Covert and Secure Communications in NOMA Networks with Internal Eavesdropping

Qiang Li, *Student Member, IEEE*, Dongyang Xu, *Member, IEEE*, Keivan Navaie, *Senior Member, IEEE* and Zhiguo Ding, *Fellow, IEEE*

***Abstract*—This correspondence investigates the joint covert and secure communication problem in the non-orthogonal multiple access (NOMA) network with internal eavesdropping. The strong user of the NOMA network wiretaps the signals of the weak user while an external warden monitors the communication behaviors of the strong user. To deal with the issue, a random artificial noise (AN) based beamforming transmission strategy is proposed. Specifically, the transmitter sends the AN information with beamforming and the random power when communicating. It not only reduces the eavesdropping rate of the strong user but also confuses the warden efficiently. We consider the worst case, where the warden can minimize its detection error probability (DEP) by optimizing the decision threshold. Following the proposed principle, we characterize the closed-form expressions of the average minimum DEP of the warden, the connection outage probabilities of the NOMA users and the secrecy outage probability of the weak user. An effective covert rate maximization problem is formulated, subject to the covertness, reliability and secrecy constraints, which is solved by the 1D search algorithm. Numerical results validate the superiority of the proposed strategy.**

***Index Terms*—NOMA, internal eavesdropping, covert communications.**

I. Introduction

The ubiquitous personalized services need to be processed in parallel for the six-generation (6G) wireless networks, which imposes a heavy burden on the finite spectrum resources [1]. Non-orthogonal multiple access (NOMA) has been a promising technology attributed to its higher spectral efficiency [2], and its capability for supporting multiple services by the signal superposition and the successive interference cancellation (SIC) [3]. Owing to the sharing of the mediums, the NOMA networks suffer great challenges in terms of the information security [4].

One of the challenges is the information leakage, i.e., the eavesdropping attacks [5]. The researchers proposed the physical layer security (PLS) technology to overcome the issue. The authors in [6] arranged a friendly jammer emitting the jamming signals in the NOMA network, which degraded the eavesdropping rate of malicious users. A beamforming and power allocation scheme was proposed to enhance the secrecy sum rate of the NOMA users in [7]. Because of the heterogeneity of the terminals, there may be eavesdroppers insides the NOMA networks, which are the communication terminals while attempting to overhear the signals from other users. To mitigate the drawback, a precoding strategy was considered in [8] to ensure a positive secrecy rate of the internal user. The authors in [9] proposed a beamforming-aided power allocation scheme to combat the internal and external overhearing.

Another challenge is the covertness issue. For some adversaries, they are more interested in the communication itself than the transmitted information. For instance, in unmanned aerial systems, once detecting communications successfully, adversaries can disrupt the mission execution by sending the interference. Covert communications, aiming at keeping the transmissions from detecting, was proposed to remedy the gap. The authors in [10] investigated the channel uncertainty-based covert transmission scheme in the uplink NOMA network, which increased the detection error probability (DEP) of the adversary. In order to confuse the adversary, the sender transmitted the signals using the random transmit power, which enhanced the covert rate of the NOMA user [11]. Even more dangerously, the networks sometimes suffer from both security attacks at the same time. [12] considered the joint secure and covert transmissions in the finite blocklength. A jamming-based covert communication scheme was investigated in the networks with an untrusted relay in [13]. The authors in [14] proposed a power allocation-based transmission scheme to tackle the untrusted user and the warden.

Nevertheless, joint internal eavesdropping and external surveillance has not been explored in the NOMA networks. Inspired by this, this paper considers the joint covert and secure communication design in a two-user NOMA network, for the first time. In the network, each user faces a security threat. The strong user (SU), which has a better channel condition between the two users, attempts to overhear the signal of the weak user (WU). There is an external warden which monitors the interaction between the transmitter and the SU using a radiometer. To mitigate the threats, we propose a random artificial noise (AN) based beamforming strategy. The transmitter emits the AN signal with the beamforming and the random power, when transmitting the useful information. In terms of the security, the eavesdropping rate of the SU is reduced. In terms of the covertness, the signals of the AN and the WU provide shelter for the covert signal, keeping the warden from detecting correctly. We consider the worst case, where warden can minimize its DEP by adjusting the decision threshold for each observation. The close-form expressions of

Q. Li and D. Xu are with the School of Information and Communications Engineering, Xi'an Jiaotong University, Xi'an 710049, China. (e-mail: liqiang16@stu.xjtu.eud.cn, xudongyang@xjtu.edu.cn.)

K. Navaie is with the School of Computing and Communications, Lancaster University, LA1 4WA Lancaster, U.K. (e-mail: k.navaie@lancaster.ac.uk).

Z. Ding is with Department of Electrical Engineering and Computer Science, Khalifa University, Abu Dhabi, UAE. (e-mail: zhiguo.ding@manchester.ac.uk).

average minimum DEP (MDEP), connect outage probabilities and secrecy outage outage probability are derived in this paper. An effective covert rate optimization problem is designed, subject to the reliability, secrecy and covertness constraints, which can be solved by the 1D search algorithm. Numerical results are preened to demonstrate that the proposed strategy outperforms the benchmark schemes.

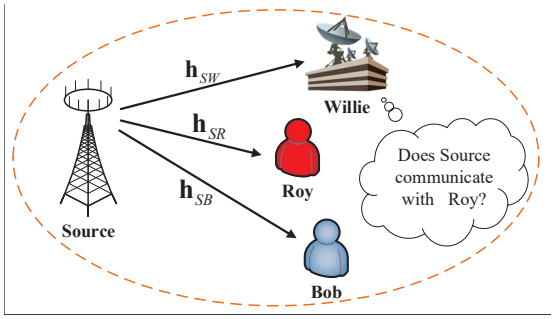

Fig. 1. System model.

II. System Model

A. System Description

We investigate in this paper a downlink NOMA network, as depicted in Fig. 1. A base station, termed as Source, transmits the secure signal x_B and the covert signal x_R to Bob and Roy, respectively. With the NOMA protocol, the signal of the WU is allocated more power and is firstly decoded, so the SU is a potential internal eavesdropper. In the network, we assume Roy is the SU overhearing x_B. Meanwhile, there is an external malicious user, Willie, who wants to detect whether Source emits the signal to Roy. If detected, Roy will face security risks, such as attack on purpose. Source shares the secret codewords with Bob and Roy, but Willie has no access to these information.

Source and other users, working in the half-duplex mode, are equipped with A_S antennas and one antenna, respectively. Assuming that all channels experience i.d. flat Rayleigh fading. Specifically, the channel gains between Source and Bob, Roy and Willie can be $\mathbf{h}_{SX} \sim \mathcal{CN}(0, \lambda_{SX}\mathbf{I}_{A_S})$, where $X \in \{B, R, W\}$. Source has perfect knowledge of the channel state information (CSI) of Bob and Roy, in accordance with the downlink channel estimation and feedback. Only the statistical CSI of Willie is available to Source, since the external user Willie will not provide feedback.

B. Random AN Based Beamforming Transmission Strategy

In the network, there are the security risk for Bob and the covertness risk for Roy, so Source performs the precoding design. Under the accustomed NOMA protocol, Roy has to decode the signal of Bob firstly for the SIC, which will potentially cause the information leakage. To avoid this, Source employs the maximum ratio transmission (MRT) beamforming to enhance the channel condition of Bob. The signal of Roy will be allocated more power and decoded firstly. The beamforming vector is calculated as $\mathbf{w}_1 = \frac{\mathbf{h}_{SB}^H}{\|\mathbf{h}_{SB}\|}$. Source simultaneously emits the AN to protect the signals of the NOMA users. If the received AN power is too large, the legitimate transmissions will also be limited. Source first preprocesses $\mathbf{h}_{SR}$, splitting it into two parts, i.e., $\mathbf{h}_{SR} = \overline{\mathbf{h}}_{SR} + \widehat{\mathbf{h}}_{SR}$ [15]. $\widehat{\mathbf{h}}_{SR} \sim \mathcal{CN}(0, \phi\lambda_{SR}\mathbf{I}_{A_S})$ and $0 \le \phi \le 1$ is the power allocation factor. To degrade the interference of the AN on the users, Source then precodes the AN signal and the precoding matrix $\mathbf{W}_{AN}$ satisfies $\mathbf{h}_{SB}^H\mathbf{W}_{AN} = \mathbf{0}$, $\overline{\mathbf{h}}_{SR}^H\mathbf{W}_{AN} = \mathbf{0}$ and the rank of $\mathbf{W}_{AN}$ is $A_S - 1$. As such, Roy will receive the controllable part ϕ AN power, which reduces the eavesdropping channel of Roy. At the same time, the AN can also confuse Willie. But it is easily identifiable by means of multiple observations if the power of the AN signal stays constant. To create the uncertainty at Willie, Source transmits the AN signal using random power P_J following a uniform distribution $U[0, P_J^{max}]$, where P_J^{max} is the maximum AN power. The received power at Willie will be changing from slot to slot. Willie needs to see if Source communicates with Roy after each observation. As such, the AN signal keeps x_B from eavesdropping, while the signals of AN and Bob protect the communications between Source and Roy.

The superimposed signal transmitted at Source can be denoted by $x_s[i] = \sqrt{a_1 P_S}x_B[i] + \sqrt{a_2 P_S}x_R[i]$, where P_S is the transmit power of useful signals. a_1 and a_2, satisfying $a_1 + a_2 = 1$, are the power allocation coefficients at Source. x_R is allocated more power, which means that $0 < a_1 < 0.5$. $i = 1, 2, ..., N$ is the index of the channel use. The received signals at the terminals can be denoted by

$$y_X[i] = \mathbf{h}_{SX}\mathbf{w}_1 x_s[i] + \frac{P_J}{A_S - 1}\mathbf{h}_{SX}\mathbf{W}_{AN}\mathbf{v}[i] + n_X[i], \quad (1)$$

where $\mathbf{v}$ is the AN signal, a $(A_S - 1) \times 1$ Gaussian vector with $\mathbf{0}$ mean and unit covariance matrix. $n_X \sim \mathcal{CN}(0, N_0)$ is the additive white Gaussian noise (AWGN) at X, $X \in \{B, R, W\}$. N_0 is the noise power at the terminals. In the network, perfect SIC is assumed. Bob first decodes x_R and then decodes x_B after eliminating x_R. The signal to interference plus noise ratio (SINR) for decoding x_R and the signal to noise ratio (SNR) for decoding x_B can be calculated as

$$\mathbb{SINR}_{B\to R} = \frac{|\mathbf{h}_{SB}\mathbf{w}_1|^2 a_2 P_S}{|\mathbf{h}_{SB}\mathbf{w}_1|^2 a_1 P_S + N_0}, \quad (2)$$

and

$$\mathbb{SINR}_B = \begin{cases} \dfrac{|\mathbf{h}_{SB}\mathbf{w}_1|^2 a_1 P_S}{N_0}, & \mathbb{SINR}_{B\to R} > \gamma_R \\ 0, & \text{otherwise.} \end{cases} \quad (3)$$

respectively. $\gamma_R = 2^{R_R} - 1$ and R_R is the predefined target rate of Roy. Roy first decodes x_R and then eavesdrops x_B after removing x_R. The SINR decoding x_R and the SNR overhearing x_B can be written as

$$\mathbb{SINR}_R = \frac{|\mathbf{h}_{SR}\mathbf{w}_1|^2 a_2 P_S}{|\mathbf{h}_{SR}\mathbf{w}_1|^2 a_1 P_S + \frac{P_J}{A_S - 1}\|\widehat{\mathbf{h}}_{SR}\mathbf{W}_{AN}\|^2 + N_0}, \quad (4)$$

and

$$\mathbb{SINR}_{R\to B} = \frac{|\mathbf{h}_{SR}\mathbf{w}_1|^2 a_1 P_S}{\frac{P_J}{A_S - 1}\|\widehat{\mathbf{h}}_{SR}\mathbf{W}_{AN}\|^2 + N_0}, \quad (5)$$

respectively. Based on those, we can acquire the channel

capacities of Bob and Roy as $C_B = \log_2(1+\mathbb{SINR}_B)$ and $C_R = \log_2(1+\mathbb{SINR}_R)$. The eavesdropping rate at Roy can be written as $C_E = \log_2(1+\mathbb{SINR}_{R\to B})$. To ensure the reliable transmission of Bob, $\mathbb{SINR}_{B\to R} \geq \gamma_R$ should be satisfied, so we can acquire

$$a_1 \leq a_1^{\dagger} = \frac{|\mathbf{h}_{SB}\mathbf{w}_1|^2 P_S - \gamma_R N_0}{|\mathbf{h}_{SB}\mathbf{w}_1|^2 P_S(1+\gamma_R)}. \tag{6}$$

Source transmits the covert signal x_R with the prior probability ρ within one slot. At the same time, the secure signal and the AN signal are always emitted in each slot. Due to the randomness of P_J, Willie is not aware of whether the received signal is the covert signal or the AN. He needs to judge the communication behaviors of Source by its own observations. We in the following detail the detection strategy of Willie.

III. Detection Stategy at Willie

Based on the described surveillance strategy, Willie makes a judgment on the received signals for each slot. A binary hypothesis testing model is utilized here. The null hypothesis $\mathcal{H}0$ represents x_R is not sent by Source, while the alternative hypothesis $\mathcal{H}1$ means Source emits x_R to Bob. Under $\mathcal{H}1$, the corresponding system model is shown as in (1). Under $\mathcal{H}0$, the received signal at Willie can be written as

$$y_W[i] = \mathbf{h}_{SW}\mathbf{w}_1\sqrt{a_1 P_S}x_B[i] + \frac{P_J}{A_S-1}\mathbf{h}_{SW}\mathbf{W}_{AN}\mathbf{v}[i] + n_W[i]. \tag{7}$$

Where Willie is not aware of the actual value of P_S but only statistical properties of P_J. In line with the Neyman-Pearson criterion [13], the optimal detector is the radiometer at Willie, and the detection strategy is given by

$$\mathbb{P}_W = \frac{1}{N}\sum_{i=1}^{N}|y_W[i]|^2 \underset{\mathcal{D}0}{\overset{\mathcal{D}1}{\gtrless}} \tau, \tag{8}$$

where the detection statistics $\mathbb{P}_W$ is the average power over all channel use within each slot. N is the blocklength. τ is the detection threshold of the detector. $\mathcal{D}0$ and $\mathcal{D}1$ denotes the two decisions by Willie in favor of $\mathcal{H}0$ and $\mathcal{H}1$ respectively. We in this paper consider the infinite blocklength regime, i.e., $N\to\infty$. $\mathbb{P}_W$ can be calculated as

$$\mathbb{P}_W = \begin{cases} a_1 t_1 P_S + \dfrac{t_2 P_J}{A_S-1} + N_0, & \mathcal{H}0 \\ t_1 P_S + \dfrac{t_2 P_J}{A_S-1} + N_0. & \mathcal{H}1 \end{cases} \tag{9}$$

Where $t_1 = |\mathbf{h}_{SW}\mathbf{w}_1|^2$ and $t_2 = \|\mathbf{h}_{SW}\mathbf{W}_{AN}\|^2$. After receiving the signals, Willie needs to judge whether Source has emitted x_R to Roy. Willie is only conscious of the statistical property of P_J and P_J is time-varying, so he may make a wrong decision. A *false alarm* (FA) indicates that a decision for x_R being transmitted to Roy is made when $\mathcal{H}0$ is true, and a *miss detection* (MD) indicates that a decision for x_R not being sent to Roy is made when $\mathcal{H}1$ is true. We denote the probabilities of the FA and MD by $\mathbb{P}_{\mathbb{FA}}$ and $\mathbb{P}_{\mathbb{MD}}$, respectively. Their close-form expressions are acquired in *Theorem* 1.

Theorem 1: The false alarm probability and the miss detection probability can be respectively given by

$$\mathbb{P}_{\mathbb{FA}} = \begin{cases} 1, & \tau \leq \tau_1 \\ 1 - \dfrac{(A_S-1)(\tau-\tau_1)}{t_2 P_J^{max}}, & \tau_1 < \tau \leq \tau_2 \\ 0, & \tau > \tau_2 \end{cases} \tag{10}$$

and

$$\mathbb{P}_{\mathbb{MD}} = \begin{cases} 0, & \tau \leq \tau_3 \\ \dfrac{(A_S-1)(\tau-\tau_3)}{t_2 P_J^{max}}, & \tau_3 < \tau \leq \tau_4 \\ 1, & \tau > \tau_4 \end{cases} \tag{11}$$

where $\tau_1 = t_1 a_1 P_S + N_0$, $\tau_2 = \tau_1 + t_2 P_J^{max}/(A_S-1)$, $\tau_3 = t_1 P_S + N_0$ and $\tau_4 = \tau_3 + t_2 P_J^{max}/(A_S-1)$.

Proof: In the light of the detection strategy (8), $\mathbb{P}_{\mathbb{FA}}$ and $\mathbb{M}_{\mathbb{MD}}$ can be computed by $\mathbb{P}_{\mathbb{FA}} = \Pr(\mathcal{D}1|\mathcal{H}0) = \Pr(t_1 a_1 P_S + N_0 + t_2 P_J/(A_S-1) \geq \tau)$ and $\mathbb{M}_{\mathbb{MD}} = \Pr(\mathcal{D}0|\mathcal{H}1) = \Pr(t_1 P_S + N_0 + t_2 P_J/(A_S-1) < \tau)$, respectively. The p.d.f. of P_S is $U[0, P_J^{max}]$. After some derivation, their closed-form expressions are formulated and the *Theorem* 1 is proved. ■

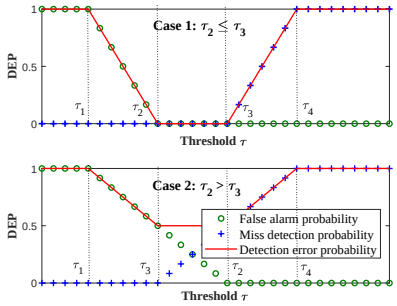

Fig. 2. Detection error probability v.s. decision threshold.

Assuming that Source transmits the covert signal x_R with the prior probability 0.5, i.e., $\rho = \Pr(\mathcal{H}0) = \Pr(\mathcal{H}1) = 0.5$. In this case, the DEP of Willie can be defined as $\Xi = \mathbb{P}_{\mathbb{FA}} + \mathbb{P}_{\mathbb{MD}}$ [13]. To detect the communication successfully, Willie needs to minimize the DEP by optimizing the decision threshold τ. The optimal detector is shown in the following *Theorem* 2.

Theorem 2: The optimal decision threshold τ^* is given by

$$\tau^* \in \begin{cases} [\tau_2, \tau_3], & \tau_2 \leq \tau_3 \\ [\tau_3, \tau_2], & \tau_2 > \tau_3. \end{cases} \tag{12}$$

and the corresponding MDEP can be written as

$$\Xi^* = \begin{cases} 0, & \tau_2 \leq \tau_3 \\ 1 - \dfrac{a_2 t_1 P_S(A_S-1)}{t_2 P_J^{max}}, & \tau_2 > \tau_3. \end{cases} \tag{13}$$

Proof: Willie designs the optimal detector by formulating the optimization problem $\min_\tau \ \Xi = \mathbb{P}_{\mathbb{FA}} + \mathbb{P}_{\mathbb{MD}}$. By calculating, Ξ is a piecewise function w.r.t. τ and the segmentation points are respectively τ_1, τ_2, τ_3 and τ_4, satisfying $\tau_1 < \tau_2(\tau_3) < \tau_4$. Owing to the randomness of P_J, the relationship between τ_2 and τ_3 is not fixed. We have a categorised discussion under $case1: \tau_2 \leq \tau_3$ and $case2: \tau_2 > \tau_3$, shown in Fig. 2. With some straightforward

$$\Pi = \Pi_1 \times \left\{1 - \frac{(A_S-1)a_2P_S}{(A_S-2)P_J^{max}}\left(1-\left(1+\frac{P_J^{max}}{(A_S-1)a_2P_S}\right)^{2-A_S}\right)+\left(1+\frac{P_J^{max}}{(A_S-1)a_2P_S}\right)^{1-A_S}\right\}. \quad (14)$$

$$\Pi^B = 1-\theta\left\{\exp\left(-\frac{N_0\gamma_B}{\lambda_{SB}a_1P_S}-\frac{N_0\gamma_R}{\lambda_{SB}P_S(a_2-a_1\gamma_R)}\right)\sum_{k=0}^{A_S-1}\frac{1}{k!}\left(\frac{N_0\gamma_B}{\lambda_{SB}a_1P_S}\right)^k\sum_{k=0}^{A_S-1}\frac{1}{k!}\left(\frac{N_0\gamma_R}{\lambda_{SB}P_S(a_2-a_1\gamma_R)}\right)^k\right\}. \quad (18)$$

algebraic manipulations, the *Theorem* 2 is proved. ∎

IV. Joint Secure and Covert NOMA Communications

In this section, we analyze the joint secure and covert NOMA transmission scheme from the perspective of the terminals.

A. Average MDEP

Source has access to the statistical CSI of Willie only, so we derive the expected value of Ξ^* over all realizations of $\mathbf{h}_{SW}$ as the covertness indicator, show in the *Theorem* 3.

Theorem 3: The average MDEP Π of the radiometer at Willie can be given in (14), where $\Pi_1 = 1 - \left(1+\frac{P_J^{max}}{(A_S-1)a_2P_S}\right)^{1-A_S}$.

Proof: According to 13, Π can be computed by

$$\Pi = \underbrace{\Pr(\tau_2>\tau_3)}_{\Pi_1}\underbrace{\mathbb{E}\left(\Xi^*|\tau_2>\tau_3\right)}_{\Pi_2} + \Pr(\tau_2\le\tau_3)\times 0. \quad (15)$$

$$\Pi_1 = \Pr\left(t_1 < \frac{t_2P_J^{max}}{a_2P_S(A_S-1)}\right) = \int_0^{\infty}\int_0^{\frac{P_J^{max}y}{a_2P_S(A_S-1)}} f_{t_1}(x)f_{t_2}(y)dxdy. \quad (16)$$

$$\Pi_2 = 1-\mathbb{E}\left\{\frac{a_2t_1P_S(A_S-1)}{t_2P_J^{max}} \mid \tau_2>\tau_3\right\} = 1- \int_0^{\infty}\int_0^{\frac{P_J^{max}y}{a_2P_S(A_S-1)}} \frac{a_2P_S(A_S-1)x}{P_J^{max}y} f_{t_1}(x)f_{t_2}(y)dxdy, \quad (17)$$

where $f_{t_1}(x)$ and $f_{t_2}(y)$ are the p.d.f.s of t_1 and t_2, respectively. Because $\mathbf{h}_{SW}$ is independent of $\mathbf{h}_{SB}$, t_1 and t_2 follow the exponential distribution $\exp(\frac{1}{\lambda_{SW}})$ and the Gamma distribution Gamma(A_S-1,λ_{SW}), respectively. Substituting their p.d.f.s into (16) and (17), *Theorem* 3 is proved after some mathematical derivation. ∎

B. Connection and Secrecy Outage Probabilities

Source aims to successfully transmit the covert signal x_R and the secure signal x_B to Roy and Bob, respectively. We preset the target rates of Bob and Roy and the target secrecy rate of Bob to R_B, R_R and R_S, respectively. When the channel capacities are less than the target rates, the network will experience a connection outage. When the eavesdropping rate at Roy is greater than the rate redundancy $(R_B - R_S)$, Bob will experience a secrecy outage [4]. Following, we detail the COPs and the SOP.

Theorem 4: The COPs of Bob and Roy can be given in (18) and (19), respectively.

$$\Pi^R = 1-\theta\times\left\{\frac{(\frac{1}{\phi})^{2-A_S}-m_3^{2-A_S}}{m_1P_J^{max}(A_S-2)\phi^{A_S-1}}\exp\left(-\frac{m_2}{\lambda_{SR}}\right)\right\}, \quad (19)$$

where $m_1 = \frac{\gamma_R}{(A_S-1)P_S(a_2-a_1\gamma_R)}$, $m_2 = \frac{N_0\gamma_R}{P_S(a_2-a_1\gamma_R)}$, $m_3 = \frac{1}{\phi}+m_1P_J^{max}$, $\gamma_R = 2^{R_R}-1$ and $\gamma_B = 2^{R_B}-1$. $\theta = 1$, if $a_1 < 1/(1+\gamma_R)$; otherwise $\theta = 0$, which means the communication is suspended.

Theorem 5: The SOP of Bob can be given by

$$\Pi^S = \left\{\left(\frac{1}{\phi}\right)^{2-A_S}-\left(\frac{1}{\phi}+\frac{P_J^{max}\gamma_S}{a_1P_S(A_S-1)}\right)^{2-A_S}\right\} \times\frac{a_1P_S(A_S-1)}{\gamma_S(A_S-2)P_J^{max}\phi^{A_S-1}}\exp\left(-\frac{N_0\gamma_S}{\lambda_{SR}a_1P_S}\right) \times(1-\Pi^R), \quad (20)$$

where $\gamma_S = 2^{R_B-R_S}-1$.

Proof: Π^B, Π^R and Π^S can be calculated by $\Pi^B = 1-\Pr(\mathbb{SINR}_{B\to R}>\gamma_R)\Pr(\mathbb{SINR}_B>\gamma_B)$, $\Pi^R = \Pr(\mathbb{SINR}_R<\gamma_R)$ and $\Pi^S = \Pr(\mathbb{SINR}_R>\gamma_R)\Pr(\mathbb{SINR}_{R\to B}>\gamma_S)$, respectively. Through some mathematical derivation, *Theorem* 4 and *Theorem* 5 can be proved. ∎

C. Optimal Transmission Strategy

Source needs to protect x_B from eavesdropping while avoiding x_R being detected successfully. By optimizing a_1, we in this subsection maximize the effective covert rate of Roy, defined as $(1-\Pi^R)R_R$, subject to the covertness requirement of Roy and the reliability and secrecy constraints of Bob. Similar to [13], x_R can be covertly transmitted to Roy when, for a sufficiently small $\varepsilon > 0$, $\Pi \ge 1-\varepsilon$ is satisfied. The optimization problem can be formulated as

$$\max_{a_1}\ (1-\Pi^R)R_R \quad (21a)$$
$$s.t.\ \Pi \ge 1-\varepsilon, \quad (21b)$$
$$\Pi^B \le \pi^B, \quad (21c)$$
$$\Pi^S \le \pi^S, \quad (21d)$$
$$0<a_1<0.5,\ a1+a2=1 \text{ and } (6). \quad (21e)$$

,where π^B and π^S are the maximum tolerable outage and secrecy outage probabilities at Bob. (21b) is the covertness demand of Roy. (21c) and (21d) are the reliability and secrecy demands of Bob, respectively. (21e) is the boundary constraint of a_1. Numerically, we can verify that Π_R and Π are two monotonically increasing functions w.r.t. $a1$. To maximize

$(1-\Pi^R)R_R$, $a1$ should be as small as possible. From (21c), we can acquire $a_1 \geq a_1^{\ddagger}$, where $a_1^{\ddagger}$ is the solution of $\Pi(a1) = 1-\varepsilon$. From (18) and (20), it is found that Π^B and Π^S are not the monotonic functions w.r.t. $a1$. We can acquire the optimal value $a1^*$ satisfying (21c) and (21d), by using the 1D numerical search algorithm over the interval $[a_1^{\ddagger}, \min(a_1^{\dagger}, 0.5)]$.

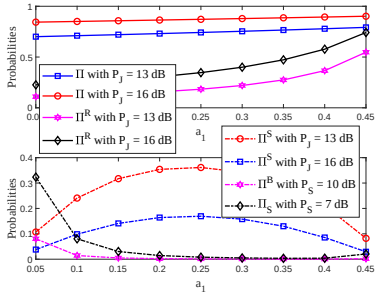

Fig. 3. Probabilities v.s. the power allocation factor a_1.

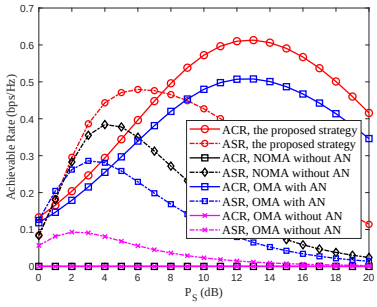

Fig. 4. ACRs and ASRs for the different strategy.

V. Numerical Results and Discussions

In this section, numerical results are presented to study the proposed strategy. Some system parameters are set as follows: $A_S = 5$, $\phi = 0.1$, $N0 = -10$ dB, $P_S = 7$ dB, $P_J^{max} = 13$ dB, $\pi^B = \pi^S = \varepsilon = 0.15$, $R_R = R_B = 1$ bps/Hz and $R_S = 0.5$ bps/Hz.

Fig. 3 demonstrates the relationships between Π, Π^B, Π^S, and Π^R and $a1$. We can find that Π and Π^R are the monotonically increasing functions. The larger $a1$, the smaller the power allocated to x_C and the larger the COP of Roy and the DEP of Willie. As $a1$ increases, Π^S first increases and then decreases, which means that Roy can decode x_C and x_B. And then, the power allocated to x_C gets smaller, which causes the decoding errors of Roy and the decreasing Π^S. Π^B first decreases and then increases with $a1$. When $a1$ is close to 0.5, Bob cannot decode x_c for the SIC, which enlarges Π^B. Also, Fig. 3 verifies that the optimization problem (21) can be solved by a 1D numerical search.

Fig. 3 compares the covertness and security of our proposed strategy and three benchmark schemes, NOMA without AN, OMA with AN and OMA without AN. The used metrics are respectively the achievable effective covert rate (ACR) and the achievable secrecy rate (ASR), defined as $\Pi(1-\Pi^R)R_R$ and $(1-\Pi^B)(1-\Pi^S)R_S$. It is observed that our proposed strategy outperforms the benchmark schemes in terms of the ACR and the ASR. Without the NOMA, the decoding SINRs will be reduced. Without the AN, the warden and eavesdropper are more likely to detect and overhear.

VI. Conclusion

In this paper, we investigated the joint covert and secure transmission problem in the NOMA network against the internal eavesdropping and the external detecting. The transmitter sent the AN signal with random power when communicating. To reduce the impact on the NOMA, a beamforming strategy was performed at the transmission. The eavesdropping rate of the internal SU was degraded while the external warden could not successfully monitor. The warden minimized its DEP by optimizing the decision threshold of the radiometer. The transmitter had no specific CSI of the warden, so the average MDEP was characterized over all realizations of the channel. The closed-form expressions of the COP of the NOMA users and the SOP of the WU were derived. Following the paradigm, we formulated an effective covert rate maximization problem, under the constraints of the covertness of the SU and the security and reliability of the WU, which could be solved by a 1D numerical search. Finally, simulation results validated the proposed paradigm had higher security and reliability, as compared with the benchmark schemes.

References

[1] X. Lu et al., "Reinforcement Learning-Based Physical Cross-Layer Security and Privacy in 6G," *IEEE Commun. Surv. Tutor.*, vol. 25, no. 1, pp. 425-466, Nov. 2022.

[2] X. Pei et al., "Next-Generation Multiple Access Based on NOMA With Power Level Modulation," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 4, pp. 1072-1083, Apr. 2022.

[3] Y. Mao et al., "Rate-Splitting Multiple Access: Fundamentals, Survey, and Future Research Trends," *IEEE Commun. Surv. Tutor.*, vol. 24, no. 4, pp. 2073-2126, Jul. 2022.

[4] G. Pan et al., "On The Secrecy Performance of MISO SWIPT Systems with TAS and Imperfect CSI," *IEEE Trans. Commun.*, vol. 64, no. 9, pp. 3831-3843, Sep. 2016.

[5] X. Li et al., "Enhancing Secrecy Performance for STAR-RIS NOMA Networks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 2, pp. 2684-2688, Feb. 2023.

[6] K. Cao et al., "Improving Physical Layer Security of Uplink NOMA via Energy Harvesting Jammers," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 786-799, Sep. 2020.

[7] Y. Feng et al., "Beamforming Design and Power Allocation for Secure Transmission With NOMA," *IEEE Trans. Wireless Commun.*, vol. 18, no. 5, pp. 2639-2651, May 2019.

[8] F. Jia et al., "Guaranteeing Positive Secrecy Rate for NOMA System Against Internal Eavesdropping," *IEEE Commun. Lett.*, vol. 25, no. 6, pp. 1805-1809, Jun. 2021.

[9] K. Cao et al., "Secure Transmission Designs for NOMA Systems Against Internal and External Eavesdropping," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 2930-2943, Mar. 2020.

[10] Z. Duan et al., "Covert Communication in Uplink NOMA Systems under Channel Distribution Information Uncertainty," *IEEE Commun. Lett.*, early access, doi: 10.1109/LCOMM.2023.3255838.

[11] L. Tao et al., "Covert Communication in Downlink NOMA Systems With Random Transmit Power," *IEEE Wireless Commun. Lett.*, vol. 9, no. 11, pp. 2000-2004, Nov. 2020.

[12] C. Wang et al., "Achieving Covertness and Security in Broadcast Channels With Finite Blocklength," *IEEE Trans. Wireless Commun.*, vol. 21, no. 9, pp. 7624-7640, Sep. 2022.

[13] R. Sun et al., "Covertness and Secrecy Study in Untrusted Relay-Assisted D2D Networks" *IEEE Internet Things J.*, vol. 10, no. 1, pp. 17-30, Jau. 2023.

[14] M. Forouzesh et al., "Joint Information-Theoretic Secrecy and Covert Communication in the Presence of an Untrusted User and Warden" *IEEE Internet Things J.*, vol. 8, no. 9, pp. 7170-7181, May 2021.

[15] Y. Jiang, W. W. Hager and J. Li, "Tunable Channel Decomposition for MIMO Communications Using Channel State Information," *IEEE Trans. Signal Process.*, vol. 54, no. 11, pp. 4405-4418, Nov. 2006.