Design of Secure NOMA Against Full-Duplex Proactive Eavesdropping

Lu Lv, Zhiguo Ding, *Senior Member, IEEE*, Jian Chen, *Member, IEEE*, and Naofal Al-Dhahir, *Fellow, IEEE*

***Abstract*—We investigate the problem of secure non-orthogonal multiple access (NOMA) against full-duplex proactive eavesdropping, where the eavesdropper performs passive eavesdropping and active jamming simultaneously to interrupt the NOMA transmissions. To avoid the transmission outage caused by the unknown jamming level from the eavesdropper, we propose a novel transmission outage constrained scheme to limit the transmission outage probabilities of the users to a maximum tolerable threshold, which is also helpful in reducing the secrecy outage. We derive analytical expressions for the secrecy outage probability and secrecy diversity order to characterize the secrecy performance. Simulation results are provided to demonstrate the accuracy of the derived analytical results and the efficiency of the proposed scheme.**

***Index Terms*—Non-orthogonal multiple access, secure transmission, full-duplex, proactive eavesdropper.**

I. Introduction

Non-orthogonal multiple access (NOMA) has been proposed as a promising solution to improve spectral efficiency and reduce transmission latency for future wireless networks [1]. With the use of superposition coding and successive interference cancellation (SIC) techniques, multiple users can be simultaneously served in the same resource block (i.e. time/frequency/code), and massive connectivity can be realized efficiently by NOMA.

However, the support of massive connectivity in NOMA is also a critical weakness which can be exploited by eavesdroppers to intercept signals of all users, due to the broadcast nature of wireless channels [2], [3]. In this context, security provisioning for NOMA using physical layer security techniques has attracted considerable research efforts [4]–[9]. In [4], the optimal designs of transmission rate, decoding order, and power allocation for NOMA with secrecy considerations were investigated. Secure beamforming with artificial noise for NOMA was studied in [5], [6]. Robust secure power allocation and subcarrier assignment for full-duplex NOMA were addressed in [7]. The secrecy issues in cooperative relay assisted NOMA systems were designed and analyzed in [8], [9].

All of the aforementioned works on NOMA security assume that the eavesdropper operates in a half-duplex mode and only performs passive eavesdropping. However, the eavesdropper may have more powerful signal processing capability, for example, the full-duplex radio [10]–[12] that simultaneously performs passive eavesdropping and active jamming. Since NOMA is interference-limited, the emitted jamming can significantly decrease the users' data rates, which in turn enhances the interception capability of the eavesdropper. Theoretical studies of secure NOMA with full-duplex proactive eavesdropping are still lacking in the literature. Furthermore, the eavesdropper is often passive, and it is difficult for the users to obtain the jamming level of the eavesdropper. Without precisely knowing the jamming level, the NOMA users may experience transmission outage with a high probability, which further leads to secrecy outage.

To address the above challenging secrecy issues, we investigate a secrecy-enhancing design for NOMA against full-duplex proactive eavesdropping. We propose a novel transmission outage constrained scheme, where the codeword rates for the paired users are specifically designed to guarantee that the transmission outage probabilities of the paired users affected by the unknown jamming level of the eavesdropper are constrained to a maximum tolerable threshold, to avoid the transmission outage and reduce the secrecy outage. We derive closed-form expressions for the secrecy outage probability and the secrecy diversity order. Our simulation results show that full secrecy diversity orders at the paired users can be achieved by the proposed scheme.

II. System Model

Consider a downlink NOMA transmission, consisting of one base station denoted by S, one eavesdropper denoted by E, and K users denoted by $D_1 \ldots D_K$. Each node in the system is equipped with a single antenna. To mitigate the strong inter-user interference and the high processing power for SIC, user pairing for NOMA is adopted, in which two users, i.e., D_n and D_m are selected to perform NOMA jointly.

All channels undergo independent quasi-static fading. The channel coefficients from S to D_k and E are denoted by $h_{s,k}$ and $h_{s,e}$, and the channel coefficient from E to D_k is denoted by $h_{e,k}$ ($k \in \{1, \ldots, K\}$). For brevity, we denote the channel gains by $g_{s,k} = |h_{s,k}|^2$, $g_{s,e} = |h_{s,e}|^2$, and $g_{e,k} = |h_{e,k}|^2$. Throughout this letter, the following set of assumptions are made

a) We assume independent Rayleigh fading with parameters $\mathbb{E}[g_{s,k}] = \omega_{s,k}$, $\mathbb{E}[g_{s,e}] = \omega_{s,e}$, and $\mathbb{E}[g_{e,k}] = \omega_{e,k}$.
b) The channel gains from S to $D_1 \ldots D_K$ are ordered in an ascending manner as $g_{s,1} \leq \cdots \leq g_{s,n} \leq \cdots \leq g_{s,m} \leq \cdots \leq g_{s,K}$ to facilitate the application of NOMA.
c) We assume that S knows the instantaneous channel state information (CSI) of $h_{s,k}$. However, S does not know any instantaneous CSI related to E, i.e., $h_{s,e}$ and $h_{e,k}$, since E is a malicious user to the legitimate system, and it is difficult for S to obtain the CSI of E. Only the statistical CSI of $\omega_{s,e}$ and $\omega_{e,k}$ is available at S, which can be estimated by using the knowledge of the distance between S and E.
d) Both S and D_k work in a half-duplex mode. While E has the full-duplex capability and performs simultaneous eavesdropping and jamming to obstruct the NOMA transmissions.
e) The average transmission power at S and E is denoted by P_s and P_e, and the additive noise at each receiver is a complex Gaussian random variable with mean equal to zero

Manuscript received December 25, 2018; revised March 10, 2019; accepted March 24, 2019. The work of L. Lv and J. Chen was supported in part by the National Natural Science Foundation of China under grants 61601347 and 61771366, and in part by the 111 Project of China under grant B08038. The work of Z. Ding was supported in part by the UK EPSRC under grant EP/N005597/2, and in part by H2020-MSCA-RISE-2015 under grant 690750. The work of N. Al-Dhahir was supported by NPRP under grant NPRP 8-627-2-260 from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors. The associate editor coordinating the review of this paper and approving it for publication was T. Riihonen. *(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_xidian@hotmail.com; jianchen@mail.xidian.edu.cn).

Z. Ding is with the School of Electrical and Electronic Engineering, The University of Manchester, Manchester M13 9PL, UK (e-mail: zhiguo.ding@manchester.ac.uk).

N. Al-Dhahir is with the Department of Electrical Engineering, University of Texas at Dallas, Richardson, TX 75080, USA (e-mail: aldhahir@utdallas.edu).

and variance equal to ω_0. The transmit signal-to-noise ratios (SNRs) at S and E are denoted by $\rho_s = \frac{P_s}{\omega_0}$ and $\rho_e = \frac{P_e}{\omega_0}$.

During each fading block, S uses NOMA to send a superimposed signal $(\sqrt{\alpha_n}x_n + \sqrt{\alpha_m}x_m)$ to D_n and D_m, where α_n and α_m are the NOMA power allocation coefficients satisfying $\alpha_n + \alpha_m = 1$ and $\alpha_n < \alpha_m$ for fairness considerations. Since E operates in a full-duplex mode, it not only intercepts the superimposed signal for eavesdropping purpose, but also emits a jamming signal z to D_n and D_m to interfere with their signal reception, which is challenging for secure communications.

In NOMA, SIC decoding at each receiver always starts from the weak signal towards the strong signal. The receiver of D_n first decodes and subtracts x_m via SIC, and then decodes x_n using the residual signal, yielding the received signal-to-interference-plus-noise ratios (SINRs) as

$$\gamma_n^{x_m} = \frac{\alpha_m \rho_s g_{s,n}}{\alpha_n \rho_s g_{s,n} + \rho_e g_{e,n} + 1}, \ \gamma_n^{x_n} = \frac{\alpha_n \rho_s g_{s,n}}{\rho_e g_{e,n} + 1}. \quad (1)$$

The receiver of D_m decodes x_m directly by treating other signals as noise. Accordingly, its received SINR is given by

$$\gamma_m^{x_m} = \frac{\alpha_m \rho_s g_{s,m}}{\alpha_n \rho_s g_{s,m} + \rho_e g_{e,m} + 1}. \quad (2)$$

Similar to [4], [6], [8], the worst-case eavesdropping from the users' perspective is assumed, where x_m is completely decoded at E before it starts to decode x_n. This assumption overestimates the eavesdropper's capability, which makes the design and analysis in this letter robust in practical scenarios. Thus, the upper bounds on the received SINRs at E are

$$\gamma_e^{x_m} = \frac{\alpha_m \rho_s g_{s,e}}{\alpha_n \rho_s g_{s,e} + \zeta \rho_e + 1}, \ \gamma_e^{x_n} = \frac{\alpha_n \rho_s g_{s,e}}{\zeta \rho_e + 1}, \quad (3)$$

where $\zeta \in [0, 1]$ is the residual self-interference coefficient due to the imperfect self-interference cancellation.

III. Transmission Outage Constrained Scheme and Its Performance Analysis

Since S does not know the CSI of $h_{e,n}$ and $h_{e,m}$, it cannot adopt the variable-rate strategy for codeword transmission, and only fixed codeword rates, i.e., $R_b^{x_m}$ and $R_b^{x_n}$, can be utilized to send x_m and x_n. In this situation, a transmission outage happens if the main channel capacity of x_m (or x_n) is smaller than the codeword rate $R_b^{x_m}$ (or $R_b^{x_n}$).

To proceed, we introduce the following lemma.

Lemma 1: To achieve the optimal transmission outage performance for a given SIC decoding $x_m \to x_n$, the NOMA power allocation coefficients should satisfy the following condition

$$\frac{\alpha_m}{\tau_m} - \alpha_n \geq \frac{\alpha_n}{\tau_n}, \quad (4)$$

where $\tau_m = 2^{R_b^{x_m}} - 1$ and $\tau_n = 2^{R_b^{x_n}} - 1$.

Proof: The transmission outage event $\mathcal{O}_n$ at D_n can be expressed as

$$\begin{aligned} \mathcal{O}_n &= \left\{\gamma_n^{x_m} < \tau_m\right\} \bigcup \left\{\gamma_n^{x_m} \geq \tau_m, \gamma_n^{x_n} < \tau_n\right\} \\ &= \left\{g_{s,n} < \max\left(\Lambda_m, \Lambda_n\right)\right\}, \end{aligned} \quad (5)$$

where $\Lambda_m = \frac{\tau_m(1+\rho_e g_{e,n})}{\alpha_m - \alpha_n \tau_m}$, $\Lambda_n = \frac{\tau_n(1+\rho_e g_{e,n})}{\alpha_n}$. In particular, the condition $\alpha_m > \alpha_n \tau_m$ holds when applying NOMA. Since the SIC ordering at D_n is to decode the signal x_m first and then decode the signal x_n, the condition $\Lambda_m \leq \Lambda_n$ should be satisfied to achieve the optimal transmission outage performance, based on [1, Theorem 1]. Therefore, after some algebraic manipulations, we readily obtain the result in (4). ■

Using Lemma 1, the transmission outage probabilities of D_n and D_m conditioned on $g_{s,n}$ and $g_{s,m}$ can be computed by

$$\begin{aligned} P_{\text{top}}^n &= 1 - \Pr\left(\gamma_n^{x_m} \geq \tau_m, \gamma_n^{x_n} \geq \tau_n \mid g_{s,n}\right) \\ &= 1 - \Pr\left(g_{e,n} \leq \frac{1}{\rho_e} \min\left\{\left(\frac{\alpha_m}{\tau_m} - \alpha_n\right)\rho_s g_{s,n} \right.\right. \\ &\quad \left.\left. - 1, \frac{\alpha_n}{\tau_n}\rho_s g_{s,n} - 1\right\}\right) = e^{-\frac{\alpha_n \rho_s g_{s,n} - \tau_n}{\rho_e \tau_n \omega_{e,n}}}, \end{aligned} \quad (6)$$

$$\begin{aligned} P_{\text{top}}^m &= \Pr\left(\gamma_m^{x_m} < \tau_m \mid g_{s,m}\right) \\ &= \Pr\left(g_{e,m} > \frac{(\alpha_m - \alpha_n \tau_m)\rho_s g_{s,m} - \tau_m}{\rho_e \tau_m}\right) \\ &= e^{-\frac{(\alpha_m - \alpha_n \tau_m)\rho_s g_{s,m} - \tau_m}{\rho_e \tau_m \omega_{e,m}}}. \end{aligned} \quad (7)$$

1) Proposed Scheme: To guarantee both reliability and security for NOMA, next we propose a transmission outage constrained scheme. Specifically, a maximum tolerable transmission outage constraint ϵ for both information signals is introduced to achieve reliable transmission. Hence, the codeword rates of x_n and x_m should be selected to ensure that the transmission outage probabilities of D_m and D_n are bounded by ϵ, i.e., $P_{\text{top}}^n \leq \epsilon$ and $P_{\text{top}}^m \leq \epsilon$, and thus, the transmission outage event can be potentially avoided. Based on (6) and (7), we can obtain the optimal codeword rates as

$$R_b^{x_n}(\epsilon) = \log_2\left(1 + \alpha_n \delta_n(\epsilon) \rho_s g_{s,n}\right), \quad (8)$$

$$R_b^{x_m}(\epsilon) = \log_2\left(1 + \frac{\alpha_m \delta_m(\epsilon) \rho_s g_{s,m}}{\alpha_n \delta_m(\epsilon) \rho_s g_{s,m} + 1}\right), \quad (9)$$

where $\delta_n(\epsilon) = (1 - \rho_e \omega_{e,n} \ln \epsilon)^{-1}$ and $\delta_m(\epsilon) = (1 - \rho_e \omega_{e,m} \ln \epsilon)^{-1}$. It is worth noting that our analysis still holds in a general case where different values of ϵ for the transmission outage probabilities of D_m and D_n are assumed.

Therefore, the secrecy rate at D_n (D_m) under the transmission outage constraint ϵ is expressed as

$$R_{\text{sec}}^{x_{n(m)}} = \left\{R_b^{x_{n(m)}}(\epsilon) - \log_2\left(1 + \gamma_e^{x_{n(m)}}\right)\right\}^+, \quad (10)$$

where $\{A\}^+ = \max(A, 0)$.

Remark 1: It is easy to validate that both $\delta_n(\epsilon)$ and $\delta_m(\epsilon)$ are monotonically increasing functions with ϵ. This means that by decreasing ϵ, the transmission outage probabilities for D_n and D_m can be lowered, while the codeword rates $R_b^{x_n}(\epsilon)$ and $R_b^{x_m}(\epsilon)$ are decreased, which leads to an increase in the secrecy outage probabilities for D_n and D_m due to the reduced secrecy rates. Therefore, there exits a reliability-security tradeoff.

2) Secrecy Outage Probability: Several channel statistics are provided in what follows, which are useful for characterizing the secrecy outage probability.

Lemma 2: Utilizing order statistics, the cumulative distribution functions for $g_{s,n}$ and $g_{s,m}$ can be computed by

$$F_{g_{s,n}}(x) = b_n \widetilde{\sum}_{k_1,i} \frac{(-1)^{k_1+i}}{n + k_1} e^{-\frac{ix}{\omega_{s,n}}}, \quad (11)$$

$$F_{g_{s,m}}(x) = b_m \widetilde{\sum}_{k_2,j} \frac{(-1)^{k_2+j}}{m + k_2} e^{-\frac{jx}{\omega_{s,m}}}, \quad (12)$$

where we have used the following notations: $b_n = \frac{K!}{(K-n)!(n-1)!}$, $b_m = \frac{K!}{(K-m)!(m-1)!}$, $\widetilde{\sum}_{k_1,i} = \sum_{k_1=0}^{K-n}\sum_{i=0}^{n+k_1}\binom{K-n}{k_1}\binom{n+k_1}{i}$, and $\widetilde{\sum}_{k_2,j} = \sum_{k_2=0}^{K-m}\sum_{j=0}^{m+k_2}\binom{K-m}{k_2}\binom{m+k_2}{j}$.

Lemma 3: According to (3), the probability density functions for $\gamma_e^{x_n}$ and $\gamma_e^{x_m}$ can be computed by

$$f_{\gamma_e^{x_n}}(y) = \frac{\beta e^{-\frac{\beta y}{\alpha_n \rho_s \omega_{s,e}}}}{\alpha_n \rho_s \omega_{s,e}}, \tag{13}$$

$$f_{\gamma_e^{x_m}}(z) = \begin{cases} \frac{\beta \alpha_m e^{-\frac{\beta z}{\rho_s \omega_{s,e}(\alpha_m - \alpha_n z)}}}{\rho_s \omega_{s,e}(\alpha_m - \alpha_n z)^2}, & z \le \frac{\alpha_m}{\alpha_n}, \\ 0, & z > \frac{\alpha_m}{\alpha_n}, \end{cases} \tag{14}$$

where $\beta = \zeta\rho_e + 1$.

Utilizing (11) and (13), the secrecy outage probability for D_n can be derived as

$$\begin{aligned} P_{\text{sop}}^n &= \Pr\left(R_{\text{sec}}^{x_n} < R_s^{x_n}\right) \\ &= \int_0^\infty \Pr\Big(g_{s,n} < \Psi_1(y)\Big) f_{\gamma_e^{x_n}}(y) dy \\ &= b_n \widetilde{\sum}_{k_1,i} \frac{(-1)^{k_1+i}\delta_n(\epsilon)\beta\omega_{s,n} e^{-\frac{i(\eta_n-1)}{\alpha_n \delta_n(\epsilon)\rho_s\omega_{s,n}}}}{(n+k_1)(i\eta_n\omega_{s,e} + \delta_n(\epsilon)\beta\omega_{s,n})}, \end{aligned} \tag{15}$$

where $\Psi_1(y) = \frac{\eta_n(1+y)-1}{\alpha_n\delta_n(\epsilon)\rho_s}$, $\eta_n = 2^{R_s^{x_n}}$, and $R_s^{x_n}$ denotes the targeted secrecy rate for x_n.

Similarly, based on (12) and (14), the secrecy outage probability for D_m can be computed by

$$\begin{aligned} P_{\text{sop}}^m &= \Pr\left(R_{\text{sec}}^{x_m} < R_s^{x_m}\right) \\ &= \int_0^{\frac{\alpha_m}{\alpha_n}} \Pr\left(\Big(\alpha_m - \alpha_n\big[\eta_m(1+z)-1\big]\Big)\right. \\ &\quad \left. \times\, g_{s,m} < \frac{\eta_m(1+z)}{\delta_m(\epsilon)\rho_s}\right) f_{\gamma_e^{x_m}}(z) dz \\ &\overset{\text{(i)}}{=} \int_{\frac{1-\eta_m\alpha_n}{\eta_m\alpha_n}}^{\frac{\alpha_m}{\alpha_n}} f_{\gamma_e^{x_m}}(z) dz + \int_0^{\frac{1-\eta_m\alpha_n}{\eta_m\alpha_n}} f_{\gamma_e^{x_m}}(z) \\ &\quad \times \Pr\left(g_{s,m} < \frac{\eta_m(1+z)-1}{\delta_m(\epsilon)\rho_s\big[1-\alpha_n\eta_m(1+z)\big]}\right) dz \\ &\overset{\text{(ii)}}{\approx} e^{-\frac{\beta(1-\eta_m\alpha_n)}{\alpha_n\rho_s(\eta_m-1)\omega_{s,e}}} + b_m \widetilde{\sum}_{k_2,j} \frac{(-1)^{k_2+j}\beta\alpha_m}{(m+k_2)\rho_s\omega_{s,e}} \\ &\quad \times \frac{\pi(1-\eta_m\alpha_n)}{2\eta_m\alpha_n L} \sum_{l=1}^{L} \sqrt{1-x_l^2}\,\Phi(y_l), \end{aligned} \tag{16}$$

where $\eta_m = 2^{R_s^{x_m}}$, $x_l = \cos(\frac{2l-1}{2L}\pi)$, $y_l = \frac{(1-\eta_m\alpha_n)(x_l+1)}{2\eta_m\alpha_n}$, $R_s^{x_m}$ denotes the target secrecy rate for x_m, and L denotes the number of terms for the Gauss-Chebyshev quadrature approximation. In (16), step (i) is obtained based on the fact that $\frac{1-\eta_m\alpha_n}{\eta_m\alpha_n} = \frac{1}{\eta_m}(\frac{\alpha_m}{\alpha_n}+1) - 1 < \frac{\alpha_m}{\alpha_n}$ due to $\eta_m > 1$, and step (ii) is obtained by using the Gauss-Chebyshev quadrature approximation. In (16), $\Phi(y_l)$ is given by

$$\Phi(y_l) = \frac{e^{-\frac{\beta y_l}{\rho_s\omega_{s,e}(\alpha_m - \alpha_n y_l)} - \frac{j\eta_m(1+y_l)-j}{\delta_m(\epsilon)\rho_s\omega_{s,m}[1-\alpha_n\eta_m(1+y_l)]}}}{(\alpha_m - \alpha_n y_l)^2}. \tag{17}$$

Next, we evaluate the secrecy outage probability for the selected user pair, which can be derived as

$$\begin{aligned} P_{\text{sop}}^{nm} &= 1 - \Pr\left(R_{\text{sec}}^{x_n} \ge R_s^{x_n}, R_{\text{sec}}^{x_m} \ge R_s^{x_m}\right) \\ &= 1 - \int_0^\phi \Pr\Big(g_{s,n} \ge \Psi_1(y), g_{s,m} \ge \Psi_2(y)\Big) f_{\gamma_e^{x_n}}(y) dy \\ &= 1 - \int_0^\phi \Pr\Big(g_{s,n} < \Psi_1(y), g_{s,m} < \Psi_2(y)\Big) f_{\gamma_e^{x_n}}(y) dy \\ &\quad + \int_0^\phi \Pr\Big(g_{s,n} < \Psi_1(y)\Big) f_{\gamma_e^{x_n}}(y) dy \\ &\quad + \int_0^\phi \Pr\Big(g_{s,m} < \Psi_2(y)\Big) f_{\gamma_e^{x_n}}(y) dy - F_{\gamma_e^{x_n}}(\phi), \end{aligned} \tag{18}$$

where $\phi = \frac{\alpha_m\eta_m}{\eta_m - 1} - 1$ and $\Psi_2(y) = \frac{\eta_m[1+\frac{\alpha_m y}{\alpha_n(y+1)}]-1}{\delta_m(\epsilon)\rho_s[1-\alpha_n\eta_m(1+\frac{\alpha_m y}{\alpha_n(y+1)})]}$. In the last equation of (18), we denote the first, the second, and the third integrals as I_1, I_2, and I_3, which are computed by

$$\begin{aligned} I_1 &= \frac{\beta b_n b_m}{\alpha_n\rho_s\omega_{s,e}} \widetilde{\sum}_{k_1,i} \widetilde{\sum}_{k_2,j} \frac{(-1)^{k_1+k_2+i+j}}{(n+k_1)(m+k_2)} \\ &\quad \times \frac{\phi\pi}{2L} \sum_{l=1}^{L} \sqrt{1-x_l^2}\, e^{-\frac{i\Psi_1(z_l)}{\omega_{s,n}} - \frac{j\Psi_2(z_l)}{\omega_{s,m}} - \frac{\beta z_l}{\alpha_n\rho_s\omega_{s,e}}}, \end{aligned} \tag{19}$$

$$\begin{aligned} I_2 &= b_n \widetilde{\sum}_{k_1,i} \frac{(-1)^{k_1+i}\delta_n(\epsilon)\beta\omega_{s,n}}{(n+k_1)(i\eta_n\omega_{s,e} + \delta_n(\epsilon)\beta\omega_{s,n})} \\ &\quad \times e^{-\frac{i(\eta_n-1)}{\alpha_n\delta_n(\epsilon)\rho_s\omega_{s,n}}} \left(1 - e^{-\frac{i\eta_n\phi}{\alpha_n\delta_n(\epsilon)\rho_s\omega_{s,n}} - \frac{\beta\phi}{\alpha_n\rho_s\omega_{s,e}}}\right), \end{aligned} \tag{20}$$

$$\begin{aligned} I_3 &= b_m \widetilde{\sum}_{k_2,j} \frac{(-1)^{k_2+j}\beta\alpha_m}{(m+k_2)\rho_s\omega_{s,e}} \\ &\quad \times \frac{\pi(1-\eta_m\alpha_n)}{2\eta_m\alpha_n L} \sum_{l=1}^{L} \sqrt{1-x_l^2}\,\Phi(y_l), \end{aligned} \tag{21}$$

where $z_l = \frac{\phi(x_l+1)}{2}$. Now, by substituting the results in (19)–(21) into (18), a closed-form P_{sop}^{nm} is obtained straightforwardly.

3) Secrecy Diversity Order: To gain more useful insights, we analyze the secrecy diversity order. As indicated by [3], the secrecy diversity order shows the asymptotic secrecy outage behavior when both ρ_s and main-to-eavesdropper ratio approach to infinity, i.e., $\rho_s \to \infty$ and $\lambda = \frac{\omega_{\text{M}}}{\omega_{s,e}} \to \infty$, where ω_{M} is related to the average channel gains from S to D_n and D_m. Specifically, we rewrite $\omega_{s,n}$ and $\omega_{s,m}$ as $\omega_{s,n} = \mu_{s,n}\omega_{\text{M}}$ and $\omega_{s,m} = \mu_{s,m}\omega_{\text{M}}$, where $\mu_{s,n}$ and $\mu_{s,m}$ are positive constants. Then, we obtain $\rho_{\text{M}} = \rho_s\omega_{\text{M}} \to \infty$ and $\rho_{\text{E}} = \rho_s\omega_{s,e} = o(\rho_{\text{M}})$, where $o(\cdot)$ denotes infinitesimal of higher order. Hence, the secrecy diversity order at D_k can be defined as $d_k = -\lim_{\rho_{\text{M}}\to\infty} \frac{\log P_{\text{sop}}^k}{\log \rho_{\text{M}}}$ for $k \in \{n, m\}$.

When $\rho_{\text{M}} \to \infty$, we can approximate (15) as

$$P_{\text{sop}}^n \overset{\rho_{\text{M}}\to\infty}{\simeq} \frac{\tilde{b}_n \int_0^\infty [\eta_n(1+y)-1]^n f_{\gamma_e^{x_n}}(y) dy}{(\alpha_n\delta_n(\epsilon)\rho_{\text{M}})^n}, \tag{22}$$

where $\tilde{b}_n = \frac{K!}{(K-n)!n!}$, and the integral in the numerator of (22) is independent of ρ_{M}. Similarly, we can approximate (16) in the high ρ_{M} regime as

$$P_{\text{sop}}^m \overset{\rho_{\text{M}}\to\infty}{\simeq} \frac{\tilde{b}_m \int_0^{\frac{1-\eta_m\alpha_n}{\eta_m\alpha_n}} \left(\frac{\eta_m(1+z)}{1-\alpha_n\eta_m(1+z)}\right)^m f_{\gamma_e^{x_m}}(z) dz}{(\delta_m(\epsilon)\rho_{\text{M}})^m}, \tag{23}$$

where $\tilde{b}_m = \frac{K!}{(K-m)!m!}$, and the integral in the numerator of (23) is also independent of ρ_{M}.

Remark 2: By combining the definition of the secrecy diversity order with (22) and (23), a secrecy diversity order of n is achieved at D_n and a secrecy diversity order of m is achieved at D_m. This means that full secrecy diversity orders are obtained at D_n and D_m by the proposed transmission outage constrained scheme, showing its advantage in guaranteeing security.

Remark 3: Applying the same rationale with (22) and (23), it is easy to show that the secrecy diversity order of the selected

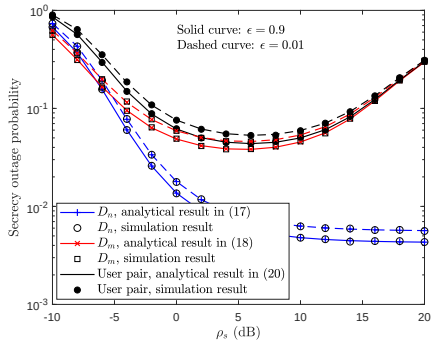

Fig. 1. Secrecy outage probability versus ρ_s with $K = 5$.

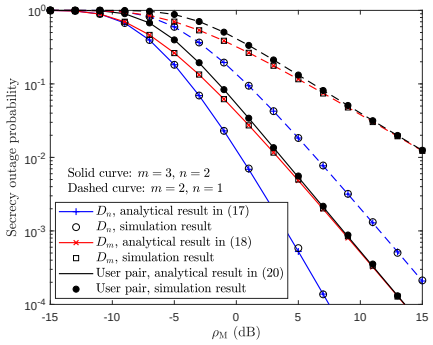

Fig. 2. Secrecy outage probability versus ρ_M with $\epsilon = 0.4$ and $K = 3$.

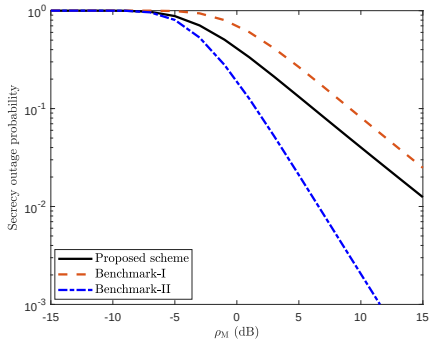

Fig. 3. Comparison of different schemes with $\epsilon = 0.4$, $m = 2$, $n = 1$, and $K = 3$.

user pair is m, which is equal to the secrecy diversity order of D_m. This observation suggests that, since the secrecy diversity order of the selected user pair is dominated by the user with the worse channel gain, it is preferable to pair the best channel gain user with the second best channel gain user to achieve a better secrecy outage performance.

IV. Simulation Results

For illustration, we assume that S is located at the origin $(0, 0)$, E is located at $(0, 10)$, and K users are uniformly deployed inside a circle centered at $(0, 5)$ and with radius equal to 3. Therefore, the average channel gains can be obtained as $\omega_{s,k} = d_{s,k}^{-\varsigma}$, $\omega_{s,e} = d_{s,e}^{-\varsigma}$, and $\omega_{e,k} = d_{e,k}^{-\varsigma}$, where d denotes the Euclidean distance and $\varsigma = 2.7$. The other system parameters are set as: $R_b^{x_n} = R_b^{x_m} = 1$ bps/Hz, $R_s^{x_n} = R_s^{x_m} = 0.1$ bps/Hz, $\rho_e = -10$ dB, $\zeta = 0.5$, $a_n = 0.3$, $a_m = 0.7$, and $L = 20$.

Fig. 1 shows the secrecy outage probability of the proposed scheme versus ρ_s. It can be observed that the analytical results perfectly match the simulated ones, thus validating the accuracy of the theoretical analysis. It can be observed from the figure, the secrecy outage probability for D_n first decreases with ρ_s in the low to medium ρ_s regime, then it reaches a floor if ρ_s further increases. In sharp contrast to D_m, the secrecy outage probability for D_m first decreases and then increases with an increase in ρ_s. This can be intuitively explained as follows. Both the main channel capacity of D_m and the wiretap channel capacity of E become interference-dominated in the high ρ_s regime, and in this case, increasing ρ_s will cause more channel capacity loss to D_m than that to E, which degrades the secrecy rate of D_m. The secrecy outage probability of the user pair exhibits a similar trend with D_m, since the overall secrecy outage probability is dominated by the worst case. Moreover, it can be also observed from the figure that the secrecy outage probability for both users becomes higher when the transmission outage constraint ϵ is more stringent, therefore confirming Remark 1.

Fig. 2 shows the secrecy outage probability of the proposed scheme versus ρ_M. As seen from this figure, full secrecy diversity orders are achieved at both users, which is consistent with our findings in Remark 2 and demonstrates the effectiveness of the proposed transmission outage constraint scheme. Interestingly, the secrecy diversity order of the user pair remains the same as that of D_m, and the secrecy outage probability of the user pair converges to that of D_m in the medium to high ρ_M regime. This observation is also verified by the insights in Remark 3.

Fig. 3 compares the secrecy outage probability of the proposed scheme with two benchmark schemes. Benchmark-I is an orthogonal multiple access scheme with a full-duplex eavesdropper, while Benchmark-II is a NOMA scheme with a half-duplex eavesdropper. As expected, the proposed scheme achieves a lower secrecy outage probability than Benchmark-I, due to the increased spectral efficiency. Compared with Benchmark-II, the full-duplex eavesdropping significantly degrades the transmission secrecy.

V. Conclusion

This letter studied the design of secure NOMA against full-duplex proactive eavesdropping and proposed a novel transmission outage constrained scheme for both reliability and security guarantees. The secrecy outage probability and the secrecy diversity order of the proposed scheme were analyzed to evaluate the secrecy performance and gain valuable design insights. The proposed solution can be used to prevent confidential information leakage against the proactive eavesdropper in practical heterogeneous or tactical networks.

References

[1] Z. Wei, D. W. K. Ng, J. Yuan, *et al.*, "Optimal resource allocation for power-efficient MC-NOMA with imperfect channel state information," *IEEE Trans. Commun.*, vol. 65, no. 9, pp. 3944–3961, Sep. 2017.

[2] S. Yan, N. Yang, I. Land, R. Malaney, and J. Yuan, "Three artificial-noise-aided secure transmission schemes in wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 67, no. 4, pp. 3669–3673, Apr. 2018.

[3] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.

[4] 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.

[5] L. Lv, Z. Ding, Q. Ni, and J. Chen, "Secure MISO-NOMA transmission with artificial noise," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6700–6705, Jul. 2018.

[6] Y. Feng, S. Yan, Z. Yang, N. Yang, and J. Yuan, "Beamforming design and power allocation for secure transmission with NOMA," online available: https://arxiv.org/abs/1806.09421, 2018.

[7] Y. Sun, D. W. K. Ng, J. Zhu, and R. Schober, "Robust and secure resource allocation for full-duplex MISO multicarrier NOMA systems," *IEEE Trans. Commun.*, vol. 66, no. 9, pp. 4119–4137, Sep. 2018.

[8] B. Zheng, M. Wen, C.-X. Wang, *et al.*, "Secure NOMA based two-way relay networks using artificial noise and full duplex," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1426–1440, Jul. 2018.

[9] H. Zhang, N. Yang, K. Long, *et al.*, "Secure communications in NOMA systems: Subcarrier assignment and power allocation," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1441–1452, Jul. 2018.

[10] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 574–583, Mar. 2015.

[11] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Dual antenna selection in secure cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 7993–8002, Oct. 2016.

[12] G. Chen, J. P. Coon, *et al.*, "Secrecy outage analysis for downlink transmissions in the presence of randomly located eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 5, pp. 1195–1206, May 2017.