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 (MIMO) 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 considered.

- 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 analyzed, 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.
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 \( \sigma^2 \). 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 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 \( s = (\sqrt{\alpha_n} x_n + \sqrt{\alpha_m} x_m) \) 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., \( \mathbb{E}[|x_n|^2] = \mathbb{E}[|x_m|^2] = 1 \), and the \( \alpha_i \) 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

\[
\gamma_{n}^{x} = \frac{\alpha_n \rho g_n}{\alpha_n \rho g_n + 1}, \quad \gamma_{n}^{x} = \frac{\alpha_n \rho g_n}{\alpha_n \rho g_n + 1},
\]

(1)

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

\[
\gamma_{m}^{x} = \frac{\alpha_m \rho g_m}{\alpha_m \rho g_m + 1}.
\]

(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 \( x_1 \), and the corresponding SINRs, \( \gamma_{e}^{x} \), 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 \( x_1 \) is given by

\[
\gamma_{e}^{x} = \alpha_i \rho g_e.
\]

(3)

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

Case 2: \( E \) has 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

\[
\gamma_{e}^{x} = \frac{\alpha_n \rho g_e}{\alpha_n \rho g_e + 1}, \quad \gamma_{m}^{x} = \frac{\alpha_m \rho g_e}{\alpha_m \rho g_e + 1}.
\]

(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 \( \gamma_1, \gamma_2, \gamma_3 \) into \( \{\gamma_n, \gamma_2, \gamma_3\} \), \( \{\gamma_1, \gamma_2, \gamma_3\} \), \( \{\gamma_1, \gamma_2, \gamma_3\} \), and \( \{\gamma_1, \gamma_2, \gamma_3\} \). The cumulative distribution function (CDF) of \( \gamma_1 \) is obtained as

\[
F_{\gamma_1}(x) = P(\gamma_1 < x) = P\left\{ \frac{\alpha_n \rho g_{j_1} + 1}{\alpha_n \rho g_{j_1} + 1} < x \right\} = P\left\{ \frac{\alpha_n - \alpha_n \rho g_{j_1} + 1}{\alpha_n \rho g_{j_1} + 1} < x \right\} = 1 - e^{-\frac{\alpha_n \rho g_{j_1}}{\alpha_n \rho g_{j_1} + 1}}, \quad x < \frac{\alpha_n}{\alpha_n \rho g_{j_1} + 1},
\]

(5)

And the CDF of \( \gamma_2 \) and \( \gamma_3 \) are given by

\[
F_{\gamma_2}(x) = 1 - e^{-\frac{\alpha_n \rho g_{j_2}}{\alpha_n \rho g_{j_2} + 1}}, \quad F_{\gamma_3}(x) = \begin{cases} 1 - e^{-\frac{\alpha_n \rho g_{j_3}}{\alpha_n \rho g_{j_3} + 1}}, & x < \frac{\alpha_n}{\alpha_n \rho g_{j_3} + 1}, \\ 1, & x \geq \frac{\alpha_n}{\alpha_n \rho g_{j_3} + 1}, \end{cases}
\]

(6)

respectively.

Fig. 1. System model consisting of a base station (S), two legitimate users (\( U_n \) and \( U_m \)), and an illegitimate eavesdropper (E).
\[ P_{\text{out}} = \Pr \{ C_{b,i}^x (\varepsilon_i) < R_{b,i}^x \} \]

\[ = \Pr \left\{ \left( \alpha_n - \omega_n \alpha_m \left( \frac{\alpha_n \eta_b^x \rho(\varepsilon_i) g_b + \eta_b^x - 1}{\Lambda_1} \right) \rho(\varepsilon_i) g_n < \frac{\alpha_n \eta_b^x \rho(\varepsilon_i) g_b + \eta_b^x - 1}{\Lambda_1}, \Lambda_1 > 0 \right) \right\} \]

\[ = 1 - \Pr \left\{ g_n > \frac{\alpha_n \eta_b^x \rho(\varepsilon_i) g_b + \eta_b^x - 1}{\Lambda_1 \rho(\varepsilon_i)} \right\} \]

\[ = 1 - \Pr \left\{ g_n > \Phi_1 (g_e), g_e < b_1 \right\} \]

\[ = 1 - b_1 \frac{\lambda}{2n} \sum_{k=1}^{\lambda} \frac{\omega_k}{\sqrt{1 - \phi_{k_1}^2 (\xi_n)}} \frac{\eta_b^x}{\phi_{k_1}}. \]  

(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

\[ C_b^x = \log_2 \left( 1 + \gamma_b^x \right). \]  

(8)

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

\[ O_x (R_{b,i}^x) = \Pr \{ R_{b,i}^x > C_b^x \}, \]  

(9)

where \( R_{b,i}^x \) 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

\[ O_x (R_{b,i}^x) = \Pr \{ C_b^x < R_{b,i}^x \} \leq \varepsilon \]

\[ \Leftrightarrow (\alpha_i - \omega_i (1 - \alpha_i) \tau_i) \rho \lambda_i \geq - \frac{\tau_i}{\ln (1 - \varepsilon)}. \]  

(10)

where \( \tau_i = 2R_{b,i}^x - 1, \varepsilon \) 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 \( \alpha_i - \omega_i (1 - \alpha_i) \tau_i < 0 \). This signifies that in order to ensure reliability at \( U_i \), there is a constraint for the power allocation coefficients, which is expressed as

\[ \alpha_i > \frac{\omega_i \tau_i}{1 + \omega_i \tau_i}. \]  

(11)

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

\[ \frac{\omega_i \tau_i}{1 + \omega_i \tau_i} < \alpha_n < \frac{1}{1 + \tau_m}. \]  

(12)

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

\[ \rho (\varepsilon_i) \geq - \frac{\tau_i}{\ln (1 - \varepsilon)} \]

\[ = - \frac{1}{\lambda_i} \frac{\omega_i (\alpha_i - (1 - \alpha_i) \omega_i \tau_i) \ln (1 - \varepsilon_i)}{1 - \alpha_i} \]

\[ \alpha_n > \frac{\omega_i (\eta_b^x - 1)}{1 + \omega_i (\eta_b^x - 1)}. \]  

(13)

**Remark 2.** From (13), one can observe that \( \rho (\varepsilon_i) \) monotonically decreases as \( \lambda_i \) 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 \( \alpha_i \) on \( \rho (\varepsilon_i) \) is same as that of \( \lambda_i \).

**Remark 3.** From (13), one can deduce that \( \rho (\varepsilon_i) \) monotonically decreases as maximum tolerance of \( \varepsilon_i \) increases. This is also easy to accept since larger \( \varepsilon_i \) implies lower the requirement for ROP, which subsequently implies \( \rho (\varepsilon_i) \) 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 \( \rho_{\text{min}} (\varepsilon) \) must be satisfied i.e., \( \rho_{\text{min}} (\varepsilon) = \max \{ \rho(\varepsilon_n), \rho(\varepsilon_m) \} \).

### IV. Secrecy Outage Probability Analysis with Reliability Outage Constraint

The user \( U_i \)’s instantaneous secrecy capacity is expressed as

\[ C_{s,j}^x = \left[ C_b^x - C_{e,j}^x \right]^+, \]  

(14)

where \( j \in \{1, 2\} \) represents the case of \( E \)’s decoding capability, \( C_{s,j}^x = \log_2 (1 + \gamma_s^x) \) signifies the capacity of the wiretap channel, and \( [x]^+ = \max \{ x, 0 \} \).

ROP 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 \( \varepsilon_n \) and the corresponding minimum transmit SNR \( \rho (\varepsilon_n) \), utilizing (14) and Gaussian-cholesky quadrature [17, (25.4.38)], the SOP for \( U_n \) is given by (15), shown at the top of this page, where \( R_{b_i}^x \) denotes the targeted secrecy rate of the signal \( x_i \), \( \eta_b^x = 2R_{b_i}^x \), \( \Phi_1 (x) = -a_1 + \frac{\alpha_i}{\eta_b^x}, a_1 = \frac{\omega_i (\alpha_i - \omega_i \tau_i)}{\alpha_n \omega_i \tau_i}, b_1 = \frac{\omega_i (\alpha_i - \omega_i \tau_i) \ln (1 - \varepsilon_i)}{\alpha_n \omega_i \tau_i}, c_1 = \frac{\omega_i \tau_i}{\eta_b^x}, K \) denotes the number of terms, \( \omega_K = \frac{\pi}{K}, \phi_{k_1} = \cos \left( \frac{2k_1 - 1}{2K} \pi \right) \), and \( \theta_{k_1} = \frac{\pi}{2} (\phi_{k_1} + 1) \).

**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 \( \alpha_n \) as

\[ \alpha_n > \frac{\omega_i (\eta_b^x - 1)}{1 + \omega_i (\eta_b^x - 1)}. \]  

(16)
When \( \bar{\omega}_n = 0 \), which signifies pSIC is operated on the user \( U_n \), (15) is rewritten as
\[
P_{out}^{m,p} = \Pr \left\{ C_{s,1}^{m} < R_{s}^{m} \right\} = 1 - \frac{\lambda_n}{\lambda_e \eta_n^m - \lambda_n} e^{-\frac{\pi^2}{\lambda_n \eta_n^m \alpha_m m^2 \pi^2}} \tag{17}
\]
where \( \Phi_m^P(x) = \frac{\eta_n^m (1 + \alpha_m \rho(x_\bar{n}) \rho(x) - 1)}{\alpha_m \rho(x_\bar{n}) \rho(x)} \). 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 \( \eta_n^m = \eta_n^m \), \( \Phi_m^P(x) = -a_2 + \frac{b_2}{b_2 - x} \), \( a_2 = \frac{1}{2 \alpha_m \rho(x_\bar{n})}, \) \( b_2 = \frac{2 \alpha_m \rho(x_\bar{n}) \rho(x)}{\eta_n^m}, \) \( c_2 = \frac{a_2^2}{\eta_n^m}, \) \( \phi_k^m = \cos \left( \frac{2 k \eta_n^m - 1}{\eta_n^m} \right) \), and \( \theta_k^m = b_2 \left( \phi_k^m + 1 \right) \).

\textbf{Remark 6.} Similar to (15), to obtain security at \( U_m \), there is a constrain on \( \alpha_m \) as
\[
\alpha_m < \frac{1}{\eta_n^m}. \tag{19}
\]
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 \( b_5 = \min \{ b_1, b_2 \}, \) \( \phi_k^m = \cos \left( \frac{2 k \eta_n^m - 1}{\eta_n^m} \right) \), and \( \theta_k^m = b_2 \left( \phi_k^m + 1 \right) \).

\textbf{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 \( \Phi_3(x) = -a_3 + \frac{\eta_n^m}{\eta_n^m}, \) \( a_3 = \frac{1}{2 \alpha_m \rho(x_\bar{n}) \rho(x)}, \) \( b_3 = \frac{2 \alpha_m \rho(x_\bar{n}) \rho(x)}{\eta_n^m}, \) \( c_3 = \frac{a_3^2}{\eta_n^m}, \) \( \phi_k^m = \cos \left( \frac{2 k \eta_n^m - 1}{\eta_n^m} \right) \), and \( \theta_k^m = b_2 \left( \phi_k^m + 1 \right) \). When \( \bar{\omega}_n = 0 \), 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 \( \Phi_4(x) = -a_4 + \frac{\eta_n^m}{\eta_n^m}, \) \( a_4 = \frac{1}{2 \alpha_m \rho(x_\bar{n}) \rho(x)}, \) \( b_4 = \frac{2 \alpha_m \rho(x_\bar{n}) \rho(x)}{\eta_n^m}, \) \( c_4 = \frac{a_4^2}{\eta_n^m}, \) \( \phi_k^m = \cos \left( \frac{2 k \eta_n^m - 1}{\eta_n^m} \right) \), and \( \theta_k^m = b_2 \left( \phi_k^m + 1 \right) \). Although the decoding capability of \( E \) is different under the two scenarios, we obtain the same constraint for the power coefficient.

\textbf{Remark 8.} Generally, the codeword rate is larger than the targeted secrecy rate : i.e., \( R_x^e > R_x^m \). Since \( 1 + \tau_i = \frac{2 \tau_i}{\alpha_m \rho(x_\bar{n}) \rho(x)} \) and \( \eta_n^m = \frac{2 \tau_i}{\alpha_m \rho(x_\bar{n}) \rho(x)} \), we have \( \tau_i + 1 > \eta_n^m \), then, \( \frac{\bar{\omega}_n \eta_n^m}{\alpha_m \rho(x_\bar{n}) \rho(x)} > \frac{1}{\alpha_m \rho(x_\bar{n}) \rho(x)} \) and \( 1 + \tau_i > \eta_n^m \). 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.

\[ R_x^e = R_x^m - R_x^e \] is defined as the equivocation rate for \( x_i \) [14].
\[ P_{\text{out}}^{m,2} = \Pr \left\{ C_{s,2} (\varepsilon) < R_{s}^{x_m} \right\} \]
\[ = \Pr \left\{ \frac{\alpha - \mu_n \left( \eta_n^{x} \left( 1 + \frac{\alpha_n \rho (\varepsilon_n) g_e}{\epsilon_n \rho (\varepsilon_n) g_e + 1} \right) - 1 \right)}{\Lambda_2} < \frac{\rho (\varepsilon_n) g_n}{\eta_n^{x}} \left( 1 + \frac{\alpha_n \rho (\varepsilon_n) g_e}{\epsilon_n \rho (\varepsilon_n) g_e + 1} \right) - 1 \right\} \]
\[ = 1 - \Pr \left\{ g_n > \frac{\eta_n^{x} \left( 1 + \frac{\alpha_n \rho (\varepsilon_n) g_e}{\epsilon_n \rho (\varepsilon_n) g_e + 1} \right) - 1}{\Lambda_2} \right\} \]
\[ = 1 - \Pr \left\{ g_n > \Phi_3 (g_e), g_e < b_3 \right\} \]
\[ = 1 - \frac{b_3}{2 \lambda_e} \sum_{k=1}^{K} \omega_e \sqrt{1 - \phi_k^2} e^{-\frac{s_3 (s_4)}{x_n}} \frac{s_4}{x_n} \]  

\[ P_{\text{out}}^{m,2} = \Pr \left\{ C_{s,2} (\varepsilon) < R_{s}^{x_m} \right\} \]
\[ = \Pr \left\{ \log_2 \left( 1 + \frac{\alpha_n \rho (\varepsilon_n) g_m}{\alpha_n \rho (\varepsilon_n) g_m + 1} \right) - \log_2 \left( 1 + \frac{\alpha_n \rho (\varepsilon_n) g_m}{\alpha_n \rho (\varepsilon_n) g_m + 1} \right) < R_{s}^{x_m} \right\} \]
\[ = \Pr \left\{ \frac{1 - \alpha_n \eta_n^{x_m} \left( 1 + \frac{\alpha_n \rho (\varepsilon_n) g_e}{\epsilon_n \rho (\varepsilon_n) g_e + 1} \right)}{\Lambda_4} < \frac{\eta_n^{x_m} \left( 1 + \frac{\alpha_n \rho (\varepsilon_n) g_e}{\epsilon_n \rho (\varepsilon_n) g_e + 1} \right) - 1}{\rho (\varepsilon_m)} \right\} \]
\[ = 1 - \Pr \left\{ g_m > \frac{\eta_n^{x_m} \left( 1 + \frac{\alpha_n \rho (\varepsilon_n) g_e}{\epsilon_n \rho (\varepsilon_n) g_e + 1} \right) - 1}{\Lambda_4} \right\} \]
\[ = 1 - \Pr \left\{ g_m > \Phi_4 (g_e), g_e < b_4 \right\} \]
\[ = 1 - \frac{b_4}{2 \lambda_e} \sum_{k=1}^{K} \omega_e \sqrt{1 - \phi_k^2} e^{-\frac{s_3 (s_4)}{x_n}} \frac{s_4}{x_n} \]

Fig. 2. \( \rho (\varepsilon) \) for various \( \alpha_n \) and \( \varepsilon \) with \( \lambda_n = 15 \) dB, \( \lambda_m = 10 \) dB, \( \omega_n = 0.01 \), \( R_{s}^{x_n} = 2 \) bit/s/Hz, and \( R_{s}^{x_m} = 1 \) bit/s/Hz.

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 \( \sigma^2 = 1 \), \( \varepsilon_n = \varepsilon_m = \varepsilon \), \( R_{s}^{x_n} = 2 \) bit/s/Hz, \( R_{s}^{x_m} = 1 \) bit/s/Hz, \( R_{s}^{x_n} = 0.5 \) bit/s/Hz, and \( \omega_n = 0.01 \). ‘Ana’ and ‘Sim’ are utilized to represent ‘Analysis’ and ‘Simulation’, respectively.

Fig. 3. \( \rho (\varepsilon) \) for various \( \lambda_n \), \( \omega_n \), and \( R_{s}^{x_m} \) with \( \alpha_n = 0.1 \), \( \varepsilon_n = \varepsilon_m = 0.1 \), and \( \lambda_m = 0.5 \lambda_n \).
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 cstc2019jcjmsxmX0032, and the Open Fund of the Shaanxi Key Laboratory of Information Communication Network and Security under Grant ICNS201807.

REFERENCES