SUM SECRECY RATE MAXIMIZATION FOR FULL-DUPLEX TWO-WAY RELAY NETWORKS

Qiang Li[⋆] *and Dong Han*[‡]

[⋆]School of Comm. & Info. Eng., University of Electronic Science & Technology of China, P. R. China
[‡]Dept. of Electrical & Computer Engineering, The National University of Singapore
E-mail: lq@uestc.edu.cn, E0012343@u.nus.edu

ABSTRACT

Consider a full-duplex two-way relay network, where two legitimate nodes simultaneously transmit and receive confidential information through a full-duplex multiantenna relay, in the presence of an eavesdropper. To secure the communications, an artificial-noise (AN)-aided amplify-and-forward (AF) strategy is employed at the relay, with a goal of maximizing the sum secrecy rate of the two-way transmissions. This sum secrecy rate maximization (SSRM) problem is nonconvex by nature, but can be converted into the form of the difference-of-concave (DC) functions after the semidefinite relaxation (SDR). Thus, the classical DC programming naturally applies. We prove that the SDR is tight and give a specific way to recover a stationary solution of the SSRM problem from the relaxed DC problem. Moreover, to reduce the iteration complexity of DC, we proposed an inexact DC framework, which uses an approximate solution to iterate, rather than a globally optimal one. The convergence of the inexact DC to a stationary solution of the SSRM problem is also established.

Index Terms— physical-layer security, full-duplex relay, DC program, semidefinite relaxation

1. INTRODUCTION

With the recent advances of self-interference cancelation (SIC) techniques [1], full-duplex (FD) communications have gained renewed interest, owing to its potential to double the spectral efficiency by simultaneously transmitting and receiving (STR) over the same frequency bands. Besides the spectral efficiency improvement, this new STR feature also provides new opportunities for system designs to achieve some specific goals, such as physical-layer (PHY) security. PHY security is a means of securing communications at the PHY without bothering the high-layer encryption and decryption. To achieve PHY security, it is usually required that the legitimate user should have better reception quality than the eavesdropper. An effective way to achieve this is to intentionally send artificial noise (AN) to jam the eavesdropper's reception. This transmitter-side jamming strategy has been widely studied in the PHY literature; see [2–4] and the references therein. More recently, the work [5] proposed an alternative receiver-side jamming strategy, where an FD receiver receives confidential information from the transmitter, and meanwhile sends AN to jam the eavesdropper. The study of using full duplex to enhance PHY security has thus triggered several works under various scenarios, including the point-to-point FD secure communications [5, 6], the FD secure relay networks [7–9], and the FD cellular secure communications [10].

This work was supported in part by the National Natural Science Foundation of China under Grants 61401073 and 61531009, and in part by the Applied Basic Research Programs of Sichuan Province, China (2015JY0102).

In this work, we consider an FD two-way relay network, where two FD legitimate radios exchange confidential information through an FD relay, in the presence of an eavesdropper. Unlike the previous works on FD two/multi-hop relay network [7–9], where the relay works in either FD relaying mode or FD jamming mode, we consider a more general relaying strategy—simultaneously relaying information and sending AN. Specifically, we assume that the FD relay receives confidential information from the two legitimate radios, and meanwhile amplify-and-forwards (AF) the received information to them, with the AN being superimposed in the AF signal to jam the eavesdropper. Our goal is to design the AF matrix and the AN covariance at the relay such that the sum secrecy rate of the two-way transmissions is maximized. This sum secrecy rate maximization (SSRM) problem is nonconvex by nature, but can be converted into a form of the difference-of-concave (DC) functions after the semidefinite relaxation (SDR). Hence, the classical DC programming approach naturally applies.

Our main contributions are as follows: 1) We prove that the SDR is tight, and provide a specific way to recover a stationary solution for the SSRM problem from every limit point of the DC iterations; 2) To reduce the iteration complexity of DC, we also proposed an inexact DC framework, which proceeds with an approximate solution, rather than a globally optimal one, throughout the DC iterations; convergence of the inexact DC is also established.

2. SYSTEM MODEL AND PROBLEM FORMULATION

Consider a full-duplex two-way relay network, where Alice and Bob simultaneously transmit and receive confidential information from each other through a relay, in the presence of an eavesdropper (Eve). Specifically, we focus on the following scenario: 1) Alice, Bob and relay are full-duplex and relay works in AF mode; 2) Alice and Bob both have two antennas—one for transmission and the other for reception; relay has N transmit antennas and M receive antennas with $N \neq M$; and Eve has a single antenna; 3) no direct link exists among Alice, Bob and Eve.[1] Let $\boldsymbol{h}_{i,R} \in \mathbb{C}^M$ and $\boldsymbol{h}_{R,i} \in \mathbb{C}^N$, $i \in \{A, B, E\}$ be the channels from node i to the relay and the relay to node i, respectively. Let $\boldsymbol{H}_{RR} \in \mathbb{C}^{M\times N}$, $h_{AA} \in \mathbb{C}$ and $h_{BB} \in \mathbb{C}$ be the self interference channel at the relay, Alice and Bob, respectively. Then, the received signal at the relay can be expressed as

$$\boldsymbol{y}_R(t) = \boldsymbol{h}_{AR}x_A(t) + \boldsymbol{h}_{BR}x_B(t) + \boldsymbol{H}_{RR}\boldsymbol{x}_R(t) + \boldsymbol{n}_R(t),$$

where $x_A(t), x_B(t) \in \mathbb{C}$ are coded confidential information sent by Alice and Bob with $\mathbb{E}\{|x_A(t)|^2\} = p_A$ and $\mathbb{E}\{|x_B(t)|^2\} = p_B$, respectively; $\boldsymbol{n}_R(t) \sim \mathcal{CN}(\boldsymbol{0}, \sigma_R^2\boldsymbol{I})$ is the additive white Gaussian

[1]The last assumption is made for simplifying the subsequent derivation; the inclusion of direct links can be handled in a similar manner.

noise at the relay; $\boldsymbol{x}_R(t) \in \mathbb{C}^N$ is the transmit signal (a.k.a. full-duplex self interference) at the relay, which takes the following form:

$$\boldsymbol{x}_R(t) = \boldsymbol{W}\boldsymbol{y}_R(t-\tau) + \boldsymbol{z}(t).$$

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 Eve. We assume $\boldsymbol{z}(t) \sim \mathcal{CN}(\boldsymbol{0}, \boldsymbol{Q})$ with $\boldsymbol{Q} \succeq \boldsymbol{0}$.

Accordingly, the received signal at Alice is given by

$$\begin{aligned} y_A(t) &= \boldsymbol{h}_{RA}^H \boldsymbol{x}_R(t) + h_{AA}x_A(t) + n_A(t) \\ &= \boldsymbol{h}_{RA}^H \boldsymbol{W}\boldsymbol{h}_{BR}x_B(t-\tau) + v(t), \end{aligned} \tag{1}$$

where $v(t) = \boldsymbol{h}_{RA}^H\boldsymbol{W}\boldsymbol{h}_{AR}x_A(t-\tau) + \boldsymbol{h}_{RA}^H\boldsymbol{W}\boldsymbol{H}_{RR}(\boldsymbol{W}\boldsymbol{y}_R(t-2\tau)+\boldsymbol{z}(t-\tau))+h_{AA}x_A(t)+\boldsymbol{h}_{RA}^H\boldsymbol{z}(t)+\boldsymbol{h}_{RA}^H\boldsymbol{W}\boldsymbol{n}_R(t-\tau)+n_A(t)$. The first term of $v(t)$ is the self interference (SI) induced by two-way communications, which can be eliminated by Alice herself with a prior knowledge of $x_A(t-\tau)$. The second term is the SI induced by full-duplex operation at the relay, which can be canceled at the relay by using zero-forcing (ZF) beamforming; we will detail this shortly in the problem formulation. The third term is the SI induced by full-duplex operation at Alice, which in practice can be suppressed to some extent, but not completely removed, owing to the proximity of the transmit and receive antennas and the insufficient spatial degree of freedom [1]. Therefore, after SI cancelation, the received signal at Alice reads

$$\begin{aligned} \hat{y}_A(t) =& \boldsymbol{h}_{RA}^H\boldsymbol{x}_R(t) + \sqrt{\zeta_A}h_{AA}x_A(t) + \boldsymbol{h}_{RA}^H\boldsymbol{z}(t) \\ &+ \boldsymbol{h}_{RA}^H\boldsymbol{W}\boldsymbol{n}_R(t-\tau) + n_A(t), \end{aligned}$$

where $0 < \zeta_A < 1$ represents the full-duplex SI suppression factor, and the achievable rate at Alice is given by

$$R_A = \log(1+\frac{|\boldsymbol{h}_{RA}^H\boldsymbol{W}\boldsymbol{h}_{BR}|^2 p_B}{\zeta_A|h_{AA}|^2p_A + \sigma_R^2\|\boldsymbol{h}_{RA}^H\boldsymbol{W}\|^2 + \boldsymbol{h}_{RA}^H\boldsymbol{Q}\boldsymbol{h}_{RA} + \sigma_A^2}).$$

Similarly, the achievable rate at Bob can be deduced as

$$R_B = \log(1+\frac{|\boldsymbol{h}_{RB}^H\boldsymbol{W}\boldsymbol{h}_{AR}|^2 p_A}{\zeta_B|h_{BB}|^2p_B + \sigma_R^2\|\boldsymbol{h}_{RB}^H\boldsymbol{W}\|^2 + \boldsymbol{h}_{RB}^H\boldsymbol{Q}\boldsymbol{h}_{RB} + \sigma_B^2}),$$

and the achievable sum rate at Eve can be upper bounded as

$$R_E = \log(1 + \frac{|\boldsymbol{h}_{RE}^H\boldsymbol{W}\boldsymbol{h}_{AR}|^2 p_A + |\boldsymbol{h}_{RE}^H\boldsymbol{W}\boldsymbol{h}_{BR}|^2 p_B}{\sigma_R^2\|\boldsymbol{h}_{RE}^H\boldsymbol{W}\|^2 + \boldsymbol{h}_{RE}^H\boldsymbol{Q}\boldsymbol{h}_{RE} + \sigma_E^2})$$

by using the two-user (i.e., Alice and Bob) MAC capacity result [11]. In addition, the transmit power at the relay can be shown to be

$$p(\boldsymbol{W}, \boldsymbol{Q}) = p_A\|\boldsymbol{W}\boldsymbol{h}_{AR}\|^2 + p_B\|\boldsymbol{W}\boldsymbol{h}_{BR}\|^2 + \sigma_R^2\|\boldsymbol{W}\|_F^2 + \mathrm{Tr}(\boldsymbol{Q}).$$

With the above system model, our problem of interest is to design the AF matrix $\boldsymbol{W}$ and the AN covariance $\boldsymbol{Q}$ such that the sum secrecy rate of the two-way communications is as large as possible. Mathematically, the sum secrecy rate maximization (SSRM) problem may be formulated as[2]

$$\max_{\boldsymbol{Q}\succeq\boldsymbol{0},\, \boldsymbol{W}} \quad R_s \triangleq R_A + R_B - R_E \tag{2a}$$

$$\text{s.t. } p(\boldsymbol{W}, \boldsymbol{Q}) \le P_R, \tag{2b}$$

$$(\boldsymbol{W}, \boldsymbol{Q}) \in \mathcal{F}, \tag{2c}$$

[2]The sum secrecy rate R_s in (2a) implicitly assumes that Alice and Bob can coordinately allocate their transmission rates. This coordination may be possible under some situations, e.g., in cellular network with Alice, Bob and Eve being mobile users and relay being the base station. If there is no coordination between Alice and Bob, one may alternatively consider a more conservative sum secrecy rate $\tilde{R}_s = (R_A - R_E) + (R_B - R_E) = R_A + A_B - 2R_E$. Since $\tilde{R}_s$ differs R_s only in a constant, we will focus on R_s throughout this paper.

where (2b) is the total power constraint at the relay with the power threshold $P_R > 0$, and (2c) is the ZF constraint imposed to cancel the full-duplex SI at the relay [cf. the discussion after Eq. (1)]. In particular, depending on the relationship between M and N, $\mathcal{F}$ may take the following two forms:

1. $M > N$: $\mathcal{F} \triangleq \{(\boldsymbol{W}, \boldsymbol{Q}) \mid \boldsymbol{W}\boldsymbol{H}_{RR} = \boldsymbol{0}\}$,
2. $M < N$: $\mathcal{F} \triangleq \{(\boldsymbol{W}, \boldsymbol{Q}) \mid \boldsymbol{H}_{RR}\boldsymbol{W} = \boldsymbol{0},\ \boldsymbol{H}_{RR}\boldsymbol{Q} = \boldsymbol{0}\}$.

In the following, we will focus on the case of $M > N$. The other case can be handled in a similar manner.

3. A DC APPROACH TO THE SSRM PROBLEM

The SSRM problem (2) is a nonconvex optimization problem, but can be converted into a form a difference-of-concave functions. To see this, let us first rewrite problem (2) into an alternative form.

Claim 1 *Let $r = \mathrm{rank}(\boldsymbol{H}_{RR})$ and $\boldsymbol{U}_0 \in \mathbb{C}^{M\times(M-r)}$ be the left singular vectors associated with the zero singular values of $\boldsymbol{H}_{RR}$. Then, problem* (2) *can be equivalently written as:*

$$\max_{\boldsymbol{Q}\succeq\boldsymbol{0},\, \boldsymbol{w}} \ f(\boldsymbol{w}\boldsymbol{w}^H, \boldsymbol{Q}) - g(\boldsymbol{w}\boldsymbol{w}^H, \boldsymbol{Q}) \tag{3a}$$

$$\text{s.t. } \mathrm{Tr}(\boldsymbol{w}\boldsymbol{w}^H) + \mathrm{Tr}(\boldsymbol{Q}) \le P_R, \tag{3b}$$

where $\boldsymbol{W} = \mathrm{vec}^{-1}(\boldsymbol{F}^{-1/2}\boldsymbol{w})\boldsymbol{U}_0^H$ with $\mathrm{vec}^{-1}(\cdot)$ being the inverse operation of vectorization, $\boldsymbol{F} = p_A(\boldsymbol{U}_0^T\boldsymbol{h}_{AR}^*\otimes\boldsymbol{I})(\boldsymbol{U}_0^T\boldsymbol{h}_{AR}^*\otimes\boldsymbol{I})^H + p_B(\boldsymbol{U}_0^T\boldsymbol{h}_{BR}^*\otimes\boldsymbol{I})(\boldsymbol{U}_0^T\boldsymbol{h}_{BR}^*\otimes\boldsymbol{I})^H + \sigma_R^2\boldsymbol{I}$, $f(\boldsymbol{w}\boldsymbol{w}^H, \boldsymbol{Q})$ and $g(\boldsymbol{w}\boldsymbol{w}^H, \boldsymbol{Q})$ are defined as follows:

$$\begin{aligned} f(\boldsymbol{w}\boldsymbol{w}^H, \boldsymbol{Q}) &\triangleq \textstyle\sum_{i=1}^3 \log\left(c_i + \alpha_i(\boldsymbol{w}\boldsymbol{w}^H, \boldsymbol{Q})\right), \\ g(\boldsymbol{w}\boldsymbol{w}^H, \boldsymbol{Q}) &\triangleq \textstyle\sum_{i=1}^3 \log\left(c_i + \beta_i(\boldsymbol{w}\boldsymbol{w}^H, \boldsymbol{Q})\right), \end{aligned}$$

where $c_1 = \zeta_A|h_{AA}|^2p_A + \sigma_A^2$, $c_2 = \zeta_B|h_{BB}|^2p_B + \sigma_B^2$, $c_3 = \sigma_E^2$, α_i and β_i are defined on the top of the next page. Claim 1 can be deduced straightforwardly by some matrix manipulations; the detail of the proof is omitted due to the page limit.

Our next step is to apply the semidefinite relaxation (SDR) technique to fit problem (3) into the DC framework. Specifically, by letting $\boldsymbol{\mathcal{W}} = \boldsymbol{w}\boldsymbol{w}^H$ and dropping the rank-one constraint on $\boldsymbol{\mathcal{W}}$, we obtain the SDR of (3) as follows:

$$\max_{\boldsymbol{\mathcal{W}}\succeq\boldsymbol{0},\boldsymbol{Q}\succeq\boldsymbol{0}} \ \phi(\boldsymbol{\mathcal{W}}, \boldsymbol{Q}) \triangleq f(\boldsymbol{\mathcal{W}}, \boldsymbol{Q}) - g(\boldsymbol{\mathcal{W}}, \boldsymbol{Q}) \tag{4a}$$

$$\text{s.t. } \mathrm{Tr}(\boldsymbol{\mathcal{W}}) + \mathrm{Tr}(\boldsymbol{Q}) \le P_R. \tag{4b}$$

Since $f(\boldsymbol{\mathcal{W}}, \boldsymbol{Q})$ and $g(\boldsymbol{\mathcal{W}}, \boldsymbol{Q})$ are both concave w.r.t. $(\boldsymbol{\mathcal{W}}, \boldsymbol{Q})$, problem (4) falls into the context of DC program. A standard way to handle problem (4) is to locally linearize the nonconcave function $-g(\boldsymbol{\mathcal{W}}, \boldsymbol{Q})$ at some feasible point $(\boldsymbol{\mathcal{W}}^k, \boldsymbol{Q}^k)$ and iteratively solve the linearized problem, i.e.,

$$(\boldsymbol{\mathcal{W}}^{k+1}, \boldsymbol{Q}^{k+1}) \in \max_{\boldsymbol{\mathcal{W}}\succeq\boldsymbol{0},\boldsymbol{Q}\succeq\boldsymbol{0}} \ \tilde{\phi}(\boldsymbol{\mathcal{W}}, \boldsymbol{Q}; \boldsymbol{\mathcal{W}}^k, \boldsymbol{Q}^k) \tag{5a}$$

$$\text{s.t. } \mathrm{Tr}(\boldsymbol{\mathcal{W}}) + \mathrm{Tr}(\boldsymbol{Q}) \le P_R, \tag{5b}$$

where $\tilde{\phi}(\boldsymbol{\mathcal{W}}, \boldsymbol{Q}; \boldsymbol{\mathcal{W}}^k, \boldsymbol{Q}^k) \triangleq f(\boldsymbol{\mathcal{W}}, \boldsymbol{Q}) - \tilde{g}(\boldsymbol{\mathcal{W}}, \boldsymbol{Q}; \boldsymbol{\mathcal{W}}^k, \boldsymbol{Q}^k)$ and $\tilde{g}(\boldsymbol{\mathcal{W}}, \boldsymbol{Q}; \boldsymbol{\mathcal{W}}^k, \boldsymbol{Q}^k) \triangleq \mathrm{Tr}\left(\nabla_{\boldsymbol{\mathcal{W}}}g(\boldsymbol{\mathcal{W}}^k, \boldsymbol{Q}^k)^H(\boldsymbol{\mathcal{W}} - \boldsymbol{\mathcal{W}}^k)\right) + \mathrm{Tr}\left(\nabla_{\boldsymbol{Q}}g(\boldsymbol{\mathcal{W}}^k, \boldsymbol{Q}^k)^H(\boldsymbol{Q} - \boldsymbol{Q}^k)\right) + g(\boldsymbol{\mathcal{W}}^k, \boldsymbol{Q}^k)$. Problem (5) is a convex problem, which can be optimally solved, e.g., by CVX [12]. Moreover, by directly applying the DC convergence result [13], we immediately have the following conclusion: Every limit point of $\{(\boldsymbol{\mathcal{W}}^k, \boldsymbol{Q}^k)\}_k$ is a stationary point of problem (4).

$$
\begin{aligned}
\alpha_1(\boldsymbol{w}\boldsymbol{w}^H,\boldsymbol{Q}) =& \beta_1(\boldsymbol{w}\boldsymbol{w}^H,\boldsymbol{Q}) + p_B(\boldsymbol{U}_0^T\boldsymbol{h}_{BR}^*\otimes\boldsymbol{h}_{RA})^H\boldsymbol{F}^{-1/2}\boldsymbol{w}\boldsymbol{w}^H\boldsymbol{F}^{-1/2}(\boldsymbol{U}_0^T\boldsymbol{h}_{BR}^*\otimes\boldsymbol{h}_{RA}),\\
\alpha_2(\boldsymbol{w}\boldsymbol{w}^H,\boldsymbol{Q}) =& \beta_2(\boldsymbol{w}\boldsymbol{w}^H,\boldsymbol{Q}) + p_A(\boldsymbol{U}_0^T\boldsymbol{h}_{AR}^*\otimes\boldsymbol{h}_{RB})^H\boldsymbol{F}^{-1/2}\boldsymbol{w}\boldsymbol{w}^H\boldsymbol{F}^{-1/2}(\boldsymbol{U}_0^T\boldsymbol{h}_{AR}^*\otimes\boldsymbol{h}_{RB}),\\
\alpha_3(\boldsymbol{w}\boldsymbol{w}^H,\boldsymbol{Q}) =& \boldsymbol{h}_{RE}^H\boldsymbol{Q}\boldsymbol{h}_{RE} + \mathrm{Tr}(\sigma_R^2(\boldsymbol{I}\otimes\boldsymbol{h}_{RE})^H\boldsymbol{F}^{-1/2}\boldsymbol{w}\boldsymbol{w}^H\boldsymbol{F}^{-1/2}(\boldsymbol{I}\otimes\boldsymbol{h}_{RE})),\\
\beta_1(\boldsymbol{w}\boldsymbol{w}^H,\boldsymbol{Q}) =& \mathrm{Tr}(\sigma_R^2(\boldsymbol{I}\otimes\boldsymbol{h}_{RA})^H\boldsymbol{F}^{-1/2}\boldsymbol{w}\boldsymbol{w}^H\boldsymbol{F}^{-1/2}(\boldsymbol{I}\otimes\boldsymbol{h}_{RA})) + \boldsymbol{h}_{RA}^H\boldsymbol{Q}\boldsymbol{h}_{RA},\\
\beta_2(\boldsymbol{w}\boldsymbol{w}^H,\boldsymbol{Q}) =& \mathrm{Tr}(\sigma_R^2(\boldsymbol{I}\otimes\boldsymbol{h}_{RB})^H\boldsymbol{F}^{-1/2}\boldsymbol{w}\boldsymbol{w}^H\boldsymbol{F}^{-1/2}(\boldsymbol{I}\otimes\boldsymbol{h}_{RB})) + \boldsymbol{h}_{RB}^H\boldsymbol{Q}\boldsymbol{h}_{RB},\\
\beta_3(\boldsymbol{w}\boldsymbol{w}^H,\boldsymbol{Q}) =& \alpha_3(\boldsymbol{w}\boldsymbol{w}^H,\boldsymbol{Q}) + p_A(\boldsymbol{U}_0^T\boldsymbol{h}_{AR}^*\otimes\boldsymbol{h}_{RE})^H\boldsymbol{F}^{-1/2}\boldsymbol{w}\boldsymbol{w}^H\boldsymbol{F}^{-1/2}(\boldsymbol{U}_0^T\boldsymbol{h}_{AR}^*\otimes\boldsymbol{h}_{RE}) + \ldots\\
& p_B(\boldsymbol{U}_0^T\boldsymbol{h}_{BR}^*\otimes\boldsymbol{h}_{RE})^H\boldsymbol{F}^{-1/2}\boldsymbol{w}\boldsymbol{w}^H\boldsymbol{F}^{-1/2}(\boldsymbol{U}_0^T\boldsymbol{h}_{BR}^*\otimes\boldsymbol{h}_{RE}).
\end{aligned}
$$

Thus far, we have shown how to handle the relaxed SSRM problem (4) by DC program. Now, let us turn our attention back to the original SSRM problem (3). In particular, let $(\bar{\boldsymbol{\mathcal{W}}},\bar{\boldsymbol{Q}})$ be a limit point of $\{(\boldsymbol{\mathcal{W}}^k,\boldsymbol{Q}^k)\}_k$. Then, the following question arises naturally: *Can we construct a stationary solution of problem* (3) *from* $(\bar{\boldsymbol{\mathcal{W}}},\bar{\boldsymbol{Q}})$*? If yes, how to do it?*

To answer the above question, let us consider the following problem:

$$
\begin{aligned}
\max_{\boldsymbol{\mathcal{W}}\succeq\boldsymbol{0},\boldsymbol{Q}\succeq\boldsymbol{0}}\ & \mathrm{Tr}\left((\nabla_{\boldsymbol{\mathcal{W}}}f(\bar{\boldsymbol{\mathcal{W}}},\bar{\boldsymbol{Q}})^H\boldsymbol{\mathcal{W}}) + (\nabla_{\boldsymbol{Q}}f(\bar{\boldsymbol{\mathcal{W}}},\bar{\boldsymbol{Q}})^H\boldsymbol{Q})\right)\\
\text{s.t. }\ & \beta_i(\boldsymbol{\mathcal{W}},\boldsymbol{Q}) = \beta_i(\bar{\boldsymbol{\mathcal{W}}},\bar{\boldsymbol{Q}}),\quad i=1,2,3,\\
& \mathrm{Tr}(\boldsymbol{\mathcal{W}}) + \mathrm{Tr}(\boldsymbol{Q}) = \mathrm{Tr}(\bar{\boldsymbol{\mathcal{W}}}) + \mathrm{Tr}(\bar{\boldsymbol{Q}}).
\end{aligned}
\tag{6}
$$

Problem (6) is closely related to problems (3) and (4). In particular,

Theorem 1 *Suppose that* $(\hat{\boldsymbol{\mathcal{W}}},\hat{\boldsymbol{Q}})$ *is any optimal solution of problem* (6) *and* $\hat{\boldsymbol{Q}}\neq\boldsymbol{0}$*. Then, there exists a rank-one optimal solution* $\hat{\boldsymbol{\mathcal{W}}} = \hat{\boldsymbol{w}}\hat{\boldsymbol{w}}^H$ *for problem* (6)*. Moreover,* $(\hat{\boldsymbol{w}},\hat{\boldsymbol{Q}})$ *is a stationary solution or Karush-Kuhn-Tucker (KKT) solution of problem* (3)*.*

The proof of Theorem 1 relies on the rank reduction result in [14] as well as some judiciously constructed problems that help link the KKT conditions of problems (3), (4) and (6). The detailed proof is omitted due to the page limit.

4. AN INEXACT DC APPROACH TO SSRM PROBLEM

As one may note that each DC iteration in (5) requires solving a convex optimization problem to globally optimality, which could be time consuming in practice. To save the computational load, we consider an inexact DC update by finding an approximate solution for problem (5), rather than a globally optimal one. Before delving into the detail of the inexact DC, let us first introduce the notion of *gradient mapping* [15], which is useful for characterizing the solution inexactness as well as stationarity. Consider maximizing a continuously differentiable function $\varphi(\boldsymbol{x})$ over a convex compact feasible set $\mathcal{C}$. The gradient mapping of $\varphi(\boldsymbol{x})$ at $\bar{\boldsymbol{x}}\in\mathcal{C}$ is denoted as

$$
\tilde{\nabla}\varphi(\bar{\boldsymbol{x}}) \triangleq \mathcal{P}\left(\bar{\boldsymbol{x}} + \nabla\varphi(\bar{\boldsymbol{x}})\right) - \bar{\boldsymbol{x}},
\tag{7}
$$

where $\mathcal{P}(\boldsymbol{x})$ represents the projection of a point $\boldsymbol{x}$ onto the set $\mathcal{C}$. It is well known that a point $\bar{\boldsymbol{x}}\in\mathcal{C}$ is a stationary point if and only if $\tilde{\nabla}\varphi(\bar{\boldsymbol{x}})=\boldsymbol{0}$ [16]. Now, let us turn back to the DC subproblem (5), which is restated below:

$$
\max_{\boldsymbol{x}}\ \tilde{\phi}(\boldsymbol{x};\boldsymbol{x}^k)\quad \text{s.t. } \boldsymbol{x}\in\mathcal{D},
\tag{8}
$$

where for notational convenience, we have denoted $\boldsymbol{x}\triangleq(\boldsymbol{\mathcal{W}},\boldsymbol{Q})$ and $\mathcal{D}\triangleq\{(\boldsymbol{\mathcal{W}},\boldsymbol{Q})\mid \mathrm{Tr}(\boldsymbol{\mathcal{W}}+\boldsymbol{Q})\le P_R,\ \boldsymbol{\mathcal{W}}\succeq\boldsymbol{0},\ \boldsymbol{Q}\succeq\boldsymbol{0}\}$. Instead of solving problem (8) to global optimality, we do the following inexact DC update:

> *Find an (approximate) solution* $\boldsymbol{x}^{k+1}\in\mathcal{D}$ *for problem* (8) *such that the following relationship holds:*
>
> $$\tilde{\phi}(\boldsymbol{x}^{k+1};\boldsymbol{x}^k) - \tilde{\phi}(\boldsymbol{x}^k;\boldsymbol{x}^k) \ge \zeta^k\|\tilde{\nabla}\tilde{\phi}(\boldsymbol{x}^k;\boldsymbol{x}^k)\|^2,\tag{9}$$
>
> *where* $\zeta^k>0,\ \forall k$ *is some iteration-dependent constant and bounded away from zero.*

The inexact DC updating rule (9) is quite flexible. It is easy to see that the previous exact DC update fulfills (9). Moreover, without computing a globally optimal solution for (5), the inexact DC may iterate in a more computationally efficient manner; we will detail this in the next subsection. Despite that somehow low-quality or approximate solutions are sought at each inexact DC iteration, interestingly the same convergence as the exact DC is still guaranteed, as revealed by the following proposition.

Proposition 1 *Suppose that* $\{\boldsymbol{x}^k\}$ *is a sequence generated by the inexact DC, fulfilling the relationship* (9)*. Then, every limit point of* $\{\boldsymbol{x}^k\}$ *is a stationary point of problem* (4)*.*

The key to the proof of Proposition 1 is that the updating rule (9) ensures that there is a sufficient improvement between the consecutive iterations if the current point is nonstationary. By accumulating these improvements, the DC iteration will finally reside at some stationary point. Due to the page limit, we omit the detailed proof. In light of Proposition 1, a similar result as Theorem 1 can be readily established.

Theorem 2 *Let* $\bar{\boldsymbol{x}} = (\bar{\boldsymbol{\mathcal{W}}},\bar{\boldsymbol{Q}})$ *be a limit point generated by the inexact DC with each iteration fulfilling* (9)*. Suppose that* $(\hat{\boldsymbol{\mathcal{W}}},\hat{\boldsymbol{Q}})$ *is any optimal solution of problem* (6) *and* $\hat{\boldsymbol{Q}}\neq\boldsymbol{0}$*. Then, there exists a rank-one solution* $\hat{\boldsymbol{\mathcal{W}}}=\hat{\boldsymbol{w}}\hat{\boldsymbol{w}}^H$ *for problem* (6)*. Moreover,* $(\hat{\boldsymbol{w}},\hat{\boldsymbol{Q}})$ *is a stationary solution or KKT solution of problem* (3)*.*

While the inequality (9) poses a general sufficient condition for achieving a stationary solution of problem (3), it is still not clear how to algorithmically generate such an iteration sequence, especially in a computationally efficient manner. In the next subsection, we will give a simple implementation of the inexact DC by leveraging first-order optimization methods.

4.1. A Projected Gradient-based Inexact DC Implementation

We consider generating the inexact solution $\boldsymbol{x}^{k+1}$ for (8) by projected gradient method (PGM), where only a small finite number of PG operations are performed to produce $\boldsymbol{x}^{k+1}$ from $\boldsymbol{x}^k$. Algorithm 1 summarizes the inexact PGM for problem (8).

Algorithm 1 An Inexact PGM for Problem (8)

1: Set $l = 0$, $\boldsymbol{x}^{k,0} = \boldsymbol{x}^k$ and the number of PG operations $L_k \geq 1$
2: **while** $l \leq L_k - 1$ **do**
3: Set $\boldsymbol{x}^{k,l+1} = \boldsymbol{x}^{k,l} + \alpha^{k,l}\tilde{\nabla}\tilde{\phi}(\boldsymbol{x}^{k,l}; \boldsymbol{x}^k)$, where $\alpha^{k,l} > 0$ is the stepsize determined by either Armijo's rule or (limited) minimization rule [16].
4: $l = l + 1$;
5: **end while**
6: $\boldsymbol{x}^{k+1} = \boldsymbol{x}^{k,L_k}$.

Remark 1 When $L_k = 1$ for all k, one can verify that Algorithm 1 degenerates into directly applying PGM to the original DC problem (4). However, for $L_k > 1$, Algorithm 1 has an incentive to making more progress at each DC subproblem by performing L_k PG operations. One extreme case is to let L_k approach infinity for all k. Then, Algorithm 1 becomes the exact DC and converges to a stationary solution of problem (3) by Theorem 1. For finite L_k, the following proposition reveals that the same convergence is still guaranteed.

Proposition 2 *Suppose that $\{\boldsymbol{x}^k\}$ is a sequence generated by Algorithm 1. Then, every limit point of $\{\boldsymbol{x}^k\}$ is a stationary point of problem* (4)*. Moreover, by using the same construction as that in Theorem 1, a stationary solution of problem* (3) *can be constructed from every limit point of $\{\boldsymbol{x}^k\}$.*

The key to the proof is to show that each iteration of Algorithm 1 fulfills the inequality (9). Thus, the result follows directly from Proposition 1 and Theorem 2. The detailed proof is omitted due to the page limit.

Thus far, we have established the convergence of Algorithm 1. The remaining issue is whether Algorithm 1 can be efficiently implemented. Clearly, the main computation lies in performing the PG operations, particularly, the computation of $\tilde{\nabla}\tilde{\phi}(\boldsymbol{x}^{k,l}; \boldsymbol{x}^k)$ (cf. line 3 of Algorithm 1). From the definition of the gradient mapping, one needs to find an efficient way to calculate $\mathcal{P}(\boldsymbol{x}^{k,l} + \nabla\tilde{\phi}(\boldsymbol{x}^{k,l}; \boldsymbol{x}^k))$, i.e., solving the following projection problem:

$$\min_{\boldsymbol{\mathcal{W}},\boldsymbol{Q}} \left\| \begin{pmatrix} \boldsymbol{\mathcal{W}} \\ \boldsymbol{Q} \end{pmatrix} - \begin{pmatrix} \boldsymbol{\mathcal{W}}^{k,l} + \nabla_{\boldsymbol{\mathcal{W}}}\tilde{\phi}(\boldsymbol{x}^{k,l}; \boldsymbol{x}^k) \\ \boldsymbol{Q}^{k,l} + \nabla_{\boldsymbol{Q}}\tilde{\phi}(\boldsymbol{x}^{k,l}; \boldsymbol{x}^k) \end{pmatrix} \right\|^2 \quad (10)$$
$$\text{s.t. } \mathrm{Tr}(\boldsymbol{\mathcal{W}} + \boldsymbol{Q}) \leq P_R, \quad \boldsymbol{\mathcal{W}} \succeq \boldsymbol{0}, \quad \boldsymbol{Q} \succeq \boldsymbol{0}.$$

Problem (10) admits a water-filling-like solution. Specifically, the optimal solution of (10) is given by [17, Fact 1]

$$\boldsymbol{\mathcal{W}}^\star = \boldsymbol{F}_1 \mathrm{Diag}(\boldsymbol{\eta}_1^\star)\boldsymbol{F}_1^H, \quad \boldsymbol{Q}^\star = \boldsymbol{F}_2 \mathrm{Diag}(\boldsymbol{\eta}_2^\star)\boldsymbol{F}_2^H,$$

where $\boldsymbol{F}_1 \mathrm{Diag}(\tilde{\boldsymbol{\eta}}_1)\boldsymbol{F}_1^H$ and $\boldsymbol{F}_2 \mathrm{Diag}(\tilde{\boldsymbol{\eta}}_2)\boldsymbol{F}_2^H$ are the eigenvalue decompositions of $\boldsymbol{\mathcal{W}}^{k,l} + \nabla_{\boldsymbol{\mathcal{W}}}\tilde{\phi}(\boldsymbol{x}^{k,l}; \boldsymbol{x}^k)$ and $\boldsymbol{Q}^{k,l} + \nabla_{\boldsymbol{Q}}\tilde{\phi}(\boldsymbol{x}^{k,l}; \boldsymbol{x}^k)$, respectively, and

$$\boldsymbol{\eta}_1^\star = [\tilde{\boldsymbol{\eta}}_1 - \nu^\star \boldsymbol{1}]^+, \quad \boldsymbol{\eta}_2^\star = [\tilde{\boldsymbol{\eta}}_2 - \nu^\star \boldsymbol{1}]^+,$$

with $\nu^\star \geq 0$ being the water-filling level. The value $\nu^\star$ relates to the total power P_R and can be efficiently determined. Readers are referred to [17, Fact 1] for the details.

Table 1: Averaged running times of CVX and PGM

$p_A = p_B$	Averaged Running Times (in Sec.)					
	2dB	4dB	6dB	8dB	10dB	12dB
2dB (CVX)	3.63	4.38	5.02	5.62	6.09	6.45
2dB (PGM)	0.92	1.20	1.37	1.24	1.09	0.98
10dB (CVX)	3.38	4.20	4.84	5.29	5.68	5.88
10dB (PGM)	0.87	1.17	1.35	1.37	1.21	1.07

5. NUMERICAL RESULTS AND CONCLUSIONS

In this section, we showcase two examples to compare the rate and complexity performances of the exact and inexact DC. More comparisons will be provided in the full paper. Our simulation settings are as follows: The number of transmit antennas and receive antennas at the relay are set to be $N = 3$ and $M = 6$, respectively; all the channels are randomly generated following i.i.d. complex Gaussian distribution with zero mean and unit variance; the receive noise at each node has the same unit variance, i.e., $\sigma_A^2 = \sigma_B^2 = \sigma_E^2 = 1$; for simplicity, we assume that Alice and Bob have the same full-duplex SI suppression factor $\zeta_A = \zeta_B = 0.1$, and the same transmit power $p_A = p_B$; all the results were averaged over 100 random channel realizations.

Fig. 1 shows the sum secrecy rates (in nats/s/Hz) of the exact DC by CVX and the inexact DC by PGM (cf. Algorithm 1) when increasing the relay power P_R from 0 dB to 12 dB. Specifically, for inexact DC we set $L_k = 5$, $\forall\ k$ and the stepsize $\alpha^{k,l}$ is chosen according to Armijo's rule. For both exact and inexact DC, the DC iterations stop when the relative rate increase is less than 5×10^{-3}. From the figure, we see that there is negligible rate performance loss between the exact DC and the inexact DC, especially for small relay power region, say, $P_R \leq 8$ dB. This demonstrates that while the inexact DC proceeds with an approximate or low-quality solution per iteration, for a long run it is able to attain almost the same progress as the exact DC. As mentioned before, the main benefit of inexact DC lies in the computational complexity saving. To verify this, we tabulated the averaged running times of CVX and PGM in Table 1 under the same setting as Fig. 1. As seen, the PGM runs much faster than CVX for both $p_A = p_B = 2$ dB and $p_A = p_B = 10$ dB. In particular, the running time of PGM is almost invariant to the increase of P_R, whereas that of CVX scales nearly linearly with P_R.

To conclude, in this paper we have studied the sum secrecy rate maximization (SSRM) problem for two-way full-duplex relay networks. The SSRM problem is nonconvex by nature. However, by resorting to the semidefinite relaxation (SDR) and the difference-of-concave (DC) program techniques, we show that a stationary solution of the SSRM problem can be iteratively computed. To further reduce the iteration complexity, an inexact DC approach was also proposed with a provable convergence to a stationary solution of the SSRM problem.

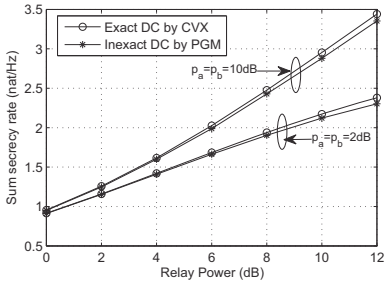

Fig. 1: Sum secrecy rate vs. the relay power threshold P_R.

6. REFERENCES

[1] D. Bharadia, E. McMilin, and S. Katti, "Full duplex radios," in *Proc. ACM SIGCOMM*, 2013, pp. 1–12.

[2] R. Negi and S. Goel, "Secret communication using artificial noise," in *IEEE Vehicular Technology Conference*, Sept. 2005, pp. 1906–1910.

[3] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-Eves secrecy rate maximization," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2704–2717, May 2013.

[4] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.

[5] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.

[6] R. Feng, Q. Li, Q. Zhang, and J. Qin, "Robust secure beamforming in MISO full-duplex two-way secure communications," *to appear in IEEE Trans. Vel. Tech.*, 2015.

[7] J.-H. Lee, "Full-duplex relay for enhancing physical layer security in multi-hop relaying systems," *IEEE Commun. Lett.*, vol. 19, no. 4, pp. 525–528, Apr. 2015.

[8] S. Parsaeefard and T. Le-Ngoc, "Improving wireless secrecy rate via full-duplex relay-assisted protocols," *IEEE Trans. Info. Forensics Secruity*, vol. 10, no. 10, pp. 2095–2107, Oct. 2015.

[9] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inf. Forensics Secruity*, vol. 10, no. 3, pp. 574–583, Mar. 2015.

[10] Y. Sun, D. W. K. Ng, J. Zhu, and R. Schober, "Multi-objective optimization for robust power efficient and secure full-duplex wireless communication systems," 2015, aviliable online at http://arxiv.org/abs/1509.01425.

[11] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. U.K.: Cambridge Univ. Press, 2005.

[12] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 2.1," http://cvxr.com/cvx, Mar. 2014.

[13] B. Sriperumbudur and G. Lanckriet, "On the convergence of the concave-convex procedure," *Advances in Neural Information Processing Systems*, pp. 1759–1767, 2009.

[14] Y. Huang and D. P. Palomar, "Rank-constrained separable semidefinite programming with applications to optimal beamforming," *IEEE Trans. Signal Process.*, vol. 58, no. 2, pp. 664–678, 2010.

[15] Y. Nesterov, *Introductory lectures on convex optimization: A basic course*. Kluwer Academic Publisher, 2004.

[16] D. Bertsekas, *Nonlinear Programming*. Belmont, MA: Athena Scientific, 1999.

[17] Q. Li, M. Hong, H.-T. Wai, Y.-F. Liu, W.-K. Ma, and Z.-Q. Luo, "Transmit solutions for MIMO wiretap channels using alternating optimization," *IEEE Journal Sel. Area. Commun.*, vol. 31, no. 9, pp. 1714–1727, Nov. 2013.