right)\otimes\left(\boldsymbol{h}_{\mathrm{b}}^{\mathrm{H}}\left(\boldsymbol{h}_{\mathrm{b}}\boldsymbol{h}_{\mathrm{b}}^{\mathrm{H}}\right)\boldsymbol{h}_{\mathrm{b}}\right)}\\&=\frac{\mu_2^2g^4h_{\mathrm{b}}^4}{1+\mu_2^2g^2h_{\mathrm{b}}^4}.\end{aligned} \tag{B1}$$

The process (a) comes from the theorem $(\boldsymbol{AB})\otimes(\boldsymbol{CD})=(\boldsymbol{A}\otimes\boldsymbol{C})(\boldsymbol{B}\otimes\boldsymbol{D})$.

Substituting Eq. (22) into Eq. (18), we obtain

$$\begin{aligned}\bar{\gamma}_{\mathrm{e}}(\mu_2)&=\frac{\mu_2^2(\boldsymbol{g}^*\otimes\boldsymbol{h}_{\mathrm{b}})^{\mathrm{H}}\left(\left(\boldsymbol{g}\boldsymbol{g}^{\mathrm{H}}\right)^{\mathrm{T}}\otimes\hat{\boldsymbol{H}}_{\mathrm{e}}\right)(\boldsymbol{g}^*\otimes\boldsymbol{h}_{\mathrm{b}})}{1+\mu_2^2(\boldsymbol{g}^*\otimes\boldsymbol{h}_{\mathrm{b}})^{\mathrm{H}}\left(\boldsymbol{I}_M\otimes\hat{\boldsymbol{H}}_{\mathrm{e}}\right)(\boldsymbol{g}^*\otimes\boldsymbol{h}_{\mathrm{b}})}\\&=\frac{\mu_2^2g^4m}{1+\mu_2^2g^2m},\end{aligned} \tag{B2}$$

where $m=\boldsymbol{h}_{\mathrm{b}}^{\mathrm{H}}\hat{\boldsymbol{H}}_{\mathrm{e}}\boldsymbol{h}_{\mathrm{b}}$ is a constant with respect to h_{b} and the covariance matrix of $\boldsymbol{h}$.

Substituting Eq. (22) into Eq. (19), the power constraint can be written as

$$\begin{aligned}p(\mu_2)&=\mu_2^2(\boldsymbol{g}^*\otimes\boldsymbol{h}_{\mathrm{b}})^{\mathrm{H}}\left(\hat{\boldsymbol{G}}^{\mathrm{T}}\otimes\boldsymbol{I}_M\right)\boldsymbol{g}^*\otimes\boldsymbol{h}_{\mathrm{b}}\\&=\mu_2^2\left(\boldsymbol{g}^{\mathrm{T}}\boldsymbol{g}^*+\boldsymbol{g}^{\mathrm{T}}\boldsymbol{g}^*\boldsymbol{g}^{\mathrm{T}}\boldsymbol{g}^*\right)\otimes\left(\boldsymbol{h}_{\mathrm{b}}^{\mathrm{H}}\boldsymbol{h}_{\mathrm{b}}\right)\\&=\mu_2^2g^2\left(1+g^2\right)h_{\mathrm{b}}^2\\&\leq p_{\mathrm{r}}.\end{aligned} \tag{B3}$$

Plugging Eqs. (B1), (B2), and (B3) into problem (14), and letting $x=\mu_2^2$, the optimization problem becomes

$$\begin{aligned}&\max_{x}\ \log_2\left(1+\frac{g^4h_{\mathrm{b}}^4x}{1+g^2h_{\mathrm{b}}^4x}\right)-\log_2\left(1+\frac{g^4mx}{1+g^2mx}\right)\\&\text{s.t.}\ \ g^2\left(1+g^2\right)h_{\mathrm{b}}^2x\leq p_{\mathrm{r}}.\end{aligned} \tag{B4}$$

Let $f(x)$ be the objective function of problem (B4). The derivative of $f(x)$ with respect to x is shown in Eq. (B5):

$$\frac{\mathrm{d}f(x)}{\mathrm{d}x} = \frac{g^4\left(m-h_{\mathrm{b}}^4\right)\left(\left(g^2+1\right)g^4h_{\mathrm{b}}^4mx^2-1\right)}{\left(1+\left(g^2+1\right)g^2mx\right)\left(1+g^2mx\right)\left(1+\left(g^2+1\right)g^2h_{\mathrm{b}}^4x\right)\left(1+g^2h_{\mathrm{b}}^4x\right)}. \tag{B5}$$

From problem (B4), the power constraint can be written as

$$\begin{aligned} x &\le \frac{p_{\mathrm{r}}}{g^2h_{\mathrm{b}}^2\left(g^2+1\right)} \\ &\triangleq x_0. \end{aligned}$$

Let Eq. (B5) be equal to zero. The positive root can be obtained as

$$x_1 = \sqrt{\frac{1}{\left(g^2+1\right)g^4h_{\mathrm{b}}^4m}}. \tag{B6}$$

According to the derivative theory, the results of problem (B4) can be presented as follows:

$$f_{\max} = \begin{cases} 0, & m \ge h_{\mathrm{b}}^4, \\ f(x_0), & m < \min\left(h_{\mathrm{b}}^4, (g^2+1)/p_{\mathrm{r}}^2\right), \\ f(x_1), & \text{otherwise}, \end{cases} \tag{B7}$$

and the corresponding optimal μ_2 is

$$\mu_2 = \begin{cases} 0, & m \ge h_{\mathrm{b}}^4, \\ \sqrt{x_0}, & m < \min\left(h_{\mathrm{b}}^4, (g^2+1)/p_{\mathrm{r}}^2\right), \\ \sqrt{x_1}, & \text{otherwise}. \end{cases} \tag{B8}$$