Secure Relay Beamforming with Correlated Channel Models in Dual-hop Wireless Communication Networks

Zhenhua Yuan*, Chen Chen*, Lin Bai†, Ye Jin*, and Jinho Choi‡
*State Key Laboratory of Advanced Optical Communication Systems and Networks, Peking University, China

†School of Electronic and Information Engineering, Beihang University, China
‡School of Information and Communications,
Gwangju Institute of Science and Technology (GIST), Korea
Email:*{yuanzhenhua, c.chen, yejin}@pku.edu.cn,
†l.bai@buaa.edu.cn, ‡jchoi0114@gist.ac.kr

***Abstract*—In this article, the authors focus on a correlated channel model for secure relay beamforming in the relay-eavesdropper network. In this network, a single-antenna source-destination pair transmits secure information with the help of a amplify-and-forward (AF) relay equipped with multiple antennas. The relay cannot obtain the instantaneous channel state information (CSI) of the eavesdropper. The relay only have the knowledge of correlation information between the legitimate and eavesdropping channels. Depending on this information, we derived the conditional distribution of the eavesdropping channel. Three beamformers at the relay are studied: the zero-forcing (ZF) beamformer, the generalized match-forward (GMF) beamformer and the general-rank beamformer (GRBF). The authors found that the ZF beamformer is invalid in this system, and the GMF beamformer is the optimal rank-1 beamformer, and the GRBF is the iteratively optimal beamformer. Numerical results are presented to illustrate three beamformers' performance, and the impacts of different parameters, especially the channel correlation, on the system performance are analyzed.**

I. Introduction

Security is an important aspect of a wireless communication system due to the broadcast nature of radio propagation.

In 1975, Wyner proposed the wiretap channel model, and proved that when the wiretap channel is a degraded version of the main source-destination channel, the source can send secret messages to the destination without leaking any information to the eavesdropper, by exploiting the physical properties of the channel [1]. Leung-Yan-Cheong *et al.* [2] and Csiszár and Korner [3] respectively generalized Wyner's approach to scenarios with Gaussian channels and broadcast channels. However, physical layer security was not really attractive for researchers in 1980s and 1990s. In a single-antenna system, the secrecy rate is typically zero when the legitimate channel is worse than the eavesdropping channel.

In recent years, many works [4]–[10] have been proposed to avoid that limitation by taking the advantage of multiple antennas. Four cooperative schemes (decode-and-forward (DF), amplify-and-forward (AF), compress-and-forward (CF), cooperative jamming (CJ)) and antenna selection are respectively studied in [4]–[9]. Wang *et al.* designed the optimal and suboptimal relay selection algorithms for backscatter wireless communication systems under the information security constraint [10].

It is noteworthy that most of the previous works of relay wireless networks assumed the legitimate channel and the wiretap channel are independent. However, in practical scenarios, correlations between channels usually exist [11]–[13], depending on antenna deployments, scatters around the legitimate receiver and eavesdropper and so on.

In this paper, we investigate the beamforming schemes to maximize the secrecy capacity of a wireless relay network in which the legitimate channel is correlated with the eavesdropper's. We suppose that the relay with multiple antennas cannot obtain the instantaneous channel state information (CSI) of the eavesdropper's channel, and the legitimate receiver estimates the correlation information between the two channels and feeds it back to the relay.

Notation: We use uppercase and lowercase boldface letters denote matrices and vectors, respectively. $\mathbf{I}_M$ 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. $\mathrm{tr}(\cdot)$ denotes the trace of a matrix. The Kronecker product is denoted as $\otimes$. $\mathrm{vec}(\cdot)$ denotes the column vectorising operator which stacks the columns of a matrix in a column vector, while $\mathrm{unvec}(\cdot)$ is the corresponding inverse-transforming operator.

II. System Model and Problem Formulation

A. System Model

We consider a four-node network, which consists of a source (Alice), a destination (Bob), a relay, and an eavesdropper (Eve). The relay is to help secure transmissions from Alice to Bob. There are no direct channels from Alice to Bob and

978-1-5090-1328-9/16/$31.00 ©2016 IEEE

Eve. Eve is to eavesdrop the signal from the relay to Bob. We consider the following scenarios:

A1) The relay is equipped with M antennas for secure and reliable transmissions to Bob, while Alice, Bob and Eve are equipped with single antenna.

A2) Eve may be close to Bob for eavesdropping, which allows Bob to estimate the Eve's channel and feed it back to the relay.

Let $\mathbf{h}_\mathrm{b}$ denote the channel vector to Bob from the relay. In addition, denote by $\mathbf{h}_\mathrm{e}$ the channel vector to Eve from the relay. According to **A2)**, $\mathbf{h}_\mathrm{b}$ and $\mathbf{h}_\mathrm{e}$ could be correlated and this correlation can be observed by Bob. Note that if Eve is not close to Bob, the two channel vectors are uncorrelated and Bob does not need to know their correlation. Assuming Rayleigh fading, $\mathbf{h}_\mathrm{b}$ and $\mathbf{h}_\mathrm{e}$ can be modeled as jointly circularly symmetric complex Gaussian (CSCG) random vectors:

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

where $\mathbf{R}_{11} = \mathbb{E}\{\mathbf{h}_b\mathbf{h}_b^\mathrm{H}\}$, $\mathbf{R}_{12} = \mathbb{E}\{\mathbf{h}_b\mathbf{h}_e^\mathrm{H}\}$, $\mathbf{R}_{21} = \mathbb{E}\{\mathbf{h}_e\mathbf{h}_b^\mathrm{H}\}$, and $\mathbf{R}_{22} = \mathbb{E}\{\mathbf{h}_e\mathbf{h}_e^\mathrm{H}\}$.

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

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

where $\mathbf{R}$ is Hermitian and positive definite, and denotes the channel correlation matrix, and σ^2 is the variance for each correspondingly independent channel. According to the above discussion, it is easily obtained that $\left[\begin{array}{cc}\mathbf{R}_{11} & \mathbf{R}_{12}\\ \mathbf{R}_{21} & \mathbf{R}_{22}\end{array}\right] = \sigma^2\mathbf{R}$.

At Bob, with knowing its channel vector $\mathbf{h}_\mathrm{b}$, the conditional distribution of $\mathbf{h}_\mathrm{e}$ can be found as [14],

$$\mathbf{h}_\mathrm{e} \mid \mathbf{h}_\mathrm{b} \sim \mathcal{CN}\left(\bar{\mathbf{h}}_e, \bar{\mathbf{R}}_e\right). \tag{3}$$

where $\bar{\mathbf{h}}_e = \mathbf{R}_{21}\mathbf{R}_{11}^{-1}\mathbf{h}_\mathrm{b}$, and $\bar{\mathbf{R}}_e = \mathbf{R}_{22} - \mathbf{R}_{21}\mathbf{R}_{11}^{-1}\mathbf{R}_{12}$. The proof has been omitted.

According to [15], the channel correlation matrix can be divided into two parts, i.e., $\mathbf{R} = \mathbf{R}_r \otimes \mathbf{R}_s$, where $\mathbf{R}_r$ and $\mathbf{R}_s$ are 2×2 and $M \times M$ matrices, and denote the receive and transmit correlation matrix, respectively.

B. 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

$$\mathbf{y}_r = \mathbf{g}s + \mathbf{n}, \tag{4}$$

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

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

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

where n_b and n_e is the background complex Gaussian noise variables at Bob and Eve, respectively.

It is assumed that

$$\begin{aligned} p\left(\mathbf{F}\right) &= \mathrm{tr}\left(\mathbf{F}\mathbf{g}\mathbf{g}^\mathrm{H}\mathbf{F}^\mathrm{H}\right) + \mathrm{tr}\left(\mathbf{F}\mathbf{F}^\mathrm{H}\right)\\ &= \mathrm{tr}\left(\mathbf{F}\hat{\mathbf{G}}\mathbf{F}^\mathrm{H}\right)\\ &\leq p_r, \end{aligned} \tag{7}$$

where $\hat{\mathbf{G}} = \mathbf{G} + \mathbf{I}_\mathbf{M}$, $\mathbf{G} = \mathbf{g}\mathbf{g}^\mathrm{H}$, and p_r is the relay power constraint in the second stage.

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

C. Problem Formulation

In this paper, 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 $\mathbf{F}$, defined as

$$\gamma_b\left(\mathbf{F}\right) = \frac{|\mathbf{h}_b^\mathrm{H}\mathbf{F}\mathbf{g}|^2}{1 + \|\mathbf{h}_b^\mathrm{H}\mathbf{F}\|^2}, \tag{8}$$

and the SNR at Eve, γ_e, as a function of $\mathbf{h}_e$ and $\mathbf{F}$, defined as

$$\gamma_e\left(\mathbf{F}, \mathbf{h}_e\right) = \frac{|\mathbf{h}_e^\mathrm{H}\mathbf{F}\mathbf{g}|^2}{1 + \|\mathbf{h}_e^\mathrm{H}\mathbf{F}\|^2}. \tag{9}$$

For fast fading channels, with $\gamma_b\left(\mathbf{F}\right)$ and $\gamma_e\left(\mathbf{F}, \mathbf{h}_e\right)$ in (8) and (9), for given $\mathbf{h}_\mathrm{b}$, the performance metric can be the ergodic secrecy rate,

$$R_{eg}\left(\mathbf{F}\right) = \frac{1}{2}\left(\begin{array}{l}\log_2(1 + \gamma_b(\mathbf{F})) - \\ \mathbb{E}_{\mathbf{h}_e|\mathbf{h}_b}\left[\log_2(1 + \gamma_e(\mathbf{F}, \mathbf{h}_e))\right]\end{array}\right)^+. \tag{10}$$

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

$$\bar{R}\left(\mathbf{F}\right) = \frac{1}{2}\left(\log(1 + \gamma_b(\mathbf{F})) - \log(1 + \bar{\gamma}_e(\mathbf{F}))\right)^+, \tag{11}$$

where the approximate average SNR at Eve is

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

where $\hat{\mathbf{H}}_e = \bar{\mathbf{H}}_e + \bar{\mathbf{R}}_e$, and $\bar{\mathbf{H}}_e = \bar{\mathbf{h}}_e\bar{\mathbf{h}}_e^\mathrm{H}$.

Note that the same approximation method has been adopted in [16], [17] to maximize the average secrecy rate with imperfect CSI at the transmitter. The beamforming matrix is to maximize the secrecy rate for a given $\mathbf{h}_{\mathrm{b}}$. For convenience, we drop the operator $(\cdot)^{+}$ and the constant coefficient $1/2$. Mathematically, the optimal beamforming problem can be expressed as

$$\begin{aligned} &\max_{\mathbf{F}} \left\{\log(1+\gamma_b(\mathbf{F})) - \log(1+\bar{\gamma}_e(\mathbf{F}))\right\} \\ &s.t.\ \operatorname{tr}\left(\mathbf{F}\hat{\mathbf{G}}\mathbf{F}^{\mathrm{H}}\right) \le p_r. \end{aligned} \tag{13}$$

III. Relay Beamformer Design

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

According to (8), γ_b can be rewritten as

$$\begin{aligned} \gamma_b(\mathbf{F}) &= \frac{\mathbf{g}^{\mathrm{H}}\mathbf{F}^{\mathrm{H}}\mathbf{H}_b\mathbf{F}\mathbf{g}}{1+\operatorname{tr}\left(\mathbf{F}^{\mathrm{H}}\mathbf{H}_b\mathbf{F}\right)} \\ &\overset{a}{=} \frac{\operatorname{vec}(\mathbf{F})^{\mathrm{H}}\operatorname{vec}\left(\mathbf{H}_b\mathbf{F}\mathbf{G}\right)}{1+\operatorname{vec}(\mathbf{F})^{\mathrm{H}}\operatorname{vec}\left(\mathbf{H}_b\mathbf{F}\right)} \\ &\overset{b}{=} \frac{\operatorname{vec}(\mathbf{F})^{\mathrm{H}}\left(\mathbf{G}^{\mathrm{T}}\otimes\mathbf{H}_b\right)\operatorname{vec}(\mathbf{F})}{1+\operatorname{vec}(\mathbf{F})^{\mathrm{H}}\left(\mathbf{I}_M\otimes\mathbf{H}_b\right)\operatorname{vec}(\mathbf{F})}, \end{aligned} \tag{14}$$

where $\mathbf{H}_b = \mathbf{h}_b\mathbf{h}_b^{\mathrm{H}}$. The derivations (a) and (b) come from the theorems $\operatorname{tr}\left(\mathbf{A}^{\mathrm{H}}\mathbf{B}\right) = \operatorname{vec}(\mathbf{A})^{\mathrm{H}}\operatorname{vec}(\mathbf{B})$ and $\operatorname{vec}(\mathbf{A}\mathbf{B}\mathbf{C}) = \left(\mathbf{C}^{\mathrm{T}}\otimes\mathbf{A}\right)\operatorname{vec}(\mathbf{B})$, respectively [18].

So let $\mathbf{w} = \operatorname{vec}(\mathbf{F})$, then

$$\gamma_b(\mathbf{w}) = \frac{\mathbf{w}^{\mathrm{H}}\left(\mathbf{G}^{\mathrm{T}}\otimes\mathbf{H}_b\right)\mathbf{w}}{1+\mathbf{w}^{\mathrm{H}}\left(\mathbf{I}_M\otimes\mathbf{H}_b\right)\mathbf{w}}. \tag{15}$$

In a similar way as (15), $\bar{\gamma}_e$ can be rewritten as

$$\bar{\gamma}_e(\mathbf{w}) = \frac{\mathbf{w}^{\mathrm{H}}\left(\mathbf{G}^{\mathrm{T}}\otimes\hat{\mathbf{H}}_e\right)\mathbf{w}}{1+\mathbf{w}^{\mathrm{H}}\left(\mathbf{I}_M\otimes\hat{\mathbf{H}}_e\right)\mathbf{w}}, \tag{16}$$

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

$$p(\mathbf{w}) = \mathbf{w}^{\mathrm{H}}\left(\hat{\mathbf{G}}^{\mathrm{T}}\otimes\mathbf{I}_M\right)\mathbf{w} \le p_r. \tag{17}$$

Let $\mathbf{H}_{gb} = \mathbf{G}^{\mathrm{T}}\otimes\mathbf{H}_b$, $\mathbf{H}_{ib} = \mathbf{I}_M\otimes\mathbf{H}_b$, $\mathbf{H}_{ge} = \mathbf{G}^{\mathrm{T}}\otimes\hat{\mathbf{H}}_e$, $\mathbf{H}_{ie} = \mathbf{I}_M\otimes\hat{\mathbf{H}}_e$ and $\mathbf{H}_{gi} = \hat{\mathbf{G}}^{\mathrm{T}}\otimes\mathbf{I}_M$. Plugging (15), (16) and (17) into (13), the optimization problem can be rewritten as

$$\begin{array}{cc} \max\limits_{\mathbf{w}} & \left\{\log\left(1+\frac{\mathbf{w}^{\mathrm{H}}\mathbf{H}_{gb}\mathbf{w}}{1+\mathbf{w}^{\mathrm{H}}\mathbf{H}_{ib}\mathbf{w}}\right) - \log\left(1+\frac{\mathbf{w}^{\mathrm{H}}\mathbf{H}_{ge}\mathbf{w}}{1+\mathbf{w}^{\mathrm{H}}\mathbf{H}_{ie}\mathbf{w}}\right)\right\} \\ s.t. & \mathbf{w}^{\mathrm{H}}\mathbf{H}_{gi}\mathbf{w} \le p_r \end{array}. \tag{18}$$

Because of $\mathbf{w} = \operatorname{vec}(\mathbf{F})$, when we get the optimal $\mathbf{w}$, we can obtain the optimal $\mathbf{F}$ by solving $\mathbf{F} = \operatorname{unvec}(\mathbf{w})$.

A. Zero-forcing beamformer design

In this subsection, we first focus on the zero-forcing (ZF) beamformer, and learn the feasibility of the ZF beamformer.

According to the definition of the ZF beamformer, we need design the beamformer to make sure that the approximate channel capacity of Eve reduce to zero, that is $\bar{\gamma}_e(\mathbf{F}) = 0$. According to (12), we can obtain that

$$|\bar{\mathbf{h}}_e^{\mathrm{H}}\mathbf{F}\mathbf{g}|^2 + \mathbf{g}^{\mathrm{H}}\mathbf{F}^{\mathrm{H}}\bar{\mathbf{R}}_e\mathbf{F}\mathbf{g} = 0. \tag{19}$$

It is clear that the first term and the second term of the left-hand expression of (19) are both no less than zero for any $\mathbf{F}$. In order to satisfy the constraint of (19), for the ZF beamformer $\mathbf{F}_{ZF}$ need to satisfy

$$|\bar{\mathbf{h}}_e^{\mathrm{H}}\mathbf{F}_{ZF}\mathbf{g}|^2 = 0, \tag{20}$$

$$\mathbf{g}^{\mathrm{H}}\mathbf{F}_{ZF}^{\mathrm{H}}\bar{\mathbf{R}}_e\mathbf{F}_{ZF}\mathbf{g} = 0. \tag{21}$$

Combining the constraint (20) and the fact $\bar{\mathbf{h}}_e = \mathbf{R}_{21}\mathbf{R}_{11}^{-1}\mathbf{h}_{\mathrm{b}}$, we can obtain the fact that

$$\gamma_{\mathrm{b}}(\mathbf{F}_{ZF}) = 0, \tag{22}$$

i.e., the channel capacity of Bob is zero.

In summary, when the ZF beamformer is adopted for the relay, the secrecy channel capacity of the system is zero all the time.

B. Generalized match-and-forward beamformer design

The zero-forcing beamformer is designed to transmit signals without leaking out to the eavesdropper, while the generalized match-and-forward (GMF) beamformer is designed to use the maximal-ratio-combining(MRC) strategy to make Bob obtain the biggest channel capacity.

Using (5), we can see

$$\begin{aligned} y_{\mathrm{b}} &= \mathbf{h}_{\mathrm{b}}^{\mathrm{H}}\mathbf{F}\mathbf{g}s + \mathbf{h}_{\mathrm{b}}^{\mathrm{H}}\mathbf{F}\mathbf{n} + n_{\mathrm{b}} \\ &= \left(\mathbf{g}^{\mathrm{T}}\otimes\mathbf{h}_{\mathrm{b}}^{\mathrm{H}}\right)\mathbf{w}s + \mathbf{h}_{\mathrm{b}}^{\mathrm{H}}\mathbf{F}\mathbf{n} + n_{\mathrm{b}}. \end{aligned} \tag{23}$$

According to the MRC strategy, we can get that the optimal $\mathbf{w}$ of the generalized MF beamformer is

$$\mathbf{w} = \mu_2\mathbf{q}_{gb}, \tag{24}$$

where $\mathbf{q}_{gb} = \mathbf{g}^{*}\otimes\mathbf{h}_{\mathbf{b}}$, and μ_2 is a scale number which makes sure $\mathbf{w}$ satisfies the power constraint.

Plugging (24) into Problem (18), the problem becomes a single variable optimization problem. According to the theoretical derivation process in Appendix A, the optimal μ can be obtained as

$$\mu_2 = \left\{\begin{array}{cc} 0 & m \ge h_b^4 \\ \sqrt{x_0} & m < \min\left(h_b^4, \frac{g^2+1}{p_r^2}\right) \\ \sqrt{x_1} & \text{else} \end{array}\right., \tag{25}$$

where $h_b = \|\mathbf{h}_b\|$, $g = \|\mathbf{g}\|$, $m = \mathbf{h}_{\mathrm{b}}^{\mathrm{H}}\hat{\mathbf{H}}_e\mathbf{h}_{\mathrm{b}}$, $x_0 = \frac{p_r}{g^2h_b^2(g^2+1)}$ and $x_1 = \sqrt{\frac{1}{(g^2+1)g^4h_b^4m}}$.

As $\mathbf{F} = \operatorname{unvec}(\mathbf{w})$, the generalized match-and-forward beamformer can be rewritten as $\mathbf{F}_{GMF} = \mu_2\mathbf{h}_{\mathbf{b}}\mathbf{g}^{\mathrm{H}}$. Compared with the MF beamformer in [16], it is easily obtained that the generalized match-and-forward beamformer is essentially the MF beamformer in [16], i.e., the optimal rank-1 beamformer. The proof is omitted.

C. General-rank beamformer (GRBF) design

In this subsection, we do not impose any other constraints to the beamforming matrices. By dropping the $\log$ constraint, the optimization problem (18) can be formulated as

$$\begin{array}{cc} \max\limits_{\mathbf{w}} & \frac{1+\mathbf{w}^{\mathrm{H}}(\mathbf{H}_{gb}+\mathbf{H}_{ib})\mathbf{w}}{1+\mathbf{w}^{\mathrm{H}}\mathbf{H}_{ib}\mathbf{w}} \frac{1+\mathbf{w}^{\mathrm{H}}\mathbf{H}_{ie}\mathbf{w}}{1+\mathbf{w}^{\mathrm{H}}(\mathbf{H}_{ie}+\mathbf{H}_{ge})\mathbf{w}} \\ s.t. & \mathbf{w}^{\mathrm{H}}\mathbf{H}_{gi}\mathbf{w} \le p_r \end{array}. \tag{26}$$

We introduce a slacking variable τ which satisfies

$$\tau = \frac{1+\mathbf{w}^{\mathrm{H}}\mathbf{H}_{ie}\mathbf{w}}{1+\mathbf{w}^{\mathrm{H}}\left(\mathbf{H}_{ie}+\mathbf{H}_{ge}\right)\mathbf{w}}. \tag{27}$$

Plugging (27) into (26), for each given τ, (26) can be rewritten as

$$\begin{array}{cc} \max\limits_{\mathbf{w}} & \tau \frac{1+\mathbf{w}^{\mathrm{H}}(\mathbf{H}_{gb}+\mathbf{H}_{ib})\mathbf{w}}{1+\mathbf{w}^{\mathrm{H}}\mathbf{H}_{ib}\mathbf{w}} \\ s.t. & \left\{ \begin{array}{c} \mathbf{w}^{\mathrm{H}}\mathbf{H}_{gi}\mathbf{w} \le p_r \\ \mathbf{w}^{\mathrm{H}}\left(\tau\mathbf{H}_{ge}+(\tau-1)\mathbf{H}_{ie}\right)\mathbf{w} = 1-\tau \end{array} \right. \end{array}. \tag{28}$$

To solve the above problem, Semi-Definite Relaxation (SDR) is used. We define a matrix $\mathbf{W}$ which satisfies $\mathbf{W} = \mathbf{w}\mathbf{w}^{\mathrm{H}}$. Dropping the non-convex rank-1 constraint, (28) becomes

$$\begin{array}{cc} \max\limits_{\mathbf{W}} & \tau \frac{1+\mathrm{tr}((\mathbf{H}_{gb}+\mathbf{H}_{ib})\mathbf{W})}{1+\mathrm{tr}(\mathbf{H}_{ib}\mathbf{W})} \\ s.t. & \left\{ \begin{array}{c} \mathrm{tr}\left(\mathbf{H}_{gi}\mathbf{W}\right) \le p_r \\ \mathrm{tr}\left(\left(\tau\mathbf{H}_{ge}+(\tau-1)\mathbf{H}_{ie}\right)\mathbf{W}\right) = 1-\tau \\ \mathbf{W} \succcurlyeq \mathbf{0} \end{array} \right. \end{array}. \tag{29}$$

The problem (29) is a Quasi-Convex problem, in order to solve this problem, we adopt the Charnes-Cooper transformation. We introduce two variables $\mathbf{Z} \succcurlyeq \mathbf{0}$ and $\eta > 0$, and define that $\mathbf{W} = \frac{\mathbf{Z}}{\eta}$, then the problem (29) can be rewritten as

$$\begin{array}{cc} \max\limits_{\mathbf{Z},\eta} & \tau\left(\eta+\mathrm{tr}\left(\left(\mathbf{H}_{gb}+\mathbf{H}_{ib}\right)\mathbf{Z}\right)\right) \\ s.t. & \left\{ \begin{array}{c} \mathrm{tr}\left(\mathbf{H}_{gi}\mathbf{Z}\right) \le \eta p_r \\ \mathrm{tr}\left(\left(\tau\mathbf{H}_{ge}+(\tau-1)\mathbf{H}_{ie}\right)\mathbf{Z}\right) = \eta(1-\tau) \\ \eta+\mathrm{tr}\left(\mathbf{H}_{ib}\mathbf{Z}\right) = 1 \\ \mathbf{Z} \succcurlyeq \mathbf{0}, \eta > 0 \end{array} \right. \end{array}. \tag{30}$$

Problem (30) is a Semi-Definite Programming (SDP) problem which is convex, it can be solved by many convex optimization tools, such as CVX.

We assume that the optimal result of (30) is denoted by $\phi(\tau)$, for it is calculated with a given τ. In order to obtain the optimal solution of (26), the single-variable optimization problem as

$$\begin{array}{cc} \max\limits_{\tau} & \phi(\tau) \\ s.t. & \tau_{lb} \le \tau \le \tau_{ub} \end{array} \tag{31}$$

need to be solved, where τ_{lb} and τ_{ub} is the lower bound and upper bound, respectively. According to the constraint (27), we can see

$$\begin{aligned} \tau &= \frac{1+\mathbf{w}^{\mathrm{H}}\mathbf{H}_{ie}\mathbf{w}}{1+\mathbf{w}^{\mathrm{H}}\left(\mathbf{H}_{ie}+\mathbf{H}_{ge}\right)\mathbf{w}} \\ &\ge \frac{\mathbf{w}^{\mathrm{H}}\left(\mathbf{H}_{ie}+\frac{\mathbf{H}_{gi}}{p_r}\right)\mathbf{w}}{\mathbf{w}^{\mathrm{H}}\left(\mathbf{H}_{ie}+\mathbf{H}_{ge}+\frac{\mathbf{H}_{gi}}{p_r}\right)\mathbf{w}} \\ &\ge \lambda_{\min}\left(\left(\mathbf{H}_{ie}+\mathbf{H}_{ge}+\frac{\mathbf{H}_{gi}}{p_r}\right)^{-1}\left(\mathbf{H}_{ie}+\frac{\mathbf{H}_{gi}}{p_r}\right)\right) \\ &\triangleq \tau_{lb}, \end{aligned} \tag{32}$$

and

$$\begin{aligned} \tau &= \frac{1+\mathbf{w}^{\mathrm{H}}\mathbf{H}_{ie}\mathbf{w}}{1+\mathbf{w}^{\mathrm{H}}\left(\mathbf{H}_{ie}+\mathbf{H}_{ge}\right)\mathbf{w}} \\ &\le 1 \\ &\triangleq \tau_{ub}. \end{aligned} \tag{33}$$

From (32) and (33), we can see that $\tau = \tau_{lb}$ denotes that Eve's approximate wiretapping channel capacity reaching the best, while $\tau = \tau_{ub}$ denotes that Eve cannot get any information from the channel.

Problem (31) is a one-variable optimization problem. Its optimal solution can be obtained by the one-dimension search algorithm.

Notation: Problem (29) is solved by dropping the rank-1 constraint. We assume that $(\mathbf{Z}^*, \eta^*)$ is the optimal solution of (30), and $\mathbf{W}^* = \frac{\mathbf{Z}^*}{\eta^*}$. If $\mathbf{W}^*$ is rank-1, we can obtain the optimal $\mathbf{w}^*$ via the eigenvalue decomposition of $\mathbf{W}^*$. If the rank of $\mathbf{W}^*$ is larger than one, we can extract an approximate solution $\mathbf{w}^*$ by the Gaussian Randomization procedure [19].

IV. Numerical results

In this section, we show simulation results to present the performance of the proposed relay beamformers. In addition, R_{eg} in (10) for the proposed relay beamformers are also given with high precision numerical methods, and the MF beamformers from [16] is presented for the sake of comparison. In the simulation, we let $g^2 = \|\mathbf{g}\|^2 = 10$ dB.

We assume that the receive correlation matrix $\mathbf{R}_r = \begin{bmatrix} 1 & \varepsilon \\ \varepsilon^* & 1 \end{bmatrix}$. $\varepsilon = 0$ means that the receive channel states of Bob and Eve are independent, while $|\varepsilon| = 1$ means 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, since the relative positions among the relay's antennas could be well designed to reduce their correlation.

In the simulations, the approximate ergodic secrecy rate $\bar{R}$ for ZF beamformer are also obtained like [5] to verify our analysis. For simulations, $\mathbf{g}$ and $\mathbf{h}_{\mathrm{b}}$ are randomly generated for each run, and average values of 1000 runs are used.

Fig. 1 shows the impact of the receive correlation coefficient on the secrecy rate. As expected, $\bar{R}$ for the ZF beamformer is always zero. As observed, the performance of the GRBF overpasses that of the GMF beamformer. When $|\varepsilon|$ increases, $\bar{R}$ decreases for the GRBF and GMF beamformer. Especially,

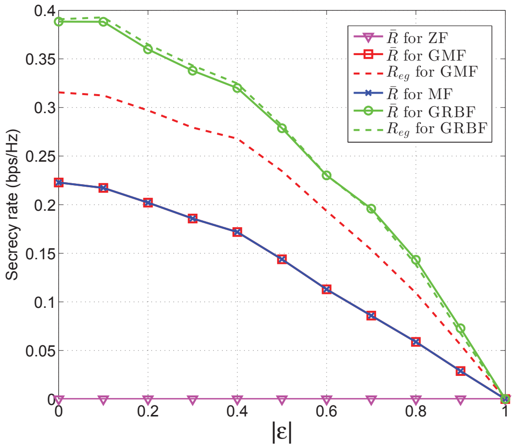

Fig. 1. Approximate ergodic secrecy rate $\bar{R}$, ergodic secrecy rate R_{eg} versus $|\varepsilon|$, $M = 2$, $p_r = 10$ dB, $\sigma^2 = 1$.

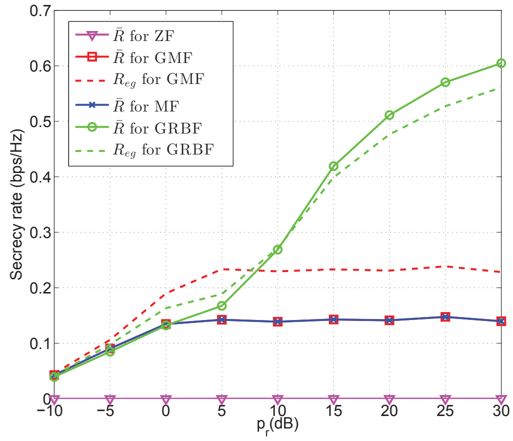

Fig. 2. Approximate ergodic secrecy rate $\bar{R}$, ergodic secrecy rate R_{eg} versus p_r, $M = 2$, $|\varepsilon| = 0.5$, $\sigma^2 = 1$.

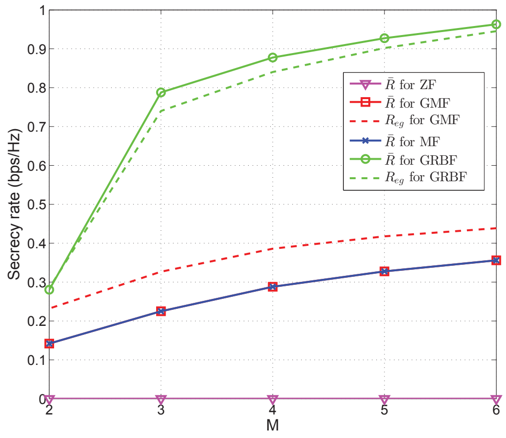

Fig. 3. Approximate ergodic secrecy rate $\bar{R}$, ergodic secrecy rate R_{eg} versus M, $\sigma^2 = 1$, $|\varepsilon| = 0.5$, $p_r = 10$ dB.

when $|\varepsilon| = 0$, i.e., Bob and Eve's channels are independent, $\bar{R}$ for both beamformers reach the biggest, while $|\varepsilon| = 1$, i.e., Bob and Eve's channels are fully correlated, both $\bar{R}$ become zero. Along with the increase of the correlation, it becomes harder to exploit the difference between the channels to transmit secure information. $\bar{R}$ for the MF beamformer is coincident to $\bar{R}$ for the GMF beamformer, which proves that the GMF beamformer is the optimal rank-1 beamformer.

Fig. 2 depicts the curves of system performance versus the relay power p_r. When p_r increases, $\bar{R}$ for the GRBF increases fast, and $\bar{R}$ for the GMF beamformer increases at the beginning, then becomes flat. From (25) we can see that when p_r is low, the performance of the GMF beamformer is improved with the increase of p_r, when p_r is in the high region, the performance of the GMF beamformer is irrelevant to p_r.

Fig. 3 presents the curves of the secrecy rates versus the number of the relay's antennas. When M increases, the performance for the GMF beamformer and the GRBF is both improved, however, the improvement rate becomes lower. That is 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.

V. Conclusion

In this paper, a dual-hop wireless communication system was studied. In this system, the relay was equipped with multiple antennas, and the legitimate channel was correlated with the eavesdropping one. The authors studied three different beamformers at the relay: the ZF beamformer, the GMF beamformer, and the GRBF. It could be found that the ZF beamformer became invalid in this system, the performance of the GRBF was the best, and the GMF had the lower computation complexity.

Acknowledgment

This work is supported in part by the National Science Foundation of China (NSFC, Grant No. 61471008). The correspondence author is Chen Chen (E-mail: c.chen@pku.edu.cn).

Appendix A
Procedure of Obtaining the Optimal μ_2

Substituting (24) into (15), then

$$\begin{aligned}\gamma_b(\mu_2) &= \frac{\mu_2^2 (\mathbf{g}^* \otimes \mathbf{h}_\mathrm{b})^\mathrm{H} \left(\left(\mathbf{g}\mathbf{g}^H\right)^\mathrm{T} \otimes \left(\mathbf{h}_\mathrm{b}\mathbf{h}_\mathrm{b}^\mathrm{H}\right) \right) (\mathbf{g}^* \otimes \mathbf{h}_\mathrm{b})}{1+\mu_2^2 (\mathbf{g}^*\otimes \mathbf{h}_\mathrm{b})^\mathrm{H} \left(\mathbf{I}_M \otimes \left(\mathbf{h}_\mathrm{b}\mathbf{h}_\mathrm{b}^\mathrm{H}\right)\right)(\mathbf{g}^*\otimes\mathbf{h}_\mathrm{b})} \\ &\overset{a}{=} \frac{\mu_2^2 \left(\mathbf{g}^\mathrm{T}\mathbf{g}^*\mathbf{g}^\mathrm{T}\mathbf{g}^*\right)\otimes\left(\mathbf{h}_\mathrm{b}^\mathrm{H}\mathbf{h}_\mathrm{b}\mathbf{h}_\mathrm{b}^\mathrm{H}\mathbf{h}_\mathrm{b}\right)}{1+\mu_2^2\left(\mathbf{g}^\mathrm{T}\mathbf{I}_M\mathbf{g}^*\right)\otimes\left(\mathbf{h}_\mathrm{b}^\mathrm{H}\left(\mathbf{h}_\mathrm{b}\mathbf{h}_\mathrm{b}^\mathrm{H}\right)\mathbf{h}_\mathrm{b}\right)} \\ &= \frac{\mu_2^2 g^4 h_\mathrm{b}^4}{1+\mu_2^2 g^2 h_\mathrm{b}^4}. \end{aligned} \tag{35}$$

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

$$\frac{d\mathrm{f}\left(x\right)}{dx}=\frac{g^4\left(m-h_b^4\right)\left(\left(g^2+1\right)g^4h_b^4mx^2-1\right)}{\left(1+\left(g^2+1\right)g^2mx\right)\left(1+g^2mx\right)\left(1+\left(g^2+1\right)g^2h_b^4x\right)\left(1+g^2h_b^4x\right)} \tag{34}$$

Substituting (24) into (16), then

$$\begin{aligned}\bar{\gamma}_e\left(\mu_2\right)&=\frac{\mu_2^2(\mathbf{g}^*\otimes\mathbf{h}_{\mathrm{b}})^{\mathrm{H}}\left(\left(\mathbf{g}\mathbf{g}^{\mathrm{H}}\right)^{\mathrm{T}}\otimes\hat{\mathbf{H}}_e\right)(\mathbf{g}^*\otimes\mathbf{h}_{\mathrm{b}})}{1+\mu_2^2(\mathbf{g}^*\otimes\mathbf{h}_{\mathrm{b}})^{\mathrm{H}}\left(\mathbf{I}_M\otimes\hat{\mathbf{H}}_e\right)(\mathbf{g}^*\otimes\mathbf{h}_{\mathrm{b}})}\\&=\frac{\mu_2^2g^4m}{1+\mu_2^2g^2m},\end{aligned} \tag{36}$$

where $m=\mathbf{h}_{\mathrm{b}}^{\mathrm{H}}\hat{\mathbf{H}}_e\mathbf{h}_{\mathrm{b}}$ is a constant w.r.t h_{b} and the covariance matrix of $\mathbf{h}$.

Substituting (24) into (17), the power constraint can be written as

$$\begin{aligned}p\left(\mu_2\right)&=\mu_2^2(\mathbf{g}^*\otimes\mathbf{h}_{\mathrm{b}})^{\mathrm{H}}\left(\hat{\mathbf{G}}^{\mathrm{T}}\otimes\mathbf{I}_M\right)\mathbf{g}^*\otimes\mathbf{h}_{\mathrm{b}}\\&=\mu_2^2\left(\mathbf{g}^{\mathrm{T}}\mathbf{g}^*+\mathbf{g}^{\mathrm{T}}\mathbf{g}^*\mathbf{g}^{\mathrm{T}}\mathbf{g}^*\right)\otimes\left(\mathbf{h}_{\mathrm{b}}^{\mathrm{H}}\mathbf{h}_{\mathrm{b}}\right)\\&=\mu_2^2g^2\left(1+g^2\right)h_{\mathrm{b}}^2\\&\le p_r\end{aligned} \tag{37}$$

Plugging (35), (36) and (37) into (13), and let $x=\mu_2^2$, the optimization problem becomes

$$\begin{array}{cc}\max\limits_{x} & \left\{\log\left(1+\frac{g^4h_{\mathrm{b}}^4x}{1+g^2h_{\mathrm{b}}^4x}\right)-\log\left(1+\frac{g^4mx}{1+g^2mx}\right)\right\}\\ s.t. & g^2\left(1+g^2\right)h_{\mathrm{b}}^2x\le p_r\end{array} \tag{38}$$

Let $\mathrm{f}\left(x\right)$ be the objective function of (38), the derivative of $\mathrm{f}\left(x\right)$ w.r.t. x is shown as (34).

From (38), the power constraint can be written as

$$\begin{aligned}x&\le\frac{p_r}{g^2h_b^2\left(g^2+1\right)}\\&\triangleq x_0\end{aligned} \tag{39}$$

Let (34) equal to zero, the positive root can be obtained as

$$x_1=\sqrt{\frac{1}{\left(g^2+1\right)g^4h_b^4m}} \tag{40}$$

According to the derivative theory, the optimum results of (38) can be presented as follows:

$$\mathrm{f}_{max}=\left\{\begin{array}{cc}0 & m\ge h_b^4\\ \mathrm{f}\left(x_0\right) & m<\min\left(h_b^4,\frac{g^2+1}{p_r^2}\right)\\ \mathrm{f}\left(x_1\right) & \text{else}\end{array}\right., \tag{41}$$

and the corresponding optimal μ_2 is

$$\mu_2=\left\{\begin{array}{cc}0 & m\ge h_b^4\\ \sqrt{x_0} & m<\min\left(h_b^4,\frac{g^2+1}{p_r^2}\right)\\ \sqrt{x_1} & \text{else}\end{array}\right.. \tag{42}$$

References

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

[2] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[3] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[4] J. Li, A. Petropulu, and S. Weber, "On Cooperative Relaying Schemes for Wireless Physical Layer Security," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.

[5] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Improving Wireless Physical Layer Security via Cooperating Relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[6] L. Chen, "Physical layer security for cooperative relaying in broadcast networks," in *MILITARY COMMUNICATIONS CONFERENCE, 2011 - MILCOM 2011*, pp. 91–96, Nov. 2011.

[7] J.-H. Lee, "Cooperative Relaying Protocol for Improving Physical Layer Security in Wireless Decode-and-Forward Relaying Networks," *Wireless Personal Communications*, pp. 1–12, Apr. 2015.

[8] L. Song, G. Hong, B. Jiao, and M. Debbah, "Joint Relay Selection and Analog Network Coding Using Differential Modulation in Two-Way Relay Channels," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 6, pp. 2932–2939, Jul. 2010.

[9] H. Zhang, H. Xing, J. Cheng, A. Nallanathan, and V. Leung, "Secure Resource Allocation for OFDMA Two-Way Relay Wireless Sensor Networks Without and With Cooperative Jamming," *IEEE Transactions on Industrial Informatics*, vol. PP, no. 99, pp. 1–1, Oct. 2015.

[10] X. Wang, Z. Su, and G. Wang, "Relay selection for secure backscatter wireless communications," *Electronics Letters*, vol. 51, no. 12, pp. 951–952, 2015.

[11] A. Tulino, A. Lozano, and S. Verdu, "Impact of antenna correlation on the capacity of multiantenna channels," *IEEE Transactions on Information Theory*, vol. 51, no. 7, pp. 2491–2509, Jul. 2005.

[12] N. Ferdinand, D. da Costa, A. de Almeida, and M. Latva-aho, "Physical Layer Secrecy Performance of TAS Wiretap Channels with Correlated Main and Eavesdropper Channels," *IEEE Wireless Communications Letters*, vol. 3, no. 1, pp. 86–89, Feb. 2014.

[13] G. Geraci, A. Al-Nahari, J. Yuan, and I. Collings, "Linear Precoding for Broadcast Channels with Confidential Messages under Transmit-Side Channel Correlation," *IEEE Communications Letters*, vol. 17, no. 6, pp. 1164–1167, Jun. 2013.

[14] M. Barkat, *Signal Detection and Estimation*. Artech House, Jan. 2005.

[15] A.-Y. Kim, H.-N. Cho, J.-W. Lee, and Y.-H. Lee, "Allocation of transmit power in Spatially-correlated dual-hop MIMO relay channels," in *9th International Symposium on Communications and Information Technology, 2009. ISCIT 2009*, pp. 332–336, Sep. 2009.

[16] X. Wang, K. Wang, and X.-D. Zhang, "Secure Relay Beamforming With Imperfect Channel Side Information," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2140–2155, Jun. 2013.

[17] M. Kobayashi and G. Caire, "Joint Beamforming and Scheduling for a Multi-Antenna Downlink with Imperfect Transmitter Channel Knowledge," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 7, pp. 1468–1477, Sep. 2007.

[18] J. R. Magnus and H. Neudecker, *Matrix differential calculus with applications in statistics and econometrics*. Wiley, Apr. 1988.

[19] Z.-Q. Luo, W.-K. Ma, A.-C. So, Y. Ye, and S. Zhang, "Semidefinite Relaxation of Quadratic Optimization Problems," *IEEE Signal Processing Magazine*, vol. 27, no. 3, pp. 20–34, May 2010.