Research Article

Exploiting Opportunistic Scheduling for Physical-Layer Security in Multitwo User NOMA Networks

Kyusung Shim ¹ and Beongku An ²

¹Department of Electronics and Computer Engineering in Graduate School, Hongik University, 30016, Republic of Korea

²Department of Software and Communications Engineering, Hongik University, 30016, Republic of Korea

Correspondence should be addressed to Beongku An; beongku@hongik.ac.kr

Received 1 August 2018; Revised 17 September 2018; Accepted 2 October 2018; Published 23 October 2018

Guest Editor: Mostafa Zaman Chowdhury

Copyright © 2018 Kyusung Shim and Beongku An. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In this paper, we address the opportunistic scheduling in multitwo user NOMA system consisting of one base station, multinear user, multifar user, and one eavesdropper. To improve the secrecy performance, we propose the users selection scheme, called best-secure-near-user best-secure-far-user (BSNBSF) scheme. The BSNBSF scheme aims to select the best near-far user pair, whose data transmission is the most robust against the overhearing of an eavesdropper. In order to facilitate the performance analysis of the BSNBSF scheme in terms of secrecy outage performance, we derive the exact closed-form expression for secrecy outage probability (SOP) of the selected near user and the tight approximated closed-form expression for SOP of the selected far user, respectively. Additionally, we propose the descent-based search method to find the optimal values of the power allocation coefficients that can minimize the total secrecy outage probability (TSOP). The developed analyses are corroborated through Monte Carlo simulation. Comparisons with the random-near-user random-far-user (RNRF) scheme are performed and show that the proposed scheme significantly improves the secrecy performance.

1. Introduction

To support the 5G-and-beyond-5G communication networks, called future communication networks, nonorthogonal multiple access (NOMA) has been considered as a solution to increase the spectral efficiency by superposing multiple users in resource domain (e.g., time and frequency) [1–3]. More specifically, the downlink scenario of the multitwo user NOMA networks consisting of one base station, a near user (that has strong channel state information (CSI)), and a far user (that has low CSI) is actively considered. The base station simultaneously transmits message to both users using the superposition coding; then the transmit power of the far user message is allocated more than that of the near user message. Under the NOMA scenario, the near user first subtracts the far user message using the successive interference cancellation (SIC) technique [4]; after that the near user decodes its own message. Different from the near user, the far user directly decodes its own message from the received signal without the interference elimination process

since the far user message has allocated higher transmit power than that of the near user message.

The NOMA system can allocate the multiple information on the transmit signal using the superposition coding. Thus, the NOMA system has an advantage in terms of spectrum efficiency compared to that of the OMA system [5–7]. However, this point is a disadvantage in terms of the security [8, 9]. For example, if the eavesdropper succeeds in the interception of one NOMA signal, then the eavesdropper can obtain multiple user information [10]. Thus, the security issue is more important in the NOMA system. Physical layer security (PLS) is one of the possible solutions against the attack of the malicious user. More specifically, from the information-theoretical aspect, the message can be confidentially transmitted if the main channel (between legitimate users) and the eavesdropper channel (between a legitimate user and an eavesdropper) can be controlled so that the legitimate user can decode the received message successfully while the eavesdropper is not able to decode their intercepted message [11]. It is shown that PLS is on the cutting edge of the

technique of security in wireless communication to prevent eavesdropping attacks [12–14].

In PLS, the secrecy outage probability is defined as the probability that the achievable system secrecy capacity of the near/far user drops below a predefined target secrecy rate as in [15]. From the secrecy outage probability, we can measure the degree of security on the system. For example, the low secrecy outage probability system means that the system is more robust compared to that of the high secrecy outage probability system in the viewpoints of security. To improve the PLS performance, the CSI-based opportunistic scheduling [16], that is, the source (destination), communicates with one scheduled destination (source) in a certain resource block (e.g., time and frequency). It has been recognized as an attractive scheduling scheme [17–19] since the time-varying nature of wireless channels is exploited. Thus, opportunistic scheduling is expected as one of techniques to enhance the secrecy performance on NOMA system.

Indeed, the authors of [20] studied the security performance of single-input-single-output (SISO) NOMA system. The authors confirmed that the secrecy sum rate of SISO NOMA system has better performance than that of the OMA system. Liu *et al.* [21] compared the multiple-input-multiple-output (MIMO) NOMA system and MIMO OMA system. Additionally, the authors proved that MIMO NOMA system is better than MIMO OMA system in terms of sum channel capacity. In [22], the authors proposed the transmit antenna selection (TAS) scheme to improve the secrecy performance for downlink multiple-input-single-output (MISO) NOMA system. The first proposed antenna selection scheme is the optimal antenna selection scheme for near user and far user, respectively, while the second proposed antenna selection scheme is the suboptimal antenna selection scheme for the main channel performance of the near user and far user, respectively. The authors of [23] addressed the PLS of large-scale NOMA system. This network consisted of the multiple-antenna base station; the legitimate users were uniformly distributed within a disc, and the eavesdroppers were distributed in an infinite two-dimensional plane via a homogeneous Poisson point process (PPP). The authors derived new exact and asymptotic analyses for the secrecy outage probability (SOP). Li *et al.* [24] optimized the secure beamforming and power allocation design on the MISO NOMA system. From the numerical results, the authors demonstrated that their proposed scheme outperformed that of the conventional OMA system. The authors of [25] designed a secure NOMA system under secrecy constraints where a transmitter sends a signal to multiusers in the presence of an eavesdropper. The authors minimized the total transmit power subject to the QoS and secrecy constraints. The authors of [26] exploited the artificial-noise-aided secure transmission for NOMA full-duplex relay network. The authors proposed the novel joint NOMA and artificial-noise-aided full-duplex relay (NOMA-ANFDR) scheme to enhance the physical security. Specifically, this paper derived the SOP and secrecy throughput. The NOMA-ANFDR outperformed the joint NOMA and artificial-noise half-duplex relay (NOMA-ANHDR) scheme.

Very recently, in [8], the authors proposed the cooperative NOMA system to enhance PLS performance. The authors

considered the NOMA system including a base station, two users (near user and far user), a relay, and an eavesdropper. The authors derived the closed-form and asymptotic analysis for security outage probability and strictly positive secrecy capacity, respectively. The authors of [27] designed a secure massive NOMA system with multiclouds. The authors studied the interuser interference in the designed NOMA system and proposed the power control and power allocation algorithm for maximizing the secrecy capacity. In [28], the authors studied the security impact in the multiuser visible light communication (VLC) [29] with NOMA system. The authors considered both single eavesdropper and multiple eavesdroppers scenarios when the one transmitter communicates with multiple users. The authors derived the exact secrecy outage probability in this network. The author in [30] proposed the relay-supported cooperative NOMA system. The proposed system helped to transmit data using the multiple antenna equipped with relay. In a certain time block, this system selected the transmitted antenna in the relay based on the legitimate channel state information. The authors derived the exact closed-form expression in the proposed system. Lei *et al.* [31] proposed the NOMA system consisting of multiple-antenna base station, multidestinations equipped with multiple antennas, and multieavesdroppers equipped with multiple antennas. Then, the authors proposed and analyzed the max-min based transmit antenna selection scheme when the eavesdroppers work independently or collude.

In the related works, the authors proposed the several schemes to improve the PLS performance. However, the opportunistic scheduling in the multitwo user NOMA network was not considered in the literature. Thus, in this paper, we propose a new users selection scheme to improve the PLS performance in downlink multitwo user NOMA system using the opportunistic scheduling in the presence of one eavesdropper. Compared with the aforementioned works, the main contribution and feature of this paper can be summarized as follows.

- (i) In this paper, we propose a new near/far user selection scheme on the multiple-two user NOMA system. The proposed scheme, denoted by best-secure-near-user best-secure-far-user (BSNBSF) scheme, aims to select the best near-far user pairs, whose data transmission is the most robust combat against the eavesdropper's attack. More specifically, in a certain resource block, we take into account the main/eavesdropper channel state information to select the received user pairs.
- (ii) We derive novel expressions for the selected user pairs, respectively, to estimate the secrecy performance achieved by the proposed scheme. The analyses are not reported in the literature. More specifically, for the selected near user case, we derive an exact closed-form expression on the SOP, whereas, for the selected far user case, we obtain a tight approximated closed-form expression on the SOP, respectively.
- (iii) We present other results, called the asymptotic SOP, for the proposed scheme. These expressions provide the insight into the behavior of the average far user channel power gain (λ_{sf}).

FIGURE 1: Schematic illustration of the multitwo user NOMA system with the presence of an eavesdropper.

- (iv) We conduct the optimal analysis of the power allocation coefficient (θ_N). More specifically, the proposed optimal analysis finds the optimal power allocation coefficient value to make the total SOP minimum on the proposed system based on the descent method.
- (v) Through the numerical results, we demonstrate that the BSNBSF scheme significantly enhances the secrecy performance on the multitwo user NOMA system compared to that of the benchmarked scheme. More specifically, in the case of the SOP for the selected near user, the floor occurs and the selected far user shows the convex pattern as a function of the transmit SNR. Additionally, the secrecy sum throughput of the BSNBSF scheme shows better performance than that of the RNRF scheme.

The rest of this paper is organized as follows. In Section 2, the proposed system model and user pair selection scheme are described. Section 3 investigates the closed-form and asymptotic analyses of the multitwo user NOMA systems. Section 4 presents the optimal analysis of the power allocation coefficients. Section 5 presents some illustrative numerical results based on the insightful discussion. Monte Carlo simulations are shown to corroborate the proposed analyses. Finally, Section 6 concludes the paper.

Notations: $X \sim \mathcal{CN}(0, \sigma^2)$ denotes a circularly symmetric complex Gaussian random variable X with zero mean and variance σ^2 ; $\Pr(\cdot)$ is the probability; $f_X(\cdot)$ and $F_X(\cdot)$ represent the probability density function (PDF) and cumulative distribution function (CDF) of the random variable X , respectively.

2. System Model

Let us consider a downlink multitwo user NOMA system including a base station (S), a set of K near users, $\mathcal{N} = \{N_i \mid i = 1, 2, \dots, K\}$, and a set of M far users, $\mathcal{F} = \{F_j \mid j = 1, 2, \dots, M\}$, and an eavesdropper (E), as shown in Figure 1. More specifically, the near users can perfectly use the SIC technique to subtract the far x_F [22]. Both the legitimate and the illegitimate receivers are equipped with a single antenna and operate in half-duplex mode. In this paper, h_{XY} and $|h_{XY}|^2$, where $X \in \{S\}$, $Y \in \mathcal{N} \cup \mathcal{F} \cup \{E\}$, present the channel coefficient and the corresponding channel gain of $X \rightarrow Y$, respectively. Assuming that all wireless channels exhibit Rayleigh block fading channel, h_{XY} can be modeled as independent and identically distributed (i.i.d.) complex Gaussian random variable with zero mean and variance λ_{XY} . Thus, the corresponding channel gain, $|h_{XY}|^2$, is an exponential random variable with probability density function (PDF), $f_{|h_{XY}|^2}(z) = (1/\lambda_{XY})\exp(-z/\lambda_{XY})$, if $z \geq 0$; otherwise, $f_{|h_{XY}|^2}(z) = 0$ as in [32–34]. More specifically, the average channel gain can be written as $\lambda_{XY} = (d_{XY}/d_0)^{-\epsilon}\mathcal{L}$, where $\mathcal{L}$ is the reference signal power attenuation, d_{XY} denotes the distance between X and Y , d_0 presents the reference distance, and ϵ is the path-loss exponent [33]. And the channel noise is followed by $\omega_Y \sim \mathcal{CN}(0, \sigma_Y^2)$. We also assume that the source perfectly knows the channel state information (CSI) of all legitimate users and eavesdropper, as in [11, 35].

2.1. Communication Process. In this subsection, we present in detail the communication process in two-user NOMA system. Assuming that N_i and F_j are selected to receive its data from the S in a certain time slot. From the principle of NOMA, the messages x_N and x_F that will be allocated to θ_N

and θ_F , respectively, are superposed as $\sqrt{\theta_N}x_N + \sqrt{\theta_F}x_F$ and then broadcasted by S, where θ_N and θ_F denote the power allocation coefficients. We suppose that $|h_{SN_i}|^2 > |h_{SF_j}|^2$, and set $0 < \theta_N < \theta_F$ and $\theta_N + \theta_F = 1$ as in [21].

At the near user N_i , the received signal is given by

$$y_{SN_i} = \sqrt{P_S \theta_N} h_{SN_i} x_N + \sqrt{P_S \theta_F} h_{SN_i} x_F + \omega_{N_i}, \quad (1)$$

where P_S denotes the transmit power of the S. Because of the power allocation coefficient condition, the near user needs to subtract the component, x_F , from the y_{SN_i} using the SIC process [36]. The signal-to-interference-plus-noise-ratio (SINR) of the eliminated component, x_F , is expressed as

$$\gamma_{SN_i}^{x_F} = \frac{P_S \theta_F |h_{SN_i}|^2}{P_S \theta_N |h_{SN_i}|^2 + \sigma_{SN_i}^2}. \quad (2)$$

After the SIC process, the N_i archives its own message, x_N , from the received signal in which signal-to-noise-ratio (SNR) is obtained as

$$\gamma_{SN_i}^{x_N} = \frac{P_S \theta_N |h_{SN_i}|^2}{\sigma_{SN_i}^2}. \quad (3)$$

At the far user F_j , the received signal is given by

$$y_{SF_j} = \sqrt{P_S \theta_F} h_{SF_j} x_F + \sqrt{P_S \theta_N} h_{SF_j} x_N + \omega_{F_j}. \quad (4)$$

Different from the near user, the F_j directly decodes the SINR from the received signal because of the power allocation coefficient condition. The received SINR at F_j to decode x_F is given by

$$\gamma_{SF_j}^{x_F} = \frac{P_S \theta_F |h_{SF_j}|^2}{P_S \theta_N |h_{SF_j}|^2 + \sigma_{SF_j}^2}. \quad (5)$$

Meanwhile, the eavesdropper can intercept the signal due to the broadcast nature of wireless medium. Thus, the received signal at E can be written as

$$y_{SE} = \sqrt{P_S \theta_N} h_{SE} x_N + \sqrt{P_S \theta_F} h_{SE} x_F + \omega_E. \quad (6)$$

Different from the legitimate user, we assume that the E has enough ability to distinguish each message from the received signal. Thus, the SINRs of the received signal are given by

$$\gamma_{SE}^{x_F} = \frac{P_S \theta_F |h_{SE}|^2}{P_S \theta_N |h_{SE}|^2 + \sigma_{SE}^2}, \quad (7)$$

and

$$\gamma_{SE}^{x_N} = \frac{P_S \theta_N |h_{SE}|^2}{\sigma_{SE}^2}, \quad (8)$$

respectively.

In physical-layer security, the secrecy capacity means the difference between main channel capacity and eavesdropper channel capacity. Thus, in two-user NOMA system, the secrecy capacities of x_N and x_F are given by [22, 37]

$$C_{s,N_i} = \left[\log_2 (1 + \gamma_{SN_i}^{x_N}) - \log_2 (1 + \gamma_{SE}^{x_N}) \right]^+, \quad (9)$$

$$C_{s,F_j} = \left[\log_2 (1 + \gamma_{SF_j}^{x_F}) - \log_2 (1 + \gamma_{SE}^{x_F}) \right]^+, \quad (10)$$

respectively, where $[x]^+ = \max\{x, 0\}$.

2.2. The Proposed Best-Secure-Near-User Best-Secure-Far-User (BSNBSF) Scheme. The proposed user selection process is conducted through the channel state information (CSI) estimation/calculation system. Thus, this process is carried out before the data communication process as in [11, 35]. In this paper, we propose the BSNBSF user selection scheme to maximize the secrecy capacity at N_i and F_j , respectively. The proposed scheme can be mathematically expressed as

$$N_b = \arg \max_{i \in \mathcal{N}} \left\{ \log_2 \left(\frac{1 + \gamma_{SN_i}^{x_N}}{1 + \gamma_{SE}^{x_N}} \right) \right\}, \quad (11)$$

and

$$F_b = \arg \max_{j \in \mathcal{F}} \left\{ \log_2 \left(\frac{1 + \gamma_{SF_j}^{x_F}}{1 + \gamma_{SE}^{x_F}} \right) \right\}. \quad (12)$$

(11) and (12) mean that the selected users are the best secrecy capacity of a certain time slot.

3. Secrecy Outage Performance Analysis

In this section, the performance investigation of the proposed user selection scheme in terms of secrecy outage probability (SOP) is presented. Because the wireless channels undergo i.i.d. Rayleigh fading, for the sake of notational convenience, we assume that $\lambda_{SN_i} = \lambda_{SN_2} = \dots = \lambda_{SN_i} = \lambda_{SN}$, $\lambda_{SF_1} = \lambda_{SF_2} = \dots = \lambda_{SF_j} = \lambda_{SF}$.

We also assume the all nodes have the same noise variance. Let $\gamma = P_S/\sigma^2$ present the transmit SNR as in [11, 22]. The SOP of a user can be defined as the probability that the instantaneous secrecy capacity of the user falls below a predefined target data rate [23]. Thus, the SOPs at N_b and F_b are obtained as

$$P_{SOP,N_b} = \Pr(C_{s,N_b} < R_{th,N_b}), \quad (13)$$

and

$$P_{SOP,F_b} = \Pr(C_{s,F_b} < R_{th,F_b}), \quad (14)$$

where R_{th,N_b} and R_{th,F_b} denote the target data rate at N_b and F_b , respectively.

3.1. The Exact Secrecy Outage Probability. At the selected near user, the SOP of N_b can be expressed as

$$P_{SOP,N_b} = \Pr \left(\log_2 \left(\frac{1 + \gamma \theta_N |h_{SN_b}|^2}{1 + \gamma \theta_N |h_{SE}|^2} \right) < R_{th,N_b} \right). \quad (15)$$

Because all wireless channels are assumed to be independent, (15) can be rewritten as

$$P_{\text{SOP},N_b} = \Pr \left(\max_{i \in \mathcal{N}} \left\{ \frac{1 + \gamma \theta_N |h_{\text{SN}_i}|^2}{1 + \gamma \theta_N |h_{\text{SE}}|^2} \right\} < \gamma_{\text{th},N_b} \right), \quad (16)$$

where $\gamma_{\text{th},N_b} \triangleq 2^{R_{\text{th},N_b}}$. As we can observe that the events of the probability in (16) are not mutually exclusive because they include the same components $|h_{\text{SE}}|^2$, therefore conditioning on $|h_{\text{SE}}|^2 = z$, the P_{SOP,N_b} can be further expressed as

$$P_{\text{SOP},N_b} = \int_0^\infty \Pr \left(\bigcap_{i=1}^K \left(\frac{1 + \gamma \theta_N |h_{\text{SN}_i}|^2}{1 + \gamma \theta_N z} < \gamma_{\text{th},N_b} \right) \right) \cdot f_Z(z) dz. \quad (17)$$

Since the assumption that all wireless channels are identical, (17) can be further expressed as

$$P_{\text{SOP},N_b} = \int_0^\infty \prod_{i=1}^K \Pr \left(|h_{\text{SN}_i}|^2 < \frac{\gamma_{\text{th},N_b} - 1}{\gamma \theta_N} + \gamma_{\text{th},N_b} z \right) \cdot f_Z(z) dz. \quad (18)$$

For the sake of notational convenience, let $X_i \triangleq |h_{\text{SN}_i}|^2$; Ψ in (18) can be rewritten as

$$\Psi = \int_0^{(\gamma_{\text{th},N_b} - 1)/\gamma \theta_N + \gamma_{\text{th},N_b} z} f_{X_i}(x) dx. \quad (19)$$

After some algebra manipulations, Ψ can be obtained as

$$\Psi = 1 - \exp \left(-\frac{1}{\lambda_{\text{SN}}} \left(\frac{\gamma_{\text{th},N_b} - 1}{\gamma \theta_N} + \gamma_{\text{th},N_b} z \right) \right). \quad (20)$$

Plugging (20) into (18) and making use of the binomial theorem [38, Eq. (1.111)]

$$(a + b)^N = \sum_{k=0}^N \binom{N}{k} a^{N-k} b^k, \quad (21)$$

P_{SOP,N_b} in (18) can be further expressed as

$$P_{\text{SOP},N_b} = \sum_{n=0}^K \binom{K}{n} (-1)^n \frac{1}{\lambda_{\text{SE}}} \exp \left(-\frac{n(\gamma_{\text{th},N_b} - 1)}{\lambda_{\text{SN}} \gamma \theta_N} \right) \cdot \int_0^\infty \exp \left(-\left(\frac{n \gamma_{\text{th},N_b}}{\lambda_{\text{SN}}} + \frac{1}{\lambda_{\text{SE}}} \right) z \right) dz. \quad (22)$$

After some algebra manipulations and making use of the fact that $\int_0^\infty \exp(-(1/a)x) dx = a$ [38, Eq. (3.310)], consequently, the exact closed-form expression for SOP of the selected near user can be obtained as

$$P_{\text{SOP},N_b} = \sum_{n=0}^K \binom{K}{n} (-1)^n \frac{\lambda_{\text{SN}}}{n \gamma_{\text{th},N_b} \lambda_{\text{SE}} + \lambda_{\text{SN}}} \cdot \exp \left(-\frac{n(\gamma_{\text{th},N_b} - 1)}{\lambda_{\text{SN}} \gamma \theta_N} \right). \quad (23)$$

At the selected far user, the SOP of F_b can be expressed as

$$P_{\text{SOP},F_b} = \Pr \left(\log_2 \left(\frac{1 + \gamma \theta_F |h_{\text{SF}_b}|^2 / (\gamma \theta_N |h_{\text{SE}}|^2 + 1)}{1 + \gamma \theta_F |h_{\text{SE}}|^2 / (\gamma \theta_N |h_{\text{SE}}|^2 + 1)} \right) < R_{\text{th},F_b} \right). \quad (24)$$

Similar to the case of the selected near user, all wireless channels are independent and identical. And the events of the probability in (24) are not mutually exclusive because they include the same components $\gamma \theta_F |h_{\text{SE}}|^2 / (\gamma \theta_N |h_{\text{SE}}|^2 + 1)$. Therefore, conditioning on $\gamma \theta_F |h_{\text{SE}}|^2 / (\gamma \theta_N |h_{\text{SE}}|^2 + 1) = t$, (24) can be further expressed as

$$P_{\text{SOP},F_b} = \int_0^\infty \prod_{j=1}^M \Pr \left(\underbrace{\frac{\gamma \theta_F |h_{\text{SF}_j}|^2}{\gamma \theta_N |h_{\text{SF}_j}|^2 + 1}}_{\Phi} < \gamma_{\text{th},F_b} - 1 + \gamma_{\text{th},F_b} t \right) \cdot f_T(t) dt. \quad (25)$$

In order to further simplify the integral (25), the following lemma enables us to characterize the SINR at far user and eavesdropper to decode x_F .

Lemma 1. Suppose that $U \triangleq \gamma \theta_F \rho / (\gamma \theta_N \rho + 1)$ ($\rho \in \{|h_{\text{SF}_j}|^2, |h_{\text{SE}}|^2\}$); the cumulative distribution function (CDF) and probability density function (PDF) can be expressed as

$$F_U(u) = \begin{cases} 1 - \varphi(\lambda_U, u), & \text{if } 0 \leq u < \frac{\theta_F}{\theta_N}, \\ 1, & \text{if } \frac{\theta_F}{\theta_N} \leq u, \end{cases} \quad (26)$$

and

$$f_U(u) = \begin{cases} \frac{\theta_F}{\lambda_U \gamma (\theta_F - \theta_N u)^2} \varphi(\lambda_U, u), & \text{if } 0 \leq u < \frac{\theta_F}{\theta_N}, \\ 0, & \text{if } \frac{\theta_F}{\theta_N} \leq u, \end{cases} \quad (27)$$

respectively, where $\varphi(\alpha, t) = \exp(-t/\alpha \gamma (\theta_F - \theta_N t))$; λ_U represents the average channel power gain.

Proof. The CDF of U can be written as

$$F_U(u) = \Pr(\gamma \theta_F \rho < (\gamma \theta_N \rho + 1)u). \quad (28)$$

After some basic manipulations, (28) can be rewritten as

$$F_U(u) = \Pr \left(\rho < \frac{u}{\gamma (\theta_F - \theta_N u)} \right), \quad (29)$$

if $\rho < \theta_F/\theta_N$; otherwise, $F_U(u) = 1$. After some calculation steps, the PDF of U can be obtained as presented in equation (27). This completes the proof of Lemma 1. $\square$

For the sake of notational convenience, let $Y_j \triangleq |h_{SF_j}|^2$. After some algebra manipulations, since Y_j is a nonnegative random variable and constants are strictly positive constants, Φ in (25) can be further obtained as

$$\begin{aligned} \Phi &= \Pr\left(Y_j < \frac{\gamma_{th,F_b} - 1 + \gamma_{th,F_b} t}{\gamma(\theta_F - \theta_N(\gamma_{th,F_b} - 1 + \gamma_{th,F_b} t))}\right) \\ &= \int_0^{(\gamma_{th,F_b} - 1 + \gamma_{th,F_b} t)/\gamma(\theta_F - \theta_N(\gamma_{th,F_b} - 1 + \gamma_{th,F_b} t))} f_{Y_j}(y) dy \\ &= \begin{cases} 1 - \varphi(\lambda_{SF}, \gamma_{th,F_b} - 1 + \gamma_{th,F_b} t), & \text{if } \frac{1}{\theta_N \gamma_{th,F_b}} - 1 > t, \\ 1, & \text{if } \frac{1}{\theta_N \gamma_{th,F_b}} - 1 \leq t. \end{cases} \end{aligned} \quad (30)$$

By plugging (27) and (30) into (25), since $\theta_F/\theta_N \geq 1/\gamma_{th,F_b} \theta_N - 1$, the P_{SOP,F_b} can be further expressed as

$$P_{SOP,F_b} = \int_0^{1/\gamma_{th,F_b} \theta_N - 1} \prod_{j=1}^M [1 - \varphi(\lambda_{SF}, \gamma_{th,F_b} - 1 + \gamma_{th,F_b} t)]$$

$$\begin{aligned} &\cdot \frac{\theta_F}{\lambda_{SE} \gamma(\theta_F - \theta_N t)^2} \varphi(\lambda_{SE}, t) dt \\ &+ \int_{1/\gamma_{th,F_b} \theta_N - 1}^{\theta_F/\theta_N} \frac{\theta_F}{\lambda_{SE} \gamma(\theta_F - \theta_N t)^2} \varphi(\lambda_{SE}, t) dt. \end{aligned} \quad (31)$$

Similar to (20), we rely on the binomial theorem [38, eq. (1.111)]. Consequently, (31) can be further written as

$$\begin{aligned} P_{SOP,F_b} &= \int_0^{1/\gamma_{th,F_b} \theta_N - 1} \sum_{k=0}^M \binom{M}{k} (-1)^k \\ &\cdot \exp\left(-\frac{k(\gamma_{th,F_b} - 1 + \gamma_{th,F_b} t)}{\lambda_{SF} \gamma(\theta_F - \theta_N(\gamma_{th,F_b} - 1 + \gamma_{th,F_b} t))}\right) \\ &\cdot \frac{\theta_F}{\lambda_{SE} \gamma(\theta_F - \theta_N t)^2} \exp\left(-\frac{t}{\lambda_{SE} \gamma(\theta_F - \theta_N t)}\right) dt \\ &+ \int_{1/\gamma_{th,F_b} \theta_N - 1}^{\theta_F/\theta_N} \frac{\theta_F}{\lambda_{SE} \gamma(\theta_F - \theta_N t)^2} \exp\left(-\frac{t}{\lambda_{SE} \gamma(\theta_F - \theta_N t)}\right) dt. \end{aligned} \quad (32)$$

To the best of the authors' knowledge, it is very difficult to obtain the exact closed-form expression of (32). Thus, in this paper, we approximate (32) using Gaussian-Chebyshev quadrature [39, eq. (25.4.38)]. First, to utilize the Gaussian-Chebyshev quadrature, the range of (32) can be coordinated as

$$\begin{aligned} P_{SOP,F_b} &= \beta_1 \int_{-1}^1 \sum_{k=0}^M \binom{M}{k} (-1)^k \exp\left(-\frac{k(\gamma_{th,F_b} - 1 + \gamma_{th,F_b}(\beta_1 x + \beta_1))}{\lambda_{SF} \gamma(\theta_F - \theta_N(\gamma_{th,F_b} - 1 + \gamma_{th,F_b}(\beta_1 x + \beta_1)))}\right) \\ &\cdot \frac{\theta_F}{\lambda_{SE} \gamma(\theta_F - \theta_N(\beta_1 x + \beta_1))^2} \exp\left(-\frac{\beta_1 x + \beta_1}{\lambda_{SE} \gamma(\theta_F - \theta_N(\beta_1 x + \beta_1))}\right) dx \\ &+ \beta_2 \int_{-1}^1 \frac{\theta_F}{\lambda_{SE} \gamma(\theta_F - \theta_N(\beta_2 x + \beta_3))^2} \exp\left(-\frac{\beta_2 x + \beta_3}{\lambda_{SE} \gamma(\theta_F - \theta_N(\beta_2 x + \beta_3))}\right) dx, \end{aligned} \quad (33)$$

where $\beta_1 = ((1/\gamma_{th,F_b} \theta_N) - 1)/2$, $\beta_2 = ((\theta_F/\theta_N) - (1/\gamma_{th,F_b} \theta_N) + 1)/2$, $\beta_3 = ((\theta_F/\theta_N) + (1/\gamma_{th,F_b} \theta_N) - 1)/2$. Next, to approximate P_{SOP,F_b} in (33), (33) can be transformed using the fact that

$$\int_{-1}^1 \frac{f(x) \sqrt{1-x^2}}{\sqrt{1-x^2}} dx = \sum_{i=1}^N w_i \sqrt{1-\tau_i^2} f(x_i), \quad (34)$$

where $w_i = \pi/N$, $\tau_i = \cos(((2i-1)/2N)\pi)$, and N is the number of terms, respectively. Plugging (33) into (34), and after some manipulations, eventually, the tight approximated closed-form expression for SOP of the selected far user can be obtained as

$$\begin{aligned} P_{SOP,F_b} &= \beta_1 \sum_{i=1}^N \frac{\pi}{N} \sqrt{1-\tau_i^2} \sum_{k=0}^M \binom{M}{k} (-1)^k \\ &\cdot \exp\left(-\frac{k(\gamma_{th,F_b} - 1 + \gamma_{th,F_b}(\beta_1 \tau_i + \beta_1))}{\lambda_{SF} \gamma(\theta_F - \theta_N(\gamma_{th,F_b} - 1 + \gamma_{th,F_b}(\beta_1 \tau_i + \beta_1)))}\right) \end{aligned}$$

$$\begin{aligned} &\cdot \frac{\theta_F}{\lambda_{SE} \gamma(\theta_F - \theta_N(\beta_1 \tau_i + \beta_1))^2} \\ &\cdot \exp\left(-\frac{\beta_1 \tau_i + \beta_1}{\lambda_{SE} \gamma(\theta_F - \theta_N(\beta_1 \tau_i + \beta_1))}\right) \\ &+ \beta_2 \sum_{i=1}^N \frac{\pi}{N} \sqrt{1-\tau_i^2} \frac{\theta_F}{\lambda_{SE} \gamma(\theta_F - \theta_N(\beta_2 \tau_i + \beta_3))^2} \\ &\cdot \exp\left(-\frac{\beta_2 \tau_i + \beta_3}{\lambda_{SE} \gamma(\theta_F - \theta_N(\beta_2 \tau_i + \beta_3))}\right). \end{aligned} \quad (35)$$

3.2. The Asymptotic Analysis. In this subsection, we derive the asymptotic SOP in the high SINR regime, which is mathematically described as $\lambda_{SF} \rightarrow \infty$ and $\lambda_{SN} = \beta \lambda_{SF}$ ($\beta > 1$) [21, 40]. This expression gives insight into the behavior of

Input: system parameters such as γ_{th,N_b} , γ_{th,F_b} , λ_{SN} , λ_{SF} , λ_{SE} , θ_N , θ_F , γ ; and the given optimization parameters such as step size, $s_t = 10^{-2}$, search length, $\Delta k = 1$

Output: θ_{N^*}

- (1) Assign iteration index to the initial: $k \leftarrow 1$
- (2) Choose a starting point of the searching optimal value: $\theta_{N_k} \leftarrow 10^{-9}$
- (3) **while** $P_{TSOP}(\theta_{N_k}) > P_{TSOP}(\theta_{N_k} + s_t \Delta k)$ **do**
- (4) Update the searching optimal value: $\theta_{N_{k+1}} \leftarrow \theta_{N_k} + s_t \Delta k$, $k \leftarrow k + 1$
- (5) **end while**
- (6) **return** θ_{N_k}

ALGORITHM 1: The Descent-based Algorithm for Finding θ_{N^*} .

the secrecy outage for high SINR. Using the Taylor's series approximation of the term, that is, $\exp(-a/x) \approx 1 - a/x$, and after some algebraic manipulations, the asymptotic SOP of the selected near user can be obtained as

$$P_{SOP,N_b}^{asym} = \sum_{n=0}^K \binom{K}{n} (-1)^n \cdot \frac{\beta \lambda_{SF}}{n \gamma_{th,N_b} + \beta \lambda_{SF}} \left(1 - \frac{n(\gamma_{th,N_b} - 1)}{\gamma \theta_N \beta \lambda_{SF}} \right). \quad (36)$$

Similar to the asymptotic SOP for the selected near user, the asymptotic SOP for selected far user can be expressed as

$$P_{SOP,F_b}^{asym} = \beta_1 \sum_{i=1}^N \frac{\pi}{N} \sqrt{1 - \tau_i^2} \cdot \sum_{k=0}^M \binom{M}{k} (-1)^k \frac{\theta_F}{\lambda_{SE} \gamma [\theta_F - \theta_N (\beta_1 \tau_i + \beta_1)]^2} \cdot \exp \left(- \frac{\beta_1 \tau_i + \beta_1}{\lambda_{SE} \gamma [\theta_F - \theta_N (\beta_1 \tau_i + \beta_1)]} \right) \cdot \left(1 - \frac{k(\gamma_{th,F_b} - 1 + \gamma_{th,F_b} (\beta_1 \tau_i + \beta_1))}{\gamma [\theta_F - \theta_N (\gamma_{th,F_b} - 1 + \gamma_{th,F_b} (\beta_1 \tau_i + \beta_1))] \lambda_{SF}} \right) + \beta_2 \sum_{i=1}^N \frac{\pi}{N} \sqrt{1 - \tau_i^2} \frac{\theta_F}{\lambda_{SE} \gamma [\theta_F - \theta_N (\beta_2 \tau_i + \beta_3)]^2} \cdot \exp \left(- \frac{\beta_2 \tau_i + \beta_3}{\lambda_{SE} \gamma [\theta_F - \theta_N (\beta_2 \tau_i + \beta_3)]} \right). \quad (37)$$

4. Optimal Analysis of the Power Allocation Coefficients θ_N

In this section, we carry out the optimal analysis of the power allocation coefficient θ_N . Specifically, using the descent algorithm [41], we propose a descent-based algorithm (Algorithm 1) for finding the optimal point of θ_N , denoted as θ_{N^*} , which results from the minimum value of the total secrecy outage probability (TSOP) as follows.

In our paper, the optimization algorithm is applied to obtain the optimal power allocation coefficient of $\theta_N \in$

(0, 0.5) that minimizes the TSOP. The process of the proposed optimization algorithm can be explained as follows.

- (i) At the starting point θ_{N_k} , we determine a descent direction satisfying $P_{TSOP}(\theta_{N_k}) > P_{TSOP}(\theta_{N_{k+1}})$, where k presents the index of the iteration.
- (ii) We update the searching optimal value, that is, $\theta_{N_{k+1}} = \theta_{N_k} + s_t \Delta k$, where s_t means the step size. If $\theta_{N_k} < \theta_{N_{k+1}}$, we can obtain $P_{TSOP}(\theta_{N_k}) > P_{TSOP}(\theta_{N_{k+1}})$; otherwise θ_{N_k} is optimal.
- (iii) As we can see, when θ_{N_k} is its optimal value, $P_{TSOP}(\theta_{N_k})$ becomes the smallest value. Therefore, the iteration process of updating θ_{N_k} will be stopped when $P_{TSOP}(\theta_{N_k}) < P_{TSOP}(\theta_{N_{k+1}})$.

Please note that the proposed algorithm is operated on the system parameters collected through CSI estimation process before data transmission process.

5. Numerical Results

In this section, we present the representative numerical results to illustrate the achievable performance of the proposed scheme. Monte Carlo simulation results are generated to validate the developed analysis. In simulation setting, we assume that positions of the source S, the cluster of near users, the cluster of far users, and the eavesdropper E are randomly deployed satisfying some given distance constraints. Specifically, we set that the distance between S and the cluster near users is $d_{SN} = 10\text{m}$, the distance between S and the cluster of far users is $d_{SF} = 20\text{m}$, and the distance between S and eavesdropper is $d_{SE} = 30\text{m}$, respectively. It is noted that although multiple near or far users are located at the same location, their channel characteristics are different from one to another. The power allocation coefficients of the near user (θ_N) and far user (θ_F) are 0.2 and 0.8, respectively. Additionally, the reference distance $d_0 = 1\text{m}$, and power degradation at d_0 is $L = 30$ (dB), the path-loss exponent $\epsilon = 2.7$.

Figure 2 presents the performance comparison of the BSNBSF scheme and random near user and random far user (RNRF) scheme, in which the number of the near users is 3, and the number of the far users is 3, respectively. As can be seen in Figure 2, the SOP of the BSNBSF scheme is lower than that of random selection scheme. The reason is that

FIGURE 2: Performance comparison between the proposed BSNBSF scheme and the RNRF scheme with secrecy outage probability as a function of the transmit SNR, where $\theta_N = 0.2$, $R_{th,N_b} = R_{th,F_b} = 0.1$ bps/Hz.

the proposed scheme considers the secrecy channel capacity to select the near user and far user, respectively. When the transmit power increases, the SOP of the selected near user is increased until it reaches a performance floor. Different from the case of the selected near user, the SOP of the selected far user is plotted as in convex pattern with respect to the transmit SNR.

Next, we investigate the TSOP of the proposed scheme and RNRF scheme, which can be mathematically defined as [23]

$$P_{TSOP} = 1 - (1 - P_{SOP,N_b})(1 - P_{SOP,F_b}). \quad (38)$$

Figure 3 illustrates the impact of the transmit SNR and the number of near and far users on the performance of the proposed scheduling scheme. As can be seen in Figure 3, increasing the number of near and far users does not improve the performance of the RNRF while the performance of the proposed scheme is improved when the number of the near and far users is higher. The reason is that the BSNBSF scheme exploits the difference in channel conditions between users to select the best near and far users pair.

In Figure 4, we plot the SOP as a function of the transmit SNR with different numbers of the near user and the far user, respectively. As can be observed in Figure 4, the SOP decreases when the number of the near user increases. The reason is that the security performance increases when more nodes take into account the data transmission. In contrast to the case of near user, when the number of the far user increases, the secrecy performance is impacted a little bit. One of possible reasons is that the channel condition of the far user is not so much stronger than that of near user.

FIGURE 3: Illustration of the impact of the number of near users and far users as a function of the transmit SNR, where $R_{th,F_b} = R_{th,N_b} = 0.1$.

Thus, security performance does not have much effect on the number of far participants. Additionally, we can observe that the results of the asymptotic analysis tightly approximate the closed-form analysis as a function of the increase of average far user channel power gain.

Figure 5 illustrates the TSOP as a function of the distance between the base station and eavesdropper with different numbers of the near users and the far users. As can be seen in Figure 5, when the distance between the base station and eavesdropper increases, the TSOP decreases. The reason is that, when the distance between the base station and eavesdropper increases, it is difficult for the eavesdropper to intercept the information between the legitimate users. Additionally, we can observe that the proposed scheme has better secrecy performance than the benchmarked scheme with the same transmit power.

Figure 6 presents the TSOP as a function of the secrecy target data rate, R_{th} (bps/Hz), with different numbers of the near users and the far users. As can be seen in Figure 6, the total secrecy outage probability increases when the secrecy target data rate increases. This means that if the base station is allowed to transmit with a higher secrecy data rate (in order to obtain higher secrecy throughput), the data transmission will be vulnerable to the eavesdropper.

We investigate the effect on power allocation mechanism on the secrecy performance of the proposed scheduling scheme as shown in Figure 7, where the total secrecy outage probability of the selected user pair is plotted as a function of the transmit power and power allocation coefficient of the near user, θ_N . It is noted that $\theta_F = 1 - \theta_N$. As can be observed, the TSOP poses a complicated convex characteristic with

FIGURE 4: Illustration of the impact of the number of near users and far users on the secrecy outage probability as a function of the average far user channel power gains, where transmit SNR = 30 dBm, $R_{th,F_b} = R_{th,N_b} = 0.1$ bps/Hz.

FIGURE 5: Illustration of the total secrecy outage probability as a function of the distance between base station and eavesdropper with different numbers of the near users and the far users, where transmit SNR = 30 dBm, $R_{th,F_b} = R_{th,N_b} = 0.1$ bps/Hz.

respect to θ_N . More specifically, the total secrecy outage probability is a convex function with respect to θ_N when the transmit SNR is less than 30 dBm or greater than 45 dBm under our setting, while it is not a convex function when the transmit power is in the range from 30 dBm to 45 dBm. Hence, we apply the optimization algorithm for finding the minimum power allocation coefficient of the near user, θ_N , when the transmit SNR is less than 30 dBm.

FIGURE 6: Illustration of the total secrecy outage probability as a function of the secrecy target data rate, R_{th} (bps/Hz), with different numbers of the near users and far users, where transmit SNR = 30 dBm.

Figure 8 illustrates the TSOP with different transmit SNR as a function of the power allocation coefficient of the near user, denoted as θ_N . When the transmit SNR increases, the TSOP decreases. Additionally, there is the optimal value of θ_N where the TSOP is minimum as presented in Figure 8. It is noted that the minimum TSOPs are obtained using the proposed descent-based search method.

Finally, we investigate the secrecy performance improvements of the proposed scheme in terms of the secrecy sum throughput as a function of the transmit SNR. The secrecy sum throughput can be defined as [42]

$$\mathcal{T}_{\text{sum}} = (1 - P_{\text{SOP},N_b}) R_{th,N_b} + (1 - P_{\text{SOP},F_b}) R_{th,F_b}. \quad (39)$$

As can be observed in Figure 9, comparing the proposed scheme with the RNRF scheme, the proposed scheme significantly improves the secrecy sum throughput. More specifically, when the number of the near and far users increases, the secrecy sum throughput increases. Different from the proposed scheme, the RNRF scheme does not affect the number of the near and far users. The reason is that, when the near and far users are selected in the proposed system, we consider the channel condition of the main channel and eavesdropper channel. However, the benchmarked scheme does not consider that condition to select the near and far users, respectively.

6. Conclusion

In this paper, we propose the opportunistic scheduling scheme to enhance the secrecy performance in multitwo user NOMA system. The proposed BSNBSF scheme aims to improve the physical layer security of the considered NOMA system. Specifically, the BSNBSF scheme selects the

FIGURE 7: The total secrecy outage probability of the selected users pair as a function of the transmit SNR and the power allocation coefficients of the near user, with $K = 3$, $M = 3$, $R_{th,N_b} = R_{th,F_b} = 0.1$ bps/Hz.

FIGURE 8: Illustration of the total secrecy outage probability with different transmit power as a function of the power allocation for the near user (θ_N), with $K = 5$, $M = 5$, $R_{th,N_b} = R_{th,F_b} = 0.1$ bps/Hz.

user pair by estimating both main channel and eavesdropper channel characteristics to select the most robust near and far users, respectively. The exact closed-form expression for the SOP of the selected near user and the tight approximated closed-form expression for the SOP of the selected far user are presented. In order to get more insightful results, the asymptotic results for the SOP of the selected near user and the selected far user are obtained. Moreover, we propose the optimization algorithm, called the descent-based search algorithm, to find the optimal value of θ_N that minimizes the TSOP when the transmit SNR is less than 35 dBm. The obtained results are verified by the computer simulation. From the numerical results, the proposed scheme provides

FIGURE 9: Illustration of the secrecy sum throughput with the different numbers of the near users and far users as a function of the transmit power, where $R_{th,F_b} = R_{th,N_b} = 0.1$ bps/Hz.

better secrecy performance compared to that of the RNRF scheme. Additionally, the increasing number of participant near and/or far users improves the robustness of the BSNBSF scheme. The descent-based search algorithm has been proposed to find out the optimal value of θ_N^* that minimizes the secrecy performance. The BSNBSF scheme can also support better performance than the RNRF scheme in terms of the secrecy sum throughput.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Disclosure

This article is the extended version based on International Conference on Ubiquitous and Future Networks (ICUFN 2018), Prague, Czech Republic, July 2018 [43].

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (Grant no. 2016R1D1A1B03934898) and by the Leading Human Resource Training Program of Regional Neo Industry through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT and future planning (Grant no. 2016H1D5A1910577).

References

- [1] IMT-2020 (5G) Promotion Group, "5G Vision and Requirements," *White Paper*, pp. 1–18, 2015, Available: <http://www.imt-2020.org.cn/en/documents/download/3>.
- [2] NTT DOCOMO, "5G radio access: Requirements, concept and technologies," *White Paper*, June 2014.
- [3] K. Saito, Y. Saito, and Y. Kishiyama, "Special articles on 5G technologies toward deployment," *NTT DOCOMO Technical Journal*, vol. 17, no. 4, pp. 16–28, 2016.
- [4] Y. Saito, Y. Kishiyama, A. Benjebbour, T. Nakamura, A. Li, and K. Higuchi, "Non-orthogonal multiple access (NOMA) for cellular future radio access," in *Proceedings of the IEEE 77th Vehicular Technology Conference (VTC '13)*, pp. 1–5, Dresden, Germany, June 2013.
- [5] L. Dai, B. Wang, Y. Yuan, S. Han, C. I, and Z. Wang, "Non-orthogonal multiple access for 5G: solutions, challenges, opportunities, and future research trends," *IEEE Communications Magazine*, vol. 53, no. 9, pp. 74–81, 2015.
- [6] Z. Ding, Y. Liu, J. Choi et al., "Application of Non-Orthogonal Multiple Access in LTE and 5G Networks," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 185–191, 2017.
- [7] M. Shirvanimoghaddam, M. Dohler, and S. J. Johnson, "Massive Non-Orthogonal Multiple Access for Cellular IoT: Potentials and Limitations," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 55–61, 2017.
- [8] J. Chen, L. Yang, and M. Alouini, "Physical Layer Security for Cooperative NOMA Systems," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 4645–4649, 2018.
- [9] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao, "A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, 2018.
- [10] Z. Qin, Y. Liu, Z. Ding, Y. Gao, and M. ElKashlan, "Physical layer security for 5G non-orthogonal multiple access in large-scale networks," in *Proceedings of the 2016 IEEE International Conference on Communications, ICC 2016*, Malaysia, May 2016.
- [11] K. Shim, N. T. Do, and B. An, "Performance analysis of physical layer security of opportunistic scheduling in multiuser multirelay cooperative networks," *Sensors*, vol. 17, no. 2, 2017.
- [12] N. Yang, L. Wang, G. Geraci, M. ElKashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20–27, 2015.
- [13] W. Trappe, "The challenges facing physical layer security," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 16–20, 2015.
- [14] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 114, no. 1, pp. 19–26, 2017.
- [15] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, 2010.
- [16] A. Asadi and V. Mancuso, "A survey on opportunistic scheduling in wireless communications," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 1671–1688, 2013.
- [17] L. Yang, J. Chen, H. Jiang, S. A. Vorobyov, and H. Zhang, "Optimal relay selection for secure cooperative communications with an adaptive eavesdropper," *IEEE Transactions on Wireless Communications*, vol. 16, no. 1, pp. 26–42, 2017.
- [18] L. Fan, N. Yang, T. Q. Duong, M. ElKashlan, and G. K. Karagiannis, "Exploiting direct links for physical layer security in multiuser multirelay networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 3856–3867, 2016.
- [19] N. T. Do, D. B. Da Costa, T. Q. Duong, and B. An, "A BNBF user selection scheme for NOMA-based cooperative relaying systems with SWIPT," *IEEE Communications Letters*, vol. 21, no. 3, pp. 664–667, 2017.
- [20] Y. Zhang, H.-M. Wang, Q. Yang, and Z. Ding, "Secrecy sum rate maximization in non-orthogonal multiple access," *IEEE Communications Letters*, vol. 20, no. 5, pp. 930–933, 2016.
- [21] Y. Liu, G. Pan, H. Zhang, and M. Song, "On the capacity comparison between MIMO-NOMA and MIMO-OMA," *IEEE Access*, vol. 4, pp. 2123–2129, 2016.
- [22] H. Lei, J. Zhang, K.-H. Park et al., "On secure NOMA systems with transmit antenna selection schemes," *IEEE Access*, vol. 5, pp. 17450–17464, 2017.
- [23] 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 Transactions on Wireless Communications*, vol. 16, no. 3, pp. 1656–1672, 2017.
- [24] Y. Li, M. Jiang, Q. Zhang, Q. Li, and J. Qin, "Secure beamforming in downlink MISO nonorthogonal multiple access systems," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 8, pp. 7563–7567, 2017.
- [25] B. He, A. Liu, N. Yang, and V. K. N. Lau, "On the design of secure non-orthogonal multiple access systems," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 10, pp. 2196–2206, 2017.
- [26] Y. Feng, Z. Yang, and S. Yan, "Non-orthogonal multiple access and artificial-noise aided secure transmission in FD relay networks," in *Proceedings of the 2017 IEEE Globecom Workshops (GC Wkshps)*, pp. 1–6, Singapore, December 2017.
- [27] X. Chen, Z. Zhang, C. Zhong, D. W. Ng, and R. Jia, "Exploiting inter-user interference for secure massive non-orthogonal multiple access," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 788–801, 2018.

- [28] X. Zhao, H. Chen, and J. Sun, "On physical-layer security in multiuser visible light communication systems with non-orthogonal multiple access," *IEEE Access*, vol. 6, pp. 34004–34017, 2018.
- [29] A. Mostafa and L. Lampe, "Physical-layer security for indoor visible light communications," in *Proceedings of the 1st IEEE International Conference on Communications (ICC '14)*, pp. 3342–3347, Sydney, Australia, June 2014.
- [30] D. Deng, C. Li, L. Fan, X. Liu, and F. Zhou, "Impact of antenna selection on physical-layer security of NOMA networks," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 2390834, 11 pages, 2018.
- [31] H. Lei, J. Zhang, K. Park et al., "Secrecy outage of maximin tas scheme in mimo-noma systems," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 8, pp. 6981–6990, August 2018.
- [32] K. Shim, H. Oh, T. N. Do, and B. An, "A physical layer security-based transmit antenna selection scheme for NOMA systems," in *Proceedings of the 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN)*, pp. 597–602, Prague, Czech Republic, July 2018.
- [33] T. N. Do, D. B. da Costa, T. Q. Duong, and B. An, "Improving the performance of cell-edge users in NOMA systems using cooperative relaying," *IEEE Transactions on Communications*, vol. 66, no. 5, pp. 1883–1901, 2018.
- [34] H. Liu, K. J. Kim, K. S. Kwak, and H. V. Poor, "Power splitting-based SWIPT with decode-and-forward full-duplex relaying," *IEEE Transactions on Wireless Communications*, vol. 15, no. 11, pp. 7561–7577, 2016.
- [35] N. T. Do, D. B. Da Costa, T. Q. Duong, V. N. Q. Bao, and B. An, "Exploiting direct links in multiuser multirelay SWIPT cooperative networks with opportunistic scheduling," *IEEE Transactions on Wireless Communications*, vol. 16, no. 8, pp. 5410–5427, 2017.
- [36] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, John Wiley & Sons, 2012.
- [37] K. Shim, N. T. Do, B. An, and S.-Y. Nam, "Outage performance of physical layer security for multi-hop underlay cognitive radio networks with imperfect channel state information," in *Proceedings of the 15th International Conference on Electronics, Information, and Communications, ICEIC 2016*, pp. 1–4, Da Nang, Vietnam, January 2016.
- [38] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, Academic Press is an imprint of Elsevier, 7th edition, 2007.
- [39] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions: with Formulas, Graphs, and Mathematical Tables*, vol. 55, Courier Corporation, 1964.
- [40] H. Lei, C. Gao, I. S. Ansari et al., "Secrecy outage performance of transmit antenna selection for MIMO underlay cognitive radio systems over nakagami-m channels," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2237–2250, 2017.
- [41] S. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge University Press, 2004.
- [42] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Relaying protocols for wireless energy harvesting and information processing," *IEEE Transactions on Wireless Communications*, vol. 12, no. 7, pp. 3622–3636, 2013.
- [43] K. Shim, T. N. Do, and B. An, "Improving physical layer security of noma networks by using opportunistic scheduling," in *Proceedings of the 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN)*, pp. 262–267, Prague, Czech Republic, July 2018.