Secure Transmission to the Strong User with Optimal Power Allocation in NOMA

Youhong Feng, Student Member, IEEE, Shihao Yan, Member, IEEE, and Zhen Yang

Abstract—With non-orthogonal multiple access (NOMA), 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 optimal power allocation and the 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 explicitly revealed.

Index Terms—Non-orthogonal multiple access, physical layer security, power allocation, redundancy rate.

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 data 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 ever-lasting and information-theoretic security [8]–[12]. For example, the authors of [9]–[10] examined PLS of the wireless NOMA network with perfect knowledge of Eves’ channel state information (CSI), which indicated a significant secrecy performance improvement achieved by NOMA relative to OMA. In addition, the authors of [11], [12] considered a practical scenario where the transmitter does not know Eve’s instantaneous CSI, where PLS of both the strong and weak users were studied.

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 trustiness 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 a tele-medical treatment, while the weak user only needs a non-secure broadcast service.

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. In addition, our analysis reveals that the cost of the considered security decreases and the optimal power allocation becomes less sensitive to the maximum allowable SOP as the transmission rate requirement to the weak user increases. Furthermore, our analysis demonstrates that the equal power allocation is asymptotically optimal and the redundancy rate approaches one as the transmit power increases to infinity.

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. We assume that each of the transceivers is equipped with a single antenna. 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 $\delta_k^2$ and $\delta_e^2$ respectively. We assume that 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 $\delta_1^2 \leq \delta_2^2$, i.e., $0 < |h_1|^2 \leq |h_2|^2$.

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 $\phi_k$...
(0 < \phi_k \leq 1) as the fraction of the transmit power allocated to user \(k\) and then the transmitted superposition signal can be expressed as \(\sum_{k=1}^{2} \sqrt{\phi_k} s_k\), where \(\sum_{k=1}^{2} \phi_k = 1\). In this work, we consider PLS only for the transmission to user 2 (i.e., the strong user with a higher channel gain). This is due to the fact that in a NOMA system user 2 always has to first decode the signal transmitted to user 1 (i.e., the weak user with a lower channel gain) in order to conduct SIC, which leads to the fact that the information-theoretic PLS of the signal transmitted to user 1 cannot be achieved (i.e., user 2 may release the information transmitted to user 1).

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

\[
\gamma_1 = \frac{\phi_1 |h_1|^2}{\sigma_1^2 + \sigma_2^2 |h_2|^2}, \quad \gamma_2 = \frac{\phi_2 |h_2|^2}{\sigma_1^2 |h_1|^2 + \sigma_2^2}
\]

respectively, where \(\rho_1 = \frac{\sigma_1^2}{\sigma_2^2}\) and \(\rho_2 = \frac{\sigma_2^2}{\sigma_1^2}\).

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 \(\rho_2 |h_2|^2 < \rho_1 |h_1|^2\) (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

\[
\gamma_{c1} = \frac{\phi_2 |h_2|^2}{\phi_1 |h_1|^2 + \sigma_2^2} = \frac{\phi_2 |h_2|^2}{\rho_2 |h_2|^2 + \sigma_2^2}
\]

with \(\rho_c = \frac{\sigma_1^2}{\sigma_2^2}\). When \(\rho_2 |h_2|^2 \geq \rho_1 |h_1|^2\), Eve can first decode \(s_1\) to in order to cancel the interference caused by \(s_1\) with SIC and then decode \(s_2\). Then, in this case the SNR of \(s_2\) at Eve is given by \(\gamma_{c2} = \frac{\phi_2 |h_2|^2}{\rho_2 |h_2|^2 + \sigma_2^2}\). Considering Rayleigh fading, the cumulative distribution functions (cdfs) of \(\gamma_{c1}\) and \(\gamma_{c2}\) are obtained as

\[
F_{\gamma_{c1}}(\gamma) = \begin{cases} 1 - e^{-\frac{\gamma}{\rho_c(\gamma_1 + \sigma_1^2)}}, & \gamma \leq \frac{\phi_2}{\phi_1} \\ 1, & \gamma > \frac{\phi_2}{\phi_1} \end{cases}
\]

\[
F_{\gamma_{c2}}(\gamma) = 1 - e^{-\frac{\gamma}{\rho_c \gamma_2}}. \tag{2}
\]

III. PHYSICAL LAYER SECURITY OF THE STRONG USER

In this section, we aim to maximize the secrecy rate subjective to a maximum allowable SOP for user 2 while guaranteeing a requirement on the transmission rate to user 1. The exactly and asymptotically optimal power allocation coefficients \(\phi_k\) and the redundancy rate are determined, based on which the associated maximum secrecy rate is determined.

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. Then, the instantaneous secrecy rate for user 2 as a function of \(\phi_2\) and \(R_E\) is given by

\[
R^s_2(\phi_2, R_E) = [C_2 - R_E]^+ = [\log_2(1 + \phi_2 \rho_2) - R_E]^+ \tag{3}
\]

where \(\rho_2 = \rho_2 |h_2|^2\) and \([x]^+ = \max(x, 0)\). However, a secrecy outage occurs when \(C_E > R_E\), where \(C_E = \log_2(1 + \gamma_E)\). \(\gamma_E \in \{\gamma_{c1}, \gamma_{c2}\}\) 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 \(s_2\) is given by

\[
P_{\text{out}}(R_E, \phi_2) = \begin{cases} (1 - e^{-\frac{\rho_2 |h_2|^2}{\sigma_2^2}}) P_{\text{out},1}(R_E, \phi_2) + e^{-\frac{\rho_2 |h_2|^2}{\sigma_2^2}} P_{\text{out},2}(R_E, \phi_2), & \text{when } 2R_E - 1 < \frac{\rho_2 |h_2|^2}{\sigma_2^2}, \end{cases}
\]

\[
P_{\text{out},1}(R_E, \phi_2) = e^{-\frac{2R_E - 1}{\sigma_2^2(\rho_2 - 1)(2R_E - 1)}} \text{ when } 2R_E - 1 < \frac{\rho_2 |h_2|^2}{\sigma_2^2}, \quad \text{and} \quad P_{\text{out},2}(R_E, \phi_2) = e^{-\frac{2R_E - 1}{\sigma_2^2}}.
\]

**Proof:** Based on the analysis in Section II-B, the SOP of \(s_2\) can be given by

\[
P_{\text{out}}(R_E, \phi_2) = Pr(\rho_c |h_c|^2 < \rho_1 |h_1|^2) P_{\text{out},1}(R_E, \phi_2) + Pr(\rho_c |h_c|^2 \geq \rho_1 |h_1|^2) P_{\text{out},2}(R_E, \phi_2),
\]

where

\[
P_{\text{out},1}(R_E, \phi_2) = Pr(\gamma_{c1} \geq 2R_E - 1) \quad \text{and} \quad P_{\text{out},2}(R_E, \phi_2) = Pr(\gamma_{c2} \geq 2R_E - 1).
\]

Considering Rayleigh fading for \(h_c\), we have \(Pr(\rho_c |h_c|^2 < \rho_1 |h_1|^2) = 1 - e^{-\frac{\rho_1 |h_1|^2}{\sigma_2^2}}\) and \(Pr(\rho_c |h_c|^2 > \rho_1 |h_1|^2) = e^{-\frac{\rho_1 |h_1|^2}{\sigma_2^2}}\). 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 \(h_c\) is unknown and the maximum value of \(R_E\) is \(C_2\) to ensure a positive secrecy rate 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 \(\epsilon_n = e^{-\frac{\rho_1 |h_1|^2}{\sigma_2^2}} e^{-\frac{\rho_1 |h_1|^2}{\sigma_2^2}}\), which is achieved by substituting \(R_E = C_2\) into (4) and noting \(P_{\text{out},1}(R_E, \phi_2)\) can be enforced to zero by varying \(\phi_2\). In the OMA system, this minimum value is \(\epsilon_n = e^{-\frac{\rho_1 |h_1|^2}{\sigma_2^2}}\), since in the OMA system Eve does not have interference for decoding \(s_2\). We note that \(\epsilon_n < \epsilon_0\) due to \(e^{-\frac{\rho_1 |h_1|^2}{\sigma_2^2}} < 1\), which is one explicit benefit of NOMA for secure transmission. Specifically, for \(\epsilon_0 \leq \epsilon < \epsilon_n\), where \(\epsilon\) is the maximum allowable SOP for user 2 in the considered system, NOMA can achieve a positive secrecy rate, while OMA cannot. In this work we assume \(\epsilon_n \leq \epsilon\) in order to guarantee the feasibility of the considered optimization problem and in the comparison between NOMA and OMA we consider \(\epsilon_0 \leq \epsilon\).

In this work, we optimize the power allocation coefficients (i.e., \(\phi_1\) and \(\phi_2\)) and the redundancy rate \(R_E\) to maximize the instantaneous secrecy rate \(R^s_2(\phi_2, R_E)\) subject to the maximum allowable SOP \(\epsilon\) for user 2 and a minimum data rate \(Q_1\) for user 1. Then, the optimization problem at the transmitter is given by

\[
\textbf{P1: } \max_{R_E, \phi_1, \phi_2} R^s_2(\phi_2, R_E) \tag{6}
\]

s.t.

\[
C_1 \geq Q_1, \tag{7}
\]

\[
P_{\text{out}}(R_E, \phi_2) \leq \epsilon, \tag{8}
\]

\[
\phi_1 + \phi_2 = 1. \tag{9}
\]
Lemma 2: For any given $\phi_1$ or $\phi_2$, there is a unique $R_E$ that maximizes $R_2^*(\phi_2, R_E)$ subject to $P_{out}(R_E, \phi_2) \leq \varepsilon$ and this value is $R_E^k(\phi_2)$ that guarantees $P_{out}(R_E, \phi_2) = \varepsilon$.

Proof: Following (3), we note that $R_2^2(\phi_2, R_E)$ 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 P1

Theorem 1: The feasible condition of P1 is $P > \max(\frac{2\phi_1}{|h_1|^2}, \sigma_1^2, P_{\text{min}})$, under which the optimal power allocation coefficients and redundancy rate are derived as

$$\phi_2^* = \min \left( \frac{1}{2Q_1} + \frac{\sigma_1^2}{|h_1|^2|2Q_1|}, \frac{\sigma_1^2}{|h_1|^2} \right), \quad \phi_1^* = 1 - \phi_2^*, \quad R_E^* = R_E^k(\phi_2^*),$$

where $\phi_1^*$ is the value of $\phi_1$ that maximizes $\log_2(1 + \phi_2 P_{\text{min}} |h_2|^2) - R_E^k(\phi_2^*)$.

Proof: Following the expression of $\gamma_1$, $C_1$ is maximized when $\phi_1 \to 1$ and $\phi_2 \to 0$. In order to guarantee the constraint (7), we have to ensure $P > \frac{2\phi_1}{|h_1|^2}$, which leads to $P \geq \frac{2\phi_1}{|h_1|^2}$. As per Lemma 2, we have $P_{out}(R_E, \phi_2) = \varepsilon$ in the solution to P1, which leads to $R_E = R_E^k(\phi_2^*)$. Substituting this value of $R_E$ into (3), we have $R_2^2(\phi_2) = \log_2(1 + \phi_2 P_{\text{min}} |h_2|^2) - R_E^k(\phi_2^*)$. In order to guarantee $R_2^2(\phi_2) > 0$, we have to ensure $\phi_2 P_{\text{min}} |h_2|^2 > 2R_E^k(\phi_2^*) - 1$, which requires that $P_{\text{min}}$ satisfies $P_{\text{min}} |h_2|^2 > 2Q_1(\phi_2^*) - 1$ with the constraint of $\phi_1 + \phi_2 = 1$. Under this feasible condition, the optimal $\phi_2$ that maximizes $R_2^2(\phi_2)$ without the constraint $C_1 \geq Q_1$ can be obtained through $\phi_2^* = \max \left( \frac{1}{2Q_1} + \frac{\sigma_1^2}{|h_1|^2|2Q_1|}, \frac{\sigma_1^2}{|h_1|^2} \right)$. Due to $\phi_1 + \phi_2 = 1$, $C_1$ is a monotonically decreasing function of $\phi_2$ and thus in order to guarantee $C_1 \geq Q_1$ we have the desired result in (10), based on which (11) and (12) are achieved as per $\phi_1 + \phi_2 = 1$ and Lemma 2, respectively.

Remark 2: Comparing $\varepsilon_n \leq \varepsilon < 1$ in Theorem 1 with $\varepsilon = 1$ (i.e., the optimization problem in [8] without security constraint in (3)), we note that the considered PLS is not only at the cost of a positive redundancy rate $R_E^*$, but also a possible reduction in $\phi_2$, since this $\phi_2^*$ is no larger than that in case without considering security. Meanwhile, as per (10) in Theorem 1, we note that $\phi_2^*$ decreases with $Q_1$. This indicates that, as $Q_1$ increases, the power allocation will be more likely determined by $C_1 \geq Q_1$ and not sensitive to the required secrecy levels (i.e., the values of $\varepsilon$). We also note that when $\phi_2^* = \phi_2^*$ the cost of PLS in terms of $R_E^*$ decreases with $Q_1$. Intuitively, this is due to the fact that the power allocated to user 1 also causes interference at Eve.

C. Asymptotic Solution to the Optimization Problem P1

In order to provide useful insights on the secrecy performance of our considered communication system, in this subsection we focus on the secrecy rate $R_2^2(\phi_2, R_E)$ with a high MER (i.e., $\rho_1/\rho_c = \sigma_c^2/\sigma_1^2 \to \infty$) [6].

Lemma 3: With $\rho_1/\rho_c \to \infty$, the asymptotic SOP of $s_2$ is derived as

$$P_{\text{sout}}(R_E, \phi_2) = \begin{cases} \frac{2R_E - 1}{\rho_2}, & 2R_E - 1 < \frac{\phi_2}{\phi_1} \\ 0, & \text{otherwise} \end{cases}$$

Proof: Following (4), we have $\lim_{\rho_1/\rho_c \to \infty} e^{-\frac{\phi_2}{\rho}} |h_2|^2 = 0$. As such, we conclude that the asymptotic SOP of $s_2$ is equal to $P_{\text{sout},1}(R_E, \phi_2)$ when $\phi_2 \to \infty$. This completes the proof.

Theorem 2: For $\rho_1/\rho_c \to \infty$ with $\varepsilon > 0$, $P > \max(\frac{2\phi_1}{|h_1|^2}, \sigma_1^2, P_{\text{min}})$ is the feasible condition of P1, under which the optimal power allocation coefficients and redundancy rate are derived as

$$\phi_2^* = \min \left( \frac{1}{2Q_1} + \frac{\sigma_1^2}{|h_1|^2|2Q_1|}, \frac{\sigma_1^2}{|h_1|^2} \right), \quad \phi_1^* = 1 - \phi_2^*, \quad R_E^* = \log_2 \left( 1 + \frac{\phi_2^* P_{\text{min}} |h_2|^2}{\sigma_1^2 + \phi_2^* P_{\text{min}} |h_2|^2} \right).$$

Proof: Similar to the proof of Theorem 1, in order to guarantee $C_1 \geq Q_1$ we have $P > \frac{2\phi_1}{|h_1|^2}$, as per Lemma 1, we have $P_{\text{sout}}(R_E, \phi_2) = \varepsilon$ in the solution to P1, which leads to $R_E = R_E^k(\phi_2^*)$ based on (4) for $\varepsilon > 0$. Substituting this value of $R_E$ into (3), we have $R_2^2(\phi_2) = \log_2(1 + \phi_2 P_{\text{min}} |h_2|^2) - \log_2(1 + \phi_2 P_{\text{min}} |h_2|^2)$. In order to guarantee $R_2^2(\phi_2) > 0$, we have to ensure $\phi_2 P_{\text{min}} |h_2|^2 > 1$. Due to (11) and (12), we have $P_{\text{sout}}(R_E, \phi_2) = \varepsilon$ in the solution to P1, which leads to $R_E = R_E^k(\phi_2^*)$ based on (4) for $\varepsilon > 0$. Substituting this value of $R_E$ into (3), we have $R_2^2(\phi_2) = \log_2(1 + \phi_2 P_{\text{min}} |h_2|^2) - \log_2(1 + \phi_2 P_{\text{min}} |h_2|^2)$. In order to guarantee $R_2^2(\phi_2) > 0$, we have to ensure $\phi_2 P_{\text{min}} |h_2|^2 > 1$. We also note that when $\phi_2^* = \phi_2^*$ the cost of PLS in terms of $R_E^*$ decreases with $Q_1$. Intuitively, this is due to the fact that the power allocated to user 1 also causes interference at Eve.
guarantee $C_1 \geq Q_1$. We can obtain the desired result in (14), based on which (15) and (16) are obtained.

**Remark 3:** Based on (14) in Theorem 2 we note that as $P \to \infty$ we have $\phi_2^* \to \frac{1}{2Q_1}$ and $\phi_2^* \to \frac{1}{1}$. This indicates that in the limit of $P \to \infty$ we have $\phi_2^* = \frac{1}{2Q_1}$ when $Q_1 > 1$ and $\phi_2^* = \frac{1}{2}$ when $Q_1 \leq 1$. As per (16) in Theorem 2 we note that as $P \to \infty$ we have $R_E^* \to \log_2 (1 + \frac{\phi_2^*}{\phi_1^*})$. Therefore, we can conclude that in the limit of $P \to \infty$ equal power allocation is optimal and $R_E^* = \log_2(2)$ when $Q_1 \leq 1$, and the power allocation is solely determined by the required transmission rate to user 1 while $R_E^*$ decreases with $Q_1$ when $Q_1 > 1$.

In addition, we observe that $\phi_2^*$ significantly higher than that achieved by the OMA scheme and thus it may require a higher transmit power to user 1 in downlink MIMO non-orthogonal multiple access networks. This is due to the fact that the transmission time to user 1 in the considered PLS that less power will be allocated to user 2.

In Fig. 1 (a), we observe that $\phi_2^*$ versus $P$, $\phi_2^*$ versus $P$, and (d) Maximum secrecy rate versus $Q_1$, where $Q_1 = 0.4$ for (a) and (c), $P = 4$ dB for (d), $\sigma_1^2 = \frac{\epsilon}{2} = 5$ dB and $\sigma_2^2 = 2$ dB for (b)-(d), $|h_1|^2 = 0.5$, $|h_2|^2 = 4$ for (a)-(d).

**IV. NUMERICAL RESULTS**

In Fig. 1 (a), we plot the maximum secrecy rate for user 2 achieved by our exact and asymptotic solutions to P1. In Fig. 1 (b) and Fig. 1 (c), we plot $\phi_2^*$ and $R_E^*$ versus the transmit power $P$, respectively. In Fig. 1 (a), we first observe that the asymptotic results approach to the exact results in the high MER regime, which verifies the correctness of our analysis. In Fig. 1 (a), we also observe that $\phi_2^*$ is lower when $\epsilon < 1$ is larger 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 the other half is 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 $0.8 \leq Q_1 \leq 1$).

This is due to the fact that the transmission time to user 1 in the OMA scheme is only half of that in the NOMA scheme and thus it may require a higher transmit power to user 1 in the OMA scheme.

**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. The security of the weak user was not considered, since the signal dedicated to the weak user should be decoded by the strong user for SIC in NOMA. Our analysis explicitly revealed the cost of the considered PLS in terms of the reduction in the secrecy rate to the strong user, which as shown decreases as the requirement on the transmission rate to the weak user increases.

**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] Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan, and V. K. Bhargava, “A survey on non-orthogonal multiple access for 5G networks: Research challenges and future trends,” *IEEE J. Select. Areas Commun.*, vol. 35, no. 10, pp. 2181–2195, Oct. 2017.

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

[4] Z. Ding, H. Dai, and H. V. Poor, “Relay selection for cooperative NOMA,” *IEEE Wireless Commun. Lett.*, vol. 5, no. 4, pp. 416–419, Aug. 2016.

[5] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, and T. Q. Duong, “Relay selection for security enhancement in cognitive relay networks,” *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 46–49, Feb. 2015.

[6] 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.

[7] Y. Feng, S. Yan, Z. Yang, N. Yang, and W.-P. Zhu, “TAS-based incremental hybrid decode-amplify-forward relaying for physical layer security enhancement,” *IEEE Trans. Commun.*, vol. 65, no. 9, pp. 3876–3891, Sep. 2017.

[8] 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.

[9] M. Jiang, Y. Li, Q. Zhang, Q. Li, and J. Qin, “Secure beamforming in downlink MIMO non-orthogonal multiple access networks,” *IEEE Signal Process. Lett.*, vol. 24, no. 12, pp. 1852–1855, Aug. 2017.

[10] M. Tian, Q. Zhang, S. Zhao, Q. Li, and J. Qin, “Secrecy sum rate optimization for downlink MIMO non-orthogonal multiple access systems,” *IEEE Signal Process. Lett.*, vol. 24, no. 8, pp. 1113–1117, Aug. 2017.

[11] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, “Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks,” *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1656–1671, Dec. 2017.

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

[13] S. Yan, N. Yang, Ingmar 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.