Joint Information- and Jamming-Beamforming for Physical Layer Security With Full Duplex Base Station

Fengchao Zhu, Feifei Gao, *Senior Member, IEEE*, Minli Yao, and Hongxing Zou

***Abstract*—In this paper, we design joint information beamforming and jamming beamforming to guarantee both transmit security and receive security for a full-duplex base-station (FD-BS). Specifically, we aim to maximize the secret transmit rate while constrain the secret receive rate to be greater than a predefined bound. When FD-BS is equipped with a single transmit antenna, we derive the optimal solutions in closed-form, and interestingly, the results say that simultaneous information and jamming transmission cannot be optimal. When FD-BS is equipped with multiple transmit antennas, we convert the original nonconvex problem into a sequence of subproblems where the semidefinite programming (SDP) relaxation can be applied to efficiently find the optimal solutions. We strictly prove that such a relaxation does not change the optimality for these subproblems. Then the global optimal solutions of the original nonconvex problem can be obtained via a one-dimensional search. Simulation results are provided to verify the efficiency of the proposed algorithms.**

***Index Terms*—Artificial noise, beamforming, full duplex, jamming, physical layer security, SDP relaxation.**

I. Introduction

PHYSICAL layer security for wireless communications has received lots of attention since it can prevent eavesdropping without upper layer data encryption. The basic idea of physical layer security is to exploit physical characteristics of the wireless channel when transmitting confidential messages.

Manuscript received January 26, 2014; revised June 04, 2014 and September 10, 2014; accepted October 10, 2014. Date of publication October 24, 2014; date of current version November 12, 2014. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Tongtong Li. This work was supported in part by the National Basic Research Program of China (973 Program) under Grant 2013CB336600 and Grant 2012CB316102; by National Major Project (NO.2013ZX03004007); by the Beijing Natural Science Foundation under Grant 4131003; by the National Natural Science Foundation of China under Grant 61422109; by the Importation and Development of High-Caliber Talents Project of Beijing Municipal Institutions under Grant YETP0110; by the Opening Project of Key Lab of Digital Signal and Image Processing of Guangdong (No. 2013GDDSIPL-05). (*Corresponding author: F. Gao*.)

F. Zhu, F. Gao, and H. Zou are with the State Key Laboratory of Intelligent Technology and Systems, Tsinghua National Laboratory for Information Science and Technology, Department of Automation, Tsinghua University, Beijing, 100084, China (e-mail: fengchao_zhu@126.com; feifeigao@ieee.org; hongxing_zou@tsinghua.edu.cn).

M. Yao and F. Zhu are with the Xi'an Research Institute of High Technology, Xi'an, Shaanxi, 710025, China (e-mail: yaominli@sohu.com).

Digital Object Identifier 10.1109/TSP.2014.2364786

Different channel models as well as their secrecy limits have been studied in [1]–[6]. For example, the information-theoretic approach to guarantee secrecy was initiated by Wyner [1], where the concept of secrecy capacity was defined in degraded discrete memoryless wiretap channels. The results of [1] were later generalized to various channel models, such as the broadcast channels [2], the single-input single-output (SISO) fading channels [3], the multiple access channels (MAC) [4], the multiple-input multiple-output (MIMO) channels [5], full duplex relay channels [6], etc.

To increase the secret rate in wireless systems, artificial noise (AN), also known as jamming, was proposed to be sent from the transmitter [7] such that the decoding capabilities of eavesdroppers are degraded. An important result of [7] is that a non-zero secret rate can be achieved even when the channel condition of the legitimate user is worse than that of the eavesdropper. Motivated by [7], a vast works have been developed to study the physical layer security based on AN. When the channel state information (CSI) from the transmitter to the eavesdropper is unknown, [8]–[10] designed algorithms that spread AN within the null-space of the legitimate receiver's channel, while [11]–[13] cooperatively generated AN from different users. When such CSI is known, more flexible considerations of AN were proposed, such as the signal-to-interference plus noise ratio (SINR) based algorithm [14] and the mean-square-error (MSE) based algorithm [15] that aim to provide the legitimate receiver with different quality of service (QoS). Moreover, [16] studied joint optimization of the covariances of both the confidential information and the jamming, where the latter could take any spatial pattern and thus achieves more flexibility.

An interesting work was proposed in [17], where AN was sent by a full-duplex receiver equipped with both the receive antenna and the transmit antenna. The secrecy performance of [17] was evaluated by an outage secrecy region from a geometrical perspective. Recently, aiming to improve the secret receive rate, a self-protection mechanism at the receiver side was designed in [18] using a full duplex receiver that is equipped with multiple receive antennas and transmit antennas. However, both [17] and [18] assume that the full-duplex receiver does not have its own information to transmit.

In this paper, we consider a more general scenario of physical layer security where a full-duplex base-station (FD-BS) simultaneously receives information from a transmitter (Tx) and transmits information to a legitimate receiver (Rx). We design joint information beamforming and jamming beamforming at

FD-BS aiming to protect both the transmit security and the receive security.[1] The main contributions of this paper are summarized as follows:

1) When FD-BS has a single transmit antenna, the optimization problem reduces to a power allocation problem, whose closed-form solutions are derived. An important indication is that the FD-BS should either transmit information or transmit jamming, in order to achieve the optimal performance.
2) When FD-BS has multiple transmit antennas, we convert the original non-convex optimization into a sequence of convex semidefinite programmings (SDPs) and prove the optimality of the SDP relaxation. A low complex dual method is used to find the solutions of SDP problem while the global optimal solutions can be found from one dimensional search.

The rest of this paper is organized as follows: Section II describes the system model and formulates the secret rate maximization problem; Section III considers FD-BS with a single transmit antenna and derives the closed-form power allocation; Section IV considers FD-BS with multiple transmit antennas and presents the optimal algorithms, as well as the dual method. The simulation results are provided in Section V and conclusions are drawn in Section VI.

Notation: Vectors and matrices are boldface small and capital letters, respectively; the Hermitian of $\boldsymbol{A}$ is denoted by $\boldsymbol{A}^{\mathrm{H}}$; $\mathrm{Tr}(\boldsymbol{A})$ defines the trace; $\boldsymbol{I}$ and $\boldsymbol{0}$ represent an identity matrix and an all-zero matrix, respectively, with appropriate dimensions; $\boldsymbol{A} \succeq \boldsymbol{0}$ and $\boldsymbol{A} \succ \boldsymbol{0}$ mean that $\boldsymbol{A}$ is positive semi-definite and positive definite, respectively; $\mathbb{E}[\cdot]$ denotes the statistical expectation; The unit-norm vector of a vector $\boldsymbol{x}$ is described as $\vec{\boldsymbol{x}} = \boldsymbol{x}/\|\boldsymbol{x}\|$; The distribution of a circularly symmetric complex Gaussian (CSCG) random variable with zero mean and variance σ^2 is defined as $\mathcal{CN}(0,\sigma^2)$, and $\sim$ means "distributed as"; $\mathbb{C}^{a\times b}$ denotes the space of $a \times b$ matrices with complex entries; $\|\boldsymbol{x}\|$ is the Euclidean norm of a vector $\boldsymbol{x}$, and $\bar{e}$ denotes the conjugate of a complex number e; $\min\{x,y\}$ denote the minimum between two real numbers, x and y, and $(x)^+ \triangleq \max\{x,0\}$.

II. System Model and Problem Formulation

Consider a wireless communication system with one FD-BS, one transmitter (Tx), one receiver (Rx) and one eavesdropper (Ev), as shown in Fig. 1. Tx and Rx communicate with BS, respectively, via uplink and downlink channels that reside in the same frequency band. FD-BS has $M+N$ antennas, where $M \geq 1$ antennas are used for receiving while $N \geq 1$ antennas are used for transmitting [18]. Moreover, Tx, Rx and Ev are all equipped with a single antenna. The baseband equivalent channels from Tx to FD-BS and Ev are denoted by $\boldsymbol{h}_t \in \mathbb{C}^{M\times 1}$ and $g_e \in \mathbb{C}^{1\times 1}$ respectively. The channels from FD-BS to Rx and Ev are denoted by $\boldsymbol{h}_r \in \mathbb{C}^{N\times 1}$ and $\boldsymbol{h}_e \in \mathbb{C}^{N\times 1}$ respectively. The loop interference channel of FD-BS is denoted as $\boldsymbol{H}_b \in \mathbb{C}^{N\times M}$ [17]–[21].

Since Tx has only one antenna and cannot be used for jamming, then functionality to guarantee the transmit/receive

[1]The transmit security and the receive security used in this paper are refereed from the BS viewpoint.

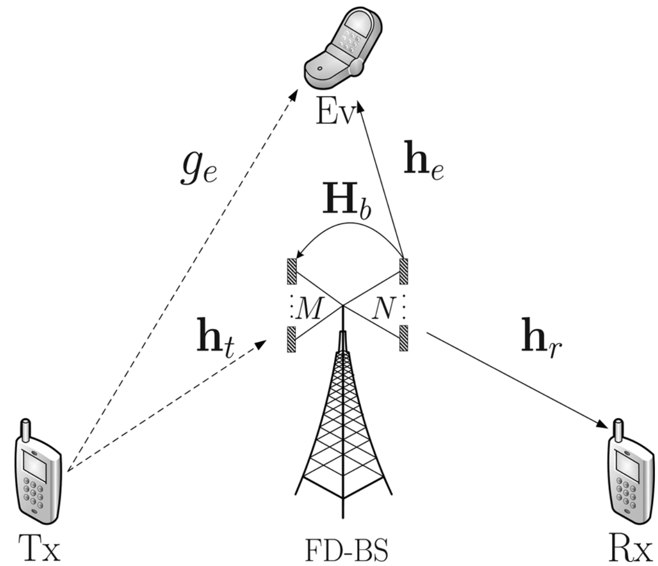


Fig. 1. Physical layer security for an FD-BS via simultaneous information beamforming and jamming beamforming.

secrecy has to be equipped at FD-BS. Denote the baseband transmit signal from FD-BS as

$$\boldsymbol{x}_b = \boldsymbol{s} + \boldsymbol{w}, \tag{1}$$

where $\boldsymbol{s} \in \mathbb{C}^{N\times 1}$ and $\boldsymbol{w} \in \mathbb{C}^{N\times 1}$ are CSCG information vector and jamming vector respectively.

Suppose $v_t \sim \mathcal{CN}(0,1)$ is the symbols transmitted from Tx, and denote P_t as the corresponding transmit power. Then, the received signal at FD-BS, after eliminating the loop-interference[2] from $\boldsymbol{x}_b$, can be expressed as [17]

$$\boldsymbol{y}_b = \boldsymbol{h}_t\sqrt{P_t}v_t + \boldsymbol{z}_b, \tag{2}$$

where $\boldsymbol{z}_b \in \mathbb{C}^{M\times 1}$ is the jamming[3] vector that is assumed to have the distribution $\boldsymbol{z}_b \sim \mathcal{CN}(\boldsymbol{0},\boldsymbol{I})$.

The signals received by Rx and Ev are expressed as

$$y_r = \boldsymbol{h}_r^{\mathrm{H}}\boldsymbol{x}_b + z_r, \quad y_e = g_e\sqrt{P_t}v_t + \boldsymbol{h}_e^{\mathrm{H}}\boldsymbol{x}_b + z_e, \tag{3}$$

where $z_r \sim \mathcal{CN}(0,1)$ and $z_e \sim \mathcal{CN}(0,1)$ are the corresponding noise at Rx and Ev, respectively.

Before we state our results, we also define the following notations, which will be used extensively in the rest of this paper:

$$C_{b,r}(\boldsymbol{S},\boldsymbol{W}) = \log_2\left(1+\frac{\boldsymbol{h}_r^{\mathrm{H}}\boldsymbol{S}\boldsymbol{h}_r}{1+\boldsymbol{h}_r^{\mathrm{H}}\boldsymbol{W}\boldsymbol{h}_r}\right), \tag{4}$$

$$C_{b,e}(\boldsymbol{S},\boldsymbol{W}) = \log_2\left(1+\frac{\boldsymbol{h}_e^{\mathrm{H}}\boldsymbol{S}\boldsymbol{h}_e}{1+P_t\|g_e\|^2+\boldsymbol{h}_e^{\mathrm{H}}\boldsymbol{W}\boldsymbol{h}_e}\right), \tag{5}$$

$$C_{t,e}(\boldsymbol{S},\boldsymbol{W}) = \log_2\left(1+\frac{P_t\|g_e\|^2}{1+\boldsymbol{h}_e^{\mathrm{H}}\boldsymbol{S}\boldsymbol{h}_e+\boldsymbol{h}_e^{\mathrm{H}}\boldsymbol{W}\boldsymbol{h}_e}\right), \tag{6}$$

[2]Loop-interference cancelation has received lots of attention recently [19]–[21]. Meanwhile, full duplex systems for wireless communication has been thoroughly studied [22]–[24].

[3]Here, the jamming signal is assumed to be random Gaussian noise. In frequency hopping based systems, the idea of disguised jamming [25], [26] is a more advanced algorithm, which would be very interesting and would definitely serve as a good future topic.

$$C_{t,b} = \log_2\left(1 + P_t\|\boldsymbol{h_t}\|^2\right), \tag{7}$$

where $\boldsymbol{S} = \mathbb{E}\{\boldsymbol{s}\boldsymbol{s}^{\mathrm{H}}\}$ and $\boldsymbol{W} = \mathbb{E}\{\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}}\}$ are the information covariance and the jamming covariance respectively.

Since we aim to protect information secrecy for both uplink channel and downlink channel simultaneously, i.e., Ev cannot decode both v_t and $\mathbf{x}_b$, the secret receive rate and secret transmit rates can be separately formulated as

$$C_{t,b} - C_{t,e}(\boldsymbol{S},\boldsymbol{W}),\ C_{b,r}(\boldsymbol{S},\boldsymbol{W}) - C_{b,e}(\boldsymbol{S},\boldsymbol{W}), \tag{8}$$

respectively. If both the secret rates defined in (8) are kept no smaller than zero, then we know that either the signal transmitted from Tx or sent to Rx is "undecodable"[4]. From Ev's perspective, the two "undecodable" signals could serve as jamming signals for each other.

In this paper, we propose to maximize the secret transmit rate of FD-BS while ensures its secret receive rate being above a predefined bound. Its counterparts to maximize the secret receive rate of FD-BS while constraining on the secret transmit rate could be similarly designed and are omitted for brevity. The optimization problem can then be formulated as

$$\mathbf{P1}: \max_{\boldsymbol{S}\succeq\mathbf{0},\boldsymbol{W}\succeq\mathbf{0}} \quad C_{b,r}(\boldsymbol{S},\boldsymbol{W}) - C_{b,e}(\boldsymbol{S},\boldsymbol{W}) \tag{9}$$

$$\text{s.t.} \quad \mathrm{Tr}(\boldsymbol{S}) + \mathrm{Tr}(\boldsymbol{W}) \le P_b, \tag{10}$$

$$C_{t,b} - C_{t,e}(\boldsymbol{S},\boldsymbol{W}) \ge R, \tag{11}$$

where P_b is the transmit power of FD-BS, and $R \ge 0$ is a predefined target of the secret receive rate at FD-BS.

At the optimal point of $\mathbf{P1}$, we know the objective function (9) must be greater than or equal to zero,[5] then the proposed optimization $\mathbf{P1}$ will provide both uplink and downlink channels with nonnegative secret rates.

III. Optimization for Single Transmit-Antenna FD-BS

Let us first consider the traditional scenario when FD-BS is equipped with $N = 1$ transmit antenna. In this case, the covariances design of $\boldsymbol{S}$ and $\boldsymbol{W}$ reduces to the power allocation as $P_s = \mathrm{Tr}(\boldsymbol{S})$ and $P_w = \mathrm{Tr}(\boldsymbol{W})$ for information transmitting and jamming transmitting, respectively. Problem $\mathbf{P1}$ can then be re-expressed as

$$\mathbf{P2}: \max_{P_s\ge0,P_w\ge0} \quad C_{b,r}(P_s,P_w) - C_{b,e}(P_s,P_w) \tag{12}$$

$$\text{s.t.} \quad P_s + P_w \le P_b, \tag{13}$$

$$C_{t,b} - C_{t,e}(P_s,P_w) \ge R, \tag{14}$$

where (4) to (6) are simplified to

$$C_{b,r}(P_s,P_w) = \log_2\left(1 + \frac{P_s\|h_r\|^2}{1+P_w\|h_r\|^2}\right), \tag{15}$$

$$C_{b,e}(P_s,P_w) = \log_2\left(1 + \frac{P_s\|h_e\|^2}{1+P_t\|g_e\|^2+P_w\|h_e\|^2}\right), \tag{16}$$

[4]The definition of "undecodable" can be found in [27]. A transmitted signal is "undecodable" when the secret rate is greater than or equal to zero.

[5]It can be easily shown that the worst secret transmit rate is equal to zero when $\boldsymbol{S} = \mathbf{0}$.

$$C_{t,e}(P_s,P_w) = \log_2\left(1 + \frac{P_t\|g_e\|^2}{1+P_s\|h_e\|^2+P_w\|h_e\|^2}\right). \tag{17}$$

Observing the objective function and the constraints of $\mathbf{P2}$, we know that $\mathbf{P2}$ has the same optimal solutions as the following new problem

$$\mathbf{P2.1}: \max_{P_s\ge0,P_w\ge0} \left(1+\frac{P_s}{\frac{1}{\|h_r\|^2}+P_w}\right) \Bigg/ \left(1+\frac{P_s}{\frac{1+P_t\|g_e\|^2}{\|h_e\|^2}+P_w}\right) \tag{18}$$

$$\text{s.t.} P_s + P_w \le P_b, \tag{19}$$

$$P_s + P_w \ge \frac{2^R P_t\|g_e\|^2 + 2^R - P_t\|\boldsymbol{h_t}\|^2 - 1}{\|h_e\|^2(1+P_t\|\boldsymbol{h_t}\|^2 - 2^R)}, \tag{20}$$

which is feasible when

$$\frac{2^R P_t\|g_e\|^2 + 2^R - P_t\|\boldsymbol{h_t}\|^2 - 1}{\|h_e\|^2(1+P_t\|\boldsymbol{h_t}\|^2 - 2^R)} \le P_b. \tag{21}$$

1) Case 1: $1/\|h_r\|^2 \ge (1+P_t\|g_e\|^2)/\|h_e\|^2$: In this case, the optimal value of $\mathbf{P2.1}$ is easily proved to be 1 when $P_s^* = 0$ and

$$P_w \in \left[\frac{2^R P_t\|g_e\|^2 + 2^R - P_t\|\boldsymbol{h_t}\|^2 - 1}{\|h_e\|^2(1+P_t\|\boldsymbol{h_t}\|^2 - 2^R)}, P_b\right]. \tag{22}$$

Nevertheless, we should choose

$$P_w^* = \left(\frac{2^R P_t\|g_e\|^2 + 2^R - P_t\|\boldsymbol{h_t}\|^2 - 1}{\|h_e\|^2(1+P_t\|\boldsymbol{h_t}\|^2 - 2^R)}\right)^+, \tag{23}$$

to reduce power consumption.

2) Case 2: $1/\|h_r\|^2 < (1+P_t\|g_e\|^2)/\|h_e\|^2$: Let us first provide the following lemma.

Lemma 1: When $1/\|h_r\|^2 < (1+P_t\|g_e\|^2)/\|h_e\|^2$, the optimal power allocation P_s^* and P_w^* of $\mathbf{P2.1}$ must satisfy $P_s^* + P_w^* = P_b$.

Proof: See Appendix A. ■

With Lemma 1, the optimal power allocation for $\mathbf{P2.1}$ can be derived from the following new problem

$$\mathbf{P2.2}: \max_{P_w\ge0} \frac{\left(\frac{1+P_t\|g_e\|^2}{\|h_e\|^2}+P_w\right)\left(\frac{1}{\|h_r\|^2}+P_b\right)}{\left(\frac{1}{\|h_r\|^2}+P_w\right)\left(\frac{1+P_t\|g_e\|^2}{\|h_e\|^2}+P_b\right)} \tag{24}$$

$$\text{s.t.} \quad P_s + P_w = P_b. \tag{25}$$

Define

$$f_2(P_w) = \frac{\left(\frac{1+P_t\|g_e\|^2}{\|h_e\|^2}+P_w\right)\left(\frac{1}{\|h_r\|^2}+P_b\right)}{\left(\frac{1}{\|h_r\|^2}+P_w\right)\left(\frac{1+P_t\|g_e\|^2}{\|h_e\|^2}+P_b\right)}, \tag{26}$$

whose partial derivative can be computed as

$$\frac{\partial f_2(P_w)}{\partial P_w} = \frac{\left(\frac{1}{\|h_r\|^2}-\frac{1+P_t\|g_e\|^2}{\|h_e\|^2}\right)\left(\frac{1}{\|h_r\|^2}+P_b\right)}{\left(\frac{1}{\|h_r\|^2}+P_w\right)^2\left(\frac{1+P_t\|g_e\|^2}{\|h_e\|^2}+P_b\right)} < 0. \tag{27}$$

Hence, $f_2(P_w)$ is a monotonically decreasing function with respect to P_w. Consequently, we obtain $P_w^* = 0$ and $P_s^* = P_b$.

Remark 1: Interestingly, simultaneous information and jamming transmission cannot be optimal when FD-BS is equipped with a single transmit antenna.

IV. Optimization for Multiple Transmit-Antenna FD-BS

When FD-BS is equipped with $N > 1$ transmit antennas, $\mathbf{P1}$ can be equivalently expressed as

$$\mathbf{P3}: \quad \max_{\theta \geq 0} \quad \chi(\theta), \tag{28}$$

where θ is an auxiliary variable and $\chi(\theta)$ is defined as

$$\chi(\theta) = \max_{\boldsymbol{S}\succeq\mathbf{0},\boldsymbol{W}\succeq\mathbf{0}} \quad C_{b,r}(\boldsymbol{S},\boldsymbol{W}) - \log_2(1+\theta) \tag{29}$$

$$\text{s.t.} \quad (11), C_{b,e}(\boldsymbol{S},\boldsymbol{W}) \leq \log_2(1+\theta). \tag{30}$$

Let us further define

$$\xi = \frac{2^R P_t \|g_e\|^2 + 2^R - P_t\|\boldsymbol{h}_t\|^2 - 1}{1 + P_t\|\boldsymbol{h}_t\|^2 - 2^R} \tag{31}$$

for later use. The global optimal θ^* of $\mathbf{P3}$ can be obtained from one dimensional search, while our main task in this section is to solve $\chi(\theta)$ for each trial θ.

A. Tight SDP Relaxation

Denote $\boldsymbol{H}_r = \boldsymbol{h}_r\boldsymbol{h}_r^{\mathrm{H}}$ and $\boldsymbol{H}_e = \boldsymbol{h}_e\boldsymbol{h}_e^{\mathrm{H}}$, both being rank 1 matrices. We know that $\chi(\theta)$ has the same optimal solutions with the following new problem

$$\mathbf{P3.1}: \max_{\boldsymbol{S},\boldsymbol{W}} \frac{\mathrm{Tr}(\boldsymbol{H}_r\boldsymbol{S})}{1+\mathrm{Tr}(\boldsymbol{H}_r\boldsymbol{W})} \tag{32}$$

$$\text{s.t.} \mathrm{Tr}(\boldsymbol{H}_e\boldsymbol{S}) - \theta\mathrm{Tr}(\boldsymbol{H}_e\boldsymbol{W}) \leq \theta(1+P_t\|g_e\|^2), \tag{33}$$

$$\mathrm{Tr}(\boldsymbol{S}) + \mathrm{Tr}(\boldsymbol{W}) \leq P_b, \tag{34}$$

$$\mathrm{Tr}(\boldsymbol{H}_e\boldsymbol{S}) + \mathrm{Tr}(\boldsymbol{H}_e\boldsymbol{W}) \geq \xi, \tag{35}$$

$$\boldsymbol{S} \succeq \mathbf{0}, \quad \boldsymbol{W} \succeq \mathbf{0}, \tag{36}$$

$$\mathrm{Rank}(\boldsymbol{S}) = 1, \mathrm{Rank}(\boldsymbol{W}) = 1. \tag{37}$$

We may change variables as

$$\boldsymbol{\Phi_s} = \varphi\boldsymbol{S}, \quad \boldsymbol{\Phi_w} = \varphi\boldsymbol{W}, \quad \varphi > 0, \tag{38}$$

and from Charnes-Cooper transformation [28], $\mathbf{P3.1}$ can be equivalently expressed as

$$\mathbf{P3.2}: \max_{\boldsymbol{\Phi_s},\boldsymbol{\Phi}_w,\varphi} \quad \mathrm{Tr}(\boldsymbol{H}_r\boldsymbol{\Phi_s}) \tag{39}$$

$$\text{s.t.} \ \varphi + \mathrm{Tr}(\boldsymbol{H}_r\boldsymbol{\Phi_w}) = 1, \tag{40}$$

$$\mathrm{Tr}(\boldsymbol{H}_e\boldsymbol{\Phi_s}) - \theta\mathrm{Tr}(\boldsymbol{H}_e\boldsymbol{\Phi}_w) - \varphi\theta(1+P_t\|g_e\|^2) \leq 0, \tag{41}$$

$$\mathrm{Tr}(\boldsymbol{\Phi_s}) + \mathrm{Tr}(\boldsymbol{\Phi_w}) - \varphi P_b \leq 0, \tag{42}$$

$$\mathrm{Tr}(\boldsymbol{H}_e\boldsymbol{\Phi_s}) + \mathrm{Tr}(\boldsymbol{H}_e\boldsymbol{\Phi_w}) - \varphi\xi \geq 0, \tag{43}$$

$$\varphi > 0, \boldsymbol{\Phi_s} \succeq \mathbf{0}, \boldsymbol{\Phi_w} \succeq \mathbf{0}, \tag{44}$$

$$\mathrm{Rank}(\boldsymbol{\Phi_s}) = 1, \mathrm{Rank}(\boldsymbol{\Phi_w}) = 1. \tag{45}$$

Dropping the rank-one constraints in (45), $\mathbf{P3.2}$ becomes a convex SDP problem, which is also known as SDP relaxation [29]. Note that SDP relaxation in general does not guarantee rank one solutions. Nevertheless, we can prove that there always exist the optimal $\boldsymbol{\Phi_s^*}$ and $\boldsymbol{\Phi_w^*}$ with ranks one for the SDP relaxed $\mathbf{P3.2}$, so they are also the optimal solutions for the original $\mathbf{P3.2}$.

The Lagrange [30] of SDP relaxed $\mathbf{P3.2}$ can be defined as

$$\begin{aligned}\mathcal{L}(\boldsymbol{\Phi_s},\boldsymbol{\Phi_w},\alpha,\beta,\lambda,\mu) &= \mathrm{Tr}(\boldsymbol{H}_r\boldsymbol{\Phi_s}) - \alpha\left(\mathrm{Tr}(\boldsymbol{H}_r\boldsymbol{\Phi_w}) + \varphi - 1\right)\\ &- \beta\left(\mathrm{Tr}(\boldsymbol{H}_e\boldsymbol{\Phi_s}) - \theta\mathrm{Tr}(\boldsymbol{H}_e\boldsymbol{\Phi_w}) - \varphi\theta(1+P_t\|g_e\|^2)\right)\\ &- \lambda\left(\mathrm{Tr}(\boldsymbol{\Phi_s}) + \mathrm{Tr}(\boldsymbol{\Phi_w}) - \varphi P_b\right)\\ &+ \mu\left(\mathrm{Tr}(\boldsymbol{H}_e\boldsymbol{\Phi_s}) + \mathrm{Tr}(\boldsymbol{H}_e\boldsymbol{\Phi_w}) - \varphi\xi\right),\end{aligned} \tag{46}$$

where α, $\beta \geq 0$, $\lambda \geq 0$ and $\mu \geq 0$ are the dual variables associated with the constraints (40) to (43), respectively. Then the Lagrange in (46) can be reformulated as

$$\mathcal{L}(\boldsymbol{\Phi_s},\boldsymbol{\Phi_w},\varphi,\alpha,\beta,\lambda,\mu) = \mathrm{Tr}(\boldsymbol{\Sigma}_1\boldsymbol{\Phi_s}) + \mathrm{Tr}(\boldsymbol{\Sigma}_2\boldsymbol{\Phi_w}) + \Sigma_3\varphi + \alpha, \tag{47}$$

where for simplicity, we define $\boldsymbol{\Sigma}_1$, $\boldsymbol{\Sigma}_2$ and Σ_3 as

$$\boldsymbol{\Sigma}_1 = \boldsymbol{H}_r - \beta\boldsymbol{H}_e - \lambda\boldsymbol{I} + \mu\boldsymbol{H}_e, \tag{48}$$

$$\boldsymbol{\Sigma}_2 = -\alpha\boldsymbol{H}_r + \beta\theta\boldsymbol{H}_e - \lambda\boldsymbol{I} + \mu\boldsymbol{H}_e, \tag{49}$$

$$\Sigma_3 = -\alpha + \beta\theta(1+P_t\|g_e\|^2) + \lambda P_b - \mu\xi. \tag{50}$$

Lemma 2: The optimal dual variable α^* of SDP relaxed $\mathbf{P3.2}$ must satisfy $\alpha^* > 0$.

Proof: See Appendix B. ■

Using Lemma 2, the Karush-Kuhn-Tucker (KKT) conditions [30] related to $\boldsymbol{\Phi_s}$, $\boldsymbol{\Phi_w}$ and φ, can be formulated as

$$\boldsymbol{H}_r - \beta^*\boldsymbol{H}_e - \lambda^*\boldsymbol{I} + \mu^*\boldsymbol{H}_e = \boldsymbol{\Sigma}_1^*, \tag{51}$$

$$-\alpha^*\boldsymbol{H}_r + \beta^*\theta\boldsymbol{H}_e - \lambda^*\boldsymbol{I} + \mu^*\boldsymbol{H}_e = \boldsymbol{\Sigma}_2^*, \tag{52}$$

$$-\alpha^* + \beta^*\theta(1+P_t\|g_e\|^2) + \lambda^*P_b - \mu^*\xi = \Sigma_3^*, \tag{53}$$

$$\Sigma_3^*\varphi^* = 0, \quad \boldsymbol{\Sigma}_1^*\boldsymbol{\Phi_s^*} = \mathbf{0}, \quad \boldsymbol{\Sigma}_2^*\boldsymbol{\Phi_w^*} = \mathbf{0}, \tag{54}$$

where $\beta^* \geq 0$, $\lambda^* \geq 0$ and $\mu^* \geq 0$ denote the corresponding optimal dual variables.

Lemma 3: The optimal dual variable λ^* in the KKT conditions satisfies $\lambda^* > 0$.

Proof: See Appendix C. ■

From Lemma 3 and (42), we know that the optimal $\boldsymbol{\Phi_s^*}$ and $\boldsymbol{\Phi_w^*}$ satisfy

$$\mathrm{Tr}(\boldsymbol{\Phi_s^*}) + \mathrm{Tr}(\boldsymbol{\Phi_w^*}) = \varphi^*P_b. \tag{55}$$

In other words, FD-BS will always use full power in the multiple transmit-antenna scenario. Moreover, since $\lambda^* > 0$, it follows that

$$\begin{aligned}\mathrm{Rank}(\boldsymbol{\Sigma}_1^*) \geq \mathrm{Rank}(-\lambda^*\boldsymbol{I}) &- \mathrm{Rank}\left((\mu^*-\beta^*)\boldsymbol{H}_e\right)\\ &- \mathrm{Rank}(\boldsymbol{H}_r) \geq N-2.\end{aligned} \tag{56}$$

If $\mathrm{Rank}(\boldsymbol{\Sigma}_1^*) = N$, then we know from (54) that $\boldsymbol{\Phi_s^*} = \mathbf{0}$, which says that there is no information transmitted. Hence, $\mathrm{Rank}(\boldsymbol{\Sigma}_1^*) = N$ cannot be the optimal choice and there must be

$$N-2 \leq \mathrm{Rank}(\boldsymbol{\Sigma}_1^*) \leq N-1. \tag{57}$$

Since $\mathbf{\Sigma}_1^*\mathbf{\Phi}_{\boldsymbol{s}}^* = \mathbf{0}$, we know that

$$\mathrm{Rank}(\mathbf{\Sigma}_1^*) + \mathrm{Rank}(\mathbf{\Phi}_{\boldsymbol{s}}^*) \le N, \tag{58}$$

should be satisfied. Thus, there is

$$\mathrm{Rank}(\mathbf{\Phi}_{\boldsymbol{s}}^*) \le 2. \tag{59}$$

Lemma 4: There always exist optimal solutions $\mathbf{\Phi}_{\boldsymbol{s}}^*$ and $\mathbf{\Phi}_{\boldsymbol{w}}^*$ for the SDP relaxed $\mathbf{P3.2}$ with $\mathrm{Rank}(\mathbf{\Phi}_{\boldsymbol{s}}^*) = 1$ and $\mathrm{Rank}(\mathbf{\Phi}_{\boldsymbol{w}}^*) = 1$.

Proof: See Appendix D. ■

Lemma 4 implies that SDP relaxation does not change the optimal solutions for $\mathbf{P3.2}$. Moreover, the optimal transmit covariances $\boldsymbol{S}^* = \mathbf{\Phi}_{\boldsymbol{s}}^*/\varphi^*$ and $\boldsymbol{W}^* = \mathbf{\Phi}_{\boldsymbol{w}}^*/\varphi^*$ can be obtained from $\mathbf{\Phi}_{\boldsymbol{s}}^*$, $\mathbf{\Phi}_w{}^*$ and φ^*, as indicated in (38).

For now the SDP relaxed $\mathbf{P3.2}$ can be efficiently solved using the standard convex optimization techniques, e.g., the interior-point method [30]. If the founded $\mathbf{\Phi}_{\boldsymbol{s}}^*$ has $\mathrm{Rank}(\mathbf{\Phi}_{\boldsymbol{s}}^*) = 2$, then the equivalent optimal rank-one $\mathbf{\Phi}_{\boldsymbol{s}}^*$ can be obtained using (D.22) in Appendix D. The optimal information and jamming beamforming vectors, $\boldsymbol{s}^*, \boldsymbol{w}^*$ can then be derived from singular value decomposition (SVD) of $\mathbf{\Phi}_{\boldsymbol{s}}^*$ and $\mathbf{\Phi}_{\boldsymbol{w}}^*$.

B. The Lagrangian Dual Approach

Besides directly solving SDP relaxed $\mathbf{P3.2}$ from standard convex tool, we continue to derive more insightful results in this subsection.

With Lemma 4, we know simultaneous information and jamming beamforming is optimal, and then $\mathbf{P3.2}$ can be equivalently reformulated as

$$\mathbf{P3.3}: \max_{\boldsymbol{s}',\boldsymbol{w}',\varphi>0} \quad \|\boldsymbol{h}_r^{\mathrm{H}}\boldsymbol{s}'\|^2 \tag{60}$$

$$\text{s.t. } \varphi + \|\boldsymbol{h}_r^{\mathrm{H}}\boldsymbol{w}'\|^2 - 1 = 0, \tag{61}$$

$$\|\boldsymbol{h}_e^{\mathrm{H}}\boldsymbol{s}'\|^2 - \theta\|\boldsymbol{h}_e^{\mathrm{H}}\boldsymbol{w}'\|^2 - \varphi\theta(1+P_t\|g_e\|^2) \le 0, \tag{62}$$

$$\|\boldsymbol{s}'\|^2 + \|\boldsymbol{w}'\|^2 - \varphi P_b = 0, \tag{63}$$

$$\|\boldsymbol{h}_e^{\mathrm{H}}\boldsymbol{s}'\|^2 + \|\boldsymbol{h}_e^{\mathrm{H}}\boldsymbol{w}'\|^2 - \varphi\xi \ge 0, \tag{64}$$

where $\boldsymbol{s} = \boldsymbol{s}'/\sqrt{\varphi}$ and $\boldsymbol{w} = \boldsymbol{w}'/\sqrt{\varphi}$ are the information beamforming vector and jamming beamforming vector to be calculated, respectively. The Lagrange of $\mathbf{P3.3}$ is defined as

$$\begin{aligned}&\boldsymbol{\mathcal{L}}(\boldsymbol{s}',\boldsymbol{w}',\varphi,\alpha',\beta',\lambda',\mu') = \boldsymbol{s}'^{\mathrm{H}}\boldsymbol{h}_r\boldsymbol{h}_r^{\mathrm{H}}\boldsymbol{s}'\\&-\alpha'\left(\varphi + \boldsymbol{w}'^{\mathrm{H}}\boldsymbol{h}_r\boldsymbol{h}_r^{\mathrm{H}}\boldsymbol{w}' - 1\right)\\&-\beta'\left(\boldsymbol{s}'^{\mathrm{H}}\boldsymbol{h}_e\boldsymbol{h}_e^{\mathrm{H}}\boldsymbol{s}' - \theta\boldsymbol{w}'^{\mathrm{H}}\boldsymbol{h}_e\boldsymbol{h}_e^{\mathrm{H}}\boldsymbol{w}' - \varphi\theta(1+P_t\|g_e\|^2)\right)\\&-\lambda'\left(\|\boldsymbol{s}'\|^2 + \|\boldsymbol{w}'\|^2 - \varphi P_b\right)\\&+\mu'\left(\boldsymbol{s}'^{\mathrm{H}}\boldsymbol{h}_e\boldsymbol{h}_e^{\mathrm{H}}\boldsymbol{s}' + \boldsymbol{w}'^{\mathrm{H}}\boldsymbol{h}_e\boldsymbol{h}_e^{\mathrm{H}}\boldsymbol{w}' - \varphi\xi\right),\end{aligned} \tag{65}$$

where α', $\beta' \ge 0$, λ', and $\mu' \ge 0$ denote the dual variables associated with the constraints from (61) to (64), respectively. The Lagrange in (65) can be further formulated as

$$\begin{aligned}&\mathcal{L}(\boldsymbol{s}',\boldsymbol{w}',\varphi,\alpha',\beta',\lambda',\mu')\\&\qquad = \boldsymbol{s}'^{\mathrm{H}}\mathbf{\Sigma}_1'\boldsymbol{s}' + \boldsymbol{w}'^{\mathrm{H}}\mathbf{\Sigma}_2'\boldsymbol{w}' + \Sigma_3'\varphi + \alpha',\end{aligned} \tag{66}$$

where for simplicity, we define $\mathbf{\Sigma}_1'$, $\mathbf{\Sigma}_2'$ and Σ_3' as

$$\mathbf{\Sigma}_1' = \boldsymbol{h}_r\boldsymbol{h}_r^{\mathrm{H}} - \beta'\boldsymbol{h}_e\boldsymbol{h}_e^{\mathrm{H}} - \lambda'\boldsymbol{I} + \mu'\boldsymbol{h}_e\boldsymbol{h}_e^{\mathrm{H}}, \tag{67}$$

$$\mathbf{\Sigma}_2' = -\alpha'\boldsymbol{h}_r\boldsymbol{h}_r^{\mathrm{H}} + \beta'\theta\boldsymbol{h}_e\boldsymbol{h}_e^{\mathrm{H}} - \lambda'\boldsymbol{I} + \mu'\boldsymbol{h}_e\boldsymbol{h}_e^{\mathrm{H}}, \tag{68}$$

$$\Sigma_3' = -\alpha' + \beta'\theta(1+P_t\|g_e\|^2) + \lambda'P_b - \mu'\xi. \tag{69}$$

The Lagrangian dual function is then

$$\zeta(\alpha',\beta'\ge 0,\lambda',\mu'\ge 0) = \max_{\boldsymbol{s}',\boldsymbol{w}',\varphi} \mathcal{L}(\boldsymbol{s}',\boldsymbol{w}',\varphi,\alpha',\beta',\lambda',\mu'). \tag{70}$$

To guarantee that (70) is not unbounded to infinity, $\mathbf{\Sigma}_1' \preceq \mathbf{0}$, $\mathbf{\Sigma}_2' \preceq \mathbf{0}$ and $\Sigma_3' \le 0$ should be satisfied. Consequently, the Lagrangian dual problem can be expressed as

$$\min_{\alpha',\beta',\lambda',\mu'} \quad \zeta(\alpha',\beta'\ge 0,\lambda',\mu'\ge 0), \tag{71}$$

which can be equivalently expanded as

$$\mathbf{P3.4}: \min_{\alpha',\beta',\lambda',\mu'} \quad \alpha' \tag{72}$$

$$\text{s.t. } -\mathbf{\Sigma}_1' \succeq \mathbf{0}, -\mathbf{\Sigma}_2' \succeq \mathbf{0}, -\Sigma_3' \ge 0, \tag{73}$$

$$\beta' \ge 0, \quad \mu' \ge 0. \tag{74}$$

Since the duality gap between $\mathbf{P3.3}$ and $\mathbf{P3.4}$ is zero, the optimal dual variable α'^* should be equal to the optimal value of (60), and then $\alpha'^* > 0$ must hold. Similar to Lemma 3, we can prove $\lambda'^* > 0$. Thus the constraints $\alpha' > 0$ and $\lambda' > 0$ should be included into $\mathbf{P3.4}$.

Using the duality between SDP relaxed $\mathbf{P3.2}$ and $\mathbf{P3.4}$, at the optimal point, we know that $\mathbf{\Sigma}_1'$ has the same value as $\mathbf{\Sigma}_1^*$, and $\mathbf{\Sigma}_2'$ has the same value as $\mathbf{\Sigma}_2^*$. Thus from (D.22) in Appendix D, the optimal beamforming directions $\vec{\boldsymbol{s}}^* = \boldsymbol{s}^*/\|\boldsymbol{s}^*\|$ and $\vec{\boldsymbol{w}}^* = \boldsymbol{w}^*/\|\boldsymbol{w}^*\|$ can be derived from the null space of $\mathbf{\Sigma}_1'$ and $\mathbf{\Sigma}_2'$. The SVD of $\mathbf{\Sigma}_1'$ and $\mathbf{\Sigma}_2'$ can be calculated, respectively, as

$$\mathbf{\Sigma}_1' = \boldsymbol{U}_1\begin{bmatrix}\boldsymbol{D}_1 & \mathbf{0}\\ \mathbf{0} & \mathbf{0}\end{bmatrix}\boldsymbol{V}_1^{\mathrm{H}}, \mathbf{\Sigma}_2' = \boldsymbol{U}_2\begin{bmatrix}\boldsymbol{D}_2 & 0\\ 0 & 0\end{bmatrix}\boldsymbol{V}_2^{\mathrm{H}}, \tag{75}$$

where from Appendix D we know $\mathrm{Rank}(\boldsymbol{D}_1) = N-1$ or $\mathrm{Rank}(\boldsymbol{D}_1) = N-2$, and $\mathrm{Rank}(\boldsymbol{D}_2) = N-1$. Let $\boldsymbol{u}_{1,N-1}$ and $\boldsymbol{u}_{1,N}$ be the last two columns of $\boldsymbol{U}_1$, and $\boldsymbol{u}_{2,N}$ be the last column of $\boldsymbol{U}_2$.

1) Case 1) $\mathrm{Rank}(\boldsymbol{D}_1) = N-1$: We obtain

$$\vec{\boldsymbol{s}}^* = \boldsymbol{u}_{1,N}, \quad \vec{\boldsymbol{w}}^* = \boldsymbol{u}_{2,N}. \tag{76}$$

2) Case 2) $\mathrm{Rank}(\boldsymbol{D}_1) = N-2$: Let us first define the following notations:

$$\mathbf{\Theta}_1 = [\boldsymbol{u}_{1,N-1}\boldsymbol{u}_{1,N}][\boldsymbol{u}_{1,N-1}\boldsymbol{u}_{1,N}]^{\mathrm{H}}, \tag{77}$$

$$\mathbf{\Theta}_2 = \boldsymbol{u}_{2,N}\boldsymbol{u}_{2,N}^{\mathrm{H}}, \tag{78}$$

$$\mathbf{\Theta}_{\boldsymbol{s}} = \mathbf{\Theta}_1 - \mathbf{\Theta}_2. \tag{79}$$

From Appendix D, we know that $\boldsymbol{u}_{2,N}$ must be in the null space of $-\mathbf{\Sigma}_1'$. Hence $\mathbf{\Theta}_{\boldsymbol{s}}$ must satisfy $\mathrm{Rank}(\mathbf{\Theta}_{\boldsymbol{s}}) = 1$.

Then the SVD of $\mathbf{\Theta}_{\boldsymbol{s}}$ can be calculated as

$$\mathbf{\Theta}_{\boldsymbol{s}} = \boldsymbol{U}_3\begin{bmatrix}D_3 & \mathbf{0}\\ \mathbf{0} & \mathbf{0}\end{bmatrix}\boldsymbol{V}_3^{\mathrm{H}}, \tag{80}$$

TABLE I
NUMBER OF VARIABLES COMPARISON

Variables \ Problems	$\mathbf{P3.3}$	$\mathbf{P3.4}$
Number of Real	1	4
Number of Complex	$2N$	0
Total Variables	$2N+1$	4

where D_3 is a scalar. Let $\boldsymbol{u}_{3,1}$ be the first column of $\boldsymbol{U}_3$. We obtain

$$\vec{\boldsymbol{s}}^* = \boldsymbol{u}_{3,1}, \quad \vec{\boldsymbol{w}}^* = \boldsymbol{u}_{2,N}. \tag{81}$$

Let us further denote $\eta_{\boldsymbol{s}}$ and $\eta_{\boldsymbol{w}}$ as the coefficients of $\boldsymbol{s}^* = \eta_{\boldsymbol{s}}\vec{\boldsymbol{s}}^*$ and $\boldsymbol{w}^* = \eta_{\boldsymbol{w}}\vec{\boldsymbol{w}}^*$ respectively. The unknown variables $\eta_{\boldsymbol{s}}$, $\eta_{\boldsymbol{w}}$ and φ^* can be derived with the following equations

$$\begin{cases} \|\boldsymbol{h}_r^{\mathrm{H}}\eta_{\boldsymbol{s}}\vec{\boldsymbol{s}}^*\|^2 = \alpha'^* & \text{due to (60)},\\ \varphi^* + \|\boldsymbol{h}_r^{\mathrm{H}}\eta_{\boldsymbol{w}}\vec{\boldsymbol{w}}^*\|^2 - 1 = 0 & \text{due to (61)},\\ \|\eta_{\boldsymbol{s}}\vec{\boldsymbol{s}}^*\|^2 + \|\eta_{\boldsymbol{w}}\vec{\boldsymbol{w}}^*\|^2 - \varphi^* P_b = 0 & \text{due to (63)}. \end{cases} \tag{82}$$

Then $\eta_{\boldsymbol{s}}$, $\eta_{\boldsymbol{w}}$ and φ^* can be successively derived as

$$\eta_{\boldsymbol{s}} = \sqrt{\frac{\alpha'^*}{\|\boldsymbol{h}_r^{\mathrm{H}}\vec{\boldsymbol{s}}^*\|^2}}, \tag{83}$$

$$\eta_{\boldsymbol{w}} = \sqrt{\frac{P_b - \|\eta_{\boldsymbol{s}}\vec{\boldsymbol{s}}^*\|^2}{\|\vec{\boldsymbol{w}}^*\|^2 + P_b\|\boldsymbol{h}_r^{\mathrm{H}}\vec{\boldsymbol{w}}^*\|^2}}, \tag{84}$$

$$\varphi^* = \frac{\|\eta_{\boldsymbol{s}}\vec{\boldsymbol{s}}^*\|^2 + \|\eta_{\boldsymbol{w}}\vec{\boldsymbol{w}}^*\|^2}{P_b}. \tag{85}$$

Using (83)∼(85), we can obtain the optimal information beamforming vector $\boldsymbol{s}^*/\sqrt{\varphi^*}$ and jamming beamforming vector $\boldsymbol{w}^*/\sqrt{\varphi^*}$.

C. Complexity Comparison

The number of variables to be solved in $\mathbf{P3.3}$ and $\mathbf{P3.4}$ are compared in Table I. For $\mathbf{P3.3}$, the unknown auxiliary variable φ and beamforming vectors $\boldsymbol{s}, \boldsymbol{w}$ totally contain one real variable and $2N$ complex variables. While for $\mathbf{P3.4}$, the unknown dual variables α', β', λ' and μ' contain only four real variables. Consequently, $\mathbf{P3.4}$ possesses a much lower computational complexity than $\mathbf{P3.3}$. Note that with the increasing of the number of FD-BS transmit antennas, we can achieve a remarkable complexity reduction by solving $\mathbf{P3.4}$ instead of $\mathbf{P3.3}$.

V. SIMULATION RESULTS

In this section, computer simulations are presented to evaluate the performance of the proposed algorithms. The transmit power of Tx is set as $P_t = 5\ \mathrm{dBm}$. The entries of the channel vectors $\boldsymbol{h}_e$, $\boldsymbol{h}_r$, $\boldsymbol{h}_t$ and g_e are all generated as independent CSCG random variables distributed with $\mathcal{CN}(0,1)$. Moreover, the FD-BS transmit power P_b sweeps from 1 mW to 1000 mW, which is equivalent to the range of average SNRs per receive antenna from 0 dB to 30 dB. The results are derived by averaging over 10000 simulation trails. Note that from (11) there is

$$\begin{aligned} R_{\max} &= \max C_{t,b} - C_{t,e}(\boldsymbol{S},\boldsymbol{W}) \\ &= \log_2\left(1 + P_t\|\boldsymbol{h}_t\|^2\right) - \log_2\left(1 + \frac{P_t\|g_e\|^2}{1 + P_b\|\boldsymbol{h}_e\|^2}\right). \end{aligned} \tag{86}$$

When $R_{\max}$ of any specific run (due to the channel realization of each run) is smaller than R, then $\mathbf{P1}$, $\mathbf{P2}$ and $\mathbf{P3}$ are infeasible. In fact, using (86), the FD-BS can easily choose an appropriate R (i.e., $R <= R_{\max}$) to make $\mathbf{P1}$, $\mathbf{P2}$ and $\mathbf{P3}$ feasible. To provide more insightful results for different values of R, we will still discuss the infeasible cases where we simply set the secret transmit/receive rates, as well as power allocations to be zero.

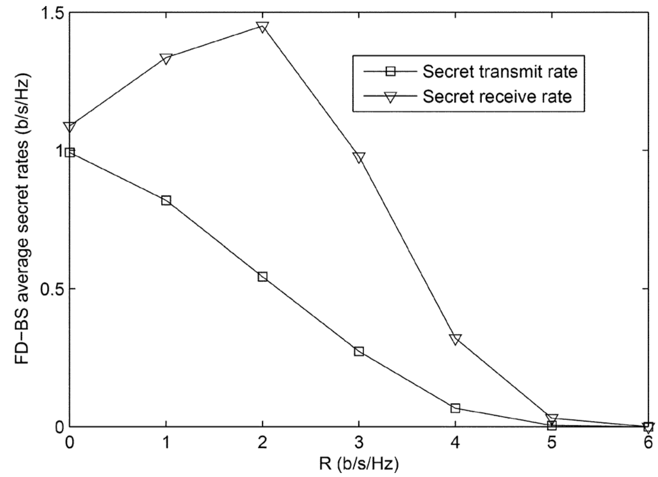


Fig. 2. Single-antenna FD-BS achievable secret rates versus R with $P_t = 5\ \mathrm{dBm}$ and $P_b = 20\ \mathrm{dBm}$.

A. Single Transmit Antenna at FD-BS

For single transmit-antenna scenario, we assume that FD-BS is equipped with $M = 1$ receive antenna and $N = 1$ transmit antenna.

The average secret transmit/receive rates versus R are shown in Fig. 2 for FD-BS transmit power $P_b = 20\ \mathrm{dBm}$. It is seen that the average secret transmit rate monotonically decreases with R, especially when $R \geq 6\ \mathrm{b/s/Hz}$, the average secret transmit rate almost approaches zero. The reason is that $\mathbf{P2}$ with more runs will be infeasible with the increasing of R. Moreover, the average secret receive rate is an increasing function of R when $R \leq 2\ \mathrm{b/s/Hz}$, while starts to decrease when $R > 2\ \mathrm{b/s/Hz}$. It also approaches zero when $R \geq 6\ \mathrm{b/s/Hz}$. The reason is that when $R \leq 2\ \mathrm{b/s/Hz}$, the increasing of the R is faster than the effect of the infeasible runs so the overall effect of the secret receive rate is still increasing. However, when $R \geq 2\ \mathrm{b/s/Hz}$, more and more infeasible runs appear, while the increase of R cannot compensate for such kind of the effect, so the average secret receive rate is decreasing.

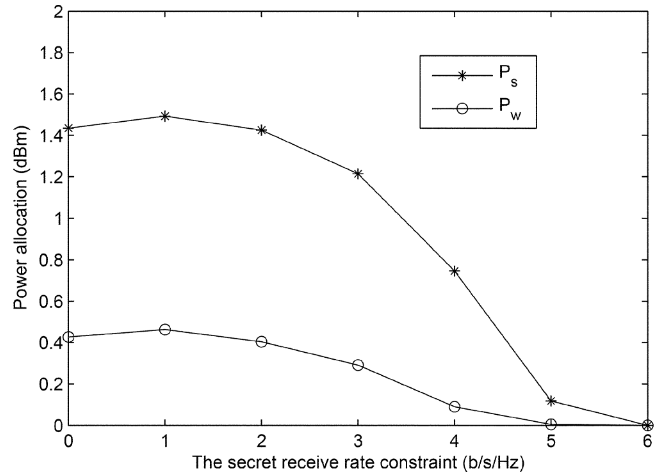


Fig. 3. Average power allocation versus R with $P_t = 5$ dBm and $P_b = 20$ dBm.

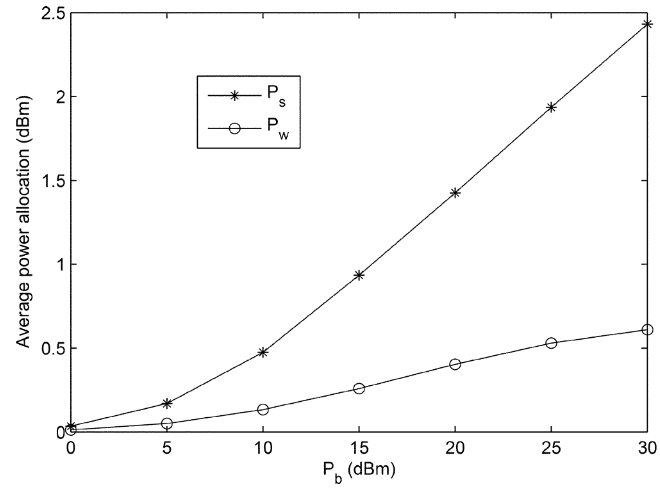


Fig. 5. Average power allocation versus P_b with $P_t = 5$ dBm and $R = 2$ b/s/Hz.

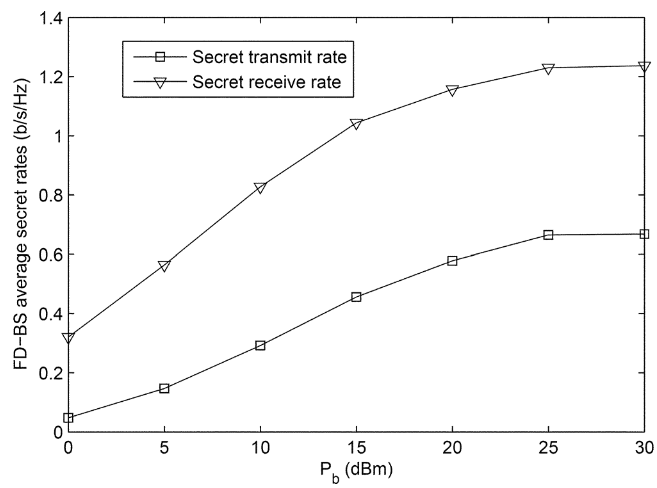


Fig. 4. Achievable secret rates versus P_b with $P_t = 5$ dBm and $R = 2$ b/s/Hz.

The corresponding average power allocations versus R are demonstrated in Fig. 3. It is seen that the average power allocated for information transmitting decreases with R. Moreover, the average power allocated for jamming transmitting increases with R when $R \leq 1$ b/s/Hz and decreases with R when $R > 1$ b/s/Hz. When $R \leq 1$ b/s/Hz, from (23) we know FD-BS can use low power to achieve the maximum secret transmit rate for some runs. With the increase of R, more power will be used to satisfy the secret receive constraint. Thus, we observe that P_w is increasing. While when $R > 1$ b/s/Hz, the probability of infeasible runs increases with R and thus both powers allocated for information/jamming transmissions will decrease with R, until almost every run is infeasible at $R \geq 6$ b/s/Hz.

In the next example, we plot the average secret transmit/receive rates versus P_b in Fig. 4 for $R = 2$ b/s/Hz. Obviously, both the average secret transmit/receive rates increase with the increase of P_b. Nevertheless, the growth of the average secret transmit/receive rates becomes slow when $P_b \geq 25$ dBm. In fact we can analytically explain this phenomenon as follows:

For each simulation trail, when $1/\|h_r\|^2 < (1 + P_t\|g_e\|^2)/\|h_e\|^2$, from (12) the secret transmit rate satisfies

$$\lim_{P_b\to\infty} C_{b,r}(P_s,P_w) - C_{b,e}(P_s,P_w) = \log_2\left(\frac{\|h_e\|^2}{\|h_r\|^2(1+P_t\|g_e\|^2)}\right), \quad (87)$$

while from (14) the secret receive rate satisfies

$$\lim_{P_b\to\infty} C_{t,b} - C_{t,e}(P_s,P_w) = \log_2\left(1 + P_t\|\boldsymbol{h}_t\|^2\right). \quad (88)$$

However, when $1/\|h_r\|^2 \geq (1 + P_t\|g_e\|^2)/\|h_e\|^2$, from (12) the secret transmit rate satisfies

$$\lim_{P_b\to\infty} C_{b,r}(P_s,P_w) - C_{b,e}(P_s,P_w) = 1, \quad (89)$$

while from (14) the secret receive rate satisfies

$$\lim_{P_b\to\infty} C_{t,b} - C_{t,e}(P_s,P_w) = R. \quad (90)$$

Combing the above cases, we can conclude that with large P_b, both the secret transmit/receive rates approach constants in each simulation run. Thus, the average secret transmit/receive rates (over 10000 channel realizations) also approach constants. The corresponding average power allocations versus P_b are demonstrated in Fig. 5. It is seen that both the average power allocated for information/jamming transmissions monotonically increase with P_b.

B. Multiple Transmit Antennas at FD-BS

For multiple transmit-antenna FD-BS, we assume that FD-BS is equipped with $M = 1$ receive antennas and $N = 2$ transmit antennas.

We first show the average secret transmit/receive rates versus R in Fig. 6 for the FD-BS transmit power $P_b = 20$ dBm. When $R \leq 3$ b/s/Hz, the average secret transmit rate monotonically decreases with the increase of R and reaches the lowest value at 2.5 b/s/Hz, while the average secret receive rate monotonically increases and approaches the highest value at 1.7 b/s/Hz. This

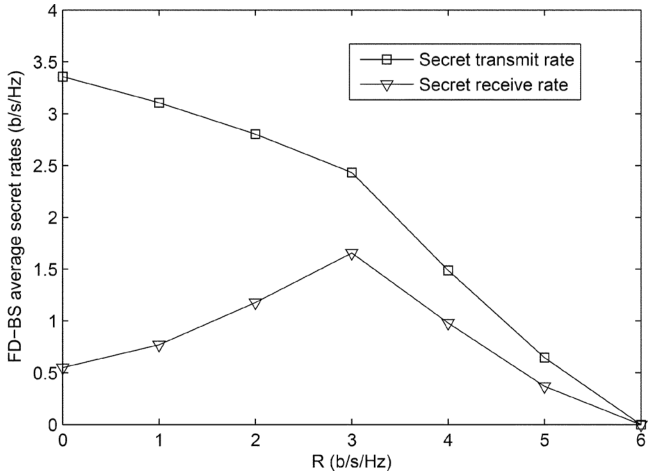


Fig. 6. Multiple-antenna FD-BS achievable secret rates versus R with $P_t = 5\ \mathrm{dBm}$ and $P_b = 20\ \mathrm{dBm}$.

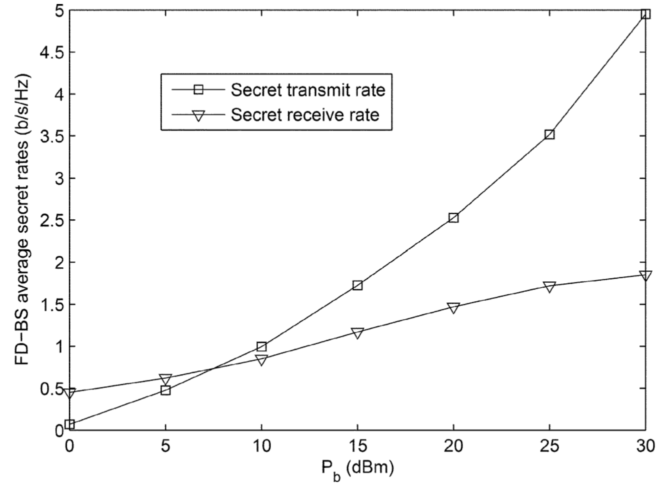


Fig. 7. Multiple-antenna FD-BS achievable secret rates versus P_b with $P_t = 5\ \mathrm{dBm}$ and $R = 3\ \mathrm{b/s/Hz}$.

is mainly due to the fact that with the increasing of R, the secret receive rate constraint is more difficult to be satisfied. Thus, the secret transmit rate decreases with R. For the secret receive rate, the increasing of R is faster than the effect of the infeasible runs so the overall effect of the secret receive rate is still increasing. However, when $R > 3\ \mathrm{b/s/Hz}$, more and more infeasible runs appear, while the increase of R cannot compensate for such kind of the effect, so both the average secret transmit/receive rates are decreasing.

The average secret transmit/receive rates versus P_b are demonstrated in Fig. 7 for $R = 3\ \mathrm{b/s/Hz}$. We see that both the average secret transmit/receive rates monotonically increase with the increase of P_b. Note that the growth of the average secret receive rate is slower than that of the average secret transmit rate. The reason is that with large P_b, the secret receive rate will approach a constant in each simulation run, as can be mathematically showed here. From (11) and using $\boldsymbol{w}^* = \eta_{\boldsymbol{w}} \vec{\boldsymbol{w}}^*$, the secret receive rate satisfies

$$\begin{aligned} &\lim_{P_b \to \infty} C_{t,b} - C_{t,e}(\boldsymbol{S}, \boldsymbol{W}) \\ &\geq \lim_{\eta_{\boldsymbol{w}} \to \infty} \log_2\left(1 + P_t\|\boldsymbol{h}_t\|^2\right) - \log_2\left(1 + \frac{P_t\|g_e\|^2}{1 + \eta_{\boldsymbol{w}}^2 \|\boldsymbol{h}_r^{\mathrm{H}} \vec{\boldsymbol{w}}^*\|^2}\right) \\ &\geq \log_2\left(1 + P_t\|\boldsymbol{h}_t\|^2\right). \end{aligned} \tag{91}$$

On the other hand, from (11) the secret receive rate also satisfies

$$\begin{aligned} &\lim_{P_b \to \infty} C_{t,b} - C_{t,e}(\boldsymbol{S}, \boldsymbol{W}) \\ &\leq \lim_{P_b \to \infty} \log_2\left(1 + P_t\|\boldsymbol{h}_t\|^2\right) - \log_2\left(1 + \frac{P_t\|g_e\|^2}{1 + P_b\|\boldsymbol{h}_e\|^2}\right) \\ &\leq \log_2\left(1 + P_t\|\boldsymbol{h}_t\|^2\right). \end{aligned} \tag{92}$$

Combing (91) and (92), there is

$$\lim_{P_b \to \infty} C_{t,b} - C_{t,e}(\boldsymbol{S}, \boldsymbol{W}) = \log_2\left(1 + P_t\|\boldsymbol{h}_t\|^2\right). \tag{93}$$

Hence, the secret receive rate approaches a constant in each simulation run, and the average secret receive rate also approaches a constant.

TABLE II
RUNNING TIME COMPARISON

Problems \ N	2	4	6	8
P3.3	0.18 s	0.28 s	0.36 s	0.48 s
P3.4	0.11 s	0.13 s	0.15 s	0.17 s

C. Running Time Comparison

In this example, we solve $\mathbf{P3.3}$ as the second order cone programming (SOCP) and solve $\mathbf{P3.4}$ as the SDP from the same convex optimization tools [30]. The average CPU running times for solving $\mathbf{P3.3}$ and $\mathbf{P3.4}$ under different value of N are compared in Table II. We see both the CPU running time of $\mathbf{P3.3}$ and $\mathbf{P3.4}$ increases with N. However, the CPU running time of $\mathbf{P3.3}$ increase much faster and is much larger than that of $\mathbf{P3.4}$. Hence with the increase of N, we could achieve a remarkable complexity reduction by solving $\mathbf{P3.4}$ instead of $\mathbf{P3.3}$. Note that, we understand that comparing the running time may not be a strict way but it does provide insightful results indicating the complexity difference between the two approaches.

VI. CONCLUSIONS

In this paper, we proposed a new transmission strategy for an FD-BS that could guarantee both the transmit secrecy and the receive secrecy. We formulate the problem as maximizing the secret transmit rate under the secret receive rate constraint and the FD-BS transmit power constraint. For the single transmit-antenna scenario, the original problem reduces to the optimal power allocation and we proved that the simultaneous information and the jamming transmission can never be optimal. For the multiple transmit antennas scenario, we proved that the rank-one information beamforming and jamming beamforming could serve as the optimal strategy. In addition, we also designed a low complex algorithm from the dual approach. Simulation results are provided to corroborate the proposed studies.

APPENDIX A
PROOF OF LEMMA 1

Let us prove $P_s^* + P_w^* = P_b$ from contradiction. Define

$$f_1(P_s, P_w) = \left(1 + \frac{P_s}{\frac{1}{\|h_r\|^2} + P_w}\right) \Big/ \left(1 + \frac{P_s}{\frac{1+P_t\|g_e\|^2}{\|h_e\|^2} + P_w}\right) = \frac{\left(\frac{1+P_t\|g_e\|^2}{\|h_e\|^2} + P_w\right)\left(\frac{1}{\|h_r\|^2} + P_s + P_w\right)}{\left(\frac{1}{\|h_r\|^2} + P_w\right)\left(\frac{1+P_t\|g_e\|^2}{\|h_e\|^2} + P_s + P_w\right)}. \quad \text{(A.1)}$$

When $1/\|h_r\|^2 < (1 + P_t\|g_e\|^2)/\|h_e\|^2$, the partial derivative of $f_1(P_s, P_w)$ with respect to P_s can be computed as

$$\frac{\partial f_1(P_s, P_w)}{\partial P_s} = \frac{\left(\frac{1+P_t\|g_e\|^2}{\|h_e\|^2} + P_w\right)\left(\frac{1+P_t\|g_e\|^2}{\|h_e\|^2} - \frac{1}{\|h_r\|^2}\right)}{\left(\frac{1}{\|h_r\|^2} + P_w\right)\left(\frac{1+P_t\|g_e\|^2}{\|h_e\|^2} + P_s + P_w\right)^2} > 0, \quad \text{(A.2)}$$

which says that $f_1(P_s, P_w)$ is a monotonically increasing function with respect to P_s. Assuming P_s^* and P_w^* are the optimal solutions for $\mathbf{P2.1}$ with $P_s^* + P_w^* < P_b$ and satisfy the constraint (20). Then, the unused power $\Delta P_b = P_b - P_s^* - P_w^*$ can be added to P_s^* to obtain

$$f_1(P_s^* + \Delta P_b, P_w^*) > f_1(P_s^*, P_w^*), \quad \text{(A.3)}$$

which contradicts to assumption that P_s^* and P_w^* are optimal. Then, the proof is completed.

APPENDIX B
PROOF OF LEMMA 2

Using (47), the Lagrangian dual function [30] can be defined as

$$\zeta(\alpha, \beta \geq 0, \lambda \geq 0, \mu \geq 0) = \max_{\mathbf{\Phi_s}, \mathbf{\Phi_w}, \varphi} \boldsymbol{\mathcal{L}}(\mathbf{\Phi_s}, \mathbf{\Phi_w}, \varphi, \alpha, \beta, \lambda, \mu). \quad \text{(B.1)}$$

To guarantee that (B.1) is not unbounded to infinity, we know that $\mathbf{\Sigma}_1 \preceq \mathbf{0}$, $\mathbf{\Sigma}_2 \preceq \mathbf{0}$ and $\Sigma_3 \leq 0$ should be satisfied. Consequently, the Lagrangian dual problem [30] can be expressed as

$$\min_{\alpha,\beta,\lambda,\mu} \quad \zeta(\alpha, \beta \geq 0, \lambda \geq 0, \mu \geq 0). \quad \text{(B.2)}$$

We can equivalently express (B.2) as

$$\min_{\alpha,\beta,\lambda,\mu} \quad \alpha \quad \text{(B.3)}$$
$$\text{s.t.} \quad \mathbf{\Sigma}_1 \preceq \mathbf{0}, \quad \mathbf{\Sigma}_2 \preceq \mathbf{0}, \quad \Sigma_3 \leq 0, \quad \text{(B.4)}$$
$$\beta \geq 0, \quad \lambda \geq 0, \quad \mu \geq 0. \quad \text{(B.5)}$$

Since the duality gap between SDP relaxed $\mathbf{P3.2}$ and its Lagrangian dual problem is zero, α^* should be equal to the optimal value of (39). Thus, $\alpha^* > 0$ must be satisfied.

APPENDIX C
PROOF OF LEMMA 3

Assuming $\lambda^* = 0$, from (51) we obtain

$$\mathbf{\Sigma}_1^* = \boldsymbol{H}_r - (\beta^* - \mu^*)\boldsymbol{H}_e. \quad \text{(C.1)}$$

Case 1: $\beta^* - \mu^* \leq 0$: From (C.1) it is obvious that $\mathbf{\Sigma}_1^* \succ \mathbf{0}$ which contradicts to $\mathbf{\Sigma}_1^* \preceq \mathbf{0}$. Thus, we obtain $\lambda^* > 0$ in this case.

Case 2: $\beta^* - \mu^* > 0$: Using the constraint $\mathbf{\Sigma}_1^* \preceq \mathbf{0}$, for any $\boldsymbol{x} \neq \mathbf{0}$, we have $\boldsymbol{x}^{\mathrm{H}}\mathbf{\Sigma}_1^*\boldsymbol{x} \leq 0$. Assuming $\boldsymbol{x}^{\mathrm{H}}\boldsymbol{H}_e\boldsymbol{x} = 0$, from (C.1) we obtain

$$\boldsymbol{x}^{\mathrm{H}}\mathbf{\Sigma}_1^*\boldsymbol{x} = \boldsymbol{x}^{\mathrm{H}}\boldsymbol{H}_r\boldsymbol{x} \leq 0. \quad \text{(C.2)}$$

Since $\boldsymbol{H}_r \succeq \mathbf{0}$, there is $\boldsymbol{x}^{\mathrm{H}}\boldsymbol{H}_r\boldsymbol{x} \geq 0$. Thus we know $\boldsymbol{x}^{\mathrm{H}}\boldsymbol{H}_r\boldsymbol{x} = 0$ must hold. It requires that any $\boldsymbol{x} \neq \mathbf{0}$ lies in the null space of $\boldsymbol{H}_e$ must also be in the null space of $\boldsymbol{H}_r$. However, it cannot be true since $\boldsymbol{h}_e$ and $\boldsymbol{h}_r$ are independent and randomly generated vectors, and should be linear independent. Consequently, $\lambda^* > 0$ must hold in this case.

Combining the above two cases, it follows that $\lambda^* > 0$ always holds and the proof is completed.

APPENDIX D
PROOF OF LEMMA 4

Proof of $\mathrm{Rank}(\mathbf{\Phi}_{\boldsymbol{w}}^*)$*:* Since $\alpha^* > 0$, there is

$$\mathrm{Rank}\left(-\lambda^*\boldsymbol{I} - \alpha^*\boldsymbol{H}_r\right) = N. \quad \text{(D.1)}$$

Moreover,

$$\mathrm{Rank}\left((\beta^*\theta + \mu^*)\boldsymbol{H}_e\right) \leq 1. \quad \text{(D.2)}$$

It then follows from (52) that $\mathrm{Rank}(\mathbf{\Sigma}_2^*) \geq N - 1$. From (54) we have

$$\mathrm{Rank}(\mathbf{\Sigma}_2^*) + \mathrm{Rank}(\mathbf{\Phi}_w^*) \leq N. \quad \text{(D.3)}$$

Thus, $\mathrm{Rank}(\mathbf{\Phi}_{\boldsymbol{w}}^*) \leq 1$ should hold.

Proof of $\mathrm{Rank}(\mathbf{\Phi}_{\boldsymbol{s}}^*)$*:* From (59), we know $\mathrm{Rank}(\mathbf{\Phi}_{\boldsymbol{s}}^*) = 1$ or $\mathrm{Rank}(\mathbf{\Phi}_{\boldsymbol{s}}^*) = 2$.

Assume $\mathrm{Rank}(\mathbf{\Phi}_{\boldsymbol{s}}^*) = 2$. From (54) we also know $\mathrm{Rank}(\mathbf{\Sigma}_1^*) + \mathrm{Rank}(\mathbf{\Phi}_{\boldsymbol{s}}^*) \leq N$. Thus, there is

$$\mathrm{Rank}(\mathbf{\Sigma}_1^*) \leq N - 2. \quad \text{(D.4)}$$

Combining (57), we obtain

$$\mathrm{Rank}(\mathbf{\Sigma}_1^*) = N - 2. \quad \text{(D.5)}$$

Since $\lambda^* > 0$, it follows that

$$N - 1 \leq \mathrm{Rank}\left(-\lambda^*\boldsymbol{I} - (\beta^* - \mu^*)\boldsymbol{H}_e\right) \leq N. \quad \text{(D.6)}$$

If $\mathrm{Rank}\left(-\lambda^*\boldsymbol{I} - (\beta^* - \mu^*)\boldsymbol{H}_e\right) = N$, we know that

$$\mathrm{Rank}(\mathbf{\Sigma}_1^*) = \mathrm{Rank}\left(-\lambda^*\boldsymbol{I} - (\beta^* - \mu^*)\boldsymbol{H}_e + \boldsymbol{H}_r\right) \geq N - 1, \quad \text{(D.7)}$$

which contradicts (D.5). Thus, there is

$$\mathrm{Rank}\left(-\lambda^*\boldsymbol{I} - (\beta^* - \mu^*)\boldsymbol{H}_e\right) = N - 1. \quad \text{(D.8)}$$

Since $\lambda^* > 0$, from (D.8) we know $\beta^* - \mu^* < 0$ must hold. Let $\boldsymbol{\pi}_1 \in \mathbb{C}^{N\times 1}$ denote the basis of the null space of $-\lambda^*\boldsymbol{I} - (\beta^* - \mu^*)\boldsymbol{H}_e$. Note that $\boldsymbol{\pi}_1$ must be parallel to $\boldsymbol{h}_e$.

Left and right multiplying both sides of (51) by $\boldsymbol{\pi}_1^{\rm H}$ and $\boldsymbol{\pi}_1$, respectively, yields

$$\begin{aligned}\boldsymbol{\pi}_1^{\rm H}\boldsymbol{\Sigma}_1^*\boldsymbol{\pi}_1 &= \boldsymbol{\pi}_1^{\rm H}\left(-\lambda^*\boldsymbol{I} - (\beta^* - \mu^*)\boldsymbol{H}_e + \boldsymbol{H}_r\right)\boldsymbol{\pi}_1\\ &= \boldsymbol{\pi}_1^{\rm H}\boldsymbol{H}_r\boldsymbol{\pi}_1.\end{aligned} \tag{D.9}$$

Since $\boldsymbol{\Sigma}_1^* \preceq \boldsymbol{0}$ and $\boldsymbol{H}_r \succeq \boldsymbol{0}$, there must be $\boldsymbol{\pi}_1^{\rm H}\boldsymbol{\Sigma}_1^*\boldsymbol{\pi}_1 = 0$ and $\boldsymbol{\pi}_1^{\rm H}\boldsymbol{H}_r\boldsymbol{\pi}_1 = 0$. Thus $\boldsymbol{\pi}_1$ is one basis of the null space of $\boldsymbol{\Sigma}_1^*$ and is also one basis of the null space of $\boldsymbol{H}_r$. Let $\boldsymbol{\pi}_2 \in \mathbb{C}^{N\times 1}$ be another basis of the null space of $\boldsymbol{\Sigma}_1^*$ satisfying $\boldsymbol{\pi}_1^{\rm H}\boldsymbol{\pi}_2 = 0$. Note that $\boldsymbol{H}_e\boldsymbol{\pi}_2 = \boldsymbol{0}$ must also hold.

From (54) we know $\boldsymbol{\Phi}_{\boldsymbol{s}}^*$ must be in the null space of $\boldsymbol{\Sigma}_1^*$. Thus $\boldsymbol{\Phi}_{\boldsymbol{s}}^*$ can be expressed as

$$\boldsymbol{\Phi}_{\boldsymbol{s}}^* = \tau_1\boldsymbol{\pi}_1\boldsymbol{\pi}_1^{\rm H} + \tau_2\boldsymbol{\pi}_2\boldsymbol{\pi}_2^{\rm H} + \tau_3\boldsymbol{\pi}_1\boldsymbol{\pi}_2^{\rm H} + \bar{\tau}_3\boldsymbol{\pi}_2\boldsymbol{\pi}_1^{\rm H}, \tag{D.10}$$

where $\tau_1 \geq 0$, $\tau_2 \geq 0$ are two real values.

Next, left and right multiplying both sides of (52) by $\boldsymbol{\pi}_1^{\rm H}$ and $\boldsymbol{\pi}_1$, respectively, yields

$$\begin{aligned}\boldsymbol{\pi}_1^{\rm H}\boldsymbol{\Sigma}_2^*\boldsymbol{\pi}_1 &= \boldsymbol{\pi}_1^{\rm H}\left(-\alpha^*\boldsymbol{H}_r + \beta^*\theta\boldsymbol{H}_e - \lambda^*\boldsymbol{I} + \mu^*\boldsymbol{H}_e\right)\boldsymbol{\pi}_1\\ &= \boldsymbol{\pi}_1^{\rm H}\boldsymbol{\Sigma}_1^*\boldsymbol{\pi}_1 - (1+\alpha^*)\boldsymbol{\pi}_1^{\rm H}\boldsymbol{H}_r\boldsymbol{\pi}_1 + \beta^*(1+\theta)\boldsymbol{\pi}_1^{\rm H}\boldsymbol{H}_e\boldsymbol{\pi}_1\\ &= \beta^*(1+\theta)\boldsymbol{\pi}_1^{\rm H}\boldsymbol{H}_e\boldsymbol{\pi}_1.\end{aligned} \tag{D.11}$$

Due to the fact that $\boldsymbol{\Sigma}_2^* \preceq \boldsymbol{0}$, $\boldsymbol{H}_e \succ \boldsymbol{0}$, $\theta \geq 0$, $\beta^* \geq 0$ and $\boldsymbol{h}_e$ being parallel to $\boldsymbol{\pi}_1$, there must be

$$\boldsymbol{\pi}_1^{\rm H}\boldsymbol{\Sigma}_2^*\boldsymbol{\pi}_1 = 0, \quad \beta^* = 0. \tag{D.12}$$

Thus we know that $\boldsymbol{\pi}_1$ is one basis of the null space of $\boldsymbol{\Sigma}_2^*$. Since $\boldsymbol{\Sigma}_2^*\boldsymbol{\Phi}_{\boldsymbol{w}}^* = \boldsymbol{0}$ and $\mathrm{Rank}(\boldsymbol{\Sigma}_2^*) \geq N-1$, $\boldsymbol{\Phi}_{\boldsymbol{w}}^*$ can be expressed as

$$\boldsymbol{\Phi}_{\boldsymbol{w}}^* = \tau_4\boldsymbol{\pi}_1\boldsymbol{\pi}_1^{\rm H}, \tag{D.13}$$

where $\tau_4 > 0$ is a real scale.

Then let us show $\tau_3\boldsymbol{\pi}_1\boldsymbol{\pi}_2^{\rm H} + \bar{\tau}_3\boldsymbol{\pi}_2\boldsymbol{\pi}_1^{\rm H} = \boldsymbol{0}$ must hold at the optimal point. Substituting (D.10) and (D.13) into the SDP relaxed $\mathbf{P3.2}$, i.e., (39) to (44), we obtain

$$\mathrm{Tr}(\boldsymbol{H}_r\boldsymbol{\Phi}_{\boldsymbol{s}}^*) = \mathrm{Tr}(\boldsymbol{H}_r(\tau_2\boldsymbol{\pi}_2\boldsymbol{\pi}_2^{\rm H})), \tag{D.14}$$

$$\varphi^* + \mathrm{Tr}(\boldsymbol{H}_r\boldsymbol{\Phi}_{\boldsymbol{w}}^*) = \varphi^* = 1, \tag{D.15}$$

$$\begin{aligned}&\mathrm{Tr}(\boldsymbol{H}_e\boldsymbol{\Phi}_{\boldsymbol{s}}^*) - \theta\mathrm{Tr}(\boldsymbol{H}_e\boldsymbol{\Phi}_{\boldsymbol{w}}^*) - \varphi^*\theta(1 + P_t\|g_e\|^2)\\ &\quad = \mathrm{Tr}(\boldsymbol{H}_e(\tau_1\boldsymbol{\pi}_1\boldsymbol{\pi}_1^{\rm H})) - \theta\mathrm{Tr}(\boldsymbol{H}_e(\tau_4\boldsymbol{\pi}_1\boldsymbol{\pi}_1^{\rm H}))\\ &\qquad - \varphi^*\theta(1 + P_t\|g_e\|^2) \leq 0,\end{aligned} \tag{D.16}$$

$$\begin{aligned}&\mathrm{Tr}(\boldsymbol{\Phi}_{\boldsymbol{s}}^*) + \mathrm{Tr}(\boldsymbol{\Phi}_{\boldsymbol{w}}^*) - \varphi^* P_b\\ &\quad = \mathrm{Tr}(\tau_1\boldsymbol{\pi}_1\boldsymbol{\pi}_1^{\rm H} + \tau_2\boldsymbol{\pi}_2\boldsymbol{\pi}_2^{\rm H} + \tau_3\boldsymbol{\pi}_1\boldsymbol{\pi}_2^{\rm H} + \bar{\tau}_3\boldsymbol{\pi}_2\boldsymbol{\pi}_1^{\rm H})\\ &\qquad + \mathrm{Tr}(\tau_4\boldsymbol{\pi}_1\boldsymbol{\pi}_1^{\rm H}) - \varphi^* P_b \leq 0,\end{aligned} \tag{D.17}$$

$$\begin{aligned}\mathrm{Tr}(\boldsymbol{H}_e\boldsymbol{\Phi}_{\boldsymbol{s}}^*) + \mathrm{Tr}(\boldsymbol{H}_e\boldsymbol{\Phi}_{\boldsymbol{w}}^*) - \varphi^*\xi &= \mathrm{Tr}(\boldsymbol{H}_e(\tau_1\boldsymbol{\pi}_1\boldsymbol{\pi}_1^{\rm H}))\\ &\quad + \mathrm{Tr}(\boldsymbol{H}_e(\tau_4\boldsymbol{\pi}_1\boldsymbol{\pi}_1^{\rm H})) - \varphi^*\xi \geq 0,\end{aligned} \tag{D.18}$$

$$\varphi^* > 0, \quad \boldsymbol{\Phi}_{\boldsymbol{w}}^* = \tau_4\boldsymbol{\pi}_1\boldsymbol{\pi}_1^{\rm H} \succeq \boldsymbol{0}, \tag{D.19}$$

$$\boldsymbol{\Phi}_{\boldsymbol{s}}^* = \tau_1\boldsymbol{\pi}_1\boldsymbol{\pi}_1^{\rm H} + \tau_2\boldsymbol{\pi}_2\boldsymbol{\pi}_2^{\rm H} + \tau_3\boldsymbol{\pi}_1\boldsymbol{\pi}_2^{\rm H} + \bar{\tau}_3\boldsymbol{\pi}_2\boldsymbol{\pi}_1^{\rm H} \succeq \boldsymbol{0}, \tag{D.20}$$

where the property that $\boldsymbol{H}_r\boldsymbol{\pi}_1 = \boldsymbol{0}$ and $\boldsymbol{H}_e\boldsymbol{\pi}_2 = \boldsymbol{0}$ are utilized in the above derivations.

It can be directly observed that at the optimal point the term $\tau_3\boldsymbol{\pi}_1\boldsymbol{\pi}_2^{\rm H} + \bar{\tau}_3\boldsymbol{\pi}_2\boldsymbol{\pi}_1^{\rm H}$ must be zero, because it does not change the objective value (D.14) and the constraints (D.15), (D.16), (D.18), and (D.19), but it could assign more freedom for the constraint (D.17) and satisfies (D.20).

Therefore, the optimal $\boldsymbol{\Phi}_{\boldsymbol{s}}^*$ can be re-expressed as

$$\boldsymbol{\Phi}_{\boldsymbol{s}}^* = \tau_1\boldsymbol{\pi}_1\boldsymbol{\pi}_1^{\rm H} + \tau_2\boldsymbol{\pi}_2\boldsymbol{\pi}_2^{\rm H}. \tag{D.21}$$

Moreover, from (D.15), we know that $\varphi^* = 1$. Let us further show

$$\begin{cases}\boldsymbol{\Phi}_{\boldsymbol{s}}'^* = \boldsymbol{\Phi}_{\boldsymbol{s}}^* - \tau_1\boldsymbol{\pi}_1\boldsymbol{\pi}_1^{\rm H} = \tau_2\boldsymbol{\pi}_2\boldsymbol{\pi}_2^{\rm H},\\ \boldsymbol{\Phi}_{\boldsymbol{w}}'^* = \boldsymbol{\Phi}_{\boldsymbol{w}}^* + \tau_1\boldsymbol{\pi}_1\boldsymbol{\pi}_1^{\rm H} = (\tau_1 + \tau_4)\boldsymbol{\pi}_1\boldsymbol{\pi}_1^{\rm H},\\ \varphi'^* = \varphi^* = 1,\end{cases} \tag{D.22}$$

are also the optimal solutions for the SDP relaxed $\mathbf{P3.2}$.

Remark 2: The new solutions in (D.22) provide a rank-1 solution of $\boldsymbol{\Phi}_{\boldsymbol{s}}$ but still guarantee that $\mathrm{Rank}(\boldsymbol{\Phi}_{\boldsymbol{w}}^*) = 1$, which is consistent with the previous discussion.

Substituting (D.22) into (39)$\sim$(44) of the SDP relaxed $\mathbf{P3.2}$, we obtain

$$\mathrm{Tr}\left(\boldsymbol{H}_r\boldsymbol{\Phi}_{\boldsymbol{s}}'^*\right) = \mathrm{Tr}\left(\boldsymbol{H}_r\boldsymbol{\Phi}_{\boldsymbol{s}}^*\right), \tag{D.23}$$

$$\varphi'^* = \varphi^* = 1, \tag{D.24}$$

$$\begin{aligned}&\mathrm{Tr}(\boldsymbol{H}_e\boldsymbol{\Phi}_{\boldsymbol{s}}'^*) - \theta\mathrm{Tr}(\boldsymbol{H}_e\boldsymbol{\Phi}_{\boldsymbol{w}}'^*) - \varphi'^*\theta(1 + P_t\|g_e\|^2)\\ &\quad < \mathrm{Tr}(\boldsymbol{H}_e\boldsymbol{\Phi}_{\boldsymbol{s}}^*) - \theta\mathrm{Tr}(\boldsymbol{H}_e\boldsymbol{\Phi}_{\boldsymbol{w}}^*) - \varphi^*\theta(1 + P_t\|g_e\|^2) \leq 0,\end{aligned} \tag{D.25}$$

$$\begin{aligned}&\mathrm{Tr}(\boldsymbol{\Phi}_{\boldsymbol{s}}'^*) + \mathrm{Tr}(\boldsymbol{\Phi}_{\boldsymbol{w}}'^*) - \varphi'^* P_b\\ &\quad = \mathrm{Tr}(\boldsymbol{\Phi}_{\boldsymbol{s}}^*) + \mathrm{Tr}(\boldsymbol{\Phi}_{\boldsymbol{w}}^*) - \varphi^* P_b \leq 0,\end{aligned} \tag{D.26}$$

$$\begin{aligned}&\mathrm{Tr}(\boldsymbol{H}_e\boldsymbol{\Phi}_{\boldsymbol{s}}'^*) + \mathrm{Tr}(\boldsymbol{H}_e\boldsymbol{\Phi}_{\boldsymbol{w}}'^*) - \varphi'^*\xi\\ &\quad = \mathrm{Tr}(\boldsymbol{H}_e\boldsymbol{\Phi}_{\boldsymbol{s}}^*) + \mathrm{Tr}(\boldsymbol{H}_e\boldsymbol{\Phi}_{\boldsymbol{w}}^*) - \varphi^*\xi \geq 0,\end{aligned} \tag{D.27}$$

$$\begin{aligned}&\varphi'^* = \varphi^* > 0, \boldsymbol{\Phi}_{\boldsymbol{s}}'^* = \tau_2\boldsymbol{\pi}_2\boldsymbol{\pi}_2^{\rm H} \succeq \boldsymbol{0},\\ &\boldsymbol{\Phi}_{\boldsymbol{w}}'^* = (\tau_1 + \tau_4)\boldsymbol{\pi}_1\boldsymbol{\pi}_1^{\rm H} \succeq \boldsymbol{0},\end{aligned} \tag{D.28}$$

where the property that $\boldsymbol{H}_r\boldsymbol{\pi}_1 = \boldsymbol{0}$ and $\boldsymbol{H}_e\boldsymbol{\pi}_2 = \boldsymbol{0}$ are utilized in the above derivations. From (D.23), we know that $\boldsymbol{\Phi}_{\boldsymbol{s}}'^*$, $\boldsymbol{\Phi}_{\boldsymbol{w}}'^*$ and φ'^* will provide the same optimal objective value of the SDP relaxed $\mathbf{P3.2}$. Moreover, from (D.24) to (D.28), we can conclude that $\boldsymbol{\Phi}_{\boldsymbol{s}}'^*$, $\boldsymbol{\Phi}_{\boldsymbol{w}}'^*$ and φ'^* satisfy all the constraints of the SDP relaxed $\mathbf{P3.2}$. Consequently, $\boldsymbol{\Phi}_{\boldsymbol{s}}'^*$, $\boldsymbol{\Phi}_{\boldsymbol{w}}'^*$ and φ'^* are also optimal solutions of the SDP relaxed $\mathbf{P3.2}$.

From all the above discussions, we know at the optimal point, there always exist optimal solutions $\boldsymbol{\Phi}_{\boldsymbol{s}}^*$ and $\boldsymbol{\Phi}_{\boldsymbol{w}}^*$ with $\mathrm{Rank}(\boldsymbol{\Phi}_{\boldsymbol{s}}^*) = 1$ and $\mathrm{Rank}(\boldsymbol{\Phi}_{\boldsymbol{w}}^*) = 1$.

References

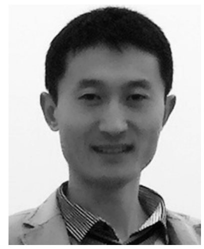
[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.

[2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[3] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[4] Y. Liang and H. V. Poor, "Generalized multiple access channels with confidential messages," in *Proc. IEEE ISIT*, Seattle, WA, USA, Jul. 2006, pp. 952–956.

[5] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.
[6] H. Alves, G. Brante, R. Demo Souza, D. B. d. Costa, and M. Latvaaho, "On the performance of full-duplex relaying under phy security constraints," in *Proc. IEEE ICASSP*, Florence, Italy, May 2014, pp. 3978–3981.
[7] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE VTC'05*, Dallas, TX, USA, Sep. 3, 2005, vol. 3, pp. 1906–1910.
[8] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
[9] J. Huang and A. L. Swindlehurst, "Robust secure transmission in MISO channels based on worst-case optimization," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1696–1707, Apr. 2012.
[10] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Trans. Inf. Forenics Security*, vol. 7, no. 2, pp. 704–716, Apr. 2012.
[11] S. A. A. Fakoorian and A. L. Swindlehurst, "Solutions for the MIMO Gaussian wiretap channel with a cooperative jammer," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 5013–5022, Oct. 2011.
[12] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.
[13] G. Zheng, L. C. Choo, and K. K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.
[14] 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.
[15] M. Pei, J. Wei, K. K. Wong, and X. Wang, "Masked beamforming for multiuser MIMO wiretap channels with imperfect CSI," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 544–549, Feb. 2012.
[16] 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.
[17] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: outage secrecy capacity/region analysis," *IEEE Commun. Lett.*, vol. 16, no. 10, pp. 1628–1631, Oct. 2012.
[18] 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.
[19] S. W. Kim, Y. J. Chun, and S. Kim, "Co-channel interference cancellation using single radio frequency and baseband chain," *IEEE Trans. Commun.*, vol. 58, no. 7, pp. 2169–2175, Jul. 2010.
[20] T. Riihonen, S. Werner, and R. Wichman, "Mitigation of loopback self-interference in full-duplex MIMO relays," *IEEE Trans. Signal Process.*, vol. 59, no. 12, pp. 5983–5993, Dec. 2011.
[21] M. Jain, J. I. Choi, and T. Kim, "Practical, real-time, full duplex wireless," in *The MobiCom*, Las Vegas, Nevada, USA, 2011.
[22] V. R. Cadambe and S. A. Jafar, "Degrees of freedom of wireless networks with relays, feedback, cooperation, and full duplex operation," *IEEE Trans. Inf. Theory*, vol. 55, no. 5, pp. 2334–2344, May 2009.
[23] H. Ju, E. Oh, and D. Hong, "Catching resource-devouring worms in next-generation wireless relay systems: two-way relay and full-duplex relay," *IEEE Commun. Mag.*, vol. 47, no. 9, pp. 58–65, Sep. 2009.
[24] B. P. Day, A. R. Margetts, D. W. Bliss, and P. Schniter, "Full-duplex MIMO relaying: achievable rates under limited dynamic range," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 8, pp. 1541–1553, Sep. 2012.
[25] L. Zhang, H. Wang, and T. Li, "Anti-jamming message-driven frequency hopping-part I: System design," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 70–79, Jan. 2013.
[26] L. Zhang and T. Li, "Anti-jamming message-driven frequency hopping-part II: capacity analysis under disguised jamming," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 80–88, Jan. 2013.
[27] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.
[28] A. Charnes and W. W. Cooper, "Programming with linear fractional functionals," *Naval Res. Logist. Quarter.*, vol. 9, no. 3-4, pp. 181–186, Dec. 1962.
[29] Z. Q. Luo, W. K. Ma, A. M. C. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems," *IEEE Signal Process. Mag.*, vol. 27, no. 3, pp. 20–34, May 2010.
[30] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.



Fenghao Zhu received the B.E. and M.E. degrees in signal and information processing from Xi'an Research Institute of High Technology, Xi'an, China, in 2008 and 2011, respectively. He is currently working toward the Ph.D. degree in the Department of Automation, Tsinghua University, Beijing, China.

His research interests mainly include MIMO techniques, multi-carrier communications, cooperative communication, cognitive radio networks, and convex optimizations.

Feifei Gao (M'09–SM'14) received the Ph.D. degree from National University of Singapore, Singapore, in 2007.

He was a Research Fellow with the Institute for Infocomm Research (I2R), A*STAR, Singapore, in 2008 and an Assistant Professor with the School of Engineering and Science, Jacobs University, Bremen, Germany, from 2009 to 2010. In 2011, he joined the Department of Automation, Tsinghua University, Beijing, China, where he is currently an Associate Professor. His research areas include communication theory, signal processing for communications, array signal processing, and convex optimizations. He has authored/ coauthored more than 60 refereed IEEE journal papers and more than 80 IEEE conference proceeding papers.

Prof. Gao has served as an Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE WIRELESS COMMUNICATIONS LETTERS, the *International Journal on Antennas and Propagations*, and *China Communications*. He has also served as the Symposium Co-Chair for 2015 IEEE Conference on Communications (ICC), 2014 IEEE Global Communications Conference (GLOBECOM), 2014 IEEE Vehicular Technology Conference Fall (VTC), as well as Technical Committee Members for many other IEEE conferences.

Minli Yao received the M.Sc. degree from Xi'an Research Institute of High Technology and the Ph.D. degree from Xi'an Jiao Tong University, both in Xi'an, China, in 1992 and 1999, respectively.

He is currently a professor at the Department of Communication Engineering, Xi'an Research Institute of High Technology. His current interests include satellite navigation signal structure design and signal processing, Sat-COM, and spreading communication.

Hongxing Zou received the B.E. degree in electronic engineering, the M.E. degree in signal and information processing, and the Ph.D. degree (with highest distinction) in pattern recognition and intelligent system from the Department of Automation, School of Information Science and Technology, Tsinghua University, Beijing, China, in 1988, 1996, and 2002, respectively.

Since 2002, he has been with the Department of Automation, Tsinghua University, where he currently is a Professor and Member of the Information Processing Faculty. His current research interests include time-frequency signal analysis, pattern recognition, matrix factorization, and inertial navigation systems.