Ann. Telecommun. (2018) 73:341–352
https://doi.org/10.1007/s12243-017-0604-5

Secure communication via an energy-harvesting untrusted relay with imperfect CSI

Van Phu Tuan[1] · **Hyung Yun Kong**[1]

Received: 4 April 2017 / Accepted: 9 August 2017 / Published online: 29 August 2017

Abstract This paper studies the secure communication of an energy-harvesting system in which a source communicates with a destination via an amplify-and-forward (AF) untrusted relay. The relay uses the power-splitting policy to harvest energy from wireless signals. The source is equipped with multiple antennas and uses transmit antenna selection (TAS) and maximum ratio transmission (MRT) to enhance the harvested energy at the relay; for performance comparison, random antenna selection (RAS) is examined. The relay and destination are single-antenna nodes. To create a positive secrecy capacity, destination-assisted jamming is deployed. Because the use of multiple antennas can cause the imperfect channel state information (CSI), the channel between the source and the relay is examined in two cases: perfect CSI and imperfect CSI. To evaluate the secrecy performance, analytical expressions for the secrecy outage probability (SOP) and the average secrecy capacity (ASC) for the TAS, MRT, and RAS schemes are derived. Moreover, a high-power approximation for the SOP is presented. The accuracy of the analytical results is verified by Monte Carlo simulations. The results show the benefit of using multiple antennas in improving the secrecy performance. Specifically, MRT performs better than TAS, and both of them outperform RAS. Moreover, the results provide valuable insight into the effects of various system parameters, such as the channel correlation coefficient, energy-harvesting efficiency, secrecy rate threshold, power-splitting ratio, transmit powers, and locations of the relay, on the secrecy performance.

Keywords Energy harvesting · Power-splitting architecture · Untrusted relay · Amplify-and-forward · Imperfect CSI · Physical layer security

1 Introduction

Wireless energy harvesting (WEH) has considered as a potential technology for prolonging the lifetime of wireless networks in which wireless energy-constrained nodes power their batteries by scavenging energy from ambient radio frequency (RF) signals; hence, much costly and inconvenient of frequent battery replacement and recharging can be reduced [1, 2]. Since the RF signals can carry information as well as energy at the same time, an appealing new research direction of WEH known as "simultaneous wireless information and power transfer" (SWIPT) has recently emerged [3]. To realize the idea of SWIPT, the author of [3] designed two practical receiver architectures, namely, time switching (TS), where each processing block time is separated for harvesting energy and decoding information, and power splitting (PS), where the received signal strength is split into two streams, one for energy harvesting and the other for information decoding.

In [4], SWIPT was implemented in a cooperative communication strategy in which an energy-harvesting (EH) relay collects energy from a source and helps the source to send information to a destination. Work related to SWIPT with multiple cooperative relays was reported in [5]. In [6], the author considered a full duplex relaying SWIPT system where an EH relay collects energy from its two antennas

✉ Hyung Yun Kong
hkong@mail.ulsan.ac.kr

Van Phu Tuan
phutuan87@mail.ulsan.ac.kr

[1] Department of Electrical Engineering, University of Ulsan, Ulsan, South Korea

and operates in full duplex mode to assist the communication between a source and a destination. In the presence of co-channel interference (CCI), the author of [7] studied the effect of CCI on a SWIPT system with a single-antenna EH relay; the extension of [7] to a scenario with a multiple-antenna EH relay was studied in [8]. It was shown in [7, 8] that the CCI could be exploited as a potential energy source. More recently, security in SWIPT has become a focus of research. The authors of [9] studied the effects of artificial noise (AN) and beamforming on the secure transmission of a multiple-input-single-output (MISO) SWIPT system containing a single information receiver (IR) and multiple energy receivers (ERs) which are capable of overhearing the information of IR. The similar work as in [9] for a scenario containing multiple IRs was presented in [10] in which each IR is not only decoding its information but also overhearing the information of the other IRs. For a case in which the relay is considered as a potential eavesdropper (i.e., an untrusted node), the authors of [11] showed that destination-assisted jamming could be effectively exploited to enhance the secrecy performance of an untrusted relaying SWIPT.

Most studies in SWIPT were conducted under the assumption that perfect channel state information (CSI) is available. However, in practical systems, the assumption of perfect CSI is not always valid due to the presence of feedback delay and channel estimation errors. Specifically, for the multiple-antenna systems, an exceedingly large amount of training/feedback overhead in the CSI acquisition causes high feedback delay which leads to the inaccurate CSI. For that reason, imperfect CSI is commonly assumed in the case of employing multiple-antenna techniques, such as transmit antenna selection (TAS) and maximum ratio transmission (MRT) at the transmitter, and selection combining (SC) and maximal ratio combining (MRC) at the receiver [12, 14]. This is because the increase in the number of antenna lead to the significant increase in the CSI acquisition. To the best of our knowledge, there have been no such works in literature to investigate the effect of an imperfect CSI on the secrecy performance of untrusted relaying SWIPT systems.

In this paper, we investigate the secure communication of a SWIPT system in which a multiple-antenna source communicates with a single-antenna destination via an amplify-and-forward (AF) untrusted EH relay. Two multiple-antenna schemes, TAS and MRT, are employed at the source to exploit the benefit of using multiple antennas; moreover, a random antenna selection (RAS) scheme is considered at the source for performance comparison. Although the use of multiple antennas improves the secrecy performance, it can cause the imperfect CSI. Thus, the CSI of the source-to-relay link is examined in two cases: perfect CSI and imperfect CSI whereas the CSI of the relay-to-destination link is assumed to be perfect. To create positive secrecy capacity, a destination-assisted jamming signal that is completely cancelled at the destination is adopted. Moreover, the jamming signal is also exploited as an additional energy source. The power-splitting (PS) receiver architecture is adopted. The secrecy performance is evaluated by analyzing the secrecy outage probability (SOP) and average secrecy capacity (ASC). To accomplish this, we derive the SOP expressions involving a single integral and a tight closed-form upper bound for the ASC. Moreover, closed-form expressions for the SOP at high power levels are also derived. The accuracy of the analytical results is verified by Monte Carlo simulations. Numerical results provide valuable insight into the effects of various system parameters, such as the correlation coefficient between the perfect CSI and imperfect CSI, the energy-harvesting efficiency, the transmit powers, the secrecy rate threshold, the power-splitting ratio, and the locations of the relay, on the secrecy performance.

Notation: $|\cdot|$ is the absolute value operator; $\|\cdot\|$ is the Frobenius norm; $[\cdot]^\top$ is the transpose operator; $[\cdot]^\dagger$ is the Hermitian transpose operator; $\mathcal{CN}(0,\Omega)$ is a complex Gaussian distribution with zero mean and variance Ω; $\mathbb{E}\{\cdot\}$ is the expectation of a random variable; $[x]^+ = \max\{x, 0\}$; $K_\upsilon(\cdot)$ is the υth order modified Bessel function [15, Eq. (8.407.1)]; $Ei(\cdot)$ is the exponential integral function [15, Eq. (8.310.1)]; $\psi(x)$ is the Digamma function [15, Eq. (8.360.1)]; $\Gamma(\cdot)$ is the gamma function [15, Eq. (8.310.1)]; $\Gamma(\alpha, x)$ the lower and upper incomplete gamma functions [15, Eq. (8.350.2)]; and $U(a, b; x)$ is the confluent hypergeometric function of the second kind [15, Eq. (9.211.4)].

2 System model

We consider the secure communication of an energy-harvesting system illustrated in Fig. 1a in which a source S is equipped with N antennas whereas an untrusted relay R and a destination D are single-antenna nodes. R uses the PS policy shown in Fig. 1b to harvest energy and uses the AF protocol to forward the source's signal. In each block time T, the entire communication consists of two time slots, $T/2$. During the first time slot, R harvests energy and decodes information with a power-splitting ratio $0 < \theta < 1$ [4]. Then, R uses all harvested energy to forward the received signal to D during the second time slot. Throughout this paper, we assume that (1) no direct link between S and D exists, (2) the channels follow independent and identical Rayleigh distributions, hence, the channel gains are exponential random variables (RVs), (3) the CSI of the $S \to R$ link is examined in two cases: perfect CSI and imperfect CSI (because of using N antennas at S), whereas the CSI of the $R \to D$ link is perfect, and (4) a local CSI is required at S and R, and the full CSI and the value of transmit power

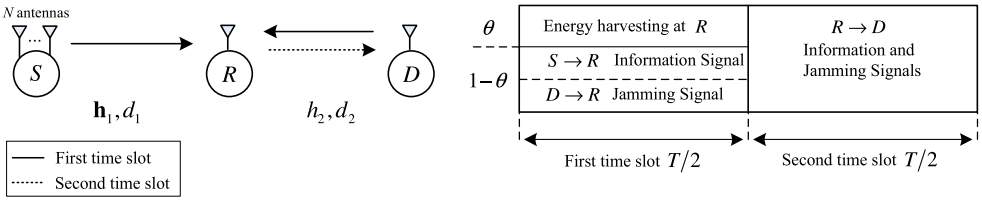

Fig. 1 System model

at R are assumed to be available at D. The full CSI at D is a necessary condition to successfully decode the source signal. This is because the received signal at D in the AF protocol contains both the $S \rightarrow R$ and $R \rightarrow D$ CSI [13]. When D does not attain the $S \rightarrow R$ CSI, D is not capable of decoding the source signal. Moreover, because the $S \rightarrow R$ CSI can be imperfect, R sends the value of its transmit power to D for decoding the source signal optimally.

We denote $\mathbf{h}_1 = \left[h_{1,1}, \ldots, h_{1,N}\right]$ as the channel vector between S and R during the channel estimation and feedback process. The elements of $\mathbf{h}_1$ follow identically and independently distributed (i.i.d.) $\mathcal{CN}(0, \lambda_1^{-1})$ where $\lambda_1 = d_1^{\tau}$, d_1 is the normalized distance between S and R, and τ is the path loss exponent. We denote $\tilde{\mathbf{h}}_1$ as the time-delayed version of $\mathbf{h}_1$. Mathematically, $\tilde{\mathbf{h}}_1$ can be modeled as

$$\tilde{\mathbf{h}}_1 = \sqrt{\zeta}\mathbf{h}_1 + \sqrt{1-\zeta}\mathbf{e}, \tag{1}$$

where $\zeta \in [0, 1]$ is the channel correlation coefficient, and $\mathbf{e}$ is an error vector in which the elements of $\mathbf{e}$ are i.i.d. $\mathcal{CN}(0, \lambda_1^{-1})$. We also denote $h_2 \sim \mathcal{CN}(0, \lambda_2^{-1})$ as the channel between R and D where $\lambda_2 = d_2^{\tau}$ and d_2 is the normalized distance between R and D.

We investigate two transmit antenna schemes, TAS and MRT. In addition, a random antenna selection (RAS) scheme is also considered for performance comparison. In the RAS scheme, S randomly chooses an antenna to transmit its signal x_s, whereas, in the TAS scheme, S selects the best antenna (denote as the n^*-th antenna) to transmit x_s, which satisfies the condition given in Eq. 2.

$$n^* = \underset{1 \leqslant n \leqslant N}{\arg\max} \left\{ \left|h_{1,n}\right|^2 \right\}. \tag{2}$$

In the MRT scheme, S calculates a weight vector $\mathbf{w} = \frac{\mathbf{h}^{\dagger}}{\|\mathbf{h}\|}$ and applies $\mathbf{w}$ to x_s before transmitting x_s on N antennas in the data transmission phase.

2.1 Communication in the first time slot

The received signal at R for three transmit antenna schemes in the first time slot is given by

$$y_r = \begin{cases} \tilde{h}_{1,ran}\sqrt{(1-\theta)\,P_s}x_s + h_2\sqrt{(1-\theta)\,P_d}x_d + n_r & ; \text{(RAS)} \\ \tilde{h}_{1,n*}\sqrt{(1-\theta)\,P_s}x_s + h_2\sqrt{(1-\theta)\,P_d}x_d + n_r & ; \text{(TAS)} \\ \tilde{\mathbf{h}}_1\mathbf{w}_1\sqrt{(1-\theta)\,P_s}x_s + h_2\sqrt{(1-\theta)\,P_d}x_d + n_r & ; \text{(MRT)} \end{cases}, \tag{3}$$

where P_s and P_d are the transmit powers of S and D, respectively, x_d is the AN of D, and $n_r \sim \mathcal{CN}(0, \sigma_0^2)$ is the additive white Gaussian noise (AWGN) at R. Using Eq. 1, we can rewrite Eq. 3 as

$$y_r = \begin{cases} h_{1,ran}\sqrt{\zeta\,(1-\theta)\,P_s}x_s + e\sqrt{(1-\zeta)\,(1-\theta)\,P_s}x_s \\ \quad + h_2\sqrt{(1-\theta)\,P_d}x_d + n_r & ; \text{(RAS)} \\ h_{1,n*}\sqrt{\zeta\,(1-\theta)\,P_s}x_s + e\sqrt{(1-\zeta)\,(1-\theta)\,P_s}x_s \\ \quad + h_2\sqrt{(1-\theta)\,P_d}x_d + n_r & ; \text{(TAS)} \\ \mathbf{h}_1\mathbf{w}_1\sqrt{\zeta\,(1-\theta)\,P_s}x_s + \mathbf{e}\mathbf{w}_1\sqrt{(1-\zeta)\,(1-\theta)\,P_s}x_s \\ \quad + h_2\sqrt{(1-\theta)\,P_d}x_d + n_r & ; \text{(MRT)} \end{cases}. \tag{4}$$

For notational convenience, we define X_1 and $\tilde{X}_1$ as follows.

$$X_1 = \begin{cases} |h_{1,\text{ran}}|^2 & ; \text{(RAS)} \\ |h_{1,n^*}|^2 & ; \text{(TAS)} \\ \|\mathbf{h}_1\mathbf{w}_1\|^2 & ; \text{(MRT)} \end{cases}, \text{ and } \tilde{X}_1 = \begin{cases} |\tilde{h}_{1,\text{ran}}|^2 & ; \text{(RAS)} \\ |\tilde{h}_{1,n^*}|^2 & ; \text{(TAS)} \\ \|\tilde{\mathbf{h}}_1\mathbf{w}_1\|^2 & ; \text{(MRT)} \end{cases}. \tag{5}$$

Then, the harvested energy at R is calculated as

$$E_h = \eta\theta Y T/2, \tag{6}$$

where η is the RF-to-DC conversion efficiency, $Y = P_s\tilde{X}_1 + P_d X_2$ and $X_2 = |h_2|^2$.

From Eq. 4, the signal-to-interference-and-noise ratio (SINR) at R can be expressed as

$$\gamma_r = \frac{\zeta(1-\theta)\rho_s X_1}{(1-\theta)\rho_d X_2 + \mu}, \tag{7}$$

where $\rho_s = P_s/\sigma_0^2$, $\rho_d = P_d/\sigma_0^2$, and $\mu = (1-\zeta)(1-\theta)\frac{\rho_s}{\lambda_1} + 1$.

2.2 Communication in the second time slot

In the second time slot, R uses all harvested energy in Eq. 6 to forward its received signal; therefore, the transmit power of R is $P_r = 2E_h/T = \eta\theta Y$. The received signal at D is given by

$$y_d = \sqrt{P_r}h_2 G y_r + n_d, \tag{8}$$

where $G = 1/\sqrt{\kappa P_r + \sigma_0^2}$ with $\kappa = (1-\theta)/\eta\theta$. Substituting Eqs. 4 into 8 yields

$$y_d = \begin{cases} \underbrace{h_{1,ran} h_2 \sqrt{\zeta\,(1-\theta)\,P_s P_r} G x_s}_{\text{desired signal}} + \underbrace{h_2^2 \sqrt{(1-\theta)\,P_d P_r} G x_d}_{AN} \\ \quad \underbrace{+ e h_2 \sqrt{(1-\zeta)\,(1-\theta)\,P_s P_r} G x_s + h_2 \sqrt{P_r} G n_r + n_d}_{\text{overall noise}} \quad ; \text{(RAS)} \\ \underbrace{h_{1,n*} h_2 \sqrt{\zeta\,(1-\theta)\,P_s P_r} G x_s}_{\text{desired signal}} + \underbrace{h_2^2 \sqrt{(1-\theta)\,P_d P_r} G x_d}_{AN} \\ \quad \underbrace{+ e h_2 \sqrt{(1-\zeta)\,(1-\theta)\,P_s P_r} G x_s + h_2 \sqrt{P_r} G n_r + n_d}_{\text{overall noise}} \quad ; \text{(TAS)} \\ \underbrace{\mathbf{h}_1 \mathbf{w}_1 h_2 \sqrt{\zeta\,(1-\theta)\,P_s P_r} G x_s}_{\text{desired signal}} + \underbrace{h_2^2 \sqrt{(1-\theta)\,P_d P_r} G x_d}_{AN} \\ \quad \underbrace{+ \mathbf{e}\mathbf{w}_1 h_2 \sqrt{(1-\zeta)\,(1-\theta)\,P_s P_r} G x_s + h_2 \sqrt{P_r} G n_r + n_d}_{\text{overall noise}} \quad ; \text{(MRT)} \end{cases} \tag{9}$$

Because D can eliminate the AN in Eq. 9 and $\mathbb{E}\{\mathbf{ew}_1\,(\mathbf{ew})^*\} = \lambda_1^{-1}$, the end-to-end signal-to-noise (SNR) at D is calculated as

$$\gamma_d = \frac{\zeta\,(1-\theta)\,\rho_s X_1 X_2 P_r}{P_r\,(X_2\mu + \kappa) + \sigma_0^2} \approx \frac{\zeta\,(1-\theta)\,\rho_s X_1 X_2}{X_2\mu + \kappa}. \tag{10}$$

The approximation in Eq. 10 is acceptable because the noise variance term is negligible compared to the other factors in the denominator.

3 Performance analysis

3.1 The outage probability

According to [16], the instantaneous secrecy rate of the proposed system is calculated as

$$R_{\text{sec}} = [\mathcal{C}_{\text{d}} - \mathcal{C}_{\text{r}}]^+, \tag{11}$$

where $\mathcal{C}_d = \log_2(1+\gamma_d)$, and $\mathcal{C}_r = \log_2(1+\gamma_r)$. Then, the SOP is given by

$$\begin{aligned} \text{SOP} &= \Pr\left(R_{\text{sec}} < R_{\text{th}}\right) \\ &= \Pr\left(\zeta\,(1-\theta)\,\rho_s X_1 \Xi\,(X_2;\beta) < \beta - 1\right) \\ &= 1 - \Pr\left(X_1 > \frac{\beta-1}{\zeta\,(1-\theta)\,\rho_s \Xi\,(X_2;\beta)} | X_2 > \bar{x}_1\right), \end{aligned} \tag{12}$$

where $\beta = 2^{R_{th}}$, $\Xi(x;\beta) = \frac{x}{\mu x + \kappa} - \frac{\beta}{x(1-\theta)\rho_d + \mu}$, and $\bar{x}_1 = \frac{\mu(\beta-1) + \sqrt{\mu^2(\beta-1)^2 + 4\beta(1-\theta)\rho_d\kappa}}{2(1-\theta)\rho_d}$ is the positive root of the equation $\Xi(x;\beta) = 0$.

Proposition 1 *The SOP of the RAS, TAS, and MRT schemes can be expressed as*

$$SOP_{RAS} = 1 - \lambda_2 \int_{\bar{x}_1}^{+\infty} e^{-\frac{\alpha}{\Xi(x;\beta)} - \lambda_2 x} dx, \tag{13}$$

$$SOP_{TAS} = 1 + \lambda_2 \sum_{n=1}^{N} \binom{N}{n} (-1)^n \int_{\bar{x}_1}^{+\infty} e^{-\frac{n\alpha}{\Xi(x;\beta)} - \lambda_2 x} dx, \tag{14}$$

$$SOP_{MRT} = 1 - \lambda_2 \sum_{n=0}^{N-1} \frac{\alpha^n}{n!} \int_{\bar{x}_1}^{\infty} \Xi(x;\beta)^{-n} e^{-\frac{\alpha}{\Xi(x;\beta)} - \lambda_2 x} dx, \tag{15}$$

where $\alpha = \frac{\lambda_1(\beta-1)}{\zeta(1-\theta)\rho_s}$.

Proof See Appendix A. □

In the case of perfect CSI ($\zeta = 1$), Eq. 13 identically matches with [11, Eq. (15)]. This is because the increase in N in the RAS scheme does not influence the system performance. For that reason, the secrecy performance of the RAS scheme for the case $N > 1$ is equal to that for the case $N = 1$ (when $N = 1$ and $\zeta = 1$, our proposed system is the same with the proposed system of [11]). Similarly, in the case of $N = 1$ and $\zeta = 1$, Eqs. 14 and 15 reduce to the same expression with [11, Eq. (15)].

To the best of our knowledge, the integrals in Eqs. 13–15 do not admit closed-form expressions. Below, we derive the asymptotic functions for the SOP at high power levels, i.e., $(P_s, P_d) \to (\infty, \infty)$.

Proposition 2 *In the case of perfect CSI ($\zeta = 1$), the asymptotic functions for the SOP of the RAS, TAS, and MRT schemes are given by*

$$SOP_{RAS}^{\infty} = SOP_{TAS}^{\infty} = SOP_{MRT}^{\infty} = \lambda_2 \sqrt{\frac{\beta}{\eta\theta\rho_d}}. \tag{16}$$

In the case of imperfect CSI ($0 < \zeta < 1$)

$$SOP_{RAS}^{\infty} = 1 - 2e^{-\frac{\bar{x}_2\lambda_1}{\zeta\omega} - \lambda_2\bar{x}_2} \sqrt{\frac{\bar{x}_2\,(1-\zeta)\,\beta\lambda_2}{\zeta}} K_1\left(2\sqrt{\frac{\bar{x}_2\,(1-\zeta)\,\beta\lambda_2}{\zeta}}\right), \tag{17}$$

$$SOP_{TAS}^{\infty} = 1 + 2\sum_{n=1}^{N} \binom{N}{n} (-1)^n e^{-\frac{n\bar{x}_2\lambda_1}{\zeta\omega} - \lambda_2\bar{x}_2} \times \sqrt{\frac{n\bar{x}_2\,(1-\zeta)\,\beta\lambda_2}{\zeta}} K_1\left(2\sqrt{\frac{n\bar{x}_2\,(1-\zeta)\,\beta\lambda_2}{\zeta}}\right), \tag{18}$$

$$SOP_{MRT}^{\infty} = 1 - \sum_{n=0}^{N-1} \frac{2}{n!} e^{-\frac{\bar{x}_2\lambda_1}{\zeta\omega} - \lambda_2\bar{x}_2} \sum_{k=0}^{n} \binom{n}{k} (\mu_0\alpha)^{n-k} \times \left(\frac{\mu_0\alpha\bar{x}_2\beta\lambda_2}{\beta-1}\right)^{\frac{k+1}{2}} K_{1-k}\left(2\sqrt{\frac{\mu_0\alpha\bar{x}_2\beta\lambda_2}{\beta-1}}\right), \tag{19}$$

where $\omega = \rho_s/\rho_d$, $\mu_0 = (1-\zeta)(1-\theta)\frac{\rho_s}{\lambda_1}$, *and* $\bar{x}_2 = (1-\zeta)(\beta-1)\frac{\omega}{\lambda_1}$.

Proof See Appendix B. □

3.2 The average secrecy capacity

The ASC of the proposed system is given by

$$\bar{R}_{\text{sec}} = \mathbb{E}\left\{[\mathcal{C}_{\text{d}} - \mathcal{C}_{\text{r}}]^+\right\}. \tag{20}$$

Using the fact that $\mathbb{E}\{\max\{x, y\}\} \geqslant \max\{\mathbb{E}\{x\}, \mathbb{E}\{y\}\}$, the lower bound of the ASC can be determined as

$$\bar{R}_{\text{sec,low}} = \left[\bar{\mathcal{C}}_d - \bar{\mathcal{C}}_r\right]^+, \tag{21}$$

where $\bar{\mathcal{C}}_d = \mathbb{E}\left\{\log_2(1+\gamma_d)\right\}$, and $\bar{\mathcal{C}}_r = \mathbb{E}\left\{\log_2(1+\gamma_r)\right\}$.

We first derive the closed-form expression for $\bar{\mathcal{C}}_d$. Considering the function $f(x) = \ln(1+e^x)$, it can be seen that $f(x)$ is a convex function and linearly increases for high values of x. Then, using Jensen's inequality for $f(x)$, we can approximate $\bar{\mathcal{C}}_d$ as

$$\begin{aligned}\mathcal{C}_d &= \mathbb{E}\left\{\log_2\left(1+e^{\ln(\gamma_d)}\right)\right\}\\ &\approx \log_2\left(1+e^{\mathbb{E}\{\ln(\gamma_d)\}}\right)\\ &\approx \log_2\left(1+e^{\ln(\zeta(1-\theta)\rho_s)+\mathcal{J}_1+\mathcal{J}_2-\mathcal{J}_3}\right),\end{aligned} \tag{22}$$

where $\mathcal{J}_1 = \mathbb{E}\{\ln(X_1)\}$, $\mathcal{J}_2 = \mathbb{E}\{\ln(X_2)\}$, and $\mathcal{J}_3 = \mathbb{E}\{\ln(X_2\mu+\kappa)\}$.

Proposition 3 *$\bar{\mathcal{C}}_d$ of the RAS, TAS, and MRT schemes can be approximated as*

$$\mathcal{C}_d^{RAS} \approx \log_2\left(1+\exp\left(\ln\left(\tfrac{\zeta(1-\theta)\rho_s}{\kappa\lambda_1\lambda_2}\right)+2\Psi(1)+e^{\frac{\lambda_2\kappa}{\mu}}Ei\left(-\tfrac{\lambda_2\kappa}{\mu}\right)\right)\right), \tag{23}$$

$$\begin{aligned}\mathcal{C}_d^{TAS} \approx \log_2\Bigg(1+\exp\Bigg(&\ln\left(\tfrac{\zeta(1-\theta)\rho_s}{\kappa\lambda_2}\right)+2\Psi(1)+e^{\frac{\lambda_2\kappa}{\mu}}Ei\left(-\tfrac{\lambda_2\kappa}{\mu}\right)\\ &-N\sum_{n=0}^{N-1}\binom{N-1}{n}\frac{(-1)^n}{(n+1)}\ln((n+1)\lambda_1)\Bigg)\Bigg),\end{aligned} \tag{24}$$

$$\begin{aligned}\mathcal{C}_d^{MRT} \approx \log_2\Bigg(1+\exp\Bigg(&\ln\left(\tfrac{\zeta(1-\theta)\rho_s}{\kappa\lambda_1\lambda_2}\right)+\psi(N)+\Psi(1)\\ &+e^{\frac{\lambda_2\kappa}{\mu}}Ei\left(-\tfrac{\lambda_2\kappa}{\mu}\right)\Bigg)\Bigg).\end{aligned} \tag{25}$$

Proof See Appendix C. □

Next, we derive the closed-form expression for $\bar{\mathcal{C}}_r$. According to [17], $\bar{\mathcal{C}}_r$ is calculated as

$$\bar{\mathcal{C}}_r = \mathbb{E}\left\{\log_2(1+\gamma_r)\right\} = \frac{1}{\ln(2)}\int_0^\infty \frac{1-F_{\gamma_r}(\gamma)}{1+\gamma}. \tag{26}$$

Proposition 4 *$\bar{\mathcal{C}}_r$ of the RAS scheme is calculated as follows.*

- *For* $\lambda_1 \neq \lambda_2\zeta\omega$*:*

$$\begin{aligned}\bar{\mathcal{C}}_r^{RAS} \approx \frac{1}{\ln(2)\left(1-\frac{\lambda_1}{\lambda_2\zeta\omega}\right)}\Bigg(&e^{\frac{\mu\lambda_2\zeta\omega}{\zeta(1-\theta)\rho_s}}Ei\left(\tfrac{-\mu\lambda_2\omega}{(1-\theta)\rho_s}\right)\\ &-e^{\frac{\lambda_1\mu}{\zeta(1-\theta)\rho_s}}Ei\left(\tfrac{-\lambda_1\mu}{\zeta(1-\theta)\rho_s}\right)\Bigg).\end{aligned} \tag{27}$$

- *For* $\lambda_1 = \lambda_2\zeta\omega$*:*

$$\bar{\mathcal{C}}_r^{RAS} \approx \frac{1}{\ln(2)}\left(1+\frac{\lambda_1\mu}{\zeta(1-\theta)\rho_s}e^{\frac{\lambda_1\mu}{\zeta(1-\theta)\rho_s}}Ei\left(\tfrac{-\lambda_1\mu}{\zeta(1-\theta)\rho_s}\right)\right). \tag{28}$$

$\bar{\mathcal{C}}_r$ of the TAS scheme is calculated as follows.

- *For* $n\lambda_1 \neq \lambda_2\zeta\omega$*:*

$$\begin{aligned}\bar{\mathcal{C}}_r^{TAS} \approx &\sum_{n=1}^{N}\binom{N}{n}\frac{(-1)^{n+1}}{\ln(2)\left(1-\frac{n\lambda_1}{\lambda_2\zeta\omega}\right)}\\ &\times\left(e^{\frac{\mu\lambda_2\zeta\omega}{\zeta(1-\theta)\rho_s}}Ei\left(\tfrac{-\mu\lambda_2\omega}{(1-\theta)\rho_s}\right)-e^{\frac{n\lambda_1\mu}{\zeta(1-\theta)\rho_s}}Ei\left(\tfrac{-n\lambda_1\mu}{\zeta(1-\theta)\rho_s}\right)\right).\end{aligned} \tag{29}$$

- *For* $n\lambda_1 = \lambda_2\zeta\omega$*:*

$$\bar{\mathcal{C}}_r^{TAS} \approx \sum_{n=1}^{N}\binom{N}{n}\frac{(-1)^{n+1}}{\ln(2)}\left(1+\frac{n\lambda_1\mu}{\zeta(1-\theta)\rho_s}e^{\frac{n\lambda_1\mu}{\zeta(1-\theta)\rho_s}}Ei\left(\tfrac{-n\lambda_1\mu}{\zeta(1-\theta)\rho_s}\right)\right). \tag{30}$$

$\bar{\mathcal{C}}_r$ of the MRT scheme is calculated as follows.

- *For* $\lambda_1 \neq \lambda_2\zeta\omega$*:*

$$\begin{aligned}\bar{\mathcal{C}}_r^{MRT} \approx &\frac{\lambda_2}{\ln(2)}\sum_{n=0}^{N-1}\frac{1}{n!}\left(\frac{\lambda_1}{\zeta\omega}\right)^n\sum_{k=0}^{n}\binom{n}{k}\left(\frac{\mu}{(1-\theta)\rho_d}\right)^{n-k}\Gamma(k+1)\\ &\times\Bigg(A_0e^{\frac{\lambda_1\mu}{\zeta(1-\theta)\rho_s}}\Gamma(n+1)\Gamma\left(-n, \tfrac{\lambda_1\mu}{\zeta(1-\theta)\rho_s}\right)\\ &+\sum_{i=1}^{k+1}\frac{A_i}{\lambda_2^i}\left(\frac{\zeta\omega\lambda_2}{\lambda_1}\right)^{n+1}\Gamma(n+1)U\left(n+1, n-i+2; \tfrac{\omega\lambda_2\mu}{(1-\theta)\rho_s}\right)\Bigg).\end{aligned} \tag{31}$$

- *For* $\lambda_1 = \lambda_2\zeta\omega$*:*

$$\begin{aligned}\bar{\mathcal{C}}_r^{MRT} \approx &\frac{\lambda_2}{\ln(2)}\sum_{n=0}^{N-1}\frac{1}{n!}\left(\frac{\lambda_1}{\zeta\omega}\right)^n\sum_{k=0}^{n}\binom{n}{k}\left(\frac{\mu}{(1-\theta)\rho_d}\right)^{n-k}\\ &\times\left(\frac{\zeta\omega}{\lambda_1}\right)^{k+1}\Gamma(k+1)\Gamma(n+1)U\left(n+1, n-k; \tfrac{\omega\lambda_2\mu}{(1-\theta)\rho_s}\right).\end{aligned} \tag{32}$$

where $A_0 = \left(\lambda_2-\frac{\lambda_1}{\zeta\omega}\right)^{-k-1}$ *and* $A_i = \frac{-\lambda_1}{\zeta\omega}\left(\lambda_2-\frac{\lambda_1}{\zeta\omega}\right)^{-k-2+i}$.

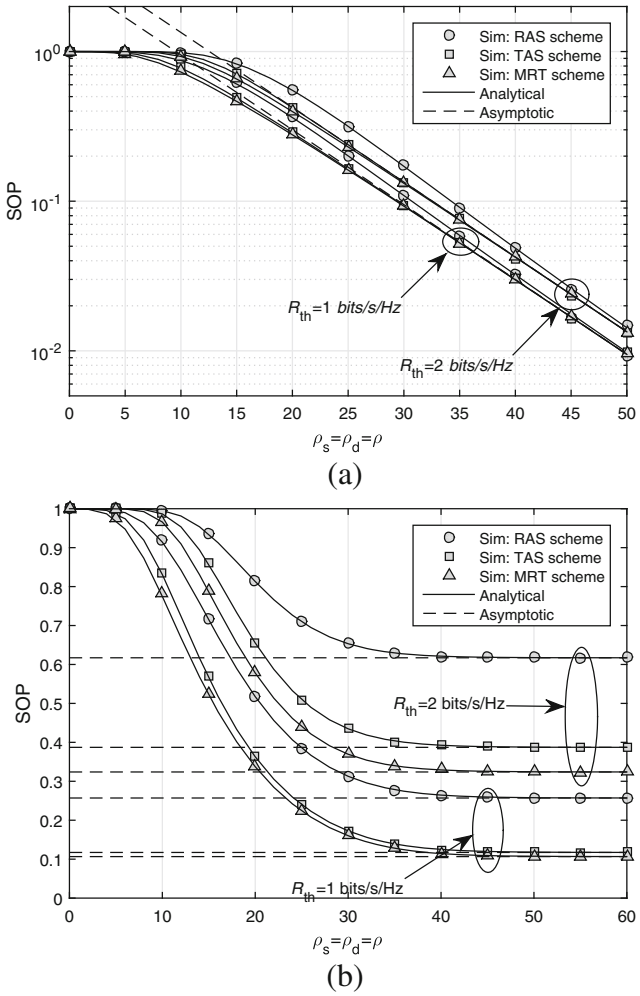

Fig. 2 The effect of ρ on the SOP and its asymptote in the cases of **a** $\zeta = 1$ and **b** $\zeta = 0.9$. Other parameters: $d = 1$ and $\rho_s = \rho_d = \rho$

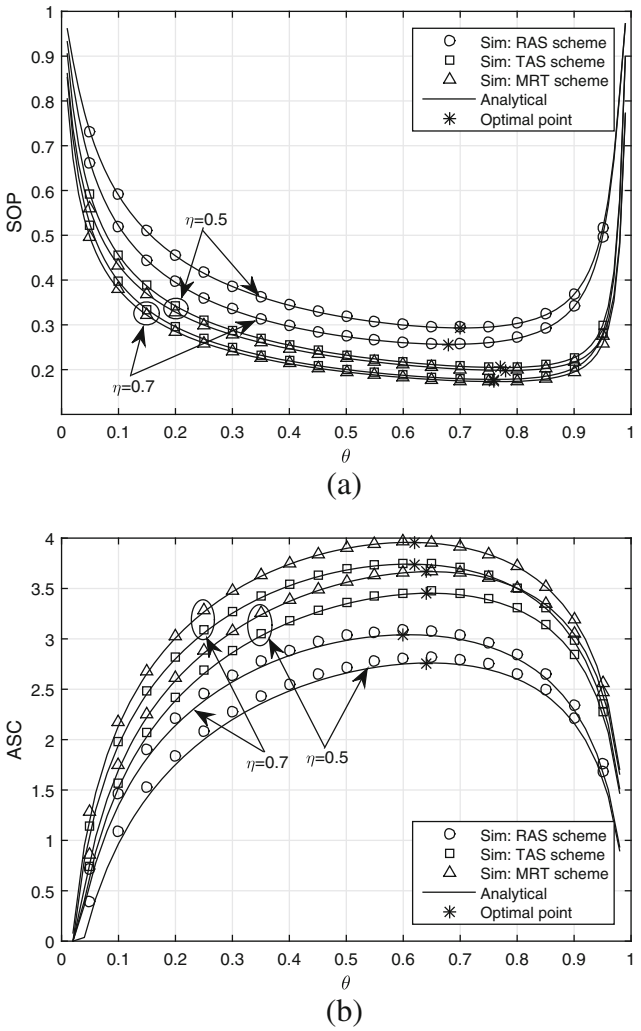

Fig. 3 The effect of θ on the SOP and ASC. Other parameters: $d = 1$, $\rho_s = \rho_d = 25(dB)$ and $R_s = 2(bits/sec/Hz)$

Proof See Appendix D. □

4 Results and discussion

In this section, we present numerical results to validate the analytical expressions presented in Section 3. Unless otherwise specified, we set $\eta = 0.5, \theta = 0.5, \tau = 3$, $R_{th} = 1 bits/s/Hz$, $N = 3$, and $\sigma_0^2 = 1$. The coordinates in the two-dimensional plane of S, D, and R are set to $(0, 0)$, $(2, 0)$, and $(d, 0.2)$, respectively.

In Fig. 2, we show the SOP and its asymptote when both S and D increase their transmit powers, i.e., $\rho_s = \rho_d = \rho$. As can be seen, when ρ increases, the SOP for perfect CSI remarkably improves while that in the case of imperfect CSI converges to a determined value. These results can be explained using the effect of the noise caused by imperfect CSI on the SOP. Particularly, in the case of imperfect CSI, the strength of this noise linearly increases with the signal strength; hence, the SOP converges at high ρ values. Comparing the three antenna schemes, we observe that the MRT provides a better SOP than the TAS scheme, and both the MRT and TAS schemes outperform the RAS scheme; especially in the case of imperfect CSI, these trends become even clearer. Additionally, the SOP is an increasing function of R_{th}. This result can be explained by Eq. 12, in which the probability that R_{sec} is less than R_{th} becomes greater as R_{th} increases. Moreover, as shown in Fig. 2, the asymptote agrees well with the exact SOP at high ρ values.

In Fig. 3, we investigate the effect of θ on the SOP and ASC. The value of θ is varied from 0 to 1. As shown, the SOP and ASC improve as θ increases from 0 to the corresponding optimal power-splitting ratios, at which point the SOP or ASC achieve the best values, and they rapidly become worse with further increases in θ. This result can be explained using the effect of θ on the harvested energy

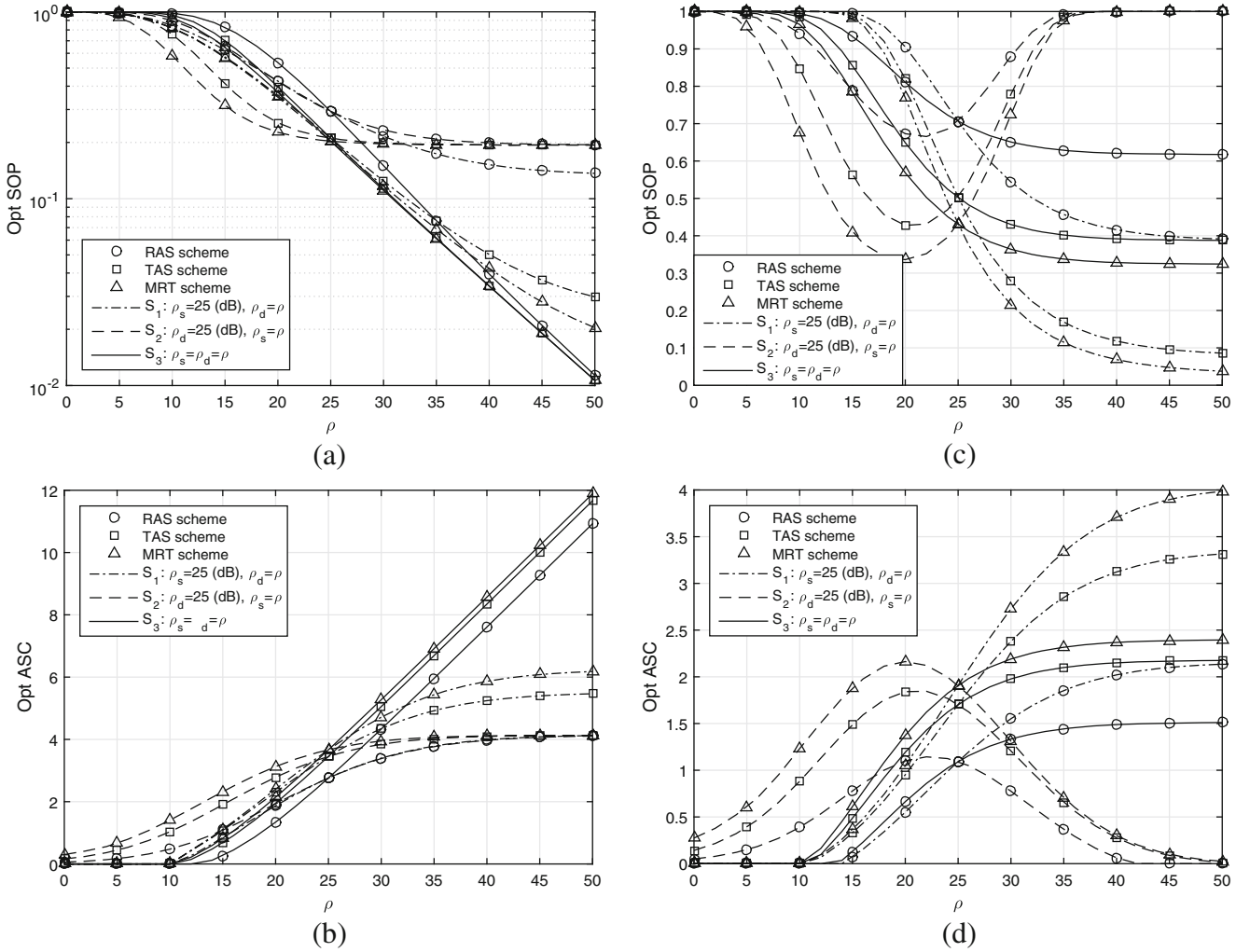

Fig. 4 The effect of ρ_s and ρ_d on the optimal SOP and optimal ASC. Other parameters: $d = 1$ and $R_{th} = 2(bits/sec/Hz)$

and the signal strength portion used for information decoding at R. At low θ values, the secrecy performance is low due to the low harvested energy at R; at high θ values, the secrecy performance is low due to the low input signal strength at the information-decoding component of R. Thus, the optimal power-splitting ratio θ^*, which balances the signal strength portions employed for the information-receiving task and energy-harvesting task at R, provides the best secrecy performance. The value of θ^* for each performance metric is determined using a numerical search method. Moreover, the effects of η on the SOP and ASC are also examined. It can be observed that the secrecy performance is enhanced as η increases.

In Fig. 4, we investigate the effects of ρ_s and ρ_d on the optimal SOP and optimal ASC in different scenarios: S_1, S_2, and S_3. We fix ρ_s and ρ_d in scenarios S_1 and S_2, respectively, while we vary their values in scenario S_3. Comparing the three antenna schemes, it can be observed that the MRT scheme provide the best secrecy performance, whereas the RAS scheme yields the poorest secrecy performance. Moreover, we consider the secrecy performance in two cases, perfect CSI (see Fig. 4a, b) and imperfect CSI with $\zeta = 0.9$ (see Fig. 4c, d).

In the case of perfect CSI, the optimal SOP is an increasing function of ρ, and the optimal ASC is a decreasing function of ρ. Moreover, as ρ increases, the secrecy performance in scenarios S_1 and S_2 converges, whereas it linearly increases in scenario S_3. These results can be explained using the trends of $\mathcal{C}_r$ and $\mathcal{C}_d$ in the three scenarios. In scenario S_1, the fixed ρ_s value leads to a fixed $\mathcal{C}_d$, which limits the secrecy performance. In scenario S_2, the same increasing rates of $\mathcal{C}_r$ and $\mathcal{C}_d$ cause the secrecy performance to converge. In scenario S_3, the increasing trends of ρ_s and ρ_d leads to substantial growth in $\mathcal{C}_d$ and the limit in $\mathcal{C}_r$, respectively, which contribute to the remarkable increase in secrecy performance. Additionally, at low ρ values, the

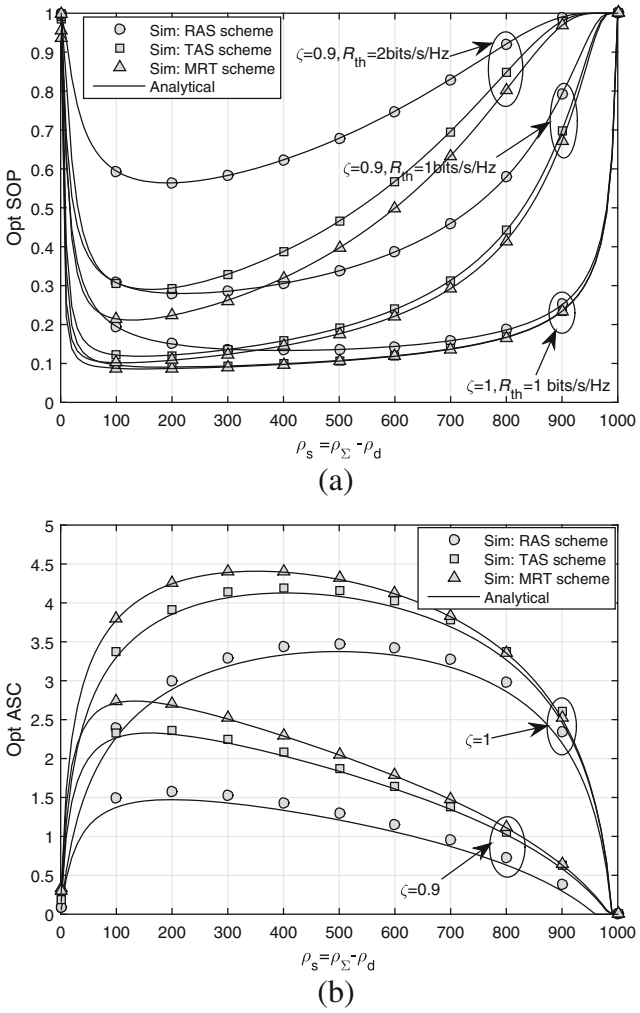

Fig. 5 The optimal SOP and optimal ASC in term of the trade-off between ρ_s and ρ_d ($\rho_s + \rho_d = \rho_\Sigma$). Other parameter: $d = 1$ and $\rho_\Sigma = 30(dB)$

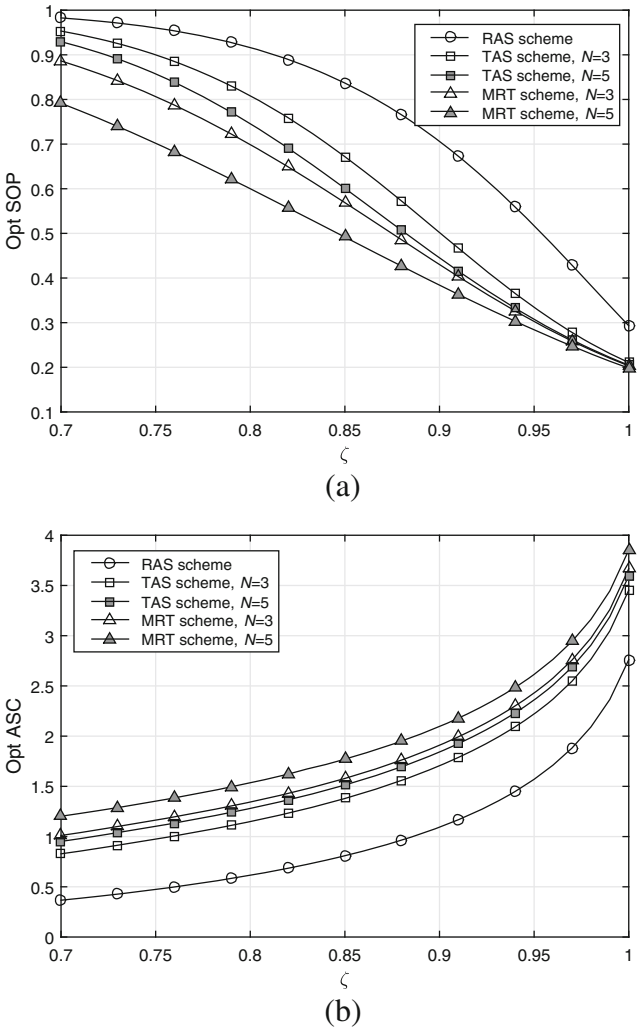

Fig. 6 The effect of ζ on the SOP and ASC. Other parameter: $d = 1$, $\rho_s = \rho_d = 25(dB)$ and $R_s = 2(bits/sec/Hz)$

secrecy performance in scenario S_2 overcomes those in scenarios S_1 and S_3.

In the case of imperfect CSI, the secrecy performance in scenarios S_1 and S_3 decreases and converges, whereas that in scenario S_2 improves at first and then degrades. Comparing these results with that in the perfect CSI case, we have the follows. For scenario S_1, the secrecy performance trends in both perfect CSI and imperfect CSI cases are similar, except for the limit of each case. In contrast, the secrecy performance trends in the perfect CSI and imperfect CSI cases are different for scenarios S_2 and S_3. This is because of the effect of the noise caused by imperfect CSI. Particularly, for scenario S_2, both $\mathcal{C}_r$ and $\mathcal{C}_d$ converge to a value in which the convergence rate of $\mathcal{C}_d$ is higher than that of $\mathcal{C}_r$ due to the effect of the AN; therefore, the optimal SOP and optimal ASC follow a convex function and a concave function of ρ, respectively. In scenario S_3, $\mathcal{C}_d$ converges to a higher value than $\mathcal{C}_r$ due to the effect of the AN, hence, the secrecy performance converges to a non-zero value. On the other hand, at high ρ values, the secrecy performance in scenario S_1 becomes better than that in the other scenarios, whereas at low ρ values, the secrecy performance in scenario S_2 outperforms that in the other scenarios.

In Fig. 5, we present the optimal SOP and optimal ASC results in term of the trade-off between the transmit powers of S and D. The overall transmit power over noise power is $\rho_\Sigma = 10^3$, i.e., $\rho_s + \rho_d = \rho_\Sigma$. As shown in Fig. 5, the highest secrecy performance is obtained as ρ_s is between 0 and ρ_Σ, and the secrecy performance rapidly decreases as ρ_s tends to 0 or ρ_Σ. These results show an important role of the destination-assisted jamming in creating the positive secrecy capacity, such as, with low destination-assisted jamming signal's powers, the secure communication between S and D does not exist. Moreover, it can be seen that the peaks of the optimal SOP and ASC curves move toward to the left

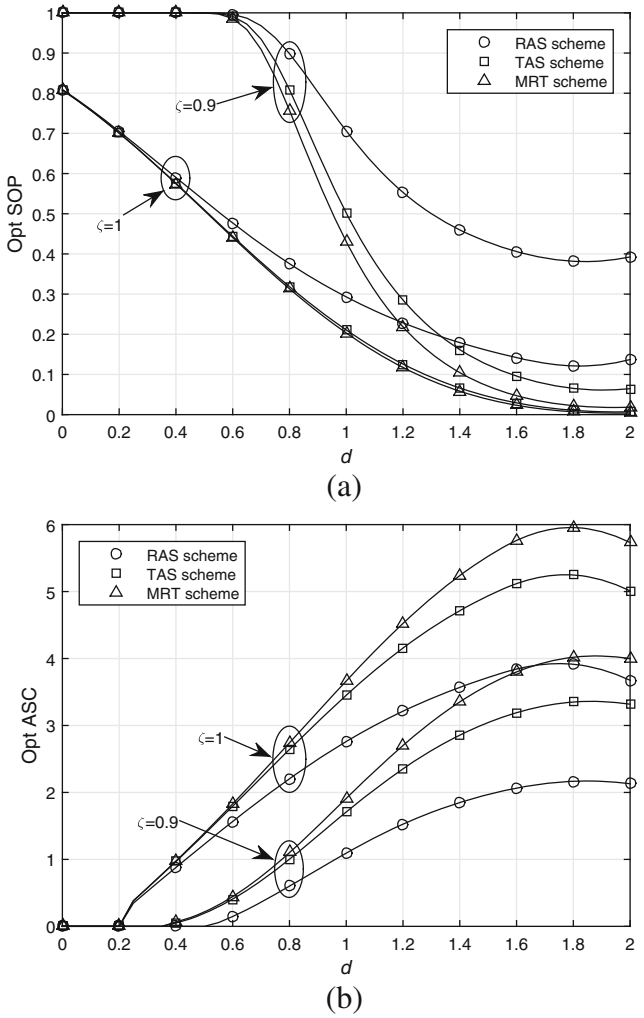

Fig. 7 The effect of the relay's location on the optimal SOP and optimal ASC. Other parameters: $\rho_s = \rho_d = 15(dB)$

(the decreasing trend of ρ_s) when ζ increases. Comparing three considered schemes, the peaks of the optimal SOP and ASC curves for the TAS scheme is located in the left side of that for the RAS scheme and in the right side of that for the MRT scheme. For all values of $\rho_s \in (0, \rho_\Sigma]$, the MRT scheme yields the best secrecy performance while the RAS scheme gives a lowest secrecy performance.

In Fig. 6, we investigate the effects of N and ζ on the optimal SOP and optimal ASC. From Eq. 9, it can be seen that the signal strength that can be decoded at the receiver decreases and the noise power caused by the imperfect CSI increases as ζ decreases; therefore, the secrecy performance degrades as ζ decreases. On the other hand, it can be seen in Eq. 9 that, when S is equipped with a larger antenna, the signal strength used for information decoding at the receiver for the TAS and MRT schemes is enhanced, whereas the noise power caused by the imperfect CSI does not change. Therefore, when N increases, the secrecy performances for both the MRT and TAS schemes improves. Moreover, it can be seen in Fig. 5 that the MRT scheme outperform the TAS scheme for all values of ζ.

In Fig. 7, we investigate the effect of the relay's location on the optimal SOP and optimal ASC. As shown, the secrecy performance improves as d increases from 0 to an optimal distance, and then it slightly degrades with further increase in d. These results can be explained by using the effect of the $R - D$ link on the AN at R and the overall noise at D. When R is near S, the AN's strength becomes weak due to the decreasing trend of the $R - D$ channel gain, hence, the secrecy performance is low. In contrast, when R is near D, the overall noise at D increases because of an increasing trend in the $R - D$ channel gain; therefore, the secrecy performance slightly degrades. Comparing with the conventional cooperative SWIPT system (which uses the trusted relay in which a high performance is achieved when R is located near S), our proposed system achieves high performance when R is located between S and D. Moreover, it can be observed from Fig. 7 that the optimal SOP is approximately zero if R is close to S, such as $d < 0.2$, for the case of $\zeta = 1$, and $d < 0.4$ for the case of $\zeta = 0.9$.

5 Conclusion

In this paper, we studied the secure communication of a cooperative system using an energy-harvesting untrusted relay. The source was equipped with multiple antennas and used TAS and MRT to enhance the harvested energy at the relay. For performance comparison, RAS was examined. Additionally, the destination-assisted jamming was employed to create a positive secrecy capacity. The analytical expression of the SOP and ASC for the two cases, i.e., perfect CSI and imperfect CSI, were derived; moreover, the closed-form expression for the SOP at high-power levels was also presented. We used the Monte Carlo simulations to verify the accuracy of the analytical results. Our results demonstrated that (1) the secrecy performance in both the perfect CSI case and imperfect CSI is improved as the source's antennas increases. (2) MRT performs better than TAS; and both MRT and TAS provide a significant improvement in secrecy performance compared with RAS. Especially in the imperfect CSI's case, these trends has shown clearer. (3) The best location for the untrusted relay is between the source and the destination. Moreover, the effects of various system parameters, such as the channel correlation coefficient, energy-harvesting efficiency, secrecy rate threshold, power-splitting ratio, and transmit powers on secrecy performance were studied, and these findings provide valuable insight into system design.

Appendix A: Proof of Proposition 1

Let $x_1, \ldots, x_N$ be N exponential RVs with a rate parameter λ, and the PDF and CDF of x_n, $1 \leqslant n \leqslant N$, are respectively given by

$$f(\lambda; x) = \lambda e^{-\lambda x}, \tag{33}$$

$$F(\lambda; x) = 1 - e^{-\lambda x}. \tag{34}$$

Let us define $Y = \max\{x_1, \ldots, x_N\}$ and $Z = \sum_{n=1}^{N} x_n$. The CDFs of Y and Z are respectively given by

$$F_Y(\lambda, N; x) = F(\lambda; x)^N = 1 + \sum_{n=1}^{N} \binom{N}{n} (-1)^n e^{-n\lambda x}, \tag{35}$$

$$F_Z(\lambda, N; x) = 1 - e^{-\lambda x} \sum_{n=0}^{N-1} \frac{(\lambda x)^n}{n!}. \tag{36}$$

Next, we rewrite Eq. 12 as

$$\mathrm{SOP} = 1 - \int_{\bar{x}_1}^{+\infty} \left(1 - F_{X_1}\left(\lambda_1, N; \tfrac{\beta - 1}{\zeta(1-\theta)\rho_s \Xi(x;\beta)}\right)\right) f_{X_2}(\lambda_2; x)\, dx. \tag{37}$$

where $F_{X_1}(\lambda_1, N; x)$ and $f_{X_2}(\lambda_2; x)$ are the cumulative distribution function (CDF) of X_1 and the probability density function (PDF) of X_2, respectively.

A.1 Calculation for $\mathrm{SOP}_{\mathrm{RAS}}$

Replacing $F_{X_1}(\lambda_1, N; x)$ and $f_{X_2}(\lambda_2; x)$ in Eq. 37 with $F(\lambda_1; x)$ and $f(\lambda_2; x)$, respectively, we obtain Eq. 13.

A.2 Calculation for $\mathrm{SOP}_{\mathrm{TAS}}$

Replacing $F_{X_1}(\lambda_1, N; x)$ and $f_{X_2}(\lambda_2; x)$ in Eq. 37 with $F_Y(\lambda_1, N; x)$ and $f(\lambda_2; x)$, respectively, we obtain Eq. 14.

A.3 Calculation for $\mathrm{SOP}_{\mathrm{MRT}}$

Replacing $F_{X_1}(\lambda_1, N; x)$ and $f_{X_2}(\lambda_2; x)$ in Eq. 37 with $F_Z(\lambda_1, N; x)$ and $f(\lambda_2; x)$, respectively, we obtain Eq. 15.

Finally, Proposition 1 is proved.

Appendix B: Proof of Proposition 2

B.1 Calculation for case of perfect CSI ($\zeta = 1$)

In this case, we have $\mu = 1$, $\Xi(x; \beta) \approx \frac{x}{x+\kappa}$, and $\bar{x}_1 \approx \sqrt{\frac{\beta}{\eta\theta\rho_d}}$. Therefore, Eq. 12 can be approximated as

$$\mathrm{SOP} = 1 - \Pr(X_1 > \bar{x}_3 | X_2 > \bar{x}_1) \approx F_{X_2}(\lambda_2; \bar{x}_1), \tag{38}$$

where $\bar{x}_3 = \frac{(\beta-1)}{(1-\theta)\rho_s}\left(1 + \frac{\kappa}{X_2}\right)$, and the approximation in Eq. (38) is obtained due to the fact that $\lim_{(\rho_s, \rho_d) \to (\infty, \infty)} \frac{\bar{x}_3}{\bar{x}_1} = 0$.

Using the series representation of the exponential function given in [15, Eq. (1.211.1)], we can prove (16).

B.2 Calculation for case of perfect CSI ($0 < \zeta < 1$)

In this case, we have $\mu \approx \mu_0 := (1-\zeta)(1-\theta)\frac{\rho_s}{\lambda_1}$ and $\Xi(x; \beta) \approx \frac{1}{\mu} - \frac{\beta}{(1-\theta)\rho_d X_2 + \mu}$. Therefore, $\frac{1}{\Xi(x;\beta)}$ can be approximated by

$$\frac{1}{\Xi(x; \beta)} \approx \mu\left(1 + \frac{(1-\zeta)\omega\beta}{\lambda_1(X_2 - \bar{x}_2)}\right). \tag{39}$$

Then, the asymptotic functions for the SOP are calculated by

$$\begin{aligned}\mathrm{SOP}^{\infty} &= 1 - \Pr\left(X_1 > \tfrac{\bar{x}_2}{\omega\zeta}\left(1 + \tfrac{(1-\zeta)\omega\beta}{\lambda_1(X_2 - \bar{x}_2)}\right) | X_2 > \bar{x}_2\right) \\ &= 1 - \int_{\bar{x}_2}^{\infty} \left(1 - F_{X_1}\left(\lambda_1, N; \tfrac{\bar{x}_2}{\omega\zeta}\left(1 + \tfrac{(1-\zeta)\omega\beta}{\lambda_1(x - \bar{x}_2)}\right)\right)\right) f_{X_2}(\lambda_2; x)\, dx.\end{aligned} \tag{40}$$

Let us define $t = x - \bar{x}_2$, Eq. 40 can be rewritten as

$$\mathrm{SOP}^{\infty} = 1 - \int_{0}^{\infty} \left(1 - F_{X_1}\left(\lambda_1, N; \tfrac{\bar{x}_2}{\omega\zeta}\left(1 + \tfrac{(1-\zeta)\omega\beta}{\lambda_1 t}\right)\right)\right) f_{X_2}(\lambda_2; t + \bar{x}_2)\, dt. \tag{41}$$

B.2.1 Calculation for $\mathrm{SOP}^{\infty}_{\mathrm{RAS}}$

Replacing $F_{X_1}(\lambda_1, N; x)$ and $f_{X_2}(\lambda_2; x)$ in Eq. 41 with $F(\lambda_1; x)$ and $f(\lambda_2; x)$, respectively, we have

$$\mathrm{SOP}^{\infty} = 1 - \lambda_2 e^{-\frac{\lambda_1 \bar{x}_2}{\omega\zeta} - \lambda_2 \bar{x}_2} \int_{0}^{\infty} e^{-\frac{\bar{x}_2(1-\zeta)\beta}{\zeta t} - \lambda_2 t} dt. \tag{42}$$

With the help of [15, Eq. (3.471.9)], Eq. 42 can be expressed as Eq. 17.

B.2.2 Calculation for $\mathrm{SOP}^{\infty}_{\mathrm{TAS}}$

Replacing $F_{X_1}(\lambda_1, N; x)$ and $f_{X_2}(\lambda_2; x)$ in Eq. 41 with $F_Y(\lambda_1, N; x)$ and $f(\lambda_2; x)$, respectively, and using the same step in the calculation for $\mathrm{SOP}^{\infty}_{\mathrm{RAS}}$, we obtain Eq. 18.

B.2.3 Calculation for $\mathrm{SOP}^{\infty}_{\mathrm{MRT}}$

Replacing $F_{X_1}(\lambda_1, N; x)$ and $f_{X_2}(\lambda_2; x)$ in Eq. 41 with $F_Z(\lambda_1, N; x)$ and $f(\lambda_2; x)$, respectively, and using the same step in the calculation for $\mathrm{SOP}^{\infty}_{\mathrm{RAS}}$, we obtain Eq. 19.

Finally, Proposition 2 is proved.

Appendix C: Proof of Proposition 3

C.1 Calculation for the RAS scheme

Using the PDFs of X_1 and X_2 for the RAS scheme given by $f(\lambda_1; x)$ and $f(\lambda_2; x)$, respectively, and [15, Eq.(4.352.1)], $\mathcal{J}_1$ and $\mathcal{J}_2$ for the RAS scheme are calculated as

$$\mathcal{J}_1^{\text{RAS}} = \Psi(1) - \ln(\lambda_1), \tag{43}$$

$$\mathcal{J}_2^{\text{RAS}} = \Psi(1) - \ln(\lambda_2) \tag{44}$$

Moreover, using the PDFs of X2 and [15, Eq.(4.337.1)], $\mathcal{J}_3$ for the RAS scheme is calculated as

$$\mathcal{J}_3^{\text{RAS}} = \ln(\kappa) - e^{\frac{\lambda_2\kappa}{\mu}} Ei\left(-\frac{\lambda_2\kappa}{\mu}\right). \tag{45}$$

Substituting Eqs. 43, 44, and 45 into Eq. 22 yields (23).

C.2 Calculation for the TAS scheme

According to [18], the PDF of Y defined in Appendix A is given by

$$f_Y(\lambda, N; x) = N f(\lambda; x) F(\lambda; x)^{N-1}. \tag{46}$$

Using the PDF of X_1 for the TAS scheme given by $f_Y(\lambda_1, N; x)$ and [15, Eq.(4.352.1)], $\mathcal{J}_1$ for the TAS scheme is calculated as

$$\mathcal{J}_1^{\text{TAS}} = N \sum_{n=0}^{N-1} \binom{N-1}{n} \frac{(-1)^n}{n+1} \left(\Psi(1) - \ln((n+1)\lambda_1)\right). \tag{47}$$

Using the fact that $N \sum_{n=0}^{N-1} \binom{N-1}{n} \frac{(-1)^n}{(n+1)} = 1$, we can rewrite Eq. 47 as

$$\mathcal{J}_1^{\text{TAS}} = \Psi(1) - N \sum_{n=0}^{N-1} \binom{N-1}{n} \frac{(-1)^n}{n+1} \ln((n+1)\lambda_1). \tag{48}$$

Because $\mathcal{J}_2$ and $\mathcal{J}_3$ for the TAS scheme are the same as for the RAS scheme, Eq. 24 is obtained by substituting Eqs. 44, 45 and 48 into Eq. 22.

C.3 Calculation for the MRT scheme

According to [8], the PDF of Z defined in Appendix A is given by

$$f_Z(\lambda, N; x) = \frac{\lambda^N x^{N-1}}{\Gamma(N)} e^{-\lambda x}. \tag{49}$$

Using the PDF of X_1 for the MRT scheme given by $f_Z(\lambda_1, N; x)$ and [15, Eq.(4.352.1)], $\mathcal{J}_1$ for the MRT scheme is calculated as

$$\mathcal{J}_1^{\text{MRT}} = \psi(N) - \ln(\lambda_1). \tag{50}$$

Because $\mathcal{J}_2$ and $\mathcal{J}_3$ for the MRT scheme are the same as for the RAS scheme, Eq. 25 is obtained by substituting Eqs. 44, 45, and 50 into Eq. 22.

Appendix D: Proof of Proposition 4

From Eq. 7, the PDF of γ_r is calculated as

$$F_{\gamma_r}(\gamma) = \Pr(\gamma_r < \gamma) = \int_0^\infty F_{X_1}\left(\lambda_1, N; \tfrac{\gamma((1-\theta)\rho_d x+\mu)}{\zeta(1-\theta)\rho_s}\right) f_{X_2}(\lambda_2; x)\, dx. \tag{51}$$

D.1 Calculation for the RAS scheme

Replacing $F_{X_1}(\lambda_1, N; x)$ and $f_{X_2}(\lambda_2; x)$ in Eq. 50 with $F(\lambda_1; x)$ and $f(\lambda_2; x)$, respectively, Eq. 50 can be expressed as

$$F_{\gamma_r}(\gamma) = 1 - \left(\frac{\lambda_1\gamma}{\lambda_2\zeta\omega} + 1\right)^{-1} e^{-\frac{\lambda_1\gamma\mu}{\zeta(1-\theta)\rho_s}}. \tag{52}$$

Substituting Eqs. 50 into Eq. 26, we have the following:

$$\bar{C}_r = \frac{1}{\ln(2)} \int_0^\infty \left(\tfrac{\lambda_1\gamma}{\lambda_2\zeta\omega} + 1\right)^{-1} (1+\gamma)^{-1} e^{-\frac{\lambda_1\gamma\mu}{\zeta(1-\theta)\rho_s}} d\gamma. \tag{53}$$

In the case of $\lambda_1 \neq \lambda_2\zeta\omega$, $\left(\frac{\lambda_1\gamma}{\lambda_2\zeta\omega}+1\right)^{-1}(1+\gamma)^{-1}$ can be expressed as $\left(1-\frac{\lambda_1}{\lambda_2\zeta\omega}\right)^{-1}\left((\gamma+1)^{-1} - \left(\gamma+\frac{\lambda_2\zeta\omega}{\lambda_1}\right)^{-1}\right)$. Then, using [15, Eq.(3.383.10)], we obtain Eq. 27. In the case of $\lambda_1 = \lambda_2\zeta\omega$, we obtain Eq. 28 with the help of [15, Eq. (3.353.2)].

D.2 Calculation for the TAS scheme

The result for the TAS scheme can be obtained by replacing $F_{X_1}(\lambda_1, N; x)$ and $f_{X_2}(\lambda_2; x)$ in Eq. 50 with $F_Y(\lambda_1, N; x)$ and $f(\lambda_2; x)$, respectively, and using the same step as in Appendix D.1.

D.3 Calculation for the MRT scheme

Replacing $F_{X_1}(\lambda_1, N; x)$ and $f_{X_2}(\lambda_2; x)$ in Eq. 50 with $F_Z(\lambda_1, N; x)$ and $f(\lambda_2; x)$, respectively, and using [15, Eq.(8.350.2)], Eq. 50 can be expressed as

$$F_{\gamma_r}(\gamma) = 1 - \lambda_2 e^{-\frac{\lambda_1\mu\gamma}{\zeta(1-\theta)\rho_s}} \sum_{n=0}^{N-1} \frac{1}{n!}\left(\frac{\lambda_1\gamma}{\zeta\omega}\right)^n \times \sum_{k=0}^{n} \binom{n}{k} \left(\frac{\mu}{(1-\theta)\rho_d}\right)^{n-k} \frac{\Gamma(k+1)}{\left(\frac{\lambda_1\gamma}{\zeta\omega}+\lambda_2\right)^{k+1}}. \tag{54}$$

Substituting Eq. 53 into Eq. 26, we have the following:

$$\bar{C}_r = \frac{\lambda_2}{\ln(2)} \sum_{n=0}^{N-1} \frac{1}{n!} \left(\frac{\lambda_1}{\zeta\omega}\right)^n \sum_{k=0}^{n} \binom{n}{k} \left(\frac{\mu}{(1-\theta)\rho_d}\right)^{n-k} \times \Gamma(k+1) \int_0^{\infty} \gamma^n \mathcal{I}(\gamma) e^{-\frac{\lambda_1 \mu \gamma}{\zeta(1-\theta)\rho_s}} d\gamma, \quad (55)$$

where $\mathcal{I}(\gamma) = (1+\gamma)^{-1} \left(\frac{\lambda_1}{\zeta\omega}\gamma + \lambda_2\right)^{-k-1}$.

In the case of $\lambda_1 \neq \lambda_2\zeta\omega$, $\mathcal{I}(\gamma)$ can be decomposed using partial fraction decomposition as follows.

$$\mathcal{I}(\gamma) = \frac{A_0}{(1+\gamma)} + \sum_{i=1}^{k+1} \frac{A_i}{\left(\frac{\lambda_1}{\zeta\omega}\gamma + \lambda_2\right)^i}. \quad (56)$$

Substituting Eq. 55 into Eq. 54 and using [15, Eq.(3.383.10) and Eq.(9.211.4)], we obtain Eq. 31.

In the case of $\lambda_1 = \lambda_2\zeta\omega, \mathcal{I}(\gamma) = \left(\frac{\zeta\omega}{\lambda_1}\right)^{k+1} (\gamma+1)^{-k-2}$. Then, with the help of [15, Eq. (9.211.4)], we obtain Eq. 32.

References

1. Valenta CR, Durgin GD (2014) Harvesting wireless power: survey of energy-harvester conversion efficiency in far-field, wireless power transfer systems. IEEE Microw Mag 15(4):108–120
2. Ding Z, Perlaza SM, Esnaola I, Poor HV (2014) Power allocation strategies in energy harvesting wireless cooperative networks. IEEE Trans Wireless Commun 13(2):846–860
3. Zhou X, Zhang R, Ho CK (2013) Wireless information and power transfer: architecture design and rate-energy tradeoff. IEEE Trans Commun 61:4754–4767
4. Nasir A, Zhou X, Durrani S, Kennedy R (2013) Relaying protocols for wireless energy harvesting and information processing. IEEE Trans Wireless Commun 12:3622–3636
5. Son PN, Kong HY (2015) Cooperative communication with energy-harvesting relays under physical layer security. IET Commun 9(17):2131–2139
6. Zhong C, Suraweera H, Zheng G, Krikidis I, Zhang Z (2014) Wireless information and power transfer with full duplex relaying. IEEE Trans Commun 62:3447–3461
7. Gu Y, Aïssa S (2015) RF-based energy harvesting in decode-and-forward relaying systems: ergodic and outage capacities. IEEE Trans Commun 14(11):6425–6434
8. Zhu G, Zhong C, Suraweera H, Karagiannidis G, Zhang Z, Tsiftsis T (2015) Wireless information and power transfer in relay systems with multiple antennas and interference. IEEE Trans Commun 63:1400–1418
9. Liu L, Zhang R, Chua KC (2014) Secrecy wireless information and power transfer with MISO beamforming. IEEE Trans Signal Process 62(7):1850–1863
10. Zhang H, Li C, Huang Y, Yang L (2016) Secure beamforming for SWIPT in multiuser MISO broadcast channel with confidential messages. IEEE Commun Lett 19(8):1347–1350
11. Kalamkar SS, Banerjee A (2016) Secure communication via a wireless energy harvesting untrusted relay. IEEE Trans. Veh. Technol. (Accepted)
12. Gucluoglu T, Panayirci E (2008) Performance of transmit and receive antenna selection in the presence of channel estimation errors. IEEE Commun Lett 12(5):371–373
13. Chalise BK, Zhang YD, Amin MG (2013) Local CSI based full diversity achieving relay selection for amplify-and-forward cooperative systems. IEEE Trans Signal Process 61(21):5165–5180
14. Pan G, Lei H, Deng Y, Fan L, Yang J, Chen Y, Ding Z (2016) On secrecy performance of MISO SWIPT systems with TAS and imperfect CSI. IEEE Trans Commun 64(9):3831–3843
15. Gradshteyn IS, Ryzhik IM, Jeffrey A, Zwillinger D (2007) Table of integral, series and products, 7th edn. Elsevier, Amsterdam
16. Lv L, Chen J, Yang L, Kuo Y (2017) Improving physical layer security in untrusted relay networks: cooperative jamming and power allocation. IET Commun 11(3):393–399
17. Zhu G, Zhong C, Suraweera HA, Zhang Z, Yuen C, Yin R (2014) Ergodic capacity comparison of different relay precoding schemes in dual-hop AF systems with co-Channel interferer. IEEE Trans Commun 62(7):2314–2328
18. David HA, Nagaraja HN (2003) Order Statistics, 3rd edn. Wiley, Hoboken