Secure MISO-NOMA Transmission With Artificial Noise

Lu Lv, *Student Member, IEEE*, Zhiguo Ding, *Senior Member, IEEE*, Qiang Ni, *Senior Member, IEEE*, and Jian Chen, *Member, IEEE*

***Abstract*—This paper studies a new secrecy beamforming (SBF) scheme for multiple-input single-output non-orthogonal multiple access (MISO-NOMA) systems. In particular, the proposed SBF scheme efficiently exploits artificial noise to protect the confidential information of two NOMA assisted legitimate users, such that only the eavesdropper's channel is degraded. Considering a practical assumption of the imperfect worst-case successive interference cancellation which is a unique character in employing NOMA transmission, we derive a closed-form expression for the secrecy outage probability to characterize the secrecy performance. After that, we carry out an analysis of secrecy diversity order to provide further insights about secure MISO-NOMA transmission. Numerical results are provided to demonstrate the accuracy of the developed analytical results and the effectiveness of the proposed SBF scheme.**

***Index Terms*—Non-orthogonal multiple access, multiple-input single-output, physical layer security, artificial noise.**

I. Introduction

Non-orthogonal multiple access (NOMA), which efficiently exploits power domain multiplexing at transmitter(s) and successive interference cancellation (SIC) at receiver(s) to serve multiple users in the same resource block (e.g., time/frequency/code domain), has shown its promising potential to improve wireless spectrum efficiency [1]–[4]. Owing to the broadcast nature of radio frequency communications, the confidential information is vulnerable to passive eavesdropping, and thus, guaranteeing secure NOMA transmission by enlisting the help of physical layer security technique has attracted enormous research attention (see, e.g., [5]–[10] and references therein).

It is known that better secrecy can be achieved with the aid of artificial noise (AN) masking in conventional multiple-input single-output orthogonal multiple access (MISO-OMA) systems [11]–[13]. This concept has been applied in MISO-NOMA systems, where two precoding matrices are designed to secure two NOMA assisted legitimate users (LUs) against a passive eavesdropper (Eve) [5]. However, directly employing conventional AN-aided scheme to secure MISO-NOMA transmission has the following limitations:

- The NOMA assisted LUs are severely subjected to interference, and thus the secrecy beamforming (SBF) scheme in [5] inevitably causes the situation that AN leaks into the range space of the NOMA assisted LUs, which yields more interference and leads to a poor reception quality at the NOMA assisted LUs.
- The individual precoding matrix exclusively increases the signal strength for its intended LU, indicating that the weak LU's signal strength becomes worse than that of the strong LU at the time of NOMA signal detection. This may cause an unsuccessful SIC processing, which further results in both transmission outage and secrecy outage.

On this basis, the conventional AN-aided scheme for MISO-OMA systems should be carefully modified to be applicable for secure MISO-NOMA transmission. To overcome the aforementioned limitations, we propose a new SBF scheme which efficiently exploits AN for security enhancement of MISO-NOMA tarnsmission. The main contributions of this paper are summarized as follows.

- To guarantee secure MISO-NOMA transmission, we develop a new SBF scheme by exploiting AN. Particularly, AN is generated such that it lies in the null space of the main channel and no AN leaks into the range space of LUs, yielding an acceptable reception quality. Furthermore, the proposed beamforming matrix artificially creates the difference between LUs' channel gains, thus the potential of NOMA can be fully realized even if the two LUs have the same channel statistics.
- The secrecy outage performance of the proposed SBF scheme is analyzed by considering the imperfect worst-case SIC assumption, which is found to be highly realistic for scenarios of practical interest. Note that the imperfect worst-case SIC may induce either a transmission outage or a secrecy outage at the NOMA assisted LUs, which is an essential characteristic in analyzing secure NOMA communications. This makes the secrecy outage analysis of our proposed SBF scheme being different from that in [5], where an optimistic assumption of the perfect SIC at the NOMA assisted LUs has been adopted.
- We theoretically derive closed-form expression of the secrecy outage probability (SOP) for each LU, and validate its accuracy by computer simulations. In order to provide further insights, we also carry out an analysis of secrecy diversity order. Numerical results show that an improved secrecy outage performance for MISO-NOMA systems can be achieved by our proposed SBF scheme.

The work of L. Lv and J. Chen was supported in part by the National Natural Science Foundation of China under Grants 61771366 and 61601347, in part by the Natural Science Basic Research Plan in Shaanxi Province of China under Grant 2017JQ6055, and in part by the "111" project of China under Grant B08038. The work of Z. Ding was supported by the UK EPSRC under Grants EP/P009719/1 and EP/N005597/1. The work of Q. Ni was supported in part by the EU FP7 CROWN project under Grant PIRSES-GA-2013-610524, and in part by the UK EPSRC under Grant EP/K011693/1. The associate editor coordinating the review of this paper and approving it for publication was Dr. R. Souza. *(Corresponding author: Jian Chen.)*

L. Lv and J. Chen are with the State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China (e-mail: lulv@stu.xidian.edu.cn; jianchen@mail.xidian.edu.cn).

Z. Ding and Q. Ni are with the School of Computing and Communications, Lancaster University, Lancaster LA1 4WA, UK (e-mail: z.ding@lancaster.ac.uk; q.ni@lancaster.ac.uk).

II. System Model and Scheme Description

A. Channel Model

Consider a downlink secure MISO-NOMA scenario, where the confidential communication between a M-antenna base station (BS) and two NOMA assisted single-antenna LUs (e.g., LU_1 and LU_2) is overheard by a N-antenna Eve.[1] We assume that $M > N$, because otherwise the Eve can eliminate AN and cannot support perfect secrecy communication [11], [13]. The channels in the system experience quasi-static fading, e.g., the channel gains remain unchanged during one fading block but vary independently among different fading blocks. The length of a fading block is one time unit. Consider one fading block, the $1 \times M$ channel vector between BS and LU_k is denoted by $\mathbf{h}_k$ for $k = 1, 2$, and the $N \times M$ channel matrix between BS and Eve is denoted by $\mathbf{H}_\text{e}$. The entries of $\mathbf{h}_k$ and $\mathbf{H}_\text{e}$ are modeled as independent and identically distributed (i.i.d.) complex Gaussian variables with mean being zero and variance being unit. In this work, we focus on the scenario without path loss, and thus, the channel gains of the two LUs have the same statistics, which yields a challenging situation to exploit the potential of NOMA.[2] Similar to [5], [11]–[13], we consider a practical passive eavesdropping scenario which means that the Eve only listens but does not transmit, therefore the instantaneous knowledge of $\mathbf{H}_\text{e}$ is not available at Eve. While $\mathbf{h}_k$ can be precisely estimated by LU_k and fed back to BS and Eve over an authenticated broadcast channel. The noises corrupted by LUs and Eve are modeled as the additive white Gaussian noises (AWGNs) with mean being zero and variances being σ_b^2 and σ_e^2, respectively.

Notations: Throughout the paper, the following notations will be used: $[\cdot]^T$ denotes the matrix transpose operation, $[\cdot]^\dagger$ denotes the complex conjugate transpose operation, diag$[\cdot]$ denotes the diagonal matrix, $\mathbf{I}_n$ denotes the $n \times n$ identity matrix, $\mathbb{E}[\cdot]$ denotes the expectation operation, $||\cdot||$ denotes the norm of a vector, $|\cdot|$ denotes the determinant of a matrix, and $(\cdot)^{-1}$ denotes the inverse.

B. Proposed SBF Scheme

To guarantee secure MISO-NOMA transmission, a new SBF scheme which efficiently exploits AN is proposed to protect the confidential information. Specifically, we design an $M \times (M-1)$ beamforming matrix $\mathbf{W} = [\mathbf{w}_1, \mathbf{W}_2]$, where $\mathbf{w}_1$ is used to transmit information-bearing signals and $\mathbf{W}_2$ is used to transmit AN. The design of $\mathbf{W}_2$ is to intentionally degrade the Eve's channel quality by transmitting AN isotropically except toward the LUs. The construction of $\mathbf{W}_2$ is based on the information of the $2 \times M$ main channel matrix $\mathbf{H}_\text{m} = [\mathbf{h}_1, \mathbf{h}_2]^T$, which contains $(M-2)$ eigenvectors of the orthogonal projection matrix $\left(\mathbf{I}_M - \frac{\mathbf{H}_\text{m}^\dagger \mathbf{H}_\text{m}}{\mathbf{H}_\text{m} \mathbf{H}_\text{m}^\dagger}\right)$ corresponding to its $(M-2)$ non-zero eigenvalues due to the fact that the rank of the orthogonal projection matrix is $(M-2)$, and holds that $\mathbf{W}_2^\dagger \mathbf{W}_2 = \text{diag}[0; \mathbf{I}_{M-2}]$. This beamforming matrix ensures that AN lies in the null space of $\mathbf{H}_\text{m}$, and the reception quality of the LUs is not affected by AN. Furthermore, the design of $\mathbf{w}_1$ is to artificially improve the effective channel gain of LU_1, such that $\mathbf{w}_1 = \mathbf{h}_1^\dagger / ||\mathbf{h}_1||$. Benefits of such construction include: 1) the effective channel gains between the two LUs become distinct, creating an ideal situation for implementing NOMA, and 2) the signal strength for detection at the LUs maintains the same at the time of transmission at the BS, which is beneficial for the SIC processing to distinguish the individual information-bearing signal.

The $M \times 1$ transmitted signal vector at the BS is

$$\mathbf{x} = \mathbf{w}_1(\alpha_1 s_1 + \alpha_2 s_2) + \mathbf{W}_2 \mathbf{v}, \tag{1}$$

where s_1 and s_2 denote the information-bearing signals intended for LU_1 and LU_2 with $\mathbb{E}[||s_1||] = \mathbb{E}[||s_2||] = 0$ and $\mathbb{E}[||s_1||^2] = \mathbb{E}[||s_2||^2] = \sigma_s^2$, α_1 and α_2 denote the power allocation coefficients satisfying $\alpha_1^2 + \alpha_2^2 = 1$, and $\mathbf{v}$ is an $(M-2) \times 1$ AN vector. In particular, the BS chooses elements of $\mathbf{v}$ to be i.i.d. complex Gaussian random variables with mean being zero and variance being σ_v^2, and independent in different fading blocks as well. We consider an aggragrate power constraint P_T, and denote ϕ as the power sharing factor between the information-bearing signals and AN, such that $\sigma_s^2 = \phi P_T$ and $\sigma_v^2 = (1-\phi) P_T / (M-2)$ with $0 < \phi < 1$.

Based on the proposed SBF scheme, the received signals at LU_k for $k = 1, 2$ are given by

$$y_k = \mathbf{h}_k \mathbf{w}_1 (\alpha_1 s_1 + \alpha_2 s_2) + n_k, \tag{2}$$

where n_k denotes the AWGN at LU_k. Since the proposed beamforming vector $\mathbf{w}_1$ improves the effective channel gain of $\mathbf{h}_1$, the power allocation coefficients should satisfy $\alpha_2 > \alpha_1$ in consideration of user fairness [5]. Then, SIC will be carried out at LU_1 following the decoding order $s_2 \rightarrow s_1$. As such, the signal-to-interference-plus-noise ratio (SINR) at LU_1 to decode s_2 is

$$\gamma_{1,s_2} = \frac{\phi \alpha_2^2 \rho_\text{b} ||\mathbf{h}_1||^2}{\phi \alpha_1^2 \rho_\text{b} ||\mathbf{h}_1||^2 + 1}, \tag{3}$$

where $\rho_\text{b} = P / \sigma_\text{b}^2$ is called the transmit signal-to-noise ratio (SNR). Conditioned on s_2 being correctly decoded, LU_1 first subtracts s_2 and then tries to recover its own signal s_1 by utilizing the following SNR

$$\gamma_{1,s_1} = \phi \alpha_1^2 \rho_\text{b} ||\mathbf{h}_1||^2. \tag{4}$$

Upon treating s_1 as interference, LU_2 decodes s_2 by using the following SINR

$$\gamma_{2,s_2} = \frac{\phi \alpha_2^2 \rho_\text{b} ||\mathbf{h}_2 \mathbf{w}_1||^2}{\phi \alpha_1^2 \rho_\text{b} ||\mathbf{h}_2 \mathbf{w}_1||^2 + 1}. \tag{5}$$

Simultaneously, Eve tries to extract s_1 and s_2 from its observations for the eavesdropping purpose. The received signal vector at Eve can be expressed as

$$\mathbf{y}_\text{e} = \mathbf{H}_\text{e} \mathbf{w}_1 (\alpha_1 s_1 + \alpha_2 s_2) + \mathbf{H}_\text{e} \mathbf{W}_2 \mathbf{v} + \mathbf{n}_\text{e}, \tag{6}$$

where $\mathbf{n}_\text{e}$ denotes the $N \times 1$ AWGN vector at Eve. To guarantee secure NOMA communications, it is reasonable to consider a worst-case eavesdropping scenario, where 1) Eve is capable of strong multiuser detection techniques [5], [12], e.g., subtracting the inter-user interference generated by the superimposed

[1]The two-user form of NOMA is one most typical NOMA scenario in the literature [2]–[8], and is recommended to be used in practical systems, such as multi-user superposition transmission (MUST) in 3rd-generation partnership project long-term evolution (3GPP-LTE). Moreover, the proposed solutions in this work can be extended to a scenario consisting more than two LUs, where user pairing can be applied to construct a hybrid NOMA system [3].

[2]The situation where the two LUs have similar channel conditions makes the benefits of implementing NOMA marginal, since the distinction in LUs' channel conditions is crucial for NOMA to achieve significant performance gains compared to conventional OMA [3].

information-bearing signals from each other, thus the individual signal will be distinguishable at Eve, and 2) the AWGN vector at Eve is arbitrarily small [11]. As a result, the received signal-to-interference ratio (SIR) at Eve to decode s_k for $k = 1, 2$ is

$$\gamma_{\mathrm{e},s_k} = \frac{\alpha_k^2(M-2)}{\phi^{-1}-1}\mathbf{w}_1^\dagger \mathbf{H}_\mathrm{e}^\dagger \left(\mathbf{H}_\mathrm{e}\mathbf{W}_2\mathbf{W}_2^\dagger\mathbf{H}_e^\dagger\right)^{-1}\mathbf{H}_\mathrm{e}\mathbf{w}_1. \quad (7)$$

Although the expression of (7) indeed overestimates Eve's interception capability, in the following, we will demonstrate that the proposed SBF scheme can achieve a robust approach against the worst-case eavesdropping in the considered MISO-NOMA systems.

The secrecy capacity is defined as the non-negative capacity difference between the main channel and the Eve's channel. Therefore, based on (3)–(7) and the imperfect worst-case SIC, the secrecy capacity for LU_1 is obtained as

$$C_{\mathrm{sec},s_1} = \begin{cases} \left[\log_2\left(\frac{1+\gamma_{1,s_1}}{1+\gamma_{\mathrm{e},s_1}}\right)\right]^+, & \text{if } \gamma_{1,s_2} \geq \gamma_{\mathrm{th},s_2} \\ 0, & \text{otherwise} \end{cases} \quad (8)$$

where $[x]^+ = \max\{x, 0\}$, $\gamma_{\mathrm{th},s_2} = 2^{R_{\mathrm{b},s_2}} - 1$, and R_{b,s_2} denotes the codeword rate for s_2. It is clear from (8) that the secrecy capacity for LU_1 becomes zero if it fails to decode the signal s_2. This is reasonable in the sense that error propagation occurs when SIC fails, corresponding to the imperfect worst-case SIC. Such a characteristic is unique in NOMA systems, which needs to be appropriately incorporated into the design and analysis of secure NOMA communications.

In addition, the secrecy capacity for LU_2 is obtained as

$$C_{\mathrm{sec},s_2} = \left[\log_2(1+\gamma_{2,s_2}) - \log_2(1+\gamma_{\mathrm{e},s_2})\right]^+. \quad (9)$$

III. Analysis of Secrecy Outage Probability and Secrecy Diversity Order

This section presents a comprehensive performance analysis achieved by the proposed SBF scheme in terms of SOP and secrecy diversity order, which are useful for practical setup.

A. Analysis of SOP

1) SOP for LU_1: Based on total probability theorem, the SOP for LU_1 can be mathematically formulated as

$$\begin{aligned} P_{\mathrm{sop},1} = &\Pr\left(C_{\mathrm{sec},s_1} < R_{\mathrm{s},s_1} | \gamma_{1,s_2} \geq \gamma_{\mathrm{th},s_2}\right) \\ &\times \Pr\left(\gamma_{1,s_2} \geq \gamma_{\mathrm{th},s_2}\right) + \Pr\left(\gamma_{1,s_2} < \gamma_{\mathrm{th},s_2}\right) \\ &\times \Pr\left(C_{\mathrm{sec},s_1} < R_{\mathrm{s},s_1} | \gamma_{1,s_2} < \gamma_{\mathrm{th},s_2}\right), \end{aligned} \quad (10)$$

where the first and second products on the right-hand side of (10) are the probabilities that the secrecy capacity is below the target secrecy rate R_{s,s_1} conditioned on whether signal s_2 can be decoded or not. Since the secrecy capacity is always equal to zero if LU_1 fails to decode s_2, e.g., $\gamma_{1,s_2} < \gamma_{\mathrm{th},s_2}$, which leads to a secrecy outage for sure, and thus, we obtain the probability $\Pr(C_{\mathrm{sec},s_1} < R_{\mathrm{s},s_1} | \gamma_{1,s_2} < \gamma_{\mathrm{th},s_2}) = 1$. Then, the probability $\Pr(\gamma_{1,s_2} < \gamma_{\mathrm{th},s_2})$ can be simplified as

$$\begin{aligned} \Pr\left(\gamma_{1,s_2} < \gamma_{\mathrm{th},s_2}\right) &= \Pr\left(\phi\rho_\mathrm{b}||\mathbf{h}_1||^2 < \frac{\gamma_{\mathrm{th},s_2}}{\alpha_2^2 - \alpha_1^2\gamma_{\mathrm{th},s_2}}\right) \\ &= \Pr\left(\gamma_{1,s_1} < \zeta_1\right), \end{aligned} \quad (11)$$

where $\zeta_1 = \frac{\alpha_1^2\gamma_{\mathrm{th},s_2}}{\alpha_2^2 - \alpha_1^2\gamma_{\mathrm{th},s_2}}$, and the second equality is derived from multiplying both sides in $\Pr(\cdot)$ of the first equation by α_1^2. From (11), the power allocation $\alpha_2^2 > \alpha_1^2\gamma_{\mathrm{th},s_2}$ should be satisfied in application of NOMA, because otherwise the SOP for LU_1 is always equal to one [5]. Combining the results in (8) and (11), we can rewrite (10) as

$$P_{\mathrm{sop},1} = \Pr\left(\zeta_1 \leq \gamma_{1,s_1} < \zeta_2(\gamma_{\mathrm{e},s_1})\right) + \Pr\left(\gamma_{1,s_1} < \zeta_1\right), \quad (12)$$

where $\zeta_2(\gamma_{\mathrm{e},s_1}) = 2^{R_{\mathrm{s},s_1}}(1+\gamma_{\mathrm{e},s_1}) - 1$. A non-zero probability $\Pr(\zeta_1 \leq \gamma_{1,s_1} < \zeta_2(\gamma_{\mathrm{e},s_1}))$ exists if and only if $\zeta_2(\gamma_{\mathrm{e},s_1}) \geq \zeta_1$, thus we obtain that γ_{e,s_1} should be in the range of $[\varpi, \infty)$, where $\varpi = \frac{\alpha_2^2 2^{-R_{\mathrm{s},s_1}}}{\alpha_2^2 - \alpha_1^2\gamma_{\mathrm{th},s_2}} - 1$.

To proceed forward, we denote $X = \gamma_{1,s_1}$ and $Y_1 = \gamma_{\mathrm{e},s_1}$, and their statistics are shown in the following lemma.

Lemma 1: The cumulative density functions (CDFs) of X and Y are computed, respectively, by

$$F_X(x) = 1 - e^{-\frac{\theta_1 x}{\rho_\mathrm{b}}}\sum_{m=0}^{M-1}\frac{1}{m!}\left(\frac{\theta_1 x}{\rho_\mathrm{b}}\right)^m, \quad (13)$$

$$F_{Y_1}(y_1) = 1 - \frac{\sum_{m=0}^{N-1}\binom{M-2}{m}(\theta_1\eta y_1)^m}{(1+\theta_1\eta y_1)^{M-2}}, \quad (14)$$

where $\theta_1 = \frac{1}{\phi\alpha_1^2}$ and $\eta = \frac{1-\phi}{M-2}$.

Proof: See Appendix A.1. ∎

Using the results in Lemma 1, the SOP for LU_1 is addressed in the following theorem.

Theorem 1: The SOP for LU_1 is computed by (15), shown at the top of the next page, where A_{11} and A_{12} can be found in Appendix A.2.

Proof: See Appendix A.2. ∎

2) SOP for LU_2: According to (9), the SOP for LU_2 can be expressed as

$$\begin{aligned} P_{\mathrm{sop},2} &= \Pr\left(C_{\mathrm{sec},s_2} < R_{\mathrm{s},s_2}\right) \\ &= \Pr\left(\gamma_{2,s_2} < 2^{R_{\mathrm{s},s_2}}(1+\gamma_{\mathrm{e},s_2}) - 1\right), \end{aligned} \quad (16)$$

where R_{s,s_2} denotes the target secrecy rate of LU_2. For brevity, we denote $Y_2 = \gamma_{\mathrm{e},s_2}$ and $Z = \gamma_{2,s_2}$. The CDF of Y_2 can be obtained by following the same rationale with (14), and the CDF of Z is characterized in the following lemma.

Lemma 2: The CDF of Z is obtained as

$$F_Z(z) = \delta(\kappa - z) + \delta(\kappa - z)\left(1 - e^{-\frac{\theta_1 z}{\rho_\mathrm{b}(\kappa - z)}}\right), \quad (17)$$

where $\kappa = \alpha_2^2/\alpha_1^2$, and $\delta(\cdot)$ denotes the unit step function.

Proof: See Appendix B.1. ∎

Theorem 2: The SOP for LU_2 can be numerically approximated as

$$P_{\mathrm{sop},2} \approx 1 - \chi_3(m)B_{11} + \chi_4(m)B_{12}, \quad (18)$$

in which $\chi_3(m) = \sum_{m=0}^{N-1}\binom{M-2}{m}(\theta_2\eta)^m$, and $\chi_4(m) = \sum_{m=1}^{N-1}\binom{M-2}{m}m(\theta_2\eta)^{m-1}$. In addition, B_{11} and B_{12} can be found in Appendix B.2.

Proof: See Appendix B.2. ∎

Remark 1: We highlight the fact that our new closed-form expressions of (15) and (18) are easy to compute, due to their simple forms which consist of power functions, fractional functions, exponential functions, and trigonometric functions. These results provide an efficient method for system designers to characterize the secrecy performance in practical MISO-NOMA systems without carrying out extensive Monte Carlo simulations.

$$P_{sop,1} \approx 1 - e^{-\frac{\theta_1\zeta_1}{\rho_\mathrm{b}}} \sum_{m=0}^{M-1} \frac{1}{m!}\left(\frac{\theta_1\zeta_1}{\rho_\mathrm{b}}\right)^m \left(1 - \frac{\sum_{m=0}^{N-1}\binom{M-2}{m}(\theta_1\eta\varpi)^m}{(1+\theta_1\eta\varpi)^{M-2}}\right) - e^{-\frac{\theta_1(2^{R_{\mathrm{s},s_1}}-1)}{\rho_\mathrm{b}}} \times \sum_{m=0}^{M-1} \frac{\theta_1^m(2^{R_{\mathrm{s},s_1}}-1)^m}{m!\rho_\mathrm{b}^m} \sum_{n=0}^{m}\binom{m}{n}\left(\frac{2^{R_{\mathrm{s},s_1}}}{2^{R_{\mathrm{s},s_1}}-1}\right)^n \Big(A_{11} - A_{12}\Big). \quad (15)$$

B. Analysis of Secrecy Diversity Order

Although the SOP expressions shown in (15) and (18) can be used to evaluate the secrecy performance of the proposed SBF scheme, they fail to provide intuitive insights. To this end, we carry out the secrecy diversity analysis. As defined in [5], the secrecy diversity order is achieved when the transmit SNR is sufficiently high, e.g., $\rho_\mathrm{b} \to \infty$. The secrecy diversity order at LU_k for $k = 1, 2$ is defined as

$$D_{\mathrm{sec},k} \triangleq -\lim_{\rho_\mathrm{b}\to\infty} \frac{\log P_{\mathrm{sop},k}^{\infty}}{\log \rho_\mathrm{b}}, \quad (19)$$

where $P_{\mathrm{sop},k}^{\infty}$ denotes the asymptotic SOP for LU_k.

***Corollary** 1:* The asymptotic SOPs for LU_1 and LU_2 can be computed by

$$P_{\mathrm{sop},1}^{\infty} = \frac{\theta_1^M}{\rho_b^M M!}\Bigg[\zeta_1^M F_Y(\varpi) + \left(2^{R_{\mathrm{s},s_1}}-1\right)^M \times \sum_{n=0}^{M}\binom{M}{n}\left(\frac{2^{R_{\mathrm{s},s_1}}}{2^{R_{\mathrm{s},s_1}}-1}\right)^n \Big(A_{11}^{\infty} - A_{12}^{\infty}\Big)\Bigg], \quad (20)$$

$$P_{\mathrm{sop},2}^{\infty} = \rho_\mathrm{b}^{-1}\Big(\chi_3(m)B_{11}^{\infty} - \chi_4(m)B_{12}^{\infty}\Big). \quad (21)$$

In particular, A_{11}^{∞}, A_{12}^{∞}, B_{11}^{∞}, and B_{12}^{∞} are expressed as

$$A_{11}^{\infty} \approx \frac{\chi_1(m)\pi}{4L}\sum_{l=1}^{L}\sqrt{1-u_l^2}\,\Xi_1^{\infty}\left(\frac{\pi(u_l+1)}{4}\right), \quad (22)$$

$$A_{12}^{\infty} \approx \frac{\chi_2(m)\pi}{4L}\sum_{l=1}^{L}\sqrt{1-u_l^2}\,\Xi_2^{\infty}\left(\frac{\pi(u_l+1)}{4}\right), \quad (23)$$

$$B_{11}^{\infty} \approx \frac{\varphi(\kappa)\pi}{2L}\sum_{l=1}^{L}\sqrt{1-v_l^2}\,\frac{\omega^m(v_l)}{\big(1+\theta_2\eta\omega(v_l)\big)^{M-3}}, \quad (24)$$

$$B_{12}^{\infty} \approx \frac{\varphi(\kappa)\pi}{2L}\sum_{l=1}^{L}\sqrt{1-v_l^2}\,\frac{\omega^{m-1}(v_l)}{\big(1+\theta_2\eta\omega(v_l)\big)^{M-2}}, \quad (25)$$

where $\Xi_1^{\infty}(\tau)$ and $\Xi_2^{\infty}(\tau)$ can be obtained by substituting $\rho_\mathrm{b} \to \infty$ into (35) and (36), shown in Appendix A.2.

Proof: When $\rho_\mathrm{b} \to \infty$, the CDFs of X and Z can be asymptotically rewritten as

$$F_X(x) \overset{\rho_\mathrm{b}\to\infty}{\simeq} \frac{1}{M!}\left(\frac{\theta_1 x}{\rho_\mathrm{b}}\right)^M, \quad (26)$$

$$F_Z(z) \overset{\rho_\mathrm{b}\to\infty}{\simeq} \delta(\kappa - z) + \frac{\delta(\kappa-z)\theta_1 z}{\rho_\mathrm{b}(\kappa - z)}. \quad (27)$$

Using results of (26) and (27), and applying the similar procedures in Appendices A.2 and B.2, Corollary 1 can be proved straightforwardly. ■

***Remark** 2:* Substituting results of (20) and (21) into (19), it is straightforward that a secrecy diversity order $D_{\mathrm{sec},1} = M$ is obtained at LU_1. While a secrecy diversity order $D_{\mathrm{sec},2} = 1$ is achieved at LU_2, due to the fact that the beamforming vector $\mathbf{w}_1$ shrinks the effective channel gain between BS and LU_2 from a $1 \times M$ vector to a scalar. This secrecy diversity loss is sacrificed for creating the channel difference between the two LUs, which is beneficial for guaranteeing secure NOMA communications.

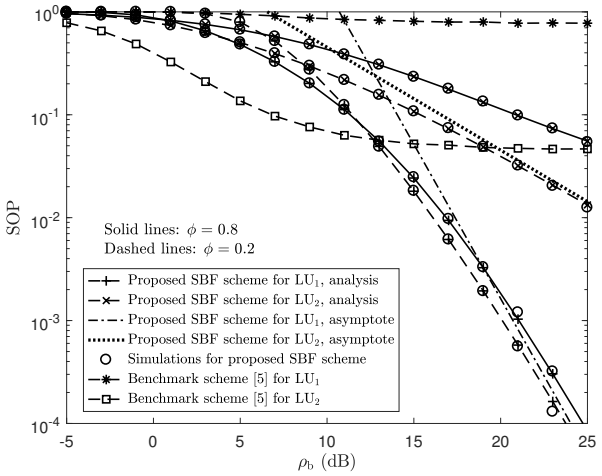

Fig. 1. The variation of SOP as a function of ρ_b with $M = 3$ and $N = 2$.

IV. Numerical Studies

In this section, the secrecy performance of the proposed SBF scheme is evaluated by using Monte Carlo simulations. For illustration purpose, the codeword rates of the two LUs are set as $R_{\mathrm{b},s_1} = 1$ bps/Hz and $R_{\mathrm{b},s_2} = 0.5$ bps/Hz, and the target secrecy rates are set as $R_{\mathrm{s},s_1} = 0.6$ bps/Hz and $R_{\mathrm{s},s_2} = 0.1$ bps/Hz. The power allocation coefficients used are $\alpha_1 = 0.3$ and $\alpha_2 = 0.7$, respectively. The Gauss-Chebyshev node is chosen as $L = 20$ to yield a close approximation.

Fig. 1 shows the SOP versus ρ_b achieved by the proposed SBF scheme, where a close agreement between the simulated and analytical results can be observed, and the asymptotic curves become very tight in high ρ_b regime. For a comparison, the SOP achieved by the benchmark scheme [5] is also plotted. From this figure, we have the following informative observations:

- The proposed SBF scheme achieves a lower SOP than the benchmark scheme [5] for LU_1, where the SOP remains very close to one. The reasons are twofold. First, the beamforming vector for LU_2 inevitably causes additional AN to the range space of LU_1, which leads to the SOP approaching to a constant in medium to high ρ_b regime. Second, the beamforming vector for LU_1 exclusively enhances the power strength of its intended signal, while limiting the power strength of LU_2's signal. This may result in an unsuccessful SIC processing at LU_1 with a high probability. Furthermore, our proposed SBF scheme outperforms the benchmark scheme for LU_2 in high ρ_b regime, because a SOP floor occurs in [5].

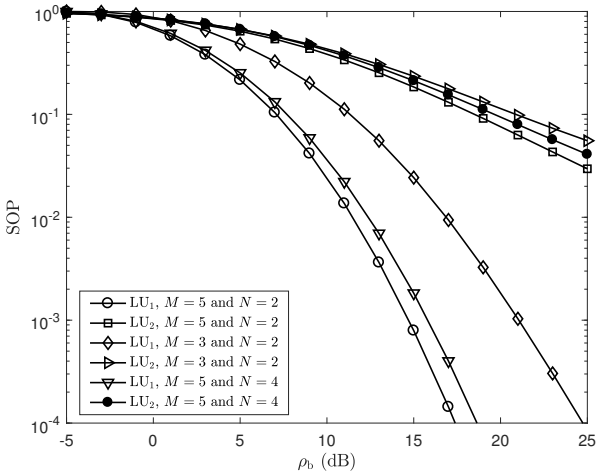

Fig. 2. The variation of SOP as a function of ρ_b with $\phi = 0.8$.

- For the proposed SBF scheme, the SOP of LU_1 decreases faster than that of LU_2, e.g., a secrecy diversity order of M is achieved at LU_1 while a secrecy diversity order of one is obtained at LU_2. This is consistent with Corollary 1, in the sense that the propose SBF scheme not only intentionally decreases the capability for Eve, but also effectively creates channel difference for the two LUs, thus ensuring a robust secure MISO-NOMA transmission.
- The power sharing factor ϕ has different impacts on the two LUs. For LU_1, a better SOP is achieved with a large value of ϕ (e.g., $\phi = 0.8$) in low to medium ρ_b regime, but with a small value of ϕ (e.g., $\phi = 0.2$) in medium to high ρ_b regime. For LU_2, a better SOP is always obtained with a small value of ϕ. This indicates that in low to medium ρ_b regime, there exists an optimal power sharing factor ϕ, which balances the SOP of the two LUs. Therefore, it is of salient significance to select the appropriate ϕ for the SOP improvement.

Fig. 2 depicts the SOP versus ρ_b in the system with different number of antennas. A general trend is that the SOP for LU_1 significantly decreases with an increase in M due to a secrecy diversity order of M, e.g., a full secrecy diversity order, is achieved at LU_1. By contrast, the SOP for LU_2 decreases slightly with the increased M, though the secrecy diversity order at LU_2 is one. This is because the degree of freedom for generating AN is enhanced with a large value of M. Therefore, increasing the transmit antenna at the BS is an efficient yet simple method to improve the secrecy performance of MISO-NOMA systems. Furthermore, we find that an increase in N leads to an increase in the SOP for both LUs, which shows the detrimental effect of multiple receive antennas at Eve.

V. Conclusion

This paper has investigated the problem of secure MISO-NOMA transmission in the presence of a multiple-antenna Eve. A new SBF scheme by exploiting AN has been proposed, where AN is generated in the null space of the main channel, such that only the Eve's channel is degraded. Moreover, the developed beamforming matrix artificially creates the difference for the two LUs' channel conditions, therefore fully realizing the potential of NOMA. To evaluate the secrecy performance, we have derived closed-form expressions for the SOP and the secrecy diversity order. The results manifest that an improved secrecy performance is achieved by the SBF scheme.

Appendix A
Mathematical Proofs for LU_1

A.1-Proof of Lemma 1: Observing γ_{1,s_1} from (4), we find that X follows a Gamma distribution with a shape parameter M and a scale parameter $\frac{\rho_b}{\theta_1}$, which is due to the fact that $||\mathbf{h}_1||^2$ is the sum of the squares of M independent Gaussian random variables. Therefore, an explicit expression for the CDF of X is obtained in (13) straightforwardly.

Based on the construction of the beamforming matrix $\mathbf{W}$, we know that the entries of $\mathbf{H}_e\mathbf{W}$ are i.i.d. complex Gaussian random variables, because the entries of $\mathbf{H}_e$ are i.i.d. complex Gaussian random variables and $\mathbf{W}$ is a unitary matrix. This indicates the fact that the elements of $\mathbf{H}_e\mathbf{w}_1$ and $\mathbf{H}_e\mathbf{W}_2$ in (7) are independent. Therefore, the quantity of (7) is equivalent to the SIR of a N-branch MMSE diversity combiner with $(M-2)$ interferers. With the help of [11], and after the variable substitution, the CDF of Y_1 is computed by (14).

Hence, we complete the proof of Lemma 1.

A.2-Proof of Theorem 1: According to the properties of the statistics for X and Y, $P_{\text{sop},1}$ can be rewritten as

$$P_{\text{sop},1} = \underbrace{\int_{\varpi}^{\infty} F_X\big(\zeta_2(y_1)\big) f_{Y_1}(y_1) dy_1}_{A_1} - \underbrace{\int_{\varpi}^{\infty} F_X(\zeta_1) f_{Y_1}(y_1) dy_1}_{A_2} + F_X(\zeta_1). \quad (28)$$

From (14), by taking the first derivative with y_1, we derive the probability density function (PDF) $f_{Y_1}(y_1)$ as

$$f_{Y_1}(y_1) = \frac{\sum_{m=0}^{N-1} \binom{M-2}{m} (\theta_1 \eta y_1)^m}{(1+\theta_1\eta y_1)^{M-3}} - \frac{\sum_{m=1}^{N-1} \binom{M-2}{m} m\theta_1\eta(\theta_1\eta y_1)^{m-1}}{(1+\theta_1\eta y_1)^{M-2}}. \quad (29)$$

Substituting (29) into (28), A_1 can be further computed by

$$A_1 = \int_{\varpi}^{\infty} f_{Y_1}(y_1) dy_1 - e^{-\frac{\theta_1(2^{R_{s,s_1}}-1)}{\rho_b}} \sum_{m=0}^{M-1} \frac{(2^{R_{s,s_1}}-1)^m}{\rho_b^m} \times \frac{\theta_1^m}{m!} \sum_{n=0}^{m} \binom{m}{n} \left(\frac{2^{R_{s,s_1}}}{2^{R_{s,s_1}}-1}\right)^n \Big(A_{11} - A_{12}\Big). \quad (30)$$

In (30), A_{11} and A_{12} are formulated as

$$A_{11} = \int_{\varpi}^{\infty} y_1^n e^{-\frac{\theta_1 2^{R_{s,s_1}} y_1}{\rho_b}} \frac{\sum_{m=0}^{N-1} \binom{M-2}{m} (\theta_1\eta y_1)^m}{(1+\theta_1\eta y_1)^{M-3}} dy_1, \quad (31)$$

$$A_{12} = \int_{\varpi}^{\infty} y_1^n e^{-\frac{\theta_1 2^{R_{s,s_1}} y_1}{\rho_b}} \times \frac{\sum_{m=1}^{N-1} \binom{M-2}{m} m\theta_1\eta(\theta_1\eta y_1)^{m-1}}{(1+\theta_1\eta y_1)^{M-2}} dy_1. \quad (32)$$

However, it is rather challenging to derive the closed-form expressions for A_{11} and A_{12}, due to their complicated integrals. To overcome this problem, we will use an efficient L-node Gauss-Chebyshev quadrature [14, eq. (25.4.45)] to yield

a close approximation. Specifically, by changing variable of $y_1 = \varpi + \tan\tau$, we can approximate A_{11} and A_{12} as

$$A_{11} = \chi_1(m)\int_0^{\frac{\pi}{2}} \Xi_1(\tau)d\tau \approx \frac{\chi_1(m)\pi}{4L}\sum_{l=1}^{L}\sqrt{1-u_l^2}\Xi_1\bigg(\frac{\pi(u_l+1)}{4}\bigg), \quad (33)$$

$$A_{12} = \chi_2(m)\int_0^{\frac{\pi}{2}} \Xi_2(\tau)d\tau \approx \frac{\chi_2(m)\pi}{4L}\sum_{l=1}^{L}\sqrt{1-u_l^2}\Xi_2\bigg(\frac{\pi(u_l+1)}{4}\bigg), \quad (34)$$

where $u_l = \cos(\frac{2l-1}{2L}\pi)$, L denotes the number of the Gauss-Chebyshev nodes, $\chi_1(m) = \sum_{m=0}^{N-1}\binom{M-2}{m}(\theta_1\eta)^m$, and $\chi_2(m) = \sum_{m=1}^{N-1}\binom{M-2}{m}m(\theta_1\eta)^{m-1}$. Furthermore, $\Xi_1(\tau)$ and $\Xi_2(\tau)$ are given by

$$\Xi_1(\tau) = \frac{(\varpi+\tan\tau)^{m+n}\sec^2\tau e^{-\frac{\theta_1 2^{R_{s,s_1}}}{\rho_b}(\varpi+\tan\tau)}}{\big(1+\theta_1\eta(\varpi+\tan\tau)\big)^{M-3}}, \quad (35)$$

$$\Xi_2(\tau) = \frac{(\varpi+\tan\tau)^{m+n}\sec^2\tau e^{-\frac{\theta_1 2^{R_{s,s_1}}}{\rho_b}(\varpi+\tan\tau)}}{(\varpi+\tan\tau)\big(1+\theta_1\eta(\varpi+\tan\tau)\big)^{M-2}}. \quad (36)$$

Substituting (33) and (34) into (30), an explicit expression for A_1 is obtained. In addition, A_2 can be derived as

$$A_2 = F_X(\zeta_1)\Big(1 - F_{Y_1}(\varpi)\Big). \quad (37)$$

Combining the aforementioned results, Theorem 1 is proved.

APPENDIX B
MATHEMATICAL PROOFS FOR LU_2

B.1-Proof of Lemma 2: It is clear that $\mathbf{h}_2$ is independent of $\mathbf{h}_1$, and we have $\mathbf{h}_2$ is independent of $\mathbf{w}_1$ (since $\mathbf{w}_1 = \mathbf{h}_1^\dagger/||\mathbf{h}_1||$). Thus, $||\mathbf{h}_2\mathbf{w}_1||^2$ follows the exponential distribution. Using this result, the CDF of Z can be easily computed by

$$F_Z(z) = \Pr\left(||\mathbf{h}_2\mathbf{w}_1||^2 < \frac{\theta_1 z}{\rho_b(\kappa - z)}\right) = 1 - e^{-\frac{\theta_1 z}{\rho_b(\kappa-z)}}, \quad (38)$$

where (38) holds only if $z < \kappa$, otherwise, $F_Z(z) = 1$. As a result, we prove (17) in Lemma 2.

B.2-Proof of Theorem 2: Upon using results in Lemma 2, the SOP for LU_2 can be rewritten as

$$\begin{aligned} P_{\text{sop},2} &= \int_0^{\infty}\Pr\Big(Z < 2^{R_{s,s_2}}(1+y_2)-1\Big)f_{Y_2}(y_2)dy_2 \\ &\overset{\text{(i)}}{=} \int_0^{\varphi(\kappa)} F_Z\Big(2^{R_{s,s_2}}(1+y_2)-1\Big)f_{Y_2}(y_2)dy_2 + \int_{\varphi(\kappa)}^{\infty} f_{Y_2}(y_2)dy_2 \\ &= 1 - \underbrace{\int_0^{\varphi(\kappa)} e^{-\frac{\theta_1\zeta_3(y_2)}{\rho_b(\kappa-\zeta_3(y_2))}} f_{Y_2}(y_2)dy_2}_{B_1}, \end{aligned} \quad (39)$$

where $\varphi(\kappa) = 2^{-R_{s,s_2}}(\kappa+1)-1$, and step (i) is obtained by using the fact that $F_Z(z) = 1$ when $z < \kappa$ (corresponds to $y_2 > \varphi(\kappa)$). Similarly, we can obtain the PDF $f_{Y_2}(y_2)$ as

$$f_{Y_2}(y_2) = \frac{\sum_{m=0}^{N-1}\binom{M-2}{m}(\theta_2\eta y_2)^m}{(1+\theta_2\eta y_2)^{M-3}} - \frac{\sum_{m=1}^{N-1}\binom{M-2}{m}m\theta_2\eta(\theta_2\eta y_2)^{m-1}}{(1+\theta_2\eta y_2)^{M-2}}. \quad (40)$$

Substituting (40) into (39), B_1 can be rewritten as

$$B_1 = \chi_3(m)B_{11} - \chi_4(m)B_{12}. \quad (41)$$

Again, we apply the Gauss-Chebyshev quadrature to obtain the close approximations for B_{11} and B_{12} as

$$B_{11} = \int_0^{\varphi(\kappa)} \frac{y_2^m e^{-\frac{\theta_1\zeta_3(y_2)}{\rho_b(\kappa-\zeta_3(y_2))}}}{(1+\theta_2\eta y_2)^{M-3}}dy_2 \approx \frac{\varphi(\kappa)\pi}{2L}\sum_{l=1}^{L}\sqrt{1-v_l^2}\frac{\omega^m(v_l)e^{-\frac{\theta_1\zeta_3(\omega(v_l))}{\rho_b(\kappa-\zeta_3(\omega(v_l)))}}}{\big(1+\theta_2\eta\omega(v_l)\big)^{M-3}}, \quad (42)$$

$$B_{12} = \int_0^{\varphi(\kappa)} \frac{y_2^{m-1} e^{-\frac{\theta_1\zeta_3(y_2)}{\rho_b(\kappa-\zeta_3(y_2))}}}{(1+\theta_2\eta y_2)^{M-2}}dy_2 \approx \frac{\varphi(\kappa)\pi}{2L}\sum_{l=1}^{L}\sqrt{1-v_l^2}\frac{\omega^{m-1}(v_l)e^{-\frac{\theta_1\zeta_3(\omega(v_l))}{\rho_b(\kappa-\zeta_3(\omega(v_l)))}}}{\big(1+\theta_2\eta\omega(v_l)\big)^{M-2}}, \quad (43)$$

where $\omega(v) = \frac{\varphi(\kappa)(v+1)}{2}$, and $v_l = \cos(\frac{2l-1}{2L}\pi)$.

Substituting these results into (39), Theorem 2 is proved in a straightforward manner.

REFERENCES

[1] L. Dai, B. Wang, Y. Yuan, S. Han, C.-L. I, and Z. Wang, "Non-orthogonal multiple access for 5G: Solutions, challenges, opportunities, and future research trends," *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 74–81, Sep. 2015.

[2] L. Lv, J. Chen, Q. Ni, and Z. Ding, "Design of cooperative non-orthogonal multicast cognitive multiple access for 5G systems: User scheduling and performance analysis," *IEEE Trans. Commun.*, vol. 65, no. 6, pp. 2641–2656, Jun. 2017.

[3] Z. Ding, P. Fan, and H. V. Poor, "Impact of user pairing on 5G nonorthogonal multiple-access downlink transmissions," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6010–6023, Aug. 2016.

[4] Z. Chen, Z. Ding, X. Dai, and G. K. Karagiannidis, "On the application of quasi-degradation to MISO-NOMA downlink," *IEEE Trans. Signal Process.*, vol. 64, no. 23, pp. 6174–6189, Dec. 2016.

[5] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing 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.

[6] Z. Ding, Z. Zhao, M. Peng, and H. V. Poor, "On the spectral efficiency and security enhancements of NOMA assisted multicast-unicast streaming," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 3151–3163, Jul. 2017.

[7] 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, Sep. 2017.

[8] 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.

[9] B. He, A. Liu, N. Yang, and V. K. N. Lau, "On the design of secure non-orthogonal multiple access systems," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 10, pp. 2196–2206, Oct. 2017.

[10] Y. Zhang, H.-M. Wang, Q. Yang, and Z. Ding, "Secrecy sum rate maximization in non-orthogonal multiple access," *IEEE Commun. Lett.*, vol. 20, no. 5, pp. 930–933, May 2016.

[11] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[12] X. Zhang, X. Zhou, and M. R. McKay, "Enhancing secrecy with multi-antenna transmission in wireless ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1802–1814, Nov. 2013.

[13] N. Yang, M. Elkashlan, T. Q. Duong, J. Yuan, and R. Malaney, "Optimal transmission with artificial noise in MISOME wiretap channels" *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2170–2181, Apr. 2016.

[14] M. Abramowitz and I. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, New York, NY, USA: Dover, 1972.