Hindawi
Journal of Sensors
Volume 2022, Article ID 4915583, 14 pages
https://doi.org/10.1155/2022/4915583

Research Article

Dual-Hop Transmission and Multiple Relays for Performance Analysis of Designing Physical Layer Security for IoT Networks

Nhan Duc Nguyen,[1] **Anh-Tu Le**,[2] **Dinh-Thuan Do**,[3] **and Munyaradzi Munochiveyi**[4]

[1]*Faculty of Mechanical-Electrical and Computer Engineering, School of Engineering and Technology, Van Lang University, 69/68 Dang Thuy Tram Street, Ward 13, Binh Thanh District, Ho Chi Minh City 70000, Vietnam*
[2]*Faculty of Electronics Technology, Industrial University of Ho Chi Minh City, Vietnam*
[3]*Department of Computer Science and Information Engineering, Asia University, Taichung 41354, Taiwan*
[4]*Electrical and Electronic Engineering Department, University of Zimbabwe, Mount Pleasant, Harare, Zimbabwe*

Correspondence should be addressed to Munyaradzi Munochiveyi; mmunochiveyi@eng.uz.ac.zw

Received 24 August 2021; Revised 4 September 2021; Accepted 28 August 2022; Published 15 September 2022

Academic Editor: Akilesh Pathak

This article presents a secure performance metric of a downlink nonorthogonal multiple access (NOMA) in the presence of interference from the traditional user. In the context of NOMA, we deploy two-hop transmission to improve the performance of destinations. Further, multiple relays are implemented to aid robust signal-to-interference-plus-noise ratio (SINR) at destinations. We derive a closed-form expression of secure outage probability (SOP) to characterize security concerns in the case an eavesdropper exists in the overage of second hop transmission. We verify all expressions by employing Monte Carlo simulations.

1. Introduction

1.1. Motivation. The nonorthogonal multiple access (NOMA) procedures can progress the effectiveness of the spectrum since it can allocate the same frequency band to multiple users by differentiating the power levels of each user in the cluster [1–5]. Successive interference cancellation (SIC) is a technique that is achieved at the receiver's end to distinguish the received signals [6]. The addition of the NOMA technique into cognitive radio (CR) networks has shown advantages like improving better spectral efficiency and also serving increased numerous secondary users, realizing 5th generation (5G) communication systems [7]. In [8], the author mentioned repetition-based NOMA, which can achieve high diversity gain by utilizing repetition. This method is different compared to the conventional power domain NOMA as all users possess the same power level but a diverse number of repetitions. Since it has high diversity gain, we can achieve low outage probability with no need for instant channel state information (CSI) response for power allocation. The key parameters are constrained to sustain the outage probability (OP) lesser than the target value by deriving a closed-form expression of OP. Moreover, in [9] the authors examined the impact of imperfect CSI and imperfect SIC on NOMA-enabled coordinated direct and relay transmission (CDRT) network consisting of a base station communicating directly with a cell-centered user and an FD relay responsible for communicating with a user located at the cell-edge. Here, the authors obtained exact OP and ergodic rates for the users under the assumption of imperfect CSI and SIC. Also, the authors considered the channel links to be operating under Nakagami-m fading conditions. Numerical results demonstrated the adverse impact of imperfect CSI and SIC on the OP performance of the system. To remedy this, the authors determined a suitable base-station power allocation coefficient to ensure fair outage for both network users under imperfect CSI and SIC conditiIn [10], the authors studied the performance of downlink NOMA in vehicular communication over double Rayleigh fading channels, where a base station communicates with a

far-user and a near-user. Due to the impact of mobility, the authors derived OP expressions of the individual users as well as for the overall system considering the scenario of when the NOMA rate falls below the system target rate and when Orthogonal Multiple Access (OMA) outperforms the NOMA system. Additionally, the authors derived ergodic capacity and Average Bit Error Rate (ABER) expressions. Numerical results showed that in terms of OP and ergodic capacity, NOMA outperforms OMA, however in terms of ABER, OMA outperforms NOMA as OMA users lack inter-user interferences.

In the presence of massive communications, security becomes the major apprehension among the users. Because of the diverse nature of radio propagation, the communication networks are exposed to the eavesdropper, and this also becomes a major challenge for researchers to overcome [11]. We know that cognitive radio (CR) networks permit unlicensed users in the spectrum that increases the risk of wiretapping, particularly when the users are malicious. In previous generations, cryptographic algorithms are utilized in the top layers to protect the data. But these algorithms are time-consuming and complicated since they have to perform encryption and decryption to protect the data [12]. Whereas, Physical Layer Security (PLS) has become the single utmost significant tactic to secure the data. Since the evolution of CR networks, there has been a giant exploration going on to enhance the performance of PLS [13–20]. Authors in [13, 14] have designed CR networks user-scheduling schemes, to improve the secrecy performance by achieving multiuser diversity for a primary user under the Quality of Service (QoS) limitation. Authors in [13] have shown that the scheme can achieve maximum diversity, whereas in [14], the three user-scheduling schemes show that the secrecy performance rate is significantly enhanced by growing the number of cognitive users. Authors in [15] have employed multiple relay selection policies where one relay aids in transmitting the information and the other acts as a friendly jammer. This way, the authors were able to obtain efficient performance in terms of secrecy outage of the cognitive transmission system. In [16], the authors proposed an Artificial Noise (AN) assisted optimal beamforming scheme, in which the ergodic secrecy rate is maximized by obtaining optimal power allocation among data and AN signal.

Until now, all the works discussed are based on Rayleigh fading channels, whereas the works in [17–20] are based on Nakagami-m fading channels. In [17] the authors have provided a consistent method to identify the secrecy performance of the framework by determining the mathematical expression of Secrecy Outage Probability (SOP) and nonzero secrecy capacity probability. Authors in [18] have considered a multi-antenna networks approach by proposing optimal and suboptimal antenna selecting schemes for secured underlay CR networks. The authors have also derived mathematical descriptions of the exact and asymptotic SOP of both schemes. In [19], the authors considered enhancing the secrecy performance by increasing the number of relays or legitimate channel Nakagami parameters. In [20], the authors considered PLS in a CR network with multiple primary and secondary users. PLS also plays a pivotal role in NOMA communications in terms of secure transmission [20–25]. Especially, the authors in [24–26] mentioned that the secrecy performance of the NOMA technique outperforms the Orthogonal Multiple Access (OMA) technique. Authors in [24] optimized the transmit power to achieve a maximum secrecy rate. Along with these techniques, authors in [25, 26] have adopted beamforming and power allocation policies. In [25], the authors considered a NOMA-assisted multicast-unicast system and studied the risk of multicast receivers intercepting the unicasting messages. Whereas, in [26], the cell-edge user is considered an eavesdropper who spies on the data and information of a cell-center user. Authors in [27] have considered the user pairing method to improve the security of the NOMA system. In this model, the users are arranged according to their channel gains and paired with unlike channel gains to achieve the NOMA protocol. The outcomes explain that the secrecy diversity order of the user is equal to the ascending direction of channel ordering.

1.2. Related Works. Recently, several authors have been interested in studying secrecy in NOMA-aided Full-Duplex (FD) systems in the vicinity of eavesdroppers. One of these works is found in [28], where the authors investigated the SOP of NOMA-assisted dual-hop FD amplify-and-forward networks in the presence of a colluding and noncolluding wiretapping eavesdropper. This system comprised a base station, a multiple antenna FD relay, an eavesdropper, and multiple users. In [29], the authors studied the trade-off between reliability and security of PLS techniques in cooperative NOMA-enabled dual-hop Internet-of-Things (IoT) systems under in-phase and quadrature-phase imbalance (IQI) conditions at the transceivers. The system consisted of a single source, a relay, an eavesdropper, and multiple devices. Here, the authors derived closed-form OP and Intercept Probability (IP) expressions. The simulation results showed that IQI increases OP while reducing IP, demonstrating that reliability is impacted but security is enhanced. In [30], the author considered the PLS of a dual-hop NOMA system consisting of a single source, relay, an eavesdropper, and numerous users. The authors maximized the system's secure sum rate over different source subcarriers with optimal power allocation. Further, the authors solved the nonconvex and mixed-integer programming problem via duality theory. Simulation results demonstrated that the proposed system outperforms OMA systems. In [31], the authors examined the Strictly Positive Secrecy Capacity (SPSC) and SOP of a NOMA-aided dual-hop DF system under different scenarios of untrusted and trusted relays. Here, the network is made up of a base station, a DF relay, an eavesdropper, and a multiple users. The authors derived exact expressions for SPSC and SOP under independent Rayleigh fading. Moreover, numerical results compared the secrecy performance of the proposed system against OMA. Similarly, in [32], the authors examined the secrecy performance of cooperative downlink and uplink NOMA-aided network with an untrusted relay. To minimize secrecy failure at the untrusted relay, the authors proposed adaptive downlink and uplink jamming strategies. For each strategy, the authors derived lower bound ergodic secrecy sum rates

for the proposed system. Furthermore, in [33], the authors considered different scenarios of single and multiple antenna relay configurations at the source and the untrusted relay. In this work, the authors derived closed-form lower bound ergodic secrecy sum rate (ESSR) and proved via simulation results how the proposed system outperforms OMA systems.

Differently, in [34], the authors considered the SOP of a cooperative NOMA-aided system with multiple relays over Nakagami-m fading channels in the presence of an eavesdropper. Here, the authors proposed three different types of relay selection (RS) strategies which are Optimal Single Relay Selection (OSRS), Two-Step Single Relay Selection (TSRS), and Optimal Dual Relay Selection (ODRS). The authors obtained closed-form SOP expressions under different RS strategies. Similarly, in [35], the authors considered the asymptotic SOP of NOMA-assisted multiple-DF relay network over Rayleigh fading channels with two RS schemes—OSRS and TSRS. The authors also derived exact asymptotic SOP for both RS schemes considering fixed and dynamic power allocations. In [36], the authors investigated a cooperative NOMA network with multiple relays, where one relay transmits information and the other relays act as jammers. Here, the authors considered two RS schemes, random and max–min RS. The authors derived closed-form SOP for both RS schemes. Simulation results proved that in the moderate to high signal-to-noise ratio (SNR) region, the proposed scheme obtains a lower SOP than systems without jammers. Also, the max-min RS scheme enhances the SOP in the low SNR range.

However, it would be unreasonable for us not to mention the hidden cost of multiple relays in NOMA-aided massive IoT networks. Large CSI signaling overhead, power allocation feedback, and computational complexity emerge when there are a massive number of devices and relays in NOMA-enabled multiple-relay networks [37, 38]. In such a scenario, feedback delay from the multiple relays becomes a critical issue resulting in channel estimation and synchronization errors in the uplink [37, 38]. Therefore, obtaining perfect CSI is difficult to achieve [37, 38]. These issues are still open research problems, and we welcome more research in this area to enable NOMA-enabled multiple relay networks to be implemented practically.

Furthermore, another area of interest this research work did not consider, but is also worth researching, is the security in simultaneous wireless information and power transfer- (SWIPT-) enabled IoT networks. The authors in [39, 40] proposed a PLS approach for SWIPT-enabled multiple relays IoT network. Additionally, the authors investigated the impact of static power splitting relaying (SPSR) and dynamic power splitting relaying (DPSR) on secure communications in the presence of an eavesdropper. Similarly, in [41], the authors also considered the impact of SPSR and DPSR on the outage and throughput performance for a DF relay SWIPT system, consisting of a single source, multiple relays, and a destination. Differently, in [42], the authors proposed partial and full relay selection techniques for self-energy recycling (S-ER) FD multiple-relay networks, in which the self-interference energy is harvested back at the relay for future use.

1.3. Contributions. In several works, such as [34–36], the authors considered systems with multiple relays and different RS strategies when examining the SOP of such proposed systems. However, the practical issue of interference was not investigated in those works. Therefore, in this work, we propose a NOMA-enabled multiple-relay communication network reliant on partial relay selection (PRS) and investigate the SOP performance of the proposed system. In particular, we take into consideration the aspect of interferences on the NOMA-aided communication system. Table 1 provides a comparison of this work versus the works in [28–36]. Our contributions are listed as follows:

(i) We consider transmission assisted by NOMA where a single antenna base station communicates with two devices arranged in a near and far position from the base station in the presence of an eavesdropper, multiple relays, and interference causing conventional user equipment (CUE). The proposed system employs a partial relay selection (PRS) scheme. We study the secrecy performance to determine the downlink SOP and SPSC performance under Rayleigh fading channels

(ii) We then determine the signal-to-interference-plus-noise ratios (SINRs) of the two devices and use them to formulate exact SOP and SPSC formulas over Rayleigh fading channels. The derived expressions are validated by Monte Carlo simulations

(iii) We analyze and compare the SOP and SPSC under various conditions. In particular, we find that transmit SNR at source, interference channel, the number of relays, and power allocation factors are the main impacts on SOP and SPSC. The obtained numerical results demonstrate that the proposed scheme can increase secrecy and achieve significant SOP via many practical scenarios

1.4. Organization. The rest of this paper is organized as follows. Section 2 describes the downlink NOMA under Rayleigh channels in the dual-hop multiple-relay network in the presence of an eavesdropper and interference. In Section 3, we consider the scenario of NOMA in terms of secrecy outage performance. In Section 4, we consider strictly positive secrecy capacity. In Section 5, we provide extensive numerical simulations, and Section 6 concludes the paper.

2. System Model

A downlink NOMA cooperative relay network is studied, as shown in Figure 1. In particular, we consider a base station (S), a K DF relays, two main destinations (D_i), an eavesdropper (E), and a conventional user equipment (CUE). This CUE causes interference to the two main users (D_i) as in Figure 1. In addition, the channel coefficient from S to R_k, $(k = 1, \cdots, K)$, from R_k to D_i, from R_k to E, and from the CUE to D_i are g_{SR_k}, $g_{R_kD_i}$, $g_{R_kE,}$ and g_{CU_i}, respectively. All channels experience Rayleigh fading, i.e., channel g with

Table 1: A comparison of existing works on PLS for dual-hop transmission and multiple relays.

System setup	Reference	Major contributions	Scenario
Dual-hop FD-AF-NOMA	[28]	Closed-form SOP expressions	Colluding and noncolluding wiretapping eavesdropper
Dual-hop DF-NOMA-IoT	[29]	Closed-form OP and IP expressions	In-phase and quadrature-phase imbalance (IQI) conditions at the transceivers
Dual-hop AF-NOMA	[30]	Secure sum rate maximization over different source subcarriers with optimal power allocation	Single eavesdropper
Dual-hop untrusted DF-NOMA	[31]	Closed-form SPSC and SOP expressions	Untrusted and trusted relays
Dual-hop untrusted AF-NOMA	[32]	Closed-form lower bound ESSR	Untrusted AF relay engaged in both relaying and eavesdropping
Dual-hop untrusted AF-NOMA	[33]	Closed-form lower bound ESSR	Untrusted relay
Dual-hop relay-selection DF-HD-NOMA	[34]	Closed-form SOP expressions under different RS strategies	Single eavesdropper
Dual-hop relay-selection DF-NOMA	[35]	Closed-form asymptotic SOP for both RS schemes considering fixed and dynamic power allocations.	Single eavesdropper
Dual-hop jamming HD-DF-NOMA	[36]	Closed-form SOP under different RS schemes	Jamming relay
Dual-hop interference DF-NOMA-IoT	Our work	Closed-form SOP and SPSC under PRS setup	Single eavesdropper, interference causing conventional user equipment (CUE)

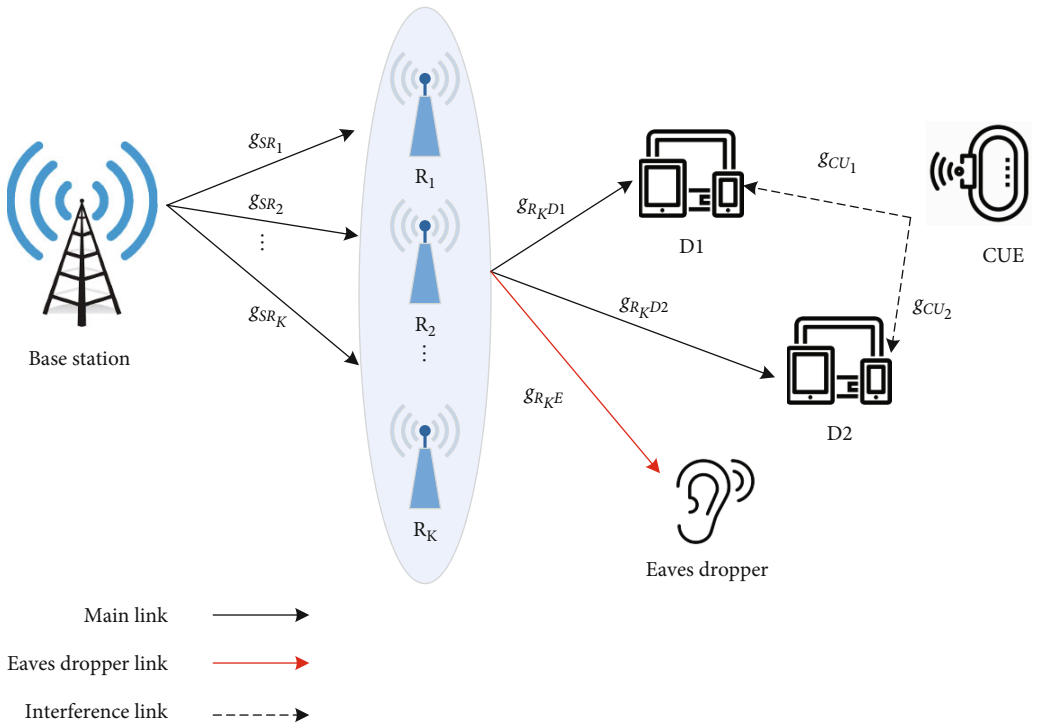

Figure 1: Downlink dual-hop NOMA-aided multiple-relay network in the presence of an eavesdropper and interference.

parameter $CN(0, \Omega)$. Moreover, we assume all channels follow perfect CSI as in [4].

In the first time slot, the source (S) transmits the signal $\sqrt{a_1}x_1 + \sqrt{a_2}x_2$ to the selected relay R_k in which a_1 and a_2 are the power allocation coefficient and $a_1 < a_2$, and x_i is the signal dedicated to D_i. Therefore, the received signal R_k is given by

$$r_{SR_k} = \sqrt{P_S}(\sqrt{a_1}x_1 + \sqrt{a_2}x_2)g_{SR_k} + n_{R_k}, \quad (1)$$

where P_S is the transmit power at S, and n_{R_k} is $CN(0, \sigma^2_{R_k})$. When R_k decodes x_2, the signal-to-interference-plus-noise ratio (SINR) is formulated by

$$\vartheta_{R_k \longrightarrow x_2} = \frac{P_S a_2 \left| g_{SR_k} \right|^2}{P_S a_1 \left| g_{SR_k} \right|^2 + \sigma^2_{R_k}} = \frac{\rho_S a_2 \left| g_{SR_k} \right|^2}{\rho_S a_1 \left| g_{SR_k} \right|^2 + 1}, \quad (2)$$

where $\rho_S = ((P_S)/(\sigma^2_{R_k}))$. Following the principle of the NOMA scheme [4], the instantaneous signal-to-noise-ratio (SNR) after using successive interference cancellation (SIC) to detect x_1 at R_k is given by

$$\vartheta_{R_k \longrightarrow x_1} = \rho_S a_1 \left| g_{SR_k} \right|^2. \quad (3)$$

In the second time slot, the relay R_k forwards the signal from source S to D_i. As a result, the received signal D_i is formulated by

$$r_{RD_i} = \sqrt{P_R}(\sqrt{a_1} x_1 + \sqrt{a_2} x_2) g_{R_k D_i} + P_{CE} g_{CU_i} + n_i, \quad (4)$$

where P_R is the transmit power at R_k, P_{CE} is the power of the CUE, and n_i is $CN(0, \sigma^2_i)$. Next, the SINR at D_2 when detecting its own signal x_2 is given as

$$\begin{aligned} \vartheta_{D_2 \longrightarrow x_2} &= \frac{P_R a_2 \left| g_{R_k D_2} \right|^2}{P_R a_1 \left| g_{R_k D_2} \right|^2 + P_{CE} \left| g_{CU_2} \right|^2 + \sigma^2_2} \\ &= \frac{\rho_R a_2 \left| g_{R_k D_2} \right|^2}{\rho_R a_1 \left| g_{R_k D_2} \right|^2 + \rho_{CE} \left| g_{CU_2} \right|^2 + 1}, \end{aligned} \quad (5)$$

where $\rho_R = ((P_R)/(\sigma^2_i))$, $\rho_{CE} = ((P_{CE})/(\sigma^2_i))$. Next the SINR at D_1 when detecting signal x_2 is expressed by

$$\vartheta_{D_1 \longrightarrow x_2} = \frac{\rho_R a_2 \left| g_{R_k D_1} \right|^2}{\rho_R a_1 \left| g_{R_k D_1} \right|^2 + \rho_{CE} \left| g_{CU_1} \right|^2 + 1}. \quad (6)$$

By conducting SIC, the SINR to detect signal x_1 at D_1 is expressed by

$$\vartheta_{D_1 \longrightarrow x_1} = \frac{\rho_R a_1 \left| g_{R_k D_1} \right|^2}{\rho_{CE} \left| g_{CU_1} \right|^2 + 1}. \quad (7)$$

To consider the impact of the eavesdropper, we need to compute the received signal at E as

$$r_E = \sqrt{P_R}(\sqrt{a_1} x_1 + \sqrt{a_2} x_2) g_{R_k E} + n_E, \quad (8)$$

where n_E is $CN(0, \sigma^2_E)$ and $\rho_E = ((P_E)/(\sigma^2_E))$. Similar to [43], the instantaneous SNR of detecting the signal D_i are given as

$$\vartheta_{E \longrightarrow x_i} = \rho_E a_i \left| g_{R_k E} \right|^2. \quad (9)$$

By employing partial relay selection (PRS), the selected relay R_k is chosen as follows based on criteria [44].

$$k^* = \arg \max_{k=1,\cdots,K} \left| g_{SR_k} \right|^2. \quad (10)$$

3. Performance Analysis

In this section, we derive the closed-form of Secrecy Outage Probability (SOP) for D_i. The secrecy rate of D_i is given as

$$C_i = \left[\frac{1}{2} \log_2 \left(1 + \min \left(\vartheta_{R_{k*} \longrightarrow x_2}, \vartheta_{D_2 \longrightarrow x_2} \right) \right) - \frac{1}{2} \log_2 \left(1 + \vartheta_{E \longrightarrow x_2} \right) \right]^+, \quad (11)$$

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

3.1. Secrecy Outage Probability of D_2. Following the result reported in [45], the cumulative distribution functions (CDF) of $|g_{SR_{k*}}|^2 = \max_{k=1,\cdots,K} |g_{SR_k}|^2$ is given as

$$\begin{aligned} F_{\left| g_{SR_{k*}} \right|^2}(x) &= \left(1 - e^{-\left(x/\left(\Omega_{SR_{k*}} \right) \right)} \right)^K \\ &= 1 - \sum_{k=1}^{K} \binom{K}{k} (-1)^{k-1} e^{-\left((kx)/\left(\Omega_{SR_{k*}} \right) \right)}. \end{aligned} \quad (12)$$

Then, the SOP of D_2 is computed by

$$\begin{aligned} \mathrm{SOP}_{D_2} &= \Pr(C_2 < R_2) \\ &= \Pr\left(\frac{1 + \min \left(\vartheta_{R_{k*} \longrightarrow x_2}, \vartheta_{D_2 \longrightarrow x_2} \right)}{1 + \vartheta_{E \longrightarrow x_2}} < \gamma_2 \right) \\ &= 1 - \Pr\left(\frac{1 + \vartheta_{R_{k*} \longrightarrow x_2}}{1 + \vartheta_{E \longrightarrow x_2}} > \gamma_2, \frac{1 + \vartheta_{D_2 \longrightarrow x_2}}{1 + \vartheta_{E \longrightarrow x_2}} > \gamma_2 \right), \end{aligned} \quad (13)$$

where $\gamma_i = 2^{2R_i}$ and R_i is the targeted secrecy rate. Substituting (2), (5), and (9) into (12), it can be written such SOP for D_2 as

$$\begin{aligned}\mathrm{SOP}_{D_2} &= 1-\Pr\left(\vartheta_{R_{k_*}\longrightarrow x_2}>\delta_2+\gamma_2\vartheta_{E\longrightarrow x_2},\vartheta_{D_2\longrightarrow x_2}>\delta_2+\gamma_2\vartheta_{E\longrightarrow x_2}\right)\\ &= 1-\Pr\left(\left|g_{SR_{k_*}}\right|^2>\frac{\delta_2+\beta_2\left|g_{R_{k_*}E}\right|^2}{a_1\rho_S\beta_2\left(\chi_2-\left|g_{R_{k_*}E}\right|^2\right)},\left|g_{R_{k_*}D_2}\right|^2>\frac{\left(\delta_2+\beta_2\left|g_{R_{k_*}E}\right|^2\right)\left(\rho_{CE}\left|g_{CU_2}\right|^2+1\right)}{a_1\rho_R\beta_2\left(\chi_2-\left|g_{R_{k_*}E}\right|^2\right)}\right),\end{aligned} \tag{14}$$

where $\beta_i=\gamma_i a_i\rho_E$, $\delta_i=\gamma_i-1$. Then, the SOP of D_2 can be rewritten by

$$\begin{aligned}\mathrm{SOP}_{D_2} &= 1-\sum_{k=1}^{K}\binom{K}{k}\frac{(-1)^{k-1}}{\Omega_{CU_2}\Omega_{R_{k_*}E}}\int_0^{\chi_2}e^{-(((\delta_2+\beta_2z)k)/(\theta_2(\chi_2-z)))}e^{-((\delta_2+\beta_2z)/(\theta_1(\chi_2-z)))}e^{-\left(z/\left(\Omega_{R_{k_*}E}\right)\right)}\int_0^{\infty}e^{-((\rho_{CE}(\delta_2+\beta_2z)y)/(\theta_1(\chi_2-z)))}e^{-\left(y/\left(\Omega_{CU_2}\right)\right)}dydz\\ &= 1-\sum_{k=1}^{K}\binom{K}{k}\frac{(-1)^{k-1}}{\Omega_{R_{k_*}E}}\int_0^{\chi_2}\frac{e^{-(((\delta_2+\beta_2z)k)/(\theta_2(\chi_2-z)))}e^{-((\delta_2+\beta_2z)/(\theta_1(\chi_2-z)))}e^{-\left((z)/\left(\Omega_{R_{k_*}E}\right)\right)}}{1+(\theta_3(\delta_2+\beta_2z)/\chi_2-z)}dz,\end{aligned} \tag{15}$$

where $\chi_2=(1/(a_1\beta_2))-((\gamma_2)/(\beta_2))$, $\theta_1=\Omega_{R_{k_*}D_2}a_1\rho_R\beta_2$, $\theta_2=\Omega_{SR_{k_*}}a_1\rho_S\beta_2$, and $\theta_3=((\Omega_{CU_2}\rho_{CE})/(\theta_1))$. Using Gaussian-Chebyshev Quad with $\phi_n=\cos((2n-1)/(2N))$, SOP_{D_2} is given by

$$\mathrm{SOP}_{D_2}\approx 1-\frac{\pi}{2N}\sum_{k=1}^{K}\binom{K}{k}\frac{\chi_2(-1)^{k-1}}{\Omega_{R_{k_*}E}}\sum_{n=1}^{N}\sqrt{1-\phi_n^2}\frac{e^{-((((2\delta_2+\beta_2\chi_2(1+\phi_n))k)/(\theta_2\chi_2(1-\phi_n))))}e^{-(((2\delta_2+\beta_2\chi_2(1+\phi_n))/(\theta_1\chi_2(1-\phi_n))))}e^{-\left(\chi_2(1+\phi_n)(\,)/\left(2\Omega_{R_{k_*}E}\right)\right)}}{1+((\theta_3(2\delta_2+\beta_2\chi_2(1+\phi_n)))/(\chi_2(1-\phi_n)))}. \tag{16}$$

3.2. Secrecy Outage Probability of D_1. In here, the SOP of D_1 is given by

$$\begin{aligned}\mathrm{SOP}_{D_1} &= \Pr(C_1<R_1)\\ &= \Pr\left(\frac{1+\min\left(\vartheta_{R_{k_*}\longrightarrow x_1},\vartheta_{D_1\longrightarrow x_1}\right)}{1+\vartheta_{E\longrightarrow x_1}}<\gamma_1\right)\\ &= 1-\Pr\left(\vartheta_{R_{k_*}\longrightarrow x_1}>\gamma_1\left(1+\vartheta_{E\longrightarrow x_1}\right)-1,\vartheta_{D_1\longrightarrow x_1}>\gamma_1\left(1+\vartheta_{E\longrightarrow x_1}\right)-1\right).\end{aligned} \tag{17}$$

Proposition 1. *The expression SOP of D_1 is given by*

$$\begin{aligned}SOP_{D_1} &= 1+\sum_{k=1}^{K}\binom{K}{k}\frac{(-1)^{k-1}\mu_2e^{-\delta_1\mu_1}}{\Omega_{R_{k_*}E}}\\ &\quad\cdot e^{\left(\left(\mu_3\left(\beta_1\mu_1\Omega_{R_{k_*}E}+1\right)\right)/\left(\Omega_{R_{k_*}E}\right)\right)}Ei\left(-\frac{\mu_3\left(\beta_1\mu_1\Omega_{R_{k_*}E}+1\right)}{\Omega_{R_{k_*}E}}\right).\end{aligned} \tag{18}$$

Proof. Putting (3), (7), and (9) into (17), we have

$$\begin{aligned}\mathrm{SOP}_{D_1} &= 1-\Pr\left(\left|g_{SR_{k_*}}\right|^2>\frac{\delta_1+\beta_1\left|g_{R_{k_*}E}\right|^2}{a_1\rho_S},\left|g_{R_{k_*}D_1}\right|^2>\frac{\left(\delta_1+\beta_1\left|g_{R_{k_*}E}\right|^2\right)\left(\rho_{CE}\left|g_{CU_1}\right|^2+1\right)}{a_1\rho_R}\right),\\ &= 1-\int_0^{\infty}\int_0^{\infty}f_{\left|g_{R_{k_*}E}\right|^2}(z)f_{\left|g_{CU_1}\right|^2}(y)\left(1-F_{\left|g_{SR_{k_*}}\right|^2}\left(\frac{\delta_1+\beta_1z}{a_1\rho_S}\right)\right)\left(1-F_{\left|g_{R_{k_*}D_1}\right|^2}\left(\frac{(\delta_1+\beta_1z)(\rho_{CE}y+1)}{a_1\rho_R}\right)\right)dydz.\end{aligned} \tag{19}$$

After some variable substitutions and manipulations, (19) can be transformed by

$$\begin{aligned}\mathrm{SOP}_{D_1} &= 1 - \sum_{k=1}^{K}\binom{K}{k}\frac{(-1)^{k-1}e^{-\delta_1\mu_1}}{\Omega_{CU_1}\Omega_{R_{k*}E}}\int_0^{\infty} e^{-\beta_1\mu_1 z}e^{-\left(z/\left(\Omega_{R_{k*}E}\right)\right)} \\ &\cdot \int_0^{\infty} e^{-\left((\rho_{CE}(\delta_1+\beta_1 z))/\left(\Omega_{R_{k*}D_1}a_1\rho_R\right)\right)y}e^{-\left(y/\left(\Omega_{CU_1}\right)\right)}dyd \\ &= 1 - \sum_{k=1}^{K}\binom{K}{k}\frac{(-1)^{k-1}\mu_2 e^{-\delta_1\mu_1}}{\Omega_{R_{k*}E}}\int_0^{\infty}\frac{e^{-\left(\beta_1\mu_1+\left(1/\left(\Omega_{R_{k*}E}\right)\right)\right)z}}{\mu_3+z}dz,\end{aligned} \tag{20}$$

where $\mu_1 = (1/(\Omega_{SR_{k*}}a_1\rho_S)) + (1/(\Omega_{R_{k*}D_1}a_1\rho_R))$, $\mu_2 = ((\Omega_{R_{k*}D_1}a_1\rho_R)/(\rho_{CE}\Omega_{CU_1}\beta_1))$, and $\mu_3 = \mu_2 + ((\delta_1)/(\beta_1))$. Using ([46], 3.352.4), (18) can be obtained.

The proof is completed. □

3.3. Asymptotic SOP Analysis. In this section, the asymptotic SOP expression could be derived at high SNR $\rho_S = \rho_R \longrightarrow \infty$ to provide more insights of performance analysis. It can be performed by applying the first-order Maclaurin's series expansions $e^{-x} = 1 - x$ and use $Ei(-x) = \ln(x) + C$ as [46]. The asymptotic SOP of D_2 and D_1 are expressed as, respectively,

$$\begin{aligned}\mathrm{SOP}_{D_2} &\approx 1 - \frac{\pi}{2N}\sum_{k=1}^{K}\binom{K}{k}\frac{\chi_2(-1)^{k-1}}{\Omega_{R_{k*}E}}\sum_{n=1}^{N}\sqrt{1-\phi_n^2} \\ &\cdot \left(1 + \frac{\theta_3(2\delta_2 + \beta_2\chi_2(1+\phi_n))}{\chi_2(1-\phi_n)}\right)^{-1} \\ &\times \left(1 - \frac{(2\delta_2 + \beta_2\chi_2(1+\phi_n))(k+1)}{\theta_2\chi_2(1-\phi_n)} - \frac{\chi_2(1+\phi_n)}{2\Omega_{R_{k*}E}}\right),\end{aligned} \tag{21}$$

$$\begin{aligned}\mathrm{SOP}_{D_1} &= 1 + \sum_{k=1}^{K}\binom{K}{k}\frac{(-1)^{k-1}\mu_2}{\Omega_{R_{k*}E}}\left(1 + \frac{\mu_3\left(\beta_1\mu_1\Omega_{R_{k*}E}+1\right)}{\Omega_{R_{k*}E}} - \delta_1\mu_1\right) \\ &\cdot \left(\ln\left(\frac{\mu_3\left(\beta_1\mu_1\Omega_{R_{k*}E}+1\right)}{\Omega_{R_{k*}E}}\right) + C\right).\end{aligned} \tag{22}$$

4. Strictly Positive Secrecy Capacity Analysis

In this section, we analyze the strictly positive secrecy capacity (SPSC). Then, the SPSC of the system is given as [47].

$$\mathrm{SPCP}_{\mathrm{out}} = \Pr(C_1 > 0, C_2 > 0). \tag{23}$$

Table 2: Table of parameter.

System parameters	Value
The power allocation	$a_1 = 0.2$ and $a_2 = 0.8$
The number of relay	$K = 2$
The power of CUE	$\rho_{CU} = 1$
The parameter of channel	$\Omega_{SR_{k*}} = \Omega_{R_{k*}D_i} = \Omega_{R_{k*}E} = \Omega_{CU_1} = \Omega_{CU_2} = 1$
The target rate	$R_1 = 1$ and $R_2 = 0.1$ bit per channel use

Proposition 2. *The close-form of SPSC is given by*

$$\begin{aligned}SPCP_{out} &= -\sum_{k=1}^{K}\binom{K}{k}\frac{(-1)^{k-1}\Omega_{R_{k*}D_1}\rho_R}{\rho_{CE}\rho_E\Omega_{CU_1}\Omega_{R_{k*}E}}e^{\left(\varpi_1/\left(\Omega_{CU_1}\right)\right)}Ei \\ &\cdot \left(-\frac{\varpi_1}{\Omega_{CU_1}}\right) \times \sum_{k_1=1}^{K}\binom{K}{k_1}\frac{(-1)^{k_1-1}}{2\rho_E a_1\Omega_{R_{k*}E}}\frac{\pi}{N}\sum_{n=1}^{N} \\ &\cdot \frac{\sqrt{1-\phi_n^2}e^{-\varpi_2(1+\phi_n)}}{1 + \left(\left((1+\phi_n)\rho_{CE}\Omega_{CU_2}\right)/\left((1-\phi_n)\rho_R a_1\Omega_{R_{k*}D_2}\right)\right)}.\end{aligned} \tag{24}$$

Proof. See Appendix. □

5. Simulation Results

In this section, we present the numerical analysis of our SOP of D_i along with the corroboration of analytical results. The parameters of the system can be expressed in Table 2.

Figure 2 considers the SOP versus transmit SNR while varying K DF relays. Different values of SOP can be seen for the two destinations. For D_1 and D_2, the best SOP is achieved with $K = 2$. This shows that the addition of more relays is beneficial to SOP. Furthermore, we observe that the different values of SOP for D_2 converge to a single floor at high SNR values. This is due to the absence of SIC at D_2, therefore, the SOP is impacted in high SNR regions despite the number of relays. In addition, D_2 NOMA performs better than OMA in the range of SNR from 0 to 30 dB. And D_1 NOMA performs better than OMA in all SNR.

In Figure 3, we consider the SOP versus transmit SNR while varying ρ_E. Different values of SOP can be seen for the two destinations. For D_1 and D_2, the best SOP is achieved with $\rho_E = -5$(dB). This shows that increasing ρ_E impacts on SOP. Also, in Figure 3, the analytical and simulated results closely match. Looking closely at the results, we can see that the SOP of D_2 is impacted the most by larger ρ_E values. Furthermore, we observe that the SOP for D_2 approaches a floor at high SNR values for $\rho_E = 1$ (dB). As in Figure 2, this can be attributed to the lack of SIC at D_2.

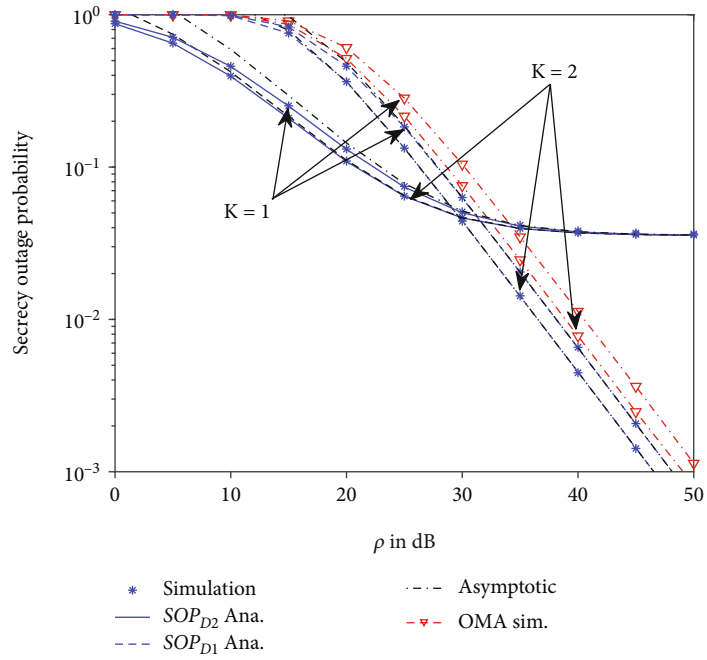

Figure 2: The SOP versus ρ in dB varying K with $\rho_E = 1$ (dB).

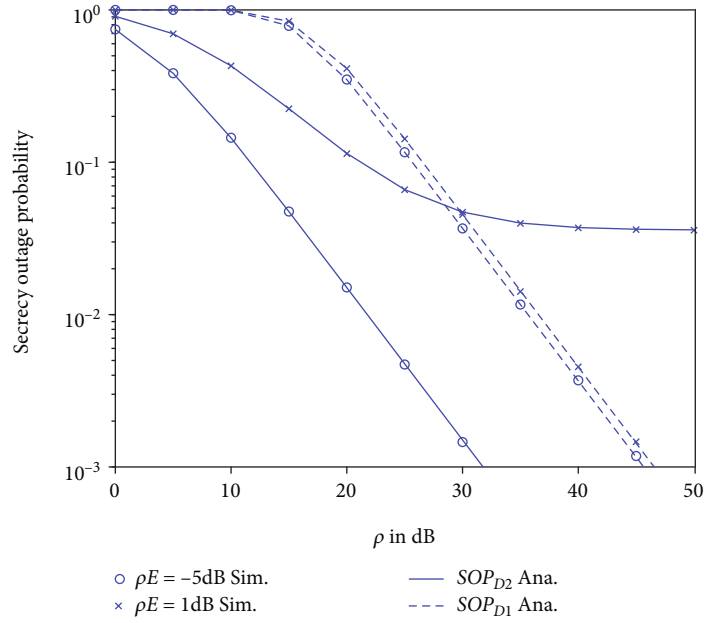

Figure 3: The SOP versus ρ in dB varying ρ_E.

In Figure 4, we consider the SOP versus transmit SNR while varying ρ_{CU}. Different values of SOP can be seen for the two destinations. For D_1 and D_2, the best SOP is achieved with $\rho_{CU} = -5$ (dB). In Figure 4, the analytical and simulated results closely match. Furthermore, we observe that the different SOP values for D_2 converge at a floor at high SNR values, this is due to the absence of SIC at the far user D_2. Hence, D_2 is impacted by the interference of the CUE, unlike D_1 which employs SIC. Figure 4, clearly shows the impact of SIC on SOP at the different NOMA devices.

In Figure 5, we consider the SOP versus a_2 varying ρ in dB with $\rho_E = 1$ (dB). Different values of SOP can be seen for the two destinations. For D_1 and D_2, the best SOP is achieved with an SNR of 30 dB. Furthermore, the analytical and simulated results closely match. Figure 5 clearly shows the impact of power allocation on SOP at the different NOMA devices.

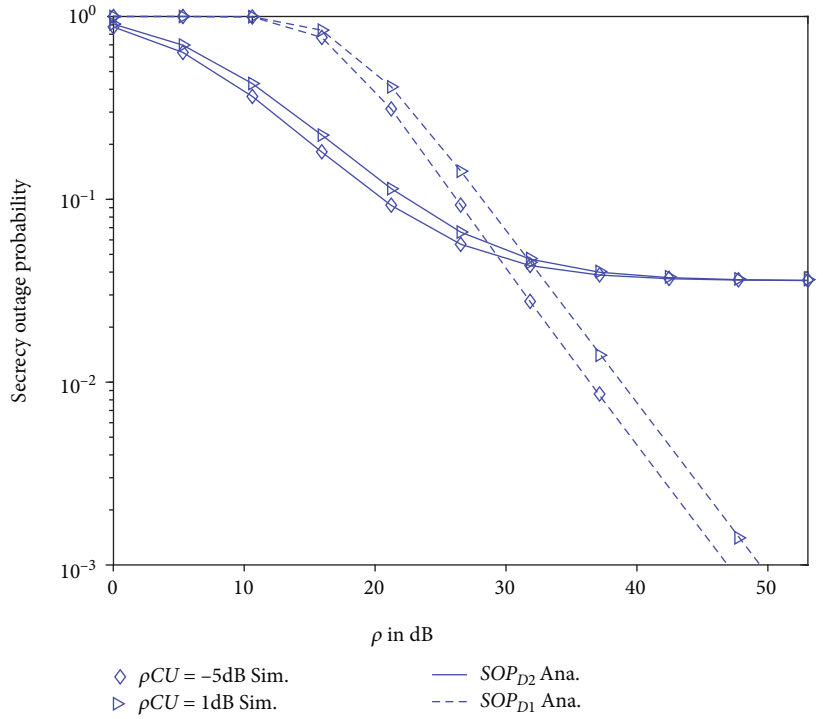

FIGURE 4: The SOP versus ρ in dB varying ρ_{CU} with $\rho_E = 1$ (dB).

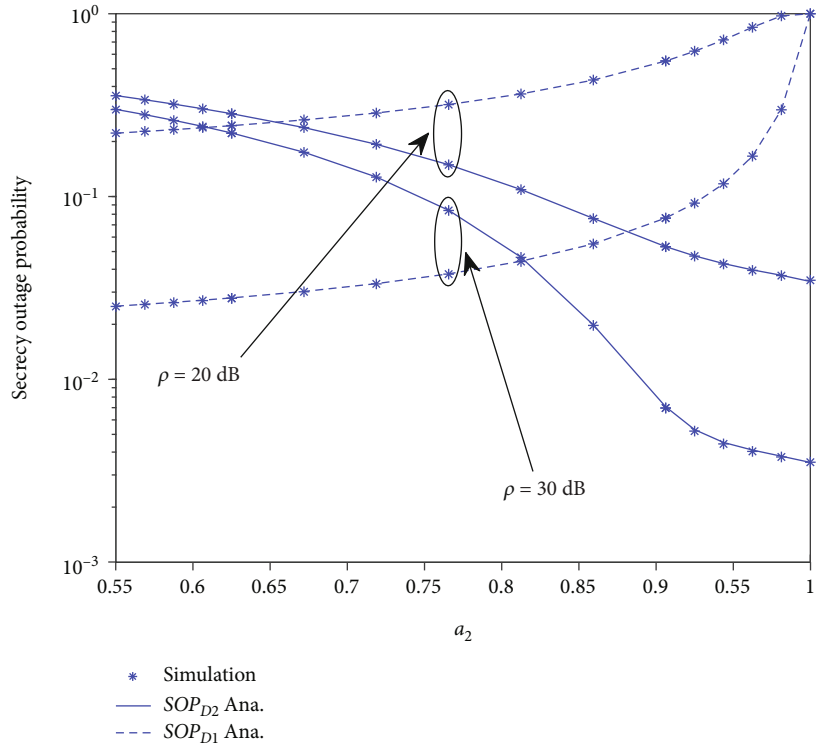

FIGURE 5: The SOP versus a_2 in dB varying ρ with $\rho_E = 1$ (dB).

In Figure 6, we consider the SPSC versus transmit SNR while varying K. Different values of SPSC can be observed depending on the value of K. The best SPSC curve is achieved with $K = 3$. In Figure 6, the analytical and simulated results closely match. Furthermore, we observe that the different SPSC values converge at a ceiling at high SNR

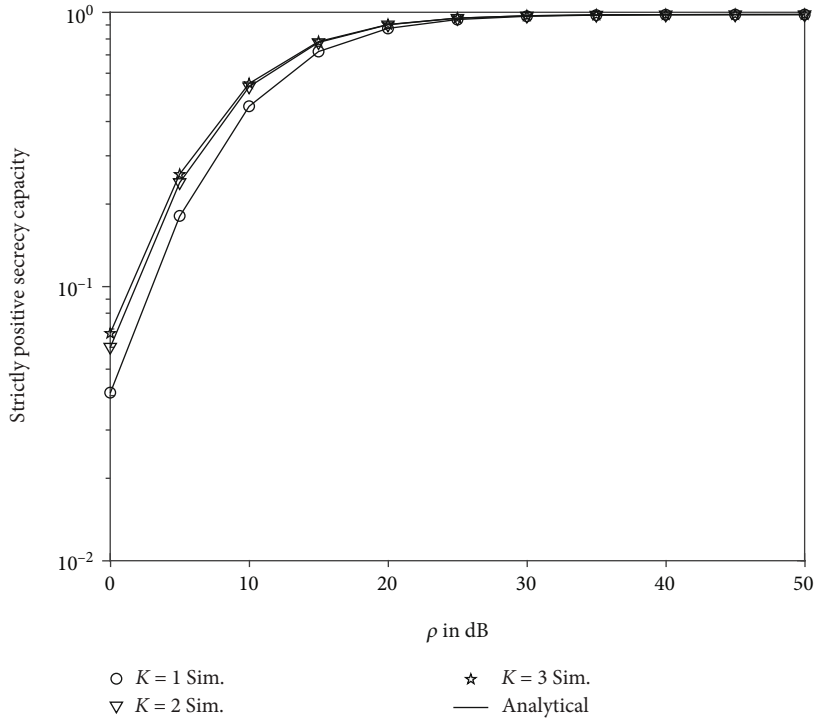

Figure 6: The SPSC versus ρ in dB varying K with $\rho_E = 1$ (dB).

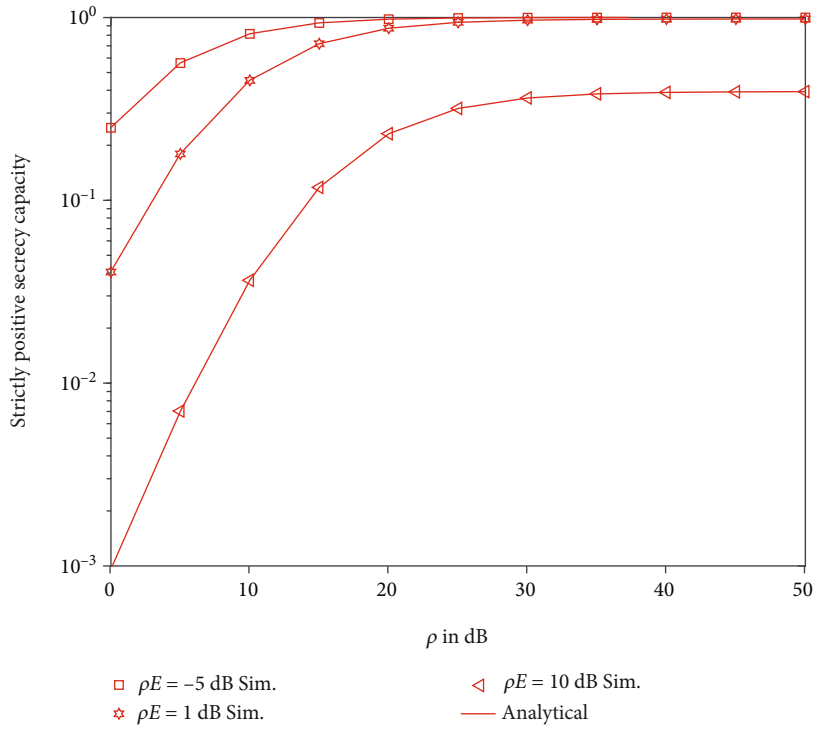

Figure 7: The SPSC versus ρ in dB varying ρ_E.

values. Demonstrating that at moderate to high SNR values, the number of relays has no significant impact on the SPSC of the proposed system.

In Figure 7, we consider the SPSC versus transmit SNR while varying ρ_E. Different values of SPSC can be observed depending on the value of ρ_E. In Figure 7, the analytical

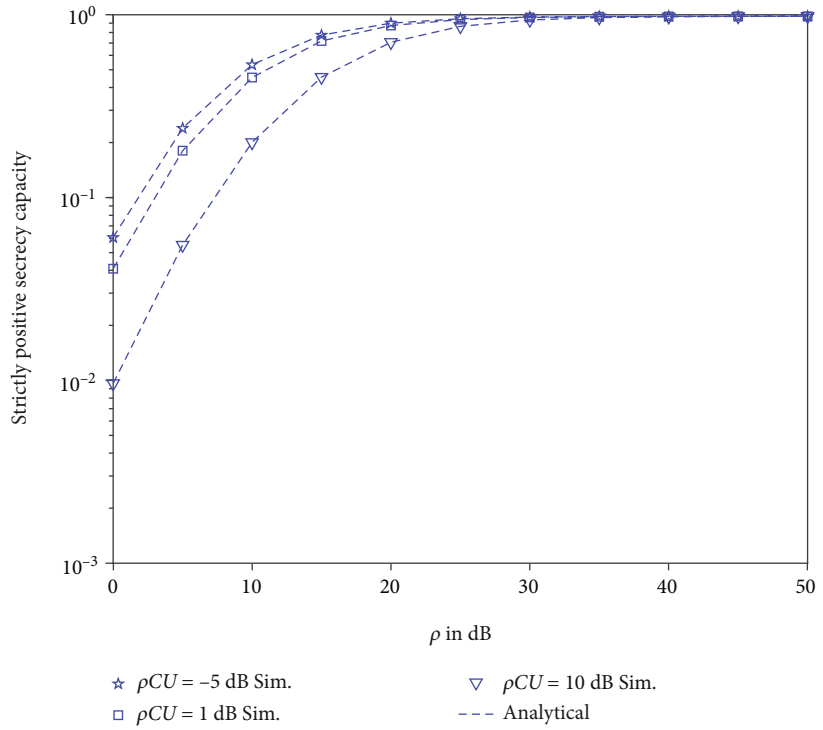

FIGURE 8: The SPSC versus ρ in dB varying ρ_{CU} with $\rho_E = 1$ (dB).

and simulated results closely match. Furthermore, we observe that the different SPSC values approach ceilings at high SNR values. Also, for Figure 7, it is clear that a tenfold increase in ρ_E significantly reduces the ceiling of SPSC of our system in the moderate to high SNR region. This is due to the increased signal strength at the eavesdropper affecting the proposed system.

In Figure 8, we consider the SPSC versus transmit SNR while varying ρ_{CU}. Different values of SPSC can be observed depending on the value of ρ_{CU}. In Figure 8, the analytical and simulated results closely match. Furthermore, we observe that the different SPSC values converge at a similar ceiling at high SNR values. For this figure, unlike in Figure 6, a tenfold increase in interference power ρ_{CU} does not significantly reduce the ceiling of the SPSC of our system. Demonstrating the reliability and security of our proposed system in the moderate to high SNR region in the presence of interference.

6. Conclusions

In this paper, the PLS problem of two destinations (NOMA users) has been studied in the context of downlink NOMA network under the presence of interference from traditional user CUE. Once an eavesdropper can overhear a signal in second hop transmission, SOP can be evaluated to verify the security of the dual-hop downlink transmission. By designing multiple relays, we can have a higher chance to improve SOP. We found that better SOP can be achieved by having more relays to forward signals. We derived the closed-form expressions SOP and lots of scenarios are presented in numerical simulation to confirm the impact of the studied parameters on secrecy performance. Simulation results are presented to examine the impact of the following parameters, i.e., transmit SNR at source, interference channel, the number of relays, and power allocation factors, on system performance. In future work, we may consider the secure performance of multiple NOMA users.

Appendix

A. Proof of Proposition 2

The SPSC can be expressed as

$$\mathrm{SPCP}_{\mathrm{out}} = \underbrace{\Pr\left(\min\left(\vartheta_{R_{k*}\longrightarrow x_1}, \vartheta_{D_1\longrightarrow x_1}\right) > \vartheta_{E\longrightarrow x_1}\right)}_{I_1} \underbrace{\Pr\left(\min\left(\vartheta_{R_{k*}\longrightarrow x_2}, \vartheta_{D_1\longrightarrow x_2}\right) > \vartheta_{E\longrightarrow x_2}\right)}_{I_2}. \quad (A.1)$$

Next, the first term of I_1 can be calculated by

$$\begin{aligned} I_1 &= \Pr\left(\min\left(\vartheta_{R_{k*}\longrightarrow x_1}, \vartheta_{D_1\longrightarrow x_1}\right) > \vartheta_{E\longrightarrow x_1}\right) \\ &= \Pr\left(\vartheta_{R_{k*}\longrightarrow x_1} > \vartheta_{E\longrightarrow x_1}, \vartheta_{D_1\longrightarrow x_1} > \vartheta_{E\longrightarrow x_1}\right) \\ &= \Pr\left(\left|g_{SR_{k*}}\right|^2 > \frac{\rho_E\left|g_{R_{k*}E}\right|^2}{\rho_S}, \left|g_{R_{k*}D_1}\right|^2 > \frac{\rho_E\left|g_{R_{k*}E}\right|^2\left(\rho_{CE}\left|g_{CU_1}\right|^2+1\right)}{\rho_R}\right). \end{aligned} \tag{A.2}$$

Then, it can be calculated as

$$\begin{aligned} I_1 &= \int_0^\infty\int_0^\infty f_{\left|g_{CU_1}\right|^2}(y) f_{\left|g_{R_{k*}E}\right|^2}(x) \\ &\quad\cdot\left(1-F_{\left|g_{SR_{k*}}\right|^2}\left(\frac{\rho_E x}{\rho_S}\right)\right)\left(1-F_{\left|g_{SR_{k*}}\right|^2}\left(\frac{\rho_E x(\rho_{CE}y+1)}{\rho_R}\right)\right)dxdy \\ &= \sum_{k=1}^{K}\binom{K}{k}\frac{(-1)^{k-1}}{\Omega_{CU_1}\Omega_{R_{k*}E}}\int_0^\infty\int_0^\infty e^{-\left(y/\left(\Omega_{CU_1}\right)\right)} \\ &\quad\cdot e^{-\left(\left((\rho_E kx)/\left(\Omega_{SR_{k*}}\rho_S\right)\right)+\left(1/\left(\Omega_{R_{k*}E}\right)\right)+\left((\rho_E(\rho_{CE}y+1))/\left(\Omega_{R_{k*}D_1}\rho_R\right)\right)\right)x}dxdy \\ &= \sum_{k=1}^{K}\binom{K}{k}\frac{(-1)^{k-1}\Omega_{R_{k*}D_1}\rho_R}{\rho_{CE}\rho_E\Omega_{CU_1}\Omega_{R_{k*}E}}\int_0^\infty\frac{e^{-\left(y/\left(\Omega_{CU_1}\right)\right)}}{\varpi_1+y}dy, \end{aligned} \tag{A.3}$$

where $\varpi_1 = ((\Omega_{R_{k*}D_1}\rho_R k)/(\Omega_{\mathrm{SR}_{k*}}\rho_{\mathrm{CE}}\rho_S)) + ((\Omega_{R_{k*}D_1}\rho_R)/(\Omega_{R_{k*}E}\rho_E\rho_{\mathrm{CE}})) + (1/(\rho_{\mathrm{CE}}))$. Similarly, we can obtain I_1 as

$$I_1 = -\sum_{k=1}^{K}\binom{K}{k}\frac{(-1)^{k-1}\Omega_{R_{k*}D_1}\rho_R}{\rho_{CE}\rho_E\Omega_{CU_1}\Omega_{R_{k*}E}}e^{\left(\varpi_1/\left(\Omega_{CU_1}\right)\right)}Ei\left(-\frac{\varpi_1}{\Omega_{CU_1}}\right). \tag{A.4}$$

In addition, the second term I_2 is given by

$$I_2 = \Pr\left(\min\left(\vartheta_{R_{k*}\longrightarrow x_2}, \vartheta_{D_2\longrightarrow x_2}\right) > \vartheta_{E\longrightarrow x_2}\right) = \Pr\left(\left|g_{SR_{k*}}\right|^2 > \frac{\rho_E\left|g_{R_{k*}E}\right|^2}{\rho_S-\rho_S\rho_E a_1\left|g_{R_{k*}E}\right|^2}, \left|g_{R_{k*}D_2}\right|^2 > \frac{\rho_E\left|g_{R_{k*}E}\right|^2\left(\rho_{CE}\left|g_{CU_1}\right|^2+1\right)}{\rho_R-\rho_R\rho_E a_1\left|g_{R_{k*}E}\right|^2}\right). \tag{A.5}$$

Similar in above, it can be rewritten by

$$\begin{aligned} I_2 &= \int_0^\infty\int_0^{(1/(\rho_E a_1))} f_{\left|g_{CU_2}\right|^2}(y) f_{\left|g_{R_{k*}E}\right|^2}(x) \\ &\quad\cdot\left(1-F_{\left|g_{SR_{k*}}\right|^2}\left(\frac{\rho_E x}{\rho_S-\rho_S\rho_E a_1 x}\right)\right) \\ &\quad\cdot\left(1-F_{\left|g_{R_{k*}D_2}\right|^2}\left(\frac{\rho_E x(\rho_{CE}y+1)}{\rho_R-\rho_R\rho_E a_1 x}\right)\right)dxdy. \\ &= \sum_{k_1=1}^{K}\binom{K}{k_1}\frac{(-1)^{k_1-1}}{\Omega_{CU_2}\Omega_{R_{k*}E}}\int_0^\infty\int_0^{(1/(\rho_E a_1))} e^{-\left(y/\left(\Omega_{CU_2}\right)\right)} \\ &\quad\cdot e^{-\left(x/\left(\Omega_{R_{k*}E}\right)\right)}e^{-\left((\rho_E k_1 x)/\left(\rho_S\Omega_{SR_{k*}}(1-\rho_E a_1 x)\right)\right)} \\ &\quad\cdot e^{-\left((\rho_E x(\rho_{CE}y+1))/\left(\rho_R\Omega_{R_{k*}D_2}(1-\rho_E a_1 x)\right)\right)}dxdy. \end{aligned} \tag{A.6}$$

Then, using Gaussian-Chebyshev Quad we can approximate I_2 as

$$\begin{aligned} I_2 &\approx \sum_{k_1=1}^{K}\binom{K}{k_1}\frac{(-1)^{k_1-1}}{2\rho_E a_1\Omega_{CU_2}\Omega_{R_{k*}E}}\frac{\pi}{N}\sum_{n=1}^{N}\sqrt{1-\phi_n^2}e^{-\varpi_2(1+\phi_n)} \\ &\quad\cdot\int_0^\infty e^{-\left(y/\left(\Omega_{CU_2}\right)\right)}e^{-\left(\left((1+\phi_n)\rho_{CE}y\right)/\left((1-\phi_n)\rho_R a_1\Omega_{R_{k*}D_2}\right)\right)}dy \\ &\approx \sum_{k_1=1}^{K}\binom{K}{k_1}\frac{(-1)^{k_1-1}}{2\rho_E a_1\Omega_{R_{k*}E}}\frac{\pi}{N}\sum_{n=1}^{N} \\ &\quad\cdot\frac{\sqrt{1-\phi_n^2}e^{-\varpi_2(1+\phi_n)}}{1+\left(\left((1+\phi_n)\rho_{CE}\Omega_{CU_2}\right)/\left((1-\phi_n)\rho_R a_1\Omega_{R_{k*}D_2}\right)\right)}, \end{aligned} \tag{A.7}$$

where $\varpi_2 = (1/(2\rho_E a_1\Omega_{R_{k*}E})) + (k_1/((1-\phi_n)\rho_S a_1\Omega_{SR_{k*}})) + (1/((1-\phi_n)\rho_R a_1\Omega_{R_{k*}D_2}))$. Putting (A.5) and (A.7) into (A.1), the proof is completed.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work has been supported by Van Lang University, Ho Chi Minh City, Vietnam, under the Project 1000.

References

[1] M. Coşandal, E. B. Koca, and H. Sari, "NOMA-2000 versus PD-NOMA: an outage probability comparison," *IEEE Communications Letters*, vol. 25, no. 2, pp. 427–431, 2021.

[2] B. Xu, Z. Xiang, P. Ren, and X. Guo, "Outage performance of downlink full-duplex network-coded cooperative NOMA," *IEEE Wireless Communications Letters*, vol. 10, no. 1, pp. 26–29, 2021.

[3] M.-S. Van Nguyen, S. Dinh-Thuan Do, S. Al-Rubaye, A. A.-D. Mumtaz, and O. Dobre, "Exploiting impacts of antenna selection and energy harvesting for massive network connectivity," *IEEE Transactions on Communications*, vol. 69, no. 11, pp. 7587–7602, 2021.

[4] D.-T. Do, A. Le, and B. M. Lee, "NOMA in cooperative underlay cognitive radio networks under imperfect SIC," *IEEE Access*, vol. 8, pp. 86180–86195, 2020.

[5] D.-T. Do, M. -S. V. Nguyen, F. Jameel, R. Jäntti, and I. S. Ansari, "Performance evaluation of relay-aided CR-NOMA for beyond 5G communications," *IEEE Access*, vol. 8, pp. 134838–134855, 2020.

[6] D.-T. Do, A.-T. Le, Y. Liu, and A. Jamalipour, "User grouping and energy harvesting in UAV-NOMA system with AF/DF relaying," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 11, pp. 11855–11868, 2021.

[7] F. Zhou, Y. Wu, Y.-C. Liang, Z. Li, Y. Wang, and K.-K. Wong, "State of the art, taxonomy, and open issues on cognitive radio networks with NOMA," *IEEE Wireless Communications*, vol. 25, no. 2, pp. 100–108, 2018.

[8] J. Choi, "Repetition-based NOMA transmission and its outage probability analysis," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5913–5922, 2020.

[9] V. Aswathi and A. V. Babu, "Full/half duplex cooperative NOMA under imperfect successive interference cancellation and channel state estimation errors," *IEEE Access*, vol. 7, pp. 179961–179984, 2019.

[10] N. Jaiswal and N. Purohit, "Performance of downlink NOMA-enabled vehicular communications over double Rayleigh fading channels," *IET Communications*, vol. 14, no. 20, pp. 3652–3660, 2020.

[11] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[12] Y. Liu, H. H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: theories, technologies, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 347–376, 2017.

[13] Y. Zou, X. Wang, and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," *IEEE Transactions on Communications*, vol. 61, no. 12, pp. 5103–5113, 2013.

[14] Y. Zou, X. Li, and Y. C. Liang, "Secrecy outage and diversity analysis of cognitive radio systems," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 11, pp. 2222–2236, 2014.

[15] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, and T. Q. Duong, "Relay selection for security enhancement in cognitive relay networks," *IEEE Wireless Communications Letters*, vol. 4, no. 1, pp. 46–49, 2015.

[16] A. Al-Nahari, G. Geraci, M. Al-Jamali, M. H. Ahmed, and N. Yang, "Beamforming with artificial noise for secure MISOME cognitive radio transmissions," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 1875–1889, 2018.

[17] C. Tang, G. Pan, and T. Li, "Secrecy outage analysis of underlay cognitive radio unit over Nakagami-*m* fading channels," *IEEE Wireless Communications Letters*, vol. 3, no. 6, pp. 609–612, 2014.

[18] H. Lei, C. Gao, I. S. Ansari et al., "Secrecy outage performance of transmit antenna selection for MIMO underlay cognitive radio systems over Nakagami-*m* channels," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2237–2250, 2017.

[19] R. Zhao, Y. Yuan, L. Fan, and Y. C. He, "Secrecy performance analysis of cognitive decode-and-forward relay networks in Nakagami- *m* fading channels," *IEEE Transactions on Communications*, vol. 65, no. 2, pp. 549–563, 2017.

[20] Z. Xiang, W. Yang, G. Pan, Y. Cai, and Y. Song, "Physical layer security in cognitive radio inspired NOMA network," *IEEE Journal of Selected Topics in Signal Processing*, vol. 13, no. 3, pp. 700–714, 2019.

[21] B. Zheng, M. Wen, C. X. Wang et al., "Secure NOMA based two-way relay networks using artificial noise and full duplex," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 7, pp. 1426–1440, 2018.

[22] L. Lv, Z. Ding, Q. Ni, and J. Chen, "Secure MISO-NOMA transmission with artificial noise," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 7, pp. 6700–6705, 2018.

[23] J. Chen, L. Yang, and M. S. Alouini, "Physical layer security for cooperative NOMA systems," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 4645–4649, 2018.

[24] B. He, A. Liu, N. Yang, and V. K. N. Lau, "On the design of secure non-orthogonal multiple access systems," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 10, pp. 2196–2206, 2017.

[25] Z. Ding, Z. Zhao, M. Peng, and H. V. Poor, "On the spectral efficiency and security enhancements of NOMA assisted multicast-unicast streaming," *IEEE Transactions on Communications*, vol. 65, no. 7, pp. 3151–3163, 2017.

[26] Y. Li, M. Jiang, Q. Zhang, Q. Li, and J. Qin, "Secure beamforming in downlink MISO nonorthogonal multiple access systems," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 8, pp. 7563–7567, 2017.

[27] X. Li, M. Zhao, M. Zeng et al., "Hardware impaired ambient backscatter NOMA systems: reliability and security," *IEEE Transactions on Communications*, vol. 69, no. 4, pp. 2723–2736, 2021.

[28] N. Zaghdoud, A. B. Mnaouer, H. Boujemaa, and F. Touati, "Secrecy performance of cooperative NOMA system with multiple full-duplex relays against non-colluding/colluding eavesdroppers," in *2020 IEEE 45th LCN Symposium on Emerging Topics in Networking (LCN Symposium)*, pp. 70–77, Sydney, Australia, 2020.

[29] X. Li, M. Zhao, X. C. Gao et al., "Physical layer security of cooperative NOMA for IoT networks under I/Q imbalance," *IEEE Access*, vol. 8, pp. 51189–51199, 2020.

[30] W. U. Khan, "Maximizing physical layer security in relay-assisted multicarrier nonorthogonal multiple access transmission," *Internet Technology Letters*, vol. 2, no. 2, 2019.

[31] M.-S. Van Nguyen and D.-T. Do, "Evaluating secrecy performance of cooperative NOMA networks under existence of relay link and direct link," *International Journal of Communication Systems*, vol. 33, no. 6, 2020.

[32] L. Lv, H. Jiang, Z. Ding, L. Yang, and J. Chen, "Secrecy-enhancing design for cooperative downlink and uplink NOMA with an untrusted relay," *IEEE Transactions on Communications*, vol. 68, no. 3, pp. 1698–1715, 2020.

[33] L. Lv, F. Zhou, J. Chen, and N. Al-Dhahir, "Secure cooperative communications with an untrusted relay: a NOMA-inspired jamming and relaying approach," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 12, pp. 3191–3205, 2019.

[34] H. Lei, Z. Yang, K. H. Park et al., "Secrecy outage analysis for cooperative NOMA systems with relay selection schemes," *IEEE Transactions on Communications*, vol. 67, no. 9, pp. 6282–6298, 2019.

[35] H. Lei, Z. Yang, K. Park, I. S. Ansari, G. Pan, and M. Alouini, "On physical layer security of multiple-relay assisted NOMA systems," in *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*, Shanghai, China, 2019.

[36] C. Yu, H. Ko, X. Peng, W. Xie, and P. Zhu, "Jammer-aided secure communications for cooperative NOMA systems," *IEEE Communications Letters*, vol. 23, no. 11, pp. 1935–1939, 2019.

[37] D. Wan, M. Wen, F. Ji, H. Yu, and F. Chen, "Non-orthogonal multiple access for cooperative communications: challenges, opportunities, and trends," *IEEE Wireless Communications*, vol. 25, no. 2, pp. 109–117, 2018.

[38] X. Chen, R. Jia, and D. W. K. Ng, "The application of relay to massive non-orthogonal multiple access," *IEEE Transactions on Communications*, vol. 66, no. 11, pp. 5168–5180, 2018.

[39] T. N. Nguyen, D. H. Tran, T. V. Chien et al., "Security-reliability trade-off analysis for SWIPT-and AF-based IoT networks with friendly jammers," 2022, http://arxiv.org/abs/2206.04428.

[40] V.-D. Phan, T. N. Nguyen, A. V. Le, and M. Voznak, "A study of physical layer security in SWIPT-based decode-and-forward relay networks with dynamic power splitting," *Sensors*, vol. 21, no. 17, p. 5692, 2021.

[41] T. N. Nguyen, D. H. Tran, V. D. Phan et al., "Throughput enhancement in FD- and SWIPT-enabled IoT networks over nonidentical Rayleigh fading channels," *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 10172–10186, 2022.

[42] T. N. Nguyen, T. T. Duy, P. T. Tran, M. Voznak, X. Li, and H. V. Poor, "Partial and full relay selection algorithms for AF multi-relay full-duplex networks with self-energy recycling in non-identically distributed fading channels," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 6, pp. 6173–6188, 2022.

[43] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 1656–1672, 2017.

[44] D.-T. Do and A.-T. Le, "NOMA based cognitive relaying: transceiver hardware impairments, relay selection policies and outage performance comparison," *Computer Communications*, vol. 146, pp. 144–154, 2019.

[45] I. Krikidis, J. Thompson, S. Mclaughlin, and N. Goertz, "Amplify-and-forward with partial relay selection," *IEEE Communications Letters*, vol. 12, no. 4, pp. 235–237, 2008.

[46] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, Academic Press, San Diego, CA, 2000.

[47] N. M. S. Do DT and T. A. Hoang, "Exploiting secure performance in power domain–based multiple access: impacts of relay link/direct link and secure analysis," *International Journal of Communication Systems*, vol. 32, no. 15, 2019.