Security performance analysis for power domain NOMA employing in cognitive radio networks

Thi-Anh Hoang, Chi-Bao Le, Dinh-Thuan Do
Industrial University of Ho Chi Minh City, Vietnam

ABSTRACT
The power domain non-orthogonal multiple access (NOMA) technique introduces one of the fundamental characteristics and it exhibits the possibility of users to decode the messages of the other paired users on the same resources. In cognitive radio inspired NOMA (CR-NOMA), the base station (BS) has to serve untrusted users or users with different security clearance. This phenomenon raises a security threat particularly in such CR-NOMA. This paper develops a tractable analysis framework to evaluate the security performance of cooperative non-orthogonal multiple access (NOMA) in cognitive networks, where relay is able to serve two far NOMA users in the presence of external eavesdropper. In particular, we study the secrecy outage probability in a two-user NOMA system. This situation happens in practical the BS is pairing a legitimate user with another untrusted user. Main reason is that the non-uniform distribution in terms of trusted and untrusted users in the cell. By performing numerical results demonstrate the performance improvements of the proposed NOMA scheme in comparison to that of several situations in terms of different parameters. Furthermore, the security performance of NOMA is shown to verify the derived expressions.

Keywords: Cognitive radio
Non-orthogonal multiple access (NOMA)
Physical-layer security

1. INTRODUCTION
As a promising multiple access (MA) technique, Non-orthogonal multiple access (NOMA) has been proposed to adapt the challenging requirements of the future mobile communication networks. Several strict requirements in 5G wireless communication can be achieved such as high data speed, spectral efficiency, massive connectivity and low latency [1-10]. In [11, 12] the NOMA can be integrated with green communication to enable ability of wireless power transfer in cooperative NOMA network. Other application of device-to-device (D2D) to NOMA is introduced as in [13]. Different with the conventional MA techniques, the power domain is used to serve a multiple user in NOMA at different power levels and such paradigm exhibits a high spectral efficiency [14]. To permit the unlicensed users operating on the spectrum allocated for the licensed users, cognitive radio networks (CRNs) have been recommended to achieve full advantage of radio resource. In these situations, the quality of service of the primary user networks is maintained [15, 16]. In general, power domain multiple access scheme and spectrum efficiency are advantages are able to achieved. Hence, by introducing NOMA to PUNs, the system performance of cognitive radio can be further increased.
In the other trend, dedicated relays [17-19] are also deployed to reform cooperative NOMA transmission [20]. To enhance the reliability of the NOMA-weak users, [21] adopted a dedicated relay network. Also, with the help of a relay (both AF and DF protocols) [22] presented a secrecy analysis of a NOMA system. The other works reported in [23-25], in which the CR networks are studied with an underlay paradigm. From raised analytical results according to the previous analysis, the improved system performance benefits from combining system between overlay CR and NOMA. Unfortunately, overlay CR can enhance system performance and also produce the risk of infection of illegal information simultaneously. On the contrary, NOMA can achieve better secrecy performance than OMA [22]. The physical layer security performance in overlay CR-NOMA networks is still a challenging issue and it motivates this study. This paper determines physical layer security (PLS) in cognitive radio inspired non-orthogonal multiple access (CR-NOMA) networks with secondary source and multiple secondary users under impact of primary destination.

To manage the interference among the users and guarantee the quality of services (QoS) of primary users, a new secure NOMA transmission strategy is designed, where the primary and secondary users are paired according to their channel gains, respectively, and power-domain NOMA is employed to transmit the signal. This paper studies a downlink cooperative CR-NOMA model with interference temperature constraint (ITC) at the primary receiver. Exact closed-form expressions for the OP of the far NOMA users are derived. These expressions are verified by Monte-Carlo simulations.

2. SYSTEM MODEL

A downlink cooperative underlay CR-NOMA is considered in this study. In this model, secondary network (SN) consists of a secondary base station (S), a relay (R) and two far NOMA users (D1; D2) can operate together with primary network containing primary destination (PD) who make impact on system performance at secondary network, as shown in Figure 1. Regarding secure performance, existence of eavesdropper E need be concerned. The links are assigned channel as in Figure 1 and these channels follow flat Rayleigh fading model. $h_{SR}$ is the channel between BS and relay, $h_{RD}$ is the channel between Relay and two users. $P_S$ is transmit power at the BS. We denote the superimposed signal to transmit from the BS to secondary destinations $\sqrt{a_1 P_S x_1} + \sqrt{a_2 P_S x_2}$. While $a_1, a_2$ are power allocation factors in NOMA satisfying $a_1 + a_2 = 1 (a_1 > a_2)$.

![Figure 1. System model of secure CR-NOMA](image)

The transmit power constraint is determined at the BS:

$$P_S \leq \min \left( \frac{1}{|h_{SP}|^2}, P_S \right)$$  \hspace{1cm} (1)
where $\bar{P}_s$ and $I$ stand for maximum average transmit power available at the BS and ITC at $P_o$. In the first time, $R$ received the following signal:

$$y_R = h_{tx} \left( \sqrt{a_1 P_1 x_1} + \sqrt{a_2 P_2 x_2} \right) + n_R$$  \hspace{1cm} (2)$$

in which $n_R$ stand for the AWGN noise terms at $R$.

Then, we compute signal-to-interference-plus-noise ratio (SINR) and signal-to-noise ratio (SNR) of decoding $x_1$ and $x_2$ at $R$ and they can be respectively written as:

$$\gamma_R^1 = \frac{a_1 \rho_x |h_{tx}|^2}{a_1 \rho_x |h_{tx}|^2 + 1}$$  \hspace{1cm} (3)$$

and

$$\gamma_R^2 = a_2 \rho_x |h_{tx}|^2$$  \hspace{1cm} (4)$$

where $\rho_x = \frac{P_x}{\sigma^2}$ is the transmit SNR at the BS.

In the second phase, the detected superimposed signal $\sqrt{b_1 P_1 x_1} + \sqrt{b_2 P_2 x_2}$ will be forwarded to destinations. It is noted that $P_s$ is the transmit power at $R$. The received signal at $D_i$ can be given as:

$$y_{D_i} = h_{Rx} \left( \sqrt{b_1 P_1 x_1} + \sqrt{b_2 P_2 x_2} \right) + n_{D_i}, \forall i \in \{1, 2\}$$  \hspace{1cm} (5)$$

where $n_{D_i}$ is the AWGN noise terms at $D_i$. Further, due to the fact that $D_i$ is allocated with higher power factor, it can detect $x_1$ by treating $x_2$ as a background noise and it can be achieved following SINR.

$$\gamma_{D_i} = \frac{|h_{Rx}|^2 b_1 \rho_r}{|h_{Rx}|^2 b_2 \rho_r + 1}$$  \hspace{1cm} (6)$$

Furthermore, $D_2$ with SIC is required to detect $x_1$ while $x_2$ is considered as a noise. The SINR in this case can be expressed:

$$\gamma_{D2-1} = \frac{|h_{Rx}|^2 b_1 \rho_r}{|h_{Rx}|^2 b_2 \rho_r + 1}$$  \hspace{1cm} (7)$$

where $\rho_r = \frac{P_r}{\sigma^2}$ is the transmit SNR at $R$. the following SNR can be obtained to $D_2$ detects its own signal.

$$\gamma_{D_2} = |h_{Rx}|^2 b_2 \rho_r$$  \hspace{1cm} (8)$$

The signal received at $E$

$$y_E = h_{RE} \left( \sqrt{b_1 P_1 x_1} + \sqrt{b_2 P_2 x_1} \right) + n_E$$  \hspace{1cm} (9)$$

where $n_E$ indicates the AWGN noise terms at $E$. $h_{RE}$ is the channel between Relay and $E$.

The signal-to-noise ratio (SNR) at $E$:

$$\gamma_E = \beta L \rho_x |h_{RE}|^2$$  \hspace{1cm} (10)$$
where $\rho_\ell = \frac{P_\ell}{\sigma^2}$ is transmit SNR at $E$. The achievable rates of $x_1$ and $x_2$ are derived respectively:

$$K_1 = \frac{1}{2} \log_2 \left( 1 + \min \left( \gamma_k \cdot \gamma_{D2} \cdot \gamma_{D1} \right) \right)$$

(11)

$$K_2 = \frac{1}{2} \log_2 \left( 1 + \min \left( \gamma_k \cdot \gamma_{D2} \right) \right)$$

(12)

and the achievable rates of eavesdropper’s signal is given by:

$$K_{E_i} = \frac{1}{2} \log_2 \left( 1 + \gamma_{E_i} \right)$$

(13)

the secrecy capacity for $D_1$ is obtained as:

$$C_i = \left[ \frac{1}{2} \log_2 \left( 1 + \frac{\min \left( \gamma_k \cdot \gamma_{D2} \cdot \gamma_{D1} \right)}{1 + \gamma_{E2}} \right) \right]^+$$

(14)

the secrecy capacity for $D_2$ is obtained as:

$$C_2 = \left[ \frac{1}{2} \log_2 \left( 1 + \frac{\min \left( \gamma_k \cdot \gamma_{D2} \right)}{1 + \gamma_{E2}} \right) \right]^+$$

(15)

where $\left[ x \right]^+ = \max \{ x, 0 \}$.

3. SECRECY PERFORMANCE ANALYSIS

In NOMA systems, with the help of a relay two signals are transmitted from the source to $D_1$ and $D_2$, respectively. As a result, outage happens when either $C_1$ or $C_2$ falls below their own target rates. By exploiting this definition, the secure outage probability (SOP) can be formulated as following sections:

3.1. SOP at $D_1$

$$P_{SOP_1} = \text{Pr} \left( C_i < R_i \right)$$

$$= 1 - \text{Pr} \left( \frac{a_1 \rho_3 \left| h_{ab} \right|^2}{a_2 \rho_3 \left| h_{ab} \right|^2 + 1} > \theta \left| h_{ab} \right|^2 + \alpha_1 \right) \times \text{Pr} \left( \frac{h_{bD2}^2 \beta \rho_h}{h_{bD2}^2 \beta \rho_e + 1} > \theta \left| h_{bD2} \right|^2 + \alpha_2 \right)$$

(16)

where $\theta = 2^{2R_i} \beta \rho_h, \alpha_1 = 2^{2R_i} - 1$.

Firstly, $A$ can be written by:

$$A = \text{Pr} \left( \left| h_{ab} \right|^2 \geq \frac{\theta \left| h_{ab} \right|^2 + \alpha_1}{a_2 \rho_3} a_2 \rho_3 - \rho_3 \right) + \text{Pr} \left( \left| h_{ab} \right|^2 \geq \frac{\theta \left| h_{ab} \right|^2 + \alpha_2}{a_2 \rho_3} a_2 \rho_3 - \rho_3 \right)$$

we have $A$ as:
\( A_1 = \Pr \left( |h_{SR}|^2 \geq \frac{\theta \| h_{RE} \|^2 + \alpha_1}{\alpha_2 \beta_2 - (\theta \| h_{RE} \|^2 + \alpha_1) \alpha_2 \beta_2}, |h_{SR}|^2 < \frac{\rho_2}{\rho_2} \right) \)

provided that \( |h_{RE}|^2 < \frac{\alpha_1 - \alpha_2 \alpha_1}{\alpha_2 \theta} \), then \( A_1 \) can be calculated as:

\[
A_1 = \int_0^{\rho_2} f_{|h_{RE}|^2}(x) \int_0^{\frac{\alpha_1 - \alpha_2 \alpha_1}{\alpha_2 \theta}} f_{|h_{RE}|^2}(y) \int_0^{\frac{\theta + \alpha_1}{\alpha_2 \theta}} f_{|h_{SR}|^2}(z) \, dx \, dy \, dz
\]

\[
= \left(1 - e^{-\frac{\rho_2}{\lambda_{RE}}} \right) \int_0^{\frac{\alpha_1 - \alpha_2 \alpha_1}{\alpha_2 \theta}} e^{-\frac{y}{\lambda_{RE}}} e^{-\frac{\theta + \alpha_1}{\alpha_2 \theta}} dy
\]

where \( u = \alpha_1 - \alpha_2 \alpha_1, v = \alpha_2 \theta \), we have:

\[
A_1 = \left(1 - e^{-\frac{\rho_2}{\lambda_{RE}}} \right) e^{-\frac{u}{\lambda_{RE}}} e^{-\frac{\theta}{\lambda_{RE}}} \xi_1
\]

(17)

where \( \xi_1 = \int_0^u e^{-\frac{\alpha_1 - \alpha_2 \alpha_1}{\alpha_2 \theta}} \frac{\theta}{\lambda_{RE}} dq \).

Similarly, \( A_1 \), we can calculated \( A_2 \) as:

\[
A_2 = \frac{1}{\lambda_{RE}} e^{-\frac{\rho_2}{\lambda_{RE}}} e^{-\frac{u}{\lambda_{RE}}} e^{-\frac{\theta}{\lambda_{RE}}} \xi_2
\]

(18)

where \( \xi_2 = \int_0^u \frac{q\lambda_{SR}}{q \rho \lambda_{SR} \lambda_{SP} + \lambda_{SR} (\theta u - \theta q + \alpha_1)} e^{-\frac{\alpha_1 - \alpha_2 \alpha_1}{\alpha_2 \theta}} \frac{\theta}{\lambda_{RE}} dq \).

From (17) and (18) we find \( A \) by:

\[
A = \left(1 - e^{-\frac{\rho_2}{\lambda_{RE}}} \right) e^{-\frac{u}{\lambda_{RE}}} e^{-\frac{\theta}{\lambda_{RE}}} \xi_1 + \frac{1}{\lambda_{RE}} e^{-\frac{\rho_2}{\lambda_{RE}}} e^{-\frac{u}{\lambda_{RE}}} e^{-\frac{\theta}{\lambda_{RE}}} \xi_2
\]

(19)

the secondly, \( B \) can be written as:

\[
B = \Pr \left( |h_{SR}|^2 > \frac{\theta \| h_{RE} \|^2 + \alpha_1}{\beta_1 - \alpha_1 \beta_2 - \beta_2 \theta \| h_{RE} \|^2} \rho_R \right)
\]
provided that \( |h_{\text{rel}}| < \frac{\beta_2 - \alpha_1 \beta_2}{\theta \beta_2} \), \( B \) calculated as:

\[
B = \int_{0}^{\infty} e^{-\frac{\beta_2 - \alpha_1 \beta_2}{\theta \beta_2}} f_{h_{\text{rel}}} (x) \int_{0}^{\alpha_1 + \alpha_2} f_{\theta_{\text{rel}}} (y) \, dy \, dx = \frac{1}{\lambda_{\text{RE}}} \int_{0}^{\infty} e^{-\frac{\beta_2 - \alpha_1 \beta_2}{\theta \beta_2}} e^{-\frac{\theta_1 + \alpha_2}{\theta_{\text{rel}}}} \left( \frac{\beta_2 - \alpha_1 \beta_2}{\theta \beta_2} \right) \, dx
\]

where \( n = \beta_1 - \alpha_1 \beta_2, m = \theta \beta_2 \), we have:

\[
B = \frac{\lambda_{\text{RE}}}{\theta \beta_2} \int_{0}^{\infty} e^{-\frac{\beta_1 - \alpha_1 \beta_2}{\theta \beta_2}} e^{-\frac{\theta_1 + \alpha_2}{\theta_{\text{rel}}}} \, dx
\]

let \( t = n - mx \Leftrightarrow x = \frac{n-t}{m} \Leftrightarrow dx = \frac{dt}{-m} \). We have:

\[
B = e^{\frac{n - \theta \lambda_{\text{RE}}}{m \theta_{\text{rel}}}} \partial_1
\]

where \( \partial_1 = \int_{0}^{\infty} e^{-\frac{\theta_1 + \alpha_2}{\theta_{\text{rel}}}} e^{\frac{\theta_1 + \alpha_2}{m \theta_{\text{rel}}}} \, dt \).

Similar (20), we can calculated \( C \) as:

\[
C = e^{\frac{n - \theta \lambda_{\text{RE}}}{m \theta_{\text{rel}}}} \partial_2
\]

where \( \partial_2 = \int_{0}^{\infty} e^{-\frac{\theta_1 + \alpha_2}{\theta_{\text{rel}}}} e^{\frac{\theta_1 + \alpha_2}{m \theta_{\text{rel}}}} \, dt \).

From (19), (20) and (21) we calculated \( P_{\text{SOP}_1} \) as:

\[
P_{\text{SOP}_1} = 1 - \left[ 1 - e^{\frac{\beta + \lambda_{\text{RE}}}{\gamma \lambda_{\text{RE}}}} e^{\frac{\theta_1 + \alpha_2}{\theta_{\text{rel}}}} e^{-\frac{u \lambda_{\text{RE}}}{\gamma \lambda_{\text{RE}}}} \right] \frac{\lambda_{\text{RE}}}{\theta_{\text{rel}}} \partial_1 + \left[ e^{\frac{\beta + \lambda_{\text{RE}}}{\gamma \lambda_{\text{RE}}}} e^{\frac{\theta_1 + \alpha_2}{\theta_{\text{rel}}}} e^{-\frac{u \lambda_{\text{RE}}}{\gamma \lambda_{\text{RE}}}} \right] \frac{\lambda_{\text{RE}}}{\theta_{\text{rel}}} \partial_2
\]

(22)

3.2. SOP at D2

By definition, we have SOP as:

\[
P_{\text{SOP}_2} = \Pr \left( C < R_2 \right)
\]

\[
= 1 - \Pr \left( \alpha_1 \beta_3 |h_{xR}|^2 < \psi |h_{\text{rel}}|^2 + \omega_k \right) \Pr \left( \beta_2 \rho_{\text{rel}} |h_{zR}|^2 > \psi |h_{\text{rel}}|^2 + \omega_k \right)
\]

(23)

where \( \psi = 2^{2\rho} \beta_2 \rho_{\text{rel}}, \omega_k = 2^{2\rho_k} - 1 \). Firstly, \( D \) can be rewritten as:

\[
D = \Pr \left( \frac{a_1 \beta_3 |h_{xR}|^2 + \omega_k |h_{zR}|^2}{\beta_3} < \frac{\rho_{\text{rel}}}{\beta_3} \right) + \Pr \left( \frac{a_2 \beta_3 |h_{xR}|^2}{|h_{xR}|^2} > \psi |h_{\text{rel}}|^2 + \omega_k |h_{zR}|^2 > \frac{\rho_{\text{rel}}}{\beta_3} \right)
\]
let \( \beta = \frac{1}{a} \), \( D_1 \) can be computed as:

\[
D_1 = \Pr \left( |h_{SR}|^2 > \frac{\psi \sigma}{h_{RE}} |h_{SR}|^2 + \alpha_2 |h_{SP}|^2 < \frac{P_1}{\lambda_{SR}} \right) = \left( 1 - e^{-\frac{\lambda_{SR}}{\psi \sigma \lambda_{SR} \beta}} \right) e^{-\frac{\alpha_2 \sigma}{\lambda_{SR} \beta}} \left( \frac{\lambda_{RE} \psi \sigma}{\lambda_{SR}} + 1 \right)^{-1} \tag{24}
\]

next, let \( \alpha = \frac{1}{a} \), \( D_2 \) can calculated as:

\[
D_2 = \Pr \left( |h_{SR}|^2 > \frac{\psi \sigma}{h_{RE}} |h_{SR}|^2 + \alpha_2 |h_{SP}|^2 > \frac{P_1}{\lambda_{SR}} \right) = e^{\frac{\lambda_{SR}}{\psi \sigma \lambda_{SR} \beta}} \left( e^{\frac{1}{\lambda_{SR} \beta}} \lambda_{RE} \psi \sigma \lambda_{SR} \beta \right)^{\frac{\lambda_{SR}}{\psi \sigma \lambda_{SR} \beta}} (x + \frac{\lambda_{SR} + \lambda_{SP} \alpha_2}{\psi \lambda_{SR} \beta}) dx
\]

Let \( \beta = \frac{\lambda_{SR} + \lambda_{SP} \alpha_2}{\psi \lambda_{SR} \beta} \), \( \mu = \left( \frac{1}{\lambda_{RE} \lambda_{SR} \beta} \right) \), we have \( D_2 \)

\[
D_2 = e^{\frac{\lambda_{SR}}{\psi \sigma \lambda_{SR} \beta}} \left( e^{\frac{1}{\lambda_{SR} \beta}} \lambda_{RE} \psi \sigma \lambda_{SR} \beta \right)^{\frac{\lambda_{SR}}{\psi \sigma \lambda_{SR} \beta}} (x + \beta) e^{\frac{\lambda_{SR}}{\psi \sigma \lambda_{SR} \beta}} \left( \frac{\lambda_{RE} \psi \sigma}{\lambda_{SR}} + 1 \right)^{-1} \tag{25}
\]

from (22) and (23) \( D \) can be as:

\[
D = \left( 1 - e^{\frac{\lambda_{RE}}{\psi \sigma \beta}} \right) e^{\frac{\lambda_{RE} \psi \sigma}{\lambda_{SR}} \left( \frac{\lambda_{RE} \psi \sigma}{\lambda_{SR}} + 1 \right)^{-1}} + e^{\frac{\lambda_{RE}}{\psi \sigma \beta}} \left( \frac{\lambda_{RE} \psi \sigma}{\lambda_{SR}} + 1 \right)^{-1} \tag{26}
\]

next, with \( \beta = \frac{1}{\beta_{PR}} \) \( E \) can be calculated as:

\[
E = \int_0^\infty \int_0^\infty \frac{f_{|h_{SR}|^2}}{f_{|h_{RE}|^2}} \frac{f_{|h_{SP}|^2}}{f_{|h_{SP}|^2}} (x) dy = \frac{\lambda_{RD2}}{\psi \beta \lambda_{RE} + \lambda_{RD2} e^{\mu \beta}} \tag{27}
\]

from (24) and (25) it can be calculated \( P_{SOP2} \) as:

\[
P_{SOP2} = 1 - \frac{\lambda_{RD2}}{\psi \beta \lambda_{RE} + \lambda_{RD2}} e^{\frac{\alpha_2 \sigma}{\lambda_{SR} \beta}} \left( 1 - e^{\frac{\lambda_{RE} \psi \sigma}{\lambda_{SR} \beta}} \left( \frac{\lambda_{RE} \psi \sigma}{\lambda_{SR}} + 1 \right)^{-1} \right) - \frac{\lambda_{SR} \lambda_{RD2}}{\psi \beta \lambda_{RE} \lambda_{SR} \beta} e^{\mu \beta} \tag{28}
\]

4. NUMBER RESULTS

This section of this study represents numerical and simulation results for the SOP over related Rayleigh fading channels. The adopted system parameters are given in each figure. We evaluate the impact of target rates on the secrecy outage performance for NOMA-based cognitive radio as in Figure 2. Higher target rates result in worse SOP performance. It can be seen performance gap among two signals is large at \( R_1 = R_2 = 0.5 \). The reason is that different power allocation factors for each signal leads to different SOP
performance. In other observation, impact of interference $\rho_\varphi = 10, 15, 20 \, (dB)$ to secure performance of two signals can be seen as Figure 3. It can be confirmed lower interference provides better secure performance. Such performance gap will be reduced at $R_1 = R_2 = 1$. The analytical values of the OP for $x_1, x_2$ with various target rates and SNR threshold values are shown in Figure 4. It is observed that curves of the OP improve by increasing the transmit SNR. It is worth noting that no ICT case exhibits better secure performance.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure2}
\caption{SOP versus transmit SNR with different $\rho_\varphi$ ($\alpha_1 = \beta_1 = 0.9, \alpha_2 = \beta_2 = 0.1, \rho_1 = 15dB$, $\rho_\varphi = 5dB$, $\lambda_{xy} = 0.1, \lambda_{xy} = 1, \lambda_{y21} = 0.9, \lambda_{y22} = 0.6$ and $\lambda_{x2} = 0.1$)}
\end{figure}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure3}
\caption{SOP versus transmit SNR with different $\rho_\varphi$ ($\alpha_1 = \beta_1 = 0.9, \alpha_2 = \beta_2 = 0.1, \rho_1 = 15dB$, $\rho_\varphi = 5dB$, $\lambda_{xy} = 0.1, \lambda_{xy} = 1, \lambda_{y21} = 0.9, \lambda_{y22} = 0.6$ and $\lambda_{x2} = 0.1$)}
\end{figure}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure4}
\caption{SOP versus transmit SNR as ICT consideration ($\alpha_1 = \beta_1 = 0.9, \alpha_2 = \beta_2 = 0.1, \rho_1 = 15dB$, $\rho_\varphi = 5dB$, $\lambda_{xy} = 0.1, \lambda_{xy} = 1, \lambda_{y21} = 0.9, \lambda_{y22} = 0.6$ and $\lambda_{x2} = 0.1$)}
\end{figure}

5. **CONCLUSION**

In this paper, in order to evaluate security performance of CR-NOMA systems, SOP performance in condition of fixed power allocation scheme is examined. A limitation of transmit power at the secondary in CR-NOMA results in varying secure performance. The threshold data rates and impact of interference from the primary network are main factors affecting to system performance.
REFERENCES


