Exact secure outage probability performance of uplink-downlink multiple access network under imperfect CSI

Dinh-Thuan Do, Minh-Sang Van Nguyen
Department of Electronics and Communications, Faculty of Electronics Technology, Industrial University of Ho Chi Minh City (IUH), Vietnam

Article Info
Article history:
Received Mar 18, 2021
Revised Aug 6, 2021
Accepted Oct 13, 2021

Keywords:
Channel state information
Non-orthogonal multiple access
Secure performance

ABSTRACT
In this paper, we study uplink-downlink non-orthogonal multiple access (NOMA) systems by considering the secure performance at the physical layer. In the considered system model, the base station acts a relay to allow two users at the left side communicate with two users at the right side. By considering imperfect channel state information (CSI), the secure performance need be studied since an eavesdropper wants to overhear signals processed at the downlink. To provide secure performance metric, we derive exact expressions of secrecy outage probability (SOP) and evaluating the impacts of main parameters on SOP metric. The important finding is that we can achieve the higher secrecy performance at high signal to noise ratio (SNR). Moreover, the numerical results demonstrate that the SOP tends to a constant at high SNR. Finally, our results show that the power allocation factors, target rates are main factors affecting to the secrecy performance of considered uplink-downlink NOMA systems.

1. INTRODUCTION
Due to high demands in terms of system capacity and spectrum efficiency, the traditional orthogonal multiple access (OMA) has been unable to meet the user needs associated with the rapid growth of internet of things (IoT) and mobile communications [1]–[7]. In order to meet the heavy demand for mobile services, non-orthogonal multiple access (NOMA) is researched in recent years with promising applications [8], [9]. In some scenarios, NOMA benefits to device-to-device communications [10], [11] and cognitive radio (CR)-aided NOMA [12]-[14] and these are considered as potential key technologies for the fifth generation mobile communications (5G). The authors Do, et al. in [13] studied the secondary network of the considered CR-NOMA by enabling the relaying scheme. In such network, the secondary transmitter is able to conduct energy harvesting (EH) to perform signal forwarding to distant secondary users. Two main metrics including outage behavior and throughput performance are studied in the context of EH-assisted CR-NOMA while imperfect successive interference cancellation (SIC) is considered. Reference Do, et al. [14] presented relay-aided CR-NOMA networks to improve the performance of far users by enabling partial relay selection architecture. They explored system performance in terms of full-duplex (FD) and half duplex (HD) relays for both uplink and downlink communications.

Recently, an alternative approach is enabled to conduct cryptography at physical layer security (PLS)
has considered. This method is more advanced due to complications of secure techniques applied at higher layers in existing RFID systems. To aim to decrease chance of eavesdroppers getting information from the legal transmitter, the wireless channel characteristics is utilized to PLS-based system act relevant approach to against eavesdroppers’ overhearing operations. The authors in [15]-[20] studied PLS applied for a 5G NOMA system. The authors in [15] explored the two-user case and then extend our results to a multi-user case. The main results indicated that the given users’ data rate corresponds to positive secrecy rate. The PLS of millimeter wave (mmWave) NOMA networks was studied for mmWave channels in [16] by examining imperfect CSI at receivers and the limited scattering characteristics of concerned channels. the formula of the secrecy outage probability (SOP) was derived since the system adopts random distributions of legitimate users and eavesdroppers. While [15], [16] presented NOMA downlink scenario, the authors in [18] investigated uplink secure NOMA system. The typical system including one base station, one eavesdropper and multiple users. However, there is lack of work considering secure performance of uplink-downlink NOMA system under imperfect CSI circumstance, which motive us to study secure outage probability in this article.

2. SYSTEM MODEL

In this system model, we consider uplink-downlink of two pairs of source-destination $S_1-D_1, S_2-D_2$ under existence of eavesdropper $E$, shown in Figure 1. The flat slow Rayleigh fading is assumed for all links and the channel coefficients pertaining to the links $S_1 \rightarrow R, S_2 \rightarrow R, R \rightarrow D_1, R \rightarrow D_2$ and $R \rightarrow E$ are denoted as $g_{1r}, g_{2r}, g_{dl_1}, g_{dl_2}$ and $g_e$, respectively. Accordingly, the corresponding channel power gains conform to $|g_{1r}|^2 \sim CN(0, \lambda_{1r}), |g_{2r}|^2 \sim CN(0, \lambda_{2r}), |g_{dl_1}|^2 \sim CN(0, \lambda_{d1}), |g_{dl_2}|^2 \sim CN(0, \lambda_{d2})$ and $|g_e|^2 \sim CN(0, \lambda_e)$, respectively.

![System model](Figure 1. System model)

Two sources sends their signals to the relay $R$ in the same time. In particular, the received signal at $R$ can be expressed as [21].

$$y_{S-R} = (g_{1r} + h_1r) \sqrt{a_1P_{s1}}z_1 + (g_{2r} + h_2r) \sqrt{a_2P_{s2}}z_2 + n_r,$$

where $P_{s1}$ represents the transmit power at $S_1$; $n_r$ is denoted as the variance of the additive white Gaussian noise (AWGN) at $R$ with $n_r \sim CN(0, N_0)$; $z_i$ is the signal of $D_i$; $a_i$ are the power allocation coefficients of $z_i$ transmitted signals with $a_1 + a_2 = 1$ and assuming that $a_1 > a_2$; $h_{ir}$ is the error term related to imperfect CSI, which follow a complex Gaussian distributed random variable with $CN(0, \sigma_{hi}^2)$. In this circumstance, $\sigma_{hi}^2$ is assumed as constant [22].

With regard to higher priority, the relay always first decodes $z_1$ by considering $z_2$ as noise. Following NOMA principle, the system can performs SIC to decode $z_2$. To further compute system performance metric, we first calculaye the received signal-to-interference-plus-noise ratio (SINR) for symbol $z_1$. Then, we can
determine the signal-to-noise (SNR) for symbol $z_2$. In particular, these values are given as,

$$
\gamma_{z_1}^u = \frac{a_1 \rho_s |g_{1r}|^2}{a_2 \rho_s |g_{2r}|^2 + a_1 \rho_s \sigma_i^2 + a_2 \rho_s \sigma_h^2 + 1},
\gamma_{z_2}^u = \frac{a_2 \rho_s |g_{2r}|^2}{a_1 \rho_s \sigma_i^2 + a_2 \rho_s \sigma_h^2 + 1}.
$$

(2)

where $\rho_s = \frac{P_s}{N_0}$, $\rho_s = \frac{P_s}{N_0}$ which represent SNR at sources.

Next, the SINR of $\gamma_{z_1}^d$ is computed in these steps. By processing signals transferred from $R$, $D_1$ decodes its intended symbol $z_1$ when it treats $z_2$ as noise. Then, we compute the achievable secrecy rates of $z_1$ at $D_1$ as,

$$
\gamma_{z_1}^d = \frac{a_1 \rho_s |g_{d1}|^2}{a_2 \rho_s |g_{d2}|^2 + \rho_s \sigma_{d1}^2 + 1}
$$

(4)

where $\rho_s = \frac{P_s}{N_0}$.

At the other side, user $D_2$ first decodes $z_1$ and then employing SIC to achieve signal $z_2$. At user $D_2$, the achievable secrecy rates of $z_1$ and the SNR of $z_2$ are expressed respectively by

$$
\gamma_{z_2}^d = \frac{a_2 \rho_s |g_{d2}|^2}{a_2 \rho_s |g_{d2}|^2 + \rho_s \sigma_{d2}^2 + 1},
\gamma_{z_2}^e = \frac{a_2 \rho_s |g_{d2}|^2}{\rho_s \sigma_{d2}^2 + 1}
$$

(5)

The received signal at $E$ from $R$ can be expressed as

$$
y_E = g_e \left( \sqrt{a_1 P_r} z_1 + \sqrt{a_2 P_r} z_2 \right) + n_e
$$

(6)

After employing the parallel interference cancellation (PIC) scheme, the received SINR at the eavesdropper to detect $D_i$’s message can be formulated by [23].

$$
\gamma_{z_i}^e = a_i \rho_e |g_e|^2
$$

(7)

where $\rho_e = \frac{P_e}{N_0}$.

In the next step, the achievable secrecy rates of two pairs of users can be examined. Following (2), (4), and (7), we compute the achievable secrecy rates of $S_1 - D_1$ as,

$$
\chi_1 = \frac{1}{2} \left[ \log_2 \min \left( \frac{1 + \gamma_{z_1}^u}{1 + \gamma_{z_1}^e}, \frac{1 + \gamma_{z_1}^d}{1 + \gamma_{z_1}^e} \right) \right]^+, \chi_2 = \frac{1}{2} \left[ \log_2 \min \left( \frac{1 + \gamma_{z_2}^d}{1 + \gamma_{z_2}^e}, \frac{1 + \gamma_{z_2}^d}{1 + \gamma_{z_2}^e} \right) \right]^+.
$$

(8)

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

From (2), (5) and (7), the achievable secrecy rates of $S_2 - D_2$ is written as,

$$
\chi_2 = \frac{1}{2} \left[ \log_2 \min \left( \frac{1 + \gamma_{z_2}^u}{1 + \gamma_{z_2}^e}, \frac{1 + \gamma_{z_2}^d}{1 + \gamma_{z_2}^e} \right) \right]^+.
$$

(9)

In the next section, we intends to examine secure performance metric which relies on secrecy rates obtained in these steps.
3. SECRECY OUTAGE PROBABILITY (SOP)

3.1. SOP for user pair $S_1 - D_1$

To evaluate SOP performance, the secrecy outage event $S_1 - D_1$ need be known when $z_1$ cannot be securely decoded by $R$ or by $D_1$, the SOP for $S_1 - D_1$ can be expressed as [23], [24].

$$SOP_{S_1 D_1} = Pr (\chi_1 < R_1) = 1 - Pr \left( \min \left( \frac{1 + \gamma_1^n}{1 + \gamma_1^n}, \frac{1 + \gamma_2^n}{1 + \gamma_2^n} \right) \geq \gamma_{d_1} \right) = 1 - \Pr \left( \frac{1 + \gamma_1^n}{1 + \gamma_2^n} \geq \gamma_{d_1} \right) \Pr \left( \frac{1 + \gamma_2^n}{1 + \gamma_2^n} \geq \gamma_{d_1} \right). \tag{10}$$

3.1.1. Proposition 1

The SOP of user pair $S_1 - D_1$ is approximated computed as.

$$SOP_{S_1 D_1} = 1 + \frac{\rho_{s_1} \lambda_{1r} \eta_1}{\gamma_{d_1} \rho_{s_1} \lambda_{1r} a_2 \rho_{s_2} \lambda_{2r}} \exp \left( \beta_1 \beta_2 - \frac{\phi_1 \kappa_1}{\alpha_1 \rho_{s_1} \lambda_{1r}} \right) Ei(-\beta_1 \beta_2), \tag{11}$$

where $\phi_1 = \gamma_{d_1} - 1, \gamma_{d_2} = 2^{R_1} (i = 1, 2), R_i$ is the target data rate for user $D_i, \kappa_1 = \alpha_1 \rho_{s_1} \lambda_{1r} a_2 \rho_{s_2} \lambda_{2r} + 1$, $\kappa_2 = \rho_2 \sigma_2^2 + 1, \eta_1 = \int \exp \left( - \frac{\kappa_2 \gamma_{d_1} a_2 \rho_{s_2} \lambda_{2r} + \phi_1 \kappa_2}{\alpha_1 \rho_{s_1} \lambda_{1r}} \right) dx, \beta_1 = \frac{\gamma_{d_1} \rho_{s_1} \lambda_{1r} a_2 \rho_{s_2} \lambda_{2r}}{\gamma_{d_1} \rho_{s_1} \lambda_{1r} a_2 \rho_{s_2} \lambda_{2r}}, \beta_2 = \frac{\phi_1 \sigma_2^2}{\alpha_1 \rho_{s_1} \lambda_{1r}} + \frac{1}{\chi_3}.$

3.1.2. Proof

From (10), $\Psi_1$ can be written by.

$$\Psi_1 = \Pr \left( \frac{1 + \gamma_1^n}{1 + \gamma_2^n} \geq \gamma_{d_1} \right) = \Pr \left( \gamma_2^n \geq \gamma_{d_1} \right)$$

$$= \Pr \left( |g_{1r}|^2 \geq \frac{\rho_{a_2 \rho_{s_2}} (|g_{2r}|^2 + \sigma_1^2 + \gamma_{d_1} \rho_{s_1} \lambda_{1r} |g_{1r}|^2)}{a_1 \rho_{s_1} \lambda_{1r}} \right)$$

$$= \int_0^\infty \int_0^\infty \left( 1 - F_{|g_1|^2} (x) F_{|g_2|^2} (y) \right) dxdy,$$  

where $\phi_1 = \gamma_{d_1} - 1$ and $\kappa_1 = \alpha_1 \rho_{s_1} \lambda_{1r} a_2 \rho_{s_2} \lambda_{2r} + 1$. By convolving the Rayleigh distribution with probability density function (PDF) and cumulative density function (CDF) $f_X (x) = \frac{1}{\sqrt{\pi x}} \exp \left( - \frac{x}{\lambda_3} \right), F_{|X|^2} (x) = 1 - \exp \left( - \frac{x}{\lambda_3} \right)$, $\Psi_1$ can be formulated by.

$$\Psi_1 = \int_0^\infty \int_0^\infty \exp \left( \frac{-\gamma_{d_1} a_1 \rho_{s_1} \lambda_{1r} |g_{2r}|^2 + \phi_1 \rho_{s_2} \lambda_{2r} y + \phi_1 \kappa_1}{a_1 \rho_{s_1} \lambda_{1r}} \right) \frac{1}{\sqrt{\pi x}} \exp \left( - \frac{x}{\lambda_3} \right) \frac{1}{\sqrt{\pi y}} \exp \left( - \frac{y}{\lambda_3} \right) dxdy$$

$$= \frac{1}{\chi_3} \frac{1}{\chi_3} \int_0^\infty \int_0^\infty \exp \left( \frac{-\phi_1 \kappa_1}{a_1 \rho_{s_1} \lambda_{1r}} \right) \frac{1}{\sqrt{\pi x}} \exp \left( - \frac{x}{\lambda_3} \right) \frac{1}{\sqrt{\pi y}} \exp \left( - \frac{y}{\lambda_3} \right) dxdy$$

$$= \frac{1}{\chi_3} \frac{1}{\chi_3} \int_0^\infty \int_0^\infty \exp \left( - \phi_1 \kappa_1 \frac{1}{a_1 \rho_{s_1} \lambda_{1r}} \right) \frac{1}{\sqrt{\pi x}} \exp \left( - \frac{x}{\lambda_3} \right) \frac{1}{\sqrt{\pi y}} \exp \left( - \frac{y}{\lambda_3} \right) dxdy.$$  

\begin{equation} \tag{13}
\end{equation}

By applying some polynomial expansion manipulations and based on [25] (3.352.4) a5, we obtain $\Psi_1$ as.

$$\Psi_1 = - \frac{\rho_{s_1} \lambda_{1r}}{\gamma_{d_1} \rho_{s_1} \lambda_{1r} a_2 \rho_{s_2} \lambda_{2r}} \exp \left( \beta_1 \beta_2 - \frac{\phi_1 \kappa_1}{a_1 \rho_{s_1} \lambda_{1r}} \right) Ei(-\beta_1 \beta_2), \tag{14}$$

where $\beta_1 = \frac{\gamma_{d_1} \rho_{s_1} \lambda_{1r} a_2 \rho_{s_2} \lambda_{2r}}{\gamma_{d_1} \rho_{s_1} \lambda_{1r} a_2 \rho_{s_2} \lambda_{2r}}, \beta_2 = \frac{\phi_1 \sigma_2^2}{a_1 \rho_{s_1} \lambda_{1r}} + \frac{1}{\chi_3}.$
From (10), \( \Psi_2 \) can be written by
\[
\Psi_2 = \Pr \left( \frac{1+\gamma'^2}{\kappa_2} \geq \gamma_{d_1} \right) \\
= \Pr \left( g_{d_1}^2 \geq \phi_1 + \gamma_{d_1} \gamma_{z_1}^2 \right) \\
= \Pr \left( |g_{d_1}|^2 \geq \frac{\kappa_2 \gamma_{d_1} \gamma_{d_1} \rho_x \phi \kappa_2}{(a_1 - a_2 \gamma_{d_1} \gamma_{d_1} \rho_x \phi \kappa_2)} \right) \\
= \int_{0}^{\infty} \left( 1 - F_{|g_{d_1}|^2} \left( \frac{\kappa_2 \gamma_{d_1} \gamma_{d_1} \rho_x \phi \kappa_2}{(a_1 - a_2 \gamma_{d_1} \gamma_{d_1} \rho_x \phi \kappa_2)} \right) \right) f_{|g_{d_1}|^2} (x) \, dx \\
= \int_{0}^{\infty} \exp \left( - \frac{\kappa_2 \gamma_{d_1} \gamma_{d_1} \rho_x \phi \kappa_2}{(a_1 - a_2 \gamma_{d_1} \gamma_{d_1} \rho_x \phi \kappa_2)} - \frac{x}{\kappa_2} \right) \, dx 
\]
where \( \kappa_2 = \rho_x \sigma^2 + 1 \).

It completes the proof.

3.2. SOP for \( S_2 - D_2 \)

Similar the user pair \( S_1 - D_1 \), we need examine the secrecy outage event for user pair \( S_2 - D_2 \). Several cases are examined such as \( R \) cannot detect \( z_2 \), \( D_2 \) cannot detect its own message \( z_2 \) when \( D_1 \) can detect \( z_1 \) successfully. As a result, we compute the SOP for user pair \( S_2 - D_2 \) as.

\[
SOP_{D_2} = Pr \left( \chi_2 < R \right) = 1 - \Pr \left( \min \left( \frac{1+\gamma''}{1+\gamma''}, \frac{1+\gamma''}{1+\gamma''}, \frac{1+\gamma''}{1+\gamma''} \right) \right) \\
= 1 - \Pr \left( \frac{1+\gamma''}{1+\gamma''} \geq \gamma_{d_2} \right) \Pr \left( \frac{1+\gamma''}{1+\gamma''} \geq \gamma_{d_2} \right) \Pr \left( \frac{1+\gamma''}{1+\gamma''} \geq \gamma_{d_2} \right) 
\]

3.2.1. Proposition 2

The exact SOP for user pair \( S_2 - D_2 \) is calculated by.

\[
SOP_{D_2} = 1 - \frac{a_2 \rho_x \lambda_{r_2}}{\kappa_1 \gamma_{d_2} \gamma_{d_2} \gamma_{d_2} + a_2 \rho_x \lambda_{r_2} \gamma_{d_2} \gamma_{d_2} + a_2 \rho_x \lambda_{r_2} \gamma_{d_2} \gamma_{d_2}} \exp \left( - \frac{\kappa_2 \phi_2}{a_2 \rho_x \lambda_{r_2} \gamma_{d_2} \gamma_{d_2}} \right) 
\]
where \( \kappa_2 = \rho_x \sigma^2 + 1, \eta_2 = \int_{0}^{\infty} \exp \left( - \frac{\kappa_2 \phi_2}{a_2 \rho_x \lambda_{r_2} \gamma_{d_2} \gamma_{d_2}} - \frac{x}{\kappa_2} \right) \, dx. \)

3.2.2. Proof

From (16), \( \Phi_1 \) can be calculated as.

\[
\Phi_1 = \Pr \left( \frac{1+\gamma''}{1+\gamma''} \geq \gamma_{d_2} \right) = \Pr \left( g_{d_2}^2 \geq \phi_2 + \gamma_{d_2} \gamma_{d_2} \gamma_{z_1}^2 \right) \\
= \Pr \left( |g_{d_2}|^2 \geq \frac{\kappa_2 \phi_2 + \kappa_2 \gamma_{d_2} \gamma_{d_2} \rho_x \phi \kappa_2}{a_2 \rho_x \phi} \right) \\
= \int_{0}^{\infty} \left( 1 - F_{|g_{d_2}|^2} \left( \frac{\kappa_2 \phi_2 + \kappa_2 \gamma_{d_2} \gamma_{d_2} \rho_x \phi \kappa_2}{a_2 \rho_x \phi} \right) \right) f_{|g_{d_2}|^2} (x) \, dx \\
= \frac{1}{\kappa_2} \exp \left( - \frac{\kappa_2 \phi_2}{a_2 \rho_x \phi \gamma_{d_2} \gamma_{d_2}} \right) \int_{0}^{\infty} \exp \left( - \frac{\kappa_2 \gamma_{d_2} \gamma_{d_2} \rho_x \phi \kappa_2}{a_2 \rho_x \phi \gamma_{d_2} \gamma_{d_2}} + \frac{1}{\kappa_2} \right) x \, dx 
\]
where \( \phi_2 = \gamma_{d_2} - 1 \).
Next, $\Phi_2$ can be computed as.
\[
\Phi_2 = \Pr \left( \frac{1+\gamma_2^d}{1+\gamma_2^d} \geq \gamma_d \right) \\
= \Pr \left( \gamma_2^d \geq \phi_2 + \gamma_d \gamma_2^d \right) \\
= \Pr \left( |g_2|^2 \geq \frac{\kappa_3(\phi_2 + \gamma_d \phi_2, \lambda_2, \rho_r, \lambda_{R2})}{(a_1-a_2 \phi_2-\gamma_d a_2 \phi_2, \rho_r, \lambda_{R1})} \right) \\
= f_0 \int_0^\infty \left( 1 - F_{|g_2|^2} \left( \frac{\kappa_3(\phi_2 + \gamma_d \phi_2, \lambda_2, \rho_r, \lambda_{R2})}{(a_1-a_2 \phi_2-\gamma_d a_2 \phi_2, \rho_r, \lambda_{R1})} \right) \right) f_{|g_2|^2}(x) \, dx \\
= \frac{1}{\kappa_3} \int_0^\infty \exp \left( - \frac{\kappa_3 \phi_2}{a_2 \rho_r \lambda_{D2}} \right) \int_0^\infty \exp \left( - \frac{\kappa_3 \gamma_d \phi_2}{a_2 \rho_r \lambda_{R2}} \right) \, dx,
\]
where $\kappa_3 = \rho_r \sigma_{d2}^2 + 1$.

Using result from (16), $\Phi_3$ is expressed by.
\[
\Phi_3 = \Pr \left( \frac{1+\gamma_3^d}{1+\gamma_3^d} \geq \gamma_d \right) \\
= \Pr \left( \gamma_3^d \geq \phi_2 + \gamma_d \gamma_3^d \right) \\
= \Pr \left( |g_3|^2 \geq \frac{\kappa_3(\phi_2 + \gamma_d \phi_2, \lambda_3, \rho_r, \lambda_{R2})}{(a_1-a_2 \phi_2-\gamma_d a_2 \phi_2, \rho_r, \lambda_{R1})} \right) \\
= f_0 \int_0^\infty \left( 1 - F_{|g_3|^2} \left( \frac{\kappa_3(\phi_2 + \gamma_d \phi_2, \lambda_3, \rho_r, \lambda_{R2})}{(a_1-a_2 \phi_2-\gamma_d a_2 \phi_2, \rho_r, \lambda_{R1})} \right) \right) f_{|g_3|^2}(x) \, dx \\
= \frac{1}{\kappa_3} \int_0^\infty \exp \left( - \frac{\kappa_3 \phi_2}{a_3 \rho_r \lambda_{D2}} \right) \int_0^\infty \exp \left( - \frac{\kappa_3 \gamma_d \phi_2}{a_3 \rho_r \lambda_{R2}} \right) \, dx.
\]
This is end of the proof.

4. SIMULATION RESULTS

To conduct these simulations, we set $\rho = \rho_{S1} = \rho_{S2} = \rho_r$, $\sigma = \sigma_{h1} = \sigma_{h2} = \sigma_{d1} = \sigma_{d2}$. In Figure 2, we show the SOP versus transmit SNR at the source. It can be seen clearly that higher transmit power at the source will enhance SOP performance, especially in high SNR region. By assigning different power allocation factors, the second user pair $S_2 - D_2$ outperforms that of $S_1 - D_1$ when SNR is greater than 20 dB. The higher power factor $\alpha_1 = 0.9$ leads to improvement of SOP for $S_1 - D_1$. Similarly, we evaluate the impact of rates $R_1 < R_2$ on SOP performance, shown in Figure 3. The lower requirement of target rates indicate the best SOP among three cases of $R_1 < R_2$ examined. In Figure 4, we can see similar SOP performance for two user pairs when we change $\sigma$. It can be concluded that the quality of channels make influence on SOP metric.

![Figure 2. SOP for $S_1 - D_1$ and $S_2 - D_2$ versus $\rho$ as changing $\alpha_1$ with $R_1 = R_2 = 1$ (bps/Hz), $\sigma = 0.001$, $\lambda_{1r} = \lambda_{2r} = 1$, $\lambda_{d2} = 2$, $\lambda_c = 1$, $\rho_c = -20$ (dB)](image1)

![Figure 3. SOP for $S_1 - D_1$ and $S_2 - D_2$ versus $\rho$ as changing $R_1 = R_2$ with $\alpha_1 = 0.9$, $\sigma = 0.001$, $\lambda_{1r} = \lambda_{2r} = 1$, $\lambda_{d2} = 2$, $\lambda_c = 1$, $\rho_c = -20$ (dB)](image2)

Exact secure outage probability performance of uplink-downlink multiple access network ... (Dinh-Thuan Do)
5. CONCLUSION

This paper investigates the joint uplink and downlink approach to evaluate SOP performance of two user pairs. By assigning fixed power allocation, we can derive exact formulas of SOP for two user pairs. Specifically, we can conclude that SOP will be enhanced at high transmit power at the sources. We further examine the impacts of target rate on SOP performance. Under the existence of eavesdropper, we guarantee operation of uplink-downlink if we control the quality of channels. Furthermore, we have found that the imperfect CSI has slight impact on SOP performance.

REFERENCES


