SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

February 2018, Vol. 61 022307:1–022307:10
doi: 10.1007/s11432-017-9110-x

Robust secrecy beamforming for full-duplex two-way relay networks under imperfect channel state information

Si LI[1], Qiang LI[2*] & Shihai SHAO[1]

[1]*National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu* 611731*, China;*
[2]*School of Communication and Information Engineering, University of Electronic Science and Technology of China, Chengdu* 611731*, China*

Received 1 April 2017/Accepted 4 May 2017/Published online 22 September 2017

Abstract Consider a two-way amplify-and-forward (AF) relay network where two legitimate nodes communicate through a relay in the presence of an eavesdropper. Assuming full duplexity at the legitimate nodes and the relay, a robust artificial noise (AN)-aided AF scheme is proposed to maximize the worst-case sum secrecy rate under imperfect channel state information (CSI) of the eavesdropper. This robust sum secrecy rate maximization (SSRM) problem is formulated as a max-min semi-infinite problem and is tackled by the semidefinite relaxation (SDR) method. In particular, we first convert the max-min semi-infinite problem into a maximization problem with a finite number of constraints. Then, an efficient two-block alternating difference-of-concave (DC) programming approach is proposed to iteratively solve the SDR problem, with one of the blocks computed in closed form. In addition, a specific robust rank-one solution construction procedure is presented to extract a feasible solution for the original robust SSRM problem from the SDR solution. The efficacy of the proposed method is demonstrated by numerical simulations.

Keywords physical-layer security, full-duplex relay, difference-of-concave program, semidefinite relaxation, MIMO

Citation Li S, Li Q, Shao S H. Robust secrecy beamforming for full-duplex two-way relay networks under imperfect channel state information. Sci China Inf Sci, 2018, 61(2): 022307, doi: 10.1007/s11432-017-9110-x

1 Introduction

Relay communications have received considerable attention, owing to their capability of enlarging coverage. In the last several decades, extensive studies have been conducted on one-hop relays and multi-hop relays, and more recently on two-way relays. Compared with the one-way relay, a two-way relay can achieve higher spectral efficiency by using the idea of analog network coding to mitigate the self interference (SI) at the user end. Recent advances in SI mitigation techniques make it possible to further improve the spectral efficiency by using full-duplex (FD) relays. Theoretically, an FD relay can provide double the spectral efficiency of a half-duplex relay. Apart from that, full duplexity also provides more design flexibility owing to simultaneous transmission and reception.

Recently, there has been growing interest in applying full duplexity to enhance physical-layer (PHY) security [1–8]. PHY security is a means of achieving confidentiality by using information-theoretic PHY

* Corresponding author (email: lq@uestc.edu.cn)

coding and decoding strategies, without leveraging upper-layer encryption and decryption [9]. In this work, we focus on the PHY secrecy design for FD two-way relay networks, where two FD legitimate nodes exchange confidential information through a trusted FD relay, and an eavesdropper intercepts the transmission. Our goal is to design the forwarding strategy at the relay to prevent information leakage to the eavesdropper during two-way transmissions. Specifically, by assuming erroneous channel state information (CSI) of the eavesdropper, a robust artificial noise (AN)-aided amplify-and-forward (AF) beamforming strategy is proposed to maximize the worst-case sum secrecy rate by jointly optimizing the AN covariance matrix and the AF matrix. This robust sum secrecy rate maximization (SSRM) problem is a nonconvex and semi-infinite problem. By applying a $\mathcal{S}$-procedure, the robust SSRM problem is first reformulated into a form with only a finite number of constraints, and is then relaxed by semidefinite relaxation (SDR). Building upon the relaxation, an alternating difference-of-concave (DC) optimization approach is developed to iteratively solve the relaxed problem. Since the SDR may not be tight, we further present a rank-one solution recovery procedure to extract an approximate solution for the original SSRM problem.

Our contributions are summarized as follows.

(1) A robust AN-aided AF beamforming strategy is proposed to achieve PHY security for FD two-way relay networks.

(2) An SDR-based alternating DC approach is developed to iteratively maximize the worst-case sum secrecy rate, and we show that one of the DC subproblems can be solved efficiently with a closed form.

(3) A novel rank-one solution recovery procedure is proposed to extract a feasible robust solution for the SSRM problem from the SDR solution.

There are some related studies worth mentioning. Two-way relay network beamforming under full and partial CSI was considered in [10, 11]. This work [10] focused on the half-duplex relay with the objective of minimizing the total mean square error (MSE) of two-way relay transmissions. Both full and partial statistical CSI are investigated in [10]. In [11], the authors considered MIMO two-way relays under statistical CSI. By leveraging the Lagrangian multiplier method, an analytical MSE-optimal solution is derived. We should mention that Refs. [10, 11] focus on the MSE performance metric without a secrecy consideration, but in this work we aim for a secrecy-based optimal relaying scheme under a worst-case CSI error model. With regard to PHY security, FD relay secure communications were also considered in [3–5], but their focus was on one-way relay transmission and secrecy outage analysis under different relaying modes, namely, FD jamming and FD transmission. Herein, we consider simultaneous FD transmission and jamming in two-way communications. The most related work is [6]. Different from [6], herein we include the imperfect CSI of the eavesdropper, and aim for a robust secrecy design, whereas Ref. [6] assumes accurate CSI of the eavesdropper, which may not be practical, especially for a passive eavesdropper.

This paper is organized as follows. The system model and problem formulation are given in Section 2. In Section 3, we propose an SDR-based alternating optimization for the robust SSRM problem. Numerical results are given in Section 4. Section 5 concludes the paper.

Our notations are as follows. $(\cdot)^{\mathrm{T}}$ and $(\cdot)^{\mathrm{H}}$ denote the transpose and conjugate transpose, respectively; $\boldsymbol{I}$ denotes an identity matrix with appropriate dimension; $\boldsymbol{A} \succeq \boldsymbol{0}$ means that $\boldsymbol{A}$ is Hermitian positive semidefinite; $\mathrm{Diag}(\boldsymbol{A}, \boldsymbol{B})$ represents a block diagonal matrix with $\boldsymbol{A}$ and $\boldsymbol{B}$ on the main diagonal; $\mathrm{Tr}(\cdot)$ denotes a trace operation, and $\mathcal{CN}(\boldsymbol{a}, \boldsymbol{\Sigma})$ represents a complex Gaussian distribution with mean $\boldsymbol{a}$ and covariance matrix $\boldsymbol{\Sigma}$.

2 System model and problem formulation

Our considered model is similar to [6], where two legitimate nodes, named Alice and Bob, exchange confidential information through an AF relay, and an eavesdropper, named Eve, overhears the transmission from the relay; see Figure 1. We assume that Alice, Bob, and the relay all work in FD mode, and that all nodes have a single transmit antenna and/or receive antenna except for the relay, which employs multiple

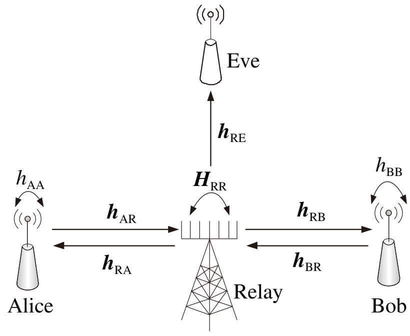

Figure 1 System model.

transmit and receive antennas to perform secure beamforming. Let $\boldsymbol{h}_{\mathrm{AR}} \in \mathbb{C}^M$, $\boldsymbol{h}_{\mathrm{RA}} \in \mathbb{C}^N$ and h_{AA} be the channels between Alice to the relay and the SI channel at Alice, respectively, where N and M represent the number of transmit and receive antennas at the relay, respectively. Similarly, we denote $\boldsymbol{h}_{\mathrm{BR}} \in \mathbb{C}^M$, $\boldsymbol{h}_{\mathrm{RB}} \in \mathbb{C}^N$ and h_{BB} for Bob. Let $x_{\mathrm{A}}(t) \in \mathbb{C}$ and $x_{\mathrm{B}}(t) \in \mathbb{C}$ be transmit signals at Alice and Bob with $\mathrm{E}\{|x_{\mathrm{A}}(t)|^2\} = p_{\mathrm{A}}$ and $\mathrm{E}\{|x_{\mathrm{B}}(t)|^2\} = p_{\mathrm{B}}$. Then, the received signal $\boldsymbol{y}_{\mathrm{R}}(t)$ at the relay consists of the sources' signals and the relay's SI, i.e.,

$$\boldsymbol{y}_{\mathrm{R}}(t) = \boldsymbol{h}_{\mathrm{AR}} x_{\mathrm{A}}(t) + \boldsymbol{h}_{\mathrm{BR}} x_{\mathrm{B}}(t) + \boldsymbol{H}_{\mathrm{RR}} \boldsymbol{x}_{\mathrm{R}}(t) + \boldsymbol{n}_{\mathrm{R}}(t),$$

where $\boldsymbol{H}_{\mathrm{RR}} \in \mathbb{C}^{M\times N}$ is the SI channel at the relay, $\boldsymbol{n}_{\mathrm{R}}(t) \sim \mathcal{CN}(\boldsymbol{0}, \sigma_{\mathrm{R}}^2 \boldsymbol{I})$ is the additive white Gaussian noise, and $\boldsymbol{x}_{\mathrm{R}}(t) \in \mathbb{C}^N$ is the SI arising from in-band FD operation at the relay, which has the following form:

$$\boldsymbol{x}_{\mathrm{R}}(t) = \boldsymbol{W} \boldsymbol{y}_{\mathrm{R}}(t-\tau) + \boldsymbol{z}(t). \tag{1}$$

Herein, $\tau > 0$ is the processing delay at the relay, $\boldsymbol{W} \in \mathbb{C}^{N\times M}$ is the AF matrix employed at the relay, and $\boldsymbol{z}(t)$ is the artificial noise (AN) used for interfering with Eve. We assume $\boldsymbol{z}(t) \sim \mathcal{CN}(\boldsymbol{0}, \boldsymbol{Q})$ with $\boldsymbol{Q} \succeq \boldsymbol{0}$.

Upon (1), the received signal at Alice is expressed as

$$\begin{aligned} y_{\mathrm{A}}(t) &= \boldsymbol{h}_{\mathrm{RA}}^{\mathrm{H}} \boldsymbol{x}_{\mathrm{R}}(t) + h_{\mathrm{AA}} x_{\mathrm{A}}(t) + n_{\mathrm{A}}(t) \\ &= \boldsymbol{h}_{\mathrm{RA}}^{\mathrm{H}} \boldsymbol{W} \boldsymbol{h}_{\mathrm{BR}} x_{\mathrm{B}}(t-\tau) + v(t), \end{aligned} \tag{2}$$

where $v(t) = \boldsymbol{h}_{\mathrm{RA}}^{\mathrm{H}} \boldsymbol{W} \boldsymbol{h}_{\mathrm{AR}} x_{\mathrm{A}}(t-\tau) + h_{\mathrm{AA}} x_{\mathrm{A}}(t) + \boldsymbol{h}_{\mathrm{RA}}^{\mathrm{H}} \boldsymbol{W} \boldsymbol{H}_{\mathrm{RR}} \boldsymbol{x}_{\mathrm{R}}(t-\tau) + \boldsymbol{h}_{\mathrm{RA}}^{\mathrm{H}} \boldsymbol{z}(t) + \boldsymbol{h}_{\mathrm{RA}}^{\mathrm{H}} \boldsymbol{W} \boldsymbol{n}_{\mathrm{R}}(t-\tau) + n_{\mathrm{A}}(t)$. Notice that the term $\boldsymbol{h}_{\mathrm{RA}}^{\mathrm{H}} \boldsymbol{W} \boldsymbol{h}_{\mathrm{AR}} x_{\mathrm{A}}(t-\tau)$ is SI induced by two-way communications, which is approximately at the same power level as the useful signal. Therefore, following the standard two-way relay reception model, $\boldsymbol{h}_{\mathrm{RA}}^{\mathrm{H}} \boldsymbol{W} \boldsymbol{h}_{\mathrm{AR}} x_{\mathrm{A}}(t-\tau)$ can be safely eliminated by Alice herself with a priori knowledge of $x_{\mathrm{A}}(t-\tau)$. The second and the third terms in $v(t)$ are SI induced by FD operations at Alice and the relay. Since the relay has multiple antennas, zero-forcing receive beamforming, i.e., by imposing $\boldsymbol{W}\boldsymbol{H}_{\mathrm{RR}} = \boldsymbol{0}$, can be employed to eliminate $\boldsymbol{h}_{\mathrm{RA}}^{\mathrm{H}} \boldsymbol{W} \boldsymbol{H}_{\mathrm{RR}} \boldsymbol{x}_{\mathrm{R}}(t-\tau)$. However, as for $h_{\mathrm{AA}} x_{\mathrm{A}}(t)$, its power level is overwhelmingly larger than the far-end useful signal, and analog and digital SIC should be leveraged to suppress the $h_{\mathrm{AA}} x_{\mathrm{A}}(t)$ to some extent, but are not completely removed in practice. To take this residual FD SI effect into account, let $0 < \kappa_{\mathrm{A}} < 1$ denote the SI residual factor after the analog and digital SIC at Alice. Then, after two-way SI cancelation and FD SI suppression, the received signal at Alice may be modeled as

$$\hat{y}_{\mathrm{A}}(t) = \boldsymbol{h}_{\mathrm{RA}}^{\mathrm{H}} \boldsymbol{x}_{\mathrm{R}}(t) + \sqrt{\kappa_{\mathrm{A}}} h_{\mathrm{AA}} x_{\mathrm{A}}(t) + \boldsymbol{h}_{\mathrm{RA}}^{\mathrm{H}} \boldsymbol{z}(t) + \boldsymbol{h}_{\mathrm{RA}}^{\mathrm{H}} \boldsymbol{W} \boldsymbol{n}_{\mathrm{R}}(t-\tau) + n_{\mathrm{A}}(t),$$

and the achievable rate at Alice is calculated as

$$R_{\mathrm{A}}(\boldsymbol{W}, \boldsymbol{Q}) = \log\left(1 + \frac{|\boldsymbol{h}_{\mathrm{RA}}^{\mathrm{H}} \boldsymbol{W} \boldsymbol{h}_{\mathrm{BR}}|^2 p_{\mathrm{B}}}{\kappa_{\mathrm{A}} |h_{\mathrm{AA}}|^2 p_{\mathrm{A}} + \sigma_{\mathrm{R}}^2 \|\boldsymbol{h}_{\mathrm{RA}}^{\mathrm{H}} \boldsymbol{W}\|^2 + \boldsymbol{h}_{\mathrm{RA}}^{\mathrm{H}} \boldsymbol{Q} \boldsymbol{h}_{\mathrm{RA}} + \sigma_{\mathrm{A}}^2}\right),$$

where the residual SI is treated as Gaussian noise for simplicity. In the same way, we can express the achievable rate at Bob as

$$R_{\mathrm{B}}(\boldsymbol{W},\boldsymbol{Q}) = \log\left(1 + \frac{|\boldsymbol{h}_{\mathrm{RB}}^{\mathrm{H}}\boldsymbol{W}\boldsymbol{h}_{\mathrm{AR}}|^2 p_{\mathrm{A}}}{\kappa_{\mathrm{B}}|h_{\mathrm{BB}}|^2 p_{\mathrm{B}} + \sigma_{\mathrm{R}}^2\|\boldsymbol{h}_{\mathrm{RB}}^{\mathrm{H}}\boldsymbol{W}\|^2 + \boldsymbol{h}_{\mathrm{RB}}^{\mathrm{H}}\boldsymbol{Q}\boldsymbol{h}_{\mathrm{RB}} + \sigma_{\mathrm{B}}^2}\right)$$

and the achievable sum rate at Eve as

$$R_{\mathrm{E}}(\boldsymbol{W},\boldsymbol{Q}) = \log\left(1 + \frac{|\boldsymbol{h}_{\mathrm{RE}}^{\mathrm{H}}\boldsymbol{W}\boldsymbol{h}_{\mathrm{AR}}|^2 p_{\mathrm{A}} + |\boldsymbol{h}_{\mathrm{RE}}^{\mathrm{H}}\boldsymbol{W}\boldsymbol{h}_{\mathrm{BR}}|^2 p_{\mathrm{B}}}{\sigma_{\mathrm{R}}^2\|\boldsymbol{h}_{\mathrm{RE}}^{\mathrm{H}}\boldsymbol{W}\|^2 + \boldsymbol{h}_{\mathrm{RE}}^{\mathrm{H}}\boldsymbol{Q}\boldsymbol{h}_{\mathrm{RE}} + \sigma_{\mathrm{E}}^2}\right).$$

According to [12], the sum secrecy rate of the two-way relay system is calculated as

$$R_{\mathrm{s}}(\boldsymbol{W},\boldsymbol{Q}) = \left[R_{\mathrm{A}}(\boldsymbol{W},\boldsymbol{Q}) + R_{\mathrm{B}}(\boldsymbol{W},\boldsymbol{Q}) - R_{\mathrm{E}}(\boldsymbol{W},\boldsymbol{Q})\right]^+. \tag{3}$$

Moreover, the total transmit power at the relay is given by

$$p(\boldsymbol{W},\boldsymbol{Q}) = p_{\mathrm{A}}\|\boldsymbol{W}\boldsymbol{h}_{\mathrm{AR}}\|^2 + p_{\mathrm{B}}\|\boldsymbol{W}\boldsymbol{h}_{\mathrm{BR}}\|^2 + \sigma_{\mathrm{R}}^2\|\boldsymbol{W}\|_F^2 + \mathrm{Tr}(\boldsymbol{Q}).$$

In [6], the authors considered the sum secrecy rate optimization under perfect CSIs of all links; however, this could be too ideal, especially for Eve's link. In this work, we focus on imperfect CSI of Eve by adopting the widely used norm-bounded deterministic error model:

$$\boldsymbol{h}_{\mathrm{RE}} = \bar{\boldsymbol{h}}_{\mathrm{RE}} + \Delta\boldsymbol{h}_{\mathrm{RE}}, \tag{4}$$

where $\bar{\boldsymbol{h}}_{\mathrm{RE}}$ is the estimated CSI of Eve, and $\Delta\boldsymbol{h}_{\mathrm{RE}}$ is the estimation error. Herein, we assume that $\Delta\boldsymbol{h}_{\mathrm{RE}}$ lies in an uncertain sphere with radius ϵ, i.e.,

$$\Delta\boldsymbol{h}_{\mathrm{RE}} \in \mathcal{B} \triangleq \{\Delta\boldsymbol{h} \mid \|\Delta\boldsymbol{h}\| \leqslant \epsilon\}.$$

Using the above imperfect CSI model, we aim to design the AF matrix $\boldsymbol{W}$ and the AN covariance $\boldsymbol{Q}$ such that the sum secrecy rate of two-way relay communications is maximized for arbitrary Eve's CSI error $\Delta\boldsymbol{h}_{\mathrm{RE}}$ in $\mathcal{B}$. Mathematically, this robust sum secrecy rate maximization (SSRM) problem may be formulated as the following max-min problem:

$$\max_{\boldsymbol{W},\boldsymbol{Q}} \min_{\Delta\boldsymbol{h}_{\mathrm{RE}}\in\mathcal{B}} \quad \{R_{\mathrm{A}}(\boldsymbol{W},\boldsymbol{Q}) + R_{\mathrm{B}}(\boldsymbol{W},\boldsymbol{Q}) - R_{\mathrm{E}}(\boldsymbol{W},\boldsymbol{Q})\} \tag{5}$$

$$\text{s.t.} \quad p(\boldsymbol{W},\boldsymbol{Q}) \leqslant P_{\mathrm{R}}, \tag{5a}$$

$$\boldsymbol{W}\boldsymbol{H}_{\mathrm{RR}} = \boldsymbol{0}, \tag{5b}$$

where $P_{\mathrm{R}} > 0$ is the maximal transmit power at the relay. Notice that a zero-forcing constraint (5b) is imposed to eliminate the FD SI at the relay, and $M > N$ is implicitly assumed.

The robust SSRM problem (5) is challenging to solve because (1) the uncertainty set $\mathcal{B}$ contains an infinite number of CSI errors, thereby making problem (5) essentially a semi-infinite optimization problem, which is generally hard to solve; and (2) the objective of (5) is nonconcave and depends on the variables $\boldsymbol{W}$ and $\boldsymbol{Q}$ in a highly nonlinear manner. In the following section, we develop a tractable approach to iteratively obtain an approximate solution for (5) by leveraging the SDR technique and the alternating DC programming.

3 SDR-based alternating optimization approach to robust SSRM problem

In this section, we develop an SDR-based alternating optimization approach to the robust SSRM problem (5). Our approach is described as follows.

Since $\Delta\boldsymbol{h}_{\mathrm{RE}}$ appears only in R_{E}, problem (5) can be rewritten as

$$\max_{\boldsymbol{W},\boldsymbol{Q},\gamma_{\mathrm{E}}} \quad R_{\mathrm{A}}(\boldsymbol{W},\boldsymbol{Q}) + R_{\mathrm{B}}(\boldsymbol{W},\boldsymbol{Q}) - \log(1+\gamma_{\mathrm{E}}^{-1}) \tag{6a}$$

$$\text{s.t. } R_{\rm E}(\boldsymbol{W},\boldsymbol{Q}) \leqslant \log(1+\gamma_{\rm E}^{-1}), \quad \forall \Delta \boldsymbol{h}_{\rm RE} \in \mathcal{B}, \tag{6b}$$

$$\text{(5a) and (5b)}, \tag{6c}$$

where $\gamma_{\rm E} \geqslant 0$ is a slack variable introduced to simplify the objective. The main difficulty of problem (6) lies in the constraint (6b). Essentially, it involves an infinite number of inequalities because the uncertainty set $\mathcal{B}$ has an infinite number of elements. To turn (6b) into a more tractable form, let us denote

$$\boldsymbol{\Xi}(\boldsymbol{W},\gamma_{\rm E}) \triangleq p_{\rm A}\gamma_{\rm E}\boldsymbol{W}\boldsymbol{h}_{\rm AR}\boldsymbol{h}_{\rm AR}^{\rm H}\boldsymbol{W}^{\rm H} + p_{\rm B}\gamma_{\rm E}\boldsymbol{W}\boldsymbol{h}_{\rm BR}\boldsymbol{h}_{\rm BR}^{\rm H}\boldsymbol{W}^{\rm H} - \sigma_{\rm R}^2\boldsymbol{W}\boldsymbol{W}^{\rm H}.$$

Then, a simple algebraic calculation shows that the robust constraint (6b) can be rewritten as

$$(\bar{\boldsymbol{h}}_{\rm RE}+\Delta\boldsymbol{h}_{\rm RE})^{\rm H}(\boldsymbol{\Xi}(\boldsymbol{W},\gamma_{\rm E})-\boldsymbol{Q})(\bar{\boldsymbol{h}}_{\rm RE}+\Delta\boldsymbol{h}_{\rm RE}) \leqslant \sigma_{\rm E}^2, \quad \forall \Delta\boldsymbol{h}_{\rm RE}\in\mathcal{B}, \tag{7}$$

or equivalently as the following implication:

$$\Delta\boldsymbol{h}_{\rm RE}\in\mathcal{B} \Longrightarrow (\bar{\boldsymbol{h}}_{\rm RE}+\Delta\boldsymbol{h}_{\rm RE})^{\rm H}(\boldsymbol{\Xi}(\boldsymbol{W},\gamma_{\rm E})-\boldsymbol{Q})(\bar{\boldsymbol{h}}_{\rm RE}+\Delta\boldsymbol{h}_{\rm RE}) \leqslant \sigma_{\rm E}^2. \tag{8}$$

In view of the structure of $\mathcal{B}$ and the quadratic inequality on the right-hand side of (8), the implication in (8) can be further reexpressed as a matrix inequality by applying the following lemma.

Lemma 1 ($\mathcal{S}$-procedure [13])**.** Let

$$f_k(\boldsymbol{x}) = \boldsymbol{x}^{\rm H}\boldsymbol{A}_k\boldsymbol{x} + 2{\rm Re}\{\boldsymbol{b}_k^{\rm H}\boldsymbol{x}\} + c_k$$

for $k=1,2$, where $\boldsymbol{A}_k\in\mathbb{H}^n$, $\boldsymbol{b}_k\in\mathbb{C}^n$, $c_k\in\mathbb{R}$. The implication $f_1(\boldsymbol{x})\leqslant 0 \Rightarrow f_2(\boldsymbol{x})\leqslant 0$ holds if and only if there exists $\mu\geqslant 0$ such that

$$\mu\begin{bmatrix}\boldsymbol{A}_1 & \boldsymbol{b}_1\\ \boldsymbol{b}_1^{\rm H} & c_1\end{bmatrix} - \begin{bmatrix}\boldsymbol{A}_2 & \boldsymbol{b}_2\\ \boldsymbol{b}_2^{\rm H} & c_2\end{bmatrix} \succeq \boldsymbol{0}$$

provided that there exists a point $\hat{\boldsymbol{x}}$ such that $f_1(\hat{\boldsymbol{x}})<0$.

To apply Lemma 1, note that

$$\Delta\boldsymbol{h}_{\rm RE}\in\mathcal{B} \Longleftrightarrow \Delta\boldsymbol{h}_{\rm RE}^{\rm H}\Delta\boldsymbol{h}_{\rm RE}\leqslant\epsilon^2,$$

which together with (8) yields

$$\Delta\boldsymbol{h}_{\rm RE}^{\rm H}\Delta\boldsymbol{h}_{\rm RE}\leqslant\epsilon^2 \Longrightarrow (\bar{\boldsymbol{h}}_{\rm RE}+\Delta\boldsymbol{h}_{\rm RE})^{\rm H}(\boldsymbol{\Xi}(\boldsymbol{W},\gamma_{\rm E})-\boldsymbol{Q})(\bar{\boldsymbol{h}}_{\rm RE}+\Delta\boldsymbol{h}_{\rm RE}) \leqslant \sigma_{\rm E}^2. \tag{9}$$

Now, by setting $\boldsymbol{A}_1=\boldsymbol{I}$, $\boldsymbol{b}_1=\boldsymbol{0}$, $c_1=-\epsilon^2$ and $\boldsymbol{A}_2=\boldsymbol{\Xi}(\boldsymbol{W},\gamma_{\rm E})-\boldsymbol{Q}$, $\boldsymbol{b}_2=(\boldsymbol{\Xi}(\boldsymbol{W},\gamma_{\rm E})-\boldsymbol{Q})\bar{\boldsymbol{h}}_{\rm RE}$, $c_2=\bar{\boldsymbol{h}}_{\rm RE}^{\rm H}(\boldsymbol{\Xi}(\boldsymbol{W},\gamma_{\rm E})-\boldsymbol{Q})\bar{\boldsymbol{h}}_{\rm RE}-\sigma_{\rm E}^2$ and invoking Lemma 1, we can express the robust constraint (6b) as the following equivalent matrix inequality:

$$\begin{bmatrix}\eta\boldsymbol{I} & \\ & \sigma_{\rm E}^2-\eta\epsilon^2\end{bmatrix} \succeq \begin{bmatrix}\boldsymbol{I}\\ \bar{\boldsymbol{h}}_{\rm RE}^{\rm H}\end{bmatrix}(\boldsymbol{\Xi}(\boldsymbol{W},\gamma_{\rm E})-\boldsymbol{Q})\begin{bmatrix}\boldsymbol{I}\\ \bar{\boldsymbol{h}}_{\rm RE}^{\rm H}\end{bmatrix}^{\rm H} \tag{10}$$

for some $\eta\geqslant 0$. Substituting (10) into (6) yields

$$\begin{aligned}\max_{\boldsymbol{W},\boldsymbol{Q},\gamma_{\rm E},\eta\geqslant 0}\quad & R_{\rm A}(\boldsymbol{W},\boldsymbol{Q})+R_{\rm B}(\boldsymbol{W},\boldsymbol{Q})-\log(1+\gamma_{\rm E}^{-1})\\ \text{s.t. }\quad & p(\boldsymbol{W},\boldsymbol{Q})\leqslant P_{\rm R},\\ & \boldsymbol{W}\boldsymbol{H}_{\rm RR}=\boldsymbol{0},\\ & \begin{bmatrix}\eta\boldsymbol{I} & \\ & \sigma_{\rm E}^2-\eta\epsilon^2\end{bmatrix} \succeq \begin{bmatrix}\boldsymbol{I}\\ \bar{\boldsymbol{h}}_{\rm RE}^{\rm H}\end{bmatrix}(\boldsymbol{\Xi}(\boldsymbol{W},\gamma_{\rm E})-\boldsymbol{Q})\begin{bmatrix}\boldsymbol{I}\\ \bar{\boldsymbol{h}}_{\rm RE}^{\rm H}\end{bmatrix}^{\rm H}.\end{aligned} \tag{11}$$

Problem (11) can be expressed into a form suitable for SDR.

Lemma 2. Let $r = \mathrm{rank}(\boldsymbol{H}_{\mathrm{RR}})$ and $\boldsymbol{U}_0 \in \mathbb{C}^{M\times(M-r)}$ be the left singular vectors associated with the zero singular values of $\boldsymbol{H}_{\mathrm{RR}}$. Then, problem (11) can be equivalently written as

$$\max_{\boldsymbol{w},\boldsymbol{Q},\gamma_{\mathrm{E}},\eta} \ f(\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}},\boldsymbol{Q}) - g(\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}},\boldsymbol{Q}) - \log(1+\gamma_{\mathrm{E}}^{-1}) \tag{12}$$

$$\text{s.t. } \boldsymbol{\Psi}(\eta,\gamma_{\mathrm{E}},\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}},\boldsymbol{Q}) \triangleq \begin{bmatrix}\eta\boldsymbol{I} & \\ & \sigma_{\mathrm{E}}^2-\eta\epsilon^2\end{bmatrix} - \begin{bmatrix}\boldsymbol{I}\\ \bar{\boldsymbol{h}}_{\mathrm{RE}}^{\mathrm{H}}\end{bmatrix}\boldsymbol{F}(\gamma_{\mathrm{E}},\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}},\boldsymbol{Q})\begin{bmatrix}\boldsymbol{I}\\ \bar{\boldsymbol{h}}_{\mathrm{RE}}^{\mathrm{H}}\end{bmatrix}^{\mathrm{H}} \succeq \boldsymbol{0}, \tag{12a}$$

$$\mathrm{Tr}(\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}}) + \mathrm{Tr}(\boldsymbol{Q}) \leqslant P_{\mathrm{R}},\ \eta \geqslant 0, \tag{12b}$$

where $\boldsymbol{W} = \mathrm{vec}^{-1}(\boldsymbol{T}^{-\frac{1}{2}}\boldsymbol{w})\boldsymbol{U}_0^{\mathrm{H}}$ with $\mathrm{vec}^{-1}(\cdot)$ being the inverse operation of vectorization,

$$\begin{gathered}
\boldsymbol{T} = p_{\mathrm{A}}(\boldsymbol{U}_0^{\mathrm{T}}\boldsymbol{h}_{\mathrm{AR}}^{*}\otimes\boldsymbol{I})(\boldsymbol{U}_0^{\mathrm{T}}\boldsymbol{h}_{\mathrm{AR}}^{*}\otimes\boldsymbol{I})^{\mathrm{H}} + p_{\mathrm{B}}(\boldsymbol{U}_0^{\mathrm{T}}\boldsymbol{h}_{\mathrm{BR}}^{*}\otimes\boldsymbol{I})(\boldsymbol{U}_0^{\mathrm{T}}\boldsymbol{h}_{\mathrm{BR}}^{*}\otimes\boldsymbol{I})^{\mathrm{H}} + \sigma_{\mathrm{R}}^2\boldsymbol{I},\\
f(\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}},\boldsymbol{Q}) = \textstyle\sum_{i=1}^{2}\log(c_i+\alpha_i(\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}},\boldsymbol{Q})),\\
g(\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}},\boldsymbol{Q}) = \textstyle\sum_{i=1}^{2}\log(c_i+\beta_i(\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}},\boldsymbol{Q})),\\
c_1 = \kappa_{\mathrm{A}}|h_{\mathrm{AA}}|^2 p_{\mathrm{A}} + \sigma_{\mathrm{A}}^2,\\
c_2 = \kappa_{\mathrm{B}}|h_{\mathrm{BB}}|^2 p_{\mathrm{B}} + \sigma_{\mathrm{B}}^2,\\
\alpha_1(\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}},\boldsymbol{Q}) = \beta_1(\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}},\boldsymbol{Q}) + p_{\mathrm{B}}(\boldsymbol{U}_0^{\mathrm{T}}\boldsymbol{h}_{\mathrm{BR}}^{*}\otimes\boldsymbol{h}_{\mathrm{RA}})^{\mathrm{H}}\boldsymbol{T}^{-\frac{1}{2}}\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}}\boldsymbol{T}^{-\frac{1}{2}}(\boldsymbol{U}_0^{\mathrm{T}}\boldsymbol{h}_{\mathrm{BR}}^{*}\otimes\boldsymbol{h}_{\mathrm{RA}}),\\
\alpha_2(\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}},\boldsymbol{Q}) = \beta_2(\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}},\boldsymbol{Q}) + p_{\mathrm{A}}(\boldsymbol{U}_0^{\mathrm{T}}\boldsymbol{h}_{\mathrm{AR}}^{*}\otimes\boldsymbol{h}_{\mathrm{RB}})^{\mathrm{H}}\boldsymbol{T}^{-\frac{1}{2}}\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}}\boldsymbol{T}^{-\frac{1}{2}}(\boldsymbol{U}_0^{\mathrm{T}}\boldsymbol{h}_{\mathrm{AR}}^{*}\otimes\boldsymbol{h}_{\mathrm{RB}}),\\
\beta_1(\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}},\boldsymbol{Q}) = \mathrm{Tr}(\sigma_{\mathrm{R}}^2(\boldsymbol{I}\otimes\boldsymbol{h}_{\mathrm{RA}})^{\mathrm{H}}\boldsymbol{T}^{-\frac{1}{2}}\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}}\boldsymbol{T}^{-\frac{1}{2}}(\boldsymbol{I}\otimes\boldsymbol{h}_{\mathrm{RA}})) + \boldsymbol{h}_{\mathrm{RA}}^{\mathrm{H}}\boldsymbol{Q}\boldsymbol{h}_{\mathrm{RA}},\\
\beta_2(\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}},\boldsymbol{Q}) = \mathrm{Tr}(\sigma_{\mathrm{R}}^2(\boldsymbol{I}\otimes\boldsymbol{h}_{\mathrm{RB}})^{\mathrm{H}}\boldsymbol{T}^{-\frac{1}{2}}\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}}\boldsymbol{T}^{-\frac{1}{2}}(\boldsymbol{I}\otimes\boldsymbol{h}_{\mathrm{RB}})) + \boldsymbol{h}_{\mathrm{RB}}^{\mathrm{H}}\boldsymbol{Q}\boldsymbol{h}_{\mathrm{RB}},\\
\boldsymbol{F}(\gamma_{\mathrm{E}},\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}},\boldsymbol{Q}) = \gamma_{\mathrm{E}}\hat{\boldsymbol{\Xi}}_1(\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}}) - \hat{\boldsymbol{\Xi}}_2(\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}}) - \boldsymbol{Q},\\
\begin{aligned}
\hat{\boldsymbol{\Xi}}_1(\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}}) = {} & p_{\mathrm{A}}(\boldsymbol{U}_0^{\mathrm{T}}\boldsymbol{h}_{\mathrm{AR}}^{*}\otimes\boldsymbol{I})^{\mathrm{H}}\boldsymbol{T}^{-\frac{1}{2}}\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}}\boldsymbol{T}^{-\frac{1}{2}}(\boldsymbol{U}_0^{\mathrm{T}}\boldsymbol{h}_{\mathrm{AR}}^{*}\otimes\boldsymbol{I})\\
& + p_{\mathrm{B}}(\boldsymbol{U}_0^{\mathrm{T}}\boldsymbol{h}_{\mathrm{BR}}^{*}\otimes\boldsymbol{I})^{\mathrm{H}}\boldsymbol{T}^{-\frac{1}{2}}\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}}\boldsymbol{T}^{-\frac{1}{2}}(\boldsymbol{U}_0^{\mathrm{T}}\boldsymbol{h}_{\mathrm{BR}}^{*}\otimes\boldsymbol{I}),
\end{aligned}\\
\hat{\boldsymbol{\Xi}}_2(\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}}) = \sigma_{\mathrm{R}}^2\textstyle\sum_{i=1}^{M-r}\boldsymbol{E}_i\boldsymbol{T}^{-\frac{1}{2}}\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}}\boldsymbol{T}^{-\frac{1}{2}}\boldsymbol{E}_i^{\mathrm{H}}.
\end{gathered}$$

Herein, $\boldsymbol{E}_i \triangleq [\boldsymbol{0}_N,\ldots,\boldsymbol{I}_N,\ldots,\boldsymbol{0}_N] \in \mathbb{R}^{N\times N(M-r)}$ is a zero matrix, except for the columns from $(i-1)N+1$ to iN, which forms an identity matrix $\boldsymbol{I}_N$, and $\otimes$ denotes Kronecker product.

Proof. It follows from (5b) that any feasible $\boldsymbol{W}$ must be in the form of $\boldsymbol{W} = \tilde{\boldsymbol{W}}\boldsymbol{U}_0^{\mathrm{H}}$ for some $\tilde{\boldsymbol{W}} \in \mathbb{C}^{N\times(M-r)}$. Plugging $\tilde{\boldsymbol{W}}\boldsymbol{U}_0^{\mathrm{H}}$ into (5a), the total power is expressed as $p(\tilde{\boldsymbol{W}},\boldsymbol{Q}) = \tilde{\boldsymbol{w}}^{\mathrm{H}}\boldsymbol{T}\tilde{\boldsymbol{w}} + \mathrm{Tr}(\boldsymbol{Q}) = \mathrm{Tr}(\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}}) + \mathrm{Tr}(\boldsymbol{Q})$, where $\tilde{\boldsymbol{w}} = \mathrm{vec}(\tilde{\boldsymbol{W}})$ and $\boldsymbol{w} = \boldsymbol{T}^{\frac{1}{2}}\tilde{\boldsymbol{w}}$. From the definition of $\boldsymbol{w}$, it is clear $\boldsymbol{W} = \mathrm{vec}^{-1}(\boldsymbol{T}^{-\frac{1}{2}}\boldsymbol{w})\boldsymbol{U}_0^{\mathrm{H}}$. Then, after some tedious matrix manipulations, one can express R_{A}, R_{B} and (10) into the desired form in (12).

By denoting $\boldsymbol{\mathcal{W}} = \boldsymbol{w}\boldsymbol{w}^{\mathrm{H}}$ and dropping the rank-one constraint on $\boldsymbol{\mathcal{W}}$, we get an SDR of (12):

$$\max_{\boldsymbol{\mathcal{W}},\boldsymbol{Q},\gamma_{\mathrm{E}},\eta} \ f(\boldsymbol{\mathcal{W}},\boldsymbol{Q}) - g(\boldsymbol{\mathcal{W}},\boldsymbol{Q}) - \log(1+\gamma_{\mathrm{E}}^{-1}) \tag{13a}$$

$$\text{s.t. } \boldsymbol{\Psi}(\eta,\gamma_{\mathrm{E}},\boldsymbol{\mathcal{W}},\boldsymbol{Q}) \succeq \boldsymbol{0},\quad \eta \geqslant 0, \tag{13b}$$

$$\mathrm{Tr}(\boldsymbol{\mathcal{W}}) + \mathrm{Tr}(\boldsymbol{Q}) \leqslant P_{\mathrm{R}},\ \boldsymbol{\mathcal{W}} \succeq \boldsymbol{0},\ \boldsymbol{Q} \succeq \boldsymbol{0}. \tag{13c}$$

The objective of (13) is in the difference-of-concave (DC) form, and the constraints are convex except for (13b), where γ_{E} and $\boldsymbol{\mathcal{W}}$ are coupled. However, fixing either γ_{E} or $\boldsymbol{\mathcal{W}}$, constraints (13b) and (13c) are convex with respect to the remaining variables. In light of this, we proposed an alternating DC (ADC) approach to handling problem (13). Specifically, given some initial point $(\boldsymbol{\mathcal{W}}^0,\boldsymbol{Q}^0,\eta^0,\gamma_{\mathrm{E}}^0)$, we repeatedly solve the following two problems:

- Fix γ_{E}^k and optimize $(\boldsymbol{\mathcal{W}},\boldsymbol{Q},\eta)$

$$\begin{aligned}
(\boldsymbol{\mathcal{W}}^{k+1},\boldsymbol{Q}^{k+1},\eta^{k+1}) = \mathrm{argmax}_{\boldsymbol{\mathcal{W}},\boldsymbol{Q},\eta}\ & f(\boldsymbol{\mathcal{W}},\boldsymbol{Q}) - \mathrm{Tr}(\nabla_{\boldsymbol{\mathcal{W}}}g(\boldsymbol{\mathcal{W}}^k,\boldsymbol{Q}^k)^{\mathrm{H}}\boldsymbol{\mathcal{W}})\\
& - \mathrm{Tr}(\nabla_{\boldsymbol{Q}}g(\boldsymbol{\mathcal{W}}^k,\boldsymbol{Q}^k)^{\mathrm{H}}\boldsymbol{Q}) - g(\boldsymbol{\mathcal{W}}^k,\boldsymbol{Q}^k)\\
\text{s.t.}\quad & \boldsymbol{\Psi}(\eta,\gamma_{\mathrm{E}}^k,\boldsymbol{\mathcal{W}},\boldsymbol{Q}) \succeq \boldsymbol{0},\quad \eta \geqslant 0,\\
& \mathrm{Tr}(\boldsymbol{\mathcal{W}}) + \mathrm{Tr}(\boldsymbol{Q}) \leqslant P_{\mathrm{R}},\ \boldsymbol{\mathcal{W}} \succeq \boldsymbol{0},\ \boldsymbol{Q} \succeq \boldsymbol{0}.
\end{aligned} \tag{14}$$

- Fix $(\boldsymbol{\mathcal{W}}^{k+1}, \boldsymbol{Q}^{k+1}, \eta^{k+1})$ and optimize $\gamma_{\rm E}$,

$$\gamma_{\rm E}^{k+1} = \mathrm{argmax}_{\gamma_{\rm E}}\ \gamma_{\rm E} \quad \text{s.t. } \boldsymbol{\Psi}(\eta^{k+1}, \gamma_{\rm E}, \boldsymbol{\mathcal{W}}^{k+1}, \boldsymbol{Q}^{k+1}) \succeq \boldsymbol{0}, \tag{15}$$

for $k = 0, 1, 2, \ldots$, until some stopping criterion is satisfied.

Problem (14) is a convex optimization problem, which can be efficiently solved with interior-point methods [14], e.g., an off-the-shelf solver CVX[1)]. Meanwhile, problem (15) can be solved in closed form, as revealed in the following lemma.

Lemma 3. Problem (15) has a closed-form solution

$$\gamma_{\rm E}^{k+1} = \lambda_{\max}^{-1}\left(\left[\boldsymbol{A}^{k+1}\right]^{\dagger}\begin{bmatrix}\boldsymbol{I}\\ \bar{\boldsymbol{h}}_{\rm RE}^{\rm H}\end{bmatrix}\hat{\boldsymbol{\Xi}}_1^{k+1}\begin{bmatrix}\boldsymbol{I}\\ \bar{\boldsymbol{h}}_{\rm RE}^{\rm H}\end{bmatrix}^{\rm H}\right),$$

where $\boldsymbol{A}^{k+1} \triangleq \mathrm{Diag}\left(\eta^{k+1}\boldsymbol{I},\ \ \sigma_{\rm E}^2 - \eta^{k+1}\epsilon^2\right) + \left[\begin{smallmatrix}\boldsymbol{I}\\ \bar{\boldsymbol{h}}_{\rm RE}^{\rm H}\end{smallmatrix}\right](\boldsymbol{Q}^{k+1} + \hat{\boldsymbol{\Xi}}_2^{k+1})\left[\begin{smallmatrix}\boldsymbol{I}\\ \bar{\boldsymbol{h}}_{\rm RE}^{\rm H}\end{smallmatrix}\right]^{\rm H}$, $\lambda_{\max}$ and $(\cdot)^{\dagger}$ represent the maximum eigenvalue and the Moore-Penrose pseudoinverse, respectively. For notational simplicity, we used $\hat{\boldsymbol{\Xi}}_i^{k+1}$ to represent $\hat{\boldsymbol{\Xi}}_i(\boldsymbol{\mathcal{W}}^{k+1}), i = 1, 2$.

Proof. The constraint in (15) amounts to

$$\begin{aligned}
&\boldsymbol{A}^{k+1} \succeq \gamma_{\rm E}\begin{bmatrix}\boldsymbol{I}\\ \bar{\boldsymbol{h}}_{\rm RE}^{\rm H}\end{bmatrix}(\hat{\boldsymbol{\Xi}}_1^{k+1})^{\frac{1}{2}}(\hat{\boldsymbol{\Xi}}_1^{k+1})^{\frac{1}{2}}\begin{bmatrix}\boldsymbol{I}\\ \bar{\boldsymbol{h}}_{\rm RE}^{\rm H}\end{bmatrix}^{\rm H}\\
&\Longleftrightarrow \begin{bmatrix}\boldsymbol{A}^{k+1} & \begin{bmatrix}\boldsymbol{I}\\ \bar{\boldsymbol{h}}_{\rm RE}^{\rm H}\end{bmatrix}(\hat{\boldsymbol{\Xi}}_1^{k+1})^{\frac{1}{2}}\\ (\hat{\boldsymbol{\Xi}}_1^{k+1})^{\frac{1}{2}}\begin{bmatrix}\boldsymbol{I} & \bar{\boldsymbol{h}}_{\rm RE}\end{bmatrix} & \gamma_{\rm E}^{-1}\boldsymbol{I}\end{bmatrix} \succeq \boldsymbol{0}\\
&\Longleftrightarrow \gamma_{\rm E}^{-1}\boldsymbol{I} \succeq (\hat{\boldsymbol{\Xi}}_1^{k+1})^{\frac{1}{2}}\begin{bmatrix}\boldsymbol{I}\\ \bar{\boldsymbol{h}}_{\rm RE}^{\rm H}\end{bmatrix}^{\rm H}\left[\boldsymbol{A}^{k+1}\right]^{\dagger}\begin{bmatrix}\boldsymbol{I}\\ \bar{\boldsymbol{h}}_{\rm RE}^{\rm H}\end{bmatrix}(\hat{\boldsymbol{\Xi}}_1^{k+1})^{\frac{1}{2}}\\
&\Longleftrightarrow \gamma_{\rm E} \leqslant \lambda_{\max}^{-1}\left(\left[\boldsymbol{A}^{k+1}\right]^{\dagger}\begin{bmatrix}\boldsymbol{I}\\ \bar{\boldsymbol{h}}_{\rm RE}^{\rm H}\end{bmatrix}\hat{\boldsymbol{\Xi}}_1^{k+1}\begin{bmatrix}\boldsymbol{I}\\ \bar{\boldsymbol{h}}_{\rm RE}^{\rm H}\end{bmatrix}^{\rm H}\right),
\end{aligned}$$

where the last two steps follow from Schur's complement [15].

Regarding the above alternating optimization, the following result is readily established.

Proposition 1. The iterate $(\boldsymbol{\mathcal{W}}^k, \boldsymbol{Q}^k, \eta^k, \gamma_{\rm E}^k), k = 0, 1, \ldots$, generated by (14) and (15), yields a nondecreasing objective value for (13). Thus, the alternating optimization process converges (in the sense of the objective value).

Proof. Since $(\boldsymbol{\mathcal{W}}^k, \boldsymbol{Q}^k, \eta^k)$ is a feasible solution of (14) and the first-order approximation of $g(\boldsymbol{\mathcal{W}}, \boldsymbol{Q})$ is tight at $(\boldsymbol{\mathcal{W}}^k, \boldsymbol{Q}^k)$, we have

$$\begin{aligned}
&f(\boldsymbol{\mathcal{W}}^k, \boldsymbol{Q}^k) - g(\boldsymbol{\mathcal{W}}^k, \boldsymbol{Q}^k) - \log\left(1 + \frac{1}{\gamma_{\rm E}^k}\right)\\
&\leqslant f(\boldsymbol{\mathcal{W}}^{k+1}, \boldsymbol{Q}^{k+1}) - g(\boldsymbol{\mathcal{W}}^{k+1}, \boldsymbol{Q}^{k+1}) - \log\left(1 + \frac{1}{\gamma_{\rm E}^k}\right)\\
&\leqslant f(\boldsymbol{\mathcal{W}}^{k+1}, \boldsymbol{Q}^{k+1}) - g(\boldsymbol{\mathcal{W}}^{k+1}, \boldsymbol{Q}^{k+1}) - \log\left(1 + \frac{1}{\gamma_{\rm E}^{k+1}}\right),
\end{aligned}$$

where the last inequality is a result of the optimality of $\gamma_{\rm E}^{k+1}$ for problem (15). Moreover, owing to the power constraint, the sum secrecy rate must be upper bounded, and thus it follows from the monotone convergence theorem that the iterate leads to a convergent objective value of (13a).

1) Grant M, Boy S. CVX: Matlab software for disciplined convex programming. 2014. http://cvxr.com/cvx/.

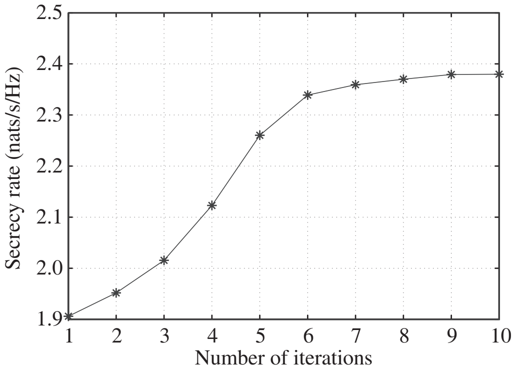

Figure 2 Secrecy rate vs. iteration number.

In general, the SDR (13) may not be tight. In such a case, one needs to extract a feasible rank-one solution for (12) from the high-rank SDR solution. Below, we give a particular way to construct a feasible rank-one $\boldsymbol{\mathcal{W}}$ for problem (12).

Proposition 2. Let $(\boldsymbol{\mathcal{W}}^o, \boldsymbol{Q}^o, \eta^o, \gamma_{\rm E}^o)$ be a solution of the SDR problem (13), and $\boldsymbol{\mathcal{W}}^o = \sum_{l=1}^{s} \boldsymbol{w}_l^o \boldsymbol{w}_l^{o\rm H}$ with $s \geqslant 2$ being the rank of $\boldsymbol{\mathcal{W}}^o$. Pick an arbitrary $l \in \{1, \dots, s\}$ and let $\breve{\boldsymbol{w}} = \boldsymbol{w}_l^o$ and $\breve{\boldsymbol{Q}} = \boldsymbol{Q}^o + \sigma_{\rm R}^2 \sum_{j \neq l} \sum_{i=1}^{M-r} \boldsymbol{E}_i \boldsymbol{T}^{-1/2} \boldsymbol{w}_j^o \boldsymbol{w}_j^{o\rm H} \boldsymbol{T}^{-1/2} \boldsymbol{E}_i^{\rm H}$. Then, $(\breve{\boldsymbol{w}}, \breve{\boldsymbol{Q}}, \eta^o, \gamma_{\rm E}^o)$ is feasible for problem (12).

Proof. It follows from the definition of $\boldsymbol{F}(\gamma_{\rm E}, \boldsymbol{\mathcal{W}}, \boldsymbol{Q})$ that $\boldsymbol{F}(\gamma_{\rm E}^o, \boldsymbol{\mathcal{W}}^o, \boldsymbol{Q}^o) \succeq \boldsymbol{F}(\gamma_{\rm E}^o, \breve{\boldsymbol{w}}\breve{\boldsymbol{w}}^{\rm H}, \breve{\boldsymbol{Q}})$ holds. Hence, $(\breve{\boldsymbol{w}}\breve{\boldsymbol{w}}^{\rm H}, \breve{\boldsymbol{Q}}, \eta^o, \gamma_{\rm E}^o)$ fulfills (13b) [also (12a)]. Moreover, we have

$$\begin{aligned}
\mathrm{Tr}(\breve{\boldsymbol{Q}}) &= \mathrm{Tr}(\boldsymbol{Q}^o) + \sigma_{\rm R}^2 \sum_{j \neq l} \mathrm{Tr}\left(\sum_{i=1}^{M-r} \boldsymbol{E}_i \boldsymbol{T}^{-1/2} \boldsymbol{w}_j^o \boldsymbol{w}_j^{o\rm H} \boldsymbol{T}^{-1/2} \boldsymbol{E}_i^{\rm H} \right) \\
&= \mathrm{Tr}(\boldsymbol{Q}^o) + \sigma_{\rm R}^2 \sum_{j \neq l} \mathrm{Tr}\left(\boldsymbol{T}^{-1/2} \boldsymbol{w}_j^o \boldsymbol{w}_j^{o\rm H} \boldsymbol{T}^{-1/2} \right) \\
&= \mathrm{Tr}(\boldsymbol{Q}^o) + \sigma_{\rm R}^2 \sum_{j \neq l} \mathrm{Tr}\left(\boldsymbol{w}_j^o \boldsymbol{w}_j^{o\rm H} \boldsymbol{T}^{-1} \right) \\
&\leqslant \mathrm{Tr}(\boldsymbol{Q}^o) + \sum_{j \neq l} \mathrm{Tr}\left(\boldsymbol{w}_j^o \boldsymbol{w}_j^{o\rm H} \right),
\end{aligned}$$

where the second equality is because $\boldsymbol{T}^{-1/2} \boldsymbol{w}_j^o \boldsymbol{w}_j^{o\rm H} \boldsymbol{T}^{-1/2}$ and $\sum_{i=1}^{M-r} \boldsymbol{E}_i \boldsymbol{T}^{-1/2} \boldsymbol{w}_j^o \boldsymbol{w}_j^{o\rm H}\ \boldsymbol{T}^{-1/2} \boldsymbol{E}_i^{\rm H}$ have the same diagonal elements, and the last inequality is a result of $\boldsymbol{T} \succeq \sigma_{\rm R}^2 \boldsymbol{I}$ (cf. the definition of $\boldsymbol{T}$ in Claim 2). Therefore, $(\breve{\boldsymbol{w}}, \breve{\boldsymbol{Q}})$ also satisfies the power constraint (12b).

4 Numerical results

We use Monte Carlo simulations to evaluate the performances of the proposed robust design. Our default simulation settings are as follows, unless otherwise specified: $(N, M) = (3, 6)$, $\kappa_{\rm A} = \kappa_{\rm B} = \kappa = 0.01$, $\sigma_{\rm A} = \sigma_{\rm B} = \sigma_{\rm E} = 1$, $p_{\rm A} = p_{\rm B} = 10$ dB, $P_{\rm R} = 15$ dB, $\epsilon = 0.5$. All channels are randomly generated following standard i.i.d. complex Gaussian distribution.

Figure 2 shows the convergence behavior of the proposed robust design for one random channel realization. From the figure, we see that the secrecy rate increases monotonically and becomes stable after eight iterations. This observation is consistent with Proposition 1. We also tested the convergence of the algorithm under different settings, and the results were basically the same as Figure 2, i.e., after tens of iterations the secrecy rate becomes stable.

In the second example, we investigate the secrecy rate performance of different methods when the source power at Alice and Bob is increased. The result is shown in Figure 3. To make a comparison, we also include the perfect CSI-based design in [6] and its nonrobust version based on estimated CSI

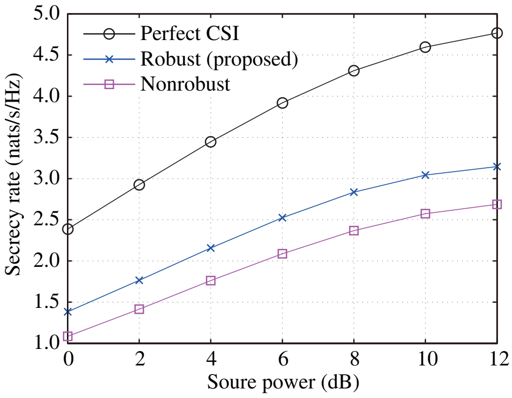

Figure 3 (Color online) Secrecy rate vs. source power.

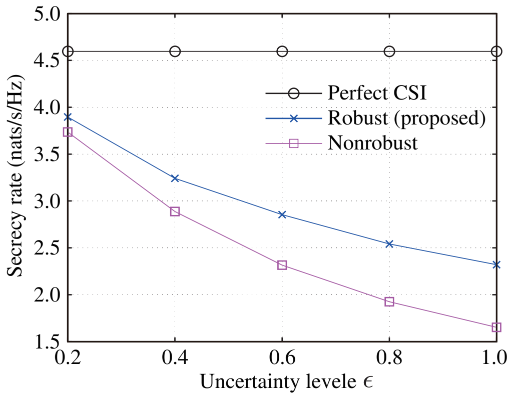

Figure 4 (Color online) Secrecy rate vs. ϵ.

$\bar{\boldsymbol{h}}_{\mathrm{RE}}$. Specifically, the perfect CSI-based design in [6] assumes that accurate CSI of Eve is available, and that the sum secrecy rate is optimized under the perfect CSI case. However, it should be noted that in practice, the perfect CSI is usually not available, and thus the perfect CSI-based design serves as a benchmark and provides an upper bound on the worst-case sum secrecy rate. For a nonrobust design, the relay ignores the CSI uncertainty and presumes the estimated CSI $\bar{\boldsymbol{h}}_{\mathrm{RE}}$ as the "true" CSI. Clearly, owing to ignoring the CSI imperfection, it is expected that the nonrobust design cannot attain a satisfactory secrecy performance. From Figure 3, we have the following observations: (1) The secrecy rates of all three methods increase as the source power changes from 0 dB to 12 dB. In particular, the secrecy rates of the three methods increase quickly for the small power region ($\leqslant$ 8 dB), but when the source power exceeds 8 dB, the secrecy rates tend to be flattened. (2) As expected, the perfect CSI-based design attains the best secrecy rate among the three; however, when there is CSI uncertainty, its nonrobust version's secrecy rate degrades significantly, say from 4.8 to 2.6 nats/s/Hz at a power level 12 dB. This implies that the perfect CSI-based design is very sensitive to CSI errors and cannot provide satisfactory robust secrecy performance.

In the last example, we study the relationship between the sum secrecy rate and the CSI uncertainty level ϵ. The result is shown in Figure 4. Since the perfect CSI-based design is independent of ϵ, its secrecy rate is constant over all ϵ. However, the performance of nonrobust design and the proposed robust design are degraded as ϵ increases. Nevertheless, we see from Figure 4 that the rate gap between the nonrobust and the robust designs is enlarged as ϵ increases. In particular, for $\epsilon = 0.2$ there is a negligible rate gap between the two methods; however, when $\epsilon = 1$, the robust design outperforms the nonrobust one by nearly 0.8 nats/s/Hz. This enlarged rate gap between the robust and nonrobust designs implies that the robust design is less sensitive to the CSI uncertainty than the nonrobust one, because the former already takes the CSI uncertainty into account in the precoder design, whereas the latter does not.

5 Conclusion

This paper considered a worst-case sum secrecy rate maximization (SSRM) problem for a two-way full duplex relay network under the imperfect CSI of an eavesdropper (Eve). A robust artificial-noise (AN)-aided amplify-and-forward scheme is proposed to alternately optimize the legitimate receptions and those of Eve. This alternating optimization gradually improves the sum secrecy rate. By comparing it with a nonrobust design, the proposed robust design can achieve better secrecy gains, especially for a large Eve's CSI uncertainty.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61401073, 61531009).

Conflict of interest The authors declare that they have no conflict of interest.

References

1 Zheng G, Krikidis I, Li J, et al. Improving physical layer secrecy using full-duplex jamming receivers. IEEE Trans Sig Process, 2013, 61: 4962–4974

2 Sun Y, Ng D W K, Zhu J, et al. Multi-objective optimization for robust power efficient and secure full-duplex wireless communication systems. IEEE Trans Wirel Commun, 2016, 15: 5511–5526

3 Parsaeefard S, Le-Ngoc T. Improving wireless secrecy rate via full-duplex relay-assisted protocols. IEEE Trans Inf Foren Sec, 2015, 10: 2095–2107

4 Chen G, Gong Y, Xiao P, et al. Physical layer network security in the full-duplex relay system. IEEE Trans Inf Foren Sec, 2015, 10: 574–583

5 Lee J. Full-duplex relay for enhancing physical layer security in multi-hop relaying systems. IEEE Commun Lett, 2015, 19: 525–528

6 Li Q, Han D. Sum secrecy rate maximization for full-duplex two-way relay networks. In: Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing, Shanghai, 2016. 3641–3645

7 Gong S Q, Xing C W, Fei Z S, et al. Cooperative beamforming design for physical-layer security of multi-hop MIMO communications. Sci China Inf Sci, 2016, 59: 062304

8 Zhao R, Lin H X, He Y C, et al. Impacts of outdated CSI for secure cooperative systems with opportunistic relay selection. Sci China Inf Sci, 2017, 60: 069303

9 Liang Y, Poor H V, Shamai S. Information theoretic Ssecurity. Found Trends Commun Inf Theory, 2008, 5: 355–580

10 Li C, Yang L, Zhu W-P. Minimum mean squared error design of single-antenna two-way distributed relays based on full or partial channel state information. IET Commun, 2011, 5: 728–735

11 Li C, Yang L, Zhu W-P. A two-way MIMO relaying scheme with partial channel state information. Wirel Pers Commun, 2013, 72: 1949–1968

12 Tekin E, Yener A. The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming. IEEE Trans Inf Theory, 2008, 54: 2735–2751

13 Boyd S, Vandenberghe L. Convex Optimization. Cambridge: Cambridge University Press, 2004

14 Wright S. Primal-Dual Interior-Point Methods. Philadelphia: SIAM, 1997

15 VanAntwerp J, Braat R. A tutorial on linear and bilinear matrix inequalities. J Process Contr, 2000, 10: 363–385