Secrecy Outage Probability Analysis for Downlink NOMA with Imperfect SIC at Untrusted Users

Sapna Thapar[1], Insha Amin[1], Deepak Mishra[2], and Ravikant Saini[1]
[1]Department of Electrical Engineering, Indian Institute of Technology Jammu, India
[2]School of Electrical Engineering and Telecommunications, University of New South Wales, Australia
Emails: thaparsapna25@gmail.com, 2018ree0052@iitjammu.ac.in, d.mishra@unsw.edu.au, ravikant.saini@iitjammu.ac.in

***Abstract*—Non-orthogonal multiple access (NOMA) has come to the fore as a spectrally efficient technique for fifth-generation networks and beyond. At the same time, NOMA faces severe security issues in the presence of untrusted users due to successive interference cancellation (SIC)-based decoding at receivers. In this paper, to make the system model more realistic, we consider the impact of imperfect SIC during the decoding process. Assuming the downlink mode, we focus on designing a secure NOMA communication protocol for the considered system model with two untrusted users. In this regard, we obtain the power allocation bounds to achieve a positive secrecy rate for both near and far users. Analytical expressions of secrecy outage probability (SOP) for both users are derived to analyze secrecy performance. Closed-form approximations of SOPs are also provided to gain analytical insights. Lastly, numerical results have been presented, which validate the exactness of the analysis and reveal the effect of various key parameters on achieved secrecy performance.**

I. Introduction

Non-orthogonal multiple access (NOMA) has been perceived as a promising enabling technology for fifth-generation (5G) wireless networks and beyond, as it entertains the possibility of serving more users in limited available resources [1]. At the same time, the broadcast nature of NOMA poses a security problem as the signal is vulnerable to eavesdropping. The use of physical layer security (PLS) has sparked widespread interest in solving the security concerns of the information-carrying signal in wireless communication. Therefore, achieving secure NOMA communication by utilizing the potential of PLS is a promising area of research [2].

A. Related Works

Based on the concept of PLS, existing works have the prior objective of securing the information-carrying signal against external eavesdroppers [2]. Additionally, the users who share the same resource block in NOMA may be untrusted, thereby making it compulsory to provide secrecy against internal eavesdropping. An untrusted users' scenario is a hostile situation where no users have mutual trust amongst each other, and therefore, they focus on securing their data from others [3], [4]. In this regard, [5], [6] have considered the secrecy issue of only near user against the far untrusted user. However, a robust NOMA system should be designed such that even the far user is provided secrecy against the near untrusted user. Based on this, [7] proposed a PLS design for NOMA with a stronger near untrusted user. In [8], a directional demodulation approach is followed to protect the data of weak user from an untrusted strong user. In [9], a linear precoding technique is proposed to prevent NOMA users from eavesdropping on each other. In [4], [10], a novel secure decoding order is suggested to provide positive secrecy rate for both strong and weak users. In [11], feasible secure decoding orders are investigated to ensure a positive secrecy rate for all users in an N-user system.

B. Research Gap and Motivation

A common assumption in [7]-[10] is that perfect successive interference cancellation (SIC) is performed by the receivers. Here, the interference from the decoded users is cancelled altogether while decoding later users. However, this might not be a realistic approach due to practical implementation problems such as decoding errors and complexity scaling [12]. Consequently, imperfect SIC, where the residual interference (RI) from incorrectly decoded users remains while decoding later users, would be a practical model [12], [13]. In NOMA literature, researchers have assumed either a fixed value of RI [14], [15] or considered RI as a linear function of the interfering power [12], [13]. However, in the direction of untrusted NOMA security, imperfect SIC has not received much focus yet. In [4], secrecy outage probability (SOP) of an untrusted NOMA system has been analyzed with a fixed RI value, which is a strong unrealistic assumption. In contrast, the linear model can more effectively represent the relationship between RI and power of the received signal. In [11], though the linear SIC model has been considered, no SOP analysis has been done. *Hence, to analyze the realistic impact of imperfect SIC, we investigate the secrecy performance analysis for a two-user untrusted NOMA system with linear SIC model, which to the best of our knowledge, has not been explored yet.*

C. Key Contributions

The key contributions of this work are summarized below: (1) Considering the impact of RI with linear imperfect SIC model in a two-user untrusted NOMA system, the power allocation (PA) bounds to achieve a positive secrecy rate for both users are investigated. (2) To analyze secrecy performance, the analytical expressions of SOP for both near and far users are derived. (3) The exact closed-form approximations of SOPs have also been obtained to attain analytical insights. (4) Numerical results have been provided to validate the analytical expressions, followed by insightful discussions on the impact of different key parameters on the system performance.

ISBN: 978-9-0827-9706-0

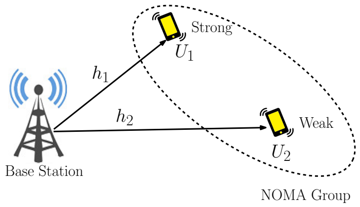


Fig. 1. Illustration of a downlink two-user untrusted NOMA system.

II. NOMA Transmission among Untrusted Users

Here we first present the system model. Then, the possible decoding orders for an untrusted NOMA system are discussed.

A. System Model and NOMA Principle

Downlink of a NOMA system is considered, where one base station (BS) communicates with two untrusted users (Fig. 1). We denote the n-th user by U_n, where $n \in \mathcal{N} = \{1, 2\}$. All the nodes in the network are assumed to be equipped with one antenna. The Rayleigh fading channel gain coefficient from BS to U_n is denoted by h_n. The channel power gains $|h_n|^2$ obeys an exponential distribution with mean parameter $\lambda_n = L_p d_n^{-e}$, where d_n denotes the distance between BS and U_n, L_p is the path loss constant, and e indicates the path loss exponent.Without loss of generality, we assume that $|h_1|^2 > |h_2|^2$, and thus, near and far user, i.e., U_1 and U_2 could be regarded as strong and weak user, respectively. The BS superposes information signals of users and broadcasts the superimposed signal with a total BS transmission power P_t. The fraction of P_t allocated for U_1 is denoted by α. The remaining fraction $(1-\alpha)$ is alloted to U_2. At the receiver side, each user performs SIC wherein inter-user interference imposed by the superposition is cancelled out to extract the desired signal [16]. Without loss of generality, received additive white Gaussian noise is assumed with mean 0 and variance σ^2 at both users. We consider an imperfect SIC scenario where RI from inaccurately decoded signals exists while decoding later users. β, $0 \leq \beta \leq 1$, denotes the RI factor, where $\beta = 1$ corresponds to the scenario of maximum interference, and $\beta = 0$ indicates perfect SIC [12], [13].

B. Decoding Orders for Untrusted NOMA

In an untrusted NOMA system, during the SIC process, each user can decode its own signal and other users' signal as well [4], [16]. This SIC process is performed in a certain sequence, which is known as the "*decoding order*" of the system. In a two users' scenario, the total possible decoding orders are 4 [4]. Let us denote the decoding order as a 2×2 matrix $\mathbf{D}_o$, where $o \in \{1, 2, 3, 4\}$ represents the index of o-th decoding order. Here m-th column of matrix $\mathbf{D}_o$ is specified by a column vector $\mathbf{d}_m$ of size 2×1, which depicts the SIC sequence observed by U_m, where $m \in \mathcal{N}$. To be more explicit, $[\mathbf{d}_m]_k = n$ signifies that U_m decodes data of U_n at k-th stage, where $n, k \in \mathcal{N}$ and $[\mathbf{d}_m]_1 \neq [\mathbf{d}_m]_2$. Thus, the 4 possible decoding orders can be written as $\mathbf{D}_1 = [2, 1; 2, 1]$, $\mathbf{D}_2 = [2, 1; 1, 2]$, $\mathbf{D}_3 = [1, 2; 2, 1]$, and $\mathbf{D}_4 = [1, 2; 1, 2]$. In [4, Theorem 2], it is proved that the optimal decoding order with respect to providing maximum secrecy rate at both users is $\mathbf{D}_2$. So, all further investigations will be carried out for $\mathbf{D}_2$.

III. PA Bounds from Secrecy Perspective

With the objective of securing one user's data from another, first we investigate the feasible PA bounds that ensure positive secrecy rate for both users. In $\mathbf{D}_2$, both near and far users first decode signals of other user, perform SIC, and then decode their own signal [4]. Thereby, using linear SIC model [11]-[13], the achievable signal-to-interference-plus-noise-ratio (SINR) Γ_{nm} at U_m, when U_n is decoded by U_m, where $m, n \in \mathcal{N}$, is given as

$$\Gamma_{21} = \frac{(1-\alpha)|h_1|^2}{\alpha|h_1|^2 + \frac{1}{\rho_t}}, \quad \Gamma_{12} = \frac{\alpha|h_2|^2}{(1-\alpha)|h_2|^2 + \frac{1}{\rho_t}},$$
$$\Gamma_{11} = \frac{\alpha|h_1|^2}{(1-\alpha)\beta|h_1|^2 + \frac{1}{\rho_t}}, \quad \Gamma_{22} = \frac{(1-\alpha)|h_2|^2}{\alpha\beta|h_2|^2 + \frac{1}{\rho_t}}, \tag{1}$$

where $\rho_t \triangleq \frac{P_t}{\sigma^2}$ denotes the BS transmit signal-to-noise ratio (SNR). The achievable secrecy rates R_{s1} and R_{s2} at U_1 and U_2, respectively, can be given as [2]

$$R_{s1} = R_{11} - R_{12}, \quad R_{s2} = R_{22} - R_{21}, \tag{2}$$

where $R_{nm} = \log_2(1 + \Gamma_{nm})$ denotes the data rate at U_m as given by Shannon's Theorem. To achieve positive secrecy rate for a given user, the rate of the legitimate channel has to be higher than that of the eavesdropper's channel. Thus, for U_1, the positive secrecy rate condition, i.e., $R_{11} > R_{12}$, which simplifies to $\Gamma_{11} > \Gamma_{12}$, must be appeased. This gives

$$\alpha < 1 + \frac{|h_1|^2 - |h_2|^2}{|h_1|^2|h_2|^2\rho_t(1-\beta)}. \tag{3}$$

Similarly, $\Gamma_{22} > \Gamma_{21}$ to obtain positive R_{s2} for U_2 gives

$$\alpha > \frac{|h_1|^2 - |h_2|^2}{|h_1|^2|h_2|^2\rho_t(1-\beta)}. \tag{4}$$

From (3) and (4), we can easily infer that in decoding order $\mathbf{D}_2$, positive secrecy rate can be obtained at both the users, provided $\frac{|h_1|^2-|h_2|^2}{|h_1|^2|h_2|^2\rho_t(1-\beta)} < \alpha < 1 + \frac{|h_1|^2-|h_2|^2}{|h_1|^2|h_2|^2\rho_t(1-\beta)}$.

IV. Secrecy Performance Analaysis

In this section, we derive the analytical expressions of SOP to explore secrecy performance for $\mathbf{D}_2$. Asymptotic approximations are also provided to gain analytical insights.

A. Secrecy Outage Probability

The SOP is defined as the probability that the maximum achievable secrecy rate at a user is less than a threshold secrecy rate [5]. Let us denote SOP for U_n as s_n, where $n \in \mathcal{N}$.

1) Near User: Assuming target and achievable secrecy rate, respectively, for U_1 as R_{s1}^{th} and R_{s1}, the SOP s_1 is given as (5). Here Pr$\{.\}$ denotes the probability measure, $\Pi_1 \triangleq 2^{R_{s1}^{th}}$, $N_1 = (\Pi_1 - 1)((1-\alpha)|h_2|^2\rho_t + 1) + \alpha|h_2|^2\rho_t\Pi_1$, $D_1 = \alpha\rho_t((1-\alpha)|h_2|^2\rho_t + 1) - (\Pi_1 - 1)((1-\alpha)|h_2|^2\rho_t + 1)\beta(1-\alpha)\rho_t - \Pi_1\beta\alpha(1-\alpha)\rho_t^2|h_2|^2$, $T_1 = \frac{\alpha-(\Pi_1-1)\beta(1-\alpha)}{(1-\alpha)\rho_t((\Pi_1-1)\beta(1-\alpha)+\alpha\Pi_1\beta-\alpha)}$, $\alpha_{1a} = \frac{\beta(\Pi_1-1)}{1+\beta(\Pi_1-1)}$, $\alpha_{1b} = \frac{\beta(\Pi_1-1)}{1-\beta}$, and $f_{|h_2|^2}(x)$ is the probability density function (PDF) of $|h_2|^2$. Note that $\alpha_{1b} > \alpha_{1a}$, as this simplifies to $\beta\Pi_1 > 0$, which is always true.

$$
\begin{aligned}
s_1 &= \Pr\{R_{s1} < R_{s1}^{th}\} = \Pr\left\{\frac{1+\Gamma_{11}}{1+\Gamma_{12}} < \Pi_1\right\} = \Pr\left\{|h_1|^2 D_1 < N_1\right\} = \Pr\left\{|h_1|^2 < \frac{N_1}{D_1}, D_1 > 0\right\} + \Pr\left\{|h_1|^2 \geq \frac{N_1}{D_1}, D_1 \leq 0\right\}, \\
&= \Pr\left\{|h_1|^2 < \frac{N_1}{D_1}, |h_2|^2 < T_1\right\} + \Pr\left\{|h_1|^2 \geq \frac{N_1}{D_1}, |h_2|^2 \geq T_1\right\}, \\
&= \begin{cases}
\int_0^{T_1}\left(1-\exp\left\{\frac{-N_1}{D_1\lambda_1}\right\}\right) f_{|h_2|^2}(y_1)dy_1 + \int_{T_1}^{\infty} 1 \times f_{|h_2|^2}(y_1)dy_1, & \alpha_{1a} < \alpha < \alpha_{1b} \\
\int_0^{\infty}\left(1-\exp\left\{\frac{-N_1}{D_1\lambda_1}\right\}\right) f_{|h_2|^2}(y_1)dy_1, & \alpha \geq \alpha_{1b} \\
\int_0^{\infty} 1 \times f_{|h_2|^2}(y_1)dy_1, & \text{otherwise}
\end{cases} \\
&= \begin{cases}
1-\frac{1}{\lambda_2}\int_0^{T_1}\exp\left\{\frac{-((\Pi_1-1)((1-\alpha)y_1\rho_t+1)+\alpha y_1\rho_t\Pi_1)}{(\alpha\rho_t((1-\alpha)y_1\rho_t+1)-(\Pi_1-1)((1-\alpha)y_1\rho_t+1)\beta(1-\alpha)\rho_t-\Pi_1\beta\alpha(1-\alpha)\rho_t^2 y_1)\lambda_1} - \frac{y_1}{\lambda_2}\right\}dy_1, & \alpha_{1a} < \alpha < \alpha_{1b} \\
1-\frac{1}{\lambda_2}\int_0^{\infty}\exp\left\{\frac{-((\Pi_1-1)((1-\alpha)y_1\rho_t+1)+\alpha y_1\rho_t\Pi_1)}{(\alpha\rho_t((1-\alpha)y_1\rho_t+1)-(\Pi_1-1)((1-\alpha)y_1\rho_t+1)\beta(1-\alpha)\rho_t-\Pi_1\beta\alpha(1-\alpha)\rho_t^2 y_1)\lambda_1} - \frac{y_1}{\lambda_2}\right\}dy_1, & \alpha \geq \alpha_{1b} \\
1, & \text{otherwise}
\end{cases}
\end{aligned} \tag{5}
$$

$$
\begin{aligned}
s_2 &= \Pr\{R_{s2} < R_{s2}^{th}\} = \Pr\left\{\frac{1+\Gamma_{22}}{1+\Gamma_{21}} < \Pi_2\right\} = \Pr\left\{|h_2|^2 D_2 < N_2\right\} = \Pr\left\{|h_2|^2 < \frac{N_2}{D_2}, D_2 > 0\right\} + \Pr\left\{|h_2|^2 \geq \frac{N_2}{D_2}, D_2 \leq 0\right\}, \\
&= \Pr\left\{|h_2|^2 < \frac{N_2}{D_2}, |h_1|^2 < T_2\right\} + \Pr\left\{|h_2|^2 \geq \frac{N_2}{D_2}, |h_1|^2 \geq T_2\right\}, \\
&= \begin{cases}
\int_0^{T_2}\left(1-\exp\left\{\frac{-N_2}{D_2\lambda_2}\right\}\right) f_{|h_1|^2}(y_2)dy_2 + \int_{T_2}^{\infty} 1 \times f_{|h_1|^2}(y_2)dy_2, & \alpha_{2a} < \alpha < \alpha_{2b} \\
\int_0^{\infty}\left(1-\exp\left\{\frac{-N_2}{D_2\lambda_2}\right\}\right) f_{|h_1|^2}(y_2)dy_2, & \alpha \leq \alpha_{2a} \\
\int_0^{\infty} 1 \times f_{|h_1|^2}(y_2)dy_2, & \text{otherwise}
\end{cases} \\
&= \begin{cases}
1-\frac{1}{\lambda_1}\int_0^{T_2}\exp\left\{\frac{-((\Pi_2-1)(\alpha y_2\rho_t+1)+(1-\alpha)y_2\rho_t\Pi_2)}{((1-\alpha)\rho_t(\alpha y_2\rho_t+1)-(\Pi_2-1)(\alpha y_2\rho_t+1)\beta\alpha\rho_t-\Pi_2\beta\alpha(1-\alpha)\rho_t^2 y_2)\lambda_2} - \frac{y_2}{\lambda_1}\right\}dy_2, & \alpha_{2a} < \alpha < \alpha_{2b} \\
1-\frac{1}{\lambda_1}\int_0^{\infty}\exp\left\{\frac{-((\Pi_2-1)(\alpha y_2\rho_t+1)+(1-\alpha)y_2\rho_t\Pi_2)}{((1-\alpha)\rho_t(\alpha y_2\rho_t+1)-(\Pi_2-1)(\alpha y_2\rho_t+1)\beta\alpha\rho_t-\Pi_2\beta\alpha(1-\alpha)\rho_t^2 y_2)\lambda_2} - \frac{y_2}{\lambda_1}\right\}dy_2, & \alpha \leq \alpha_{2a} \\
1, & \text{otherwise}
\end{cases}
\end{aligned} \tag{6}
$$

$$
s_{1[C]} = \begin{cases}
1-\frac{1}{\lambda_2}\int_0^{T_{1[C]}}\exp\left\{\frac{-((\Pi_1-1)(\beta(1-\alpha)y_1\rho_t+1)+\alpha y_1\rho_t\Pi_1)}{(\alpha\rho_t(\beta(1-\alpha)y_1\rho_t+1)-(\Pi_1-1)(\beta(1-\alpha)y_1\rho_t+1)\beta(1-\alpha)\rho_t-\Pi_1\beta\alpha(1-\alpha)\rho_t^2 y_1)\lambda_1} - \frac{y_1}{\lambda_2}\right\}dy_1, & \alpha > \alpha_{1[C]} \\
1, & \text{otherwise}
\end{cases} \tag{7}
$$

$$
s_{2[C]} = \begin{cases}
1-\frac{1}{\lambda_1}\int_0^{T_{2[C]}}\exp\left\{\frac{-((\Pi_2-1)(\alpha y_2\rho_t+1)+(1-\alpha)y_2\rho_t\Pi_2)}{((1-\alpha)\rho_t(\alpha y_2\rho_t+1)-(\Pi_2-1)(\alpha y_2\rho_t+1)\alpha\rho_t-\Pi_2\alpha(1-\alpha)\rho_t^2 y_2)\lambda_2} - \frac{y_2}{\lambda_1}\right\}dy_2, & \alpha < \alpha_{2[C]} \\
1, & \text{otherwise}
\end{cases} \tag{8}
$$

2) Far user: Considering R_{s2}^{th} and R_{s2}, respectively, as target and achievable secrecy rate, of U_2, s_2 is given as (6), where $\Pi_2 \triangleq 2^{R_{s2}^{th}}$, $N_2 = (\Pi_2-1)(\alpha|h_1|^2\rho_t+1)+(1-\alpha)|h_1|^2\rho_t\Pi_2$, $D_2 = (1-\alpha)\rho_t(\alpha|h_1|^2\rho_t+1)-(\Pi_2-1)(\alpha|h_1|^2\rho_t+1)\beta\alpha\rho_t-\Pi_2\beta\alpha(1-\alpha)\rho_t^2|h_1|^2$, $T_2 = \frac{(1-\alpha)-(\Pi_2-1)\beta\alpha}{\alpha\rho_t((\Pi_2-1)\beta\alpha+(1-\alpha)\Pi_2\beta-(1-\alpha))}$, $\alpha_{2a} = \frac{1-\Pi_2\beta}{1-\beta}$, $\alpha_{2b} = \frac{1}{1+\beta(\Pi_2-1)}$, and $f_{|h_1|^2}(x)$ is PDF of $|h_1|^2$. Here $\alpha_{2b} > \alpha_{2a}$, as it gives $\Pi_2 > 1$, which holds true.

Similarly, we can obtain SOP expressions for other decoding orders. As a special case, the SOPs, $s_{1[C]}$ and $s_{2[C]}$ for conventional decoding order $\mathbf{D}_1$, are given in (7) and (8), respectively. Here $T_{1[C]} = \frac{\alpha-(\Pi_1-1)\beta(1-\alpha)}{(1-\alpha)\rho_t\beta((\Pi_1-1)\beta(1-\alpha)+\alpha(\Pi_1-1))}$, $\alpha_{1[C]} = \frac{(\Pi_1-1)\beta}{1+\beta(\Pi_1-1)}$, $T_{2[C]} = \frac{(1-\alpha)-(\Pi_2-1)\alpha}{\alpha\rho_t((\Pi_2-1)\alpha+(1-\alpha)(\Pi_2-1))}$ and $\alpha_{2[C]} = \frac{1}{\Pi_2}$. $[C]$ stands for conventional decoding order.

B. Asymptotic Approximations

Next, to provide analytical insights, we present closed-form approximations of SOPs at both users U_1 and U_2 for $\mathbf{D}_2$.

1) Near User: The exact closed-form expression of s_1, i.e., $\widehat{s}_1$, obtained by using $((1-\alpha)\rho_t y_1 + 1) \approx (1-\alpha)\rho_t y_1$ for $\rho_t \gg 1$ in (5) is given in (9).

2) Far User: The closed-form asymptotic approximation $\widehat{s}_2$ of s_2, which we obtain by setting $(\alpha\rho_t y_2 + 1) \approx \alpha\rho_t y_2$ for high ρ_t in (6), is provided in (10).

$$\widehat{s}_1 = \begin{cases} 1-\left(\left(1-\exp\left\{\frac{-T_1}{\lambda_2}\right\}\right)\times\exp\left\{\frac{-((\Pi_1-1)(1-\alpha)\rho_t+\alpha\rho_t\Pi_1)}{(\alpha\rho_t^2(1-\alpha)-(\Pi_1-1)(1-\alpha)^2\beta\rho_t^2-\Pi_1\beta\alpha(1-\alpha)\rho_t^2)\lambda_1}\right\}\right), & \alpha_{1a}<\alpha<\alpha_{1b} \\ 1-\exp\left\{\frac{-((\Pi_1-1)(1-\alpha)\rho_t+\alpha\rho_t\Pi_1)}{(\alpha\rho_t^2(1-\alpha)-(\Pi_1-1)(1-\alpha)^2\beta\rho_t^2-\Pi_1\beta\alpha(1-\alpha)\rho_t^2)\lambda_1}\right\}, & \alpha\geq\alpha_{1b} \\ 1, & \text{otherwise} \end{cases} \tag{9}$$

$$\widehat{s}_2 = \begin{cases} 1-\left(\left(1-\exp\left\{\frac{-T_2}{\lambda_1}\right\}\right)\times\exp\left\{\frac{-((\Pi_2-1)\alpha\rho_t+(1-\alpha)\rho_t\Pi_2)}{((1-\alpha)\rho_t^2\alpha-(\Pi_2-1)\alpha^2\rho_t^2\beta-(1-\alpha)\Pi_2\rho_t^2\alpha\beta)\lambda_2}\right\}\right), & \alpha_{2a}<\alpha<\alpha_{2b} \\ 1-\exp\left\{\frac{-((\Pi_2-1)\alpha\rho_t+(1-\alpha)\rho_t\Pi_2)}{((1-\alpha)\rho_t^2\alpha-(\Pi_2-1)\alpha^2\rho_t^2\beta-(1-\alpha)\Pi_2\rho_t^2\alpha\beta)\lambda_2}\right\}, & \alpha\leq\alpha_{2a} \\ 1, & \text{otherwise} \end{cases} \tag{10}$$

$$\widehat{s}_{1[C]} = \begin{cases} 1-\left(\left(1-\exp\left\{\frac{-T_{1[C]}}{\lambda_2}\right\}\right)\times\exp\left\{\frac{-((\Pi_1-1)\beta(1-\alpha)\rho_t+\alpha\rho_t\Pi_1)}{(\beta\alpha\rho_t^2(1-\alpha)-(\Pi_1-1)(1-\alpha)^2\beta^2\rho_t^2-\Pi_1\beta\alpha(1-\alpha)\rho_t^2)\lambda_1}\right\}\right), & \alpha>\alpha_{1[C]} \\ 1, & \text{otherwise} \end{cases} \tag{11}$$

$$\widehat{s}_{2[C]} = \begin{cases} 1-\left(\left(1-\exp\left\{\frac{-T_{2[C]}}{\lambda_1}\right\}\right)\times\exp\left\{\frac{-((\Pi_2-1)\alpha\rho_t+(1-\alpha)\rho_t\Pi_2)}{(\alpha\rho_t^2(1-\alpha)-(\Pi_2-1)\alpha^2\rho_t^2-\Pi_2\alpha(1-\alpha)\rho_t^2)\lambda_2}\right\}\right), & \alpha<\alpha_{2[C]} \\ 1, & \text{otherwise} \end{cases} \tag{12}$$

Similar to above approximations, closed-form SOP expressions for other decoding orders can also be obtained. For conventional decoding order $\mathbf{D}_1$, the asymptotic SOP expressions, $\widehat{s}_{1[C]}$ and $\widehat{s}_{2[C]}$, are given in (11) and (12), respectively.

V. Numerical Results

Downlink NOMA system is considered with one BS and two untrusted users. Near user is assumed to be at a distance of $d_1 = 50$ meter from BS, and for far user, distance $d_2 = 100$ meter is adopted. Noise power is set to -90 dBm with noise signal following Gaussian distribution at all users. Small scale fading is presumed to obey an exponential distribution with a 1 mean value at both links [5]. Simulations are averaged over 10^6 randomly generated channel realizations by using Rayleigh distribution for both users. The value of L_p and e, respectively, are taken to be 1 and 3. ρ_r is assumed as the received SNR in decibels (dB) at U_2. The value of β is taken to be 0.1. Simulation, analytical, and asymptotic results are, respectively, marked as Sim, Ana, and Asy.

A. Validation of Analysis

Here in Fig. 2, the validation of SOPs, s_1 with R_{s1}^{th} and s_2 with R_{s2}^{th} for different values of ρ_r are shown. The perfect agreement between simulated and analytical curves confirms the exactness of s_1 and s_2 analysis. It can be visualized from the results that s_1 and s_2 increase with the increase in threshold rates R_{s1}^{th} and R_{s2}^{th}, respectively. Because outage occurs when the maximum achievable secrecy rate drops below a threshold rate, it is clear that increasing threshold secrecy rates at the user will, in turn, increase SOP. It can also be observed that an increase in ρ_r decreases both s_1 and s_2. This happens because the secrecy rates achieved at users increase by an increase in SNR, and so, for a given threshold secrecy rate, SOP decreases. From Fig. 3, we can visualize that analytical results match with asymptotic results at high SNR, and it confirms the exactness of asymptotic expressions.

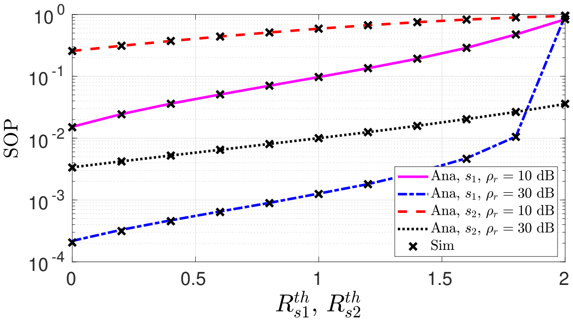


Fig. 2. Validation of SOPs at U_1 and U_2 for $\mathbf{D}_2$, $\alpha = 0.33$.

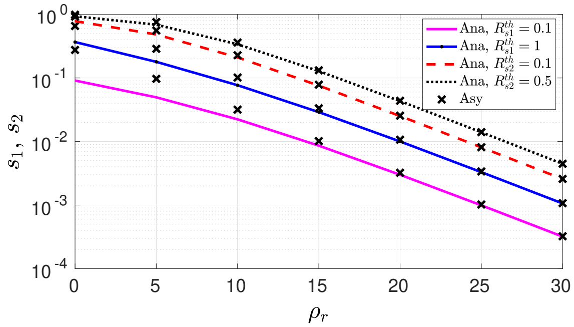
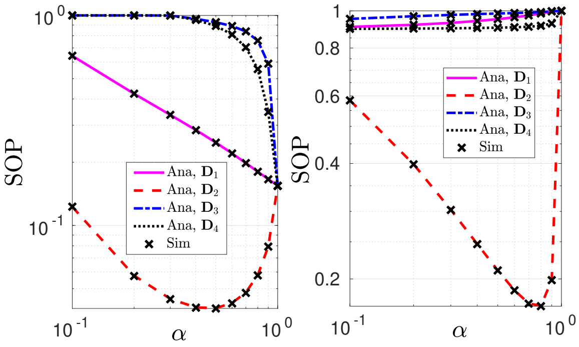
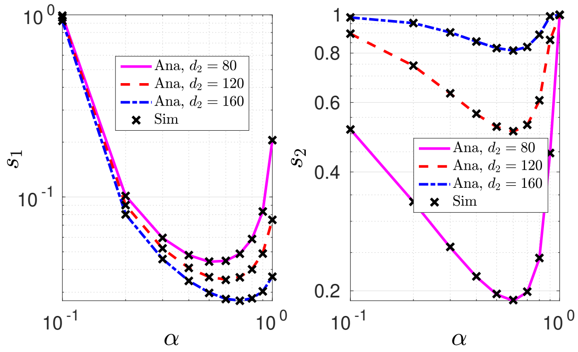


Fig. 3. Validation of the accuracy of the proposed closed-form asymptotic approximations of SOPs for $\mathbf{D}_2$ with $\alpha = 0.5$.



(a) (b)

Fig. 4. Verification of the optimality of the decoding order $\mathbf{D}_2$ among 4 possibilities $\{\mathbf{D}_1, \mathbf{D}_2, \mathbf{D}_3, \mathbf{D}_4\}$, for U_1 in (a) and U_2 in (b) with $\rho_r = 10$ dB, $R_{s1}^{th} = 0.5$ and $R_{s2}^{th} = 0.1$.



(a) (b)

Fig. 5. Insights on optimal power allocation α that minimizes SOPs, s_1 in (a) and s_2 in (b), for different values of d_2, for $\mathbf{D}_2$, $d_1 = 40$ meter, $\rho_t = 70$ dB, $R_{s1}^{th} = 1$ and $R_{s2}^{th} = 0.5$.

B. Validation of Optimal Decoding Order

Here we have sketched a plot to validate that the optimal decoding order for providing the highest secrecy rate for both near and far users is $\mathbf{D}_2$, as given in [4, Theorem 2]. In Fig. 4, SOPs at both U_1 and U_2 for all 4 decoding orders with respect to α are shown. The results corroborate that better SOP performance is obtained for $\mathbf{D}_2$, and hence it is optimal.

C. Impact of Relative Distance between Users

In Fig. 5(a), we notice the effect of varying the distance d_2 from BS on achievable SOPs. d_1 is fixed at 40 meters. It can be seen that s_1 decreases with an increase in d_2. This happens because an increase in distance d_2 causes a drop in achievable data rate at U_2, which in turn provide better secrecy rate at U_1, thereby decreasing the SOP at U_1. Conversely, as shown in Fig. 5(b), a decrease in data rate at U_2 signifies a reduction in secrecy rate at U_2, which further increases the SOP for U_2. Thus, it can be observed that increasing the distance from BS to U_2 has a contradictory effect on s_1 and s_2. Fig. 5(a) and Fig. 5(b) also confirm the existence of an optimal PA that minimizes the SOP performance for both users U_1 and U_2.

VI. Concluding Remarks

We have focused on the practical but adverse problem of SIC being imperfect in a secure NOMA system. Considering RI, the PA bounds are calculated to provide a positive secrecy rate for users. Analytical and asymptotic expressions of SOP are derived. Numerical results have are provided to validate the analytical expressions and exhibit the effects of different key parameters on performance. Future work includes extending the study of SOP in a multi-user untrusted NOMA scenario.

Acknowledgement

This work was partially supported by the Faculty Funded Postdoctoral Research Fellowship support of EET School at UNSW Sydney.

References

[1] Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan, and V. K. Bhargava, "A survey on non-orthogonal multiple access for 5G networks: Research challenges and future trends," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 10, pp. 2181–2195, Oct. 2017.

[2] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, Secondquarter 2019.

[3] R. Saini, D. Mishra, and S. De, "OFDMA-based DF secure cooperative communication with untrusted users," *IEEE Commun. Lett.*, vol. 20, no. 4, pp. 716–719, Apr. 2016.

[4] S. Thapar, D. Mishra, and R. Saini, "Novel outage-aware NOMA protocol for secrecy fairness maximization among untrusted users," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13 259–13 272, Sep. 2020.

[5] B. M. ElHalawany and K. Wu, "Physical-layer security of NOMA systems under untrusted users," in *Proc. IEEE GLOBECOM*, United Arab Emirates, Dec. 2018, pp. 1–6.

[6] Y. Li, M. Jiang, Q. Zhang, Q. Li, and J. Qin, "Secure beamforming in downlink MISO nonorthogonal multiple access systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7563–7567, Aug. 2017.

[7] C. Zhang, F. Jia, Z. Zhang, J. Ge, and F. Gong, "Physical layer security designs for 5G NOMA systems with a stronger near-end internal eavesdropper," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13 005 – 13 017, Aug. 2020.

[8] R. M. Christopher and D. K. Borah, "Physical layer security for weak user in MISO NOMA using directional modulation (NOMAD)," *IEEE Commun. Lett.*, vol. 24, no. 5, pp. 956–960, Feb. 2020.

[9] Y. Qi and M. Vaezi, "Secure transmission in MIMO-NOMA networks," *IEEE Commun. Lett.*, vol. 24, no. 12, pp. 2696–2700, Aug. 2020.

[10] S. Thapar, D. Mishra, and R. Saini, "Secrecy fairness aware NOMA for untrusted users," in *Proc. IEEE GLOBECOM*, Hawaii, USA, Dec. 2019, pp. 1–6.

[11] S. Thapar, D. Mishra, and R. Saini, "Decoding orders for securing untrusted NOMA," *IEEE Networking Lett.*, vol. 3, no. 1, pp. 27–30, Jan. 2021.

[12] H. Sun, B. Xie, R. Q. Hu, and G. Wu, "Non-orthogonal multiple access with SIC error propagation in downlink wireless MIMO networks," in *Proc. IEEE VTC-Fall*, Montreal, Canada, Sep. 2016, pp. 1–5.

[13] X. Wang, R. Chen, Y. Xu, and Q. Meng, "Low-complexity power allocation in NOMA systems with imperfect SIC for maximizing weighted sum-rate," *IEEE Access*, vol. 7, pp. 94 238–94 253, July 2019.

[14] X. Yue, Z. Qin, Y. Liu, S. Kang, and Y. Chen, "A unified framework for non-orthogonal multiple access," *IEEE Transactions on Communications*, vol. 66, no. 11, pp. 5346–5359, May 2018.

[15] B. T. F.T. Miandoab, "NOMA performance enhancement-based imperfect SIC minimization using a novel user pairing scenario involving three users in each pair," *Wireless Networks*, vol. 26, no. 5, pp. 3735–3748, Mar. 2020.

[16] X. Chen, A. Beiijebbour, A. Li, H. Jiang, and H. Kayama, "Consideration on successive interference canceller (SIC) receiver at cell-edge users for non-orthogonal multiple access (NOMA) with SU-MIMO," in *Proc. IEEE PIMRC*, Hong Kong, China, Aug. 2015, pp. 522–526.