Studying strictly positive secure capacity in cognitive radio-based non-orthogonal multiple access

Chi-Bao Le, Dinh-Thuan Do
Faculty of Electronics Technology, Industrial University of Ho Chi Minh City (IUH), Ho Chi Minh City, Vietnam

ABSTRACT
This paper studies a downlink security-aware secure outage performance in the secondary network of cognitive radio-assisted non-orthogonal multiple access network (CR-NOMA). The multiple relay is employed to assist transmission from the secondary source to destinations. The security-aware performance is subject to constraints in fixed power allocation factor assigned to each secondary user. The security-aware secure performance is based on channel state information (CSI) at the physical layer in which an eavesdropper intends to steal information. According to the considered system, exact expressions of Strictly positive secure capacity (SPSC) are proved to analyze system in terms of secure performance. Finally, the secondary user secure problem is evaluated via Monte-Carlo simulation method. The main results indicate that the secure performance of proposed system can be improved significantly.

This is an open access article under the CC BY-SA license.

Copyright 

Corresponding Author:
Dinh-Thuan Do
Faculty of Electronics Technology, Industrial University of Ho Chi Minh City
12 Nguyen Van Bao Road, Go Vap District, Ho Chi Minh City, Vietnam
Email: dodinhthuan@iuh.edu.vn

1. INTRODUCTION
Both non-orthogonal multiple access (NOMA) and physical-layer security (PLS) have been introduced as promising enabling technologies to implement some applications for Internet of Things (IoT) or future systems [1-4]. Recently, the coexistence of these two important communication techniques benefits from cognitive ability and massive connections and these hybrid techniques have been considered to provide spectral efficient improvement for wireless transmission such as recent work [6-8].

Furthermore, physical-layer security (PHY) has attracted great interests while wireless applications are more popular. PHY based secure method does not require extra resources for the secret key [10-14]. In order to achieve secure communication, one can exploit the physical layer characteristics of the wireless channels. However, the secrecy rate of wireless communication systems is constrained by the channel state information [15]. In order to improve the secrecy rate, many methods are introduced such as jamming, multiple antennas, cooperative relaying and artificial noise (AN)-aided techniques have been studied [16]. Main results reported in [17-24] that these techniques benefit to improve the secrecy rate.

Interestingly, most existing works have mainly focused on the performance and optimization of the PLS in NOMA systems. However, there is still open problems to rigorously study the feasibility of achieving the better secure performance by using best relay selection in secondary network of CR-NOMA systems. Although the joint user scheduling and power allocation problems are investigated for NOMA-based wireless network in [17], how cognitive radio technology affects the secure performance for NOMA-based wireless network needs further studies. In this paper, we study the security-aware SPSC metric CR-NOMA network.

Journal homepage: http://beei.org
2. SYSTEM MODEL

In Figure 1, we consider the CR system containing the secondary network including base station (BS). To enhance performance of distance users, we need \(N\) relay nodes. Regarding distance users, two destination \(U_1, U_2\), one eavesdropper \(E\) are considered their performance. Through the paper, \(h_u\) is denoted as channel for node \(u\), and it follows Rayleigh fading model with channel gain \(\lambda_u\). It is noted that \(P_S\) is transmit power at BS and it is limited under constraint with the primary network which contains primary destination \(P_D\). The interference channel from BS to the primary network is \(h_{SP}\). \(h_{R_n}\) is the channel between BS and \(R_n\). \(h_{R_n}\) is denoted as the channel between relay and \(U_i\).

![Figure 1. Secure CR-NOMA system](image)

In CR-NOMA, the transmit power at the BS is constrained by (1)

\[
P_S \leq \min \left( \frac{I}{|h_{SP}|^2}, \bar{P}_S \right)
\]

in which, we call \(\bar{P}_S\) and \(I\) as maximum average transmit power at the BS and interference temperature constraint (ITC) at primary destination \(P_D\), respectively. At the first hop transmission, the \(n\)-th node among \(N\) relay node, the received signal can be formulated by (2)

\[
y_R = h_{R_n} \left( \sqrt{a_1 P_S} x_1 + \sqrt{a_2 P_S} x_2 \right) + n_{R_n}
\]

where the AWGN noise terms at \(R\) is \(n_{R_n}\). Regarding the relay is used to forward signal, the criteria to select relay with its index, i.e. \(n^*\) is formulated related the best channel

\[
n^* = \arg \max_{1, 2, \ldots, N} |h_{R_n}|^2
\]

To decode signal \(x_1\) and \(x_2\) at \(R\), the signal-to-interference-plus-noise ratio (SINR) is given by (4).

\[
SNR_{R_1}^1 = \frac{a_1 \rho_S |h_{R_n}|^2}{a_2 \rho_S |h_{R_n}|^2 + 1}
\]

where \(\rho_S = \frac{P_S}{\sigma^2}\) is the transmit signal to noise ratio (SNR) at the BS. At relay relying SIC, it is necessary to examine the received SNR at \(R\) to detect message \(x_2\) as (5).

\[
SNR_{R_2}^2 = a_2 \rho_S |h_{R_n}|^2
\]

In the next phase, the link between selected relay \(R_i\) and \(U_i, i = 1, 2\) is required to proceed signal \(\sqrt{a_1 P_{R_i} x_1} + \sqrt{a_2 P_{R_i} x_2}\). \(P_R\) is called as the transmit power at \(R\). The received signal \(U_i\) is expressed by (6)

\[
y_{U_i} = h_{U_i} \left( \sqrt{a_1 P_{R_i} x_1} + \sqrt{a_2 P_{R_i} x_2} \right) + n_{U_i}, \forall i \in \{1, 2\}
\]

in which the AWGN noise terms is \(n_{U_i}\) measured at \(U_i\). Further, principle of NOMA applied to \(U_i\) with higher power factor, it can detect \(x_1\) by considering \(x_2\) as a background noise with (7)

\[
\text{(Chi-Bao Le)}
\]
where \( \rho_R = \frac{P_R}{\sigma^2} \) is the transmit SNR at \( R \). To continue detecting procedure, \( U_2 \) needs SIC to decode \( \bar{x}_1 \) while considering its own data \( \bar{x}_2 \) as a noise. The SINR is written as (8).

\[
SNR_{U_2} = \frac{a_1 \rho_R |h_{U_1}|^2}{a_2 \rho_R |h_{U_2}|^2 + 1} \tag{7}
\]

In this regard, \( U_2 \) detects its own signal and the corresponding SNR is given as (9).

\[
SNR_{U_2,x_2} = a_2 \rho_R |h_{U_2}|^2 \tag{9}
\]

Unfortunately, eavesdropper steals information from the selected relay, the received signal at \( E \) is given as (10).

\[
y_E = h_E \left( \sqrt{a_1 P_E} \bar{x}_1 + \sqrt{a_2 P_E} \bar{x}_1 \right) + n_E \tag{10}
\]

where \( n_E \) is the AWGN noise terms at \( E \). The channel between Relay and \( E \) is \( h_E \). Then, SNR at \( E \) is given as

\[
SNR_{E_i} = a_i \rho_E |h_E|^2, \quad i \in \{1, 2\} \tag{11}
\]

where \( \rho_E = \frac{P_E}{\sigma^2} \) is transmit SNR at \( E \). The secrecy capacity for \( U_1, U_2 \) are computed respectively as

\[
C_1 = \left\lceil \frac{1}{2} \log_2 \left( \frac{1 + \min \left( SNR_{R_i}, SNR_{U_1} \right)}{1 + SNR_{E_i}} \right) \right\rceil^+, \tag{12}
\]

\[
C_2 = \left\lceil \frac{1}{2} \log_2 \left( \frac{1 + \min \left( SNR_{R_i}, SNR_{U_2} \right)}{1 + SNR_{E_i}} \right) \right\rceil^+, \tag{13}
\]

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

3. SPSC ANALYSIS

3.1. SPSC computation at \( U_1 \)

We first using decode-and-forward scheme at relay node and consider SPSC performance of the first user \( U_1 \) as (14).

\[
G_1 = \Pr \left( C_1 > 0 \right)
= \Pr \left( \min \left( SNR_{R_i}, SNR_{U1} \right) > SNR_{E_1} \right)
= \Pr \left( \left| h_{R_{i_1}} \right|^2 > \frac{\rho_E |h_E|^2}{\rho_S (1 - \rho_E a_2 |h_E|^2)}, \rho_S < \frac{\rho_I}{|h_{SP}|^2} \right)_{G_{1,1}}
+ \Pr \left( \left| h_{R_{i_2}} \right|^2 > \frac{\rho_E |h_E|^2 |h_{SP}|^2}{\rho_I (1 - a_2 \rho_E |h_E|^2)}, \rho_S > \frac{\rho_I}{|h_{SP}|^2} \right)_{G_{1,2}}
\times \Pr \left( \left| h_{U_1} \right|^2 > \frac{\rho_E |h_E|^2}{\rho_R (1 - a_2 \rho_E |h_E|^2)} \right)_{G_{1,3}}
\]
We then compute each component $G_{1,1}, G_{1,2}, G_{1,3}$ as (15).

\[
G_{1,1} = \Pr \left( |h_{R_1}|^2 > \frac{\rho_E |h_E|^2}{\rho_I \left( 1 - a_2 \rho_E |h_E|^2 \right)}, |h_E|^2 < \eta, \rho_S < \frac{\rho_I}{|h_{SP}|^2} \right) = \int_0^{\eta} f_{|h_E|^2} (x) \int_0^{\eta} f_{|h_{SP}|^2} (y) \left[ 1 - F_{|h_{R_1}|^2} \left( \frac{\rho_E y}{\rho_I \left( 1 - a_2 \rho_E y \right)} \right) \right] dx dy
\]

(15)

\[
G_{1,1} = \left( 1 - e^{-\frac{\eta}{\rho_S |h_{SP}|^2}} \right) \sum_{n=1}^{N} \left( \begin{array}{c} N \\ n \end{array} \right) \left( -1 \right)^{n-1} \frac{\eta \pi}{2} \frac{1}{2P \lambda_E} \times e^{-\frac{(n+1)^2}{\rho_S |h_{SP}|^2 \rho_I \lambda_{SR}(1-a_2 \rho_E)}}
\]

where $\eta = \frac{1}{\rho_S |h_{SP}|^2}$.

The closed-form expression for $G_{1,1}$ is very difficult to achieve, then using the formula Gaussian-Chebyshev quadrature, $G_{1,1}$ is given as (16)

\[
G_{1,1} \approx \left( 1 - e^{-\frac{\eta}{\rho_S |h_{SP}|^2}} \right) \sum_{n=1}^{N} \left( \begin{array}{c} N \\ n \end{array} \right) \left( -1 \right)^{n-1} \frac{\eta \pi}{2} \frac{1}{2P \lambda_E} \times e^{-\frac{(n+1)^2}{\rho_S |h_{SP}|^2 \rho_I \lambda_{SR}(1-a_2 \rho_E)}}
\]

(16)

Next, $G_{1,2}$ is calculated as (17).

\[
G_{1,2} = \Pr \left( |h_{R_2}|^2 > \frac{\rho_E |h_E|^2|h_{SP}|^2}{\rho_I \left( 1 - a_2 \rho_E |h_E|^2 \right)}, |h_E|^2 < \eta, \rho_S > \frac{\rho_I}{|h_{SP}|^2} \right) = \int_0^{\eta} f_{|h_E|^2} (x) \int_0^{\eta} f_{|h_{SP}|^2} (y) \left[ 1 - F_{|h_{R_2}|^2} \left( \frac{\rho_E y}{\rho_I \left( 1 - a_2 \rho_E y \right)} \right) \right] dx dy
\]

(17)

\[
G_{1,2} = \sum_{n=1}^{N} \left( \begin{array}{c} N \\ n \end{array} \right) \left( -1 \right)^{n-1} \frac{\eta \pi}{\lambda_{SP} \lambda_E (1-a_2 \rho_E \lambda_{SR})} \times e^{-\frac{(n+1)^2}{\rho_S \lambda_{SP} \lambda_E}} \left( \frac{\eta}{\rho_S \lambda_{SP} \lambda_E} \right)^{-1}
\]

\[
G_{1,2} \approx \sum_{n=1}^{N} \sum_{v=1}^{V} \left( \begin{array}{c} N \\ n \end{array} \right) \left( \begin{array}{c} V \\ v \end{array} \right) \frac{\eta \pi \left( 1 \right)^{n-1} \left( n+1 \right)^2}{2V \lambda_{SP} \lambda_E \Phi(w)} e^{-\frac{(n+1)^2}{\rho_S \lambda_{SP} \lambda_E}} \times e^{-\frac{\eta}{\rho_S \lambda_{SP} \lambda_E}}
\]

(18)

where $\nu_v = \cos \left( \frac{2\nu-1}{2V} \pi \right)$ and $\Phi(w) = \left( \frac{1}{\lambda_{SP}} + \frac{\nu_p (\nu_0 + \eta)}{2(a_2 \rho_E (\nu_0 + \eta))} \right)$.

**Studying strictly positive secure capacity in cognitive radio-based non-orthogonal multiple ... (Chi-Bao Le)**
Next, $G_{1,3}$ is calculated as (19)

$$G_{1,3} = \Pr \left( |h_{U_1}|^2 > \frac{\rho_E |h_E|^2}{\rho_R (1 - a_2 \rho_E |h_E|^2)}, |h_E|^2 < \eta \right)$$

$$= \int_0^\eta f_{|h_E|^2}(x) \left[ 1 - F_{|h_{U_1}|^2} \left( \frac{\rho_E x}{\rho_R (1 - a_2 \rho_E x)} \right) \right] dx$$

$$= \frac{1}{\lambda_E} \int_0^\eta e^{-\left( \frac{1}{2 \lambda_E^2} + \frac{\rho_E}{\lambda_E} (1 - a_2 \rho_E \eta) \right)} \, dx$$

(19)

Keep using the formula Gaussian-Chebyshev quadrature, $G_{1,3}$ is given by (20)

$$G_{1,3} \approx \frac{\pi \eta}{2 \lambda_E Q} \sum_{q=1}^Q \sqrt{1 - \zeta_q^2} e^{-\left( \frac{(q+1)\pi}{2 \lambda_E} \right)} \frac{(q+1)\pi \rho_E}{\lambda_E \rho_R (1 - a_2 \rho_E \eta)}$$

(20)

where $\zeta_q = \cos \left( \frac{2q+1}{2Q} \pi \right)$.

Substituting (20), (18) and (16) into (14), $G_1$ is given by (21)

$$G_1 = \left[ (1 - e^{-\frac{\rho_E}{\lambda_E} \rho_R}) \sum_{n=1}^N \sum_{p=1}^{P} {N \choose n} \frac{\eta \pi (-1)^{n-1} \sqrt{1 - \zeta_q^2}}{2 \lambda_E^2} \right]$$

$$\times e^{-\frac{(n+1)\pi}{2 \lambda_E}} \frac{\rho_R \lambda_R (1 - a_2 \rho_E (n+1))}{\rho_R \lambda_R (1 - a_2 \rho_E (n+1))}$$

$$+ \sum_{n=1}^N \sum_{n=1}^V {N \choose n} \frac{\eta \pi (-1)^{n-1} \sqrt{1 - \zeta_q^2}}{2 \lambda_E^2} e^{-\frac{(n+1)\pi}{2 \lambda_E}} \frac{\rho_R \lambda_R (n+1)}{\rho_R \lambda_R (n+1)}$$

$$\times \frac{\pi \eta}{2 \lambda_E Q} \sum_{q=1}^Q \sqrt{1 - \zeta_q^2} e^{-\left( \frac{(q+1)\pi}{2 \lambda_E} \right)} \frac{(q+1)\pi \rho_E}{\lambda_E \rho_R (1 - a_2 \rho_E \eta)}$$

(21)

3.2. SPSC computation at $U_2$

In similar way, SPSC of user $U_2$ is expressed by (22)

$$G_2 = \Pr (C_2 > 0)$$

$$= \Pr \left( \min \left( SNR_{R1}, SNR_{U_2,x_2} \right) > SNR_{E2} \right)$$

$$= \Pr \left( |h_{R_{a_1}}|^2 > \tilde{a} a_2 \rho_E |h_E|^2, |h_{SP}|^2 < \frac{\rho_I}{\rho_S} \right)$$

$$G_{2,1}$$

$$+ \Pr \left( |h_{R_{a_2}}|^2 > \tilde{a} a_2 \rho_E |h_E|^2, |h_{SP}|^2 > \frac{\rho_I}{\rho_S} \right)$$

$$G_{2,2}$$

$$\times \Pr \left( |h_{U_2}|^2 > \frac{\rho_E |h_E|^2}{\rho_R} \right)$$

$$G_{2,3}$$

(22)

where $\tilde{a} = \frac{1}{a_2 \rho_S}$ and $\tilde{a} = \frac{1}{a_2 \rho_I}$. These terms $G_{2,1}, G_{2,2}, G_{2,3}$ are respectively formulated by (23) and (24)
\[
G_{2,1} = \Pr \left( |h_{R_n}|^2 > \bar{a}a_2\rho_E|h_E|^2, |h_{SP}|^2 < \frac{\rho_I}{\rho_S} \right) \\
= \int_{0}^{\frac{\rho_I}{\rho_S}} f_{|h_{SP}|^2}(x) \int_{0}^{\infty} f_{|h_E|^2}(y) \left[ 1 - F_{|h_{R_n}|^2}(\bar{a}a_2\rho_Ey) \right] dx dy \\
= (1 - e^{-\frac{\rho_I}{\rho_S}\lambda_{SR}}) \sum_{n=1}^{N} \binom{N}{n} \frac{(-1)^{n-1}}{\lambda_E} \int_{0}^{\infty} e^{-\frac{\rho_I}{\rho_S}y} \frac{\bar{a}a_2\rho_Ey}{\lambda_{SR} + n\lambda_E}\bar{a}a_2\rho_E \right] dy \\
= (1 - e^{-\frac{\rho_I}{\rho_S}\lambda_{SR}}) \sum_{n=1}^{N} \binom{N}{n} \frac{(-1)^{n-1}\lambda_{SR}}{\lambda_{SR} + n\lambda_E\bar{a}a_2\rho_E} \\
\]

where \( \ell_n = \frac{1}{\lambda_E} + \frac{\bar{a}a_2\rho_E}{\lambda_{SR}} \) and \( \varpi_n = \frac{\lambda_{SR}}{\lambda_{SR} + n\lambda_E\bar{a}a_2\rho_E} \).

We are using [[25], 8.211.1], \( G_{2,2} \) is given by (25).

\[
G_{2,2} = \sum_{n=1}^{N} \binom{N}{n} \frac{\lambda_{SR}(-1)^ne^{-\frac{\rho_I}{\rho_S}\lambda_{SR} + \ell_n\varpi_n}}{na_2\bar{a}_2\rho_E\lambda_E\lambda_{SP}} Ei(-\ell_n\varpi_n) \\
\]

Next, we are calculated \( G_{2,3} \) as (26).

\[
G_{2,3} = \Pr \left( |h_{U_2}|^2 > \frac{\rho_E|h_E|^2}{\rho_R} \right) \\
= \int_{0}^{\infty} f_{|h_E|^2}(x) \left[ 1 - F_{|h_{U_2}|^2}\left(\frac{\rho_Ex}{\rho_R}\right) \right] dx \\
= \frac{1}{\lambda_E} \int_{0}^{\infty} e^{-\left(\frac{1}{\lambda_E} + \frac{\rho_Ex}{\rho_R}\right)} dx \\
= \frac{\rho_R\lambda_{U_2}}{\rho_R\lambda_{U_2} + \lambda_E\rho_E} \\
\]

Substituting (26), (25) and (23) into (22), \( G_2 \) is given by (27).

\[
G_2 = \sum_{n=1}^{N} \binom{N}{n} \frac{\rho_R\lambda_{U_2}\lambda_{SR}}{\rho_R\lambda_{U_2} + \lambda_E\rho_E} \left[ 1 - e^{-\frac{\rho_I}{\rho_S}\lambda_{SR}} \right] \frac{(-1)^{n-1}}{\lambda_{SR} + n\lambda_E\bar{a}a_2\rho_E} \\
+ \frac{(-1)^n e^{-\frac{\rho_I}{\rho_S}\lambda_{SR} + \ell_n\varpi_n}}{na_2\bar{a}_2\rho_E\lambda_E\lambda_{SP}} Ei(-\ell_n\varpi_n) \\
\]

Studying strictly positive secure capacity in cognitive radio-based non-orthogonal multiple ... (Chi-Bao Le)
4. **NUMERICAL RESULTS**

Our simulation parameters here are $a_1 = 0.7$ and $a_2 = 0.3$, $N = 2$, $R_1 = R_2 = 1$. $\rho_I = 5$ dB, $\rho_E = 15$ dB, $\lambda_{SP} = 0.1$, $\lambda_{SR} = 1$, $\lambda_{RD1} = 0.9$, $\lambda_{RD2} = 0.6$ and $\lambda_{RE} = 0.1$. $Q = V = 1000$.

Figure 2 depicts SPSC performance versus transmit SNR. We consider many cases related to CR-NOMA for $\rho_E = 5, 10, 15$ (dB). It is very high value of SPSC when increasing $\rho$ to 20 (dB) and greater. Signal $x_2$ provides better SPSC performance compared with signal $x_2$, and it can be explained that different power allocated to each signal. Comparing the simulation results with the analytical results, there are tight matching curves.

It can be seen how the number of the relay nodes make impacts on SPSC performance at Figure 3. Similar trend of SPSC can be reported in Figure 3, it means SPSC will be worse as increasing $\rho$ to 30 (dB). Figure 3 depicts SPSC curves is highest at $N = 15$. When $\rho$ is greater than 25 (dB), SPSC curves meet saturation.

![Figure 2](image1.png)  
Figure 2. SPSC versus transmit SNR at BS

![Figure 3](image2.png)  
Figure 3. SPSC versus transmit SNR at BS with different number of relay nodes

5. **CONCLUSION**

The paper studied SPSC in cognitive radio network using NOMA and relay selection. Secure performance is considered as existence of an eavesdropper and acceptable SPSC can be known. Moreover, the approximate expressions in term of SPSC are derived to exhibit performance of two destinations. The derivations and analysis results showed that the proposed relay selection in CR-NOMA can effectively enhance the secure performance.

**REFERENCES**


