On Secure NOMA-Aided Semi-Grant-Free Systems

Hongjiang Lei, Senior Member, IEEE, Fangtao Yang, Hongwu Liu, Senior Member, IEEE, Imran Shafique Ansari, Senior Member, IEEE, Kyeong Jin Kim, Senior Member, IEEE, and Theodoros A. Tsiftsis, Senior Member, IEEE

Abstract—Semi-grant-free (SGF) transmission scheme enables grant-free (GF) users to utilize resource blocks allocated for grant-based (GB) users while maintaining the quality of service of GB users. This work investigates the secrecy performance of non-orthogonal multiple access (NOMA)-aided SGF systems. First, analytical expressions for the exact and asymptotic secrecy outage probability (SOP) of NOMA-aided SGF systems with a single GF user are derived. Then, the SGF systems with multiple GF users and the best-user scheduling scheme is considered. By utilizing order statistics theory, analytical expressions for the exact and asymptotic SOP are derived. Monte Carlo simulation results are provided and compared with two benchmark schemes. The effects of system parameters on the SOP of the considered system are demonstrated and the accuracy of the developed analytical results is verified. The results indicate that both the outage target rate for GB and the secure target rate for GF are the main factors of the secrecy performance of SGF systems.

Index Terms—Non-orthogonal multiple access (NOMA), semi-grant-free (SGF) transmission scheme, grant-free (GF) user, grant-based (GB) user, secrecy outage probability.

I. INTRODUCTION

A. Background and Related Work

Ultra-reliable low latency communications (URLLC) and massive machine-type communications (mMTC) are the two most important scenarios for the next internet of things (IoT). URLLC focuses on mission-critical applications wherein unprecedented levels of reliability and latency are of the utmost importance in the fifth generation and it’s beyond [1]. In contrast, mMTC aspires to connect a vast number of intelligent devices to the Internet. The user initiates the traditional grant-based (GB) access scheme with an access request to the base station (BS) in long term evolution. The BS responds by allocating an access grant through a four-step handshake procedure strategy. Once the BS grants the access request, data packets can be successfully transmitted without collision under ideal channel conditions. However, GB scheme does not suit these scenarios due to high latency and heavy signaling overhead [2], [3]. Moreover, the initial request transmission is still subject to collision and could require multiple transmissions depending on traffic load and the available resources at the BS.

To tackle these issues, grant-free (GF) transmission schemes were introduced in [4], [5], and [6], in which multiple users may occupy the same resource without the initial access request procedure. Unlike the GB principle, no dedicated request transmission for granting access and allocating resource blocks is required for GF communications before starting a data transmission. Although the GF scheme makes it possible to allow users to choose resource blocks independently and transmit data directly to reduce signaling overhead and latency effectively, collisions will become severe when multiple users select the same resource block to transmit simultaneously [7]. The collision issue can be resolved using massive multiple-input multiple-output (MIMO) or non-orthogonal multiple access (NOMA) technologies. The former solution utilizes spatial degrees of freedom to mitigate multi-user collisions, while the latter focuses on spectrum sharing among multiple users with successive interference cancellation (SIC) [8], [9], [10], [11].

Even though the massive connectivity can be supported through GF schemes, GB schemes are still desired, especially when strict quality of service (QoS) requirements exist [11]. The GB and GF transmission scheme must coexist in scenarios where URLLC applications are served by the GB scheme and mMTC applications in the same system are served by the GF scheme. For example, a new hybrid access scheme was proposed in [12] to meet the various requirements of IoT networks wherein machine-type users with small data packets and delay-tolerant traffic utilized the GF scheme, and some users with large data packets and delay-sensitive traffic used the GB scheme. NOMA-aided Semi-GF (SGF) transmission scheme was first explicitly introduced in [13] to alleviate the collisions and obtain massive connectivity. A single GB user with multiple GF users to perform NOMA
and two contention control mechanisms were proposed to suppress the interference on the GB user from the GF users. Closed-form expressions for the outage probability (OP) of GF users were derived and the impact of different SIC decoding orders was investigated. Their results demonstrated the superior performance of NOMA-aided SGF schemes. Based on the relationship between the GB user’s targeted rate and channel conditions, an adaptive power allocation strategy was proposed to control the transmit power of GB users to ensure that the GB user’s signals are always decoded in the second stage of SIC [14]. In [15], the authors investigated the performance of an uplink SGF system with multiple uniformly distributed GF and GB users considered, in which the GF user whose received power is lower at the BS than that of the GB user was selected to pair with the connected GB user. Closed-form expressions for GB and GF users’ exact and approximate ergodic rates were derived. Further, the authors in [16] studied the effect of random locations of GF users on the performance of NOMA-assisted SGF systems by utilizing stochastic geometry. A dynamic threshold protocol was proposed to reduce the interference to GB users, and the outage performance was analyzed and compared with the open-loop protocol.

Relative to the SGF schemes proposed in [13], a new QoS-guarantee scheme for NOMA-aided SGF systems was proposed in [17] to ensure that the QoS of the GB user is the same as that when it solely occupies the channel. Closed-form expressions were derived for the exact and asymptotic OP with the best-user scheduling (BUS) scheme and a hybrid SIC scheme. The results demonstrated that the proposed scheme could significantly improve the reliability of the GF users’ transmissions. Based on [17], a new adaptive power control strategy was proposed to solve OP error floors entirely by adjusting the GF user’s transmit power to change the decoding order of SIC in [18]. In [19], the authors analyzed the outage performance of the NOMA-aided SGF systems with multiple randomly distributed GF users with fixed power and dynamic power schemes. To solve the fairness problem, a cumulative distribution function (CDF)-based user scheduling (CUS) scheme was proposed where the GF user with the maximal CDF value will be admitted to the channel. The analytical expressions for the OP with the CUS and BUS schemes were derived and the impacts of small-scale fading, path loss, and random user locations were jointly investigated.

Recently, physical layer security for NOMA systems has attracted considerable attention [20], [21], [22], [23], [24], [25], [26], [27]. In [20], the authors investigated the secrecy performance of NOMA systems. Stochastic geometry was utilized to model the locations of legitimate and illegitimate receivers and the analytical expressions for the exact and asymptotic secrecy outage probability (SOP) for both single-antenna and multi-antenna scenarios were derived. In [21], the authors investigated the optimal decoding order, transmission rates, and power allocation in the design of NOMA systems. Their results indicated that the optimal decoding order would not vary with the secrecy outage constraint in the considered problems and the power allocation ratio to the user must be increased as the secrecy constraint becomes more stringent. In [22], Lv et al. proposed a new NOMA-inspired jamming and forwarding scheme to improve the security of cooperative communication systems and derived the analytical expressions for the lower bound of the ergodic secrecy sum rate (ESSR) and the asymptotic ESSR. Three relay selection schemes were proposed to enhance the secrecy performance of the multi-relay cooperative NOMA systems and the analytical expressions for the exact and asymptotic SOP were derived in [23]. In [24], the authors proposed a novel downlink multi-user transmission scheme to meet the heterogeneous service requirements for the airborne NOMA systems consisting of security-sensitive users and QoS-sensitive users. The scenario where the QoS-sensitive users act as potential internal eavesdroppers was considered. The achievable secrecy rate was maximized through the joint optimization of user scheduling, power allocation, and trajectory design. In [25], two new schemes were proposed to enhance the security of airborne NOMA systems by the single user requiring and multiple users requiring security, respectively, and the effectiveness of the proposed schemes in ensuring secure transmissions were analyzed. In [26], the relationship between the reliability and security of a two-user NOMA system was investigated. Considering different decoding capabilities at eavesdroppers and imperfect SIC, the analytical expressions of the SOP under the reliability outage probability constraint were derived. In [27], the authors investigated the secrecy performance of a NOMA-based MEC system using the hybrid SIC decoding scheme. The latency was minimized by jointly optimizing the power allocation, task allocation, and computational resource allocation. A reinforcement learning-based and a matching-based algorithm were proposed to solve the optimization problems for the single-user and multi-user scenarios.

B. Motivation and Contributions

Based on the authors’ knowledge, there are two main differences between traditional NOMA and SGF schemes: 1) In traditional NOMA systems, all the NOMA users can utilize the resource blocks, such as time slots or subcarriers. In NOMA-based SGF systems, only the selected GF users based on scheduling schemes are allowed to opportunistically gain access to those resource blocks that GB users would exclusively occupy. 2) For the conventional NOMA systems, the static SIC technology, either channel state information (CSI)-based SIC or QoS-based SIC, is utilized to cancel inter-user interference. The method in SGF systems to enhance spectral efficiency is through the hybrid (dynamic) SIC scheme. For these reasons, although the secrecy performance of NOMA systems has been investigated in many works, the results are not applicable to NOMA-based SGF systems. This is the motivation for this work. Technically speaking, it is much more challenging to investigate the secrecy performance with a hybrid (dynamic) SIC scheme than that with a static SIC scheme.

In this work, we investigate a NOMA-aided SGF system with a single GF user, and then the results have been extended to SGF systems with multiple GF users. The main contributions of this paper are summarized as follows.
1) We analyze the secrecy performance of an uplink NOMA-aided SGF system with a single GF user as a benchmark. The analytical expression for the exact SOP of the GF user is derived. To obtain more insights, we derive asymptotic expressions for the SOP of the GF user in the high transmit signal-to-noise ratio (SNR) regime.

2) We further investigate the secrecy performance of NOMA-aided SGF systems with multiple GF users. The analytical expression for the exact and asymptotic SOP with the BUS scheme is developed based on order statistics to facilitate the performance analysis. Monte Carlo simulation results are provided and compared with two different scheduling schemes. The effects of system parameters on the SOP of the considered system are demonstrated and the accuracy of the developed analytical results is verified.

3) In contrast to the metrics, such as OP and ergodic rate, derived in [13], [14], [15], [16], [17], [18], and [19], the secrecy performance of SGF systems is investigated in this work. Note that it is much more challenging to obtain the analytical expressions of the SOP relative to that of the OP for SGF systems, especially in the presence of multiple GF users.

C. Organization

The rest of this paper is organized as follows. Section II describes the considered system model. The SOP of the SGF systems with a single GF user and multiple GF users are analyzed in Sections III and IV, respectively. Section V presents the numerical and simulation results to demonstrate the analysis and the paper is concluded in Section VI. The notations utilized in this paper are summarized in Table I, which is shown at the top of this page.

II. SYSTEM MODEL

A. NOMA-Aided Semi-GF Systems

Consider an uplink SGF system illustrated in Fig. 1, a GB user \( (U_B) \) transmits signals to the BS \( (S) \), and the channel is re-used by \( K \) GF users \( (U_k, k = 1, \cdots, K) \) in SGF mode. In other words, \( U_k \) is allowed to utilize the resource block that would be solely occupied by \( U_B \) employing NOMA technology while \( U_B \)’s QoS experience is the same as when it occupies the channel alone. All the GF users are assumed to transmit signals with the same power \( P_c \) and the channel gains are ordered as \( |h_1|^2 \leq \cdots \leq |h_K|^2 \), where \( |h_k|^2 = \min_{1 \leq k \leq K} \left( \frac{|g_k|^2}{r_k} \right) \) and \( |h_k|^2 = \max_{1 \leq k \leq K} \left( \frac{|g_k|^2}{r_k} \right) \) where \( g_k \) denotes \( U_k \)’s channel coefficient, \( r_k \) denotes the distance between \( U_k \) and \( S \), and \( \alpha \) signifies the path loss exponent. All the channels are assumed to undergo an independent identically and quasi-static Rayleigh fading model. To facilitate performance analysis, it is assumed that all the GF users are located in a small size cluster, such that the distances between \( U_k \) and \( S \) are same \( (r_k = r_F) \).

The received signal at \( S \) is expressed as \( y_B = \sqrt{P_c} h_B x_B + \sqrt{P_c} h_k x_F + n \), where \( P_i \) \( (i \in \{ B, F \}) \) denotes the transmit power, \( |h_B|^2 = \frac{|g_B|^2}{r_B^2} \), \( g_B \) denotes \( U_B \)’s channel coefficient, \( r_B \) denotes the distance between \( U_B \) and \( S \), \( x_F \) is the signals from \( U_i \) with unit power, i.e., \( E| x_F|^2 = 1 \), and \( n \) is the additive white Gaussian noise (AWGN) with zero mean and variance \( \sigma^2 \).

In this work, the BUS scheme is considered, which means the GF user achieving the maximum data rate is scheduled to transmit signals [17], [19]. The admission procedure consists of the following steps [19]: 1) The \( S \) sends pilot signals, 2) Each user estimates its own channel state information (CSI), 3) \( U_B \) feedbacks its transmit SNR, target rate, and CSI to \( S \), 4) The \( S \) calculates \( U_B \)’s decoding threshold and broadcasts \( U_B \)’s effective received SNR and decoding threshold to all GF users, 5) Each GF user calculates its transmit data rate, and 6) Each GF user sets its back-off time, which is a strictly decreasing function of the user’s data rate. Then the GF user with the maximal data rate will be admitted to transmitting through distributed contention control protocol [13].

To ensure the \( U_B \)’s QoS, there must have \( \log_2 \left( 1 + \frac{\rho_B |h_B|^2}{1 + \tau_f |h_B|^2} \right) \geq R_B \), where \( \rho_B = \frac{P_B}{\sigma^2} \), \( R_B \) is the maximal data rate.
denotes the target data of $U_B$ and $\tau \left( |h_B|^2 \right) = \max \{ 0, \tau_B \}$ denotes the maximum interference power tolerated when $U_B$'s signal is decoded during the first stage of SIC [17].

$S$ first broadcasts $\tau \left( |h_B|^2 \right)$ before scheduling. By comparing their received power of GF's signals on $S$ to $\tau \left( |h_B|^2 \right)$, all the GF users are divided into two groups ($S_1$ and $S_{II}$).

- For $U_k \in S_1$ ($1 \leq k \leq |S_1| \leq K$), they experience $\rho_F |h_k|^2 > \tau \left( |h_B|^2 \right)$ with $\rho_F = \frac{\rho_B}{1+\rho_B}$, which will lead to $\log_2 \left( 1 + \frac{\rho_B |h_B|^2}{1+\rho_B |h_B|^2} \right) < R_B$. This signifies that $U_k$'s signals must be decoded before decoding $U_B$'s signals to guarantee that $U_k$'s QoS experience is the same as when it occupies the channel alone. Then, the achievable rate of $U_B$ and $U_k$ are expressed as $R^I_k = \log_2 \left( 1 + \frac{\rho_B |h_B|^2}{1+\rho_B |h_B|^2} \right)$ and $R^{II}_k = \log_2 \left( 1 + \rho_F |h_k|^2 \right)$, respectively.

- For those GF users in $U_k \in S_{II}$ ($1 \leq k \leq |S_{II}| \leq K$), they experience $\rho_F |h_k|^2 < \tau \left( |h_B|^2 \right)$, which will lead to $\log_2 \left( 1 + \frac{\rho_B |h_B|^2}{1+\rho_B |h_B|^2} \right) > R_B$. This signifies that the GF user's signal in this group will be decoded at either the first or the second stage of SIC. Accordingly, $U_k$ will achieve a data rate of $R^I_k = \log_2 \left( 1 + \frac{\rho_B |h_B|^2}{1+\rho_B |h_B|^2} \right)$ or $R^{II}_k = \log_2 \left( 1 + \rho_F |h_k|^2 \right)$. Due to $R^{II}_k > R^I_k$, to achieve the maximum data rate at the GF user, $U_k$'s signal must be decoded during the first stage of SIC [17], [19]. Thus, the achievable rate of $U_B$ and $U_k$ are expressed as $R^I_k = \log_2 \left( 1 + \frac{\rho_B |h_B|^2}{1+\rho_B |h_B|^2} \right)$ and $R^{II}_k = \log_2 \left( 1 + \rho_F |h_k|^2 \right)$, respectively.

Then, the achievable rate of $U_k$ ($1 \leq k \leq K-1$) is expressed as

$$R_k = \begin{cases} R^I_K, & |S_{II}| = 0, \\ R^{II}_K, & |S_{II}| = K, \\ \max \{ R^I_K, R^{II}_K \}, & |S_{II}| = k. \end{cases}$$

It must be noted that only one GF user is selected to access the channel. The grouping stated before is logically grouped for analysis of the achievable rate of the selected GF user. Specifically, the signals from the users in different groups have different decode orders at the base station.

Remark 1: It must be noted the SIC scheme only guarantees that admitting the GF user is transparent to the GB user whose QoS experience is the same as when it occupies the channel alone. In other words, the SIC scheme does not always guarantee no outage for the GB user. Further, the outage of the GB user in this case ($|h_B|^2 < \alpha_B$) does not signify outage of the GF user.

Remark 2: $\tau \left( |h_B|^2 \right) = \max \{ 0, \tau_B \}$ denotes the maximum interference power tolerated when $U_B$'s signals is decoded during the first stage of SIC. Based on the definition of $\tau_B$, it can be observed that $\alpha_B$ is the threshold when $U_B$ occupies the channel alone. Specifically, due to $\tau_B = \frac{|h_B|^2}{\alpha_B} - 1 < 0 \iff |h_B|^2 < \alpha_B$, $\alpha_B$ signifies the reliability threshold when $U_B$ occupies the channel alone. $|h_B|^2 < \alpha_B$ denotes reliability outage occurs on $U_B$ due to the weakness of the GB link and $\tau_B > 0 \iff |h_B|^2 > \alpha_B$ denotes the channels can be shared with $U_F$ under SIC scheme.

In this work, we consider the worst-case security scenario wherein $E$ is equipped with $N$ antennas using maximal ratio combining (MRC) scheme to fully decode the users’ information. Then, the eavesdropping rate is expressed as $R_E = \log_2 \left( 1 + \rho_F |H_E|^2 \right)$, where $|H_E|^2 = \sum_{i=1}^{\infty} |h_{ki}|^2 / |f_{ke}|^2$. $|h_{ki}|^2$ denotes channel coefficient between $k$-th GF user and $i$-th receive antenna at $E$, and $|f_{ke}|^2$ denotes the distance between the GF users and $E$.

B. Statistical Properties of Channel Power Gains

This subsection provides the statistical law of channel power gains, laying the performance analysis foundation. The probability density function (PDF) of $|H|^2$ is expressed as $f_{h_k}(x) = \frac{1}{\Gamma(\alpha)}x^{\alpha-1}e^{-x}$, where $\Gamma(z) = \int_0^\infty e^{-t}t^{z-1}dt$ is the Gamma function as defined by [29, (8.310.1)]. The CDF of $|h_{k,j}|^2$ is expressed as $F_{|h_{k,j}|^2}(x) = \sum_{i=0}^{\infty} \varphi_{i}x^{i-\alpha}$, where $\varphi_{i} = \left( \frac{K}{\alpha} \right)^{i-1} \varphi_{i-1}$, and $\varphi_{i} = \frac{K^{i-1}}{\Gamma(K-i)}$. The joint PDF of $|h_{i,j}|^2$ and $|h_{j}|^2$ ($1 < i < j < K$) is expressed as [17]

$$f_{|h_{i,j}|^2,|h_{j}|^2}(x,y) = \sum_{n=0}^{m} \sum_{m=0}^{n} \varphi_{i}e^{-\varphi_{x}x-\varphi_{y}y}$$

where $\varphi_{i} = \frac{K^{i-1}}{\Gamma(K-i)} \left( \frac{1}{\tau_{e}^{\alpha-1}} \right)^{(i-1)}$, $\varphi_{j} = \frac{K^{j-1}}{\Gamma(K-j)} \left( \frac{1}{\tau_{e}^{\alpha-1}} \right)^{(i-1)}$, $\varphi_{j} = \frac{K^{j-1}}{\Gamma(K-j)} \left( \frac{1}{\tau_{e}^{\alpha-1}} \right)^{(i-1)}$, and $\varphi_{j} = \frac{K^{j-1}}{\Gamma(K-j)} \left( \frac{1}{\tau_{e}^{\alpha-1}} \right)^{(i-1)}$. Then, the joint CDF of $|h_{i,j}|^2$ and $|h_{j}|^2$ ($1 < i < j < K$) is obtained as

$$F_{|h_{i,j}|^2,|h_{j}|^2}(x,y) = \sum_{n=0}^{m} \sum_{m=0}^{n} \varphi_{i}e^{-\varphi_{x}x-\varphi_{y}y}$$
When \( i = 1, j = K \), we obtain

\[
F|h_1|^2,h_K|^2(x,y) = \sum_{n=0}^{K-2} \mu_0 e^{-r_F^p(K-n-1)} x e^{-r_F^p(n+1)y},
\]

and

\[
F|h_1|^2,h_K|^2(x,y) = \sum_{n=0}^{K-2} \left( \mu_1 e^{-r_F^z(x)} + \mu_2 e^{-r_F^y} y \right)
- \mu_3 e^{-(K-n-1)x e^{-r_F^p(n+1)y}},
\]

respectively, where \( \mu_0 = \frac{K!}{(K-2)!} r_F^p \), \( \mu_1 = \frac{\mu_0}{r_F^p K(n+1)} \), \( \mu_2 = \frac{\mu_0}{r_F^p K(n+1)} \), and \( \mu_3 = \frac{\mu_0}{r_F^p K(n+1)} \).

The joint PDF and CDF of \( |h_k|^2 \), \( |h_{k+1}|^2 \) (1 \( \leq k \leq K - 2 \)), and \( |h_K|^2 \) is given as [17]

\[
f|h_k|^2,h_{k+1}|^2,h_K|^2(x,y,z) = \sum_{n=0}^{K-2-k-1} m \sum_{n=0}^{K-2-k-1} m \sum_{i=1}^{k-6} e^{-(A_i x + B_i y + C_i z + W_i w)},
\]

and

\[
F|h_k|^2,h_{k+1}|^2,h_K|^2(x,y,z,w)
\]

respectively, where \( s_0 = \frac{K!}{(K-n-1)!} r_F^p \), \( A_0 = r_F^p (m+1), B_0 = r_F^p K(n-1), C_0 = r_F^p (n+1), W_0 = B_0 + C_0, s_2 = r_F^p, s_3 = r_F^p, s_4 = r_F^p, W_0 = B_0 + C_0, s_5 = r_F^p, A_1 = A_3 = A_0 = 0, A_2 = A_4 = A_6 = A_0, B_1 = B_3 = B_5 = A_0, B_2 = B_4 = B_0 = 0, C_1 = C_2 = B_0, C_3 = C_4 = 0, C_5 = C_6 = W_0, W_1 = W_2 = C_0, W_3 = W_4 = W_0, W_5 = W_0 = 0.

For \( k = K - 1 \), we have \( |h_{k+1}|^2 = |h_K|^2 \), the joint PDF and CDF of \( |h_{K-1}|^2 \) and \( |h_K|^2 \) are expressed as

\[
f|h_{K-1}|^2,h_K|^2(x,y) = \sum_{n=0}^{K-2} \mu_0 e^{-C_n x e^{-r_F^p y}},
\]

and

\[
F|h_{K-1}|^2,h_K|^2(x,y,z,w)
\]

respectively, where \( a_1 = a_4 = 0, a_2 = a_3 = C_0, b_1 = b_4 = C_0, b_2 = b_3 = 0, c_1 = c_2 = 0, c_3 = c_4 = r_F^p, q_1 = q_2 = r_F^p, \) and \( q_3 = 0 = 0 \).

### III. Secrecy Outage Probability Analysis With a Single Grant-Free User

In this section, the secrecy performance of the SFG systems with a single GF user is investigated to pay the road to the performance analysis of SFG systems with multiple GF users. When \( K = 1 \), there is no need to consider scheduling. It must be noted that this scenario can also be viewed as the multiple-GF-user SFG systems using a random user scheduling (RUS) scheme. The achievable rate of \( U_F \) in (1) is rewritten as

\[
R_F = \begin{cases} R_{U_F}^1, & \rho_F |h_F|^2 > \tau \left( |h_B|^2 \right), \\ R_{U_F}^{II}, & \rho_F |h_F|^2 < \tau \left( |h_B|^2 \right). \end{cases}
\]

where \( R_{U_F}^1 = \log_2 \left( 1 + \frac{\rho_F |h_F|^2}{1 + \rho_F |h_B|^2} \right) \) and \( R_{U_F}^{II} = \log_2 \left( 1 + \rho_F |h_F|^2 \right) \), which denote the achievable rate at \( U_F \) in scenarios when \( U_F \)'s signal is decoded at the first and second stages of the SIC, respectively. It must be noted that when there is an outage on \( U_B \), the \( U_F \)’s signals must be decoded at the first stage of the SIC.

The user \( U_I \)'s achievable secrecy rate is expressed as \( R_{S_{I,F}}^i = [R_{I} - R_{B}] \) [31], where \( j \in \{ F, B \}, i \in \{ I, II \} \) and \( [x] = \max \{ x, 0 \} \). \( \rho \) denotes the probability that the maximum achievable secrecy rate is less than a target secrecy rate [31]. Based on (10), the SOP for \( U_F \) is given as

\[
P_{out,F} = \text{Pr} \left\{ R_{S_{I,F}}^1 < R_{th}, \rho_F |h_F|^2 > \tau \left( |h_B|^2 \right) \right\} + \text{Pr} \left\{ R_{S_{I,F}}^{II} < R_{th}, \rho_F |h_F|^2 < \tau \left( |h_B|^2 \right) \right\}.
\]

where \( R_{th} \) represents the secrecy threshold rate, \( P_{out,F}^i \) denotes \( U_F \)'s signal is decoded at the first stage, and \( P_{out,F}^{II} \) denotes \( U_F \)'s signal is decoded at the second stage.

Similarly, the SOP for \( U_B \) is expressed as

\[
P_{out,B} = \text{Pr} \left\{ R_{S_{I,B}}^1 < R_{th}, \rho_F |h_F|^2 > \tau \left( |h_B|^2 \right) \right\} + \text{Pr} \left\{ R_{S_{I,B}}^{II} < R_{th}, \rho_F |h_F|^2 < \tau \left( |h_B|^2 \right) \right\}.
\]

The analysis of the secrecy outage probability of the GB user is similar to that of the GF user, expressed in Eq. (11). Due to space limitations, the analysis of the \( U_B \)'s secrecy outage probability is regrettably omitted here. In this work, the SOP of the NOMA-aided SFG system is equivalent to the SOP of the GF user, unless stated otherwise.

**Remark 3:** It must be noted that \( \rho \) affects the SNR/SINR of \( U_B \) and the maximum interference that \( U_B \) can tolerate when \( U_I \)'s signal is decoded during the first stage of SIC simultaneously. In the lower-\( \rho_B \) region, the signals from \( U_F \) must be decoded in the first stage of SIC. With the increase of \( \rho_B \), the interference to \( U_F \) increases and the secrecy performance worsens. In the larger-\( \rho_B \) region, the signals from \( U_F \) will be decoded in the second stage of SIC. There is no interference from \( U_B \) to \( U_F \). Then, the SOP decreases to a constant. Thus, there is a worst \( \rho_B \) for the security of \( U_F \).

**Remark 4:** In contrast, \( \rho_B \) affects the SNR/SINR of \( U_F \) and \( \rho \) simultaneously. In the lower-\( \rho_B \) region, the signals from \( U_B \) will be decoded in the first stage of SIC. For a small \( \rho_B \), there is

\[
\text{Pr} \left\{ \rho_F |h_F|^2 > \tau \left( |h_B|^2 \right) \right\} > \text{Pr} \left\{ \rho_B |h_B|^2 \right\}.
\]

Thus, \( P_{out}^{III} \) is the main part of \( P_{out} \) in the lower-\( \rho_B \) region while \( P_{out}^{II} \) is the main part of \( P_{out} \) in the larger-\( \rho_B \) region. Based on the results in [32],
increasing $\rho_F$ will enhance the security of $U_F$ in the lower-$\rho_F$ region. In the larger-$\rho_F$ region, the signals from $U_F$ will be decoded in the first stage of SIC. Although both the SNIR of $U_F$ and SNR of $E$ improve with increasing $\rho_F$, the SNIR of $U_F$ improves slower than the SNR of $E$, so the security of the SGF system deteriorates. Thus, there is an optimal $\rho_F$ to minimize the SOP of $U_F$.

Remark 5: Furthermore, the effect from $r_B$ on $P_{\text{out}}^1$ ($P_{\text{out}}^{1,2}$) is the opposite of the effect from $\rho_B$, while the effect of $\rho_B$ and $r_B$ on the secrecy performance of the SGF systems are similar. $r_B$ only affects the INSR/SNR of $U_F$. Larger $r_B$ denotes stronger path loss on $U_F$ thereby higher SOP. $r_E$ only affects the SNR of $E$ where larger $r_E$ denotes stronger path loss on $E$ and hence lower SOP.

The following theorem provides an exact expression for the SOP achieved applicable to the considered SGF scheme. All the proof in detail can be found in the online version [33].

**Theorem 1:** The SOP of $U_F$ is expressed as

$$P_{\text{out}} = \begin{cases} P_{\text{out}}^{1,1} + P_{\text{out}}^{1,2} + P_{\text{out}}^{1,3}, & \varepsilon_B < 1, \\ P_{\text{out}}^{1,1} + P_{\text{out}}^{1,2} + P_{\text{out}}^{1,3}, & \varepsilon_B < 1, \end{cases}$$

where

$$P_{\text{out}}^{1,1} = 1 - e^{-r_\alpha \rho_B} - \frac{r_B}{r_E} e^{-\frac{r_B}{r_E} N_\alpha \lambda \Gamma(N) \epsilon_1},$$

$$P_{\text{out}}^{1,2} = e^{-r_\alpha \rho_B} + \frac{r_B}{r_E} e^{-\frac{r_B}{r_E} N_\alpha \lambda \Gamma(N) \epsilon_1} - e^{-\frac{r_B}{r_E} N_\alpha \lambda \Gamma(N) \epsilon_1},$$

$$P_{\text{out}}^{1,3} = \frac{r_B}{r_E} e^{-\frac{r_B}{r_E} N_\alpha \lambda \Gamma(N) \epsilon_1} - \frac{r_B}{r_E} e^{-\frac{r_B}{r_E} N_\alpha \lambda \Gamma(N) \epsilon_1},$$

$$P_{\text{out}}^{1,4} = \frac{r_B}{r_E} e^{-\frac{r_B}{r_E} N_\alpha \lambda \Gamma(N) \epsilon_1} - \frac{r_B}{r_E} e^{-\frac{r_B}{r_E} N_\alpha \lambda \Gamma(N) \epsilon_1}.$$

**Remark 6:** Based on (20), one can observe that $\Pr \{\rho_F | h_F^2 > 0\}$, which is independent of $\rho_F$. With the help of the result in [32], secrecy capacity improves with increasing transmit SNR then gradually tends to a constant. So, $P_{\text{out}}$ decreases and gradually tends to a constant for a given $\alpha_B$. Furthermore, $\Pr \{h_F^2 > \frac{\rho_F}{\rho_F}\}$ increases gradually tending to 1 with increasing $\rho_F$. Thus, for a given $\alpha_B$, $P_{\text{out}}^{1,2}$ increases with increasing $\rho_F$ until gradually tending to a constant and independent of $\rho_F$.

**Remark 7:** Based on (22), it must be noted that the relationship between $\omega_0\left|h_B^2|^2\right|E_F^2\right|$ and $\frac{\omega_0}{\rho_F}$ act as the constraint for the GF link. More specifically, the former is constraint on security while the latter is constraint on decoding order. The relationship between constraint on security and on decoding order directly affects the SOP of $U_F$.

**Remark 8:** The analysis in (23) demonstrates that SOP of $U_F$ depends on the relationship between $\varepsilon_B \epsilon_B \theta$ and 1, which determines the relationship between the constraint on decoding order and the constraint on security. When $\varepsilon_B \epsilon_B \theta < 1$, the constraint on decoding order is always less than that on security, $\varepsilon_B \epsilon_B \theta < 1$ means that $R_F$ needs to be small for a given $R_B$, which is a generalized condition in practice since SIC is invoked to encourage spectrum sharing between a GB user and a GF user with a low secrecy threshold data rate. However, for $\varepsilon_B \epsilon_B \theta > 1$, it also offers secrecy outage performance achieved by the SGF scheme will be worse.

The analytical expression provided in (13) is complicated because many factors affect the secrecy performance of the GF user, specifically, the decoding order, the target data rate of $U_B$, the target secrecy rate of $U_F$, and the quality of the eavesdropping channel. We derive asymptotic expressions of the SOP in the high transmit SNR regime to obtain more insights.

**Corollary 1:** When $\rho_B \to \infty$, the asymptotic SOP of $U_F$ is approximated as

$$P_{\text{out}}^{\rho_B \to \infty} \approx 1 - e^{-r_\alpha \rho_B} \left(1 + \left(\frac{r_F}{r_E}\right)^\alpha \theta \right)^{-N}.$$  

**Proof:** See Appendix B.

**Remark 9:** The increasing $\rho_B$ leads to larger $\tau\left|h_F^2|^2\right|E_F^2\right|$, which means it is easy to guarantee the QoS of $U_B$. Then, the probability of decoding the $U_F$’s signals in the second stage of SIC increases. Thus, $P_{\text{out}}^{\rho_B \to \infty} \approx \Pr \left\{R_B^1 < R_{th}\right\}$, which simply depends on $\rho_F$, $R_{th}$, $r_F$, and $N$.

**Corollary 2:** When $\rho_F \to \infty$, the asymptotic SOP of $U_F$ is approximated as

$$P_{\text{out}}^{\rho_F \to \infty} \approx 1 - \left(\frac{r_F}{r_E}\right)^\alpha \theta \right)^{-N}.$$  

**Proof:** See Appendix B.

**Remark 10:** The increasing $\rho_F$ leads to $\Pr \left\{\rho_F | h_F^2 \right\} < \tau\left|h_B^2|^2\right|E_B^2\right| \to 0$, which leads to $P_{\text{out}} \to 0$. Then, the probability of decoding the $U_F$’s signals in the first stage of SIC increases. Thus, $P_{\text{out}}^{\rho_F \to \infty} \approx \Pr \left\{R_B^1 < R_{th}\right\}$, which depends on $\rho_B$, $R_{th}$, $r_F$, $r_E$, and $N$.

**Corollary 3:** When $\rho_B = \rho_F \to \infty$, the asymptotic SOP of $U_F$ is approximated as

$$P_{\text{out}} = P_{\text{out}}^{\infty} + P_{\text{out}}^{\infty} \approx 1 - \left(1 + \left(\frac{r_F}{r_E}\right)^\alpha \theta \right)^{-N} \times \left(1 + \theta \left(\frac{r_F}{r_E}\right)^\alpha + \varepsilon_B \theta \left(\frac{r_F}{r_E}\right)^\alpha\right)^{-N}.$$  

![Image]

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
Proof: See Appendix B.

Remark 11: In this scenarios with \( \rho_B = \rho_F \to \infty \), it must be noted that \( \Pr\left\{ h_F^2 < \frac{|\beta|^2}{\epsilon_B} \right\} = 1 \).

The decoding order depends on the relationship between \( |\beta|^2 \) and \( |\beta|^2 \). Then, we have \( P_{out}^{\infty} = \Pr\left\{ R_k < R_{th}, |h_F|^2 > \frac{|\beta|^2}{\epsilon_B} \right\} \) and \( P_{out}^{\infty} = \Pr\left\{ R_k^H < R_{th}, |h_F|^2 > \frac{|\beta|^2}{\epsilon_B} \right\} \) which are constants independent of \( \rho_B \) and \( \rho_F \) depends on \( R_B, R_{th}, R_F, r_F, \) and \( r_E \).

IV. Secrecy Outage Probability Analysis With Multiple-Grant-Free Users

In this section, the secrecy performance of the multiple-GF-user SG systems with BUS scheme is investigated.

A. Secrecy Outage Probability Analysis

When \( K > 1 \), both user scheduling and decoding order issues should be considered simultaneously. It should be noted that \( |S_{II}| = K \) denotes that the signals from GF users should be decoded on the secondary stage of SIC to maximize the achievable rate. Based on (1), the SOP of \( U_k \) is given by

\[
P_{out} = \Pr \left\{ R_k^H < R_E < R_{th}, |S_{II}| = 0 \right\} \\
= P_{out,1} + P_{out,2} + P_{out,3} \\
\leq P_{out,1} + P_{out,2} + P_{out,3} \\
= \sum_{k=1}^{K-1} \Pr \left\{ \max \left\{ R_k^H, R_k^E \right\} < R_{th}, |S_{II}| = k \right\},
\]

where \( P_{out,1} \) and \( P_{out,2} \) denotes the SOP for \( U_k \) when groups \( S_{II} \) and \( S_I \) are empty, respectively, and \( P_{out,3} \) denotes the SOP for \( U_k \) when there are \( K \) GF users in groups \( S_{II} \). In the first two terms, \( U_K \) is always selected to transmit signals. The following theorem provides the exact expression for the SOP of the considered SG scheme with multiple GF users. All the proofs in detail can be found in the online version [33].

Theorem 2: The SOP of \( U_F \) is expressed as

\[
P_{out} = \begin{cases} 
P_{out,1}^1 + P_{out,1}^{21} + P_{out,2} + P_{out,3}, \quad \epsilon_B \leq \epsilon < 1, \\ P_{out,2} + P_{out,1} + P_{out,2} + P_{out,1}^{22}, \quad \epsilon_B > \epsilon > 1, \\ \end{cases}
\]

where \( P_{out,1}^{1} = 1 - \epsilon - e^{-\frac{h_F^2}{\epsilon_B}} - \epsilon - e^{-\frac{h_F^2}{\epsilon_B}} - e^{-\frac{h_F^2}{\epsilon_B}} \), and \( P_{out,2}^{22} \)

Proof: See Appendix C.

Remark 12: It can be observed that the number of the users in Groups I and II depends on the relationship between \( |h_k|^2 \) and \( \frac{\rho_B}{\rho_F} \).

Relative to SG systems with a single GF user, the expression of SOP presented in Theorem 2 is exceptionally complicated, and the main reason is that in addition to the factors highlighted in Theorem 1, the number of users in each group has a significant effect on the secrecy performance.

B. Asymptotic Secrecy Outage Probability Analysis

To obtain more insights, we derive asymptotic expressions of the SOP in the high transmit SNR regime.

Corollary 4: When \( \rho_B = \rho_F \to \infty \), the SOP of \( U_k \) is approximated at high SNR as

\[
P_{out}^\infty \approx P_{out,1}^{22} + P_{out,2}^{22} + P_{out,3}^{22},
\]

where \( P_{out,1}^{22} \approx \sum_{k=1}^{K-1} \frac{\epsilon_B^k}{K^{\frac{k-1}{2}}} + \frac{\epsilon_B^k}{K^{\frac{k-1}{2}}} \), and \( P_{out,2}^{22} \approx \sum_{k=1}^{K-1} \frac{\epsilon_B^k}{K^{\frac{k-1}{2}}} + \frac{\epsilon_B^k}{K^{\frac{k-1}{2}}} \).
Remark 13: Based on Corollary 4, it must be noted that there is $\Pr \left\{ \rho_F | h_k |^2 < \tau \left( | h_B |^2 \right) \right\} = \Pr \left\{ | h_k |^2 < \frac{| h_B |^2}{\tau} \right\}$.

The number of the users in Groups I and II depends on the relationship between $\frac{| h_k |^2}{\tau}$ and $\frac{| h_B |^2}{\tau}$. More specifically, $P_{\text{out,3}}$ depends on $R_B$, $R_f$, $r_B$, $r_F$, $r_{E}$, and $K$. Further, $P_{\text{out,3}}$ is the main part of the SOP.

Remark 14: Based on Corollary 4, one can observe that when $\rho_B = \rho_F \rightarrow \infty$, the SOP of the SGF systems with multiple GF users is a constant, which depends on $R_B$, $R_f$, $r_B$, and $r_F$. This is because the secrecy performance of the considered SGF systems, such as the target rate of $U_B$, the secrecy threshold rate of $U_F$, and the distance between the transmitters and receivers.

V. NUMERICAL RESULTS AND DISCUSSIONS

This section presents Monte-Carlo simulations and numerical results to prove the secrecy performance analysis on the NOMA-aided SGF systems through varying parameters, such as transmit SNR, target data rate, and the number of antennas, etc. The main parameters are set as $R_{th} = 0.1$ bps/Hz, $R_B = 0.9$ bps/Hz, $N = 2$, $\alpha = 2.2$, $r_B = r_F = r_{E} = 10$ m, unless stated otherwise. In all the figures, “Sim”, “Ana”, and “Asy” denote the simulation, numerical results, and asymptotic analysis respectively. The results in all the figures demonstrate that the analytical results perfectly match the simulation results, verifying our analysis’s accuracy.

A. SOP of the NOMA-Aided SGF System With a Single-GF-User

Fig. 2 demonstrates the SOP of the single-GF-user NOMA-aided SGF system with varying $\rho_B$. One can easily observe that the SOP increases initially and subsequently decreases with increasing $\rho_B$. This is because $\alpha_B$ decreases as $\rho_B$ increases, then the probability that the signals from $U_F$ are decoded first decreases for a given $\rho_F$. In the lower-$\rho_B$ region,
Fig. 4. SOP of the single-GF-user NOMA-aided SGF system with respect to $\epsilon_B\epsilon_{th}$ under increasing $\rho_B = \rho_F$.

Fig. 5. SOP of the multiple-GF-user NOMA-aided SGF system experiencing $\rho_F = 10$ dB.

(1) SOP for varying $K$.

(2) SOP for varying $R_{th}$ and $R_B$.

Fig. 6. SOP of the multiple-GF-user NOMA-aided SGF system experiencing $\rho_B = 10$ dB.

...
Fig. 7. SOP of the multiple-GF-user NOMA-aided SGF system versus varying $\rho_B = \rho_F$.

Fig. 8. SOP of the multiple-GF-user NOMA-aided SGF system for different user scheduling schemes with $\rho_B = \rho_F = 5$ dB.

There is an optimal transmit SNR depending on $R_B$ and $R_{th}$ to obtain the minimum SOP in these scenarios.

B. SOP of the NOMA-Aided SGF System With Multiple GF Users

Figs. 5 and 6 demonstrate the impact of various $K$, $R_B$, and $R_{th}$ on SOP of $U_F$. As can be observed from the figure, with the increase of $\rho_B$, SOP first increases and then decreases to a constant depending on $K$ and $R_{th}$. Moreover, with an increase in $K$, the SOP improves since the better GF user is selected to access the channel, enhancing the secrecy performance. Based on Figs. 5 and 6, one can observe that the effect of the transmit SNR, $\rho_B$, and $\rho_F$, on the SOP with multiple GF users is similar to that in Figs. 2 - 3 with a single GF user.

Fig. 7 plots the effects of varying $K$, $R_B$, $R_{th}$, and $N$ on SOP versus varying $\rho_B = \rho_F$. One can observe that the curves of SOP in these scenarios are similar to those demonstrated in Fig. 4. Moreover, from Fig. 5(c), one can observe that SOP of $U_F$ becomes worse until it tends to be a constant depending on $N$. This can be explained by the fact that weakening diversity at $E$ implies a better security performance of the considered SGF system.

Comparing Figs. (2) and (5), (3) and (6), one interesting conclusion can be drawn that the transmit power of the GF and GB users has an opposite impact on the GF user’s secrecy performance. From the point of view of security of GF users, there exists an optimal $P_F$ and a worst $P_B$.

Fig. 8 demonstrates the NOMA-aided SGF system for different user scheduling schemes with varying $r_B$, $r_F$, and $r_E$. From Fig. 8(a), one can observe that the SOP increases initially and subsequently decreases with increasing $r_B$. The achievable rate for $U_F$ decreases with increasing $r_B$ thereby the secrecy performance deteriorates. As the $r_B$ increases, $\tau_B$ increases, whereas the probability of decoding signals from $U_F$ during the second stage of SIC increases. Thus, security of $U_F$ with all the schemes is enhanced. Figs. 8(b) and 8(c) demonstrate that $r_F$ and $r_E$ have an opposite impact on the GF user’s secrecy performance, which is easy to follow. Furthermore, the BUS scheme obtains the best security while the RUS scheme obtains the worst secrecy performance. This is because the GF user with maximum data rate is scheduled to transmit signals in the BUS scheme while a GF user is selected randomly in the RUS scheme. Moreover, it can be observed that the difference between the secrecy performance with the BUS and CUS schemes is minor in the lower/larger-$r_B$ region (Fig. 8(a)) and lower/larger-$r_F$ (Fig. 8(b)). The reason is as follows. The CUS scheme is proposed to solve the fairness between GF users due to the difference in path loss in each group. In the scenarios with lower/larger-$r_B$ region (Fig. 8(a)) or lower/larger-$r_F$ (Fig. 8(b)), the GF users belong to the same group with high probability. Assuming the same distance between the GF user and the base station, the user with the maximum power gain leads to the maximum rate. Thus, the secrecy performance with BUS and CUS schemes is equal.

VI. CONCLUSION

In this paper, we investigated the secrecy outage performance of the NOMA-aided SGF systems. With the premise
that GF users are entirely transparent for GB users, we first analyzed the NOMA-aided SGF system with a single GF user. Subsequently, the secrecy performance of NOMA-aided SGF systems with multiple GF users was investigated. The effects of all the parameters, such as the target data rate of GB users, the secrecy threshold rate of GF users, and transmit powers on GB and GF users, were discussed. Monte-Carlo simulation results were presented to validate the correctness of the derived analytical expressions.

SIC and CSI are assumed to be perfect in this work, which is a typical assumption in many works, like [10], [11], [12], [13], [14]. An exciting direction for future research is investigating the performance of NOMA-aided SGF systems with imperfect SIC and CSI. In this work, it assumed that all users transmit at fixed power. However, the results in [18] and [19] showed that the system performance could be enhanced by carefully adjusting the transmit power of the GF and GB users.

As we analyzed previously, there exists an optimal $P_F$ and a worst $P_B$ for the security of GF users. Thus, analyzing the secrecy performance of the NOMA-based SGF systems wherein both the transmit powers of the GB and GF users are dynamically adjusted in a coordinated manner will be exciting subsequent work. To facilitate performance analysis, it is assumed that all the GF users are located in a small cluster, such that the distances between GF users and the base station are the same. Another interesting problem is analyzing the performance of NOMA-aided SGF systems with multiple randomly distributed GB users, GF users, and eavesdroppers via stochastic geometry. Furthermore, machine-type GF users in mMTC applications often have small data packets. Fairness is another issue that is as important as security. Analyzing the secrecy performance of NOMA-based SGF systems for short-packet transmission with the different user scheduling schemes also is an exciting problem.

**APPENDIX A**

**PROOF OF THEOREM 1**

### A. Derivation of $P_{out}^{1}$

Based on the definition of $\tau \left( |h_B|^2 \right)$, $P_{out}^{1}$ is expressed as

$$P_{out}^{1} = \Pr \left\{ R_s^{pl} < R_{th}, |h_B|^2 < \alpha_B \right\}$$

Substituting (10) into (20) and after some algebraic manipulations, we obtain (21), shown at the bottom of the page, where

$$\omega_1(a, b, c) = \frac{h^{N-1}(N)}{a^N} \left( \Gamma (1 - N, \frac{bc}{a}) - \Gamma (1, N, b\alpha_B + \frac{bc}{a}) \right) = \Gamma (1 - \frac{\varepsilon_{th}}{\tau_B}, \frac{\varepsilon_{th}}{\tau_B} = \theta_{th} - 1, \theta_{th} = 2R_B, \quad \lambda_1 = r_B^\frac{\varepsilon_{th}}{\tau_B} \theta_{th}, \lambda_2 = r_B^\frac{\varepsilon_{th}}{\tau_B} \theta_{th} + r_E^\frac{\varepsilon_{th}}{\tau_B}$$

and $(a)$ is obtained via utilizing [29, (3.83.10)].

Similarly, we obtain

$$P_{out}^{1,2} = \Pr \left\{ |h_F|^2 < \omega_0 \left( |h_B|^2, |H_E|^2 \right), |h_F|^2 > \frac{\tau_B}{\rho_F}, |h_B|^2 > \alpha_B \right\},$$

The relationship between $\omega_0 \left( |h_B|^2, |H_E|^2 \right)$ and $\frac{\tau_B}{\rho_F}$ is expressed as

$$P \left\{ \frac{\tau_B}{\rho_F} < \omega_0 \left( |h_B|^2, |H_E|^2 \right) \right\} = \Pr \left\{ |H_E|^2 > \alpha_1 \right\} + \Pr \left\{ |H_E|^2 < \alpha_1, |h_B|^2 < \alpha_2 \right\},$$

where $\theta_B = 2R_B, \quad \alpha_1 = \frac{1 - \varepsilon_{th}}{\rho_F \theta_{th} \varepsilon_{th} B}, \quad \alpha_2 = \frac{\alpha_3}{\rho_F \theta_{th} \varepsilon_{th} B |H_E|^2 + \varepsilon_1} = \frac{\alpha_3}{\rho_F \theta_{th} \varepsilon_{th} B |H_E|^2 + \varepsilon_1}, \quad \varepsilon_1 = \varepsilon_{th} \theta_{th}$, and $\alpha_3 = \frac{\rho_F \theta_{th} \varepsilon_{th} B}{\rho_F \theta_{th} \varepsilon_{th} B |H_E|^2 + \varepsilon_1}$. Moreover, the relationship $\alpha_1$ and $0$ has important effect on the relationship between $\omega_0 \left( |h_B|^2, |H_E|^2 \right)$ and $\frac{\tau_B}{\rho_F}$.

(i) When $\varepsilon B \varepsilon_{th} < 1$, we have $\alpha_3 > 0$. Then, based on (22), $P_{out}^{1,2}$ is obtained as

$$P_{out}^{1,2} = \Pr \left\{ |h_F|^2 < \omega_0 \left( |h_B|^2, |H_E|^2 \right), |h_F|^2 > \frac{\tau_B}{\rho_F}, |h_B|^2 > \alpha_B \right\} = \frac{e^{-r_B^\frac{\varepsilon_{th}}{\tau_B} \alpha_B} \Gamma (N, r_B^\frac{\varepsilon_{th}}{\tau_B} \alpha_1)}{\varepsilon_2^\frac{\varepsilon_{th}}{\tau_B} \Gamma (N)} + \frac{r_B^\frac{\varepsilon_{th}}{\tau_B} \alpha_B}{\Gamma (N)} \omega_3 \left( \frac{\varepsilon_B \varepsilon_{th}}{\varepsilon_B \varepsilon_{th}}, \frac{\varepsilon_B \varepsilon_{th}}{\varepsilon_B \varepsilon_{th}} \omega_2 \left( \lambda_1, \lambda_2, \lambda_3 \right) \right) + \omega_3 \left( \frac{\varepsilon_B \varepsilon_{th}}{\varepsilon_B \varepsilon_{th}}, \frac{\varepsilon_B \varepsilon_{th}}{\varepsilon_B \varepsilon_{th}} \omega_2 \left( \lambda_1, \lambda_2, \lambda_3 \right) \right) \Gamma (N),$$

where

$$\omega_2 \left( a, b, c \right) = \int_{a}^{\infty} e^{-xy} e^{-c} dx dy = \frac{b^N - 1}{a} \Gamma (1 - N, N, b \alpha_B + \frac{bc}{a}) - e^{-b \alpha_B} \Delta,$$

$$\Delta =$$
introduction
(b) holds by applying \([29, (3.383.10)]\), \(\omega_3 (a, b, c) = \int_0^{\alpha_n} F_n y^{-1} e^{-a y - b x - c y} d x d y (d) \), \(\frac{\Gamma(1 - N, b, a)}{\alpha_n} \), and \((d)\) holds by \([29, (3.383.10)]\) and applying Gaussian-Chebyshev quadrature \([34, (25.4.30)]\), \(R \) and \(L \) is the summation item, which reflects accuracy vs. complexity, \(e = \cos \left(\frac{2\pi - \pi}{2} \right), \) \(h_e \) = \(2L \), \(\ell_t = \cos \left(\frac{2\pi + \pi}{2} \right), \) and \(v_t = \frac{\pi}{2} \). (ii) When \(\ell_B \leq \ell_t \), it has \(\alpha_n < 0 \), then,\[ \Pr \left[ \left| h_B \right|^2 < \omega_0 \left( \left| h_B \right|^2, \left| H_E \right|^2 \right) \right] = \Pr \left[ \left| H_E \right|^2 > \alpha_n \right] = 1. \]Thus, \(P_{out}^{1,2} \) is expressed as\[ P_{out}^{1,2} = \Pr \left[ \left| h_F \right|^2 < \omega_0 \left( \left| h_B \right|^2, \left| H_E \right|^2 \right), \left| h_B \right|^2 > \alpha_n \right] \leq \varepsilon_2, \quad (25) \]where \(\omega_4 (a, b, c) = \int_0^{\infty} \int_0^{\infty} \int_0^{\infty} y^{-1} e^{-a y - b x - c y} d x d y - 1 \). Based on \((11)\), \(P_{out}^{1,2} \) is approximated as\[ P_{out}^{1,2} \approx \Pr \left[ \frac{r_F}{r_E} < \left( \left| h_B \right|^2, \varepsilon B \right) \right] \leq \frac{1}{1 + \varepsilon B} \frac{r_E}{r_F}. \quad (31) \]where \((f)\) holds by applying \([29, (3.383.10)]\) and \(\Gamma (a, x) \xrightarrow{x \to \infty} 0 \). Based on \((28)\), \(P_{out}^{1,2} \) is approximated as\[ P_{out}^{1,2} \approx \Pr \left[ \frac{r_F}{r_E} < \left( \left| h_B \right|^2, \varepsilon B \right) \right] \leq \frac{1}{1 + \varepsilon B} \frac{r_E}{r_F}. \quad (32) \]APPENDIX C

Proof of Theorem 2

1) Derivation of \( P_{out,1} \)

Based on \((17)\) and \(\Pr \left[ \tau \left( \left| h_B \right|^2 \right) < 0 \right] = 0 \), \(P_{out,1} \) is rewritten as\[ P_{out,1} = 0. \]
where $|h_B|^2 < \alpha_B$ denotes $U_B$ is reliability outage. Utilizing [29, (3.383.10)], we obtain

$$P_{out,1} = \Pr \left\{|h_B|^2 < \omega_0 (|h_B|^2, |H_E|^2) ; |h_B|^2 < \alpha_B \right\}$$

$$= 1 - e^{-r_B^2 \alpha_B} + \sum_{i=0}^{K} \frac{\phi r_B^2 r_{\nu E}^N}{\Gamma (N)} (i \lambda_1, \varepsilon_3, \varepsilon_4),$$

(34)

where $\varepsilon_4 = \nu r_B^2 \alpha_B r_B r_{\nu E}^b$ and $\varepsilon_4 = \nu r_B^2 \theta_B + r_{\nu E}^b$. Similarly, $P_{out,1}$ is expressed as (35), shown at the bottom of the next page.

Considering $|h_1|^2 \leq \cdots \leq |h_K|^2$ and the relationship between $\omega_0 (|h_B|^2, |H_E|^2)$ and $\frac{\nu r_B^2}{r_E}$, given in (23), two scenarios ($\varepsilon_B e_{th} < 1$ and $\varepsilon_B e_{th} > 1$) are considered as follows.

(i) When $\varepsilon_B e_{th} < 1$, we have $\alpha_1 > 0$. Due to $\alpha_B < \alpha_2$, based on (23), we obtain (36), shown at the bottom of the next page.

Based on (5), we obtain (37), shown at the bottom of the next page, where $\alpha_4 = \frac{K r_B^2}{\nu r_B^2} + r_{\nu E}^b$, $\eta_1 = K r_B^2 \rho_B \theta_B$, $\eta_2 = K r_B^2 \rho_B \alpha_B + r_{\nu E}^b$, $\eta_3 = K r_B^2 \rho_B \theta_B + r_{\nu E}^b$, $\eta_4 = C \rho_B \theta_B$, $\eta_5 = C \rho_B \alpha_B + r_{\nu E}^b$, and $\eta_6 = C \rho_B \theta_B + r_{\nu E}^b$. Similarly, we obtain (38), shown at the bottom of the next page.

(ii) When $\varepsilon_B e_{th} > 1$, we have $\alpha_1 < 0$, then

$$\Pr \left\{ \frac{\nu r_B^2}{r_E} < \omega_0 (|h_B|^2, |H_E|^2) \right\} = 1.$$ Thus, we obtain (39), shown at the bottom of the next page.

2) Derivation of $P_{out,2}$

When $|S_{II}| = K$, $U_B$'s signal must be decoded during the first stage of SIC and the signals of all the GF users will be decoded in the second stage of SIC. Utilizing the best-user scheduling scheme, $U_K$ will be selected. Then, with some simple algebraic manipulations, the SOP in this case is expressed as (40), which is shown at the bottom of the next page.

3) Derivation of $P_{out,3}$

When both $S_I$ and $S_{II}$ are not empty, SOP is expressed as

$$P_{out,3} = \sum_{k=1}^{K-2} \Pr \left\{ \max \left\{ R_{K}, R_{K-1} \right\} - R_E < R_{th}, |S_{II}| = k \right\}$$

$$+ \Pr \left\{ \max \left\{ R_{K}, R_{K-1} \right\} - R_E < R_{th}, |S_{II}| = K-1 \right\}.$$
APPENDIX D
PROOF OF COROLLARY 4

When \( \rho_F = \rho_B \to \infty \), we have \( \alpha_B \to 0, \alpha_{th} \to 0 \). One can obtain \( P_{out,1}^1 \approx 0 \) due to \( \Pr \{ |h_B|^2 < \alpha_B \} \approx 0 \). Based on (35) and (36), \( P_{out,1}^2 \) is approximated as

\[
P_{out,1}^2 \approx \Pr \left\{ \frac{|h_B|^2}{\varepsilon_B} < |h_1|^2 < |h_K|^2 < \omega_0 \left( \frac{|h_B|^2}{|H_E|^2} \right) \right\}
\]

(47)

where \( g \) holds with the same method as \( f \).

Based on (40), \( P_{out,2} \) is approximated as

\[
P_{out,2}^\infty \approx \Pr \left\{ \left| h_K \right|^2 < \theta_{th} |H_E|^2, |h_B|^2 > \varepsilon_B |H_E|^2 \right\}
= \Pr \left\{ \left| h_K \right|^2 < \frac{|h_B|^2}{\varepsilon_B}, |h_B|^2 < \varepsilon_B |H_E|^2 \right\}
= \sum_{i=0}^{K} \frac{\varphi_i \varepsilon_B}{i + \varepsilon_B} + \sum_{i=0}^{K} \frac{i \varphi_i (i \chi_1 + \chi_2)^N}{i + \varepsilon_B (\frac{\tau_B}{\rho_F})^\alpha},
\]

(48)

where \( \chi_1 = \theta_{th} \left( \frac{\tau_B}{\rho_F} \right)^\alpha \) and \( \chi_2 = \varepsilon_B \theta_{th} \left( \frac{\tau_B}{\rho_F} \right)^\alpha + 1 \).

\[
P_{out,1}^2 = \Pr \left\{ \log_2 \left( 1 + \frac{\rho_F |h_B|^2}{1 + \rho_F |h_B|^2} \right) - \log_2 \left( 1 + \rho_F |H_E|^2 \right) < R_{th}, |h_1|^2 > \frac{\tau_B}{\rho_F}, |h_B|^2 > \alpha_B \right\}
\]

(35)

\[
P_{out,1}^2 = \Pr \left\{ |h_K|^2 < \omega_0 \left( \frac{|h_B|^2}{|H_E|^2} \right), |h_1|^2 > \frac{\tau_B}{\rho_F}, |h_B|^2 > \alpha_B \right\}
\]

(36)

\[
I_1 = \int_{\alpha_B}^{\infty} \int_{\alpha_B}^{\infty} \left( F_{|h_1|^2, |h_K|^2} \left( \frac{\tau_B}{\rho_F}, \omega_0 (x, y) \right) \right) f_{|h_B|^2} (x) f_{|H_E|^2} (y) dy
= \frac{r_B^{\rho_F \alpha_B} \Gamma (N)}{\Gamma (N)} \sum_{n=0}^{K-2} \left( \mu_1 e^{-K r_F^{\alpha_B} \omega_2 (0, \alpha_4, r_E^0)} + \mu_2 e^{-K r_F^{\alpha_B} \alpha_2, \eta_3} - \mu_3 e^{-K r_F^{\alpha_B} \omega_2 (0, \alpha_4, r_E^0) - C_0 \alpha_2, \eta_3} \right)
\]

(37)

\[
I_2 = \int_{\alpha_B}^{\infty} \int_{\alpha_B}^{\infty} \left( F_{|h_1|^2, |h_K|^2} \left( \frac{\tau_B}{\rho_F}, \omega_0 (x, y) \right) \right) f_{|h_B|^2} (x) f_{|H_E|^2} (y) dy
= \frac{r_B^{\rho_F \alpha_B} \Gamma (N)}{\Gamma (N)} \sum_{n=0}^{K-2} \left( \mu_1 e^{-K r_F^{\alpha_B} \omega_3 (0, \alpha_4, r_E^0)} + \mu_2 e^{-K r_F^{\alpha_B} \alpha_2, \eta_3} - \mu_3 e^{-K r_F^{\alpha_B} \omega_3 (0, \alpha_4, r_E^0) - C_0 \alpha_2, \eta_3} \right)
\]

(38)

\[
P_{out,1}^2 = \Pr \left\{ \frac{\tau_B}{\rho_F} < |h_1|^2 < |h_K|^2 < \omega_0 \left( \frac{|h_B|^2}{|H_E|^2} \right), |h_B|^2 > \alpha_B \right\}
\]

(39)

\[
P_{out,2} = \Pr \left\{ |h_K|^2 < \theta_{th} |H_E|^2 + \alpha_{th}, |h_B|^2 > \left( \frac{\rho_F |H_E|^2}{2} + 1 \right) \varepsilon_1 \right\}
+ \Pr \left\{ |h_K|^2 < \frac{\tau_B}{\rho_F}, \alpha_B < |h_B|^2 < \left( \frac{\rho_F |H_E|^2}{2} + 1 \right) \varepsilon_1 \right\}
= \sum_{i=0}^{K} \frac{\varphi_i}{i r_F^{\alpha_B} + r_B^{\rho_F \alpha_B}} \left( \frac{e^{-i r_F^{\alpha_B} \omega_1 + r_B^{\rho_F \alpha_B} \varepsilon_1} + \rho_F \alpha_B r_F^{\alpha_B} e^{-r_B^{\rho_F \alpha_B}}} {i r_F^{\alpha_B} + r_B^{\rho_F \alpha_B} \varepsilon_1 + r_E^0} \right)
\]

(40)
\[ P_{\text{out}, 3}^k = \text{Pr}\left\{ |h_k|^2 < \min\left( \frac{\tau_B}{\rho_F}, \theta th |H_E|^2 + \alpha th \right), |h_B|^2 > \alpha_B \frac{\tau_B}{\rho_F} < |h_{k+1}|^2 < |h_K|^2 < \omega_0 \left( |h_B|^2, |H_E|^2 \right) \right\} \]

\[ = \text{Pr}\left\{ |h_k|^2 < \frac{\tau_B}{\rho_F} < |h_{k+1}|^2 < |h_K|^2 < \omega_0 \left( |h_B|^2, |H_E|^2 \right), \alpha_B < |h_B|^2 < \left( \rho_F |H_E|^2 + 1 \right) \varepsilon_1 \right\} \]

\[ + \text{Pr}\left\{ |h_k|^2 < \alpha th + \theta th |H_E|^2, |h_B|^2 > \left( \rho_F |H_E|^2 + 1 \right) \varepsilon_1, \frac{\tau_B}{\rho_F} < |h_{k+1}|^2 < |h_K|^2 < \omega_0 \left( |h_B|^2, |H_E|^2 \right) \right\} \quad (42) \]

\[ I_3^{\infty} \approx \text{Pr}\left\{ |h_k|^2 < \frac{|h_B|^2}{\varepsilon_B} < |h_{k+1}|^2 < |h_K|^2 < \omega_0 \left( |h_B|^2, |H_E|^2 \right), |h_B|^2 < \varepsilon_B \theta th |H_E|^2 \right\} \]

\[ (h) \sum_{n=0}^{K-k-2} \sum_{m=0}^{k-1} \frac{c_i \varepsilon_B \chi_3}{(K - \varepsilon_k) \left( \frac{\tau_F}{\tau_B} \right) + \varepsilon_B} \quad (49) \]

\[ I_4^{\infty} \approx \text{Pr}\left\{ |h_k|^2 < \theta th |H_E|^2, |h_B|^2 < \varepsilon_B |h_{k+6}^6|, |h_K|^2 < \omega_0 \left( |h_B|^2, |H_E|^2 \right), |h_B|^2 > \varepsilon_B \theta th |H_E|^2 \right\} \]

\[ (i) \sum_{n=0}^{K-k-2} \sum_{m=0}^{k-1} \sum_{j=5}^{6} \frac{c_i \varepsilon_B \chi_3}{(K - k) \left( \frac{\tau_F}{\tau_B} \right) + \varepsilon_B} \]

\[ (50) \]

Based on (42), we obtain (49) and (50), shown at the top of the page, respectively, where \( \chi_3 = \left((K + \varepsilon_k) \chi_1 + \chi_2\right)^{-N} \), (h) and (i) hold with the same method as (f), and \( \varepsilon = [0, 0, n + 2, 1, m + 1 - k, -k] \).

Thus, \( P_{\text{out}, 3}^k \), when \( \rho_F = \rho_B \to \infty \), is approximated as \( P_{\text{out}, 3}^{K, \infty} = \sum_{k=1}^{K-2} (I_3^{\infty} + I_4^{\infty}) \). With the same method and based on (46), \( P_{\text{out}, 3}^{K-1, \infty} \) is approximated as

\[ P_{\text{out}, 3}^{K-1, \infty} \approx \text{Pr}\left\{ R_k^{K-1} < R_{th}, |S_{11}| = K - 1 \right\} \]

\[ = \sum_{n=0}^{K-2} \sum_{j=3}^{4} \frac{(-1)^{j+1} \varepsilon_B}{(\varepsilon_j \frac{\tau_B}{\alpha} + \frac{\tau_F}{\alpha} + \varepsilon_B) \left( \frac{1 - \chi_4}{\varepsilon_j \frac{\tau_B}{\alpha} + \frac{\tau_F}{\alpha} + \varepsilon_B} + \frac{\chi_4}{\varepsilon_k \frac{\tau_B}{\alpha} + \frac{\tau_F}{\alpha} + \varepsilon_B} \right)} , \quad (51) \]

where \( \mu_4 = \frac{K^{(-1)}(K-2)}{(K-2)(n+1)} \) and \( \chi_4 = \left(\frac{\varepsilon_B}{\varepsilon_j \chi_1 + \chi_2}\right)^{-N} \).

REFERENCES

[1] W. Jiang, B. Han, M. A. Habibi, and H. D. Schotten, “The road towards 6G: A comprehensive survey,” IEEE Open J. Commun. Soc., vol. 2, pp. 334–366, 2021.

[2] M. Shirvanimoghaddam et al., “Short block-length codes for ultra-reliable low latency communications,” IEEE Commun. Mag., vol. 57, no. 2, pp. 130–137, Feb. 2019.

[3] M. El-Tanab and W. Hamouda, “An overview of uplink access techniques in machine-type communications,” IEEE Netw., vol. 35, no. 3, pp. 246–251, May/June 2021.

[4] UL Grant-Free Transmission for URLLC, document R1-1705654, 3GPP TSG-RAN WG1 #88, Apr. 2017.

[5] Z. Ma, M. Xiao, Y. Xiao, Z. Pang, H. V. Poor, and B. Vucetic, “High-reliability and low-latency wireless communication for Internet of Things: Challenges, fundamentals, and enabling technologies,” IEEE Internet Things J., vol. 6, no. 5, pp. 7946–7970, Oct. 2019.

[6] J. Choi, J. Ding, N.-P. Le, and Z. Ding, “Grant-free random access in machine-type communication: Approaches and challenges,” IEEE Wireless Commun., vol. 29, no. 1, pp. 151–158, Feb. 2022.

[7] J. Zhang, X. Yao, H. Wu, N. Zhang, and X. Zhang, “Deep reinforcement learning for throughput improvement of the uplink grant-free NOMA system,” IEEE Internet Things J., vol. 7, no. 7, pp. 6369–6379, Jul. 2020.

[8] 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. Sel. Areas Commun., vol. 35, no. 10, pp. 2181–2195, Oct. 2017.

[9] M. B. Shahab, R. Abbas, M. Shirvanimoghaddam, and S. J. Johnson, “Grant-free non-orthogonal multiple access for IoT: A survey,” IEEE Commun. Surv. Tuts., vol. 22, no. 3, pp. 1805–1838, 3rd Quart., 2020.

[10] R. Abbas, M. Shirvanimoghaddam, Y. Li, and B. Vucetic, “A novel analytical framework for massive grant-free NOMA,” IEEE Trans. Veh. Technol., vol. 67, no. 3, pp. 2436–2449, Mar. 2019.

[11] J. Chen, L. Guo, J. Jia, J. Shang, and X. Wang, “Resource allocation for IRS assisted SFG NOMA transmission: A MADRL approach,” IEEE J. Sel. Areas Commun., vol. 40, no. 4, pp. 1302–1316, Apr. 2022.

[12] K. Yang, N. Yang, N. Ye, M. Jia, Z. Gao, and R. Fan, “Non-orthogonal multiple access: Achieving sustainable future radio access,” IEEE Commun. Mag., vol. 57, no. 2, pp. 116–121, Feb. 2019.

[13] Z. Ding, R. Schober, P. Fan, and H. V. Poor, “Simple semi-grant-free transmission strategies assisted by non-orthogonal multiple access,” IEEE Trans. Commun., vol. 67, no. 6, pp. 4464–4478, Jun. 2019.

[14] Z. Yang, P. Xu, J. A. Hussein, Y. Wu, Z. Ding, and P. Fan, “Adaptive power allocation for uplink non-orthogonal multiple access with semi-grant-free transmission,” IEEE Wireless Commun. Lett., vol. 9, no. 10, pp. 1725–1729, Oct. 2020.
[15] C. Zhang, Y. Liu, W. Yi, Z. Qin, and Z. Ding, “Semi-grant-free NOMA: Ergodic rates analysis with random deployed users,” IEEE Wireless Commun. Lett., vol. 10, no. 4, pp. 692–695, Apr. 2021.

[16] C. Zhang, Y. Liu, and Z. Ding, “Semi-grant-free NOMA: A stochastic geometry model,” IEEE Trans. Wireless Commun., vol. 21, no. 2, pp. 1197–1213, Feb. 2022.

[17] Z. Ding, R. Schober, and H. V. Poor, “A new QoS-guarantee strategy for NOMA assisted semi-grant-free transmission,” IEEE Trans. Commun., vol. 69, no. 11, pp. 7489–7503, Nov. 2021.

[18] Y. Sun, Z. Ding, and X. Dai, “A new design of hybrid SIC for improving transmission robustness in uplink NOMA,” IEEE Trans. Veh. Technol., vol. 70, no. 5, pp. 5083–5087, May 2021.

[19] H. Lu, X. Xie, Z. Shi, H. Lei, H. Yang, and J. Cai, “Advanced NOMA assisted semi-grant-free transmission schemes for distributed random users,” IEEE Trans. Wireless Commun., early access, Dec. 14, 2022, doi: 10.1109/TWC.2022.3272555.

[20] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, “Enhancing the physical layer security of NOMA in large-scale networks,” IEEE Trans. Wireless Commun., vol. 16, no. 3, pp. 1656–1672, Mar. 2017.

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

[22] L. Lv, F. Zhou, J. Chen, and N. Al-Dhahir, “Secure cooperative communications with an untrusted relay: A NOMA-inspired jamming and relaying approach,” IEEE Trans. Inf. Forensics Security, vol. 14, no. 12, pp. 3191–3205, Dec. 2019.

[23] K. Lei et al., “Secrecy outage analysis for cooperative NOMA systems with relay selection schemes,” IEEE Trans. Commun., vol. 67, no. 9, pp. 6282–6298, Sep. 2019.

[24] H.-M. Wang and X. Zhang, “UAV secure downlink NOMA transmissions: A users oriented perspective,” IEEE Trans. Commun., vol. 68, no. 9, pp. 5732–5746, Sep. 2020.

[25] N. Zhao et al., “Security enhancement for NOMA-UAV networks,” IEEE Trans. Veh. Technol., vol. 69, no. 4, pp. 3994–4005, Apr. 2020.

[26] H. Lei, R. Gao, K. Park, I. S. Ansari, K. J. Kim, and M.-S. Alouini, “On secure downlink NOMA systems with outage constraint,” IEEE Trans. Commun., vol. 68, no. 12, pp. 7824–7836, Dec. 2020.

[27] K. Wang, H. Li, Z. Ding, and P. Xiao, “Reinforcement learning based latency minimization in secure NOMA-MEC systems with hybrid SIC,” IEEE Trans. Wireless Commun., vol. 22, no. 1, pp. 408–422, Jan. 2023.

[28] Z. Ding, R. Schober, and H. V. Poor, “Unveiling the importance of SIC in NOMA systems—Part II: New results and future directions,” IEEE Commun. Lett., vol. 24, no. 11, pp. 2378–2382, Nov. 2020.

[29] I. S. Gradshteyn and I. M. Ryzhik, Table of Integrals, Series, and Products, 7th ed. New York, NY, USA: Academic, 2007.

[30] S. Verdu, Multiuser Detection. Cambridge, U.K.: Cambridge Univ. Press, 1998.

[31] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[32] H. Lei, I. S. Ansari, G. Pan, B. Alomair, and M.-S. Alouini, “Secrecy capacity analysis over $\alpha$–$\mu$ fading channels,” IEEE Commun. Lett., vol. 21, no. 6, pp. 1445–1448, Jun. 2017.

[33] H. Lei, F. Yang, H. Liu, I. S. Ansari, K. J. Kim, and T. A. Tsiftsis, “On secure NOMA-aided semi-grant-free systems,” 2022, arXiv:2204.08135. [Online]. Available: https://arxiv.org/abs/2204.08135

[34] M. Abramowitz and I. Stegun, Handbook of Mathematical Functions With Formulas, Graphs, and Mathematical Tables, 9th ed. New York, NY, USA: Dover, 1972.

[35] V. S. Adamchik and O. I. Marichev, “The algorithm for calculating integrals of hypergeometric type functions and its realization in REDUCE system,” in Proc. Int. Symp. Symbolic Algbr. Comput., Jul. 1990, pp. 212–224.

[36] M. D. Springer, The Algebra of Random Variables. New York, NY, USA: Wiley, 1979.

[37] P. K. Mittal and K. C. Gupta, “An integral involving generalized function of two variables,” Proc. Indian Acad. Sci.-Sect. A, vol. 75, no. 3, pp. 117–123, Mar. 1972.
Kyeong Jin Kim (Senior Member, IEEE) received the M.S. degree from the Korea Advanced Institute of Science and Technology (KAIST) in 1991 and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of California at Santa Barbara, Santa Barbara, CA, USA, in 2000. From 1991 to 1995, he was a Research Engineer with the Video Research Center, Daewoo Electronics Ltd., South Korea. In 1997, he joined the Data Transmission and Networking Laboratory, University of California at Santa Barbara. After receiving his degrees, he joined the Nokia Research Center and Nokia Inc., Dallas, TX, USA, as a Senior Research Engineer, where he was an L1 Specialist from 2005 to 2009. From 2010 to 2011, he was a Visiting Scholar with Inha University, South Korea. Since 2012, he has been a Senior Principal Research Staff with Mitsubishi Electric Research Laboratories (MERL), Cambridge, MA, USA. His research interests include transceiver design, resource management, scheduling in the cooperative wireless communications systems, cooperative spectrum sharing systems, physical layer secrecy systems, device-to-device communications, local and private 5G networks, and AI-based cyber-physical and smart grid systems. He received the Best Paper Reward from the 2014 IEEE-Chinacom, IEEE ICC 2019, and IEEE PES-GM 2020. He served as an Editor for IEEE COMMUNICATIONS LETTERS and a Guest Editor for the IET COMMUNICATIONS Special Issue on Secure Physical Layer Communications. Recently, he also served as a leading Guest Editor for the IEEE JOURNAL OF SELECTED AREAS IN COMMUNICATIONS Special Issue on Spatial Modulation for Emerging Wireless Systems. He serves as a leading Guest Editor for the IEEE JOURNAL OF SELECTED TOPICS IN SIGNAL PROCESSING Special Issue on Advanced Signal Processing for Local and Private 5G Networks and an Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS.

Theodoros A. Tsiftsis (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from the University of Patras, Greece, in 2006. He is currently a Professor with the Department of Informatics and Telecommunications, University of Thessaly, Greece. His research interests include communication theory and wireless communications, with an emphasis on wireless communications theory, reconfigurable intelligent surfaces, optical wireless communications, and physical layer security. He served on the editorial boards for the IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, and IEEE COMMUNICATIONS LETTERS. He is an Associate Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and IEEE TRANSACTIONS ON MOBILE COMPUTING. He was appointed as an IEEE Vehicular Technology Society Distinguished Lecturer for two terms (2018–2022).