Joint Optimization of Power Splitting and Beamforming in Energy Harvesting Cooperative Networks

Haiyan Guo, Zhen Yang, Yulong Zou*, *Senior Member, IEEE,*
Mujun Qian, Jia Zhu, and Lajos Hanzo*, *Fellow, IEEE*

Abstract—A new joint best relay and jammer selection (JBRJS) scheme is conceived for enhancing the physical layer security (PLS) of cooperative networks relying on multiple energy harvesting (EH) aided intermediate nodes, which accumulate energy based on the power splitting (PS) protocol. Specifically, we select the best intermediate node as the relay, whilst exploiting all the remaining nodes as friendly jammers. Furthermore, we investigate the joint optimization of the PS ratio and the relay-aided beamforming for maximizing the system's secrecy rate and present a full channel state information (CSI) based joint PS and beamforming (fJPSB) scheme as the optimal solution by converting the optimization problem formulated into a single-variable optimization problem. We also propose a partial-CSI based JPSB (pJPSB) method for the scenario where only the main link's CSI is available. Our numerical results show that the proposed JBRJS scheme beneficially enhances the PLS compared to the joint random relay and jammer selection (JRRJS) and to the pure best relay selection (PBRS) schemes. Moreover, the secrecy rate of the proposed fJPSB and pJPSB schemes is obviously higher than that of the fixed PS and beamforming (FPSB) method, and it further increases with the number of the relay's transmit antennas.

Index Terms—Physical layer security (PLS), energy harvesting (EH), relay selection, beamforming, jamming, power splitting (PS).

I. INTRODUCTION

TETHERLESS communication has become the norm. To expand the coverage of wireless networks, node cooperation is widely used. However, due to the broadcast nature of wireless links, the signal transmitted from the source to the legitimate receiver is prone to malicious eavesdropping. Physical layer security (PLS), which exploits the unique characteristics of wireless channels to guarantee confidential signal transfer, has been extensively explored [1]-[2]. There are two main techniques of improving the PLS of node cooperation networks, namely relaying and jamming, respectively. Specifically, the relaying scheme aims for enhancing the signal received at the destination [3]-[9], while the jamming scheme imposes the artificial noise on the eavesdropper [10]-[17].

Hence, sophisticated joint cooperative relaying and jamming methods have been proposed for further improving the PLS of wireless transmissions. In [18], an intermediate node was selected as the relay for delivering the source signal, and a pair of other intermediate nodes were exploited as friendly jammers for degrading the eavesdropper's reception. In [19], Wang *et al*. adopted a joint relay and jammer selection (JRJS) method for enhancing the PLS of amplify-and-forward (AF) networks and quantified its advantage over the best stand-alone relay selection scheme dispensing with jamming in terms of its secrecy throughput. In [20], Hui *et al*. proposed to group the intermediate nodes into relay sets as well as jammer sets, and investigated the relay/jammer selection problem by minimizing the secrecy outage probability (SOP). In [21], a relay and jammer selection policy was proposed for maximizing the relay activation ratio and minimizing the jammer activation ratio. In [22], a compressive survey of recent cooperative relaying and jamming techniques was presented. In [23], Nakai *et al*. proposed to select relay sets based on buffer states and introduced cooperative jamming into the proposed buffer-state-based relay system. In our earlier work [24], we proposed to select the single best relay and multiple jammers for improving the PLS of cooperative relay networks, and focused on the joint optimization of relay selection and power allocation for maximizing the secrecy rate. This work was later extended to a more general cooperative network, where multiple relays and jammers are exploited [25].

Another challenge in cooperative networks is minimizing the energy consumption of wireless nodes. In many wireless cooperative networks, the nodes are generally energy-

constrained and have no connections to power lines due to mobility or other constraints. Moreover, in many application scenarios, it is not convenient to replace the embedded battery of wireless nodes. As a result, the lifetime of the cooperative network is strictly limited by the energy budget of the nodes. Energy harvesting (EH), gleaning energy from radio-frequency (RF) signals, provides an attractive technique of recharging the nodes' batteries [26]-[27]. Compared to traditional solar, wind and thermal energy scavenging, RF-based EH is affected by the environment to a lesser extent and thus it is more stable. For making the application of far-field wireless power transfer promising, efficient rectenna design, waveform design, beamforming and power allocation have been studied to increase the end-to-end power transfer efficiency [28]-[29]. At the time of writing, there are two general EH protocols, namely time switching (TS) and power splitting (PS) [26] [30], respectively. The TS receivers switch between information processing and EH, while the PS receivers split the received signal energy into two parts for simultaneous signal processing and EH.

Recently, to improve security and to exploit EH for efficient energy transfer, numerous ideas have been presented on the relaying/jamming schemes, EH protocols, resource allocation and on the secrecy performance analysis of wirelessly-powered cooperative networks [31]-[39]. In [31]-[32], the authors proposed to use a wireless EH-aided relay based on the TS protocol for enhancing the information security, and optimized the resource allocation for maximizing the secrecy rate. In [33], the authors proposed an accumulate-and-jam protocol in which a friendly but energy-constrained jammer uses the energy harvested from the received RF signal to transmit artificial noise for securing the transmission. In [34]-[36], the artificial noise was exploited for drowning the eavesdroppers, whilst simultaneously powering the relays. In [37], the authors used multiple harvest-and-jam helpers for securing the AF relaying network and jointly optimized the artificial noise covariance matrix and the AF beamforming matrix. In [38]-[39], an EH relay and an EH jammer were relied upon for securing the source-destination transmission. Specifically, in [38], the secrecy performance was analyzed for four different relay selection schemes, while in [39] the optimal TS ratio was derived for maximizing the secrecy rate.

Against this backdrop, we investigate the security of a cooperative wireless network, where the source transmits confidential information to the destination aided by multiple energy-constrained intermediate nodes in the presence of an eavesdropper. The intermediate nodes are EH-enabled and harvest energy from the RF signals transmitted by the source based on the PS protocol. In contrast to [38]-[39] and our previous work [24]-[25], the relay and jammers are equipped with multiple antennas chosen for beamforming. To benefit from both relaying and jamming, we propose a new joint best relay and jammer selection (JBRJS) scheme for improving the security, and then maximize the secrecy rate by the joint optimization of the PS ratio and the relay's beamformer. The main contributions of this paper are summarized as follows.

1) We conceive a new JBRJS scheme for cooperative networks relying on multiple EH aided intermediate nodes

for securing the source-destination (SD) link. Specifically, we select the specific intermediate node, which receives the highest power as the relay for forwarding the source message, whilst harnessing the remaining nodes as the friendly jammers to drown out the eavesdroppers. Both the relay and the jammers first harvest energy from the RF signal transmitted by the source and then transmit both the source signal and jamming signals relying on the accumulated energy using beamforming. This is in contrast to [37] where only the jammers are EH-aided and the relay has a constant power supply. It is noted that the relay only uses a specific portion of the harvested energy based on the PS protocol for its transmission, while the jammers use all the harvested energy to send artificial noise. This scenario is different from our previous work [24] where each intermediate node is equipped with a single antenna and is not EH-enabled. Furthermore, the relay selection scheme in [24] is also different.

2) We investigate the joint optimization of the PS ratio and the relay-based beamforming for the sake of maximizing the secrecy rate as well as propose a full-CSI based joint PS and beamforming (fJPSB) method as the optimal solution under the idealized simplifying assumption that the channel state information (CSI) of both the main and wiretap links is perfectly known[1]. Specifically, we convert the joint optimization problem formulated into a single-variable optimization problem, which is the algebraic expression of the PS ratio by exploiting the relationship between the optimal beamforming vector and the PS ratio.

3) Upon considering the scenario in which only the main link's CSI is known, we present a partial-CSI based JPSB (pJPSB) method for maximizing the attainable rate of the main link and derive the optimal closed-form solution.

The outline of the paper is as follows. In Section II, the system model is introduced and our secrecy rate analysis is presented. Section III investigates the joint optimization of the PS ratio as well as of the relay beamforming, and presents both our fJPSB and pJPSB methods, respectively. Our simulation results are provided in Section IV, while Section V concludes the paper.

Notation: Bold letters are used for the vectors or matrices; $(\cdot)^{\mathrm{T}}$ represents the transpose and $(\cdot)^*$ represents the conjugate vector; $(\cdot)^{\mathrm{H}}$ denotes the conjugate transpose; $||\cdot||$ is the l_2 norm of a vector; $[\cdot]^+$ is defined as max $\{\cdot, 0\}$; $\lambda_{max}(\cdot)$ denotes the largest eigenvalue of a matrix and $\boldsymbol{v}_{max}(\cdot)$ denotes the eigenvector associated with $\lambda_{max}(\cdot)$; $\lambda_{gen}(\cdot)$ defines an eigenvalue of a matrix and $\boldsymbol{u}_{gen}(\cdot)$ denotes an eigenvector of a matrix; $\boldsymbol{I}$ represents the identity matrix.

II. SYSTEM MODEL AND SECRECY RATE ANALYSIS

Let us consider a wireless network consisting of a source S, a legitimate destination D, an eavesdropper E and K

---

[1]In the scenario where a legal user in the wireless network is captured by Trojan and slaved as an eavesdropper to tap the signal transmission, the instantaneous CSI of the eavesdropping link may be available. For another example, in a scenario where a single active eavesdropper is registered in the wireless network as a subscribed user and exchanges signaling messages with the source and intermediate nodes, the global instantaneous CSI of the eavesdropper may be known.

EH-enabled intermediate nodes. The intermediate nodes are energy-constrained and are capable of harvesting energy from the RF signals transmitted by the source. In the network, S, D and E are single-antenna nodes while all the intermediate nodes are equipped with multiple antennas. We propose to select the best intermediate node as the relay R for forwarding the source signal, whilst harnessing the remaining intermediate nodes as the jammers $J_1, J_2, ..., J_{K-1}$ to impose AN for drowning the eavesdropper, as shown in Fig.1. We assume that the relay applies the decode-and-forward (DF) protocol. It is assumed that there is no direct link from S to D due to the long distance, while there is a direct link between S and E since E can be intentionally closer to S for tapping the transmission.

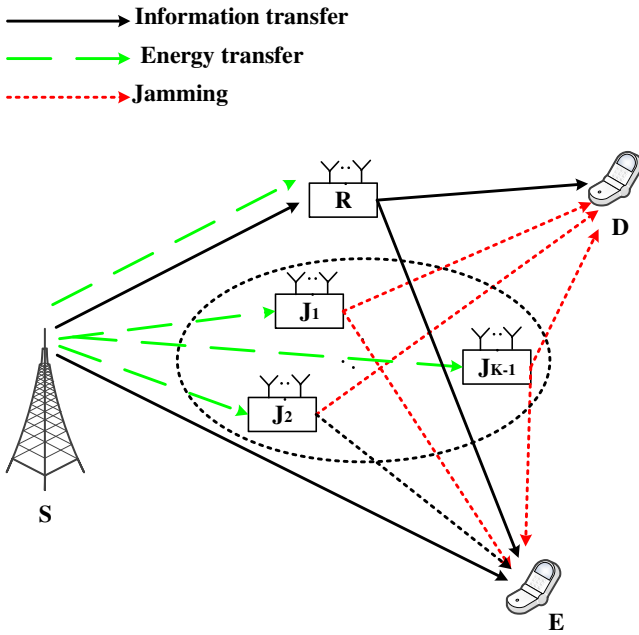In the first transmission phase, S transmits a signal s,

Fig. 1. A wireless network consisting of one source, one destination, one eavesdropper and multiple EH-enabled intermediate nodes equipped with multiple antennas.

which has unity normalized power, given the power P_s and the rate R_d. The signal received by the kth intermediate node ($k = 1, 2, ..., K$) can be expressed as

$$y_k = \sqrt{P_s}(\boldsymbol{w}_k^r)^{\mathrm{T}}\boldsymbol{h}_{sk}s + (\boldsymbol{w}_k^r)^{\mathrm{T}}\boldsymbol{n}_{ka} \quad (1)$$

where $\boldsymbol{h}_{sk} = [h_{sk}^1 \quad h_{sk}^2 \quad ... \quad h_{sk}^{M_k}]^{\mathrm{T}}$ is a $(M_k \times 1)$-element vector denoting the channel between S and the kth intermediate node, h_{sk}^m is the fading coefficient of the channel between S to the mth receive antenna (RA) of the kth intermediate node, M_k is the number of antennas used by the kth intermediate node, $\boldsymbol{w}_k^r$ is the relay's receive beamforming (BF) matrix conditioned for receiving the source signal, $\boldsymbol{n}_{ka} = [n_{ka}^1, n_{ka}^2, ..., n_{ka}^{M_k}]^{\mathrm{T}}$ is a $(M_k \times 1)$-element vector composed of the additive white Gaussian noise (AWGN) received by each RA, and finally, $n_{ka}^m \in \mathcal{CN}(0, \delta_n^2)$ denotes the AWGN received at the mth RA of the kth intermediate node. For notational convenience, we use $n_{ka} \in \mathcal{CN}(0, \delta_n^2)$ uniformly

for $n_{ka}^m \in \mathcal{CN}(0, \delta_n^2)$.

The relay uses the maximal ratio combining (MRC) method of [40] to perform BF for receiving the source signal, that is, $\boldsymbol{w}_k^r = \frac{\boldsymbol{h}_{sk}^*}{||\boldsymbol{h}_{sk}||}$. Then, the received signal y_k becomes

$$y_k = \sqrt{P_s}||\boldsymbol{h}_{sk}||s + \frac{1}{||\boldsymbol{h}_{sk}||}\boldsymbol{h}_{sk}^{\mathrm{H}}\boldsymbol{n}_{ka}. \quad (2)$$

The signal received at E is given by

$$y_e^{(1)} = \sqrt{P_s}h_{se}s + n_e^{(1)} \quad (3)$$

where h_{se} is the fading coefficient of the S to E channel, and $n_e^{(1)} \in \mathcal{CN}(0, \delta_n^2)$ represents the AWGN received at E.

We select the specific intermediate node as the relay which receives the highest power. This implies that the relay is most likely to successfully decode the source signal. The best relay selection criterion can be obtained from (2) as

$$R = \arg\max_k ||\boldsymbol{h}_{sk}||. \quad (4)$$

The remaining intermediate nodes are exploited as the jammers to send artificial noise.

The received signal of R is split into two parts based on the PS protocol: a fraction ρ is used for EH and $(1 - \rho)$ is used for signal processing, yielding

$$y_{R,h} = \sqrt{\rho P_s}||\boldsymbol{h}_{sR}||s + \sqrt{\rho}\frac{1}{||\boldsymbol{h}_{sR}||}\boldsymbol{h}_{sR}^{\mathrm{H}}\boldsymbol{n}_{Ra} \quad (5)$$

and

$$y_{R,p} = \sqrt{(1-\rho)P_s}||\boldsymbol{h}_{sR}||s + \sqrt{1-\rho}\frac{1}{||\boldsymbol{h}_{sR}||}\boldsymbol{h}_{sR}^{\mathrm{H}}\boldsymbol{n}_{Ra} + n_{Rc}, \quad (6)$$

where $\boldsymbol{h}_{sR}$ denotes the channel between S and R, ρ is the PS ratio, and $n_{Rc} \in \mathcal{CN}(0, \zeta\delta_n^2)$ is the AWGN incurred by the conversion of the RF signal to the baseband signal. Then, the energy harvested from $y_{R,h}$ is given by

$$E_R = \eta\rho P_s||\boldsymbol{h}_{sR}||^2\frac{T}{2}, \quad (7)$$

where $\eta \in [0, 1]$ denotes the energy-conversion efficiency and $\frac{T}{2}$ is the first half of the time block. Thus, the relay's transmit power is given by

$$P_R = \eta\rho P_s||\boldsymbol{h}_{sR}||^2. \quad (8)$$

For each jammer, the total received signal is used for EH since no source decoding is needed. Thus, the energy harvested at the ith jammer J_i can be computed as

$$E_J^i = \eta P_s||\boldsymbol{h}_{sJ_i}||^2\frac{T}{2}, \quad (9)$$

where $\boldsymbol{h}_{sJ_i}$ denotes the fading coefficient between S and the ith jammer J_i. Then, the transmit power of J_i is given by

$$P_{J_i} = \eta P_s||\boldsymbol{h}_{sJ_i}||^2. \quad (10)$$

In the second transmission phase, R transmits the re-encoded source signal by exploiting BF, and each jammer sends artificial noise to interfere with E. Let us denote the relay's transmit BF vector as $\boldsymbol{w}_R^t = [w_1 \quad w_2 \quad ... \quad w_{M_R}]^{\mathrm{T}}$ and the artificial noise transmitted by J_i as $\boldsymbol{z}_i = [z_i^1 \quad z_i^2 \quad ... \quad z_i^{M_{J_i}}]^{\mathrm{T}}$, where M_R and M_{J_i} are the number

of transmit antennas (TAs) used at R and J_i, respectively. Then, the signal received at the destination D is obtained as

$$y_d = \sqrt{P_R}(\boldsymbol{w}_R^t)^{\mathrm{T}}\boldsymbol{h}_{Rd}s + \sum_{i=1}^{K-1}\sqrt{P_{J_i}}(\boldsymbol{z}_i)^{\mathrm{T}}\boldsymbol{h}_{J_id} + n_d, \quad (11)$$

where $\boldsymbol{h}_{Rd} = [h_{Rd}^1 \quad h_{Rd}^2 \quad ... \quad h_{Rd}^{M_R}]^{\mathrm{T}}$ and $\boldsymbol{h}_{J_id} = [h_{J_id}^1 \quad h_{J_id}^2 \quad ... \quad h_{J_id}^{M_{J_i}}]^{\mathrm{T}}$ denote the channel spanning from R to D and the channel from J_i to D, respectively. Furthermore, h_{Rd}^m is the channel coefficient between the mth TA of R and D, while $h_{J_id}^m$ is that between the mth TA of J_i and D, and $\boldsymbol{z}_i$ denotes the artificial noise transmitted by J_i. Similarly, the signal received by E is given by

$$y_e^{(2)} = \sqrt{P_R}(\boldsymbol{w}_R^t)^{\mathrm{T}}\boldsymbol{h}_{Re}s + \sum_{i=1}^{K-1}\sqrt{P_{J_i}}(\boldsymbol{z}_i)^{\mathrm{T}}\boldsymbol{h}_{J_ie} + n_e, \quad (12)$$

where $\boldsymbol{h}_{Re} = [h_{Re}^1 \quad h_{Re}^2 \quad ... \quad h_{Re}^{M_R}]^{\mathrm{T}}$ and $\boldsymbol{h}_{J_ie} = [h_{J_ie}^1 \quad h_{J_ie}^2 \quad ... \quad h_{J_ie}^{M_{J_i}}]^{\mathrm{T}}$ denote the channel spanning from R to E and from J_i to E, respectively, while h_{Re}^m is the coefficient between the mth TA of R and E, and $h_{J_ie}^m$ is the coefficient between the mth TA of J_i and E. We design $\boldsymbol{z}_i$ as a vector in the null-space of $\boldsymbol{h}_{J_id}$, that is, $(\boldsymbol{z}_i)^{\mathrm{T}}\boldsymbol{h}_{J_id} = 0$. Thus, by substituting (8) into (11), we can express (11) as

$$y_d = \sqrt{\eta\rho P_s}||\boldsymbol{h}_{sR}||(\boldsymbol{w}_R^t)^{\mathrm{T}}\boldsymbol{h}_{Rd}s + n_d. \quad (13)$$

Similarly, by combining (8), (10) and (12), we obtain (12) as

$$y_e^{(2)}=\sqrt{\eta\rho P_s}||\boldsymbol{h}_{sR}||(\boldsymbol{w}_R^t)^{\mathrm{T}}\boldsymbol{h}_{Re}+\sum_{i=1}^{K-1}\sqrt{\eta P_s}||\boldsymbol{h}_{sJ_i}||(\boldsymbol{z}_i)^{\mathrm{T}}\boldsymbol{h}_{J_ie}+n_e. \quad (14)$$

Upon defining

$$\boldsymbol{z}^{\mathrm{all}} = [||\boldsymbol{h}_{sJ_1}||(\boldsymbol{z}_1)^{\mathrm{T}} \quad ||\boldsymbol{h}_{sJ_2}||(\boldsymbol{z}_2)^{\mathrm{T}} \quad ... \quad ||\boldsymbol{h}_{sJ_{K-1}}||(\boldsymbol{z}_{N-1})^{\mathrm{T}}]^{\mathrm{T}}$$

and

$$\boldsymbol{h}_{Je}^{\mathrm{all}} = [(\boldsymbol{h}_{J_1e})^{\mathrm{T}} \quad (\boldsymbol{h}_{J_2e})^{\mathrm{T}} \quad ... \quad (\boldsymbol{h}_{J_{K-1}e})^{\mathrm{T}}]^{\mathrm{T}},$$

we can rewrite (14) as

$$y_e^{(2)}=\sqrt{\eta\rho P_s}||\boldsymbol{h}_{sR}||(\boldsymbol{w}_R^t)^{\mathrm{T}}\boldsymbol{h}_{Re} + \sqrt{\eta P_s}(\boldsymbol{z}^{\mathrm{all}})^{\mathrm{T}}\boldsymbol{h}_{Je}^{\mathrm{all}} + n_e. \quad (15)$$

From (3), (13) and (15), we can obtain the instantaneous signal-to-noise ratio (SNR) at D as

$$\gamma_d(\rho, \boldsymbol{w}_R^t) = \frac{\eta\rho P_s}{\delta_n^2}||\boldsymbol{h}_{sR}||^2(\boldsymbol{w}_R^t)^{\mathrm{H}}\boldsymbol{h}_{Rd}\boldsymbol{h}_{Rd}^{\mathrm{H}}\boldsymbol{w}_R^t \quad (16)$$

and the instantaneous SNR at E as

$$\gamma_e(\rho, \boldsymbol{w}_R^t) = \frac{\eta\rho P_s||\boldsymbol{h}_{sR}||^2(\boldsymbol{w}_R^t)^{\mathrm{H}}\boldsymbol{h}_{Re}\boldsymbol{h}_{Re}^{\mathrm{H}}\boldsymbol{w}_R^t}{\delta_n^2 + \eta P_s(\boldsymbol{z}^{\mathrm{all}})^{\mathrm{H}}\boldsymbol{h}_{Je}^{\mathrm{all}}(\boldsymbol{h}_{Je}^{\mathrm{all}})^{\mathrm{H}}\boldsymbol{z}^{\mathrm{all}}} + \frac{P_s|h_{se}|^2}{\delta_n^2}. \quad (17)$$

Then, the achievable rate at D and E is given by

$$C_d = \frac{1}{2}\log_2[1 + \gamma_d(\rho, \boldsymbol{w}_R^t)] \quad (18)$$

and

$$C_e = \frac{1}{2}\log_2[1 + \gamma_e(\rho, \boldsymbol{w}_R^t)], \quad (19)$$

respectively. Thus, combining (18) and (19), we can obtain the achievable secrecy rate as

$$C_s = (C_d - C_e)^+ = \frac{1}{2}\left\{\log_2[\frac{1 + \gamma_d(\rho, \boldsymbol{w}_R^t)}{1 + \gamma_e(\rho, \boldsymbol{w}_R^t)}]\right\}^+. \quad (20)$$

III. JOINT OPTIMIZATION OF POWER SPLITTING AND BEAMFORMING

In this section, we jointly optimize the PS ratio ρ and the BF weight vector $\boldsymbol{w}_R^t$ to enhance the security of the proposed JBRJS scheme. We first propose the fJPSB method for the full-CSI case, where the CSI of both the main link and of the wiretap link is known. For instance, in a scenario where a legitimate user is captured by a Trojan and slaved as an eavesdropper, the CSI of the eavesdropper may be inferred. Then, upon considering the case where only the desired channel's CSI is known, we present the pJPSB method.

A. fJPSB

In this subsection, we aim for maximizing the secrecy rate C_s by jointly optimizing ρ and $\boldsymbol{w}_R^t$ under the full CSI assumption. The optimization problem is formulated as

$$[\rho_{opt}^{f\mathrm{JPSB}}, (\boldsymbol{w}_R^t)_{opt}^{f\mathrm{JPSB}}] = \arg \max_{\rho, \boldsymbol{w}_R^t}\log_2\frac{1 + \gamma_d(\rho, \boldsymbol{w}_R^t)}{1 + \gamma_e(\rho, \boldsymbol{w}_R^t)}$$
$$\mathrm{s.t.} \quad \frac{1}{2}\log_2(1 + \frac{(1-\rho)P_s||\boldsymbol{h}_{sR}||^2}{(1-\rho)\delta_n^2 + \zeta\delta_n^2}) \geq R_d$$
$$(\boldsymbol{w}_R^t)^{\mathrm{H}}\boldsymbol{w}_R^t = 1 \quad (21)$$
$$0 \leq \rho \leq 1.$$

The constraint $\frac{1}{2}\log_2(1 + \frac{(1-\rho)P_s||\boldsymbol{h}_{sR}||^2}{(1-\rho)\delta_n^2 + \zeta\delta_n^2}) \geq R_d$ implies that the relay can successfully decode the source signal from $y_{R,p}$.

Let us now introduce the notation of $\epsilon_e = (\boldsymbol{z}^{\mathrm{all}})^{\mathrm{H}}\boldsymbol{h}_{Je}^{\mathrm{all}}(\boldsymbol{h}_{Je}^{\mathrm{all}})^{\mathrm{H}}\boldsymbol{z}^{\mathrm{all}}$, $\alpha = \delta_n^2(\delta_n^2 + \eta P_s\epsilon_e)$, $\beta = P_s||\boldsymbol{h}_{se}||^2(\delta_n^2 + \eta P_s\epsilon_e)$, $\xi_1 = \delta_n^2\eta P_s||\boldsymbol{h}_{sR}||^2$, $\xi_2 = \eta^2 P_s^2\epsilon_e||\boldsymbol{h}_{sR}||^2$, $\boldsymbol{H}_{Rd} = \boldsymbol{h}_{Rd}\boldsymbol{h}_{Rd}^{\mathrm{H}}$ and $\boldsymbol{H}_{Re} = \boldsymbol{h}_{Re}\boldsymbol{h}_{Re}^{\mathrm{H}}$. By substituting (16) and (17) into (21), we can rewrite Problem (21) equivalently as

$$[\rho_{opt}^{f\mathrm{JPSB}}, (\boldsymbol{w}_R^t)_{opt}^{f\mathrm{JPSB}}]=\arg \max_{\rho, \boldsymbol{w}_R^t}\frac{1 + \gamma_d(\rho, \boldsymbol{w}_R^t)}{1 + \gamma_e(\rho, \boldsymbol{w}_R^t)}$$
$$=\arg \max_{\rho, \boldsymbol{w}_R^t}\frac{\alpha+(\xi_1+\xi_2)\rho(\boldsymbol{w}_R^t)^{\mathrm{H}}\boldsymbol{H}_{Rd}\boldsymbol{w}_R^t}{(\alpha+\beta)+\xi_1\rho(\boldsymbol{w}_R^t)^{\mathrm{H}}\boldsymbol{H}_{Re}\boldsymbol{w}_R^t}$$
$$=\arg \max_{\rho, \boldsymbol{w}_R^t}\frac{(\boldsymbol{w}_R^t)^{\mathrm{H}}(\frac{\alpha}{\alpha+\beta}\boldsymbol{I}+\frac{\xi_1+\xi_2}{\alpha+\beta}\rho\boldsymbol{H}_{Rd})\boldsymbol{w}_R^t}{(\boldsymbol{w}_R^t)^{\mathrm{H}}(\boldsymbol{I}+\frac{\xi_1}{\alpha+\beta}\rho\boldsymbol{H}_{Re})\boldsymbol{w}_R^t}$$
$$\mathrm{s.t.} \quad 0 \leq \rho \leq \min(1, \rho_{th})$$
$$(\boldsymbol{w}_R^t)^{\mathrm{H}}\boldsymbol{w}_R^t = 1 \quad (22)$$

where

$$\rho_{th} = 1 - \frac{\zeta}{\frac{P_s||\boldsymbol{h}_{sR}||^2}{(2^{2R_d}-1)\delta_n^2} - 1}. \quad (23)$$

The optimal solution $(\boldsymbol{w}_R^t)_{opt}^{f\mathrm{JPSB}}$ of Problem (22) is given by

$$(\boldsymbol{w}_R^t)_{opt}^{f\mathrm{JPSB}}=\boldsymbol{v}_{max}[(\boldsymbol{I}+\frac{\xi_1}{\alpha+\beta}\rho\boldsymbol{H}_{Re})^{-1}(\frac{\alpha}{\alpha+\beta}\boldsymbol{I}+\frac{\xi_1+\xi_2}{\alpha+\beta}\rho\boldsymbol{H}_{Rd})], \quad (24)$$

Correspondingly, when we have $\boldsymbol{w}_R^t = (\boldsymbol{w}_R^t)_{opt}^{f\mathrm{JPSB}}$, the term $\frac{1+\gamma_d(\rho, \boldsymbol{w}_R^t)}{1+\gamma_e(\rho, \boldsymbol{w}_R^t)}$ achieves its largest value, which is given as (25) at the top of the following page.

Then, Problem (22) is transformed to Problem (26) which is stated at the top of the following page.

Upon defining $(\boldsymbol{I} - \frac{\frac{\rho\xi_1}{\alpha+\beta}\boldsymbol{H}_{Re}}{1+\frac{\rho\xi_1}{\alpha+\beta}||\boldsymbol{h}_{Re}||^2})^{\frac{1}{2}} = \boldsymbol{U}\Lambda^{\frac{1}{2}}\boldsymbol{U}^{\mathrm{H}}$ where

$$\frac{1+\gamma_d(\rho,(\boldsymbol{w}_R^t)_{opt}^{f\mathrm{JPSB}})}{1+\gamma_e(\rho,(\boldsymbol{w}_R^t)_{opt}^{f\mathrm{JPSB}})} = \lambda_{max}[(\boldsymbol{I}+\frac{\xi_1}{\alpha+\beta}\rho\boldsymbol{H}_{Re})^{-1}(\frac{\alpha}{\alpha+\beta}\boldsymbol{I}+\frac{\xi_1+\xi_2}{\alpha+\beta}\rho\boldsymbol{H}_{Rd})]. \tag{25}$$

$$\rho_{opt}^{f\mathrm{JPSB}} = \arg\max_{\rho}\lambda_{max}[(\boldsymbol{I}+\frac{\xi_1}{\alpha+\beta}\rho\boldsymbol{H}_{Re})^{-1}(\frac{\alpha}{\alpha+\beta}\boldsymbol{I}+\frac{\xi_1+\xi_2}{\alpha+\beta}\rho\boldsymbol{H}_{Rd})]$$
$$\text{s.t.} \quad 0 \leq \rho \leq \min(1,\rho_{th}). \tag{26}$$

$\boldsymbol{U}=[\boldsymbol{u}_1\boldsymbol{u}_2\cdots\boldsymbol{u}_M]$ is a square matrix, whose columns are the eigenvectors of $(\boldsymbol{I}-\frac{\frac{\rho\xi_1}{\alpha+\beta}\boldsymbol{H}_{Re}}{1+\frac{\rho\xi_1}{\alpha+\beta}||\boldsymbol{h}_{Re}||^2})^{\frac{1}{2}}$ and $\Lambda^{\frac{1}{2}}$ is a diagonal matrix, whose diagonal elements are the corresponding eigenvalues, we arrive at

$$\lambda_{max}[(\boldsymbol{I}+\frac{\xi_1}{\alpha+\beta}\rho\boldsymbol{H}_{Re})^{-1}(\frac{\alpha}{\alpha+\beta}\boldsymbol{I}+\frac{\xi_1+\xi_2}{\alpha+\beta}\rho\boldsymbol{H}_{Rd})] \tag{27}$$
$$= \frac{\alpha}{\alpha+\beta}+\frac{1}{2}(||\boldsymbol{x}||^2-||\boldsymbol{y}||^2+\sqrt{(||\boldsymbol{x}||^2+||\boldsymbol{y}||^2)^2-4||\boldsymbol{y}^{\mathrm{H}}\boldsymbol{x}||^2}),$$

where $\boldsymbol{x}=\sqrt{\frac{(\xi_1+\xi_2)\rho}{\alpha+\beta}}\boldsymbol{U}\Lambda^{\frac{1}{2}}\boldsymbol{U}^{\mathrm{H}}\boldsymbol{h}_{Rd}$ and $\boldsymbol{y}=\sqrt{\frac{\alpha\xi_1\rho}{(\alpha+\beta+\rho\xi_1||\boldsymbol{h}_{Re}||^2)(\alpha+\beta)}}\boldsymbol{h}_{Re}$. See Appendix A.

After a few further steps, we can derive the expression of $||\boldsymbol{x}||^2$ as

$$||\boldsymbol{x}||^2=\frac{(\xi_1+\xi_2)\rho||\boldsymbol{h}_{Re}^{\mathrm{H}}\boldsymbol{h}_{Rd}||^2}{[\rho\xi_1||\boldsymbol{h}_{Re}||^2+(\alpha+\beta)]||\boldsymbol{h}_{Re}||^2}+\frac{(\xi_1+\xi_2)\rho}{\alpha+\beta}\sum_{m=2}^{M_R}||\boldsymbol{u}_m^{\mathrm{H}}\boldsymbol{h}_{Rd}||^2. \tag{28}$$

The derivation details are in Appendix B.

By substituting the expressions of $\boldsymbol{x}$ and $\boldsymbol{y}$ into $\boldsymbol{y}^{\mathrm{H}}\boldsymbol{x}$, we obtain $||\boldsymbol{y}^{\mathrm{H}}\boldsymbol{x}||^2$ which is given by (29) at the top of the following page.

Upon using (B.3) and (B.4) stated in Appendix B, (29) can be expressed as

$$||\boldsymbol{y}^{\mathrm{H}}\boldsymbol{x}||^2 = \frac{\alpha\xi_1(\xi_1+\xi_2)\rho^2}{(\alpha+\beta)(\alpha+\beta+\xi_1\rho||\boldsymbol{h}_{Re}||^2)^2}||\boldsymbol{h}_{Re}^{\mathrm{H}}\boldsymbol{h}_{Rd}||^2. \tag{30}$$

Upon defining $||\boldsymbol{h}_{Re}||^2=e$, $||\boldsymbol{h}_{Re}^H\boldsymbol{h}_{Rd}||^2=c$, $\sum_{m=2}^{M_R}||\boldsymbol{u}_m^H\boldsymbol{h}_{Rd}||^2=\mu$, $\theta=\frac{(\xi_1+\xi_2)c}{e}-\frac{\alpha\xi_1 e}{\alpha+\beta}$ and $f_1(\rho)=\frac{\rho}{\alpha+\beta+\rho\xi_1 e}$ which is a function of ρ, we can rewrite $||\boldsymbol{x}||^2$, $||\boldsymbol{y}||^2$ and $||\boldsymbol{y}^{\mathrm{H}}\boldsymbol{x}||^2$ as

$$||\boldsymbol{x}||^2 = \frac{c}{e}(\xi_1+\xi_2)f_1(\rho)+\frac{\xi_1+\xi_2}{\alpha+\beta}\mu\rho, \tag{31}$$

$$||\boldsymbol{y}||^2 = \frac{\alpha\xi_1 e}{\alpha+\beta}f_1(\rho) \tag{32}$$

and

$$||\boldsymbol{y}^H\boldsymbol{x}||^2 = \frac{\xi_1+\xi_2}{\alpha+\beta}\alpha\xi_1 c f_1^2(\rho). \tag{33}$$

To simplify the expression, we define $f_2(\rho)=[\theta+\frac{2\alpha\xi_1 e}{\alpha+\beta}+\frac{\xi_1+\xi_2}{\alpha+\beta}(\alpha+\beta+\xi_1 e\rho)\mu]^2$, $f_3(\rho)=\sqrt{f_2(\rho)-4\frac{\xi_1+\xi_2}{\alpha+\beta}\alpha\xi_1 c}$ and

$f_4(\rho)=\frac{\xi_1+\xi_2}{2(\alpha+\beta)}\mu\rho$. By substituting (31), (32) and (33) into (27), we can express Problem (26) as

$$\rho_{opt}^{f\mathrm{JPSB}} = \arg\max_{\rho}g(\rho)=\frac{\alpha}{\alpha+\beta}+\frac{1}{2}f_1(\rho)[\theta+f_3(\rho)]+f_4(\rho)$$
$$\text{s.t.} \quad 0 \leq \rho \leq \min(1,\rho_{th}). \tag{34}$$

The details are given in Appendix C.

Since it is a challenge to obtain a closed-form solution of Problem (34), we apply the exhaustive search method to compute the solution $\rho_{opt}^{f\mathrm{JPSB}}$. The exhaustive search method will be shown to be effective by our numerical results. Then, we can obtain the optimal BF weight vector $\boldsymbol{w}_{opt}^{f\mathrm{JPSB}}$ as (35) stated at the top of the following page.

Finally, we provide the computational complexity analysis of the proposed fJPSB scheme. To simplify the expressions, we assumed that $M_R=M_{J_i}=M$. Upon exploiting $\epsilon_e=(\boldsymbol{z}^{\mathrm{all}})^{\mathrm{H}}\boldsymbol{h}_{Je}^{\mathrm{all}}(\boldsymbol{h}_{Je}^{\mathrm{all}})^{\mathrm{H}}\boldsymbol{z}^{\mathrm{all}}=||(\boldsymbol{z}^{\mathrm{all}})^{\mathrm{H}}\boldsymbol{h}_{Je}^{\mathrm{all}}||^2$, $\alpha=\delta_n^2(\delta_n^2+\eta P_s\epsilon_e)$ and $\beta=P_s||\boldsymbol{h}_{se}||^2(\delta_n^2+\eta P_s\epsilon_e)$, we can quantify the complexity of deriving of α and β, which is on the order of $O(KM)$. Then, upon combining $\xi_1=\delta_n^2\eta P_s||\boldsymbol{h}_{sR}||^2$, $\xi_2=\eta^2 P_s^2\epsilon_e||\boldsymbol{h}_{sR}||^2$, $\boldsymbol{H}_{Re}=\boldsymbol{h}_{Re}\boldsymbol{h}_{Re}^{\mathrm{H}}$, $(\boldsymbol{I}-\frac{\frac{\rho\xi_1}{\alpha+\beta}\boldsymbol{H}_{Re}}{1+\frac{\rho\xi_1}{\alpha+\beta}||\boldsymbol{h}_{Re}||^2})^{\frac{1}{2}}=\boldsymbol{U}\Lambda^{\frac{1}{2}}\boldsymbol{U}^{\mathrm{H}}$, $\boldsymbol{U}=[\boldsymbol{u}_1\boldsymbol{u}_2\cdots\boldsymbol{u}_M]$ and $\sum_{m=2}^{M_R}||\boldsymbol{u}_m^H\boldsymbol{h}_{Rd}||^2=\mu$, the computational complexity of deriving μ is approximately on the order of $O(KM)+O(M)+O(M^2)+O(M^3)\approx O(KM)+O(M^3)$. Since $\xi_1,\xi_2,\alpha,\beta,e,c$ and θ are the same for each candidate ρ, their values can be stored in memory for speeding up the computation of the optimization function $g(\rho)=\frac{\alpha}{\alpha+\beta}+\frac{1}{2}f_1(\rho)[\theta+f_3(\rho)]+f_4(\rho)$ stated in Problem (34) for each ρ. Upon defining σ as the step size used in the exhaustive search method, we can readily show that the computational complexity of solving Problem (34) is approximately on the order of $O(1/\sigma)+O(KM)+O(M^3)$. From Equation (35), we can show that the computational complexity of deriving $\boldsymbol{w}_{opt}^{f\mathrm{JPSB}}$ by using $\rho_{opt}^{f\mathrm{JPSB}}$ is approximately $O(M^3)$. Thus, the computational complexity of the proposed fJPSB scheme is approximately $O(1/\sigma)+O(KM)+O(M^3)$.

B. pJPSB

In this subsection, we present the joint optimization of the PS ratio and the BF weight vector for the scenario, where the CSI of the wiretap channel is not available. Since only the CSI of the main link is known, we aim for maximizing the achievable rate at the destination D. The optimization problem

$$||\boldsymbol{y}^{\mathrm{H}}\boldsymbol{x}||^2 = \frac{\alpha\xi_1\rho}{(\alpha+\beta+\rho\xi_1||\boldsymbol{h}_{Re}||^2)(\alpha+\beta)}||\sqrt{\frac{(\xi_1+\xi_2)\rho}{\rho\xi_1||\boldsymbol{h}_{Re}||^2+\alpha+\beta}}\boldsymbol{u}_1^{\mathrm{H}}\boldsymbol{h}_{Rd}(\boldsymbol{h}_{Re})^{\mathrm{H}}\boldsymbol{u}_1 + \sqrt{\frac{(\xi_1+\xi_2)\rho}{\alpha+\beta}}\sum_{m=2}^{M_R}(\boldsymbol{u}_m^{\mathrm{H}}\boldsymbol{h}_{Rd}(\boldsymbol{h}_{Re})^{\mathrm{H}}\boldsymbol{u}_m)||^2 \quad (29)$$

$$\boldsymbol{w}_{opt}^{f\mathrm{JPSB}} = \boldsymbol{v}_{max}[(\boldsymbol{I}+\frac{\xi_1}{\alpha+\beta}\rho_{opt}^{f\mathrm{JPSB}}\boldsymbol{H}_{Re})^{-1}(\frac{\alpha}{\alpha+\beta}\boldsymbol{I}+\frac{\xi_1+\xi_2}{\alpha+\beta}\rho_{opt}^{f\mathrm{JPSB}}\boldsymbol{H}_{Rd})] \quad (35)$$

is stated as

$$[\rho_{opt}^{p\mathrm{JPSB}},(\boldsymbol{w}_R^t)_{opt}^{p\mathrm{JPSB}}] = \arg \max_{\rho,\boldsymbol{w}_R^t}\log_2[1+\gamma_d(\rho,\boldsymbol{w}_R^t)]$$
$$\text{s.t.}\quad 0\le\rho\le\min(1,\rho_{th})$$
$$(\boldsymbol{w}_R^t)^{\mathrm{H}}\boldsymbol{w}_R^t = 1, \quad (36)$$

which can be equivalently rewritten as

$$[\rho_{opt}^{p\mathrm{JPSB}},(\boldsymbol{w}_R^t)_{opt}^{p\mathrm{JPSB}}] = \arg \max_{\rho,\boldsymbol{w}_R^t}\rho(\boldsymbol{w}_R^t)^{\mathrm{H}}\boldsymbol{h}_{Rd}\boldsymbol{h}_{Rd}^{\mathrm{H}}\boldsymbol{w}_R^t$$
$$\text{s.t.}\quad 0\le\rho\le\rho_{th}$$
$$(\boldsymbol{w}_R^t)^{\mathrm{H}}\boldsymbol{w}_R^t = 1. \quad (37)$$

The solution of Problem (36) can then be obtained as

$$[\rho_{opt}^{p\mathrm{JPSB}},(\boldsymbol{w}_r^t)_{opt}^{p\mathrm{JPSB}}] = [\rho_{th},\frac{\boldsymbol{h}_{Rd}^*}{||\boldsymbol{h}_{Rd}||}]. \quad (38)$$

Observe from (23) that the complexity of computing ρ_{th} is approximately on the order of $O(M)$. Since the computational complexity of $\frac{\boldsymbol{h}_{Rd}^*}{||\boldsymbol{h}_{Rd}||}$ is also $O(M)$, we confirm that the computational complexity of the proposed pJPSB scheme is approximately $O(M)$.

IV. NUMERICAL RESULTS AND DISCUSSIONS

This section presents the secrecy rate results for the proposed fJPSB and pJPSB schemes. The conventional fixed PS and beamforming (FPSB) method is used as the benchmark. We also compare the proposed JBRJS scheme both to the joint random relay and jammer selection (JRRJS) as well as to the pure best relay selection (PBRS) schemes in our EH-aided cooperative network. Moreover, we illustrate that the secrecy performance is improved, as the number of the antennas used at each intermediate node increases. In our numerical simulations, we use $R_d = 1$ bit/s/Hz and $\delta_n^2 = 0$ dBm, while the step size σ of the exhaustive search method is set to 5×10^{-7}.

In Fig. 2 and Fig. 3, we present the secrecy rate results of the proposed JBRJS scheme, in comparison to the JRRJS and the PBRS schemes. In the JRRJS scheme, one of the nodes is randomly selected as the relay for forwarding the source signal, while the others are used as the jammers to interfere with E. In the PBRS scheme, only the intermediate node satisfying the criterion (4) is selected as the relay for improving the security, but no jammers are activated. In Fig.2 and Fig.3, we use a fixed PS ratio of $\rho = 0.5$ and a MRC based transmit BF vector, for the case of illustrating the advantage of the proposed JBRJS scheme in our EH-aided cooperative network.

Fig. 2 shows the secrecy rate versus the transmit power P_s of the proposed JBRJS scheme, of the JRRJS scheme, and

of the PBRS scheme for $K = 4$ intermediate nodes and for $M = 4$ TAs at each intermediate node. All cases in Fig.2 clearly show that the proposed JBRJS scheme has a higher secrecy rate than the JRRJS and PBRS schemes. From Fig. 2, we can also observe that as P_s increases, the secrecy rate of both the proposed JBRJS scheme and of the JRRJS scheme improve. This is because upon increasing P_s, the power of the artificial noise received at E increases. It can be seen from Fig. 2 that the secrecy rate of the PBRS scheme remains near constant when P_s is increased, because upon increasing P_s, the achievable rate improvement at E is similar to that at D without using jammers provided that P_s is higher than a threshold.

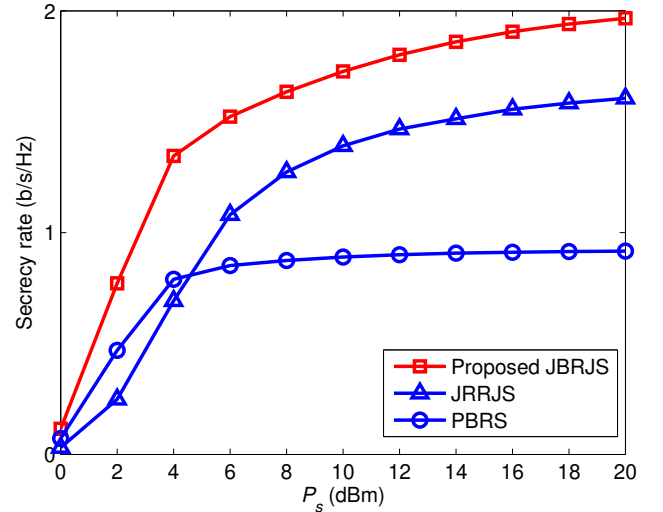In Fig. 3, we depict the secrecy rate versus the number

Fig. 2. Secrecy rate versus transmit power P_s of the proposed JBRJS, JRRJS and PBRS schemes for $K = 4$ and $M = 4$.

of intermediate nodes K at $P_s = 15$ dBm and $M = 4$ TAs used for BF at each intermediate node. Observe from Fig. 3 that the proposed JBRJS scheme outperforms both the JRRJS and PBRS schemes in terms of its secrecy rate. Fig. 3 also shows that as K increases, the secrecy rate of the proposed JBRJS scheme improves more substantially than that of both the JRRJS and PBRS schemes. This is because increasing K leads to an additional relay selection gain as well as to an artificial noise power boost, both of which benefit the secrecy performance.

Fig.4 shows the secrecy rate versus P_s for the proposed fJPSB scheme, for the pJPSB scheme advocated and for the FPSB scheme associated with $K = 4$ and $M = 4$. In the

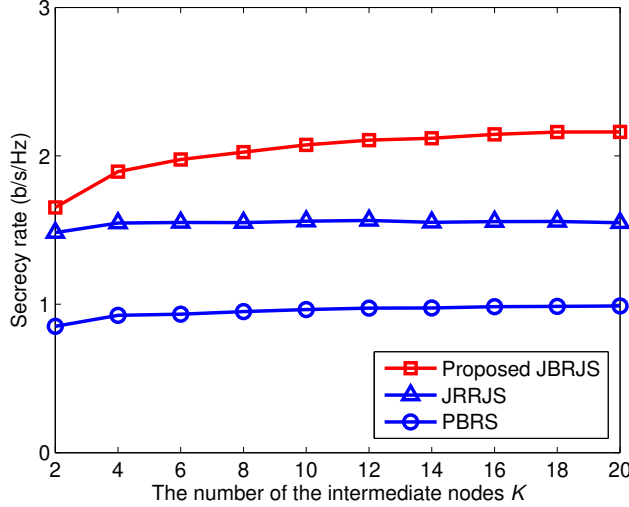achieves a much higher secrecy rate than the pJPSB scheme, indicating that the joint optimization of the PS ratio and the relay BF substantially improves the secrecy performance when the CSI of the eavesdropping link is taken into account. In addition, as shown in Fig. 5, the secrecy rate of all the proposed fJPSB, pJPSB and traditional FPSB schemes increases with K on average. However indeed, the secrecy rate of the proposed fJPSB scheme does not increase as monotonically as that of the proposed pJPSB and of the traditional FPSB schemes. The secrecy rate fluctuation of the proposed fJPSB scheme is mainly due to the fact that the step size of $\sigma = 5 \times 10^{-7}$ does not always lead to the optimal $\rho_{opt}^{f\mathrm{JPSB}}$ for each K. By considering the secrecy rate vs. the computational complexity tradeoff which is linearly increasing at the order of $O(1/\sigma)$, we opt for $\sigma = 5 \times 10^{-7}$.

Fig. 6 illustrates the secrecy rate of the proposed JBRJS

Fig. 3. Secrecy rate versus the number of intermediate nodes K for the proposed JBRJS, JRRJS and PBRS schemes for $P_s = 15$ dBm and $M = 4$.

FPSB scheme, the PS ratio is set to $\rho = 0.5$ and the transmit BF $\boldsymbol{w}_R^t$ is set based on the MRC scheme. It is observed that the secrecy rate of the proposed fJPSB and pJPSB schemes is approximately 1∼3 bit/s/Hz and 0.3∼0.4 bit/s/Hz higher than that of the conventional FPSB scheme, respectively. In addition, the proposed fJPSB scheme achieves a much higher secrecy rate than the others, explicitly showing the advantage of using the joint optimization of PS and BF. Additionally, as shown in Fig.4, the secrecy rate increases with P_s.

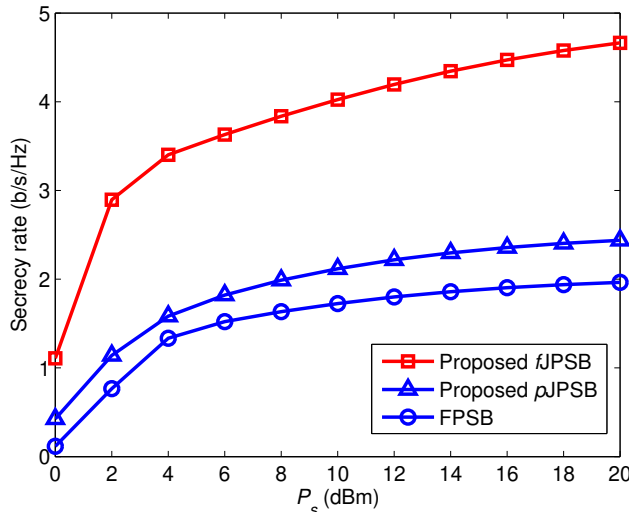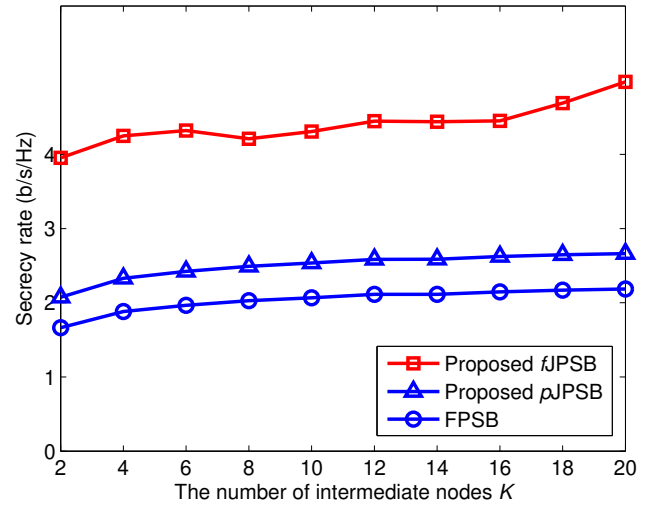In Fig. 5, we show the secrecy rate comparison of the

Fig. 5. Secrecy rate versus the number of intermediate nodes K of the proposed fJPSB, pJPSB and FPSB schemes for $P_s = 15$ dBm and $M = 4$.

scheme for $K = 4$ and $M = 4$, where the PS ratio is set to $\rho = \rho_{th}$ and the BF weight vector is set to $\boldsymbol{w}_R^t = \boldsymbol{v}_{max}[(\boldsymbol{I} + \frac{\xi_1}{\alpha+\beta}\rho_{th}\boldsymbol{H}_{re})^{-1}(\frac{\alpha}{\alpha+\beta}\boldsymbol{I} + \frac{\xi_1+\xi_2}{\alpha+\beta}\rho_{th}\boldsymbol{H}_{rd})]$ following Equation (24) for comparison. Observe from Fig. 6 that our proposed fJPSB scheme using the exhaustive search method for computing the optimal PS ratio $\rho_{opt}^{f\mathrm{JPSB}}$ always performs much better than using $\rho = \rho_{th}$, verifying the efficiency of the exhaustive search method. This also implies that the optimization of the PS ratio substantially improves the secrecy performance.

In Fig.7, we show the secrecy rate versus the number of TAs M used at each intermediate node for the proposed fJPSB and pJPSB schemes at $P_s = 15$ dBm and $K = 4$. It can be observed from Fig. 7 that upon increasing the number of TAs, the secrecy rate of both the proposed fJPSB and pJPSB schemes increases, showing that the secrecy performance can be further improved by using more TAs at each intermediate node.

Fig. 4. Secrecy rate versus transmit power P_s of the proposed fJPSB, pJPSB and FPSB schemes for $K = 4$ and $M = 4$.

fJPSB, pJPSB and FPSB schemes for $P_s = 15$ dBm and $M = 4$. Observe from Fig. 5 that the proposed fJPSB and pJPSB schemes lead to approximately 2.3∼2.8 bit/s/Hz and 0.4∼0.5 bit/s/Hz higher secrecy rate than the traditional FPSB scheme. One can also see that the proposed fJPSB scheme
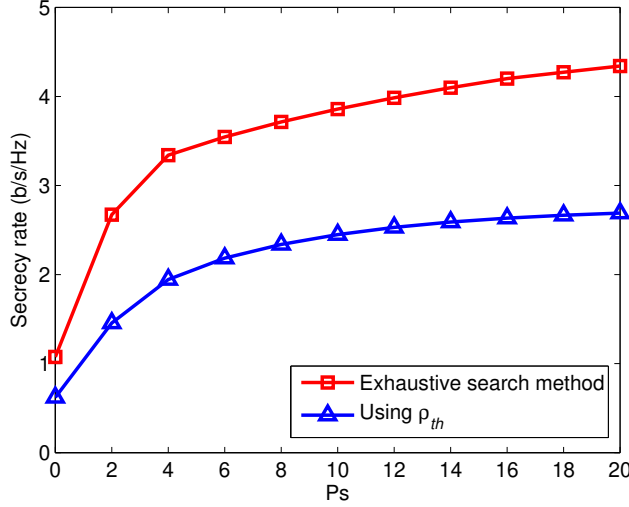
Fig. 6. Secrecy rate versus the transmit power P_s of the proposed fJPSB scheme using the exhaustive search method and the proposed JBRJS scheme using $\rho = \rho_{th}$ for $K = 4$ and $M = 4$.
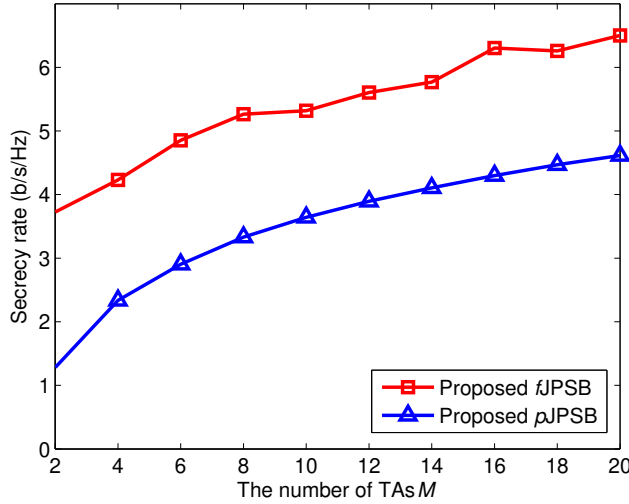

Fig. 7. Secrecy rate versus the number of TAs M equipped at each intermediate node of the proposed fJPSB and pJPSB schemes for $P_s = 15$ dBm and $K = 4$.

V. CONCLUSION

In this paper, we have investigated the PLS of cooperative wireless networks assisted by multiple EH-aided intermediate nodes, which accumulate energy based on the PS protocol. We proposed a JBRJS scheme for enhancing the security in which the best relay is selected to forward the source signal, and all the remaining intermediate nodes are exploited as jammers to transmit artificial noise. Furthermore, we studied the joint optimization of the PS ratio and the relay BF for the sake of maximizing the secrecy rate and proposed the fJPSB scheme for the full-CSI scenario to find the optimal solution. We also conceived the pJPSB scheme for the case where only the main link's CSI is available. Our simulation results demonstrate that the proposed JBRJS scheme outperforms

both the JRRJS scheme and the PBRS scheme in terms of its secrecy rate, while the proposed fJPSB and pJPSB methods lead to higher secrecy rate than the FPSB method. Moreover, our simulation results show that the secrecy rate increases with the number of TAs.

APPENDIX A
PROOF OF EQUATION (27)

By exploiting that $\lambda(\boldsymbol{AB}) = \lambda(\boldsymbol{BA})$ where $\lambda(\boldsymbol{AB})$ denotes the eigenvalues of the product of matrices $\boldsymbol{A}$ and $\boldsymbol{B}$, we can obtain $\lambda_{max}[(\boldsymbol{I} + \frac{\xi_1}{\alpha+\beta}\rho\boldsymbol{H}_{Re})^{-1}(\frac{\alpha}{\alpha+\beta}\boldsymbol{I} + \frac{\xi_1+\xi_2}{\alpha+\beta}\rho\boldsymbol{H}_{Rd})]$ which is given by (A.1) at the top of the following page.

According to the Sherman-Morrison formula [41], we have

$$(\frac{\alpha+\beta}{\rho\xi_1}\boldsymbol{I} + \boldsymbol{h}_{Re}\boldsymbol{h}_{Re}^{\mathrm{H}})^{-1} = \frac{\rho\xi_1}{\alpha+\beta}\boldsymbol{I} - \frac{\frac{\rho\xi_1}{\alpha+\beta}\boldsymbol{I}\boldsymbol{h}_{Re}\boldsymbol{h}_{Re}^{\mathrm{H}}\frac{\rho\xi_1}{\alpha+\beta}\boldsymbol{I}}{1 + \boldsymbol{h}_{Re}^{\mathrm{H}}\frac{\rho\xi_1}{\alpha+\beta}\boldsymbol{I}\boldsymbol{h}_{Re}}$$
(A.2)

$$= \frac{\rho\xi_1}{\alpha+\beta}\boldsymbol{I} - \frac{(\frac{\rho\xi_1}{\alpha+\beta})^2\boldsymbol{H}_{Re}}{1 + \frac{\rho\xi_1}{\alpha+\beta}||\boldsymbol{h}_{Re}||^2}.$$

Then, we can readily show that

$$(\boldsymbol{I} + \frac{\xi_1}{\alpha+\beta}\rho\boldsymbol{H}_{Re})^{-1} = [\frac{\rho\xi_1}{\alpha+\beta}(\frac{\alpha+\beta}{\rho\xi_1} + \boldsymbol{h}_{Re}\boldsymbol{h}_{Re}^{\mathrm{H}})]^{-1}$$
(A.3)

$$= \frac{\alpha+\beta}{\rho\xi_1}(\frac{\alpha+\beta}{\rho\xi_1}\boldsymbol{I} + \boldsymbol{h}_{Re}\boldsymbol{h}_{Re}^{\mathrm{H}})^{-1}$$

$$= \boldsymbol{I} - \frac{\frac{\rho\xi_1}{\alpha+\beta}\boldsymbol{H}_{Re}}{1 + \frac{\rho\xi_1}{\alpha+\beta}||\boldsymbol{h}_{Re}||^2}.$$

Thus, we have

$$(\boldsymbol{I} + \frac{\xi_1}{\alpha+\beta}\rho\boldsymbol{H}_{Re})^{-\frac{1}{2}}\frac{\alpha}{\alpha+\beta}\boldsymbol{I}(\boldsymbol{I} + \frac{\xi_1}{\alpha+\beta}\rho\boldsymbol{H}_{Re})^{-\frac{1}{2}} \quad \text{(A.4)}$$

$$= \frac{\alpha}{\alpha+\beta}(\boldsymbol{I} + \frac{\xi_1}{\alpha+\beta}\rho\boldsymbol{H}_{Re})^{-1}$$

$$= \frac{\alpha}{\alpha+\beta}(\boldsymbol{I} - \frac{\frac{\rho\xi_1}{\alpha+\beta}\boldsymbol{H}_{Re}}{1 + \frac{\rho\xi_1}{\alpha+\beta}||\boldsymbol{h}_{Re}||^2})$$

and

$$(\boldsymbol{I} + \frac{\xi_1}{\alpha+\beta}\rho\boldsymbol{H}_{Re})^{-\frac{1}{2}}\frac{\xi_1+\xi_2}{\alpha+\beta}\rho\boldsymbol{H}_{Rd}(\boldsymbol{I} + \frac{\xi_1}{\alpha+\beta}\rho\boldsymbol{H}_{Re})^{-\frac{1}{2}}$$
(A.5)

$$= \frac{\xi_1+\xi_2}{\alpha+\beta}\rho(\boldsymbol{I} - \frac{\frac{\rho\xi_1}{\alpha+\beta}\boldsymbol{H}_{Re}}{1 + \frac{\rho\xi_1}{\alpha+\beta}||\boldsymbol{h}_{Re}||^2})^{\frac{1}{2}}\boldsymbol{H}_{Rd}(\boldsymbol{I} - \frac{\frac{\rho\xi_1}{\alpha+\beta}\boldsymbol{H}_{Re}}{1 + \frac{\rho\xi_1}{\alpha+\beta}||\boldsymbol{h}_{Re}||^2})^{\frac{1}{2}}.$$

Upon combining (A.4) and (A.5), we have Equation (A.6) stated at the top of the following page.

Define $\boldsymbol{y} = \sqrt{\frac{\alpha\xi_1\rho}{(\alpha+\beta+\rho\xi_1||\boldsymbol{h}_{Re}||^2)(\alpha+\beta)}}\boldsymbol{h}_{Re}$, $\boldsymbol{U}\Lambda^{\frac{1}{2}}\boldsymbol{U}^{\mathrm{H}}$ as the eigen value decomposition of $(\boldsymbol{I} - \frac{\frac{\rho\xi_1}{\alpha+\beta}\boldsymbol{H}_{Re}}{1 + \frac{\rho\xi_1}{\alpha+\beta}||\boldsymbol{h}_{Re}||^2})^{\frac{1}{2}}$ and $\boldsymbol{x} =$

$$\lambda_{max}[(\boldsymbol{I} + \frac{\xi_1}{\alpha+\beta}\rho\boldsymbol{H}_{Re})^{-1}(\frac{\alpha}{\alpha+\beta}\boldsymbol{I} + \frac{\xi_1+\xi_2}{\alpha+\beta}\rho\boldsymbol{H}_{Rd})] \tag{A.1}$$

$$= \lambda_{max}[(\boldsymbol{I} + \frac{\xi_1}{\alpha+\beta}\rho\boldsymbol{H}_{Re})^{-\frac{1}{2}}(\boldsymbol{I} + \frac{\xi_1}{\alpha+\beta}\rho\boldsymbol{H}_{Re})^{-\frac{1}{2}}(\frac{\alpha}{\alpha+\beta}\boldsymbol{I} + \frac{\xi_1+\xi_2}{\alpha+\beta}\rho\boldsymbol{H}_{Rd})]$$

$$= \lambda_{max}[(\boldsymbol{I} + \frac{\xi_1}{\alpha+\beta}\rho\boldsymbol{H}_{Re})^{-\frac{1}{2}}(\frac{\alpha}{\alpha+\beta}\boldsymbol{I} + \frac{\xi_1+\xi_2}{\alpha+\beta}\rho\boldsymbol{H}_{Rd})(\boldsymbol{I} + \frac{\xi_1}{\alpha+\beta}\rho\boldsymbol{H}_{Re})^{-\frac{1}{2}}]$$

$$(\boldsymbol{I} + \frac{\xi_1}{\alpha+\beta}\rho\boldsymbol{H}_{Re})^{-\frac{1}{2}}(\frac{\alpha}{\alpha+\beta}\boldsymbol{I} + \frac{\xi_1+\xi_2}{\alpha+\beta}\rho\boldsymbol{H}_{Rd})(\boldsymbol{I} + \frac{\xi_1}{\alpha+\beta}\rho\boldsymbol{H}_{Re})^{-\frac{1}{2}} \tag{A.6}$$

$$= \frac{\alpha}{\alpha+\beta}(\boldsymbol{I} - \frac{\frac{\rho\xi_1}{\alpha+\beta}\boldsymbol{H}_{Re}}{1 + \frac{\rho\xi_1}{\alpha+\beta}||\boldsymbol{h}_{Re}||^2}) + \frac{\xi_1+\xi_2}{\alpha+\beta}\rho(\boldsymbol{I} - \frac{\frac{\rho\xi_1}{\alpha+\beta}\boldsymbol{H}_{Re}}{1 + \frac{\rho\xi_1}{\alpha+\beta}||\boldsymbol{h}_{Re}||^2})^{\frac{1}{2}}\boldsymbol{H}_{Rd}(\boldsymbol{I} - \frac{\frac{\rho\xi_1}{\alpha+\beta}\boldsymbol{H}_{Re}}{1 + \frac{\rho\xi_1}{\alpha+\beta}||\boldsymbol{h}_{Re}||^2})^{\frac{1}{2}}$$

$$= \frac{\alpha}{\alpha+\beta}\boldsymbol{I} + \frac{\xi_1+\xi_2}{\alpha+\beta}\rho\boldsymbol{U}\Lambda^{\frac{1}{2}}\boldsymbol{U}^{\mathrm{H}}\boldsymbol{h}_{Rd}\boldsymbol{h}_{Rd}^{\mathrm{H}}\boldsymbol{U}\Lambda^{\frac{1}{2}}\boldsymbol{U}^{\mathrm{H}} - \frac{\alpha\xi_1\rho}{(\alpha+\beta+\rho\xi_1||\boldsymbol{h}_{Re}||^2)(\alpha+\beta)}\boldsymbol{h}_{Re}\boldsymbol{h}_{Re}^{\mathrm{H}}.$$

$\sqrt{\frac{(\xi_1+\xi_2)\rho}{\alpha+\beta}}\boldsymbol{U}\Lambda^{\frac{1}{2}}\boldsymbol{U}^{\mathrm{H}}\boldsymbol{h}_{Rd}$. By substituting $\boldsymbol{x}$, $\boldsymbol{y}$ into Equation (A.6), we have

$$\lambda_{max}[(\boldsymbol{I} + \frac{\xi_1}{\alpha+\beta}\rho\boldsymbol{H}_{Re})^{-1}(\frac{\alpha}{\alpha+\beta}\boldsymbol{I} + \frac{\xi_1+\xi_2}{\alpha+\beta}\rho\boldsymbol{H}_{Rd})] \tag{A.7}$$

$$= \lambda_{max}(\frac{\alpha}{\alpha+\beta}\boldsymbol{I} + \boldsymbol{x}\boldsymbol{x}^{\mathrm{H}} - \boldsymbol{y}\boldsymbol{y}^{\mathrm{H}})$$

$$= \frac{\alpha}{\alpha+\beta} + \lambda_{max}(\boldsymbol{x}\boldsymbol{x}^{\mathrm{H}} - \boldsymbol{y}\boldsymbol{y}^{\mathrm{H}}).$$

Then, according to [42], we arrive at Equation (27).

APPENDIX B
PROOF OF EQUATION (28)

Since $(\boldsymbol{I} - \frac{\frac{\rho\xi_1}{\alpha+\beta}\boldsymbol{H}_{Re}}{1+\frac{\rho\xi_1}{\alpha+\beta}||\boldsymbol{h}_{Re}||^2})^{\frac{1}{2}} = \boldsymbol{U}\Lambda^{\frac{1}{2}}\boldsymbol{U}^{\mathrm{H}}$, we have $\boldsymbol{I} - \frac{\frac{\rho\xi_1}{\alpha+\beta}\boldsymbol{H}_{Re}}{1+\frac{\rho\xi_1}{\alpha+\beta}||\boldsymbol{h}_{Re}||^2} = \boldsymbol{U}\Lambda\boldsymbol{U}^{\mathrm{H}}$ [41]. Thus, we can show that $\lambda_{gen}(\boldsymbol{I} - \frac{\frac{\rho\xi_1}{\alpha+\beta}\boldsymbol{H}_{Re}}{1+\frac{\rho\xi_1}{\alpha+\beta}||\boldsymbol{h}_{Re}||^2}) = 1 - \lambda_{gen}(\frac{\frac{\rho\xi_1}{\alpha+\beta}\boldsymbol{H}_{Re}}{1+\frac{\rho\xi_1}{\alpha+\beta}||\boldsymbol{h}_{Re}||^2})$. Since the rank of the matrix $\frac{\frac{\rho\xi_1}{\alpha+\beta}\boldsymbol{H}_{Re}}{1+\frac{\rho\xi_1}{\alpha+\beta}||\boldsymbol{h}_{Re}||^2}$ is 1, we can show that $\frac{\frac{\rho\xi_1}{\alpha+\beta}\boldsymbol{H}_{Re}}{1+\frac{\rho\xi_1}{\alpha+\beta}||\boldsymbol{h}_{Re}||^2}$ has only a single non-zero eigenvalue. Therefore, Λ is obtained as

$$\Lambda = \begin{bmatrix} 1 - tr(\frac{\frac{\rho\xi_1}{\alpha+\beta}\boldsymbol{H}_{Re}}{1+\frac{\rho\xi_1}{\alpha+\beta}||\boldsymbol{h}_{Re}||^2}) & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 - \frac{\rho\xi_1|\boldsymbol{h}_{Re}^2||}{\rho\xi_1||\boldsymbol{h}_{Re}||^2+\alpha+\beta} & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

$$= \begin{bmatrix} \frac{\alpha+\beta}{\rho\xi_1||\boldsymbol{h}_{Re}||^2+\alpha+\beta} & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}, \tag{B.1}$$

where $tr(\boldsymbol{A})$ denotes the trace of matrix $\boldsymbol{A}$. Then, correspondingly, $\Lambda^{\frac{1}{2}}$ is given by

$$\Lambda^{\frac{1}{2}} = \begin{bmatrix} \sqrt{\frac{\alpha+\beta}{|\rho\xi_1|\boldsymbol{h}_{Re}||^2+\alpha+\beta}} & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}. \tag{B.2}$$

Since we have $\boldsymbol{u}_{gen}(I - \frac{\frac{\rho\xi_1}{\alpha+\beta}\boldsymbol{H}_{Re}}{1+\frac{\rho\xi_1}{\alpha+\beta}||\boldsymbol{h}_{Re}||^2}) = \boldsymbol{u}_{gen}(\frac{\frac{\rho\xi_1}{\alpha+\beta}\boldsymbol{H}_{Re}}{1+\frac{\rho\xi_1}{\alpha+\beta}||\boldsymbol{h}_{Re}||^2})$, where $\boldsymbol{u}_{gen}(\boldsymbol{A})$ denotes the eigenvectors of the matrix $\boldsymbol{A}$, due to $\lambda_{gen}(\frac{\frac{\rho\xi_1}{\alpha+\beta}\boldsymbol{H}_{Re}}{1+\frac{\rho\xi_1}{\alpha+\beta}||\boldsymbol{h}_{Re}||^2})\boldsymbol{u}_{gen}(\frac{\frac{\rho\xi_1}{\alpha+\beta}\boldsymbol{H}_{Re}}{1+\frac{\rho\xi_1}{\alpha+\beta}||\boldsymbol{h}_{Re}||^2}) = \frac{\frac{\rho\xi_1}{\alpha+\beta}\boldsymbol{H}_{Re}}{1+\frac{\rho\xi_1}{\alpha+\beta}||\boldsymbol{h}_{Re}||^2}\boldsymbol{u}_{gen}(\frac{\frac{\rho\xi_1}{\alpha+\beta}\boldsymbol{H}_{Re}}{1+\frac{\rho\xi_1}{\alpha+\beta}||\boldsymbol{h}_{Re}||^2})$, we have

$$\boldsymbol{u}_1 = \frac{\boldsymbol{h}_{Re}}{||\boldsymbol{h}_{Re}||} \tag{B.3}$$

and

$$\boldsymbol{h}_{Re}^{\mathrm{H}}\boldsymbol{u}_m = 0 \qquad m = 2,3,\cdots,M_r, \tag{B.4}$$

where $\boldsymbol{u}_1^{\mathrm{H}}\boldsymbol{u}_1 = 1$ and $\boldsymbol{u}_m^{\mathrm{H}}\boldsymbol{u}_m = 1$.

By substituting $\boldsymbol{U} = [\boldsymbol{u}_1\boldsymbol{u}_2\cdots\boldsymbol{u}_M]$, Equation (B.2) and (B.3) into the expression of $\boldsymbol{x} = \sqrt{\frac{(\xi_1+\xi_2)\rho}{\alpha+\beta}}\boldsymbol{U}\Lambda^{\frac{1}{2}}\boldsymbol{U}^{\mathrm{H}}\boldsymbol{h}_{Rd}$, we obtain the expression of $\boldsymbol{x}$ which is given by (B.5) at the top of the following page. Then, we can express $||\boldsymbol{x}||^2$ in Equation (28).

APPENDIX C
DERIVATION OF (34)

Since $||\boldsymbol{x}||^2 = \frac{(\xi_1+\xi_2)c}{e}f_1(\rho) + \frac{(\xi_1+\xi_2)\mu}{\alpha+\beta}\rho$, $||\boldsymbol{y}||^2 = \frac{\alpha\xi_1 e}{\alpha+\beta}f_1(\rho)$ and $||\boldsymbol{y}^{\mathrm{H}}\boldsymbol{x}||^2 = \frac{\alpha\xi_1(\xi_1+\xi_2)c}{\alpha+\beta}f_1(\rho)$, we have $(||\boldsymbol{x}||^2 + ||\boldsymbol{y}||^2)^2 - 4||\boldsymbol{y}^H\boldsymbol{x}||^2$ which is given by (C.1) at the top of the following page.

As $f_1(\rho) = \frac{\rho}{\alpha+\beta+\rho\xi_1 e}$, we have $\rho = (\alpha + \beta + \rho\xi_1 e)f_1(\rho)$. Then, (C.1) can be expressed equivalently as (C.2) at the top of the following page. Thus, we arrive at Equation

$$\boldsymbol{x} = \sqrt{\frac{(\xi_1+\xi_2)\rho}{\rho\xi_1||\boldsymbol{h}_{re}||^2+(\alpha+\beta)}}(\boldsymbol{u}_1^{\mathrm{H}}\boldsymbol{h}_{Rd})\boldsymbol{u}_1 + \sqrt{\frac{(\xi_1+\xi_2)\rho}{\alpha+\beta}}\sum_{m=2}^{M_r}(\boldsymbol{u}_m^{\mathrm{H}}\boldsymbol{h}_{Rd})\boldsymbol{u}_m \tag{B.5}$$

$$(||\boldsymbol{x}||^2+||\boldsymbol{y}||^2)^2-4||\boldsymbol{y}^H\boldsymbol{x}||^2 = (||\boldsymbol{x}||^2-||\boldsymbol{y}||^2)^2 + 4(||\boldsymbol{x}||^2||\boldsymbol{y}||^2-||\boldsymbol{y}^{\mathrm{H}}\boldsymbol{x}||^2) = [\theta f_1(\rho)+\frac{\xi_1+\xi_2}{\alpha+\beta}\mu\rho]^2+4\frac{\alpha\xi_1(\xi_1+\xi_2)e\mu}{(\alpha+\beta)^2\rho f_1(\rho)} \tag{C.1}$$

$$(||\boldsymbol{x}||^2+||\boldsymbol{y}||^2)^2-4||\boldsymbol{y}^{\mathrm{H}}\boldsymbol{x}||^2 = \theta^2 f_1^2(\rho) + [\frac{(\xi_1+\xi_2)\mu}{\alpha+\beta}]^2(\alpha+\beta+\rho\xi_1 e)^2 f_1^2(\rho) + 2\frac{(\xi_1+\xi_2)\mu}{\alpha+\beta}(\theta+\frac{2\alpha\xi_1 e}{\alpha+\beta})(\alpha+\beta+\rho\xi_1 e)f_1^2(\rho) \tag{C.2}$$

$$= f_1^2(\rho)\left\{[(\theta+\frac{2\alpha\xi_1 e}{\alpha+\beta}) + \frac{\xi_1+\xi_2}{\alpha+\beta}\mu(\alpha+\beta+\rho\xi_1 e)]^2 - 4\frac{\xi_1+\xi_2}{\alpha+\beta}\alpha\xi_1 c\right\}.$$

$$||\boldsymbol{x}||^2-||\boldsymbol{y}||^2+\sqrt{(||\boldsymbol{x}||^2+||\boldsymbol{y}||^2)^2-4||\boldsymbol{y}^{\mathrm{H}}\boldsymbol{x}||^2} = \theta f_1(\rho)+\frac{(\xi_1+\xi_2)}{\alpha+\beta}\mu\rho +f_1(\rho)\sqrt{[(\theta+\frac{2\alpha\xi_1 e}{\alpha+\beta})+\frac{\xi_1+\xi_2}{\alpha+\beta}\mu(\alpha+\beta+\rho\xi_1 e)]^2-4\frac{\xi_1+\xi_2}{\alpha+\beta}\alpha\xi_1 c} \tag{C.3}$$

(C.3) stated at the top of the following page. Upon defining $f_2(\rho) = [\theta + \frac{2\alpha\xi_1 e}{\alpha+\beta} + \frac{\xi_1+\xi_2}{\alpha+\beta}(\alpha+\beta+\xi_1 e\rho)\mu]^2$, $f_3(\rho) = \sqrt{f_2(\rho)-4\frac{\xi_1+\xi_2}{\alpha+\beta}\alpha\xi_1 c}$ and $f_4(\rho) = \frac{\xi_1+\xi_2}{2(\alpha+\beta)}\mu\rho$, then we can express Problem (26) as Problem (34).

REFERENCES

[1] 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.
[2] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commu. Surv. Tut.*, vol. 19, no. 2, pp. 1027-1053, 2017.
[3] 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.
[4] Y. Zou, X. Wang and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas in Commun.*, vol. 31, no. 10, pp. 2099-2111, Oct. 2013.
[5] L. Fan, X. Lei, T. Q. Duong, M. E. and G. K. Karagiannidis, "Secure multiuser communications in multiple amplify-and-forward relay networks," *IEEE Trans. Commun.*, vol. 62, no. 9, pp. 3299-3310, Sep. 2014.
[6] Y. Zou, J. Zhu, X. Wang, and V. C.M. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Network*, vol. 29, no. 1, pp. 42-48, 2015.
[7] H. Wang, K. Huang, Q. Yang, and Z. Han, "Joint source-relay secure precoding for MIMO relay networks with direct links," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 2781-2793, Jul. 2017.
[8] Y. Feng, S. Yan, Z. Yang, N. Yang, and W. Zhu, " TAS-based incremental hybrid decode-amplify-forward relaying for physical layer security enhancement," *IEEE Trans. Commun.*, vol. 65, no. 9, pp. 3876-3891, Sep. 2017.
[9] X. Hu, C. Kai, Z. Guo, and J. Gao, "A fast forward full-duplex cooperative relay scheme for securing wireless communications," *IEEE Signal Process. Lett.*, vol. 26, no. 5, pp. 775-779, May 2019.
[10] S. A. A. Fakoorian, and A. L. Swindlehurst, "Solutions for the MIMO Gaussian wiretap channel with a cooperative jammer," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 5013-5022, Oct. 2011.
[11] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, " Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962-4974, Oct. 2013.
[12] J. H. Lee and W. Choi, "Multiuser diversity for secrecy communications using opportunistic jammer selection: Secure DoF and jammer scaling law," *IEEE Trans. Signal Process.*, vol. 62, no. 4, pp. 828-839, Feb. 2014.
[13] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Y. 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.
[14] K. Cumanan, G. C. Alexandropoulos, Z. Ding, and G. K. Karagiannidis, "Secure communications with cooperative jamming: Optimal power allocation and secrecy outage analysis ," *IEEE Trans. Veh. Technol.*,vol. 66, no. 8, pp. 7495-7505, Aug. 2017.
[15] L. Hu, H. Wen, B. Wu, F. Pan, R. Liao, H. Song, J. Tang, and X. Wang, "Cooperative jamming for physical layer security enhancement in Internet of things," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 219-228, Feb. 2018.
[16] S. Xu, S. Han, W. Meng, Y. Du, and L. He, "Multiple-jammer-aided secure transmission with receiver-side correlation," *IEEE Trans. Wireless Commu.*, vol. 18, no. 6, pp. 3093-3103, Jun. 2019.
[17] B. Li, Y. Zou, J. Zhou, F. Wang, W. Cao, and Y. Yao, " Secrecy outage probability analysis of friendly jammer selection aided multiuser scheduling for wireless networks," *IEEE Trans. Commu.*, vol. 67, no. 5, pp. 3482-3495, Jan. 2019.
[18] J. Chen, R. Zhang, L. Song, Z. Han and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inf. Theory*, vol. 7, no. 1, pp. 310-320, Feb. 2012.
[19] L. Wang, Y. Cai, Y. Zou, W. Yang, and L. Hanzo, "Joint relay and jammer selection improves the physical layer security in the face of CSI feedback delays," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6259-6274, Aug. 2016.
[20] H. Hui, A. L. Swindlehurst, G. Li, and J. Liang, "Secure relay and jammer selection for physical layer security," *IEEE Signal Process. Lett.*, vol. 22, no. 8, pp. 1147-1151, Aug. 2015.
[21] K. Wang, L. Yuan, T. Miyazaki, D. Zeng, S. Guo, and Y. Sun, "Strategic anti-eavesdropping game for physical layer security in wireless cooperative networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 9448-9457, Oct. 2017.
[22] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A comprehensive survey on cooperative relaying and jamming strategies for physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2734-2771, 2019.
[23] R. Nakai and S. Sugiura, " Physical layer security in buffer-state-based max-ratio relay selection exploiting broadcasting with cooperative beamforming and jamming," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 2, pp. 431-444, Feb. 2019.
[24] H. Guo, Z. Yang, L. Zhang, J. Zhu, and Y. Zou, "Power-constrained secrecy rate maximization for joint relay and jammer selection assisted wireless networks," *IEEE Trans. Commun.*, vol. 65, no. 5, pp. 2180-2193, May 2017.
[25] H. Guo, Z. Yang, L. Zhang, J. Zhu, and Y. Zou, "Joint cooperative beamforming and jamming for physical-layer security of decode-and-forward relay networks," *IEEE Access*, vol. 5, pp. 19620-19630, 2017.

[26] 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.

[27] L. Liu, R. Zhang, and K. Chua, "Wireless information transfer with opportunistic energy harvesting," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 288-300, Jan. 2013.

[28] H. J. Visser and R. J. M. Vullers, "RF energy harvesting and transport for wireless sensor network applications: Principles and requirements," *Proc. IEEE*, vol. 101, no. 6, pp. 1410-1423, Jun. 2013.

[29] B. Clerckx and E. Bayguzina, "Waveform design for wireless power transfer," *IEEE Trans. Signal Process.*, vol. 64, no. 23, pp. 6313-6328, Dec. 2016.

[30] L. Zhao and X. Wang, "Massive MIMO downlink for wireless information and energy transfer with energy harvesting receivers," *IEEE Trans. Commun.*, vol. 67, no. 5, pp. 3309-3322, Jan. 2019.

[31] J. Qiao, H. Zhang, X. Zhou, and D. Yuan, "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.

[32] J. Qiao, H. Zhang, F. Zhao, and D. Yuan, "Secure transmission and self-energy recycling with partial eavesdropper CSI," *IEEE J. Sel. Topics Commun.*, 2018, vol. 36, no. 7, pp. 1531-1543, Jul. 2018.

[33] Y. Bi and H. Chen, "Accumulate and jam: Towards secure communication via a wireless-powered full-duplex jammer," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1538-1550, Dec. 2016.

[34] M. Zhao, X. Wang, and S. Feng, "Joint power splitting and secure beamforming design in the multiple non-regenerative wireless-powered relay networks," *IEEE Commun. Lett.*, vol. 19, no. 9, pp. 1540-1543, Sep. 2015.

[35] A. Salem, K. A. Hamdi, and K. M. Rabie, "Physical layer security with RF energy harvesting in AF multi-antenna relaying networks," *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 3025-3038, Jul. 2016.

[36] K. Lee, J. Hong, H. Choi, and T. Q. S. Quek, "Wireless-powered two-way relaying protocols for optimizing physical layer security," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 1, pp. 162-174, Jan. 2019.

[37] H. Xing, K. Wong, Z. Chu, and A. Nallanathan, "To harvest and jam: A paradigm of self-sustaining friendly jammers for secure AF relaying," *IEEE Trans. Signal Process.*, vol. 63, no. 24, pp. 6616-6631, Dec. 2015.

[38] T. M. Hoang, T. Q. Duong, N. Vo, and C. Kundu, "Physical layer security in cooperative energy harvesting networks with a friendly jammer," *IEEE Wireless Commun. Lett.*, vol. 6, no. 2, pp. 174-177, Apr. 2017.

[39] Z. Mobini, M. Mohammadi, and C. Tellambura, "Wireless-powered full-duplex relay and friendly jamming for secure cooperative communications," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 3, pp. 621-634, Mar. 2019.

[40] A. Maaref and S. Aissa, "Closed-form expressions for the outage and ergodic Shannon capacity of MIMO MRC systems," *IEEE Trans. Commun.*, vol. 53, no. 7, pp. 1092-1095, Apr. 2005.

[41] X. Zhang, "Matrix analysis and applications," *Tsinghua University Press*, Nov. 2013.

[42] A. Zappone, P. Lin, E. A. Jorswieck, "Energy efficiency in secure multi-antenna systems," *https://arxiv.org/abs/1505.02385*.

Zhen Yang is a professor at the Nanjing University of Posts and Telecommunications (NUPT), Nanjing, China. He received his B.Eng. and M.E. degrees in electrical engineering from NUPT, Nanjing, China, in 1983 and 1988, respectively, and the Ph.D. degree in electrical engineering from Shanghai Jiao Tong University, Shanghai, China, in 1999. From 1992 to 1993, he was a visiting scholar in Bremen University, Bremen, Germany, and in 2003, he was an exchange scholar in the University of Maryland, College Park. His research interests include various aspects of signal processing and communication, such as communication systems and networks, cognitive radio, spectrum sensing, speech and audio processing, compressive sensing and wireless communication.

Dr. Yang has served as the Vice Chair of the Chinese Institute of Communications and acted as members of the editorial board for several journals, including Chinese Journal of Electronics, Journal on Communications, and China Communications.

Yulong Zou (SM'13) is a Full Professor and Doctoral Supervisor at the Nanjing University of Posts and Telecommunications (NUPT), Nanjing, China. He received the B.Eng. degree in information engineering from NUPT, Nanjing, China, in July 2006, the first Ph.D. degree in electrical engineering from the Stevens Institute of Technology, New Jersey, USA, in May 2012, and the second Ph.D. degree in signal and information processing from NUPT, Nanjing, China, in July 2012.

Dr. Zou was awarded the 9th IEEE Communications Society Asia-Pacific Best Young Researcher in 2014. He has served as an editor for the IEEE Communications Surveys & Tutorials, IEEE Communications Letters, EURASIP Journal on Advances in Signal Processing, IET Communications, and China Communications. In addition, he has acted as TPC members for various IEEE sponsored conferences, e.g., IEEE ICC/GLOBECOM/WCNC/VTC/ICCC, etc.

Mujun Qian is an assistant professor at the Nanjing University of Posts and Telecommunications (NUPT), Nanjing, China. She received the B. Eng. degree in communication engineering in 2008, the M. Eng. and Ph.D. degrees in telecommunication and information systems in 2011 and 2016, respectively, from NUPT, Nanjing, China. Her research interests include cooperative communications, physical layer security and simultaneous wireless information and power transfer.

Haiyan Guo is an assistant professor at the Nanjing University of Posts and Telecommunications (NUPT), Nanjing, China. She received her B.Eng. and Ph.D. degrees in signal and information processing from NUPT, Nanjing in 2005 and 2011, respectively. From 2013 to 2014, she was a postdoctoral research fellow with Southeast University. Her research interests include physical-layer security, energy harvesting and speech signal processing.

Jia Zhu is a professor at the Nanjing University of Posts and Telecommunications (NUPT), Nanjing, China. She received the B.Eng. degree in computer science and technology from Hohai University, Nanjing, China, in 2005, and the Ph.D. degree in signal and information processing from NUPT, Nanjing, in 2010. From 2010 to 2012, she was a postdoctoral research fellow with the Stevens Institute of Technology, NJ, USA. Her general research interests include cognitive radio, physical-layer security, and communications theory.

Lajos Hanzo (M'91-SM'92-F'04) FREng, FIEEE, FIET, Fellow of EURASIP, DSc, received his degree in electronics in 1976 and his doctorate in 1983. In 2009 he was awarded an honorary doctorate by the Technical University of Budapest and in 2015 by the University of Edinburgh. In 2016 he was admitted to the Hungarian Academy of Science.

During his 40-year career in telecommunications he has held various research and academic posts in Hungary, Germany and the UK. Since 1986 he has been with the School of Electronics and Computer Science, University of Southampton, UK, where he holds the chair in telecommunications. He has successfully supervised 119 PhD students, co-authored 18 John Wiley/IEEE Press books on mobile radio communications totalling in excess of 10,000 pages, published 1800+ research contributions at IEEE Xplore, acted both as TPC and General Chair of IEEE conferences, presented keynote lectures and has been awarded a number of distinctions. Currently he is directing an academic research team, working on a range of research projects in the field of wireless multimedia communications sponsored by industry, the Engineering and Physical Sciences Research Council (EPSRC) UK, the European Research Council's Advanced Fellow Grant. He is an enthusiastic supporter of industrial and academic liaison and he offers a range of industrial courses. He is also a Governor of the IEEE VTS. During 2008-2012 he was the Editor-in-Chief of the IEEE Press and a Chaired Professor also at Tsinghua University, Beijing.