IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 19, 2019, accepted January 31, 2019, date of publication February 4, 2019, date of current version March 7, 2019.

*Digital Object Identifier 10.1109/ACCESS.2019.2897357*

# Physical Layer Security in an Untrusted Energy Harvesting Relay Network

**HUI SHI[1], YUEMING CAI[1], (Senior Member, IEEE), DECHUAN CHEN[2], JIANWEI HU[1], (Student Member, IEEE), WEIWEI YANG[1], (Member, IEEE), AND WENDONG YANG[1]**

[1]College of Communication Engineering, Army Engineering University of PLA, Nanjing 210007, China
[2]Wuhan Zhongyuan Electronics Group Company, Ltd., Wuhan 430205, China

Corresponding author: Yueming Cai (caiym@vip.sina.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61771487, Grant 61471393, Grant 61371122, and Grant 61501512, and in part by the Jiangsu Provincial Natural Science Foundation under Grant BK20150718.

**ABSTRACT** The security performance in an amplify-and-forward dual-hop untrusted relay network is considered. It is assumed that the source and multiple destinations are equipped with multiple antennas, and the information transmission is aided by a single-antenna but energy-constrained relay. On the one hand, the relay can harvest the energy from its received signals by applying power splitting relaying and time switching relaying protocols and then forward the information to the destinations. To enhance the reliability performance, multiple destinations are exploited to receive the information simultaneously. On the other hand, the relay may be a potential passive attacker and eavesdrop the received information, but this kind of illegal activity may not be discovered by the sources. To investigate the security and the reliability performance, the secrecy outage probability (SOP) and the connection outage probability (COP) of the considered system are especially examined. In particular, the exact closed-form expressions of SOP and COP are derived. Since the SOP and COP are contradictory metrics, the effective secrecy throughput (EST) performance is further characterized to comprehensively examine the security and the reliability performance. Moreover, the asymptotic analysis of EST in high signal-to-noise ratio (SNR) regime is provided. The theoretical analysis and simulations reveal the impact of different parameters on the system performance, such as the transmit SNR, the power allocation coefficient, the antenna numbers, and other parameters. The Monte Carlo simulations are in excellent agreement with the theoretical expressions.

**INDEX TERMS** Untrusted relay, energy harvesting, multiple antennas, performance analysis, power splitting relaying, time switching relaying.

## I. INTRODUCTION

As an effective solution to extend the coverage area and improve communication quality in wireless communications, the relaying technique has received widespread concerns [1]–[4]. In [2], the performance and comparison between the one-way and two-way full-duplex relaying were detailed researched. Whereas, a half-duplex two way relay networks was presented in [3]. To prolong the lifetime of energy-constrained relay communication systems and to avoid replacing batteries frequently, energy harvesting (EH) from the surrounding environment or the received signals has attracted considerable attention [5]–[8]. The two energy harvesting methods are power splitting and time switching, respectively [9]–[11]. The combination of EH approaches and the relay networks, has led to two major protocols, i.e., power splitting relaying (PSR) and time switching relaying (TSR). In [12], all relays harvested energy from the renewable energy and RF sources, and RF signal was split for EH and information transmission with the power splitting protocol. In [13], the relays harvested energy from multiple power transfer stations with the time switching receiver protocol. Ju *et al.* [14] considered the PSR and TSR protocols for decode-and-forward (DF) relay networks, where the optimal power splitting coefficient and time switching coefficient were examined to maximize the transmission rate.

While the relay can assist the confidential information transmission between the source and the destination, it may

The associate editor coordinating the review of this manuscript and approving it for publication was Yu-Chi Chen.

carry out the attacks such as eavesdropping or decoding the information. The traditional security mechanisms applied to protect the confidential information are cryptographic techniques, which rely mainly on the strong encryption algorithm, the secret key and computational infeasibility. The gradual improvement of computing abilities makes the information security more critical. However, the physical-layer security(PLS), which exploits the inherent nature of wireless channels, provides a new solution to realize secure communications.

The works in [15]–[19] researched a two-hop untrusted relay transmission, where the network was comprised of a source, an untrusted relay and a destination and each node operated in a half-duplex mode. In [15]–[18], each node was equipped with a single antenna. He and Yener [15] investigated an upper bound for the secrecy rate in the presence of cooperative jammer based on compress-and-forward at the relay. Mekkawy *et al.* [16] considered a cooperative jamming amplify-and-forward (AF) relay network. The instantaneous secrecy rate was maximized by optimizing the power allocation for confidential and jamming signals. The ergodic secrecy rate (ESR) was further derived to evaluate the maximum average secrecy rate. The works in [17] considered a EH and untrusted AF relay transmission. By jointly optimizing the energy splitting for the source and destination, the maximal achievable secrecy rate was analyzed. Su *et al.* [18] investigated the secrecy capacity (SC) in an AF energy-constrained untrusted cooperative relay network. The SC was maximized by investigating the optimal power split ratio. The works in [19] considered the secure transmission in the two-hop AF untrusted relay networks. The ergodic secrecy capacity (ESC) with optimal power allocation (OPA) was analyzed based on the two networks, i.e., the source or the destination was equipped with multi-antenna, whereas the other two nodes had a single antenna.

In [20], both the source and the destination were multiple antennas, whereas the untrusted relay was a single antenna. The maximal ratio transmission (MRT) beamforming was applied at the source and destination-based cooperative signaling (DBCS) was utilized to prevent the relay from decoding the source message. The optimal power allocation was introduced to maximize the secrecy rate of the system under a sum-power constraint at the network nodes. The closed-form expressions of the secrecy outage probability (SOP) and the ESR of the optimized system both for uplink and downlink were examined. Chen *et al.* [21] studied the secure performance in a cognitive network in the presence of a primary destination, where the secondary source communicated with the secondary destination both aided by the direct link and the untrusted relay link. Each node was equipped with a single antenna. The performance of the SOP, the connection outage probability (COP) and the effective secrecy throughput (EST) were examined.

The works in [22]–[26] investigated the performance of a two-way relay network. Gupta *et al.* [22] and Mamaghani *et al.* [23] considered the secure communication via an untrusted relay, in the presence of the friendly jammer. The works in [22] examined the optimal power splitting ratio and power allocation which could maximize the sum-secrecy rate. The effect of imperfect channel state information at both sources on the sum-secrecy rate was further examined. In [23], the time switching (TS) protocol at the relay was utilized. The lower bound expression for the ergodic secrecy sum rate (ESSR) was derived, besides the impact of different parameters on the security performance was researched. The works in [24] investigated the performance of an AF relay network, where both two sources were equipped with multiple antennas, whereas the untrusted relay was equipped with a single antenna, and all channels were subject to Nakagami-$m$ fading. For the two sources, MRT and the maximal ratio combining (MRC) were utilized to transmit or receive the information. Because the relay was assumed to be trusted, thus only the connection outage probability was derived. And the throughput was examined both in the delay-limited and the delay-tolerant transmissions working modes. Sharma *et al.* [25], [26] investigated the SOP performance of a two-way communication via two half duplex DF relays.

In light of the aforementioned literatures, it makes sense to examine the SOP and the COP performance in the untrusted relay and energy harvesting system, besides the trade-off between SOP and COP in multi-antenna multi-destination networks. Motivated by this, in this paper we focus on characterizing the security performance in an untrusted EH relay network, which consists of a source, multiple destinations, and one untrusted relay. To enhance the information transmission performance, the source and the destinations are equipped with multiple antennas [27]. To reduce computational complexity, the untrusted relay is equipped with a single antenna. Each destination receives the information from the relay with MRC technique. Once one of the destinations reliably receives the information, then the others destinations can exchange the information and work cooperatively. Multiple destinations are ensured the destinations can reliably receive the information. Both PSR and TSR protocols are exploited to obtain the optimal performance of the system. Our contributions can be summarized as follows.

- The closed-form expressions of SOP, COP, and EST under both PSR and TSR protocols in an untrusted relay network are derived. The EST is utilized to comprehensively measure the security and the reliability performance. The theoretical analysis and simulations reveal the impact of the transmit signal-to-noise ratio (SNR), the power allocation coefficient, the number of the destinations and other parameters on the EST performance.
- In the high transmit SNR regime, the exact asymptotic expressions of EST are derived under both PSR and TSR protocols. The asymptotic results show that the EST approaches a constant. Besides the EST of PSR is superior to the EST of TSR. Finally, the analysis is verified by the Monte-Carlo simulation, and the simulations are in excellent agreement with the theoretical expressions.

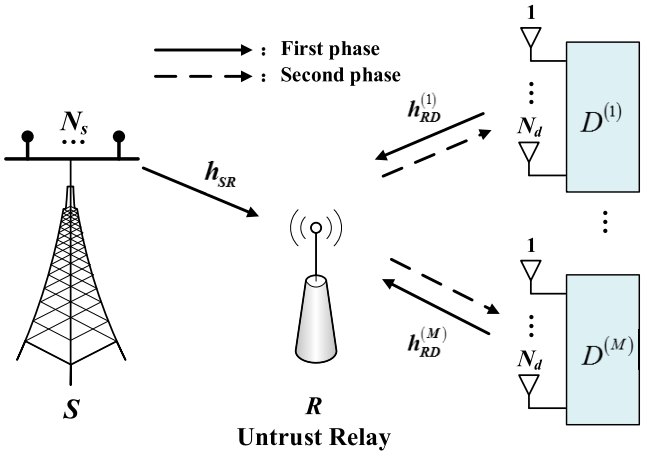



**FIGURE 1.** System model.

The remainder of this paper is organized as follows. The system model is described in Section II, where the network descriptions and the information transmission under both PSR and TSR are presented. A set of analytical expressions for the SOP, COP, and EST performance, as well as the asymptotic analysis of the EST in the high transmit SNR regime are formulated in Section III. Then the simulation analysis and the effect of system parameters on the reliability and security performance are discussed in Section IV. Finally, Section V summarizes the conclusions.

## II. SYSTEM MODEL

### A. NETWORK DESCRIPTIONS

An untrusted and energy harvesting relay network is considered as shown in Fig. 1. The source $S$ communicates with destinations $D^{(m)}$ ($m \in \{1, ..., M\}$) with assistance of an untrusted relay $R$. The untrusted relay is an energy-constraint node equipped with a single antenna, while $S$ and $D^{(m)}$ are equipped with $N_s$ and $N_d$ antennas, respectively. It is assumed that each node operates in half-duplex mode and there are no direct links between the source and the destinations [7]. The channels of the $S-R$ link, the $R-D^{(m)}$ link, are subject to frequently flat Rayleigh fading, distributed independently and identically, and denoted by $\mathbf{h_{SR}} \in \mathbb{C}^{N_s \times 1}$ and $\mathbf{h_{RD}}^{(m)} \in \mathbb{C}^{1 \times N_d}$, respectively. The channels of the $R-D^{(m)}$ link are reciprocity, i.e., $\mathbf{h_{RD}}^{(m)} = \mathbf{h_{DR}}^{(m)}$ [28], [29]. It is further assumed that the channel gains are random variables, which are exponentially distributed with means $\bar{\gamma}_{SR}$ and $\bar{\gamma}_{RD}$, respectively.

The overall information transmission is divided into two phases, as shown in Fig. 1. In the first phase, MRT technique is applied at the source $S$ and the destination $D^{(m*)}$ to maximize the received SNR of the signal at the relay $R$ [20], [30], [31]. $S$ and $D^{(m*)}$ transmit the confidential information and the jamming signal to $R$, respectively. Here $D^{(m*)}$ is the selected destination from the $M$ destinations to achieve the largest channel vector. During the second phase, $R$ amplifies and forwards the information to $D^{(m*)}$, and $D^{(m*)}$ utilizes MRC to receive the information in the $R \to D^{(m*)}$ links.

It is assumed that the wiretap codes for the confidential information employ the fixed-rate Wyner code mechanism. The codeword transmission rate and the confidential information rate are denoted by $R_0$ and $R_s$, respectively. The positive difference rate between $R_0$ and $R_s$ is used for providing protection against the eavesdropper [32].

### B. POWER SPLITTING RELAYING

Considering PSR, the overall communication time $T$, is divided into two phases equally. During the first $T/2$ phase, $S$ and $D^{(m*)}$ transmit signals to $R$ with power $\beta P$ and $(1-\beta)P$, respectively, where $P$ is the total transmitted power of the system, and $\beta$ is defined as the power allocation coefficient between $S$ and $D^{(m*)}$, $\beta \in (0, 1)$. The received signal power at $R$ is split into $\rho$ and $(1-\rho)$ two parts for harvesting energy and transmitting the information, respectively, where $\rho$ is the power splitting coefficient and $\rho \in (0, 1)$.

Hence, the received signal at $R$ is given by

$$y_R^{PSR} = \sqrt{\beta(1-\rho)P}\,\mathbf{h_{SR}}x_S + \sqrt{(1-\beta)(1-\rho)P}\,\mathbf{h_{DR}}x_D + n_R. \quad (1)$$

where $x_S$ and $x_D$ denote the confidential information and jamming signal. $n_R$ is the additive white Gaussian noise (AWGN) at $R$, and $n_R \sim CN(0, N_0)$, where $N_0$ denotes the noise power.

MRT is applied at $S$ and $D^{(m*)}$, then the received instantaneous signal-to-interference-plus-noise ratio (SINR) at $R$ can be expressed as

$$\gamma_R^{PSR} = \frac{(1-\rho)\beta\lambda\|\mathbf{h_{SR}}\|^2}{(1-\rho)(1-\beta)\lambda\|\mathbf{h_{DR}}\|^2 + 1}, \quad (2)$$

where $\|\mathbf{h_{SR}}\|^2$, $\|\mathbf{h_{DR}}\|^2$ denote the channel gain and $\|\bullet\|$stands for the Frobenius Norm, besides $\lambda = P/N_0$ denotes the transmit SNR.

The harvested energy at $R$ can be expressed as

$$E_H^{PSR} = \frac{\eta\rho T\left(\beta P\|\mathbf{h_{SR}}\|^2 + (1-\beta)P\|\mathbf{h_{DR}}\|^2\right)}{2}, \quad (3)$$

where $\eta$ is the energy conversion efficiency coefficient, $\eta \in (0, 1)$.

It is assumed that $E_H^{PSR}$ is divided into two parts, $\omega E_H^{PSR}$ and $(1-\omega)E_H^{PSR}$, used for transmitting information and decoding consumption, respectively, where $\omega$ is defined as the harvested energy allocation coefficient. In the second $T/2$ phase, $R$ amplifies and forwards the confidential information to $D^{(m*)}$ with the transmit power $P_R^{PSR} = 2\omega E_H^{PSR}/T$. $D^{(m*)}$ adopts the MRC to receive the confidential information with $N_d$ antennas. Therefore, the received signal at $D^{(m*)}$ can be written as

$$y_D^{PSR} = G_R^{PSR}\sqrt{(1-\rho)\beta P P_R^{PSR}}\,\|\mathbf{h_{SR}}\|\,\|\mathbf{h_{RD}}\|\,x_S + G_R^{PSR}\sqrt{P_R^{PSR}}\,\|\mathbf{h_{RD}}\|\,n_R + n_D, \quad (4)$$

where $n_D \sim CN(0, N_0)$, $G_R^{PSR} = 1/\sqrt{(1-\rho)P\Delta + N_0}$, and $\Delta = \left(\beta\|\mathbf{h_{SR}}\|^2 + (1-\beta)\|\mathbf{h_{RD}}\|^2\right)$.

The received SINR at $D^{(m*)}$ can be calculated as

$$\gamma_D^{PSR} = \frac{\omega\eta\rho\,(1-\rho)\,\beta\lambda^2\|\mathbf{h_{SR}}\|^2\|\mathbf{h_{RD}}\|^2\Delta}{\lambda\left(\omega\eta\rho\|\mathbf{h_{RD}}\|^2+1-\rho\right)\,\Delta\,+1}. \tag{5}$$

### C. TIME SWITCHING RELAYING

For TSR, during the $\alpha T/2$ period, $R$ harvests energy from its received signals sent from $S$ and $D^{(m*)}$, where $\alpha$ is the time switching factor and $\alpha \in (0, 1)$. Afterwards, during the $(1-\alpha)\,T/2$ period, $S$ transmits the confidential information to $R$. Thus, the received instantaneous SINR at $R$ can be written as

$$\gamma_R^{TSR} = \frac{\beta\lambda\|\mathbf{h_{SR}}\|^2}{(1-\beta)\,\lambda\|\mathbf{h_{RD}}\|^2+1}. \tag{6}$$

Accordingly, the harvested energy at $R$ can be given by

$$E_H^{TSR} = \eta\alpha T\left(\beta P\|\mathbf{h_{SR}}\|^2+(1-\beta)\,P\|\mathbf{h_{DR}}\|^2\right). \tag{7}$$

In the remaining $(1-\alpha)\,T/2$ period, $R$ forwards the confidential information to $D^{(m*)}$ with the transmit power $P_R^{TSR} = 2\omega E_H^{TSR}/\left((1-\alpha)\,T\right)$, where $\omega$ is defined as the harvested energy allocation coefficient. Hence, the received signal at $D^{(m*)}$ can be written as

$$y_D^{TSR} = \sqrt{\beta P P_R^{TSR}}\;\|\mathbf{h_{SR}}\|\,\|\mathbf{h_{RD}}\|\,G_R^{TSR}x_S + \sqrt{P_R^{TSR}}\,\|\mathbf{h_{RD}}\|\,G_R^{TSR}n_R + n_D, \tag{8}$$

where $G_R^{TSR} = 1/\sqrt{P\Delta+N_0}$.

The received SINR at $D^{(m*)}$ can be calculated as

$$\gamma_D^{TSR} = \frac{2\omega\eta\alpha\beta\lambda^2\|\mathbf{h_{SR}}\|^2\|\mathbf{h_{RD}}\|^2\Delta}{\lambda\left(2\omega\eta\alpha\|\mathbf{h_{RD}}\|^2+1-\alpha\right)\Delta+1-\alpha}. \tag{9}$$

## III. PERFORMANCE ANALYSIS

To analyze the security and the reliability performance of the considered system, we first derive the closed-form expressions for SOP, COP, and EST under both PSR and TSP protocols. To obtain further insights, we also provide the asymptotic analysis of the EST in high transmit SNR regime.

### A. PRELIMINARIES

Before analyzing the performance of PSR and TSR, we first define random variables $X = \|\mathbf{h_{SR}}\|^2$, and $Y = \|\mathbf{h_{DR}}\|^2$. Then, the probability density function (PDF) and the cumulative distributed function (CDF) of $X$ and $Y$, frequently invoked in the following analysis, are presented.

*Lemma 1:* The PDF and CDF of $X$ can be expressed as

$$f_X(x) = \frac{x^{N_s-1}e^{-\frac{x}{\bar{\gamma}_{SR}}}}{(\bar{\gamma}_{SR})^{N_s}\,(N_s-1)!} \tag{10}$$

and

$$F_X(x) = 1-e^{-\frac{x}{\bar{\gamma}_{SR}}}\sum_{n_s=0}^{N_s-1}\frac{1}{n_s!}\left(\frac{x}{\bar{\gamma}_{SR}}\right)^{n_s}. \tag{11}$$

*Proof:* The proof can be found in [35, eqs. (2.3-21) and (2.3-24)], respectively. Note that X is a central chi-square distribution random variable with $2N_s$ degrees of freedom.

*Lemma 2:* The PDF and CDF of $Y$ can be expressed as

$$f_Y(y) = \sum_{m=0}^{M-1}\sum_{p=0}^{m(N_d-1)}\binom{M-1}{m} \times\frac{(-1)^m v_p^m M y^{N_d+p-1}e^{-\frac{(m+1)y}{\bar{\gamma}_{RD}}}}{\Gamma(N_d)\,(\bar{\gamma}_{RD})^{N_d+p}} \tag{12}$$

and

$$F_Y(y) = 1-\sum_{m=1}^{M}\sum_{p=0}^{m(N_d-1)}\binom{M}{m}\times\frac{(-1)^{m-1}\,v_p^m\,y^p\,e^{-\frac{my}{\bar{\gamma}_{RD}}}}{(\bar{\gamma}_{RD})^p}, \tag{13}$$

where $\Gamma(\bullet)$ is the Gamma function. The coefficients $v_p^m$, for $0 \le p \le m(N_d-1)$, can be derived as $v_0^m = (\varepsilon_0)^m$, $v_1^m = m\varepsilon_1$, $v_{m(N_d-1)}^m = \left(\varepsilon_{N_d-1}\right)^m$, $v_p^m = \frac{1}{p}\sum_{w=1}^{p}(mw-p+w)\,\varepsilon_w v_{p-w}^m$. For $2 \le p \le N_d-1$, and $v_p^m = \frac{1}{p}\sum_{w=1}^{N_d-1}(mw-p+w)\,\varepsilon_w v_{p-w}^m$ for $N_d \le p \le m(N_d-1)$ with $\varepsilon_w = \frac{1}{w!}$.

*Proof:* Based on the equation (11) and applying [33, eq. (0.314)], the CDF of $Y$ can be derived as the equation (13). And then being taken derivation of $Y$, the PDF of $Y$ can be derived as the equation (12).

### B. SECRECY OUTAGE PROBABILITY

When the channel capacity of the eavesdropper is higher than the positive difference between $R_0$ and $R_s$, the perfect secrecy cannot be guaranteed, which is denoted by secrecy outage event. SOP is utilized to measure the secrecy performance. According to [21], SOP is defined as follows.

$$P_{SOP} = \mathbf{Pr}\left\{\frac{1}{2}\log_2(1+\gamma_R) > R_0-R_s\right\}, \tag{14}$$

where $\gamma_R \in \left\{\gamma_R^{PSR}, \gamma_R^{TSR}\right\}$, and the coefficient 1/2 is due to two phases.

#### 1) THE SOP OF PSR

Substituting (2) into (14), we can rewrite (14) as

$$P_{SOP}^{PSR} = \mathbf{Pr}\left\{\gamma_R^{PSR} > 2^{2(R_0-R_s)}-1\right\} = \mathbf{Pr}\left\{Y < \frac{\beta X}{(1-\beta)\,\theta_1}-\frac{1}{(1-\rho)\,(1-\beta)\lambda}\right\}, \tag{15}$$

where $\theta_1 = 2^{2(R_0-R_s)}-1$.

Substituting (10) and (13) into (15), the SOP of PSR can be calculated as

$$P_{SOP}^{PSR} = 1 - \sum_{m=1}^{M} \sum_{p=0}^{m(N_d-1)} \sum_{k=0}^{p} \binom{M}{m} \binom{p}{k} \times \frac{(-1)^{m+p-k-1} e^{\frac{m}{(1-\rho)(1-\beta)\lambda\bar{\gamma}_{RD}}} v_p^m {\theta_1}^{N_s}}{\Gamma(N_s)((1-\rho)\lambda)^{p-k}} \times \frac{(\beta\bar{\gamma}_{SR})^k \Gamma(N_s+k)((1-\beta)\bar{\gamma}_{RD})^{N_s+k-p}}{u^{N_s+k}}, \quad (16)$$

where $u = (1-\beta)\theta_1\bar{\gamma}_{RD} + (m+1)\beta\bar{\gamma}_{SR}$.

From the equation (16), the SOP of PSR is related to the parameters $\beta$, $\rho$, $N_s$, $N_d$ and $M$. Besides, the SOP increases as $\beta$ increases, while the SOP decreases by increasing $\rho$.

#### 2) THE SOP OF TSR

Substituting (6) into (14), the SOP of TSR can be written as

$$P_{SOP}^{TSR} = \mathbf{Pr}\left\{\gamma_R^{TSR} > 2^{2(R_0-R_s)} - 1\right\} = \mathbf{Pr}\left\{Y < \frac{\beta X}{(1-\beta)\theta_1} - \frac{1}{(1-\beta)\lambda}\right\}. \quad (17)$$

Substituting (10) and (13) into (17), the SOP of TSR is calculated as

$$P_{SOP}^{TSR} = 1 - \sum_{m=1}^{M} \sum_{p=0}^{m(N_d-1)} \sum_{k=0}^{p} \binom{M}{m} \binom{p}{k} v_p^m {\theta_1}^{N_s} \times \frac{(-1)^{m+p-k-1}\Gamma(N_s+k) e^{\frac{m}{(1-\beta)\lambda\bar{\gamma}_{RD}}}}{\Gamma(N_s)\lambda^{p-k}} \times \frac{(\beta\bar{\gamma}_{SR})^k((1-\beta)\bar{\gamma}_{RD})^{N_s+k-p}}{u^{N_s+k}}. \quad (18)$$

The SOP of TSR is also associated with parameters $\beta$ and $\rho$. Moreover, the trends of the changes are the same as the SOP of PSR.

### C. CONNECTION OUTAGE PROBABILITY

Only when the channel capacity of the legitimate node is bigger than $R_0$, the legitimate node can decode the received signal correctly. COP is used for measuring the reliability performance, and it can be formulated as follows [21].

$$P_{COP} = \mathbf{Pr}\left\{\frac{1}{2}\log_2(1+\gamma_D) < R_0\right\}, \quad (19)$$

where $\gamma_D \in \left\{\gamma_D^{PSR}, \gamma_D^{TSR}\right\}$.

#### 1) THE COP OF PSR

Substituting (5) into (19), the COP can be written as

$$P_{COP}^{PSR} = \mathbf{Pr}\left\{\gamma_D^{PSR} < 2^{2R_0} - 1\right\} \approx \mathbf{Pr}\left\{\frac{(1-\rho)\omega\eta\rho\beta\lambda XY}{\omega\eta\rho Y + 1 - \rho} < \theta_2\right\}, \quad (20)$$

where $\theta_2 = 2^{2R_0} - 1$. The approximation is tenable when the denominator in equation (5) neglects 1 item, and then approximated as $\lambda\left(\omega\eta\rho\|h_{RD}\|^2 + 1 - \rho\right)\Delta$, under the condition of high transmit SNR compared to the transmit power and channel gains [7], [28], [34].

Substituting (10) and (12) into (20), the COP of PSR can be calculated as

$$P_{COP}^{PSR} = 1 - \frac{2M}{\Gamma(N_d)} \sum_{n_s=0}^{N_s-1} \sum_{d=0}^{n_s} \sum_{m=0}^{M-1} \sum_{p=0}^{m(N_d-1)} \left(-v_p\right)^m \times \frac{\binom{n_s}{d}\binom{M-1}{m} e^{-\frac{\theta_2}{(1-\rho)\beta\lambda\bar{\gamma}_{SR}}} {\theta_2}^{\frac{N_d+p+2n_s-d}{2}}}{n_s!\,(1-\rho)^{n_s-d}(\beta\lambda\bar{\gamma}_{SR})^{\frac{N_d+p+2n_s-d}{2}}} \times \frac{\mathrm{K}_{(N_d+p-d)}\left(\sqrt{\frac{4\theta_2(m+1)}{\omega\eta\rho\beta\lambda\bar{\gamma}_{SR}\bar{\gamma}_{RD}}}\right)}{(\omega\eta\rho\bar{\gamma}_{RD})^{\frac{N_d+p+d}{2}}(m+1)^{\frac{N_d+p-d}{2}}}. \quad (21)$$

where $K_z(\bullet)$ represents the $z^{th}$ order modified Bessel functions of second kind.

Equation (21) shows that the COP decreases with the power allocation coefficient $\beta$. This is because more power allocated for information would lead to a higher probability of successful decoding the information.

#### 2) THE COP OF TSR

Substituting (9) into (19), the COP of TSR is given by

$$P_{COP}^{TSR} = \mathbf{Pr}\left\{\gamma_D^{TSR} < 2^{2R_0} - 1\right\} \approx \mathbf{Pr}\left\{\frac{2\omega\eta\alpha\beta\lambda XY}{2\omega\eta\alpha Y + 1 - \alpha} < \theta_2\right\}. \quad (22)$$

The approximation is based on the fact that the second item $(1-\alpha)$ of the denominator in equation (9) can be neglected, when the SNR is relatively high [7], [28], [34].

After calculating integrals of $X$, $Y$, the COP of TSR can be calculated as

$$P_{COP}^{TSR} = 1 - \sum_{n_s=0}^{N_s-1} \sum_{d=0}^{n_s} \sum_{m=0}^{M-1} \sum_{p=0}^{m(N_d-1)} \binom{n_s}{d}\binom{M-1}{m} \times \frac{2M\left(-v_p\right)^m e^{-\frac{\theta_2}{\beta\lambda\bar{\gamma}_{SR}}} {\theta_2}^{\frac{N_d+p+2n_s-d}{2}}(1-\alpha)^{\frac{N_d+p+d}{2}}}{\Gamma(N_d)\,n_s\,!\;(\beta\lambda\bar{\gamma}_{SR})^{\frac{N_d+p+2n_s-d}{2}}} \times \frac{K_{(N_d+p-d)}\left(\sqrt{\frac{2(1-\alpha)(m+1)\theta_2}{\alpha\omega\eta\beta\lambda\bar{\gamma}_{SR}\bar{\gamma}_{RD}}}\right)}{(m+1)^{\frac{N_d+p-d}{2}}(2\alpha\omega\eta\bar{\gamma}_{RD})^{\frac{N_d+p+d}{2}}}. \quad (23)$$

Note that the COP depends on the time switching factor $\alpha$, e.g., the COP decreases with increasing $\alpha$. This is because more power used for information transmission at $R$ would lead to higher reliability.

### D. EFFECTIVE SECRECY THROUGHPUT

Via the help of the untrusted relay $R$, the confidential information transmission from $S$ to $D^{(m*)}$, both requires the security and the reliability. Moreover, based on the definitions of SOP and COP, EST is defined as the product of secrecy rate and the

probability of a successful transmission, which is given by

$$\zeta = R_s \, \mathbf{Pr}\left\{\frac{1}{2}\log_2(1+\gamma_R) < R_0 - R_s, \frac{1}{2}\log_2(1+\gamma_D) > R_0\right\}. \tag{24}$$

### 1) THE EST OF PSR

Plugging (2) and (5) into (24), and integrating over the PDF of $X$ and $Y$, the EST of PSR is calculated as

$$\begin{aligned}\zeta^{PSR} &\approx \frac{R_s}{2}\,\mathbf{Pr}\left\{\gamma_R^{PSR} < \theta_1\ ,\ \gamma_D^{PSR} > \theta_2\right\} \\ &= \frac{R_s}{2}\,\mathbf{Pr}\left\{X < \frac{(1-\beta)\,\theta_1 Y}{\beta} + \frac{\theta_1}{(1-\rho)\,\beta\lambda}\right. \\ &\qquad \left. X > \frac{\theta_2}{(1-\rho)\,\beta\lambda} + \frac{\theta_2}{\omega\eta\rho\beta\lambda Y}\right\}. \end{aligned} \tag{25}$$

After some manipulations, we can get the EST expression of PSR as follows.

$$\zeta^{PSR} = \frac{R_s}{2}\left\{\ \Xi_1\ -\Xi_2\ \right\}, \tag{26}$$

where $\Xi_1$ and $\Xi_2$ are given by

$$\begin{aligned}\Xi_1 = &\sum_{n_s=0}^{N_s-1}\sum_{d=0}^{n_s}\sum_{m=0}^{M-1}\sum_{p=0}^{m}\sum_{k=0}^{(N_d-1)}\sum^{\infty}\binom{n_s}{d}\binom{M-1}{m} \\ &\times\frac{(-1)^{m+k}e^{-\frac{\theta_2}{(1-\rho)\beta\lambda\bar{\gamma}_{SR}}}v_p^m\theta_2{}^{n_s+k}(m+1)^{d+k-N_d-p}}{n_s!\ \ k!\ \ (\beta\lambda\bar{\gamma}_{SR})^{n_s+k}} \\ &\times\frac{M\Gamma\left(N_d+p-d-k\ ,\ \frac{(m+1)u_{PSR}}{\bar{\gamma}_{RD}}\right)}{\Gamma(N_d)\,(\omega\eta\rho\bar{\gamma}_{RD})^{d+k}(1-\rho)^{n_s-d}} \end{aligned} \tag{27}$$

and

$$\begin{aligned}\Xi_2 = &\sum_{n_s=0}^{N_s-1}\sum_{d=0}^{n_s}\sum_{m=0}^{M-1}\sum_{p=0}^{m}\binom{n_s}{d}\binom{M-1}{m} \\ &\times\frac{M\left(-v_p\right)^m\theta_1{}^{n_s}e^{-\frac{\theta_1}{(1-\rho)\beta\lambda\bar{\gamma}_{SR}}}(\beta\bar{\gamma}_{SR})^{N_d+p+d-n_s}}{\Gamma(N_d)\ \ n_s!\,((1-\rho)\,\lambda)^{n_s-d}} \\ &\times\frac{((1-\beta)\,\bar{\gamma}_{RD})^d\,\Gamma\left(N_d+p+d,\ \frac{u\,u_{PSR}}{\beta\bar{\gamma}_{SR}\bar{\gamma}_{RD}}\right)}{u^{N_d+p+d}}, \end{aligned} \tag{28}$$

respectively, where $u_{PSR} = \left(b_1 + \sqrt{b_1^2 + 4a_1c_1}\right)/2a_1$, $a_1 = \omega\eta\rho\lambda(1-\rho)(1-\beta)\theta_1$, $b_1 = \omega\eta\rho(\theta_2-\theta_1)$, and $c_1 = (1-\rho)\theta_2$.

*Proof:* See Appendix.

The equation (26) shows that the EST is related to $\beta$, and the impact of $\beta$ on the EST is illustrated in Fig. 5.

When the transmit SNR goes to infinity, the asymptotical expression of EST can be calculated as

$$\begin{aligned}\lim_{\lambda\to\infty}\zeta^{PSR} = \frac{R_s}{2}\left\{1-\sum_{n_s=0}^{N_s-1}\sum_{m=0}^{M-1}\sum_{p=0}^{m(N_d-1)}\binom{M-1}{m}\right. \\ \left.\times\frac{\left(-v_p\right)^m M\ \Gamma(N_d+p+n_s)}{\Gamma(N_d)\ \ n_s!} \right. \\ \left.\times\frac{((1-\beta)\,\theta_1\bar{\gamma}_{RD})^{n_s}(\beta\ \bar{\gamma}_{SR})^{N_d+p}}{u^{N_d+p+n_s}}\right\}. \end{aligned} \tag{29}$$

### 2) THE EST OF TSR

Similar to PSR, the EST of TSR is calculated as

$$\begin{aligned}\zeta^{TSR} &\approx \frac{(1-\alpha)\ R_s}{2}\,\mathbf{Pr}\left\{\gamma_R^{TSR} < \theta_1\ ,\ \gamma_D^{TSR} > \theta_2\right\} \\ &= \frac{(1-\alpha)\ MR_s}{2\Gamma(N_d)}\left\{\ \Xi_3\ -\Xi_4\ \right\}, \end{aligned} \tag{30}$$

where $\Xi_3$ and $\Xi_4$ are as follows.

$$\begin{aligned}\Xi_3 = &\sum_{n_s=0}^{N_s-1}\sum_{d=0}^{n_s}\sum_{m=0}^{M-1}\sum_{p=0}^{m}\sum_{k=0}^{(N_d-1)}\sum^{\infty}\binom{n_s}{d}\binom{M-1}{m} \\ &\times\frac{(-1)^{m+k}\ v_p^m e^{-\frac{\theta_2}{\beta\lambda\bar{\gamma}_{SR}}}(1-\alpha)^{d+k}(m+1)^{d+k-N_d-p}}{n_s!\ \ k!\ \ (\beta\lambda\bar{\gamma}_{SR})^{n_s}} \\ &\times\frac{\theta_2{}^{n_s+k}\Gamma\left(N_d+p-d-k\ ,\ \frac{(m+1)u_{TSR}}{\bar{\gamma}_{RD}}\right)}{(2\omega\eta\alpha\bar{\gamma}_{RD})^{d+k}} \end{aligned} \tag{31}$$

and

$$\begin{aligned}\Xi_4 = &\sum_{n_s=0}^{N_s-1}\sum_{d=0}^{n_s}\sum_{m=0}^{M-1}\sum_{p=0}^{m}\binom{n_s}{d}\binom{M-1}{m} \\ &\times\frac{\left(-v_p\right)^m\theta_1^{n_s}e^{-\frac{\theta_1}{\beta\lambda\bar{\gamma}_{SR}}}(\beta\bar{\gamma}_{SR})^{N_d+p+d-n_s}}{n_s!\ \ \lambda^{n_s-d}} \\ &\times\frac{((1-\beta)\,\bar{\gamma}_{RD})^d\ \Gamma\left(N_d+p+d,\ \frac{u\,u_{TSR}}{\beta\bar{\gamma}_{SR}\bar{\gamma}_{RD}}\right)}{u^{N_d+p+d}}, \end{aligned} \tag{32}$$

respectively, where $u_{TSR} = \left(b_2 + \sqrt{b_2^2 + 4a_2c_2}\right)/2a_2$, $a_2 = 2\theta_1\omega\eta\alpha\lambda(1-\beta)$, $b_2 = 2(\theta_2-\theta_1)$ and $c_2 = \theta_2(1-\alpha)$.

When the transmit SNR goes to infinity, the asymptotical EST expressions of TSR can be calculated as

$$\begin{aligned}\lim_{\lambda\to\infty}\zeta^{TSR} = \frac{(1-\alpha)\,R_s}{2}\left\{1-\sum_{n_s=0}^{N_s-1}\sum_{m=0}^{M-1}\sum_{p=0}^{m(N_d-1)}\right. \\ \left.\times\frac{\binom{M-1}{m}\left(-v_p\right)^m M\ \Gamma(N_d+p+n_s)}{\Gamma(N_d)\ \ n_s!} \right. \\ \left.\times\frac{((1-\beta)\,\theta_1\bar{\gamma}_{RD})^{n_s}(\beta\ \bar{\gamma}_{SR})^{N_d+p}}{u^{N_d+p+n_s}}\right\}. \end{aligned} \tag{33}$$

The equations (29) and (33) show that the ESTs are irrelevant with the transmit SNR when the transmit SNR goes to infinity. The accuracy of the asymptotic expressions are validated by simulation results in Section IV.

## IV. NUMERICAL RESULTS

In this section, the numerical results in terms of SOP, COP, and EST are presented to examine the security and the reliability performance. Unless otherwise stated, the simulation parameters in all figures are set as follows. The codeword transmission rate and the confidential information rate are set $R_0 = 2$bit/s/Hz, $R_s = 1$bit/s/Hz, respectively. In addition, the energy conversion efficiency coefficient $\eta = 0.8$, and the harvested energy allocation coefficient $\omega = 0.9$.

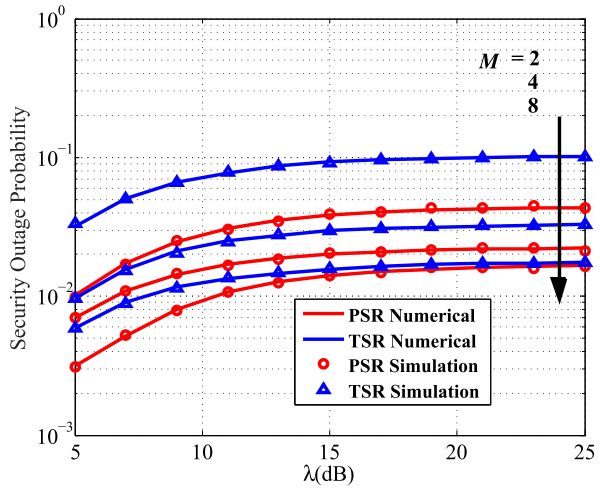



**FIGURE 2.** The SOPs of PSR and TSR versus λ.

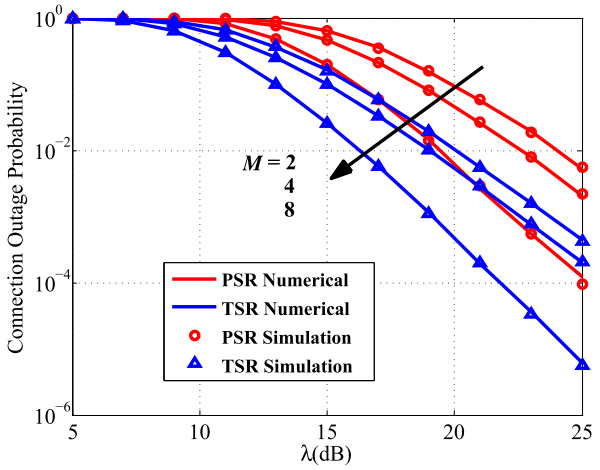



**FIGURE 3.** The COPs of PSR and TSR versus λ.

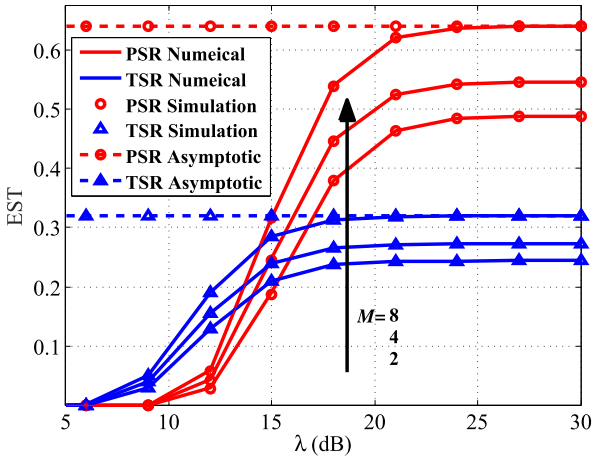



**FIGURE 4.** The ESTs of PSR and TSR for different λ and *M*.

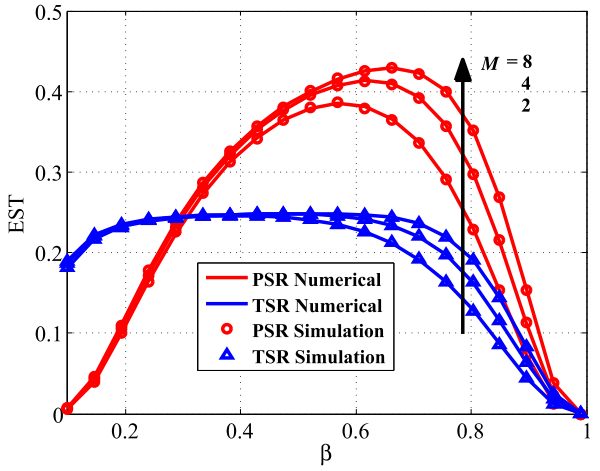



**FIGURE 5.** Impact of $\beta$ on the ESTs of PSR and TSR.

The symbols 'o' and 'Δ' denote PSR and TSR simulation results, respectively, and the dashed lines represent their asymptotic analysis. The solid curves are the numerical analysis in each figure. It is observed that the numerical analysis of the metrics are in excellent agreement with corresponding simulation points.

Fig. 2 and Fig. 3 plot the SOP and COP performance of PSR and TSR over different λ, respectively, with $\alpha = \beta = 0.5$, where $\lambda = P/N_0$ denotes the transmit SNR. When the number of the destinations is fixed, three observations can be drawn: 1) The SOP of either PSR or TSR increases accordingly with the transmit SNR increases, and then reaches a constant in the high transmit SNR regime, respectively. This is because the untrusted relay obtains more information by increasing the transmit SNR firstly, and then the jamming signals transmitted by the destination guarantees the security of information in high SNR regime. 2) The COP of either PSR or TSP gradually decreases along with increasing the transmit SNR. The reason is that the destination can obtain more information with higher the transmit SNR. 3) The SOP of PSR is smaller than TSR, while the COP of PSR is bigger than TSR. It implies that the security performance of PSR is superior to TSR, whereas the reliability performance of PSR is inferior to TSR. For the fixed transmit power, it is observed that increasing the destination numbers significantly decreasing the outage probabilities. It is because increasing the number of destinations results in a higher transmit SNR at the destination, and the destination transmits the jamming signal and receives the information with larger power compared with the noise power.

Fig. 4 plots the ESTs of PSR and TSR versus the transmit SNR λ for the different destination numbers $M$, with $\alpha = \beta = 0.5$. The EST asymptotic curves of PSR and TSR are given when $M = 8$, which are marked as the dashed curves with 'o' and 'Δ', respectively. It is observed that: 1) For a fixed $M$, the EST continuously increases along with increasing λ, and then approaches a saturation. It is validated by the asymptotic curve when λ goes to infinity. 2) The EST of TSR is obviously larger than PSR firstly. With the continuously increasing λ, the EST of TSR is smaller than PSR. This can be explained that the effective communication time of TSR is less than PSR in the high transmit SNR regime.

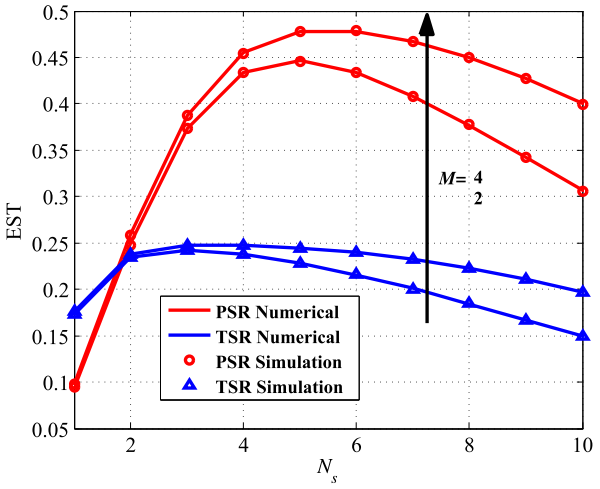



**FIGURE 6.** The ESTs of PSR and TSR versus $N_s$.

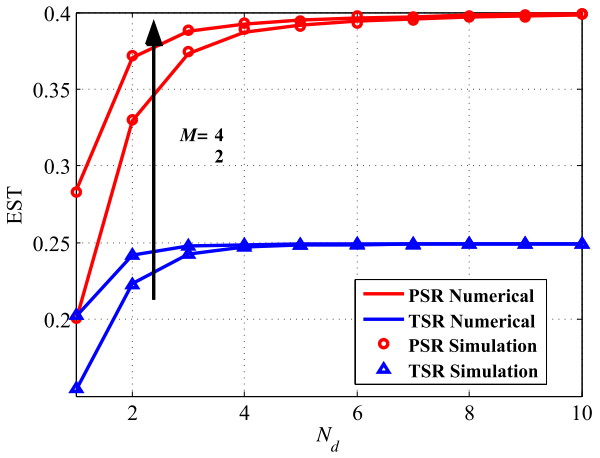



**FIGURE 7.** The ESTs of PSR and TSR versus $N_d$.

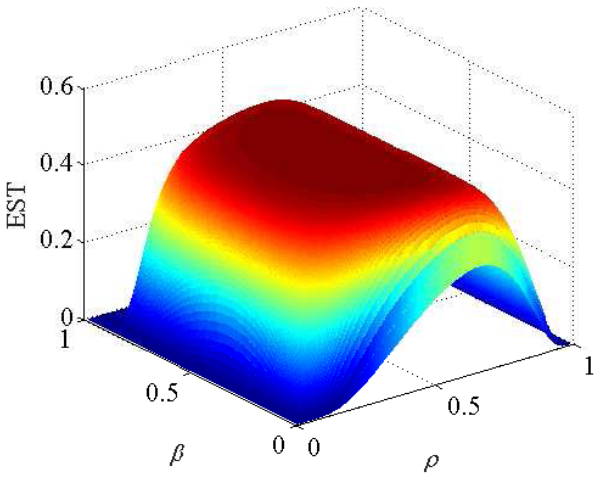



**FIGURE 8.** The EST of TSR versus $\beta$ and $\rho$ with $M = 4$.

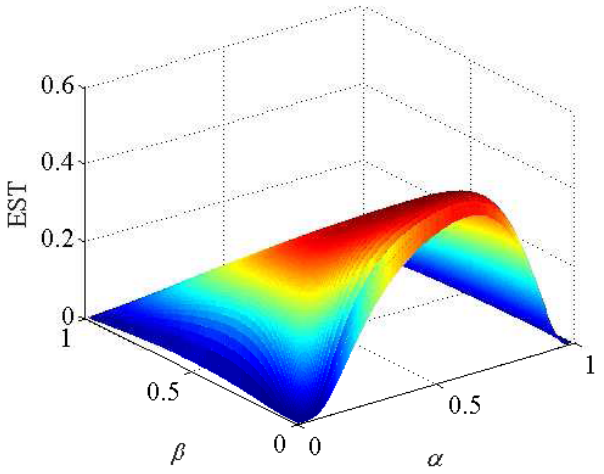



**FIGURE 9.** The EST of TSR versus $\beta$ and $\alpha$ with $M = 4$.

3) The EST of either PSR or TSR increases with increasing $M$. This is due to the fact that the outage probabilities decrease with increasing $M$.

Fig. 5 illustrates the impact of the power allocation coefficient $\beta$ on the ESTs of PSR and TSR with different $M$, where $\alpha = 0.5$. Several observations are observed: 1) When $\beta$ is small, the EST of TSR is superior to PSR. This is due to that the transmit power is so small at the source node, then the relay and the destination gain the less information, which leads to smaller EST. By increasing $\beta$, the allocated transmit power for the source increases. The EST of either PSR and TSR increases and the EST of PSR is bigger than TSR. Nevertheless, bigger $\beta$ results in less transmit power for the destination, which degrades the security performance, furthermore, the EST degrades. Hence, there is a maximal EST with an optimal $\beta$. 2) When $\beta$ is small, the ESTs of PSR and TSR are almost unchanged with different $M$. This is because small $\beta$ leads to small EST, and then there is limited significance effect on the EST along with increasing $M$. With more allocated transmit power for the source, the EST continuously increases with increasing $M$. Because increasing $M$ can improve the reliability performance of the system.

Fig. 6 and Fig. 7 show the impact of the number of $N_s$ and $N_d$ on the ESTs of PSR and TSR, where $\alpha = \beta = 0.5$. It is observed that the EST of either PSR and TSR will be enlarged by increasing $N_s$ firstly. However continuously increasing $N_s$ results in leaking more information to the untrusted relay, therefore, the EST deteriorates. Moreover, the connection performance can be improved by increasing $N_d$. Due to constraint of the total transmit power, the EST tends to the floor and no longer increases with more $N_d$.

Fig. 8 and Fig. 9 show the impact of the power splitting coefficient $\rho$ and the time switching factor $\alpha$ on the ESTs for PSR and TSR with different $\beta$. It is noted that for a fixed $\beta$, the EST gradually increases and reaches the maximum value with an optimal $\rho$ and an optimal $\alpha$. Afterwards, the EST begins to deteriorate as $\rho$ and $\alpha$ continuously increases. This is because small $\rho$ and $\alpha$ will decline the harvested energy

at $R$, which degrade the EST. On the flip side, less energy for transmitting information of PSR and less effective communication time of TSR, i.e., the larger $\rho$ and $\alpha$, both decline the EST.

## V. CONCLUSION

In this paper, the secure communications in an untrusted and energy harvesting relay network is investigated. Multiple destinations are employed to improve the reliability of receiving information. By applying the SOP, COP, and EST metrics, the closed-form analytical expressions have been derived under both PSR and TSR. In addition, the asymptotic analysis of EST has also been presented. Our analysis and simulations highlight that the EST increases with increasing $M$, and optimal ETS performance can be obtained by switching PSR and TSR protocols.

## APPENDIX

In Appendix, we provide the proof of the EST expression under PSR protocol. In (25), let $x_2 = \frac{(1-\beta)\theta_1 Y}{\beta} + \frac{\theta_1}{(1-\rho)\beta\lambda}$ and $x_1 = \frac{\theta_2}{(1-\rho)\beta\lambda} + \frac{\theta_2}{\omega\eta\rho\beta\lambda Y}$. Then the formula (25) can be rewritten as

$$\begin{aligned}\zeta^{PSR} &= \frac{R_s}{2}\,\mathbf{Pr}\left\{x < x_2\ ,\ x > x_1\right\} \\ &= \frac{R_s}{2}\int_{u_{PSR}}^{\infty}\int_{x_1}^{x_2} f\left(x\right) f\left(y\right) dxdy \end{aligned} \tag{34}$$

Note that when $y > u_{PSR}$, $x_2$ is larger than $x_1$, where $u_{PSR} = \left(b_1 + \sqrt{b_1^2 + 4a_1c_1}\right)/2a_1$, $a_1 = \omega\eta\rho\lambda(1-\rho)(1-\beta)\theta_1$, $b_1 = \omega\eta\rho(\theta_2 - \theta_1)$, and $c_1 = (1-\rho)\theta_2$. Plugging (11) into (34), the EST of PSR can be rewritten as

$$\begin{aligned}\zeta^{PSR} = \frac{R_s}{2}\Bigg\{ &\underbrace{\int_{u_{PSR}}^{\infty} e^{-\frac{x_1}{\bar{\gamma}_{SR}}} \sum_{n_s=0}^{N_s-1} \frac{\left(\frac{x_1}{\bar{\gamma}_{SR}}\right)^{n_s}}{n_s\,!} f\left(y\right)\, dy}_{\Xi_{11}} \\ &- \underbrace{\int_{u_{PSR}}^{\infty} e^{-\frac{x_2}{\bar{\gamma}_{SR}}} \sum_{n_s=0}^{N_s-1} \frac{\left(\frac{x_2}{\bar{\gamma}_{SR}}\right)^{n_s}}{n_s\,!} f\left(y\right)\, dy}_{\Xi_{22}}\Bigg\} \end{aligned} \tag{35}$$

Plugging (12) into (35), and after some manipulations, the integral of $\Xi_{11}$ and $\Xi_{22}$ are calculated as

$$\begin{aligned}\Xi_{11} = &\frac{M}{\Gamma\left(N_d\right)} \sum_{n_s=0}^{N_s-1}\sum_{d=0}^{n_s}\sum_{m=0}^{M-1}\sum_{p=0}^{m(N_d-1)}\sum_{k=0}^{\infty} \frac{(-1)^{m+k} v_p^m}{n_s\,!\,k!} \\ &\times \frac{\binom{n_s}{d}\binom{M-1}{m} e^{-\frac{\theta_2}{(1-\rho)\beta\lambda\bar{\gamma}_{SR}}} \theta_2^{n_s+k}}{(\beta\lambda\bar{\gamma}_{SR})^{n_s+k}(\omega\eta\rho)^{d+k}(1-\rho)^{n_s-d}(\bar{\gamma}_{RD})^{N_d+p}} \\ &\times \int_{u_{PSR}}^{\infty} y^{N_d+p-d-k-1} e^{-\frac{(m+1)y}{\bar{\gamma}_{RD}}} dy \end{aligned} \tag{36}$$

and

$$\begin{aligned}\Xi_{22} = &\frac{M}{\Gamma\left(N_d\right)} \sum_{n_s=0}^{N_s-1}\sum_{d=0}^{n_s}\sum_{m=0}^{M-1}\sum_{p=0}^{m(N_d-1)}\sum_{k=0}^{\infty} (-1)^m \\ &\times \frac{\binom{n_s}{d}\binom{M-1}{m} e^{-\frac{\theta_1}{(1-\rho)\beta\lambda\bar{\gamma}_{SR}}} \theta_1^{n_s} v_p^m (1-\beta)^d}{n_s\,!\,(\beta\bar{\gamma}_{SR})^{n_s}((1-\rho)\,\lambda)^{n_s-d}(\bar{\gamma}_{RD})^{N_d+p}} \\ &\times \int_{u_{PSR}}^{\infty} y^{N_d+p+d-1} e^{-\left(\frac{(1-\beta)\theta_1}{\beta\bar{\gamma}_{SR}} + \frac{m+1}{\bar{\gamma}_{RD}}\right)y} dy. \end{aligned} \tag{37}$$

Applying [33, eq. (3.381.3.8)], the $\Xi_{11}$ and $\Xi_{22}$ are calculated as equations (27) and (28), respectively.

## REFERENCES


[1] Y. Ye, Y. Li, Z. Wang, X. Chu, and H. Zhang, "Dynamic asymmetric power splitting scheme for SWIPT-based two-way multiplicative AF relaying," *IEEE Signal Process. Lett.*, vol. 25, no. 7, pp. 1014–1018, Jul. 2018.

[2] Z. Zhang, Z. Ma, Z. Ding, M. Xiao, and G. K. Karagiannidis, "Full-duplex two-way and one-way relaying: Average rate, outage probability, and tradeoffs," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 3920–3933, Jun. 2016.

[3] C. Peng, F. Li, and H. Liu, "Optimal power splitting in two-way decode-and-forward relay networks," *IEEE Commun. Lett.*, vol. 21, no. 9, pp. 2009–2012, Sep. 2017.

[4] B. V. Nguyen and K. Kim, "Secrecy outage probability of optimal relay selection for secure anf cooperative networks," *IEEE Commun. Lett.*, vol. 19, no. 12, pp. 2086–2089, Dec. 2015.

[5] S. Ulukus *et al.*, "Energy harvesting wireless communications: A review of recent advances," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 3, pp. 360–381, Apr. 2015.

[6] N. Qi, M. Xiao, T. A. Tsiftsis, L. Zhang, M. Skoglund, and H. Zhang, "Efficient coded cooperative networks with energy harvesting and transferring," *IEEE Trans. Wireless Commun.*, vol. 16, no. 10, pp. 6335–6349, Oct. 2017.

[7] 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, Jul. 2013.

[8] R. Yao, F. Xu, T. Mekkawy, and J. Xu, "Optimised power allocation to maximise secure rate in energy harvesting relay network," *Electron. Lett.*, vol. 52, no. 22, pp. 1879–1881, Oct. 2016.

[9] 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, Sep. 2013.

[10] 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.

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

[12] A. Alsharoa, H. Ghazzai, A. E. Kamal, and A. Kadri, "Optimization of a power splitting protocol for two-way multiple energy harvesting relay system," *IEEE Trans. Green Commun. Netw.*, vol. 1, no. 4, pp. 444–457, Dec. 2017.

[13] V. N. Vo, T. G. Nguyen, C. So-In, and D.-B. Ha, "Secrecy performance analysis of energy harvesting wireless sensor networks with a friendly jammer," *IEEE Access*, vol. 5, pp. 25196–25206, 2017.

[14] M. Ju, K.-M. Kang, K.-S. Hwang, and C. Jeong, "Maximum transmission rate of PSR/TSR protocols in wireless energy harvesting DF-based relay networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 12, pp. 2701–2717, Dec. 2015.

[15] X. He and A. Yener, "Two-hop secure communication using an untrusted relay: A case for cooperative jamming," in *Proc. IEEE Global Telecommun. Conf.*, Nov./Dec. 2008, pp. 1–5.

[16] T. Mekkawy, R. Yao, F. Xu, and L. Wang, "Optimal power allocation for achievable secrecy rate in an untrusted relay network with bounded channel estimation error," in *Proc. 26th Wireless Opt. Commun. Conf. (WOCC)*, Apr. 2017, pp. 1–5.

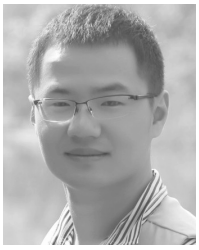
[17] R. Yao, Y. Lu, T. A. Tsiftsis, N. Qi, T. Mekkawy, and F. Xu, "Secrecy rate-optimum energy splitting for an untrusted and energy harvesting relay network," *IEEE Access*, vol. 6, pp. 19238–19246, 2018.

[18] D. J. Su, S. A. Mousavifar, and C. Leung, "Secrecy capacity and wireless energy harvesting in amplify-and-forward relay networks," in *Proc. IEEE Pacific Rim Conf. Commun., Comput. Signal Process. (PACRIM)*, Aug. 2015, pp. 258–262.
[19] 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, Jun. 2014.
[20] A. Kuhestani, A. Mohammadi, and M. Noori, "Optimal power allocation to improve secrecy performance of non-regenerative cooperative systems using an untrusted relay," *IET Commun.*, vol. 10, no. 8, pp. 962–968, May 2016.
[21] D. Chen, Y. Cheng, W. Yang, J. Hu, and Y. Cai, "Physical layer security in cognitive untrusted relay networks," *IEEE Access*, vol. 6, pp. 7055–7065, 2017.
[22] V. Gupta, S. S. Kalamkar, and A. Banerjee, "On secure communication using rf energy harvesting two-way untrusted relay," in *Proc. IEEE Global Commun. Conf.*, Dec. 2017, pp. 1–7.
[23] M. T. Mamaghani, A. Mohammadi, P. L. Yeoh, and A. Kuhestani, "Secure two-way communication via a wireless powered untrusted relay and friendly jammer," in *Proc. IEEE Global Commun. Conf.*, Dec. 2017, pp. 1–6.
[24] D.-D. Tran, H.-V. Tran, D.-B. Ha, H. Tran, and G. Kaddoum, "Performance analysis of two-way relaying system with RF-EH and multiple antennas," in *Proc. IEEE 84th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2016, pp. 1–5.
[25] S. Sharma, S. D. Roy, and S. Kundu, "Two way secure communication with two half-duplex DF relay," in *Proc. IEEE Region 10 Conf. (TENCON)*, Nov. 2017, pp. 869–874.
[26] S. Sharma, S. D. Roy, and S. Kundu, "Secrecy performance of a two-way communication network with two half-duplex DF relays," *Inst. Eng. Technol.* [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-com.2018.5635. doi: 10.1049/iet-com.2018.5635.
[27] 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.
[28] S. S. Kalamkar and A. Banerjee, "Secure communication via a wireless energy harvesting untrusted relay," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2199–2213, Mar. 2017.
[29] 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.
[30] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.
[31] J. Chen, H. Chen, H. Zhang, and F. Zhao, "Spectral-energy efficiency tradeoff in relay-aided massive MIMO cellular networks with pilot contamination," *IEEE Access*, vol. 4, pp. 5234–5242, Jul. 2016.
[32] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[33] I. S. Gradshteyn and I. M. Ryzhik, *Tables of Integrals, Series, and Products*, 7th ed. Boca Raton, FL, USA: Academic, 2007.
[34] Z. Wang, Z. Chen, B. Xia, L. Luo, and J. Zhou, "Cognitive relay networks with energy harvesting and information transfer: Design, analysis, and optimization," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2562–2576, Apr. 2015.
[35] J. G. Proakis, *Digital Communications*, 5th ed. New York, NY, USA: McGraw-Hill, 2001.

**HUI SHI** received the M.S. degree from the Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2007. She is currently pursuing the Ph.D. degree in information and communications engineering with the College of Communications Engineering, Army Engineering University of PLA, Nanjing. Her current research interests include cooperative communications, wireless sensor networks, the Internet of Things, physical layer security, SWIPT, and cognitive radio systems.

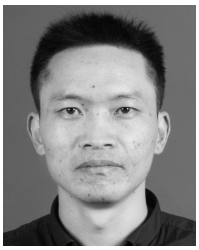
**YUEMING CAI** (M'05–SM'12) received the B.S. degree in physics from Xiamen University, Xiamen, China, in 1982, and the M.S. degree in micro-electronics engineering and the Ph.D. degree in communications and information systems from Southeast University, Nanjing, China, in 1988 and 1996, respectively. His current research interests include multi-in multi-out systems, OFDM systems, signal processing in communications, cooperative communications, and wireless sensor networks.

**DECHUAN CHEN** received the M.S. degree in information and communication engineering from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2017, where he is currently pursuing the Ph.D. degree in information and communications engineering. His research interests include cooperative communications, physical-layer security, energy harvesting, and cognitive radio systems.



**JIANWEI HU** (S'14) received the B.S. degree in communication engineering from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2012, where he is currently pursuing the Ph.D. degree in communications and information system. His research interests include multi-in multi-out systems, cooperative communications, and network security.

**WEIWEI YANG** (S'08–M'12) received the B.S., M.S., and Ph.D. degrees from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2003, 2006, and 2011, respectively. His research interests include orthogonal frequency domain multiplexing systems, signal processing in communications, cooperative communications, wireless sensor networks, and network security.



**WENDONG YANG** received the B.S. degree in communications engineering and the Ph.D. degree in communications and information systems from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2004 and 2009, respectively. His current research interests include multi-in multi-out systems, OFDM systems, cooperative communications, and cognitive radio.