Article

Secure Transmission for Simultaneous Wireless Information and Power Transfer in AF Untrusted Relay Networks

Hui Shi ¹, Weiwei Yang ^{1,*}, Dechuan Chen ², Yunpeng Luo ¹ and Yueming Cai ¹

¹ Army Engineering University of PLA, No. 88 Houbiaoying, Qinhuai District, Nanjing 210007, China; lgdhpky@aliyun.com (H.S.); luoyunp@aliyun.com (Y.L.); caiym@vip.sina.com (Y.C.)

² Wuhan Zhong Yuan Electronics Group Company Ltd., Wuhan 430205, China; Chenchuan927@163.com

* Correspondence: wwyang1981@163.com; Tel.: +86-025-8082-9409

Received: 9 November 2018; Accepted: 21 December 2018; Published: 26 December 2018

Abstract: This paper investigates secure communications of energy harvesting untrusted relay networks, where the destination assists jamming signal to prevent the untrusted relay from eavesdropping and to improve the forwarding ability of the energy constrained relay. Firstly, the source and the destination transmit the signals to the relay with maximal ratio transmission (MRT) technique or transmit antenna selection (TAS) technique. Then, the destination utilizes maximal ratio combining (MRC) technique or receive antenna selection (RAS) technique to receive the forwarded information. Therefore, four transmission and reception schemes are considered. For each scheme, the closed-form expressions of the secrecy outage probability (SOP) and the connection outage probability (COP) are derived. Besides, the effective secrecy throughput (EST) metric is analyzed to achieve a good tradeoff between security and reliability. In addition, the asymptotic performance of EST is also considered at the high signal-to-noise ratio (SNR). Finally, simulation results illustrate that: (1) the EST of the system with MRT and MRC scheme are superior to other schemes, however, in the high SNR regime, the EST of the system with MRT scheme is inferior to TAS; and (2) for the source node, there exists an optimal number of antennas to maximize the EST of the proposed schemes.

Keywords: energy harvesting; amplify-and-forward; multiple antennas; untrusted relay; outage probability; effective secrecy throughput

1. Introduction

Because of the inherent broadcasting characteristics of the wireless channel, wireless communications are vulnerable to be attacked by the eavesdroppers through the public channel. The traditional method to protect the information privacy is the assistance of upper-layer cryptographic secure schemes, which mainly depends on computation complexity. However, with the rapid advancement of the computing capability, the security of the wireless communication encounters tremendous challenges and risks. In view of this, the physical layer security (PLS) has been proposed as a complement of current cryptographic method, which takes advantage of time-varying characteristics and the randomness of the wireless channel. The research on PLS was pioneered by Wyner, who introduced the degraded wire-tap channel and gave the definition of secrecy capacity [1]. The notion of secrecy capacity measures the maximal secrecy rate at which the confidential information can be transmitted to the destination secretly and reliably [1–3].

Recently, cooperative communication is an effective way to extend the coverage of the transmission and to increase the secrecy capacity. The performance of the dual-hop relay network has been studied for both the single relay and multiple relays under Rayleigh fading channels

in [4–7]. In [6], the authors significantly improve the security of the system with source relay selection scheme. Taking the place of full-duplex relaying, two-path successive relaying protocol is proposed to reduce the probability of being intercepted [7]. However, the relay may not be trusted, which is also a potential eavesdropper [8–16]. Several works about the untrusted relay have been published, where the destination node transmits the jamming signals to the untrusted relay for securing the transmissions [9–15]. In [16], a destination-assisted jamming scheme is put forward and the instantaneous secrecy rate is studied in multiple amplify-and-forward (AF) untrusted relay networks. In [17,18], a jamming signal is designed in a smart way. The artificial noise symbols are designed and transmitted to degrade the error probability performance [17]. The artificial noise parameter is derived for two kinds of optimal points, max-min point and single user point [18].

Ref. [19] considers an untrusted relay cognitive Internet of Things (IoT) network, where the probability of successfully secure transmission metric is investigated to evaluate the security of the network. To further improve the secrecy performance of cooperative networks, multiple antennas technique has been implemented into the system [20–22]. Both the source and the destination are multi-antennas, while the relay is only one antenna in the considered network [20]. Ref. [21] studies the AF multiple-input multiple-output (MIMO) system with untrusted relay; besides, both the destination and the relay are multiple antennas. In [22], a large-scale MIMO relaying system with an energy harvesting relay is investigated, and the secrecy performance of the system under imperfect channel state information (CSI) is analyzed.

Utilizing the precoding techniques could also improve the secrecy performance of the cooperative networks [23–26]. In [23], precoding at both the source and the relay scheme is proposed. To maximize the secrecy rate, the source, relay, and destination precoding matrices are jointly designed. In [24], to maximize the secrecy sum rate, the source's signal, artificial noise precoders and the relay's precoder, under the sources and relay transmit power constraints, are jointly designed. In [25], the authors investigate the source and relay precoders that characterize the relationship between the achievable stored energy at the relay and the achievable source-to-destination rate. In [26], the authors examine the maximal energy efficiency by design of the optimum precoding matrices at the transceivers and the relay node as well as the optimum power splitting factor for SWIPT.

In some special application scenarios, many energy-constrained cooperative relays are configured to cover larger districts where recharging and exchanging relay batteries are not convenient and economical [27]. Energy harvesting (EH) has been developed as a promising energy source for dealing with this problem [28–30]. Moreover, EH and information processing simultaneously has been applied in cooperative relaying [31–35], where they relay harvests energy from the receipt signals and then forwards the information to the destination via the received power. To harvest energy and decode information from the received signals, the power splitting relaying (PSR) and the time switching relaying (TSR) are proposed [36–38]. Besides, EH is considered in energy-free Internet of Things (IoT) device within the bistatic scatter (BS) mode [39].

The effects of EH relay on the secrecy performance have been studied in [38,40,41]. In [38], the authors focus on an AF two-way relay network employing the multiple access broadcast protocol and TSR protocol, where the legitimate communication parties are multi-antennas while the assisted relay is only one antenna. However, the communication parties adopt MRT/MRC techniques. Moreover, the relay is considered to be trusted, thus only the connection outage probability (COP) is considered for MRT/MRC techniques, and the secrecy outage probability (SOP) performance is not analyzed. The SOP and COP metrics of the system are analyzed in [40]. The SOP performance is analyzed over Nakagami-m Fading Channels [41,42]. The authors improve the harvested energy with multiple antennas, and study the maximal harvested power by jointly different parameters [43–45]. The cooperative jamming is considered in [45], and the maximal secrecy rate is investigated. The author studies the secrecy transmission with the unreliable wireless backhaul link, and derives the closed-expressions for SOP ergodic secrecy rate and non-zero achievable secrecy rate to examine the effect of the backhaul

reliability on the system performance [46]. However, each node is equipped with a single antenna and all relays are considered to be trusted.

Some efforts on the multi-user scenarios have been considered in [47–50]. In [47], the authors investigate the relay network consisting of a source, a set of relays and users in the presence of an eavesdropper. Each terminal is equipped with a single antenna. The cooperative beamforming and user selection techniques are applied to protect the confidential message. The secrecy rate (SR) and SOP of the network are investigated. Dong-Hua Chen et al. [48] investigates full-duplex (FD) secure transmissions with simultaneous wireless information and power transfer (SWIPT) on downlink (DL), where an FD base station, with multiple transmit antennas and multiple receive antennas, serves a group of single-antenna users on both DL and uplink (UL). The minimization of the system power under constraints on EH and security rates is examined. In [49], a MIMO relay system consists of one base station, one relay station, multiple legitimate users and malicious eavesdroppers. The system worst-case secrecy rate is maximized by jointly optimizing base station beamforming matrix, the relay station amplify-and-forward transformation matrix, and the covariance matrix of artificial noise. In [50], the authors investigate the secrecy performance of multiuser dual-hop relay networks where a base station communicates with multiple legitimate users through the assistance of a trustful regenerative relay in the presence of multiple eavesdroppers. To evaluate the secrecy performance of the considered system, two practical situations are addressed based on the availability of eavesdropper's CSI, where the eavesdropper's CSI is unavailable or available at the relay. The new exact and asymptotic closed form expressions for the SOP and the ergodic secrecy rate (ESR) are accordingly derived. However, the relay in the aforementioned multiple users system model is trusted.

Thus, few works have examined the SOP performance of the SWIPT untrusted relay MIMO system. Besides, the trade-off between the SOP and COP has not been studied in the above literature. Note that the SOP and COP are used for characterizing the security and reliability performance of the system, respectively. However, the SOP and COP are a pair of contradictory metrics. Thus, the trade-off between SOP and COP also deserves careful consideration. Motivated by the above, this paper concentrates on an AF untrusted relay network, where both the source and the destination are multi-antennas. To reduce the computational complexity, the relay is equipped with a single antenna. Hence, to enhance the PLS of the system, four transmission and reception schemes are considered, i.e., transmit antenna selection-receive antenna selection (TAS-RAS), maximal ratio transmission-receive antenna selection (MRT-RAS), transmit antenna selection-maximal ratio combining (TAS-MRC), and maximal ratio transmission-maximal ratio combining (MRT-MRC). The main contributions of this work can be summarized as follows.

- The SOP and COP performance of the energy harvesting multi-antenna untrusted relay network under PSR are studied. The paper further researches on the correlation between SOP and COP using the metric of effective secrecy throughput (EST). The SOP, COP and EST expressions of closed form are orderly derived for the proposed schemes, which provide deep insights into the effect of the system performance. In addition, the signal-to-noise ratio (SNR), the antennas number at the source and other parameters were also researched.
- When the transmit SNR goes to infinity, a comprehensive study on the asymptotic analysis of the EST was conducted to elicit the optimal energy harvesting strategy for the network. The deduced expressions and simulation results illustrate that, for the four schemes, the EST approaches to a constant at high transmit SNR. The EST of the TAS-MRC scheme is superior to the three other schemes. In addition, the effect of the power allocation coefficient, the power splitting ratio factor and the number of antennas were researched on the EST.

The remainder of the paper is organized as follows. Section 2 introduces the system model and describes TAS-RAS scheme, MRT-RAS scheme, TAS-MRC scheme and MRT-MRC scheme, respectively. Section 3 presents the SOP, COP and EST expressions of the four schemes. Besides, the asymptotic expressions of the EST at high transmit SNR are investigated. Then, simulation analyses are discussed in Section 4. Finally, Section 5 summarizes the whole paper.

2. System Model

Consider a SWIPT untrusted relay MIMO system as shown in Figure 1, which consists of a source S and a destination D , equipped with N_s and N_d antennas, respectively. An untrusted energy harvesting relay R is equipped with a single antenna. It is assumed that the perfect CSI of all channels are available [51]. Each node operates in half-duplex mode and the AF protocol is adopted. $\mathbf{h}_{SR}$ denotes the $N_s \times 1$ channels vector between S and R links, and the $\mathbf{h}_{RD}$ stands for the $1 \times N_d$ channels vector between R and D links. h_{SR}^* and h_{RD}^* denote channel coefficients between the source and the relay, between the relay and the destination, respectively. $|h_{SR}^*|^2$ and $|h_{RD}^*|^2$ represent the maximal channel gain selected from the multiple antennas, i.e., $|h_{SR}^*|^2 = \arg \max_{1 \leq s \leq N_s} |h_{SR}^s|^2$ and $|h_{RD}^*|^2 = \arg \max_{1 \leq d \leq N_d} |h_{RD}^d|^2$. Then, $|h_{SR}^*|^2$ and $|h_{RD}^*|^2$ follow exponential distribution with means $\bar{\gamma}_{SR}$ and $\bar{\gamma}_{RD}$, respectively. It is assumed that each channel is independent and identically distributed (i.i.d.) and undergoes Rayleigh fading. In addition, the channels between the relay and destination are reciprocal, i.e., $h_{RD}^* = h_{DR}^*$ [15,16]. For simplicity, all noises are additive white Gaussian noise (AWGN) with zero mean and variance N_0 .

Figure 1. System model.

For the PSR, the entire communication is divided into two phases. In the first phase, the source transmits the confidential information to the untrusted relay. To enhance PLS, the destination simultaneously sends the jamming signal to prevent the untrusted relay from eavesdropping the confidential information. The relay harvests energy from the information sent by the source and the jamming signal transmitted by the destination. In the second phase, the relay employs the harvested energy to forward the confidential information. The jamming signal can be eliminated via the self-interference cancellation techniques [52]. It is assumed that the harvested energy at R is divided into two proportions. The ω denotes the allocation coefficient of the harvested energy, $\omega \in (0, 1)$. The ω proportion of the harvested energy is utilized for forwarding the confidential information to D and the other proportion is used for eavesdropping and decoding consumption.

Based on different proceed strategy at S and D , the transmission and reception of four schemes in the above system are considered.

2.1. TAS-RAS Scheme

For the TAS-RAS scheme, during the first phase, S selects only a single transmit antenna from N_s antennas to send the confidential signal with power βP , where P represents the total transmitted power of the S and D , and β denotes the power allocation coefficient between S and D , where $0 < \beta \leq 1$. Concurrently, D selects a single transmit antenna from N_d antennas to transmit the jamming signal with allocated power $(1 - \beta)P$. The signal power received by R is split into two parts. The ρ portion of the received power is used for harvesting energy, while the rest power is applied for transmitting

information to D , where $0 < \rho < 1$. Hence, the received instantaneous signal-to-interference-plus-noise rate (SINR) at R can be written as

$$\gamma_R^{TAS-RAS} = \frac{(1-\rho)\beta\lambda|h_{SR}^*|^2}{(1-\rho)(1-\beta)\lambda|h_{RD}^*|^2 + 1}, \quad (1)$$

where $\lambda = P/N_0$ denotes the transmit SNR.

From Equation (1), the transmit power at R , $P_R^{TAS-RAS}$, is given by

$$P_R^{TAS-RAS} = \omega\eta\rho \left(\beta P|h_{SR}^*|^2 + (1-\beta)P|h_{RD}^*|^2 \right), \quad (2)$$

where η denotes the energy conversion efficiency factor of the harvested energy, $0 < \eta < 1$, and ω denotes the allocation coefficient of the harvested energy; the ω proportion of the harvested energy is utilized for forwarding the confidential information to D .

In the second phase, R forwards the information to D with the power normalization coefficient $1/\sqrt{\beta P|h_{SR}^*|^2 + (1-\beta)P|h_{RD}^*|^2 + N_0}$. Therefore, the received instantaneous SINR of D can be calculated as

$$\gamma_D^{TAS-RAS} = \frac{\omega\eta\rho(1-\rho)\beta\lambda^2|h_{SR}^*|^2|h_{RD}^*|^2 \left(\beta|h_{SR}^*|^2 + (1-\beta)|h_{RD}^*|^2 \right)}{\lambda \left(\omega\eta\rho|h_{RD}^*|^2 + 1 - \rho \right) \left(\beta|h_{SR}^*|^2 + (1-\beta)|h_{RD}^*|^2 \right) + 1}. \quad (3)$$

2.2. MRT-RAS Scheme

For the MRT-RAS scheme, S firstly transmits the confidential information to R with N_s antennas to maximize SNR of the relay. At the same time, D selects a single transmit antenna from N_d antennas to transmit the jamming signal. Thus, the received instantaneous SINR of R can be written as

$$\gamma_R^{MRT-RAS} = \frac{(1-\rho)\beta\lambda\|\mathbf{h}_{SR}\|^2}{(1-\rho)(1-\beta)\lambda|h_{RD}^*|^2 + 1}, \quad (4)$$

where $\|\bullet\|^2$ denotes the Frobenius norm.

The transmit power at R is denoted by $P_R^{MRT-RAS}$, which is calculated as

$$P_R^{MRT-RAS} = \omega\eta\rho \left(\beta P\|\mathbf{h}_{SR}\|^2 + (1-\beta)P|h_{RD}^*|^2 \right). \quad (5)$$

The R forwards the information to D with the power constraint factor $1/\sqrt{\beta P\|\mathbf{h}_{SR}\|^2 + (1-\beta)P|h_{RD}^*|^2 + N_0}$. Thus, the received instantaneous SINR of D can be written as

$$\gamma_D^{MRT-RAS} = \frac{\omega\eta\rho(1-\rho)\beta\lambda^2\|\mathbf{h}_{SR}\|^2|h_{RD}^*|^2 \left(\beta\|\mathbf{h}_{SR}\|^2 + (1-\beta)|h_{RD}^*|^2 \right)}{\lambda \left(\omega\eta\rho|h_{RD}^*|^2 + 1 - \rho \right) \left(\beta\|\mathbf{h}_{SR}\|^2 + (1-\beta)|h_{RD}^*|^2 \right) + 1}. \quad (6)$$

2.3. TAS-MRC Scheme

In the TAS-MRC scheme, in the first phase, S transmits the information to R with only a single antenna. Meanwhile, D sends the jamming signal to R with N_d antennas. Hence, the received instantaneous SINR of R is given by

$$\gamma_R^{TAS-MRC} = \frac{(1-\rho)\beta\lambda|h_{SR}^*|^2}{(1-\rho)(1-\beta)\lambda\|\mathbf{h}_{RD}\|^2 + 1}. \quad (7)$$

The transmit power at R is denoted by $P_R^{TAS-MRC}$, which is written as

$$P_R^{TAS-MRC} = \omega\eta\rho \left(\beta P |h_{SR}^*|^2 + (1 - \beta) P \|\mathbf{h}_{RD}\|^2 \right). \quad (8)$$

During the second phase, R forwards the received information with the power normalization coefficient $1/\sqrt{\beta P |h_{SR}^*|^2 + (1 - \beta) P \|\mathbf{h}_{RD}\|^2 + N_0}$, and D adopts MRC technique to receive the information. Hence, the received instantaneous SINR of D can be calculated as

$$\gamma_D^{TAS-MRC} = \frac{\omega\eta\rho(1 - \rho)\beta\lambda^2 |h_{SR}^*|^2 \|\mathbf{h}_{RD}\|^2 \left(\beta |h_{SR}^*|^2 + (1 - \beta) \|\mathbf{h}_{RD}\|^2 \right)}{\lambda \left(\omega\eta\rho \|\mathbf{h}_{RD}\|^2 + 1 - \rho \right) \left(\beta |h_{SR}^*|^2 + (1 - \beta) \|\mathbf{h}_{RD}\|^2 \right) + 1}. \quad (9)$$

2.4. MRT-MRC Scheme

For the MRT-MRC scheme, R firstly receives the information from S with N_s antennas and the jamming signal from D with N_d antennas, respectively. Hence, the received SINR of R can be given by

$$\gamma_R^{MRT-MRC} = \frac{(1 - \rho)\beta\lambda \|\mathbf{h}_{SR}\|^2}{(1 - \rho)(1 - \beta)\lambda \|\mathbf{h}_{RD}\|^2 + 1}. \quad (10)$$

The transmit power of R is denoted by $P_R^{MRT-MRC}$, which can be expressed as

$$P_R^{MRT-MRC} = \omega\eta\rho \left(\beta P \|\mathbf{h}_{SR}\|^2 + (1 - \beta) P \|\mathbf{h}_{RD}\|^2 \right). \quad (11)$$

In the second phase, R forwards the information with the power constraint factor $1/\sqrt{\beta P \|\mathbf{h}_{SR}\|^2 + (1 - \beta) P \|\mathbf{h}_{RD}\|^2 + N_0}$, and D applies MRC technique to receive the information. Therefore, the received SINR of D can be calculated as

$$\gamma_D^{MRT-MRC} = \frac{\omega\eta\rho(1 - \rho)\beta\lambda^2 \|\mathbf{h}_{SR}\|^2 \|\mathbf{h}_{RD}\|^2 \left(\beta \|\mathbf{h}_{SR}\|^2 + (1 - \beta) \|\mathbf{h}_{RD}\|^2 \right)}{\lambda \left(\omega\eta\rho \|\mathbf{h}_{RD}\|^2 + 1 - \rho \right) \left(\beta \|\mathbf{h}_{SR}\|^2 + (1 - \beta) \|\mathbf{h}_{RD}\|^2 \right) + 1}. \quad (12)$$

3. Performance Analysis

In this work, the wiretap codes for confidential information are assumed the fixed-rate Wyner coded strategy. R_s is the confidential information rate and R_0 is the codeword transmission rate. To protect the information from eavesdropping, the redundancy rate should be positive, denoted by $R_e = R_0 - R_s$. On the contrary, when the channel capacity of the untrusted relay R is higher than redundancy rate, the information is unsafe, which is the definition of SOP. The SOP can be formulated as follows [53].

$$P_{SOP}^i = \Pr \left[I_R^i > R_e \right], \quad (13)$$

where $I_R^i = \frac{1}{2} \log_2 (1 + \gamma_R^i)$ and i is TAS-RAS scheme, MRT-RAS scheme, TAS-MRC scheme or MRT-MRC scheme. The coefficient $1/2$ is due to two phases.

If the channel capacity of D is lower than R_0 , D is unable to decode the information correctly, and this is the definition of COP. The COP can be formulated as follows [53].

$$P_{COP}^i = \Pr \left[I_D^i < R_0 \right], \quad (14)$$

where $I_D^i = \frac{1}{2} \log_2 (1 + \gamma_D^i)$.

SOP and COP can be used to measure the security and reliability performance, respectively. Furthermore, to comprehensively characterize the security and reliability performance, the EST is proposed in [40]. The EST is defined as the product of the secrecy rate and the probability of a successful transmission, which is given by

$$\zeta^i = R_s \Pr \left[I_R^i < R_e, I_D^i > R_0 \right]. \quad (15)$$

Next, we derive the exactly equations of the SOP, COP and EST of the aforementioned four transmission and reception schemes.

3.1. TAS-RAS Scheme

For the TAS-RAS scheme, let $X_1 = |h_{SR}^*|^2$ and $Y_1 = |h_{RD}^*|^2$. Substituting Equation (1) into Equation (13), the SOP can be calculated as

$$\begin{aligned} P_{sop}^{TAS-RAS} &= \Pr \left[I_R^{TAS-RAS} > R_e \right] \\ &= \Pr \left[\frac{1}{2} \log_2 \left(1 + \frac{(1-\rho)\beta\lambda|h_{SR}^*|^2}{(1-\rho)(1-\beta)\lambda|h_{RD}^*|^2 + 1} \right) > R_e \right] \\ &= \int_0^\infty \int_{X_{1b}}^\infty f_{X_1}(x_1) f_{Y_1}(y_1) dx_1 dy_1, \end{aligned} \quad (16)$$

where $X_{1b} = \frac{(1-\beta)t_1 Y_1}{\beta} + \frac{t_1}{(1-\rho)\beta\lambda}$ and $t_1 = 2^{2(R_0-R_s)} - 1$.

Firstly, the preliminary of the following lemma is present.

Lemma 1. The cumulative distribution function (CDF) of X_1 is given by

$$F_{X_1}(x_1) = \left(1 - e^{-\frac{x_1}{\gamma_{SR}}} \right)^{N_s}. \quad (17)$$

Proof. By taking the derivation operation of X_1 , the probability density function (PDF) of X_1 is calculated as

$$f_{X_1}(x_1) = \frac{N_s}{\gamma_{SR}} e^{-\frac{x_1}{\gamma_{SR}}} \left(1 - e^{-\frac{x_1}{\gamma_{SR}}} \right)^{N_s-1}. \quad (18)$$

□

Similarly, the PDF of Y_1 is calculated as follows.

$$f_{Y_1}(y_1) = \frac{N_d}{\gamma_{RD}} e^{-\frac{y_1}{\gamma_{RD}}} \left(1 - e^{-\frac{y_1}{\gamma_{RD}}} \right)^{N_d-1}. \quad (19)$$

Substituting Equations (18) and (19) into Equation (16), the SOP can be calculated as

$$P_{sop}^{TAS-RAS} = \frac{N_s N_d}{\gamma_{SR} \gamma_{RD}} \int_0^\infty \int_{X_{1b}}^\infty e^{-\left(\frac{x_1}{\gamma_{SR}} + \frac{y_1}{\gamma_{RD}}\right)} \left(1 - e^{-\frac{x_1}{\gamma_{SR}}} \right)^{N_s-1} \left(1 - e^{-\frac{y_1}{\gamma_{RD}}} \right)^{N_d-1} dx_1 dy_1. \quad (20)$$

After some manipulations, the SOP expression of the TAS-RAS scheme can be rewritten as

$$P_{sop}^{TAS-RAS} = 1 - \sum_{n_s=0}^{N_s} \sum_{n_d=0}^{N_d-1} \binom{N_s}{n_s} \binom{N_d-1}{n_d} \frac{(-1)^{n_s+n_d} N_d \beta \gamma_{SR} e^{-\frac{t_1 n_s}{(1-\rho)\beta\lambda\gamma_{SR}}}}{(1-\beta)t_1 n_s \gamma_{RD} + (n_d + 1)\beta\gamma_{SR}}. \quad (21)$$

From Equation (21), the SOP of the TAS-RAS scheme is closely related to β and ρ . In particular, the SOP is improved when β increases from 0 to 1. This is because the allocated power for transmitting information increases when gradually increasing β , which in turn leads to the descent of transmit power for the jamming signal. Besides, the security of the system improves when ρ continuously increases. The reason is that R extracts less information from the source signal when the portion of harvested energy increases.

Substituting Equation (3) into Equation (14), the COP of the TAS-RAS scheme is given by

$$\begin{aligned} P_{cop}^{TAS-RAS} &= \Pr \left[I_D^{TAS-RAS} < R_0 \right] \\ &\approx \Pr \left[\frac{\omega\eta\rho(1-\rho)\beta\lambda|h_{SR}^*|^2|h_{RD}^*|^2}{\omega\eta\rho|h_{RD}^*|^2+1-\rho} < t_2 \right] \\ &= \int_0^\infty \int_0^{X_{1s}} f_{X_1}(x_1) f_{Y_1}(y_1) dx_1 dy_1, \end{aligned} \quad (22)$$

where $X_{1s} = \frac{t_2}{(1-\rho)\beta\lambda} + \frac{t_2}{\omega\eta\rho\beta\lambda Y_1}$, $t_2 = 2^{2R_0} - 1$.

The approximation follows the fact that when λ is sufficiently high compared with the transmit power and channel gains, the sum item of the denominator in Equation (3) can be negligible and the denominator can be approximated as $\lambda \left(\omega\eta\rho|h_{RD}^*|^2 + 1 - \rho \right) \left(\beta|h_{SR}^*|^2 + (1-\beta)|h_{RD}^*|^2 \right)$ [15,31,54].

Substituting Equations (18) and (19) into Equation (22), the COP of the TAS-RAS scheme can be rewritten as

$$P_{cop}^{TAS-RAS} = \frac{N_d}{\tilde{\gamma}_{RD}} \sum_{n_s=0}^{N_s} \sum_{n_d=0}^{N_d-1} \binom{N_s}{n_s} \binom{N_d-1}{n_d} (-1)^{n_s+n_d} e^{-\frac{n_s t_2}{(1-\rho)\beta\lambda\tilde{\gamma}_{SR}}} \int_0^\infty e^{-\left(\frac{n_s t_2}{\omega\eta\rho\beta\lambda\tilde{\gamma}_{SR}y_1} + \frac{(n_d+1)y_1}{\tilde{\gamma}_{RD}}\right)} dy_1. \quad (23)$$

Applying Equation (3.324.1) in [55], the COP can be given by

$$P_{cop}^{TAS-RAS} = \sum_{n_s=0}^{N_s} \sum_{n_d=0}^{N_d-1} \binom{N_s}{n_s} \binom{N_d-1}{n_d} (-1)^{n_s+n_d} e^{-\frac{n_s t_2}{(1-\rho)\beta\lambda\tilde{\gamma}_{SR}}} \sqrt{\frac{4n_s t_2 N_d^2}{\omega\eta\rho\beta\lambda\tilde{\gamma}_{SR}\tilde{\gamma}_{RD}(n_d+1)}} K_1 \left(\sqrt{\frac{4n_s t_2 (n_d+1)}{\omega\eta\rho\beta\lambda\tilde{\gamma}_{SR}\tilde{\gamma}_{RD}}} \right), \quad (24)$$

where $K_1(\bullet)$ is the second kind of Modified Bessel function.

Equation (24) shows the COP decreases with continuously increasing β . The probability of decoding the confidential information improves when the allocated power of S increases.

Based on the expressions of SOP and COP, it can be noted that increasing λ improves the reliability of the system. Nevertheless, it also leads to increasing the risk of information leakage. Therefore, the EST is used for comprehensively measuring the reliability and security in untrusted energy harvesting networks. Based on Equation (15), the EST is given by

$$\begin{aligned} \zeta^{TAS-RAS} &= \frac{R_s}{2} \Pr \left[I_R^{TAS-RAS} < R_e, I_D^{TAS-RAS} > R_0 \right] \\ &\approx \frac{R_s}{2} \Pr \left[\frac{(1-\rho)\beta\lambda|h_{SR}^*|^2}{(1-\rho)(1-\beta)\lambda|h_{RD}^*|^2+1} < t_1, \frac{\omega\eta\rho(1-\rho)\beta\lambda|h_{SR}^*|^2|h_{RD}^*|^2}{\omega\eta\rho|h_{RD}^*|^2+1-\rho} > t_2 \right] \\ &= \frac{R_s}{2} \Pr [X_1 < X_{1b}, X_1 > X_{1s}]. \end{aligned} \quad (25)$$

Note that X_{1b} is larger than X_{1s} only when $Y_1 > u$, where $u = \left(b + \sqrt{b^2 + 4ac} \right) / 2a$, $a = \omega\eta\rho\lambda(1-\rho)(1-\beta)t_1$, $b = \omega\eta\rho(t_2 - t_1)$, $c = (1-\rho)t_2$.

Hence, $\zeta^{TAS-RAS}$ can be calculated as

$$\begin{aligned}\zeta^{TAS-RAS} &= \frac{R_s}{2} \int_u^\infty \int_{X_{1s}}^{X_{1b}} f_{X_1}(x_1) f_{Y_1}(y_1) dx_1 dy_1 \\ &= \frac{R_s N_d}{2 \tilde{\gamma}_{RD}} \left\{ \int_u^\infty e^{-\frac{y_1}{\tilde{\gamma}_{RD}}} \left(1 - e^{-\frac{y_1}{\tilde{\gamma}_{RD}}}\right)^{N_d-1} \left(\left(1 - e^{-\frac{X_{1b}}{\tilde{\gamma}_{SR}}}\right)^{N_s} - \left(1 - e^{-\frac{X_{1s}}{\tilde{\gamma}_{SR}}}\right)^{N_s} \right) dy_1 \right\}. \quad (26)\end{aligned}$$

Applying Equations (1.111) and (3.381.4) in [55], the EST expression is given by

$$\begin{aligned}\zeta^{TAS-RAS} &= \frac{R_s N_d}{2} \sum_{n_s=0}^{N_s} \sum_{n_d=0}^{N_d-1} \binom{N_s}{n_s} \binom{N_d-1}{n_d} (-1)^{n_s+n_d} \\ &\times \left\{ \frac{\beta \tilde{\gamma}_{SR} e^{-u_1}}{(1-\beta) t_1 n_s \tilde{\gamma}_{RD} + (n_d+1) \beta \tilde{\gamma}_{SR}} - \sum_{m=0}^{\infty} \frac{(-t_2 n_s (n_d+1))^m e^{-\frac{t_2 n_s}{(1-\rho)\beta\lambda\tilde{\gamma}_{SR}}} \Gamma\left(1-m, \frac{(n_d+1)u}{\tilde{\gamma}_{RD}}\right)}{(n_d+1) m! (\omega\eta\rho\beta\lambda\tilde{\gamma}_{SR}\tilde{\gamma}_{RD})^m} \right\}, \quad (27)\end{aligned}$$

where $u_1 = [(1-\beta)(1-\rho)\lambda t_1 n_s u \tilde{\gamma}_{RD} + \beta(1-\rho)(n_d+1)\lambda u \tilde{\gamma}_{SR} + t_1 n_s \tilde{\gamma}_{RD}] / [(1-\rho)\lambda\beta\tilde{\gamma}_{SR}\tilde{\gamma}_{RD}]$.

Based on Equations (21), (24) and (27), there are optimal values of β and ρ that maximize the EST, as shown in Figures 4 and 7, respectively.

When λ goes to infinity, the asymptotical performance of the EST is considered. According to Equation (25) and after some manipulations, the asymptotic approximation analysis of the EST in the TAS-RAS scheme can be derived as

$$\begin{aligned}\lim_{\lambda \rightarrow \infty} \zeta^{TAS-RAS} &= \lim_{\lambda \rightarrow \infty} \frac{R_s}{2} \Pr \left[X_1 < \frac{(1-\beta)t_1 y}{\beta} \right] \\ &= \frac{R_s N_d}{2} \sum_{n_s=0}^{N_s} \sum_{n_d=0}^{N_d-1} \binom{N_s}{n_s} \binom{N_d-1}{n_d} \frac{(-1)^{n_s+n_d} \beta \tilde{\gamma}_{SR}}{(1-\beta)t_1 n_s \tilde{\gamma}_{RD} + (n_d+1)\beta \tilde{\gamma}_{SR}}. \quad (28)\end{aligned}$$

Equation (28) shows that the EST of the TAS-RAS scheme is independent of the transmit SNR at high transmit SNR. Hence, the EST should be a constant when $\lambda \rightarrow \infty$.

3.2. MRT-RAS Scheme

In the MRT-RAS scheme, substituting Equation (4) into Equation (13), the SOP can be rewritten as

$$\begin{aligned}P_{sop}^{MRT-RAS} &= \Pr \left[I_R^{MRT-RAS} > R_e \right] \\ &= \Pr \left[\frac{1}{2} \log_2 \left(1 + \frac{(1-\rho)\beta\lambda \|\mathbf{h}_{SR}\|^2}{(1-\rho)(1-\beta)\lambda |h_{RD}^*|^2 + 1} \right) > R_e \right] \\ &= \int_0^\infty \int_{X_{1b}}^\infty f_{X_2}(x_2) f_{Y_1}(y_1) dx_2 dy_1, \quad (29)\end{aligned}$$

where $X_2 = \|\mathbf{h}_{SR}\|^2$, and the PDF of X_2 can be written as

$$f_{X_2}(x_2) = \frac{x_2^{N_s-1} e^{-\frac{x_2}{\tilde{\gamma}_{SR}}}}{\Gamma(N_s) \tilde{\gamma}_{SR}^{N_s}}. \quad (30)$$

Submitting Equations (19) and (30) into Equation (29), the SOP can be expressed as

$$P_{sop}^{MRT-RAS} = \frac{N_d}{\Gamma(N_s) \tilde{\gamma}_{SR}^{N_s} \tilde{\gamma}_{RD}} \int_0^\infty \int_{X_{1b}}^\infty x_2^{N_s-1} e^{-\left(\frac{x_2}{\tilde{\gamma}_{SR}} + \frac{y_1}{\tilde{\gamma}_{RD}}\right)} \left(1 - e^{-\frac{y_1}{\tilde{\gamma}_{RD}}}\right)^{N_d-1} dx_2 dy_1. \quad (31)$$

Hence, the SOP of the MRT-RAS scheme can be calculated as

$$P_{sop}^{MRT-RAS} = \sum_{n_s=0}^{N_s-1} \sum_{n_d=0}^{N_d-1} \sum_{k=0}^{n_s} \binom{N_d-1}{n_d} \binom{n_s}{k} \frac{(-1)^{n_d} N_d k! t_1^{n_s} ((1-\beta)\bar{\gamma}_{RD})^k e^{-\frac{t_1}{(1-\rho)\beta\lambda\bar{\gamma}_{SR}}}}{n_s! (\beta\bar{\gamma}_{SR})^{n_s-k-1} ((1-\rho)\lambda)^{n_s-k} u_2^{k+1}}. \quad (32)$$

where $u_2 = (1-\beta)t_1\bar{\gamma}_{RD} + (n_d+1)\beta\bar{\gamma}_{SR}$. The SOP of the MRT-RAS scheme is associated with parameters β and ρ . Moreover, the SOP increases when β increases, and it decreases as ρ increases.

Plugging Equation (6) into Equation (14), the COP of the MRT-RAS scheme is given by

$$\begin{aligned} P_{cop}^{MRT-RAS} &= \Pr \left[I_D^{MRT-RAS} < R_0 \right] \\ &\approx \Pr \left[\frac{\omega\eta\rho(1-\rho)\beta\lambda\|\mathbf{h}_{SR}\|^2 |h_{RD}^*|^2}{\omega\eta\rho|h_{RD}^*|^2 + 1 - \rho} < t_2 \right] \\ &= \int_0^\infty \int_0^{X_{1s}} f_{X_2}(x_2) f_{Y_1}(y_1) dx_2 dy_1. \end{aligned} \quad (33)$$

Substituting Equations (19) and (30) into Equation (33), the COP can be written as

$$P_{cop}^{MRT-RAS} = 1 - N_d \sum_{n_s=0}^{N_s-1} \sum_{n_d=0}^{N_d-1} \sum_{m=0}^{n_s} \binom{N_d-1}{n_d} \binom{n_s}{m} \frac{(-1)^{n_d} t_2^{n_s} e^{-\frac{t_2}{(1-\rho)\beta\lambda\bar{\gamma}_{SR}}} \int_0^\infty y_1^m e^{-\left(\frac{t_2}{\omega\eta\rho\beta\lambda\bar{\gamma}_{SR}y_1} + \frac{(n_d+1)y_1}{\bar{\gamma}_{RD}}\right)} dy_1}{\bar{\gamma}_{RD} n_s! (1-\rho)^{n_s-m} (\beta\lambda\bar{\gamma}_{SR})^{n_s} (\omega\eta\rho)^m}. \quad (34)$$

Utilizing Equation (3.471.9) in [55], the expression of COP is given by

$$P_{cop}^{MRT-RAS} = 1 - \frac{2N_d \sum_{n_s=0}^{N_s-1} \sum_{n_d=0}^{N_d-1} \sum_{m=0}^{n_s} \binom{N_d-1}{n_d} \binom{n_s}{m} (-1)^{n_d} t_2^{\frac{2n_s+1-m}{2}} e^{-\frac{t_2}{(1-\rho)\beta\lambda\bar{\gamma}_{SR}}} K_{1-m} \left(\sqrt{\frac{4t_2(n_d+1)}{\omega\eta\rho\beta\lambda\bar{\gamma}_{SR}\bar{\gamma}_{RD}}} \right)}{n_s! (1-\rho)^{n_s-m} (\beta\lambda\bar{\gamma}_{SR})^{\frac{2n_s+1-m}{2}} (\omega\eta\rho\bar{\gamma}_{RD})^{\frac{m+1}{2}} (n_d+1)^{\frac{1-m}{2}}}. \quad (35)$$

Equation (35) shows that the COP of the MRT-RAS scheme decreases with the increase of β . According to Equation (15), the closed-form EST expression is calculated as follows.

$$\begin{aligned} \zeta^{MRT-RAS} &= \frac{R_s}{2} \Pr \left[I_R^{MRT-RAS} < R_e, I_D^{MRT-RAS} > R_0 \right] \\ &\approx \frac{R_s}{2} \Pr \left[\frac{(1-\rho)\beta\lambda\|\mathbf{h}_{SR}\|^2}{(1-\rho)(1-\beta)\lambda|h_{RD}^*|^2 + 1} < t_1, \frac{\omega\eta\rho(1-\rho)\beta\lambda\|\mathbf{h}_{SR}\|^2 |h_{RD}^*|^2}{\omega\eta\rho\|\mathbf{h}_{RD}\|^2 + 1 - \rho} > t_2 \right] \\ &= \frac{R_s}{2} \int_u^\infty \int_{X_{1s}}^{X_{1b}} f_{X_2}(x_2) f_{Y_1}(y_1) dx_2 dy_1. \end{aligned} \quad (36)$$

Substituting Equations (19) and (30) into Equation (36), the EST can be rewritten as

$$\begin{aligned} \zeta^{MRT-RAS} &= \frac{R_s N_d}{2\bar{\gamma}_{RD}} \left\{ \int_u^\infty \sum_{n_s=0}^{N_s-1} \frac{1}{n_s!} \left(\frac{X_{1s}}{\bar{\gamma}_{SR}} \right)^{n_s} e^{-\left(\frac{X_{1s}}{\bar{\gamma}_{SR}} + \frac{y_1}{\bar{\gamma}_{RD}}\right)} \left(1 - e^{-\frac{y_1}{\bar{\gamma}_{RD}}} \right)^{N_d-1} dy_1 \right. \\ &\quad \left. - \int_u^\infty \sum_{n_s=0}^{N_s-1} \frac{1}{n_s!} \left(\frac{X_{1b}}{\bar{\gamma}_{SR}} \right)^{n_s} e^{-\left(\frac{X_{1b}}{\bar{\gamma}_{SR}} + \frac{y_1}{\bar{\gamma}_{RD}}\right)} \left(1 - e^{-\frac{y_1}{\bar{\gamma}_{RD}}} \right)^{N_d-1} dy_1 \right\} \\ &= \frac{R_s N_d}{2} \{ \Xi_1 - \Xi_2 \}. \end{aligned} \quad (37)$$

Applying Equation (3.381.3.8) in [55], Ξ_1 and Ξ_2 , respectively, are as follows.

$$\Xi_1 = \sum_{n_s=0}^{N_s-1} \sum_{n_d=0}^{N_d-1} \sum_{m=0}^{n_s} \sum_{k=0}^\infty \binom{N_d-1}{n_d} \binom{n_s}{m} \frac{(-1)^{n_d+k} t_2^{n_s+k} (n_d+1)^{m+k-1} e^{-\frac{t_2}{(1-\rho)\beta\lambda\bar{\gamma}_{SR}}} \Gamma\left(1-m-k, \frac{(n_d+1)u}{\bar{\gamma}_{RD}}\right)}{n_s! k! (1-\rho)^{n_s-m} (\beta\lambda\bar{\gamma}_{SR})^{n_s+k} (\omega\eta\rho\bar{\gamma}_{RD})^{m+k}}, \quad (38)$$

$$\Xi_2 = \sum_{n_s=0}^{N_s-1} \sum_{n_d=0}^{N_d-1} \sum_{m=0}^{n_s} \binom{N_d-1}{n_d} \binom{n_s}{m} \frac{(-1)^{n_d} t_1^{n_s} ((1-\beta)\bar{\gamma}_{RD})^m e^{-\frac{t_1}{(-\rho)\beta\lambda\bar{\gamma}_{SR}}} \Gamma\left(1+m, \frac{u_2 u}{\beta \bar{\gamma}_{SR} \bar{\gamma}_{RD}}\right)}{n_s! u_2^{m+1} ((1-\rho)\lambda)^{n_s-m} (\beta \bar{\gamma}_{SR})^{n_s-m-1}}. \quad (39)$$

The maximal EST with the optimal β and ρ is illustrated in Figures 4 and 7, respectively.

Based on Equations (37), (38) and (39), when λ goes to infinity, the asymptotical performance of the EST in the MRT-RAS scheme can be calculated as

$$\lim_{\lambda \rightarrow \infty} \zeta^{MRT-RAS} = \frac{R_s}{2} \left(1 - \sum_{n_s=0}^{N_s-1} \sum_{n_d=0}^{N_d-1} \binom{N_d-1}{n_d} \frac{(-1)^{n_d} N_d \beta \bar{\gamma}_{SR} ((1-\beta) t_1 \bar{\gamma}_{RD})^{n_s}}{((1-\beta) t_1 \bar{\gamma}_{RD} + (n_d+1) \beta \bar{\gamma}_{SR})^{n_s+1}} \right). \quad (40)$$

Equation (40) shows that the EST of the MRT-RAS scheme is irrelevant with the transmit SNR at high transmit SNR.

3.3. TAS-MRC Scheme

In TAS-MRC scheme, plugging Equation (7) into Equation (13), the SOP can be rewritten as

$$\begin{aligned} P_{sop}^{TAS-MRC} &= \Pr \left[I_R^{TAS-MRC} > R_e \right] \\ &= \Pr \left[\frac{1}{2} \log_2 \left(1 + \frac{(1-\rho)\beta\lambda |h_{SR}^*|^2}{(1-\rho)(1-\beta)\lambda \|\mathbf{h}_{RD}\|^2 + 1} \right) > R_e \right] \\ &= \int_0^\infty \int_{X_{2b}}^\infty f_{X_1}(x_1) f_{Y_2}(y_2) dx_1 dy_2, \end{aligned} \quad (41)$$

where $X_{2b} = \frac{(1-\beta)t_1 Y_2}{\beta} + \frac{t_1}{(1-\rho)\beta\lambda}$.

Let $Y_2 = \|\mathbf{h}_{RD}\|^2$, then the PDF of Y_2 is given by

$$f_{Y_2}(y_2) = \frac{y_2^{N_d-1} e^{-\frac{y_2}{\bar{\gamma}_{RD}}}}{\bar{\gamma}_{RD}^{N_d} \Gamma(N_d)}. \quad (42)$$

Substituting Equations (18) and (42) into Equation (41), the SOP can be calculated as

$$P_{sop}^{TAS-MRC} = 1 - \sum_{n_s=0}^{N_s} \binom{N_s}{n_s} \frac{(-1)^{n_s} e^{-\frac{t_1 n_s}{(1-\rho)\beta\lambda\bar{\gamma}_{SR}}} \int_0^\infty y_2^{N_d-1} e^{-\frac{(1-\beta)t_1 n_s \bar{\gamma}_{RD} + \beta \bar{\gamma}_{SR}}{\beta \bar{\gamma}_{SR} \bar{\gamma}_{RD}} y_2} dy_2}{\bar{\gamma}_{RD}^{N_d} \Gamma(N_d) ((1-\beta) t_1 n_s \bar{\gamma}_{RD} + \beta \bar{\gamma}_{SR})^{N_d}}. \quad (43)$$

Using Equation (3.35.3) in [55], the expression of SOP can be calculated as

$$P_{sop}^{TAS-MRC} = 1 - \sum_{n_s=0}^{N_s} \binom{N_s}{n_s} \frac{(-1)^{n_s} (\beta \bar{\gamma}_{SR})^{N_d} e^{-\frac{t_1 n_s}{(1-\rho)\beta\lambda\bar{\gamma}_{SR}}}}{((1-\beta) t_1 n_s \bar{\gamma}_{RD} + \beta \bar{\gamma}_{SR})^{N_d}}. \quad (44)$$

Combining Equations (9) and (14), the COP of the TAS-MRC scheme is written as

$$\begin{aligned} P_{cop}^{TAS-MRC} &= \Pr \left[I_D^{TAS-MRC} < R_0 \right] \\ &\approx \Pr \left[\frac{\omega \eta \rho (1-\rho) \beta \lambda |h_{SR}^*|^2 \|\mathbf{h}_{RD}\|^2}{\omega \eta \rho \|\mathbf{h}_{RD}\|^2 + 1 - \rho} < t_2 \right] \\ &= \int_0^\infty \int_0^{X_{2s}} f_{X_1}(x_1) f_{Y_2}(y_2) dx_1 dy_2, \end{aligned} \quad (45)$$

where $X_{2s} = \frac{t_2}{(1-\rho)\beta\lambda} + \frac{t_2}{\omega\eta\rho\beta\lambda Y_2}$.

Substituting Equations (18) and (42) into Equation (45) and utilizing Equation (3.471.9) in [55], the COP can be calculated as

$$P_{cop}^{TAS-MRC} = 1 + 2 \sum_{n_s=1}^{N_s} \binom{N_s}{n_s} \frac{(-1)^{n_s} (t_2 n_s)^{\frac{N_d}{2}} e^{-\frac{t_2 n_s}{(1-\rho)\beta\lambda\tilde{\gamma}_{SR}}} K_{N_d} \left(\sqrt{\frac{4t_2 n_s}{\omega\eta\rho\beta\lambda\tilde{\gamma}_{SR}\tilde{\gamma}_{RD}}} \right)}{\Gamma(N_d) (\omega\eta\rho\beta\lambda\tilde{\gamma}_{SR}\tilde{\gamma}_{RD})^{\frac{N_d}{2}}}. \quad (46)$$

To measure the trade-off between the SOP and COP, the EST can be written as

$$\begin{aligned} \zeta^{TAS-MRC} &= \frac{R_s}{2} \Pr \left[I_R^{TAS-MRC} < R_e, I_D^{TAS-MRC} > R_0 \right] \\ &\approx \frac{R_s}{2} \Pr \left[\frac{(1-\rho)\beta\lambda|h_{SR}^*|^2}{(1-\rho)(1-\beta)\lambda\|\mathbf{h}_{RD}\|^2 + 1} < t_1, \frac{\omega\eta\rho(1-\rho)\beta\lambda|h_{SR}^*|^2\|\mathbf{h}_{RD}\|^2}{\omega\eta\rho\|\mathbf{h}_{RD}\|^2 + 1 - \rho} > t_2 \right] \\ &= \frac{R_s}{2} \int_u^\infty \int_{X_{2s}}^{X_{2b}} f_{X_1}(x_1) f_{Y_2}(y_2) dx_1 dy_2. \end{aligned} \quad (47)$$

Substituting Equations (18) and (42) into Equation (47), using Equation (3.381.3.8) in [55], and after some manipulations, the EST can be calculated as

$$\begin{aligned} \zeta^{TAS-MRC} &= \frac{R_s}{2\tilde{\gamma}_{RD}^{N_d} \Gamma(N_d)} \int_u^\infty y_2^{N_d-1} e^{-\frac{y_2}{\tilde{\gamma}_{RD}}} \times \left(\left(1 - e^{-\frac{X_{2b}}{\tilde{\gamma}_{SR}}} \right)^{N_s} - \left(1 - e^{-\frac{X_{2s}}{\tilde{\gamma}_{SR}}} \right)^{N_s} \right) dy_2 \\ &= \frac{R_s}{2\Gamma(N_d)} \{ \Xi_3 - \Xi_4 \}, \end{aligned} \quad (48)$$

where Ξ_3 and Ξ_4 are as follows.

$$\Xi_3 = \sum_{n_s=0}^{N_s} \binom{N_s}{n_s} \frac{(-1)^{n_s} (\beta\tilde{\gamma}_{SR})^{N_d} e^{-\frac{t_1 n_s}{(1-\rho)\beta\lambda\tilde{\gamma}_{SR}}} \Gamma \left(N_d, \frac{(1-\beta)t_1 n_s u \tilde{\gamma}_{RD} + \beta u \tilde{\gamma}_{SR}}{\beta\tilde{\gamma}_{SR}\tilde{\gamma}_{RD}} \right)}{((1-\beta)t_1 n_s \tilde{\gamma}_{RD} + \beta\tilde{\gamma}_{SR})^{N_d}}, \quad (49)$$

$$\Xi_4 = \sum_{n_s=0}^{N_s} \sum_{k=0}^{\infty} \binom{N_s}{n_s} \frac{(-1)^{n_s+k} e^{-\frac{t_2 n_s}{(1-\rho)\beta\lambda\tilde{\gamma}_{SR}}} (t_2 n_s)^k \Gamma \left(N_d - k, \frac{u}{\tilde{\gamma}_{RD}} \right)}{k! (\omega\eta\rho\beta\lambda\tilde{\gamma}_{SR}\tilde{\gamma}_{RD})^k}. \quad (50)$$

Therefore, when $\lambda \rightarrow \infty$, the asymptotical performance of the EST in the TAS-MRC scheme can be calculated as

$$\lim_{\lambda \rightarrow \infty} \zeta^{TAS-MRC} = \frac{R_s}{2} \sum_{n_s=0}^{N_s} \binom{N_s}{n_s} \frac{(-1)^{n_s} (\beta\tilde{\gamma}_{SR})^{N_d}}{((1-\beta)t_1 n_s \tilde{\gamma}_{RD} + \beta\tilde{\gamma}_{SR})^{N_d}}. \quad (51)$$

Equation (51) indicates that the EST of the TAS-MRC scheme is a constant at high transmit SNR.

3.4. MRT-MRC Scheme

In the MRT-MRC scheme, combining Equations (10), (12), (13) and (14), the exact expressions of the SOP and COP can be obtained as Equations (52) and (53).

$$\begin{aligned}
P_{sop}^{MRT-MRC} &= \Pr \left[I_R^{MRT-MRC} > R_e \right] \\
&= \Pr \left[\frac{1}{2} \log_2 \left(1 + \frac{(1-\rho)\beta\lambda \|\mathbf{h}_{SR}\|^2}{(1-\rho)(1-\beta)\lambda \|\mathbf{h}_{RD}\|^2 + 1} \right) > R_e \right] \\
&= \sum_{n_s=0}^{N_s-1} \sum_{m=0}^{n_s} \binom{n_s}{m} \frac{(N_d+m-1)! t_1^{n_s} (\beta\tilde{\gamma}_{SR})^{N_d} ((1-\beta)\tilde{\gamma}_{RD})^m e^{-\frac{t_1}{(1-\rho)\beta\lambda\tilde{\gamma}_{SR}}}}{n_s! \Gamma(N_d) ((1-\rho)\lambda\beta\tilde{\gamma}_{SR})^{n_s-m} u_3^{N_d+m}}, \quad (52)
\end{aligned}$$

where $u_3 = (1-\beta)t_1\tilde{\gamma}_{RD} + \beta\tilde{\gamma}_{SR}$.

$$\begin{aligned}
P_{cop}^{MRT-MRC} &= \Pr \left[I_D^{MRT-MRC} < R_0 \right] \\
&\approx \Pr \left[\frac{\omega\eta\rho(1-\rho)\beta\lambda \|\mathbf{h}_{SR}\|^2 \|\mathbf{h}_{RD}\|^2}{\omega\eta\rho \|\mathbf{h}_{RD}\|^2 + 1 - \rho} < t_2 \right] \\
&= 1 - \frac{2}{\Gamma(N_d)} \sum_{n_s=1}^{N_s-1} \sum_{m=0}^{n_s} \binom{n_s}{m} \frac{(t_2)^{\frac{2n_s+N_d-m}{2}} e^{-\frac{t_2}{(1-\rho)\beta\lambda\tilde{\gamma}_{SR}}} K_{N_d-m} \left(\sqrt{\frac{4t_2}{\omega\eta\rho\beta\lambda\tilde{\gamma}_{SR}\tilde{\gamma}_{RD}}} \right)}{n_s! ((1-\rho)\beta\lambda\tilde{\gamma}_{SR})^{n_s-m} (\omega\eta\rho\beta\lambda\tilde{\gamma}_{SR}\tilde{\gamma}_{RD})^{\frac{N_d+m}{2}}}. \quad (53)
\end{aligned}$$

Equation (53) shows that the COP decreases when β increases. When much power is allocated for the source signal, the probability of successfully decoding the source information increases.

The EST of the MRT-MRC scheme is calculated as

$$\begin{aligned}
\zeta^{MRT-MRC} &= \frac{R_s}{2} \Pr \left[I_R^{MRT-MRC} < R_e, I_D^{MRT-MRC} > R_0 \right] \\
&\approx \frac{R_s}{2} \Pr \left[\frac{(1-\rho)\beta\lambda \|\mathbf{h}_{SR}\|^2}{(1-\rho)(1-\beta)\lambda \|\mathbf{h}_{RD}\|^2 + 1} < t_1, \frac{\omega\eta\rho(1-\rho)\beta\lambda \|\mathbf{h}_{SR}\|^2 \|\mathbf{h}_{RD}\|^2}{\omega\eta\rho \|\mathbf{h}_{RD}\|^2 + 1 - \rho} > t_2 \right] \\
&= \frac{R_s}{2\Gamma(N_d)} \{ \Xi_5 - \Xi_6 \}, \quad (54)
\end{aligned}$$

where Ξ_5 and Ξ_6 can be calculated as Equations (55) and (56), respectively.

$$\Xi_5 = \sum_{n_s=0}^{N_s-1} \sum_{m=0}^{n_s} \sum_{k=0}^{\infty} \binom{n_s}{m} \frac{(-1)^k t_2^{n_s+k} e^{-\frac{t_2}{(1-\rho)\beta\lambda\tilde{\gamma}_{SR}}} \Gamma(N_d - m - k, \frac{u}{\tilde{\gamma}_{RD}})}{n_s! k! ((1-\rho)\beta\lambda\tilde{\gamma}_{SR})^{n_s-m} (\omega\eta\rho\beta\lambda\tilde{\gamma}_{SR}\tilde{\gamma}_{RD})^{m+k}}, \quad (55)$$

$$\Xi_6 = \sum_{n_s=0}^{N_s-1} \sum_{m=0}^{n_s} \binom{n_s}{m} \frac{t_1^{n_s} (\beta\tilde{\gamma}_{SR})^{N_d} ((1-\beta)\tilde{\gamma}_{RD})^m e^{-\frac{t_1}{(1-\rho)\beta\lambda\tilde{\gamma}_{SR}}} \Gamma(N_d + m, \frac{u_3 u}{\beta\tilde{\gamma}_{SR}\tilde{\gamma}_{RD}})}{n_s! ((1-\rho)\beta\lambda\tilde{\gamma}_{SR})^{n_s-m} u_3^{N_d+m}}. \quad (56)$$

Based on Equations (54)–(56), when $\lambda \rightarrow \infty$, the asymptotical performance of the EST in the MRT-MRC scheme can be calculated as

$$\lim_{\lambda \rightarrow \infty} \zeta^{MRT-MRC} = \frac{R_s}{2} \left[1 - \sum_{n_s=0}^{N_s-1} \frac{(N_d + n_s + 1)! (\beta\tilde{\gamma}_{SR})^{N_d} ((1-\beta)t_1\tilde{\gamma}_{RD})^{n_s}}{n_s! (N_d + 1)! ((1-\beta)t_1\tilde{\gamma}_{RD} + \beta\tilde{\gamma}_{SR})^{N_d+n_s+1}} \right]. \quad (57)$$

Equation (57) denotes that the EST of the MRT-MRC scheme is irrelevant with λ when λ is sufficiently high.

4. Simulation and Discussion

The Monte Carlo simulation was utilized to verify the analytical expressions carried out in Section 4, and compare the performance of the four schemes. For each figure, $R_0 = 2$ bit/s/Hz,

$R_s = 1$ bit/s/Hz, $\eta = 0.5$, $\omega = 0.8$ and $\bar{\gamma}_{SR} = \bar{\gamma}_{RD} = 0$. The black solid lines represent the numerical analyses in all figures. The dashed-lines are the asymptotic analysis results.

Figure 2 illustrates the SOP and COP versus the transmit SNR under the four schemes, where β and ρ were set as 0.5. As shown in Figure 2, the derived analytical curves excellently match with simulation results, which validate our derivation. Several observations can be obtained as follows: (1) The SOP of the four schemes increases continuously with increasing the transmit SNR, whereas the COP decreases. This is because, as the transmit SNR increases, the received SNR at R and D are improved. Therefore, there is a trade-off between security and reliability. (2) The SOP of each scheme approaches saturation when the transmit SNR is sufficient high. The reason is that the utilization of jamming signal protects the confidential information. (3) Both the TAS-RAS scheme and TAS-MRC scheme are superior to MRT-RAS scheme and MRT-MRC in terms of security performance, while inferior to MRT-RAS scheme and MRT-MRC in terms of reliability performance. It denotes that the security performance of TAS scheme is superior to MRT, while the reliability performance of RAS scheme is worse than MRC.

Figure 2. SOP and COP vs. the transmit SNR.

Figure 3 depicts that the EST versus the transmit SNR under the four schemes. It can be easily observed that the analytical approximations are close to the exact simulation results for all schemes. It is shown that, when $\lambda \rightarrow \infty$, the EST approaches to a constant for each scheme, which verifies the asymptotical optimality property shown in Equations (28), (40), (51) and (57). Therefore, by applying excessive transmit power to improve the EST is meaningless. In the high transmit SNR regime, several observations can be drawn as follows: (1) The EST performance of TAS-MRC scheme outperforms MRT-MRC scheme, and TAS-RAS scheme outperforms MRT-RAS scheme. This is because that the source node may leak more confidential information to the untrusted relay when applying the MRT. (2) The saturation values of TAS-RAS and MRT-MRC are very close. However, TAS-RAS is less complicated than MRT-MRC. (3) The EST of TAS-MRC scheme is more advantageous than MRT-RAS scheme.

Figure 3. EST vs. the transmit SNR.

Figure 4 depicts the curves of the ESTs versus β for four schemes. It is shown that: (1) There is an optimal β value that maximizes the EST. When β is less than the optimal value, the EST increases, and when β is greater than the optimal value, the EST decreases. This is because, when β is small, the source allocated power is small, thus the reliable link cannot be established between S and D , which leads to small EST. While β is large, the security of the transmitted information cannot be guaranteed, which also degrades EST. (2) For a given β , the EST of MRT-MRC scheme outperforms MRT-RAS scheme, and TAS-MRC scheme outperforms TAS-RAS scheme. This is because utilizing the MRC technique can obtain superior reliability to RAS. (3) In terms of EST, MRT-MRC scheme outperforms TAS-MRC scheme when $\beta \in (0, 0.7)$, and then with continuously increasing β , MRT-MRC scheme is inferior to TAS-MRC scheme. Similarly, MRT-RAS scheme outperforms than TAS-RAS scheme when $\beta \in (0, 0.675)$. This is explained as, with increase of β , the allocated power for the source increases, and the reliability of the system would improve. However, the allocated power for the destination decreases, and this leads to worse security performance.

Figure 5 depicts the EST with the number of antennas N_s at the source node under four schemes. The figures show that: (1) The EST increases and then decreases when N_s is increasing, thus there is an optimal N_s that maximizes the EST. For MRT and TAS, the optimal N_s is 4 and 17, respectively. This can be explained as increasing N_s can improve the connection reliability. Therefore, the EST would increase firstly. However, the source node may leak more information to the untrusted relay with continuously increasing N_s , which degrades the security performance. (2) When the source antennas are more than 4, the EST of MRT-MRC scheme and MRT-RAS scheme decreases rapidly, whereas the EST of TAS-MRC scheme and TAS-RAS scheme declines slowly when the antenna number is higher than 17. This implies that MRT is more sensitive to the number of the source antennas compared with TAS.

Figure 4. EST vs. the power allocation factor β .

Figure 5. EST vs. the number of antenna N_s .

Figure 6 shows that the EST versus the number of antennas N_d . It is observed that: (1) The EST increases with the increase of N_d and then approaches a saturation value. This is because increase of N_d improves the security of the system. The growing trend would saturate because the power of the destination is constrained. (2) The EST of MRT-MRC scheme outperforms TAS-MRC scheme, and MRT-RAS scheme outperforms TAS-RAS scheme. The reason is that MRT outperforms TAS for the source node. (3) The EST of MRT-MRC scheme outperforms MRT-RAS scheme, and TAS-MRC scheme outperforms TAS-RAS scheme. The reason is that MRC is more advantageous than RAS for the destination node.

Figure 7 depicts the curves of the derived EST versus ρ for four schemes. It is observed that: (1) There is an optimal ρ that maximizes the EST. Smaller ρ implies the harvested energy at R is smaller, which leads to the lower EST. For a larger ρ , the harvested energy for information transmission is small, which also degrades the EST. (2) The EST of MRT-MRC scheme is superior to TAS-MRC scheme, and MRT-RAS scheme outperforms TAS-RAS scheme. The EST of MRT-MRC scheme is superior to

MRT-RAS scheme, and TAS-MRC scheme outperforms TAS-RAS scheme. The reason is as same as for the results shown in Figure 6. (3) The EST of TAS-MRC scheme is very close to MRT-RAS scheme.

Figure 6. EST vs. the number of antenna N_d .

Figure 7. EST vs. the power splitting ratio ρ .

Figure 8 shows the EST of the four schemes versus ω . Here, the ω proportion of the harvested energy is utilized for forwarding the confidential information to D and the other proportion is used for eavesdropping and decoding consumption. The results show that: (1) The EST is increasing according with the increase of ω . The reason is that, when ω increases, the allocated harvested energy at R for forwarding the confidential information to D is improved. As a result, the harvested energy for eavesdropping and decoding the information is reduced at R . Therefore, the security performance is promoted. (2) MRT-MRC scheme and MRT-RAS scheme are superior to TAS-MRC scheme and TAS-RAS scheme, respectively.

Figure 8. EST vs. the power splitting ratio ω .

5. Conclusions

This paper presents secure transmission for a half-duplex AF untrusted and energy harvesting relay network under the PSR strategy, where both S and D are multi-antennas and R is a single antenna. The expressions of SOP, COP and EST for the four schemes are successively derived. Moreover, the EST asymptotic analysis of each scheme is provided in the high transmits SNR regime. These expressions were verified by Monte-Carlo simulation. The effects of various key parameters on the EST, such as λ , β , ρ , N_s and N_d , were taken into account. In general, the EST of MRT-MRC scheme was superior to the other schemes in terms of the parameters β , N_d , ρ , and ω . However, the EST of MRT-MRC scheme was inferior to TAS-MRC scheme in the high transmit SNR regime. There existed an optimal N_s to maximize the EST of the proposed schemes, i.e., 4 or 17 antennas.

Author Contributions: H.S., W.Y., and D.C. conceived the main proposal of the secure transmission schemes. H.S. carried out formal analysis. W.Y. and D.C. provided methodology. H.S. and D.C. designed software. H.S. and W.Y. wrote the original draft. Y.L. and Y.C. supervised the analysis and numerical simulation of the proposed schemes, and reviewed and edited the manuscript.

Funding: This work was supported in part by the National Natural Science Foundation of China under Grant Nos. 61771487, 61471393, and 61501512, in part by the Jiangsu Provincial National Science Foundation under Grant No. BK20150718.

Acknowledgments: The authors extend their gratitude to the anonymous reviewers for their valuable and constructive comments, which have largely improved and clarified this paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

- Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *53*, 1355–1387. [\[CrossRef\]](#)
- Yang, N.; Wang, L.; Geraci, G.; Elkashlan, M. Safeguarding 5G wireless communication networks using physical layer security. *IEEE Commun. Mag.* **2015**, *53*, 20–27. [\[CrossRef\]](#)
- Liu, T.; Shamai, S. A Note on the Secrecy Capacity of the Multi-antenna Wiretap Channel. *IEEE Trans. Inf. Theory* **2009**, *55*, 2547–2553. [\[CrossRef\]](#)
- Hasna, M.O.; Alouini, M.S. End-to-end performance of transmission systems with relays over Rayleigh-fading channels. *IEEE Trans. Wirel. Commun.* **2003**, *2*, 1126–1131. [\[CrossRef\]](#)
- Anghel, P.A.; Kaveh, M. Exact Symbol Error Probability of a Cooperative Network in a Rayleigh-Fading Environment. *IEEE Trans. Wirel. Commun.* **2004**, *3*, 1416–1421. [\[CrossRef\]](#)
- Shim, K.; Do, N.; An, B. Performance Analysis of Physical Layer Security of Opportunistic Scheduling in Multiuser Multirelay Cooperative Networks. *Sensors* **2017**, *17*, 377. [\[CrossRef\]](#)

7. Liao, Q.Y.; Leow, C.Y.; Ding, Z. Physical Layer Security Using Two-Path Successive Relaying. *Sensors* **2016**, *16*, 846. [\[CrossRef\]](#)
8. Kuhestani, A.; Mohammadi, A. Destination-based cooperative jamming in untrusted amplify-and-forward relay networks: Resource allocation and performance study. *IET Commun.* **2016**, *10*, 17–23. [\[CrossRef\]](#)
9. Kuhestani, A.; Yeoh, P.L.; Mohammadi, A. Optimal Power Allocation and Secrecy Sum Rate in Two-Way Untrusted Relaying. In Proceedings of the 2017 IEEE Global Communications Conference GLOBECOM, Singapore, 4–8 December 2017; pp. 1–6. [\[CrossRef\]](#)
10. Kuhestani, A.; Mohammadi, A.; Mohammadi, M. Joint Relay Selection and Power Allocation in Large-Scale MIMO Systems with Untrusted Relays and Passive Eavesdroppers. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 341–355. [\[CrossRef\]](#)
11. Mekki, T.; Yao, R.; Xu, F.; Wang, L. Optimal power allocation for achievable secrecy rate in an untrusted relay network with bounded channel estimation error. In Proceedings of the 26th Wireless and Optical Communication Conference (WOCC), Newark, NJ, USA, 7–8 April 2017; pp. 1–5. [\[CrossRef\]](#)
12. Kuhestani, A.; Mohammadi, A.; Noori, M. Optimal power allocation to improve secrecy performance of non-regenerative cooperative systems using an untrusted relay. *IET Commun.* **2016**, *10*, 962–968. [\[CrossRef\]](#)
13. Atapattu, S.; Rajatheva, N.; Tellambura, C. Performance Analysis of TDMA Relay Protocols Over Nakagami- m Fading. *IEEE Trans. Veh. Technol.* **2010**, *59*, 93–104. [\[CrossRef\]](#)
14. Zhong, C.; Jin, S.; Wong, K.K. Dual-hop systems with noisy relay and interference-limited destination. *IEEE Trans. Commun.* **2010**, *58*, 764–768. [\[CrossRef\]](#)
15. Kalamkar, S.S.; Banerjee, A. Secure Communication via a Wireless Energy Harvesting Untrusted Relay. *IEEE Trans. Veh. Technol.* **2017**, *66*, 2199–2213. [\[CrossRef\]](#)
16. Huang, J.; Mukherjee, A.; Swindlehurst, A. Secure Communication Via an Untrusted Non-Regenerative Relay in Fading Channels. *IEEE Trans. Signal Process.* **2013**, *61*, 2536–2550. [\[CrossRef\]](#)
17. Liu, Y.; Li, L.; Alexandropoulos, G.C.; Pesavento, M. Securing Relay Networks with Artificial Noise: An Error Performance-Based Approach. *Entropy* **2017**, *19*, 384. [\[CrossRef\]](#)
18. Zhu, J.; Mo, J.; Tao, M. Cooperative Secret Communication with Artificial Noise in Symmetric Interference Channel. *IEEE Commun. Lett.* **2010**, *14*, 885–887. [\[CrossRef\]](#)
19. Hu, H.; Gao, Z.; Liao, X.; Leung, V.C.M. Secure Communications in CIoT Networks with a Wireless Energy Harvesting Untrusted Relay. *Sensors* **2017**, *17*, 2023. [\[CrossRef\]](#) [\[PubMed\]](#)
20. Chen, S.; Wang, W.; Zhang, X. Capacity Performance of Amplify-and-Forward MIMO Relay with Transmit Antenna Selection and Maximal-Ratio Combining. In Proceedings of the IEEE Wireless Communications and Networking Conference (WCN), Budapest, Hungary, 5–8 April 2009; pp. 1–6. [\[CrossRef\]](#)
21. Jeong, C.; Kim, I.M.; Kim, D.I. Joint Secure Beamforming Design at the Source and the Relay for an Amplify-and-Forward MIMO Untrusted Relay System. *IEEE Trans. Signal Process.* **2012**, *60*, 310–325. [\[CrossRef\]](#)
22. Chen, X.; Chen, J.; Liu, T. Secure wireless information and power transfer in large-scale MIMO relaying systems with imperfect CSI. In Proceedings of the IEEE Global Communications Conference (GLOBECOM), Austin, TX, USA, 8–12 December 2014; pp. 4131–4136. [\[CrossRef\]](#)
23. Xiong, J.; Cheng, L.; Ma, D.; Wei, J. Destination Aided Cooperative Jamming for Dual-Hop Amplify-and-Forward MIMO Untrusted Relay Systems. *IEEE Trans. Veh. Technol.* **2016**, *65*, 7274–7284. [\[CrossRef\]](#)
24. Li, Q.; Yang, L. Artificial Noise Aided Secure Precoding for MIMO Untrusted Two-Way Relay Systems with Perfect and Imperfect Channel State Information. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2628–2638. [\[CrossRef\]](#)
25. Benkhelifa, F.; Member, I.S.; Fellow, I.; Alouini, M.S. Precoding Design of MIMO Amplify-and-Forward Communication System with an Energy Harvesting Relay and Possibly Imperfect CSI. *IEEE Access* **2017**, *5*, 578–594. [\[CrossRef\]](#)
26. Rostampoor, J.; Razavizadeh, S.M.; Lee, I. Energy Efficiency Maximization Precoding Design for SWIPT in MIMO Two-Way Relay Networks. *IEEE Trans. Veh. Technol.* **2017**, *66*, 7888–7896. [\[CrossRef\]](#)
27. Seah, W.K.G.; Zhi, A.E.; Tan, H. Wireless sensor networks powered by ambient energy harvesting (WSN-HEAP)—Survey and challenges. In Proceedings of 2009 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology, Aalborg, Denmark, 17–20 May 2009; pp. 1–5. [\[CrossRef\]](#)

28. Paradiso, J.A.; Starner, T. Energy Scavenging for Mobile and Wireless Electronics. *IEEE Pervasive Comput.* **2005**, *4*, 18–27. [[CrossRef](#)]
29. Visser, H.J.; Vullers, R.J.M. RF Energy Harvesting and Transport for Wireless Sensor Network Applications: Principles and Requirements. *Proc. IEEE* **2013**, *101*, 1410–1423. [[CrossRef](#)]
30. Lu, X.; Wang, P.; Niyato, D. Wireless Networks with RF Energy Harvesting: A Contemporary Survey. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 757–789. [[CrossRef](#)]
31. Nasir, A.A.; Zhou, X.; Durrani, S. Relaying Protocols for Wireless Energy Harvesting and Information Processing. *IEEE Trans. Wirel. Commun.* **2013**, *12*, 3622–3636. [[CrossRef](#)]
32. Kalamkar, S.S.; Banerjee, A. Interference-Assisted Wireless Energy Harvesting in Cognitive Relay Network with Multiple Primary Transceivers. In Proceedings of 2015 IEEE Global Communications Conference (GLOBECOM), San Diego, CA, USA, 6–10 December 2015; pp. 1–6. [[CrossRef](#)]
33. Chen, H.; Li, Y.; Jiang, Y. Distributed Power Splitting for SWIPT in Relay Interference Channels Using Game Theory. *IEEE Trans. Wirel. Commun.* **2014**, *14*, 410–420. [[CrossRef](#)]
34. Nasir, A.A.; Zhou, X.; Durrani, S.; Kennedy, R.A. Wireless-Powered Relays in Cooperative Communications: Time-Switching Relaying Protocols and Throughput Analysis. *IEEE Trans. Commun.* **2015**, *63*, 1607–1622. [[CrossRef](#)]
35. Yang, Z.; Ding, Z.; Fan, P. Outage Performance of Cognitive Relay Networks With Wireless Information and Power Transfer. *IEEE Trans. Veh. Technol.* **2016**, *65*, 3828–3833. [[CrossRef](#)]
36. Zhang, R.; Ho, C.K. MIMO Broadcasting for Simultaneous Wireless Information and Power Transfer. *IEEE Trans. Wirel. Commun.* **2013**, *12*, 1989–2001. [[CrossRef](#)]
37. Zhou, X.; Zhang, R.; Ho, C.K. Wireless Information and Power Transfer: Architecture Design and Rate-Energy Tradeoff. *IEEE Trans. Commun.* **2013**, *61*, 4754–4767. [[CrossRef](#)]
38. Tran, D.D.; H.V.; Ha, D.B. Performance Analysis of Two-Way Relaying System with RF-EH and Multiple Antennas. In Proceedings of the IEEE 84th Vehicular Technology Conference (VTC-Fall), Montreal, QC, Canada, 18–21 September 2016. [[CrossRef](#)]
39. Bin, L.; Haiyan, G.; Zhen, Y.; Guan, G. Throughput Maximization for Hybrid Backscatter Assisted Cognitive Wireless Powered Radio Networks. *IEEE IoT.* **2018**, *5*, 2015–2024. [[CrossRef](#)]
40. Wang, L.; Cai, Y.; Zou, Y. Joint Relay and Jammer Selection Improves the Physical Layer Security in the Face of CSI Feedback Delays. *IEEE Trans. Veh. Technol.* **2016**, *65*, 6259–6274. [[CrossRef](#)]
41. Alexandropoulos, G.C.; Peppas, K.P. Secrecy Outage Analysis over Correlated Composite Nakagami- m /Gamma Fading Channels. *IEEE Commun. Lett.* **2018**, *22*, 77–80. [[CrossRef](#)]
42. Cheng, Y.; Nguyen, N.P.; Garcia-Palacios, E.; Xuan, N.T.; Le-Tien, T. Secure Energy Harvesting Communications with Relay Selection over Nakagami- m Fading Channels. *Mob. Netw. Appl.* **2017**, *23*, 1–8. [[CrossRef](#)]
43. Mishra, D.; Alexandropoulos, G.C. Transmit Precoding and Receive Power Splitting for Harvested Power Maximization in MIMO SWIPT Systems. *IEEE Trans. Green Commun. Netw.* **2018**, *2*, 774–786. [[CrossRef](#)]
44. Mishra, D.; Alexandropoulos, G.C. Jointly Optimal Spatial Channel Assignment and Power Allocation for MIMO SWIPT Systems. *IEEE Wirel. Commun. Lett.* **2017**, *7*, 214–217. [[CrossRef](#)]
45. Cumanan, K.; Alexandropoulos, G.C.; Ding, Z.; Karagiannidis, G.K. Secure Communications with Cooperative Jamming Optimal Power Allocation and Secrecy Outage Analysis. *IEEE Trans. Veh. Technol.* **2017**, *6*, 7495–7505. [[CrossRef](#)]
46. Cheng, Y.; Nguyen, H.T.; Kundu, C.; Kaleem, Z.; Garcia-Palacios, E.; Duong, T.Q. Secure Energy Harvesting Relay Networks with Unreliable Backhaul Connections. *IEEE Access* **2018**, *6*, 12074–12084. [[CrossRef](#)]
47. Hoang, T.M.; Duong, T.Q.; Suraweera, H.A.; Tellambura, C.; Poor, V. Cooperative Beamforming and User Selection for Improving the Security of Relay-Aided Systems. *IEEE Trans. Commun.* **2015**, *63*, 5039–5051. [[CrossRef](#)]
48. Chen, D.H.; He, Y.C. Full-Duplex Secure Communications in Cellular Networks With Downlink Wireless Power Transfer. *IEEE Trans. Commun.* **2018**, *66*, 265–277. [[CrossRef](#)]
49. Cai, Y.; Shi, Q.; Champagne, B.; Li, G.Y. Joint Transceiver Design for Secure Downlink Communications Over an Amplify and Forward MIMO Relay. *IEEE Trans. Commun.* **2017**, *65*, 3691–3704. [[CrossRef](#)]
50. Yang, M.; Guo, D.; Huang, Y.; Duong, T.Q.; Zhang, B. Secure Multiuser Scheduling in Downlink Dual-Hop Regenerative Relay Networks Over Nakagami- m Fading Channels. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 8009–8024. [[CrossRef](#)]

51. Alessio, Z.; Pan, C.; Jorswieck, E.A. Energy Efficiency Optimization in Relay-Assisted MIMO Systems with Perfect and Statistical CSI. *IEEE Trans. Signal Process.* **2014**, *62*, 443–457. [[CrossRef](#)]
52. Kang, Y.Y.; Kwak, B.J.; Cho, J.H. An Optimal Full-Duplex AF Relay for Joint Analog and Digital Domain Self-Interference Cancellation. *IEEE Trans. Commun.* **2014**, *62*, 2758–2772. [[CrossRef](#)]
53. Chen, D.; Cheng, Y.; Yang, W.; Hu, J.; Cai, Y. Physical Layer Security in Cognitive Untrusted Relay Networks. *IEEE Access* **2017**, *6*, 7055–7065. [[CrossRef](#)]
54. Wang, Z.; Chen, Z.; Xia, B. Cognitive Relay Networks with Energy Harvesting and Information Transfer: Design, Analysis, and Optimization. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 2562–2576. [[CrossRef](#)]
55. Gradshteyn, I.S.; Ryzhik, I.M. *Table of Integrals, Series, and Products*, 7th ed.; Elsevier/Academic Press: Amsterdam, The Netherlands, 2007.

© 2018 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).