Secure Transmission to the Strong User in Non-Orthogonal Multiple Access

Youhong Feng\textsuperscript{\textcopyright}, Student Member, IEEE, Shihao Yan\textsuperscript{\textcircled{L}}, Member, IEEE, and Zhen Yang\textsuperscript{\textcircled{C}}

Abstract—With non-orthogonal multiple access (NOMA) in a passive eavesdropping scenario, we tackle the maximization of the secrecy rate for the strong user subject to a maximum allowable secrecy outage probability while guaranteeing a constraint on the transmission rate to the weak user. For the first time, the dependence between the eavesdropper’s ability to conduct successive interference cancellation and her channel quality is considered. We determine the exact optimal power allocation and redundancy rate, based on which the cost of security in terms of the reduction in the strong user’s secrecy rate is examined, and the benefits of NOMA for secure transmissions are revealed.

Index Terms—Non-orthogonal multiple access, physical layer security, power allocation, secrecy outage probability.

I. INTRODUCTION

NON-ORTHOGONAL multiple access (NOMA), which can significantly boost spectral efficiency, is envisaged as a potentially promising technique for the fifth-generation (5G) and beyond wireless communication networks [1], [2]. Different from the conventional orthogonal multiple access (OMA), NOMA efficiently exploits power domain multiplexing at a transmitter and successive interference cancellation (SIC) at a receiver to serve multiple users in the same resource block (e.g., time/frequency/code domain). Specifically, these users are normally divided into two types [3], [4], i.e., the strong users and the weak users, where the strong users require a high date rate, e.g., to support live sports streaming, while the weak users may only require a predetermined low data rate, e.g., to support text messaging. Meanwhile, physical layer security (PLS), as a complementary and alternative technique to the traditional cryptographic methods, can defend against eavesdroppers (Eves) by exploiting the property (e.g., randomness) of the wireless medium [5]–[7]. Naturally, PLS can be applied to NOMA communication networks in order to achieve the information-theoretic security [8]–[13].

In a NOMA system, the transmitted signals to a weak user should be decoded by the strong user in order to enable SIC at the strong user. This leads to the fact that the achieved security of the weak user is conditioned on the assumption that the strong user will not release any information transmitted to the weak user. If there is no trust between the weak and strong users, the information-theoretic security of weak user’s information is hard to be guaranteed in NOMA systems. Against this background, in this work we propose a new framework to examine PLS in a NOMA communication system by considering a passive eavesdropping scenario without Eve’s instantaneous CSI. This framework aims to maximize the secrecy rate for the strong user subject to a maximum allowable secrecy outage probability (SOP), while guaranteeing a specific requirement on the transmission rate to the weak user. One specific applicable scenario of our new framework is where the strong user desires a high data rate with security requirement to support specific services (e.g., a tele-medical treatment), while the weak user only needs a non-secure broadcast service (e.g., a public weather alert).

We note that in the literature there are several related works that studied secure communications in NOMA systems (e.g., [8]–[19]). Zhang et al. [8], Jiang et al. [9], Tian et al. [10], Lv et al. [13], Zhou et al. [17], Sun et al. [18], and Zhang et al. [19] examined PLS of NOMA networks with perfect or imperfect knowledge of Eves’ channel state information (CSI). Liu et al. [11], He et al. [12], and Chen et al. [14] assumed that Eve can cancel the inter-user interference, which was justified by that this assumption arises from the worst-case scenario (where Eve’s decoding ability is extremely strong). However, it is well known that this assumption overestimates the decoding ability of Eve. On the contrary, Yu et al. [15] assumed that Eve does not conduct any SIC, which underestimated the decoding ability of Eve. Furthermore, Nandan et al. [16] studied PLS for a multiple-input multiple-out (MIMO)-NOMA-based cognitive radio network with the primary user as Eve and did not consider any external Eve. In this work, we consider a practical scenario where the transmitter does not know Eve’s instantaneous CSI. In addition, in order to guarantee the fairness between the legitimate users and Eve, for the first time, we consider that Eve’s decoding ability depends on her channel conditions from an signal processing point of view.

Adopting this new framework, we determine the exactly and asymptotically optimal power allocation between the strong and weak users and the optimal redundancy rate for the strong user, based on which the cost of the considered security for the strong user is explicitly examined in terms of the reduction in the secrecy rate to the strong user. Our analysis indicates that the asymptotic results accurately approach to the corresponding exact results in the high main-to-eavesdropper ratio (MER) regime.

II. SYSTEM MODEL

A. Considered Scenario and Adopted Assumptions

We consider a NOMA communication scenario, where a transmitter is serving two legitimate receivers in the presence of an Eve. Following [8], [12], [14], and [15], we assume...
that each transceiver is equipped with a single antenna in this work. We note that multi-antenna techniques can be applied to NOMA in order to significantly improve the achievable secrecy rates (e.g., [9], [10], [13], [16]). The main contribution of this work is to, for the first time, determine the dependence between Eve’s ability to conduct successive interference cancellation and her channel quality, and then solve the resultant optimization problem. As such, we will consider multi-antenna techniques in our future works on NOMA.

The channel gains from the transmitter to the legitimate receivers and Eve are denoted $h_k$, $k \in \{1, 2\}$ and $h_e$, respectively, which are the Rayleigh fading gains with independent and identically distributed (i.i.d.) entries with zero mean and variance $\delta_1^2$ and $\delta_2^2$, respectively. We assume that the CSI of all the legitimate channels is known at the transmitter, while only the statistical CSI of Eve’s channel is available. Without loss of generality, we also assume that the legitimate channel gains are sorted in ascending order [8], [12], i.e., $0 \leq |h_1|^2 \leq |h_2|^2$.

Employing the NOMA scheme, the transmitter sends two information signals $s_1$ and $s_2$ to user 1 and user 2, respectively, where the transmit power is denoted by $P$. We denote $\phi_k = \frac{P}{\delta_k^2} \leq 1$ as the fraction of the transmit power allocated to user $k$ and then the transmitted superposition signal can be expressed as $\sum_{k=1}^{2} \sqrt{\phi_k} h_k$, where $\sum_{k=1}^{2} \phi_k = 1$. In addition, we would like to clarify that one more motivation for consider security for the strong user only is that the security of the weak user is based on the assumption that the strong user does not release the weak user’s information to Eve. This is due to the fact that, in a NOMA system, the strong user can decode the weak user’s information for conducting SIC.

### B. SNRs in the NOMA System

Based on downlink NOMA scheme, user 1 decodes its own signal $s_1$ by treating $s_2$ as interference, while user 2 first decodes user 1’s information (i.e., $s_1$) and applies SIC to decode its own information $s_2$. Thus, the received signal-to-interference-plus-noise ratio (SINR) for $s_1$ at user 1 and signal-to-noise (SNR) for $s_2$ at user 2 can be expressed as

$$\gamma_1 = \frac{\phi_1 |h_1|^2}{\phi_2 |h_2|^2 + \sigma^2}$$

and

$$\gamma_2 = \frac{\phi_2 |h_2|^2}{\phi_1 |h_1|^2 + \sigma^2}$$

respectively, where $\rho_1 = \frac{P}{\delta_1^2}$ and $\rho_2 = \frac{P}{\delta_2^2}$.

Considering that $h_1$ and $h_2$ are known at the transmitter in the considered NOMA system, the codeword rates for $s_1$ and $s_2$ are chosen such that $R_1 = C_1$ and $R_2 = C_2$, respectively, where $C_1 = \log_2 (1 + \gamma_1)$ and $C_2 = \log_2 (1 + \gamma_2)$. As such, Eve can decode $s_1$ and then cancel the interference caused by $s_1$ only when Eve’s channel quality is no lower than that of user 1. Therefore, there are two cases with regard to Eve’s ability to decode $s_2$. When $\rho_e |h_e|^2 < \rho_1 |h_1|^2$ (i.e., when Eve’s channel quality is lower than that of user 1), Eve cannot decode $s_1$ and thus decodes $s_2$ directly by treating $s_1$ as interference. In this case, the SINR of $s_2$ at Eve is given by

$$\gamma_2 = \frac{\phi_2 |h_2|^2}{\phi_1 |h_1|^2 + \rho_e |h_e|^2}$$

with $\rho_e = \frac{P}{\delta_e^2}$. When $\rho_e |h_e|^2 \geq \rho_1 |h_1|^2$, Eve can first decode $s_1$ in order to cancel the interference caused by $s_1$ with SIC and then decode $s_2$. Then, in this case the SINR of $s_2$ at Eve is given by

$$\gamma_2 = \frac{\phi_2 |h_2|^2}{\phi_1 |h_1|^2 + \rho_1 |h_1|^2}$$

Considering Rayleigh fading, the cumulative distribution functions (cdfs) of $\gamma_1$ and $\gamma_2$ are obtained as

$$F_{\gamma_1}(\gamma) = \begin{cases} 1 - e^{-\frac{\gamma}{\phi_1}}, & \gamma \leq \frac{\phi_2}{\phi_1} \\ 1, & \gamma > \frac{\phi_2}{\phi_1} \end{cases}$$

$$F_{\gamma_2}(\gamma) = 1 - e^{-\frac{\gamma}{\phi_2}}$$

### III. PHYSICAL LAYER SECURITY OF THE STRONG USER

#### A. Transmission Scheme and the Optimization Problem

In order to achieve PLS for user 2, in addition to $R_2$, a redundancy rate $R_E$ for transmitting $s_2$ should be determined [20]. Then, the instantaneous secrecy rate for user 2 as a function of $\phi_2$ and $R_E$ is given by

$$R_2^*(\phi_2, R_E) = [C_2 - R_E]^+] + [\log_2 (1 + \phi_2 \rho_2) - R_E]^+$$

(3)

where $\rho_2 = \rho_2 |h_2|^2$ and $[x]^+ = \max (x, 0)$. However, a secrecy outage occurs when $C_E > R_E$, where $C_E = \log_2 (1 + \gamma_E)$. $\gamma_E \in \{\gamma_1, \gamma_2\}$ is the unknown channel capacity of Eve. We derive the SOP in the following lemma.

**Lemma 1:** For our considered NOMA communication scenario, the SOP of $s_2$ can be given by

$$P_{out}(R_E, \phi_2) = (1 - e^{-\frac{\gamma_1^2}{\phi_1}}) P_{out,1}(R_E, \phi_2) + e^{-\frac{\gamma_1^2}{\phi_1}} e^{-\frac{\gamma_2^2}{\phi_2}} P_{out,2}(R_E, \phi_2),$$

(4)

where $P_{out,1}(R_E, \phi_2) = e^{-\frac{\gamma_1^2}{\phi_1}} e^{-\frac{\gamma_2^2}{\phi_2}}$ when $R_E < 1 - \frac{\gamma_1^2}{\phi_1}, P_{out,1}(R_E, \phi_2) = 0$ when $R_E \geq 1 - \frac{\gamma_1^2}{\phi_1}$, and $P_{out,2}(R_E, \phi_2) = e^{-\frac{\gamma_2^2}{\phi_2}}$.

Proof: Based on the analysis in Section II-B, the SOP of $s_2$ can be given by

$$P_{out}(R_E, \phi_2) = Pr(\rho_e |h_e|^2 < \rho_1 |h_1|^2) P_{out,1}(R_E, \phi_2) + Pr(\rho_e |h_e|^2 \geq \rho_1 |h_1|^2) P_{out,2}(R_E, \phi_2),$$

(5)

where $P_{out,1}(R_E, \phi_2) = Pr(\gamma_1 \geq 2 R_E - 1)$ and $P_{out,2}(R_E, \phi_2) = Pr(\gamma_2 \geq 2 R_E - 1)$. Considering Rayleigh fading for $h_e$, we have

$$Pr(\rho_e |h_e|^2 < \rho_1 |h_1|^2) = 1 - e^{-\frac{\gamma_1^2}{\phi_1}}$$

and

$$Pr(\rho_e |h_e|^2 \geq \rho_1 |h_1|^2) = e^{-\frac{\gamma_1^2}{\phi_1}}.$$ Then, substituting (1) and (2) into (5), we obtain (4), which proves Lemma 1.

**Remark 1:** Following Lemma 1, we note that there is a minimum value for the SOP in order to guarantee a positive secrecy rate, since $h_e$ is unknown and the maximum value of $R_E$ is $C_2$ to ensure a positive secrecy rate as per (3). We note that this minimum value of the SOP exists in both the NOMA and OMA systems. In the NOMA system, this minimum value is $\varepsilon_n = e^{-\frac{\gamma_1^2}{\phi_1}} e^{-\frac{\gamma_2^2}{\phi_2}}$, which is achieved by substituting $R_E = C_2$ into (4) and noting $P_{out,1}(R_E, \phi_2)$ can be enforced to zero by varying $\phi_2$. In the OMA system, this minimum value is $\varepsilon_o = e^{-\frac{\gamma_2^2}{\phi_2^2}}$, since in the OMA system Eve does not have interference for decoding $s_2$. We note that $\epsilon_n < \varepsilon_o$ due to $\frac{\gamma_1^2}{\phi_1^2} < 1$, which is one explicit benefit of NOMA for secure transmission.

In this work, the focused optimization problem at the transmitter is given by

$$\mathbf{P}_1 : \max_{R_E, \phi_1, \phi_2} R_2^*(\phi_2, R_E)$$

subject to

$$C_1 \geq Q_1,$$

(7)

$$P_{out}(R_E, \phi_2) \leq \varepsilon,$$

(8)

$$\phi_1 + \phi_2 = 1.$$
Lemma 2: For any given \( \phi_1 \) or \( \phi_2 \), there is a unique \( R_E \) that maximizes \( R^*_E(\phi_2, R_E) \) subject to \( P_{out}(R_E, \phi_2) \leq \varepsilon \) and this value is \( R^*_E(\phi_2) \) that guarantees \( F_{out}(R_E, \phi_2) = \varepsilon \).

Proof: Following (3), we note that \( R^*_E(\phi_2, R_E) \) monotonically decreases with \( R_E \), while \( P_{out}(R_E, \phi_2) \) is a non-increasing function of \( R_E \) as per (4). This proves Lemma 2.

B. Exact Solution to the Optimization Problem PI

Theorem 1: The feasible condition of PI is \( P > \max(\frac{\sigma^2}{|h_1|^2}, \frac{\sigma^2}{|h_2|^2}, P_{min}) \), under which the optimal power allocation coefficients and redundancy rate are derived as

\[
\phi^*_2 = \min \left( \frac{1}{2Q^*_2 + \frac{\sigma^2}{|h_1|^2} + \frac{\sigma^2}{|h_2|^2}}, \phi_2 \right),
\]

(10)

\[
\phi^*_1 = 1 - \phi^*_2,
\]

(11)

\[
R^*_E = R^*_E(\phi^*_2),
\]

(12)

where \( \phi^*_1 \) is the value of \( \phi_2 \) that maximizes \( \log_2(1 + \phi_2 \rho_2 |h_2|^2) \). The proof follows from the maximization of the objective function subject to the constraint

\[
\phi^*_2 = \max \left( \frac{1}{2Q^*_2 + \frac{\sigma^2}{|h_1|^2} + \frac{\sigma^2}{|h_2|^2}}, \phi_2 \right),
\]

(13)

\[
\phi^*_1 = 1 - \phi^*_2,
\]

(14)

\[
R^*_E = \log_2 \left( 1 + \frac{\phi^*_2 P \ln(\frac{1}{\varepsilon})}{\phi^*_2 + \phi_1 P \ln(\frac{1}{\varepsilon})} \right),
\]

(15)

\[
\phi^*_2 = \min \left( \frac{1}{2Q^*_2 + \frac{\sigma^2}{|h_1|^2} + \frac{\sigma^2}{|h_2|^2}}, \phi_2 \right),
\]

(16)

Proof: Following (4), we have \( \lim_{\rho_1/\rho_2 \to \infty} e^{\frac{-\rho_1 |h_1|^2}{\rho_2 |h_2|^2}} = 0 \). As such, we conclude that the asymptotic SOP of \( s_2 \) is equal to \( F_{out}(R_E, \phi_2) \) when \( \frac{\rho_1}{\rho_2} \to \infty \). This completes the proof.

Corollary 1: For \( \rho_1/\rho_2 \to \infty \) and \( \rho_2/\rho_e \to \infty \) with \( \varepsilon > 0 \), \( P > \frac{\rho_1 |h_1|^2}{|h_2|^2} + \frac{\sigma^2}{|h_2|^2} \) is the feasible condition of PI, under which the optimal power allocation coefficients and redundancy rate are derived as

\[
\phi^*_2 = \min \left( \frac{1}{2Q^*_2 + \frac{\sigma^2}{|h_1|^2} + \frac{\sigma^2}{|h_2|^2}}, \phi_2 \right),
\]

(17)

\[
\phi^*_1 = 1 - \phi^*_2,
\]

(18)

\[
R^*_E = \log_2 \left( 1 + \frac{\phi^*_2 P \ln(\frac{1}{\varepsilon})}{\phi^*_2 + \phi_1 P \ln(\frac{1}{\varepsilon})} \right),
\]

(19)

Proof: Similar to the proof of Theorem 1, in order to guarantee \( C_1 \geq Q_1 \) we have \( P > \frac{\rho_1 |h_1|^2}{|h_2|^2} + \frac{\sigma^2}{|h_2|^2} \). As per Lemma 1, we have \( P_{out}(R_E, \phi_2) = \varepsilon \) in the solution to PI, which leads to \( R_E = \log_2 \left( 1 + \frac{\phi^*_2 P \ln(\frac{1}{\varepsilon})}{\phi^*_2 + \phi_1 P \ln(\frac{1}{\varepsilon})} \right) \). Substituting this value of \( R_E \) into (3), we have \( R^*_E(\phi_2) = \log_2(1 + \phi_2 \rho_2 |h_2|^2) - \log_2(1 + \phi_1 \rho_2 |h_2|^2) \). In order to guarantee \( R^*_E(\phi_2) > 0 \), we have to ensure \( \phi_2 \rho_2 |h_2|^2 > \frac{\min(\phi_1, \phi_2) \rho_e \ln(x)}{1 + (1 - \phi_2) \rho_e \ln(x)} \), which at least requires

\[
\rho_2 |h_2|^2 > \frac{\rho_e \ln(\frac{1}{\varepsilon})}{1 + \rho_e \ln(\frac{1}{\varepsilon})},
\]

(20)

since \( \frac{\min(\phi_1, \phi_2) \rho_e \ln(x)}{1 + (1 - \phi_2) \rho_e \ln(x)} \) is minimized when \( \phi_2 \to 0 \). We note that the constraint of (17) must be satisfied due to \( \rho_2/\rho_e \to \infty \). As such, the feasible condition of PI is \( P > \frac{\rho_1 |h_1|^2}{|h_2|^2} + \frac{\sigma^2}{|h_2|^2} \). Under this feasible condition, the first and second derivatives of \( R^*_E(\phi_2) \) with respect to \( \phi_2 \) are derived as

\[
\frac{\partial R^*_E(\phi_2)}{\partial \phi_2} = \frac{1}{\ln^2(1 + \phi_2 \rho_2 |h_2|^2)} \left( \frac{\rho_2 |h_2|^2}{1 + \phi_2 \rho_2 |h_2|^2} - \frac{\rho_e \ln(\frac{1}{\varepsilon})}{1 + (1 - \phi_2) \rho_e \ln(\frac{1}{\varepsilon})} \right),
\]

(21)

\[
\frac{\partial^2 R^*_E(\phi_2)}{\partial \phi_2^2} = \frac{1}{\ln^2(1 + \phi_2 \rho_2 |h_2|^2)} \left( \frac{\rho_2 |h_2|^4}{1 + \phi_2 \rho_2 |h_2|^2} - \frac{(\rho_e \ln(\frac{1}{\varepsilon}))^2}{1 + (1 - \phi_2) \rho_e \ln(\frac{1}{\varepsilon})} \right).
\]

(22)

Following (19), we have \( \partial^2 R^*_E(\phi_2)/\partial \phi_2^2 < 0 \) by noting \( \rho_2/\rho_e \to \infty \), which indicates that \( R^*_E(\phi_2) \) is a concave function of \( \phi_2 \). As such, per (18) by setting \( \partial^2 R^*_E(\phi_2)/\partial \phi_2^2 = 0 \) we achieve \( \phi_2 = \frac{\rho_2 |h_2|^2}{\rho_e \ln(\frac{1}{\varepsilon})} \). By setting \( C_1 = Q_1 \) in (7), we have \( \phi_2 = \frac{\rho_1 |h_1|^2 - 2Q^*_2 - \rho_2 |h_2|^2}{\rho_e \ln(\frac{1}{\varepsilon})} \). Due to \( \phi_1 + \phi_2 = 1 \), \( C_1 \) is a monotonically decreasing function of \( \phi_2 \) in order to guarantee \( C_1 \geq Q_1 \). We can obtain the desired result in (14), based on which (15) and (16) are obtained.

Remark 2: We first note that Corollary 1 cannot be directly achieved from Theorem 1, since \( \phi^*_2 \) can only be numerically obtained in Theorem 1. This \( \phi^*_2 \) is achieved in a closed-form expression in Corollary 1, since SOP is simplified in Lemma 3. Based on (14) in Corollary 1, we note that as \( P \to \infty \) we have \( \phi^*_2 \to \frac{1}{2Q^*_2} \) and \( \phi^*_1 \to \frac{1}{2Q^*_2} \). This indicates that in the limit of \( P \to \infty \) we have \( \phi^*_2 = \frac{1}{2Q^*_2} \) when \( Q_1 > 1 \) and \( \phi^*_2 = \frac{1}{2Q^*_2} \) when \( Q_1 \leq 1 \). As per (16) in Corollary 1, we note that as
cost of the considered PLS that less power will be allocated (c).

Fig. 1. (a) Maximum secrecy rate versus MER, (b) $P^*$ versus $P$, and (d) Maximum secrecy rate versus $Q_1$, where $Q_1 = 0.4$ for (a) and (c), $P = 4$dB for (d), $\sigma_1^2 = \sigma_2^2 = -5$dB and $\sigma_3^2 = 2$dB for (b)-(d), $|h_1|^2 = 0.5$, $|h_2|^2 = 4$ for (a)-(d).

$P \to \infty$ we have $R_{E}^* \to \log_2\left(1 + \frac{\phi_2^*}{\epsilon}\right)$. Therefore, we can conclude that in the limit of $P \to \infty$ equal power allocation is optimal and $R_{E}^* = \log_2(2)$ when $Q_1 \leq 1$.

IV. Numerical Results

In Fig 1 (a), we observe that $R_{E}^*$ for $\epsilon < 1$ is lower than that for $\epsilon = 1$ (without considering security), where the performance reduction is the cost of considered PLS. In Fig 1 (b), we observe that $\phi_2^*$ for either $\epsilon = 0.01$ or $\epsilon = 0.001$ is lower than that for $\epsilon = 1$, which shows one specific cost of the considered PLS that less power will be allocated to user 2. As expected from Remark 3, $\phi_2^*$ for either $\epsilon = 0.01$ or $0.001$ approaches $1/2$ as $P \to \infty$ when $Q_1$ is small, which demonstrates the optimality of the equal power allocation in the limit of $P \to \infty$ with a small $Q_1$. In Fig 1 (c), we observe that $R_{E}^*$ increases with $P$ and $R_{E}^* \to 1$ as $P \to \infty$, which can be explained by our theorems and Remark 3. In Fig 1 (d), we plot the maximum secrecy rate achieved by the NOMA and OMA schemes versus $Q_1$. Here, the OMA scheme refers to the conventional TDMA scheme, in which half of the transmission time is allocated to user 1 and the other half is allocated to user 2. In this figure, we first observe that the maximum secrecy rate $R_{E}^*$ achieved by the NOMA scheme is significantly higher than that achieved by the OMA scheme under the specific system settings. In addition, we observe that the NOMA scheme can still achieve a positive secrecy rate when the OMA scheme cannot (i.e., when $0.8 \leq Q_1 \leq 1$).

V. Conclusion

In this work, we determined the optimal power allocation and redundancy rate in order to maximize the secrecy rate for the strong user subject to a maximum allowable SOP, while guaranteeing the non-secure transmission rate requirement to the weak user. Our analysis explicitly revealed the cost of the considered PLS in terms of the reduction in the secrecy rate to the strong user.

REFERENCES