

Article

# Secrecy Outage Probability of a NOMA Scheme and Impact Imperfect Channel State Information in Underlay Cooperative Cognitive Networks

Tan-Phuoc Huynh <sup>1,2</sup>, Duy-Hung Ha <sup>1</sup>, Cong Truong Thanh <sup>1</sup>, Peppino Fazio <sup>1</sup> and Miroslav Voznak <sup>1,\*</sup>

<sup>1</sup> Department of Telecommunications, VSB-Technical University of Ostrava, 17. listopadu 2172/15, 708 00 Ostrava, Czech Republic; htphuocsuna@gmail.com (T.-P.H.); duy.hung.ha.st@vsb.cz (D.-H.H.); cong.thanh.truong.st@vsb.cz (C.T.T.); peppino.fazio@vsb.cz (P.F.)

<sup>2</sup> Department of Computer Networks and Data Communications, Eastern International University (EIU), Nam Ky Khoi Nghia, Binh Duong 75000, Vietnam

\* Correspondence: miroslav.voznak@vsb.cz; Tel.: +420-603-565-965

Received: 29 December 2019; Accepted: 3 February 2020; Published: 7 February 2020

**Abstract:** Security performance and the impact of imperfect channel state information (CSI) in underlay cooperative cognitive networks (UCCN) is investigated in this paper. In the proposed scheme, relay R uses non-orthogonal multiple access (NOMA) technology to transfer messages  $e_1$ ,  $e_2$  from the source node S to User 1 ( $U_1$ ) and User 2 ( $U_2$ ), respectively. An eavesdropper (E) is also proposed to wiretap the messages of  $U_1$  and  $U_2$ . The transmission's security performance in the proposed system was analyzed and performed over Rayleigh fading channels. Through numerical analysis, the results showed that the proposed system's secrecy performance became more efficient when the eavesdropper node E was farther away from the source node S and the intermediate cooperative relay R. The secrecy performance of  $U_1$  was also compared to the secrecy performance of  $U_2$ . Finally, the simulation results matched the Monte Carlo simulations well.

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

## 1. Introduction

The UCCN is known as the CR which is a promising technology and innovative solution for dealing with the radio spectrum allocation and precise requirements issues [1]. CR permits secondary users (SUs or unlicensed users) to access the dormant frequency spectrum without causing interruption to the primary users (PUs or licensed user). Due to SUs being accepted to the PUs at the same time, the SUs have to keep their transmit powers within the acceptable levels. Besides that, with rapidly extending wireless sensor networks (WSNs) in many areas of industry, the security of information transfer becomes a more serious problem. Many researchers investigated PLS to help security transmission between the source node and the destination node to improve and enhance the secrecy of WSNs.

Recently, many solutions and technologies have been investigated for the purposes of speeding up mobile data transmission, extending wireless communication range, and assisting users in connecting security together. Examples of these technologies include amplify-and-forward (AF), orthogonal multiple access (OMA), and energy harvesting [2–4]. NOMA technology, however, is a promising method and has attracted significant attention in recent years [5–10].

NOMA technology has gradually become one of the most efficient solutions in developing the fifth-generation mobile network (5G). In the NOMA technique, the users can share both time and

frequency resources and only adjust their power allocation ratios. The users with better channel conditions can serve as relays to enhance the system performance by using SIC [9]. This technology improves the limitation of orthogonal multiple access (OMA). It meets the needs of end users in providing access to data quickly and securely. NOMA and PLS are therefore very important techniques in data transfer. They assist in transmitting signals from the source node to destination node with high speed, efficiency, and data confidentiality.

Several studies have examined NOMA and PLS in wireless systems [11–13]. In [11], the authors considered a cooperative relaying system using the NOMA technique to enhance the efficiency of the transmitted signal. The researchers in [13] investigated the effectiveness of new schemes that combined partial relay selection and NOMA in AF relaying systems to increase data transmission rates for 5G mobile networks.

A considerable amount of literature has been published on PLS [14–16]. In [14], the authors analyzed the secrecy performance of cooperative protocols with relay selection methods influenced by co-channel interference. The authors in [15] inspected the impact of correlated fading on the secrecy performance of multiple DF relaying that uses the optimal relay selection method. Some researchers have also combined the NOMA technique with PLS [17–19]. In [17], the authors resolved the problem of maximizing the minimum confidential information rate in users subject to the secrecy outage constraint and instantaneous transmit power constraint. Cooperative NOMA systems with PLS in both AF and DF were studied by the authors in [18].

The application of NOMA techniques and security principles in underlay cognitive radio networks were also suggested by some authors in [20–24]. In [20], the authors discussed a cooperative transmission scheme for a downlink NOMA in CR systems. This research exploited maximum spatial diversity. The researchers in [24] considered secure communication in cognitive DF relay networks in which a pair of cognitive relays were opportunistically selected for security protection against eavesdroppers.

Channel state information (CSI) has a vital role in wireless communication systems. It describes how a signal propagates from the source node to the relay, such as scattering, fading, and power decay over distance. During a receiver's set-up period, the CSI is evaluated and transferred to related nodes in the system through a media access control protocol. In [25], the authors researched the effect of imperfect channel CSI on secondary users in an underlay DF cognitive network with multiple primary receivers. In [26], scientists studied the effect of imperfect CSI on a DF cooperative underlay cognitive radio NOMA network in order to determine the optimal power allocation factors for different user distances.

In most of the literature reported above, the combination of NOMA and PLS in a UCCN influenced by CSI was not proposed. Motivated and inspired by the above ideas, a cooperative scheme is suggested in this paper. In this scheme, a proposed UCCN using NOMA is required to both decode and forward the messages  $e_1$  and  $e_2$  from node S to two destination nodes ( $U_1$  and  $U_2$ ) under the effect of CSI and an eavesdropper. The secrecy performance of the communications  $e_1$  and  $e_2$  in the proposed system were then examined and estimated in terms of secrecy outage probability over Rayleigh fading channels to improve spectral efficiency and secure communication.

The main contributions of the paper are summarized as follows:

- A study of the impact of imperfect CSI and the secrecy performance of a UCCN applying the NOMA technique to improve system performance in a 5G wireless network.
- Secrecy outage probability (SOP) is performed over Rayleigh fading channels and verified with Monte Carlo simulations.
- The results achieved by the proposed scheme demonstrate the security performance of  $U_1$  and  $U_2$ .
- The secrecy performance of the proposed system improved when the distance between the eavesdropper node E and the source and cooperative relay increased.

The paper has five sections. Section 1 introduces the topic. Section 2 describes the proposed scheme's system model. Section 3 presents the results of an analysis of the secrecy outage probability at the source nodes. Section 4 presents the simulation results. Section 5 summarizes the conclusions.

## 2. System Model

Figure 1 illustrates the influence of imperfect CSI in a UCCN using NOMA and PLS. The system model consists of the source nodes S transferring a superimposed signal  $e_1$  and  $e_2$  to  $U_1$  and  $U_2$ , respectively, through relay node R. One eavesdropper node E is proposed to wiretap the signals  $e_1$ ,  $e_2$  of the links S- $U_1$ , S- $U_2$ . In addition, the system model also consists of a node Pu which is known as the primary user having the license. Due to the interference constraint at the Pu node in the UCCN, the relay R and source S adjust their transmitting powers. In this model, we assume that the intermediate relay node R operates in DF relaying method and applies the NOMA principle under the influence of imperfect CSIs and PLS in UCCN. In addition, the variances of Zero-mean White Gaussian Noises (AWGNs) are equal, given as  $N_0$ . In this work, the corresponding distances of the links S-Pu, R-Pu, S-R, S-E, R-E, R-Pu, R- $U_1$ , and R- $U_2$  in Figure 1 are given as  $l_{SPu}, l_{RPu}, l_{SR}, l_{SE}, l_{RE}, l_{RPu}, l_1$ , and  $l_2$ .

Regarding the system channels,  $h_i$  represents the Rayleigh fading channel coefficient,  $i \in (h_{SR}, h_{SE}, h_{SPu}, h_{RE}, h_{RPu}, 1, 2)$ . We assume that the channels  $h_i$  do not change during block time T and are independently and identically distributed between two consecutive block times [10].

Finally, all of nodes in the system model have a single antenna for transmitting and receiving messages.

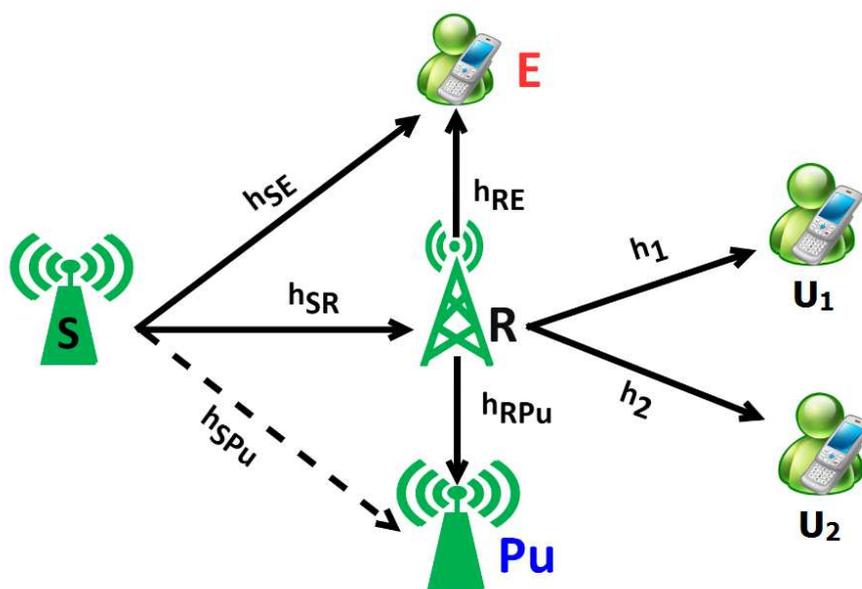


Figure 1. System model of NOMA and PLS under imperfect CSI in a UCCN.

In principle, there are two time slots involved in each system communication process, and are given as follows:

At the first time slot, the source node S transfers the information  $e_s$  to the relay R and the eavesdropper node E, which is given by the math expression as

$$e_s = \sqrt{\beta_1 P_s} e_1 + \sqrt{\beta_2 P_s} e_2, \quad (1)$$

where  $P_s$  is the power at source node S,  $e_1$ , and  $e_2$  are the messages of  $U_1$ ,  $U_2$ , respectively, with  $E\{|e_j|^2\} = 1$ ,  $j \in (1, 2)$ , ( $E\{e\}$  being notated for the expectation process of  $e$ ). The  $\beta_1$  and  $\beta_2$  are the power allocation coefficients. Following the principle of the NOMA, we assume that  $\beta_1 > \beta_2$  with  $\beta_1 + \beta_2 = 1$ .

Because of the estimation errors of channels  $h_i$ , the evaluated fading channel coefficients at the nodes are represented as follows [25]:

$$\hat{h}_i = \rho h_i + \sqrt{1 - \rho^2} \varepsilon_i, \quad (2)$$

where  $\hat{h}_i$ ,  $h_i$ , and  $\varepsilon_i$  are modeled as the additive white Gaussian noise (AWGN) with the random variable  $f_i = |\hat{h}_i|^2$ . The correlation coefficient  $\rho \in [0, 1]$  is described as the average quality of the channel estimation.

Notation: The Cumulative Distribution Function (CDF) and probability density function (pdf) of the random variable  $f_i$  is denoted respectively as  $F_{f_i}(x) = 1 - e^{-\frac{1}{\lambda_i}x}$  and  $f_{f_i}(x) = \frac{1}{\lambda_i}e^{-\frac{1}{\lambda_i}x}$ , where  $\lambda_i = l_i^{-\beta}$ , and  $\beta$  is a path-loss exponent.

The received signal at R from source node S for decode  $e_1$  under impact imperfect CSIs is given as follows:

$$y_{SR}^{e_1} = h_{SR}e_s + \sigma_R. \quad (3a)$$

Replace  $h_{SR}$  from formula (2), the signal  $y_{SR}^{e_1}$  is calculated as

$$\begin{aligned} y_{SR}^{e_1} &= \sqrt{\beta_1 P_s} e_1 \left( \frac{\hat{h}_{SR} - \sqrt{1 - \rho^2} \varepsilon_{SR}}{\rho} \right) + \sqrt{\beta_2 P_s} e_2 \left( \frac{\hat{h}_{SR} - \sqrt{1 - \rho^2} \varepsilon_{SR}}{\rho} \right) + n_R \\ &= \frac{\sqrt{\beta_1 P_s} e_1 \hat{h}_{SR}}{\rho} + \frac{\sqrt{\beta_2 P_s} e_2 \hat{h}_{SR}}{\rho} - \frac{\sqrt{\beta_1 P_s} e_1 \sqrt{1 - \rho^2} \varepsilon_{SR}}{\rho} - \frac{\sqrt{\beta_2 P_s} e_2 \sqrt{1 - \rho^2} \varepsilon_{SR}}{\rho} + n_R, \end{aligned} \quad (3b)$$

where  $n_R$  denotes the AWGNs at the relay R with the same variance  $N_0$ .

Because of applying NOMA technology, thanks to the deployment of SIC in NOMA principle, firstly, the relay R decodes the signal  $e_1$  from formula (3b) and removes it, then the signal  $e_2$  will be decoded without the component  $\frac{\sqrt{\beta_1 P_s} e_1 \hat{h}_{SR}}{\rho}$  in formula (3b). Therefore, the signal  $e_2$  received at R from source S after removing the signal  $e_1$  is expressed as follows:

$$y_{SR}^{e_2} = \frac{\sqrt{\beta_2 P_s} e_2 \hat{h}_{SR}}{\rho} - \frac{\sqrt{\beta_1 P_s} e_1 \sqrt{1 - \rho^2} \varepsilon_{SR}}{\rho} - \frac{\sqrt{\beta_2 P_s} e_2 \sqrt{1 - \rho^2} \varepsilon_{SR}}{\rho} + n_R. \quad (4)$$

Similarly, the node E also wiretaps the packets  $e_1$  and  $e_2$  from S, respectively, and the received signals at node E are obtained as follows:

$$y_{SE}^{e_1} = \frac{\sqrt{\beta_1 P_s} e_1 \hat{h}_{SE}}{\rho} + \frac{\sqrt{\beta_2 P_s} e_2 \hat{h}_{SE}}{\rho} - \frac{\sqrt{\beta_1 P_s} e_1 \sqrt{1 - \rho^2} \varepsilon_{SE}}{\rho} - \frac{\sqrt{\beta_2 P_s} e_2 \sqrt{1 - \rho^2} \varepsilon_{SE}}{\rho} + n_E \quad (5)$$

$$y_{SE}^{e_2} = \frac{\sqrt{\beta_2 P_s} e_2 \hat{h}_{SE}}{\rho} - \frac{\sqrt{\beta_1 P_s} e_1 \sqrt{1 - \rho^2} \varepsilon_{SE}}{\rho} - \frac{\sqrt{\beta_2 P_s} e_2 \sqrt{1 - \rho^2} \varepsilon_{SE}}{\rho} + n_E, \quad (6)$$

where  $n_E$  denotes the AWGNs at the E with the same variance  $N_0$ .

In the second time slot, after the received signals, the relay R sends them to the source nodes  $U_1$  and  $U_2$ . Hence, the received signals at the destination node  $U_1$ ,  $U_2$  are given respectively as

$$y_{RU_1}^{e_1} = \frac{\sqrt{\beta_1 P_R} e_1 \hat{h}_1}{\rho} + \frac{\sqrt{\beta_2 P_R} e_2 \hat{h}_1}{\rho} - \frac{\sqrt{\beta_1 P_R} e_1 \sqrt{1 - \rho^2} \varepsilon_1}{\rho} - \frac{\sqrt{\beta_2 P_R} e_2 \sqrt{1 - \rho^2} \varepsilon_1}{\rho} + n_{U_1} \quad (7)$$

$$y_{RU_2}^{e_2} = \frac{\sqrt{\beta_2 P_R} e_2 \hat{h}_2}{\rho} - \frac{\sqrt{\beta_1 P_R} e_1 \sqrt{1 - \rho^2} \varepsilon_2}{\rho} - \frac{\sqrt{\beta_2 P_R} e_2 \sqrt{1 - \rho^2} \varepsilon_2}{\rho} + n_{U_2}, \quad (8)$$

where  $n_{U_1}$ ,  $n_{U_2}$  denote the AWGNs at the destination  $U_1$ ,  $U_2$  with the same variance  $N_0$ , and  $P_R$  is a transmit power of the relay R.

In the proposed scheme, under the interference constraint at the node  $P_u$ , the source node S and relay node R have to adjust their transmitting powers so that the interference power at the  $P_u$  must be less than a threshold value, which is assumed as  $I_{th}$ . The maximum powers of nodes S and R are given, respectively,

$$P_S = \frac{I_{th}}{|\widehat{h_{SR}}|^2} = \frac{I_{th}}{f_{SR}}. \quad (9a)$$

$$P_R = \frac{I_{th}}{|\widehat{h_{RPu}}|^2} = \frac{I_{th}}{f_{RPu}}. \quad (9b)$$

Because the node E connects to the relay R directly, so it wiretaps the packets  $e_1$  and  $e_2$  from relay R. Therefore, the received signals at E through the link R-E are expressed as

$$y_{RE}^{e_1} = \frac{\sqrt{\beta_1 P_R} e_1 \widehat{h_{RE}}}{\rho} + \frac{\sqrt{\beta_2 P_R} e_2 \widehat{h_{RE}}}{\rho} - \frac{\sqrt{\beta_1 P_R} e_1 \sqrt{1-\rho^2} \varepsilon_{RE}}{\rho} - \frac{\sqrt{\beta_2 P_R} e_2 \sqrt{1-\rho^2} \varepsilon_{RE}}{\rho} + n_E. \quad (10)$$

$$y_{RE}^{e_2} = \frac{\sqrt{\beta_2 P_R} e_2 \widehat{h_{RE}}}{\rho} - \frac{\sqrt{\beta_1 P_R} e_1 \sqrt{1-\rho^2} \varepsilon_{RE}}{\rho} - \frac{\sqrt{\beta_2 P_R} e_2 \sqrt{1-\rho^2} \varepsilon_{RE}}{\rho} + n_E. \quad (11)$$

We define the received Signal-to-Interference and Noise Ratios (SINRs) as  $\gamma = E\{|\text{signal}|^2\} / E\{|\text{overall noise}|^2\}$ .

Firstly, we calculate the received Signal-to-Interference and Noise Ratios (SINRs) for decoding the information signal  $e_1$ .

Thus, from formula (3b), the SINR at the relay R with the link S-R is obtained as follows:

$$\begin{aligned} \gamma_{SR}^{e_1} &= \frac{\frac{\beta_1 P_S |\widehat{h_{SR}}|^2}{\rho^2}}{\frac{\beta_2 P_S |\widehat{h_{SR}}|^2}{\rho^2} + \frac{\beta_1 P_S (1-\rho^2) \lambda_{SR}}{\rho^2} + \frac{\beta_2 P_S (1-\rho^2) \lambda_{SR}}{\rho^2} + N_0} \\ &= \frac{\beta_1 P_S f_{SR}}{\beta_2 P_S f_{SR} + P_S (1-\rho^2) \lambda_{SR} (\beta_1 + \beta_2) + \rho^2 N_0}. \end{aligned} \quad (12a)$$

Replacing  $P_S = \frac{I_{th}}{f_{SR}}$  in (9a), and setting  $P = \frac{I_{th}}{N_0}$ ,  $\gamma_{SR}^{e_1}$  is rewritten as

$$\gamma_{SR}^{e_1} = \frac{P \beta_1 f_{SR}}{P \beta_2 f_{SR} + P (1-\rho^2) \lambda_{SR} + \rho^2 f_{SPu}}. \quad (12b)$$

Similarly, with the formula in (7), we also calculate  $\gamma_{RU_1}^{e_1}$ , and this is achieved by mathematical expression as

$$\gamma_{RU_1}^{e_1} = \frac{P \beta_1 f_1}{P \beta_2 f_1 + P (1-\rho^2) \lambda_1 + \rho^2 f_{RPu}}. \quad (13)$$

where  $P = \frac{I_{th}}{N_0}$ .

Applying formulas (5) and (10), the received SINRs at the eavesdropper node E with the link S-E and R-E are given, respectively, as follows:

$$\begin{aligned} \gamma_{SE}^{e_1} &= \frac{\beta_1 P_S f_{SE}}{\beta_2 P_S f_{SE} + P_S (1-\rho^2) \lambda_{SE} + \rho^2 N_0} \\ &= \frac{P \beta_1 f_{SE}}{P \beta_2 f_{SE} + P (1-\rho^2) \lambda_{SE} + \rho^2 f_{SPu}}. \end{aligned} \quad (14)$$

$$\gamma_{RE}^{e_1} = \frac{P \beta_1 f_{RE}}{P \beta_2 f_{RE} + P (1-\rho^2) \lambda_{RE} + \rho^2 f_{RPu}}. \quad (15)$$

In the second, similar to decoding the information signal  $e_1$ , we find the received SINRs for decoding the information signal  $e_2$  as follows.

We apply formulas (4) and (6), the received SINRs at the nodes R with the link S-R, and at the eavesdropper node E with the link S-E are expressed, respectively, as follows:

$$\gamma_{SR}^{e_2} = \frac{\beta_2 P_s f_{SR}}{\beta_1 P_s (1 - \rho^2) \lambda_{SR} + \beta_2 P_s (1 - \rho^2) \lambda_{SR} + \rho^2 N_0} = \frac{P \beta_2 f_{SR}}{P (1 - \rho^2) \lambda_{SR} + \rho^2 f_{SPu}}. \quad (16)$$

$$\gamma_{SE}^{e_2} = \frac{\beta_2 P_s f_{SE}}{P_s (1 - \rho^2) \lambda_{SE} + \rho^2 N_0} = \frac{P \beta_2 f_{SE}}{P (1 - \rho^2) \lambda_{SE} + \rho^2 f_{SPu}}. \quad (17)$$

Similarly, with formulas (8) and (12), the received SINRs at the nodes  $U_2$  and E from relay R are inferred, respectively, as follows:

$$\gamma_{RU_2}^{e_2} = \frac{P \beta_2 f_2}{P (1 - \rho^2) \lambda_2 + \rho^2 f_{RPu}}. \quad (18)$$

$$\gamma_{RE}^{e_2} = \frac{P \beta_2 f_{RE}}{P (1 - \rho^2) \lambda_{RE} + \rho^2 f_{RPu}}. \quad (19)$$

Applying the Shannon capacity formula, the achievable rates of the links  $X$ - $Y$  are formulated as

$$R_{XY}^{e_j} = \frac{1}{2} \log_2(1 + \gamma_{XY}^{e_j}). \quad (20)$$

where the ratio  $1/2$  represents the fact that data transmission is split into two time slots,  $X \in \{S, R\}$ , and  $Y \in \{E, U_1, U_2\}$ . The secrecy capacity of the UCCN systems with DF-based NOMA for the S- $U_j$  communication can be expressed as

$$SC_j = [SC_{U_j}^{e_j} - SC_E^{e_j}]^+, \quad (21)$$

where  $[x]^+ = \max(0, x)$ ;  $SC_{SR}^{e_i}$  and  $SC_{RU_j}^{e_j}$  are the secrecy capacities from the source node S to the relay R and from the relay R to the destination  $U_i$  are given, respectively, as

$$SC_{SR}^{e_j} = \max(0, R_{SR}^{e_j} - R_{SE}^{e_j}). \quad (22)$$

$$SC_{RU_i}^{e_j} = \max(0, R_{RU_i}^{e_j} - R_{RE}^{e_j}). \quad (23)$$

### 3. Secrecy Outage Probability Analysis

In this section, the secrecy outage probability for eavesdropping the signals of  $U_1$  and  $U_2$  in the proposed scheme are analyzed. We assume that a node successfully and safely decodes the received packet if its achievable secrecy capacity is larger than a threshold secrecy capacity  $SC_{th}$ .

#### 3.1. Secrecy Outage Probability of $U_1$ .

The secrecy outage probability of  $U_1$  occurring when  $U_1$  does not receive a signal safely from the source node S under the malicious attempt of the eavesdropper E is expressed as follows:

$$\begin{aligned} OP_{U_1} &= \Pr[\min(SC_{SR}^{e_1}, SC_{RU_1}^{e_1}) < SC_{th}] \\ &= 1 - \Pr[SC_{SR}^{e_1} \geq SC_{th}, SC_{RU_1}^{e_1} \geq SC_{th}]. \end{aligned} \quad (24)$$

Replacing  $SC_{SR}^{e_1} = \max(0, R_{SR}^{e_1} - R_{SE}^{e_1})$  at formula (22) and  $SC_{RU_1}^{e_1} = \max(0, R_{RU_1}^{e_1} - R_{RE}^{e_1})$  at (23) in formula (24), the  $OP_{U_1}$  is rewritten as follows:

$$OP_{U_1} = 1 - \underbrace{\Pr [R_{SR}^{e_1} - R_{SE}^{e_1} \geq SC_{th}]}_{Pr\ 1.1} \times \underbrace{\Pr [R_{RU_1}^{e_1} - R_{RE}^{e_1} \geq SC_{th}]}_{Pr\ 1.2} \tag{25}$$

**Proposition 1.** The probability of the Pr1.1, and Pr1.2 in (25) is given as

$$Pr\ 1.1 = \begin{cases} 0 & a \leq \theta b \\ \left( \frac{(1/\lambda_{SPu})e^{-\psi_{11}/\lambda_{SR}}}{(1/\lambda_{SPu})+(\psi_2/\lambda_{SR})} - (1/\lambda_{SR}\lambda_{SPu}) I_1 \right) & a > \theta b. \end{cases} \tag{26}$$

where

$$\begin{aligned} \psi_{11} &= \frac{\phi c \lambda_{SE}}{(a - \phi b)}; \psi_2 = \frac{\phi \rho^2}{(a - \phi b)} \\ I_1 &= \int_0^\infty \int_{(\psi_{11} + \psi_2 x)}^\infty e^{-\left(\frac{1}{\lambda_{SPu}}x + \frac{1}{\lambda_{SR}}y\right)} e^{-\frac{1}{\lambda_{SE}}\zeta_1} dx dy, \\ \zeta_1 &= \frac{(c\lambda_{SE} + \rho^2 x) (ay - \phi (by + c\lambda_{SR} + \rho^2 x))}{[\phi b + (\phi + 1)a] [by + c\lambda_{SR} + \rho^2 x] - aby}, \end{aligned}$$

Proof: See Appendix A.

$$Pr\ 1.2 = \begin{cases} 0 & a \leq \theta b \\ \frac{(1/\lambda_{RPu})e^{-\psi_{12}/\lambda_1}}{(1/\lambda_{RPu})+\psi_2/\lambda_1} - (1/\lambda_1\lambda_{RPu}) I_2 & a > \theta b \end{cases} \tag{27}$$

where

$$\begin{aligned} \psi_{12} &= \frac{\phi c \lambda_1}{(a - \phi b)}; \psi_2 = \frac{\phi \rho^2}{(a - \phi b)} \\ I_2 &= \int_0^\infty \int_{(\psi_{12} + \psi_2 x)}^\infty e^{-\left(\frac{1}{\lambda_{RPu}}x + \frac{1}{\lambda_1}y\right)} e^{-\frac{1}{\lambda_{RE}}\zeta_2} dx dy, \\ \zeta_2 &= \frac{(c\lambda_{RE} + \rho^2 x) (ay - \phi (by + c\lambda_1 + \rho^2 x))}{[\phi b + (\phi + 1)a] [by + c\lambda_1 + \rho^2 x] - aby}, \end{aligned}$$

Proof: See Appendix B.

From formulas in (26) and (27), the secrecy outage probability of the  $U_1$  is obtained as

$$OP_{U_1} = \begin{cases} 1 & a \leq \phi b \\ 1 - \left( \left( \frac{(1/\lambda_{SPu})e^{-\psi_{11}/\lambda_{SR}}}{(1/\lambda_{SPu})+(\psi_2/\lambda_{SR})} - (1/\lambda_{SR}\lambda_{SPu}) \times I_1 \right) \times \left( \frac{1/\lambda_{RPu}e^{-\psi_{12}/\lambda_1}}{1/\lambda_{RPu}+\psi_2/\lambda_1} - (1/\lambda_1\lambda_{RPu}) \times I_2 \right) \right) & a > \phi b \end{cases} \tag{28}$$

### 3.2. Secrecy Outage Probability of $U_2$

Similar to  $U_1$ , the SOP of  $U_2$  can be expressed as

$$OP_{U_2} = \Pr \left[ \min \left( SC_{SR}^{e_2}, SC_{RU_2}^{e_2} \right) < SC_{th} \right] = 1 - \Pr \left[ SC_{SR}^{e_2} \geq SC_{th}, SC_{RU_2}^{e_2} \geq SC_{th} \right]. \quad (29)$$

**Proposition 2.** The secrecy outage probability of  $U_2$  in (26) is given as

$$OP_{U_2} = 1 - \left( 1 - \frac{1}{\lambda_{SPu} \lambda_{SE}} \times I_3 \right) \times \left( 1 - \frac{1}{\lambda_{RPu} \lambda_{RE}} I_4 \right) \quad (30)$$

where

$$\zeta_3 = \left( \frac{\phi(c\lambda_{SR} + \rho^2 x)}{b} + (\phi + 1) \frac{(c\lambda_{SR} + \rho^2 x)}{(c\lambda_{SE} + \rho^2 x)} y \right),$$

$$\zeta_4 = \left( \frac{\phi(c\lambda_2 + \rho^2 x)}{b} + (\phi + 1) \frac{(c\lambda_2 + \rho^2 x)}{(c\lambda_{RE} + \rho^2 x)} y \right),$$

$$I_3 = \int_0^\infty \int_0^\infty \left[ e^{-\left( \frac{1}{\lambda_{SPu}} x + \frac{1}{\lambda_{SE}} y \right)} \times \left( 1 - e^{-\frac{\zeta_3}{\lambda_{SR}}} \right) \right] dx dy,$$

$$I_4 = \int_0^\infty \int_0^\infty \left[ e^{-\left( \frac{1}{\lambda_{RPu}} x + \frac{1}{\lambda_{RE}} y \right)} \times \left( 1 - e^{-\frac{\zeta_4}{\lambda_2}} \right) \right] dx dy.$$

Proof: See Appendix C.

The integrals  $I_1$  and  $I_2$  in (28) and  $I_3$  and  $I_4$  in (30) are complex integrals and are difficult to resolve practically. In this paper, however, the value of  $I_1, I_2, I_3$  and  $I_4$  can be found using numerical methods.

## 4. Simulation Results

In this section, the secrecy performance of a NOMA scheme and the impact of imperfect CSI in a UCCN were examined, analyzed, and evaluated. The theoretical results of the analyses were verified with Monte Carlo simulations. The coordinates of S, R,  $U_1$ ,  $U_2$ , Pu, and E were set to  $S(0,0), R(x_R,0), U_1(x_{U_1},y_{U_1}) = (1,0), U_2(x_{U_2},y_{U_2}) = (0.75,-0.5), Pu(x_{Pu},y_{Pu}), E(x_E,y_E)$ , respectively, in the two-dimensional plane and satisfying ( $x_i > 0$ ). Hence,  $l_{SR} = x_R, l_{RU_1} = x_{U_1} - x_R, l_{RU_2} = \sqrt{y_{U_2}^2 + (x_{U_2} - x_R)^2}, l_{RPu} = \sqrt{y_{Pu}^2 + (x_{Pu} - x_R)^2}, l_{RE} = \sqrt{y_E^2 + (x_E - x_R)^2}, l_{SE} = \sqrt{y_E^2 + x_E^2}$ , and  $l_{SPu} = \sqrt{x_{Pu}^2 + y_{Pu}^2}$ . We assume that the target secrecy capacity  $SC_{th} = 0.5$  (bit/s/Hz) and the exponent  $\beta$  is set to a constant  $\beta = 3$ .

Figures 2 and 3 graph the SOP of the two Users  $U_1$  and  $U_2$  via SNR (dB) with  $SC_{th} = 0.5$  (bit/s/Hz). The relay R, Pu,  $U_1$ ,  $U_2$ , and eavesdropper E are located in positions  $R(x_R,0) = (0.5,0), Pu(x_{Pu},y_{Pu}) = (0.5,-1), U_1(x_{U_1},y_{U_1}) = (1,0), U_2(x_{U_2},y_{U_2}) = (0.75,-0.5), E(x_E,y_E) = (0.5,1)$ , respectively. From the results in Figure 2, we can see the effect of the eavesdropping node E to the SOP when SNR is changed from 0 dB to 20 dB. With  $\rho = 0.95$ , the SOP values of User  $U_1$  are greater than User  $U_2$  when SNR < 2.5 dB. Nevertheless, when the SNR increases from 2.5 dB to 30 dB, the SOP of User  $U_2$  is better than User  $U_1$ , and both also increase when the SNR increases as a result of large transmitting power. Besides that, it is noted that imperfect CSI degrades the SOP of the signal.

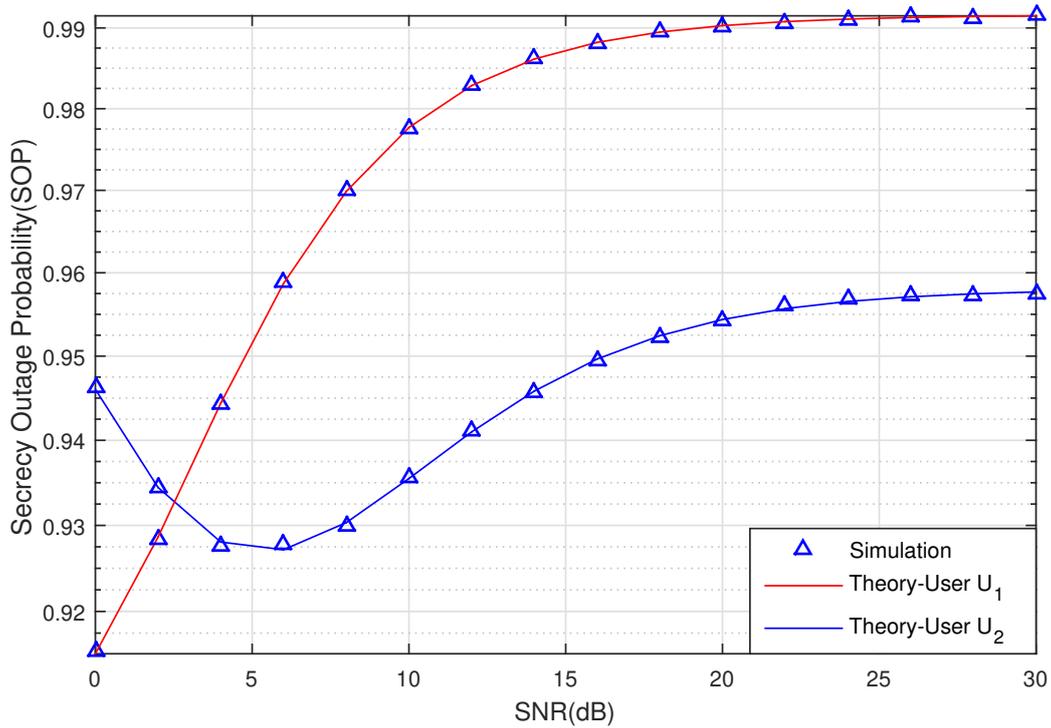


Figure 2. The SOP of  $U_1$  and  $U_2$  versus SNR (dB).

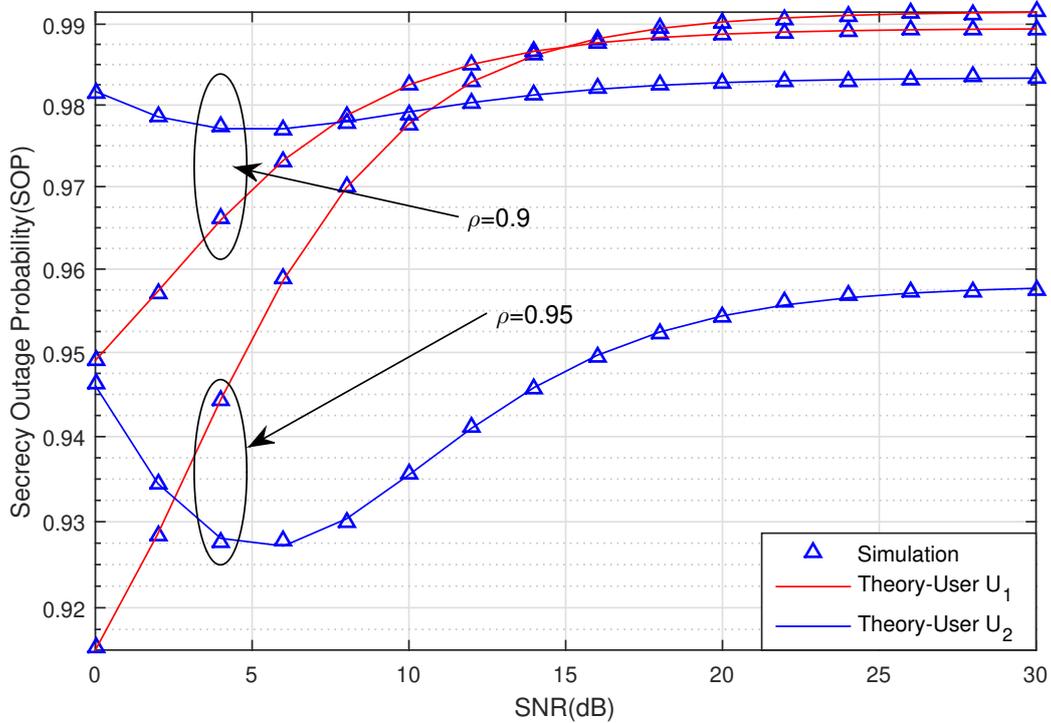


Figure 3. The SOP of  $U_1$  and  $U_2$  versus SNR (dB) when  $\rho = 0.9$  and  $\rho = 0.95$ .

In Figure 3, we observe the obvious affection of the channel estimation coefficient  $\rho$  to the SOP. The SOP of the two users in case  $\rho = 0.95$  outperforms the SOP in case  $\rho = 0.9$ . It means that the system has been impacted by imperfect CSI. We also can see that the secrecy performance of the two

Users also decreases when the SNR increases. The security system will be better and it is difficult for the eavesdropper to wiretap the signal. These theoretical results match the simulation results of the proposed system well. Hence, the derived equations are sufficiently accurate for use in analysis.

Figure 4 graphs the SOP of the two Users  $U_1$  and  $U_2$  via  $\rho$  when SNR=10 (dB) with  $SC_{th} = 0.5$  (bit/s/Hz). The relay R, Pu,  $U_1$ ,  $U_2$ , and eavesdropper E are located in positions  $R(x_R, 0) = (0.5, 0)$ ,  $Pu(x_{Pu}, y_{Pu}) = (0.5, -1)$ ,  $U_1(x_{U_1}, y_{U_1}) = (1, 0)$ ,  $U_2(x_{U_2}, y_{U_2}) = (0.75, -0.5)$ ,  $E(x_E, y_E) = (0.5, 1)$ , respectively. As observed in Figure 4, the secrecy performance of  $U_1$  is better than  $U_2$  when  $\rho < 0.9$ . However, when the correlation coefficient  $\rho > 0.9$ , the SOP of  $U_2$  is less than  $U_1$ . This means that the effects of the evaluation errors decrease when the correlation coefficients  $\rho$  increase. In addition, the secrecy performance of two Users is more efficient when the channel estimation coefficient  $\rho$  is higher.

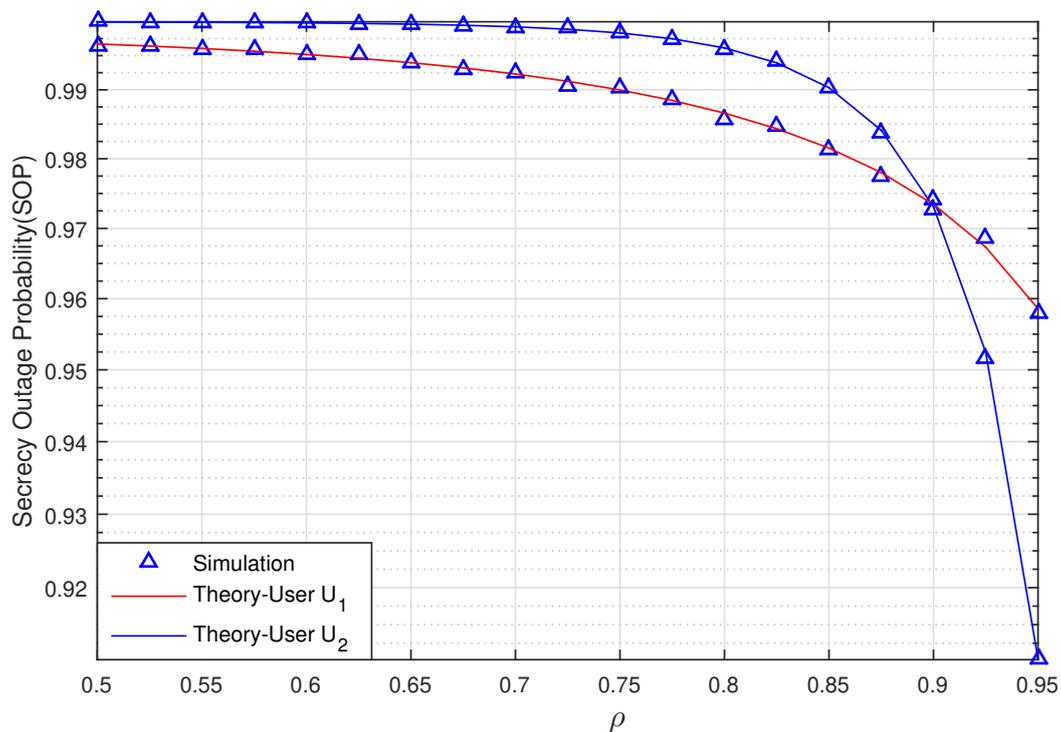


Figure 4. The SOP of  $U_1$  and  $U_2$  via  $\rho$  when SNR = 10 (dB).

Figure 5 graphs the SOP of the proposed scheme versus the position of the of eavesdropper E on the  $y$ -axis when the coordinate value  $y_E$  changes from 0.2 to 2 when SNR = 10 (dB), (bit/s/Hz),  $R(x_R, 0) = (0.5, 0)$ ,  $Pu(x_{Pu}, y_{Pu}) = (0.5, -1)$ ,  $U_1(x_{U_1}, y_{U_1}) = (1, 0)$ ,  $U_2(x_{U_2}, y_{U_2}) = (0.75, -0.5)$ . Figure 5 shows that the SOP of  $U_1$  and  $U_2$  decrease when  $y_E$  increases. This means that the secrecy transmission of the two Users will be intact when eavesdropper E moves farther away from source S and relay R.

We can also see that the secrecy performance of  $U_2$  is better than  $U_1$  as a result of the proposed scheme applying NOMA and using SIC to detect the signal under the effect of imperfect CSI on the system.

Figure 6 graphs the SOP of User  $U_1$  and  $U_2$  versus the power allocation coefficients  $\beta_1$  (changing from 0.6 to 0.95) when SNR = 10 (dB),  $SC_{th} = 0.5$  (bit/s/Hz),  $R(x_R, 0) = (0.5, 0)$ ,  $Pu(x_{Pu}, y_{Pu}) = (0.5, -1)$ ,  $U_1(x_{U_1}, y_{U_1}) = (1, 0)$ ,  $U_2(x_{U_2}, y_{U_2}) = (0.75, -0.5)$ ,  $E(x_E, y_E) = (0.5, 1)$ . This figure shows the impact of a varying  $\beta_1$  on the system. When  $\beta_1$  increases from 0.6 to 0.85, the SOP of  $U_2$  outperforms the SOP of  $U_1$ . The secrecy transmission of  $U_1$  is then better than  $U_2$  when  $\beta_1 > 0.85$ . We can thus observe the impact of  $\beta_1$  on the security performance of a UCCN system with a NOMA solution under the effect of imperfect CSI.

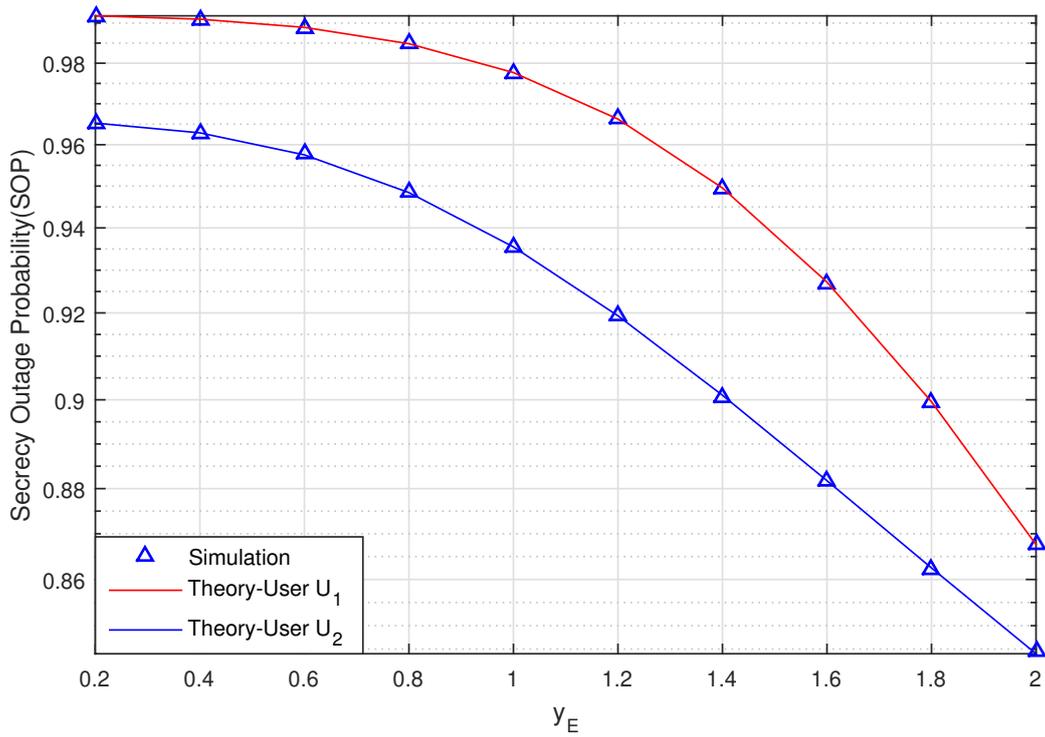


Figure 5. The SOP of  $U_1$  and  $U_2$  versus coordinate  $y_E$  of eavesdropper E when SNR = 10 (dB).

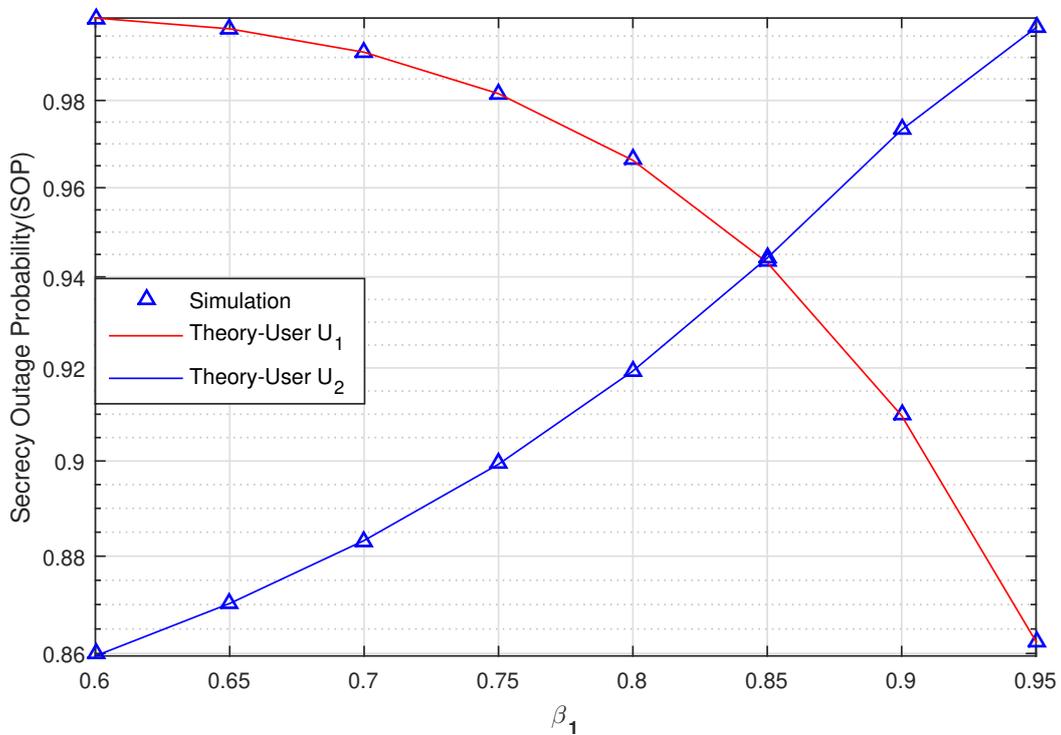


Figure 6. The SOP of  $U_1$  and  $U_2$  versus the power allocation coefficients  $\beta_1$  when SNR = 10 (dB).

### 5. Conclusions

A NOMA scheme with imperfect CSI in a UCCN was proposed in this paper. We also researched the physical layer security to improve the secrecy performance. The secrecy performance was examined

analyzed, evaluated by the secrecy outage probability of the achievable secrecy capacity, and over Rayleigh fading channels. The obtained results show that the security performance of the system model is decreased when the imperfect CSIs exists as well as the SNR increases. The proposed scheme with the optimal imperfect CSIs can achieve the best performance. Besides that, we can see that the node eavesdropper E is far from the source S and relay R, the security performance became more security. In addition, the security performance of U1 and the security performance of U2 are also compared with together. Lastly, the achieved results of the SOP matched well with the Monte Carlo simulation results.

**Author Contributions:** T.-P.H. designed the concept; D.-H.H. and C.T.T. analyzed and performed the simulation; C.T.T. contributed to developing some of the mathematical analyses; T.-P.H. organized and wrote the paper; M.V. and P.F. improved and critically reviewed the paper. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work was supported by the institutional grant SGS reg. No. SP2019/41 conducted at VSB—Technical University of Ostrava and also by the ESF project “Science without borders” reg. No. CZ.02.2.69/0.0/0.0/16 027/0008463 within the Operational Programme Research, Development and Education in the Czech Republic.

**Conflicts of Interest:** The authors declare that they have no conflicts of interest.

## Abbreviations

The following abbreviations were used in this manuscript:

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

## Appendix A

The probability Pr1.1 in formula (25) is rewritten as

$$\text{Pr 1.1} = \Pr [R_{SR}^{e_1} - R_{SE}^{e_1} \geq SC_{th}] = 1 - \Pr [R_{SR}^{e_1} - R_{SE}^{e_1} < SC_{th}]. \quad (\text{A1})$$

Applying formula in (20), we calculate  $R_{SR}^{e_1} = \frac{1}{2} \log_2(1 + \gamma_{SR}^{e_1})$ , and  $R_{SE}^{e_1} = \frac{1}{2} \log_2(1 + \gamma_{SE}^{e_1})$ . Hence, the probability Pr1.1 in (A1) is calculated by replacing  $R_{SR}^{e_1}$ ,  $R_{SE}^{e_1}$  and is expressed as

$$\text{Pr 1.1} = 1 - \Pr \left[ \frac{1}{2} \log_2(1 + \gamma_{SR}^{e_1}) < SC_{th} + \frac{1}{2} \log_2(1 + \gamma_{SE}^{e_1}) \right] \quad (\text{A2})$$

Replacing  $\gamma_{SR}^{e_1}$  in (12b) and  $\gamma_{SE}^{e_1}$  (14) into (A2), the probability Pr1.1 is obtained as

$$\begin{aligned} \text{Pr 1.1} &= 1 - \Pr \left[ \frac{af_{SR}}{bf_{SR} + c\lambda_{SR} + \rho^2 f_{SPu}} < \phi + (\phi + 1) \frac{af_{SE}}{bf_{SE} + c\lambda_{SE} + \rho^2 f_{SPu}} \right] \\ &= 1 - \Pr \left[ f_{SE} > \frac{af_{SR}(c\lambda_{SE} + \rho^2 f_{SPu}) - \phi(c\lambda_{SE} + \rho^2 f_{SPu})(bf_{SR} + c\lambda_{SR} + \rho^2 f_{SPu})}{[\phi b + (\phi + 1)a][bf_{SR} + c\lambda_{SR} + \rho^2 f_{SPu}] - abf_{SR}} \right] \end{aligned} \quad (\text{A3})$$

where

$$\phi = 2^{2SC_{th}} - 1; a = P\beta_1; b = P\beta_2; c = P(1 - \rho^2)$$

Using the pdf of the random variable  $f_{SPu}$  into (A3), the probability Pr1.1 is expressed as

$$\begin{aligned} \text{Pr 1.1} &= 1 - \Pr \left[ f_{SE} > \frac{af_{SR} (c\lambda_{SE} + \rho^2 f_{SPu}) - \phi (c\lambda_{SE} + \rho^2 f_{SPu}) (bf_{SR} + c\lambda_{SR} + \rho^2 f_{SPu})}{[\phi b + (\phi + 1)a] [bf_{SR} + c\lambda_{SR} + \rho^2 f_{SPu}] - abf_{SR}} \right] \\ &= 1 - \int_0^\infty f_{f_{SPu}}(x) \Pr \left[ f_{SE} > \frac{af_{SR} (c\lambda_{SE} + \rho^2 x) - \phi (c\lambda_{SE} + \rho^2 x) (bf_{SR} + c\lambda_{SR} + \rho^2 x)}{[\phi b + (\phi + 1)a] [bf_{SR} + c\lambda_{SR} + \rho^2 x] - abf_{SR}} \right] dx. \end{aligned} \tag{A4}$$

We can see that  $[\phi b + (\phi + 1)a] [bf_{SR} + c\lambda_{SR} + \rho^2 f_{SPu}] - abf_{SR} > 0$ .

Set  $M = af_{SR} (c\lambda_{SE} + \rho^2 f_{SPu})$ , and  $N = \phi (c\lambda_{SE} + \rho^2 f_{SPu}) (bf_{SR} + c\lambda_{SR} + \rho^2 f_{SPu})$ .

If  $M \leq N$ , then  $(a - \phi b) f_{SR} \leq \phi (c\lambda_{SR} + \rho^2 x)$ .

If  $M > N$ , then  $(a - \phi b) f_{SR} > \phi (c\lambda_{SR} + \rho^2 x)$ .

Hence, Pr 1.1 in (A4) is rewritten as

$$\text{Pr 1.1} = 1 - \int_0^\infty f_{f_{SPu}}(x) \times (K_1 + K_2) dx, \tag{A5}$$

where

$$K_1 = \Pr [(a - \phi b) f_{SR} \leq \phi (c\lambda_{SR} + \rho^2 x)];$$

$$K_2 = \Pr \left[ \begin{aligned} &f_{SE} > \frac{af_{SR}(c\lambda_{SE} + \rho^2 x) - \phi(c\lambda_{SE} + \rho^2 x)(bf_{SR} + c\lambda_{SR} + \rho^2 x)}{[\phi b + (\phi + 1)a][bf_{SR} + c\lambda_{SR} + \rho^2 x] - abf_{SR}}; \\ &(a - \phi b) f_{SR} > \phi (c\lambda_{SR} + \rho^2 x) \end{aligned} \right]$$

$K_1$  is resolved as follows:

$$K_1 = \Pr [(a - \phi b) f_{SR} \leq \phi (c\lambda_{SR} + \rho^2 x)]$$

$$= \begin{cases} 1 & a \leq \phi b \\ \Pr \left[ f_{SR} \leq \frac{\phi(c\lambda_{SR} + \rho^2 x)}{(a - \phi b)} \right] & a > \phi b \end{cases} = \begin{cases} 1 & a \leq \phi b \\ F_{f_{SR}} \left[ \frac{\phi(c\lambda_{SR} + \rho^2 x)}{(a - \phi b)} \right] & a > \phi b \end{cases} \tag{A6}$$

Applying the CDF of the random variable  $f_{SR}$  into (A6),  $K_1$  is solved in a closed-form expression as

$$K_1 = \begin{cases} 1 & a \leq \phi b \\ 1 - e^{-\frac{1}{\lambda_{SR}} \left[ \frac{\phi c\lambda_{SR}}{(a - \phi b)} + \frac{\phi \rho^2 x}{(a - \phi b)} \right]} & a > \phi b \end{cases} = \begin{cases} 1 & a \leq \phi b \\ 1 - e^{-\frac{1}{\lambda_{SR}} (\psi_{11} + \psi_2 x)} & a > \phi b \end{cases} \tag{A7}$$

where  $\psi_{11} = \frac{\phi c\lambda_{SR}}{(a - \phi b)}$ ;  $\psi_2 = \frac{\phi \rho^2}{(a - \phi b)}$ .

Similar to calculating  $K_1$ ,  $K_2$  is resolved as

$$K_2 = \begin{cases} 0 & a \leq \phi b \\ \int_{(\psi_{11} + \psi_2 x)}^\infty f_{f_{SR}}(y) \Pr \left[ f_{SE} > \left( \frac{(c\lambda_{SE} + \rho^2 x) (ay - \phi (by + c\lambda_{SR} + \rho^2 x))}{[\phi b + (\phi + 1)a] [by + c\lambda_{SR} + \rho^2 x] - aby} \right) \right] dy & a > \phi b \end{cases} \tag{A8}$$

We apply the pdf of the random variable  $f_{SR}$  and the CDF of the random variable  $f_{SE}$ ,  $K_2$  in (A8) is obtained as

$$K_2 = \begin{cases} 0 & a \leq \phi b \\ \int_{(\psi_{11} + \psi_2 x)}^{\infty} f_{f_{SR}}(y) \times e^{-\frac{1}{\lambda_{SE}} \left( \frac{(c\lambda_{SE} + \rho^2 x)(ay - \phi(by + c\lambda_{SR} + \rho^2 x))}{[\phi b + (\phi + 1)a][by + c\lambda_{SR} + \rho^2 x] - aby} \right)} dy & a > \phi b \end{cases} \quad (\text{A9})$$

Substituting  $K_1$  in (A7), and  $K_2$  in (A9) into (A5), Pr 1.1 is shown in two cases as  
If  $a \leq \phi b$ :

$$\text{Pr 1.1} = 1 - \int_0^{\infty} \frac{1}{\lambda_{SPu}} \times e^{-\frac{1}{\lambda_{SPu}} x} dx = 0 \quad (\text{A10})$$

If  $a > \phi b$ :

$$\text{Pr 1.1} = 1 - \left( \underbrace{\int_0^{\infty} f_{f_{SPu}}(x) (1 - e^{-\frac{1}{\lambda_{SR}}(\psi_{11} + \psi_2 x)}) dx}_{\Omega_{1.1}} + \underbrace{\int_0^{\infty} f_{f_{SPu}}(x) \int_{(\psi_{11} + \psi_2 x)}^{\infty} f_{f_{SR}}(y) e^{-\frac{1}{\lambda_{SE}} \zeta_1} dx dy}_{\Omega_{1.2}} \right) \quad (\text{A11})$$

where

$$\zeta_1 = \frac{(c\lambda_{SE} + \rho^2 x)(ay - \phi(by + c\lambda_{SR} + \rho^2 x))}{[\phi b + (\phi + 1)a][by + c\lambda_{SR} + \rho^2 x] - aby}$$

The  $\Omega_{1.1}$  in (A11) is calculated as

$$\begin{aligned} \Omega_{1.1} &= \int_0^{\infty} f_{f_{SPu}}(x) (1 - e^{-\frac{1}{\lambda_{SR}}(\psi_{11} + \psi_2 x)}) dx \\ &= \int_0^{\infty} \frac{1}{\lambda_{SPu}} e^{-\frac{1}{\lambda_{SPu}} x} \left( 1 - e^{-\frac{1}{\lambda_{SR}}(\psi_{11} + \psi_2 x)} \right) dx \\ &= 1 - \frac{\frac{1}{\lambda_{SPu}} e^{-\frac{1}{\lambda_{SR}} \psi_{11}}}{\frac{1}{\lambda_{SPu}} + \frac{1}{\lambda_{SR}} \psi_2} \end{aligned} \quad (\text{A12})$$

The  $\Omega_{1.2}$  in (A11) is presented as

$$\begin{aligned} \Omega_{1.2} &= \int_0^{\infty} f_{f_{SPu}}(x) \int_{(\psi_{11} + \psi_2 x)}^{\infty} f_{f_1}(y) e^{-\frac{1}{\lambda_{SE}} \zeta_1} dx dy \\ &= \int_0^{\infty} \frac{1}{\lambda_{SPu}} e^{-\frac{1}{\lambda_{SPu}} x} \int_{(\psi_{11} + \psi_2 x)}^{\infty} \frac{1}{\lambda_{SR}} e^{-\frac{1}{\lambda_{SR}} y} e^{-\frac{1}{\lambda_{SE}} \zeta_1} dx dy \\ &= \frac{1}{\lambda_{SR} \lambda_{SPu}} \int_0^{\infty} \int_{(\psi_{11} + \psi_2 x)}^{\infty} e^{-\left(\frac{1}{\lambda_{SPu}} x + \frac{1}{\lambda_{SR}} y\right)} e^{-\frac{1}{\lambda_{SE}} \zeta_1} dx dy \end{aligned} \quad (\text{A13})$$

Replacing the results of  $\Omega_{1.1}$  in (A12), and  $\Omega_{1.2}$  in (A13) into (A11), we resolved the probability Pr1.1 as follows:

$$\text{Pr 1.1} = \begin{cases} 0 & a \leq \theta b \\ \left( \frac{(1/\lambda_{SPu})e^{-\psi_{11}/\lambda_{SR}}}{(1/\lambda_{SPu})+(\psi_2/\lambda_{SR})} - (1/\lambda_{SR}\lambda_{SPu}) I_1 \right) & a > \theta b \end{cases} \quad (\text{A14})$$

where

$$I_1 = \int_0^{\infty} \int_{(\psi_{11}+\psi_2x)}^{\infty} e^{-\left(\frac{1}{\lambda_{SPu}}x + \frac{1}{\lambda_{SR}}y\right)} e^{-\frac{1}{\lambda_{SE}}\zeta_1} dx dy$$

## Appendix B

The probability Pr1.2 in formula (25) is rewritten as follows

$$\text{Pr 1.2} = \Pr \left[ R_{RU_1}^{e_1} - R_{RE}^{e_1} \geq SC_{th} \right] = 1 - \Pr \left[ R_{RU_1}^{e_1} < R_{RE}^{e_1} + SC_{th} \right]. \quad (\text{A15})$$

using formula in (20), we calculate  $R_{RU_1}^{e_1}$ ,  $R_{RE}^{e_1}$  and they achieved, respectively, as  $R_{RU_1}^{e_1} = \frac{1}{2} \log_2(1 + \gamma_{RU_1}^{e_1})$ ,  $R_{RE}^{e_1} = \frac{1}{2} \log_2(1 + \gamma_{RE}^{e_1})$ .

Hence, the probability Pr1.2 in (A15) is calculated by replacing  $R_{RU_1}^{e_1}$ ,  $R_{RE}^{e_1}$ ,  $\gamma_{RU_1}^{e_1}$  in (13), and  $\gamma_{RE}^{e_1}$  in (15), we have a result as

$$\begin{aligned} \text{Pr 1.2} &= 1 - \Pr \left[ \frac{1}{2} \log_2 \left( 1 + \gamma_{RU_1}^{e_1} \right) < \frac{1}{2} \log_2 \left( 1 + \gamma_{RE}^{e_1} \right) + SC_{th} \right] \\ &= 1 - \Pr \left[ \frac{af_1}{bf_1 + c\lambda_1 + \rho^2 f_{RPu}} < \theta + (\theta + 1) \left( \frac{af_{RE}}{bf_{RE} + c\lambda_{RE} + \rho^2 f_{RPu}} \right) \right] \end{aligned} \quad (\text{A16})$$

Similar as Pr1.1 at (A2), Pr1.2 is obtained as

$$\text{Pr 1.2} = \begin{cases} 0 & a \leq \theta b \\ \frac{(1/\lambda_{RPu})e^{-\psi_{12}/\lambda_1}}{(1/\lambda_{RPu})+\psi_2/\lambda_1} - (1/\lambda_1\lambda_{RPu}) I_2 & a > \theta b \end{cases} \quad (\text{A17})$$

where

$$\begin{aligned} \psi_{12} &= \frac{\theta c \lambda_1}{(a - \theta b)}; \\ I_2 &= \int_0^{\infty} \int_{(\psi_{12}+\psi_2x)}^{\infty} e^{-\left(\frac{1}{\lambda_{RPu}}x + \frac{1}{\lambda_1}y\right)} e^{-\frac{1}{\lambda_{RE}}\zeta_2} dx dy; \\ \zeta_2 &= \frac{(c\lambda_{RE} + \rho^2x)(ay - \theta(by + c\lambda_1 + \rho^2x))}{[\theta b + (\theta + 1)a][by + c\lambda_1 + \rho^2x] - aby}. \end{aligned}$$

Finally, from (A14) and (A17), the secrecy outage probability  $OP_{U_1}$  of  $U_1$  is resolved as (28)

## Appendix C

Substituting formulas (22) and (23) into (29), we calculate similar to Appendices A and B, and the  $OP_{U_2}$  is given as

$$OP_{U_2} = 1 - \underbrace{\Pr [R_{SR}^{e_2} - R_{SE}^{e_2} \geq SC_{th}]}_{\Omega_{2,1}} \times \underbrace{\Pr [R_{RU_2}^{e_2} - R_{RE}^{e_2} \geq SC_{th}]}_{\Omega_{2,2}} \quad (A18)$$

Firstly, we calculate the probability of  $\Omega_{2,1}$  as follows:

$$\begin{aligned} \Omega_{2,1} &= \Pr [R_{SR}^{e_2} - R_{SE}^{e_2} \geq SC_{th}] = 1 - \Pr [R_{SR}^{e_2} < SC_{th} + R_{SE}^{e_2}] \\ &= 1 - \Pr \left[ \frac{1}{2} \log_2 (1 + \gamma_{SR}^{e_2}) < SC_{th} + \frac{1}{2} \log_2 (1 + \gamma_{SE}^{e_2}) \right] \\ &= 1 - \Pr \left[ f_{SR} < \frac{\phi (c\lambda_{SR} + \rho^2 f_{SPu})}{b} + (\phi + 1) \frac{(c\lambda_{SR} + \rho^2 f_{SPu})}{(c\lambda_{SE} + \rho^2 f_{SPu})} f_{SE} \right] \end{aligned} \quad (A19)$$

Applying the pdf of the random variables  $f_{SPu}$  and  $f_{SE}$ , (A19) is written as

$$\begin{aligned} \Omega_{2,1} &= 1 - \int_0^\infty \int_0^\infty \left[ \Pr \left[ f_{SR} < \frac{\phi (c\lambda_{SE} + \rho^2 x)}{b} + (\phi + 1) \frac{(c\lambda_{SR} + \rho^2 x)}{(c\lambda_{SE} + \rho^2 x)} y \right] \times f_{f_{SPu}}(x) f_{f_{SE}}(y) \right] dx dy \\ &= 1 - \frac{1}{\lambda_{SPu} \lambda_{SE}} \int_0^\infty \int_0^\infty \left[ e^{-\left(\frac{1}{\lambda_{SPu}} x + \frac{1}{\lambda_{SE}} y\right)} \times \left( 1 - e^{-\frac{1}{\lambda_{SR}} \left( \frac{\phi (c\lambda_{SR} + \rho^2 x)}{b} + (\phi + 1) \frac{(c\lambda_{SR} + \rho^2 x)}{(c\lambda_{SE} + \rho^2 x)} y \right)} \right) \right] dx dy \end{aligned} \quad (A20)$$

$\Omega_{2,2}$  is calculated similarly as (A20) and is given as

$$\Omega_{2,2} = 1 - \frac{1}{\lambda_{RPu} \lambda_{RE}} \int_0^\infty \int_0^\infty \left[ e^{-\left(\frac{1}{\lambda_{RPu}} x + \frac{1}{\lambda_{RE}} y\right)} \times \left( 1 - e^{-\frac{1}{\lambda_2} \left( \frac{\phi (c\lambda_2 + \rho^2 x)}{b} + (\phi + 1) \frac{(c\lambda_2 + \rho^2 x)}{(c\lambda_{RE} + \rho^2 x)} y \right)} \right) \right] dx dy \quad (A21)$$

Finally, with formulas (A20) and (A21), the secrecy outage probability of  $U_2$  is obtained by the expression as (30).

## References

1. Liu, X.; Zhang, X. NOMA-based Resource Allocation for Cluster-based Cognitive Industrial Internet of Things. *IEEE Trans. Ind. Inf.* **2019**. [CrossRef]
2. Liu, X.; Jia, M.; Zhang, X.; Lu, W. A Novel Multichannel Internet of Things Based on Dynamic Spectrum Sharing in 5G Communication. *IEEE Internet Things J.* **2019**, *6*, 5962–5970. [CrossRef]
3. Gelenbe, E.; Zhang, Y. Performance Optimization With Energy Packets. *IEEE Syst. J.* **2019**, *13*, 3770–3780. [CrossRef]
4. Gelenbe, E.; Abdelrahman, O.-H. An Energy Packet Network model for mobile networks with energy harvesting. *Nonlinear Theory App. IEICE* **2018**, *9*, 322–336. [CrossRef]
5. Anwar, A.; Seet, B.-C.; Ding, Z. Non-Orthogonal Multiple Access for Ubiquitous Wireless Sensor Networks. *Sensors* **2018**, *18*, 516. [CrossRef] [PubMed]
6. Rauniyar, A.; Engelstad, P.; Østerbø, O.-N. RF Energy Harvesting and Information Transmission Based on NOMA for Wireless Powered IoT Relay Systems. *Sensors* **2018**, *18*, 3254. [CrossRef]
7. Yang, Z.; Ding, Z.; Fan, P.; Karagiannidis, G.-K. On the Performance of Non-orthogonal Multiple Access Systems With Partial Channel Information. *IEEE Trans. Commun.* **2016**, *64*, 654–667. [CrossRef]
8. Yang, Z.; Ding, Z.; Fan, P.; Al-Dhahir, N. The Impact of Power Allocation on Cooperative Non-orthogonal Multiple Access Networks With SWIPT. *IEEE Trans. Wireless Commun.* **2017**, *16*, 4332–4343. [CrossRef]
9. Tran, T.-N.; Voznak, M. Multi-Points Cooperative Relay in NOMA System with N-1 DF Relaying Nodes in HD/FD Mode for N User Equipments with Energy Harvesting. *Electronics* **2019**, *8*, 167. [CrossRef]
10. Zhang, Y.; Wang, X.; Wang, D.; Zhao, Q. A Range-Division User Relay Selection Scheme and Performance Analysis in NOMA-based Cooperative Opportunistic Multicast Systems. *Electronic* **2019**, *8*, 554. [CrossRef]
11. Ding, Z.; Peng, M.; Poor, H.-V. Cooperative Non-Orthogonal Multiple Access in 5G Systems. *IEEE Commun. Lett.* **2015**, *19*, 1462–1465. [CrossRef]

12. Jiao, R.; Dai, L.; Zhang, J.; MacKenzie, R.; Hao, M. On the Performance of NOMA-Based Cooperative Relaying Systems over Rician Fading Channels. *IEEE Trans. Veh. Technol.* **2017**. [[CrossRef](#)]
13. 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](#)]
14. 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](#)]
15. 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](#)]
16. Hu, H.; Gao, Z.; Liao, X.; Leung, V.C.M. Secure Communications in CIoT Networks with a Wireless Energy Harvesting Untrusted Relay. *Sensors* **2017**, *17*, 2023. [[CrossRef](#)]
17. He, B.; Liu, A.; Yang, N.; Lau, V.K. On the Design of Secure Non-Orthogonal Multiple Access Systems. *IEEE J. Sel. Areas Commun.* **2017**, *35*, 2196–2206. [[CrossRef](#)]
18. Chen, J.; Yang, L.; Alouini, M.S. Physical Layer Security for Cooperative NOMA Systems. *IEEE Trans. Veh. Technol.* **2018**, *67*, 4645–4649. [[CrossRef](#)]
19. Do, D.T.; Van Nguyen, M.S.; Hoang, T.A.; Voznak, M. NOMA-Assisted Multiple Access Scheme for IoT Deployment: Relay Selection Model and Secrecy Performance Improvement. *Sensors* **2019**, *19*, 736. [[CrossRef](#)]
20. 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](#)]
21. Lv, L.; Chen, J.; Ni, Q. Cooperative Non-Orthogonal Multiple Access in Cognitive Radio. *IEEE Commun. Lett.* **2016**, *20*, 2059–2062. [[CrossRef](#)]
22. Lee, S.; Duong, T.Q.; Benevides daCosta, D.; Ha, D.B.; Nguyen, S.Q. Underlay cognitive radio networks with cooperative non-orthogonal multiple access. *IET Commun.* **2018**, *12*, 359–366. [[CrossRef](#)]
23. 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](#)]
24. Liu, Y.; Wang, L.; Duy, T.T.; Elkashlan, M.; Duong, T.Q. Relay Selection for Security Enhancement in 251 Cognitive Relay Networks. *IEEE Wirel. Commun. Lett.* **2015**, *4*, 46–49. [[CrossRef](#)]
25. Son, P.N. Joint impacts of Hardware impairments, Imperfect CSIs, and Interference constraints on Underlay Cooperative Cognitive Networks with reactive relay selection. *Telecommun. Syst.* **2019**, *71*, 65–76. [[CrossRef](#)]
26. Arzykulov, S.; Tsiftsis, T.A.; Nauryzbayev, G.; Abdallah, M. Outage Performance of Cooperative Underlay CR-NOMA With Imperfect CSI. *IEEE Commun. Lett.* **2019**, *23*, 176–179. [[CrossRef](#)]



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).