Robust Secure Beamforming for SWIPT-Aided Relay Systems With Full-Duplex Receiver and Imperfect CSI

Xinrui Li, Wei Wang, *Member, IEEE*, Miao Zhang, *Student Member, IEEE*, Fuhui Zhou, *Member, IEEE*, and Naofal Al-Dhahir, *Fellow, IEEE*

***Abstract*—This paper investigates an energy-constrained relay-assisted secure communication system in the presence of a legitimate source-destination pair and a passive eavesdropper with imperfect channel state information (CSI). The energy-constrained relay exploits a power splitting (PS) protocol to simultaneously harvest energy and decode information from the received signal from the source, and then forwards the confidential signal to the full-duplex (FD) destination while it simultaneously transmits artificial noise (AN) to confuse the passive eavesdropper. This robust beamforming design is developed by maximizing the secrecy rate under the constraints of energy harvesting (EH) requirement at the relay and AN transmit power at the destination. Specifically, we formulate the joint relay beamforming and PS ratio as well as the AN power optimization as a non-convex quadratically-constrained problem. In order to circumvent this non-convexity issue, we decompose the original problem into three subproblems which can be determined by the proposed semidefinite relaxation (SDR) and successive convex optimization methods. Furthermore, we derive closed-form expressions for the optimal solutions of each subproblem. Finally, the original non-convex problem can be solved through a convergence guaranteed iterative algorithm. Simulation results are provided to demonstrate the effectiveness and superior performance of the proposed robust design compared with the benchmark schemes.**

***Index Terms*—Robust beamforming, secrecy rate, simultaneous wireless information and power transfer (SWIPT), imperfect channel state information (CSI), full-duplex (FD), artificial noise (AN).**

Manuscript received July 11, 2019; revised October 28, 2019; accepted December 10, 2019. Date of publication December 23, 2019; date of current version February 12, 2020. This work was supported in part by the Natural Science Foundation of China under Grants 61971245 and 61701214, in part by the Stereoscopic Coverage Communication Network Verification Platform for China Sea under Grant PCL2018KP002, in part by the Six Categories Talent Peak of Jiangsu Province under Grant KTHY-039, in part by the Excellent Youth Foundation of Jiangxi Province under Grant 2018ACB21012, and in part by the Postgraduate Research and Practice Innovation Program of Jiangsu Province under Grant KYCX19-2057. The review of this article was coordinated by Dr. Hai Lin. *(Corresponding author: Wei Wang.)*

X. Li and W. Wang are with the School of Information Science and Technology, Nantong University, Nantong 226019, China, and also with Research Center of Networks and Communications, Peng Cheng Laboratory, Shenzhen, 518055, China (e-mail: 1811310045@yjs.ntu.edu.cn; wwang2011@ntu.edu.cn).

M. Zhang is with the Department of Electronic Engineering, University of York, York, YO10 5DD, United Kingdom (e-mail: mz1022@york.ac.uk).

F. Zhou is with the College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing 210000, China (e-mail: zhoufuhui@ieee.org).

N. Al-Dhahir is with the Department of Electrical Engineering, University of Texas at Dallas, Dallas, TX 75080 USA (e-mail: aldhahir@utdallas.edu).

Digital Object Identifier 10.1109/TVT.2019.2961449

I. Introduction

DUE to the broadcast nature of wireless channels, wireless communication networks are vulnerable as they can be intercepted by potential eavesdroppers [1], [2]. Cryptographic techniques are widely used to enhance information security. However, these techniques introduce different challenges in terms of key exchange and distribution [3]–[6]. To address this issue, recently there have been increasing research works focusing on physical layer security techniques [7]–[11] while complementing the conventional encryption techniques in wireless networks.

The limited battery lifetime of wireless devices is another critical challenge for wireless communication networks. Simultaneous wireless information and power transfer (SWIPT) has emerged as a promising technology to address this issue [12]–[14]. Recently, different SWIPT-based designs have been proposed to improve the secrecy performance of energy-constrained communication systems. For instance, the secrecy rate and weighted sum energy were maximized in a multiple-input-single-output (MISO) SWIPT system in [15], respectively, where the transmitter sends energy and information simultaneously to the energy and information receivers. In [16], the authors investigated the secrecy rate maximization problem in an orthogonal frequency-division multiplexing (OFDM) SWIPT network through jointly designing the transmit power at both the transmitter and the jammer. A secrecy throughput maximization problem for a full-duplex (FD) jamming SWIPT system was studied in [17], where joint design of a secrecy rate and power splitting (PS) ratio optimization scheme was proposed. Moreover, the authors in [18] investigated the secrecy rate maximization problem in a non-regenerative SWIPT relay system under the constraints of the relay transmit power and energy harvesting (EH) requirements. The authors in [19] proposed a multi-antenna transmitter relaying network to improve secrecy rate performance, in which the beamforming vector, the PS ratio and the relay coefficients were jointly optimized. In [20], the authors investigated the secrecy performance in a wireless powered multicasting system through jointly designing the energy price and transfer time. Furthermore, the time switching (TS) ratio, the energy and information beamforming vector were jointly designed to maximize the secrecy rate in an energy-constrained network with one multi-antenna FD relay in [21].

Most existing works on secure SWIPT systems assumed perfect channel state information (CSI) of the eavesdroppers [15]–[21], which is not a realistic assumption in practical scenarios. The reason is that the eavesdroppers may remain silent to hide their existence, which may result in significant degradation of security performance. Therefore, designing a robust scheme to enhance the secrecy performance of energy-constrained systems taking into account CSI errors is a very challenging problem that has received increased attention recently. The robust secrecy throughput was maximized in a single input single output (SISO) SWIPT system in [22], where the TS ratio and the codeword rate were jointly designed. In [23], the PS ratio, the precoding and artificial noise (AN) covariance matrices were jointly designed to maximize the worst-case secrecy rate in a multiple input multiple output (MIMO) SWIPT system, in which it is assumed that the energy receiver's CSI cannot be perfectly obtained at the transmitter. The authors considered a MISO SWIPT system in [24], where the PS ratio, transmit and AN covariance matrix were jointly designed to maximize the robust secrecy rate. In [25], the authors investigated a MISO SWIPT cognitive system, where a robust joint design of the AN beamforming and PS ratio was studied. A wireless powered service integration system was proposed in [26], where the integrated service and AN matrices were jointly designed to maximize the robust secrecy rate. Furthermore, the secrecy throughput maximization problem in an energy-constrained SWIPT system was studied in [27], which proposed a FD self-jamming scheme to improve the robust security performance. Although the research efforts have been devoted to designing robust resource allocation schemes in one-hop secure SWIPT systems, the exiting designs, e.g., [22]–[27], may not be applicable to the SWIPT-aided secure systems, where the source cannot communicate directly with the destination due to path loss or obstacles.

Motivated by the aforementioned facts, this paper considers a SWIPT-aided secure relaying system, where a source transmits information to a legitimate destination via an energy-constrained relay in the presence of a passive eavesdropper.[1] A practical scenario that the eavesdropper's CSI cannot be perfectly obtained at both the relay and destination is considered. The energy-constrained relay needs to harvest energy and decode information from the source, and then forwards the secret messages to the destination. Moreover, in order to combat the eavesdropper with imperfect CSI, we assume that the destination node works in the FD mode, i.e., it can simultaneously receive confidential signals from the relay and transmit malicious AN signals to confuse the eavesdropper. Furthermore, to further enhance the reliability and security of this system, we assume that the relay node has multiple antennas to perform information beamforming. Then, we define and evaluate the system's secrecy rate, which quantifies both the communication reliability between the relay and destination and the communication confidentiality to the eavesdropper. We aim to determine the beamforming vector and PS ratio of the relay as well as the required AN power of the destination that maximize the robust secrecy rate of the energy-constrained relaying system.

It is worth noting that for the SWIPT-aided secure relay system with imperfect CSI of the eavesdropper, there have been some initial attempts (e.g., [28]–[30]) that addressed the security issues from other perspectives. For instance, a SWIPT-aided amplify-and-forward (AF) relay system with imperfect CSI has been considered in [28], where the cooperative beamforming and energy transfer were jointly designed. In [29], the authors investigated the secrecy rate maximization problem in a SWIPT-aided nonregenerative MIMO relay system, where a joint design of the source and relay beamforming matrices scheme was proposed. In [30], the beamforming matrix, AN power and PS ratio were jointly designed to minimize the relay power in a SWIPT-aided AF relay system while considering imperfect CSI of eavesdroppers. Our work differs from these works in the following aspects: 1) System setting: firstly, in [28]–[30], only EH threshold has been considered while both EH requirement and energy consumption (including transmission and circuit consumption) are considered in this paper, which makes our problem more suitable for practical scenarios. Secondly, the existing works [28]–[30] only assumed that the eavesdropper's CSI cannot be perfectly obtained at the relay, whereas both the relay and destination case are considered in this work. Thirdly, we propose a PS-based EH framework, whereas only individual information and energy receivers were considered in [28], [29], which are special cases of our proposed protocol. Finally, the authors in [28], [30] did not consider path loss in the channel response, which is usually an unrealistic assumption in practical scenarios. 2) Design method: in contrast to the half-duplex (HD) scheme in [28]–[30], we consider a FD destination node which can simultaneously receive signals from the relay and cooperatively transmit AN signals to confuse eavesdroppers, which can achieve a better use of the spatial degrees of freedom. To the best of our knowledge, the robust joint design for SWIPT-aided relay systems with FD receiver and imperfect CSI of the eavesdropper has not been reported in the literature. The main contributions of our work are summarized as follows:

- Our proposed robust joint FD design enhances both the secure and robust performance of the system, which makes it more suitable for practical scenarios than the existing work on energy-constrained secure relay communications [28]–[30].
- To circumvent the non-convexity of the design problem, the considered problem is decoupled into three subproblems, which can be solved based on semidefinite relaxation (SDR) techniques and successive convex optimization methods, respectively.
- The original non-convex problem can be effectively handled through the proposed iterative suboptimal algorithm. In each iteration, we determine the optimal beamforming vector and PS ratio of the relay as well as AN power vector of the destination, respectively.
- Extensive numerical results are presented to demonstrate the impact of different system parameters and the superior performance of the proposed robust joint design against

[1] This assumption has many potential applications in wireless networks, e.g., in cellular systems, when a legitimate source-destination pair cannot communicate directly while the relay should be employed to establish this communication without a fixed power supply.

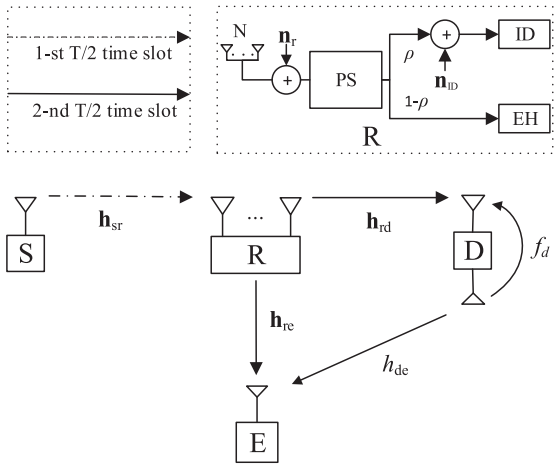

Fig. 1. A two-time slot SWIPT-based secure relaying network.

three other benchmark schemes proposed in the existing works.

The rest of this paper is organized as follows. The system model and the problem formulation are presented in Section II. Then, we design a three-step iterative algorithm to achieve the maximum secrecy rate in Section III. Section IV presents numerical results to validate the proposed scheme. Finally, Section V concludes the paper.

Notations: Boldface lowercase and uppercase letters denote vectors and matrices, respectively. $\mathbf{A}^*$, $\mathbf{A}^T$, $\mathbf{A}^H$, $\mathrm{Rank}(\mathbf{A})$, $\mathrm{Tr}(\mathbf{A})$ and $||\mathbf{A}||$ represent the conjugate, transpose, conjugate transpose, rank, trace, and Frobenius norm of matrix $\mathbf{A}$, respectively. $\mathrm{vec}(\mathbf{A})$ denotes the vectorization operation by stacking the columns of $\mathbf{A}$ into a single vector $\mathbf{a}$. $\mathbf{A} \succeq 0$ indicates that $\mathbf{A}$ is a positive semidefinite matrix. $\mathbf{I}_N$ denotes the $N \times N$ identity matrix. $\otimes$ and $\mathbb{E}(\cdot)$ represent the Kronecker product and statistical expectation, respectively. $\mathbb{C}^{x \times y}$ denotes the $x \times y$ domain of complex matrices. The distribution of a circular symmetric complex Gaussian vector with mean vector $\mathbf{x}$ and covariance matrix $\mathbf{\Sigma}$ is denoted by $\mathcal{CN}(\mathbf{x}, \mathbf{\Sigma})$.

II. System Model and Problem Formulation

This paper considers a secure relaying communication system shown in Fig. 1, which consists of one source S, one relay R, one legitimate destination D and one eavesdropper E. It is assumed that the relay is equipped with N antennas. The source and eavesdropper are equipped with a single antenna and the destination is equipped with a dual separate antenna.[2] This scenario is typical for device-to-device communications [11], [18], [32], [33], where two terminals directly communicate with each other with the help of a femtocell or a laptop. Furthermore, we assume that there is no direct link between the source and the destination or the eavesdropper, which usually occurs when the direct link does not exist due to the long-distance path loss or heavy channel fading [18], [32]. Such situation can occur in cellular networks or satellite communications, where the base station within one cell or the satellite can act as a relay to forward information for physically disconnected users. Specifically, we assume that the relay R has limited power supply which needs to harvest energy from S and then forwards the confidential signal to D. Based on the proposed two-phase SWIPT protocol, in the first $T/2$ time slot, the source transmits information (ρ) and energy $(1-\rho)$ simultaneously to the relay, where $\rho \in (0,1)$ represents the PS ratio. In the second $T/2$ time slot, the received signal at the relay is amplified and then forwarded to the destination and eavesdropper. At this phase, the FD destination also acts as a jammer to cooperatively transmit AN to degrade the received signal interference-plus-noise ratio (SINR) at the eavesdropper. The channels between S and R, R and D, R and E as well as D and E are represented by $\mathbf{h}_{sr}$, $\mathbf{h}_{rd}$, $\mathbf{h}_{re}$ and h_{de}, respectively. In addition, the self-interference channel at D is denoted by f_d.

Due to imperfectly known CSI of the passive eavesdropper, the actual channels $\mathbf{h}_{re}$ and h_{de} are modeled as

$$\mathbf{h}_{re} = \hat{\mathbf{h}}_{re} + \Delta\mathbf{h}_{re}, \tag{1}$$

$$h_{de} = \hat{h}_{de} + \Delta h_{de}, \tag{2}$$

where $\hat{\mathbf{h}}_{re}$ and $\hat{h}_{de}$ represent the estimated channel coefficients, and $\Delta\mathbf{h}_{re}$ and Δh_{de} are the estimate errors, which are bounded as $||\Delta\mathbf{h}_{re}||_2 \leq \mu$ and $||\Delta h_{de}||_2 \leq \nu$, here $\mu > 0$ and $\nu > 0$.

In the first $T/2$ phase, the received signal at the relay can be expressed as

$$\mathbf{y}_r = \mathbf{h}_{sr} x_t + \mathbf{n}_r, \tag{3}$$

where x_t denotes the transmit signal from S with transmit power $\mathbb{E}(|x_t|^2) = P_s$ and $\mathbf{n}_r$ represents the additive Gaussian noise at the relay with a distribution $\mathcal{CN}(\mathbf{0}, \sigma_r^2 \mathbf{I}_N)$. Based on the proposed PS-based SWIPT protocol, we express the received signal at the information decoding (ID) and the EH circuits respectively as

$$\mathbf{y}_r^{ID} = \sqrt{\rho}(\mathbf{h}_{sr} x_t + \mathbf{n}_r) + \mathbf{n}_{ID}, \tag{4}$$

and

$$\mathbf{y}_r^{EH} = \sqrt{1-\rho}(\mathbf{h}_{sr} x_t + \mathbf{n}_r), \tag{5}$$

where $\mathbf{n}_{ID}$ is the noise introduced by the ID circuit, which follows the distribution $\mathcal{CN}(\mathbf{0}, \sigma_{ID}^2 \mathbf{I}_N)$. In general, the harvested energy is nonlinear with respect to the received RF power [34], [35]. However, there is no a generic EH model which can captures all practical issues [36]. Thus, for simplicity, a linear EH model [28]–[30] is assumed and then the harvested energy is defined as

$$E_r^{EH} = \eta(1-\rho)\frac{T}{2}(P_s||\mathbf{h}_{sr}||_2^2 + \sigma_r^2), \tag{6}$$

where $\eta \in (0,1]$ denotes the EH efficiency.

In the second $T/2$ phase, we express the transmitted signal from the relay as

$$\begin{aligned} \mathbf{x}_r &= \mathbf{W}\mathbf{y}_r^{ID}, \\ &= \mathbf{W}(\sqrt{\rho}\mathbf{h}_{sr} x_t + \sqrt{\rho}\mathbf{n}_r + \mathbf{n}_{ID}), \end{aligned} \tag{7}$$

[2]Compared with single antenna FD communications [31] the separate antenna model has been already widely adopted in the literature [17], [21], [22], [26], [27].

where $\mathbf{W}$ represents the precoding matrix at the relay. Then, the power transmitted by the relay $\mathrm{Tr}(\mathbb{E}(\mathbf{x}_r\mathbf{x}_r^H)) = P_r$ can be defined as

$$P_r = \rho P_s||\mathbf{W}\mathbf{h}_{sr}||_2^2 + \rho\sigma_r^2||\mathbf{W}||_F^2 + \sigma_{ID}^2||\mathbf{W}||_F^2. \quad (8)$$

For the FD destination, after self-interference cancellation (SIC), the received signal is given by

$$\begin{aligned} \mathrm{y}_d &= \mathbf{h}_{rd}^T\mathbf{x}_r + f_d x_{SI} + n_d \\ &= \sqrt{\rho}\mathbf{h}_{rd}^T\mathbf{W}\mathbf{h}_{sr}x_t + \sqrt{\rho}\mathbf{h}_{rd}^T\mathbf{W}\mathbf{n}_r \\ &\quad + \mathbf{h}_{rd}^T\mathbf{W}\mathbf{n}_{ID} + f_d x_{SI} + n_d, \end{aligned} \quad (9)$$

where x_{SI} and n_d represent the residual self-interference and noise signals at the destination, which follow the distributions $n_{SI} \sim \mathcal{CN}(0, \sigma_{SI}^2)$ and $n_d \sim \mathcal{CN}(0, \sigma_d^2)$, respectively. Thus, the SINR and the achieved data rate at the destination are, respectively, defined as

$$\mathrm{SINR}_d = \frac{\rho P_s|\mathbf{h}_{rd}^T\mathbf{W}\mathbf{h}_{sr}|^2}{\rho\sigma_r^2||\mathbf{h}_{rd}^T\mathbf{W}||_2^2 + \sigma_{ID}^2||\mathbf{h}_{rd}^T\mathbf{W}||_2^2 + \sigma_{SI}^2|f_d|^2 + \sigma_d^2}, \quad (10)$$

and

$$R_d = \frac{1}{2}\log_2(1 + \mathrm{SINR}_d). \quad (11)$$

Moreover, we can express the received signal at the eavesdropper as

$$\begin{aligned} \mathbf{y}_e &= \mathbf{h}_{re}^T\mathbf{x}_r + \mathrm{h}_{de}z_d + n_e, \\ &= \sqrt{\rho}\mathbf{h}_{re}^T\mathbf{W}\mathbf{h}_{sr}x_t + \sqrt{\rho}\mathbf{h}_{re}^T\mathbf{W}\mathbf{n}_r \\ &\quad + \mathbf{h}_{re}^T\mathbf{W}\mathbf{n}_{ID} + \mathrm{h}_{de}z_d + n_e, \end{aligned} \quad (12)$$

where z_d denotes the AN from the destination following the distribution $\mathcal{CN}(0, \sigma_{Z_d}^2)$ and n_e represents the noise at the eavesdropper following the distribution $\mathcal{CN}(0, \sigma_e^2)$. Therefore, the SINR and the achieved data rate at the eavesdropper are, respectively, expressed as

$$\mathrm{SINR}_e = \frac{\rho P_s|\mathbf{h}_{re}^T\mathbf{W}\mathbf{h}_{sr}|^2}{\rho\sigma_r^2||\mathbf{h}_{re}^T\mathbf{W}||_2^2 + \sigma_{ID}^2||\mathbf{h}_{re}^T\mathbf{W}||_2^2 + \sigma_{Z_d}^2|h_{de}|^2 + \sigma_e^2}, \quad (13)$$

and

$$R_e = \frac{1}{2}\log_2(1 + \mathrm{SINR}_e). \quad (14)$$

For secure communication from S to D in the SWIPT-powered relaying system, we jointly design the beamforming vector and the PS ratio of the relay as well as the AN power of the destination to maximize the secrecy rate under the EH requirement and transmit power constraints. The optimization problem can be mathematically formulated as

$$\begin{aligned} \max_{\mathbf{W},\rho,\sigma_{Z_d}^2} \quad & [R_d - R_e]^+ \\ \text{s.t.} \quad & C1: \frac{T}{2}(P_r + P_{cr}) \le E_r^{EH}, \\ & C2: \frac{T}{2}\sigma_{Z_d}^2 + E_{\mathrm{SIC}} \le E_d, \\ & C3: \sigma_{Z_d}^2 \le P_{AN,\max}, \\ & C4: 0 < \rho < 1. \end{aligned} \quad (15)$$

where $[m]^+ \triangleq \max(m, 0)$, P_{cr} denotes the relay's circuit power consumption that is a constant value [14], E_{SIC} and E_d represent the energy consumption of SIC and the energy threshold of the destination, respectively, $P_{AN,\max}$ denotes the maximum transmit power of AN.

III. Iterative Algorithm For Secrecy Rate Maximization

In this section, a joint design scheme for solving the problem defined in (15) is proposed. We observe that the variables $\mathbf{W}$, ρ and $\sigma_{Z_d}^2$ are coupled in both the numerator and the denominator in R_d and R_e, respectively, which makes the proposed problem difficult to tackle directly. Furthermore, the operator $[\cdot]^+$ makes the objective function defined in (15) non-smooth at the zero point. Therefore, to deal with the non-convexity and non-smoothness issues of the problem defined in (15), we present Lemma 1 and then decouple it by solving its subproblems via alternating optimization approach [21], [30], [37].

Lemma 1 is proposed to handle the non-smoothness of the problem defined in (15).

Lemma 1: Problem (15) can be equivalently rewritten as follows

$$\begin{aligned} \max_{\mathbf{W},\rho,\sigma_{Z_d}^2} \quad & R_d - R_e \\ \text{s.t.} \quad & C1 - C4. \end{aligned} \quad (16)$$

Proof: Please refer to [38] and [39]. ■

Note that the transformed problem in (16) is still non-convex. Therefore, we propose an iterative suboptimal algorithm for tackling its non-convexity.

A. Optimization of Beamforming Vector $\mathbf{W}$

Proposition 1: For given ρ and $\sigma_{Z_d}^2$, by introducing the variables $\tilde{\mathbf{W}} \triangleq \mathbf{w}\mathbf{w}^H$ and $\mathbf{w} = \mathrm{vec}(\mathbf{W})$, the problem defined in (16) can be equivalently expressed as follows:

$$\begin{aligned} \max_{\tilde{\mathbf{W}}\succeq 0} \quad & \frac{1}{2}\left[\log_2\left(1 + \frac{\mathrm{Tr}(\mathbf{A}_1\tilde{\mathbf{W}})}{\mathrm{Tr}(\mathbf{A}_2\tilde{\mathbf{W}}) + a}\right)\right. \\ & \left. - \log_2\left(1 + \frac{\mathrm{Tr}(\mathbf{A}_3\tilde{\mathbf{W}})}{\mathrm{Tr}(\mathbf{A}_4\tilde{\mathbf{W}}) + b}\right)\right] \\ \text{s.t.} \quad & \mathrm{Tr}(\mathbf{A}_5\tilde{\mathbf{W}}) \le c, \\ & \mathrm{Rank}(\tilde{\mathbf{W}}) = 1, \end{aligned} \quad (17)$$

where $\mathbf{A}_1 = \rho P_s(\mathbf{h}_{sr}^*\mathbf{h}_{sr}^T \otimes \mathbf{h}_{rd}^*\mathbf{h}_{rd}^T)$, $\mathbf{A}_2 = (\rho\sigma_r^2 + \sigma_{ID}^2)(\mathbf{I}_N \otimes \mathbf{h}_{rd}^*\mathbf{h}_{rd}^T)$, $\mathbf{A}_3 = \rho P_s(\mathbf{h}_{sr}^*\mathbf{h}_{sr}^T \otimes (\hat{\mathbf{H}}_{re} + \xi\mathbf{I}_N))$, $\mathbf{A}_4 = (\rho\sigma_r^2 + \sigma_{ID}^2)(\hat{\mathbf{H}}_{re} - \xi\mathbf{I}_N)$, $\mathbf{A}_5 = \rho P_s(\mathbf{h}_{sr}^*\mathbf{h}_{sr}^T \otimes \mathbf{I}_N) + (\rho\sigma_r^2 + \sigma_{ID}^2)(\mathbf{I}_N \otimes \mathbf{I}_N)$, $a = \sigma_{SI}^2|f_d|^2 + \sigma_d^2$, $b = \sigma_{Zd}^2(\hat{H}_{de} - \zeta) + \sigma_e^2$, $c = \eta(1-\rho)(P_s||\mathbf{h}_{sr}||_2^2 + \sigma_r^2) - P_{cr}$.

Proof: Please refer to Appendix A. ■

Here, problem (17) is difficult to solve directly due to the rank-one constraint. Thus, we first consider the following relaxation problem :

$$\begin{aligned}\max_{\tilde{\mathbf{W}}\succeq 0} \quad & \frac{1}{2}\left[\log_2\left(1+\frac{\mathrm{Tr}(\mathbf{A}_1\tilde{\mathbf{W}})}{\mathrm{Tr}(\mathbf{A}_2\tilde{\mathbf{W}})+a}\right)\right. \\ & \left.-\log_2\left(1+\frac{\mathrm{Tr}(\mathbf{A}_3\tilde{\mathbf{W}})}{\mathrm{Tr}(\mathbf{A}_4\tilde{\mathbf{W}})+b}\right)\right] \\ \text{s.t.} \quad & \mathrm{Tr}(\mathbf{A}_5\tilde{\mathbf{W}})\le c. \end{aligned} \tag{18}$$

The problem defined in (18) is still intractable due to both the numerator and denominator of the fractions $\frac{\mathrm{Tr}(\mathbf{A}_1\tilde{\mathbf{W}})}{\mathrm{Tr}(\mathbf{A}_2\tilde{\mathbf{W}})+a}$ and $\frac{\mathrm{Tr}(\mathbf{A}_3\tilde{\mathbf{W}})}{\mathrm{Tr}(\mathbf{A}_4\tilde{\mathbf{W}})+b}$ containing the optimization variable $\tilde{\mathbf{W}}$. To tackle this issue, we introduce a slack variable t, then the problem defined in (18) reduces to the following problem:

$$\begin{aligned}\max_{\tilde{\mathbf{W}}\succeq 0, t\ge 1} \quad & \frac{\mathrm{Tr}((\mathbf{A}_1+\mathbf{A}_2)\tilde{\mathbf{W}})+a}{t(\mathrm{Tr}(\mathbf{A}_2\tilde{\mathbf{W}})+a)} \\ \text{s.t.} \quad & 1+\frac{\mathrm{Tr}(\mathbf{A}_3\tilde{\mathbf{W}})}{\mathrm{Tr}(\mathbf{A}_4\tilde{\mathbf{W}})+b}\le t, \\ & \mathrm{Tr}(\mathbf{A}_5\tilde{\mathbf{W}})\le c. \end{aligned} \tag{19}$$

In general, for a given t, the problem defined in (19) can be solved by using the conventional bisection search [37]. However, in this paper, an alternative method is proposed based on the Charnes-Cooper transformation [40], [41]. By defining a new variable $\tilde{\mathbf{W}}_1=\varphi\tilde{\mathbf{W}}$ with $\varphi=\frac{1}{t(\mathrm{Tr}(\mathbf{A}_2\tilde{\mathbf{W}})+a)}$, we rewrite problem (19) into the following form:

$$\begin{aligned}\max_{\tilde{\mathbf{W}}_1\succeq 0, t\ge 1, \varphi>0} \quad & \mathrm{Tr}((\mathbf{A}_1+\mathbf{A}_2)\tilde{\mathbf{W}}_1)+\varphi a \\ \text{s.t.} \quad & (\mathrm{Tr}(\mathbf{A}_2\tilde{\mathbf{W}}_1)+\varphi a)t=1, \\ & \mathrm{Tr}((\mathbf{A}_3+(1-t)\mathbf{A}_4)\tilde{\mathbf{W}}_1)\le \varphi b(t-1), \\ & \mathrm{Tr}(\mathbf{A}_5\tilde{\mathbf{W}}_1)\le \varphi c. \end{aligned} \tag{20}$$

After the transformation, for a given t, it is obvious that problem (20) is a standard semidefinite programming (SDP) problem, which can be solved efficiently by CVX [42]. Here, we assume that $\{\tilde{\mathbf{W}}_1^*(t),\varphi^*(t)\}$ and $\tilde{\mathbf{W}}^*(t)$ are the optimal solutions of problems (20) and (19), respectively, then we can easily obtain $\tilde{\mathbf{W}}^*(t)=\frac{\tilde{\mathbf{W}}_1^*(t)}{\varphi^*(t)}$. Thus, if $\tilde{\mathbf{W}}_1^*$ satisfies $\mathrm{Rank}(\tilde{\mathbf{W}}_1^*)=1$, then the optimal solution $\mathbf{W}^*$ of problem (17) can be derived through eigenvalue decomposition of $\tilde{\mathbf{W}}^*(t)$. Due to the fact that there are only three constraints with respect to $\tilde{\mathbf{W}}_1^*$ in problem (20), it is easy to check that $(\mathrm{Rank}(\tilde{\mathbf{W}}_1^*))^2\le 3$ [43], i.e., $\tilde{\mathbf{W}}_1^*$ is a rank-one matrix. Hence, by using the search algorithm on the interval $[1,t_{\max}]$ with respect to t, the optimal solution of problem (20) and (17) can be determined respectively.

Next, the tight upper bound $t_{\max}$ of problem (20) is given by Lemma 2.

Lemma 2: The interval upper bound $t_{\max}$ for updating the slack variable is given as

$$t_{\max}=1+\frac{c\mathrm{Tr}(\hat{\mathbf{H}}_{re}^T+\xi\mathbf{I}_N)}{b}. \tag{21}$$

Proof: Please refer to Appendix B. ■

B. Optimization of PS Ratio ρ

Proposition 2: For given $\mathbf{W}$ and $\sigma_{Z_d}^2$, the problem defined in (16) can be equivalently recast as follows by introducing a new variable $x=\frac{1}{\rho}$:

$$\begin{aligned}\max_{x} \quad & \frac{1+\frac{1}{k_1+k_2x}}{1+\frac{1}{k_3+k_4x}} \\ \text{s.t.} \quad & 1<k_5\le x. \end{aligned} \tag{22}$$

where $k_1=\frac{\mathrm{Tr}(\mathbf{B}_2\tilde{\mathbf{W}})}{\mathrm{Tr}(\mathbf{B}_1\tilde{\mathbf{W}})}$, $k_2=\frac{\mathrm{Tr}(\mathbf{B}_3\tilde{\mathbf{W}})+a}{\mathrm{Tr}(\mathbf{B}_1\tilde{\mathbf{W}})}$, $k_3=\frac{\mathrm{Tr}(\mathbf{B}_5\tilde{\mathbf{W}})}{\mathrm{Tr}(\mathbf{B}_4\tilde{\mathbf{W}})}$, $k_4=\frac{\mathrm{Tr}(\mathbf{B}_6\tilde{\mathbf{W}})+b}{\mathrm{Tr}(\mathbf{B}_4\tilde{\mathbf{W}})}$, $k_5=\frac{P_s\mathrm{Tr}((\mathbf{h}_{\mathbf{sr}}^*\mathbf{h}_{\mathbf{sr}}^{\mathbf{T}}\otimes\mathbf{I}_N)\tilde{\mathbf{W}})+\eta P_s\mathrm{Tr}(\mathbf{h}_{\mathbf{sr}}^*\mathbf{h}_{\mathbf{sr}}^{\mathbf{T}})+\sigma_r^2\mathrm{Tr}(\tilde{\mathbf{W}})+\eta\sigma_r^2}{\eta P_s\mathrm{Tr}(\mathbf{h}_{\mathbf{sr}}^*\mathbf{h}_{\mathbf{sr}}^{\mathbf{T}})-\sigma_{ID}^2\mathrm{Tr}(\tilde{\mathbf{W}})+\eta\sigma_r^2-P_{cr}}$, $\mathbf{B}_1=P_s(\mathbf{h}_{sr}^*\mathbf{h}_{sr}^T\otimes\mathbf{h}_{rd}^*\mathbf{h}_{rd}^T)$, $\mathbf{B}_2=\sigma_r^2(\mathbf{I}_N\otimes\mathbf{h}_{rd}^*\mathbf{h}_{rd}^T)$, $\mathbf{B}_3=\sigma_{ID}^2(\mathbf{I}_N\otimes\mathbf{h}_{rd}^*\mathbf{h}_{rd}^T)$, $\mathbf{B}_4=P_s(\mathbf{h}_{sr}^*\mathbf{h}_{sr}^T\otimes(\hat{\mathbf{H}}_{re}+\xi\mathbf{I}_N))$, $\mathbf{B}_5=\sigma_r^2(\mathbf{I}_N\otimes(\hat{\mathbf{H}}_{re}-\xi\mathbf{I}_N))$, $\mathbf{B}_6=\sigma_{ID}^2(\mathbf{I}_N\otimes(\hat{\mathbf{H}}_{re}-\xi\mathbf{I}_N))$.

Proof: By combining Proposition 1 and (16), Proposition 2 can be easily proved. ■

We employ the following theorem to efficiently tackle problem (22).

Theorem 1: Problem (22) can be solved based on the following two cases:

- If $f_1(k_5)<0$, the optimal ρ^* can be denoted as

$$\rho^*=\frac{1}{k_5}. \tag{23}$$

  where $f_1(k_5)=-(k_4-k_2)k_5^2-2(k_3-k_1)k_5+\frac{k_1k_4(1+k_1)-k_2k_3(1+k_3)}{k_2k_4}$.
- If $f_1(k_5)\ge 0$, the optimal ρ^* is given by

$$\rho^*=\frac{1}{k_7}. \tag{24}$$

  where $k_7=-\frac{k_3-k_1}{k_4-k_2}+\sqrt{(\frac{k_3-k_1}{k_4-k_2})^2+\frac{k_1k_4(1+k_1)-k_2k_3(1+k_3)}{k_2k_4(k_4-k_2)}}$.

Proof: Please refer to Appendix C. ■

C. Optimization of AN Transmit Power $\sigma_{Z_d}^2$

In this subsection, with fixed beamforming matrix $\mathbf{W}$ and PS ratio ρ, the problem defined in (16) can be reformulated into the following forms with $P_2=\frac{2(E_d-E_{\mathrm{SIC}})}{T}$:

$$\begin{aligned}\max_{\sigma_{Z_d}^2} \quad & \frac{1}{2}\left[\log_2(1+C_1)-\log_2\left(1+\frac{C_2}{C_3+\sigma_{Z_d}^2}\right)\right] \\ \text{s.t.} \quad & \sigma_{Z_d}^2\le P_2, \\ & \sigma_{Z_d}^2\le P_{AN,\max}. \end{aligned} \tag{25}$$

where $C_1=\frac{\mathrm{Tr}(\mathbf{A}_1\tilde{\mathbf{W}})}{\mathrm{Tr}(\mathbf{A}_2\tilde{\mathbf{W}})+a}$, $C_2=\frac{\rho\mathrm{Tr}(\mathbf{B}_4\tilde{\mathbf{W}})}{\hat{H}_{de}-\zeta}$ and $C_3=\frac{\rho\mathrm{Tr}(\mathbf{B}_5\tilde{\mathbf{W}})+\mathrm{Tr}(\mathbf{B}_6\tilde{\mathbf{W}})+\sigma_e^2}{\hat{H}_{de}-\zeta}$.

TABLE I
ITERATIVE SUBOPTIMAL ALGORITHM FOR PROBLEM (15)

1:	**Set** $L_{max} = 1000$, $L = 0$, $\gamma = 10^{-5}$, $R_0^L = 0$, $R_f^L = 100$;
2:	**Initialize** P_s, $\sigma_{Z_d}^2$, ρ and η;
3:	**While** $L < L_{max}$ and $R_f^L > \gamma$ do;
4:	Calculate $\mathbf{W}$ of (20) by using Lemma 2 and CVX [42];
5:	Calculate ρ of (22) based on (23) or (24);
6:	Calculate $\sigma_{Z_d}^2$ of (25) through (26);
7:	Determine $R_{SR}^L = R_d^L - R_e^L$;
8:	Update $R_f^L = \|R_0^L - R_{SR}^L\|$, $R_0^{L+1} = R_{SR}^L$ and $L = L + 1$;
9:	**Until**.

Theorem 2: The optimal AN transmit power ${\sigma_{Z_d}^2}^*$ of problem (25) can be derived as follows:

$$ {\sigma_{Z_d}^2}^* = \min\{P_2, P_{AN,\max}\}. \tag{26} $$

Proof: Suppose that f represents the objective function of (25), i.e., $f = \frac{1}{2}[\log_2(1 + C_1) - \log_2(1 + \frac{C_2}{C_3 + \sigma_{Z_d}^2})]$. First, it can be observed that the first-order derivative $\frac{df}{d\sigma_{Z_d}^2} = \frac{C_2}{2\ln 2[(C_3+\sigma_{Z_d}^2)^2 + C_2(C_3+\sigma_{Z_d}^2)]} > 0$, which shows that the value of f increases as $\sigma_{Z_d}^2$ increases. Then, there must exist a maximum value of f when two constraints of the problem defined in (25) hold with equalities. Therefore, the optimal AN transmit power ${\sigma_{Z_d}^2}^*$ can be derived as in (26). ■

D. The Iterative Algorithm

In this subsection, we combine the proposed solution approaches in subsections A, B and C to develop an iterative suboptimal algorithm. Then, the proposed algorithm that can solve problem (15) is summarized in Table I.

Lemma 3: The convergence of the proposed iterative algorithm for problem (15) is guaranteed.

Proof: Suppose that at the L_{th} iteration, since the optimal solutions of subproblems (20), (22) and (25) can be determined based on subsections A, B and C, respectively, it is easy to check that the value of the objective function in problem (15) must be monotonically nondecreasing. Because if the value of the objective function is decreased, we could keep $\mathbf{W}^{(L-1)*}$, $\rho^{(L-1)*}$ or $\sigma_{Z_d}^{2(L-1)*}$ unchanged. Furthermore, it can be observed that all constraints of the three subproblems are bounded, which makes the value of the objective function also bounded. Therefore, the proposed iterative algorithm must converge based on the monotonicity and boundedness [44]. ■

E. Computational Complexity Analysis

The computational complexity of the proposed algorithm in Table I is analyzed as follows. In each iteration of Table I, the main computational complexity of the proposed algorithm comes from the complexities introduced by solving the SDP problem in (20) [11]. In particular, the complexity of solving (20) is $O((mn^{3.5} + m^2n^{2.5} + m^3n^{0.5})log(1/\varepsilon))$, where m is the number of constraints, n is the dimension of the matrix $\tilde{\mathbf{W}}_1$, and ε is a given tolerance [11], [45]. For problem (20), $m = 3$ and $n = N^2$, which results in the complexity of problem (20) to be about $O(N^7log(1/\varepsilon))$. Thus, the total complexity of the proposed algorithm in Table I is about $O(L_1L_2\,N^7log(1/\varepsilon))$, where L_1 and L_2 denote the numbers of the line search steps and required iterations [38], respectively.

IV. SIMULATION RESULTS

In this section, we present numerical results to demonstrate the performance of the proposed robust beamforming design. Similar to the works in [11] and [21], we assume that the entries of $\mathbf{h}_{sr}$, $\mathbf{h}_{rd}$, $\mathbf{h}_{re}$ and h_{de} are independent identically distributed and generated according to $\mathcal{CN}(0, d_{ij}^{-\alpha})$, where d_{ij} is the distance between S and R, R and D, R and E, D and E, respectively, and $\alpha = 3$ is the path loss exponent [11], [21]. Moreover, the self-interference channel f_d obeys the distribution $\mathcal{CN}(0, 1)$[21]. It is assumed that the noise variances are set to be $\sigma_r^2 = \sigma_{ID}^2 = \sigma_d^2 = \sigma_e^2 = 0$ dBm. Furthermore, the working time and the energy conversion efficiency are assumed to be $T = 1$ s and $\eta = 0.8$, respectively. Moreover, unless otherwise specified, we set $u = v = 0.01$ as the channel estimate errors, the distance d_{SR}=d_{RD}=d_{RE}=d_{DE}=5 m, $\sigma_{SI}^2 = -10$ dBm as the residual self-interference noise power, $P_s = 40$ dBm and $P_{AN,\max} = 30$ dBm as the maximum transmit power of the source and destination, respectively. In addition, $P_{cr} = 10$ dBm as the relay's circuit power consumption [11], $E_d = 4$ J as the energy threshold of the destination and $E_{\mathrm{SIC}} = 1$ J as the consumption energy for SIC. All numerical results presented in the following are obtained by averaging over 1000 channel realizations.

In Fig. 2, we compare the system performance under perfect and imperfect CSI of the eavesdropper with different maximum available transmit power levels of the source and destination in subfigures (a) and (b), respectively. As shown in Fig. 2(a), the achievable secrecy rates at the destination and the eavesdropper increase with the source transmit power P_s under both perfect and imperfect CSI assumptions. The reason is that the harvested energy increases with P_s increasing, which results in the increase of the power of the signal sent by the relay. Moreover, as expected, the achieved secrecy rate performance with imperfect CSI of the eavesdropper is worse than that of the perfect CSI due to the fact that the channel estimation values suffer from estimation errors. In addition, with different $u = v$ under the imperfect CSI assumptions, the achieved secrecy rates decrease as the channel estimate error increases. The reason is that the estimation errors improve the received SINR at the eavesdropper.

With the considered different $P_{AN,\max}$ assumptions, similar comparison results are provided in Fig. 2(b). Nevertheless, different from Fig. 2(a), the achieved secrecy rates first increase and then saturate as $P_{AN,\max}$ increases. The reason is that there is an energy threshold constraint at the destination. In addition, with the imperfect CSI assumptions, when the $P_{AN,\max}$ is lower than the saturation point, increasing $P_{AN,\max}$ can rapidly improve the secrecy rate than for the perfect CSI case. The reason is that the eavesdropper's CSI uncertainties lead to more serious information leakage at the relay. Thus, increasing the AN power can rapidly degrade the received SINR at the eavesdropper.

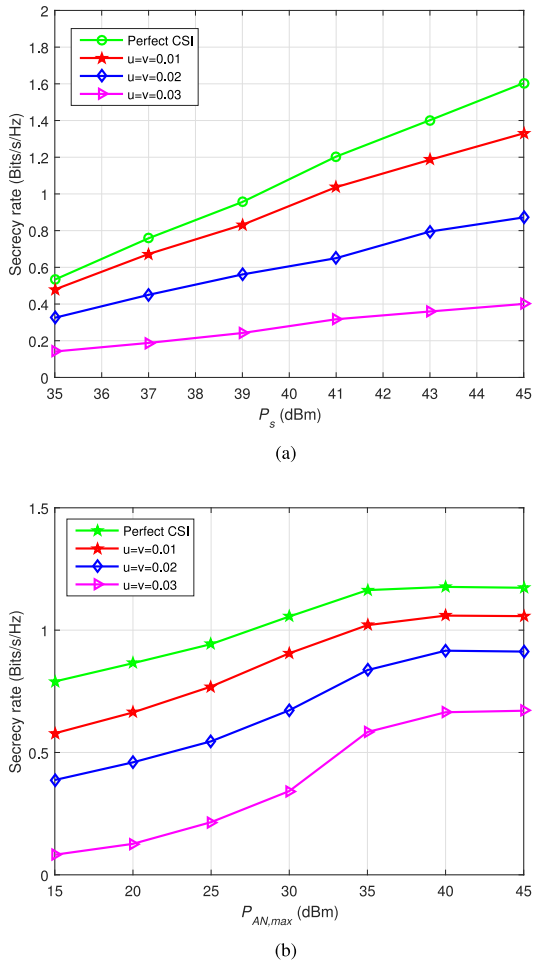

Fig. 2. Performance comparison under the perfect and imperfect CSI of the eavesdropper. (a) The secrecy rate under different P_s. (b) The secrecy rate under different $P_{AN,\max}$.

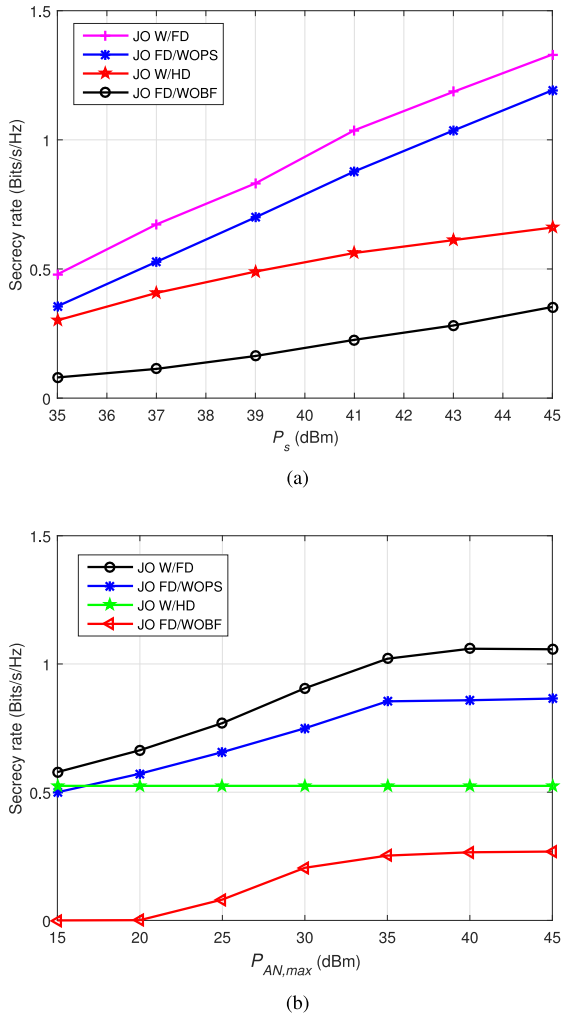

Fig. 3. Performance comparison under different algorithms. (a) The secrecy rate under different P_s. (b) The secrecy rate under different $P_{AN,\max}$.

Fig. 3 compares the system performance of our proposed robust joint design with FD destination (denoted as JO W/FD) with the other three benchmark schemes, i.e., 1) Robust joint design with half-duplex (HD) destination (JO W/HD); 2) Robust joint FD design without PS ratio optimize (JO FD/WOPS); 3) Robust joint FD design without beamforming optimize (JO FD/WOBF). As seen in Fig. 3(a), the achievable secrecy rates of all schemes increase as P_s increases, which has been explained in detail in the previous paragraph. In addition, as expected, the proposed algorithm achieves superior performance against the other three benchmark schemes. Specially, compared with the HD scheme, the proposed joint FD scheme significantly improves the system performance since it can transmit malicious AN signals to confuse the eavesdropper.

For different $P_{AN,\max}$ assumptions, similar observations are presented as in Fig. 3(b). From the simulation results, with the three FD schemes, the achieved secrecy rates increase first and then saturate with $P_{AN,\max}$ increasing, showing trends similar to Fig. 2(b). However, note that when $P_{AN,\max}$ increases, the achievable secrecy rate of the HD scheme remains constant due to the fact that the HD protocol is independent of the AN signal.

Next, Fig. 4 compares the system performance of all four schemes under the different EH efficiency η. As seen in Fig. 4, as expected, the achieved secrecy rates of all schemes increase as the EH efficiency η increases. The reason is that more energy can be harvested with η increasing and the relay has a large transmit power. Nevertheless, when η is large, the achieved secrecy rates of the four schemes increase slowly. It is because if the transmit power of the relay is large enough, a higher SINR is also achieved in the eavesdropper.

Fig. 5 presents the achievable secrecy rates with different PS ratios ρ and source transmit powers P_s. As shown in Fig. 5, the achievable secrecy rates increase with the PS ratio increasing before a saturation point for all the source transmit powers P_s assumptions. However, when the PS ratio ρ is larger than the saturation point, the achieved secrecy rates of all the curves decrease dramatically. This behavior is due to the reason that when ρ is large, the power of the EH circuit which is determined by $(1-\rho)$ would not satisfy all the energy consumption requirements at the relay. Moreover, as shown in Fig. 5, the proposed algorithm achieves a better secrecy rate performance as the source transmit power P_s increases. In addition, compared

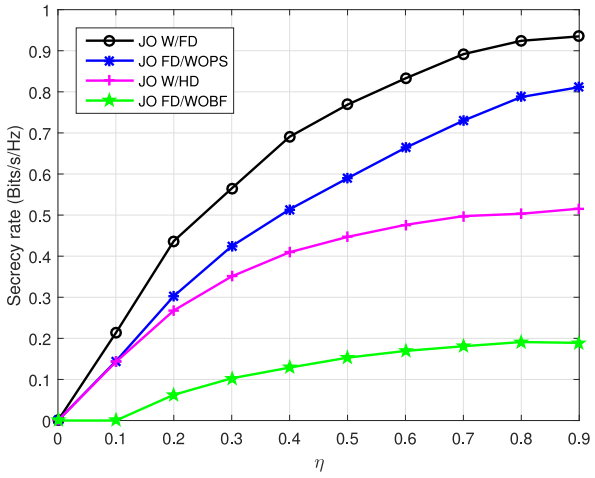

Fig. 4. Performance comparison under different algorithms versus the EH efficiency η.

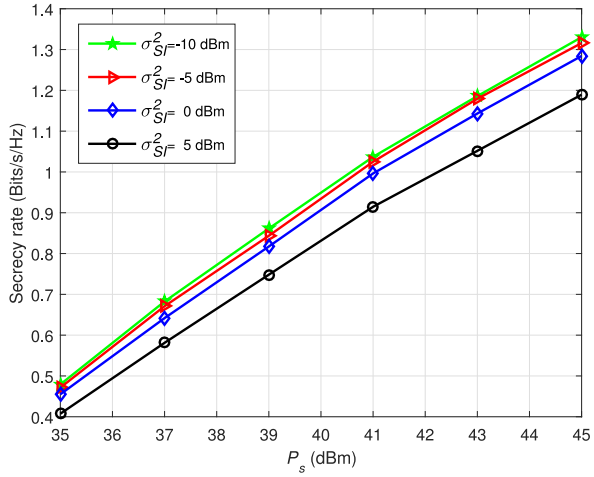

Fig. 6. The effect of the residual self-interference σ_{SI}^2 on the secrecy rate versus different source transmit power levels.

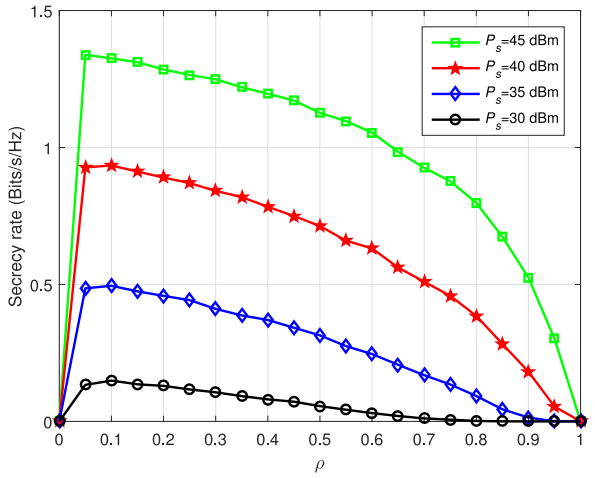

Fig. 5. The effect of the PS ratio ρ on the secrecy rate versus different source transmit power levels.

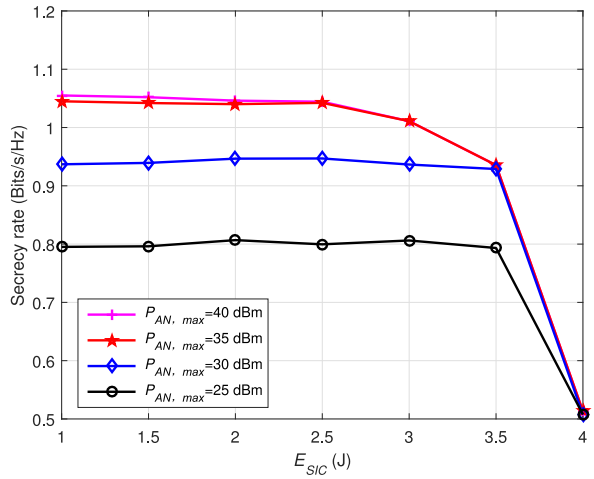

Fig. 7. The effect of the energy consumption of SIC on the secrecy rate versus different AN transmit power levels.

with the lower P_s, the larger P_s can firstly reach the saturation point of its achieved secrecy rate as the PS ratio ρ increasing. The reason is that the relay needs to harvest more energy to improve the system performance.

Next, we show the achieved the secrecy rates with different residual self-interference signal powers σ_{SI}^2 and source transmit powers P_s. As seen in Fig. 6, as expected, the achieved secrecy rates increase as P_s increases for all the σ_{SI}^2 assumptions. Furthermore, from the simulation results presented in Fig. 6, the achieved secrecy rates all steadily decrease as the residual self-interference power σ_{SI}^2 increases. The reason is that the residual self-interference term degrades the instantaneous SINR at the destination. However, since SIC needs to consume energy, the system performance will be affected by the energy consumption E_{SIC}, which will be introduced in the following simulations.

Fig. 7 illustrates the achieved secrecy rates with different energy consumption of SIC, E_{SIC}, and maximum available AN transmit power $P_{AN,\max}$. As shown in Fig. 7, when $P_{AN,\max}$ is small, the secrecy rates remain constant with the energy consumption of SIC, denoted by E_{SIC}, increasing before a saturation point for different $P_{AN,\max}$ assumptions. However, when E_{SIC} is larger than the saturation point, the achieved secrecy rates of all the curves decrease dramatically. The reason is that a lower transmit power of AN is allocated with E_{SIC} increasing, which results in a smaller AN jamming to the eavesdropper. In addition, as seen in Fig. 7, the achievable secrecy rates first increase and then stay the same as $P_{AN,\max}$ increases. The reason is that the destination does not exploit the maximum available power to transmit AN due to the fact that there is an energy threshold constraint E_d at the destination.

Next, Fig. 8 shows the achieved secrecy rates with different antennas N at the relay and transmit power P_s at the source. As shown in Fig. 8, it is observed that the achieved secrecy rates increase as P_s increases for all the number of relay antennas N assumptions, which has been explained in detail in the previous paragraph. In addition, as expected, the achieved secrecy rate

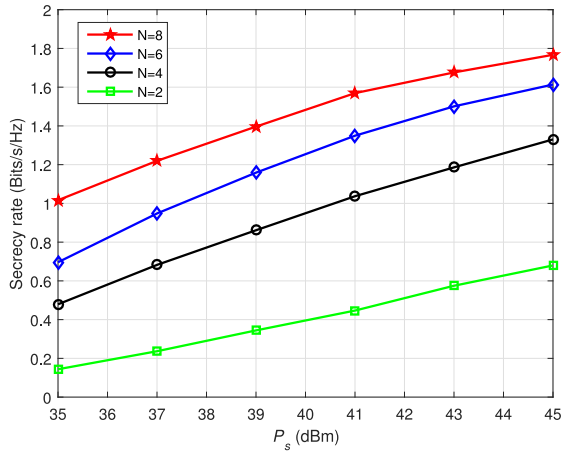

Fig. 8. The effect of the relay antennas on the secrecy rate versus different source transmit power levels.

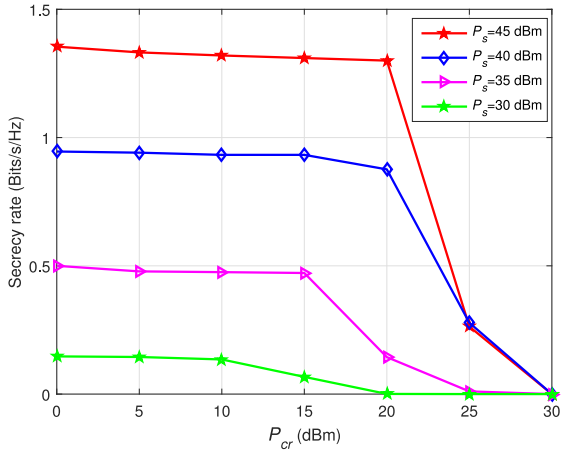

Fig. 9. The effect of circuit power consumption on the secrecy rate versus different source transmit power levels.

steadily increases as the number of relay antennas N increases. This demonstrates that the application of large or even massive antenna arrays at the relay can effectively enhance the system security performance in practical scenarios.

Finally, Fig. 9 illustrates the achievable secrecy rates with different circuit power consumption P_{cr} and source transmit powers P_s. From the simulation results presented in Fig. 9, when P_{cr} is small, the secrecy rates remain constant for all the considered values of P_s. However, when the circuit power consumption P_{cr} is larger than the saturation point, the achievable secrecy rates of all the curves decrease dramatically. The reason is that when P_{cr} is large enough, a lower transmit power is allocated for the information relaying within the entire harvested energy. Moreover, as seen in Fig. 9, the achievable secrecy rate finally reaches the saturation point when P_s is large. The reason is that the harvested energy increases as P_s increases, which enables the increase of the transmission power of the relay.

V. Conclusion

In this paper, we proposed a new paradigm to enhance the security performance in SWIPT-assisted relay communication system with imperfect CSI of the eavesdropper. In the proposed scheme, the beamforming design is performed at the relay to ensure that the secret message only forwards to the destination, and simultaneously the FD mode is applied at the destination to send artificial jamming to confuse the eavesdropper. We jointly designed the beamforming vector, PS ratio and AN power from the relay and FD destination to maximize the achievable secrecy rate under the EH requirement and transmit power constraints. Due to its non-convexity, we developed a three-step iterative algorithm to solve this optimization problem and found the suboptimal solution. Moreover, we analyzed the impact of the circuit power consumption and SIC on the maximum secure rate, and offered a better trade-off between system performance and energy consumption. Finally, numerical results were presented and practical impacts were discussed. In addition, these results demonstrated that for the case of imperfect CSI at the eavesdropper, adopting the proposed FD-aid jamming-based beamforming scheme can achieve a significant improvement in the secrecy rate compared to those benchmark relaying schemes.

Appendix A
Proof of Proposition 1

Let us suppose that $\tilde{\mathbf{W}} \triangleq \mathbf{w}\mathbf{w}^H$ and $\mathbf{w} = \mathrm{vec}(\mathbf{W})$, then using $\mathrm{Tr}(\mathbf{ABCD}) = (\mathrm{vec}(\mathbf{D}^T)^T)(\mathbf{C}^T \otimes \mathbf{A})\mathrm{vec}(\mathbf{B})$, problem (16) becomes to the following problem:

$$\begin{aligned}\max_{\tilde{\mathbf{W}}\succeq 0} \quad & \frac{1}{2}\left[\log_2\left(1+\frac{\mathrm{Tr}(\mathbf{A}_1\tilde{\mathbf{W}})}{\mathrm{Tr}(\mathbf{A}_2\tilde{\mathbf{W}})+a}\right)\right. \\ & \left. -\log_2\left(1+\frac{\mathrm{Tr}(\mathbf{A}_3^0\tilde{\mathbf{W}})}{\mathrm{Tr}(\mathbf{A}_4^0\tilde{\mathbf{W}})+b^0}\right)\right] \\ \text{s.t.} \quad & \mathrm{Tr}(\mathbf{A}_5\tilde{\mathbf{W}}) \le c, \\ & \mathrm{Rank}(\tilde{\mathbf{W}}) = 1, \end{aligned} \tag{27}$$

where $\mathbf{A}_1 = \rho P_s(\mathbf{h}_{sr}^*\mathbf{h}_{sr}^T \otimes \mathbf{h}_{rd}^*\mathbf{h}_{rd}^T)$, $\mathbf{A}_2 = (\rho\sigma_r^2+\sigma_{ID}^2)(\mathbf{I}_N \otimes \mathbf{h}_{rd}^*\mathbf{h}_{rd}^T)$, $\mathbf{A}_3^0 = \rho P_s(\mathbf{h}_{sr}^*\mathbf{h}_{sr}^T \otimes \mathbf{h}_{re}^*\mathbf{h}_{re}^T)$, $\mathbf{A}_4^0 = (\rho\sigma_r^2+\sigma_{ID}^2)(\mathbf{I}_N \otimes \mathbf{h}_{re}^*\mathbf{h}_{re}^T)$, $\mathbf{A}_5 = \rho P_s(\mathbf{h}_{sr}^*\mathbf{h}_{sr}^T \otimes \mathbf{I}_N) + (\rho\sigma_r^2+\sigma_{ID}^2)(\mathbf{I}_N \otimes \mathbf{I}_N)$, $a = \sigma_{SI}^2|f_d|^2+\sigma_d^2$, $b^0 = \sigma_{Zd}^2|h_{de}|^2+\sigma_e^2$, $c = \eta(1-\rho)(P_s||\mathbf{h}_{sr}||_2^2+\sigma_r^2) - P_{cr}$.

Based on (1) and (2), we have

$$\begin{aligned}&\mathbf{h}_{re}^*\mathbf{h}_{re}^T \\ &= (\hat{\mathbf{h}}_{re}+\Delta\mathbf{h}_{re})^*(\hat{\mathbf{h}}_{re}+\Delta\mathbf{h}_{re})^T, \\ &= \hat{\mathbf{h}}_{re}^*\hat{\mathbf{h}}_{re}^T + \hat{\mathbf{h}}_{re}^*\Delta\mathbf{h}_{re}^T + \Delta\mathbf{h}_{re}^*\hat{\mathbf{h}}_{re}^T + \Delta\mathbf{h}_{re}^*\Delta\mathbf{h}_{re}^T, \\ &= \hat{\mathbf{H}}_{re} + \Delta\mathbf{H}_{re}, \end{aligned} \tag{28}$$

and

$$\begin{aligned}&h_{de}^*h_{de}^T \\ &= (\hat{h}_{de}+\Delta h_{de})^*(\hat{h}_{de}+\Delta h_{de})^T, \\ &= \hat{h}_{de}^*\hat{h}_{de}^T + \hat{h}_{de}^*\Delta h_{de}^T + \Delta\mathbf{h}_{de}^*\hat{h}_{de}^T + \Delta h_{de}^*\Delta h_{de}^T, \\ &= \hat{H}_{de} + \Delta H_{de}, \end{aligned} \tag{29}$$

where $\hat{\mathbf{H}}_{re} = \hat{\mathbf{h}}_{re}^{*}\hat{\mathbf{h}}_{re}^{T}$ and $\hat{H}_{de} = \hat{h}_{de}^{*}\hat{h}_{de}^{T}$ represent the covariance matrix of the channel estimate values, $\Delta\mathbf{H}_{re} = \hat{\mathbf{h}}_{re}^{*}\Delta\mathbf{h}_{re}^{T} + \Delta\mathbf{h}_{re}^{*}\hat{\mathbf{h}}_{re}^{T} + \Delta\mathbf{h}_{re}^{*}\Delta\mathbf{h}_{re}^{T}$ and $\Delta H_{de} = \hat{h}_{de}^{*}\Delta h_{de}^{T} + \Delta h_{de}^{*}\hat{h}_{de}^{T} + \Delta h_{de}^{*}\Delta h_{de}^{T}$ denote the uncertainties of $\hat{\mathbf{H}}_{re}$ and $\hat{H}_{de}$, respectively. Thus, by applying the triangle and the Cauchy-Schwartz inequalities, we have

$$\begin{aligned}
&||\Delta\mathbf{H}_{re}||_2 \\
&= ||\hat{\mathbf{h}}_{re}^{*}\Delta\mathbf{h}_{re}^{T} + \Delta\mathbf{h}_{re}^{*}\hat{\mathbf{h}}_{re}^{T} + \Delta\mathbf{h}_{re}^{*}\Delta\mathbf{h}_{re}^{T}||_2, \\
&\le ||\hat{\mathbf{h}}_{re}^{*}\Delta\mathbf{h}_{re}^{T}||_2 + ||\Delta\mathbf{h}_{re}^{*}\hat{\mathbf{h}}_{re}^{T}||_2 + ||\Delta\mathbf{h}_{re}^{*}\Delta\mathbf{h}_{re}^{T}||_2, \\
&\le ||\hat{\mathbf{h}}_{re}^{*}||_2||\Delta\mathbf{h}_{re}^{T}||_2 + ||\Delta\mathbf{h}_{re}^{*}||_2||\hat{\mathbf{h}}_{re}^{T}||_2 + ||\Delta\mathbf{h}_{re}^{*}||_2||\Delta\mathbf{h}_{re}^{T}||_2, \\
&= \mu^2 + 2\mu||\hat{\mathbf{h}}_{re}||_2, \\
&= \xi,
\end{aligned} \tag{30}$$

and

$$\begin{aligned}
&||\Delta H_{de}||_2 \\
&= ||\hat{h}_{de}^{*}\Delta h_{de}^{T} + \Delta h_{de}^{*}\hat{h}_{de}^{T} + \Delta h_{de}^{*}\Delta h_{de}^{T}||_2, \\
&\le ||\hat{h}_{de}^{*}\Delta h_{de}^{T}||_2 + ||\Delta h_{de}^{*}\hat{h}_{de}^{T}||_2 + ||\Delta h_{de}^{*}\Delta h_{de}^{T}||_2, \\
&\le ||\hat{h}_{de}^{*}||_2||\Delta h_{de}^{T}||_2 + ||\Delta h_{de}^{*}||_2||\hat{h}_{de}^{T}||_2 + ||\Delta h_{de}^{*}||_2||\Delta h_{de}^{T}||_2, \\
&= \nu^2 + 2\nu||\hat{h}_{de}||_2, \\
&= \zeta.
\end{aligned} \tag{31}$$

where $\xi > 0$ and $\zeta > 0$. It is observed that $\Delta\mathbf{H}_{re}$ and ΔH_{de} are norm-bounded. Therefore, based on $-\xi\mathbf{I}_N \le \Delta\mathbf{H}_{re} \le \xi\mathbf{I}_N$ and $-\zeta \le \Delta H_{de} \le \zeta$, the problem defined in (27) can be reformulated as follows:

$$\begin{aligned}
\max_{\tilde{\mathbf{W}}\succeq 0} \quad & \frac{1}{2}\left[\log_2\left(1 + \frac{\mathrm{Tr}(\mathbf{A}_1\tilde{\mathbf{W}})}{\mathrm{Tr}(\mathbf{A}_2\tilde{\mathbf{W}}) + a}\right)\right. \\
& \left. - \log_2\left(1 + \frac{\mathrm{Tr}(\mathbf{A}_3\tilde{\mathbf{W}})}{\mathrm{Tr}(\mathbf{A}_4\tilde{\mathbf{W}}) + b}\right)\right] \\
\text{s.t.} \quad & \mathrm{Tr}(\mathbf{A}_5\tilde{\mathbf{W}}) \le c, \\
& \mathrm{Rank}(\tilde{\mathbf{W}}) = 1,
\end{aligned} \tag{32}$$

where $\mathbf{A}_3 = \rho P_s(\mathbf{h}_{sr}^{*}\mathbf{h}_{sr}^{T} \otimes (\hat{\mathbf{H}}_{re} + \xi\mathbf{I}_N))$, $\mathbf{A}_4 = (\rho\sigma_r^2 + \sigma_{ID}^2)(\hat{\mathbf{H}}_{re} - \xi\mathbf{I}_N)$, $b = \sigma_{Zd}^2(\hat{H}_{de} - \zeta) + \sigma_e^2$. This completes the proof of Proposition 1. ■

APPENDIX B
PROOF OF LEMMA 2

Based on the secrecy rate defined in problem (15), the SINR_e of the eavesdropper must has a maximum value. Therefore, the slack variable t satisfy the following inequality

$$\begin{aligned}
t &= 1 + \frac{\mathrm{Tr}(\mathbf{A}_3^0\tilde{\mathbf{W}})}{\mathrm{Tr}(\mathbf{A}_4^0\tilde{\mathbf{W}}) + b^0}, \\
&\le 1 + \frac{\mathrm{Tr}(\mathbf{A}_3^0\tilde{\mathbf{W}})}{b^0}.
\end{aligned} \tag{33}$$

By applying some further transformations and the Cauchy-Schwartz inequality, we can derive

$$\begin{aligned}
\mathrm{Tr}(\mathbf{A}_3^0\tilde{\mathbf{W}}) &= \rho P_s|\mathbf{h}_{re}^{T}\mathbf{W}\mathbf{h}_{sr}|^2, \\
&\le \rho P_s||\mathbf{h}_{re}^{T}||^2||\mathbf{W}\mathbf{h}_{sr}||^2, \\
&= \rho P_s||\mathbf{h}_{re}^{T}||^2\mathrm{Tr}((\mathbf{h}_{sr}^{*}\mathbf{h}_{sr}^{T} \otimes \mathbf{I}_N)\tilde{\mathbf{W}}).
\end{aligned} \tag{34}$$

Based on A_5 defined in (27), we have

$$\rho P_s\mathrm{Tr}((\mathbf{h}_{sr}^{*}\mathbf{h}_{sr}^{T} \otimes \mathbf{I}_N)\tilde{\mathbf{W}}) \le \mathrm{Tr}(\mathbf{A}_5\tilde{\mathbf{W}}) \le c. \tag{35}$$

Then, by substituting (35) into (34), the inequality (33) is equivalent to the following form:

$$t \le 1 + \frac{c||\mathbf{h}_{re}^{T}||^2}{b^0}. \tag{36}$$

Due to the impact of channel estimate errors, a tightly upper bound of the slack variable t is given as follows

$$t_{\max} = 1 + \frac{c\mathrm{Tr}(\hat{\mathbf{H}}_{re}^{T} + \xi\mathbf{I}_N)}{b}. \tag{37}$$

This completes the proof of Lemma 2. ■

APPENDIX C
PROOF OF THEOREM 1

Based on (22), due to the fact that $k_2 > 0$ and $k_4 > 0$, we have $k_2k_4 > 0$. Therefore, the problem defined in (22) is equivalent to the following form:

$$\begin{aligned}
\max_{x} \quad & \frac{(k_4 - k_2)x + k_3 - k_1}{x^2 + \frac{k_1k_4 + k_2k_3 + k_2}{k_2k_4}x + \frac{k_1k_3 + k_1}{k_2k_4}} \\
\text{s.t.} \quad & 1 < k_5 \le x.
\end{aligned} \tag{38}$$

By defining f as the objective function of the problem defined in (38), we derive the first-order derivative of $f(\cdot)$ with respect to x as follows:

$$\begin{aligned}
&\frac{df}{dx} \\
&= \frac{-(k_4 - k_2)x^2 - 2(k_3 - k_1)x + \frac{k_1k_4(1+k_1) - k_2k_3(1+k_3)}{k_2k_4}}{(x^2 + \frac{k_1k_4 + k_2k_3 + k_2}{k_2k_4}x + \frac{k_1k_3 + k_1}{k_2k_4})^2}.
\end{aligned} \tag{39}$$

Suppose $f_1(\cdot)$ and $f_2(\cdot)$ represent the numerator and denominator in the fraction in (39). According to (22) and due to the fact that $k_1 > 0$, $k_3 > 0$ and $x > 1$, we have $f_2 = (x^2 + \frac{k_1k_4 + k_2k_3 + k_2}{k_2k_4}x + \frac{k_1k_3 + k_1}{k_2k_4})^2 > 0$. In addition, based on (9) and (12), due to the fact of $\sigma_{Zd}^2 >> \sigma_{SI}^2$, it is easy to verify that $k_4 > k_2$, which leads to a conclusion that the univariate quadric function $f_1 = -(k_4 - k_2)x^2 - 2(k_3 - k_1)x + \frac{k_1k_4(1+k_1) - k_2k_3(1+k_3)}{k_2k_4}$ achieves its maximum values when the variable x satisfy its symmetrical axis, i.e., $x = k_6 = \frac{k_1 - k_3}{k_4 - k_2}$. Thus, the function f_1 is strictly monotonically decreased with the respect to $x \in [k_6, +\infty)$.

When $k_1 \le k_3$, according to (38) and due to the fact of the symmetrical axis $k_6 = \frac{k_1 - k_3}{k_4 - k_2} < 0$, we have $k_5 > k_6$. Thus, if $f_1(k_5) < 0$, it is observed that $f_1(x) < 0$ with $x \in [k_5, +\infty)$.

As a result, based on $f_2(x) > 0$, we have $\frac{df}{dx} < 0$, which shows that the value of f decreases as x increases. Therefore, there must exist a maximum value of $f(x^*)$ when the constraint of the problem defined in (38) is satisfied with equality. The optimal x^* to problem (38) is given as follows

$$x^* = k_5. \tag{40}$$

If $f_1(k_5) \geq 0$, there must exist two activation solutions of the variable x when $f_1(x) = 0$, in which a larger solution denoted by k_7, can be derived as $k_7 = -\frac{k_3-k_1}{k_4-k_2} + \sqrt{(\frac{k_3-k_1}{k_4-k_2})^2 + \frac{k_1k_4(1+k_1)-k_2k_3(1+k_3)}{k_2k_4(k_4-k_2)}}$. Thus, we have $k_5 < k_7$ due to the fact f_1 is strictly monotonically decreasing with respect to $x \in [k_5, +\infty)$. When $x \in [k_5, k_7]$, we have $f_1(x) \geq 0$ and $\frac{df}{dx} \geq 0$, which shows that the value of f increases as x increases. When $x \in (k_7, +\infty)$, we can derive $f_1(x) < 0$ and $\frac{df}{dx} < 0$. Therefore, f is strictly monotonically decreased with respect to $x \in (k_7, +\infty)$. Hence, combining the above two parts, the objective function value first increases and then decreases with respect to $x \in [k_5, +\infty)$. The optimal x^* to problem (38) can be obtained as follows

$$x^* = k_7. \tag{41}$$

When $k_1 > k_3$, based on (38) and (39), we have $k_6 = \frac{k_1-k_3}{k_4-k_2} > 0$ and $\frac{k_1k_4(1+k_1)-k_2k_3(1+k_3)}{k_2k_4} > 0$. Thus, there must also exist two activation solutions when $f_1(x) = 0$. If $f_1(k_5) < 0$, it is easy to verify that $k_5 > k_7 > k_6$, and then $f_1(x) < 0$ as well as $\frac{df}{dx} < 0$. Hence, f is strictly monotonically decreasing with the respect to $x \in [k_5, +\infty)$. As a result, when the constraint of the problem defined in (38) is satisfied with equality, the optimal x^* is given as follows

$$x^* = k_5. \tag{42}$$

If $f_1(k_5) \geq 0$, we can derive $k_5 < k_7$. Thus, with $x \in [k_5, k_7]$, we have $f_1(x) \geq 0$ and $\frac{df}{dx} \geq 0$, which shows that f is strictly monotonically increasing with the respect to $x \in [k_5, k_7]$. Moreover, when $x \in (k_7, +\infty)$, it is easy to verify that $f_1(x) < 0$ and $\frac{df}{dx} < 0$. Hence, the objective function value decreases as the x increases. In conclusion, with $x \in [k_5, +\infty)$, the objective function value also first increases and then decreases. Then, the optimal solution x^* of (38) can be derived as

$$x^* = k_7. \tag{43}$$

Hence, combining the above two parts, based on $x = \frac{1}{\rho}$, the optimal solution to problem (22) can be expressed as (23) and (24). This completes the proof of Theorem 1. ■

REFERENCES

[1] W. Trappe, "The challenges facing physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 16–20, Jun. 2015.

[2] Y. Liu, H. H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surv. Tut.*, vol. 19, no. 1, pp. 347–376, Aug. 2016.

[3] Y. S. Shiu, S. Y. Chang, H. C. Wu, S. C. H. Huang, and H. H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 1, pp. 66–74, Apr. 2011.

[4] N. Yang, L. Wang, G. Geraci, M. Elkashlan, and J. Yuan, "Safeguarding 5 G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[5] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A Survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[6] X. Chen, D. W. K. Ng, and H. H. Chen, "Secrecy wireless information and power transfer: Challenges and opportunities," *IEEE Wireless Commun.*, vol. 23, no. 2, pp. 54–61, May 2016.

[7] K. Cumanan, Z. G. Ding, B. Sharif, Y. G. Tian, and K. K. Leung, "Secrecy rate optimizations for a MIMO secrecy channel with a multiple-antenna eavesdropper," *IEEE Trans. Veh. Technol.*, vol. 63, no. 4, pp. 1678–1690, May 2014.

[8] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Le Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 1833–1847, May 2015.

[9] Z. Chu, H. Xing, M. Johnston, and S. Le Goff, "Secrecy rate optimizations for a MISO secrecy channel with multiple multiantenna eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 283–297, Jan. 2016.

[10] K. Koufos and C. P. Dettmann, "Boundaries as an enhancement technique for physical layer security," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 1, pp. 61–74, Jan. 2019.

[11] Q. Li and L. Yang. "Beamforming for cooperative secure transmission in cognitive two-way relay networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, no. 1, pp. 130–143, May 2019.

[12] W. Wang, R. Wang, H. Mehrpouyan, N. Zhao, and G. Zhang, "Beamforming for simultaneous wireless information and power transfer in two-way relay channels," *IEEE Access*, vol. 5, pp. 9235–9250, 2017.

[13] W. Wang, R. Wang, W. Duan, R. Feng, and G. Zhang, "Optimal transceiver designs for wireless-powered full-duplex two-way relay networks with SWIPT," *IEEE Access*, vol. 5, pp. 22329–22343, 2017.

[14] Q. Li and L. Yang, "Robust optimization for energy efficiency in MIMO two-way relay networks with SWIPT," *IEEE Syst. J.*, vol. 14, no. 1, to be published, doi:10.1109/JSYST.2019.2904721.

[15] L. Liu, R. Zhang and K. C. Chua, "Secrecy wireless information and power transfer with MISO beamforming," *IEEE Trans. Signal Process.*, vol. 62, no. 7, pp. 1850–1863, Apr. 2014.

[16] M. Liu and Y. Liu, "Power allocation for secure SWIPT systems with wireless-powered cooperative jamming," *IEEE Commun. Lett.*, vol. 21, no. 6, pp. 1353–1356, Jun. 2017.

[17] Y. Tang, W. Yang, Y. Cai, W. Yang and Y. Huang, "Security of full-duplex jamming SWIPT system with multiple non-colluding eavesdroppers," in *Proc. IEEE Int. Conf. Electron. Inf. Emergency Commun.*, Macau, China, Jul. 2017, pp. 66–69.

[18] Q. Li, Q. Zhang, and J. Qin, "Secure relay beamforming for simultaneous wireless information and power transfer in nonregenerative relay networks," *IEEE Trans. Veh. Technol.*, vol. 63, no. 5, pp. 2462–2467, Jun. 2014.

[19] H. Xing, K. K. Wong, and A. Nallanathan, "Secure wireless energy harvesting-enabled AF-relaying SWIPT networks," in *Proc. IEEE Int. Conf. Commun.*, London, U.K., Jun. 2015, pp. 2307–2312.

[20] Z. Chu, H. X. Nguyen, and G. Caire, "Game theory-based resource allocation for secure WPCN multiantenna multicasting systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 4, pp. 926–939, Apr. 2018.

[21] J. Qiao, H. Zhang, and X. Zhou, "Joint beamforming and time switching design for secrecy rate maximization in wireless-powered FD relay systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 1, pp. 567–579, Jan. 2018.

[22] W. Mou, Y. Cai, W. Yang, W. Yang, X. Xu, and J. Hu, "Exploiting full duplex techniques for secure communication in SWIPT system," in *Proc. Int. Conf. Wireless Commun. Signal Process.*, Nanjing, China, Oct. 2015, pp. 1–6.

[23] S. Wang and B. Wang, "Robust secure transmit design in MIMO channels with simultaneous wireless information and power transfer," *IEEE Signal Process. Lett.*, vol. 22, no. 11, pp. 2147-2151, Nov. 2015.

[24] Z. Chu, Z. Zhu and J. Hussein, "Robust optimization for AN-aided transmission and power splitting for secure MISO SWIPT system," *IEEE Commun. Lett.*, vol. 20, no. 8, pp. 1571–1574, Aug. 2016.

[25] F. Zhou, Z. Li, J. Cheng, Q. Cheng, and J. Si, "Robust AN-aided beamforming and power splitting design for secure MISO cognitive radio with SWIPT," *IEEE Trans. Wireless Commun.*, vol. 16, no. 4, pp. 2450–2464, Apr. 2017.

[26] Z. Chu *et al.*, "Resource allocation for secure wireless powered integrated multicast and unicast services with full duplex self-energy recycling," *IEEE Trans. Wireless Commun.*, vol. 18, no. 1, pp. 620–636, Jan. 2019.

[27] X. Tang, Y. Cai, Y. Deng, Y. Huang, W. Yang, and W. Yang, "Energy-constrained SWIPT networks: Enhancing physical layer security with FD self-jamming," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 1, pp. 212–222, Jan. 2019.
[28] Y. Feng, Z. Yang, W. P. Zhu, Q. Li, and B. Lv, "Robust cooperative secure beamforming for simultaneous wireless information and power transfer in amplify-and-forward relay networks," *IEEE Trans. Veh. Tech.*, vol. 66, no. 3, pp. 2354–2366, Mar. 2017.
[29] Q. Li and J. Qin, "Joint source and relay secure beamforming for non-regenerative MIMO relay systems with wireless information and power transfer," *IEEE Trans. Veh. Tech.*, vol. 66, no. 7, pp. 5853–5865, May 2017.
[30] H. Niu, B. Zhang, D. Guo, and Y. Huang, "Joint robust design for secure AF relay networks with SWIPT," *IEEE Access*, vol. 5, pp. 9369–9377, 2017.
[31] D. Bharadia, E. McMilin, and S. Katti, "Full duplex radios," in *Proc. ACM SIGCOMM.*, 2013, pp. 375–386.
[32] X. Wang, K. Wang, and X. Zhang, "Secure relay beamforming with imperfect channel side information," *IEEE Tans. Veh. Tech.*, vol. 62, no. 5, pp. 2140–2155, Jun. 2013.
[33] P. Janis *et al.*, "Device-to-device communication underlaying cellular communications systems," *Int. J. Commun., Netw. Syst. Sci.*, vol. 2, no. 3, pp. 169–178, Jun. 2009.
[34] C. R. Valenta and G. D. Durgin, "Harvesting wireless power: Survey of energy-harvester conversion efficiency in far-field, wireless power transfer systems," *IEEE Microw. Mag.*, vol. 15, no. 4, pp. 108–120, Jun. 2014.
[35] E. Boshkovska, D. W. K. Ng, N. Zlatanov, and R. Schober, "Practical non-linear energy harvesting model and resource allocation for SWIPT systems," *IEEE Commun. Lett.*, vol. 19, no. 12, pp. 2082–2085, Dec. 2015.
[36] Y. Zeng, B. Clerckx, and R. Zhang, "Communications and signals design for wireless power transmission," *IEEE Trans. Commun.*, vol. 65, no. 5, pp. 2264–2290, May 2017.
[37] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
[38] C. Miao, G. C. Zhang, Q. Q. Wu, and D. W. K. Ng, "Robust trajectory and transmit power design for secure UAV communications," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 9042–9046, Oct. 2018.
[39] G. Zhang, Q. Wu, M. Cui, and R. Zhang, "Securing UAV communications via joint trajectory and power control," *IEEE Trans. Wireless Commun.*, vol. 18, no. 2, pp. 1376–1389, Feb. 2019.
[40] A. Charnes and W. W. Cooper, "Programming with linear fractional functions," *Naval Res. Logist. Quart.*, vol. 9, pp. 181–186, 1962.
[41] R. Wang, M. Tao, and Y. Liu, "Optimal linear transceiver designs for cognitive two-way relay networks," *IEEE Trans. Signal Process.*, vol. 61, no. 4, pp. 992–1005, Feb. 2013.
[42] M. Grant and S. Boyd, *CVX: MATLAB Software for Disciplined Convex Programming*, Jul. 2010 [Online]. Available: http://cvxr.com/cvx
[43] 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, Feb. 2010.
[44] J. Bibby, "Axiomatisations of the average and a further generalisation of monotonic sequences," *Glasgow Math. J.*, vol. 15, pp. 63-65, 1974.
[45] A. Ben-Tal and A. Nemirovski, *Lectures on Modern Convex Optimization: Analysis, Algorithms, and Engineering Applications (MPS-SIAM Series on Optimization)*. Philadelphia, PA, USA: SIAM, 2001.

Xinrui Li received the B.S. degree in electronic and information engineering from Nantong University, Nantong, China, in 2018, where he is currently working toward the M.S. degree in information and communication engineering. His major research interests include wireless information and power transfer, physical layer security, and unmanned aerial vehicle communications.

Wei Wang (M'19) received the B.S. degree in electronic and information engineering from China West Normal University, Nanchong, China, in 2005, the M.S. degree in signal and information processing from the Chengdu University of Technology, Chengdu, China, in 2008, and the Ph. D. degree in communication and information system from Shanghai University, Shanghai, China, in 2011. From August 2011 to July 2014, he was with the School of Information Science and Technology, Nantong University as a Lecturer, where he is currently an Associate Professor. From February 2016 to August 2016, he was a Visiting Scholar with the Department of Electrical and Computer Engineering, Boise State University, ID, USA. From February 2019 to August 2019, he was an Academic Visitor with the Department of Electronic Engineering, University of York, York, U.K. His current research interests include wireless information and power transfer, physical layer security, unmanned aerial vehicle communications, and fog/edge computing.

Miao Zhang (S'18) received the B.Sc. degree in optical information science and technology from Guizhou University, Guiyang, China, the M.Sc. degree in communications and signal processing from the University of Newcastle upon Tyne, Newcastle upon Tyne, U.K., and the Ph.D. degree in electronic engineering from the University of York, in 2011, 2015, and 2019, respectively. He is currently working toward the Ph.D. degree with the Department of Electronic Engineering, University of York, York, U.K. His research interests are convex optimization techniques, wireless energy harvesting networks, physical layer security, and machine learning for wireless communications.

Fuhui Zhou (M'17) received the Ph.D. degree from Xidian University, Xian, China, in 2016. He has worked as a Senior Research Fellow with Utah State University. He is currently a Full Professor with the College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics. His research interests focus on cognitive radio, edge computing, machine learning, NOMA, physical layer security, and resource allocation. He has published more than 90 papers, including IEEE JOURNAL OF SELECTED AREAS IN COMMUNICATIONS, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE WIRELESS COMMUNICATIONS, IEEE NETWORK, IEEE GLOBECOM, etc. He has served as Technical Program Committee (TPC) Member for many international conferences, such as IEEE GLOBECOM, IEEE ICC, etc. He serves as an Editor of IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE SYSTEMS JOURNAL, IEEE ACCESS, and *Physical Communications*. He also serves as Co-Chair of IEEE ICC 2019 and IEEE Globecom 2019 workshop on Advanced Mobile Edge /Fog Computing for 5G Mobile Networks and Beyond.

Naofal Al-Dhahir (S'89–M'90–SM'98–F'08) received the Ph.D. degree in electrical engineering from Stanford University. From 1994 to 2003, he was a Principal Member of the Technical Staff with the GE Research and AT&T Shannon Laboratory. He is currently an Erik Jonsson Distinguished Professor and the ECE Associate Head of the University of Texas at Dallas.

He is Co-Inventor of 42 issued US patents, co-author of over 415 papers and co-recipient of four IEEE best paper awards. He is the Editor-in-Chief of the IEEE TRANSACTIONS ON COMMUNICATIONS and an IEEE Fellow.