sensors

MDPI

Article

Physical Layer Security Using Two-Path Successive Relaying

Qian Yu Liau [1,†], Chee Yen Leow [1,*,†] and Zhiguo Ding [2,†]

1 Wireless Communication Centre, Faculty of Electrical Engineering, Universiti Teknologi Malaysia, Skudai 81310, Johor, Malaysia; qianyuliau@gmail.com
2 School of Computing and Communications, Lancaster University, Lancaster, LA1 4YW, UK; z.ding@lancaster.ac.uk
* Correspondence: bruceleow@fke.utm.my; Tel.: +60-7-553-6105
† These authors contributed equally to this work.

Academic Editor: Leonhard M. Reindl
Received: 4 February 2016; Accepted: 7 April 2016; Published: 9 June 2016

Abstract: Relaying is one of the useful techniques to enhance wireless physical-layer security. Existing literature shows that employing full-duplex relay instead of conventional half-duplex relay improves secrecy capacity and secrecy outage probability, but this is at the price of sophisticated implementation. As an alternative, two-path successive relaying has been proposed to emulate operation of full-duplex relay by scheduling a pair of half-duplex relays to assist the source transmission alternately. However, the performance of two-path successive relaying in secrecy communication remains unexplored. This paper proposes a secrecy two-path successive relaying protocol for a scenario with one source, one destination and two half-duplex relays. The relays operate alternately in a time division mode to forward messages continuously from source to destination in the presence of an eavesdropper. Analytical results reveal that the use of two half-duplex relays in the proposed scheme contributes towards a quadratically lower probability of interception compared to full-duplex relaying. Numerical simulations show that the proposed protocol achieves the ergodic achievable secrecy rate of full-duplex relaying while delivering the lowest probability of interception and secrecy outage probability compared to the existing half duplex relaying, full duplex relaying and full duplex jamming schemes.

Keywords: wireless sensor network; 5G; physical layer secrecy; cooperative relay networks; two-path successive relaying; secrecy capacity; intercept probability; secrecy outage probability

1. Introduction

Wireless Sensor Networks (WSN) is a rapidly emerging field and is driven by a wealth of research. In the WSN, sensor nodes collect and process environmental information. Then, the sensor nodes transmit sensed information to a base station. However, data rate of the transmission is limited at low power sensor nodes for a longer battery lifetime. Relaying is a significant technique to increase the data rate for WSN under the power constraint [1–3]. Idle sensor nodes with no information to transmit can assist the network by performing as relay nodes. However, the sensor nodes must able to communicate with others sensor nodes. The fifth generation (5G) wireless network, which supports device-to-device communication, will address the demand of inter-sensor communication [4].

Following the broadcast nature of wireless channels, transmission between sensor nodes and base station can be easily overheard and possibly extracted by an eavesdropper. This makes WSN highly susceptible to eavesdropping. In order to achieve a confidential and secure wireless communication, existing systems rely on cryptographic techniques at upper layers [5,6]. However, the cryptographic techniques such as encryption rely on the assumption that the eavesdropper has limited computational

capability and is therefore not likely to decipher the key in finite time. Recently, physical layer security has been identified as a promising strategy to provide additional protection against eavesdropping.

Unlike the cryptographic techniques, physical layer security techniques do not rely on computational complexity and will not be compromised by eavesdropper with powerful computational capability. Physical layer security uses wiretap channel coding to achieve the information-theoretic perfect secrecy, where the eavesdropper gains no information about the legitimate information [7–10]. Physical-layer security exploits the characteristics of the wireless channel to improve transmission security. The secrecy of wireless transmission can be quantified by the secrecy capacity, which is defined as the maximum secrecy rate which can be conveyed to legitimate receiver while the eavesdropper gaining no information about the secrecy message [11]. On the other hand, an intercept event occurs and transmission becomes insecure when the secrecy rate falls below zero. The transmission with lower probability of occurrence of an intercept event, *i.e.*, intercept probability, is more secure and robust against eavesdropping. However, the achievable secrecy rate and intercept probability are severely degraded due to the fading effect of wireless communication. To overcome this limitation, extra cooperative node can be used to improve the secrecy [12,13].

A cooperative node injecting jamming signal to interfere the eavesdropper can improve the secrecy rate. However, the jamming signal may deteriorate the desired legitimate transmission as well. This can be avoided by performing beamforming to minimize the adverse effect of the jamming signal towards the desired data transmission [14]. As a result, the jamming signal consumes additional power resource and the design of beamformer increases the complexity. On the other hand, the cooperative relaying has been identified as a promising technique which not only improves reliability and data rate but also can be further utilized to ensure the secrecy of wireless transmission [15–20].

Conventionally, a half-duplex relay cannot perform simultaneous transmission and reception of signal within the same frequency channel. Therefore, when the half-duplex relay is transmitting a signal, the source has to stop transmission. As a result, the spectral efficiency of conventional half-duplex relay is at most half of the spectral efficiency of direct transmission. In order to improve the spectral efficiency of cooperative relaying transmission, a full-duplex relay which can perform simultaneous transmission and reception in the same frequency channel has been proposed. However, in practice, the transmission of the full-duplex relay is interfering its own reception. This self-interference is the main detrimental factor in full-duplex relaying. Since the transmit and receive antennas of full-duplex relay are co-located, the self-interference is much stronger (*i.e.*, 99 dB as reported in [21]) than the intended received signal. The self-interference saturates the analog-to-digital converter (ADC) at the receiver and making it challenging for the cancellation of known self-interference. The suppression of self-interference requires sophisticated hardware and/or advanced signal processing which significantly increase the cost and complexity of relays [22–24]. In fact, for full-duplex relaying, the combination of propagation domain, analog domain and digital domain cancellation techniques are needed to achieve good suppression of self interference [25,26]. In [27], full-duplex and full-duplex jamming secrecy network are proposed. Full-duplex relay improves achievable secrecy rate and secrecy outage probability by providing higher spectral efficiency than conventional half-duplex relay. In full-duplex jamming secrecy network, the full-duplex relay transmits jamming signal towards the eavesdroppers while concurrently receives source message, in order to achieve lower secrecy outage probability [27].

Compared to full-duplex relay, the implementation of a half-duplex relay is much simpler and cheaper. Two-path successive relaying (TPSR) has been proposed as an alternative to achieve the full-duplex spectral efficiency by scheduling a pair of half-duplex relays to assist the source transmission alternately [28]. In TPSR, since the two relays are physically separated, the separation distance between relays is able to attenuate the inter-relay interference due to the distance path loss effect. Since the inter-relay interference is much weaker than the self-interference encountered in full-duplex relay with co-located transmit and receive antennas, simple interference management techniques, such as treating the interference as noise or successive interference cancellation, is

effective [29,30]. Existing literature mainly considers the TPSR in conventional scenarios without eavesdroppers [31–35]. The performance of TPSR in secrecy communication remains unexplored.

In this paper, we propose a secure TPSR protocol that can provide full-duplex spectral efficiency. Two half-duplex relays are used to forward messages from source to destination alternately, the source transmits new messages continuously, and full-duplex spectral efficiency can be achieved. We evaluate the performance of the proposed protocol in terms of ergodic achievable secrecy rate, intercept probability and secrecy outage probability. The performance is compared with half-duplex relaying, full-duplex relaying and full-duplex jamming schemes in [27]. We also analyze the intercept probability of the proposed scheme and full-duplex relaying.

The contributions of this paper are listed as follows. Firstly, we propose secrecy TPSR which is still unexplored by any existing literature. We evaluate the achievable performance of the proposed secrecy TPSR in terms of ergodic achievable secrecy rate, intercept probability and secrecy outage probability. Secondly, we compare the achievable performance of proposed schemes with the existing half-duplex relaying, full-duplex relaying and full-duplex jamming schemes. Finally, the lower bound intercept probabilities of proposed scheme and existing full-duplex relaying are derived and verified with simulations.

The remaining of the paper is organized as follows. In Section 2, the system model and transmission protocol of TPSR are explained and the intercept probability of TPSR is analyzed in Section 3. In Section 4, the achievable secrecy rate of comparison schemes are presented. In Section 5, the numerical simulations are presented to verify the analysis. Finally, the conclusions is given in Section 6.

2. Secrecy Two-Path Successive Relaying Network

2.1. System Model

Consider a wireless network consisting of a source (S), a destination (D), two half-duplex relays (R_1 and R_2) and an eavesdropper (E) as shown in Figure 1, where all nodes are equipped with a single antenna. The eavesdropper can intercept the transmission from source and relay simultaneously. R_1 and R_2 apply the decode-and-forward relaying protocol. It is assumed that the direct S-to-D channel is not available due to severe path loss and/or shadowing. Therefore, the transmission from S to D requires the assistance of R_1 and R_2. In additional, the channel-state-information (CSI) for all channels (including the eavesdropping channels) are required for wiretap channel coding.

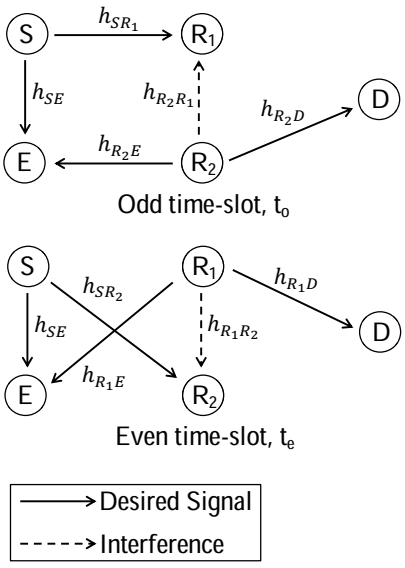

Figure 1. The secrecy two-path successive relaying (TPSR) network with an eavesdropper.

We assume that all channels experience block Rayleigh fading (Rayleigh fading represents the worst case scenario if compared with the case with strong line of sight and path loss. The results presented in this paper therefore represent the achievable lower bound if compared environment with strong line of sight) and remain constant over one block but vary independently from one block to another. The channel coefficient from node i to node j is denoted as h_{ij} and channel reciprocity is assumed, *i.e.*, $h_{ij} = h_{ji}$. The corresponding channel gain, $|h_{ij}|^2$ are independently exponentially distributed with mean of λ_{ij}. The noise at relays (R_1 and R_2), D and E are denoted as $n_{r_1}(t)$, $n_{r_2}(t)$, $n_d(t)$ and $n_e(t)$ with variances of $\sigma_{r_1}^2$, $\sigma_{r_2}^2$, σ_d^2 and σ_e^2, respectively. The transmit power of source and relays are P.

2.2. Transmission Protocol

The transmission protocol of two-path successive relaying (TPSR) is divided into $T+1$ consecutive equal-duration time-slots where S transmits independent codeword $x_s(t)$, $t = 1, 2, \ldots, T$ continuously. The protocol is alternated by odd time-slot stage ($t_o = 1, 3, \ldots, T+1$) and even time-slot stage ($t_e = 2, 4, \ldots, T$) as shown in Figure 1.

- In odd time-slots, S transmits $x_s(t_o)$ and R_2 forwards $x_s(t_o - 1)$. R_1 receives $x_s(t_o)$ from S while being interfered by R_2 (inter-relay interference) and D receives $x_s(t_o - 1)$ from R_2. E receives both $x_s(t_o)$ and $x_s(t_o - 1)$ simultaneously.
- In even time-slots, S transmits $x_s(t_e)$ and R_1 forwards $x_s(t_e - 1)$. R_2 receives $x_s(t_e)$ from S while being interfered by R_1 (inter-relay interference) and D receives $x_s(t_e - 1)$ from R_1. E receives both $x_s(t_e)$ and $x_s(t_e - 1)$ simultaneously.

In odd or even time-slot, the eavesdropper jointly decodes messages from the source and relay transmitter. At the same time, the relay receiver is interfered by the inter-relay interference from the transmitting relay. This is similar to the self-interference of full-duplex relay where the transmission from the transmitting antenna interferes the received signal at the receiving antenna. However, the interference mitigation technique of TPSR is simpler than the full-duplex relay since the two relays are physically distributed. The inter-relay interference can be mitigated to the noise floor when the two relays are sufficiently apart [30].

Let $y_{r_i}(t)$, $i \in \{1, 2\}$, $y_d(t)$ and $y_e(t)$ be the received signals in time slot t at R_i, D and E, respectively. Assume that the relays, destination and eavesdropper can always decode the data. The received signals are

$$y_{r_i}(t) = \sqrt{P}\, h_{SR_i}\, x_s(t) + \sqrt{P}\, h_{RR}\, x_s(t-1) + n_{r_i}(t) \tag{1}$$

$$y_d(t) = \sqrt{P}\, h_{R_iD}\, x_s(t-1) + n_d(t) \tag{2}$$

$$y_e(t) = \sqrt{P}\, h_{SE}\, x_s(t) + \sqrt{P}\, h_{R_iE}\, x_s(t-1) + n_e(t) \tag{3}$$

where h_{RR} is the reciprocal inter-relay channel coefficient.

2.3. Achievable Secrecy Rates

From Equations (1) and (2), the channel capacities for S-to-R_i and R_i-to-D are given by

$$C_{sr_i} = \frac{1}{2}\log_2\left(1 + \frac{P\,|h_{SR_i}|^2}{P\,|h_{RR}|^2 + \sigma_{r_i}^2}\right) \tag{4}$$

$$C_{r_id} = \frac{1}{2}\log_2\left(1 + \frac{P\,|h_{R_iD}|^2}{\sigma_d^2}\right) \tag{5}$$

respectively. The data transmission rate for R_i assisted link is

$$C_{R_i} = \min\left(C_{sr_i}, C_{r_i d}\right) \tag{6}$$

On the other hand, the eavesdropper can receive $x_s(t)$ from S and R_i at time slot t and $t+1$ respectively as specified in Equation (3). By assuming that the eavesdropper is able to jointly decode the information symbols from S and R_i, the instantaneous eavesdropping rate (with the use of instantaneous eavesdropping rate, the near-far effect when eavesdropper is located closer to R_1 than R_2 can be readily captured by the equation) for R_i assisted link can be obtained as

$$C_{e_i} = \frac{1}{2}\log_2\left(1 + \frac{P\left|h_{SE}\right|^2 + P\left|h_{R_i E}\right|^2}{\sigma_e^2}\right) \tag{7}$$

From Equations (6) and (7), the achievable secrecy rate for R_i assisted link can be obtained as

$$C_{s_i} = \left[C_{R_i} - C_{e_i}\right]^+ \tag{8}$$

where $[x]^+ = \max(x, 0)$.

In TPSR, the R_1 and R_2 operate in a time-division mode and forward messages from S to D successively in turn. The achievable secrecy rate for TPSR is the sum of achievable secrecy rate for R_1 and R_2 assisted link as follows:

$$C_{TPSR} = C_{s_1} + C_{s_2} \tag{9}$$

3. Analysis on Intercept Probability

This section provides the intercept probability analysis of the proposed TPSR. Intercept probability is the probability that the eavesdropper successfully intercepts the transmission signal. The eavesdropper can intercept the transmission signal when the transmission rate of legitimate transmission falls below the eavesdropping rate [36].

Theorem 1. *Assume that the channel gain, $\left|h_{ij}\right|^2$ of each of the channels is independently exponentially distributed with mean of λ_{ij}, the intercept probability for R_i assisted link can be obtained as follows:*

$$P_{int_i} = 1 + \alpha \exp\left(\alpha + \frac{\lambda_{sr_i} + \lambda_{r_i d}}{\lambda_{rr}\lambda_{r_i d}}\right) \mathrm{Ei}\left(-\alpha - \frac{\lambda_{sr_i} + \lambda_{r_i d}}{\lambda_{rr}\lambda_{r_i d}}\right) \tag{10}$$

where $\alpha = \frac{\lambda_{sr_i}}{\lambda_{rr}(\lambda_{se}+\lambda_{r_i e})}$ and $\mathrm{Ei}(\cdot)$ is the exponential integral function, i.e., $\mathrm{Ei}(-x) = \int_x^\infty -\exp(-t)/t\, dt$.

Proof. From Equation (8), the intercept probability for R_i assisted link can be obtained as:

$$\begin{aligned} P_{int_i} &= \Pr\left(C_{s_i} < 0\right) \\ &= \Pr\left(C_{R_i} < C_{e_i}\right) \end{aligned} \tag{11}$$

where C_{R_i} and C_{e_i} are the achievable instantaneous transmission and eavesdropping rates for R_i assisted link in Equations (6) and (7), respectively. By using the high signal-to-noise ratio (SNR) approximation, *i.e.*, $\sigma^2 \to 0$, the C_{sr_i} and $C_{r_i d}$ in Equation (6) can be approximated as follows:

$$C_{sr_i} \approx \frac{1}{2}\log_2\left(\frac{P\left|h_{SR_i}\right|^2}{P\left|h_{RR}\right|^2 + \sigma_{r_i}^2}\right) \tag{12}$$

$$C_{r_i d} \approx \frac{1}{2}\log_2\left(\frac{P\left|h_{R_i D}\right|^2}{\sigma_d^2}\right) \tag{13}$$

Then, the C_{R_i} can be approximated as follows:

$$C_{R_i} \approx \frac{1}{2}\min\left[\log_2\left(\frac{P\left|h_{SR_i}\right|^2}{P\left|h_{RR}\right|^2+\sigma_{r_i}^2}\right),\left(\log_2\frac{P\left|h_{R_i D}\right|^2}{\sigma_d^2}\right)\right] \tag{14}$$

On the other hand, because the eavesdropper can receive $x_s(t)$ from S and R_i at time slot t and $t+1$ respectively, the instantaneous eavesdropping rate with high SNR approximation can be approximated as follows:

$$\begin{aligned} C_{e_i} &= \frac{1}{2}\log_2\left(1+\frac{P\left|h_{SE}\right|^2+P\left|h_{R_i E}\right|^2}{\sigma_e^2}\right) \\ &\approx \frac{1}{2}\log_2\left(\frac{P\left|h_{SE}\right|^2+P\left|h_{R_i E}\right|^2}{\sigma_e^2}\right) \end{aligned} \tag{15}$$

by ignoring the interference of simultaneous transmission from the S and R_i. Substituting Equations (14) and (15) into Equation (11) produces the intercept probability for R_i assisted link as follows:

$$P_{int_i} = \Pr\left\{\min\left[\log_2\left(\frac{P\left|h_{SR_i}\right|^2}{P\left|h_{RR}\right|^2+\sigma_{r_i}^2}\right),\log_2\left(\frac{P\left|h_{R_i D}\right|^2}{\sigma_d^2}\right)\right] < \log_2\left(\frac{P\left|h_{SE}\right|^2+P\left|h_{R_i E}\right|^2}{\sigma_e^2}\right)\right\} \tag{16}$$

From Equation (16), the intercept probability for R_i assisted link can be obtained as follows:

$$\begin{aligned} P_{int_i} &= \int_0^\infty \int_0^y f_X(x)\, f_Y(y)\, dx\, dy \\ &= \int_0^\infty f_Y(y)\; F_X(y)\; dy \end{aligned} \tag{17}$$

where $f_X(x)$ and $f_Y(y)$ are the probability density function (PDF) of $X = \min\left(\frac{P\left|h_{SR_i}\right|^2}{P\left|h_{RR}\right|^2+\sigma_{r_i}^2}, \frac{P\left|h_{R_i D}\right|^2}{\sigma_d^2}\right)$ and $Y = \frac{P\left|h_{SE}\right|^2+P\left|h_{R_i E}\right|^2}{\sigma_e^2}$, respectively, and $F_X(y)$ is the cumulative distribution function (CDF) of X.

The $f_Y(y)$ and $F_X(y)$ (see [27]) can be obtained as,

$$f_Y(y) = \frac{1}{\lambda_{se}+\lambda_{r_i e}}\exp\left(-\frac{y}{\lambda_{se}+\lambda_{r_i e}}\right) \tag{18}$$

and

$$F_X(y) = 1-\frac{\lambda_{sr_i}}{\lambda_{sr_i}+\lambda_{rr}y}\exp\left(-\frac{y\left(\lambda_{sr_i}+\lambda_{r_i d}\right)}{\lambda_{sr_i}\lambda_{r_i d}}\right) \tag{19}$$

respectively. By using (3.352.4) in [37], the intercept probability for R_i assisted link in Equation (17) is solved and shown in Equation (10). □

Remark 1 (Remark of Theorem 1). *Theorem 1 shows the closed form intercept probability for* R_i *assisted link in TPSR. From Equation (10), the interception probability for* R_i *assisted link varies with the mean of corresponding channel gain,* i.e., λ_{ij}. *By having higher* λ_{sr_i} *and* $\lambda_{r_i d}$ *for* h_{SR_i} *and* $h_{R_i D}$, *respectively, the interception probability for* R_i *assisted link is decreased. On the other hand, the* λ_{rr}, λ_{se} *and* $\lambda_{r_i e}$ *for* h_{RR}, h_{SE}

and h_{R_iE}, respectively, are the degrading factors, which increases the probability of eavesdropper to intercept the transmission signal.

Corollary 2. *Intercept probability of TPSR is lower bounded by*

$$\begin{aligned} P_{TPSR-L} &= P_{int_1} P_{int_2} \\ &= \Pr\left(C_{s_1} < 0\right) \Pr\left(C_{s_2} < 0\right) \end{aligned} \tag{20}$$

Proof. The intercept probability of TPSR is

$$P_{TPSR} = \Pr\left(C_{TPSR} < 0\right) \tag{21}$$

where $C_{TPSR} = C_{s_1} + C_{s_2}$. The closed form of P_{TPSR} is not achievable due to complexity of derivation. Alternately, lower bound of P_{TPSR} can be obtained based on Theorem 1. Theorem 1 shows the closed form intercept probability for R_1 and R_2 assisted links in TPSR. The transmission and reception of R_1 and R_2 are mutually independent. Thus, the lower bound intercept probability of TPSR, P_{TPSR-L} is the product of intercept probability for R_1 and R_2 assisted link as shown in Equation (20). □

Remark 2 (Remark of Corollary 1)**.** *Corollary 1 in Equation (20) shows that intercept probability of TPSR is lower bounded by the product of intercept probability for* R_1 *and* R_2 *assisted link. Meanwhile, the intercept probability of full-duplex relaying (FDR) is the intercept probability for a full-duplex relay (FR) assisted link as shown in Equation (26). Equations (20) and (26) reveal that the lower bound intercept probability of TPSR is quadratically lower than the FDR. This is because of the two mutually independent assisted link of* R_1 *and* R_2 *in TPSR.*

4. Comparable Schemes

In this section, we review the achievable secrecy rate of half-duplex, full-duplex and full-duplex jamming secrecy network in [27].

4.1. Secrecy Half-Duplex Relaying Network

Half-duplex relaying (HDR) is a conventional relay scheme with a half-duplex relay, R. In the HDR scheme, S transmits $x_s(t)$ to R in time-slot t and R forwards $x_s(t)$ to D in subsequent time-slot. During the transmission, E receives $x_s(t)$ twice, from S and R at time slot t and $t-1$, respectively.

The data transmission rate for HDR is

$$C_R = \frac{1}{2} \min\left[\log_2\left(1 + \frac{P\left|h_{SR}\right|^2}{\sigma_r^2}\right), \log_2\left(1 + \frac{P\left|h_{RD}\right|^2}{\sigma_d^2}\right)\right] \tag{22}$$

On the other hand, the eavesdropping rate can be obtained as

$$C_e = \frac{1}{2} \log_2\left(1 + \frac{P\left|h_{SE}\right|^2 + P\left|h_{RE}\right|^2}{\sigma_e^2}\right) \tag{23}$$

Then, the achievable secrecy rate of HDR is given by

$$C_{HDR} = \left[C_R - C_e\right]^+ \tag{24}$$

4.2. Secrecy Full-Duplex Relaying Network

The system model of full-duplex secrecy relay network in [27] is similar to the half-duplex secrecy relay network, except now the relay has two antennas for simultaneous receiving and transmission respectively, *i.e.*, full-duplex relay, FR. With the two antennas, FR can receive $x_s(t)$ from S and forward

the previously decoded $x_s(t-1)$ to D simultaneously at time slot t. Therefore, S and D can transmit and receive continuously. However, when FR is receiving $x_s(t)$ from S, it is interfered by its own transmission known as self-interference.

The data transmission rate and eavesdropping rate for full-duplex relaying (FDR) are two times of Equations (6) and (7) respectively and h_{RR} is the self-interference channel coefficient of FR. Then, the achievable secrecy rate of FDR is given by

$$C_{FDR} = \left[\min\left(2\,C_{sr_i},\, 2\,C_{r_id}\right) - \frac{1}{T}\,\log_2\left(\det\left\{\mathbf{I} + \mathbf{H}_e^H\mathbf{H}_e\right\}\right)\right]^+ \tag{25}$$

Based on the intercept probability analysis in Section 3, the interception probability of FDR is the same as the intercept probability of R_1 or R_2 assisted link in TPSR as follows (see Equation (10))

$$\begin{aligned} P_{FDR} &= P_{int_i} \\ &= \Pr\left(C_{s_i} < 0\right) \end{aligned} \tag{26}$$

4.3. Secrecy Full-Duplex Jamming Network

The full-duplex jamming (FDJ) network is proposed in [27]. During time slot t, S transmits $x_s(t)$ to FR and FR receives and decodes $x_s(t)$ from S while transmitting a jamming signal to E. During time slot $t+1$, FR forwards previously decoded $x_s(t)$ to D and switches off its receiving antenna. At the same time, S transmits jamming signal to E.

The data transmission rate for FDJ is given in Equation (6) and h_{RR} is the self-interference channel coefficient of FR. On the other hand, the eavesdropping rate for FDJ is given by

$$C_e = \frac{1}{2}\log_2\left(1 + \frac{P\,|h_{SE}|^2}{P\,|h_{RE}|^2 + \sigma_e^2} + \frac{P\,|h_{RE}|^2}{P\,|h_{SE}|^2 + \sigma_e^2}\right) \tag{27}$$

Then, the achievable secrecy rate of FDJ can be obtained as

$$C_{FDJ} = \left[\min\left(C_{sr_i},\, C_{r_id}\right) - C_e\right]^+ \tag{28}$$

5. Numerical Results

In this section, several Monte Carlo simulation results of the proposed two-path successive relaying (TPSR) and existing half-duplex relaying (HDR), full-duplex relaying (FDR) and full-duplex jamming (FDJ) schemes are presented. In the simulations, the transmit power of source and relay, P is fixed to unity and the SNR for channel from node i to node j is defined as $\gamma_{ij} = 1/\sigma_j^2$. There are $T = 1000$ independent codewords transmitted from the source in all schemes. In this paper, we assume that the self-interference is the residual self-interference [27] after the self-interference suppression, which has the same level as the receiver noise. For fair comparison, we assume that the inter-relay interference is at noise level, which can be achieved through physical separation between the relays, relay selection, other techniques, *etc*.

Figure 2 shows the ergodic achievable secrecy rate *versus* SNR of various schemes when $\gamma_{sr} = \gamma_{rd}$, $\gamma_{se} = \gamma_{re} = 10\,\text{dB}$ and the inter-relay interference or residual self-interference, $\gamma_{rr} = 0\,\text{dB}$. It is obvious that TPSR and FDR achieved the same ergodic achievable secrecy rate. This means that the TPSR has the same bandwidth efficiency as the FDR. The TPSR and FDR also achieved 95.4 % and 63.3 % ergodic secrecy rate gain compared to HDR and FDJ, respectively, when SNR $= 40\,\text{dB}$. This is because the higher bandwidth efficiency of TPSR and FDR compared to the HDR and FDJ. The FDJ employs jamming technique to interfere the eavesdropper. As a result, the FDJ achieves higher ergodic

achievable secrecy rate than the HDR. However, FDJ achieves a lower ergodic achievable secrecy rate than TPSR and FDR because half of the bandwidth is used to transmit jamming signals.

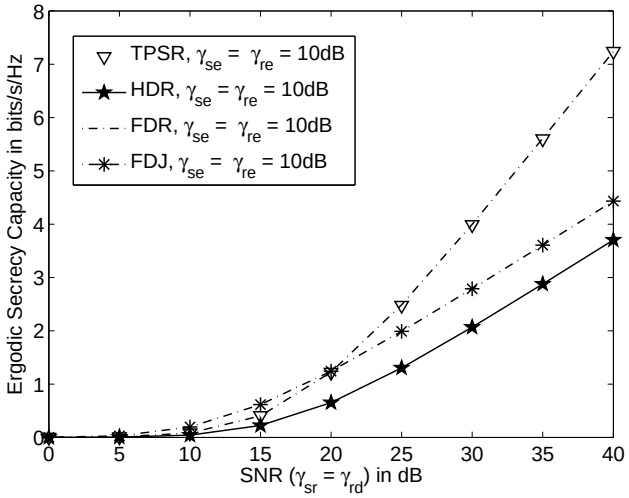

Figure 2. Ergodic achievable secrecy rate *versus* SNR where $\gamma_{sr} = \gamma_{rd}$, $\gamma_{se} = \gamma_{re} = 10$ dB and the inter-relay interference or self-interference, $\gamma_{rr} = 0$ dB.

Figure 3 shows the intercept probability of various schemes *versus* SNR when $\gamma_{sr} = \gamma_{rd}$, $\gamma_{se} = \gamma_{re} = 10$ dB and the inter-relay interference or residual self-interference, $\gamma_{rr} = 0$ dB. We observe that the FDR has higher probability of interception compared to the HDR. This is because of the residual self-interference of full-duplex relay in FDR. By transmitting jamming signal to the eavesdropper, the FDJ achieves lower probability of interception compared to the FDR and HDR. The intercept probability of TPSR is lower bounded by theoretical result. Meanwhile, the theoretical result of FDR are well matched to the simulation result. This verifies that the lower bound intercept probability of TPSR and FDR in Equations (20) and (26), respectively. TPSR also achieves the lowest probability of interception compared to all the other schemes at high SNR, *i.e.*, SNR $\geq$ 30 dB. This is because the two mutually independent assisted link of R_1 and R_2 contribute lower intercept probability to the TPSR compared to the other schemes equipped with only one relay.

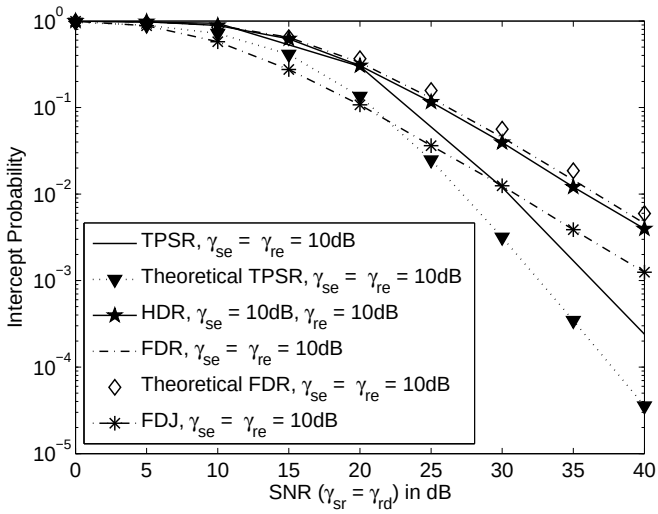

Figure 3. Intercept probability *versus* SNR where $\gamma_{sr} = \gamma_{rd}$, $\gamma_{se} = \gamma_{re} = 10$ dB and the inter-relay interference or self-interference, $\gamma_{rr} = 0$ dB.

Figure 4 shows the intercept probability *versus* inter-relay interference or residual self-interference, γ_{rr} for various schemes when $\gamma_{sr} = \gamma_{rd} = 40\,\text{dB}$ and $\gamma_{se} = \gamma_{re} = 10\,\text{dB}$. The FDR has the highest probability of interception compared to the other schemes even when $\gamma_{rr} = 0\,\text{dB}$. The residual self-interference decreases the data transmission rate of the FDR. Therefore, the FDR has higher probability of interception compared to the HDR. However, by employing jamming technique, the FDJ with low residual self-interference can achieve lower probability of interception compared to the HDR. On the other hand, when the inter-relay interference $\gamma_{rr} < 15\,\text{dB}$, the TPSR has the lowest probability of interception compared to the other schemes. This shows that the operating requirement for inter-relay interference level in TPSR is much lower and practical if compared to the self interference level in FDR.

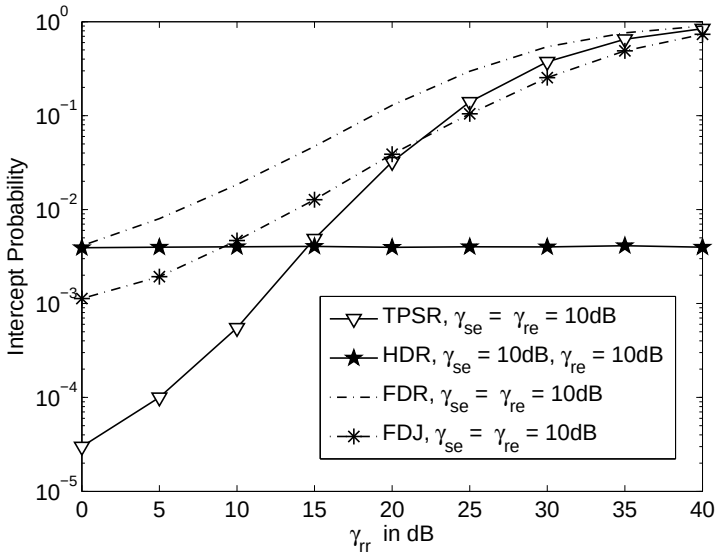

Figure 4. Intercept probability *versus* inter-relay interference or residual self-interference, γ_{rr} where $\gamma_{sr} = \gamma_{rd} = 40\,\text{dB}$ and $\gamma_{se} = \gamma_{re} = 10\,\text{dB}$.

Figure 5 shows the secrecy outage probability *versus* target secrecy rate, r of various schemes when $\gamma_{sr} = \gamma_{rd} = 40\,\text{dB}$, $\gamma_{se} = \gamma_{re} = 10\,\text{dB}$ and the inter-relay interference or residual self-interference, $\gamma_{rr} = 0\,\text{dB}$. The probability of secrecy outage of all the schemes is increasing when the target secrecy rate, r is increased. The TPSR has the lowest probability of secrecy outage compared to the other schemes and it is lower bounded by the FDR. This is due to the use of two relays in TPSR which provide additional diversity and full-duplex bandwidth efficiency. In contrast to previous results in Figure 3, where the FDR has lower probability of secrecy outage than the HDR and FDJ. This is because the "1/2" pre-log factor in achievable secrecy rate of HDR and FDJ in Equations (24) and (28). The jamming technique benefits the FDJ by delivering lower probability of secrecy outage than HDR.

Figure 6 shows the secrecy outage probability *versus* inter-relay interference or self-interference, γ_{rr} for various schemes when target secrecy rate, $r = 2\,\text{bits/s/Hz}$, $\gamma_{se} = \gamma_{re} = 10\,\text{dB}$ and $\gamma_{sr} = \gamma_{rd} = 40\,\text{dB}$. The TPSR has the lowest probability of secrecy outage compared to the FDR and FDJ. In other words, with the same γ_{rr}, TPSR is more secure than the FDR and FDJ. By considering the HDR as baseline scheme, when $\gamma_{rr} = 10\,\text{dB}$, the TPSR has lower probability of secrecy outage, whereas the FDR and FDJ have higher probability of secrecy outage. This shows that the FDR and FDJ require much lower γ_{rr} compared to the TPSR to achieve lower probability of secrecy outage than the HDR. As a result, the FDR and FDJ have a stricter requirement on residual interference compared to the TPSR.

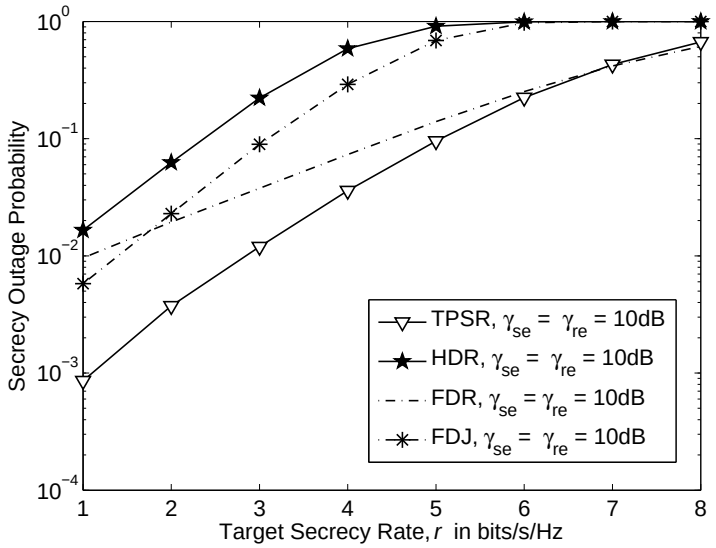

Figure 5. Secrecy outage probability *versus* target secrecy rate, r where $\gamma_{sr} = \gamma_{rd} = 40\,\text{dB}$, $\gamma_{se} = \gamma_{re} = 10\,\text{dB}$ and the inter-relay interference or self-interference, $\gamma_{rr} = 0\,\text{dB}$.

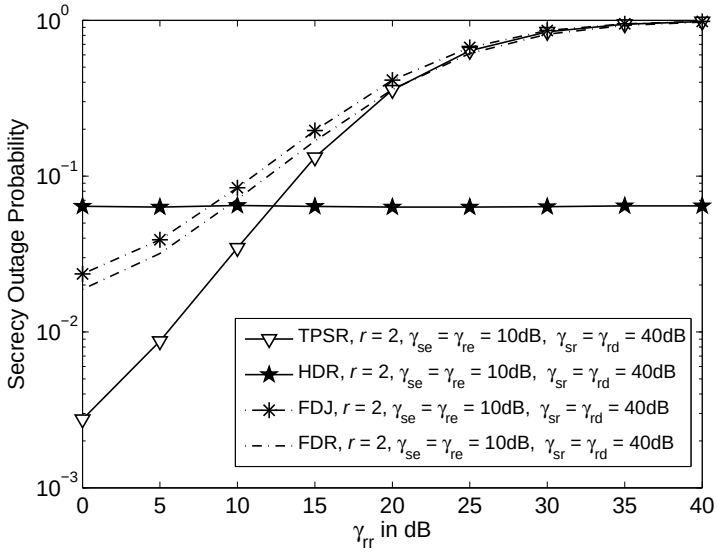

Figure 6. Outage probability *versus* inter-relay interference or self-interference, γ_{rr} where target secrecy rate, $r = 2\,\text{bits/s/Hz}$, $\gamma_{se} = \gamma_{re} = 10\,\text{dB}$ and $\gamma_{sr} = \gamma_{rd} = 40\,\text{dB}$.

6. Conclusions

In this paper, two-path successive relaying (TPSR) is proposed to improve the security of wireless transmission. We compare the ergodic achievable secrecy rate, interception probability and secrecy outage probability of the proposed TPSR against the existing half-duplex relaying (HDR), full-duplex relaying (FDR) and full-duplex jamming (FDJ). The numerical results reveal that the proposed TPSR achieves the same ergodic achievable secrecy rate as the FDR. The TPSR also delivers the lowest probability of interception and secrecy outage compared to the other schemes due to the full-duplex bandwidth efficiency and the two mutually independent links assisted by relay pair R_1 and R_2. The intercept probabilities of TPSR and FDR are analyzed and verified with simulation. The analysis shows that the intercept probability of TPSR is quadratically lower than the intercept probability of FDR. The numerical results show the TPSR has the lowest probability of interception compared to all

other schemes when the inter-relay interference, $\gamma_{rr} < 15$ dB. In terms of secrecy outage probability, the FDR and FDJ demand lower interference level compared to the TPSR in order to outperform the HDR. In short, with the proposed TPSR protocol, a secured wireless transmission can be achieved by using conventional half-duplex relays without employing sophisticated jamming and/or interference cancellation techniques.

Acknowledgments: The work of Q. Y. Liau, C. Y. Leow and Z. Ding is supported by H2020-MSCA-RISE-2015 under grant number 690750, and the Ministry of Higher Education Malaysia and Universiti Teknologi Malaysia under vote number 07085, 4J210 and 12H35.

Author Contributions: Q. Y. Liau and C. Y. Leow conceived the idea of secrecy TPSR, performed system modeling and simulation and derived analysis of the proposed scheme. Z. Ding provided substantial comments and technical review of the proposed scheme and contributed to the revision of the paper. All authors contributed to the write-up of the manuscript.

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

References

1. Wang, G.; Huang, L.; Xu, H.; Li, J. Relay Node Placement for Maximizing Network Lifetime in Wireless Sensor Networks. In Proceedings of the 4th International Conference on Wireless Communications, Networking and Mobile Computing, Dalian, China, 12–14 October 2008; pp. 1–5.
2. Zhu, Y.; Zhang, Y.; Xie, J.; Bai, C. A new optimal power allocation scheme for opportunistic cooperative multicast transmission and network coding in wireless sensor networks. In Proceedings of the IEEE 4th International Conference on Electronics Information and Emergency Communication (ICEIEC), Beijing, China, 15–17 November 2013; pp. 329–332.
3. Prathibha, V.; Aruna, T. Enhancing the network lifetime of cooperative wireless sensor networks using energy harvesting technique. In Proceedings of the IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Coimbatore, India, 18–20 December 2014; pp. 1–4.
4. Demestichas, P.; Georgakopoulos, A.; Karvounas, D.; Tsagkaris, K.; Stavroulaki, V.; Lu, J.; Xiong, C.; Yao, J. 5G on the Horizon: Key Challenges for the Radio-Access Network. *IEEE Vehicul. Technol. Mag.* **2013**, *8*, 47–53.
5. Hellman, M. An overview of public key cryptography. *IEEE Commun. Soc. Mag.* **1978**, *16*, 24–32.
6. Kartalopoulos, S. A primer on cryptography in communications. *IEEE Commun. Mag.* **2006**, *44*, 146–151.
7. Liang, Y.; Poor, H.; Shamai, S. Secure Communication Over Fading Channels. *IEEE Trans. Inf. Theory* **2008**, *54*, 2470–2492.
8. Bloch, M.; Barros, J.; Rodrigues, M.; McLaughlin, S. Wireless Information-Theoretic Security. *IEEE Trans. Inf. Theory* **2008**, *54*, 2515–2534.
9. Gopala, P.K.; Lai, L.; El Gamal, H. On the Secrecy Capacity of Fading Channels. *IEEE Trans. Inf. Theory* **2008**, *54*, 4687–4698.
10. Khisti, A.; Tchamkerten, A.; Wornell, G.W. Secure Broadcasting Over Fading Channels. *IEEE Trans. Inf. Theory* **2008**, *54*, 2453–2469.
11. Shannon, C. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715.
12. Deng, H.; Wang, H.M.; Guo, W.; Wang, W. Secrecy Transmission With a Helper: To Relay or to Jam. *IEEE Trans. Inf. Forens. Secur.* **2015**, *10*, 293–307.
13. Hui, H.; Swindlehurst, A.; Li, G.; Liang, J. Secure Relay and Jammer Selection for Physical Layer Security. *IEEE Signal Process. Lett.* **2015**, *22*, 1147–1151.
14. Liu, Y.; Li, J.; Petropulu, A. Destination Assisted Cooperative Jamming for Wireless Physical-Layer Security. *IEEE Trans. Inf. Forens. Secur.* **2013**, *8*, 682–694.
15. Popovski, P.; Simeone, O. Wireless Secrecy in Cellular Systems With Infrastructure-Aided Cooperation. *IEEE Trans. Inf. Forens. Secur.* **2009**, *4*, 242–256.
16. Zou, Y.; Wang, X.; Shen, W. Physical-Layer Security with Multiuser Scheduling in Cognitive Radio Networks. *CoRR* **2013**, *61*, 5103–5113.
17. Zou, Y.; Zhu, J.; Wang, X.; Leung, V. Improving physical-layer security in wireless communications using diversity techniques. *IEEE Netw.* **2015**, *29*, 42–48.
18. Wang, H.M.; Luo, M.; Yin, Q.; Xia, X.G. Hybrid Cooperative Beamforming and Jamming for Physical-Layer Security of Two-Way Relay Networks. *IEEE Trans. Inf. Forens. Secur.* **2013**, *8*, 2007–2020.

19. Zheng, T.X.; Wang, H.M.; Liu, F.; Lee, M.H. Outage Constrained Secrecy Throughput Maximization for DF Relay Networks. *IEEE Trans. Commun.* **2015**, *63*, 1741–1755.
20. Wang, H.M.; Xia, X.G. Enhancing wireless secrecy via cooperation: signal design and optimization. *IEEE Commun. Mag.* **2015**, *53*, 47–53.
21. Li, W.; Rikkinen, K.; Pirinen, P.; Tapio, V.; Lavin, C.; Gonzáles, L.; Debaillie, B.; van Liempd, B.; Klumperink, E.; van den Broek, D.J.; *et al. System Scenarios and Technical Requirements for Full-Duplex Concept*; Technical Report; DUPLO: Surrey, UK, 2013.
22. Bliss, D.; Hancock, T.; Schniter, P. Hardware phenomenological effects on cochannel full-duplex MIMO relay performance. In Proceedings of the 2012 Conference Record of the Forty Sixth Asilomar Conference on Signals, Systems and Computers (ASILOMAR), Pacific Grove, CA, USA, 4–7 November 2012; pp. 34–39.
23. Riihonen, T.; Werner, S.; Wichman, R. Mitigation of Loopback Self-Interference in Full-Duplex MIMO Relays. *IEEE Trans. Signal Process.* **2011**, *59*, 5983–5993.
24. Taghizadeh, O.; Mathar, R. Full-Duplex Decode-and-Forward Relaying with Limited Self-Interference Cancellation. In Proceedings of the 2014 18th International ITG Workshop on Smart Antennas (WSA), Erlangen, Germany, 12–13 March 2014; pp. 1–7.
25. Vermeulen, T.; Rosas, F.; van Liempd, B.; Verhelst, M.; Pollin, S. An energy-scalable in-band full duplex architecture. In Proceedings of the 2015 IEEE 20th International Workshop on Computer Aided Modelling and Design of Communication Links and Networks (CAMAD), Guildford, UK, 7–9 September 2015; pp. 22–26.
26. Alves, H.; Souza, R.D.; Pellenz, M.E. Brief survey on full-duplex relaying and its applications on 5G. In Proceedings of the 2015 IEEE 20th International Workshop on Computer Aided Modelling and Design of Communication Links and Networks (CAMAD), Guildford, UK, 7–9 September 2015; pp. 17–21.
27. Chen, G.; Gong, Y.; Xiao, P.; Chambers, J. Physical Layer Network Security in the Full-Duplex Relay System. *IEEE Trans. Inf. Forens. Secur.* **2015**, *10*, 574–583.
28. Rankov, B.; Wittneben, A. Spectral efficient protocols for half-duplex fading relay channels. *IEEE J. Sel. Areas Commun.* **2007**, *25*, 379–389.
29. Liau, Q.Y.; Leow, C.Y. Performance of Two-Path Successive Relaying in the Presence of Inter-Relay Interference. *J. Theor. Appl. Inf. Technol.* **2015**, *74*, 82–87.
30. Liau, Q.Y.; Leow, C.Y. Study of relay position in two-path successive relaying with interference cancellation. In Proceedings of the 2014 IEEE Asia Pacific Conference on Wireless and Mobile, Bali, France, 28–30 August 2014; pp. 254–259.
31. Nomikos, N.; Vouyioukas, D. A successive opportunistic relaying protocol with inter-relay interference mitigation. In Proceedings of the 8th International Wireless Communications and Mobile Computing Conference (IWCMC), Limassol, Cyprus, 27–31 August 2012; pp. 228–233.
32. Hu, Y.; Li, K.H.; Teh, K.C. An Efficient Successive Relaying Protocol for Multiple-Relay Cooperative Networks. *IEEE Trans. Wirel. Commun.* **2012**, *11*, 1892–1899.
33. Nomikos, N.; Vouyioukas, D.; Charalambous, T.; Krikidis, I.; Skoutas, D.; Johansson, M. Capacity improvement through buffer-aided successive opportunistic relaying. In Proceedings of the 3rd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace Electronic Systems (VITAE), Atlantic City, NJ, USA, 24–27 June 2013; pp. 1–5.
34. Nomikos, N.; Charalambous, T.; Krikidis, I.; Skoutas, D.; Vouyioukas, D.; Johansson, M. Buffer-aided successive opportunistic relaying with inter-relay interference cancellation. In Proceedings of the IEEE 24th International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), London, UK, 8–11 September 2013; pp. 1316–1320.
35. Nomikos, N.; Vouyioukas, D.; Charalambous, T.; Krikidis, I.; Makris, P.; Skoutas, D.N.; Johansson, M.; Skianis, C. Joint relay-pair selection for buffer-aided successive opportunistic relaying. *Trans. Emerg. Telecommun. Technol.* **2014**, *25*, 823–834.
36. Leung-Yan-Cheong, S.; Hellman, M. The Gaussian wire-tap channel. *IEEE Trans. Inf. Theory* **1978**, *24*, 451–456.
37. Gradshteyn, I.S.; Ryzhik, I.M. *Table of Integrals, Series, and Products*, 7th ed.; Elsevier/Academic Press: Amsterdam, The Netherlands, 2007; pp. 1148–1171.