Physical layer security in two-way SWIPT relay networks with imperfect CSI and a friendly jammer

Hayajneh, M. & Gulliver, T. A.

2023

entropy

MDPI

Article

Physical Layer Security in Two-Way SWIPT Relay Networks with Imperfect CSI and a Friendly Jammer

Maymoona Hayajneh and Thomas Aaron Gulliver *

Department of Electrical and Computer Engineering, University of Victoria, P.O. Box 1700, STN CSC, Victoria, BC V8W 2Y2, Canada
* Correspondence: agullive@ece.uvic.ca

Abstract: In this paper, the security of two-way relay communications in the presence of a passive eavesdropper is investigated. Two users communicate via a relay that depends solely on energy harvesting to amplify and forward the received signals. Time switching is employed at the relay to harvest energy and obtain user information. A friendly jammer is utilized to hinder the eavesdropping from wiretapping the information signal. The eavesdropper employs maximal ratio combining and selection combining to improve the signal-to-noise ratio of the wiretapped signals. Geometric programming (GP) is used to maximize the secrecy capacity of the system by jointly optimizing the time switching ratio of the relay and transmit power of the two users and jammer. The impact of imperfect channel state information at the eavesdropper for the links between the eavesdropper and the other nodes is determined. Further, the secrecy capacity when the jamming signal is not perfectly cancelled at the relay is examined. The secrecy capacity is shown to be greater with a jammer compared to the case without a jammer. The effect of the relay, jammer, and eavesdropper locations on the secrecy capacity is also studied. It is shown that the secrecy capacity is greatest when the relay is at the midpoint between the users. The closer the jammer is to the eavesdropper, the higher the secrecy capacity as the shorter distance decreases the signal-to-noise ratio of the jammer.

Keywords: amplify and forward; eavesdropper; imperfect channel state information; relay; secrecy capacity; simultaneous wireless information and power transfer; time switching; two-way

Citation: Hayajneh, M.; Gulliver, T.A. Physical Layer Security in Two-Way SWIPT Relay Networks with Imperfect CSI and a Friendly Jammer. *Entropy* **2023**, *25*, 122. https://doi.org/10.3390/e25010122

Academic Editors: Raúl Alcaraz, Luca Faes, Leandro Pardo and Boris Ryabko

Received: 21 November 2022
Revised: 22 December 2022
Accepted: 31 December 2022
Published: 6 January 2023

1. Introduction

There has been a shift in wireless network research from spectral efficiency and quality of service (QoS) constraints to energy efficiency and green communication [1] to reduce the power consumption [2]. Green energy resources such as solar, wind, thermal, and mechanical vibrations can be employed to improve the energy efficiency of energy-constrained devices such as in wireless sensor networks. Energy harvesting (EH) to convert the available energy in the surrounding area into electricity has been the subject of recent research [3]. Energy harvesting from radio frequency (RF) signals has been employed in wireless communication systems to prolong the lifetime of devices in energy-constrained systems [4]. Wireless power transmission (WPT) for EH is a promising solution to sustainable energy for wireless devices [5–7]. It can provide a reliable source of energy for devices that are difficult to service due to mobility and location [8–10].

RF signals can carry both information and energy, so WPT in wireless communication systems is known as simultaneous wireless information and power transfer (SWIPT) [6,8,11–13]. Two circuits are usually employed to harvest energy and retrieve information [14]. Two SWIPT protocols have been developed, power splitting (PS) and time switching (TS) [15]. With TS, the receiver switches between the two circuits, while in PS, a fraction of the signal is directed to the EH circuit, and the remaining part is sent to the information retrieval circuit. The maximum transmission rate using optimal PS and TS was derived in [16,17], respectively. In [16], the outage probability was obtained for a

decode and forward (DF) relay network, and the optimal transmission rates with PS and TS were determined. A SWIPT-enabled relay was considered in [17] for three scenarios, ideal (simultaneous EH and information retrieval), PS, and TS, and the maximum rates for each were obtained. PS and TS can be used separately or combined as a hybrid protocol, where the relay switches between PS and TS [18]. The optimal TS and PS ratios were derived to maximize the throughput with an EH relay, and the hybrid protocol was shown to provide the best performance. In [19,20], joint PS and TS schemes were considered for amplify and forward (AF) and DF relay networks, respectively. In [19], the outage probability, energy efficiency, and network throughput were derived as a function of the PS and TS ratios, and the network throughput was maximized. In [20], two optimization problems were jointly formulated to minimize the outage probability. These outage probabilities were shown to be better than that with the hybrid protocol in [18]. The system throughput of a cognitive two-way relay network was maximized in [21] using an optimal offline joint relay selection and power allocation scheme.

Wireless signals are more vulnerable to eavesdropping compared to wired signals given the broadcast nature of wireless systems. The physical layer security of the wiretap channel was introduced in [22] and is defined as the difference between the capacity of the link between the source and destination and the capacity of the wiretap link between the source and eavesdropper. This can be used to assist upper-layer cryptographic techniques [23–25]. Physical-layer-security-based solutions exploit the physical properties of wireless channels, such as fading and interference, to secure transmissions between users in the presence of eavesdroppers [26,27].

Physical layer security has been considered for relay networks [28], cellular networks [29,30], cognitive radio networks [31], Internet of Things (IoT) networks [32], and massive multiple-input multiple-output (MIMO) networks [33]. However, wireless channel conditions have a significant effect on the solutions [34]. Physical layer security with cooperative relaying has been employed to overcome this issue [35]. This was first studied in [36] for an untrusted relay network, which was considered as a possible eavesdropper. One-way communications was examined in [37] for DF and AF EH relays, and it was shown that DF outperforms AF in terms of secrecy performance. The secrecy capacity was analysed in [38] for PS and TS relaying protocols in a one-way untrusted relay network, and PS outperformed TS.

Two-way relay channels in which two users simultaneously exchange messages were first considered in [39] and more recently in [40]. The spectral efficiency with two-way relaying is higher than with one-way relaying. In [41], a two-way EH-based relay network with an eavesdropper was investigated. The secrecy capacity was maximized and an iterative method employed to obtain the optimal TS and PS ratios for high signal-to-noise ratios (SNRs) based on the instantaneous channel state information (CSI). It was shown that near-optimal secrecy capacity is achievable with the proposed approach even when the wiretapped channels are unknown. Joint secrecy capacity and energy efficiency were considered in [42] for a two-way untrusted relay network. The probability of successful eavesdropping in a two-way EH DF relay network was derived in [43] assuming independent κ-μ shadowed fading. It was shown that allocating extra power for information decoding over a small reception time improves the secrecy capacity. In [44], the intercept probability was derived for a two-way DF EH relay network in the presence of multiple eavesdroppers. The effect of the PS factor on the secrecy capacity was studied. The secrecy capacity of a two-way communication network with multi-antenna time-switching relays in the presence of an eavesdropper was maximized in [45]. It this case, the secrecy capacity with equal transmit power is better than with unequal transmit power.

Cooperative jamming can improve the secrecy capacity [46–48]. Friendly jamming (FJ) and Gaussian noise jamming (GNJ) have been considered to improve the secrecy capacity of wireless communication networks. The jamming signal is known at the receiver when FJ is used [24], while with GNJ, the jamming signal is considered to be noise at the receiver [49]. While both FJ and GNJ can improve the secrecy capacity, the performance with FJ is better

because the users can cancel this signal. In [50], a system with two eavesdroppers and an EH friendly jammer was considered. One eavesdropper is near the user, while the other is near the jammer, and they cooperate to obtain user signals and mitigate the effects of jamming. The secrecy capacity and energy efficiency of the network were maximized by optimizing the jamming signal power. In [51], the secrecy capacity with a friendly jammer was investigated for a one-way untrusted relay network with non-line-of-sight transmissions. A jammer was employed in [52] for an EH-based relay network to secure two-way communications, and a lower bound was derived for the secrecy capacity at high SNRs. It was shown that FJ with two-way communications outperforms one-way and two-way communications without jamming and with GNJ. In [53], the secrecy capacity of one-way untrusted relay communications was optimized considering the transmit and jamming powers with an EH relay threshold. The secrecy performance with untrusted EH relays and energy-aware distributed beamforming was investigated in [54]. The secrecy capacity was increased in [55] by choosing GNJ and relay nodes from multiple friendly, but selfish intermediate nodes. Price competition was used for power allocation to these nodes, and their profit to maximize the secrecy capacity was determined. In [56], a full-duplex jammer (FDJ) and half-duplex jammer (HDJ) were proposed to improve security while exploiting EH. An interference-limited scenario was considered, and closed-form cumulative distribution functions (CDFs) were derived for the signal-to-interference-plus-noise ratio at the destination and eavesdropper nodes.

A two-way untrusted relay system with multiple friendly jammers was considered in [57], and the jamming power was optimized to improve the secrecy capacity. In [58], a network with multiple relay–user pairs was investigated in the presence of multiple eavesdroppers. Joint relay–user pairs and friendly jammer selection were determined to maximize the secrecy capacity. The secrecy capacity was optimized in [57] using a Stackelberg game for power allocation between users and friendly jammers.

In [59], adaptive cooperative jamming in the presence of multiple eavesdroppers was investigated for an EH relay. The secrecy capacity was maximized by optimizing the power allocation factor. A two-way EH relay network with an eavesdroppers and a friendly jammer was considered in [60]. The optimal PS and TS factors were derived to maximize the secrecy capacity, and PS was shown to be better than TS. A two-way relay network with partial relay selection and hybrid PS and TS at the intermediate nodes was investigated in [61]. It was shown that secure communications are possible with an appropriate selection of the parameters.

In the results given above, perfect knowledge of the CSI for the user and relay signals at the eavesdropper was assumed. However, this is not a practical assumption considering unknown delays and channel estimation errors. In two-way relay networks, imperfect CSI results in imperfect self-interference cancellation [62]. In [63], a transmission scheme was proposed for multiple-input single-output (MISO) channels with imperfect CSI for the user and eavesdropper channels with cooperative jamming. In [64], the CSI for the channel between the jammer and eavesdropper was assumed to be unknown and imperfect CSI assumed between the jammer and user. The impact of imperfect CSI on the secrecy outage capacity with cooperative jamming was analysed. Although imperfect CSI has received some research attention, the impact of imperfect CSI on the security of a SWIPT two-way relay network has not yet been studied.

In this paper, the physical layer security of a two-way communication system with a relay employing TS to harvest energy, a friendly jammer, and imperfect CSI at a passive eavesdropper is studied. TS is simpler to implement than the PS considered in [65]. The eavesdropper employs maximal ratio combining (MRC) and selection combining (SC) to degrade the secrecy capacity. The power allocated to two users, a relay, and a jammer are jointly optimized in the presence of an eavesdropper with imperfect CSI. This system has not been previously considered in the literature for a TS EH relay. Furthermore, the effect of the imperfect cancellation of the jamming power at the relay is studied. The main contributions of this work are as follows:

1. The effect of channel estimation errors on the secrecy capacity is investigated when the eavesdropper employs MRC and SC. Imperfect CSI at the eavesdropper has not been previously considered.
2. The secrecy capacity is maximized by jointly optimizing the TS ratio and transmit powers of the two users and jammer.
3. The single condensation method (SCM) is used to convert the objective function into a standard geometric programming (GP) form. Then, GP is employed to transform the optimization problem into a convex form.
4. The effect of imperfect cancellation of the jamming signal at the relay is examined. This has not been considered previously in the literature.
5. The effect of the TS ratio on the secrecy capacity is investigated.
6. The secrecy capacity is evaluated with and without a jammer. In addition, results are given for different eavesdropper and jammer locations.

The remainder of this paper is organized as follows. The system model is given in Section 2. The secrecy capacity for the two-way relay network is presented in Section 3 for MRC and SC. In Section 4, the optimization problem is formulated and converted to a convex form. Section 5 presents the simulation results, and finally, some concluding remarks are given in Section 6.

2. System Model

The two-way relay network considered here is shown in Figure 1. It consists of two users A and B, a trusted relay R, a friendly jammer J, and an eavesdropper E. Each of these nodes has a single antenna and operates in half-duplex mode. The friendly jammer can be another user node or a dedicated jamming node. The eavesdropper is randomly located near the relay to listen to the signals received by and transmitted from the relay. The A-R, B-R, A-E, B-E, R-E, J-R, and J-E channel links are denoted by h_{AR}, h_{BR}, h_{AE}, h_{BE}, h_{RE}, h_{JR}, and h_{JE}, respectively. Quasi-static fading channels are assumed so the channel gains, h_{ij}, are constant over the coherence time [15,41]. Rayleigh fading is assumed so the channel coefficients are Rayleigh random variables. Then, the channel gains $|h_{ij}|^2$ are exponentially distributed random variables with means λ and λ_{Eve}. The channels are assumed to be reciprocal such that $h_{ij} = h_{ji}$, $\{i, j\} \in \{A, B, R, J, E\}, i \neq j$. The parameters n_A, n_B,n_R, and n_E denote the additive white Gaussian noise (AWGN) at A, B, R, and E, respectively, with zero mean and variance σ^2.

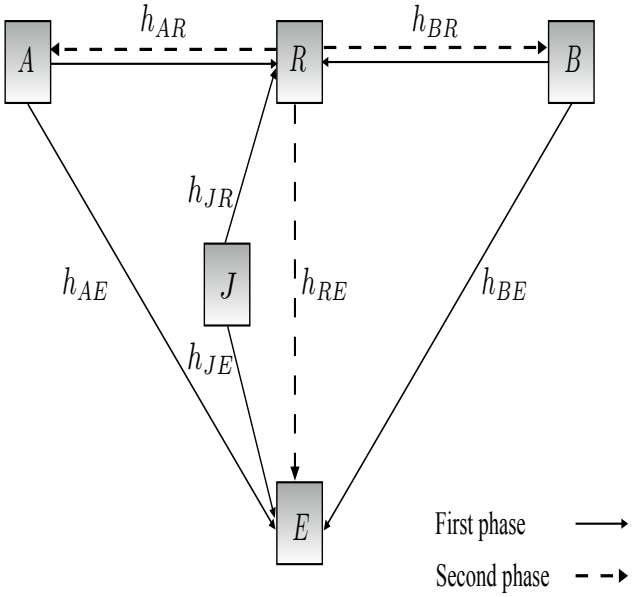

Figure 1. System model of a two-way wireless relay network with two users, a jammer, and an eavesdropper.

In this paper, the practical case is considered where the channels at A, B, R, and J can be estimated accurately given that they are trusted nodes, but there are channel estimation errors at the eavesdropper [63]. The estimated channel gain from the eavesdropper to node i, $i \in \{A, B, R, J\}, i \neq E$, is given by [62]

$$h_{iE} = \widehat{h}_{iE} + e_{iE}, \tag{1}$$

where $\widehat{h}_{iE}$ is the estimated channel gain and e_{iE} is the channel estimation error. For simplicity, denote e_{iE} by e_E, which is a Gaussian distributed random variable with zero mean and variance σ_e^2. A summary of the notation used in this paper is given in Abbreviations.

Figure 2 illustrates the two phases required to forward signals between A and B in the relay network. The first phase is dedicated to signal reception and energy harvesting at the relay and is divided into two subphases. As in [15], in the first subphase, all the received signal power is used for energy harvesting. This subphase has duration ρT, where ρ is the TS ratio, $0 \leq \rho \leq 1$. In the second subphase, all the received signal power is used for information decoding, and the duration is $(1-\rho)\frac{T}{2}$. A, B, and J send their signals x_A, x_B, and x_J with $\mathbf{E}[|x_A|^2] = \mathbf{E}[|x_B|^2] = \mathbf{E}[|x_J|^2 = 1$ and transmit powers P_A, P_B, and P_J, respectively, to R. The relay depends solely on the energy harvested from the user and jamming signals in the first subphase to amplify and forward the signals received from the users in the second subphase. The EH signal during the first subphase is

$$y_{Re} = \sqrt{P_A} h_{AR} x_A + \sqrt{P_B} h_{BR} x_B + \sqrt{P_J} h_{JR} x_J. \tag{2}$$

The noise at the relay, n_R, is neglected because it is much less than the other terms in (2) [15]. The harvested energy is

$$E_H = \rho T \zeta \left(P_A |h_{AR}|^2 + P_B |h_{BR}|^2 + P_J |h_{JR}|^2 \right), \tag{3}$$

where $\zeta, 0 < \zeta \leq 1$, is the energy conversion efficiency. In the second phase, the relay transmit power is

$$P_R = \frac{E_H}{(1-\rho)T/2} = \frac{2\rho\zeta E_R}{1-\rho}, \tag{4}$$

where $E_R = P_A |h_{AR}|^2 + P_B |h_{BR}|^2 + P_J |h_{JR}|^2$. The information retrieval part of the received signal during the second subphase is

$$\begin{aligned} y_{Ri} = &\sqrt{P_A} h_{AR} x_A + \sqrt{P_B} h_{BR} x_B \\ &+ \sqrt{P_J} h_{JR} x_J + n_R. \end{aligned} \tag{5}$$

The jamming signal term $\sqrt{P_J} h_{JR} x_J$ at the relay can be cancelled from y_{Ri} as in [66,67] as A and B are assumed to have a priori information of the jammer signal. Further, the jammer is located close to the relay and farther from A and B, so the jamming signal at A and B is negligible. Information regarding the jamming signal is securely shared among the jammer, relay, and users before cooperative jamming begins. However, the jamming signal may not be perfectly cancelled at the relay, which is the assumption here. A cancellation factor Φ, $0 \leq \Phi \leq 1$, is used to indicate the fraction of the jamming signal that is not cancelled. This fraction, $\Phi \times P_J$, is amplified and forwarded to A and B by the relay. The jamming signal is perfectly cancelled if $\Phi = 0$, and there is no cancellation if $\Phi = 1$. The value of Φ depends on the circuitry of the relay receiver and the CSI at R.

The information retrieval signal with imperfect jamming cancellation is

$$\begin{aligned} y_R = &\sqrt{P_A} h_{AR} x_A + \sqrt{P_B} h_{BR} x_B \\ &+ \Phi \sqrt{P_J} h_{JR} x_J + n_R. \end{aligned} \tag{6}$$

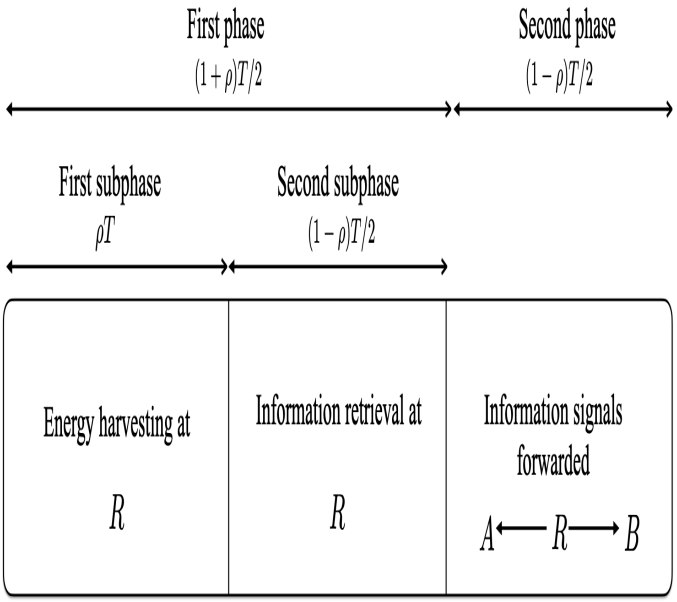

Figure 2. Transmission time frame for time switching (TS) in the two-way relay network.

2.1. First Phase

During the first phase, the signal received at E is

$$y_E^{(1)} = \sqrt{P_A}(\widehat{h}_{AE} + e_E)x_A + \sqrt{P_B}(\widehat{h}_{BE} + e_E)x_B + \sqrt{P_J}(\widehat{h}_{JE} + e_E)x_J + n_E. \tag{7}$$

The SNR at E for x_B sent to A in this phase is

$$SNR_{E,A}^{(1)} = \frac{P_B|\widehat{h}_{BE}|^2}{P_A|\widehat{h}_{AE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2}, \tag{8}$$

and the SNR at E for x_A sent to B is

$$SNR_{E,B}^{(1)} = \frac{P_A|\widehat{h}_{AE}|^2}{P_B|\widehat{h}_{BE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2}. \tag{9}$$

The eavesdropper does not have knowledge of the jamming signal. Therefore, x_J is treated as additional noise, which reduces the received SNR at E.

2.2. Second Phase

During the second phase, the relay amplifies the received signal and forwards this to the users using the harvested energy. Thus, the relay transmits the signal:

$$x_R = \frac{\sqrt{P_R}}{\sqrt{P_A|h_{AR}|^2 + P_B|h_{BR}|^2 + P_J|h_{JR}|^2 + \sigma^2}} \quad y_R \tag{10}$$

$$= \sqrt{\frac{P_R}{E_R + \sigma^2}} \quad y_R, \tag{11}$$

where $\sqrt{\frac{P_R}{E_R+\sigma^2}}$ is the relay amplifier gain. The received signal at A in this phase is

$$\begin{aligned} y_A &= h_{AR}x_R + n_A \\ &= \underbrace{\frac{\sqrt{P_R P_B}h_{AR}h_{BR}}{\sqrt{E_R+\sigma^2}}x_B}_{\text{information signal}} + \underbrace{\frac{\sqrt{P_R P_A}|h_{AR}|^2}{\sqrt{E_R+\sigma^2}}x_A}_{\text{information signal}} \\ &+ \underbrace{\Phi\frac{\sqrt{P_R P_J}h_{AR}h_{JR}}{\sqrt{E_R+\sigma^2}}x_J + \frac{\sqrt{P_R}h_{AR}n_R}{\sqrt{E_R+\sigma^2}} + n_A}_{\text{effective noise}}, \end{aligned} \tag{12}$$

and the received signal at B is

$$\begin{aligned} y_B &= h_{BR}x_R + n_B \\ &= \underbrace{\frac{\sqrt{P_R P_A}h_{AR}h_{BR}}{\sqrt{E_R+\sigma^2}}x_A}_{\text{information signal}} + \underbrace{\frac{\sqrt{P_R P_B}|h_{BR}|^2}{\sqrt{E_R+\sigma^2}}x_B}_{\text{information signal}} \\ &+ \underbrace{\Phi\frac{\sqrt{P_R P_J}h_{BR}h_{JR}}{\sqrt{E_R+\sigma^2}}x_J + \frac{\sqrt{P_R}h_{BR}n_R}{\sqrt{E_R+\sigma^2}} + n_B}_{\text{effective noise}}. \end{aligned} \tag{13}$$

A and B cancel their own signals since self-interference cancellation can be assumed [68,69]. Let

$$\gamma_A = \frac{P_A|h_{AR}|^2}{\sigma^2}, \tag{14}$$

$$\gamma_B = \frac{P_B|h_{BR}|^2}{\sigma^2}, \tag{15}$$

$$\gamma_J = \frac{P_J|h_{JR}|^2}{\sigma^2}, \tag{16}$$

$$\overline{\gamma} = \gamma_A + \gamma_B + \gamma_J = \frac{E_R}{\sigma^2}. \tag{17}$$

The SNR at A is then

$$SNR_A = \frac{2\rho\zeta\overline{\gamma}\gamma_B|h_{AR}|^2}{2\rho\zeta\overline{\gamma}|h_{AR}|^2(\Phi^2\gamma_J+1)+\widetilde{\rho}(\overline{\gamma}+1)}, \tag{18}$$

where $\widetilde{\rho} = 1-\rho$ and the achievable rate at A is [70]

$$R_A = (1-\rho)\frac{T}{2}\log_2(1+SNR_A). \tag{19}$$

The SNR at B is

$$SNR_B = \frac{2\rho\zeta\overline{\gamma}\gamma_A|h_{BR}|^2}{2\rho\zeta\overline{\gamma}|h_{BR}|^2(\Phi^2\gamma_J+1)+\widetilde{\rho}(\overline{\gamma}+1)}, \tag{20}$$

and the achievable rate at B is

$$R_B = (1-\rho)\frac{T}{2}\log_2(1+SNR_B). \tag{21}$$

The signal received at E during the second phase is

$$y_E^{(2)} = h_{RE}x_R + n_E, \tag{22}$$

$$= \underbrace{\frac{\sqrt{P_R P_A}h_{AR}h_{RE}}{\sqrt{E_R+\sigma^2}}x_A}_{\text{information signal}} + \underbrace{\frac{\sqrt{P_R P_B}h_{BR}h_{RE}}{\sqrt{E_R+\sigma^2}}x_B}_{\text{information signal}}$$

$$+ \underbrace{\Phi\frac{\sqrt{P_R P_J}h_{JR}h_{RE}}{\sqrt{E_R+\sigma^2}}x_J + \frac{\sqrt{P_R}h_{RE}n_R}{\sqrt{E_R+\sigma^2}} + n_E}_{\text{effective noise}}, \tag{23}$$

where $h_{RE} = \widehat{h}_{RE} + e_E$. The SNR at E for x_B sent to A during the second phase is

$$SNR_{E,A}^{(2)} = \frac{2\rho\zeta\overline{\gamma}\gamma_B|\widehat{h}_{RE}|^2}{2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_A+\Phi^2\gamma_J+1)} \tag{24}$$

$$+\sigma_e^2(\gamma_A+\gamma_B+\Phi^2\gamma_J+1)] + \widetilde{\rho}(\overline{\gamma}+1), \tag{25}$$

and the SNR at E for x_A sent to B during the second phase is

$$SNR_{E,B}^{(2)} = \frac{2\rho\zeta\overline{\gamma}\gamma_A|\widehat{h}_{RE}|^2}{2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_B+\Phi^2\gamma_J+1)} \tag{26}$$

$$+\sigma_e^2(\gamma_A+\gamma_B+\Phi^2\gamma_J+1)] + \widetilde{\rho}(\overline{\gamma}+1). \tag{27}$$

The achievable rate at E during both phases is then

$$R_{E,i} = \begin{cases} (1-\rho)\frac{T}{2}\log_2(1+SNR_{E,i}^{(1)}+SNR_{E,i}^{(2)}), \\ \quad \text{MRC at } E \\ (1-\rho)\frac{T}{2}\log_2(1+\max(SNR_{E,i}^{(1)}+SNR_{E,i}^{(2)})), \\ \quad \text{SC at } E. \end{cases} \tag{28}$$

3. Secrecy Capacity Analysis

The secrecy capacity in the presence of an eavesdropper is the difference between the secrecy capacity of the link between the users and the secrecy capacity of the wiretap link [70]. The total transmit power in this network is limited by the total power constraint P_T, where $P_A + P_B + P_J \leq P_T$. The goal is to determine the time switching ratio and transmit power of A, B, and J to maximize the secrecy capacity at A and B under this constraint. The secrecy capacity at A is $C_{S,A} = [R_A - R_{E,A}]^+$ and at B is $C_{S,B} = [R_B - R_{E,B}]^+$ [71], where $[x]^+ = \max(0, x)$. The secrecy capacity at user i, $i \in \{A, B\}$, is then

$$C_{S,i} = \begin{cases} (1-\rho)\frac{T}{2}\log_2\left(\frac{1+SNR_i}{1+SNR_{E,i}^{(1)}+SNR_{E,i}^{(2)}}\right), \\ \quad \text{MRC at } E \\ (1-\rho)\frac{T}{2}\log_2\left(\frac{1+SNR_i}{1+\max(SNR_{E,i}^{(1)}+SNR_{E,i}^{(2)})}\right), \\ \quad \text{SC at } E. \end{cases} \tag{29}$$

The secrecy capacity is

$$C_S = C_{S,A} + C_{S,B}, \tag{30}$$

$$= [R_A - R_{E,A}]^+ + [R_B - R_{E,B}]^+, \tag{31}$$

and the corresponding optimization problem is formulated as

$$\begin{aligned} \max_{\rho,\widetilde{\rho},P_A,P_B,P_J} \quad & C_S \\ P_A + P_B + P_J \leq \; & P_T \\ \rho + \widetilde{\rho} \leq \; & 1 \\ \rho, \widetilde{\rho}, P_A, P_B, P_J \geq \; & 0 \end{aligned}$$

3.1. MRC at the Eavesdropper

In this subsection, the secrecy capacity of the communication system is investigated with imperfect channel estimation at the eavesdropper. The eavesdropper employs MRC to combine the signals from the direct and relay links in both transmission phases. The achievable rates at E for x_B sent to A and x_A sent to B, $R_{E,A}$, and $R_{E,B}$, respectively, are defined in (28). $C_{S,A}$ is obtained by substituting SNR_A, $SNR_{E,A}^{(1)}$, and $SNR_{E,A}^{(2)}$ given by (18), (8), and (25), respectively, in (29) with $i = A$. $C_{S,B}$ is obtained by substituting SNR_B, $SNR_{E,B}^{(1)}$, and $SNR_{E,B}^{(2)}$ given by (20), (9), and (27), respectively, in (29) with $i = B$. From (31), there are four cases to consider to maximize the secrecy capacity as given below.

3.1.1. Case I: $C_{S,A} \geq 0$ and $C_{S,B} \geq 0$

In this case, the secrecy capacity is

$$\begin{aligned} C_S =& (R_A - R_{E,A}) + (R_B - R_{E,B}) \\ =& \frac{T}{2} \log_2 \left(\frac{w_I^{MRC}}{z_I^{MRC}} \right), \end{aligned} \tag{32}$$

where $(.)_I^{MRC}$ denotes the first case with MRC at the eavesdropper:

$$\begin{aligned} & w_I^{MRC} = \\ & (2\rho\zeta\overline{\gamma}\gamma_B|h_{AR}|^2 + 2\rho\zeta\overline{\gamma}|h_{AR}|^2\left(\Phi^2\gamma_J + 1\right) + \widetilde{\rho}(\overline{\gamma} + 1)) \\ & (P_A|\widehat{h}_{AE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2) \\ & (2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_A + \Phi^2\gamma_J + 1) + \\ & \quad \sigma_e^2(\gamma_A + \gamma_B + \Phi^2\gamma_J + 1)] + \widetilde{\rho}(\overline{\gamma} + 1)) \end{aligned} \tag{33}$$

$$\begin{aligned} & (2\rho\zeta\overline{\gamma}\gamma_A|h_{BR}|^2) + (2\rho\zeta\overline{\gamma}|h_{BR}|^2\left(\Phi^2\gamma_J + 1\right) + \widetilde{\rho}(\overline{\gamma} + 1)) \\ & (P_B|\widehat{h}_{BE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2) \\ & (2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_B + \Phi^2\gamma_J + 1) + \sigma_e^2(\gamma_A + \gamma_B + \Phi^2\gamma_J + 1)] \\ & \quad + \widetilde{\rho}(\overline{\gamma} + 1)), \end{aligned} \tag{34}$$

and

$$
\begin{aligned}
& z_I^{MRC} = \\
& (2\rho\zeta\overline{\gamma}|h_{AR}|^2\left(\Phi^2\gamma_J+1\right)+\widetilde{\rho}(\overline{\gamma}+1)) \\
& (2\rho\zeta\overline{\gamma}|h_{BR}|^2\left(\Phi^2\gamma_J+1\right)+\widetilde{\rho}(\overline{\gamma}+1)) \\
& [((P_B|\widehat{h}_{BE}|^2)+(P_A|\widehat{h}_{AE}|^2+P_J|\widehat{h}_{JE}|^2 \\
& \quad +\sigma_e^2(P_A+P_B+P_J)+\sigma^2))(2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_A+\Phi^2\gamma_J+1) \\
& \quad +\sigma_e^2(\gamma_A+\gamma_B+\Phi^2\gamma_J+1)] \\
& \quad +\widetilde{\rho}(\overline{\gamma}+1))+(P_A|\widehat{h}_{AE}|^2+P_J|\widehat{h}_{JE}|^2+\sigma_e^2(P_A+P_B+P_J) \\
& \quad +\sigma^2)(2\rho\zeta\overline{\gamma}\gamma_B|\widehat{h}_{RE}|^2)] \\
& [((P_A|\widehat{h}_{AE}|^2)+(P_B|\widehat{h}_{BE}|^2+P_J|\widehat{h}_{JE}|^2+\sigma_e^2(P_A+P_B+P_J) \\
& \quad +\sigma^2))(2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_B+\Phi^2\gamma_J+1)+\sigma_e^2(\gamma_A+\gamma_B+\Phi^2\gamma_J \\
& \quad +1)]+\widetilde{\rho}(\overline{\gamma}+1))+(P_B|\widehat{h}_{BE}|^2+P_J|\widehat{h}_{JE}|^2+\sigma_e^2(P_A+P_B \\
& \quad +P_J)+\sigma^2)(2\rho\zeta\overline{\gamma}\gamma_A|\widehat{h}_{RE}|^2)].
\end{aligned} \tag{35}
$$

3.1.2. Case II: $C_{S,A} \geq 0$ and $C_{S,B} \leq 0$

In this case, $C_{S,B} = 0$ since the SNR at the eavesdropper is higher than that at B. The secrecy capacity is then

$$
\begin{aligned}
C_S =& (R_A - R_{E,A}) \\
=& \frac{T}{2}\log_2\left(\frac{w_{II}^{MRC}}{z_{II}^{MRC}}\right),
\end{aligned} \tag{36}
$$

where $(.)_{II}^{MRC}$ denotes the second case with MRC at the eavesdropper:

$$
\begin{aligned}
& w_{II}^{MRC} = \\
& ((2\rho\zeta\overline{\gamma}\gamma_B|h_{AR}|^2)+(2\rho\zeta\overline{\gamma}|h_{AR}|^2\left(\Phi^2\gamma_J+1\right)+\widetilde{\rho}(\overline{\gamma}+1))) \\
& (P_A|\widehat{h}_{AE}|^2+P_J|\widehat{h}_{JE}|^2+\sigma_e^2(P_A+P_B+P_J)+\sigma^2) \\
& (2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_A+\Phi^2\gamma_J+1)+\sigma_e^2(\gamma_A+\gamma_B+\Phi^2\gamma_J \\
& \quad +1)]+\widetilde{\rho}(\overline{\gamma}+1)),
\end{aligned} \tag{37}
$$

and

$$
\begin{aligned}
& z_{II}^{MRC} = \\
& (2\rho\zeta\overline{\gamma}|h_{AR}|^2\left(\Phi^2\gamma_J+1\right)+\widetilde{\rho}(\overline{\gamma}+1)) \\
& [((P_B|\widehat{h}_{BE}|^2)+(P_B|\widehat{h}_{BE}|^2+P_J|\widehat{h}_{JE}|^2 \\
& \quad +\sigma_e^2(P_A+P_B+P_J)+\sigma^2))(2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_A \\
& \quad +\Phi^2\gamma_J+1)+\sigma_e^2(\gamma_A+\gamma_B+\Phi^2\gamma_J+1)] \\
& \quad +\widetilde{\rho}(\overline{\gamma}+1))+((P_A|\widehat{h}_{AE}|^2+P_J|\widehat{h}_{JE}|^2+\sigma_e^2(P_A+P_B \\
& \quad +P_J)+\sigma^2)*(2\rho\zeta\overline{\gamma}\gamma_B|\widehat{h}_{RE}|^2))].
\end{aligned} \tag{38}
$$

3.1.3. Case III: $C_{S,A} \leq 0$ and $C_{S,B} \geq 0$

In this case, $C_{S,A} = 0$ since the SNR at the eavesdropper is higher than that at A. The secrecy capacity is then

$$\begin{aligned} C_S =& (R_B - R_{E,B}) \\ =& \frac{T}{2} \log_2 \left(\frac{w_{III}^{MRC}}{z_{III}^{MRC}} \right), \end{aligned} \tag{39}$$

where $(.)_{III}^{MRC}$ denotes the third case with MRC at the eavesdropper:

$$\begin{aligned} & w_{III}^{MRC} = \\ & ((2\rho\zeta\overline{\gamma}\gamma_A|h_{BR}|^2) + (2\rho\zeta\overline{\gamma}|h_{BR}|^2\left(\Phi^2\gamma_J + 1\right) + \widetilde{\rho}(\overline{\gamma} + 1))) \\ & (P_B|\widehat{h}_{BE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2) \\ & (2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_B + \Phi^2\gamma_J + 1) + \sigma_e^2(\gamma_A + \gamma_B + \Phi^2\gamma_J + 1)] \\ & \quad + \widetilde{\rho}(\overline{\gamma} + 1)), \end{aligned} \tag{40}$$

and

$$\begin{aligned} & z_{III}^{MRC} = \\ & (2\rho\zeta\overline{\gamma}|h_{BR}|^2\left(\Phi^2\gamma_J + 1\right) + \widetilde{\rho}(\overline{\gamma} + 1)) \\ & [((P_A|\widehat{h}_{AE}|^2) + (P_B|\widehat{h}_{BE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) \\ & \quad + \sigma^2))(2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_B + \Phi^2\gamma_J + 1) \\ & \quad + \sigma_e^2(\gamma_A + \gamma_B + \Phi^2\gamma_J + 1)] + \widetilde{\rho}(\overline{\gamma} + 1))(P_B|\widehat{h}_{BE}|^2 \\ & \quad + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2)(2\rho\zeta\overline{\gamma}\gamma_A|\widehat{h}_{RE}|^2)]. \end{aligned} \tag{41}$$

3.1.4. Case IV: $C_{S,A} \leq 0$ and $C_{S,B} \leq 0$

In this case, the secrecy capacity is $C_S = 0$ because the secrecy capacity of the wire-tapped links is higher than the secrecy capacity at A and B.

3.2. SC at the Eavesdropper

In this subsection, the secrecy capacity of the communication system is investigated with imperfect channel estimation at the eavesdropper. The eavesdropper employs SC so the link (direct or relay) with the maximum SNR is selected. Based on $SNR_{E,A}^{(1)}$, $SNR_{E,A}^{(2)}$, $SNR_{E,B}^{(1)}$, and $SNR_{E,B}^{(2)}$ given by (8), (25), (9), and (27), respectively, the following four cases can be considered.

3.2.1. Case I: $SNR_{E,A}^{(1)} \geq SNR_{E,A}^{(2)}$ and $SNR_{E,B}^{(1)} \geq SNR_{E,B}^{(2)}$

In this case, the secrecy capacity is

$$\begin{aligned} C_S =& C_{S,A} + C_{S,B} \\ =& \frac{T}{2}\log_2\left(\frac{1+SNR_A}{1+SNR_{E,A}^{(1)}}\right) + \frac{T}{2}\log_2\left(\frac{1+SNR_B}{1+SNR_{E,B}^{(1)}}\right), \\ =& \frac{T}{2}\log_2\left(\frac{w_{I,A}^{SC}}{z_{I,A}^{SC}}\right) + \frac{T}{2}\log_2\left(\frac{w_{I,B}^{SC}}{z_{I,B}^{SC}}\right), \\ =& \frac{T}{2}\log_2\left(\frac{w_I^{SC}}{z_I^{SC}}\right), \end{aligned} \tag{42}$$

where

$$\begin{aligned} & w_{I,A}^{SC} = \\ & ((2\rho\zeta\overline{\gamma}\gamma_B|h_{AR}|^2) + (2\rho\zeta\overline{\gamma}|h_{AR}|^2\left(\Phi^2\gamma_J+1\right) + \widetilde{\rho}(\overline{\gamma}+1))) \\ & (P_A|\widehat{h}_{AE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A+P_B+P_J) + \sigma^2), \end{aligned} \tag{43}$$

$$\begin{aligned} & w_{I,B}^{SC} = \\ & ((2\rho\zeta\overline{\gamma}\gamma_A|h_{BR}|^2) + (2\rho\zeta\overline{\gamma}|h_{BR}|^2\left(\Phi^2\gamma_J+1\right) + \widetilde{\rho}(\overline{\gamma}+1))) \\ & (P_B|\widehat{h}_{BE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A+P_B+P_J) + \sigma^2), \end{aligned} \tag{44}$$

$$\begin{aligned} & z_{I,A}^{SC} = \\ & ((P_B|\widehat{h}_{BE}|^2) + (P_A|\widehat{h}_{AE}|^2 + P_J|\widehat{h}_{JE}|^2 \\ & \quad + \sigma_e^2(P_A+P_B+P_J) + \sigma^2) \\ & (2\rho\zeta\overline{\gamma}|h_{AR}|^2\left(\Phi^2\gamma_J+1\right) + \widetilde{\rho}(\overline{\gamma}+1)), \end{aligned} \tag{45}$$

$$\begin{aligned} & z_{I,B}^{SC} = \\ & ((P_A|\widehat{h}_{AE}|^2) + (P_B|\widehat{h}_{BE}|^2 + P_J|\widehat{h}_{JE}|^2 \\ & \quad + \sigma_e^2(P_A+P_B+P_J) + \sigma^2)) \\ & (2\rho\zeta\overline{\gamma}|h_{BR}|^2\left(\Phi^2\gamma_J+1\right) + \widetilde{\rho}(\overline{\gamma}+1)), \end{aligned} \tag{46}$$

$$\frac{w_I^{SC}}{z_I^{SC}} = \begin{cases} \dfrac{w_{I,A}^{SC} w_{I,B}^{SC}}{z_{I,A}^{SC} z_{I,B}^{SC}}, & C_{S,A} \geq 0 \text{ and } C_{S,B} \geq 0 \\ \dfrac{w_{I,A}^{SC}}{z_{I,A}^{SC}}, & C_{S,A} \geq 0 \text{ and } C_{S,B} < 0 \\ \dfrac{w_{I,B}^{SC}}{z_{I,B}^{SC}}, & C_{S,A} < 0 \text{ and } C_{S,B} \geq 0 \\ 0, & C_{S,A} < 0 \text{ and } C_{S,B} < 0, \end{cases} \tag{47}$$

and $(.)_I^{SC}$ denotes the first case with SC at the eavesdropper.

3.2.2. Case II: $SNR_{E,A}^{(1)} \geq SNR_{E,A}^{(2)}$ and $SNR_{E,B}^{(1)} \leq SNR_{E,B}^{(2)}$

In this case, the secrecy capacity is

$$\begin{aligned} C_S =& C_{S,A} + C_{S,B} \\ =& \frac{T}{2}\log_2\left(\frac{1+SNR_A}{1+SNR_{E,A}^{(1)}}\right) + \frac{T}{2}\log_2\left(\frac{1+SNR_B}{1+SNR_{E,B}^{(2)}}\right), \\ =& \frac{T}{2}\log_2\left(\frac{w_{II,A}^{SC}}{z_{II,A}^{SC}}\right) + \frac{T}{2}\log_2\left(\frac{w_{II,B}^{SC}}{z_{II,B}^{SC}}\right), \\ =& \frac{T}{2}\log_2\left(\frac{w_{II}^{SC}}{z_{II}^{SC}}\right), \end{aligned} \tag{48}$$

where

$$\begin{aligned} & w_{II,A}^{SC} = \\ & ((2\rho\zeta\overline{\gamma}\gamma_B|h_{AR}|^2) + (2\rho\zeta\overline{\gamma}|h_{AR}|^2\left(\Phi^2\gamma_J+1\right) + \widetilde{\rho}(\overline{\gamma}+1))) \\ & (P_A|\widehat{h}_{AE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A+P_B+P_J) + \sigma^2), \end{aligned} \tag{49}$$

$$\begin{aligned} & w_{II,B}^{SC} = \\ & ((2\rho\zeta\overline{\gamma}\gamma_A|h_{BR}|^2) + (2\rho\zeta\overline{\gamma}|h_{BR}|^2\left(\Phi^2\gamma_J+1\right) + \widetilde{\rho}(\overline{\gamma}+1))) \\ & (2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_B+\Phi^2\gamma_J+1) + \sigma_e^2(\gamma_A+\gamma_B+\Phi^2\gamma_J+1)] \\ & \quad + \widetilde{\rho}(\overline{\gamma}+1)), \end{aligned} \tag{50}$$

$$\begin{aligned} & z_{II,A}^{SC} = \\ & ((P_B|\widehat{h}_{BE}|^2) + (P_A|\widehat{h}_{AE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A+P_B+P_J) \\ & \quad + \sigma^2)(2\rho\zeta\overline{\gamma}|h_{AR}|^2\left(\Phi^2\gamma_J+1\right) + \widetilde{\rho}(\overline{\gamma}+1)), \end{aligned} \tag{51}$$

$$\begin{aligned} & z_{II,B}^{SC} = \\ & ((2\rho\zeta\overline{\gamma}\gamma_A|\widehat{h}_{RE}|^2) + (2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_B+\Phi^2\gamma_J+1) \\ & \quad + \sigma_e^2(\gamma_A+\gamma_B+\Phi^2\gamma_J+1)] + \widetilde{\rho}(\overline{\gamma}+1))) \\ & \quad (2\rho\zeta\overline{\gamma}|h_{BR}|^2\left(\Phi^2\gamma_J+1\right) + \widetilde{\rho}(\overline{\gamma}+1)), \end{aligned} \tag{52}$$

$$\frac{w_{II}^{SC}}{z_{II}^{SC}} = \begin{cases} \dfrac{w_{II,A}^{SC} w_{II,B}^{SC}}{z_{II,A}^{SC} z_{II,B}^{SC}}, & C_{S,A} \geq 0 \text{ and } C_{S,B} \geq 0 \\ \dfrac{w_{II,A}^{SC}}{z_{II,A}^{SC}}, & C_{S,A} \geq 0 \text{ and } C_{S,B} < 0 \\ \dfrac{w_{II,B}^{SC}}{z_{II,B}^{SC}}, & C_{S,A} < 0 \text{ and } C_{S,B} \geq 0 \\ 0, & C_{S,A} < 0 \text{ and } C_{S,B} < 0, \end{cases} \tag{53}$$

and $(.)_{II}^{SC}$ denotes the second case with SC at the eavesdropper.

3.2.3. Case III: $SNR_{E,A}^{(1)} \leq SNR_{E,A}^{(2)}$ and $SNR_{E,B}^{(1)} \geq SNR_{E,B}^{(2)}$

In this case, the secrecy capacity is

$$\begin{aligned} C_S =& C_{S,A} + C_{S,B} \\ =& \frac{T}{2}\log_2\left(\frac{1+SNR_A}{1+SNR_{E,A}^{(2)}}\right) + \frac{T}{2}\log_2\left(\frac{1+SNR_B}{1+SNR_{E,B}^{(1)}}\right), \\ =& \frac{T}{2}\log_2\left(\frac{w_{III,A}^{SC}}{z_{III,A}^{SC}}\right) + \frac{T}{2}\log_2\left(\frac{w_{III,B}^{SC}}{z_{III,B}^{SC}}\right), \\ =& \frac{T}{2}\log_2\left(\frac{w_{III}^{SC}}{z_{III}^{SC}}\right), \end{aligned} \tag{54}$$

where

$$\begin{aligned} & w_{III,A}^{SC} = \\ & ((2\rho\zeta\overline{\gamma}\gamma_B|h_{AR}|^2) + (2\rho\zeta\overline{\gamma}|h_{AR}|^2\left(\Phi^2\gamma_J+1\right) + \widetilde{\rho}(\overline{\gamma}+1))) \\ & (2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_A+\Phi^2\gamma_J+1) + \sigma_e^2(\gamma_A+\gamma_B+\Phi^2\gamma_J+1)] \\ & \quad + \widetilde{\rho}(\overline{\gamma}+1)), \end{aligned} \tag{55}$$

$$\begin{aligned} & w_{III,B}^{SC} = \\ & ((2\rho\zeta\overline{\gamma}\gamma_A|h_{BR}|^2) + (2\rho\zeta\overline{\gamma}|h_{BR}|^2\left(\Phi^2\gamma_J+1\right) + \widetilde{\rho}(\overline{\gamma}+1))) \\ & (P_B|\widehat{h}_{BE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A+P_B+P_J) + \sigma^2), \end{aligned} \tag{56}$$

$$\begin{aligned} & z_{III,A}^{SC} = \\ & ((2\rho\zeta\overline{\gamma}\gamma_B|\widehat{h}_{RE}|^2) + (2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_A+\Phi^2\gamma_J+1) \\ & \quad + \sigma_e^2(\gamma_A+\gamma_B+\Phi^2\gamma_J+1)] + \widetilde{\rho}(\overline{\gamma}+1))) \\ & \quad (2\rho\zeta\overline{\gamma}|h_{AR}|^2\left(\Phi^2\gamma_J+1\right) + \widetilde{\rho}(\overline{\gamma}+1)), \end{aligned} \tag{57}$$

$$\begin{aligned} & z_{III,B}^{SC} = \\ & ((P_A|\widehat{h}_{AE}|^2) + (P_B|\widehat{h}_{BE}|^2 + P_J|\widehat{h}_{JE}|^2 \\ & \quad + \sigma_e^2(P_A+P_B+P_J) + \sigma^2)) \\ & (2\rho\zeta\overline{\gamma}|h_{BR}|^2\left(\Phi^2\gamma_J+1\right) + \widetilde{\rho}(\overline{\gamma}+1)), \end{aligned} \tag{58}$$

$$\frac{w_{III}^{SC}}{z_{III}^{SC}} = \begin{cases} \dfrac{w_{III,A}^{SC} w_{III,B}^{SC}}{z_{III,A}^{SC} z_{III,B}^{SC}}, & C_{S,A} \geq 0 \text{ and } C_{S,B} \geq 0 \\ \dfrac{w_{III,A}^{SC}}{z_{III,A}^{SC}}, & C_{S,A} \geq 0 \text{ and } C_{S,B} < 0 \\ \dfrac{w_{III,B}^{SC}}{z_{III,B}^{SC}}, & C_{S,A} < 0 \text{ and } C_{S,B} \geq 0 \\ 0, & C_{S,A} < 0 \text{ and } C_{S,B} < 0, \end{cases} \tag{59}$$

and $(.)_{III}^{SC}$ denotes the third case with SC at the eavesdropper.

3.2.4. Case IV: $SNR_{E,A}^{(1)} \leq SNR_{E,A}^{(2)}$ and $SNR_{E,B}^{(1)} \leq SNR_{E,B}^{(2)}$

In this case, the secrecy capacity is

$$\begin{aligned} C_S =& C_{S,A} + C_{S,B} \\ =& \frac{T}{2}\log_2\left(\frac{1+SNR_A}{1+SNR_{E,A}^{(2)}}\right) + \frac{T}{2}\log_2\left(\frac{1+SNR_B}{1+SNR_{E,B}^{(2)}}\right), \\ =& \frac{T}{2}\log_2\left(\frac{w_{IV,A}^{SC}}{z_{IV,A}^{SC}}\right) + \frac{T}{2}\log_2\left(\frac{w_{IV,B}^{SC}}{z_{IV,B}^{SC}}\right), \\ =& \frac{T}{2}\log_2\left(\frac{w_{IV}^{SC}}{z_{IV}^{SC}}\right), \end{aligned} \tag{60}$$

where

$$\begin{aligned} & w_{IV,A}^{SC} = \\ & ((2\rho\zeta\overline{\gamma}\gamma_B|h_{AR}|^2) + (2\rho\zeta\overline{\gamma}|h_{AR}|^2\left(\Phi^2\gamma_J+1\right) + \widetilde{\rho}(\overline{\gamma}+1))) \\ & (2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_A+\Phi^2\gamma_J+1) + \sigma_e^2(\gamma_A+\gamma_B+\Phi^2\gamma_J+1)] \\ & \quad + \widetilde{\rho}(\overline{\gamma}+1)), \end{aligned} \tag{61}$$

$$\begin{aligned} & w_{IV,B}^{SC} = \\ & ((2\rho\zeta\overline{\gamma}\gamma_A|h_{BR}|^2) + (2\rho\zeta\overline{\gamma}|h_{BR}|^2\left(\Phi^2\gamma_J+1\right) + \widetilde{\rho}(\overline{\gamma}+1))) \\ & (2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_B+\Phi^2\gamma_J+1) + \sigma_e^2(\gamma_A+\gamma_B+\Phi^2\gamma_J+1)] \\ & \quad + \widetilde{\rho}(\overline{\gamma}+1)), \end{aligned} \tag{62}$$

$$\begin{aligned} & z_{IV,A}^{SC} = \\ & ((2\rho\zeta\overline{\gamma}\gamma_B|\widehat{h}_{RE}|^2) + (2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_A+\Phi^2\gamma_J+1) \\ & \quad + \sigma_e^2(\gamma_A+\gamma_B+\Phi^2\gamma_J+1)] + \widetilde{\rho}(\overline{\gamma}+1))) \\ & \quad (2\rho\zeta\overline{\gamma}|h_{AR}|^2\left(\Phi^2\gamma_J+1\right) + \widetilde{\rho}(\overline{\gamma}+1)), \end{aligned} \tag{63}$$

$$\begin{aligned} & z_{IV,B}^{SC} = \\ & ((2\rho\zeta\overline{\gamma}\gamma_A|\widehat{h}_{RE}|^2) + (2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_B+\Phi^2\gamma_J+1) \\ & \quad + \sigma_e^2(\gamma_A+\gamma_B+\Phi^2\gamma_J+1)] + \widetilde{\rho}(\overline{\gamma}+1))) \\ & \quad (2\rho\zeta\overline{\gamma}|h_{BR}|^2\left(\Phi^2\gamma_J+1\right) + \widetilde{\rho}(\overline{\gamma}+1)), \end{aligned} \tag{64}$$

$$\frac{w_{IV}^{SC}}{z_{IV}^{SC}} = \begin{cases} \dfrac{w_{IV,A}^{SC} w_{IV,B}^{SC}}{z_{IV,A}^{SC} z_{IV,B}^{SC}}, & C_{S,A} \geq 0 \text{ and } C_{S,B} \geq 0 \\ \dfrac{w_{IV,A}^{SC}}{z_{IV,A}^{SC}}, & C_{S,A} \geq 0 \text{ and } C_{S,B} < 0 \\ \dfrac{w_{IV,B}^{SC}}{z_{IV,B}^{SC}}, & C_{S,A} < 0 \text{ and } C_{S,B} \geq 0 \\ 0, & C_{S,A} < 0 \text{ and } C_{S,B} < 0, \end{cases} \tag{65}$$

and $(.)_{IV}^{SC}$ denotes the fourth case with SC at the eavesdropper.

4. Optimization Problem Formulation

The secrecy capacity optimization problem for MRC and SC at the eavesdropper is

$$\min_{\rho,\widetilde{\rho},P_A,P_B,P_J} \quad \frac{z}{w} \tag{66}$$

$$\text{s.t} \quad P_A + P_B + P_J \leq P_T \tag{67}$$

$$\rho + \widetilde{\rho} \leq 1 \tag{68}$$

$$\rho, \widetilde{\rho}, P_A, P_B, P_J \geq 0 \tag{69}$$

where w and z are defined below for each diversity scheme. We exploited the structure of this problem and made use of geometric programming (GP) to jointly optimize the time switching ratio for energy harvesting and the power allocation to the users and jammer to maximize the secrecy capacity.

The standard form of a GP problem is [72]

$$\min \quad f_0(x) \tag{70}$$

$$\text{s.t} \quad f_i(x) \leq 0, i = 1, \ldots, m, \tag{71}$$

$$g_i(x) = 0, i = 1, \ldots, p, \tag{72}$$

where $f_i(x)$ is a posynomial function, $g_i(x)$ is a monomial function, and x is an optimization variable. A monomial function g of x is a real-valued function of the form $g(x) = cx_1^{a_1}x_2^{a_2}\ldots x_n^{a_n}$, where $c > 0$, $a_i \in \mathbf{R}$, and n is the number of optimization variables. A posynomial function is the sum of two or more monomials such that $f(x) = \sum_{k=1}^{K} c_k x_1^{a_{1k}} x_2^{a_{2k}} \ldots x_n^{a_{nk}}$, where $c_k > 0$ and K is the number of monomial functions.

The constraints in (67) and (68) are posynomials. This problem can be transformed into GP form and then into a convex problem because the constraints and the objective function are posynomials. However, the objective function is the ratio of two posynomials, so it cannot be transformed into GP form. To solve this problem, $w(\rho, \widetilde{\rho}, P_A, P_B, P_J)$ is approximated as a monomial function using the single condensation method (SCM) [72]. In the SCM, the denominator of the ratio of posynomials is approximated with a monomial function. The numerator (a posynomial) is not approximated, hence the term single. In the optimization problem, $w(\mathbf{x}) = \sum_i u_i(\mathbf{x})$, where $\mathbf{x} = \left[\rho, \widetilde{\rho}, P_A, P_B, P_J\right]^T$ is the sum of i monomials, so it is a posynomial by definition. The monomial approximation of $w(\mathbf{x})$ using the SCM is

$$\overline{w}(\mathbf{x}) = \prod_i \left(\frac{u_i(\mathbf{x})}{\alpha_i}\right)^{\alpha_i}, \tag{73}$$

such that $w(\mathbf{x}) \geq \overline{w}(\mathbf{x})$. For a given $\mathbf{x}$, $\alpha_i \ \forall i$ are obtained in $w(\mathbf{x})$ so that

$$\alpha_i = \frac{u_i(\mathbf{x})}{w(\mathbf{x})}, \tag{74}$$

and $\overline{w}(\mathbf{x})$ is substituted for $w(\mathbf{x})$ in (66). The objective function after the SCM approximation is a polynomial (posynomial). The key to solving a GP efficiently is to convert it to a nonlinear, but convex optimization problem, which is a problem with a convex objective function, convex inequality constraints, and linear equality constraints. A logarithmic change of variables and a logarithmic transformation of the objective function and constraints are used to obtain a GP form. The resulting problem is convex and can be solved efficiently using CVX [72]. As the optimal solution may be far from the initial guess $\mathbf{x}_0$ used in the SCM approximation, an iterative approach is used to solve this problem.

For MRC at the eavesdropper, the initial guess is used to calculate $SNR_{E,A}^{(1)}$, $SNR_{E,A}^{(2)}$, $SNR_{E,B}^{(1)}$, and $SNR_{E,B}^{(2)}$ given by (8), (25), (9), and (27), respectively. $SNR_{E,A}^{(1)}$, $SNR_{E,A}^{(2)}$, $SNR_{E,B}^{(1)}$, and $SNR_{E,B}^{(2)}$ are then substituted in (29) along with SNR_A from (18) and SNR_B from (20) to calculate $C_{S,A}$ and $C_{S,B}$, respectively. Then, $C_{S,A}$ and $C_{S,B}$ are compared to determine which case in Section 3.1 to employ, and $\mathbf{x}_0$ is used to obtain $C_{S,A}$ and $C_{S,B}$. Next, $w_{(.)}^{MRC}$ is approximated using the SCM, and the resulting $\overline{w}_{(.)}^{MRC}(\mathbf{x})$ is used in (66) to solve the optimization problem. If the current optimal solution, $\mathbf{x}_{k+1}$ satisfies the initial assumption $C_{S,A} \geq 0$ and $C_{S,B} \geq 0$, then $\mathbf{x}_{k+1}$ is used to calculate $\overline{w}(\mathbf{x}_{k+1})$, and the optimization problem is solved again. If $\mathbf{x}_{k+1}$ violates $C_{S,A} \geq 0$ and $C_{S,B} \geq 0$, then proceed to the next case. The algorithm to obtain the optimal values $\left[\rho^*, \widetilde{\rho}^*, P_A^*, P_B^*, P_J^*\right]^T$ is summarized in Algorithm 1.

For SC at the eavesdropper, the initial guess is used to calculate $SNR_{E,A}^{(1)}$, $SNR_{E,A}^{(2)}$, $SNR_{E,B}^{(1)}$, and $SNR_{E,B}^{(2)}$ given by (8), (25), (9), and (27), respectively. The values of $SNR_{E,A}^{(1)}$ and $SNR_{E,A}^{(2)}$ are compared to determine which expression for $C_{S,A}$ to consider, and the values of $SNR_{E,B}^{(1)}$ and $SNR_{E,B}^{(2)}$ are compared to determine which expression for $C_{S,B}$ to consider. These results determine which case in Section 3.2 to employ. $\mathbf{x}_0$ is then used to calculate the values of $C_{S,A}$ and $C_{S,B}$. Next, $w_{(.)}^{SC}$ is approximated using the SCM method, and the resulting $\overline{w}_{(.)}^{SC}(\mathbf{x})$ is used in (66) to solve the optimization problem. If the current optimal solution, $\mathbf{x}_{k+1}$, satisfies the initial assumption $C_{S,A} \geq 0$ and $C_{S,B} \geq 0$, then $\mathbf{x}_{k+1}$ is used to calculate $\overline{w}(\mathbf{x}_{k+1})$, and the optimization problem is solved again. If $\mathbf{x}_{k+1}$ violates $C_{S,A} \geq 0$ and $C_{S,B} \geq 0$, then proceed to the next case. The algorithm to obtain the optimal values $\left[\rho^*, \widetilde{\rho}^*, P_A^*, P_B^*, P_J^*\right]^T$ is summarized in Algorithm 2.

Algorithm 1: Optimization of the secrecy capacity, C_S, for MRC at the eavesdropper.

Require: Channel coefficients, power constraint P_T, energy conversion efficiency ζ, noise variance σ^2, tolerance ϵ, estimation error variance σ_e^2, $k = 1$

1: **while** $|C_{S,k} - C_{S,k-1}| > \epsilon$ **do**
2: Calculate the monomial approximation $\overline{w}$ for w using the single condensation method at $\mathbf{x} = \left[\rho_k, \widetilde{\rho}_k, P_{A,k}, P_{B,k}, P_{J,k}\right]^T$
3: $k = k + 1$
4: Solve the optimization problem in (66) using $\overline{w}$ to find $\left[\rho_{k+1}, \widetilde{\rho}_{k+1}, P_{A,k+1}, P_{B,k+1}, P_{J,k+1}\right]$
5: Using the solution in Step 4, calculate $C_{S,A}$ and $C_{S,B}$
6: **if** $C_{S,A} \geq 0$ and $C_{S,B} \geq 0$ **then**
7: Go to Step 1
8: **else**
9: Continue to the next case of $C_{S,A}$ and $C_{S,B}$
10: **end if**
11: Solve the optimization problem in (32) to obtain $\left[\rho_k, \widetilde{\rho}_k, P_{A,k}, P_{B,k}, P_{J,k}\right]$
12: **end while**
13: Assign $\left[\rho^*, \widetilde{\rho}^*, P_A^*, P_B^*, P_J^*\right]^T = \left[\rho_k, \widetilde{\rho}_k, P_{A,k}, P_{B,k}, P_{J,k}\right]^T$ and $C_S = C_{S,k}$

Algorithm 2: Optimization of the secrecy capacity, C_S, for SC at the eavesdropper.

Require: Channel coefficients, power constraint P_T, energy conversion efficiency ζ, noise variance σ^2, tolerance ϵ, estimation error variance σ_e^2, $k = 1$
while $|C_{S,k} - C_{S,k-1}| > \epsilon$ **do**
Calculate $SNR_{E,A}^{(1)}$, $SNR_{E,A}^{(2)}$, $SNR_{E,B}^{(1)}$, and $SNR_{E,B}^{(2)}$
if $SNR_{E,A}^{(1)} \geq SNR_{E,A}^{(2)}$ and $SNR_{E,B}^{(1)} \geq SNR_{E,B}^{(2)}$ **then**
Calculate the monomial approximation $\overline{w}$ for w using the single condensation method at $\mathbf{x} = \left[\rho_k, \widetilde{\rho}_k, P_{A,k}, P_{B,k}, P_{J,k}\right]^T$
$k = k + 1$
Solve the optimization problem in (66) using $\overline{w}$ to find $\left[\rho_{k+1}, \widetilde{\rho}_{k+1}, P_{A,k+1}, P_{B,k+1}, P_{J,k+1}\right]$
Using the solution in Step 6, calculate $C_{S,A}$ and $C_{S,B}$
if $C_{S,A} \geq 0$ and $C_{S,B} \geq 0$ **then**
Go to Step 1
else
Continue to the next case of $C_{S,A}$ and $C_{S,B}$
end if
else
Continue to the next case of $SNR_{E,A}^{(1)} \gtrless SNR_{E,A}^{(2)}$ and $SNR_{E,B}^{(1)} \gtrless SNR_{E,B}^{(2)}$
end if
Solve the optimization problem in (32) to obtain $\left[\rho_k, \widetilde{\rho}_k, P_{A,k}, P_{B,k}, P_{J,k}\right]$
end while
Assign $\left[\rho^*, \widetilde{\rho}^*, P_A^*, P_B^*, P_J^*\right]^T = \left[\rho_k, \widetilde{\rho}_k, P_{A,k}, P_{B,k}, P_{J,k}\right]^T$ and $C_S = C_{S,k}$

5. Results and Discussion

In this section, the secrecy capacity is evaluated for a two-way relay network with a friendly jammer in the presence of an eavesdropper. Users A and B can only communicate through R since there is no direct link between them. The simulation parameters were as follows, unless noted otherwise. The noise variance was $\sigma^2 = 10^{-3}$, $\sigma_e^2 = 0.1$, $T = 1$; the optimization tolerance was $\epsilon = 0.001$, $\Phi = 0$; the energy conversion efficiency was $\zeta = 0.5$. The channel gains $|h_{AR}|^2$, $|h_{JR}|^2$, $|h_{JE}|^2$, and $|h_{BR}|^2$ are exponential random variables with mean $\lambda = 1$, $|h_{RE}|^2$ and $|h_{BE}|^2$ are exponential random variables with mean λ_{Eve}; $|h_{AE}|^2$ is an exponential random variable with mean $\frac{1}{\lambda_{Eve}}$, $\lambda_{Eve} \in \{1, 2, 3\}$. The node locations were normalized to the distance between A and B so that A and B were at (0, 0) and (1, 0), respectively. R is at the midpoint, (0.5, 0); J is at (0.5, -0.5); $P_T = 10$ dB, and $P_J = 0.1 P_T$.

Figure 3 presents the secrecy capacity versus the total transmit power, P_T, for $\lambda_{Eve} = 1$, 2, and 3 with SC and MRC at the eavesdropper. The secrecy capacity increases in all cases as the total transmit power increases. The secrecy capacity of SC outperforms MRC for all values of λ_{Eve}. The reason is that SC selects only one wiretapped link, which reduces the SNR at the eavesdropper. As a result, the secrecy capacity of the network with SC at the eavesdropper is higher than that with MRC. The effect of increasing λ_{Eve} on the secrecy capacity of SC and MRC is negligible except for MRC with $P_T \leq 8$ dB. This is because increasing λ_{Eve} improves the corresponding link of the eavesdropper, but degrades the other eavesdropper link given the total transmit power P_T.

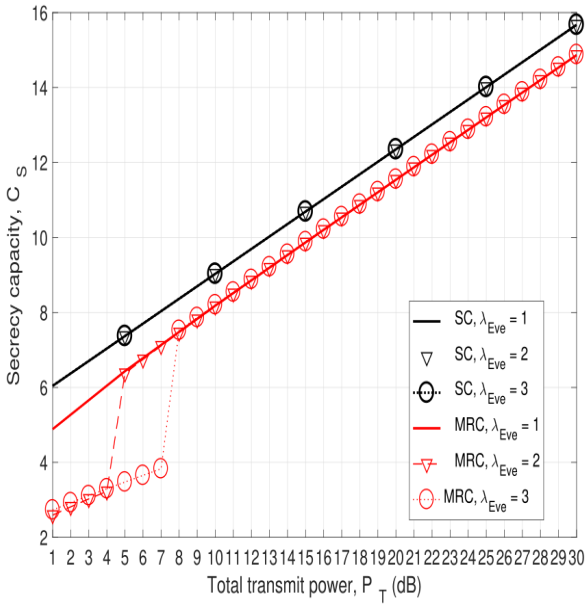

Figure 3. The secrecy capacity versus the total transmit power, P_T, with $\lambda_{Eve} = 1$ and $\sigma_e^2 = 0$.

Figure 4 presents the secrecy capacity versus the time switching ratio, ρ, with SC and MRC for $\sigma_e^2 = 0$ and 0.1. This shows that SC outperforms MRC for the given values of σ_e^2 and λ_{Eve}, and the secrecy capacity for imperfect CSI, $\sigma_e^2 = 0.1$, is better than that for perfect CSI, $\sigma_e^2 = 0$, for all values of ρ. Considering the SNR expressions of the eavesdropper links, the denominators of (8), (25), (9), and (27) contain σ_e^2, so increasing this term reduces the SNR at E. These results also show that the secrecy capacity increases as ρ increases until it reaches an optimal value, and then, the secrecy capacity decreases. As the time switching ratio increases, the relay harvests more energy for signal forwarding in the second phase. However, a larger ρ means the eavesdropper has more time to overhear the transmitted signals, so there is a tradeoff.

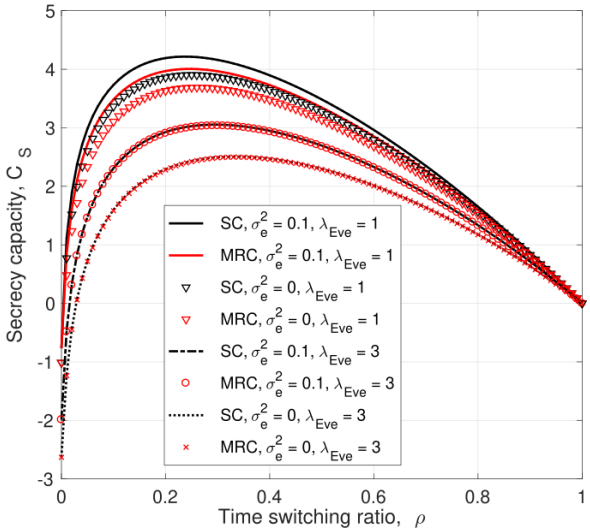

Figure 4. The secrecy capacity versus the time switching ratio, ρ, for different values of λ_{Eve} and σ_e^2 with $P_J = 0.1P_T$ and $P_T = 10$ dB.

5.1. Channel Estimation Error

Figures 5 and 6 present the effect of the channel estimation error variance, σ_e^2, on the secrecy capacity. Figure 5 shows the secrecy capacity for $\lambda_{Eve} = 1, 2$, and 3. A higher value of σ_e^2 means that the eavesdropper is less able to estimate the wiretap links, so the secrecy capacity improves. The differences in secrecy capacity between SC and MRC are

0.14, 0.023, and 0.014 bits/sec/channel use for $\lambda_{Eve} = 1, 2$, and 3, respectively, at $\sigma_e^2 = 0.1$. Thus, increasing λ_{Eve} decreases the gap between SC and MRC. This is because a larger λ_{Eve} improves the corresponding link of the eavesdropper, but degrades the other eavesdropper link.

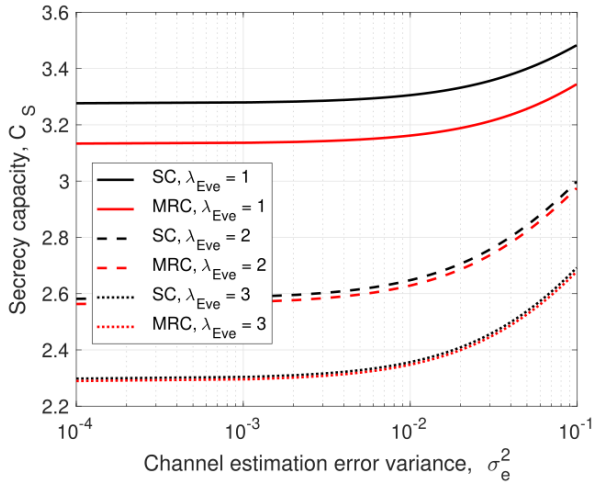

Figure 5. The secrecy capacity versus the channel estimation error variance, σ_e^2, for three values of λ_{Eve} with $\rho = 0.5$, $P_J = 0.1P_T$, and $P_T = 10$ dB.

Figure 6 shows the secrecy capacity versus the channel estimation error variance for $\rho = 0.8$ and 0.2 with $\lambda_{Eve} = 1$. At $\sigma_e^2 = 0.01$, SC outperforms MRC with a difference of 0.057 at $\rho = 0.8$ and 0.23 at $\rho = 0.2$. Thus, decreasing ρ improves the performance of SC and MRC, but does not have a significant effect on the difference between them. As ρ increases, the relay harvests more energy, so there is more transmit power at the relay. This improves the received SNR at the users.

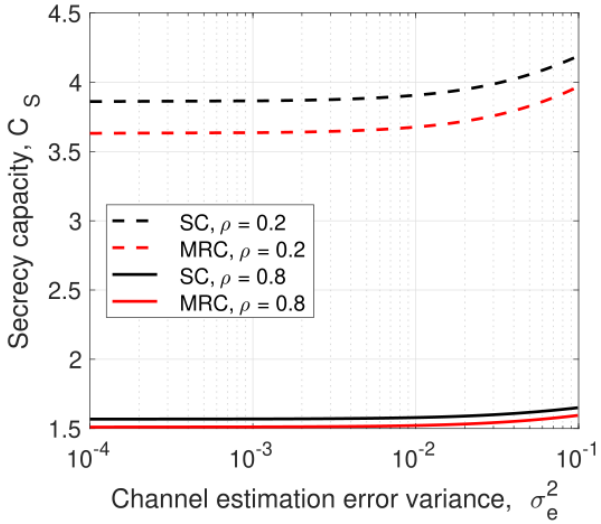

Figure 6. The secrecy capacity versus the channel estimation error variance, σ_e^2, with $\rho = 0.8$ and 0.2, $\lambda_{Eve} = 1$, $P_J = 0.1P_T$, and $P_T = 10$ dB.

5.2. Jammer, Cancellation Factor, and Locations

The secrecy capacity versus the jamming signal cancellation factor, Φ, is given in Figure 7 for $\sigma_e^2 = 0$ and 0.5. This shows that SC outperforms MRC for both values of σ_e^2. When $\Phi = 0$, the secrecy capacity is highest because the jamming signal at the relay is completely cancelled. As Φ increases, more jamming power is amplified and forwarded to A and B. Thus, the noise at A and B increases, which degrades their SNRs and, so, decreases

the secrecy capacity. The difference in secrecy capacity with SC is 0.93 bits/sec/channel use at $\Phi = 0.1$, and this decreases to 0.74 bits/sec/channel use at $\Phi = 0.8$.

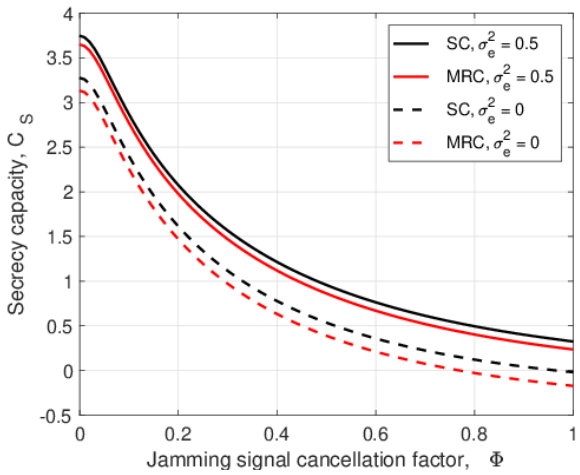

Figure 7. The secrecy capacity versus the jamming signal cancellation factor, Φ, with $\lambda_{Eve} = 1$, $\theta = 0.5$, $P_T = 10$ dB, and $P_J = 0.1P_T$.

In the following figures, the secrecy capacity is considered for different locations of the eavesdropper and jammer. The channel links can be expressed as $h_{ij} = \frac{f_{ij}}{d_{ij}^m}$, where f_{ij} is an exponential random variable with mean $= 1$, $m = 2.7$ is the path loss exponent, and d_{ij} is the distance between i and j. Figures 8 and 9 present the secrecy capacity versus Φ for SC and MRC at the eavesdropper, respectively. The jammer is at $(0.5, -0.5)$, and the location of the eavesdropper is $(0.5, -1)$ and $(0.2, -0.2)$ with $d_{AE} = 1.12$ and 0.28, respectively. These results show that the secrecy capacity increases as d_{AE} increases from 0.28 to 1.12 for both values of σ_e^2. The reason is that, as d_{AE} increases, less power is required to be allocated to the jammer. Hence, more power is allocated to A and B, and more energy is harvested at R. Figure 8 shows that, when $\sigma_e^2 = 0$, the difference in SC secrecy capacity for $d_{AE} = 1.12$ and 0.28 is 0.53 bit/sec/channel use, and this increases to 0.57 bit/sec/channel use for $\sigma_e^2 = 0.1$. Figure 9 shows that, when $\sigma_e^2 = 0$, the difference in MRC secrecy capacity for $d_{AE} = 1.12$ and 0.28 is 0.51 bit/sec/channel use, and this increases to 0.62 bit/sec/channel use for $\sigma_e^2 = 0.1$.

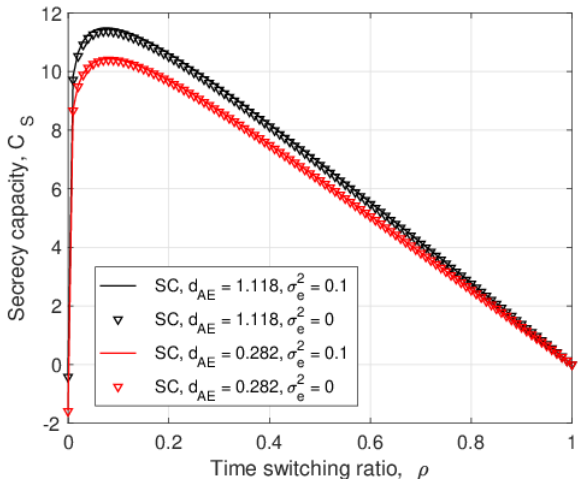

Figure 8. The secrecy capacity for SC at the eavesdropper with $d_{AE} = 0.28$ and 1.12, $\lambda_{Eve} = 1$, $P_T = 10$ dB, and $P_J = 0.1P_T$.

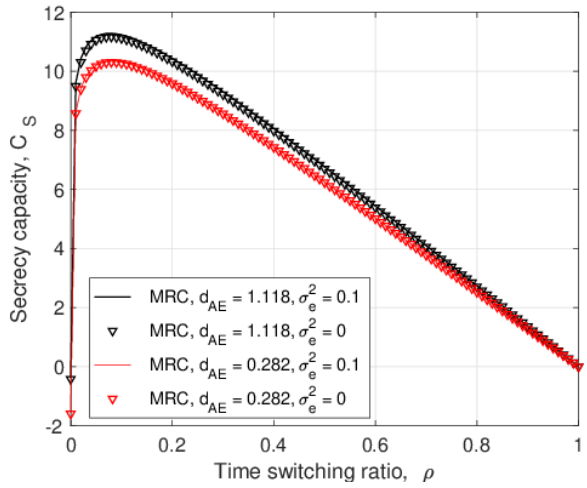

Figure 9. The secrecy capacity for MRC at the eavesdropper with $d_{AE} = 0.28$ and 1.12, $\lambda_{Eve} = 1$, $P_T = 10$ dB, and $P_J = 0.1P_T$.

Figure 10 presents the effect of Φ on the secrecy capacity when the jammer is close to the relay. In this case, E is at $(0.2, -1)$ and J is at $(0.5, -0.1)$, so significant jamming power is received by the relay. These results show that a small increase in Φ causes a significant drop in secrecy capacity for both SC and MRC. For example, with SC and $\rho = 0.5$, the secrecy capacity for SC drops by 2.74 bit/sec/channel use when Φ increases from 0 to 0.01 and by 3.17 bit/sec/channel use when Φ increases from 0.01 to 0.1. This is because the jamming signal at the relay is larger as the jammer is closer to the relay.

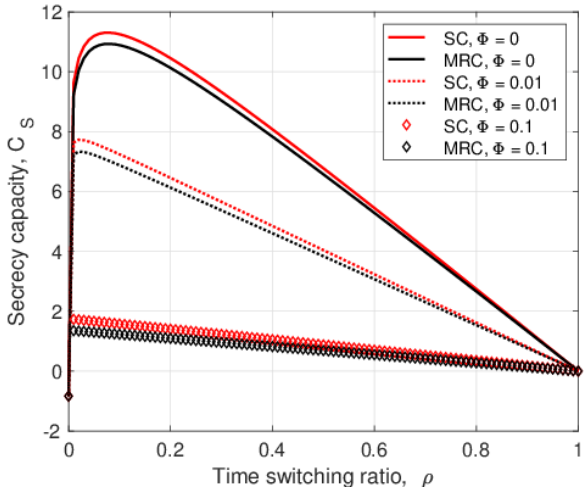

Figure 10. The secrecy capacity for different values of Φ with the jammer at $(0.5, -0.1)$, the eavesdropper at $(0.2, -1)$, $\lambda_{Eve} = 1$, $P_T = 10$ dB, and $P_J = 0.1P_T$.

Figure 11 shows the secrecy capacity versus the x-axis location of the eavesdropper (employing MRC), when the jammer is located at $(0.5, -0.5)$ and without a jammer. Results are given for y-axis eavesdropper positions -0.2, -0.5, and -0.8 and MRC at the eavesdropper. The solid lines are for the case with a jammer at $(0.5, -0.5)$, and the other lines correspond to no jammer. When the eavesdropper is at $x = 0.5$, i.e., midway between A and B, the secrecy capacity is the highest. This is because the maximum eavesdropper SNR from A and B will be smallest at this point. Further, the secrecy capacity is better with a jammer since the jamming signal reduces the SNR at the eavesdropper regardless of their y-axis position. The lowest secrecy capacity in both cases (with and without a jammer) is when the eavesdropper is at $x = 0$ and $x = 1$ since the SNR at the eavesdropper from A and B, respectively, is highest.

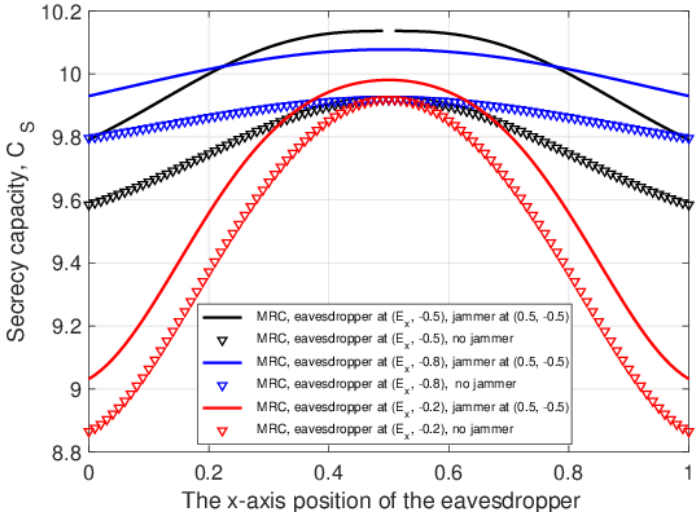

Figure 11. The secrecy capacity versus the x-axis location of the eavesdropper (employing MRC), with a jammer at a fixed location and without a jammer.

Figure 12 presents the secrecy capacity versus the x-axis position of the eavesdropper (employing MRC), with the jammer located at $(0.5, -0.5)$, $(0.5, -1)$, $(0.2, -0.5)$, $(0.2, -1)$, $(0.7, -0.5)$, and $(0.7, -1)$. The location of the eavesdropper changes from $(0, -0.7)$ to $(1, -0.7)$. In all cases, the secrecy capacity is a minimum when the eavesdropper is at $x = 0$ or $x = 1$, which is closest to A or B, respectively. As the eavesdropper moves from $x = 0$ to 1, the jamming signal power at the eavesdropper increases and the secrecy capacity increases. Then, the secrecy capacity decreases as the eavesdropper moves farther from the jammer after the maximum secrecy capacity has been reached.

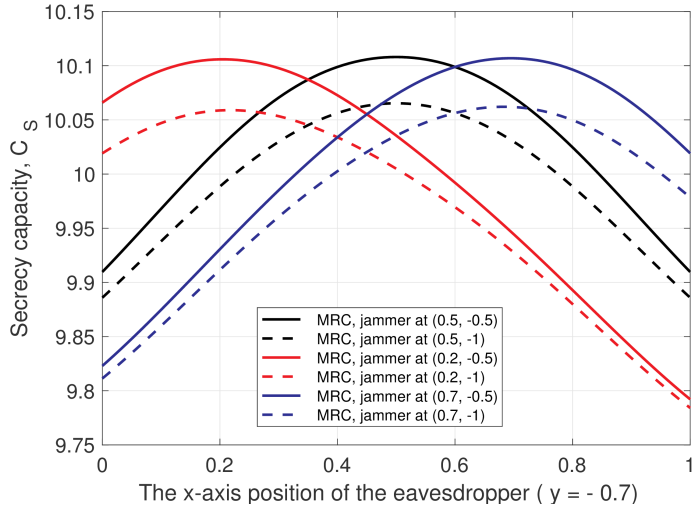

Figure 12. The secrecy capacity versus the x-axis location of the eavesdropper (employing MRC), for different jammer locations with $\sigma_e^2 = 0$, $\Phi = 0$, and $P_T = 10$ dB.

5.3. Computational Complexity

Matlab R2017a on a MacBook Pro laptop with an Intel Core i5 processor was used to obtain the simulation results. The average time to run Algorithm 1 (MRC) was 7.89 s and to run Algorithm 2 (SC) was 1.56 s. One reason for this difference is that an iteration of Algorithm 1 requires 648 arithmetic operations, while an iteration of Algorithm 2 requires 318 operations. This is because the number of monomial terms to be approximated with Algorithm 1 is 40, but only 12 with Algorithm 2. Furthermore, the average number of iterations required to solve the optimization problem for Algorithm 1 was 2.63 s and for Algorithm 2 was 1.81 s.

6. Conclusions

In this paper, the secrecy capacity was investigated for a two-way energy-constrained time-switching relay network in the presence of an eavesdropper. A friendly jammer was used to reduce the ability of the eavesdropper to intercept the user signals. The secrecy capacity was maximized by jointly optimizing the time switching ratio, ρ, and the transmit power of the two users, A and B, and the jammer J. The single condensation method (SCM) was employed to convert the objective function of the corresponding optimization problem into a posynomial form suitable for geometric programming (GP). Then, GP was used to transform the non-convex objective function to obtain a convex optimization problem. Two diversity combining techniques, MRC and SC, were employed at the eavesdropper. Imperfect cancellation of the jamming signal at the relay was also considered. Results were presented that showed that the imperfect jamming signal cancellation at the relay degrades the secrecy capacity. In addition, utilizing a jammer improves the secrecy capacity and increases the amount of harvested energy at the relay. Further, the secrecy capacity is higher if the jammer is located closer to the eavesdropper. Imperfect channel estimation at the eavesdropper was also investigated. It was shown that, as the estimation error increases, the secrecy capacity improves. MRC has been shown to provide a lower secrecy capacity than SC. Thus, to achieve the SC secrecy capacity with MRC at the eavesdropper, a higher SNR is required at A and B.

Author Contributions: Conceptualization, M.H. and T.A.G.; methodology, M.H. and T.A.G.; software, M.H.; validation, M.H. and T.A.G.; formal analysis, M.H.; investigation, M.H.; resources, T.A.G.; writing—original draft preparation, M.H.; writing—review and editing, T.A.G.; visualization, M.H.; supervision, T.A.G.; project administration, T.A.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

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

Abbreviations

Symbol	Description
A, B	Users
R	Relay
J	Jammer
E	Eavesdropper
h_{ij}	Channel between node i and node j
$\|h_{ij}\|^2$	Channel gain between node i and node j
$\widehat{h}_{iE}$	Estimated channel between E and node i
$\|\widehat{h}_{iE}\|^2$	Estimated channel gain between E and node i
e_{iE}	Channel estimation error between E and node i
σ_e^2	Channel estimation error variance
n_i	Additive white Gaussian noise (AWGN) at node i
σ^2	AWGN variance
x_i	Signal transmitted by node i
y_i	Signal received at node i
P_A	Transmit power of node A
P_B	Transmit power of node B
P_R	Transmit power of node R
P_J	Transmit power of node J
P_T	Total power constraint
$\mathbf{E}[.]$	Expected value
y_{Re}	Energy harvesting signal at the relay
y_{Ri}	Information retrieval signal at the relay
ρ	Time switching (TS) ratio

E_H	Harvested energy
ζ	Energy conversion efficiency
T	Total transmission time
m	Path loss exponent
Φ	Jamming signal cancellation factor
y_R	Information retrieval signal after jamming cancellation
$y_E^{(1)}$	Received signal at E in the first phase
$y_E^{(2)}$	Received signal at E in the second phase
$SNR_{E,A}^{(1)}$	SNR at E for x_B sent to A in the first phase
$SNR_{E,B}^{(1)}$	SNR at E for x_A sent to B in the first phase
$SNR_{E,A}^{(2)}$	SNR at E for x_B sent to A in the second phase
$SNR_{E,B}^{(2)}$	SNR at E for x_A sent to B in the second phase
SNR_A	SNR at A
SNR_B	SNR at B
R_A	Achievable rate at A
R_B	Achievable rate at B
$R_E^{(1)}$	Achievable rate at E in the first phase
$R_E^{(2)}$	Achievable rate at E in the second phase
R_E	Achievable rate at E for both phases
C_A	Secrecy capacity at A
C_B	Secrecy capacity at B
C_S	Secrecy capacity

References

1. Ahmed, I.; Butt, M.M.; Psomas, C.; Mohamed, A.; Krikidis, I.; Guizani, M. Survey on energy harvesting wireless communications: Challenges and opportunities for radio resource allocation. *Comput. Netw.* **2015**, *88*, 234–248. [CrossRef]
2. Nguyen, L.D. Resource allocation for energy efficiency in 5G wireless networks. *EAI Trans. Ind. Netw. Intell. Syst.* **2018**, *5*, e1. [CrossRef]
3. Babayo, A.A.; Anisi, M.H.; Ali, I. A review on energy management schemes in energy harvesting wireless sensor networks. *Renew. Sustain. Energy Rev.* **2017**, *76*, 1176–1184. [CrossRef]
4. Varshney, L.R. Transporting information and energy simultaneously. In Proceedings of the IEEE International Symposium on Information Theory, Toronto, ON, Canada, 6–11 July 2008; pp. 1612–1616.
5. Kazmi, S.A.A.; Coleri, S. Optimization of full-duplex relaying system with non-linear energy harvester. *IEEE Access* **2020**, *8*, 201566–201576. [CrossRef]
6. Perera, T.D.P.; Jayakody, D.N.K.; Sharma, S.K.; Chatzinotas, S.; Li, J. Simultaneous wireless information and power transfer (SWIPT): Recent advances and future challenges. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 264–302. [CrossRef]
7. Dang-Ngoc, H.; Ho-Van, K.; Do-Dac, T. Secrecy analysis of overlay mechanism in radio frequency energy harvesting networks with jamming under Nakagami-m fading. *Wirel. Pers. Commun.* **2021**, *120*, 447–479. [CrossRef]
8. Zhang, R.; Ho, C.K. MIMO broadcasting for simultaneous wireless information and power transfer. *IEEE Trans. Wirel. Commun.* **2013**, *12*, 1989–2001. [CrossRef]
9. Jang, H.H.; Choi, K.W.; Kim, D.I. Novel frequency splitting SWIPT for overcoming amplifier nonlinearity. *IEEE Wireless Commun. Lett.* **2020**, *9*, 826–829. [CrossRef]
10. Tedeschi, P.; Sciancalepore, S.; Di Pietro, R. Security in energy harvesting networks: A survey of current solutions and research challenges. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2658–2693. [CrossRef]
11. Grover, P.; Sahai, A. Shannon meets Tesla: Wireless information and power transfer. In Proceedings of the IEEE International Symposium on Information Theory, Austin, TX, USA, 13–18 June 2010; pp. 2363–2367.
12. Hossain, M.A.; Noor, R.M.; Yau, K.L.A.; Ahmedy, I.; Anjum, S.S. A survey on simultaneous wireless information and power transfer with cooperative relay and future challenges. *IEEE Access* **2019**, *7*, 19166–19198. [CrossRef]
13. Liu, L.; Zhang, R.; Chua, K.C. Wireless information transfer with opportunistic energy harvesting. *IEEE Trans. Wireless Commun.* **2013**, *12*, 288–300. [CrossRef]
14. 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]

15. Nasir, A.A.; Zhou, X.; Durrani, S.; Kennedy, R.A. Relaying protocols for wireless energy harvesting and information processing. *IEEE Trans. Wireless Commun.* **2013**, *12*, 3622–3636. [CrossRef]
16. Ju, M.; Kang, K.M.; Hwang, K.S.; Jeong, C. Maximum transmission rate of PSR/TSR protocols in wireless energy harvesting DF-based relay networks. *IEEE J. Sel. Areas Commun.* **2015**, *33*, 2701–2717. [CrossRef]
17. Di, X.; Xiong, K.; Fan, P.; Yang, H.C. Simultaneous wireless information and power transfer in cooperative relay networks with rateless codes. *IEEE Trans. Veh. Technol.* **2017**, *66*, 2981–2996. [CrossRef]
18. Atapattu, S.; Evans, J. Optimal energy harvesting protocols for wireless relay networks. *IEEE Trans. Wireless Commun.* **2016**, *15*, 5789–5803. [CrossRef]
19. Huang, S.; Yao, Y.; Feng, Z. Simultaneous wireless information and power transfer for relay assisted energy harvesting network. *Wireless Netw.* **2018**, *24*, 453–462. [CrossRef]
20. Ye, Y.; Li, Y.; Wang, D.; Zhou, F.; Hu, R.Q.; Zhang, H. Optimal transmission schemes for DF relaying networks using SWIPT. *IEEE Trans. Veh. Technol.* **2018**, *67*, 7062–7072. [CrossRef]
21. Jiang, D.; Zheng, H.; Tang, D.; Tang, Y. Relay selection and power allocation for cognitive energy harvesting two-way relaying networks. In Proceedings of the IEEE International Conference on Electronics Information and Emergency Communication, Beijing, China, 14–16 May 2015; pp. 163–166.
22. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
23. Zou, Y.; Zhu, J.; Wang, X.; Hanzo, L. A survey on wireless security: Technical challenges, recent advances, and future trends. *Proc. IEEE* **2016**, *104*, 1727–1765. [CrossRef]
24. Rodriguez, L.J.; Tran, N.H.; Duong, T.Q.; Le-Ngoc, T.; Elkashlan, M.; Shetty, S. Physical layer security in wireless cooperative relay networks: State of the art and beyond. *IEEE Commun. Mag.* **2015**, *53*, 32–39. [CrossRef]
25. Yener, A.; Ulukus, S. Wireless physical-layer security: Lessons learned from information theory. *Proc. IEEE* **2015**, *103*, 1814–1825. [CrossRef]
26. Mukherjee, A.; Fakoorian, S.A.A.; Huang, J.; Swindlehurst, A.L. Principles of physical layer security in multiuser wireless networks: A survey. *IEEE Commun. Surveys Tuts.* **2014**, *16*, 1550–1573. [CrossRef]
27. 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**, *66*, 7495–7505. [CrossRef]
28. Wang, W.; Teh, K.C.; Li, K.H. Generalized relay selection for improved security in cooperative DF relay networks. *IEEE Wireless Commun. Lett.* **2016**, *5*, 28–31. [CrossRef]
29. Pandey, A.; Yadav, S. Physical layer security for cellular multiuser two-way relaying networks with single and multiple decode-and-forward relays. *Trans. Emerg. Telecommun. Technol.* **2019**, *30*, e3639. [CrossRef]
30. Shukla, M.K.; Pandey, A.; Yadav, S.; Purohit, N. Secrecy outage analysis of full duplex cellular multiuser two-way AF relay networks. In Proceedings of the International Conference on Wireless Communications Signal Processing and Networking, Kalavakkam, Tamil Nadu, India, 21–23 March 2019; pp. 458–463.
31. Liu, Y.; Wang, L.; Duy, T.T.; Elkashlan, M.; Duong, T.Q. Relay selection for security enhancement in cognitive relay networks. *IEEE Wireless Commun. Lett.* **2015**, *4*, 46–49. [CrossRef]
32. Li, X.; Zhao, M.; Gao, X.C.; Li, L.; Do, D.T.; Rabie, K.M.; Kharel, R. Physical layer security of cooperative NOMA for IoT networks under I/Q imbalance. *IEEE Access* **2020**, *8*, 51189–51199. [CrossRef]
33. Kapetanovic, D.; Zheng, G.; Rusek, F. Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks. *IEEE Commun. Mag.* **2015**, *53*, 21–27. [CrossRef]
34. Bloch, M.; Barros, J.; Rodrigues, M.R.; McLaughlin, S.W. Wireless information-theoretic security. *IEEE Trans. Inf. Theory* **2018**, *54*, 2515–2534. [CrossRef]
35. Dong, L.; Han, Z.; Petropulu, A.P.; Poor, H.V. Improving wireless physical layer security via cooperating relays. *IEEE Trans. Signal Process.* **2010**, *58*, 1875–1888. [CrossRef]
36. Oohama, Y. Coding for relay channels with confidential messages. In Proceedings of the IEEE Information Theory Workshop, Cairns, Australia, 2–7 September 2001; pp. 87–89.
37. Son, P.N.; Kong, H.Y. Cooperative communication with energy harvesting relays under physical layer security. *IET Commun.* **2015**, *9*, 2131–2139. [CrossRef]
38. Salem, A.; Hamdi, K.A.; Rabie, K.M. Physical layer security with RF energy harvesting in AF multi-antenna relaying networks. *IEEE Trans. Commun.* **2016**, *64*, 3025–3038. [CrossRef]
39. Shannon, C.E. Two-way communication channels. In Proceedings of the Berkeley Symposium on Mathematical Statistics and Probability, Berkeley, CA, USA, 20 June–30 July 1960; pp. 611–644.
40. Rankov, B.; Wittneben, A. Achievable rate regions for the two way relay channel. In Proceedings of the IEEE International Symposium on Information Theory, Seattle, WA, USA, 9–14 July 2006; pp. 1668–1672.
41. Zhang, Y.; Zhao, X.; Xie, Y. Secure communications in SWIPT-enabled two-way relay networks. *IEEE Access* **2019**, *7*, 111890–111896. [CrossRef]
42. Zhang, J.; Tao, X.; Wu, H.; Zhang, X. Secure transmission in SWIPT-powered two-way untrusted relay networks. *IEEE Access* **2018**, *6*, 10508–10519. [CrossRef]

43. Jameel, F.; Wyne, S.; Ding, Z. Secure communications in three-step two-way energy harvesting DF relaying. *IEEE Commun. Lett.* **2018**, *22*, 308–311. [CrossRef]
44. Jameel, F.; Khan, F.; Haider, M.A.A.; Haq, A.U. On physical layer security of two way energy harvesting relays. In Proceedings of the International Conference on Frontiers of Information Technology, Islamabad, Pakistan, 18–20 December 2017; pp. 35–40.
45. Thakur, C.; Chattopadhyay, S. Secrecy performance of an improved interference-aided RF energy harvesting scheme in two-way multi-antenna relay network. In Proceedings of the IEEE Applied Signal Processing Conference, Kolkata, India, 7–9 October 2020; pp. 123–127.
46. Zheng, G.; Choo, L.C.; Wong, K.K. Optimal cooperative jamming to enhance physical layer security using relays. *IEEE Trans. Signal Process.* **2011**, *59*, 1317–1322. [CrossRef]
47. Ding, Z.; Leung, K.K.; Goeckel, D.L.; Towsley, D. Opportunistic relaying for secrecy communications: Cooperative jamming vs. relay chatting. *IEEE Trans. Wireless Commun.* **2011**, *10*, 1725–1729. [CrossRef]
48. Huang, J.; Swindlehurst, A.L. Cooperative jamming for secure communications in MIMO relay networks. *IEEE Trans. Signal Process.* **2011**, *59*, 4871–4884. [CrossRef]
49. Wang, L.; Cai, Y.; Zou, Y.; Yang, W.; Hanzo, L. 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]
50. Rajaram, A.; Jayakody, D.N.; Dinis, R.; Beko, M. Energy efficient secure communication model against cooperative eavesdropper. *Applied Sci.* **2021**, *11*, 1563. [CrossRef]
51. He, X.; Yener, A. Two-hop secure communication using an untrusted relay: A case for cooperative jamming. In Proceedings of the IEEE Global Telecommunications Conference, New Orleans, LA, USA, 30 November–4 December 2008; pp. 1–5.
52. Mamaghani, M.T.; Kuhestani, A.; Wong, K.K. Secure two-way transmission via wireless-powered untrusted relay and external jammer. *IEEE Trans. Veh. Technol.* **2018**, *67*, 8451–8465. [CrossRef]
53. Liu, M.; Liu, Y. Power allocation for secure SWIPT systems with wireless-powered cooperative jamming. *IEEE Commun. Lett.* **2017**, *21*, 1353–1356. [CrossRef]
54. Wang, Y.; Zhang, T.; Yang, W.; Yin, H.; Shen, Y.; Zhu, H. Secure communication via multiple RF-EH untrusted relays with finite energy storage. *IEEE Internet Things J.* **2020**, *7*, 1476–1487. [CrossRef]
55. Wang, K.; Yuan, L.; Miyazaki, T.; Zeng, D.; Guo, S.; Sun, Y. Strategic antieavesdropping game for physical layer security in wireless cooperative networks. *IEEE Trans. Veh. Technol.* **2017**, *66*, 9448–9457. [CrossRef]
56. Mobini, Z.; Mohammadi, M.; Tellambura, C. Wireless-powered full-duplex relay and friendly jamming for secure cooperative communications. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 621–634. [CrossRef]
57. Zhang, R.; Song, L.; Han, Z.; Jiao, B. Physical layer security for two-way untrusted relaying with friendly jammers. *IEEE Trans. Veh. Technol.* **2012**, *61*, 3693–3704. [CrossRef]
58. Jiang, X.; Li, P.; Li, B.; Zou, Y.; Wang, R. Security-reliability tradeoff for friendly jammer aided multiuser scheduling in energy harvesting communications. *Security Commun. Netw.* **2021**, *2021*, 5599334. [CrossRef]
59. Cao, K.; Wang, B.; Ding, H.; Tian, J. Adaptive cooperative jamming for secure communication in energy harvesting relay networks. *IEEE Wireless Commun. Lett.* **2019**, *8*, 1316–1319. [CrossRef]
60. Lee, K.; Hong, J.P.; Choi, H.H.; Quek, T.Q. Wireless-powered two-way relaying protocols for optimizing physical layer security. *IEEE Trans. Inf. Forens. Security* **2019**, *14*, 162–174. [CrossRef]
61. Ha, D.H.; Nguyen, T.N.; Tran, M.H.; Li, X.; Tran, P.T.; Voznak, M. Security and reliability analysis of a two-way half-duplex wireless relaying network using partial relay selection and hybrid TPSR energy harvesting at relay nodes. *IEEE Access* **2020**, *8*, 187165–187181. [CrossRef]
62. Wang, C.; Liu, T.C.K.; Dong, X. Impact of channel estimation error on the performance of amplify-and-forward two-way relaying. *IEEE Trans. Veh. Technol.* **2012**, *61*, 1197–1207. [CrossRef]
63. Huang, J.; Swindlehurst, A.L. Robust secure transmission in MISO channels based on worst case optimization. *IEEE Trans. Signal Process.* **2012**, *60*, 1696–1707. [CrossRef]
64. Chen, X.; Chen, J.; Zhang, H.; Zhang, Y.; Yuen, C. On secrecy performance of multiantenna-jammer-aided secure communications with imperfect CSI. *IEEE Trans. Veh. Technol.* **2016**, *65*, 8014–8024. [CrossRef]
65. Hayajneh, M.; Gulliver, T.A. Secrecy capacity in two-way energy harvesting relay networks with a friendly jammer. *Wireless Networks* **2021**, *27*, 4551–4566. [CrossRef]
66. Xu, J.; Liu, L.; Zhang, R. Multiuser MISO beamforming for simultaneous wireless information and power transfer. *IEEE Trans. Signal Process.* **2014**, *62*, 4798–4810 . [CrossRef]
67. Zhang, G.; Xu, J.; Wu, Q.; Cui, M.; Li, X.; Lin, F. Wireless powered cooperative jamming for secure OFDM system. *IEEE Trans. Veh. Technol.* **2018**, *67*, 1331–1346. [CrossRef]
68. Long, H.; Xiang, W.; Li, Y. Precoding and cooperative jamming in multi-antenna two-way relaying wiretap systems without eavesdropper's channel state information. *IEEE Trans. Inf. Forensics Security* **2017**, *12*, 1309–1318. [CrossRef]
69. Chen, J.; Zhang, R.; Song, L.; Han, Z.; Jiao, B. Joint relay and jammer selection for secure two-way relay networks. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 310–320. [CrossRef]
70. Leung-Yan-Cheong, S.; Hellman, M.E. The Gaussian wire-tap channel. *IEEE Trans. Inform. Theory* **1978**, *24*, 451–456. [CrossRef]

71. Wang, D.; Bai, B.; Zhao, W.; Han, Z. A survey of optimization approaches for wireless physical layer security. *IEEE Commun. Surveys Tuts.* **2019**, *21*, 1878–1911. [CrossRef]
72. Boyd, S.; Kim, S.J.; Venberghe, L.; Hassibi, A. A tutorial on geometric programming. *Optimization Eng.* **2007**, *8*, 67–127. [CrossRef]