Secure Communication Via a Wireless Energy Harvesting Untrusted Relay

Sanket S. Kalamkar *Student Member, IEEE,* and Adrish Banerjee *Senior Member, IEEE*

***Abstract*—The broadcast nature of the wireless medium allows unintended users to eavesdrop the confidential information transmission. In this regard, we investigate the problem of secure communication between a source and a destination via a wireless energy harvesting untrusted node which acts as a helper to relay the information; however, the source and destination nodes wish to keep the information confidential from the relay node. To realize the positive secrecy rate, we use destination-assisted jamming. Being an energy-starved node, the untrusted relay harvests energy from the received radio frequency signals, which include the source's information signal and the destination's jamming signal. Thus, we utilize the jamming signal efficiently by leveraging it as a useful energy source. At the relay, to enable energy harvesting and information processing, we adopt power splitting (PS) and time switching (TS) policies. To evaluate the secrecy performance of this proposed scenario, we derive analytical expressions for two important metrics, viz., the secrecy outage probability and the ergodic secrecy rate. The numerical analysis reveals the design insights into the effects of different system parameters like power splitting ratio, energy harvesting time, target secrecy rate, transmit signal-to-noise ratio (SNR), relay location, and energy conversion efficiency factor, on the secrecy performance. Specifically, the PS policy achieves better optimal secrecy outage probability and optimal ergodic secrecy rate than that of the TS policy at higher target secrecy rate and transmit SNR, respectively.**

***Index Terms*—Destination-assisted jamming, ergodic secrecy rate, secrecy outage probability, untrusted relay, wireless energy harvesting.**

I. Introduction

A. Wireless Energy Harvesting and Cooperative Relaying

ENERGY harvesting is a popular source of energy to power wireless devices [1]–[3]. It holds the potential to prolong the lifetime of energy-constrained nodes and simultaneously avoids the frequent recharging and replacement of batteries, which otherwise would be inconvenient or unacceptable (e.g., medical devices implanted inside a human body). Besides harvesting energy from natural sources like solar, thermal, and wind, the radio frequency (RF) signals in the surrounding wireless environment is a viable source of energy. Exploiting that RF signals can carry both energy and information together, [4]–[6] have proposed the simultaneous wireless energy harvesting and information transfer from the same received RF signals. Since it is difficult for a receiver to harvest energy and process information from the same signal, two practical policies for the wireless energy harvesting and information processing are proposed in [6]–[8]. One policy is the power splitting policy where the receiver splits the received power between energy harvesting and information processing. The second policy involves time switching which divides the time between energy harvesting and information processing.

Such simultaneous energy harvesting and information processing has an application in cooperative relaying [8]–[16]. Using the broadcast nature of the wireless medium, the source transmits the information to an intermediate node, that retransmits it to the destination. In this setup, the relay harvests energy from the received RF information signal and uses it further to forward the information to the destination. The energy harvesting along with the information transfer can prolong the lifetime of a relay, which in turn, facilitates the information cooperation.

B. Physical-Layer Security and Untrusted Relaying

Although the broadcast nature of the wireless medium has facilitated the cooperative communication, it has also allowed unintended nodes, also known as eavesdroppers, to hear the confidential information transmission between the source and the intended destination via a relay, leading to the insecure communication. Traditional approaches to achieve the secure communication include upper-layer cryptographic techniques which require intensive key distribution and management. Unlike this paradigm, the physical-layer information-theoretic security achieves the secure communication by exploiting the nature of the wireless channel. In this regard, Wyner introduced the wiretap channel and showed that the perfect secure communication was possible without relying on private keys [17].

As to the cooperative relaying, the works in [18]–[25] have studied the physical-layer security in the presence of external eavesdroppers that are different from the relay and try to intercept the source-relay and/or relay-destination communications. Even in the absence of external eavesdroppers, the secure communication between source and destination may still be a concern, as one may wish to keep the source-destination communication secret from the relay itself despite its cooperation in forwarding the information [26]. In this case, the relay is considered as an eavesdropper. The model of untrusted relay has practical applications in defence, financial, and government intelligence networks, where all users do not have the same rights to access the information [27]. Also, if the relay belongs to a different network, it may not have the privilege to access the information as that of the source

The authors are with the Department of Electrical Engineering, Indian Institute of Technology Kanpur, India 208016 (e-mail: {kalamkar, adrish}@iitk.ac.in).

Sanket S. Kalamkar is supported by the Tata Consultancy Services (TCS) research fellowship.

and the destination [28]–[31]. One practical scenario is the heterogeneous networks, where different network entities like macrocell, microcell, picocell, and femtocell coexist together in the same geographical area and the information communication between two nodes of the same network happens via a node belonging to a different network. In this case, the relaying node, being from the different network, may be considered untrusted. Another application scenario for the untrusted relay is the one where the relaying node is compromised [32]. For example, in a hostile region like battlefield, an intermediate node relaying the confidential information between the users of a war party can be compromised by the enemy. Considering such possibility, it is important to shield the confidential information from the relaying node to prevent its leakage to the enemy.

In [27], the authors show that even the communication via an untrusted relay can be beneficial for the relay channel with orthogonal components. The works in [33] and [34] show that the positive secrecy rate is achievable with the destination-assisted jamming, where the destination sends jamming signals during the source-relay communication. The references [28]–[30], [35]–[37] investigate the information-theoretic security performance for amplify-and-forward (AF) relays under the fading channel and destination-assisted jamming. The work in [31] studies the secrecy outage probability performance of the communication via an untrusted multi-antenna relay. In [38], the authors advocate the use of friendly jammers to secure the communication via an untrusted relay. To achieve secure as well as spectral efficient communication, the authors in [39] propose link adaptation and relay assignment. With distributed beamforming and opportunistic relaying, the reference [40] studies the capacity scaling and diversity order for secure relaying. In [41], the authors examine the secure relay-assisted communication, where legitimate users, rather considering the relay completely untrusted, have a degree of trust about the relay.

C. Wireless Energy Harvesting with Physical-Layer Security

Recently, with wireless energy harvesting, a few works have studied the physical-layer security in the presence of external eavesdroppers for different scenarios like point-to-point communication with a single antenna [42], [43] and multiple antennas [44]–[47], and the cooperative communication via a relay [48]–[51]. In [48], in the presence of the external energy harvesting receiver, the authors study the secure relay beamforming with simultaneous wireless information and energy transfer. The work in [49] investigates the secrecy performance for an AF relay wiretap channel when the external helpers, who act as jammers to the eavesdropper, harvest energy from the source's transmission. In the presence of an external eavesdropper, in [50], authors have studied the secure communication between a source and a destination via multiple energy harvesting relays; while the work in [51] investigates the secrecy performance of the source-destination communication via an energy harvesting relay with multiple antennas. However, the works in [48]–[51] assume the relay to be trusted, and external eavesdroppers attempt to intercept the relay-assisted communication between the source and the destination. Also, the works on untrusted relay till now have assumed that the conventional energy source, such as battery, powers the relay (see, e.g., [26]–[31], [33]–[36], [38]–[41]).

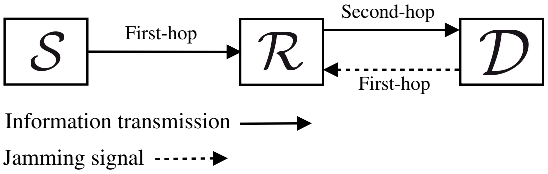


Fig. 1. System Model for the secure communication between a source ($\mathcal{S}$) and a destination ($\mathcal{D}$) via an energy harvesting untrusted relay ($\mathcal{R}$) with destination-assisted jamming.

In this work, we address the problem of secure communication via an energy harvesting untrusted relay. When an untrusted relay harvests energy from the received RF signals, the jamming signal can act as a potential energy source besides its original purpose of realizing the secure communication via untrusted relay. This allows us to use the jamming signal efficiently.

D. Contributions and Key Results

In this paper, we investigate the secrecy performance of a two-hop communication between a source and a destination, where the source uses an AF wireless energy harvesting untrusted relay to forward the confidential information to the legitimate destination. To keep the information secret from the relay, we consider the destination-assisted jamming. The relay harvests energy from received RF signals, which include the information signal from the source and the jamming signal from the destination. We use power splitting (PS) and time switching (TS) receiver architectures [6] at the relay to facilitate the energy harvesting and information processing. We summarize the main contributions and key results below.

- With the jamming signal leveraged as a useful energy source under both PS and TS policies, for an energy harvesting AF relay, we derive analytical expressions for two important measures of secrecy performance—the secrecy outage probability and the ergodic secrecy rate.
- We further compare PS and TS policies, where we show that, at higher target secrecy rate and transmit signal-to-noise ratio (SNR), PS policy achieves lower secrecy outage probability and higher ergodic secrecy rate, respectively.
- The numerical results also show that the power splitting ratio in PS policy and energy harvesting time in TS policy have both constructive and destructive effects on the secure communication between source and destination. Thus, the optimal power splitting ratio in PS policy and the optimal energy harvesting time in TS policy that maximize the secrecy performance do exist.
- For both PS and TS policies, the numerical analysis shows that, the optimal secrecy performance is achieved when the relay is located closer to the destination than to the source. This is in contrast with the case where the wireless energy harvesting relay is considered to be trusted, and the optimum location of the relay is closer to the source.

E. Organization of the Paper

We structure the rest of the paper as follows. Section II describes the system model for the two-hop secure communication via an energy harvesting untrusted relay using the destination-assisted jamming. In Sections III and IV, utilizing the jamming signal as a useful energy source, we derive analytical expressions for the secrecy outage probability and the ergodic secrecy rate for PS policy and TS policy based relaying. We present numerical results in Section V, where we discuss the effects of different system parameters on the secrecy performance of the relay-assisted communication and obtain various design insights. Finally, we provide concluding remarks in Section VI.

II. System Model

A. Destination-Assisted Jamming and Channel Model

As shown in Fig. 1, a source ($\mathcal{S}$) communicates with a destination ($\mathcal{D}$) via an AF energy harvesting relay ($\mathcal{R}$). Despite relay's information cooperation, the source and destination nodes wish to keep the information secret from the relay. To maintain the confidentiality of the source information, the destination sends a jamming signal to the relay when source transmits the information to the relay. Each node operates in a half-duplex mode and has a single antenna. The direct link between $\mathcal{S}$ and $\mathcal{D}$ is unavailable.[1] Let us denote the coefficient of the channel between nodes i and j by h_{ij}. We consider a quasi-static block-fading Rayleigh channel between two nodes, as in [8], [12], [28], [35]. That is, the channel remains constant over a slot-duration of T during which $\mathcal{S}$ transmits to $\mathcal{D}$ via $\mathcal{R}$. The channel power gain is given by $|h_{ij}|^2$, which has exponential distribution with mean λ_{ij}, i.e.,

$$f_{|h_{ij}|^2}(x) = \frac{1}{\lambda_{ij}} \exp\left(-\frac{x}{\lambda_{ij}}\right), \;\; x \geq 0, \tag{1}$$

where $f_{|h_{ij}|^2}(x)$ is the probability density function of random variable $|h_{ij}|^2$. We assume the channel between $\mathcal{R}$ and $\mathcal{D}$ reciprocal, as in [28], [29], [31], [35], [36], i.e., $h_{\mathcal{RD}} = h_{\mathcal{DR}}$. In this work, the source is assumed to have no channel state information (CSI), while the CSI of $\mathcal{S}-\mathcal{R}$ and $\mathcal{R}-\mathcal{D}$ channels are available at the relay and destination, respectively [8]–[10].

B. Energy Harvesting and Information Processing Model

The untrusted relay harvests energy from the received RF signals which it uses to forward the source's information to the destination. To activate the energy harvesting circuitry at the relay, the received power must exceed the minimum threshold power θ_H [3], [52], [53].[2] We assume that the relay has no other energy source and uses the harvested energy completely for the transmission as the power consumed by the relay's transmit/receive circuitry is negligible compared to the power required for the transmission [8], [12]. We adopt following two different receiver architectures based policies at the relay to separately harvest energy from the received RF signals and process the information [7].

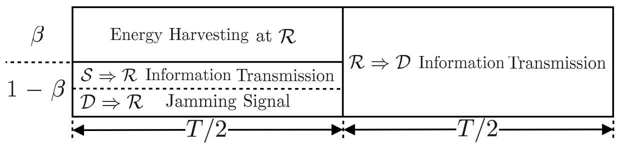

β
$1-\beta$
Energy Harvesting at $\mathcal{R}$
$\mathcal{S} \Rightarrow \mathcal{R}$ Information Transmission
$\mathcal{D} \Rightarrow \mathcal{R}$ Jamming Signal
$\mathcal{R} \Rightarrow \mathcal{D}$ Information Transmission
$T/2$
$T/2$

Fig. 2. Power splitting policy for the secure communication via an energy harvesting untrusted relay.

1. Power splitting (PS) policy: The relay uses a part of the received power to harvest the energy and the remaining part for the information processing.
2. Time switching (TS) policy: The relay switches between the energy harvesting and the information processing. That is, the relay uses a fraction of the time of a slot to harvest the energy and the remaining time for the information processing and relaying.

Note that the relay may attempt to decode the source information with the power used for the information processing.

III. Power Splitting Policy Based Relaying

Fig. 2 shows PS policy based relaying protocol, where the source-to-destination communication happens in a slot of duration T. Two phases of equal duration $T/2$ divide the slot. In the first phase, the source transmits information to the relay with power $P_{\mathcal{S}}$. At the same time, the destination sends a jamming signal with power $P_{\mathcal{D}}$ to the relay to maintain the confidentiality of the source information from the relay. The relay uses a fraction β of the received power for energy harvesting and the remaining $(1-\beta)$ portion for information processing, where $0 \leq \beta \leq 1$. Using the harvested energy, in the second phase, the relay forwards the received information to destination after amplification.

A. Energy Harvesting at Relay

In the aforementioned PS policy, the relay harvests energy E_H given as

$$E_H = \eta\beta\left(P_{\mathcal{S}}|h_{\mathcal{SR}}|^2 + P_{\mathcal{D}}|h_{\mathcal{DR}}|^2\right)(T/2), \tag{2}$$

where η is the energy conversion efficiency factor with $0 < \eta \leq 1$, which is dependent on the energy harvesting circuitry of the relay. The terms $P_{\mathcal{S}}|h_{\mathcal{SR}}|^2$ and $P_{\mathcal{D}}|h_{\mathcal{DR}}|^2$ in (2) denote the power received at the relay due to the information signal from the source and the jamming signal from the destination, respectively. In the second phase of duration $T/2$, the relay's transmit power to forward the information to destination is given as

$$P_H = \frac{E_H}{T/2} = \eta\beta\left(P_{\mathcal{S}}|h_{\mathcal{SR}}|^2 + P_{\mathcal{D}}|h_{\mathcal{DR}}|^2\right). \tag{3}$$

B. Information Processing and Relaying Protocol

In phase one, the received signal $y_{\mathcal{R}}$ for the information processing at the relay is given by

$$y_{\mathcal{R}} = \sqrt{(1-\beta)P_{\mathcal{S}}}h_{\mathcal{SR}}x_{\mathcal{S}} + \sqrt{(1-\beta)P_{\mathcal{D}}}h_{\mathcal{DR}}x_{\mathcal{D}} + n_{\mathcal{R}}, \tag{4}$$

[1] Since the destination operates in a half-duplex mode and sends the jamming signal to the relay during the source's transmission, it cannot receive the information from the source.

[2] The threshold θ_H is usually between -30 dBm to -10 dBm, depending on various factors like channel conditions, frequency of the received RF signals, and energy harvesting circuitry type (linear, non-linear, tunable, etc.) [3].

where $x_{\mathcal{S}}$ is the source message with unit power, $x_{\mathcal{D}}$ is the unit power jamming signal sent by the destination, and $n_{\mathcal{R}}$ is the additive white Gaussian noise (AWGN) at the relay. We assume that the power splitting does not affect the noise power [11], [54]. Based on the received signal $y_{\mathcal{R}}$ in (4), the relay may attempt to decode the source message $x_{\mathcal{S}}$. We can write SNR at the relay as

$$\gamma_{\mathcal{R}} = \frac{(1-\beta)P_{\mathcal{S}}|h_{\mathcal{SR}}|^2}{(1-\beta)P_{\mathcal{D}}|h_{\mathcal{DR}}|^2 + N_0}, \tag{5}$$

where N_0 is the noise power of AWGN $n_{\mathcal{R}}$.

In phase two, the relay amplifies the received signal $y_{\mathcal{R}}$ by a factor ξ based on its power constraint and forwards the resultant signal $x_{\mathcal{R}}$ to the destination, which is given as

$$\begin{aligned} x_{\mathcal{R}} &= \xi y_{\mathcal{R}} & (6)\\ &= \sqrt{\frac{P_H}{(1-\beta)P_{\mathcal{S}}|h_{\mathcal{SR}}|^2 + (1-\beta)P_{\mathcal{D}}|h_{\mathcal{DR}}|^2 + N_0}}\, y_{\mathcal{R}}. & (7) \end{aligned}$$

Then, we substitute (4) in (6) and then use (6) to write the received signal $y'_{\mathcal{D}}$ at the destination as

$$\begin{aligned} y'_{\mathcal{D}} &= h_{\mathcal{RD}} x_{\mathcal{R}} + n_{\mathcal{D}} \\ &= \xi\sqrt{(1-\beta)P_{\mathcal{S}}}h_{\mathcal{SR}}h_{\mathcal{RD}}x_{\mathcal{S}} \\ &\quad + \xi\sqrt{(1-\beta)P_{\mathcal{D}}}h_{\mathcal{RD}}h_{\mathcal{DR}}x_{\mathcal{D}} + \xi h_{\mathcal{RD}}n_{\mathcal{R}} + n_{\mathcal{D}}, \end{aligned} \tag{8}$$

where $n_{\mathcal{D}}$ is the AWGN at the destination with power N_0. Since $x_{\mathcal{D}}$ is the jamming signal sent by the destination itself to the relay in phase one, the destination can remove the term $\xi\sqrt{(1-\beta)P_{\mathcal{D}}}h_{\mathcal{RD}}h_{\mathcal{DR}}x_{\mathcal{D}}$ from (8) and decode the source information from the rest of the received signal.[3] Thus, the resultant received signal $y_{\mathcal{D}}$ at the destination becomes

$$y_{\mathcal{D}} = \xi\sqrt{(1-\beta)P_{\mathcal{S}}}h_{\mathcal{SR}}h_{\mathcal{RD}}x_{\mathcal{S}} + \xi h_{\mathcal{RD}}n_{\mathcal{R}} + n_{\mathcal{D}}. \tag{9}$$

Finally, substituting P_H from (3) in (7), and then using ξ from (7) in (9), we get

$$\begin{aligned} y_{\mathcal{D}} = &\frac{\sqrt{\eta\beta(1-\beta)P_{\mathcal{S}}\left(P_{\mathcal{S}}|h_{\mathcal{SR}}|^2 + P_{\mathcal{D}}|h_{\mathcal{DR}}|^2\right)}h_{\mathcal{SR}}h_{\mathcal{RD}}x_{\mathcal{S}}}{\sqrt{(1-\beta)P_{\mathcal{S}}|h_{\mathcal{SR}}|^2 + (1-\beta)P_{\mathcal{D}}|h_{\mathcal{DR}}|^2 + N_0}} \\ &+ \frac{\sqrt{\eta\beta\left(P_{\mathcal{S}}|h_{\mathcal{SR}}|^2 + P_{\mathcal{D}}|h_{\mathcal{DR}}|^2\right)}h_{\mathcal{RD}}n_{\mathcal{R}}}{\sqrt{(1-\beta)P_{\mathcal{S}}|h_{\mathcal{SR}}|^2 + (1-\beta)P_{\mathcal{D}}|h_{\mathcal{DR}}|^2 + N_0}} + n_{\mathcal{D}}. \end{aligned} \tag{10}$$

The first term on the right hand side of (10) represents the signal part, while the second and third terms correspond to the total received noise at the destination. Then, the SNR at the destination can be written as

$$\gamma_{\mathcal{D}} = \frac{\eta\beta(1-\beta)P_{\mathcal{S}}|h_{\mathcal{SR}}|^2|h_{\mathcal{RD}}|^2}{\eta\beta|h_{\mathcal{RD}}|^2N_0 + N_0(1-\beta) + \frac{N_0^2}{(P_{\mathcal{S}}|h_{\mathcal{SR}}|^2 + P_{\mathcal{D}}|h_{\mathcal{DR}}|^2)}}. \tag{11}$$

C. Secure Communication via an Untrusted Relay

When the relay is considered untrusted, we can write the instantaneous secrecy rate R_{sec} of the relay-assisted communication as [55]

$$\begin{aligned} R_{\text{sec}} &= \frac{1}{2}\left[\log_2\left(1+\gamma_{\mathcal{D}}\right) - \log_2\left(1+\gamma_{\mathcal{R}}\right)\right]^+ \\ &= \frac{1}{2}\left[\log_2\left(\frac{1+\gamma_{\mathcal{D}}}{1+\gamma_{\mathcal{R}}}\right)\right]^+, \end{aligned} \tag{12}$$

where $[x]^+ = \max(x,0)$. The factor $\frac{1}{2}$ represents the effective communication time between the source and the destination. For the rest of the Section III, we assume $P_{\mathcal{S}} = P_{\mathcal{D}} = P$ for analytical tractability.

1) Secrecy Outage Probability: The secrecy outage probability is an important measure of the secrecy performance. It allows us to determine the probability of attaining a target secrecy rate. Given the energy harvesting circuitry of the relay is active, we can express the secrecy outage probability as [55]

$$P_{\text{out}} = \mathbb{P}\left(R_{\text{sec}} < R_{\text{th}}\right), \tag{13}$$

where $\mathbb{P}(\cdot)$ denotes the probability, R_{sec} is the instantaneous secrecy rate given by (12), and R_{th} is the target secrecy rate. Then, substituting $\gamma_{\mathcal{R}}$ from (5) and $\gamma_{\mathcal{D}}$ from (11), we can rewrite (13) as

$$P_{\text{out}} = \mathbb{P}\left(\frac{1 + \frac{\eta\beta(1-\beta)P|h_{\mathcal{SR}}|^2|h_{\mathcal{RD}}|^2}{\left(N_0\eta\beta|h_{\mathcal{RD}}|^2 + N_0(1-\beta)\right) + \frac{N_0^2}{P(|h_{\mathcal{SR}}|^2 + |h_{\mathcal{RD}}|^2)}}}{1 + \frac{(1-\beta)P|h_{\mathcal{SR}}|^2}{(1-\beta)P|h_{\mathcal{RD}}|^2 + N_0}} < 2^{2R_{\text{th}}}\right). \tag{14}$$

We can further express the secrecy outage probability in (14) analytically as given in Proposition 1.

Proposition 1. *The secrecy outage probability for PS policy can be approximately expressed as*

$$P_{\text{out}} \approx 1 - \frac{1}{\lambda_{\mathcal{RD}}}\int_{\theta_1}^{\infty}\exp\left(-\frac{\delta-1}{\nu(x)\lambda_{\mathcal{SR}}} - \frac{x}{\lambda_{\mathcal{RD}}}\right)\mathrm{d}x, \tag{15}$$

where $\delta = 2^{2R_{\text{th}}}$ *with*

$$\theta_1 = \frac{\frac{\delta-1}{1-\beta} + \sqrt{\left(\frac{\delta-1}{1-\beta}\right)^2 + \frac{4\delta P}{\eta\beta N_0}}}{2(P/N_0)}, \tag{16a}$$

and

$$\nu(x) = (1-\beta)\left(\frac{\eta\beta P x}{N_0\left(\eta\beta x + (1-\beta)\right)} - \frac{P\delta}{P(1-\beta)x + N_0}\right). \tag{16b}$$

Proof: See Appendix A. ■

Equation (15) is obtained using the high SNR approximation of the received SNR at the destination given as

$$\gamma_{\mathcal{D}} \approx \frac{\eta\beta(1-\beta)P|h_{\mathcal{SR}}|^2|h_{\mathcal{RD}}|^2}{N_0\left(\eta\beta|h_{\mathcal{RD}}|^2 + (1-\beta)\right)}. \tag{17}$$

Equation (17) can be obtained from the exact expression given in (11) of $\gamma_{\mathcal{D}}$ by neglecting the term $\frac{N_0^2}{(P_{\mathcal{S}}|h_{\mathcal{SR}}|^2 + P_{\mathcal{D}}|h_{\mathcal{DR}}|^2)}$ (due

[3] In the case of channel estimation errors, the destination will have inaccurate knowledge of the channel gain on the relay-destination link, due to which it will not be able to cancel the jamming signal completely, causing self-interference. This, in turn, will reduce the received SNR at the destination, deteriorating the secrecy performance. Given the scope of this paper is to analyze the untrusted nature of an energy harvesting relay on the source-relay-destination communication, we restrict ourselves to study the secrecy performance without channel estimation errors.

to negligible N_0^2 at high SNR) from the denominator of (11).[4] The approximation in (17) is analytically more tractable than the exact expression in (14).[5] Although the integral in (15) cannot be expressed in a closed form, it can be easily evaluated numerically as the integrand consists of elementary functions.

As aforementioned in Section II-B, the received power at the relay must be greater than the minimum power threshold θ_H to activate the energy harvesting circuitry. Using channel reciprocity on the relay-destination link, we can write the received power P_R at the relay as

$$P_R = \left(P|h_{\mathcal{SR}}|^2 + P|h_{\mathcal{RD}}|^2\right). \tag{18}$$

If the received power P_R is less than the power threshold θ_H, the energy harvesting circuitry at the relay stays inactive, leading to the power outage. The following proposition gives the expression for the power outage probability $\mathbb{P}\left(P_R < \theta_H\right)$.

Proposition 2. *We write the power outage probability $P_{\text{p,out}}$ as follows:*

$$P_{\text{p,out}} = \begin{cases} 1 - \frac{\lambda_{\mathcal{SR}}}{\lambda_{\mathcal{SR}} - \lambda_{\mathcal{RD}}} \exp\left(-\frac{\theta_H}{P\lambda_{\mathcal{SR}}}\right) & \\ -\frac{\lambda_{\mathcal{RD}}}{\lambda_{\mathcal{RD}} - \lambda_{\mathcal{SR}}} \exp\left(-\frac{\theta_H}{P\lambda_{\mathcal{RD}}}\right), & \text{if } \lambda_{\mathcal{SR}} \neq \lambda_{\mathcal{RD}} \\ \Upsilon\left(2, \frac{\theta_H}{P\lambda_{\mathcal{SR}}}\right), & \text{if } \lambda_{\mathcal{SR}} = \lambda_{\mathcal{RD}}, \end{cases} \tag{19}$$

where $\Upsilon(a,t) = \int_0^t x^{a-1}\exp(-x)\mathrm{d}x$ is the lower incomplete Gamma function.

Proof: See Appendix B. ■

For an energy constrained untrusted relay, a secrecy outage can also occur if the power received by the relay is insufficient to activate the energy harvesting circuitry [53]. Thus, combining with (15), we can write the overall secrecy outage probability $P_{\text{out}}^{\text{s}}$ as [53]

$$P_{\text{out}}^{\text{s}} = P_{\text{p,out}} + (1 - P_{\text{p,out}})P_{\text{out}}, \tag{20}$$

where P_{out} is given by (15).

2) Probability of Positive Secrecy Rate: The destination-assisted jamming helps to keep the source information confidential from the relay and achieve the secure communication. In this regard, the probability P_{pos} of achieving strictly positive secrecy rate is an important measure of the secrecy performance. We provide the exact and approximate analytical expression for P_{pos} in the following proposition.

Proposition 3. *We write the exact and high SNR approximation analytical expressions for the probability of achieving strictly positive secrecy rate P_{pos} as follows:*

$$\begin{aligned} P_{\text{pos}} = (1 - P_{\text{p,out}}) \Bigg[& \exp\left(-\frac{\theta_3}{\lambda_{\mathcal{RD}}}\right) \\ & + \frac{1}{\lambda_{\mathcal{RD}}} \int_{\theta_2}^{\theta_3} \exp\left(-\left(\frac{\psi(x)}{\lambda_{\mathcal{SR}}} + \frac{x}{\lambda_{\mathcal{RD}}}\right)\right)\mathrm{d}x \Bigg] \qquad \text{(21a)} \\ \approx (1 - P_{\text{p,out}}) & \exp\left(-\sqrt{\frac{\theta_2}{\lambda_{\mathcal{RD}}^2}}\right), \ (\textit{high SNR approximation}), \qquad \text{(21b)} \end{aligned}$$

where

$$\theta_2 = \mathcal{A}, \tag{22a}$$

$$\begin{aligned} \theta_3 = & \left(\frac{\mathcal{B}}{2} + \sqrt{\left(\frac{\mathcal{B}}{2}\right)^2 + \left(-\frac{\mathcal{A}}{3}\right)^3}\right)^{\frac{1}{3}} \\ & + \left(\frac{\mathcal{B}}{2} - \sqrt{\left(\frac{\mathcal{B}}{2}\right)^2 + \left(-\frac{\mathcal{A}}{3}\right)^3}\right)^{\frac{1}{3}}, \end{aligned} \tag{22b}$$

with $\mathcal{A} = \frac{N_0}{\eta\beta P}$ and $\mathcal{B} = \frac{N_0^2}{\eta\beta(1-\beta)P^2}$, and

$$\psi(x) = \frac{N_0^2}{P(1-\beta)(\eta\beta P x^2 - N_0)} - x. \tag{22c}$$

with

$$\psi(x) \begin{cases} < 0, & 0 \le x < \theta_2 \\ \ge 0, & \theta_2 \le x \le \theta_3, \\ < 0, & \theta_3 < x < \infty. \end{cases} \tag{23}$$

θ_2 is the positive root of the equation $g(x) = \eta\beta P x^2 - N_0 = 0$, while θ_3 is the real root of $\psi(x) = 0$ that is equivalent to a cubic equation given as $x^3 - \mathcal{A}x - \mathcal{B} = 0$.

Proof: See Appendix C. ■

3) Ergodic Secrecy Rate: Another important secrecy metric is the ergodic secrecy rate, which is the maximum transmission rate at which the eavesdropper fails to decode the secret information that is being transmitted. We can obtain the ergodic secrecy rate by averaging out the instantaneous secrecy rate R_{sec} over all possible channel realizations. Thus, in the case of untrusted relaying, the ergodic secrecy rate, with the inclusion of power outage probability $P_{\text{p,out}}$ given by (19), can be given as

$$\begin{aligned} \bar{R}_{\text{sec}} &= (1 - P_{\text{p,out}})\mathbb{E}\{R_{\text{sec}}\} \\ &= (1 - P_{\text{p,out}})\mathbb{E}\left\{\frac{1}{2}\left[\log_2\left(\frac{1+\gamma_{\mathcal{D}}}{1+\gamma_{\mathcal{R}}}\right)\right]^+\right\}, \end{aligned} \tag{24}$$

where $\mathbb{E}\{\cdot\}$ is the expectation operator. Using (5) and (11) in (24), we can write the analytical expression for $\bar{R}_{\text{sec}}$ as

$$\begin{aligned} \bar{R}_{\text{sec}} = & (1 - P_{\text{p,out}}) \\ & \times \int_{x=0}^{\infty}\int_{y=0}^{\infty} \left[\frac{1}{2}\log_2\left(\frac{1 + \frac{\eta\beta(1-\beta)Pxy}{\eta\beta N_0 y + N_0(1-\beta) + \frac{N_0^2}{P(x+y)}}}{1 + \frac{(1-\beta)Px}{(1-\beta)Py + N_0}}\right)\right]^+ \\ & \times f_{|h_{\mathcal{SR}}|^2}(x) f_{|h_{\mathcal{RD}}|^2}(y)\,\mathrm{d}x\,\mathrm{d}y. \end{aligned} \tag{25}$$

[4] With $P_{\mathcal{S}} = P_{\mathcal{D}} = P$ and expressing (11) in terms of $\frac{P}{N_0}$, the condition for the high SNR approximation can be given as $\frac{P}{N_0} \gg \frac{1}{\left(|h_{\mathcal{SR}}|^2 + |h_{\mathcal{DR}}|^2\right)}$.

[5] In fact, the complex structure of (14) does not allow us to get an exact analytical expression for the secrecy outage probability. This is because, the term $\left(|h_{\mathcal{SR}}|^2 + |h_{\mathcal{DR}}|^2\right)$ in the denominator of (14) prevents the separation of two random variables $|h_{\mathcal{SR}}|^2$ and $|h_{\mathcal{RD}}|^2$, which in turn, impedes the simplification of (14) to get an exact analytical expression.

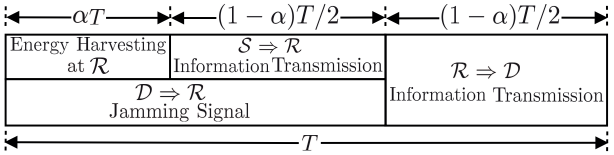


Fig. 3. Time switching policy for the secure communication via an energy harvesting untrusted relay.

Using high SNR approximation for $\gamma_{\mathcal{D}}$ as given in (17), we can write $\bar{R}_{\rm sec}$ as

$$\begin{aligned}\bar{R}_{\rm sec} &\approx (1-P_{\rm p,out}) \\ &\times \int_{x=0}^{\infty}\int_{y=0}^{\infty}\left[\frac{1}{2}\log_2\left(\frac{1+\frac{\eta\beta(1-\beta)P|h_{\mathcal{SR}}|^2|h_{\mathcal{RD}}|^2}{N_0(\eta\beta|h_{\mathcal{RD}}|^2+(1-\beta))}}{1+\frac{(1-\beta)P|h_{\mathcal{SR}}|^2}{(1-\beta)P|h_{\mathcal{RD}}|^2+N_0}}\right)\right]^+ \\ &\times f_{|h_{\mathcal{SR}}|^2}(x) f_{|h_{\mathcal{RD}}|^2}(y)\,\mathrm{d}x\,\mathrm{d}y. \end{aligned}\tag{26}$$

The expressions in (25) and (26) do not admit a closed form and are intractable. Alternatively, we provide a closed-form lower bound on (26) as given in the following Proposition. The lower bound on the ergodic secrecy rate ensures the minimum ergodic secrecy rate under all possible channel conditions for a given set of parameters.[6]

Proposition 4. *The ergodic secrecy rate $\bar{R}_{\rm sec}$ in* (26) *is lower bounded as*

$$\bar{R}_{\rm sec} \geq (1-P_{\rm p,out})\max\left(\frac{1}{2\ln(2)}(T_1-T_2),0\right), \tag{27}$$

where

$$\begin{aligned}T_1 \geq \ln\Bigg(&1+\exp\left(-2\phi-\ln\left(\frac{1}{m_x m_z}\right)\right) \\ &+\exp\left(\frac{1}{m_z}\right)+\mathrm{Ei}\left(-\frac{1}{m_z}\right)\Bigg)\end{aligned}\tag{28a}$$

and

$$T_2 = \begin{cases} 1+\frac{1}{m_x}\exp\left(\frac{1}{m_x}\right)\mathrm{Ei}\left(-\frac{1}{m_x}\right), & \frac{m_y}{m_x}=1 \\ \frac{m_x}{m_x-m_y}\Big[\exp\left(\frac{1}{m_y}\right)\mathrm{Ei}\left(-\frac{1}{m_y}\right) & \\ -\exp\left(\frac{1}{m_x}\right)\mathrm{Ei}\left(-\frac{1}{m_x}\right)\Big], & \frac{m_y}{m_x}\neq 1, \end{cases}\tag{28b}$$

with $m_x = \frac{(1-\beta)P\lambda_{\mathcal{SR}}}{N_0}$, $m_y = \frac{(1-\beta)P\lambda_{\mathcal{RD}}}{N_0}$, $m_z = \frac{\eta\beta\lambda_{\mathcal{RD}}}{1-\beta}$, $\phi \approx 0.577215$, *is the Euler's constant [56, 9.73], and* $\mathrm{Ei}(x) = -\int_{-x}^{\infty}(\exp(-t)/t)\,\mathrm{d}t$, *is the exponential integral [56, 8.21].*

Proof: See Appendix D. ■

The lower bound given in (27) is tight in high SNR regime, which is depicted in Fig. 8 of Section V. Proposition 4 shows that the ergodic secrecy rate depends on the power splitting factor β, energy conversion efficiency factor η, and mean channel gains of source-to-relay and relay-to-destination links.

IV. Time Switching Policy Based Relaying

Fig. 3 shows TS policy based relaying protocol for the secure communication via untrusted relay. The communication between the source and the destination happens over two hops and in a duration of T. The relay harvests energy for αT duration ($0 \leq \alpha \leq 1$) from the received RF signals. The relay spends its harvested energy to forward the received information from the source to the destination. The remaining $(1-\alpha)T$ duration is further split in two sub-slots of equal duration of $\frac{(1-\alpha)T}{2}$. In the first sub-slot, the source transmits the information to relay, which is forwarded to the destination in the second sub-slot after the amplification. The destination sends a jamming signal during the source-to-relay transmission.

A. Energy Harvesting at Relay

For the aforementioned TS policy, the energy E_H harvested during αT duration is given by

$$E_H = \eta\alpha T\left(P_{\mathcal{S}}|h_{\mathcal{SR}}|^2 + P_{\mathcal{D}}|h_{\mathcal{DR}}|^2\right). \tag{29}$$

The relay uses this harvested energy to forward the source information to the destination with power given by

$$P_H = \frac{E_H}{(1-\alpha)T/2} = \frac{2\eta\alpha\left(P_{\mathcal{S}}|h_{\mathcal{SR}}|^2 + P_{\mathcal{D}}|h_{\mathcal{DR}}|^2\right)}{1-\alpha}. \tag{30}$$

B. Information Processing and Relaying Protocol

After the energy harvesting phase, the relay switches to information processing phase, where the received signal is given by

$$y_{\mathcal{R}} = \sqrt{P_{\mathcal{S}}}h_{\mathcal{SR}}x_{\mathcal{S}} + \sqrt{P_{\mathcal{D}}}h_{\mathcal{DR}}x_{\mathcal{D}} + n_{\mathcal{R}}. \tag{31}$$

Note that, unless otherwise stated, all notations in this section have the same meanings as they have in Section III on the power splitting policy based relaying. Using the received signal $y_{\mathcal{R}}$ given in (31), the relay may attempt to decode source information. The received SNR at the relay is given by

$$\gamma_{\mathcal{R}} = \frac{P_{\mathcal{S}}|h_{\mathcal{SR}}|^2}{P_{\mathcal{D}}|h_{\mathcal{DR}}|^2 + N_0}. \tag{32}$$

The relay forwards the amplified version of the received signal to the destination, which is given by

$$x_{\mathcal{R}} = \xi y_{\mathcal{R}} = \sqrt{\frac{P_H}{P_{\mathcal{S}}|h_{\mathcal{SR}}|^2 + P_{\mathcal{D}}|h_{\mathcal{DR}}|^2 + N_0}}\,y_{\mathcal{R}}. \tag{33}$$

Then the received signal $y'_{\mathcal{D}}$ at the destination is given by

$$y'_{\mathcal{D}} = h_{\mathcal{RD}}x_{\mathcal{R}} + n_{\mathcal{D}}. \tag{34}$$

After subtracting the term corresponding to the known jamming signal $x_{\mathcal{D}}$, the resultant received signal $y_{\mathcal{D}}$ at the destination becomes

$$y_{\mathcal{D}} = \xi\sqrt{P_{\mathcal{S}}}h_{\mathcal{SR}}h_{\mathcal{RD}}x_{\mathcal{S}} + \xi h_{\mathcal{RD}}n_{\mathcal{R}} + n_{\mathcal{D}}. \tag{35}$$

Substituting P_H from (30) in (33), and then ξ from (33) in (35), we can write the received signal $y_{\mathcal{D}}$ as

$$\begin{aligned} y_{\mathcal{D}} = &\frac{\sqrt{2\eta\alpha P_{\mathcal{S}}\left(P_{\mathcal{S}}|h_{\mathcal{SR}}|^2 + P_{\mathcal{D}}|h_{\mathcal{DR}}|^2\right)}h_{\mathcal{SR}}h_{\mathcal{RD}}x_{\mathcal{S}}}{\sqrt{(1-\alpha)(P_{\mathcal{S}}|h_{\mathcal{SR}}|^2 + P_{\mathcal{D}}|h_{\mathcal{DR}}|^2 + N_0)}} \\ &+ \frac{\sqrt{2\eta\alpha\left(P_{\mathcal{S}}|h_{\mathcal{SR}}|^2 + P_{\mathcal{D}}|h_{\mathcal{DR}}|^2\right)}h_{\mathcal{RD}}n_{\mathcal{R}}}{\sqrt{(1-\alpha)(P_{\mathcal{S}}|h_{\mathcal{SR}}|^2 + P_{\mathcal{D}}|h_{\mathcal{DR}}|^2 + N_0)}} + n_{\mathcal{D}}. \end{aligned}\tag{36}$$

[6] Such guarantee of minimum performance is a useful criterion in the design of a secure communication system.

The first term on the right hand side of (36) represents the received signal part at the destination, while the last two terms represent the overall noise at the destination. Thus, we can write the received SNR at the destination as

$$\gamma_{\mathcal{D}} = \frac{2\eta\alpha P_{\mathcal{S}}|h_{\mathcal{SR}}|^2|h_{\mathcal{RD}}|^2}{2\eta\alpha|h_{\mathcal{RD}}|^2N_0 + N_0(1-\alpha) + \frac{N_0^2(1-\alpha)}{(P_{\mathcal{S}}|h_{\mathcal{SR}}|^2+P_{\mathcal{D}}|h_{\mathcal{DR}}|^2)}}. \tag{37}$$

For the rest of the Section IV, we assume $P_{\mathcal{S}} = P_{\mathcal{D}} = P$ for analytical tractability.

C. Secure Communication Via an Untrusted Relay

For the proposed TS policy, the instantaneous secrecy rate can be given by

$$\begin{aligned} R_{\text{sec}} &= \frac{(1-\alpha)}{2}\Big[\log_2(1+\gamma_{\mathcal{D}}) - \log_2(1+\gamma_{\mathcal{R}})\Big]^+ \\ &= \frac{(1-\alpha)}{2}\left[\log_2\left(\frac{1+\gamma_{\mathcal{D}}}{1+\gamma_{\mathcal{R}}}\right)\right]^+, \end{aligned} \tag{38}$$

where $\gamma_{\mathcal{R}}$ and $\gamma_{\mathcal{D}}$ are given by (32) and (37), respectively. The factor $(1-\alpha)/2$ denotes the effective time of information transmission between source and destination.

1) Secrecy Outage Probability: We can express the secrecy outage probability as given in the Proposition 5.

Proposition 5. *For TS policy, given the energy harvesting circuitry of the relay is active, the secrecy outage probability is analytically given by* (15)*, where* $\delta = 2^{\frac{2R_{\text{th}}}{1-\alpha}}$ *with*

$$\theta_1 = \frac{(\delta-1)+\sqrt{(\delta-1)^2+4\delta\frac{P(1-\alpha)}{2\eta\alpha N_0}}}{2(P/N_0)}, \tag{39}$$

and

$$\nu(x) = \left(\frac{2\eta\alpha P x}{N_0\left(2\eta\alpha x + (1-\alpha)\right)} - \frac{P\delta}{Px+N_0}\right). \tag{40}$$

Proof: The proof follows the same steps used in Appendix A to derive the secrecy outage probability for PS policy in Proposition 1. Thus, we skip the proof for TS policy for brevity. ■

Note that, for TS policy, the secrecy outage probability under high SNR approximation as given by (15) is obtained by approximating the exact expression of $\gamma_{\mathcal{D}}$ in (37) as

$$\gamma_{\mathcal{D}} \approx \frac{2\eta\alpha P|h_{\mathcal{SR}}|^2|h_{\mathcal{RD}}|^2}{N_0\left(2\eta\alpha|h_{\mathcal{RD}}|^2 + (1-\alpha)\right)}, \tag{41}$$

where we have used the channel reciprocity, i.e., $h_{\mathcal{RD}} = h_{\mathcal{DR}}$. We have obtained (41) from the exact expression of received SNR at the destination given in (37) by neglecting the term $\frac{N_0^2(1-\alpha)}{(P_{\mathcal{S}}|h_{\mathcal{SR}}|^2+P_{\mathcal{D}}|h_{\mathcal{DR}}|^2)}$ in the denominator of (37) due to negligible value of N_0^2 at high SNR. Now, considering the power outage probability, we can finally write the total secrecy outage probability as (20). Note that the power outage probability for PS and TS policies is the same.

2) Probability of Positive Secrecy Rate: The following proposition gives the analytical expression for P_{pos}.

Proposition 6. *We can write* P_{pos} *as* (21)*, where* $\theta_2 = \mathcal{A}$*,* θ_3 *is given by* (22b) *with* $\mathcal{A} = \frac{N_0(1-\alpha)}{2\eta\alpha P}$ *and* $\mathcal{B} = \frac{N_0^2(1-\alpha)}{2\eta\alpha P^2}$*, and*

$$\psi(x) = \frac{N_0^2}{P\left(\frac{2\eta\alpha}{1-\alpha}Px^2 - N_0\right)} - x.$$

Proof: The proof follows the same steps used in Appendix C for PS policy. We skip the proof for TS policy for brevity. ■

3) Ergodic Secrecy Rate: With the inclusion of the power outage probability $P_{\text{p,out}}$ given in (19), the ergodic secrecy rate is calculated by averaging the instantaneous secrecy rate over all possible channel realizations and is given as

$$\begin{aligned} \bar{R}_{\text{sec}} &= (1-P_{\text{p,out}})\mathbb{E}\{R_{\text{sec}}\} \\ &= (1-P_{\text{p,out}})\mathbb{E}\left\{\frac{(1-\alpha)}{2}\left[\log_2\left(\frac{1+\gamma_{\mathcal{D}}}{1+\gamma_{\mathcal{R}}}\right)\right]^+\right\}. \end{aligned} \tag{42}$$

Using (32) and (37) in (42), we can write the analytical expression for $\bar{R}_{\text{sec}}$ as

$$\begin{aligned} \bar{R}_{\text{sec}} = &(1-P_{\text{p,out}}) \\ &\times \int_{x=0}^{\infty}\int_{y=0}^{\infty}\left[\frac{(1-\alpha)}{2}\log_2\left(\frac{1+\frac{2\eta\alpha Pxy}{2\eta\alpha N_0 y + N_0(1-\alpha)+\frac{N_0^2(1-\alpha)}{P(x+y)}}}{1+\frac{Px}{Py+N_0}}\right)\right]^+ \\ &\times f_{|h_{\mathcal{SR}}|^2}(x)f_{|h_{\mathcal{RD}}|^2}(y)\,\mathrm{d}x\,\mathrm{d}y. \end{aligned} \tag{43}$$

Using high SNR approximation for $\gamma_{\mathcal{D}}$ as given in (41), we can write $\bar{R}_{\text{sec}}$ as

$$\begin{aligned} \bar{R}_{\text{sec}} \approx &(1-P_{\text{p,out}}) \\ &\times \int_{x=0}^{\infty}\int_{y=0}^{\infty}\left[\frac{(1-\alpha)}{2}\log_2\left(\frac{1+\frac{2\eta\alpha Pxy}{2\eta\alpha N_0 y + N_0(1-\alpha)}}{1+\frac{Px}{Py+N_0}}\right)\right]^+ \\ &\times f_{|h_{\mathcal{SR}}|^2}(x)f_{|h_{\mathcal{RD}}|^2}(y)\,\mathrm{d}x\,\mathrm{d}y. \end{aligned} \tag{44}$$

Both (43) and (44) do not admit a closed form. Alternatively, we present a closed-form lower bound on (44) as given in the following Proposition.

Proposition 7. *We lower bound the ergodic secrecy rate* $\bar{R}_{\text{sec}}$ *in* (44) *by*

$$\bar{R}_{\text{sec}} \geq (1-P_{\text{p,out}})\max\left(\frac{1-\alpha}{2\ln(2)}(T_1-T_2), 0\right), \tag{45}$$

where T_1 *and* T_2 *are given by* (28a) *and* (28b)*, respectively, with* $m_x = \frac{P\lambda_{\mathcal{SR}}}{N_0}$*,* $m_y = \frac{P\lambda_{\mathcal{RD}}}{N_0}$*, and* $m_z = \frac{2\eta\alpha\lambda_{\mathcal{RD}}}{1-\alpha}$*.*

Proof: The proof follows the same steps used in Appendix D to derive the lower bound on ergodic secrecy capacity for PS policy in Proposition 4. Thus, we skip the proof for TS policy for brevity. ■

The lower bound given in (45) is tight in high SNR regime, which is depicted in Fig. 8 of Section V.

V. Discussions and Results

In this section, we investigate the secrecy performance of source-destination communication via an untrusted wireless energy harvesting relay. We discuss the impact of different system parameters on the secrecy outage probability and the ergodic secrecy rate under both PS and TS policies.

A. System Parameters and Simulation Setup

Unless otherwise stated, we consider the following system parameters. The source power and destination jamming signal power, $P_S = P_D = P = 40 \text{ dBm}$; energy conversion efficiency, $\eta = 0.7$; energy harvesting circuitry activation threshold, $\theta_H = -30 \text{ dBm}$ [52]; and noise power, $N_0 = 10^{-4}$. The distances between source and relay and that between relay and destination are 5m each, i.e., $d_{\mathcal{SR}} = d_{\mathcal{RD}} = 5\text{m}$. The mean channel power gains $\lambda_{\mathcal{SR}}$ and $\lambda_{\mathcal{RD}}$ of the exponential random variables $|h_{\mathcal{SR}}|^2$ and $|h_{\mathcal{RD}}|^2$ are $d_{\mathcal{SR}}^{-\rho}$ and $d_{\mathcal{RD}}^{-\rho}$, respectively, where ρ is the path-loss exponent. Unless otherwise stated, $\rho = 2.7$.

B. Effect of power splitting ratio β and energy harvesting time α

1) Effect of β: Fig. 4 shows the effects of the power splitting ratio β under PS policy and the energy harvesting time α under TS policy on the secrecy outage probability. For PS policy, with the increase in β, the secrecy outage probability initially decreases to a minimum value. The value of β corresponding to the minimum secrecy outage probability is the optimal value of β. If we increase β further beyond the optimal value, the secrecy outage probability also increases. This is because, as β increases, the relay harvests more energy, which in turn, increases the relay's transmit power improving the information reception at the destination. Also, the increased β reduces the received signal strength at the relay which degrades the received SNR $\gamma_{\mathcal{R}}$ at the relay. This enhances the secrecy rate of the communication which reduces the secrecy outage probability. But, once β crosses the optimal value, the poor signal strength at the relay delivers a negative effect on the secrecy outage probability. Due to the amplification of the poor received signal, the relay forwards a noisy signal to the destination which reduces the received SNR $\gamma_{\mathcal{D}}$ at the destination. The increased harvested energy due to the increased β, in turn, the higher transmit power of the relay, cannot compensate for the loss in $\gamma_{\mathcal{D}}$ because of the reduced signal strength. This pushes the secret source-destination communication into the outage more often, increasing the secrecy outage probability. On the similar line, for Fig. 5, we can explain the initial increase of the ergodic secrecy rate with β and then its fall after the optimal β. Figs. 4 and 5 also show that the simulation results are in excellent agreement with analytical results.

2) Effect of α: Fig. 4 shows that, for TS policy, as the energy harvesting time α increases, the secrecy outage probability reduces initially and reaches the minimum value for the optimal value of α. However, the secrecy outage probability begins to increase as α increases beyond its optimal value. This is because, as α increases, the relay spends more time on the energy harvesting, which in turn, increases its transmit power improving the received SNR at the destination. Meanwhile, the increase in α reduces the time available for information processing at both the relay and destination. Now, at the relay, the reduced time for information processing has two opposite effects on the secrecy outage probability. Firstly, it degrades the reception of the signal at the relay and thus deteriorates the eavesdropping channel of the relay improving the secrecy outage probability. On the contrary, since the relay amplifies and forwards the received signal to the destination, the reception at the destination also degrades. Now, when α is less than its optimal value and increasing, the positive effects due to the increased harvested energy at the relay and deterioration of the eavesdropping channel are dominant, and the secrecy outage probability reduces. Once α crosses the optimal value, the effect of the reduced time for information processing becomes dominant, increasing the secrecy outage probability. Similarly, for Fig. 5, we can explain the initial increase of the ergodic secrecy rate with α and then its fall after the optimal α.

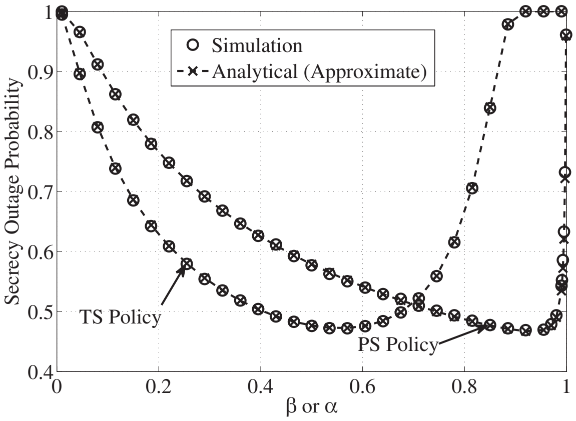


Fig. 4. Effect of the power splitting ratio β and the energy harvesting time α for PS and TS policies, respectively, on the secrecy outage probability, $R_{\text{th}} = 0.5 \text{ bits/s/Hz}$.

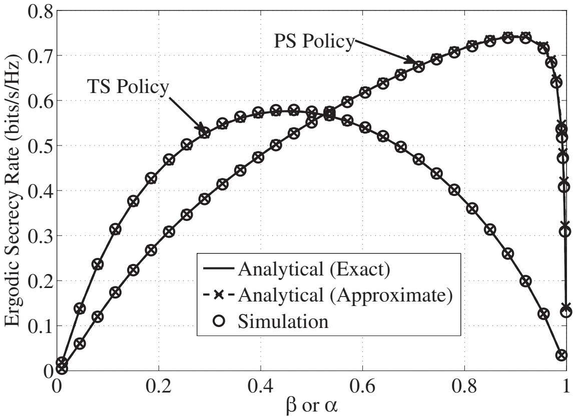


Fig. 5. Effect of the power splitting ratio β and the energy harvesting time α for PS and TS policies, respectively, on the ergodic secrecy rate.

C. Effect of Target Secrecy Rate R_{th}

Fig. 6 plots the optimal secrecy outage probability versus the target secrecy rate R_{th}. As the required secrecy rate con-

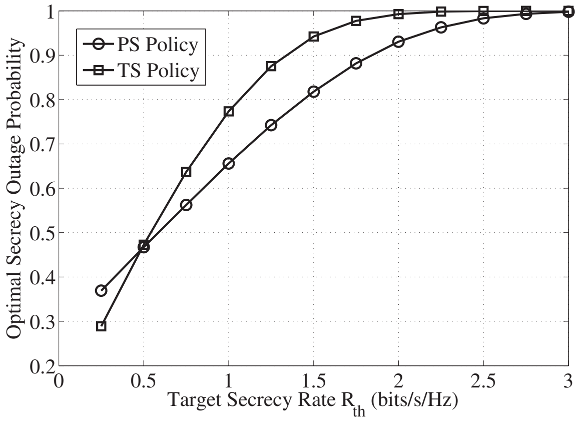


Fig. 6. Effect of target secrecy rate on the optimal secrecy outage probability for PS and TS policies.

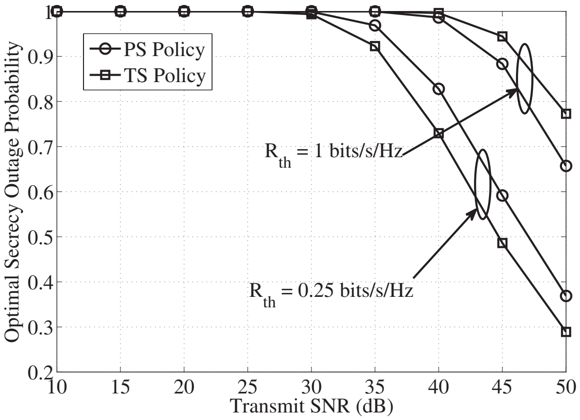


Fig. 7. Optimal secrecy outage probability versus transmit SNR (P/N_0) for PS and TS policies, $N_0 = -10$ dBm.

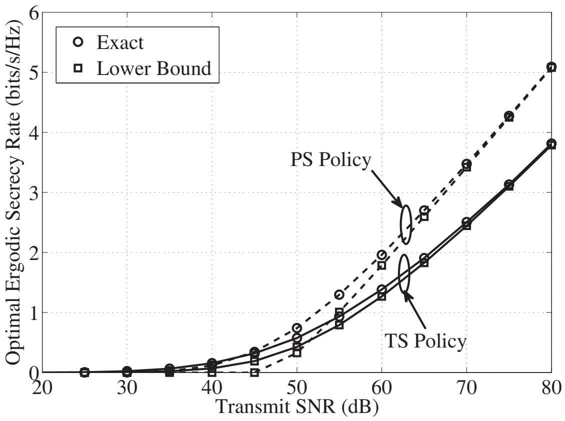


Fig. 8. Optimal ergodic secrecy rate versus transmit SNR (P/N_0) for PS and TS policies, $N_0 = -10$ dBm.

straint becomes tighter, the optimal secrecy outage probability increases. This is because, the higher $R_{\rm th}$ is set, the more it becomes difficult to satisfy, and the likelihood of the secure communication between the source and the destination running into the outage increases. Fig. 6 also shows that TS policy achieves lower secrecy outage probability at low $R_{\rm th}$ (till $0.5\ \text{bits/s/Hz}$) than that of PS policy. On the contrary, at higher secrecy rate constraint, PS policy outperforms TS policy.

D. Effect of Transmit Signal-to-Noise Ratio (SNR)

Fig. 7 illustrates the effect of the transmit SNR, i.e., P/N_0, on the optimal secrecy outage probability for both PS and TS policies. For a fixed noise power N_0, the variation in transmit SNR is equivalent to the variation of source's and destination's power P. The increase in transmit SNR has its constructive as well as destructive effects on the secure communication. The increase in transmit SNR increases the signal strengths of both information signal from the source and jamming signal from the destination. From the expressions of received SNR $\gamma_{\mathcal{R}}$ at the relay given by (5) and (32) for PS and TS policies, respectively, we can note that $\gamma_{\mathcal{R}}$ increases with the increase in transmit SNR. This increases the chances of the untrusted relay decoding the information, which leads to the increase in the secrecy outage probability. On the other hand, the increase in transmit SNR increases the energy harvested by the relay due to higher received powers from information and jamming signals. This causes an increase in the relay's transmit power, which improves SNR at the destination. Also, when relay amplifies and forwards its received signal to the destination, the signal strength is further improved due to the increased signal strength at the relay as a result of the increased transmit SNR. As Fig. 7 shows, the increase in transmit SNR has an overall positive impact on the secrecy performance of the system.

Similarly, Fig. 8 shows that the optimal ergodic secrecy rate improves with the increase in transmit SNR. One interesting observation is that, at lower transmit SNR values, TS policy achieves better optimal ergodic secrecy rate than that of PS policy. On the other hand, at higher transmit SNR, PS policy attains higher ergodic secrecy rate compared to TS policy. From Fig. 8, we can note that, with the increase in transmit SNR, the performance with the closed-form lower bound on the ergodic secrecy rate approaches the performance with the exact analytical expression. Thus, the closed-form lower bound is tight at high transmit SNR for both PS and TS policies.

E. Effect of Relay Placement

Fig. 9 depicts the effect of the relay placement on the optimal secrecy outage probability for different target secrecy rates and path-loss exponents ρ under both PS and TS policies. We vary the source-relay distance $d_{\mathcal{SR}}$, while the relay-destination distance $d_{\mathcal{RD}}$ is $10 - d_{\mathcal{SR}}$. The values of path-loss exponent ρ considered are $\rho = 2.7$ and 4. Before discussing Fig. 9, it is important to understand how $d_{\mathcal{SR}}$ affects the secrecy performance in both constructive and destructive ways. Under both PS and TS policies, as $d_{\mathcal{SR}}$ increases, the received information signal strength at the relay decreases due to the higher path-loss $d_{\mathcal{SR}}^{-\rho}$. This discourages the eavesdropping intention of the untrusted relay, improving the secrecy performance. Also, as $d_{\mathcal{SR}}$ increases, the relay-destination distance $d_{\mathcal{RD}}$ reduces, which makes the received jamming signal at the relay stronger. This further enhances the secrecy performance. The decrease in

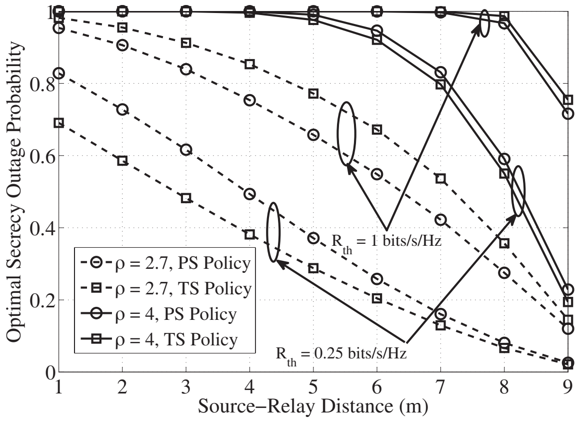


Fig. 9. Effect of relay placement on the optimal secrecy outage probability for PS and TS policies with different path-loss exponents $\rho = 2.7, 4$.

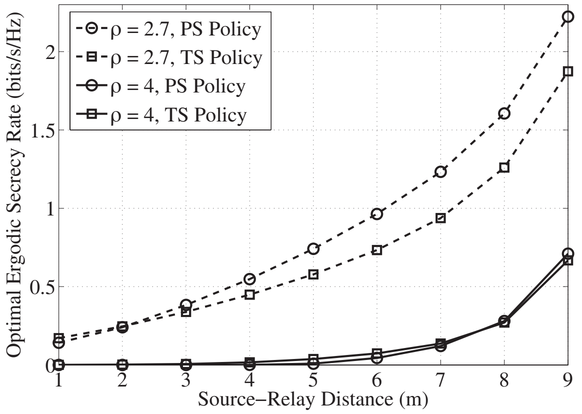


Fig. 10. Effect of relay placement on the optimal ergodic secrecy rate for PS and TS policies with different path-loss exponents $\rho = 2.7, 4$.

$d_{\mathcal{RD}}$ brings the relay closer to the destination due to which the lesser amount of harvested energy is sufficient to perform the reliable communication between relay and destination because of the reduced path-loss $d_{\mathcal{RD}}^{-\rho}$. This saving in the energy is important as, the energy harvested by the relay decreases with the increase in $d_{\mathcal{SR}}$. Another negative effect of the increased $d_{\mathcal{SR}}$ on the secrecy performance is that, due to the amplify-and-forward nature of the relay, as the received signal strength at the relay reduces with the increase in $d_{\mathcal{SR}}$, the information signal strength at the destination also deteriorates. This reduces the secrecy rate and thus increases the secrecy outage probability.

Fig. 9 shows that the constructive effects of the increase in $d_{\mathcal{SR}}$ overtake its destructive effects irrespective of the secrecy rate threshold R_{th} under both PS and TS policies and the optimal secrecy outage probability decreases monotonically with the increase in $d_{\mathcal{SR}}$. Thus, the optimum placement of the relay is closer to the destination. Note that, in the case of wireless energy harvesting communication via a relay without secrecy constraints, the optimum relay placement is close to the source [8]. But, as shown in Figs. 9 and 10, to have secure communication, the relay placement close to the source is not preferred.

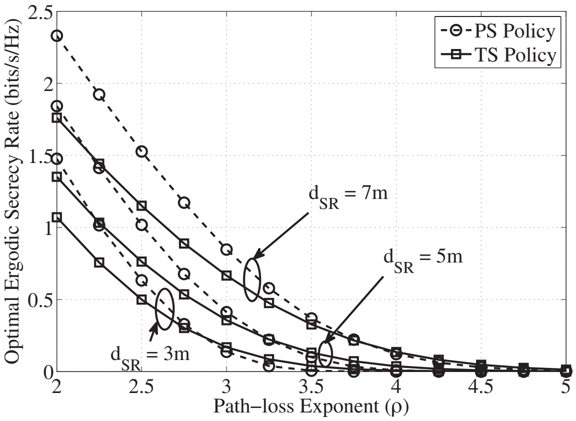
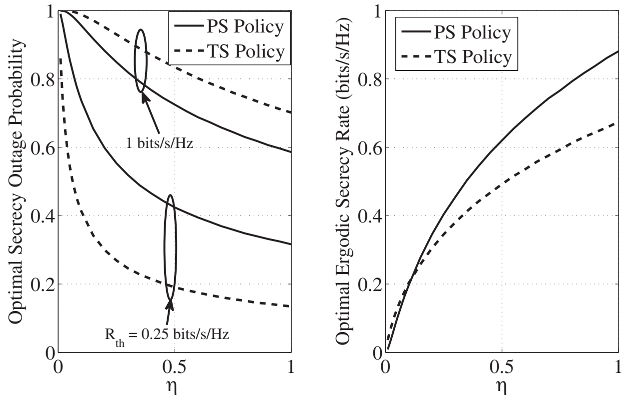


Fig. 11. Effect of path-loss exponent on the optimal ergodic secrecy rate for PS and TS policies with different source-relay distances $d_{\mathcal{SR}} = 3\text{m}, 5\text{m}, 7\text{m}$.

Fig. 10 shows that, for the optimal ergodic secrecy rate, the relay placement has similar effects on the secrecy performance as that on the optimal secrecy outage probability. One interesting observation is that, with the variation in $d_{\mathcal{SR}}$, there exists a crossover point between PS and TS policies, and the location of the crossover point depends on the path-loss exponent. For example, for the path-loss exponent $\rho = 2.7$, TS policy achieves higher optimal ergodic secrecy rate than that of PS policy below $d_{\mathcal{SR}} = 2\text{m}$, i.e., the crossover occurs at $d_{\mathcal{SR}} = 2\text{m}$; while for $\rho = 4$, TS policy achieves higher optimal ergodic secrecy rate than that of PS policy below $d_{\mathcal{SR}} = 8\text{m}$, i.e., the crossover occurs at $d_{\mathcal{SR}} = 8\text{m}$. This is because, at a given path-loss exponent, below the crossover point, the loss in information processing time due to the energy harvesting time in TS policy is lesser than the loss incurred in the relay's transmit power due to power splitting in PS policy. As the distance between relay and destination decreases (with the increase in $d_{\mathcal{SR}}$), the relay may transmit with lower power due to lower path-loss. This subsides the loss incurred in power splitting in PS policy compared to the loss in time for TS policy, and PS policy outperforms TS policy at higher $d_{\mathcal{SR}}$. The increase in path-loss exponent delays the arrival of the crossover point, because, for higher path-loss exponent, the distance between relay and destination should be lower than that in the case of lower path-loss exponent to subside the loss incurred in power splitting. This effect of path-loss exponent on the optimal ergodic secrecy rate can also be seen in Fig. 11 for different source-relay distances. In addition to the effect of the path-loss exponent on the crossover point, Fig. 11 shows that the increase in path-loss exponent is detrimental for the secure communication.

F. Effect of Energy Conversion Efficiency Factor η

The energy conversion efficiency factor η determines what fraction of the received power the relay can actually harvest. Thus, higher η allows relay to harvest more energy, which in turn, boosts relay's transmit power. This results in the enhanced received SNR at the destination, reducing the secrecy outage probability and improving the ergodic secrecy rate, as shown in Figs. 12(a) and 12(b), respectively. At lower η, TS policy



(a) (b)

Fig. 12. Effect of the energy conversion efficiency factor η (a) on the optimal secrecy outage probability, (b) on the optimal ergodic secrecy rate.

achieves better optimal ergodic secrecy rate than that of PS policy and the trend reverses at higher η.

VI. Concluding Remarks

We have investigated the secrecy performance of the source-destination communication via an energy harvesting amplify-and-forward untrusted relay. The energy-starved relay harvests energy from the received radio-frequency signals. In this case, besides keeping the information confidential from the untrusted relay, the destination-assisted jamming signal supplies energy to relay. This energy augments the energy harvested from the received information signal. The PS and TS policies at the relay enable it to harvest energy and process the received information. For this proposed scenario, we have derived analytical expressions for two secrecy metrics, namely, the secrecy outage probability and the ergodic secrecy rate.

The numerical study of the aforementioned secrecy metrics against different system parameters provides useful design insights. For instance, the variation of power splitting ratio in PS policy and energy harvesting time in TS policy affect the secrecy performance in both constructive and destructive ways. Thus, the optimal power splitting ratio and the optimal energy harvesting time exist, that maximize the secrecy performance in terms of both secrecy metrics. The optimal values of secrecy metrics depend on the system parameters. For example, the increase in target secrecy rate increases the optimal secrecy outage probability. Also, at higher target secrecy rate, PS policy achieves lower optimal secrecy outage probability that TS policy. Though the increase in transmit SNR increases the possibility of relay decoding the confidential information, the resulting higher harvested energy and the jamming power dominate the negative effect. Thus, the increase in transmit SNR is beneficial to the secure communication. The relay location is important in the secure communication. In general, having relay located away from the source is beneficial to keep the information confidential from the relay. This is in contrast with the case of trusted energy harvesting relay, where the relay is preferred to be placed closer to the source. Finally, higher energy conversion efficiency factor increases the harvested energy by the relay, which in turn, improves secrecy performance.

Appendix A
Derivation of (15)

At high SNR, using the channel reciprocity between relay and destination and substituting $\gamma_{\mathcal{R}}$ from (5) and $\gamma_{\mathcal{D}}$ from (17) in (12), and then using (12) and (13), we can write the secrecy outage probability for PS policy as

$$\begin{aligned} P_{\text{out}} &= \mathbb{P}\left(\frac{1+\frac{\eta\beta(1-\beta)P|h_{\mathcal{SR}}|^2|h_{\mathcal{RD}}|^2}{N_0(\eta\beta|h_{\mathcal{RD}}|^2+(1-\beta))}}{1+\frac{(1-\beta)P|h_{\mathcal{SR}}|^2}{(1-\beta)P|h_{\mathcal{RD}}|^2+N_0}}<\delta\right), \\ &= \mathbb{P}\left(\nu(X)|h_{\mathcal{SR}}|^2<\delta-1\right)\Big|_{X=|h_{\mathcal{RD}}|^2}, \qquad (46) \end{aligned}$$

where

$$\nu(x)=(1-\beta)\left(\frac{\eta\beta Px}{N_0\left(\eta\beta x+(1-\beta)\right)}-\frac{P\delta}{P(1-\beta)x+N_0}\right). \qquad (47)$$

Based on the sign of $\nu(X)$, we split (46) as

$$\begin{aligned} P_{\text{out}} &= \mathbb{P}\left(|h_{\mathcal{SR}}|^2<\frac{\delta-1}{\nu(X)}\middle|\nu(X)\geq 0\right)\mathbb{P}\left(\nu(X)\geq 0\right) \\ &\quad+\underbrace{\mathbb{P}\left(|h_{\mathcal{SR}}|^2\geq\frac{\delta-1}{\nu(X)}\middle|\nu(X)<0\right)}_{=1}\mathbb{P}\left(\nu(X)<0\right). \qquad (48) \end{aligned}$$

In (48), $\mathbb{P}\left(|h_{\mathcal{SR}}|^2\geq\frac{\delta-1}{\nu(X)}\middle|\nu(X)<0\right)=1$, because $|h_{\mathcal{SR}}|^2$ being an exponential random variable always takes non-negative values. Also, we have

$$\nu(x)\begin{cases}\geq 0, & \text{if } \theta_1\leq x<\infty\\ <0, & \text{if } 0\leq x<\theta_1,\end{cases} \qquad (49)$$

where

$$\theta_1=\frac{\frac{\delta-1}{1-\beta}+\sqrt{\left(\frac{\delta-1}{1-\beta}\right)^2+4\delta\frac{P}{\eta\beta N_0}}}{2(P/N_0)}. \qquad (50)$$

Note that θ_1 is the positive root of the equation $\nu(x)=0$. Using (49), we can write (48) as

$$\begin{aligned} P_{\text{out}} &= \int_{\theta_1}^{\infty}\left(1-\exp\left(-\frac{\delta-1}{\nu(x)\lambda_{\mathcal{SR}}}\right)\right)f_X(x)\,\mathrm{d}x+\int_0^{\theta_1}f_X(x)\,\mathrm{d}x, \\ &= \underbrace{\int_0^{\theta_1}f_X(x)\,\mathrm{d}x+\int_{\theta_1}^{\infty}f_X(x)\,\mathrm{d}x}_{=1} \\ &\quad-\int_{\theta_1}^{\infty}\left(\exp\left(-\frac{\delta-1}{\nu(x)\lambda_{\mathcal{SR}}}\right)\right)f_X(x)\,\mathrm{d}x. \qquad (51) \end{aligned}$$

Substituting $f_X(x)=\frac{1}{\lambda_{\mathcal{RD}}}\exp\left(-\frac{x}{\lambda_{\mathcal{RD}}}\right)$ in the third integral of (51), we reach the required expression of P_{out} as in (15).

Appendix B
Proof of Proposition 2

We can write the power outage probability as

$$\begin{aligned} P_{\text{p,out}} &= \mathbb{P}\left(P_R<\theta_H\right)=\mathbb{P}\left(P(|h_{\mathcal{SR}}|^2+|h_{\mathcal{RD}}|^2)<\theta_H\right) \\ &= \mathbb{P}\left((|h_{\mathcal{SR}}|^2+|h_{\mathcal{RD}}|^2)<\frac{\theta_H}{P}\right). \qquad (52) \end{aligned}$$

Let $Z = \left(|h_{\mathcal{SR}}|^2 + |h_{\mathcal{RD}}|^2\right)$. Since $|h_{\mathcal{SR}}|^2$ and $|h_{\mathcal{RD}}|^2$ are exponentially distributed random variables with means $\lambda_{\mathcal{SR}}$ and $\lambda_{\mathcal{RD}}$, we can write the probability density function of Z as [57]

$$f_Z(z) = \begin{cases} \frac{\exp\left(-\frac{z}{\lambda_{\mathcal{SR}}}\right)}{\lambda_{\mathcal{SR}}-\lambda_{\mathcal{RD}}} + \frac{\exp\left(-\frac{z}{\lambda_{\mathcal{RD}}}\right)}{\lambda_{\mathcal{RD}}-\lambda_{\mathcal{SR}}}, & \text{if } \lambda_{\mathcal{SR}} \neq \lambda_{\mathcal{RD}} \\ \left(\frac{1}{\lambda_{\mathcal{SR}}}\right)^2 z \exp\left(-\frac{z}{\lambda_{\mathcal{SR}}}\right), & \text{if } \lambda_{\mathcal{SR}} = \lambda_{\mathcal{RD}}. \end{cases} \tag{53}$$

Note that Z can take only non-negative values as it is the sum of two exponential random variables. Using (53) in (52), we can write

$$P_{\text{p,out}} = \mathbb{P}\left(Z < \frac{\theta_H}{P}\right) = \int_0^{\frac{\theta_H}{P}} f_Z(z)\mathrm{d}z. \tag{54}$$

Evaluating the integral in (54), we get the required expression for the power outage probability as in (19).

Appendix C
Proof of Proposition 3

A. *Proof of* (21a)

We can write the probability of achieving the positive secrecy capacity as

$$\begin{aligned} P_{\text{pos}} &= (1 - P_{\text{p,out}})\mathbb{P}\left(R_{\text{sec}} > 0\right) \\ &= (1 - P_{\text{p,out}})\mathbb{P}\left(\frac{1}{2}\log_2\left[\frac{(1+\gamma_{\mathcal{D}})}{(1+\gamma_{\mathcal{R}})}\right]^+ > 0\right) \\ &= (1 - P_{\text{p,out}})\mathbb{P}\left(\gamma_{\mathcal{D}} > \gamma_{\mathcal{R}}\right). \end{aligned} \tag{55}$$

Substituting $\gamma_{\mathcal{R}}$ from (5) and $\gamma_{\mathcal{D}}$ from (11) in (55) , we obtain

$$\begin{aligned} \mathbb{P}\left(\gamma_{\mathcal{D}} > \gamma_{\mathcal{R}}\right) = \mathbb{P}\big(\big(\left(|h_{\mathcal{SR}}|^2 + |h_{\mathcal{RD}}|^2\right) \\ \times P(1-\beta)\left(\eta\beta P|h_{\mathcal{RD}}|^4 - N_0\right)\big) > N_0^2\big). \end{aligned} \tag{56}$$

Then we can write

$$\begin{aligned} \mathbb{P}\left(\gamma_{\mathcal{D}} > \gamma_{\mathcal{R}}\right) &= \int_0^{\theta_2} F_{|h_{\mathcal{SR}}|^2}(\psi(x))f_{|h_{\mathcal{RD}}|^2}(x)\,\mathrm{d}x \\ &+ \int_{\theta_2}^{\theta_3} \left[1 - F_{|h_{\mathcal{SR}}|^2}(\psi(x))\right]f_{|h_{\mathcal{RD}}|^2}(x)\,\mathrm{d}x \\ &+ \int_{\theta_3}^{\infty} \left[1 - F_{|h_{\mathcal{SR}}|^2}(\psi(x))\right]f_{|h_{\mathcal{RD}}|^2}(x)\,\mathrm{d}x \\ &= \frac{1}{\lambda_{\mathcal{RD}}}\int_{\theta_2}^{\theta_3} \exp\left(-\left(\frac{\psi(x)}{\lambda_{\mathcal{SR}}} + \frac{x}{\lambda_{\mathcal{RD}}}\right)\right)\,\mathrm{d}x \\ &+ \exp\left(-\frac{\theta_3}{\lambda_{\mathcal{RD}}}\right), \end{aligned} \tag{57}$$

where

$$\psi(x) = \frac{N_0^2}{P(1-\beta)(\eta\beta P x^2 - N_0)} - x \tag{58}$$

with

$$\psi(x)\begin{cases} < 0, & 0 \leq x < \theta_2, \\ \geq 0, & \theta_2 \leq x \leq \theta_3, \\ < 0, & \theta_3 < x < \infty. \end{cases} \tag{59}$$

θ_2 is the positive root of the equation $g(x) = \eta\beta P x^2 - N_0 = 0$, and is given as

$$\theta_2 = \sqrt{\frac{N_0}{\eta\beta P}}, \tag{60}$$

while θ_3 is the real root of $\psi(x) = 0$ which is a cubic equation given as

$$x^3 - \mathcal{A}x - \mathcal{B} = 0, \tag{61}$$

where $\mathcal{A} = \frac{N_0}{\eta\beta P}$ and $\mathcal{B} = \frac{N_0^2}{\eta\beta(1-\beta)P^2}$. We obtain the solution to (61) using Cardano's formula [58], which allows us to find the real root of (61). The solution is given as

$$\begin{aligned} \theta_3 = &\left(\frac{\mathcal{B}}{2} + \sqrt{\left(\frac{\mathcal{B}}{2}\right)^2 + \left(-\frac{\mathcal{A}}{3}\right)^3}\right)^{\frac{1}{3}} \\ &+ \left(\frac{\mathcal{B}}{2} - \sqrt{\left(\frac{\mathcal{B}}{2}\right)^2 + \left(-\frac{\mathcal{A}}{3}\right)^3}\right)^{\frac{1}{3}}. \end{aligned} \tag{62}$$

Substituting (57) in (55), we get the exact expression of the probability of positive secrecy rate given in (21a).

B. *Proof of* (21b)

Under high SNR approximation of $\gamma_{\mathcal{D}}$ given in (17), using (55), we can write the probability of positive secrecy rate as

$$\begin{aligned} &P_{\text{pos}} = (1 - P_{\text{p,out}}) \\ &\times \mathbb{P}\left(\frac{\eta\beta(1-\beta)P|h_{\mathcal{SR}}|^2|h_{\mathcal{RD}}|^2}{N_0\left(\eta\beta|h_{\mathcal{RD}}|^2 + (1-\beta)\right)} > \frac{(1-\beta)P|h_{\mathcal{SR}}|^2}{(1-\beta)P|h_{\mathcal{RD}}|^2 + N_0}\right), \end{aligned} \tag{63}$$

where we have used $\gamma_{\mathcal{R}}$ from (5) with $P_{\mathcal{S}} = P_{\mathcal{D}} = P$ and $h_{\mathcal{DR}} = h_{\mathcal{RD}}$ (channel reciprocity between relay and destination). Simplifying (63), we obtain

$$\begin{aligned} P_{\text{pos}} &= (1 - P_{\text{p,out}})\mathbb{P}\left(|h_{\mathcal{RD}}|^2 > \sqrt{\frac{N_0}{\eta\beta P}}\right) \\ &= (1 - P_{\text{p,out}})\exp\left(-\sqrt{\frac{\theta_2}{\lambda_{\mathcal{RD}}^2}}\right), \end{aligned} \tag{64}$$

where $\theta_2 = \frac{N_0}{\eta\beta P}$.

Appendix D
Proof of Proposition 4

For PS policy, we can write the ergodic secrecy rate as

$$\bar{R}_{\text{sec}} = (1 - P_{\text{p,out}})\mathbb{E}\left\{\frac{1}{2}\left[\log_2\left(\frac{1+\gamma_{\mathcal{D}}}{1+\gamma_{\mathcal{R}}}\right)\right]^+\right\} \tag{65}$$

$$\begin{aligned} &\overset{(a)}{\geq} (1 - P_{\text{p,out}})\left[\mathbb{E}\left\{\frac{1}{2}\log_2\left(\frac{1+\gamma_{\mathcal{D}}}{1+\gamma_{\mathcal{R}}}\right)\right\}\right]^+ \\ &\overset{(b)}{=} (1 - P_{\text{p,out}})\max\left(\frac{1}{2\ln(2)}\left[\underbrace{\mathbb{E}\left\{\ln\left(1 + \frac{XZ}{Z+1}\right)\right\}}_{T_1}\right.\right. \\ &\left.\left. - \underbrace{\mathbb{E}\left\{\ln\left(1 + \frac{X}{Y+1}\right)\right\}}_{T_2}\right], 0\right), \end{aligned} \tag{66}$$

where $X = \frac{(1-\beta)P|h_{\mathcal{SR}}|^2}{N_0}$, $Y = \frac{(1-\beta)P|h_{\mathcal{RD}}|^2}{N_0}$, and $Z = \frac{\eta\beta|h_{\mathcal{RD}}|^2}{1-\beta}$ are the exponential random variables with means $m_x = \frac{(1-\beta)P\lambda_{\mathcal{SR}}}{N_0}$, $m_y = \frac{(1-\beta)P\lambda_{\mathcal{RD}}}{N_0}$, and $m_z = \frac{\eta\beta\lambda_{\mathcal{RD}}}{1-\beta}$, respectively. The inequality (a) is obtained by using the fact $\mathbb{E}\left\{\max(U,V)\right\} \geq \max\left(\mathbb{E}\left\{U\right\},\mathbb{E}\left\{V\right\}\right)$. Also, to obtain equality (b), we have used $\gamma_{\mathcal{R}}$ from (5) and $\gamma_{\mathcal{D}}$ from (17). We can further lower bound T_1 as

$$\begin{aligned} T_1 &= \mathbb{E}\left\{\ln\left(1+\frac{XZ}{Z+1}\right)\right\} \\ &= \mathbb{E}\left\{\ln\left(1+\exp\left(\ln\left(\frac{XZ}{Z+1}\right)\right)\right)\right\} \\ &\overset{\text{(c)}}{\geq} \ln\left(1+\exp\left(\mathbb{E}\left\{\ln\left(\frac{XZ}{Z+1}\right)\right\}\right)\right) \\ &= \ln\left(1+\exp\left(\underbrace{\mathbb{E}\left\{\ln\left(XZ\right)\right\}}_{\mathcal{J}_1} - \underbrace{\mathbb{E}\left\{\ln\left(Z+1\right)\right\}}_{\mathcal{J}_2}\right)\right), \end{aligned} \tag{67}$$

where we have used the convexity of $\ln(1+t\exp(x))$ for $t>0$ and Jensen's inequality to obtain inequality (c).[7] We write

$$\mathcal{J}_1 = \mathbb{E}\left\{\ln\left(XZ\right)\right\} = \int_{x=0}^{\infty}\int_{z=0}^{\infty}\ln(xz)f_X(x)f_Z(z)\,\mathrm{d}x\,\mathrm{d}z,$$

which can be further be written in a compact form using [56, 4.331.1] as

$$\mathcal{J}_1 = -2\phi - \ln\left(\frac{1}{m_x m_z}\right), \tag{68}$$

where ϕ is the Euler's constant [56, 9.73]. We can write $\mathcal{J}_2$ as

$$\mathcal{J}_2 = \mathbb{E}\left\{\ln\left(Z+1\right)\right\} = \int_{z=0}^{\infty}\ln(z+1)f_Z(z)\,\mathrm{d}z, \tag{69}$$

which we can write using [56, 4.337.2] as

$$\mathcal{J}_2 = -\exp\left(\frac{1}{m_z}\right)\mathrm{Ei}\left(-\frac{1}{m_z}\right), \tag{70}$$

where $\mathrm{Ei}(x)$ is the exponential integral [56, 8.21]. Substituting (68) and (70) in (67), we get the required lower bound for T_1.

We can rewrite T_2 as

$$T_2 = \mathbb{E}\left\{\ln\left(1+\gamma_{\mathcal{R}}\right)\right\} = \int_{u=0}^{\infty}\ln(1+u)f_{\gamma_{\mathcal{R}}}(u)\,\mathrm{d}u. \tag{71}$$

Using the integration by parts method, we can rewrite (71) as

$$T_2 = \int_{u=0}^{\infty}\frac{1}{1+u}\left[1-F_{\gamma_{\mathcal{R}}}(u)\right]\mathrm{d}u, \tag{72}$$

where we can write the cumulative distribution function (CDF) $F_{\gamma_{\mathcal{R}}}(u)$ as

$$\begin{aligned} F_{\gamma_{\mathcal{R}}}(u) &= \int_{y=0}^{\infty}F_X((1+y)u)f_Y(y)\,\mathrm{d}y \\ &= \frac{1}{m_y}\int_{y=0}^{\infty}\left[1-\exp\left(-\frac{(1+y)u}{m_x}\right)\right]\exp\left(-\frac{y}{m_y}\right)\mathrm{d}y \\ &= 1-\frac{m_x}{m_x+u m_y}\exp\left(-\frac{u}{m_x}\right). \end{aligned} \tag{73}$$

Substituting (73) in (72) and using [56, 3.353.3] and [56, 3.352.4], we finally obtain the required expression for T_2 as in (28b).

[7] Note that the lower bound on the ergodic secrecy rate is achieved by applying two inequalities (See inequality (a) in (66) and inequality (c) in (67).). Thus, the lower bound is tight in theory when the aforementioned inequalities are held with equality.

References

[1] J. A. Paradiso and T. Starner, "Energy scavenging for mobile and wireless electronics," *IEEE Pervasive Comput.*, vol. 4, no. 1, pp. 18–27, Jan. 2005.

[2] 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, June 2013.

[3] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless networks with RF energy harvesting: A contemporary survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, Second Quarter 2015.

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

[5] P. Grover and A. Sahai, "Shannon meets Tesla: Wireless information and power transfer," in *Proc. 2010 IEEE ISIT*, pp. 2363–2367.

[6] 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.

[7] 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.

[8] 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.

[9] K. Ishibashi, H. Ochiai, and V. Tarokh, "Energy harvesting cooperative communications," in *Proc. 2012 IEEE PIMRC*, pp. 1819–1823.

[10] I. Krikidis, S. Timotheou, and S. Sasaki, "RF energy transfer for cooperative networks: Data relaying or energy harvesting?," *IEEE Commun. Lett.*, vol. 16, no. 11, pp. 1772–1775, Nov. 2012.

[11] Z. Ding, S. M. Perlaza, I. Esnaola, and H. V. Poor, "Power allocation strategies in energy harvesting wireless cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 846–860, Feb. 2014.

[12] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Wireless-powered relays in cooperative communications: Time-switching relaying protocols and throughput analysis," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1607–1622, May 2015.

[13] H. Chen, Y. Li, Y. Jiang, Y. Ma, and B. Vucetic, "Distributed power splitting for SWIPT in relay interference channels using game theory," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 410–420, Jan. 2015.

[14] Z. Yang, Z. Ding, P. Fan, and G. K. Karagiannidis, "Outage performance of cognitive relay networks with wireless information and power transfer," *IEEE Trans. Veh. Technol.*, vol. 65, no. 5, pp. 3828–3833, May 2016.

[15] 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.

[16] Y. Gu and S. Aissa, "RF-based energy harvesting in decode-and-forward relaying systems: Ergodic and outage capacities," *IEEE Trans. Wireless Commun.*, vol. 14, no. 11, pp. 6425–6434, Nov. 2015.

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

[18] I. Krikidis, J. S. Thompson, and S. W. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[19] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "Opportunistic relaying for secrecy communications: Cooperative jamming vs. relay chatting," *IEEE Trans. Wireless Commun.*, vol. 10, no. 6, pp. 1725–1729, June 2011.

[20] Y. Liu, J. Li, and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 4, pp. 682–694, Apr. 2013.

[21] V. N. Q. Bao, N. Linh-Trung, and M. Debbah, "Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 12, pp. 6076–6085, Dec. 2013.

[22] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "On the application of cooperative transmission to secrecy communications," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, pp. 359–368, Feb. 2012.

[23] 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.

[24] C. Jeong and I.-M. Kim, "Optimal power allocation for secure multicarrier relay systems," *IEEE Trans. Signal Process.*, vol. 59, no. 11, pp. 5428–5442, Nov. 2011.

[25] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, and T. Q. Duong, "Relay selection for security enhancement in cognitive relay networks," *IEEE Wireless Commun. Lett.*, vol. 4, pp. 46–49, Feb 2015.

[26] Y. Oohama, "Coding for relay channels with confidential messages," in *Proc. 2001 IEEE ITW*, pp. 87–89.

[27] 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.

[28] 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.

[29] 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.

[30] M. Ju, D.-H. Kim, and K.-S. Hwang, “Opportunistic transmission of nonregenerative network with untrusted relay,” *IEEE Trans. Veh. Technol.*, vol. 64, no. 6, pp. 2703–2709, June 2015.

[31] 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.

[32] Y. Zou, J. Zhu, X. Li, and L. Hanzo, “Relay selection for wireless communications against eavesdropping: A security-reliability tradeoff perspective,” [Available online] http://arxiv.org/abs/1505.07929.

[33] X. He and A. Yener, “Two-hop secure communication using an untrusted relay: A case for cooperative jamming,” in *Proc. 2008 IEEE GLOBECOM*, pp. 1–5.

[34] X. He and A. Yener, “Two-hop secure communication using an untrusted relay,” *EURASIP J. Wireless Commun. Netw.*, vol. 2009, pp. 1–13, 2009.

[35] L. Sun, T. Zhang, Y. Li, and H. Niu, “Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes,” *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3801–3807, Oct. 2012.

[36] Y. Liu, L. Li, and M. Pesavento, “Enhancing physical layer security in untrusted relay networks with artificial noise: A symbol error rate based approach,” in *Proc. 2014 IEEE SAM*, pp. 261–264.

[37] 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.

[38] 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.

[39] H. Khodakarami and F. Lahouti, “Link adaptation with untrusted relay assignment: Design and performance analysis,” *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 4874–4883, Dec. 2013.

[40] J.-B. Kim, J. Lim, and J. M. Cioff, “Capacity scaling and diversity order for secure cooperative relaying with untrustworthy relays,” *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 3866–3876, July 2015.

[41] J. Y. Ryu, J. Lee, and T. Q. S. Quek, “Trust degree-based cooperative transmission for communication secrecy,” in *Proc. 2015 IEEE GLOBECOM*, pp. 1–6.

[42] H. Xing, L. Liu, and R. Zhang, “Secrecy wireless information and power transfer in fading wiretap channel,” *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 180–190, Jan. 2016.

[43] B. He and X. Zhou, “On the placement of RF energy harvesting node in wireless networks with secrecy considerations,” in *Proc. 2014 IEEE Globecom Workshops*, pp. 1355–1360.

[44] D. W. K. Ng, E. S. Lo, and R. Schober, “Robust beamforming for secure communication in systems with wireless information and power transfer,” *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4599–4615, Aug. 2014.

[45] M. R. A. Khandaker and K.-K. Wong, “Robust secrecy beamforming with energy-harvesting eavesdroppers,” *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 10–13, Feb. 2015.

[46] R. Feng, Q. Li, Q. Zhang, and J. Qin, “Robust secure transmission in MISO simultaneous wireless information and power transfer system,” *IEEE Trans. Veh. Technol.*, vol. 64, no. 1, pp. 400–405, Jan. 2015.

[47] Q. Shi, W. Xu, J. Wu, E. Song, and Y. Wang, “Secure beamforming for MIMO broadcasting with wireless information and power transfer,” *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2841–2853, May 2015.

[48] 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.

[49] 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.

[50] H. Xing, K.-K. Wong, and A. Nallanathan, “Secure wireless energy harvesting-enabled AF-relaying SWIPT networks,” in *Proc. 2015 IEEE ICC*, pp. 2307–2312.

[51] X. Chen, J. Chen, and T. Liu, “Secure wireless information and power transfer in large-scale MIMO relaying systems with imperfect CSI,” in *Proc. 2014 IEEE GLOBECOM*, pp. 4131–4136.

[52] J. Guo, S. Durrani, X. Zhou, and H. Yanikomeroglu, “Outage probability of ad hoc networks with wireless information and power transfer,” *IEEE Wireless Commun. Lett.*, vol. 4, no. 4, pp. 409–412, Aug. 2015.

[53] Y. Liu, L. Wang, S. A. R. Zaidi, M. Elkashlan, and T. Q. Duong, “Secure D2D communication in large-scale cognitive cellular networks: A wireless power transfer model,” *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 329–342, Jan. 2016.

[54] L. Liu, R. Zhang, and K.-C. Chua, “Wireless information and power transfer: A dynamic power splitting approach,” *IEEE Trans. Commun.*, vol. 61, no. 9, pp. 3990–4001, Sept. 2013.

[55] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[56] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*. Academic Press, 8th ed., 2015.

[57] A. Papoulis, *Probability, Random Variables and Stochastic Processes*. McGraw-Hill, 3rd ed., 1991.

[58] N. Jacobson, *Basic Algebra I.* W. H. Freeman and Company, 2nd ed., 1996.

Sanket S. Kalamkar received his BTech from College of Engineering Pune, India, in 2009. He is presently working towards his PhD at the Department of Electrical Engineering, Indian Institute of Technology Kanpur, India. His research interests include: cognitive radio networks, wireless communications, and stochastic geometry. He is a recipient of Tata Consultancy Services (TCS) research fellowship.

Adrish Banerjee received his BTech from Indian Institute of Technology Kharagpur, India, and MS and PhD from University of Notre Dame, Indiana. He is currently an Associate Professor in the Department of Electrical Engineering at Indian Institute of Technology Kanpur, India. His research interests include: physical layer aspects of wireless communications, particularly error control coding, cognitive radio, and green communications.