symmetry

MDPI

Article

Secrecy Performance of Underlay Cooperative Cognitive Network Using Non-Orthogonal Multiple Access with Opportunistic Relay Selection

Tan-Phuoc Huynh [1], Pham Ngoc Son [2,*] and Miroslav Voznak [1]

[1] Department of Telecommunications, VSB-Technical University of Ostrava, 17. listopadu 15/2172, 708 33 Ostrava-Poruba, Czech Republic; phuoc.huynh.tan.st@vsb.cz (T.-P.H.); miroslav.voznak@vsb.cz (M.V.)

[2] Faculty of Electrical and Electronics Engineering, Ho Chi Minh City University of Technology and Education, Ho Chi Minh 700000, Vietnam

* Correspondence: sonpndtvt@hcmute.edu.vn; Tel.: +84-966-609-555

Received: 22 January 2019; Accepted: 8 March 2019; Published: 15 March 2019

Abstract: In this paper, an underlay cooperative cognitive network using a non-orthogonal multiple access (UCCN-NOMA) system is investigated, in which the intermediate multiple relays help to decode and forward two signals x_1 and x_2 from a source node to two users D_1 and D_2, respectively, under wiretapping of an eavesdropper (E). We study the best relay selection strategies by three types of relay selection criteria: the first and second best relay selection is based on the maximum channel gain of the links R_i-D_1, R_i-D_2, respectively; the third one is to ensure a minimum value of the channel gains from the R_i-E link. We analyze and evaluate the secrecy performances of the transmissions x_1 and x_2 from the source node to the destination nodes D_1, D_2, respectively, in the proposed UCCN-NOMA system in terms of the secrecy outage probabilities (SOPs) over Rayleigh fading channels. Simulation and analysis results are presented as follows. The results of the (sum) secrecy outage probability show that proposed scheme can realize the maximal diversity gain. The security of the system is very good when eavesdropper node E is far from the source and cooperative relay. Finally, the theoretical analyses are verified by performing Monte Carlo simulations.

Keywords: non-orthogonal multiple access (NOMA); physical layer security (PLS); cooperative communication; successive interference cancellation (SIC); decode-and-forward; cognitive radio (CR); outage probability

1. Introduction

Today, the development of smart devices has led to the increase in the number of wireless connections, the mobile data rate, and the consumed energy in the next generation of wireless communication systems [1,2]. The users always wants to connect and get the data quickly and safely. Therefore, in order to deploy and improve the range of the wireless communication system and the connection speed, non-orthogonal multiple access (NOMA) has recently received great attention from researchers in the field of wireless systems as a promising technique to achieve enhanced spectrum efficiency of the 5G mobile network [3,4]. In the NOMA technique, the users can share both time and frequency resources and only adjust their power allocation ratios. In particular, the user with better channel conditions can be allocated to a channel that is occupied by a user with poor channel conditions. The users with strong channel conditions can serve as relays to enhance the system performance by using successive interference cancellation (SIC) [5].

In recent times, there has been many research investigations into NOMA in wireless communication systems [6–8]. Cooperative NOMA can achieve the maximum diversity gain for

wireless networks. The researchers in [6] studied the cooperative relaying system using the NOMA technique to improve the spectral efficiency. In [7], the authors considered the performance of the NOMA system in amplify-and-forward (AF) relaying systems to increase the data transmission rate for 5G communications. Approaches based on the role of chaos in game theory have been investigated in [9,10] and can be applied in multiple access schemes. The combination of cooperative communication and PLS is an effective approach to overcome the disadvantages of the fading environment, as well as to increase the security capacity of the wireless network.

PLS has been presented by published researches in [8,11]. In [8], the authors evaluated the secrecy performance of cooperative protocols with relay selection methods under the impact of co-channel interference. The authors in [11] studied the impact of correlated fading on the secrecy performance of multiple DFrelaying with the optimal relay selection method. Besides, the authors researched the NOMA technique combined with PLS in [12,13]. In [12], the authors solved the problem of maximizing the minimum confidential information rate among users subject to the secrecy outage constraint and instantaneous transmit power constraint. Cooperative NOMA systems with PLS were investigated in [13] in cases of both AF and DF operations.

In addition, the underlay cognitive radio networks applying the NOMA technique were also proposed by some authors in [14–17]. In [14], a cooperative transmission scheme has been proposed for a downlink NOMA in CR systems, and this research exploited the maximal spatial diversity. Considering the security principle [18–20], the authors in [19] studied secure communication in cognitive DF relay networks in which a pair of cognitive relays is opportunistically selected for security protection against eavesdroppers. In [20], the authors investigated tradeoffs between security and reliability in cooperative cognitive radio networks with the NOMA solution.

In most of the above research, the authors have not considered the combination of NOMA with PLS in UCCN. Excited by the above ideas, in this article, we propose a UCCN using the NOMA scheme in which the intermediate relays help to decode and forward two signals x_1 and x_2 from a source node to two destination nodes D_1 and D_2, respectively, under wiretapping of an eavesdropper. The best relay selection strategy is investigated in three types of relay selection criteria: the first and second best relay selection is based on maximizing the value of the channel gains from the links R_i-D_1, R_i-D_2, respectively; the third one is to ensure the minimum value of the channel gains from the R_i-E link. Then, we analyze and evaluate the secrecy performances of the transmissions x_1 and x_2 in the proposed UCCN-NOMA scheme in terms of the SOPs over Rayleigh fading channels to advance the spectral efficiency and secure communication in which the best intermediate relay supports power to the destination nodes and perform digital network coding (DNC) to compress the received data and then to forward the signals to the destination nodes.

The article is summarized with the main contributions as follows. Firstly, we propose a DF-formed cooperation UCCN scheme in which the best relay uses the NOMA and considers PLS to enhance the system performance in 5G wireless networks. Secondly, the SOPs over Rayleigh fading channels are derived and are confirmed by Monte Carlo simulations. Thirdly, the secrecy performances of the transmissions x_1 and x_2 in the three best relay selection strategies are compared with each other in the proposed UCCN-NOMA system. The organization of paper is as follows: Section 2 describes a UCCN system model with the best relay using NOMA combined with PLS and the operation methods of the proposed system; Section 3 analyses the results of the SOPs for the eavesdropping of the signals x_1 and x_2 in the proposed UCCN-NOMA system; the simulation results are presented in Section 4; and Section 5 summarizes our conclusions.

2. System Model

In this paper, as shown in Figure 1, we consider a wireless communication system of a UCCN, which contains one source node S, two destination nodes D_1 and D_2, multi-wireless relay nodes using the NOMA principle, and one eavesdropper node E to wiretap the signals of the links S-D_1 and S-D_2. In this figure, we assume that the communication between the source S and the destinations D_1 and

D_2 is not transmitted directly, and they are linked through the intermediate relays with the presence of the eavesdropper E. Hence, the source node transmits its packets to the destination nodes (x_1 is sent to D_1, and x_2 is sent to D_2). The R_i-D_2 link distance is farther than the R_i-D_1 link distance. In order to transmit data optimally, the best relay node using the NOMA method was selected to help the source node exchange data with destination nodes D_1 and D_2. The best relay selection strategy is presented by three types of relay selection criteria: the first and second best relay selection is based on the maximum channel gain of the links R_i-D_1 and R_i-D_2, respectively; the third one is to ensure the minimum channel gain of the link R_i-E.

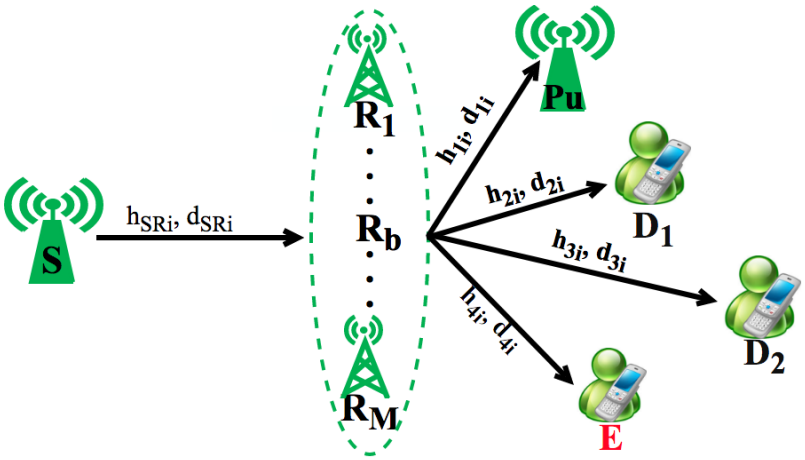

Figure 1. System model of a UCCN-NOMA scheme considering PLS.

There are some assumptions as follows. Firstly, each node has a private antenna. Secondly, the variances of zero-mean white Gaussian noises (AWGNs) are equal, denoted similarly as N_0. Thirdly, all channels are designated for flat and block Rayleigh fading. Finally, the channel state information (CSI) regarding the sources-to-eavesdropper, sources-to-relays, and relays-to eavesdropper channels is known at the source node S and the destination nodes D_1 and D_2 [5].

In Figure 1, (h_{SR_i}, d_{SR_i}),(h_{ji}, d_{ji}) are Rayleigh fading channel coefficients and the link distances of S-R_i, R_i-D_k, R_i-E, and R_i-Pu, respectively, where $j \in \{1, 4\}$, $i \in \{1, M\}$, and $k \in \{1, 2\}$. Hence, the random variables $g_{ji} = |h_{ji}|^2$ have an exponential distribution with the parameter $\lambda_j = d_{ji}^{\beta}$, where β is a path-loss exponent. The respectively distances of R_i-D_k, R_i-E, and R_i-Pu are illustrated in Figure 1. The cumulative distribution function (cdf) and probability density function (pdf) of random variables g_{ji} are expressed as $F_{g_{ji}}(a) = 1 - e^{-\lambda_j a}$ and $f_{g_{ji}}(a) = \lambda_j e^{-\lambda_j a}$, respectively. With the assumptions in this paper, the fading channels h_{ji} are fixed during a block time T, and the variables h_{ji} are independent and identically distributed between two continuous block times.

Based on a time division channel model, the operation method of the proposed UCCN-NOMA system is divided into two timeslots as presented in Figure 2. In the first timeslot, the source node S broadcasts its signal x_s, which contains signals x_1 and x_2, to the best relay R_b. The signal x_s is created by the superposition coding method [21]. The selection criteria of the best relay R_b will be discussed in the next section. The best relay R_b uses the SIC technique to decode the signals x_1 and x_2 sequentially based on the allocated powers to the signals x_1 and x_2 at the source node S. In the second timeslot, the best relay R_b combines the signals x_1 and x_2 to the coded signal x_R by the superposition coding and then sends the signal x_R to the destinations D_1 and D_2. The transmitted x_R can be wiretapped by the eavesdropper E in the wireless environment.

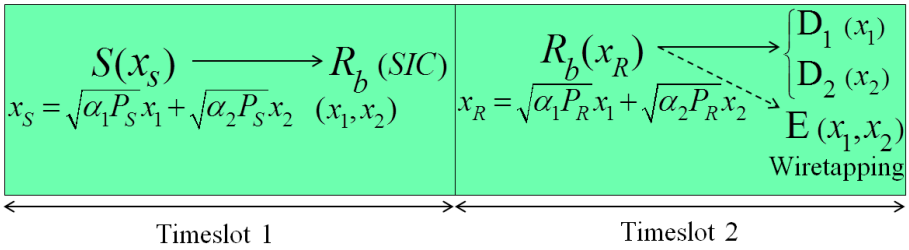

Figure 2. Operation diagram of the proposed system.

3. Secrecy Outage Probability Analysis

In this section, we analyze the sum SOP for the eavesdropping of the signals x_1 and x_2 in the proposed UCCN-NOMA system. We assume that a node successfully and safely decodes the received packet if its achievable secrecy capacity is larger than a target secrecy capacity SC_{th}.

At the first timeslot, the source node S creates the signal x_s by the superposition coding [21] and then broadcasts the x_s to all of the relays R_i. The signal x_s is given by:

$$x_s = \sqrt{\alpha_1 P_s}x_1 + \sqrt{\alpha_2 P_s}x_2, \tag{1}$$

where P_s is the power at source node S, α_1 and α_2 are the power allocation coefficients, and x_1 and x_2 are the messages sent to D_1 and D_2. Following the principle of the NOMA, we assume that $\alpha_1 > \alpha_2$ with $\alpha_1 + \alpha_2 = 1$.

The received signal at the relay R_i from the source node S for the decoding of x_1 and x_2 is given by:

$$y_{SR_i}^{x_{1,2}} = x_s h_{SR_i} + n_{R_i} = \sqrt{\alpha_1 P_s}h_{SR_i}x_1 + \sqrt{\alpha_2 P_s}h_{SR_i}x_2 + n_{R_i}, \tag{2}$$

where n_{R_i} denote the AWGNs at the relay R_i with the same variance N_0, $E\{|x_1|^2\} = 1$,$E\{|x_2|^2\} = 1$ ($E\{x\}$ denotes the expectation process of x).

Based on the NOMA scheme, firstly, the relay R_i decodes x_1 from (1) and removes it using SIC, then x_2 will be decoded and forward to D_2 without the component $\sqrt{\alpha_2 P_s}h_{SR_i}x_1$ in (2). Therefore, the signal received at R_i after decoding x_1 is expressed as follows:

$$y_{SR_i}^{x_2} = \sqrt{\alpha_2 P_s}x_2 h_{SR_i} + n_{R_i}. \tag{3}$$

In the second timeslot, the signals received at the destinations D_1 and D_2 related to links R_i-D_1 and R_i-D_2, respectively, can be written as:

$$y_{R_iD_1}^{x_1} = \sqrt{\alpha_1 P_R}h_{2i}x_1 + \sqrt{\alpha_2 P_R}h_{2i}x_2 + n_{D_1}. \tag{4}$$

$$y_{R_iD_2}^{x_2} = \sqrt{\alpha_2 P_R}x_2 h_{3i} + n_{D_2}. \tag{5}$$

where n_{D_k} denote the AWGNs at the destination D_k with the same variance N_0 and P_R is the transmit power of the relay R_i.

Similarly, the node E also wiretaps the packets x_1 and x_2 from R_i, respectively, and the received signals at node E are obtained as follows:

$$y_{R_iE}^{x_1} = \sqrt{\alpha_1 P_s}x_1 h_{4i} + \sqrt{\alpha_2 P_s}x_2 h_{4i} + n_E. \tag{6}$$

$$y_{R_iE}^{x_2} = \sqrt{\alpha_2 P_s}x_2 h_{4i} + n_E. \tag{7}$$

where n_E denote the AWGNs at E with the same variance N_0.

In the system model, under the interference constraint at the Pu node, the relays R_i have to adjust their transmitting powers so that the interference power at the Pu must be less than a threshold value, I_{th}. The maximum powers of nodes S and R_i are given, respectively, as:

$$P_R = \frac{I_{th}}{|h_{1i}|^2} = \frac{I_{th}}{g_{1i}}. \tag{8}$$

With Formulas (4) and (5), the received signal-to-interference and noise ratios (SINRs) at the destination D_k for decoding the information signals x_1 and x_2 are obtained, respectively, as follows:

$$SINR_{R_iD_1}^{x_1} = \frac{P_R\alpha_1 g_{2i}}{P_R\alpha_2 g_{2i} + N_0}. \tag{9}$$

$$SINR_{R_iD_2}^{x_2} = \frac{P_R\alpha_2 g_{3i}}{N_0}. \tag{10}$$

Applying Formulas (6) and (7), the received SINRs at the node E for eavesdropping the information signal x_1 of D_1 and the signal x_2 of D_2 from the relay R_i are obtained, respectively, as follows:

$$SINR_{R_iE}^{x_1} = \frac{P_R\alpha_1 g_{4i}}{P_R\alpha_2 g_{4i} + 1} = \frac{Q\alpha_1 g_{4i}}{Q\alpha_2 g_{4i} + g_{1i}}. \tag{11}$$

$$SINR_{R_iE}^{x_2} = \frac{P_R\alpha_2 g_{4i}}{N_0} = \frac{Q\alpha_2 g_{4i}}{g_{1i}}. \tag{12}$$

Applying the Shannon capacity formula, the achievable rates of the links R_i-Y are formulated as:

$$R_{R_iY}^{x_k} = \frac{1}{2}\log_2(1 + SINR_{R_iY}^{x_k}), \tag{13}$$

where the ratio $1/2$ represents the fact that data transmission is split into two time slots, and $Y \in \{E, D_k\}$.

The secrecy capacity of the UCCN system with DF-based NOMA for the R_i-D_k communication can be expressed as:

$$SC_w = \left[SC_{R_{bw}D_k}^{x_k} - SC_{R_{bw}E}^{x_k}\right]^+, \tag{14}$$

where $[x]^+ = \max(0, x)$; $w \in \{1, 3\}$; $SC_{R_{bw}D_k}^{x_k}$ are the secrecy capacities from the relay R_i to the destination D_k, given, respectively, as:

$$SC_{R_{bw}D_k}^{x_k} = \max(0, R_{R_{bw}D_k}^{x_k} - R_{R_{bw}E}^{x_k}). \tag{15}$$

3.1. The Sum SOP of the Secrecy Transmission in the Proposed UCCN-NOMA System with the Best Relay Selection: Case ST1

In this section, firstly, we find the best relay R_{b_1} based on the maximum channel gain of the R_i-D_1 link. Then, we calculate the SOPs of the ST1case in which the destination nodes D_1 and D_2 do not get the signal safely from the source node S through R_{b_1} under the malicious attempt of the eavesdropper E. Finally, we calculate their sum SOPs to compare fairly with the sum SOPs of the ST2 and ST3 cases in Sections 3.2 and 3.3.

First, the best relay is selected based on a criterion as follows:

$$R_{b_1} = \arg \underbrace{\max}_{i=1...M} |h_{R_iD_1}|^2 = \underbrace{\max}_{i=1...M} |h_{2i}|^2 = g_{2b_1} \tag{16}$$

From the definition of R_{b_1} in (16), the CDF of g_{2b_1} is obtained as:

$$\begin{aligned} F_{g_{2b_1}}(a) &= \Pr\left(g_{2b_1} < a\right) = \Pr\left[\underbrace{\max}_{i=1\ldots M} g_{2i} < a\right] \\ &= \prod_{i=1}^{M}\left(1-e^{-\lambda_2 a}\right) = \left(1-e^{-\lambda_2 a}\right)^M \end{aligned} \tag{17}$$

The pdf of g_{2b_1} is inferred as:

$$f_{g_{2b_1}}(a) = \frac{\partial F_{g_{2b_1}}(a)}{\partial a} = M\lambda_2 e^{-\lambda_2 a}\left(1-e^{-\lambda_2 a}\right)^{M-1}. \tag{18}$$

The next, we calculate the SOP of the ST1 case in which the destination node D_1 does not receive the signal safely from the best relay under the malicious attempt of the eavesdropper E, presented by a math expression as follows:

$$P_{\text{ST1}}^{out\_D_1} = \Pr\left(SC_{R_{b_1}D_1}^{x_1} < SC_{th}\right). \tag{19}$$

Substituting Formula (15) into (19), $P_{\text{ST1}}^{out\_D_1}$ is obtained as:

$$P_{\text{ST1}}^{out\_D_1} = \Pr\left(R_{R_{b_1}D_1}^{x_1} - R_{R_{b_1}E}^{x_1} \le SC_{th}\right) \tag{20}$$

Replacing Formula (13) in (20), $P_{\text{ST1}}^{out\_D_1}$ is expressed as:

$$\begin{aligned} P_{\text{ST1}}^{out\_D_1} &= \Pr\left[\tfrac{1}{2}\log_2\left(1+SINR_{R_{b_1}D_1}^{x_1}\right) < \tfrac{1}{2}\log_2\left(1+SINR_{R_{b_1}E}^{x_1}\right) + SC_{th}\right] \\ &= \Pr\left[\tfrac{1}{2}\log_2\left(1+\tfrac{P_R\alpha_1 g_{2b_1}}{P_R\alpha_2 g_{2b_1}+1}\right) < \tfrac{1}{2}\log_2\left(1+\tfrac{P_R\alpha_1 g_{4b_1}}{P_R\alpha_2 g_{4b_1}+1}\right) + SC_{th}\right] \\ &= \Pr\left[\tfrac{P_R\alpha_1 g_{2b_1}}{P_R\alpha_2 g_{2b_1}+1} < \theta + (\theta+1)\left(\tfrac{P_R\alpha_1 g_{4b_1}}{P_R\alpha_2 g_{4b_1}+1}\right)\right], \end{aligned} \tag{21}$$

where $\theta = 2^{2SC_{th}} - 1$.

In this paper, we consider the worst case in which the node E can take the data of D_1 with the best conditions. From (21), we have an upper constraint of $P_{\text{ST1}}^{out\_D_1}$ as follows:

$$\begin{aligned} P_{\text{ST1}}^{out\_D_1} \le P_{\text{ST1}}^{out\_upper} &= \Pr\left[\tfrac{P_R\alpha_1 g_{2b_1}}{P_R\alpha_2 g_{2b_1}+1} < \theta + (\theta+1)\left(P_R\alpha_1 g_{4b_1}\right)\right] \\ &= \Pr\left[g_{4b_1} > \tfrac{g_{2b_1}g_{1b_1}}{(\theta+1)\left(Q\alpha_2 g_{2b_1}+g_{1b_1}\right)} - \tfrac{\theta g_{1b_1}}{(\theta+1)Q\alpha_1}\right] \\ &= \int_0^\infty f_{g_{1b_1}}(x)\Pr\left[g_{4b_1} > \frac{g_{2b_1}x}{(\theta+1)\left(Q\alpha_2 g_{2b_1}+x\right)} - \frac{\theta x}{(\theta+1)Q\alpha_1}\right]dx \\ &= \int_0^\infty f_{g_{1b_1}}(x)\left(\mathrm{A}_1+\mathrm{A}_2\right)dx, \end{aligned} \tag{22}$$

where $P_R = \frac{I_{th}}{g_{1i}}$, $Q = \frac{I_{th}}{N_0}$, $\mathrm{A}_1 = \Pr\left[g_{4b_1} > \frac{g_{2b_1}x}{(\theta+1)(Q\alpha_2 g_{2b_1}+x)} - \frac{\theta x}{(\theta+1)Q\alpha_1}\right]$,

$\mathrm{A}_2 = \Pr\left[g_{4b_1} > \frac{g_{2b_1}x}{(\theta+1)\left(\alpha_2 Q g_{2b_1}+x\right)} - \frac{\theta x}{(\theta+1)Q\alpha_1}; \frac{g_{2b_1}x}{(\theta+1)\left(\alpha_2 Q g_{2b_1}+x\right)} > \frac{\theta x}{(\theta+1)Q\alpha_1}\right]$,

To solve $P_{\text{ST1}}^{out\_upper}$ in (22), we use two lemmas as follows:

Lemma 1. *A_1 is obtained by a closed-form expression as follows:*

$$\mathrm{A}_1 = \begin{cases} 1 & ,\alpha_1 \leq \alpha_2\theta \\ \left(1 - e^{-\lambda_2 \psi x}\right)^M & ,\alpha_1 > \alpha_2\theta, \end{cases} \tag{23}$$

where $\psi = \frac{\theta}{Q(\alpha_1 - \theta\alpha_2)}$.

Proof. The proof of Lemma 1 is provided in Appendix A. □

Lemma 2. *The following expression is valid for A_2:*

$$\mathrm{A}_2 = \begin{cases} 0 & ,\alpha_1 \leq \theta\alpha_2 \\ \int\limits_{\psi x}^{\infty} f_{g_{2b_1}}(y)\, e^{-\lambda_4\left(\frac{xy}{(\theta+1)(\alpha_2 Qy + x)} - \frac{\theta x}{(\theta+1)Q\alpha_1}\right)} dxdy & ,\alpha_1 > \theta\alpha_2. \end{cases} \tag{24}$$

Proof. The proof of Lemma 2 is presented clearly in Appendix B.

The exact upper expression $P_{\mathrm{ST1}}^{out\_upper}$ of the SOP $P_{\mathrm{ST1}}^{out\_D_1}$ is provided in the following theorem. □

Theorem 1. *The upper expression $P_{\mathrm{ST1}}^{out\_upper}$ is obtained by the expression as:*

$$P_{\mathrm{ST1}}^{out\_upper} = \begin{cases} 1 & ,\alpha_1 \leq \theta\alpha_2 \\ \left(\lambda_1 \sum\limits_{t=0}^{M} (-1)^t C_M^t \times \frac{1}{(\lambda_1 + \lambda_2\psi t)} + \frac{\lambda_1\lambda_2 M}{\alpha_2 Q} \times \mathrm{I}_1\right) & ,\alpha_1 > \theta\alpha_2, \end{cases} \tag{25}$$

where $\mathrm{I}_1 = \int\limits_0^{\infty}\int\limits_{px}^{\infty} \left[\begin{array}{l} \exp\left(-\lambda_1 x + nx - \frac{\lambda_4 x}{(\theta+1)\alpha_2 Q} + \frac{\lambda_2 x}{\alpha_2 Q}\right) \\ \times \exp\int\limits_{px}^{\infty} \exp\left(\frac{\lambda_4 x^2}{(\theta+1)\alpha_2 Qz} - \frac{\lambda_2 z}{\alpha_2 Q}\right)\left(1 - \exp(-\frac{\lambda_2(z-x)}{\alpha_2 Q})\right)^{M-1} \end{array} \right] dzdx$

and $n = \frac{\lambda_4\theta}{(\theta+1)\alpha_1 Q}$.

Proof. Substituting Lemma 1 and Lemma 2 into (22), $P_{\mathrm{ST1}}^{out\_upper}$ is shown in two cases as:

-When $\alpha_1 \leq \theta\alpha_2$:

$$P_{\mathrm{ST1}}^{out\_upper} = \int\limits_0^{\infty} f_{g_{1b_1}}(x)(1+0)dx = \int\limits_0^{\infty} \lambda_1 e^{-\lambda_1 x} dx = 1. \tag{26a}$$

-When $\alpha_1 > \theta\alpha_2$:

$$P_{\mathrm{ST1}}^{out\_upper} = \left(\underbrace{\int\limits_0^{\infty} f_{g_{1b_1}}(x)\left(1 - e^{-\lambda_2 x\psi}\right)^M dx}_{\mathrm{A}_3} + \underbrace{\int\limits_0^{\infty} f_{g_{1b_1}}(x) \int\limits_{\psi x}^{\infty} f_{g_{2b_1}}(y)\, e^{-\lambda_4\varphi} dxdy}_{\mathrm{A}_4} \right), \tag{26b}$$

where $\varphi = \frac{xy}{(\theta+1)(\alpha_2 Qy + x)} - \frac{\theta x}{(\theta+1)\alpha_1 Q}$.

A_3 in (26b) is calculated as

$$\begin{aligned} \mathrm{A}_3 &= \int_0^{\infty} f_{g_{1b_1}}(x)(1-e^{-\lambda_2\psi x})^M dx = \int_0^{\infty} \lambda_1 e^{-\lambda_1 x}\left(1-e^{-\lambda_2\psi x}\right)^M dx \\ &= \lambda_1 \sum_{t=0}^{M} (-1)^t C_M^t \int_0^{\infty} e^{-(\lambda_1+\lambda_2\psi t)x} dx = \lambda_1 \sum_{t=0}^{M} (-1)^t C_M^t \times \frac{1}{(\lambda_1+\lambda_2\psi t)}, \end{aligned} \tag{27}$$

where $C_m^n = \frac{(m)!}{n!(m-n)!}$.

The A_4 in (26b) is presented as:

$$\begin{aligned} \mathrm{A}_4 &= \int_0^{\infty} f_{g_{1b_1}}(x)\, dx \int_{\psi x}^{\infty} f_{g_{2b_1}}(y)\, e^{-\lambda_4\varphi} dy \\ &= \int_0^{\infty} \lambda_1 e^{-\lambda_1 x} \int_{\psi x}^{\infty} M \times \lambda_2 e^{-\lambda_2 y}\left(1-e^{-\lambda_2 y}\right)^{M-1} e^{-\lambda_4\varphi} dxdy \\ &= \lambda_1\lambda_2 M \int_0^{\infty} \exp\left(-x\left(\lambda_1 - \frac{\lambda_4\theta}{(\theta+1)\,\alpha_1 Q}\right)\right) \\ &\quad \times \int_{\psi x}^{\infty} \exp\left(\frac{-\lambda_4 xy}{(\theta+1)\,(\alpha_2 Q y + x)} - \lambda_2 y\right) \times (1-\exp(-\lambda_2 y))^{M-1} dxdy, \end{aligned} \tag{28}$$

By setting $z = \alpha_2 Q y + x$, A_4 in (28) is given as:

$$\begin{aligned} \mathrm{A}_4 &= \tfrac{\lambda_1\lambda_2 M}{\alpha_2 Q} \int_0^{\infty}\int_{px}^{\infty} \left[\begin{array}{l} \exp\left(-\lambda_1 x + nx\right) \\ \times \exp\left(\frac{-\lambda_4 x(z-x)}{(\theta+1)\alpha_2 Q z} - \frac{\lambda_2(z-x)}{\alpha_2 Q}\right) \times \left(1-\exp(-\frac{\lambda_2(z-x)}{\alpha_2 Q})\right)^{M-1} \end{array}\right] dzdx \\ &= \tfrac{\lambda_1\lambda_2 M}{\alpha_2 Q} \int_0^{\infty}\int_{px}^{\infty} \left[\begin{array}{l} \exp\left(\lambda_1 x + nx - \frac{\lambda_4 x}{(\theta+1)\alpha_2 Q} + \frac{\lambda_2 x}{\alpha_2 Q}\right) \times \exp\left(\frac{\lambda_4 x^2}{(\theta+1)\alpha_2 Q z} - \frac{\lambda_2 z}{\alpha_2 Q}\right) \\ \times\left(1-\exp(-\frac{\lambda_2(z-x)}{\alpha_2 Q})\right)^{M-1} \end{array}\right] dzdx, \end{aligned} \tag{29}$$

where $p = \alpha_2 Q\psi + 1$.

Substituting A_3 in (27) and A_4 in (29) into (26b), $P_{\mathrm{ST1}}^{out\_upper}$ is obtained as:

$$P_{\mathrm{ST1}}^{out\_upper} = \left(\lambda_1 \sum_{t=0}^{M} (-1)^t C_M^t \times \frac{1}{(\lambda_1+\lambda_2\psi t)} + \frac{\lambda_1\lambda_2 M}{\alpha_2 Q} \times \mathrm{I}_1\right). \tag{30}$$

With the results of (30) and (26a), Theorem 1 in (25) is proven successfully.

Finally, we calculate the SOP of the ST1 case in which the destination node D_2 does not receive the signal safely from the source node S through the best relay R_{b1} under the malicious attempt of the eavesdropper E as follows:

$$P_{\mathrm{ST1}}^{out\_D_2} = \Pr\left(SC_{R_{b_1}D_2}^{x_2} < SC_{th}\right). \tag{31}$$

Substituting Formula (15) into (31), $P_{\mathrm{ST1}}^{out\_D_2}$ is obtained as:

$$P_{\mathrm{ST1}}^{out\_D_2} = \Pr\left(R_{R_{b_1}D_2}^{x_2} - R_{R_{b_1}E}^{x_2} \le SC_{th}\right). \tag{32}$$

Replacing Formula (13), $P_R = \frac{I_{th}}{g_{1i}}, Q = \frac{I_{th}}{N_0}$ into (32), $P_{\mathrm{ST1}}^{out\_D_2}$ is expressed as:

$$\begin{aligned} P_{\mathrm{ST1}}^{out\_D_2} &= \mathrm{P_r}\left[\tfrac{1}{2}\log_2\left(1+SINR_{R_{b_1}D_2}^{x_2}\right)-\tfrac{1}{2}\log_2\left(1+SINR_{R_{b_1}E}^{x_2}\right)<SC_{th}\right] \\ &= \Pr\left[\tfrac{1}{2}\log_2\left(1+\tfrac{P_R\alpha_2 g_{3b_1}}{N_0}\right)-\tfrac{1}{2}\log_2\left(1+\tfrac{P_R\alpha_2 g_{4b_1}}{N_0}\right)<SC_{th}\right] \\ &= \Pr\left[g_{3b_1}<\tfrac{\theta g_{1b_1}}{Q\alpha_2}+(\theta+1)g_{4b_1}\right]. \end{aligned} \tag{33}$$

By performing the pdf of the random variables g_{1b_1}, g_{4b_1} and the cdf of the random variable g_{3b_1}, (33) is achieved by the closed-form expression as:

$$\begin{aligned} P_{\mathrm{ST1}}^{out\_D_2} &= \int_0^\infty\int_0^\infty \Pr\left[g_{3b_1}<\frac{\theta x}{Q\alpha_2}+(\theta+1)y\right] f_{g_{1b_1}}(x) f_{g_{4b_1}}(y)\,dxdy \\ &= 1-\int_0^\infty\int_0^\infty \lambda_1 e^{-\lambda_1 x}\lambda_4 e^{-\lambda_4 y} e^{-\lambda_3\left(\frac{\theta x}{Q\alpha_2}+(\theta+1)y\right)}\,dxdy \\ &= 1-\frac{\lambda_1\lambda_4}{\left(\lambda_1+\frac{\lambda_3\theta}{Q\alpha_2}\right)(\lambda_4+\lambda_3(\theta+1))}. \end{aligned} \tag{34}$$

Finally, from (25) and (34), the sum SOP of ST1 is constrained by the upper expression as:

$$\begin{aligned} Sum\,P_{\mathrm{ST1}}^{out} &= P_{\mathrm{ST1}}^{out\_D_1}+P_{\mathrm{ST1}}^{out\_D_2} \\ &\le \begin{cases} 1+\left(1-\frac{\lambda_1\lambda_4}{\left(\lambda_1+\frac{\lambda_3\theta}{Q\alpha_2}\right)(\lambda_4+\lambda_3(\theta+1))}\right) & ,\alpha_1\le\theta\alpha_2 \\ \left(\lambda_1\sum\limits_{t=0}^{M}(-1)^t C_M^t\times\frac{1}{(\lambda_1+\lambda_2\psi t)}+\frac{\lambda_1\lambda_2 M}{\alpha_2 Q}\times \mathrm{I}_1\right)+\left(1-\frac{\lambda_1\lambda_4}{\left(\lambda_1+\frac{\lambda_3\theta}{Q\alpha_2}\right)(\lambda_4+\lambda_3(\theta+1))}\right) & ,\alpha_1>\theta\alpha_2, \end{cases} \end{aligned} \tag{35}$$

□

3.2. The SOP of the Secrecy Transmission in the Proposed UCCN-NOMA System with the Best Relay Selection: Case ST2

Similar to Section 3.1, first, we find the best relay R_{b_2} based on the maximum channel gain of the R_i-D_2 link. Next, we calculate the SOPs of the ST2 case in which the destination nodes D_1, D_2 do not receive the signal safely from the source node S through R_{b_2} under the malicious attempt of the eavesdropper E. Finally, we calculate their sum SOPs.

Firstly, we calculate the best relay similarly as the expression of the best relay R_{b_1} in Section 3.1, and the best relay R_{b_2} is selected based on a criterion as follows:

$$R_{b_2}=\arg\underbrace{\max_{m=1\ldots M}}|h_{R_m D_2}|^2=\underbrace{\max_{m=1\ldots M}}|h_{3i}|^2=g_{3b_2} \tag{36}$$

The cdf and pdf of the random variable g_{3b_2} is expressed similarly as (17) and (18) and is shown as $F_{g_{3b_2}}(a)=\left(1-e^{-\lambda_3 a}\right)^M$, $f_{g_{3b_2}}(a)=M\lambda_3 e^{-\lambda_3 a}\left(1-e^{-\lambda_3 a}\right)^{M-1}$. The SOP of the ST2 case occurs when the destination D_2 does not receive signals x_2 safely from the source node S. The SOP of the ST2 is obtained by a math expression as follows:

$$P_{\mathrm{ST2}}^{out\_D_2}=\Pr\left(SC_{R_{b_2}D_2}^{x_2}<SC_{th}\right) \tag{37}$$

Substituting Formula (15) into (37), $P_{\mathrm{ST2}}^{out\_D_2}$ is calculated as:

$$P_{\mathrm{ST2}}^{out\_D_2}=\Pr\left(R_{R_{b_2}D_2}^{x_2}-R_{R_{b_2}E}^{x_2}\le SC_{th}\right) \tag{38}$$

Replacing Formula (13), $P_R = \frac{I_{th}}{g_{1i}}$,$Q = \frac{I_{th}}{N_0}$ into (37), $P_{\text{ST2}}^{out\_D_2}$ is expressed as:

$$\begin{aligned} P_{\text{ST2}}^{out\_D_2} &= \Pr\left[\tfrac{1}{2}\log_2\left(1+SINR_{R_{b_2}D_2}^{x_2}\right) - \tfrac{1}{2}\log_2\left(1+SINR_{R_{b_2}E}^{x_2}\right) < SC_{th}\right] \\ &= \Pr\left[\tfrac{1}{2}\log_2\left(1+\tfrac{P_R\alpha_2 g_{3b_2}}{N_0}\right) - \tfrac{1}{2}\log_2\left(1+\tfrac{P_R\alpha_2 g_{4b_3}}{N_0}\right) < SC_{th}\right] \\ &= \Pr\left[g_{3b_2} < \tfrac{\theta g_{1b_2}}{Q\alpha_2} + (\theta+1)g_{4b_2}\right] \end{aligned} \tag{39}$$

Similar to (33), the probability $P_{\text{ST2}}^{out\_D_2}$ in (39) is shown by the closed-form expression as follows:

$$\begin{aligned} P_{\text{ST2}}^{out\_D_2} &= \int_0^\infty\int_0^\infty \Pr\left[g_{3b_2} < \frac{\theta x}{Q\alpha_2} + (\theta+1)y\right] f_{g_{1b_2}}(x) f_{g_{4b_2}}(y)\, dxdy \\ &= \int_0^\infty\int_0^\infty \lambda_1 e^{-\lambda_1 x}\lambda_4 e^{-\lambda_4 y}\left(1 - e^{-\lambda_3\left(\frac{\theta x}{Q\alpha_2}+(\theta+1)y\right)}\right)^M dxdy \\ &= \lambda_1\lambda_4 \sum_{t=0}^{M}(-1)^t C_M^t \int_0^\infty\int_0^\infty e^{-\lambda_1 x} e^{-\lambda_4 y} e^{-\lambda_3\left(\frac{\theta x}{Q\alpha_2}+(\theta+1)y\right)t}\, dxdy \\ &= \lambda_1\lambda_4 \sum_{t=0}^{M}(-1)^t C_M^t \times \tfrac{Q\alpha_2}{\lambda_1 Q\alpha_2+\lambda_3\theta t} \times \tfrac{1}{\lambda_4+(\theta+1)\lambda_3 t}. \end{aligned} \tag{40}$$

Second, we calculate the SOP of the ST2 case in which the destination node D_1 does not receive the signal safely from the source node S through the best relay R_{b2} under the malicious attempt of the eavesdropper E as follows:

$$P_{\text{ST2}}^{out\_D_1} = \Pr\left(SC_{R_{b_2}D_1}^{x_1} < SC_{th}\right) = \Pr\left(R_{R_{b_2}D_1}^{x_1} - R_{R_{b_2}E}^{x_1} \le SC_{th}\right). \tag{41}$$

By substituting (9) and (13) into (40), we have an expression of $P_{\text{ST2}}^{out\_D_1}$ as follows:

$$\begin{aligned} P_{\text{ST2}}^{out\_D_1} &= \Pr\left[\tfrac{1}{2}\log_2\left(1+SINR_{R_{b_2}D_1}^{x_1}\right) < \tfrac{1}{2}\log_2\left(1+SINR_{R_{b_2}E}^{x_1}\right) + SC_{th}\right] \\ &= \Pr\left[\tfrac{1}{2}\log_2\left(1+\tfrac{P_R\alpha_1 g_{2b_2}}{P_R\alpha_2 g_{2b_2}+1}\right) < \tfrac{1}{2}\log_2\left(1+\tfrac{P_R\alpha_1 g_{4b_2}}{P_R\alpha_2 g_{4b_2}+1}\right) + SC_{th}\right] \\ &= \Pr\left[\tfrac{P_R\alpha_1 g_{2b_2}}{P_R\alpha_2 g_{2b_2}+1} < \theta + (\theta+1)\left(\tfrac{P_R\alpha_1 g_{4b_2}}{P_R\alpha_2 g_{4b_2}+1}\right)\right]. \end{aligned} \tag{42}$$

Similar to solving $P_{\text{ST1}}^{out\_D_1}$, we consider the worst case in which the node E can take data x_1 with the best condition. We rewrite (41), an upper constraint of $P_{\text{ST2}}^{out\_D_1}$, as follows:

$$P_{\text{ST2}}^{out\_D_1} \le P_{\text{ST2}}^{out\_upper} = \Pr\left[\frac{P_R\alpha_1 g_{2b_2}}{P_R\alpha_2 g_{2b_2}+1} < \theta + (\theta+1)\left(P_R\alpha_1 g_{4b_2}\right)\right]. \tag{43}$$

We calculate $P_{\text{ST2}}^{out\_D_1}$ similar to $P_{\text{ST1}}^{out\_D_1}$, and after some algebra, the probability of $P_{\text{ST2}}^{out\_D_1}$ can be expressed as:

$$P_{\text{ST2}}^{out\_D_1} \le P_{\text{ST2}}^{out\_upper} = \begin{cases} 1 & ,\alpha_1 \le \theta\alpha_2 \\ \frac{\lambda_2\psi}{(\lambda_1+\lambda_2\psi)} + \frac{\lambda_1\lambda_2 M}{\alpha_2 Q} \times \mathrm{I}_2 & ,\alpha_1 > \theta\alpha_2, \end{cases} \tag{44}$$

where $\mathrm{I}_2 = \int_0^\infty\int_{px}^\infty \left[\begin{array}{l} \exp\left(-\lambda_1 x + nx - \frac{\lambda_4 x}{(\theta+1)\alpha_2 Q} + \frac{\lambda_2 x}{\alpha_2 Q}\right) \\ \times \exp\int_{px}^\infty \exp\left(\frac{\lambda_4 x^2}{(\theta+1)\alpha_2 Q\mathrm{z}} - \frac{\lambda_2 z}{\alpha_2 Q}\right) \end{array}\right] dzdx.$

From Formulas (40) and (43), we have the sum SOPs of ST2 constrained by the upper expression as:

$$Sum\, P_{\mathrm{ST2}}^{out} = P_{\mathrm{ST2}}^{out\_D_1} + P_{\mathrm{ST2}}^{out\_D_2}$$

$$\leq \begin{cases} 1 + \left(\lambda_1\lambda_4 \sum\limits_{t=0}^{M} (-1)^t C_M^t \times \frac{Q\alpha_2}{\lambda_1 Q\alpha_2 + \lambda_3\theta t} \times \frac{1}{\lambda_4 + (\theta+1)\lambda_3 t}\right) & ,\alpha_1 \leq \theta\alpha_2 \\ \left(\frac{\lambda_2\psi}{(\lambda_1+\lambda_2\psi)} + \frac{\lambda_1\lambda_2 M}{\alpha_2 Q} \times \mathrm{I}_2\right) + \left(\lambda_1\lambda_4 \sum\limits_{t=0}^{M} (-1)^t C_M^t \times \frac{Q\alpha_2}{\lambda_1 Q\alpha_2 + \lambda_3\theta t} \times \frac{1}{\lambda_4 + (\theta+1)\lambda_3 t}\right) & ,\alpha_1 > \theta\alpha_2. \end{cases} \quad (45)$$

3.3. The SOP of the Secrecy Transmission in the Proposed UCCN-NOMA System with the Best Relay Selection: Case ST3

In this case, we find the best relay R_{b_3} based on the minimum channel gain of the R_i-E link. The SOPs of the ST3 case in which the destination nodes D_1 and D_2 do not receive the signal safely from the source node S under the malicious attempt of the eavesdropper E are expressed next. Finally, we calculate their sum SOPs. The best relay selection is given as:

$$R_{b_3} = \arg \underbrace{\min}_{m=1\ldots M} |h_{R_m E}|^2 = \underbrace{\min}_{m=1\ldots M} |h_{4i}|^2 = g_{4b_3} \quad (46)$$

The cdf and pdfof the random variable g_{4b_3} are calculated as:

$$\begin{aligned} F_{g_{4b_3}}(a) &= \Pr\left[\underbrace{\min}_{i=1\ldots M} g_{4i} < a\right] = 1 - \Pr\left[\underbrace{\min}_{i=1\ldots M} g_{4i} \geq a\right] \\ &= 1 - \prod_{i=1}^{M}\left[1 - F_{g_{4_i}}(a)\right] = \left(1 - e^{-\sum\limits_{i=1}^{M}\lambda_4 a}\right). \end{aligned} \quad (47)$$

$$f_{g_{4b_3}}(a) = \frac{\partial F_{g_{4b_3}}(a)}{\partial a} = M\lambda_4 e^{-\sum\limits_{i=1}^{M}\lambda_4 a}. \quad (48)$$

The SOP of the ST3 case is similar to those in Sections 3.1 and 3.2 and is shown by two math expressions, respectively, as follows:

$$P_{\mathrm{ST3}}^{out\_D_2} = \Pr\left(SC_{R_{b_3}D_2}^{x_2} < SC_{th}\right) = \Pr\left(R_{R_{b_3}D_2}^{x_2} - R_{R_{b_3}E}^{x_2} \leq SC_{th}\right) \quad (49)$$

$$P_{\mathrm{ST3}}^{out\_D_1} = \Pr\left(SC_{R_{b_3}D_1}^{x_1} < SC_{th}\right) = \Pr\left(R_{R_{b_3}D_1}^{x_1} - R_{R_{b_3}E}^{x_1} \leq SC_{th}\right) \quad (50)$$

By replacing Formula (13), $P_R = \frac{I_{th}}{g_{1i}}$, $Q = \frac{I_{th}}{N_0}$ into (48) and (49), finally, we can easily calculate the probability $P_{\mathrm{ST3}}^{out\_D_2}$, $P_{\mathrm{ST3}}^{out\_D_1}$, respectively, as:

$$P_{\mathrm{ST3}}^{out\_D_2} = 1 - \frac{M\lambda_1\lambda_4}{\left(\lambda_1 + \frac{\lambda_2\theta}{Q\alpha_2}\right)(M\lambda_4 + \lambda_2(\theta+1))} \quad (51)$$

-When $\alpha_1 \leq \theta\alpha_2$:

$$P_{\mathrm{ST3}}^{out\_D_1} = \int_0^{\infty} f\gamma_{1i}(x)(1+0)dx = \int_0^{\infty} \lambda_1 e^{-\lambda_1 x} dx = 1 \quad (52a)$$

-When $\alpha_1 > \theta\alpha_2$:

$$P_{\mathrm{ST3}}^{out\_D_1} = \left(\frac{\psi\lambda_2}{\lambda_1+\psi\lambda_2} + \frac{\lambda_1\lambda_2}{\alpha_2 Q} \times \mathrm{I}_3\right) \tag{52b}$$

where $\mathrm{I}_3 = \int_0^{\infty}\int_{px}^{\infty} \left[\begin{array}{l} \exp\left(-\lambda_1 x + \frac{M\lambda_4\theta}{(\theta+1)\alpha_1 Q}x - \frac{M\lambda_4 x}{(\theta+1)\alpha_2 Q} + \frac{\lambda_2 x}{\alpha_2 Q}\right) \\ \times \exp \int_{px}^{\infty} \exp\left(\frac{M\lambda_4 x^2}{(\theta+1)\alpha_2 Q z} - \frac{\lambda_2 z}{\alpha_2 Q}\right) \end{array} \right] dtdx.$

From Formulas (51), (52a), and (52b), $Sum\ P_{\mathrm{ST3}}^{out}$ is obtained as:

$$Sum\ P_{\mathrm{ST3}}^{out} = P_{\mathrm{ST3}}^{out\_D_1} + P_{\mathrm{ST3}}^{out\_D_2}$$

$$\leq \begin{cases} 1 + \left(1 - \frac{M\lambda_1\lambda_4}{\left(\lambda_1 + \frac{\lambda_2\theta}{Q\alpha_2}\right)(M\lambda_4 + \lambda_2(\theta+1))}\right) & ,\alpha_1 \leq \theta\alpha_2 \\ \left(\frac{\psi\lambda_2}{\lambda_1+\psi\lambda_2} + \frac{\lambda_1\lambda_2}{\alpha_2 Q} \times \mathrm{I}_3\right) + \left(1 - \frac{M\lambda_1\lambda_4}{\left(\lambda_1 + \frac{\lambda_2\theta}{Q\alpha_2}\right)(M\lambda_4 + \lambda_2(\theta+1))}\right) & ,\alpha_1 > \theta\alpha_2. \end{cases} \tag{53}$$

I_1 in (35), I_2 in (45), and I_3 in (53) contain the complex integrals, and solving of these integrals is not practical. However, we can use numerical methods to find the value of I_1, I_2, and I_3.

4. Simulation Results

In this section, the SOPs of ST1, ST2 and ST3 are analyzed and evaluated using the theoretical analyses and the Monte Carlo simulations. In the two-dimensional plane, the coordinates of S, R_i, D_1, D_2, Pu, and E were set as S(0, 0), $\mathrm{R}(x_R, 0)$, $\mathrm{D}_1(1, 0)$, $\mathrm{D}_2(x_{D_2}, y_{D_2})$, $\mathrm{Pu}(x_{Pu}, y_{Pu})$, $\mathrm{E}(x_E, y_E)$, respectively, satisfying $(0 < x_R, x_{D_2}, x_E)$. Therefore, $d_{SR_b} = x_R$, $d_{R_bD_1} = x_{D_1} - x_R$, $d_{R_bD_2} = \sqrt{(x_{D_2} - x_R)^2 + y_{D_2}^2}$, $d_{R_bPu} = \sqrt{(x_{Pu} - x_R)^2 + y_{Pu}^2}$, and $d_{R_bE} = \sqrt{(x_E - x_R)^2 + {y_E}^2}$. We assumed that the target secrecy capacity and the path-loss exponent were set to constants, $SC_{th} = 1$ (bits/s/Hz) and $\beta = 3$. The value range of β can be from 2–7, which depends on the transmission environments. To simplify the presentation, the parameters used to simulate and analyze are summarized in Table 1 as follows.

Table 1. Simulation parameters.

Symbols	Parameter Names	Values
β	Path-loss	3
M	Number of relays	3
α_1,α_2	Power allocation coefficients	0.8; 0.2
SC_{th}	Threshold	0.7, 1 (bit/s/Hz)
d_{R_bPu}	Distance of the R_b-Pu link	1
$d_{R_bD_1}$	Distance of the R_b-D_1 link	0.5
$d_{R_bD_2}$	Distance of the R_b-D_2 link	0.6, 1
d_{R_bE}	Distance of the R_b-E link	1–3

Figure 3 presents the sum SOPs of ST1, ST2 and ST3 versus Q(dB) when the symmetric network model is considered with M = 3, $\alpha_1 = 0.8$, $\alpha_2 = 0.2$, $\beta = 3$, SC_{th} = 1 (bit/s/Hz), $d_{R_bPu} = 1$, $d_{R_bD_1} = 0.5$, $d_{R_bD_2} = 1$, $d_{R_bE} = 1$. As shown in Figure 3, we can see that the secrecy performance of ST3 outperformed ST1 and ST2. The sum SOPs of ST1, ST2 and ST3 decreased when Q(dB) increased due to the increment of transmit powers. This can be explained by applying the NOMA technique and the selected relay method as in Sections 3.1–3.3.

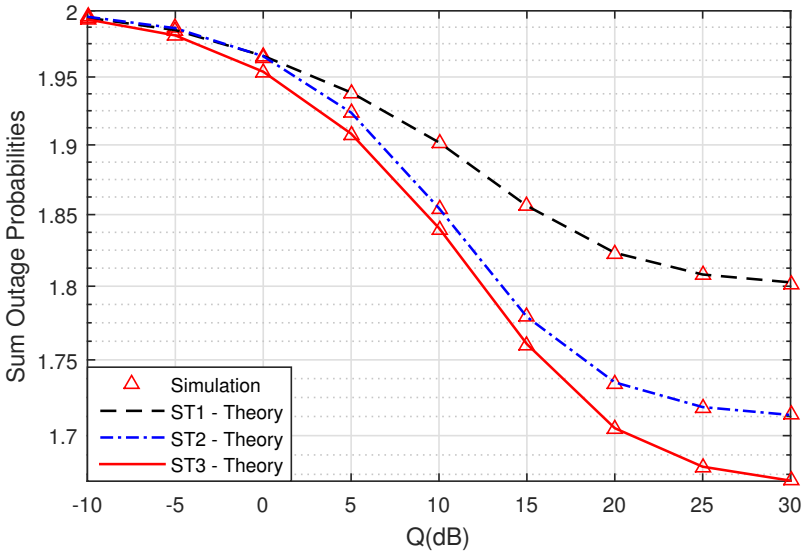

Figure 3. The sum SOPs of the UCCN-NOMA system versus Q(dB) when M = 3, $\alpha_1 = 0.8$, $\alpha_2 = 0.2$, $\beta = 3$ and SC_{th} = 1 (bit/s/Hz).

In Figure 4, we compare the sum SOPs with two defined thresholds in two values: Case 1, SC_{th} = 0.7 (bit/s/Hz), and Case 2, SC_{th} = 1 (bit/s/Hz). It is clear that the lower the threshold is, the better the sum SOPs becomes. Lastly, the simulation results in Figures 3 and 4 were suitable for the theoretical results of ST1, ST2, and ST3. Hence, we can conclude that the derived formulas during the analysis were accurate.

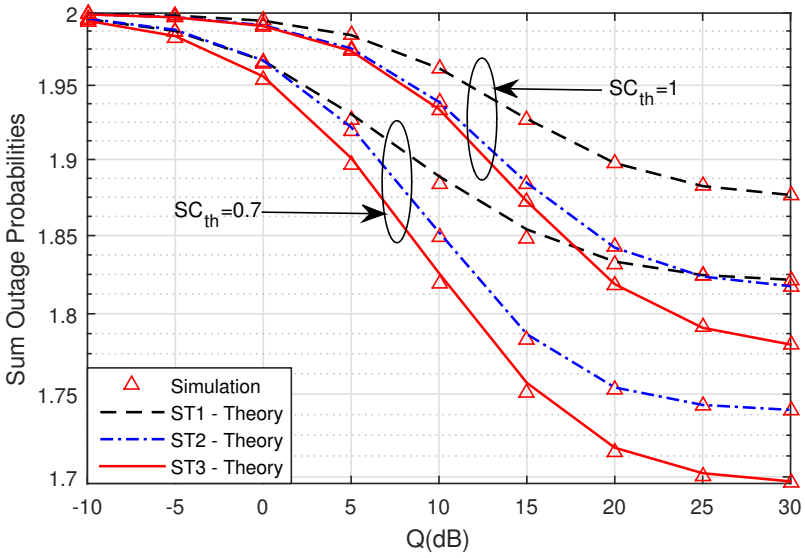

Figure 4. The sum SOPs of the UCCN-NOMA system versus Q(dB) when M = 3, $\alpha_1 = 0.8$, $\alpha_2 = 0.2$, $\beta = 3$, SC_{th} = 0.7 (bit/s/Hz) and SC_{th} = 1 (bit/s/Hz).

Figure 5 presents the sum SOPs versus the location of the eavesdropper node E when the symmetric network model is considered with M = 3, $\alpha_1 = 0.8$, $\alpha_2 = 0.2$, $\beta = 3$, Q (dB) = 10 dB, SC_{th} = 1 (bit/s/Hz), and d_{R_bE} moves from one to three. In Figure 5, the sum SOPs of ST3 are also smaller than the sum SOPs of ST1 and ST2. The simulation results and the theoretical results are logical. In addition, we can see that if the d_{R_bE} value increased, the sum SOPs decreased. This result means that the security of the system is very good when eavesdropper node E is far from the source and cooperative relay.

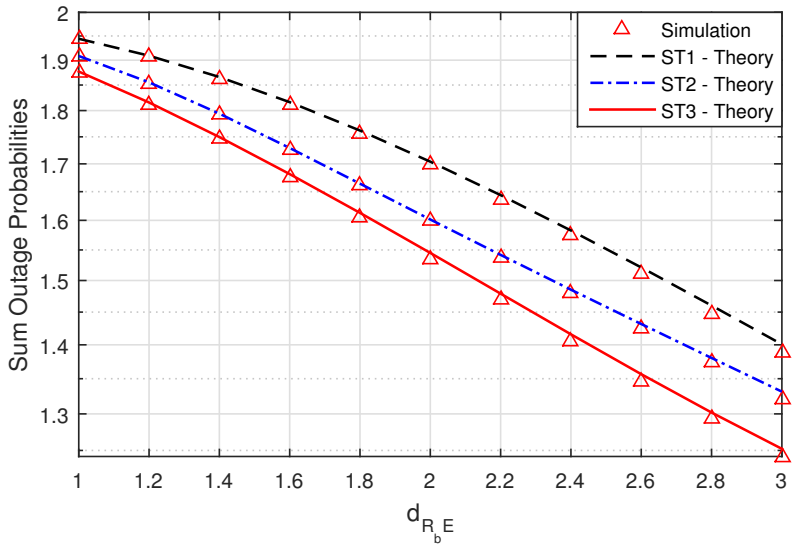

Figure 5. The sum SOPs of the UCCN-NOMA system versus d_{R_bE} when M = 3, $\alpha_1 = 0.8$, $\alpha_2 = 0.2$, $\beta = 3$ and SC_{th} = 1 (bit/s/Hz).

Figure 6 presents the sum SOPs versus Q(dB) when M = 3, $\alpha_1 = 0.8$, $\alpha_2 = 0.2$, $\beta = 3$, SC_{th} = 1 (bit/s/Hz), $d_{R_bD_2} = 0.6$, and $d_{R_bD_2} = 1$. As can be observed from Figure 6, the sum SOPs of ST1, ST2, and ST3 decreased at the higher Q(dB) regions. This clear because the proposed UCCN-NOMA system used NOMA, and the considered PLS with the best relay selection achieved higher secrecy efficiency. When link distance $d_{R_bD_2} = 0.6$, the security of the system is better than when $d_{R_bD_2} = 1$. However, the security of system in ST2 is smaller than two for the remaining cases due to D_2 being near the relay.

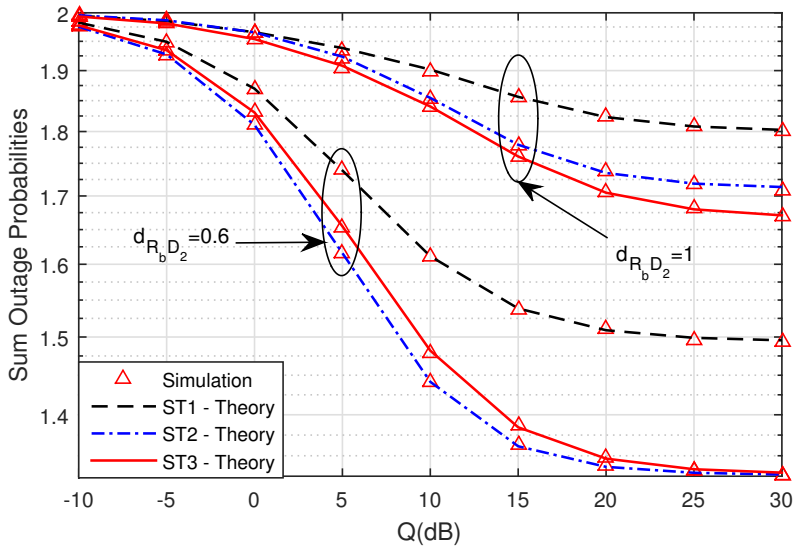

Figure 6. The sum SOPs of the UCCN-NOMA system versus Q(dB) when M = 3, $\alpha_1 = 0.8$, $\alpha_2 = 0.2$, $\beta = 3$, SC_{th} = 1 (bit/s/Hz), $d_{R_bD_2} = 0.6$, and $d_{R_bD_2} = 1$.

In Figure 7, we investigate the impact of power allocation coefficients on the security performance of the UCCN system with the NOMA solution. In this figure, we show the impacts of varying α_1 and α_2 on the system. When α_1 increased, the SOPs of the secrecy transmission of the signals x_1 and x_2 decreased and moved to small values. It is noticed that the power allocation coefficients in Figure 7 can result in significant capacity gains in the UCCN system with NOMA and the best relay selection solution.

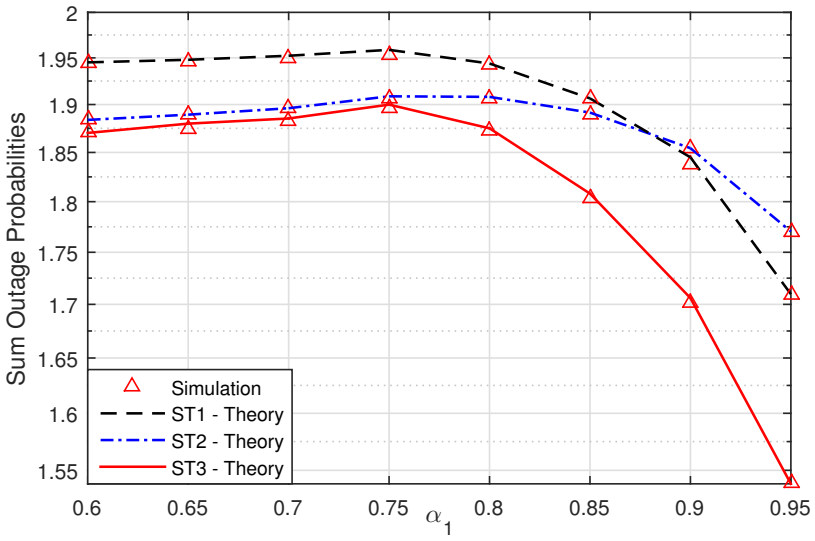

Figure 7. The sum SOPs of the UCCN-NOMA system versus α_1 when M = 3, $\beta = 3$ and SC_{th} = 1 (bit/s/Hz).

5. Conclusions

In this paper, we proposed a security system with multiple relays of the underlay cooperative cognitive network using the NOMA solution. We showed the three best relay selection cases. We calculated the maximum channel gain of the R_i-D_1 link to find the best relay for the first case. Similar to the first case, we also calculated the best relay for the second case of the R_i-D_2 link. The final case presented the minimum value of the channel gains from the R_i-E link. The secrecy performance of the UCCN-NOMA system in terms of the secrecy outage probabilities over Rayleigh fading channels was analyzed and evaluated. The simulation and analysis results were proven to be reasonable. The results of the (sum) secrecy outage probability showed that the proposed scheme can improve the secrecy performances. In addition, the security of the proposed system was better when eavesdropper node E was far from the source and cooperative relays. Finally, the simulations results verified the high accuracy of the derived theory analyses.

Author Contributions: T.-P.H. designed the idea; T.-P.H., P.N.S. analyzed and performed the simulation; P.N.S. contributed to developing some mathematical analysis parts; T.-P.H. organized and wrote the paper; P.N.S. and M.V. critically reviewed the organization of the paper.

Funding: This work was supported by the grant SGSReg. No. SP2019/41 conducted at VSBTechnical University of Ostrava, Czech Republic.

Conflicts of Interest: The authors declare that they have no competing interests.

Abbreviations

The following abbreviations are used in this manuscript:

NOMA	Non-orthogonal multiple access
UCCN	Underlay cooperative cognitive network
PLS	Physical layer security
SIC	Successive interference cancellation
DNC	Digital network coding
AF	Amplify-and-forward
DF	Decode-and-forward
SOP	Secrecy outage probability
CR	Cognitive radio

Appendix A. Proof of Lemma 1

From Formula (27), we calculate A_1 as follows:

$$\begin{aligned} A_1 &= \Pr\left[\frac{g_{2b_1}x}{(\theta+1)\left(Qg_{2b_1}\alpha_2+x\right)} \le \frac{\theta x}{(\theta+1)Q\alpha_1}\right] \\ &= \Pr\left[\frac{g_{2b_1}(\theta+1)Q\alpha_1}{(\theta+1)\left(Qg_{2b_1}\alpha_2+x\right)\theta} \le 1\right] = \Pr\left[g_{2b_1}Q\left(\alpha_1-\theta\alpha_2\right) \le x\theta\right] \\ &= \begin{cases} 1 & ,\alpha_1 \le \alpha_2\theta \\ F_{g_{2b_1}}\left[\frac{x\theta}{Q(\alpha_1-\alpha_2\theta)}\right] & ,\alpha_1 > \alpha_2\theta \end{cases} \end{aligned} \tag{A1}$$

Applying the cdf of the RVg_{2b_1} (17) to (A1), (A1) is solved in a closed-form expression as:

$$A_1 = \begin{cases} 1 & ,\alpha_1 \le \alpha_2\theta \\ \left(1-e^{-\lambda_2\psi x}\right)^M & ,\alpha_1 > \alpha_2\theta \end{cases} \tag{A2}$$

where $\psi = \frac{\theta}{Q(\alpha_1-\theta\alpha_2)}$

Hence, Appendix A is proven completely.

Appendix B. Proof of Lemma 2

To solve Lemma 2, we calculate A_2 in (22) as follows:

$$\begin{aligned} A_2 &= \Pr\left[g_{4b_1} > \frac{g_{2b_1}x}{(\theta+1)\left(\alpha_2Qg_{2b_1}+x\right)} - \frac{\theta x}{(\theta+1)Q\alpha_1}, \frac{g_{2b_1}x}{(\theta+1)\left(\alpha_2Qg_{2b_1}+x\right)} > \frac{\theta x}{(\theta+1)Q\alpha_1}\right] \\ &= \Pr\left[g_{4b_1} > \frac{g_{2b_1}x}{(\theta+1)\left(\alpha_2Qg_{2b_1}+x\right)} - \frac{\theta x}{(\theta+1)\alpha_1Q}, Qg_{2b_1}\left(\alpha_1-\theta\alpha_2\right) > \theta x\right] \\ &= \begin{cases} 0, \alpha_1 \le \theta\alpha_2 \\ \int_{\psi x}^{\infty} f_{g_{2b_1}}(y) P_r\left[g_{4b_1} > \frac{xy}{(\theta+1)(\alpha_2Qy+x)} - \frac{\theta x}{(\theta+1)\alpha_1Q}\right] dy, \alpha_1 > \theta\alpha_2 \end{cases} \end{aligned} \tag{A3}$$

Solving (A3) by using the pdf of the random variable g_{2b_1} and the cdf of the random variable g_{4b_1}, (A3) is obtained as:

$$A_2 = \begin{cases} 0 & ,\alpha_1 \le \theta\alpha_2 \\ \int_{\psi x}^{\infty} f_{g_{2b_1}}(y)\, e^{-\lambda_4\left(\frac{xy}{(\theta+1)(\alpha_2Qy+x)} - \frac{\theta x}{(\theta+1)Q\alpha_1}\right)} dxdy & ,\alpha_1 > \theta\alpha_2. \end{cases} \tag{A4}$$

Hence, Appendix B is proven completely.

References

1. Srivantana, T.; Maichalernnukul, K. Two-Way Multi-Antenna Relaying with Simultaneous Wireless Information and Power Transfer. *Symmetry* **2017**, *9*, 42. [CrossRef] [CrossRef]
2. Wu, F.; Xiao, L.; Yang, D.; Cuthbert, L.; Liu, X. Transceiver Design and Power Allocation for SWIPT in MIMO Cognitive Radio Systems. *Symmetry* **2018**, *10*, 647. [CrossRef] [CrossRef]
3. Ding, Z.; Lei, X.; Karagiannidis, G.K.; Schober, R; Yuan, J.; Bhargava, V.K. A Survey on Non-Orthogonal Multiple Access for 5G Networks: Research Challenges and Future Trends. *IEEE J. Sel. Areas Commun.* **2017**, *35*, 2181–2195. [CrossRef] [CrossRef]
4. Ly, T.T.H.; Nguyen, H.-S.; Nguyen, T.-S.; Huynh, V.V.; Nguyen, T.-L.; Voznak, M. Outage Probability Analysis in Relaying Cooperative Systems with NOMA Considering Power Splitting. *Symmetry* **2019**, *11*, 72. [CrossRef] [CrossRef]
5. Liu, Y.; Ding, Z.; Elkashlan, M.; Poor, H.V. Cooperative Non-orthogonal Multiple Access With Simultaneous Wireless Information and Power Transfer. *IEEE J. Sel. Areas Commun.* **2016**, *34*, 938–953. [CrossRef] [CrossRef]
6. Ding, Z.; Peng, M.; Poor, H.V. Cooperative Non-Orthogonal Multiple Access in 5G Systems. *IEEE Commun. Lett.* **2015**, *19*, 1462–1465. [CrossRef] [CrossRef]

7. Lee, S.; da Costa, D.B.; Vien, Q.; Duong, T.Q.; de Sousa, R.T. Non-orthogonal multiple access schemes with partial relay selection. *IET Commun.* **2017**, *11*, 846–854. [CrossRef] [CrossRef]
8. Duy, T.T.; Duong, T.Q.; Thanh, T.L; Bao, V.N.Q. Secrecy performance analysis with relay selection methods under impact of co-channel interference. *IET Commun.* **2015**, *9*, 1427–1435. [CrossRef] [CrossRef]
9. Maide, B.; Riccardo, C.; Luigi, F.; Mattia, F.; Alessandro, R. Does chaos work better than noise? *Circuits Syst. Mag. IEEE* **2003**, *2*, 4–19. [CrossRef]
10. Arena, P.; Fazzino, S.; Fortuna, L.; Maniscalco, P. Game theory and non-linear dynamics: The Parrondo Paradox case study. *Chaos Solitons Fract.* **2003**, *17*, 545–555. [CrossRef] [CrossRef]
11. Fan, L.; Lei, X.; Yang, N.; Duong, T.Q.; Karagiannidis, G.K. Secrecy Cooperative Networks with Outdated Relay Selection over Correlated Fading Channels. *IEEE Trans. Veh. Technol.* **2017**, *66*, 7599–7603. [CrossRef] [CrossRef]
12. He, B.; Liu, A.; Yang, N.; Lau, V.K.N. On the Design of Secure Non-Orthogonal Multiple Access Systems. *IEEE J. Sel. Areas Commun.* **2017**, *35*, 2196–2206. [CrossRef] [CrossRef]
13. Chen, J.; Yang, L.; Alouini, M. Physical Layer Security for Cooperative NOMA Systems. *IEEE Trans. Veh. Technol.* **2018**, *67*, 4645–4649. [CrossRef] [CrossRef]
14. Liu, X.; Wang, Y.; Liu, S.; Meng, J. Spectrum Resource Optimization for NOMA-Based Cognitive Radio in 5G Communications. *IEEE Access.* **2018**, *6*, 24904–24911. [CrossRef] [CrossRef]
15. Lv, L.; Chen, J.; Ni, Q. Cooperative Non-Orthogonal Multiple Access in Cognitive Radio. *IEEE Commun. Lett.* **2016**, *20*, 2059–2062. [CrossRef] [CrossRef]
16. Lee, S.; Duong, T.Q.; da Costa, D.B.; Ha, D.; Nguyen, S.Q. Underlay cognitive radio networks with cooperative non-orthogonal multiple access. *IET Commun.* **2018**, *12*, 359–366. [CrossRef] [CrossRef]
17. Lv, L.; Chen, J.; Ni, Q.; Ding, Z. Design of Cooperative Non-Orthogonal Multicast Cognitive Multiple Access for 5G Systems: User Scheduling and Performance Analysis. *IEEE Trans. Commun.* **2017**, *65*, 2641–2656. [CrossRef] [CrossRef]
18. Ding, X.; Song, T.; Zou, Y.; Chen, X. Relay selection for secrecy improvement in cognitive amplify-and-forward relay networks against multiple eavesdroppers. *IET Commun.* **2016**, *10*, 2043–2053. [CrossRef] [CrossRef]
19. Liu, Y.; Wang, L.; Duy, T.T.; Elkashlan, M.; Duong, T.Q. Relay Selection for Security Enhancement in Cognitive Relay Networks. *IEEE Wirel. Commun. Lett.* **2015**, *4*, 46–49. [CrossRef] [CrossRef]
20. Li, B.; Qi, X.; Huang, K.; Fei, Z.; Zhou, F.; Hu, R.Q. Security-Reliability Tradeoff Analysis for Cooperative NOMA in Cognitive Radio Networks. *IEEE Trans. Commun.* **2019**, *67*, 83–96. [CrossRef] [CrossRef]
21. Son, P.N.; Har, D.; Cho, N.I.; Kong, H.Y. Optimal Power Allocation of Relay Sensor Node Capable of Energy Harvesting in Cooperative Cognitive Radio Network. *Sensors* **2017**, *17*, 648. [CrossRef] [CrossRef] [PubMed]