entropy

MDPI

Article

Secrecy Performance Enhancement for Underlay Cognitive Radio Networks Employing Cooperative Multi-Hop Transmission with and without Presence of Hardware Impairments

Phu Tran Tin [1,2], Dang The Hung [3], Tan N. Nguyen [4,*], Tran Trung Duy [5] and Miroslav Voznak [1]

1 VSB—Technical University of Ostrava, 17. listopadu 15/2172, 708 33 Ostrava, Poruba, Czech Republic; phutrantin@iuh.edu.vn (P.T.T.); miroslav.voznak@vsb.cz (M.V.)
2 Faculty of Electronics Technology, Industrial University of Ho Chi Minh City, Ho Chi Minh City 71408, Vietnam
3 Faculty of Radio-Electronics Engineering, Le Quy Don Technical University, Hanoi 11917, Vietnam; danghung8384@gmail.com
4 Wireless Communications Research Group, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City 72912, Vietnam
5 Department of Telecommunications, Posts and Telecommunications Institute of Technology, Ho Chi Minh City 71007, Vietnam; trantrungduy@ptithcm.edu.vn
* Correspondence: nguyennhattan@tdtu.edu.vn

Received: 2 January 2019; Accepted: 20 February 2019; Published: 24 February 2019

Abstract: In this paper, we consider a cooperative multi-hop secured transmission protocol to underlay cognitive radio networks. In the proposed protocol, a secondary source attempts to transmit its data to a secondary destination with the assistance of multiple secondary relays. In addition, there exists a secondary eavesdropper who tries to overhear the source data. Under a maximum interference level required by a primary user, the secondary source and relay nodes must adjust their transmit power. We first formulate effective signal-to-interference-plus-noise ratio (SINR) as well as secrecy capacity under the constraints of the maximum transmit power, the interference threshold and the hardware impairment level. Furthermore, when the hardware impairment level is relaxed, we derive exact and asymptotic expressions of end-to-end secrecy outage probability over Rayleigh fading channels by using the recursive method. The derived expressions were verified by simulations, in which the proposed scheme outperformed the conventional multi-hop direct transmission protocol.

Keywords: physical-layer security; underlay cognitive radio; cooperative multi-hop transmission; secrecy outage probability; hardware impairments

1. Introduction

Security is one of the most important issues in wireless communication because of the broadcast nature of wireless medium. Conventionally, encryption/decryption algorithms that generate public/private keys are used to guarantee the security [1,2]. Recently, a security framework for the physical layer, called the wiretap channel or physical-layer security (PLS) [3–11], has been introduced as a potential solution. In PLS, difference between Shannon capacity of the data link and that of the eavesdropping link, named secrecy capacity, is commonly used to evaluate secrecy performance such as average secrecy capacity (ASC), secrecy outage probability (SOP) and probability of non-zero secrecy capacity (PNSC). Hence, to enhance the secrecy performance for wireless systems, researchers

proposed efficient communication methods to increase channel capacity of the data links, and/or decrease that of the eavesdropping links. Indeed, in [12–14], opportunistic relay selection protocols are considered to enhance the quality of the data channels in one-hop and dual-hop relaying networks. In [15–18], the authors considered cooperative jamming approaches to reduce the data rate received at the eavesdroppers. The authors of [19–25] considered the secrecy performance enhancement for underlay cognitive radio (UCR) networks in which transmit power of secondary users (SUs) is limited by maximum interference levels required by primary users (PUs). The authors of [26–29] proposed secure communication protocols for two-way relay networks. In [30–33], the end-to-end secrecy performance of multi-hop relaying systems is investigated.

Thus far, most published works related to performance evaluation assume that transceiver hardware of wireless terminals is perfect. However, in practice, it suffers from impairments due to phase noises, amplifier–amplitude non-linearity and in phase and quadrature imbalance (IQI) [34–36], which significantly degrade the performance of wireless communication systems. In [37,38], the authors proposed various relay selection methods to compensate the impact of the hardware imperfection. The authors of [39] studied the outage performance of partial relay selection and opportunistic relay selection schemes in the UCR networks under the joint of hardware imperfection and interference constraint.

To the best of our knowledge, several published works evaluate the secrecy performance under the impact of imperfect transceiver hardware. In [40], the authors first studied the impact of the hardware imperfection on the secrecy capacity. In particular, the work in [40] considers the effects of IQI in one-hop OFDMA communication systems. The authors of [41] designed a secure massive MIMO system in the presence of a passive multiple-antenna eavesdropper and the hardware impairments. Reference [42] provided a power-efficient resource allocation algorithm for secure wireless-powered communication networks with the hardware noises. Taking hardware imperfection into account, the authors of [43] proposed an optimal power allocation strategy to maximize the instantaneous secrecy rate of a cooperative amplify-and-forward (AF) relaying scheme. In [44], we calculated PNSC of multi-hop relay networks over Nakagami-m fading channels in presence of the hardware impairments. The results in [44] show that the hardware impairments significantly affect on the PNSC performance.

However, there is no published work related to cooperative multi-hop PLS in the UCR networks. This motivated us to propose such a scheme and evaluate its performance. In the proposed protocol, named Cooperative Multi-Hop Transmission Protocol (CMT), a secondary source sends its data to a secondary destination via multiple secondary relays. In addition, in the secondary network, a secondary eavesdropper overhears the source data transmitted by the source and relay nodes. In addition, the secondary transmitters must adjust the transmit power to satisfy the interference constraint required by a PU and a maximal power threshold. The operation of the proposed scheme can be realized via one or many orthogonal time slots. At each time slot, the current transmitter finds an intended receiver that is nearest to the destination, and can receive the data securely and successfully. If this receiver is the destination, the data transmission ends. Otherwise, the procedure is repeated with the new selected transmitter. We also design a cooperative MAC method at each time slot for reversing the channel as well as selecting the potential receiver. For performance measurement, we first formulate the secrecy capacity under joint constraint of the limited interference and the hardware imperfection. When the hardware impairments are relaxed, we derive exact and asymptotic expressions of the end-to-end SOP over Rayleigh fading channels by using a recursive expression. Computer simulations were realized to verify the theoretical derivations as well as to show the advantages of the CMT method. The results show that the proposed scheme outperformed the conventional multi-hop direct transmission (MDT) protocol, and parameters such as the imperfect CSI estimations, the number of intermediate relays, the hardware impairment level and the position of the eavesdropper significantly affected the end-to-end SOP.

The rest of this paper is organized as follows. System model of the proposed scheme is described in Section 2. In Section 3, exact and asymptotic expressions of the end-to-end SOP for the MDT and

CMT protocols are derived. The simulation results are presented in Section 4. Section 5 presents our conclusions.

2. System Model

As illustrated in Figure 1, we consider an M-hop secondary network, where the source (N_0) communicates with the destination (N_M) via $M-1$ relay nodes denoted by N_1, N_2, ..., N_{M-1}. The relay nodes are numbered according to their distances to the destination, i.e., the relay N_{M-1} is nearest and the relay N_1 is the furthest. In UCR, the source and the relay nodes must adapt the transmit power so that the co-channel interference levels caused by their transmission are below a threshold (I_{th}) given by a primary user (PU). Moreover, the transmit power of the secondary transmitters is also limited by a maximum power (P_{th}). In addition, in the secondary network, the eavesdropper (E) attempts to overhear the source data transmitted by the secondary transmitters. Before describing the operation of the proposed protocol, we give assumptions used in this paper.

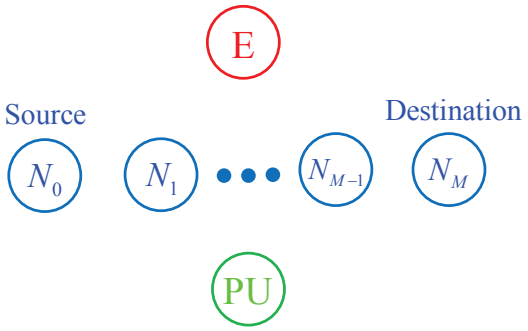

Figure 1. System model of the proposed protocol.

We assume that all of the relays are in the radio range of the source and destination nodes. We assume that all of the nodes have a single antenna, and the data transmission is hence split into orthogonal time slots. For ease of presentation and analysis, it is assumed that all of the nodes have the same structure, and the impairment levels are the same. We also assume that the eavesdropper is an active node, and hence the secondary nodes can estimate channel state information (CSI) between themselves and the node E [45]. Next, the data transmission between two secondary nodes is considered to be secure and successful if the obtained secrecy capacity is higher than a positive threshold (R_{S}). Otherwise, the data are assumed to be intercepted, which is referred to as a secrecy outage event.

2.1. Channel and Hardware Impairment Models

Let d_{N_i,N_j}, $d_{N_i,\text{PU}}$ and $d_{N_i,\text{E}}$ denote distances of the $N_i \to N_j$, $N_i \to$ PU and $N_i \to$ E links, respectively, where $i, j \in \{0, 1, ..., M-1, M\}$. We also denote h_{N_i,N_j}, $h_{N_i,\text{PU}}$ and $h_{N_i,\text{E}}$ as channel coefficients of $N_i \to N_j$, $N_i \to$ PU and $N_i \to$ E links, respectively. Because the channels experience a Rayleigh fading distribution, the channel gains such as $\gamma_{i,j} = |h_{N_i,N_j}|^2$, $\gamma_{i,\text{P}} = |h_{N_i,\text{PU}}|^2$ and $\gamma_{i,\text{E}} = |h_{N_i,\text{E}}|^2$ follow exponential distributions. To take path-loss into account, we can model the parameters of the random variables (RVs) $\gamma_{i,j}$, $\gamma_{i,P}$ and $\gamma_{i,E}$ as [46]: $\lambda_{i,j} = d^{\beta}_{N_i,N_j}$, $\lambda_{i,P} = d^{\beta}_{N_i,PU}$ and $\lambda_{i,E} = d^{\beta}_{N_i,E}$, where β is path-loss exponent.

Considering the data transmission between the transmitter X and the receiver Y ($\text{X} \in \{N_0, N_1, ..., N_{M-1}\}$, $\text{Y} \in \{N_1, N_2, ..., N_M, \text{E}, \text{PU}\}$), the received data at Y is given as in [34–36]:

$$y = \sqrt{P_{\text{X}}} h_{\text{X,Y}} \left(x_0 + \eta_{t,\text{X}}\right) + \eta_{r,\text{Y}} + \nu_{\text{Y}}, \tag{1}$$

where x_0 is the source data, P_{X} is the transmit power of X, $h_{\text{X,Y}}$ is channel coefficient of the X-Y link, $\eta_{t,\text{X}}$ and $\eta_{r,\text{Y}}$ are hardware noises at X and Y, respectively, and ν_{Y} is Gaussian noise at Y.

Similar to the work in [34–36], $\eta_{t,\mathrm{X}}$, $\eta_{r,\mathrm{Y}}$ and ν_{Y} are modeled as Gaussian random variables (RVs) with zero-mean and their variances are given, respectively, as

$$\mathrm{var}\left\{\eta_{t,\mathrm{X}}\right\} = \tau_t^2,\ \mathrm{var}\left\{\eta_{r,\mathrm{Y}}\right\} = \tau_r^2 P_{\mathrm{X}} |h_{\mathrm{X,Y}}|^2, \mathrm{var}\left\{\nu_{\mathrm{Y}}\right\} = \sigma_0^2, \tag{2}$$

where τ_t^2 and τ_r^2 are levels of the hardware impairments at X and Y, respectively.

From Equations (1) and (2), the instantaneous signal-to-interference-plus-noise ratio (SINR) is formulated by

$$\begin{aligned}\Psi_{\mathrm{X,Y}} &= \frac{P_{\mathrm{X}}|h_{\mathrm{X,Y}}|^2}{\left(\tau_t^2 + \tau_r^2\right) P_{\mathrm{X}}|h_{\mathrm{X,Y}}|^2 + \sigma_0^2} \\ &= \frac{P_{\mathrm{X}}|h_{\mathrm{X,Y}}|^2}{\kappa P_{\mathrm{X}}|h_{\mathrm{X,Y}}|^2 + \sigma_0^2},\end{aligned} \tag{3}$$

where $\kappa = \tau_t^2 + \tau_r^2$ is the total hardware impairment level.

Let us consider the transmit power P_{X} of the node X in the underlay CR network. Firstly, P_{X} is below the maximum transmit power, i.e., $P_{\mathrm{X}} \leq P_{\mathrm{th}}$. Secondly, the interference caused at the PU due to the transmission of the node X must be below the interference threshold I_{th}, i.e.,

$$P_{\mathrm{X}} \leq \frac{I_{\mathrm{th}}}{(1+\kappa)\,|h_{\mathrm{X,PU}}|^2}. \tag{4}$$

Therefore, P_{X} can be given as

$$\begin{aligned}P_{\mathrm{X}} &= \min\left(P_{\mathrm{th}}, \frac{I_{\mathrm{th}}}{(1+\kappa)\,|h_{\mathrm{X,PU}}|^2}\right) \\ &= P_{\mathrm{th}} \min\left(1, \frac{\mu}{(1+\kappa)\,|h_{\mathrm{X,PU}}|^2}\right),\end{aligned} \tag{5}$$

where $\mu = I_{\mathrm{th}}/P_{\mathrm{th}}$ is assumed to be a constant.

Combining Equations (3) and (5) yields

$$\Psi_{\mathrm{X,Y}} = \frac{P \min\left(1, \frac{\mu}{(1+\kappa)|h_{\mathrm{X,PU}}|^2}\right)|h_{\mathrm{X,Y}}|^2}{\kappa P \min\left(1, \frac{\mu}{(1+\kappa)|h_{\mathrm{X,PU}}|^2}\right)|h_{\mathrm{X,Y}}|^2 + 1}, \tag{6}$$

where $P = P_{\mathrm{th}}/\sigma_0^2$.

From Equation (6), we can formulate the SINR for the $N_i \rightarrow N_j$ and $N_i \rightarrow \mathrm{E}$ links, where $i, j \in \{0, 1, ..., M\}$, respectively, as

$$\begin{aligned}\Psi_{i,j} &= \frac{P \min\left(1, \mu/\gamma_{i,\mathrm{P}}\right)\gamma_{i,j}}{\kappa P \min\left(1, \mu/\gamma_{i,\mathrm{P}}\right)\gamma_{i,j} + 1}, \\ \Psi_{i,\mathrm{E}} &= \frac{P \min\left(1, \mu/\gamma_{i,\mathrm{P}}\right)\gamma_{i,\mathrm{E}}}{\kappa P \min\left(1, \mu/\gamma_{i,\mathrm{P}}\right)\gamma_{i,\mathrm{E}} + 1}.\end{aligned} \tag{7}$$

Moreover, when the transceiver hardware of all the nodes is perfect, i.e., $\kappa = \kappa_t^2 = \kappa_r^2 = 0$, we can rewrite Equation (7) as

$$\begin{aligned}\Psi_{i,j} &= P \min\left(1, \frac{\mu}{\gamma_{i,\mathrm{P}}}\right)\gamma_{i,j}, \\ \Psi_{i,\mathrm{E}} &= P \min\left(1, \frac{\mu}{\gamma_{i,\mathrm{P}}}\right)\gamma_{i,\mathrm{E}}.\end{aligned} \tag{8}$$

Hence, the secrecy capacity obtained at N_j due to the transmission of N_i is calculated as

$$\begin{aligned} R_{i,j} &= \max\left(0, \log_2\left(1+\Psi_{i,j}\right) - \log_2\left(1+\Psi_{i,\mathrm{E}}\right)\right) \\ &= \left[\log_2\left(\frac{1+\Psi_{i,j}}{1+\Psi_{i,\mathrm{E}}}\right)\right]^+, \end{aligned} \tag{9}$$

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

From Equations (7) and (9), because $\Psi_{i,j} \overset{P\to+\infty}{\approx} 1/\kappa$ and $\Psi_{i,\mathrm{E}} \overset{P\to+\infty}{\approx} 1/\kappa$, the secrecy capacity at high P regime can be given as

$$R_{i,j} \overset{P\to+\infty}{\approx} \left[\log_2\left(\frac{1+1/\kappa}{1+1/\kappa}\right)\right]^+ = 0. \tag{10}$$

Moreover, as $\kappa = 0$, we have

$$\begin{aligned} R_{i,j} &= \left[\log_2\left(\frac{1+P\min\left(1, \mu/\gamma_{i,\mathrm{P}}\right)\gamma_{i,j}}{1+P\min\left(1, \mu/\gamma_{i,\mathrm{P}}\right)\gamma_{i,\mathrm{E}}}\right)\right]^+ \\ &\overset{P\to+\infty}{\approx} \left[\log_2\left(\frac{\gamma_{i,j}}{\gamma_{i,\mathrm{E}}}\right)\right]^+. \end{aligned} \tag{11}$$

2.2. Operation of the Proposed Protocol

Next, we describe the operation of the proposed protocol, in which a MAC layer operation is designed to reverse the channel. Similar to the CoopMAC proposed in [47], in the first time slot, before transmitting the data, the source sends a request-to-send (RTS) message to the destination and all of the relays. By receiving this message, all of the nodes can estimate CSI between themselves and the source, calculate the instantaneous secrecy capacity by using Equation (9), and compare with R_{S}. It is assumed that the source can exactly estimate the channel coefficients of the interference and eavesdropping links, and include these values into the RTS message. If the destination can receive the source data securely and successfully, i.e., $R_{0,M} \geq R_{\mathrm{S}}$, it will feedback a clear-to-send (CTS) message to inform. In this case, the source directly sends the data to the destination without using the relays. In the case where $R_{0,M} < R_{\mathrm{S}}$, the destination has to generate a non-CTS message to request the help of the relays. Now, let us denote $\mathcal{U}_1 = \left\{N_{1_1}, N_{1_2}, ..., N_{1_{r_1}}\right\}$ as set of the potential relays which can receive the data securely and successfully, i.e., $R_{0,1_u} \geq R_{\mathrm{S}}$, where $u = 1, 2, ..., r_1$, $0 \leq r_1 \leq M-1$, $N_{1_u} \in \{N_1, N_2, ..., N_{M-1}\}$. To select the relay for the retransmission, we also propose a distributed relay selection method. Similar to the work in [48], the relay N_{1_u} will set a timer given as

$$\omega_{1_u} = \frac{\mathrm{A}}{\lambda_{1_u,M}}, \tag{12}$$

where A is a predetermined constant.

Then, the relay whose timer expires first will broadcast the CTS message, and it be selected to retransmit the data to the destination. We can observe from Equation (12) that the selected relay is nearest to the destination. It is worth noting that, if the set $\mathcal{U}_1$ is empty ($r_1 = 0$), no relay node can retransmit the data to the destination, and this case is considereda secrecy outage event. In the case where $r_1 \geq 1$, the operation will be repeated with the new source.

Generally, at the kth time slot ($k \geq 1$), assume that the current source is N_{i_k}, $i_k \in \{0, 1, ..., M-1\}$ and $i_1 = 0$. Let $\mathcal{W}_k = \left\{N_{i_k+1}, N_{i_k+2}, ..., N_M\right\}$ denote set of relays from the node N_{i_k+1} to the destination. Similarly, N_{i_k} sends the RTS message to all of the nodes belonging to W_k. Then, if $R_{i_k,M} \geq R_{\mathrm{S}}$, the destination generates the CTS message, and N_{i_k} will directly transmit the data to N_M. Otherwise, the potential relay which belongs to W_k and is nearest to the destination will become the new source and repeat the process that N_{i_k} did. Indeed, we denote $\mathcal{U}_k$ as the set of the potential relays, i.e.,

$\mathcal{U}_k = \left\{N_{k_1}, N_{k_2}, ..., N_{k_{r_k}}\right\}$, where $\mathcal{U}_k \subset \mathcal{W}_k$, $0 \leq r_k \leq M - i_k$. In addition, let us denote $\mathcal{Z}_k = \left\{N_{k_{r_k+1}}, N_{k_{r_k+2}}, ..., N_{M-i_k}\right\}$ as set of the nodes that cannot receive the data securely, where $k_{r_k+1} < k_{r_k+2} < ... < k_{M-i_k}$ and $N_{k_{M-i_k}} \equiv N_M$. Then, assume that $k_1 < k_2 < ... < k_{r_k}$ and $r_k \geq 1$, using the relay selection method described above, the relay N_{k_r} will become the new source at the $(k+1)$th time slot.

This process is only stopped when N_M can securely and successfully receive the data or there is no relay between the current source and the destination that can securely and successfully receive the data. It is noted that, to avoid the eavesdropper and combine the received data with maximal ratio combining (MRC) technique, the source and the selected relays use randomize-and-forward (RF) method [49,50].

In the proposed protocol, to select the successful relay at each time slot correctly, the CSI estimations over the data, interference and eavesdropping links are assumed to be perfect. However, in practice, the estimations may not be correct due to the time variation of the channel, finite number of pilot symbols and noises. Hence, we will discuss this problem in the next sub-section.

2.3. Imperfect Channel Estimation

In this subsection, we consider the imperfect channel estimation at the transmitter N_i and the receiver N_j. From Equation (9), if N_j wants to calculate the secrecy capacity $R_{i,j}$, it has to estimate the channel coefficient h_{N_i,N_j} correctly. In addition, N_i has to estimate the channel coefficients $h_{N_i,\mathrm{PU}}$ and $h_{N_i,\mathrm{E}}$, which are then sent to N_j through the RTS message.

Let $h^e_{N_i,N_j}$, $h^e_{N_i,\mathrm{PU}}$ and $h^e_{N_i,\mathrm{E}}$ denote the estimated CSIs of h_{N_i,N_j}, $h^e_{N_i,\mathrm{PU}}$ and $h_{N_i,\mathrm{E}}$, respectively; the correlation between $h^e_{N_i,N_j}$ and h_{N_i,N_j}; $h^e_{N_i,\mathrm{PU}}$ and $h_{N_i,\mathrm{PU}}$; and $h^e_{N_i,\mathrm{E}}$ and $h_{N_i,\mathrm{E}}$ can be expressed, respectively as in [51]:

$$\begin{aligned} h^e_{N_i,N_j} &= \phi_{\mathrm{D}} h_{N_i,N_j} + \sqrt{1-\phi^2_{\mathrm{D}}}\varepsilon_{\mathrm{D}}, \\ h^e_{N_i,\mathrm{PU}} &= \phi_{\mathrm{P}} h_{N_i,\mathrm{PU}} + \sqrt{1-\phi^2_{\mathrm{P}}}\varepsilon_{\mathrm{P}}, \\ h^e_{N_i,\mathrm{E}} &= \phi_{\mathrm{E}} h_{N_i,\mathrm{E}} + \sqrt{1-\phi^2_{\mathrm{E}}}\varepsilon_{\mathrm{E}}, \end{aligned} \tag{13}$$

where ϕ_{D}, ϕ_{P} and ϕ_{E} are channel correlation factors, and ε_{D}, ε_{P} and ε_{E} are estimation errors. We can observe that if $\phi_{\mathrm{D}} = \phi_{\mathrm{P}} = \phi_{\mathrm{E}} = 1$, all of the channel estimations are perfect. If $\phi_{\mathrm{D}} < 1, \phi_{\mathrm{P}} < 1, \phi_{\mathrm{E}} < 1$, the channel estimations have errors, and the estimated secrecy capacity in Equation (9) is written by

$$R^e_{i,j} = \left[\log_2\left(\frac{1 + P\min\left(1, \frac{\mu}{\gamma^e_{i,\mathrm{P}}}\right)\gamma^e_{i,j}}{1 + P\min\left(1, \frac{\mu}{\gamma^e_{i,\mathrm{P}}}\right)\gamma^e_{i,\mathrm{E}}}\right)\right]^+, \tag{14}$$

where $\gamma^e_{i,j} = |h^e_{N_i,N_j}|^2$, $\gamma^e_{i,\mathrm{P}} = |h^e_{N_i,\mathrm{PU}}|^2$ and $\gamma^e_{i,\mathrm{E}} = |h^e_{N_i,\mathrm{E}}|^2$. Again, we note that the CSI estimation errors may lead to the incorrect relay selection, which would degrade the system performance.

2.4. Multi-Hop Direct Transmission Protocol

To show the advantages of the proposed protocol, we compared the secrecy performance of the proposed protocol with that of the conventional multi-hop direct transmission protocol (MDT) [44]. In the MDT scheme, the data are transmitted hop-by-hop from the source to the destination. Particularly, the data transmission is split into M orthogonal time slots. At the mth time slot, where $m = 1, 2, ..., M$, the node N_m transmits the source data to the node N_{m+1}. If the communication between N_m and N_{m+1} is secure and successful, N_{m+1} will forward the data to the next hop in the next time slot. Otherwise, the data transmission is insecure and the secrecy outage event occurs. Similar to the MCT protocol, the source and relays in the MDT protocol use the RF technique.

3. Performance Analysis

Firstly, we can formulate SOP of the $N_i \to N_j$ link as

$$\begin{aligned} \mathrm{SOP}_{i,j}^{\mathrm{DT}} &= \Pr\left(R_{i,j} < R_{\mathrm{S}}\right) \\ &= \Pr\left(\frac{1+\Psi_{i,j}}{1+\Psi_{i,E}} < \rho\right), \end{aligned} \tag{15}$$

where $\rho = 2^{R_{\mathrm{S}}}$ $(\rho > 1)$.

From Equations (9) and (15), it is straightforward that, if $\kappa > 0$, then

$$\mathrm{SOP}_{i,j}^{\mathrm{DT}} \overset{P\to+\infty}{\approx} 1. \tag{16}$$

When the transceiver hardware is perfect $(\kappa = 0)$, we can derive the exact closed-form expression for $\mathrm{SOP}_{i,j}^{\mathrm{DT}}$. At first, setting $x = \gamma_{i,\mathrm{P}}$, $\mathrm{SOP}_{i,j}^{\mathrm{DT}}$ conditioned on x can be given by

$$\mathrm{SOP}_{i,j}^{\mathrm{DT}}(x) = \Pr\left(\gamma_{i,j} < \frac{\rho-1}{P\min(1,\mu/x)} + \rho\gamma_{i,\mathrm{E}}\right). \tag{17}$$

Due to the independence of $\gamma_{i,j}$ and $\gamma_{i,\mathrm{E}}$, we can write

$$\mathrm{SOP}_{i,j}^{\mathrm{DT}}(x) = \int_0^{+\infty} f_{\gamma_{i,\mathrm{E}}}(y)\, F_{\gamma_{i_j}}\left(\frac{\rho-1}{P\min(1,\mu/x)} + \rho y\right) dy. \tag{18}$$

Substituting probability density function (PDF) of the exponential RV $\gamma_{i,\mathrm{E}}$ $\left(f_{\gamma_{i,\mathrm{E}}}(y) = \lambda_{i,\mathrm{E}}\exp\left(-\lambda_{i,\mathrm{E}}y\right)\right)$, and the cumulative distribution function (CDF) of the exponential RV $\gamma_{i,j}$ $\gamma_{i,\mathrm{E}}$ $\left(F_{\gamma_{i,j}}(y) = 1-\exp\left(-\lambda_{i,j}y\right)\right)$ into Equation (18), after some manipulations, we obtain

$$\mathrm{SOP}_{i,j}^{\mathrm{DT}}(x) = 1 - \frac{\lambda_{i,\mathrm{E}}}{\lambda_{i,\mathrm{E}}+\lambda_{i,j}\rho}\exp\left(-\frac{\rho-1}{P\min(1,\mu/x)}\right). \tag{19}$$

Then, $\mathrm{SOP}_{i,j}^{\mathrm{DT}}$ can be obtained from $\mathrm{SOP}_{i,j}^{\mathrm{DT}}(x)$ by

$$\mathrm{SOP}_{i,j}^{\mathrm{DT}} = \int_0^{+\infty} \mathrm{SOP}_{i,j}^{\mathrm{DT}}(x)\, f_{\gamma_{i,\mathrm{P}}}(x)\, dx. \tag{20}$$

Substituting Equation (19) and $f_{\gamma_{i,\mathrm{P}}}(y) = \lambda_{i,\mathrm{P}}\exp\left(-\lambda_{i,\mathrm{P}}y\right)$ into Equation (20), we obtain an exact closed-form expression of $\mathrm{SOP}_{i,j}^{\mathrm{DT}}$ as

$$\begin{aligned} \mathrm{SOP}_{i,j}^{\mathrm{DT}} &= \int_0^{\mu}\left(1-\frac{\lambda_{i,\mathrm{E}}}{\lambda_{i,\mathrm{E}}+\lambda_{i,j}\rho}\exp\left(-\frac{\rho-1}{P}\right)\right)\lambda_{i,\mathrm{P}}\exp\left(-\lambda_{i,\mathrm{P}}x\right)dx \\ &+ \int_{\mu}^{+\infty}\left(1-\frac{\lambda_{i,\mathrm{E}}}{\lambda_{i,\mathrm{E}}+\lambda_{i,j}\rho}\exp\left(-\frac{\rho-1}{P\mu}x\right)\right)\lambda_{i,\mathrm{P}}\exp\left(-\lambda_{i,\mathrm{P}}x\right)dx \\ &= 1-\frac{\lambda_{i,\mathrm{E}}}{\lambda_{i,\mathrm{E}}+\lambda_{i,j}\rho}\left[\left(1-\exp(-\lambda_{i,\mathrm{P}}\mu)\right)\exp\left(-\lambda_{i,j}\frac{\rho-1}{P}\right) + \frac{\lambda_{i,\mathrm{P}}P\mu}{\lambda_{i,\mathrm{P}}P\mu+\lambda_{i,j}(\rho-1)}\exp\left(-\lambda_{i,\mathrm{P}}\mu-\lambda_{i,j}\frac{\rho-1}{P}\right)\right]. \end{aligned} \tag{21}$$

Furthermore, using the approximation in Equation (11), an asymptotic closed-form expression for $\mathrm{SOP}_{i,j}^{\mathrm{DT}}$ at high P values can be provided by

$$\mathrm{SOP}_{i,j}^{\mathrm{DT}} \overset{P\to+\infty}{\approx} \Pr\left(\frac{\gamma_{i,j}}{\gamma_{i,\mathrm{E}}} < \rho\right) = 1 - \frac{\lambda_{i,\mathrm{E}}}{\lambda_{i,\mathrm{E}}+\lambda_{i,j}\rho}. \tag{22}$$

3.1. Multi-hop Direct Transmission Protocol (MDT)

Because the transmission on each hop is independent, the end-to-end SOP of the MDT protocol can be given as

$$\mathrm{SOP}_{0,M}^{\mathrm{MDT}} = 1 - \prod_{m=1}^{M} \left(1 - \mathrm{SOP}_{m-1,m}^{\mathrm{DT}}\right). \tag{23}$$

As $\kappa = 0$, substituting Equation (21) into Equation (23), we obtain an exact closed-form expression for the end-to-end SOP of the MDT protocol as

$$\mathrm{SOP}_{0,M}^{\mathrm{MDT}} = 1 - \prod_{m=1}^{M} \left\{ \frac{\lambda_{m-1,\mathrm{E}}}{\lambda_{m-1,\mathrm{E}} + \lambda_{i,j}\rho} \left[\begin{array}{l} \left(1 - \exp\left(-\lambda_{m-1,\mathrm{P}}\mu\right)\right) \exp\left(-\lambda_{m-1,m}\frac{\rho-1}{P}\right) \\ + \frac{\lambda_{m-1,\mathrm{P}}P\mu}{\lambda_{m-1,\mathrm{P}}P\mu + \lambda_{m-1,m}(\rho-1)} \exp\left(-\lambda_{m-1,\mathrm{P}}\mu - \lambda_{m-1,m}\frac{\rho-1}{P}\right) \end{array} \right] \right\}. \tag{24}$$

At high P regions, using Equation (22), an approximate expression for Equation (24) can be obtained by

$$\mathrm{SOP}_{0,M}^{\mathrm{MDT}} \overset{P\to+\infty}{\approx} 1 - \prod_{m=1}^{M} \frac{\lambda_{m-1,\mathrm{E}}}{\lambda_{m-1,\mathrm{E}} + \lambda_{m-1,m}\rho}. \tag{25}$$

3.2. Cooperative Multi-Hop Transmission Protocol (CMT)

In the CMT protocol, the end-to-end SOP is expressed by a recursive expression as follows:

$$\begin{aligned} \mathrm{SOP}_{N_{i_k},\mathcal{U}_k}^{\mathrm{CMT}} &= \sum_{\mathcal{U}_k} \Pr\left(\begin{array}{l} \frac{1+\Psi_{i_k,k_1}}{1+\Psi_{i_k,\mathrm{E}}} \geq \rho, \frac{1+\Psi_{i_k,k_2}}{1+\Psi_{i_k,\mathrm{E}}} \geq \rho, ..., \frac{1+\Psi_{i_k,k_{r_k}}}{1+\Psi_{i_k,\mathrm{E}}} \geq \rho, \\ \frac{1+\Psi_{i_k,k_{r_k+1}}}{1+\Psi_{i_k,\mathrm{E}}} < \rho, \frac{1+\Psi_{i_k,k_{r_k+2}}}{1+\Psi_{i_k,\mathrm{E}}} < \rho, ..., \frac{1+\Psi_{i_k,k_{M-i_k}}}{1+\Psi_{i_k,\mathrm{E}}} < \rho \end{array} \right) \\ &= \sum_{\mathcal{U}_k} \Pr\left(\begin{array}{l} \frac{1+P\min\left(1,\mu/\gamma_{i_k,\mathrm{P}}\right)\gamma_{i_k,k_1}}{1+P\min\left(1,\mu/\gamma_{i_k,\mathrm{P}}\right)\gamma_{i_k,\mathrm{E}}} \geq \rho, \frac{1+P\min\left(1,\mu/\gamma_{i_k,\mathrm{P}}\right)\gamma_{i_k,k_2}}{1+P\min\left(1,\mu/\gamma_{i_k,\mathrm{P}}\right)\gamma_{i_k,\mathrm{E}}} \geq \rho, ..., \\ \frac{1+P\min\left(1,\mu/\gamma_{i_k,\mathrm{P}}\right)\gamma_{i_k,k_{r_k}}}{1+P\min\left(1,\mu/\gamma_{i_k,\mathrm{P}}\right)\gamma_{i_k,\mathrm{E}}} \geq \rho, \\ \frac{1+P\min\left(1,\mu/\gamma_{i_k,\mathrm{P}}\right)\gamma_{i_k,k_{r_k+1}}}{1+P\min\left(1,\mu/\gamma_{i_k,\mathrm{P}}\right)\gamma_{i_k,E}} < \rho, \frac{1+P\min\left(1,\mu/\gamma_{i_k,\mathrm{P}}\right)\gamma_{i_k,k_{r_k+2}}}{1+P\min\left(1,\mu/\gamma_{i_k,\mathrm{P}}\right)\gamma_{i_k,\mathrm{E}}} < \rho, ..., \\ \frac{1+P\min\left(1,\mu/\gamma_{i_k,\mathrm{P}}\right)\gamma_{i_k,k_{M-i_k}}}{1+P\min\left(1,\mu/\gamma_{i_k,\mathrm{P}}\right)\gamma_{i_k,\mathrm{E}}} < \rho \end{array} \right), \end{aligned} \tag{26}$$

where $\mathrm{SOP}_{N_{i_k},\mathcal{U}_k}^{\mathrm{CMT}}$ is SOP at kth time slot, $k = 1, 2, ..., M$. Then, the end-to-end SOP of the CMT protocol is given as

$$\mathrm{SOP}_{0,M}^{\mathrm{CMT}} = \mathrm{SOP}_{N_0,\mathcal{U}_1}^{\mathrm{CMT}}. \tag{27}$$

Before calculating $\mathrm{SOP}_{N_{i_k},\mathcal{U}_k}^{\mathrm{CMT}}$, we give an example with $M = 3$, where $\mathrm{SOP}_{0,3}^{\mathrm{CMT}}$ is expressed by

$$\begin{aligned} \mathrm{SOP}_{0,3}^{\mathrm{CMT}} = \mathrm{SOP}_{N_0,\{\emptyset\}}^{\mathrm{CMT}} + \mathrm{SOP}_{N_0,\{N_1\}}^{\mathrm{CMT}} + \mathrm{SOP}_{N_0,\{N_2\}}^{\mathrm{CMT}} \\ + \mathrm{SOP}_{N_0,\{N_1,N_2\}}^{\mathrm{CMT}}. \end{aligned} \tag{28}$$

Equation (28) shows that there are 04 possible cases for the set $\mathcal{U}_1$, i.e., $\mathcal{U}_1 = \{\emptyset\}$, $\mathcal{U}_1 = \{N_1\}$, $\mathcal{U}_1 = \{N_2\}$, $\mathcal{U}_1 = \{N_1, N_2\}$. In Equation (28), the terms $\mathrm{SOP}_{N_0,\{\emptyset\}}^{\mathrm{CMT}}$ and $\mathrm{SOP}_{N_0,\{N_2\}}^{\mathrm{CMT}}$ can be calculated as in (32). Considering the term $\mathrm{SOP}_{N_0,\{N_1\}}^{\mathrm{CMT}}$, which can be written by

$$\mathrm{SOP}^{\mathrm{CMT}}_{N_0,\{N_1\}} = \mathrm{SOP}^{\mathrm{CMT}}_{N_1,\mathcal{U}_2} = \mathrm{SOP}^{\mathrm{CMT}}_{N_1,\{\emptyset\}} + \mathrm{SOP}^{\mathrm{CMT}}_{N_1,\{N_2\}}. \tag{29}$$

In Equation (29), there are two possible cases for the set $\mathcal{U}_2$, i.e., $\mathcal{U}_2 = \{\emptyset\}$, $\mathcal{U}_2 = \{N_2\}$, and $\mathrm{SOP}^{\mathrm{CMT}}_{N_1,\{\emptyset\}}$ and $\mathrm{SOP}^{\mathrm{CMT}}_{N_1,\{N_2\}}$ are SOP at the second time slots. In addition, $\mathrm{SOP}^{\mathrm{CMT}}_{N_1,\{\emptyset\}}$ is calculated by Equation (32), while $\mathrm{SOP}^{\mathrm{CMT}}_{N_1,\{N_2\}}$ is expressed by

$$\mathrm{SOP}^{\mathrm{CMT}}_{N_1,\{N_2\}} = \mathrm{SOP}^{\mathrm{DT}}_{2,3}, \tag{30}$$

where, because the transmission between N_2 and N_3 is direct, Equation (21) is used to calculate $\mathrm{SOP}^{\mathrm{CMT}}_{N_1,\{N_2\}}$.

Next, let us consider the term $\mathrm{SOP}^{\mathrm{CMT}}_{N_0,\{N_1,N_2\}}$ in Equation (28), where the relay N_2 will be selected for retransmitting the data to the destination. Similar to Equation (30), we have

$$\mathrm{SOP}^{\mathrm{CMT}}_{N_0,\{N_1,N_2\}} = \mathrm{SOP}^{\mathrm{DT}}_{2,3}. \tag{31}$$

Now, the recursive expression of $\mathrm{SOP}^{\mathrm{CMT}}_{N_{i_k},\mathcal{U}_k}$ is given as in Lemma 1.

Lemma 1. *When* $\kappa = 0$, $\mathrm{SOP}^{\mathrm{CMT}}_{N_{i_k},\mathcal{U}_k}$ *can be expressed as*

$$\begin{aligned}
\mathrm{SOP}^{\mathrm{CMT}}_{N_{i_k},\mathcal{U}_k} = {} & \sum_{\mathcal{U}_k} \frac{\lambda_{i_k,\mathrm{E}}}{\lambda_{i_k,\mathrm{E}} + \sum\limits_{t=1}^{r_k} \lambda_{i_k,k_t}\rho} \left[\begin{array}{l} \exp\left(-\sum\limits_{t=1}^{r_k} \frac{\lambda_{i_k,k_t}(\rho-1)}{P}\right)\left(1-\exp\left(-\lambda_{i_k,\mathrm{P}}\mu\right)\right) \\ + \frac{\lambda_{i_k,\mathrm{P}}P\mu}{\lambda_{i_k,\mathrm{P}}P\mu + \sum\limits_{t=1}^{r_k}\lambda_{i_k,k_t}(\rho-1)} \exp\left(-\lambda_{i_k,\mathrm{P}}\mu - \sum\limits_{t=1}^{r_k}\lambda_{i_k,k_t}\frac{(\rho-1)}{P}\right) \end{array} \right] \\
& + \sum_{\mathcal{U}_k} \sum_{v=1}^{M-i_k-r_k} (-1)^v \sum_{\substack{N_{j_1},\ldots,N_{j_v}\in\mathcal{Z}_k \\ j_1<j_2<\ldots<j_v}}^{M-i_k-r_k} \frac{\lambda_{i_k,\mathrm{E}}}{\lambda_{i_k,\mathrm{E}} + \left(\sum\limits_{t=1}^{v}\lambda_{i_k,j_v} + \sum\limits_{t=1}^{r_k}\lambda_{i_k,k_t}\right)\rho} \\
& \times \left[\begin{array}{l} \exp\left(-\left(\sum\limits_{t=1}^{v}\lambda_{i_k,j_v} + \sum\limits_{t=1}^{r_k}\lambda_{i_k,k_t}\right)\frac{\rho-1}{P}\right)\left(1-\exp\left(-\lambda_{i_k,\mathrm{P}}\mu\right)\right) \\ + \frac{\lambda_{i_k,\mathrm{P}}P\mu}{\lambda_{i_k,\mathrm{P}}P\mu + \left(\lambda_{i_k,\mathrm{E}} + \sum\limits_{t=1}^{r_k}\lambda_{i_k,k_t}\right)(\rho-1)} \exp\left(-\lambda_{i_k,\mathrm{P}}\mu - \left(\sum\limits_{t=1}^{v}\lambda_{i_k,j_v} + \sum\limits_{t=1}^{r_k}\lambda_{i_k,k_t}\right)\frac{\rho-1}{P}\right) \end{array} \right].
\end{aligned} \tag{32}$$

Proof. At first, we set $x = \gamma_{i_k,\mathrm{E}}$ and $y = \gamma_{i_k,\mathrm{P}}$, and $\mathrm{SOP}^{\mathrm{CMT}}_{N_{i_k},\mathcal{U}_k}$ conditioned on x and y can be given by

$$\begin{aligned}
& \mathrm{SOP}^{\mathrm{CMT}}_{N_{i_k},\mathcal{U}_k}(x,y) \\
& = \sum_{\mathcal{U}_k} \left[\prod_{t=1}^{r_k} \exp\left(-\lambda_{i_k,k_t}\left(\frac{\rho-1}{P\min(1,\mu/y)} + \rho x\right)\right) \prod_{v=1}^{M-i_k-r_k} \left(1-\exp\left(-\lambda_{i_k,k_v}\left(\frac{\rho-1}{P\min(1,\mu/y)} + \rho x\right)\right)\right)\right] \\
& = \sum_{\mathcal{U}_k} \exp\left(-\sum_{t=1}^{r_k}\lambda_{i_k,k_t}\left(\frac{\rho-1}{P\min(1,\mu/y)} + \rho x\right)\right) \\
& + \sum_{\mathcal{U}_k} \sum_{v=1}^{M-i_k-r_k} (-1)^v \sum_{\substack{N_{j_1},\ldots,N_{j_v}\in\mathcal{Z}_k \\ j_1<j_2<\ldots<j_v}}^{M-i_k-r_k} \exp\left(-\left(\sum_{t=1}^{v}\lambda_{i_k,j_v} + \sum_{t=1}^{r_k}\lambda_{i_k,k_t}\right)\left(\frac{\rho-1}{P\min(1,\mu/y)} + \rho x\right)\right).
\end{aligned} \tag{33}$$

Then, $\mathrm{SOP}^{\mathrm{CMT}}_{N_{i_k},\mathcal{U}_k}$ is obtained from $\mathrm{SOP}^{\mathrm{CMT}}_{N_{i_k},\mathcal{U}_k}(x,y)$ by

$$\mathrm{SOP}^{\mathrm{CMT}}_{N_{i_k},\mathcal{U}_k} = \int_0^{+\infty} f_{\gamma_{i_k,\mathrm{P}}}(y) \underbrace{\left[\int_0^{+\infty} f_{\gamma_{i_k,\mathrm{E}}}(x)\, \mathrm{SOP}^{\mathrm{CMT}}_{N_{i_k},\mathcal{U}_k}(x,y)\, dx\right]}_{\mathcal{I}_1} dy. \tag{34}$$

Let us consider the integral $\mathcal{I}_1$ marked in Equation (34); combining the PDF $f_{\gamma_{i_k,\mathrm{E}}}$ and Equation (33), after some careful manipulations, we obtain

$$\begin{aligned}\mathcal{I}_1 = &\sum_{U_k} \frac{\lambda_{i_k,\mathrm{E}}}{\lambda_{i_k,\mathrm{E}} + \sum_{t=1}^{r_k} \lambda_{i_k,k_t}\rho} \exp\left(-\sum_{t=1}^{r_k} \frac{\lambda_{i_k,k_t}(\rho-1)}{P\min(1,\mu/y)}\right)\\ &+\sum_{U_k}\sum_{v=1}^{M-i_k-r_k}(-1)^v \sum_{\substack{N_{j_1},\ldots,N_{j_v}\in Z_k\\ j_1<j_2<\ldots<j_v}}^{M-i_k-r_k} \frac{\lambda_{i_k,\mathrm{E}}}{\lambda_{i_k,\mathrm{E}} + \left(\sum_{t=1}^{v}\lambda_{i_k,j_v} + \sum_{t=1}^{r_k}\lambda_{i_k,k_t}\right)\rho}\\ &\times \exp\left(-\left(\sum_{t=1}^{v}\lambda_{i_k,j_v} + \sum_{t=1}^{r_k}\lambda_{i_k,k_t}\right)\frac{\rho-1}{P\min(1,\mu/y)}\right).\end{aligned} \tag{35}$$

Next, substituting Equation (35) into Equation (34), and after some manipulations, we obtain Equation (32) and finish the proof.

Then, at high transmit power, i.e., $P \to +\infty$, using Equation (11), and with the same manner as derived in Equation (32), an asymptotic expression of $\mathrm{SOP}^{\mathrm{CMT}}_{N_{i_k},\mathcal{U}_k}$ can be given by

$$\begin{aligned}\mathrm{SOP}^{\mathrm{CMT}}_{N_{i_k},\mathcal{U}_k} \overset{P\to+\infty}{\approx} &\sum_{U_k} \frac{\lambda_{i_k,\mathrm{E}}}{\lambda_{i_k,\mathrm{E}} + \sum_{t=1}^{r_k}\lambda_{i_k,k_t}\rho}\\ &+\sum_{U_k}\sum_{v=1}^{M-i_k-r_k}(-1)^v \sum_{\substack{N_{j_1},\ldots,N_{j_v}\in Z_k\\ j_1<j_2<\ldots<j_v}}^{M-i_k-r_k} \frac{\lambda_{i_k,\mathrm{E}}}{\lambda_{i_k,\mathrm{E}} + \left(\sum_{t=1}^{v}\lambda_{i_k,j_v} + \sum_{t=1}^{r_k}\lambda_{i_k,k_t}\right)\rho}.\end{aligned} \tag{36}$$

Finally, it is worth noting from Equations (25) and (36) that the asymptotic formulas of SOP do not depend on P. □

4. Simulation Results

In this section, we present various Monte Carlo simulations to verify the theoretical results derived in Section 3. For the simulation environment, we considered a two-dimensional network in which the co-ordinate of the node N_i $(i = 0, 1, ..., M)$, the primary user, and the eavesdropper are $(0, i/M)$, $(x_{\mathrm{PU}}, y_{\mathrm{PU}})$ and $(x_{\mathrm{E}}, y_{\mathrm{E}})$, respectively. To focus on investigating the impact of the important system parameters on the system performance, in all of the simulations, the path-loss exponent β was fixed by 3.

In Figure 2, we present the end-to-end SOP of the MDT and CMT protocols as a function of the transmit SNR $\left(P = P_{\mathrm{th}}/\sigma_0^2\right)$ in dB, and investigate the impact of the CSI estimation errors on the secrecy performance. In this simulation, we assumed the CSI estimations of the interference links are correct, i.e., $\phi_{\mathrm{P}} = 1$, and the transceiver hardware is perfect, i.e., $\kappa = 0$. We also set the simulation parameters as follows: the target rate $R_{\mathrm{S}} = 0.2$, the ratio $\mu = 0.5$, and the number of hops M = 3. In addition, we placed the primary user and the eavesdropper at the positions $(-0.5, -1)$ and $(0.5, 0.5)$, respectively. As shown in Figure 2, when the estimations of the data and eavesdropping channels were correct, i.e., $\phi_{\mathrm{D}} = \phi_{\mathrm{E}} = 1$, the performance of the proposed protocol (CMT) was much better than that of the MDT protocol. However, the SOP performance of the CMT protocol significantly decreased with the

CSI estimation errors. Moreover, when $\phi_D = 0.95$ and $\phi_E = 0.9$, the MDT protocol outperformed the proposed protocol.

In Figure 3, we present the end-to-end SOP of the MDT and CMT protocols as a function of the transmit SNR $\left(P = P_{th}/\sigma_0^2\right)$ in dB when all of the channel estimations are perfect, i.e., $\phi_D = \phi_P = \phi_E = 1$. As we can see, the proposed protocol (CMT) outperformed the MDT protocol for all the P values because the destination and the intermediate relays in the CMT protocol could obtain higher diversity gain as compared with those in the MDT protocol. As a result, the proposed protocol enhanced the channel capacity of the data links, which hence provided better secrecy performance. In addition, it was observed that, when the transceiver hardware was perfect $(\kappa = 0)$, the secrecy performance of both protocols converged to the asymptotic results, which were independent of the P values. However, as $\kappa = 0.2$, the values of SOP reached 1 at high region, which validated the statement in Section 3. Moreover, there existed a value of P at which the value of SOP was lowest. As shown in this figure, the optimal transmit SNRs in the CMT and MDT protocols were -5 dB and -7.5 dB, respectively. Finally, it is worth noting that the simulation results (Sim) match very well with the theoretical results (Exact), and, at high P regimes, the simulation results nicely converge to the asymptotic ones (Asym). These validate the correction of our derivations expressed in Section 3.

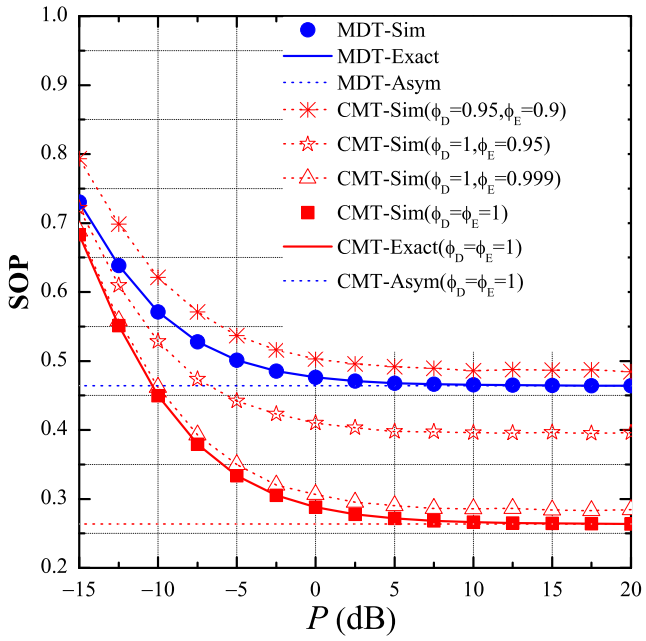

Figure 2. End-to-end secrecy outage probability (SOP) as function of P in dB when $P \in [-15\,\text{dB}, 20\,\text{dB}]$, $\mu = 0.5$, $M = 3$, $R_S = 0.2$, $\kappa = 0$, $(x_{PU}, y_{PU}) = (-0.5, -1)$ and $(x_E, y_E) = (0.5, 0.5)$.

As shown in Figure 4, we changed the number of hops (M) and observed the variant of the end-to-end SOP. We assigned the values of P, μ, R_S, x_{PU}, y_{PU}, x_E, and y_E as 5 dB, 1, 0.5, -0.5, -0.5, 0.5 and 0.5, respectively. As observed, with the perfect transceiver, the secrecy performance of the MDT and CMT protocols was better when the number of hops increased. For the CMT protocol, this result is still true with the presence of the hardware imperfection ($\kappa = 0.1$), while the performance of the MDT protocol severely degraded with higher number of hops. Again, the results in this figure validate the theoretical results provided in the previous section.

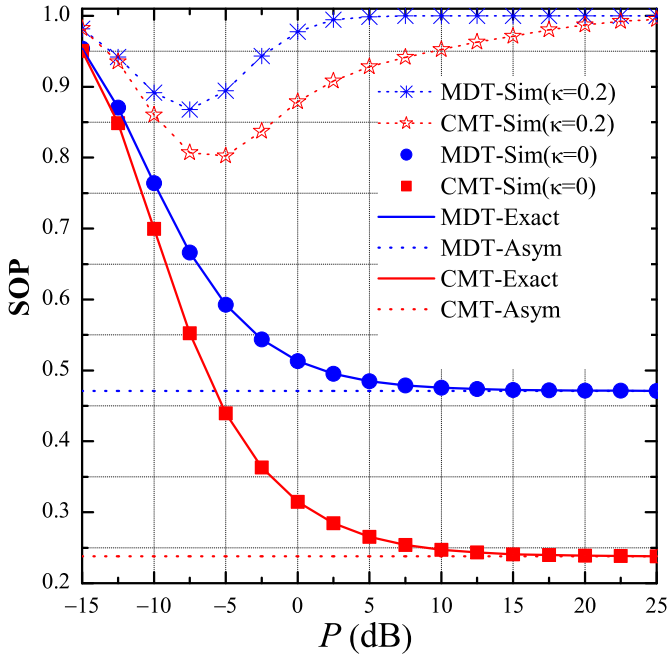

Figure 3. End-to-end secrecy outage probability (SOP) as function of P in dB when $P \in [-15\,\text{dB}, 25\,\text{dB}]$, $\mu = 0.5$, $M = 4$, $R_S = 1$, $\kappa \in \{0, 0.2\}$, $(x_{PU}, y_{PU}) = (-0.5, -1)$, $(x_E, y_E) = (0.5, 0.5)$ and $\phi_D = \phi_P = \phi_E = 1$.

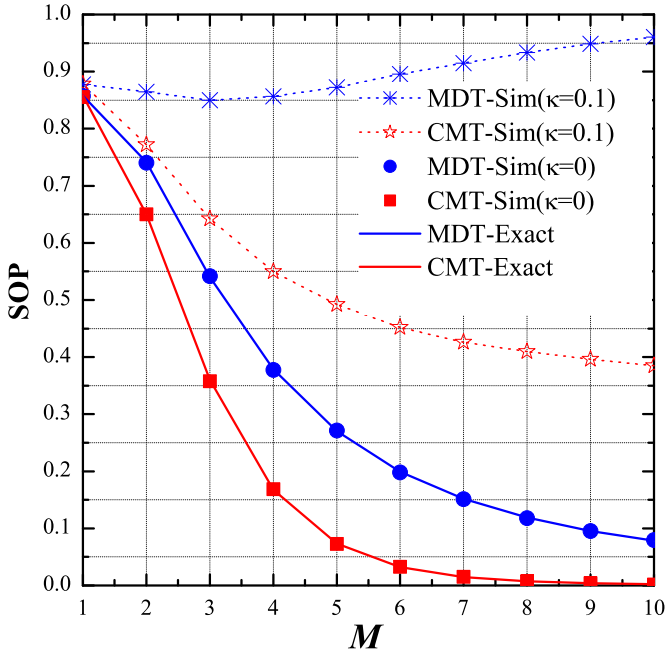

Figure 4. End-to-end secrecy outage probability (SOP) as function of M when $P = 5\,\text{dB}$, $\mu = 1$, $M \in [1, 10]$, $R_S = 0.5$, $\kappa \in \{0, 0.1\}$, $(x_{PU}, y_{PU}) = (-0.5, -0.5)$, $(x_E, y_E) = (0.5, 0.5)$ and $\phi_D = \phi_P = \phi_E = 1$.

Figure 5 presents the impact of the hardware impairment level (κ) on the secrecy performance of the CMT and MDT protocols when $P = 0$ dB, $\mu = 1$, $M = 4$, $x_{PU} = -0.5$, $y_{PU} = -1$, $x_E = 0.5$ and $y_E = 0.5$. Similarly, the proposed scheme obtained better performance, as compared the MDT scheme. It is also seen in Figure 5 that the SOP values rapidly increase as the κ value increases. In addition, the performance of the considered methods significantly enhanced with lower value of the target rate R_S.

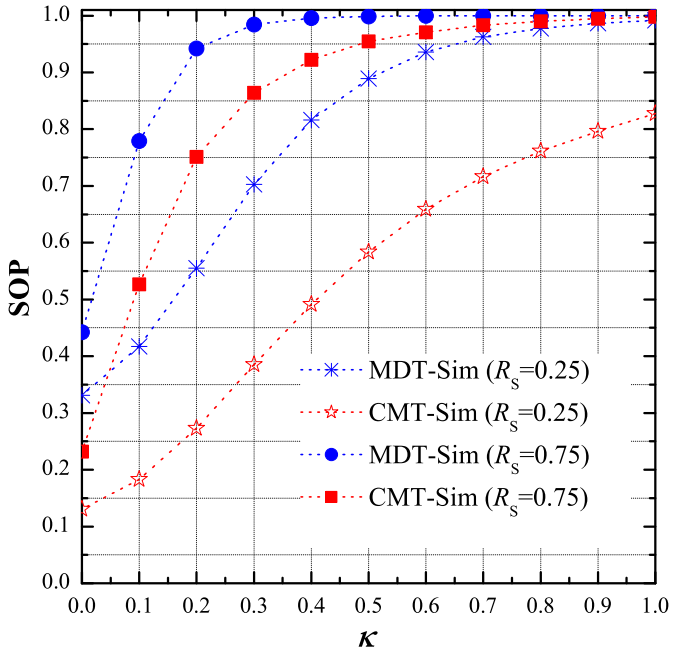

Figure 5. End-to-end secrecy outage probability (SOP) as function of κ when $P = 0$ dB, $\mu = 1$, $M = 4$, $R_S \in \{0.25, 0.75\}$, $\kappa \in [0, 1]$, $(x_{PU}, y_{PU}) = (-0.5, -1)$, $(x_E, y_E) = (0.5, 0.5)$ and $\phi_D = \phi_P = \phi_E = 1$.

As shown in Figure 6, we studied the effect of the positions of the eavesdropper on the end-to-end SOP. In particular, we fixed the value of y_E while changing x_E from 0 to 1. The remaining parameters were set as: $P = 10$ dB, $\mu = 1$, $M = 4$, $R_S = 1$, $\kappa = 0$, $x_{PU} = -0.5$ and $y_{PU} = -0.1$. It can be seen that the end-to-end SOP of the CMT protocol mostly decreased with the increasing of x_E, while that of the MDT increased at small x_E value and decreased at high x_E region. We can see in this figure that the performance of the MDT protocol was worst when x_E was about 0.4.

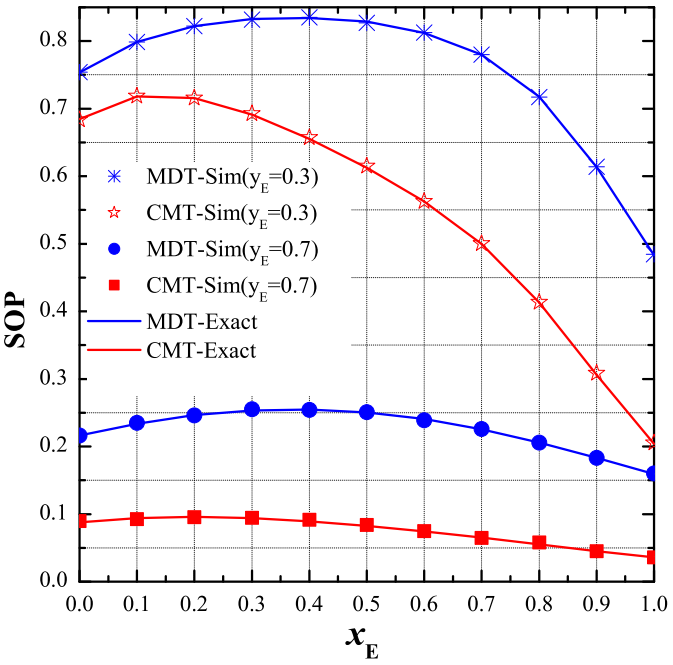

Figure 6. End-to-end secrecy outage probability (SOP) as function of x_E when $P = 10$ dB, $\mu = 1$, $M = 4$, $R_S = 1$, $\kappa = 0$, $(x_{PU}, y_{PU}) = (-0.5, -1)$, $y_E \in \{0.3, 0.7\}$ and $\phi_D = \phi_P = \phi_E = 1$.

5. Conclusions

In this paper, we propose the cooperative multi-hop transmission protocol (CMT) in the UCR networks with the presence of an eavesdropper. Because the proposed scheme uses cooperative multi-hop transmission, it significantly outperforms the conventional multi-hop direct transmission protocol (MDT), in terms of the end-to-end secrecy outage probability (SOP). The interesting results obtained in this paper can be listed as follows:

- The secrecy performance of the proposed protocol was much better than that of the MDT protocol when the CSI estimations of the data, interference and eavesdropping links were perfect. Otherwise, the SOP performance significantly degraded due to the incorrect relay selection.
- When the transceiver hardware of the nodes was imperfect, the secrecy performance severely degraded. In particular, the value of the end-to-end SOP rapidly increased with higher transmit signal-to-noise ratio (SNR) and with higher impairment level.
- In the presence of the hardware noises, there existed an optimal value of the transmit SNR, at which the secrecy performance of the CMT and DMT schemes was best.
- The performance of the proposed protocol was better when the number of hops was higher.
- When the hardware impairments were relaxed, we derived exact and asymptotic expressions of the end-to-end SOP for the CMT and MDT protocols. We then performed computer simulations to verify the derived expressions.

Author Contributions: P.T.T., D.T.H. and T.N.N. created the main ideas and executed the performance evaluation by extensive simulations. T.T.D. and M.V. worked as the advisers of P.T.T., D.T.H. and T.N.N. to discuss, create, and advise the main ideas and performance evaluations together.

Acknowledgments: This research received support from the grant SGS reg. No. SP2019/41 conducted at VSB Technical University of Ostrava, Czech Republic and was partially funded by Vietnam National Foundation for Science and Technology Development (NAFOSTED) under grant number 102.04-2017.317.

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

References

1. Ledwaba, L.P.I.; Hancke, G.P.; Venter, H.S.; Isaac, S.J. Performance Costs of Software Cryptography in Securing New-Generation Internet of Energy Endpoint Devices. *IEEE Access* **2018**, *6*, 9303–9323. [CrossRef]
2. Liu, Z.; Choo, K.-K.R.; Grossschadl, J. Securing Edge Devices in the Post-Quantum Internet of Things Using Lattice-Based Cryptography. *IEEE Commun. Mag.* **2018**, *56*, 158–162. [CrossRef]
3. Wyner, A.D. The Wire-tap Channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387, [CrossRef]
4. Csiszar, I.; Korner, J. Broadcast Channels With Confidential Messages. *IEEE Trans. Inf. Theory* **1978**, *24*, 339–348. [CrossRef]
5. Gopala, P.K.; Lai, L.; Gamal, H.E. On the secrecy capacity of fading channels. *IEEE Trans. Inf. Theory* **2008**, *54*, 4687–4698. [CrossRef]
6. Zhang, J.; Duong, T.Q.; Woods, R.; Marshall, A. Securing Wireless Communications of the Internet of Things from the Physical Layer, An Overview. *Entropy* **2017**, *19*, 420. [CrossRef]
7. Chang, S.; Li, J.; Fu, X.; Zhang, L. Energy Harvesting for Physical Layer Security in Cooperative Networks Based on Compressed Sensing. *Entropy* **2017**, *19*, 462. [CrossRef]
8. Sun, L.; Du, Q. A Review of Physical Layer Security Techniques for Internet of Things: Challenges and Solutions. *Entropy* **2018**, *20*, 730. [CrossRef]
9. Wang, L.; Wong, K.-K.; Jin, S.; Zheng, G.; Heath, R.W. A New Look at Physical Layer Security, Caching, and Wireless Energy Harvesting for Heterogeneous Ultra-Dense Networks. *IEEE Commun. Mag.* **2018**, *56*, 49–55. [CrossRef]
10. Kong, L.; Vuppala, S.; Kaddoum, G. Secrecy Analysis of Random MIMO Wireless Networks Over α-μ Fading Channels. *IEEE Trans. Veh. Technol.* **2018**, *67*, 11654–11666. [CrossRef]
11. Jameel, F.; Wyne, S.; Kaddoum, G.; Duong, T.Q. A Comprehensive Survey on Cooperative Relaying and Jamming Strategies for Physical Layer Security. *IEEE Commun. Surv. Tutor.* **2018**. [CrossRef]
12. Krikidis, I. Opportunistic Relay Selection For Cooperative Networks With Secrecy Constraints. *IET Commun.* **2010**, *4*, 1787–1791. [CrossRef]

13. Zhong, B.; Zhang, Z. Secure Full-Duplex Two-Way Relaying Networks With Optimal Relay Selection. *IEEE Commun. Lett.* **2017**, *21*, 1123–1126. [CrossRef]
14. Kuhestani, A.; Mohammadi, A.; Mohammadi, M. Joint Relay Selection and Power Allocation in Large-Scale MIMO Systems With Untrusted Relays and Passive Eavesdroppers. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 341–355. [CrossRef]
15. Hu, L.; Wen, H.; Wu, B.; Pan, F.; Liao, R.-F.; Song, H.; Tang, J.; Wang, X. Cooperative Jamming for Physical Layer Security Enhancement in Internet of Things. *IEEE Int. Things J.* **2018**, *5*, 219–228. [CrossRef]
16. Ma, H.; Cheng, J.; Wang X.; Ma, P. Robust MISO Beamforming With Cooperative Jamming for Secure Transmission From Perspectives of QoS and Secrecy Rate. *IEEE Trans. Commun.* **2018**, *66*, 767–780. [CrossRef]
17. 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]
18. Hu, L.; Wen, H.; Wu, B.; Tang, J.; Pan, F.; Liao, R.-F. Cooperative-Jamming-Aided Secrecy Enhancement in Wireless Networks With Passive Eavesdroppers. *IEEE Trans. Veh. Technol.* **2018**, *67*, 2108–2117. [CrossRef]
19. Singh, A.; Bhatnagar, M.R.; Mallik, R.K. Secrecy Outage of a Simultaneous Wireless Information and Power Transfer Cognitive Radio System. *IEEE Wirel. Commun. Lett.* **2016**, *5*, 288–291. [CrossRef]
20. Lei, H.; Zhang, H.; Ansari, I.S.; Pan, G.; Qaraqe, K.A. Secrecy Outage Analysis for SIMO Underlay Cognitive Radio Networks over Generalized-K Fading Channels. *IEEE Sig. Process. Lett.* **2016**, *23*, 1106–1110. [CrossRef]
21. Zhao, R.; Yuan, Y.; Fan, L.; He, Y.-C. Secrecy Performance Analysis of Cognitive Decode-and-Forward Relay Networks in Nakagami-m Fading Channels. *IEEE Trans. Commun.* **2017**, *65*, 549–563. [CrossRef]
22. Chakraborty, P.; Prakriva, S. Secrecy Outage Performance of a Cooperative Cognitive Relay Network. *IEEE Commun. Lett.* **2017**, *21*, 326–329. [CrossRef]
23. Al-Hraishawi, H.; Baduge, G.A.A.; Schaefer, R.F. Artificial Noise-Aided Physical Layer Security in Underlay Cognitive Massive MIMO Systems with Pilot Contamination. *Entropy* **2017**, *19*, 349. [CrossRef]
24. Hung, T.; Georges, K.; Gagnon, F.; Louis, S. Cognitive Radio Network with Secrecy and Interference Constraints. *Phys. Commun.* **2017**, *22*, 32–41.
25. Ping, X.; Ling, X.; Honghai, W.; Jung, T.S.; Ilsun, Y. Cooperative Jammer Selection for Secrecy Improvement in Cognitive Internet of Things. *Sensors* **2018**, *18*, 42–57.
26. Feng, R.; Li, Q.; Zhang, Q.; Qin, J. Robust Secure Beamforming in MISO Full-Duplex Two-Way Secure Communications. *IEEE Trans. Veh. Technol.* **2016**, *65*, 408–414. [CrossRef]
27. Sun, C.; Liu, K.; Zheng D.; Ai, W. Secure Communication for Two-Way Relay Networks with Imperfect CSI. *Entropy* **2017**, *19*, 522. [CrossRef]
28. 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]
29. 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]
30. Lee, J.-H.; Sohn, I.; Kim, Y.-H. Transmit Power Allocation for Physical Layer Security in Cooperative Multi-Hop Full-Duplex Relay Networks. *Sensors* **2016**, *16*, 1726. [CrossRef] [PubMed]
31. Alotaibi, E.R.; Hamdi, K.A. Secure Relaying in Multihop Communication Systems. *IEEE Commun. Lett.* **2016**, *20*, 1120–1123. [CrossRef]
32. Yao, J.; Liu, Y. Secrecy Rate Maximization With Outage Constraint in Multihop Relaying Networks. *IEEE Commun. Lett.* **2018**, *22*, 304–307. [CrossRef]
33. Keshav, S; Ku, M.-L.; Biswas, S.; Ratnarajah, T. Energy-Efficient Subcarrier Pairing and Power Allocation for DF Relay Networks with an Eavesdropper. *Energies* **2017**, *10*, 1953.
34. Björnson, E.; Matthaiou, M.; Debbah, M. A new look at dual-hop relaying: Performance limits with hardware impairments. *IEEE Trans. Commun.* **2013**, *61*, 4512–4525. [CrossRef]
35. Matthaiou, M.; Papadogiannis, A. Two-Way Relaying Under The Presence of Relay Transceiver Hardware Impairments. *IEEE Commun. Lett.* **2013**, *17*, 1136–1139. [CrossRef]
36. Björnson, E.; Hoydis, J.; Kountouris, M.; Debbah, M. Massive MIMO Systems With Non-Ideal Hardware: Energy Efficiency, Estimation, and Capacity Limits. *IEEE Trans. Inf. Theory* **2014**, *60*, 7112–7139. [CrossRef]
37. Guo, K.; Guo, D.; Zhang, B. Performance Analysis of Two-Way Multi-Antenna Multi-Relay Networks with Hardware Impairments. *IEEE Access* **2017**, *5*, 15971–15980. [CrossRef]
38. Balti, E.; Guizani; M.; Hamdaoui, B.; Khalfi, B. Aggregate Hardware Impairments Over Mixed RF/FSO Relaying Systems With Outdated CSI. *IEEE Trans. Commun.* **2018**, *66*, 1110–1123. [CrossRef]

39. Sharma, P.K.; Upadhyay, P.K. Cognitive relaying with transceiver hardware impairments under interference constraints. *IEEE Commun. Lett.* **2016**, *20*, 820–823. [CrossRef]
40. Boulogeorgos, A.A.; Karas, D.S.; Karagiannidis, G.K. How Much Does I/Q Imbalance Affect Secrecy Capacity? *IEEE Commun. Lett.* **2016**, *20*, 1305–1308. [CrossRef]
41. Zhu, J.; Ng, D.W.K.; Wang, N.; Schober, R.; Bhargava, V.K. Analysis and Design of Secure Massive MIMO Systems in the Presence of Hardware Impairments. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 2001–2016. [CrossRef]
42. Boshkovska, E.; Ng, D.W.K.; Dai, L.; Schober, R. Power-Efficient and Secure WPCNs with Hardware Impairments and Non-Linear EH Circuit. *IEEE Trans. Commun.* **2018**, *66*, 2642–2657. [CrossRef]
43. Kuhestani, A.; Mohamadi, A.; Wong, K.-K.; Yeoh, P.L.; Moradikia, M.; Khandaker, M.R.A. Optimal Power Allocation by Imperfect Hardware Analysis in Untrusted Relaying Networks. *IEEE Trans. Wirel. Commun.* **2018**, *17*, 4302–4314. [CrossRef]
44. Tin, P.T.; Hung, D.T.; Duy, T.T.; Voznak, M. Analysis of Probability of Non-zero Secrecy Capacity for Multi-hop Networks in Presence of Hardware Impairments over Nakagami-m Fading Channels. *RadioEngineering* **2016**, *25*, 774–782.
45. Wang, L.; Kim, K.J.; Duong, T.Q.; Elkashlan, M.; Poor, H.V. Security Enhancement of Cooperative Single Carrier Systems. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 90-103. [CrossRef]
46. Laneman, J.N.; Tse, D.N.C.; Wornell, G.W. Cooperative Diversity in Wireless Networks: Efficient Protocols and Outage Behavior. *IEEE Trans. Inform. Theory* **2004**, *50*, 3062–3080. [CrossRef]
47. Liu, P.; Tao, Z.; Lin, Z.; Erkip, E.; Panwar, S. Cooperative Wireless Communications: A Cross-layer Approach. *IEEE Wirel. Commun.* **2006**, *13*, 84–92.
48. Bletsas, A.; Khisti, A.; Reed, D.P.; Lippman, A. Simple Cooperative Diversity Method based on Network Path Selection. *IEEE J. Sel. Areas Commun.* **2006**, *24*, 659–672. [CrossRef]
49. Mo, J.; Tao, M.; Liu, Y. Relay Placement for Physical Layer Security: A Secure Connection Perspective. *IEEE Commun. Lett.* **2012**, *16*, 878–881.
50. Cai, C.; Cai, Y.; Yang, W.; Yang, W. Secure Connectivity Using Randomize-and-Forward Strategy in Cooperative Wireless Networks. *IEEE Commun. Lett.* **2013**, *17*, 1340–1343.
51. Vo, N.Q.B.; Duong, T.Q.; Tellambura, C. On the Performance of Cognitive Underlay Multihop Networks with Imperfect Channel State Information. *IEEE Trans. Commun.* **2013**, *61*, 4864–4873.