On Secure Communication using RF Energy Harvesting Two-Way Untrusted Relay

Vipul Gupta
Dept. of EECS
University of California, Berkeley, CA, USA
E-mail: vipul_gupta@berkeley.edu

Sanket S. Kalamkar
Dept. of EE
University of Notre Dame, IN, USA
E-mail: skalamka@nd.edu

Adrish Banerjee
Dept. of EE
IIT Kanpur, India
E-mail: adrish@iitk.ac.in

***Abstract*—We focus on a scenario where two wireless source nodes wish to exchange confidential information via an RF energy harvesting untrusted two-way relay. Despite its cooperation in forwarding the information, the relay is considered untrusted out of the concern that it might attempt to decode the confidential information that is being relayed. To discourage the eavesdropping intention of the relay, we use a friendly jammer. Under the total power constraint, to maximize the sum-secrecy rate, we allocate the power among the sources and the jammer optimally and calculate the optimal power splitting ratio to balance between the energy harvesting and the information processing at the relay. We further examine the effect of imperfect channel state information at both sources on the sum-secrecy rate. Numerical results highlight the role of the jammer in achieving the secure communication under channel estimation errors. We have shown that, as the channel estimation error on any of the channels increases, the power allocated to the jammer decreases to abate the interference caused to the confidential information reception due to the imperfect cancellation of jammer's signal.**

***Index Terms*—Energy harvesting, imperfect channel state information, physical layer security, two-way relay, untrusted relay**

I. Introduction

The demand for higher data rates has led to a shift towards higher frequency bands, resulting in higher path loss. Thus relays have become important for reliable long distance wireless transmissions. The two-way relay has received attention in the past few years due to its ability to make communications more spectral efficient [1], [2]. In a two-way relay assisted communication, the relay receives the information from two nodes simultaneously, which it broadcasts in the next slot.

A. Motivation

To improve the energy efficiency, harvesting energy from the surrounding environment has become a promising approach, which can prolong the lifetime of energy-constrained nodes and avoid frequent recharging and replacement of batteries. In [3] and [4], the authors have proposed the concept of using radio-frequency (RF) signals that carry information as a viable source of energy. Simultaneous wireless information and power transfer has applications in cooperative relaying. The works in [5]–[9] study throughput maximization problems when cooperating relays harvest energy from incoming RF signals to forward the information, where references [8], [9] have focused on two-way relaying.

Though the open wireless medium has facilitated cooperative relaying, it has also allowed unintended nodes to eavesdrop the communication between two legitimate nodes. Traditional ways to achieve secure communication rely on upper-layer cryptographic methods that involve intensive key distribution. Unlike this technique, the physical layer security aims to achieve secure communication by exploiting the random nature of the wireless channel. In this regard, Wyner introduced the idea of secrecy rate for the wiretap channel, where the secure communication between two nodes was obtained without private keys [10].

For cooperative relaying with energy harvesting, [11]–[13] investigate relay-assisted secure communication in the presence of an external eavesdropper. The security of the confidential message may still be a concern when the source and the destination wish to keep the message secret from the relay, despite its help in forwarding the information [14]–[18]. Hence the relay is trusted in forwarding the information, but untrusted out of the concern that the relay might attempt to decode the confidential information that is being relayed.[1] In practice, such scenario may occur in heterogeneous networks, where all nodes do not possess the same right to access the confidential information. For example, if two nodes having the access to confidential information wish to exchange information, but do not have the direct link due to severe fading and shadowing, they might need to take a help from an intermediate node that does not have the privilege to access the confidential information.

B. Related Works

In [14], the authors show that the cooperation by an untrusted relay can be beneficial and can achieve higher secrecy rate than just treating the untrusted relay as a pure eavesdropper. In [19], authors investigate the secure communication in untrusted two-way relay systems with the help of external friendly jammers and show that, though it is possible to achieve a non-zero secrecy rate without the friendly jammers, the secrecy rate at both sources can effectively be improved with the help from an external friendly jammer. In [20], authors have focused on improving the energy efficiency while

[1]In this case, the decode-and-forward relay is no longer suitable to forward the confidential information.

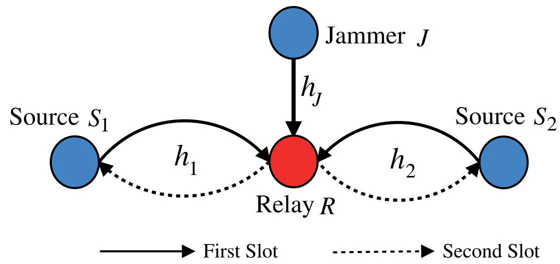

Fig. 1. Secure communication via an untrusted energy harvesting two-way relay

achieving the minimum secrecy rate for the untrusted two-way relay. The works in [14]–[20] assume that the relay is a conventional node and has a stable power supply. As to energy harvesting untrusted relaying, the works [21]–[23] analyze the effect of untrusted energy harvesting one-way relay on the secure communication between two legitimate nodes. To the best of our knowledge, for energy harvesting two-way untrusted relay, the problem of achieving secure communication has not been yet studied in the literature.

C. Contributions

The contributions and main results of this paper are as follows:

- First, assuming the perfect channel state information (CSI) at source nodes, we extend the notion of secure communication via an untrusted relay for the two-way wireless-powered relay, as shown in Fig. 1. To discourage the eavesdropping intentions of the relay, a friendly jammer sends a jamming signal during relay's reception of signals from source nodes.
- The relay uses a part of the received RF signals, which consist of two sources' transmissions and the jamming signal, to harvest energy. Hence we utilize the jamming signal effectively as a source of extra energy in addition to its original purpose of degrading relay's eavesdropping channel.
- Under the total power constraint, we exploit the structure of the original optimization problem and make use of the signomial geometric programming technique [24] to jointly find the optimal power splitting ratio for energy harvesting and the optimal power allocation among sources and the jammer, that maximize the sum-secrecy rate for two source nodes.
- Finally, with the imperfect CSI at source nodes, we study the joint effects of the energy harvesting nature of an untrusted relay and channel estimation errors on the sum-secrecy rate and the power allocated to the jammer. We particularly focus on the role of jammer in achieving the secure communication, where we show that the power allocated to the jammer decreases as the estimation error on any of the channels increases, in order to subside the detrimental effects of the imperfect cancellation of the jamming signal at source nodes.

II. Secure Communication with Perfect CSI

A. System Model

Fig. 1 shows the communication protocol between two legitimate source nodes S_1 and S_2—lacking the direct link between them—via an untrusted two-way relay R. All nodes are half-duplex and have a single antenna [19]. To discourage eavesdropping by the relay, a friendly jammer J sends the jamming signal during relay's reception of sources' signals. The communication of a secret message between S_1 and S_2 happens over two slots of equal duration $T/2$. In the first slot, the nodes S_1 and S_2 jointly send their information to the relay with powers P_1 and P_2, respectively, and the jammer J sends the jamming signal with power P_J. The powers P_1, P_2, and P_J are restricted by the power budget P such that $P_1 + P_2 + P_J \leq P$. This constraint may arise, for instance, when the sources and the jammer belong to the same network and the network has limited power budget to cater transmission requirements of sources and the jammer. The relay uses a part of the received power to harvest energy. In the second slot, using the harvested energy, the relay broadcasts the received signal in an amplify-and-forward manner.

Let h_1, h_2, and h_J denote the channel coefficients of the reciprocal channels from the relay to S_1, S_2, and jammer J, respectively. In this section, we assume that both sources have perfect CSI for all channels, which can be obtained from the classical channel training, estimation, and feedback from the relay. But if there are errors in the estimation and/or feedback, the sources will have imperfect CSI, which is the focus of Section III. Hence the relay is basically trusted when it comes to providing the services like feeding CSI back to transmitters and forwarding the information, but untrusted in the sense that it is not supposed to decode the confidential information that is being relayed [20]. Both sources have the perfect knowledge of the jamming signal [19].[2]

B. RF Energy Harvesting at Relay

The relay is an energy-starved node. It harvests energy from incoming RF signals, which include information signals from nodes S_1 and S_2 and the jamming signal from the jammer. To harvest energy from received RF signals, the relay uses power splitting (PS) policy [4]. In PS policy, the relay uses a fraction β of the total received power for energy harvesting. Under PS policy, the energy harvested by the relay is[3]

$$E_H = \beta\eta \left(P_1|h_1|^2 + P_2|h_2|^2 + P_J|h_J|^2\right)(T/2), \qquad (1)$$

where η is the energy conversion efficiency factor with $0 < \eta < 1$. The transmit power of the relay in the second slot is

$$P_H = \frac{E_H}{T/2} = \beta\eta \left(P_1|h_1|^2 + P_2|h_2|^2 + P_J|h_J|^2\right). \qquad (2)$$

[2] Jammer can use some pseudo-random codes as the jamming signals that are known to both sources beforehand, but the untrusted relay is unaware of them.

[3] For the exposition, we assume that the incident power on the energy harvesting circuitry of the relay is sufficient to activate it.

C. Information Processing and Relaying Protocol

In the first slot, the relay receives the signal

$$y_R = \sqrt{(1-\beta)}(\sqrt{P_1}h_1x_1 + \sqrt{P_2}h_2x_2 + \sqrt{P_J}h_Jx_J) + n_R, \tag{3}$$

where x_1 and x_2 are the messages of S_1 and S_2, respectively, with $\mathbb{E}[|x_1|^2] = \mathbb{E}[|x_1|^2] = 1$. Also x_J is the artificial noise by the jammer with $\mathbb{E}[|x_J|^2] = 1$, and n_R is the additive white Gaussian noise (AWGN) at relay with mean zero and variance N_0. Using the received signal y_R, the relay may attempt to decode the confidential messages x_1 and x_2. To shield the confidential messages x_1 and x_2 from relay's eavesdropping, we assume that the physical layer security coding like stochastic encoding and nested code structure can be used (see [20] and [25]). The relay can decode one of the sources' confidential messages, *i.e.*, either x_1 or x_2, if its rate is such that it can be decoded by considering other source's message as noise [26]. In this case, at relay, the signal-to-noise ratio (SNR) corresponding to x_1, *i.e.*, the message intended for S_2, is given by

$$\mathrm{SNR}_{R_2} = \frac{\widetilde{\beta}P_1|h_1|^2}{\widetilde{\beta}P_2|h_2|^2 + \widetilde{\beta}P_J|h_J|^2 + N_0}, \tag{4}$$

where $\widetilde{\beta} = 1-\beta$. Accordingly the achievable throughput of $S_1 - R$ link is $C_2^R = (1/2)\log(1+\mathrm{SNR}_{R_2})$. In (4), the term $\widetilde{\beta}P_2|h_2|^2$, corresponding to S_2's message for S_1, indirectly serves as an artificial noise for the relay in addition to the signal $\widetilde{\beta}P_J|h_J|^2$ from the jammer, if it attempts to decode x_1. Similarly, the SNR corresponding to x_2, *i.e.*, the message intended for S_1, is given by

$$\mathrm{SNR}_{R_1} = \frac{\widetilde{\beta}P_2|h_2|^2}{\widetilde{\beta}P_1|h_1|^2 + \widetilde{\beta}P_J|h_J|^2 + N_0}, \tag{5}$$

where $\widetilde{\beta}P_1|h_1|^2$ serves as an artificial noise for the relay, if it attempts to decode x_2. Thus the achievable throughput of $S_2 - R$ link is $C_1^R = (1/2)\log(1+\mathrm{SNR}_{R_1})$. Let $\gamma_i = P_i|h_i|^2/N_0$, where $i \in \{1,2,J\}$. It follows that

$$\mathrm{SNR}_{R_2} = \frac{\widetilde{\beta}\gamma_1}{\widetilde{\beta}\gamma_2 + \widetilde{\beta}\gamma_J + 1},\ \mathrm{SNR}_{R_1} = \frac{\widetilde{\beta}\gamma_2}{\widetilde{\beta}\gamma_1 + \widetilde{\beta}\gamma_J + 1}. \tag{6}$$

The relay amplifies the received signal y_R given by (3) by a factor α based on its harvested power P_H. Accordingly,

$$\begin{aligned}\alpha &= \sqrt{\frac{P_H}{\widetilde{\beta}P_1|h_1|^2 + \widetilde{\beta}P_2|h_2|^2 + \widetilde{\beta}P_J|h_J|^2 + N_0}} \\ &= \sqrt{\frac{\beta\eta(\gamma_1+\gamma_2+\gamma_J)}{\widetilde{\beta}\gamma_1 + \widetilde{\beta}\gamma_2 + \widetilde{\beta}\gamma_J + 1}}.\end{aligned} \tag{7}$$

The received signal at S_2 in the second slot is given by

$$y_2 = h_2(\alpha y_R) + n_2, \tag{8}$$

where n_2 is AWGN with power N_0. We assume that S_1 and S_2 know x_J beforehand. Hence after cancelling the terms that are known to S_2, *i.e.*, the terms corresponding to x_2 and x_J, the resultant received signal at S_2 is

$$y_2 = \underbrace{h_2\alpha\sqrt{\widetilde{\beta}P_1}h_1x_1}_{\text{desired signal}} + \underbrace{h_2\alpha n_R + n_2}_{\text{noise}}. \tag{9}$$

The perfect CSI allows S_2 to cancel unwanted components of the signal. Substituting α from (7) in (9), we can express the SNR at node S_2 as

$$\mathrm{SNR}_{S_2} = \frac{\gamma_1|h_2|^2\beta\widetilde{\beta}\eta(\gamma_1+\gamma_2+\gamma_J)}{(|h_2|^2\beta\eta + \widetilde{\beta})(\gamma_1+\gamma_2+\gamma_J)+1}, \tag{10}$$

and the corresponding achievable throughput on link $R - S_2$ is $C_2^S = (1/2)\log(1+\mathrm{SNR}_{S_2})$. Similarly the received signal at S_1 is

$$y_1 = \underbrace{h_1\alpha\sqrt{\widetilde{\beta}P_2}h_2x_2}_{\text{desired signal}} + \underbrace{h_1\alpha n_R + n_1}_{\text{noise}}. \tag{11}$$

The SNR at node S_1 is

$$\mathrm{SNR}_{S_1} = \frac{\gamma_2|h_1|^2\beta\widetilde{\beta}\eta(\gamma_1+\gamma_2+\gamma_J)}{(|h_1|^2\beta\eta + \widetilde{\beta})(\gamma_1+\gamma_2+\gamma_J)+1}, \tag{12}$$

and the corresponding achievable throughput on link $R - S_1$ is $C_1^S = (1/2)\log(1+\mathrm{SNR}_{S_1})$.

D. Secrecy Rate and Problem Formulation

For the communication via two-way untrusted relay, the sum-secrecy rate is given by

$$\begin{aligned}C_S &= \left[C_1^S - C_1^R\right]^+ + \left[C_2^S - C_2^R\right]^+ \\ &= \left[\frac{1}{2}\log_2(1+\mathrm{SNR}_{S_1}) - \frac{1}{2}\log_2(1+\mathrm{SNR}_{R_1})\right]^+ \\ &\quad + \left[\frac{1}{2}\log_2(1+\mathrm{SNR}_{S_2}) - \frac{1}{2}\log_2(1+\mathrm{SNR}_{R_2})\right]^+,\end{aligned} \tag{13}$$

where $[x]^+ \triangleq \max(x,0)$. Given the total power budget P, we have a constraint on transmit powers, *i.e.*, $P_1 + P_2 + P_J \leq P$. To maximize the sum-secrecy rate, we optimally allocate powers P_1, P_2, and P_J to S_1, S_2, and J, respectively, and find the optimal power splitting ratio β. We can formulate the optimization problem as

$$\begin{aligned}\underset{\beta,\widetilde{\beta},P_1,P_2,P_J}{\text{maximize}} \quad & C_S \\ \text{subject to} \quad & P_1 + P_2 + P_J \leq P, \\ & \beta + \widetilde{\beta} = 1, \\ & \beta, \widetilde{\beta} \leq 1, \\ & \beta, \widetilde{\beta}, P_1, P_2, P_J \geq 0.\end{aligned} \tag{14}$$

Based on the non-negativeness of two terms in the secrecy rate expression given by (13), we need to investigate four cases. We calculate the sum-secrecy rate in all four cases, with the best case being the one that gives the maximum sum-secrecy rate.

Case I: $C_1^S - C_1^R \geq 0$ *and* $C_2^S - C_2^R \geq 0$

Substituting $\gamma_i = P_i|h_i|^2/N_0$ and simplifying the problem in (14), it follows that

$$\underset{\beta,\widetilde{\beta},P_1,P_2,P_J}{\text{minimize}} \quad \frac{1}{2}\log_2 \frac{f(\beta,\widetilde{\beta},\gamma_1,\gamma_2,\gamma_J)}{g(\beta,\widetilde{\beta},\gamma_1,\gamma_2,\gamma_J)} \tag{15a}$$

$$\text{subject to} \quad \frac{\gamma_1 N_0}{|h_1|^2} + \frac{\gamma_2 N_0}{|h_2|^2} + \frac{\gamma_J N_0}{|h_J|^2} \leq P, \tag{15b}$$

$$\beta + \widetilde{\beta} = 1, \tag{15c}$$

$$\beta, \widetilde{\beta} \leq 1, \tag{15d}$$

$$\beta, \widetilde{\beta}, P_1, P_2, P_J \geq 0, \tag{15e}$$

where

$$\begin{aligned} f(\beta,\widetilde{\beta},\gamma_1,\gamma_2,\gamma_J) = {} & [\widetilde{\beta}(\gamma_1+\gamma_2+\gamma_J)+1]^2 \\ & \times [1+(\gamma_1+\gamma_2+\gamma_J)(|h_2|^2\beta\eta+\widetilde{\beta})] \\ & \times [1+(\gamma_1+\gamma_2+\gamma_J)(|h_1|^2\beta\eta+\widetilde{\beta})], \end{aligned}$$

and

$$\begin{aligned} g(\beta,\widetilde{\beta},\gamma_1,\gamma_2,\gamma_J) = {} & (\widetilde{\beta}(\gamma_2+\gamma_J)+1)(\widetilde{\beta}(\gamma_1+\gamma_J)+1) \\ & \times[(\gamma_1+\gamma_2+\gamma_J)(\widetilde{\beta}+|h_2|^2\beta\eta(\widetilde{\beta}\gamma_1+1))+1] \\ & \times[(\gamma_1+\gamma_2+\gamma_J)(\widetilde{\beta}+|h_1|^2\beta\eta(\widetilde{\beta}\gamma_2+1))+1]. \end{aligned}$$

We can drop the logarithm from the objective (15a) as it retains the monotonicity and yields the same optimal solution. We introduce an auxiliary variable t and do the following transformation.

$$\underset{\beta,\widetilde{\beta},P_1,P_2,P_J}{\text{minimize}} \quad \frac{f(\beta,\widetilde{\beta},\gamma_1,\gamma_2,\gamma_J)}{t} \tag{16a}$$

$$\text{subject to} \quad t \leq g(\beta,\widetilde{\beta},\gamma_1,\gamma_2,\gamma_J), \tag{16b}$$

$$\frac{\gamma_1 N_0}{|h_1|^2} + \frac{\gamma_2 N_0}{|h_2|^2} + \frac{\gamma_J N_0}{|h_J|^2} \leq P, \tag{16c}$$

$$\beta + \widetilde{\beta} \leq 1, \tag{16d}$$

$$\beta, \widetilde{\beta} \leq 1, \tag{16e}$$

$$t, \beta, \widetilde{\beta}, P_1, P_2, P_J \geq 0. \tag{16f}$$

The above transformation is valid for $t > 0$ because, to minimize the objective $f(\beta,\widetilde{\beta},\gamma_1,\gamma_2,\gamma_J)/t$, we need to maximize t, and it happens when $t = g(\beta,\gamma_1,\gamma_2,\gamma_J)$. Hence under the optimal condition, we have $t = g(\beta,\gamma_1,\gamma_2,\gamma_J)$, and the problems (14) and (16) are equivalent. Further we can replace the constraint (15c) by

$$\beta + \widetilde{\beta} \leq 1. \tag{17}$$

The substitution of (15c) by (17) in problem (16) yields an equivalent problem because $\beta + \widetilde{\beta} = 1$ under the optimal condition. That is, if $\beta + \widetilde{\beta} < 1$, we can always increase the value of β so that $\beta + \widetilde{\beta} = 1$. The increase in β leads to more harvested energy, which in turn, increases the transmit power of the relay and the sum-secrecy rate.

The objective (16a) is a posynomial function and (16c), (16d), and (16e) are posynomial constraints [24]. When the objective and constraints are of posynomial form, the problem can be transformed into a Geometric Programming (GP) form and converted into a convex problem [24]. Also, as the domain of GP problem includes only real positive variables, the constraint (16f) is implicit. But the constraint (16b) is not posynomial as it contains a posynomial function g which is bounded from below and GP cannot handle such constraints. We can solve this problem if the right-hand side of (16b), *i.e.*, $g(\beta,\widetilde{\beta},\gamma_1,\gamma_2,\gamma_J)$, can be approximated by a monomial. Then the problem (16) reduces to a class of problems that can be solved by Signomial Geometric Programming (SGP) [24].

To find a monomial approximation of the form $\widehat{g}(\mathbf{x}) = c\prod_{i=1}^{5} x_i^{a_i}$ of a function $g(\mathbf{x})$, where $\mathbf{x} = [\beta,\widetilde{\beta},\gamma_1,\gamma_2,\gamma_J]^T$ is the vector containing all variables, it would suffice if we find an affine approximation of $h(\mathbf{y}) = \log g(\mathbf{y})$, with ith element of $\mathbf{y}$ given by $y_i = \log x_i$ [24]. Let the affine approximation of $h(\mathbf{y})$ be $\widehat{h}(\mathbf{y}) = \log \widehat{g}(\mathbf{x}) = \log c + \mathbf{a}^T\mathbf{y}$. Using the Taylor's approximation for $h(\mathbf{y})$ around a point $\mathbf{y}_0$ in the feasible region and equating it with $\widehat{h}(\mathbf{y})$, it follows that

$$h(\mathbf{y}) \approx h(\mathbf{y}_0) + \nabla h(\mathbf{y}_0)^T(\mathbf{y}-\mathbf{y}_0) = \log c + \mathbf{a}^T\mathbf{y}, \tag{18}$$

for $\mathbf{y} \approx \mathbf{y_0}$. From (18), we have $\mathbf{a} = \nabla h(\mathbf{y}_0)$, *i.e.*,

$$a_i = \left.\frac{x_i}{g(\mathbf{x})}\frac{\partial g}{\partial x_i}\right|_{\mathbf{x}=\mathbf{x}_0},$$

and

$$c = \exp(h(\mathbf{y}_0) - \nabla h(\mathbf{y}_0)^T\mathbf{y}_0) = g(\mathbf{x}_0)\prod_{i=1}^{5} x_{0,i}^{a_i},$$

where $x_{0,i}$ is an ith element of $\mathbf{x}_0$. We substitute the monomial approximation $\widehat{g}(x)$ of $g(x)$ in (16b) and use GP technique to solve (16). The aforementioned affine approximation is, however, imprecise if the optimal solution lies far from the initial guess $\mathbf{x}_0$ as the Taylor's approximation would be inaccurate. To overcome this problem, we take an iterative approach, where, if the current guess is $\mathbf{x}_k$, we obtain the Taylor's approximation about $\mathbf{x}_k$ and solve a GP again. Let the current solution of GP be $\mathbf{x}_{k+1}$. In the next iteration, we take Taylor's approximation around $\mathbf{x}_{k+1}$ and solve a GP again. We keep iterating in this fashion until the convergence. Since the problem (16) is close to GP (as we have only one constraint in (16) that is not a posynomial), the aforementioned iterative approach works well in our case and yields the optimal solution [24]. If the obtained optimal solution contradicts with our initial assumption that $C_1^S - C_1^R \geq 0$ and $C_2^S - C_2^R \geq 0$, we move to other three cases discussed below.

Case II: $C_1^S - C_1^R \geq 0$ *and* $C_2^S - C_2^R < 0$

In this case, the secrecy rate is given by $C_S = (C_1^S - C_1^R)^+$, and we need to solve the problem (16) with the following expressions for $f(\beta,\widetilde{\beta},\gamma_1,\gamma_2,\gamma_J)$ and $g(\beta,\widetilde{\beta},\gamma_1,\gamma_2,\gamma_J)$:

$$\begin{aligned} f(\beta,\widetilde{\beta},\gamma_1,\gamma_2,\gamma_J) = {} & [\widetilde{\beta}(\gamma_1+\gamma_2+\gamma_J)+1] \\ & \times [1+(\gamma_1+\gamma_2+\gamma_J)(|h_2|^2\beta\eta+\widetilde{\beta})], \\ g(\beta,\widetilde{\beta},\gamma_1,\gamma_2,\gamma_J) = {} & (\widetilde{\beta}(\gamma_2+\gamma_J)+1) \\ & \times[1+(\gamma_1+\gamma_2+\gamma_J)(\widetilde{\beta}+|h_2|^2\beta\eta(\widetilde{\beta}\gamma_1+1))]. \end{aligned}$$

We again check if the assumption $C_1^S - C_1^R \geq 0$ and $C_2^S - C_2^R < 0$ is valid; if not, we move to the remaining two cases.

Case III: $C_1^S - C_1^R < 0$ and $C_2^S - C_2^R \geq 0$

This case is similar to Case II, and only the subscripts 1 and 2 need to be interchanged in the expressions of $f(\beta, \widetilde{\beta}, \gamma_1, \gamma_2, \gamma_J)$ and $g(\beta, \widetilde{\beta}, \gamma_1, \gamma_2, \gamma_J)$. If the solution obtained does not satisfy the initial assumptions, we move to Case IV.

Case IV: $C_1^S - C_1^R < 0$ and $C_2^S - C_2^R < 0$

In this case, the sum-secrecy rate is zero.

Algorithm 1 summarizes the aforementioned process of obtaining the optimal sum-secrecy rate and power allocation by solving (16).

Algorithm 1 Solution of (16)

Input Total power P, Channel gains h_1, h_2, and h_J, Energy conversion efficiency η, Noise variance N_0, Tolerance δ

Output Power splitting ratio β, power P_1, P_2, and P_J, Sum-secrecy rate C_S

Initialize $0 \leq P_{1,k}, P_{2,k}, P_{J,k} \leq P$, $0 < \beta_k < 1$ (Random initialization) with $k = 0$

1) **While** $|C_{S,k} - C_{S,k-1}| > \delta C_{S,k-1}$
2) Find the monomial expression $\widehat{g}$ for g using the Taylor's approximation around $\mathbf{x}_k = [\beta_k, \gamma_{1,k}, \gamma_{2,k}, \gamma_{J,k}]$
3) $k = k + 1$
4) Solve (16) with the monomial approximation $\widehat{g}$ to find $[\beta_k, \gamma_{1,k}, \gamma_{2,k}, \gamma_{J,k}]$
5) Assign C_1^S, C_1^R, C_2^S and C_2^R using above solution
6) **If** $C_1^S - C_1^R \geq 0$ and $C_2^S - C_2^R \geq 0$
   Go to step 1
   Else
   Proceed to Case II
7) Check for Cases II, III and IV in a similar fashion
8) Find the optimal $[\beta_k, \gamma_{1,k}, \gamma_{2,k}, \gamma_{J,k}]$ for the current iteration after going through all cases
9) Assign $C_{S,k} = \frac{1}{2} \log \frac{g(\beta_k, \gamma_{1,k}, \gamma_{2,k}, \gamma_{J,k})}{f(\beta_k, \gamma_{1,k}, \gamma_{2,k}, \gamma_{J,k})}$
10) **End While**

III. Secure Communication with Imperfect CSI

We now investigate the effect of imperfect CSI on sum-secrecy rate. We model the imperfection in channel knowledge as in [27], where the channel gains are given as

$$h_i = \hat{h}_i + \Delta h_i, \tag{19}$$

for $i \in \{1, 2, J\}$. Here $\hat{h}_i$ is the estimated channel coefficient and Δh_i is the error in estimation, which is bounded as $|\Delta h_i| \leq \epsilon_i$. ϵ_i is the maximum possible error in estimating h_i with respect to S_1 and S_2. We consider the worst case scenario where the relay knows all channel gains perfectly, while legitimate nodes S_1 and S_2 concede estimation errors according to (19). In this case, SNRs at the relay corresponding to the messages x_1 and x_2 remain the same as in (6). The signal received at S_2 in the second slot is

$$\begin{aligned} y_2 &= h_2\alpha\left(\sqrt{\widetilde{\beta}P_1}h_1x_1 + \sqrt{\widetilde{\beta}P_2}h_2x_2 + \sqrt{\widetilde{\beta}P_J}h_Jx_J + n_R\right) + n_2 \\ &= (\hat{h}_2 + \Delta h_2)\alpha\Bigg(\sqrt{\widetilde{\beta}P_1}(\hat{h}_1 + \Delta h_1)x_1 + \sqrt{\widetilde{\beta}P_2}(\hat{h}_2 + \Delta h_2)x_2 \\ &\quad + \sqrt{\widetilde{\beta}P_J}(\hat{h}_J + \Delta h_J)x_J) + n_R\Bigg) + n_2, \end{aligned} \tag{20}$$

where $\hat{h}_1$, $\hat{h}_2$, and $\hat{h}_J$ are the channels estimated by node S_2. Using these imperfect channel estimates, the node S_2 tries to cancel the self-interference and the known jammer's signal in the following manner:

$$\begin{aligned} y_2 &= (\hat{h}_2 + \Delta h_2)\alpha(\sqrt{\widetilde{\beta}P_1}(\hat{h}_1 + \Delta h_1)x_1 \\ &\quad + \sqrt{\widetilde{\beta}P_2}(\hat{h}_2 + \Delta h_2)x_2 + \sqrt{\widetilde{\beta}P_J}(\hat{h}_J + \Delta h_J)x_J) + n_R) \\ &\quad + n_2 - \underbrace{\hat{h}_2\alpha(\sqrt{\widetilde{\beta}P_2}\hat{h}_2x_2 + \sqrt{\widetilde{\beta}P_J}\hat{h}_Jx_J)}_{\text{imperfect interference cancellation}}. \end{aligned} \tag{21}$$

It follows that

$$\begin{aligned} y_2 &= \hat{h}_2\alpha\sqrt{\widetilde{\beta}P_1}\hat{h}_1x_1 + (\hat{h}_2 + \Delta h_2)\alpha n_R + n_2 \\ &\quad + \Delta h_2\alpha(\sqrt{\widetilde{\beta}P_1}\hat{h}_1x_1 + \sqrt{\widetilde{\beta}P_2}\hat{h}_2x_2 + \sqrt{\widetilde{\beta}P_J}\hat{h}_Jx_J) \\ &\quad + \hat{h}_2\alpha(\sqrt{\widetilde{\beta}P_1}\Delta h_1x_1 + \sqrt{\widetilde{\beta}P_2}\Delta h_2x_2 + \sqrt{\widetilde{\beta}P_J}\Delta h_Jx_J). \end{aligned}$$

As (21) shows, due to the imperfect CSI, S_2 cannot cancel the jamming signal and the self-interference completely. Here we ignore the smaller terms of the form $\Delta h_i \Delta h_j$ as they will be negligible compared to other terms. The received SNR at S_2 is thus given by (22) at the top of the next page. Using the triangle inequality, it follows that

$$|\hat{h}_i| - |\Delta h_i| \leq h_i \leq |\hat{h}_i| + |\Delta h_i|, \quad \forall\, i \in \{1, 2, J\}.$$

The worst case secrecy rate will occur when

$$h_i = |\hat{h}_i| + |\Delta h_i| = |\hat{h}_i| + \epsilon_i, \quad \forall\, i \in \{1, 2, J\},$$

and this will happen when the phase of h_i and Δh_i are the same and Δh_i concedes maximum error, *i.e.*, $|\Delta h_i| = \epsilon_i$. Then the worst case SNR (denoted by $\text{SNR}_{S_2}^{wc}$) at node S_2 is given by (23) at the top of the next page. Similarly the worst case SNR (denoted by $\text{SNR}_{S_1}^{wc}$) at S_1 is given by (24) at the top of the next page. In (24), we again denote estimated channels by $\hat{h}_1$, $\hat{h}_2$, and $\hat{h}_J$ for brevity, but these values may be different from those estimated by S_2.

Using these worst case SNRs, we maximize the worst case sum-secrecy rate and solve for the corresponding optimal power allocation and β using SGP as done for problem in (16), *i.e.*, for the case of perfect CSI.

IV. Numerical Results and Discussions

A. Effect of Power Splitting Ratio β

Fig. 2 shows the sum-secrecy rate (left y-axis) and the harvested energy (right y-axis) versus the total power budget for

$$\mathrm{SNR}_{S_2} = \frac{|\hat{h}_2|^2\alpha^2\widetilde{\beta}P_1|\hat{h}_1|^2}{N_0(|\hat{h}_2+\Delta h_2|^2\alpha^2+1)+\alpha^2\widetilde{\beta}(|\Delta h_2|^2(P_1|\hat{h}_1|^2+P_2|\hat{h}_2|^2+P_J|\hat{h}_J|^2)+|\hat{h}_2|^2(P_1|\Delta h_1|^2+P_2|\Delta h_2|^2+P_J|\Delta h_J|^2))}. \tag{22}$$

$$\mathrm{SNR}^{wc}_{S_2} = \frac{|\hat{h}_2|^2\alpha^2\widetilde{\beta}P_1|\hat{h}_1|^2}{N_0((|\hat{h}_2|+\epsilon_2)^2\alpha^2+1)+\alpha^2\widetilde{\beta}\epsilon_2^2(P_1|\hat{h}_1|^2+P_2|\hat{h}_2|^2+P_J|\hat{h}_J|^2)+\alpha^2\widetilde{\beta}|\hat{h}_2|^2(P_1\epsilon_1^2+P_2\epsilon_2^2+P_J\epsilon_J^2)}. \tag{23}$$

$$\mathrm{SNR}^{wc}_{S_1} = \frac{|\hat{h}_1|^2\alpha^2\widetilde{\beta}P_2|\hat{h}_2|^2}{N_0((|\hat{h}_1|+\epsilon_1)^2\alpha^2+1)+\alpha^2\widetilde{\beta}\epsilon_1^2(P_1|\hat{h}_1|^2+P_2|\hat{h}_2|^2+P_J|\hat{h}_J|^2)+\alpha^2\widetilde{\beta}|\hat{h}_1|^2(P_1\epsilon_1^2+P_2\epsilon_2^2+P_J\epsilon_J^2)}. \tag{24}$$

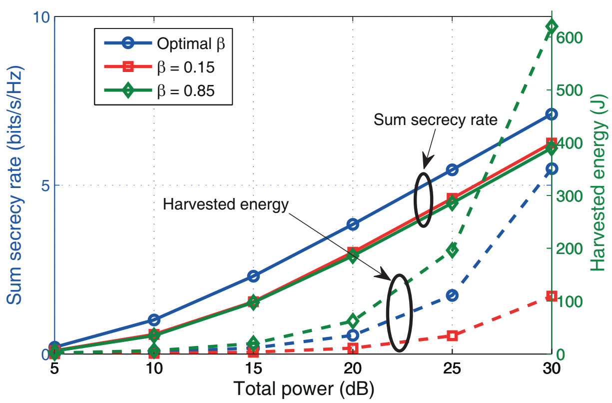

Fig. 2. Effect of β on harvested energy at relay and the sum-secrecy rate.

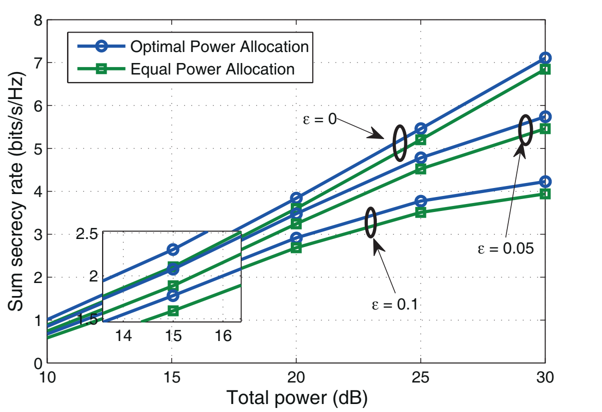

Fig. 3. Effect of power allocation on sum-secrecy rate.

a random channel realization: $|h_1|^2 = 0.6647$, $|h_2|^2 = 2.9152$, and $|h_J|^2 = 1.3289$. We set $\eta = 0.5$ and $N_0 = 1$. Higher β (= 0.85) than the optimal β (the solution of the problem (16)) results in higher harvested energy, which increases relay's transmit power. But the reduced strength of the received information signal at the relay (thus at nodes S_1 and S_2) due to higher β dominates the secrecy performance of the system. A lower β (= 0.15) ensures more power for the information processing at relay, but this reduces the harvested energy (reducing its transmit power to forward the information) and increases the chances of relay eavesdropping the secret message. As a result, the sum-secrecy rate reduces.

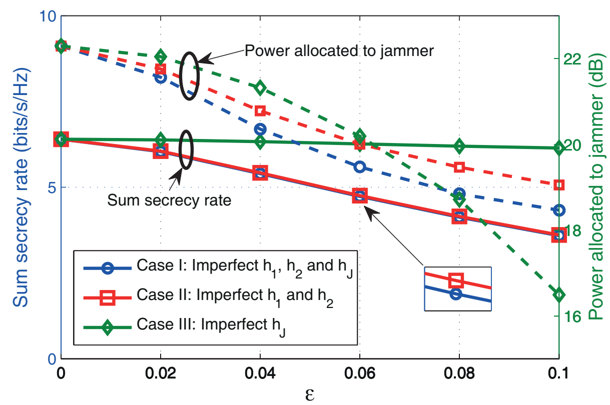

Fig. 4. Effect of ϵ on sum-secrecy rate and and power P_J allocated to the jammer, $|h_1^2| = 1.2479$, $|h_2|^2 = 1.4484$, and $|h_J|^2 = 6.0162$, $P = 30$ dB.

B. Effect of Power Allocation

For different values of maximum channel estimation errors, Fig. 3 compares the sum-secrecy rate when the total power is allocated optimally (obtained by solving the problem (16)) and equally among nodes S_1, S_2, and jammer J for the same system parameters used to obtain Fig. 2. For exposition, we consider $\epsilon_1 = \epsilon_2 = \epsilon_J = \epsilon$ in numerical results. The case $\epsilon = 0$ corresponds to the perfect CSI at S_1 and S_2. Since the equal power allocation does not use channel conditions optimally, it suffers a loss in sum-secrecy rate as expected. Due to the error in channel estimation, the nodes S_1 and S_2 cannot cancel the self-interference (information signals sent to the relay in the first slot) and the jamming signal perfectly from the received signal in the second slot. This reduces the SNR at legitimate nodes S_1 and S_2, which further reduces the sum-secrecy rate.

C. Effect of Imperfect CSI

Fig. 4 shows three cases based on the knowledge of channel conditions at S_1 and S_2.[4] The sum-secrecy rate in Case II is slightly better than that in Case I, because in Case II, a higher fraction of the total power is allocated to the jammer (see the right y-axis of Fig. 4) to use the perfect channel knowledge about h_J. But this has a side-effect: the imperfect CSI on h_1 and h_2 leads to higher interference from the jammer to S_1 and

[4]These three cases in Fig. 4 should not be confused with four cases considered in Section II-D.

S_2. As a result, Case II does not gain much compared to Case I in terms of sum-secrecy rate. Under Case III, the sum-secrecy rate is the highest, because S_1 and S_2 can cancel the jamming signal more effectively as they have imperfect CSI about only one channel. When ϵ is small enough (less than 0.06 in this case), the power allocated to the jammer in Case III is higher than that in Cases I and II. This is because when ϵ is small, if we allocate the power to S_1 and S_2 instead of jammer, it increases relay's chances of eavesdropping the information due to the increased received power, which dominates the detrimental effect incurred due to imperfect cancellation of jammer's signal at S_1 and S_2. But if ϵ goes beyond a threshold, the loss in the secrecy rate due to the imperfect cancellation of jammer's interference dominates and the system is better off by allocating more power to S_1 and S_2 and using each other's signals to confuse the relay. Hence the power allocated to jammer in Case III is smaller than that in Cases I and II at higher ϵ. In Case III, the redistribution of the power from jammer to S_1 and S_2 with the increase in ϵ keeps the sum-secrecy rate almost the same.

V. Concluding Remarks and Future Directions

In a two-way untrusted relay scenario, though the signal from one source can indirectly serve as an artificial noise to the relay while processing other source's signal, the non-zero power allocated to the jammer implies that the assistance from an external jammer can still be useful to achieve a better secrecy rate. But the knowledge of two sources about channel conditions decides the contribution of the jammer in achieving the secure communication. For example, as the channel estimation error on any of the channel increases, the power allocated to the jammer decreases to subside the interference caused at the sources due to the imperfect cancellation of the jamming signal. The optimal power splitting factor balances between the energy harvesting and the information processing at relay. Hence the joint allocation of the total power and the selection of the power splitting factor are necessary to maximize the sum-secrecy rate.

Future directions: There are several interesting future directions that are worth investigating. First the proposed model can be extended to general setups such as multiple antennas at nodes and multiple relays. Another interesting future direction is to investigate the effect of the placement of the jammer and the relay, which also incorporates the effect of path loss. Third we have considered the bounded uncertainty model to characterize the imperfect CSI. Extension to other models of imperfect CSI such as the model where only channel statistics are known is also possible.

References

[1] B. Rankov and A. Wittneben, "Achievable rate regions for the two-way relay channel," in *Proc. 2006 IEEE ISIT*, pp. 1668–1672.

[2] M. Chen and A. Yener, "Multiuser two-way relaying: detection and interference management strategies," *IEEE Trans. Wireless Commun.*, vol. 8, no. 8, pp. 4296–4305, Aug. 2009.

[3] L. Varshney, "Transporting information and energy simultaneously," in *Proc. 2008 IEEE ISIT*, pp. 1612–1616.

[4] X. Zhou, R. Zhang, and C. K. Ho, "Wireless information and power transfer: Architecture design and rate-energy tradeoff," *IEEE Trans. Commun.*, vol. 61, no. 11, pp. 4754–4767, Nov. 2013.

[5] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Relaying protocols for wireless energy harvesting and information processing," *IEEE Trans. Wireless Commun.*, vol. 12, no. 7, pp. 3622–3636, July 2013.

[6] H. Chen, Y. Jiang, Y. Li, Y. Ma, and B. Vucetic, "A game-theoretical model for wireless information and power transfer in relay interference channels," in *Proc. 2014 IEEE ISIT*, pp. 1161–1165.

[7] S. S. Kalamkar and A. Banerjee, "Interference-assisted wireless energy harvesting in cognitive relay network with multiple primary transceivers," in *Proc. 2015 IEEE GLOBECOM*, pp. 1–6.

[8] Z. Chen, B. Xia, and H. Liu, "Wireless information and power transfer in two-way amplify-and-forward relaying channels," in *Proc. 2014 IEEE GLOBALSIP*, pp. 168–172.

[9] Y. Liu, L. Wang, M. Elkashlan, T. Q. Duong, and A. Nallanathan, "Two-way relaying networks with wireless power transfer: Policies design and throughput analysis," in *Proc. 2014 IEEE GLOBECOM*, pp. 4030–4035.

[10] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Jul. 1975.

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

[12] H. Xing, Z. Chu, Z. Ding, and A. Nallanathan, "Harvest-and-jam: Improving security for wireless energy harvesting cooperative networks," in *Proc. 2014 IEEE GLOBECOM*, pp. 3145–3150.

[13] X. Chen, J. Chen, H. Zhang, Y. Zhang, and C. Yuen, "On secrecy performance of a multi-antenna jammer aided secure communications with imperfect CSI," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8014–8024, Oct. 2016.

[14] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.

[15] J. Huang, A. Mukherjee, and A. L. Swindlehurst, "Secure communication via an untrusted non-regenerative relay in fading channels," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2536–2550, May 2013.

[16] L. Wang, M. Elkashlan, J. Huang, N. H. Tran, and T. Q. Duong, "Secure transmission with optimal power allocation in untrusted relay networks," *IEEE Wireless Commun. Lett.*, vol. 3, no. 3, pp. 289–292, June 2014.

[17] L. Sun, P. Ren, Q. Du, Y. Wang, and Z. Gao, "Security-aware relaying scheme for cooperative networks with untrusted relay nodes," *IEEE Commun. Lett.*, vol. 19, no. 3, pp. 463–466, Mar. 2015.

[18] K.-H. Park and M.-S. Alouini, "Secure amplify-and-forward untrusted relaying networks using cooperative jamming and zero-forcing cancelation," in *Proc. 2015 IEEE PIMRC*, pp. 234–238.

[19] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3693–3704, Oct. 2012.

[20] D. Wang, B. Bai, W. Chen, and Z. Han, "Secure green communication via untrusted two-way relaying: A physical layer approach," *IEEE Trans. Commun.*, vol. 64, no. 5, pp. 1861–1874, May 2016.

[21] S. S. Kalamkar and A. Banerjee, "Secure communication via a wireless energy harvesting untrusted relay," *IEEE Trans. Vech. Technol.*, vol. 66, no. 3, pp. 2199–2213, Mar. 2017.

[22] M. Zhao, S. Feng, X. Wang, M. Zhang, Y. Liu, and H. Fu, "Joint power splitting and secure beamforming design in the wireless-powered untrusted relay networks," in *Proc. 2015 IEEE GLOBECOM*, pp. 1–6.

[23] D. J. Su, S. A. Mousavifar, and C. Leung, "Secrecy capacity and wireless energy harvesting in amplify-and-forward relay networks," in *Proc. 2015 IEEE PACRIM*, pp. 258–262.

[24] S. Boyd, S.-J. Kim, L. Vandenberghe, and A. Hassibi, "A tutorial on geometric programming," *Optimization and Engineering*, vol. 8, no. 1, pp. 67–127, 2007.

[25] M. Hayashi and R. Matsumoto, "Construction of wiretap codes from ordinary channel codes," in *Proc. 2010 IEEE ISIT*, pp. 2538–2542.

[26] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, June 2008.

[27] Z. Xiang and M. Tao, "Robust beamforming for wireless information and power transmission," *IEEE Wireless Commun. Lett.*, vol. 1, no. 4, pp. 372–375, Aug. 2012.