MITSUBISHI ELECTRIC RESEARCH LABORATORIES
http://www.merl.com

Collaborative Motion Prediction via Neural Motion Message Passing

Hu, Yue; Chen, Siheng; Zhang, Ya; Gu, Xiao

TR2020-072 June 16, 2020

Abstract

Motion prediction is essential and challenging for autonomous vehicles and social robots. One challenge of motion prediction is to model the interaction among traffic actors, which could cooperate with each other to avoid collisions or form groups. To address this challenge, we propose neural motion message passing (NMMP) to explicitly model the interaction and learn representations for directed interactions between actors. Based on the proposed NMMP, we design the motion prediction systems for two settings: the pedestrian setting and the joint pedestrian and vehicle setting. Both systems share a common pattern: we use an individual branch to model the behavior of a single actor and an interactive branch to model the interaction between actors, while with different wrappers to handle the varied input formats and characteristics. The experimental results show that both systems outperform the previous state-of-the-art methods on several existing benchmarks. Besides, we provide interpretability for interaction learning. Code is available at https://github.com/PhyllisH/NMMP

IEEE Conference on Computer Vision and Pattern Recognition (CVPR)

Security Performance Analysis for the Downlink NOMA Systems with Outage Constraint

Hongjiang Lei†, Rui Gao†, Ki-Hong Park§, Imran Shafique Ansari¶, Kyeong Jin Kim‡, and Mohamed-Slim Alouini§

†School of Communication and Information Engineering,
Chongqing University of Posts and Telecommunications, Chongqing 400065, China
§CEMSE Division, King Abdullah University of Science and Technology, Thuwal 23955-6900, Saudi Arabia
¶James Watt School of Engineering, University of Glasgow, Glasgow G12 8QQ, United Kingdom
‡Mitsubishi Electric Research Laboratories (MERL), Cambridge, MA, USA.

Abstract—**In this work, we investigate the relationship between the reliability and security of a typical two-user downlink non-orthogonal multiple access (NOMA) communication system. The level of successive interference cancellation (SIC) on NOMA user is considered. The impact of various key parameters on transmit signal-to-noise ratio (SNR) of the NOMA users with the reliability outage probability (ROP) constraint is discussed. Taking the minimum of transmit SNR for ROP into account, the secrecy outage performance of the downlink NOMA systems is studied and the analytical expressions of the secrecy outage probability of the NOMA system are derived under two cases of eavesdropping capability. Monte Carlo simulations are provided to verify the accuracy of our analysis.**

I. Introduction

Non-orthogonal multiple access (NOMA) has been regarded as one of the most promising technologies in the fifth-generation (5G) wireless networks [1], [2]. In NOMA systems, the superimposed coding technology enables to serve multiple users simultaneously. Power allocation strategy applied at the base station (BS) ensures more power is allocated to the signals transmitted forwards the weak users, which improves the fairness between users and makes it easy to decode the information received by the weak user. The strong user first decodes the information of the weak user and then applies successive interference cancellation (SIC) technology, which greatly reduces the interference from other users' information and improves the channel capacity of the strong user [3].

The performance of the NOMA systems has obtained a lot of attention from academia [4], [5]. Ding *et al.* investigated the reliability outage probability (ROP) and ergodic capacity (EC) of a cellular downlink NOMA scenario with randomly deployed users and testified that NOMA technology can achieve better performance relative to traditional orthogonal multiple access in [4]. The ROP and average throughput of a downlink virtual multiple-input multiple-output NOMA system in IoT networks were analyzed by using the Kronecker correlation model in [5].

In most literature focused on NOMA technology, it is assumed that perfect SIC (pSIC) is performed. In practical applications, the destructive factors that lead to errors in SIC must be considered since the near user will suffer from residual interference, which is called as imperfect SIC (ipSIC). The ROP for both code-domain and power-domain NOMA systems was analyzed in [6], wherein the locations of NOMA users were modeled by homogeneous binomial point processes and the analytical expressions of the ROP for pSIC and ipSIC were derived.

Physical layer security, utilizing the characteristics of wireless channels and signal processing technology, is an exciting complement to complex cryptographic techniques [7], [8]. Liu *et. al* investigated the security performance of large-scale NOMA networks and derived analytical expressions for the exact secrecy outage probability (SOP) and asymptotic SOP in [9]. Multiple transmit antenna selection schemes were proposed to enhance the security performance of a downlink multiple-input single-output (MISO) NOMA system in [10] and a novel power allocation scheme was proposed to obtain the non-zero secrecy diversity order (SDO). Lv *et. al* studied the design of secure NOMA against full-duplex proactive eavesdropping in [11] and proposed a novel outage-constrained transmission scheme to guarantee both reliability and security.

It is significant to investigate the detrimental effect of imperfect SIC (ipSIC) on the security of the NOMA system. Yue *et. al*, in [12], investigated the security performance of a unified NOMA framework, in which both external and internal eavesdropping scenarios were considered, the analytical expressions for the exact and asymptotic SOP were derived for both code-domain NOMA and power-domain NOMA, in which both ipSIC and pSIC were taken into account. But only security outage performance was studied and the relationship between ROP and SOP was not consider.

- We analyze the secrecy performance of a two-user downlink NOMA system while considering the ROP constraint and ipSIC. Taking the ROP constraint into account, the effect of different parameters on the minimum transmit signal-to-noise ratio (SNR) of the NOMA system is analysed, the analytical expressions for the SOP of the NOMA system are investigated for various different scenarios, and the relationship between the ROP and the secrecy performance is discussed comprehensively.
- Two different scenarios wherein the eavesdropper's decoding capability is different are considered. In Case 1, it is assumed that eavesdropper has sufficient decoding capability corresponds to the correlation between the secrecy capacity of legitimate users; In Case 2, the eavesdropper is assumed that has same decoding capability as legitimate users, correspondingly, the security of strong user is independent

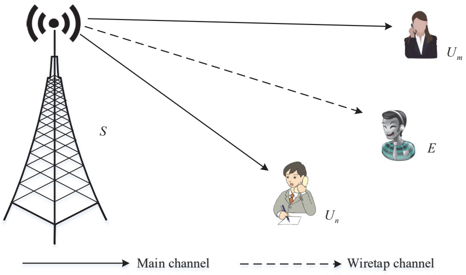

Fig. 1. System model consisting of a base station (S), two legitimate users (U_n and U_m), and an illegitimate eavesdropper (E).

of weak user.

- Relative to ipSIC performed on the strong (near) user in [12], wherein the SOP was analyzed under two cases of eavesdropping capability, we analyze the SOP of the downlink NOMA system while considering the ROP constraint and ipSIC under two different eavesdropping scenarios, and the setting of the factor measuring the level of ipSIC is more realistic.

The rest of this paper is organized as follows. Section II describes the system model. In Section III, the effect of different parameters on the transmit SNR of the downlink NOMA system with ROP constraint is analyzed. The analytical expressions for the exact SOP of the downlink NOMA system with the ROP constraint is derived in Section IV. Section V presents the numerical and simulation results to demonstrate the analysis of the security performance of the NOMA system and the paper is concluded in Section VI.

II. System Model

As shown in Fig. 1, we consider a downlink NOMA system consisting of a BS denoted by S, an eavesdropper denoted by E, and two legitimate users U_n (the near user) and U_m(the far user). All nodes in the system are equipped with a single antenna. It is assumed that all channels undergo quasi-static Rayleigh fading, which means the channel coefficients are constant for each time-slot but vary independently between different time-slots, and the received signals are agitated by additive white Gaussian noise with mean power σ^2. The channel coefficients from S to the destinations (including U_n, U_m, and E) are denoted by h_n, h_m, and h_e, respectively. For brevity, we denote the channel gains by $g_i = |h_i|^2$ and $g_e = |h_e|^2$, where $i \in \{n, m\}$ and $g_n > g_m$, and assume their respective expectations to be $\mathbb{E}[g_i] = \lambda_i$ and $\mathbb{E}[g_e] = \lambda_e$, respectively.

Similar to [9] and [11], the legitimate users are categorized by the their conditions, which means the user U_n requires a higher target rate but it is more delay-tolerant than the user U_m. During each time slot, S transmits a superimposed signal $s = \left(\sqrt{\alpha_n} x_n + \sqrt{\alpha_m} x_m\right)$ to U_n and U_m with the transmit power P at S, where x_n and x_m are normalized power signals of U_n and U_m, respectively, i.e, $\mathbb{E}\left[|x_n|^2\right] = \left[|x_m|^2\right] = 1$, and the α_i represents the NOMA power coefficients under the conditions $\alpha_n + \alpha_m = 1$ and $\alpha_m > \alpha_n$.

With the NOMA scheme [9], the user U_n utilizes SIC to detect x_n after decoding x_m and the user U_m detects its own signal x_m by considering x_n as interference. Hence, the signal-to-interference-plus-noise ratio (SINR) of the user U_n is given by

$$\gamma_n^{x_m} = \frac{\alpha_m \rho g_n}{\alpha_n \rho g_n + 1}, \gamma_n^{x_n} = \frac{\alpha_n \rho g_n}{\varpi_n \alpha_m \rho g_n + 1}, \tag{1}$$

where $\rho = \frac{P}{\sigma^2}$ signifies the transmit SNR. $\varpi_n \in [0, 1]$ represents the level of SIC, i.e., $\varpi_n \neq 0$ and $\varpi_n = 0$ denote the ipSIC and the pSIC operations, respectively [12]. The SINR of the user U_m is given by

$$\gamma_m^{x_m} = \frac{\alpha_m \rho g_m}{\alpha_n \rho g_m + 1}. \tag{2}$$

To the best of the author's knowledge within the domain of NOMA, there are two situations with regards to the eavesdropper's, E's, capability to decode x_i, and the corresponding SINRs, $\gamma_e^{x_i}$, these are as follows.

Case 1: E has sufficient decoding capability. Considering the worst-case security of the NOMA system, the eavesdropper E has powerful decoding capability to fully decode the users' information [9]. Therefore, E can wiretap both legitimate users at the same time. Then, the SINR at E when it eavesdrops the signal x_i is given by

$$\gamma_{e,1}^{x_i} = \alpha_i \rho g_e. \tag{3}$$

It must be noted that the SOP for U_n and U_m are correlated in this case [13].

Case 2: E have same decoding capability as U_i. In this case, the decoding capability of the eavesdropper E is the same as the legitimate users [10]. Thus, the SINRs at E are given by

$$\gamma_{e,2}^{x_n} = \frac{\alpha_n \rho g_e}{\varpi_n \alpha_m \rho g_e + 1}, \gamma_{e,2}^{x_m} = \frac{\alpha_m \rho g_e}{\alpha_n \rho g_e + 1}. \tag{4}$$

In this case, E is interested only in a specific user's message, which means E eavesdrops the information of legitimate users independently [10]. Thus, the secrecy capacity of legitimate users is independent.

To facilitate the following analysis, we classify the same form of SNR as $(\gamma_1, j_1) \in \left\{\left(\gamma_n^{x_n}, n\right), \left(\gamma_{e,2}^{x_n}, e\right)\right\}$, $(\gamma_2, i, j_2) \in \left\{\left(\gamma_{e,1}^{x_n}, n, e\right), \left(\gamma_{e,1}^{x_m}, m, e\right)\right\}$, and $(\gamma_3, j_3) \in \left\{\left(\gamma_m^{x_m}, m\right), \left(\gamma_{e,2}^{x_m}, e\right)\right\}$. The cumulative distribution function (CDF) of γ_1 is obtained as

$$\begin{aligned} F_{\gamma_1}(x) &= \Pr\left\{\gamma_1 < x\right\} \\ &= \Pr\left\{\frac{\alpha_n \rho g_{j_1}}{\varpi_n \alpha_m \rho g_{j_1} + 1} < x\right\} \\ &= \Pr\left\{\left(\alpha_n - \varpi_n \alpha_m x\right) \rho g_{j_1} < x\right\} \\ &= \begin{cases} 1 - e^{-\frac{x}{(\alpha_n - \varpi_n \alpha_m x)\rho \lambda_{j_1}}}, & x < \frac{\alpha_n}{\varpi_n \alpha_m} \\ 1, & x \geqslant \frac{\alpha_n}{\varpi_n \alpha_m}. \end{cases} \end{aligned} \tag{5}$$

And the CDF of γ_2 and γ_3 are given by

$$F_{\gamma_2}(x) = 1 - e^{-\frac{x}{\alpha_i \rho \lambda_{j_2}}}, \tag{6}$$

$$F_{\gamma_3}(x) = \begin{cases} 1 - e^{-\frac{x}{(\alpha_m - \alpha_n x)\rho \lambda_{j_3}}}, & x < \frac{\alpha_m}{\alpha_n} \\ 1, & x \geqslant \frac{\alpha_m}{\alpha_n} \end{cases}, \tag{7}$$

respectively.

$$
\begin{aligned}
P_{\text{out}}^{n,1} &= \Pr\left\{C_{s,1}^{x_n}\left(\varepsilon_n\right) < R_s^{x_n}\right\} \\
&= \Pr\left\{\left(\underbrace{\alpha_n - \varpi_n\alpha_m\left(\alpha_n\eta_s^{x_n}\rho\left(\varepsilon_n\right)g_e + \eta_s^{x_n} - 1\right)}_{\Lambda_1}\right)\rho\left(\varepsilon_n\right)g_n < \left(\alpha_n\eta_s^{x_n}\rho\left(\varepsilon_n\right)g_e + \eta_s^{x_n} - 1\right)\right\} \\
&= 1 - \Pr\left\{g_n > \frac{\alpha_n\eta_s^{x_n}\rho\left(\varepsilon_n\right)g_e + \eta_s^{x_n} - 1}{\Lambda_1\rho\left(\varepsilon_n\right)}, \Lambda_1 > 0\right\} \\
&= 1 - \Pr\left\{g_n > \Phi_1\left(g_e\right), g_e < b_1\right\} \\
&= 1 - \frac{b_1}{2\lambda_e}\sum_{k_1=1}^{K}\omega_K\sqrt{1-\phi_{k_1}^2}\,e^{-\frac{\Phi_1\left(\theta_{k_1}\right)}{\lambda_n} - \frac{\theta_{k_1}}{\lambda_e}}
\end{aligned} \tag{15}
$$

III. Transmit Signal-to-Noise Ratio with Reliability Outage Constraint

On the basis of Shannon's theorem, the capacity of the main channel from S to U_i and the wiretap channel from S to E are given by

$$C_b^{x_i} = \log_2\left(1+\gamma_i^{x_i}\right). \tag{8}$$

The ROP, representing the probability of outage event in which the transmission rate is higher than the channel capacity is given by

$$\mathcal{O}_r\left(R_b^{x_i}\right) = \Pr\left\{R_b^{x_i} > C_b^{x_i}\right\}, \tag{9}$$

where $R_b^{x_i}$ denotes the codeword rate of the main channel between the transmitter and the legitimate receivers.

Based on $\alpha_n + \alpha_m = 1$, (5), and (7), we obtain

$$
\begin{aligned}
&\mathcal{O}_r\left(R_b^{x_i}\right) = \Pr\left\{C_b^{x_i} < R_b^{x_i}\right\} \le \varepsilon_i \\
&\Leftrightarrow \left(\alpha_i - \varpi_i\left(1-\alpha_i\right)\tau_i\right)\rho\lambda_i \ge -\frac{\tau_i}{\ln\left(1-\varepsilon_i\right)},
\end{aligned} \tag{10}
$$

where $\tau_i = 2^{R_b^{x_i}} - 1$, ε_i signifies the target ROP for U_i, and $0 < \varepsilon_i < 1$.

Remark 1. *One can easily realize that ROP would not satisfy the requirement at U_i when $\alpha_i - \varpi_i\left(1-\alpha_i\right)\tau_i < 0$. This signifies that in order to ensure reliability at U_i, there is a constraint for the power allocation coefficients, which is expressed as*

$$\alpha_i > \frac{\varpi_i\tau_i}{1+\varpi_i\tau_i}. \tag{11}$$

Based on (11), $\varpi_m = 1$, and $\alpha_m > \alpha_n$, with some simple algebraic manipulations, we obtain

$$\frac{\varpi_n\tau_n}{1+\varpi_n\tau_n} < \alpha_n < \frac{1}{1+\tau_m}. \tag{12}$$

Based on (10) and (11), we derive

$$
\begin{aligned}
\rho\left(\varepsilon_i\right) &\geqslant -\frac{\tau_i}{\lambda_i\left(\alpha_i - \left(1-\alpha_i\right)\varpi_i\tau_i\right)\ln\left(1-\varepsilon_i\right)} \\
&= -\frac{1}{\lambda_i\left(\frac{\alpha_i}{\tau_i} - \varpi_i\left(1-\alpha_i\right)\right)\ln\left(1-\varepsilon_i\right)}.
\end{aligned} \tag{13}
$$

Remark 2. *From (13), one can observe that $\rho\left(\varepsilon_i\right)$ monotonically decreases as λ_i increases. This implies to maintain a given ROP when channel quality improves, lower transmission SNR is required, which is easily understood. Moreover, one can realize the effect of α_i on $\rho\left(\varepsilon_i\right)$ is same as that of λ_i.*

Remark 3. *From (13), one can deduce that $\rho\left(\varepsilon_i\right)$ monotonically decreases as maximum tolerance of ε_i increases. This is also easy to accept since larger ε_i implies lower the requirement for ROP, which subsequently implies $\rho\left(\varepsilon_i\right)$ being lower.*

Remark 4. *In order to ensure the overall reliability of the strong user and the weak user, the minimum transmission SNR of the entire system $\rho_{\min}\left(\varepsilon\right)$ must be satisfied i.e., $\rho_{\min}\left(\varepsilon\right) = \max\left\{\rho\left(\varepsilon_n\right), \rho\left(\varepsilon_m\right)\right\}$.*

IV. Secrecy Outage Probability Analysis with Reliability Outage Constraint

The user U_i's instantaneous secrecy capacity is expressed as [15]

$$C_{s,j}^{x_i} = \left[C_b^{x_i} - C_{e,j}^{x_i}\right]^+, \tag{14}$$

where $j \in \{1,2\}$ represents the case of E's decoding capability, $C_{e,j}^{x_i} = \log_2\left(1+\gamma_{e,j}^{x_i}\right)$ signifies the capacity of the wiretap channel , and $[x]^+ = \max\{x, 0\}$.

SOP denotes the probability that the instantaneous secrecy capacity is less than a targeted secrecy rate [16]. In this section, we analyze the SOP of each user and the overall system with the ROP constraint under two scenarios according to different decoding capability of the eavesdropper E described above earlier.

Case 1: For the ROP constraint ε_n and the corresponding minimum transmit SNR $\rho\left(\varepsilon_n\right)$, utilizing (14) and Gaussian-chebyshev quadrature [17, (25.4.38)], the SOP for U_n is given by (15), shown at the top of this page, where $R_s^{x_i}$ denotes the targeted secrecy rate of the signal x_i, $\eta_s^{x_n} = 2^{R_s^{x_n}}$, $\Phi_1(x) = -a_1 + \frac{c_1}{b_1 - x}$, $a_1 = \frac{1}{\varpi_n\alpha_m\rho\left(\varepsilon_n\right)}$, $b_1 = \frac{a_1\left(\alpha_n - \varpi_n\alpha_m\left(\eta_s^{x_n}-1\right)\right)}{\alpha_n\eta_s^{x_n}}$, $c_1 = \frac{a_1^2}{\eta_s^{x_n}}$, K denotes the number of terms, $\omega_K = \frac{\pi}{K}$, $\phi_{k_1} = \cos\left(\frac{2k_1-1}{2K}\pi\right)$, and $\theta_{k_1} = \frac{b_1}{2}\left(\phi_{k_1}+1\right)$.

Remark 5. *Based on (15), one can observe that secrecy outage would occur at U_n when $\Lambda_1 < 0$, which is equal to $g_e > b_1$. When $b_1 < 0$, there is always $\Lambda_1 < 0$, which implies that the SOP of U_n is equal to 1. Thus, to obtain security at U_n, there is a constraint on α_n as*

$$\alpha_n > \frac{\varpi_n\left(\eta_s^{x_n}-1\right)}{1+\varpi_n\left(\eta_s^{x_n}-1\right)}. \tag{16}$$

$$
\begin{aligned}
P_{\text{out}}^{m,1} &= \Pr\left\{C_{s,1}^{x_m}(\varepsilon_m) < R_s^{x_m}\right\} \\
&= \Pr\left\{\left(\underbrace{1-\alpha_n\eta_s^{x_m}\left(1+\alpha_m\rho(\varepsilon_m)g_e\right)}_{\Lambda_2}\right)g_m < \frac{\eta_s^{x_m}\left(1+\alpha_m\rho(\varepsilon_m)g_e\right)-1}{\rho(\varepsilon_m)}\right\} \\
&= 1-\Pr\left\{g_m > \frac{\eta_s^{x_m}\left(1+\alpha_m\rho(\varepsilon_m)g_e\right)-1}{\Lambda_2\rho(\varepsilon_m)}, \Lambda_2>0\right\} \\
&= 1-\Pr\left\{g_m>\Phi_2(g_e), g_e<b_2\right\} \\
&= 1-\int_0^{b_2} e^{-\frac{\Phi_2(y)}{\lambda_m}} f_{g_e}(y)\,dy \\
&= 1-\frac{b_2}{2\lambda_e}\sum_{k_2=1}^{K}\omega_K\sqrt{1-\phi_{k_2}^2}\left(e^{-\frac{\Phi_2(\theta_{k_2})}{\lambda_m}-\frac{\theta_{k_2}}{\lambda_e}}\right)
\end{aligned} \tag{18}
$$

$$
\begin{aligned}
P_{\text{out}}^{1} &= 1-\Pr\left\{C_{s,1}^{x_n}\geqslant R_s^{x_n}, C_{s,1}^{x_m}\geqslant R_s^{x_m}\right\} \\
&= 1-\Pr\left\{g_n>\Phi_1(g_e), g_m>\Phi_2(g_e), g_e<b_5\right\} \\
&= 1-\int_0^{b_5}\left(1-F_{g_n}(\Phi_1(x))\right)\left(1-F_{g_m}(\Phi_2(x))\right)f_{g_e}(x)\,dx \\
&= 1-\frac{b_5}{2\lambda_e}\sum_{k_5=1}^{K}\omega_K\sqrt{1-\phi_{k_5}^2}\left(e^{-\frac{\Phi_1(\theta_{k_5})}{\lambda_n}-\frac{\Phi_2(\theta_{k_5})}{\lambda_m}-\frac{\theta_{k_5}}{\lambda_e}}\right)
\end{aligned} \tag{20}
$$

When $\varpi_n = 0$, which signifies pSIC is operated on the user U_n, (15) is rewritten as

$$
\begin{aligned}
P_{\text{out}}^{n,\mathrm{P}} &= \Pr\left\{g_n < \Phi_1^{\mathrm{P}}(g_e)\right\} \\
&= 1-\frac{\lambda_n}{\lambda_e\eta_s^{x_n}+\lambda_n}e^{-\frac{\eta_s^{x_n}-1}{\lambda_n\alpha_n\rho(\varepsilon_n)}},
\end{aligned} \tag{17}
$$

where $\Phi_1^{\mathrm{P}}(x) = \frac{\eta_s^{x_n}(1+\alpha_n\rho(\varepsilon_n)x)-1}{\alpha_n\rho(\varepsilon_n)}$. It should be noted that (17) matches the result in [10], as a special case.

Similar to (15), the SOP of U_m is obtained as (18), shown at the top of this page, where $\eta_s^{x_m} = 2^{R_s^{x_m}}$, $\Phi_2(x) = -a_2 + \frac{c_2}{b_2-x}$, $a_2 = \frac{1}{\alpha_n\rho(\varepsilon_m)}$, $b_2 = \frac{a_2(1-\alpha_n\eta_s^{x_m})}{\alpha_m\eta_s^{x_m}}$, $c_2 = \frac{a_2^2}{\eta_s^{x_m}}$, $\phi_{k_2} = \cos\left(\frac{2k_2-1}{2K}\pi\right)$, and $\theta_{k_2} = \frac{b_2}{2}\left(\phi_{k_2}+1\right)$.

Remark 6. *Similar to (15), to obtain security at U_m, there is a constrain on α_m as*

$$
\alpha_n < \frac{1}{\eta_s^{x_m}}. \tag{19}
$$

In this case, E is assumed to eavesdrop U_n and U_m at the same time because of its powerful decoding capability, thus the SOP of the NOMA system is derived as (20), shown at the top of this page, where $b_5 = \min\{b_1, b_2\}$, $\phi_{k_5} = \cos\left(\frac{2k_5-1}{2K}\pi\right)$, and $\theta_{k_5} = \frac{b_5}{2}\left(\phi_{k_1}+1\right)$.

Case 2: Similar to (15), the SOP of U_n in Case 2 is obtained as (21), shown at the top of the next page, where $\Phi_3(x) = -a_3 + \frac{c_3}{b_3-x}$, $a_3 = \frac{a_1(\varpi_n\alpha_m(\eta_s^{x_n}-1)+\eta_s^{x_n}\alpha_n)}{(\alpha_n+\varpi_n\alpha_m)(\eta_s^{x_n}-1)}$, $b_3 = \frac{a_1(\alpha_n-\varpi_n\alpha_m(\eta_s^{x_n}-1))}{(\alpha_n+\varpi_n\alpha_m)(\eta_s^{x_n}-1)}$, $c_3 = a_3b_3 + \frac{a_1}{\rho(\varepsilon_n)(\alpha_n+\varpi_n\alpha_m)}$, $\phi_{k_3} = \cos\left(\frac{2k_3-1}{2K}\pi\right)$, and $\theta_{k_3} = \frac{b_3}{2}\left(\phi_{k_3}+1\right)$. When $\varpi_n = 0$, the SOP of U_n in Case 2 is same as (17) since the decoding capability of the eavesdropper becomes same as that in Case 1.

With the same method, the SOP of the user U_m for Case 2 is derived in (22), shown at the top of the next page, where $\Phi_4(x) = -a_4 + \frac{c_4}{b_4-x}$, $a_4 = \frac{(\eta_s^{x_m}-\alpha_n)}{(\eta_s^{x_m}-1)\alpha_n\rho(\varepsilon_m)}$, $b_4 = \frac{1-\alpha_n\eta_s^{x_m}}{(\eta_s^{x_m}-1)\alpha_n\rho(\varepsilon_m)}$, $c_4 = a_4b_4 + \frac{1}{\rho(\varepsilon_m)^2\alpha_n}$, $\phi_{k_4} = \cos\left(\frac{2k_4-1}{2K}\pi\right)$, and $\theta_{k_4} = \frac{b_4}{2}\left(\phi_{k_4}+1\right)$.

Based on (21) and (22), the SOP of the NOMA system for Case 2 is obtained as

$$
P_{\text{out}}^{2} = 1-\left(1-P_{\text{out}}^{n,2}\right)\left(1-P_{\text{out}}^{m,2}\right). \tag{23}
$$

Remark 7. *Similar to (15) and (18), to obtain security at U_n and U_m, the conditions $b_3 > 0$ and $b_4 > 0$ must be met, which are the same constraints for α_n. After some algebraic manipulations, we obtain the following condition*

$$
\frac{\varpi_n\left(\eta_s^{x_n}-1\right)}{1+\varpi_n\left(\eta_s^{x_n}-1\right)} < \alpha_n < \frac{1}{\eta_s^{x_m}}. \tag{24}
$$

Although the decoding capability of E is different under the two scenarios, we obtain the same constraint for the power coefficient.

Remark 8. *Generally, the codeword rate is larger than the targeted secrecy rate , i.e., $R_b^{x_i} > R_s^{x_i}$ [1]. Since $1+\tau_i = 2^{R_b^{x_i}}$ and $\eta_s^{x_i} = 2^{R_s^{x_i}}$, we have $\tau_i + 1 > \eta_s^{x_i}$, then, $\frac{\varpi_n\tau_n}{1+\varpi_n\tau_n} > \frac{\varpi_n(\eta_s^{x_n}-1)}{1+\varpi_n(\eta_s^{x_n}-1)}$ and $\frac{1}{1+\tau_m} < \frac{1}{\eta_s^{x_m}}$. Thus, it can be found that the condition (12) is more strict than (24), which means outage over the main link always leads to secrecy outage event of the NOMA system. The result also fits well for general communication system. In other words, the legitimate user can not decode correctly while the illegitimate use possibly wiretaps a large amount of information.*

[1] $R_e^{x_i} = R_b^{x_i} - R_s^{x_i}$ is defined as the equivocation rate for x_i [14].

$$
\begin{aligned}
P_{\text{out}}^{n,2} &= \Pr\left\{C_{s,2}^{x_n}\left(\varepsilon_n\right) < R_s^{x_n}\right\} \\
&= \Pr\left(\left(\underbrace{\alpha_n - \varpi_n\left(\eta_s^{x_n}\left(1+\frac{\alpha_n\rho\left(\varepsilon_n\right)g_e}{\varpi_n\rho\left(\varepsilon_n\right)g_e+1}\right)-1\right)}_{\Lambda_3}\right)\rho\left(\varepsilon_n\right)g_n < \eta_s^{x_n}\left(1+\frac{\alpha_n\rho\left(\varepsilon_n\right)g_e}{\varpi_n\rho\left(\varepsilon_n\right)g_e+1}\right)-1\right) \\
&= 1-\Pr\left(g_n > \frac{\eta_s^{x_n}\left(1+\frac{\alpha_n\rho(\varepsilon_n)g_e}{\varpi_n\rho(\varepsilon_n)g_e+1}\right)-1}{\Lambda_3\rho\left(\varepsilon_n\right)}, \Lambda_3 > 0\right) \\
&= 1-\Pr\left\{g_n > \Phi_3\left(g_e\right), g_e < b_3\right\} \\
&= 1-\frac{b_3}{2\lambda_e}\sum_{k_3=1}^{K}\omega_K\sqrt{1-\phi_{k_3}^2}\,e^{-\frac{\Phi_3\left(\theta_{k_3}\right)}{\lambda_n}-\frac{\theta_{k_3}}{\lambda_e}}
\end{aligned}
\tag{21}
$$

$$
\begin{aligned}
P_{\text{out}}^{m,2} &= \Pr\left\{C_{s,2}^{x_m}\left(\varepsilon_m\right) < R_s^{x_m}\right\} \\
&= \Pr\left\{\log_2\left(1+\frac{\alpha_m\rho\left(\varepsilon_m\right)g_m}{\alpha_n\rho\left(\varepsilon_m\right)g_m+1}\right)-\log_2\left(1+\frac{\alpha_m\rho\left(\varepsilon_m\right)g_e}{\alpha_n\rho\left(\varepsilon_m\right)g_e+1}\right) < R_s^{x_m}\right\} \\
&= \Pr\left(\left(\underbrace{1-\alpha_n\eta_s^{x_m}\left(1+\frac{\alpha_m\rho\left(\varepsilon_m\right)g_e}{\alpha_n\rho\left(\varepsilon_m\right)g_e+1}\right)}_{\Lambda_4}\right)g_m < \frac{\eta_s^{x_m}\left(1+\frac{\alpha_m\rho(\varepsilon_m)g_e}{\alpha_n\rho(\varepsilon_m)g_e+1}\right)-1}{\rho\left(\varepsilon_m\right)}\right) \\
&= 1-\Pr\left(g_m > \frac{\eta_s^{x_m}\left(1+\frac{\alpha_m\rho(\varepsilon_m)g_e}{\alpha_n\rho(\varepsilon_m)g_e+1}\right)-1}{\Lambda_4\rho\left(\varepsilon_m\right)}, \Lambda_4 > 0\right) \\
&= 1-\Pr\left\{g_m > \Phi_4\left(g_e\right), g_e < b_4\right\} \\
&= 1-\frac{b_4}{2\lambda_e}\sum_{k_4=1}^{K}\omega_K\sqrt{1-\phi_{k_4}^2}\,e^{-\frac{\Phi_4\left(\theta_{k_4}\right)}{\lambda_n}-\frac{\theta_{k_4}}{\lambda_e}}
\end{aligned}
\tag{22}
$$

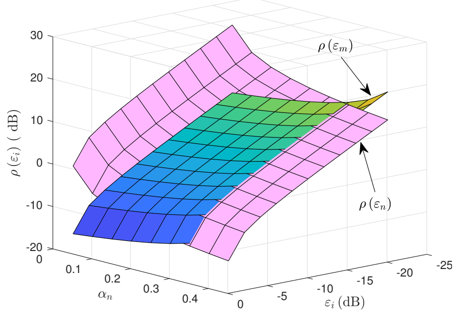

Fig. 2. $\rho(\varepsilon)$ for various α_n and ε with $\lambda_n = 15$ dB, $\lambda_m = 10$ dB, $\varpi_n = 0.01$, $R_b^{x_n} = 2$ bit/s/Hz, and $R_b^{x_m} = 1$ bit/s/Hz.

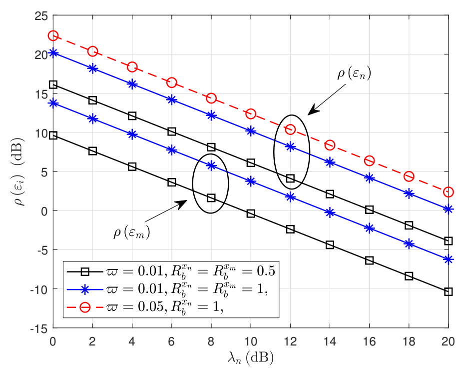

Fig. 3. $\rho(\varepsilon_i)$ for various λ_n, ϖ_n, and $R_b^{x_i}$ with $\alpha_n = 0.1$, $\varepsilon_n = \varepsilon_m = 0.1$, and $\lambda_m = 0.5\lambda_n$.

V. Numerical Results

In this section, we utilize numerical results to prove our analysis about transmission outage constraint. And the analysis of SOP is testified via Monte-Carlo simulation. The main parameters are set to $\sigma^2 = 1$, $\varepsilon_n = \varepsilon_m = \varepsilon$, $R_b^{x_n} = 2$ bit/s/Hz, $R_b^{x_m} = 1$ bit/s/Hz, $R_s^{x_n} = 1$ bit/s/Hz, $R_s^{x_m} = 0.5$ bit/s/Hz, and $\varpi_n = 0.01$. 'Ana' and 'Sim' are utilized to represent 'Analysis' and 'Simulation', respectively.

Figs. 2 - 3 present the trend of $\rho(\varepsilon_i)$, which correspond to the target ROP ε_i. We can observe $\rho(\varepsilon_n)$ intersecting with $\rho(\varepsilon_m)$, which means there is no strict distinction between the minimum transmission SNR required by users U_n and U_m. Therefore, it is necessary to take *Remark 4* into consideration when we analyze the SOP of the NOMA system. Especially, the smaller the ε_i is, the higher the reliability of user communication is. What's more interesting is that it also signifies the corresponding transmit power of system becoming higher if the NOMA system requires

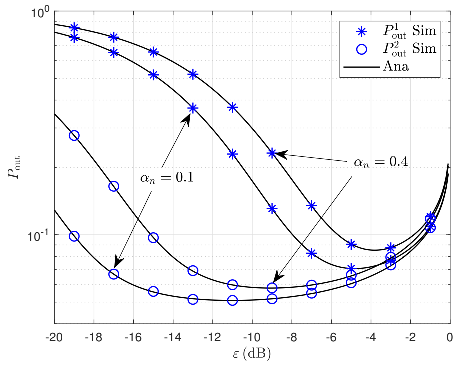

Fig. 4. SOP of the NOMA system for varying α_n and ε with $\lambda_n = 15$ dB, $\lambda_m = 10$ dB, and $\lambda_e = -5$ dB.

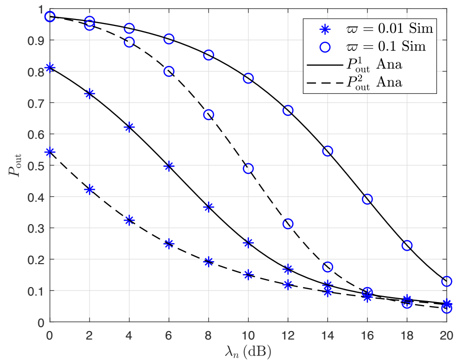

Fig. 5. SOP of the NOMA system for varying ϖ and λ_n with $\alpha_n = 0.1$, $\lambda_m = 0.5\lambda_n$, $\lambda_e = -5$ dB, $R_b^{x_n} = 1$ bit/s/Hz,$R_b^{x_m} = 0.5$ bit/s/Hz $R_s^{x_n} = 0.2$ bit/s/Hz, $R_b^{x_m} = 0.1$ bit/s/Hz, and $\varepsilon_n = \varepsilon_m = -10$ dB.

ε_i to be smaller.

Fig. 4 demonstrates the SOP of the NOMA system versus ε under two scenarios. One can easily observe the SOP of the NOMA system decreases initially and subsequently increases with improvement in the target ROP constraint ε. The SOP in Case 2 outperforms that in Case 1 since E's decoding capability in Case 1 is stronger than that in Case 2. Moreover, the secrecy performance with a larger α_n is worse to that with a lower α_n because more power is allocated for the weak user, which is the bottleneck of the NOMA systems. One can observe there is a trade-off between reliability and security of communication, which implies the reliability and security of the NOMA system must be carefully chosen for different scenarios with different requirements.

Fig. 5 presents the SOP of the NOMA system for varying ϖ under two scenarios. One can observe the secrecy outage performance of the NOMA systems improves with improvement in channel quality. Furthermore, the SOP with larger ϖ underperforms than that with a smaller ϖ since a lower ϖ signifies a higher level of SIC, which results into larger SINR at the near user and subsequently leading to better secrecy performance.

VI. Conclusion

In this work, the relationship between the reliability and security of the downlink NOMA systems was investigated. The effect of different parameters on the minimum transmit SNR for the NOMA system with the constraint of ROP and ipSIC was analyzed. With the consideration of two different decoding capabilities at the eavesdropper and ipSIC, the analytical expressions of the SOP under the ROP constraint were derived. Numerical results were validated via the Monte-Carlo simulation.

Acknowledgements

This work was supported by the National Natural Science Foundation of China under Grant 61971080, Natural Science Foundation Project of Chongqing under Grant cstc2019jcyj-msxmX0032, and the Open Fund of the Shaanxi Key Laboratory of Information Communication Network and Security under Grant ICNS201807.

References

[1] Z. Ding, Y. Liu, J. Choi, Q. Sun, M. Elkashlan, C.-L. I, and H. V. Poor, “Application of non-orthogonal multiple access in LTE and 5G networks,” *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 185-191, Feb. 2017.

[2] L. Lv, J. Chen, Q. Ni, Z. Ding, and H. Jiang, “Cognitive non-orthogonal multiple access with cooperative relaying: A new wireless frontier for 5G spectrum sharing,” *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 188-195, Apr. 2018.

[3] S. M. R. Islam, M. Zeng, O. A. Dobre, and K.-S. Kwak, “Resource allocation for downlink NOMA systems: Key techniques and open issues,” *IEEE Wireless Commun.*, vol. 25, no. 2, pp. 40-47, Apr. 2018.

[4] Z. Ding, Z. Yang, P. Fan, and H. V. Poor,“On the performance of non-orthogonal multiple access in 5G systems with randomly deployed users,” *IEEE Signal Process. Lett.*, vol. 21, no. 12, pp. 1501-1505, Dec. 2014.

[5] Z. Shi, H. Wang, Y. Fu, G. Yang, S. Ma, F. Hou, and T. A. Tsiftsis, “Zero-forcing based downlink virtual MIMO-NOMA communications in IoT networks," *IEEE Internet Things J.*, doi: 10.1109/jiot.2019.2957209, Dec. 2019.

[6] X. Yue, Z. Qin, Y. Liu, S. Kang, and Y. Chen, “A unified framework for non-orthogonal multiple access,” *IEEE Trans. Commun.*, vol. 66, no. 11, pp. 5346-5359, Nov. 2018.

[7] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, “A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727-1765, May 2016.

[8] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, “Physical layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8169-8181, Oct. 2019.

[9] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, “Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks,” *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1656-1672, Mar. 2017.

[10] H. Lei, J. Zhang, K.-H. Park, P. Xu, I. S. Ansari, G. Pan, B. Alomair, and M.-S. Alouini, “On secure NOMA systems with transmit antenna selection schemes,” *IEEE Access*, vol. 5, pp. 17450-17464, Sept. 2017.

[11] L. Lv, Z. Ding, J. Chen, and N. Al-Dhahir, “Design of secure NOMA against full-duplex proactive eavesdropping,” *IEEE Wireless Commun. Lett.*, vol. 8, no. 4, pp. 1090-1094, Aug. 2019.

[12] X. Yue, Y. Liu, Y. Yao, X. Li, Rongke Liu, and A. Nallanathan. “Secure communications in a unified non-orthogonal multiple access framework," arXiv:1904.01459, Apr. 2019, [Online]: https://arxiv.org/abs/1904.01459

[13] H. Lei, Z. Yang, K.-H. Park, I. S. Ansari, Y. Guo, G. Pan, and M.-S. Alouini, “Secrecy outage analysis for cooperative NOMA systems with relay selection schemes,” *IEEE Trans. Commun.*, vol. 67, no. 9, pp. 6282-6298, Sept. 2019.

[14] G. Gomez, F. J. Martin-Vega, F. J. Lopez-Martinez, Y. Liu, and M. Elkashlan, “Physical layer security in uplink NOMA multi-antenna systems with randomly distributed eavesdroppers,” *IEEE Access*, vol. 7, pp. 70422-70435, Jun. 2019.

[15] I. Csiszar and J. Korner,“Broadcast channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339-348, May 1978.

[16] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin,“Wireless information-theoretic security,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515-2534, Jun. 2008.

[17] M. Abramowitz and I. Stegun, *Handbook of Mathematical Functions With Formulas, Graphs, and Mathematical Tables*, 9th. New York, NY, USA: Discover, 1972.