

Received September 4, 2020, accepted September 14, 2020, date of publication September 24, 2020, date of current version October 2, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3026359

Relay Cooperative Beamforming Algorithm Based on Probabilistic Constraint in SWIPT Secrecy Networks

ZHENTAO HU¹, DONGDONG XIE¹, MINGQI JIN², LIN ZHOU¹, AND JIFANG LI³

¹School of Computer and Information Engineering, Henan University, Kaifeng 475004, China

²Department of Information and Computing Science, Northeastern University, Shenyang 110000, China

³School of Electric Power, North China University of Water Resources and Electric Power, Zhengzhou 450000, China

Corresponding author: Dongdong Xie (aaa1503788@163.com)

This work was supported in part by the National Science Foundation Council of China under Grant 61771006, Grant 61976080, and Grant U1804149; in part by the Key Research Projects of University in Henan Province of China under Grant 19A413006 and Grant 20B510001; in part by the First-Class Discipline Training Foundation of Henan University under Grant 2018YLT04; and in part by the Programs for Science and Technology Development of Henan Province under Grant 192102210254.

ABSTRACT We explore physical layer security of simultaneous wireless information and power transfer (SWIPT) relay network in this paper. Modeling channel error between relay and eavesdroppers (Eves) as random channel state information (CSI) error, we present an algorithm to optimize secret rate of SWIPT in the constraints of relay forward power, receiver signal-to-interference-plus-noise ratio (SINR) and Eves SINR. A slack variable is introduced to decompose original non-convex problem into upper and lower sub-problems, meanwhile, Bernstein-type inequality is used to convert probability constraint of lower sub-problems to linear matrix inequality constraints. Simulation experiments show that the proposed algorithm obtains higher secret rate than that of zero-forcing algorithm and worst-case algorithm.

INDEX TERMS SWIPT, Bernstein inequality, energy harvesting (EH), amplify and forward (AF) relay, secret communication.

I. INTRODUCTION

Since having characteristics of being energy-saving, cheap, flexible and convenient, the wireless sensor network (WSN) has wide application in areas such as military, traffic control, environmental monitoring, and so on. But, due to their limited energy, WSN nodes have a limited lifetime which largely limits the network performance. As we know, Radio-Frequency (RF) signals can be used not only as an energy carrier but also as a vehicle for transporting information. So, SWIPT technique has become a promising solution of energy-constrained wireless networks and attracted increasing attention [1].

Research shows that high information rate, high energy collection efficiency and high security are key requirements of SWIPT technique. Varshney defines a capacity-energy function to describe the information transmission efficiency of SWIPT systems. Using power allocation of input signal, his method gets tradeoff between the energy rates and reliable information [2]. Grover extends Varshney's method to

frequency-selective channel and uses power allocation technique to balance information transmission rate and energy collection efficiency [3]. It can be found that the above research is based on the assumption that the receiver synchronously obtains energy and decodes information from the same signal, which is difficult to realize in actual physical systems. To tackle this problem, R. Zhang *et al.* propose a time division scheme to decode and harvest energy respectively [4].

SWIPT network systems have more open architecture and more multifarious node types than that of traditional wireless network. Information exchanged in SWIPT network systems can easily be eavesdropped. Eves may have the access to attacking cryptographic protocol of SWIPT systems when physical layer security cannot be guaranteed. So, physical layer security is fundamental to SWIPT network systems. Physical layer security technology that uses statistic characteristics of wireless channel to protect user information is one of the effective technologies related to eavesdrop protecting [5] and becomes a hot spot of wireless communication research area.

The associate editor coordinating the review of this manuscript and approving it for publication was Shihao Yan.

A. RELATED WORK AND MOTIVATION

In general, energy receivers (ERs) consume more power than that of information receivers (IRs). Thus, ERs need to be set in a place which more proximity to the transmitter than IRs. This means that ERs have better channels than those of IRs thus ERs can easily eavesdrop the information sent to IRs. To solve the above problem, L. Liu *et al.* discuss the ERs energy collection efficiency in the multi-user single output (MISO) SWIPT system [6]. Supposing the state priori information of channel is accurately known, Liu's methods obtain optimum ERs energy collection efficiency under the system security rate constraint. Shi. Q *et al.* extend L. Liu's method to multiple-input multiple-output (MIMO) SWIPT system whose channel state priori information is accurately known, and get optimum system security rate under the constraint of energy collection efficiency and power of transmitter [7].

Due to non-cooperation characteristics of Eves, the transmitter may hardly obtain the information related to position and CSI of Eves. In the scene of untrusted AF relays and passive multiple-antenna aided Eves, two phase security scheme of a cooperative relaying network is discussed by Moradikia *et al.* [8]. During the first phase, an appropriate jammer is chosen among untrusted relays and destination, while in the second phase of data retransmission, the idle transmitter is forced to work as a jammer. Considering a system model consisting of a transmitter, one untrusted AF relay, a receiver and a warden, Moslem Forouzesh *et al.* inject jamming signals during the transmitter-to-relay and relay-to-receiver phases to prevent the warden from detecting the presence of communications via the transmitter-relay-receiver link and untrusted relay decoding the source signal, respectively [9]. M. Tatar Mamaghani *et al.* propose a novel cooperative secure unmanned aerial vehicle (UAV) aided transmission protocol. In order to improve physical-layer security and transmission reliability, they adopt destination-assisted cooperative jamming as well as SWIPT at the UAV-mounted relay [10]. Xiaobao Zhou *et al.* introduced the energy sustaining strategy to enhance physical layer security of directional modulation (DM) system. In their strategy, a decode-and-forward (DF) relay and self-sustained jammers is introduced into a DM system, thus application scenarios of DM system are extended. Moreover, they also respectively designed beamforming vectors at the source, relay, and jammers to enhance the secrecy performance of DM system [11]. However, artificial noise can also interfere with users while interfering with Eves, and generating artificial noise may induce extra energy consumption.

In most realistic scenarios, due to the delay, synchronization error or other reasons, receivers may only obtain imperfect CSI. Commonly, there are random CSI error model and deterministic CSI error model to describe imperfect CSI, respectively. With imperfect CSI at the transmitter and Eves, the method of maximizing the secrecy rate is proposed by Ren *et al.* [12]. This strategy uses semidefinite relaxation (SDR) and successive convex approximation (SCA)

technique to jointly optimize the information beamforming vectors and energy beamforming vectors. Similar to REN Yuan's method, B.Li explores the problem of maximizing the secrecy rate in imperfect CSI at the transmitter and IRs [13]. Their works use norm-bounded deterministic CSI error model, since the bound of CSI cannot be obtained exactly in engineering practice and the probability of the worst-case CSI error is very low, their work seems too idealistic and conservative. This problem can be partly solved by using random CSI error model.

Using random CSI error model, Zhengyu Zhu investigates an optimum robust transmit power problem under the secrecy rate outage probability constraint of legitimate users and harvested power outage probability constraint of ERs [14], B.Li *et al.* address joint optimum problem of transmit matrix, artificial noise covariance matrix and power splitting ratio subject to transmission power constraint, a outage probability constraint of SINR between receiver and the Eves, as well as probability constraint of energy harvested at the receiver. By using Bernstein-type inequality restriction technique, B.Li's method transfers probability constraint to linear matrix inequality form and gets a suboptimal solver for original non-convex problem [15]. Obviously, their method focus on the non-relay network scene, and cannot apply to SWIPT system which uses AF relay. Jinsong Hu *et al.* investigated covert communications of wireless-powered relay related to SWIPT system [16]. As we known, Hu's method transmits information of relay to the destination covertly on top of forwarding the source's message. However, energy efficiency of this method should be enhanced.

B. CONTRIBUTIONS

We explore the secure transmission strategy of the relay SWIPT system in this paper. Our main contributions are summarized below.

- Considering random CSI error model corresponding to imperfect channel between relays and Eves, we discuss the problem of optimal system security rate subject to relay transfer power constraint and probability constraint of SINR of Eves.
- By introducing a slack variable, we recast original non-convex objective function into a two-stage optimization problem to solve, moreover, we employ Bernstein-type inequality to convert non-convex probability constraint to linear matrix inequality form.

The rest of the paper is organized as follows. The system model and problem formulation are presented in Section II. The optimization of relay beamforming is presented in Section III. Complexity analysis and simulation results are given in Section IV. Finally, Section V gives the conclusion of this paper.

Notations: Column vectors and matrices are denoted by boldface lower case letters and capital letters, respectively. The Euclidean norm of a vector and the absolute value of a complex scalar are denoted by $\|\bullet\|$ and $|\bullet|$, respectively. $(\bullet)^+$ is defined as $\max\{0, \bullet\}$. The Hadamard product is

denoted by \odot . The Hermitian conjugate transpose, transpose, rank and trace of a matrix \mathbf{A} are denoted by $\mathbf{A}^H, \mathbf{A}^T, \text{rank}(\mathbf{A})$, respectively. $\text{vec}(\mathbf{A})$ is the vectorization of the matrix \mathbf{A} ; \mathbb{C}^N is the sets of complex N-dimensional vectors; \mathbf{I} denotes the identity matrix; $\text{diag}(\mathbf{v})$ is the diagonal matrix with the vector \mathbf{v} on the diagonal.

II. SYSTEM MODEL AND PROBLEM FORMULATION

As shown in Fig. 1, there are K Eves, one source (Tx), one receiver (Rx) and N relays $N > K^1$ in the scene. Tx, Rx, relays and Eves are all equipped with a single antenna. Tx communicates with the Rx through AF relays. Supposing Tx, Rx and Eves do not have a direct link, and Eves are distributed outside the security area [18] centered on Rx (Eves in the security area will be detected by Tx [19]). This scenario can be widely found in real life. Consider a remote health system where a moving patient reports its physical data to a health center with the aid of intermediary sensor nodes installed on other patients. However, hackers located in the vicinity of patients may illegally collect the physical data related to patient. In this scenario, we can use beamforming technique to against passive attacks of hackers, thus to enhance security of networks. Motivated by good characteristic related to SWIPT and cooperative relay technique such as high energy efficiency, vast degree-of-freedom and so on, for the purpose of improving physical-layer security and transmission reliability, we consider maximizing the secrecy rate with the aid of AF relays, subject to the energy harvesting power constraints of individual relays.

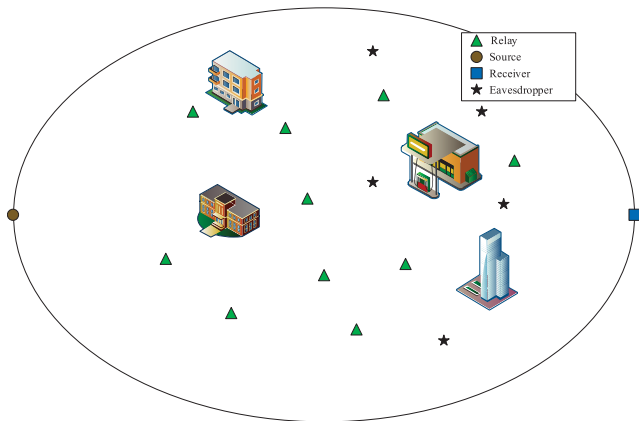


FIGURE 1. The system model for a SWIPT relay network.

Receiver of each AF relay uses a power splitting (PS) technique to collect energy and extract information from the radio frequency signal. As shown in Fig. 2, the i th relay divides the received signals y_{r_i} into two components, one ($\sqrt{\bar{\alpha}_i}y_{r_i}$) is used for energy harvesting and another ($\sqrt{1-\bar{\alpha}_i}y_{r_i}$) is used for information reception, where $\bar{\alpha}_i$ and η ($0 \leq \eta < 1$) denotes

¹We want to compare the performance of proposed method with ZF-Eves method [17]. The condition $N > K$ should be satisfied since ZF-Eves method sets the secret signal into the zero space of the relays-Eves channel.

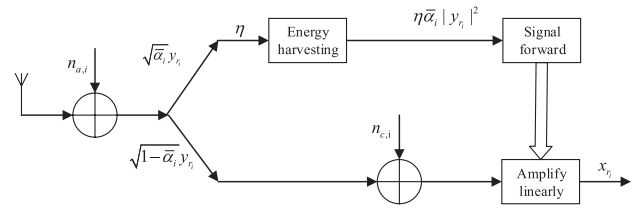


FIGURE 2. Power splitting receiver architecture for AF relay.

the power allocation factor and energy collection efficiency, respectively.

Collaboration process of AF protocol is divided into two stages. Firstly, the received signal of each relay can be expressed as

$$y_{r_i} = h_{sr_i} \sqrt{P_s} s + n_{a,i}, \quad \forall i \quad (1)$$

where $s \sim \mathcal{CN}(0, 1)$ is a complex Gaussian random variable with zero mean and unit variance, h_{sr_i} is complex coefficient of the channel from Tx to i th relay, P_s is transmit power of Tx, $n_{a,i} \sim \mathcal{CN}(0, \sigma_{n_a}^2)$ is additive white Gaussian noise(AWGN) of i th relay. After being amplified linearly, the baseband equivalent signal output of i th relay is given by

$$x_{r_i} = \beta_i \left(\sqrt{1-\bar{\alpha}_i} y_{r_i} + n_{c,i} \right), \quad \forall i \quad (2)$$

where β_i is complex coefficient, $n_{c,i} \sim \mathcal{CN}(0, \sigma_{n_c}^2)$ is baseband conversion noise of RF signal. Obviously, output power of baseband signal should be less than forward power of relays, which means $|x_{r_i}|^2 \leq \eta \bar{\alpha}_i |y_{r_i}|^2$. And we can deduce the expression below

$$\beta_i = \sqrt{\frac{\eta \bar{\alpha}_i |h_{sr_i}|^2 P_s}{(1-\bar{\alpha}_i) |h_{sr_i}|^2 P_s + (1-\bar{\alpha}_i) \sigma_{n_a}^2 + \sigma_{n_c}^2}} e^{j\angle \beta_i} \quad (3)$$

where $\angle \beta_i$ is defined as the phase of the i th relay AF coefficient.

Using (1) and (2), the transmitted signals of all relays can be expressed as the following vector form

$$\mathbf{x}_r = \mathbf{D}_{\beta\alpha} \mathbf{h}_{sr} \sqrt{P_s} s + \mathbf{D}_{\beta\alpha} \mathbf{n}_a + \mathbf{D}_{\beta} \mathbf{n}_c \quad (4)$$

where $\mathbf{D}_{\beta\alpha}$ and \mathbf{D}_{β} are diagonal matrix, the vectors on its diagonal are $(\beta_1, \dots, \beta_N)^T$ and $(\beta_1 \sqrt{1-\bar{\alpha}_1}, \dots, \beta_N \sqrt{1-\bar{\alpha}_N})^T$, respectively. In addition $\mathbf{h}_{sr} = [h_{sr_i}]_{i=1}^N$, $\mathbf{n}_a = [n_{a,i}]_{i=1}^N$, $\mathbf{n}_c = [n_{c,i}]_{i=1}^N$.

Secondly, the signal received by Rx is given by

$$y_d = \mathbf{h}_{rd}^T \mathbf{x}_r + n_d \quad (5)$$

where $n_{d,i} \sim \mathcal{CN}(0, \sigma_{n_d}^2)$ is AWGN of Rx, $\mathbf{h}_{rd} = [h_{rd}]_{i=1}^N$ represents the complex coefficient of the channel from the i th relay to Rx. Substituting (4) into (5), we get

$$y_d = \mathbf{h}_{rd}^T \mathbf{D}_{\beta\alpha} \mathbf{h}_{sr} \sqrt{P_s} s + \mathbf{h}_{rd}^T \mathbf{D}_{\beta\alpha} \mathbf{n}_a + \mathbf{h}_{rd}^T \mathbf{D}_{\beta} \mathbf{n}_c + n_d \quad (6)$$

The signal intercepted by the k th Eve denoted by

$$y_{e,k} = \mathbf{h}_{re,k}^T \mathbf{x}_r + n_{e,k} \quad (7)$$

where $\mathbf{h}_{re,k} = [h_{r_{ie},k}]_{i=1}^N$ represents the set of channels from the relay to the k th Eve, $n_{e,k} \sim \mathcal{CN}(0, \sigma_{n_{e,k}}^2)$ is AWGN of k th Eve. Substituting (4) into (7), we get

$$y_{e,k} = \mathbf{h}_{re,k}^T \mathbf{D}_{\beta\alpha} \mathbf{h}_{sr} \sqrt{P_s} s + \mathbf{h}_{re,k}^T \mathbf{D}_{\beta\alpha} \mathbf{n}_a + \mathbf{h}_{re,k}^T \mathbf{D}_{\beta} \mathbf{n}_c + n_{e,k} \quad (8)$$

So, SINR of Rx and Eves is described as (9) and (10), respectively.

$$\text{SINR}_{S,D} = \frac{P_s |\mathbf{h}_{rd}^T \mathbf{D}_{\beta\alpha} \mathbf{h}_{sr}|^2}{\sigma_{n_a}^2 \|\mathbf{h}_{rd}^T \mathbf{D}_{\beta\alpha}\|^2 + \sigma_{n_c}^2 \|\mathbf{h}_{rd}^T \mathbf{D}_{\beta}\|^2 + \sigma_{n_d}^2} \quad (9)$$

$$\text{SINR}_{S,E,k} = \frac{P_s |\mathbf{h}_{re,k}^T \mathbf{D}_{\beta\alpha} \mathbf{h}_{sr}|^2}{\sigma_{n_a}^2 \|\mathbf{h}_{re,k}^T \mathbf{D}_{\beta\alpha}\|^2 + \sigma_{n_c}^2 \|\mathbf{h}_{re,k}^T \mathbf{D}_{\beta}\|^2 + \sigma_{n_{e,k}}^2} \quad (10)$$

Considering imperfect CSI channel between relay and eavesdropper, we modify $\text{SINR}_{S,E,k}$ as (11), as shown at the bottom of the page, where $\delta_k \sim \mathcal{CN}(\mathbf{0}, \mathbf{C}_k)$ denotes complex Gaussian random error of channel variable with $\mathbf{0}$ mean and \mathbf{C}_k covariance.

Similar to the description in [20], secret rate of information transmission is defined as follow

$$r_{\text{sec}} = \left(r_{S,D} - \max_{k=1 \dots K} r_{S,E,k} \right)^+ \quad (12)$$

where mutual information of Rx is denoted by $r_{S,D} = \frac{1}{2} \log(1 + \text{SINR}_{S,D})$, and mutual information of the k th Eve is described by $r_{S,E,k} = \frac{1}{2} \log(1 + \text{SINR}_{S,E,k})$.

For convenience, we revise $r_{S,D}$ and $r_{S,E,k}$ in (12) to forms as following

$$\begin{cases} r_{S,D} = \frac{1}{2} \log_2 \left(1 + \frac{P_s |\tilde{\mathbf{h}}_{sd}^T \mathbf{w}|^2}{\mathbf{w}^H \mathbf{D}_{\hat{s}d} \mathbf{w} + \sigma_{n_d}^2} \right) \\ r_{S,E,k} = \frac{1}{2} \log_2 \left(1 + \frac{P_s |\tilde{\mathbf{h}}_{se,k}^T \mathbf{w}|^2}{\mathbf{w}^H \mathbf{D}_{\hat{s}e,k} \mathbf{w} + \sigma_{n_{e,k}}^2} \right) \end{cases} \quad (13)$$

where $\mathbf{w} = [w_i]_{i=1}^N$ is defined as the weight set of relays, and other parameters are defined as (14), as shown at the bottom of the page.

Combining (12) with (13), we should optimize secret rate of relay subject to relay forwarding power constraints.

$$\begin{aligned} (P1) \quad & \max_{\mathbf{w}} \left(r_{S,D} - \max_{k=1 \dots K} r_{S,E,k} \right)^+ \\ & \text{s.t. } \text{trace} \left(\left(\eta \bar{\alpha}_i P_x |h_{sr_i}|^2 \mathbf{w} \mathbf{w}^H \right) \mathbf{E}_i \right) \leq \eta \bar{\alpha}_i P_x |h_{sr_i}|^2, \quad \forall i \end{aligned} \quad (15)$$

III. BEAMFORMING OPTIMIZATION FOR RELAYS

In this section, we consider how to maximize the secret rate by optimizing the relay beam. Since the objective function of (P1) is a non-convex function, it is difficult to solve directly. Therefore, this paper uses a two-level optimization method [21] to tackle this problem, and (P1) is decomposed into two levels sub-problems to jointly solve by introducing a slack variable $\tau \in (0, 1]$. Firstly, the lower-level optimization problem can be viewed as a quadratic programming problem about variables \mathbf{w} after being given a fixed variable τ ,

$$\text{SINR}_{S,E,k} = \frac{P_s |(\mathbf{h}_{re,k} + \delta_k)^T \mathbf{D}_{\beta\alpha} \mathbf{h}_{sr}|^2}{\sigma_{n_a}^2 \left\| (\mathbf{h}_{re,k} + \delta_k)^T \mathbf{D}_{\beta\alpha} \right\|^2 + \sigma_{n_c}^2 \left\| (\mathbf{h}_{re,k} + \delta_k)^T \mathbf{D}_{\beta} \right\|^2 + \sigma_{n_{e,k}}^2} \quad (11)$$

$$\left[\tilde{\mathbf{h}}_{sd} \right]_i \triangleq h_{sr_i} h_{r_{id}} \sqrt{\frac{\eta \bar{\alpha}_i (1 - \bar{\alpha}_i) |h_{sr_i}|^2 P_s}{(1 - \bar{\alpha}_i) \left(|h_{sr_i}|^2 P_s + \sigma_{n_a}^2 \right) + \sigma_{n_c}^2}}, \quad \forall i \quad (14a)$$

$$\left[\mathbf{D}_{\hat{s}d} \right]_{i,i} \triangleq \frac{\eta \bar{\alpha}_i P_s |h_{sr_i}|^2 |h_{r_{id}}|^2 \left((1 - \bar{\alpha}_i) \sigma_{n_a}^2 + \sigma_{n_c}^2 \right)}{(1 - \bar{\alpha}_i) \left(|h_{sr_i}|^2 P_s + \sigma_{n_a}^2 \right) + \sigma_{n_c}^2}, \quad \forall i \quad (14b)$$

$$\left[\tilde{\mathbf{h}}_{se,k} \right]_i \triangleq h_{sr_i} (h_{r_{ie,k}} + \delta_k) \sqrt{\frac{\eta \bar{\alpha}_i (1 - \bar{\alpha}_i) |h_{sr_i}|^2 P_s}{(1 - \bar{\alpha}_i) \left(|h_{sr_i}|^2 P_s + \sigma_{n_a}^2 \right) + \sigma_{n_c}^2}} \triangleq [H_{sr}]_i (h_{r_{ie,k}} + \delta_k), \quad \forall i \quad (14c)$$

$$\left[\mathbf{D}_{\hat{s}e,k} \right]_{i,i} \triangleq \frac{\eta \bar{\alpha}_i P_s |h_{sr_i}|^2 |h_{r_{ie,k}} + \delta_k|^2 \left((1 - \bar{\alpha}_i) \sigma_{n_a}^2 + \sigma_{n_c}^2 \right)}{(1 - \bar{\alpha}_i) \left(|h_{sr_i}|^2 P_s + \sigma_{n_a}^2 \right) + \sigma_{n_c}^2} \triangleq [D_{1sr}]_{i,i} |h_{r_{ie,k}} + \delta_k|^2, \quad \forall i \quad (14d)$$

which can be expressed as a mathematical model as follows

$$(P1.1) \quad \max_{\mathbf{w}} \left(\frac{P_s |\tilde{\mathbf{h}}_{sd}^T \mathbf{w}|^2}{\mathbf{w}^H \mathbf{D}_{sd} \mathbf{w} + \sigma_{nd}^2} \right)$$

$$\text{s.t. } \text{trace} \left(\left(\eta \bar{\alpha}_i P_s |h_{sr_i}|^2 \mathbf{w} \mathbf{w}^H \right) \mathbf{E}_i \right) \leq \eta \bar{\alpha}_i P_s |h_{sr_i}|^2, \quad \forall i \quad (16a)$$

$$\frac{P_s |\tilde{\mathbf{h}}_{se,k}^T \mathbf{w}|^2}{\mathbf{w}^H \mathbf{D}_{se,k} \mathbf{w} + \sigma_{ne,k}^2} \leq 1/\tau - 1, \quad \forall k \quad (16b)$$

where $1/\tau - 1$ of (16b) is the SINR of eavesdropper with the strongest eavesdropping ability, which is the upper bound related to SINR of all Eves. The inequality (16a) is the linear forward power constraints of individual relays. It means that the relay forward power lower than the energy harvested by relay. Bruno Clerckx et al have presented three different energy harvester models in [22], namely the conventional linear model, the diode nonlinear model and the saturation nonlinear model. Elena Boshkovska *et al.* proposed a practical EH model to capture the non-linear characteristics of EH circuits and designed a resource allocation algorithm for SWIPT systems [23]. For simplicity, many allocation algorithm designs for SWIPT networks are based on a linear EH model. So, we consider the linear energy harvesting circuit model here, too.

Due to the random error δ_k of CSI related to channel between the relay and the eavesdropper, (16b) is infeasible, it means any \mathbf{w} can't be found to satisfy the (16b). So, we relax (16b) to the probability constraint which is presented as follow

$$\Pr \left\{ \frac{P_s |\tilde{\mathbf{h}}_{se,k}^T \mathbf{w}|^2}{\mathbf{w}^H \mathbf{D}_{se,k} \mathbf{w} + \sigma_{ne,k}^2} \geq 1/\tau - 1 \right\} \leq \rho_k, \quad \forall k \quad (17)$$

It means the probability of violating (16b) is small. Substituting (17) into (16b), optimal problem (P1.1) can be represented as follow

$$\max_{\mathbf{w}} \left(\frac{P_s |\tilde{\mathbf{h}}_{sd}^T \mathbf{w}|^2}{\mathbf{w}^H \mathbf{D}_{sd} \mathbf{w} + \sigma_{nd}^2} \right)$$

$$\text{s.t. } \text{trace} \left(\left(\eta \bar{\alpha}_i P_s |h_{sr_i}|^2 \mathbf{w} \mathbf{w}^H \right) \mathbf{E}_i \right) \leq \eta \bar{\alpha}_i P_s |h_{sr_i}|^2, \quad \forall i \quad (18a)$$

$$\Pr \left\{ \frac{P_s |\tilde{\mathbf{h}}_{se,k}^T \mathbf{w}|^2}{\mathbf{w}^H \mathbf{D}_{se,k} \mathbf{w} + \sigma_{ne,k}^2} \geq 1/\tau - 1 \right\} \leq \rho_k, \quad \forall k \quad (18b)$$

Subsequently, we can use Bernstein-type inequality to convert (18b) into convex form, and (18) is expressed as

$$\max_{\mathbf{w}} \left(\frac{P_s |\tilde{\mathbf{h}}_{sd}^T \mathbf{w}|^2}{\mathbf{w}^H \mathbf{D}_{sd} \mathbf{w} + \sigma_{nd}^2} \right)$$

$$\text{s.t. } \text{trace} \left(\left(\eta \bar{\alpha}_i P_x |h_{sr_i}|^2 \mathbf{w} \mathbf{w}^H \right) \mathbf{E}_i \right) \leq \eta \bar{\alpha}_i P_x |h_{sr_i}|^2, \quad \forall i$$

$$\mathcal{O}(\mathbf{w}) \quad (19)$$

Proof: See Appendix for details.

Supposing that \mathbf{w} corresponding to fixed τ to be obtained by (19), we start to solve the upper level problem by now. Firstly, we define $f(\tau)$ as an optimal solution of (19), a relaxation solution of (P1.1) namely. Let $H(\tau) = \tau f(\tau)$, the objective function of (P1) can be expressed as follow

$$\frac{1}{2} \log_2(1+f(\tau)) - \frac{1}{2} \log_2(1/\tau) = \frac{1}{2} \log_2(\tau + H(\tau)) \quad (20)$$

So the optimization problem above can be expressed as

$$(P1.2) \quad \max_{\tau} \log_2(\tau + H(\tau))$$

$$\text{s.t. } \tau_{\min} \leq \tau \leq 1 \quad (21)$$

where τ_{\min} is the lower bound of τ , and it can be defined by following inequality

$$\tau \geq \frac{1}{1 + P_s \|\tilde{\mathbf{h}}_{sd}\|^2 \|\mathbf{w}\|^2 / \sigma_{nd}^2} \geq \frac{1}{1 + N P_s \|\tilde{\mathbf{h}}_{sd}\|^2 / \sigma_{nd}^2} = \tau_{\min} \quad (22)$$

where the first inequality is followed by Cauchy-Schwarz inequality and the second inequality follows from $|w_i|^2 \leq 1, \forall i$. Supposing that $H(\tau)$ can be calculated for τ in any feasible region, and then a one-dimensional linear search within the interval $[\tau_{\min}, 1]$ will obtain the optimal solution τ^* of the upper-level problem (P1.2).

Now, we can use bi-section algorithm [24] to obtain solution to P1 problem by combining the solution to P1.1 problem with solution to P1.2 problem. The details of algorithm are described as Table 1.

TABLE 1. Algorithm for solving(P1): Beamforming Optimization for Relay.

-
- 1: Initialize parameters relate to problem (P1).
 - 2: Given $\tau_{\min} = l \leq \tau$, $1 = u \geq \tau$, $r > 0$, tolerance $\varepsilon > 0$
 - 3: **Repeat:**
 - 4: $\tau \leftarrow (l + u)/2$
 - 5: Slove(P1.1) return $H(\tau)$ and \mathbf{W}
 - 6: Slove(P1.2) return $r = (1/2) \log_2(\tau + H(\tau))$,
 $r^t = (1/2) \log_2(\tilde{\tau} + H(\tilde{\tau}))$, $\tilde{\tau} = \max(\tau - \Delta\tau, \tau_{\min})$
 where $\Delta\tau > 0$ denotes an arbitrary small value.
 - 7: If $r > r^t$, $l \leftarrow \tau$; else $u \leftarrow \tau$
 - 8: **Until** $|r - r^t| < \varepsilon$
 - 9: $\mathbf{W}^* \leftarrow \mathbf{W}$, get \mathbf{w}^* by applying EVD to \mathbf{W}^* , $r^* \leftarrow r$.
-

IV. COMPLEXITY ANALYSIS AND NUMERICAL RESULTS

In this subsection, we evaluate the complexity of the proposed robust secure scheme. We can find that the computational complexity per iteration mainly stems from the number of optimization variables, the number of SDP linear inequalities and SDP size. Consider formulation (19), which has $2K + N$ linear inequalities constraints of size 1, K linear inequalities

constraints of size 2, and $K + N$ linear inequalities constraints of size N . Moreover, the number of decision variables is on the order of KN^2 . Observing Table 1, we can find that complexity computation of proposed algorithm in each iteration is mainly determined by solving of (19). Similar to [25], the complexity computation of proposed algorithm can roughly described as the form of $O(\sqrt{N(N + K)}K^3N^6 \ln(1/\epsilon))$.

Considering that AF relays and Eves (located outside of the “security zone”) are uniformly deployed in a circular area of radius R (Fig.1). Assuming the both large-scale path loss and small-scale multi-path fading channel models, we employ (23) to describe path loss

$$L = A_0 \left(\frac{d}{d_0} \right)^{-\kappa} \tag{23}$$

Parameters related to experiment are described in Table 2. To simplify, the power splitting factor is fixed to be 0.5 all the time.

TABLE 2. Parameters of experiment.

Parameters	Notation	Typical Values
R	Circular area of radius R	1.5m
P_s	Power of transmitter	30dBm
η	Energy collection efficiency	50%
$\bar{\alpha}_i$	Power splitting ratio	0.5
$\sigma_{n_a}^2$	Noise power of relay	-80dBm
$\sigma_{n_c}^2$	Noise variances of Baseband	-50dBm
$\sigma_{n_d}^2$	Noise variances of Rx	-130dBm
$\sigma_{n_{e,k}}^2$	Noise variances of eavesdropper	-130dBm
A_0	Fade coefficient	10^{-3}
d_0	Distance	1m
κ	Path loss exponent	2.5
ρ_k	Threshold of probability constraint	0.1
\mathcal{C}_k	Channel error	$0.002I$
h_{sr_i}	Channel from Tx to ith relay	$\mathcal{CN}(0, L)$
$h_{r_i d}$	Channel from ith relay to Rx	$\mathcal{CN}(0, L)$
$h_{r_i e,k}$	Channel from ith relay to kth eavesdropper	$\mathcal{CN}(0, L)$

We evaluate the performance of proposed method with Worst-Case method [20] and ZF-Eves method [17] by comparison experiment.

Fig. 3 shows the achievable secrecy rate for the legitimate Rx versus transmitter power of Tx. It is clearly that secrecy rate of all methods enhance with transmitter power of Tx increasing, and since relaxing eavesdropper SINR constraint, the proposed method gets higher secrecy rate than that of other method. Moreover, worst-case method obtains lowest

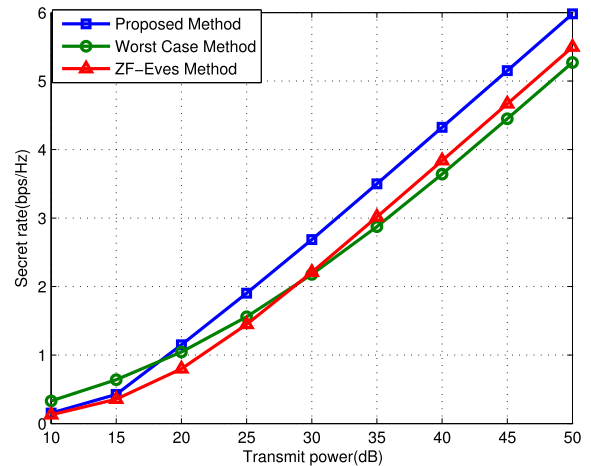


FIGURE 3. The secrecy rate versus power of transmitter(N=20,K=16).

secrecy rate among all method because its constraint conditions are too conservative.

Fig. 4 describes the maximum secrecy rate of the Rx versus the number of relays. Similar to Fig. 3, it can be found that maximum secrecy rate of each method grows with the increasing number of relays. The proposed method obtains the highest secrecy rate in all methods because of its appropriate optimal scheme. It is noteworthy that too conservative, worst-case method attains the lowest secrecy rate in all methods again.

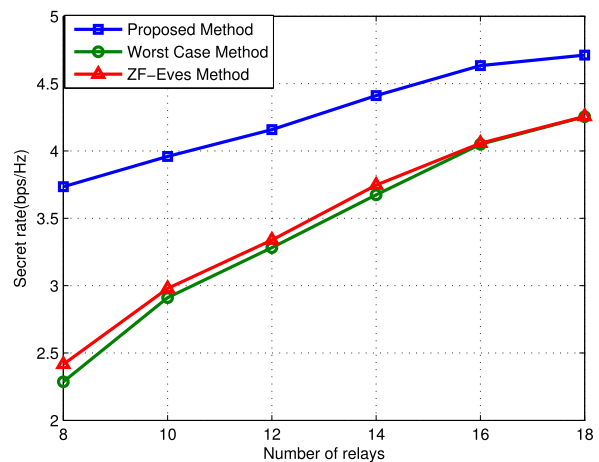


FIGURE 4. The secrecy rate versus the number of relays(K=5).

Fig. 5 describes the achievable secrecy rate for the legitimate Rx versus transmitter power of Tx in 10 relays and 15 relays, respectively. We find that secrecy rate of three methods enhance with the number of the relays increasing at the same Tx transmitting power. Moreover, same as the reason described by Fig. 3, with same Tx transmitting power, the maximum security rates of three methods listed in descending order are the proposed method, ZF-Eves method and worst-case method.

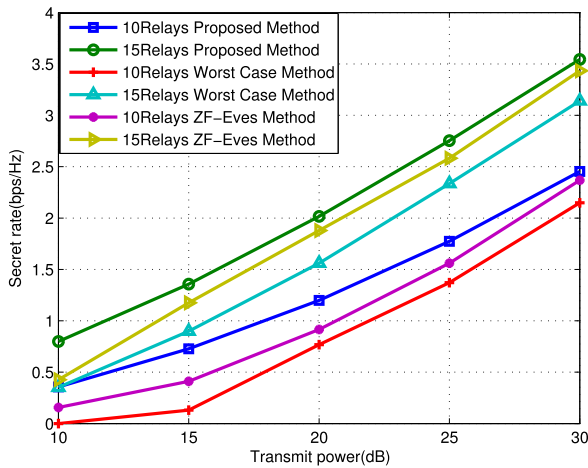


FIGURE 5. The secrecy rate versus power of transmitter in 10 relays and 15 relays, respectively ($K=5$).

Convergence rate of the proposed method and worst-case method is compared in Fig. 6. It is clearly found that because of low dimension of variables to be optimized, worst-case method converges faster than proposed method. But, as we described before, since relaxing eavesdropper SINR constraint, the proposed method obtains higher secrecy rate than worst-case method.

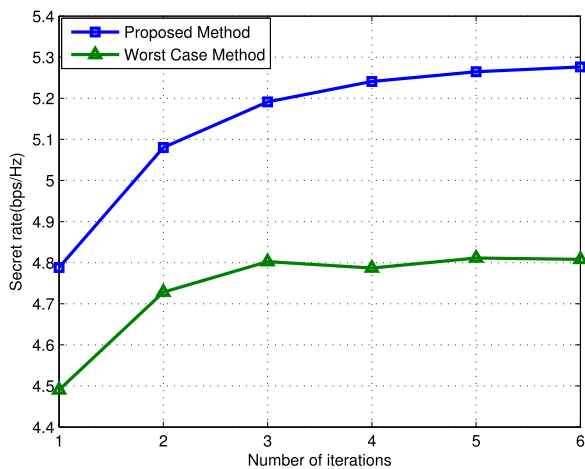


FIGURE 6. The secrecy rate versus the number of iterations ($N=20, K=16$).

Fig. 7 shows achievable secrecy rate for the legitimate Rx versus transmitter power of Tx in 0.02 channel error factor and 0.2 channel error factor, respectively. We find that the proposed method obtains higher secrecy rate than that of worst-case method. Moreover, since enhancing channel statistic information accuracy, secrecy rate of two methods are slightly heightened when channel error factor decrease.

Fig. 8 shows the maximum secrecy rate of the legitimate Rx versus power allocation factor. We can find that secrecy rate of all methods enhance with the power allocation factor increasing. It is intuitive since the forward ability of AF can be enhanced by increasing harvesting energy.

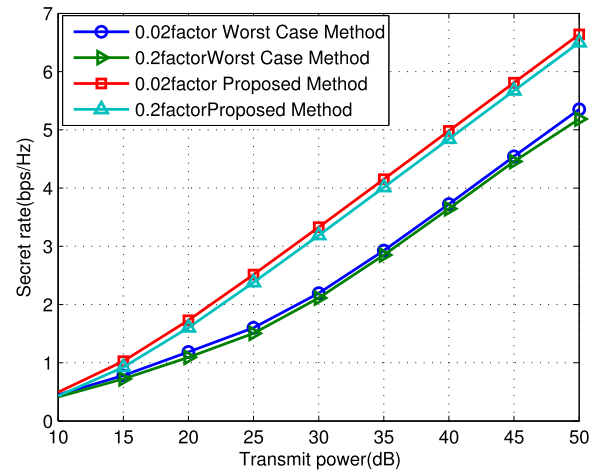


FIGURE 7. The secrecy rate versus transmitter power of Tx in different channel error factor ($N=20, K=16$).

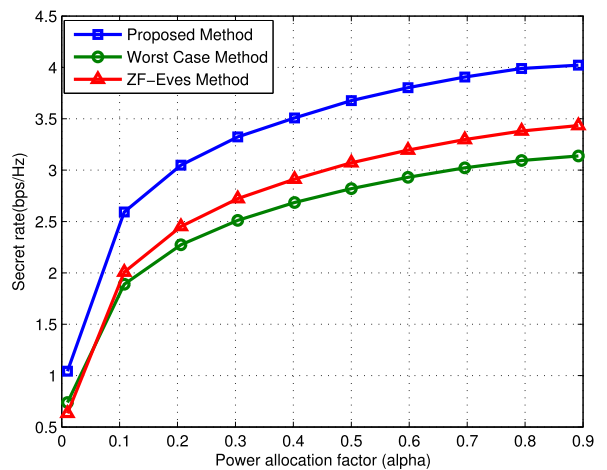


FIGURE 8. The secrecy rate versus power allocation factor ($N=20, K=16$).

Moreover, the proposed method obtains the highest secrecy rate in all methods due to its appropriate optimal scheme. However, worst-case method obtains the lowest secrecy rate in all methods because of its too conservative constraint conditions.

From comparisons above, we conclude that the proposed method obtains higher secrecy rate than that of worst-case method and ZF-Eves method in same conditions. It is reasonable since the proposed method relaxes the constraint used by other methods. However, channels between the Tx and the Eves may hardly constraint in the orthogonal space of beamforming due to the Eves increasing, thus more relay can be used as the decoder of Eves, leading to poor secrecy rate of ZF-Eves method. Meanwhile, worst-case method attains the lowest secrecy rate in all methods because of too conservative constraint conditions.

V. CONCLUSION

We explore a secure transmission scheme in relay SWIPT systems. Assuming random CSI error model corresponding to imperfect channel of relays and Eves, we optimize

system security rate subject to relay transfer power constraint and probability constraint at SINR of receiver and Eves. Using slack variable technique, we transfer original non-convex objective function into a two-stage optimization problem. Moreover, Bernstein-type inequality is used to reform non-convex probability constraint to linear matrix inequalities. Performance of the proposed method is demonstrated by comparison experiments with worst-case method and ZF-Eves method.

APPENDIX

Let $\tilde{\mathbf{w}} = \sqrt{\frac{((1-\tilde{\alpha}_i)\sigma_{na}^2 + \sigma_{nc}^2)}{1-\tilde{\alpha}_i}} \text{diag}\left(\frac{1}{\mathbf{h}_{sr}}\right) \mathbf{w}$, $\mathbf{H}_{sr} = [\mathbf{H}]_{i=1}^N$. Substituting (14c), (14d) to (18b), we get (24) and (25), (26), as shown at the bottom of the page.

Then we represent random CSI error as

$$\delta_k = \mathbf{C}_k^{1/2} \boldsymbol{\zeta}_k \quad k = 1, \dots, K \tag{27}$$

where $\mathbf{C}_k^{1/2}$ is the Power Spectrum Density (PSD) square root of \mathbf{C}_k , $\boldsymbol{\zeta}_k \in \mathcal{CN}(\mathbf{0}, \mathbf{I})$. So, (18b) can be described as (28), as shown at the top of the next page, where $\Re\{\bullet\}$ represents the real part of the associated argument and the other variables are defined as (29a), (29b) and (29c), as shown at the top of the next page.

Obviously, the constraint (28) is still a probabilistic constraint. By controlling quadratic forms of Gaussian variables involving matrices, we transform the probabilistic constraint into deterministic forms using Bernstein-type inequalities which is given by the following lemma.

Lemma: Let $G = \boldsymbol{\zeta}^H \mathbf{Q} \boldsymbol{\zeta} + 2\Re\{\boldsymbol{\zeta}^H \mathbf{u}\}$, where $\mathbf{Q} \in \mathbb{H}^N$ is a complex hermitian matrix, $\mathbf{u} \in \mathbb{C}^N$ and $\boldsymbol{\zeta} \in \mathcal{CN}(\mathbf{0}, \mathbf{I})$. Then for any $\delta > 0$, we have

$$\Pr\left\{G \geq \text{trace}(\mathbf{Q}) + \sqrt{2\gamma} \sqrt{\|\text{vec}(\mathbf{Q})\|^2 + 2\|\mathbf{u}\|^2} + \gamma(\lambda_{\max}(\mathbf{Q}))^+ \right\} \leq \exp(-\gamma) \tag{30}$$

where $\lambda_{\max}(\mathbf{Q})$ denotes the maximum eigenvalue of matrix \mathbf{Q} . Let $\gamma \triangleq -\ln(\rho)$, where $\rho \in (0, 1]$. Lemma implies that the inequalities

$$\Pr\left\{\boldsymbol{\zeta}_k^H \mathbf{Q}_k \boldsymbol{\zeta}_k + 2\Re\{\boldsymbol{\zeta}_k^H \mathbf{u}_k\} \geq c_k\right\} \leq \rho_k \tag{31}$$

hold if the following inequalities are satisfied

$$\text{trace}(\mathbf{Q}_k) + \sqrt{2\gamma} \sqrt{\|\text{vec}(\mathbf{Q}_k)\|^2 + 2\|\mathbf{u}_k\|^2} + \gamma(\lambda_{\max}(\mathbf{Q}_k))^+ \leq c_k \tag{32}$$

Then, the constraint (28) can be reformulated as constraint

$$\mathcal{O}(\mathbf{w}) := \begin{cases} \text{trace}(\mathbf{Q}_k) + \sqrt{2\gamma}x + \gamma y \leq c_k \\ \sqrt{\|\text{vec}(\mathbf{Q}_k)\|^2 + 2\|\mathbf{u}_k\|^2} \leq x \\ y\mathbf{I} - \mathbf{Q}_k \geq \mathbf{0} \\ y \geq 0 \end{cases} \tag{33}$$

so (18) can be reformulated as

$$\begin{aligned} \max_{\mathbf{w}} & \left(\frac{P_s |\tilde{\mathbf{h}}_{sd}^T \mathbf{w}|^2}{\mathbf{w}^H \mathbf{D}_{sd} \mathbf{w} + \sigma_{nd}^2} \right) \\ \text{s.t. } & \text{trace}\left(\left(\eta \tilde{\alpha}_i P_x |h_{sr_i}|^2 \mathbf{w} \mathbf{w}^H\right) \mathbf{E}_i\right) \leq \eta \tilde{\alpha}_i P_x |h_{sr_i}|^2, \quad \forall i \\ & \mathcal{O}(\mathbf{w}) \end{aligned} \tag{34}$$

Although the probabilistic constraint has been transformed into deterministic forms, it is still hard to solve due to the non-convexity of (34). Next, we will use semi-definite relaxation techniques to convert (34) into a form which can be easily tackled. By introducing $\mathbf{W} \triangleq \mathbf{w} \mathbf{w}^H$ and ignoring rank-one constraint on \mathbf{W} , (34) can be alternatively solved by

$$\begin{aligned} (\text{P1.1-SDR}) \\ \max_{\mathbf{W}} & \frac{\tau P_s \text{trace}\left(\mathbf{W} \tilde{\mathbf{h}}_{sd}^{\dagger} \tilde{\mathbf{h}}_{sd}^T\right)}{\text{trace}\left(\mathbf{W} \mathbf{D}_{sd}\right) + \sigma_{nd}^2} \\ \text{s.t. } & \text{trace}\left(\left(\eta \tilde{\alpha}_i P_x |h_{sr_i}|^2 \mathbf{W}\right) \mathbf{E}_i\right) \leq \eta \tilde{\alpha}_i P_x |h_{sr_i}|^2, \quad \forall i \\ & \mathcal{O}(\mathbf{W}) \\ & \mathbf{W} \geq \mathbf{0} \end{aligned} \tag{35}$$

Note that the objective function has been multiplied by τ compared with that of (34) for easy computation of $H(\tau)$.

Although it is easier to solve (P1.1-SDR) than (34) by rank relaxation, (P1.1-SDR) is still a quasi-convex problem considering the linear fractional form of the objective function and constraints [26], to which Charnes-Cooper transformation [27] will be applied for equivalent convex reformulation.

$$\Pr\left\{\frac{P_s |\mathbf{w}^H \odot \mathbf{H}_{sr} (\mathbf{h}_{re,k} + \delta_k)|^2}{|\tilde{\mathbf{w}}^H \odot \mathbf{H}_{sr} (\mathbf{h}_{re,k} + \delta_k)|^2 + \sigma_{ne,k}^2} \geq 1/\tau - 1\right\} \leq \rho_k \tag{24}$$

$$\Pr\left\{|\mathbf{h}_{re,k} + \delta_k|^2 \left(\frac{P_s}{1/\tau - 1} \mathbf{w} \mathbf{w}^H \odot (\mathbf{H}_{sr}^H \mathbf{H}_{sr}) - \tilde{\mathbf{w}} \tilde{\mathbf{w}}^H \odot (\mathbf{H}_{sr}^H \mathbf{H}_{sr})\right) \geq \sigma_{ne,k}^2\right\} \leq \rho_k \tag{25}$$

$$\Pr\left\{\left(\mathbf{h}_{re,k}^H \mathbf{h}_{re,k} + 2\Re\{\delta_k^H \mathbf{h}_{re,k}\} + \delta_k^H \delta_k\right) \left(\frac{P_s}{1/\tau - 1} \mathbf{w} \mathbf{w}^H \odot (\mathbf{H}_{sr}^H \mathbf{H}_{sr}) - \tilde{\mathbf{w}} \tilde{\mathbf{w}}^H \odot (\mathbf{H}_{sr}^H \mathbf{H}_{sr})\right) \geq \sigma_{ne,k}^2\right\} \leq \rho_k \tag{26}$$

$$\Pr \left\{ \zeta_k^H \mathbf{Q}_k(\mathbf{w}_1, \dots, \mathbf{w}_N) \zeta_k + 2\Re \left\{ \zeta_k^H \mathbf{u}_k(\mathbf{w}_1, \dots, \mathbf{w}_N) \right\} \geq c_k(\mathbf{w}_1, \dots, \mathbf{w}_N) \right\} \leq \rho_k \quad (28)$$

$$\mathbf{Q}_k(\mathbf{w}_1, \dots, \mathbf{w}_N) \triangleq \mathbf{C}_k^{1/2} \left(\frac{P_s}{1/\tau - 1} \mathbf{w} \mathbf{w}^H \odot \left(\mathbf{H}_{sr}^H \mathbf{H}_{sr} \right) - \tilde{\mathbf{w}} \tilde{\mathbf{w}}^H \odot \left(\mathbf{H}_{sr}^H \mathbf{H}_{sr} \right) \right) \mathbf{C}_k^{1/2} \quad (29a)$$

$$\mathbf{u}_k(\mathbf{w}_1, \dots, \mathbf{w}_N) \triangleq \mathbf{C}_k^{1/2} \left(\frac{P_s}{1/\tau - 1} \mathbf{w} \mathbf{w}^H \odot \left(\mathbf{H}_{sr}^H \mathbf{H}_{sr} \right) - \tilde{\mathbf{w}} \tilde{\mathbf{w}}^H \odot \left(\mathbf{H}_{sr}^H \mathbf{H}_{sr} \right) \right) \mathbf{h}_{re,k} \quad (29b)$$

$$c_k(\mathbf{w}_1, \dots, \mathbf{w}_N) \triangleq \sigma_{ne,k}^2 - \mathbf{h}_{re,k}^H \left(\frac{P_s}{1/\tau - 1} \mathbf{w} \mathbf{w}^H \odot \left(\mathbf{H}_{sr}^H \mathbf{H}_{sr} \right) - \tilde{\mathbf{w}} \tilde{\mathbf{w}}^H \odot \left(\mathbf{H}_{sr}^H \mathbf{H}_{sr} \right) \right) \mathbf{h}_{re,k} \quad (29c)$$

Specifically, by substituting $\mathbf{W} = \hat{\mathbf{W}}/\xi$ into (P1.1-SDR), we get

(P1.1-SDP)

$$\begin{aligned} & \max_{\hat{\mathbf{W}}, \xi \geq 0} P_s \text{trace} \left(\hat{\mathbf{W}} \tilde{\mathbf{h}}_{sd}^\dagger \tilde{\mathbf{h}}_{sd}^T \right) \\ & \text{s.t. } \text{trace} \left(\hat{\mathbf{W}} \mathbf{D}_{sd} \right) + \xi \sigma_{nd}^2 = \tau \\ & \text{trace} \left(\left(\eta \tilde{\alpha}_i P_x |h_{sri}|^2 \hat{\mathbf{W}} \right) \mathbf{E}_i \right) \leq \eta \tilde{\alpha}_i P_x |h_{sri}|^2, \quad \forall i \\ & \mathcal{O} \left(\hat{\mathbf{W}} \right) \\ & \hat{\mathbf{W}} \succeq 0 \end{aligned} \quad (36)$$

(P1.1-SDP) can now be efficiently solved using interior-point based methods by some off-the-shelf convex optimization toolboxes, e.g., CVX [28]. The optimal solution \mathbf{W}^* corresponding to (P1.1-SDP) satisfies $\text{rank}(\mathbf{W}^*) = 1$ and the rank-one relaxation of (P1.1-SDR) from (34) is tight for any given τ [21]. The optimal beamforming vector \mathbf{w}^* can be retrieved by eigenvalue decomposition (EVD) of \mathbf{W}^* .

REFERENCES

- [1] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless networks with RF energy harvesting: A contemporary survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 757–789, 2nd Quart., 2015.
- [2] L. R. Varshney, "Transporting information and energy simultaneously," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2008, pp. 1612–1616.
- [3] P. Grover and A. Sahai, "Shannon meets tesla: Wireless information and power transfer," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2010, pp. 2363–2367.
- [4] R. Zhang and C. K. Ho, "MIMO broadcasting for simultaneous wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 1989–2001, May 2013.
- [5] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, 1st Quart., 2017.
- [6] 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.
- [7] Q. Shi, W. Xu, J. Wu, E. Song, and Y. Wang, "Secure beamforming for MIMO broadcasting with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2841–2853, May 2015.
- [8] M. Moradikia, H. Bastami, A. Kuhestani, H. Behroozi, and L. Hanzo, "Cooperative secure transmission relying on optimal power allocation in the presence of untrusted relays, a passive eavesdropper and hardware impairments," *IEEE Access*, vol. 7, pp. 116942–116964, 2019.
- [9] M. Forouzes, P. Azmi, A. Kuhestani, and P. L. Yeoh, "Covert communication and secure transmission over untrusted relaying networks in the presence of multiple wardens," *IEEE Trans. Commun.*, vol. 68, no. 6, pp. 3737–3749, Jun. 2020.
- [10] M. Tatar Mamaghani and Y. Hong, "On the performance of low-altitude UAV-enabled secure AF relaying with cooperative jamming and SWIPT," *IEEE Access*, vol. 7, pp. 153060–153073, 2019.
- [11] X. B. Zhou and S. H. Yan, "Robust beamforming design for secure DM-based relay networks with self-sustained jammers," *IEEE Access*, vol. 7, 2019.
- [12] Y. Ren, T. Lv, H. Gao, and Y. Li, "Secure wireless information and power transfer in heterogeneous networks," *IEEE Access*, vol. 5, pp. 4967–4979, 2017.
- [13] B. Li, Z. Fei, Z. Chu, and Y. Zhang, "Secure transmission for heterogeneous cellular networks with wireless information and power transfer," *IEEE Syst. J.*, vol. 12, no. 4, pp. 3755–3766, Dec. 2018.
- [14] Z. Zhu, Z. Chu, Z. Wang, and I. Lee, "Outage constrained robust beamforming for secure broadcasting systems with energy harvesting," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7610–7620, Nov. 2016.
- [15] B. Li and Z. Fei, "Probabilistic-constrained robust secure transmission for energy harvesting over MISO channels," *Sci. China Inf. Sci.*, vol. 61, no. 2, Feb. 2018, Art. no. 022303.
- [16] J. Hu, S. Yan, F. Shu, and J. Wang, "Covert transmission with a self-sustained relay," *IEEE Trans. Wireless Commun.*, vol. 18, no. 8, pp. 4089–4102, Aug. 2019.
- [17] Y. Yang, Q. Li, W.-K. Ma, J. Ge, and P. C. Ching, "Cooperative secure beamforming for AF relay networks with multiple eavesdroppers," *IEEE Signal Process. Lett.*, vol. 20, no. 1, pp. 35–38, Jan. 2013.
- [18] A. Hasan and J. Andrews, "The guard zone in wireless ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 6, no. 3, pp. 897–906, Mar. 2007.
- [19] A. Mukherjee and A. L. Swindlehurst, "Detecting passive eavesdroppers in the MIMO wiretap channel," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Mar. 2012, pp. 2809–2812.
- [20] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.
- [21] H. Xing, K.-K. Wong, A. Nallanathan, and R. Zhang, "Wireless powered cooperative jamming for secrecy multi-AF relaying networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 7971–7984, Dec. 2016.
- [22] B. Clerckx, R. Zhang, R. Schober, D. W. K. Ng, D. I. Kim, and H. V. Poor, "Fundamentals of wireless information and power transfer: From RF energy harvester models to signal and system designs," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 1, pp. 4–33, Jan. 2019.
- [23] 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.
- [24] S. Boyd and L. Vandenberghe, *Convex Optimization*. New York, NY, USA: Cambridge Univ. Press, 2004.
- [25] K.-Y. Wang, A. M.-C. So, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "Outage constrained robust transmit optimization for multiuser MISO downlinks: Tractable approximations by conic optimization," *IEEE Trans. Signal Process.*, vol. 62, no. 21, pp. 5690–5705, Nov. 2014.
- [26] A. Alabbasi, Z. Rezk, and B. Shihada, "Energy efficient resource allocation for cognitive radios: A generalized sensing analysis," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2455–2469, May 2015.
- [27] A. Charnes and W. W. Cooper, "Programming with linear fractional functionals," *Nav. Res. Logistics Quart.*, vol. 9, nos. 3–4, pp. 181–186, Sep./Dec. 1962.
- [28] M. Grant and S. Boyd. (Jun. 2015). *CVX: MATLAB Software for Disciplined Convex Programming, Version 2.1*. [Online]. Available: <http://cvxr.com/cvx/>



ZHENTAO HU received the M.S. degree in application mathematics from Henan University, China, in 2006, and the Ph.D. degree in control science and engineering from Northwestern Polytechnical University, China, in 2010. He is currently an Associate Professor with the College of Computer and Information Engineering, Henan University. His research interests include target tracking, nonlinear estimation, and particle filtering.



LIN ZHOU received the M.S. degree in application mathematics from Henan University, China, in 2005, and the Ph.D. degree in control theory and control engineering from Northwestern Polytechnical University, China, in 2013. She is currently an Associate Professor with the College of Computer and Information Engineering, Henan University. Her research interests include information fusion and sensor management.



DONGDONG XIE received the B.S. degree in measurement and control technology and instruments from Henan University, Kaifeng, China, in 2017, where he is currently pursuing the M.S. degree. He is currently a Student Member of the Laboratory of Intelligent Technology and Systems, Henan University. His research interests include cognitive radio and robust beamforming.



MINGQI JIN is currently pursuing the bachelor's degree with the Department of Information and Computing Science, Northeastern University, China. Her research interest includes intelligent information processing.



JIFANG LI received the M.S. degree in control engineering from the Huazhong University of Science and Technology, China, in 2003, and the Ph.D. degree in power electronics and power drives from Shanghai Maritime University, China, in 2011. He is currently a Professor with the Electric Power College, North China University of Water Resources and Electric Power. His research interests include power electronics and power drives, new energy power generation, and smart grid.

...