Enhancing Physical-Layer Security for IoT With Nonorthogonal Multiple Access Assisted Semi-Grant-Free Transmission

Kunrui Cao, Haiyang Ding, *Member, IEEE*, Buhong Wang, *Member, IEEE*, Lu Lv, *Member, IEEE*, Jiwei Tian, Qingmei Wei, and Fengkui Gong, *Member, IEEE*

***Abstract*—Nonorthogonal multiple access (NOMA) assisted semi-grant-free transmission admits grant-free users to access the channels otherwise solely occupied by grant-based users, and has been recently attracting considerable attention in terms of accommodating massive connectivity and reducing access delay in Internet of Things (IoT). In this work, we investigate the security of semi-grant-free NOMA transmission in the presence of passive and active eavesdropping attacks. In particular, for the scenario-I with strong grant-based user and weak grant-free users, the scenario-I-based maximal user scheduling (IbMUS) and scenario-I-based optimal user scheduling (IbOUS) schemes are proposed to combat the passive and active eavesdropping, respectively. For the scenario-II with weak grant-based user and strong grant-free users, two parallel schemes, namely, the scenario-II-based maximal user scheduling (IIbMUS) and scenario-II-based optimal user scheduling (IIbOUS) schemes, are proposed to combat the passive and active eavesdropping, respectively. These proposed schemes enhance the security by scheduling a grant-free user with maximal main channel capacity/maximal secrecy capacity to access the NOMA channel on the premise of ensuring the grant-based user's Quality of Service. Based on these proposed schemes, the exact secrecy outage probability (SOP) are analyzed to evaluate the system performance. The simulation results validates the theoretic analysis and the superiority of the proposed schemes. The IbOUS and IIbOUS schemes can achieve better performance than the IbMUS and IIbMUS schemes owing to the use of active eavesdropper's channel state information (CSI). The SOP achieved by theproposed schemes can be further improved with the increasing number of grant-free users and decreasing target rate (or target secrecy rate).**

***Index Terms*—Nonorthogonal multiple access (NOMA), physical-layer security, secrecy outage probability (SOP), semi-grant-free transmission, user scheduling.**

Manuscript received 25 April 2022; accepted 18 July 2022. Date of publication 22 July 2022; date of current version 7 December 2022. This work was supported in part by the National Natural Science Foundation of China under Grant 62101560, Grant 61871387, and Grant 61901313; in part by the Natural Science Basic Research Program of Shaanxi under Grant 2022JQ-619; in part by the National University of Defense Technology Research Fund under Grant ZK21-44; in part by the Open Research Fund of the State Key Laboratory of ISN, Xidian University under Grant ISN23-04; and in part by the China Postdoctoral Science Foundation under Grant BX20190264 and Grant 2019M650258. *(Corresponding authors: Haiyang Ding; Buhong Wang.)*

Kunrui Cao is with the School of Information and Communications, National University of Defense Technology, Wuhan 430035, China, and also with the State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China (e-mail: krcao@nudt.edu.cn).

Haiyang Ding is with the School of Information and Communications, National University of Defense Technology, Wuhan 430035, China, and also with the Youth Innovation Team of Shaanxi Universities, Xi'an, China (e-mail: dinghy2003@hotmail.com).

Buhong Wang, Jiwei Tian, and Qingmei Wei are with the School of Information and Navigation, Air Force Engineering University, Xi'an 710077, China (e-mail: bhwangaf@sina.com; tianjiwei2016@163.com; marry143@sohu.com).

Lu Lv and Fengkui Gong are with the State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China (e-mail: lulv@xidian.edu.cn; fkgong@xidian.edu.cn).

Digital Object Identifier 10.1109/JIOT.2022.3193189

I. Introduction

THE NEXT generation of Internet of Things (IoT) is envisioned to provide a support for all kinds of important applications, such as wireless health-care, smart home, environment monitoring, intelligent transportation, etc. The key step to achieve the next generation IoT is to guarantee the connection of a massive number of IoT devices in the specific spectral resource [1]. However, it is challenging for conventional orthogonal multiple access (OMA) to support massive connectivity due to the scarceness of available bandwidth resources for wireless communications. Recently, non-OMA (NOMA), encouraging spectrum sharing among wireless devices, has emerged as a spectrally efficient solution to implement the massive connectivity for the IoT [2].

In typical IoT scenarios with uplink OMA transmission, each device is allocated with a dedicated orthogonal resource block for the transmission of signal, which causes a low spectral efficiency. Unlike OMA, NOMA utilizes the successive interference cancelation (SIC) at the access point to enable multiple devices to be served simultaneously in the same spectral resource blocks [3]–[12]. It is worth pointing out that many research works on NOMA [3]–[12] are based on traditional grant-based transmission with uplink scheduling requests and dynamic scheduling grants, i.e., multiple grant-based users are admitted with NOMA to access the joint resource blocks consisting of the granted resource block of each user, as shown in Fig. 1. Very recently, the uplink NOMA assisted semi-grant-free transmission scheme was proposed in [13]–[18] to further enhance the spectral efficiency and reduce the access delay for supporting a massive number of IoT users, each of which has a small amount of data to send only. Specifically, the delay-sensitive user in the system is allowed to occupy a specific bandwidth resource block as the grant-based user, while the delay-tolerant user is regraded as the grant-free user without scheduling grants of base station (BS) and opportunistically

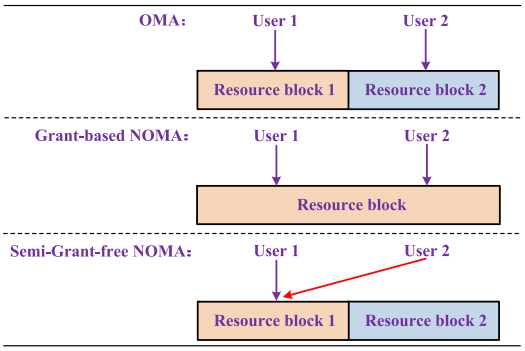


Fig. 1. Schematic diagram of different transmission schemes.

access the resource block, that is, solely occupied by the grant-based user in OMA, by using uplink NOMA. A crucial task is to ensure the grant-based user's Quality of Service (QoS) experience when the grant-free user is admitted to access the same resource block. As a further advance, Ding *et al.* [18] proposed a new semi-grant-free NOMA transmission scheme to ensure that the grant-free users can be transparent to the grant-based user, and the grant-based user's QoS is the same as when it solely occupies the resource block.

On the other hand, owing to various applications of the communication technology and the openness of wireless channels, the information security of wireless transmission is facing great challenges. Physical-layer security is an efficient solution to enhance the information security by exploiting the inherent characteristics of the wireless channel, such as fading, interference, and noise, to ensure that a malicious eavesdropper can not acquire any confidential information about the transmitted legitimate signals from the physical layer [19]–[24]. Recently, physical-layer security for NOMA transmission has been attracting considerable attention from the research community [25]–[41]. Particularly, Zhang *et al.* [25] studied a single-input single-output system with NOMA and proposed an optimal power allocation strategy to maximize the sum secrecy rate of the users. In [26], an NOMA transmission strategy to maximize the minimum confidential information was designed under the constraints of transmission power and secrecy outage probability (SOP). In order to achieve a secrecy massive NOMA, the interuser interference was used in [27] to confuse the malicious eavesdroppers. Liu *et al.* [28] considered a practical large-scale NOMA network with randomly deployed legitimate users and malicious eavesdroppers, and presented an artificial noise (AN) aided secrecy beamforming scheme to protect the transmission of the useful information for legitimate users. Further, Lv *et al.* [29] proposed a new security beamforming strategy with AN to strengthen the information security of the multiantenna downlink NOMA systems, and indicated the significant superiority of the proposed scheme compared to [28] in terms of combating the eavesdropping attack. Unlike [29], Feng *et al.* [30] presented a joint power allocation and AN aided beamforming scheme, which can achieve a tradeoff of the strength between the transmitted signal and interference to gain an enhancement of the secrecy in the downlink NOMA systems. In particular, the information security of a dual-user system was studied in [31] where the strong user acts as a friendly relay for weak user given the inherent cooperative feature of NOMA, and the exact closed-from expression of SOP for the system were obtained. Lei *et al.* [32] studied the secrecy performance for a multiple relays aided NOMA system in the presence of an external eavesdropping attack under the condition of Nakagami-*m* fading channels. In [33], a new jamming and relaying strategy with the NOMA principle was proposed to improve the secrecy for the untrusted relay system. Different from the above works, we investigated the physical-layer security of uplink NOMA systems with the help of friendly jammer in [34], according to the type of eavesdropping attack, and proposed the random jammer scheduling aided uplink NOMA transmission scheme and optimal jammer scheduling aided uplink NOMA transmission scheme to, respectively, combat the passive and active eavesdroppers for improving the security of the system. With the proposed two schemes, we analyzed the secrecy performance of the system to verify the effectiveness of the proposal. Furthermore, in [35], given the power constraints and selfishness of nodes in practical networks, we further studied the uplink NOMA with energy harvesting (EH) jammers, and correspondingly proposed the random EH jammer scheduling scheme without the requirement of any channel state information (CSI), the maximal EH jammer scheduling scheme with the CSI between BS and each EH receivers, and the optimal EH jammer scheduling scheme where both the CSIs from BS to EH receivers and from EH receivers to the eavesdropper need to be known. Owing to the distinctive merits, NOMA has been utilized in unmanned aerial vehicle (UAV)-enabled IoT to enhance the communication of terrestrial nodes. In particular, in [36], a UAV-aided NOMA network with simultaneous wireless information and power transfer (SWIPT) was proposed to guarantee the secure transmission for ground passive receivers, which can implement a practical nonlinear EH scheme and secure massive connectivity for future IoT. Moreover, Zhao *et al.* [37] proposed two schemes to enhance the security of NOMA-UAV networks with one security-required user and multiple security-required users, respectively, and analyzed the effectiveness of the proposed two schemes in terms of guaranteeing the secure transmission.

As mentioned above, physical-layer security of NOMA has been recently investigated in various scenarios. However, there is still a lack of research contributions on the security issue of semi-grant-free NOMA transmission in the presence of eavesdropping attack in the literature, and the corresponding security transmission criteria and the secrecy performance are still far from being understood, which motivates this work. In this work, we focus our attention on studying the secure communications of two semi-grant-free NOMA scenarios, i.e., scenario-I with strong grant-based user and weak grant-free users and scenario-II with strong grant-free users and weak grant-based user. Particularly, following the same protocol of semi-grant-free transmission in [13]–[18], the grant-free users utilize the NOMA to access the channel that is occupied by the grant-based user for uplink transmission. The main contributions of this work can be summarized as follows.

1) In view of two types of the eavesdropping attacks, we propose the scenario-I-based maximal user scheduling (IbMUS) and scenario-I-based optimal user scheduling (IbOUS) schemes to enhance the security of scenario-I in the presence of the passive and active eavesdropping, respectively. Also, we propose the scenario-II-based maximal user scheduling (IIbMUS) and scenario-II-based optimal user scheduling (IIbOUS) schemes for the scenario-II to combat the passive and active eavesdropping, respectively. Compared with the user scheduling schemes used in traditional grant-based NOMA, such as [24], [32], [34], and [35], the proposed schemes can guarantee the QoS of a grant-based user to be the same as for OMA and simultaneously enhance the security of grant-free user by scheduling one user with maximal main channel capacity/maximal secrecy capacity to access the NOMA channel, which is preferable for semi-grant-free NOMA where the grant-free users access resource blocks of the grant-based users and hence interfere with the grant-based users.
2) We analyze the system performance achieved by the IbMUS, IbOUS, IIbMUS, and IIbOUS schemes, respectively, and derive exact closed-form expressions of SOP to quantify the impact of the proposed schemes. These new expressions would provide an efficient approach to evaluate the total performance of the considered systems without carrying out extensive Monte Carlo calculation.
3) Fruitful insights are obtained from analytical and numerical results: a) in terms of the performance of the semi-grant-free NOMA, the proposed schemes outperform the user scheduling schemes used in traditional grant-based NOMA; b) the IbOUS and IIbOUS schemes can fulfill better performance than the IbMUS and IIbMUS schemes owing to the use of active eavesdropper's CSI; c) the SOP achieved by the proposed schemes can be further improved with the increasing number of grant-free users and decreasing target rate (or secrecy rate); and d) an increase of transmission power at the grant-based user is beneficial to the performance of scenario-I but deteriorates the performance of scenario-II.

The remainder of this article is organized as follows. In Section II, the system model is presented and corresponding schemes are proposed. In Section III, the secrecy performances of the scenario-I with the proposed IbMUS and IbOUS schemes are analyzed, and the exact closed-form expressions for SOP are derived, respectively. In Section IV, the secrecy performances of the scenario-II with the proposed IIbMUS and IIbOUS schemes are analyzed, and the exact closed-form expressions for SOP are given. Then, numerical results are shown to demonstrate our theoretical analysis in Section V. This article is concluded in Section VI.

II. System Model and Proposed Schemes

As shown in Fig. 2, we consider an IoT uplink communication system with semi-grant-free transmission consisting of a BS, a malicious eavesdropper (E), $(N+1)$ users denoted by $\{U_0, \ldots, U_N\}$. Assume that U_0 is a delay-sensitive user and allowed to solely occupy a resource block in OMA, i.e., a grant-based user.[1] The grant-free users $\{U_n | n = 1, 2, \ldots, N\}$ compete with each other and one of them is granted to access the resource block of U_0 by NOMA for improving the spectral efficiency twofold. It is detailed later that which user is granted access. It is noteworthy that massive connectivity can be still supported even though a single grant-free user is scheduled at each time. Assume that U_0 is scheduled for T time slot. During each T/m time slot, one grant-free user is served and then can be removed from the competing user set due to the short packet transmission feature of IoT, which means that m grant-free users can be served without consuming any extra bandwidth resources.

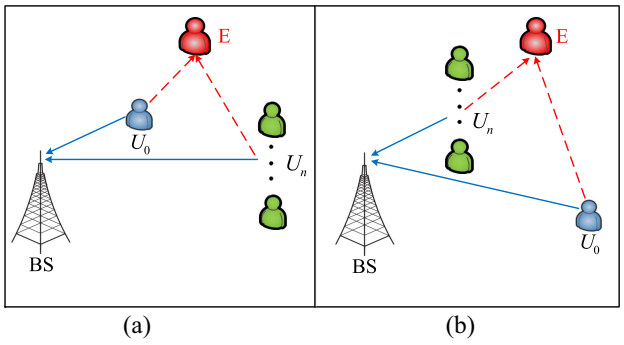


Fig. 2. System model. (a) Scenario-I. (b) Scenario-II.

Considering the spatial distributions of the users, two scenarios are investigated, i.e., scenario-I in Fig. 2(a) and scenario-II in Fig. 2(b). In particular, U_0 is a strong user with the better channel condition than U_n in the scenario-I, while U_0 is a weak user with the worse channel condition than U_n in the scenario-II. In the two scenarios, each node is equipped with a single antenna, and all the channels are subject to the independent quasi-static Rayleigh fading, where $h_{xy} \sim \mathcal{CN}(0, \lambda_{xy})$ is denoted as the channel coefficient between node x and node y.

Following the principle of uplink NOMA, the BS first decodes the signal of the strong user with the interference of the weak user, and then decodes the signal of the weak user with the aid of SIC. Hence, in the scenario-I, the instantaneous signal-to-noise ratios (SNRs) to decode the signals of U_0 and U_n at BS can be, respectively, given by

$$\gamma^I_{u_0 b} = \frac{\rho_0 |h_{u_0 b}|^2}{\rho_s |h_{u_n b}|^2 + 1} \tag{1}$$

$$\gamma^I_{u_n b} = \rho_s |h_{u_n b}|^2 \tag{2}$$

where $\rho_0 = (P_0/N_0)$ and $\rho_s = (P_s/N_0)$ are the transmission SNRs of U_0 and U_n, P_0 and P_s are the transmission powers of U_0 and U_n, respectively, and N_0 is the variance of the additive white Gaussian noise. In the scenario-II, the instantaneous SNRs to decode the signals of U_n and U_0 at BS can

[1]For the scenario with multiple grant-based users, these grant-based users would be divided into different orthogonal resource block in OMA, which is the same as the conventional OMA scenario.

be, respectively, given by

$$\gamma_{u_n b}^{II} = \frac{\rho_s |h_{u_n b}|^2}{\rho_0 |h_{u_0 b}|^2 + 1} \tag{3}$$

$$\gamma_{u_0 b}^{II} = \rho_0 |h_{u_0 b}|^2. \tag{4}$$

Note that $\gamma_{u_n b}^{I}$ in (2) and $\gamma_{u_0 b}^{II}$ in (4) are obtained just under the condition of the successful SIC.

On the other hand, owing to the broadcast nature of wireless communication, the malicious eavesdropper in the system attempts to intercept the confidential information between the NOMA users and BS. Similar to [29], [34], and [39], this work focuses on a worst-case eavesdropping scenario for the legitimate users, where the eavesdropper has powerful multiuser detection capacity (e.g., parallel interference cancelation) such that the received data stream is distinguished and the individual signal can be detected by the eavesdropper. This worst-case eavesdropping scenario may overestimate the malicious eavesdropper's detection capability, but it makes the analysis and design in this work robust for the practical scenario, which is meaningful and desirable from the perspective of security. Accordingly, the instantaneous SNRs to decode the signals of U_0 and U_n at the malicious eavesdropper can be, respectively, given by

$$\gamma_{u_0 e} = \rho_0 |h_{u_0 e}|^2 \tag{5}$$

$$\gamma_{u_n e} = \rho_s |h_{u_n e}|^2. \tag{6}$$

In view of two types of the eavesdropping attacks, four transmission schemes are proposed to ensure the QoS of U_0 to be the same as for OMA, and simultaneously enhance the security of U_n in two scenarios, which are, respectively, introduced as follows.

A. Scenario-I

In this section, we present the IbMUS and IbOUS schemes to combat the passive and active eavesdroppers, respectively, for achieving the reliable and secure transmission in the scenario-I.

1) IbMUS Scheme for Passive Eavesdropping: Passive eavesdropper is also named as external eavesdropper, which only overhears but does not transmit. In general, the CSI of the eavesdropper is not known by the system. In this case, the IbMUS scheme is proposed to ensure the QoS of U_0 and simultaneously enhance the security of U_n.[2] Specifically, prior to transmission, the BS broadcasts a threshold denoted by τ, that needs to meet

$$\log_2\left(1 + \frac{\rho_0 |h_{u_0 b}|^2}{\tau + 1}\right) \geq R_0 \tag{7}$$

where R_0 is the target rate of U_0. As a result, τ can be expressed as follows:

$$\tau = \max\left\{0, \frac{\rho_0 |h_{u_0 b}|^2}{2^{R_0} - 1} - 1\right\}. \tag{8}$$

Based on the above threshold, each grant-free user would individually compares its channel condition with the threshold, i.e., $\rho_s |h_{u_n b}|^2 \leq \tau$. In the scenario-I, there may exist multiple grant-free users whose channel conditions are below the threshold owing to the weak channel conditions of the grant-free users. It is assumed that the grant-free users whose channel conditions are below the threshold are expressed as the set S_u. In order to enhance the secrecy performance, one grant-free user with maximal main channel capacity is scheduled from S_u to access the resource block of U_0 to perform uplink NOMA transmission. Mathematically, the IbMUS scheme can be given by

$$U_{MUS}^{I} = \underset{u_i \in S_u}{\operatorname{argmax}} \left\{\log_2\left(1 + \rho_s |h_{u_i b}|^2\right)\right\}. \tag{9}$$

It is worth pointing out that a pure grant-free protocol can not guarantee the QoS of the grant-based user in NOMA. Hence, in the proposed schemes, a low-overhead distributed contention protocol [17] is used for the semi-grant-free procedure to guarantee the QoS of the grant-based user and simultaneously enhance the security of the grant-free user.[3] Specifically, prior to transmission, the BS broadcasts the channel threshold in (8). Once the contention time window starts, each grant-free user whose channel condition is below the threshold would choose a backoff time t_i, which is a strictly decreasing function of the user's channel condition. A user immediately transmits a beacon to the BS after t_i expires. As such, one user with maximal channel condition/capacity waits for the shortest time and hence transmits to the BS first. As a result, the proposed scheme is implemented.

According to the definition of secrecy capacity and theory of Wyner's wiretap code [19], the secrecy capacity of the grant-free user is enhanced as its main channel capacity is maximized by using the IbMUS scheme. It is noteworthy that the AN [34], [35] can be exploited on the basis of the proposed user scheduling schemes to further enhance the secrecy capacity of the system, but it increases the complexity of the system design and performance analysis, which is set aside for our future work.

2) IbOUS Scheme for Active Eavesdropping: Active eavesdropper is a transceiver operating with known protocols in the system but having a low-security clearance, which is also known as internal eavesdropper or untrusted node [20], [33], [42]–[44].[4] The CSI of an active eavesdropper can be computed and acquired by monitoring the eavesdropper's communication or exploiting some channel estimation approaches.

For the active eavesdropping, the IbOUS scheme is proposed to ensure the QoS of U_0 and simultaneously

[2]It is guaranteed by using the proposed schemes that the grant-free user is completely transparent to the grant-based user and the experience of the grant-based user is the same as with conventional OMA. Hence, the security of the grant-based user can be improved by using some conventional methods in the OMA system. This work primarily focuses on the security of the grant-free user.

[3]The low-overhead distributed contention protocol is not a conventional connection handshaking protocol with BS in grant-based transmission, and the selected grant-free user does not perform any connection handshaking protocol compared to the grant-based user with at least a pair of connection handshakes.

[4]In fact, the active eavesdropper has two types in the literature. One is a powerful adversary that can not only eavesdrop but also jam the legitimate communication. Differently, the other one does not transmit the malicious jamming and can be regarded as an untrusted communication node in the considered system. This article mainly focuses on the latter, and the former is beyond the scope of this article.

maximize the security of U_n. Similar to the IbMUS scheme, the BS broadcasts a threshold τ in (8) prior to transmission, and the grant-free users whose channel conditions are below the threshold are expressed as the set S_u. By using the active eavesdropper's CSI, one grant-free user with maximal secrecy capacity can be scheduled from S_u to perform uplink NOMA transmission with U_0 for achieving an optimal secrecy performance. Mathematically, the IbOUS scheme can be given by

$$U_{\text{OUS}}^{I} = \underset{u_i \in S_u}{\text{argmax}} \left\{ \log_2 \left(\frac{1+\rho_s |h_{u_i b}|^2}{1+\rho_s |h_{u_i e}|^2} \right) \right\}. \tag{10}$$

Similar to the IbMUS scheme, the proposed IbOUS scheme can be implemented with the aid of distributed contention protocols [17].

B. Scenario-II

In this section, we present the IIbMUS and IIbOUS schemes to combat the passive and active eavesdroppers for the scenario-II, respectively.

1) IIbMUS Scheme for Passive Eavesdropping: In the scenario-II, the BS first decodes the signal of U_n with the interference of U_0, and then decodes the signal of U_0 by using the SIC. In the IIbMUS scheme, the practical transmission rate of data at U_n is set as $\log_2(1+([\rho_s|h_{u_n b}|^2]/[\rho_0|h_{u_0 b}|^2+1]))$. In this case, the successful SIC can be ensured and hence U_n does not cause any performance degradation to U_0. Due to the fact that the passive eavesdropper's CSI is unknown, the grant-free user with maximal main channel capacity is scheduled to perform the uplink NOMA transmission with U_0. Accordingly, the IIbMUS scheme can be written as follows:

$$U_{MUS}^{II} = \underset{u_i \in U}{\text{argmax}} \left\{ \log_2 \left(1 + \frac{\rho_s |h_{u_i b}|^2}{\rho_0 |h_{u_0 b}|^2 + 1} \right) \right\} \tag{11}$$

where $U = \{U_1, U_2, \ldots, U_N\}$ denotes the set of all grant-free users. Based on the proposed IIbMUS scheme, the maximization of the main channel capacity enhances the secrecy capacity of the grant-free user.

2) IIbOUS Scheme for Active Eavesdropping: Similar to the IIbMUS scheme, the practical transmission rate of data at U_n is set as its channel capacity to ensure the successful SIC. In particular, by using the active eavesdropper's CSI, one grant-free user with maximal secrecy capacity is scheduled to achieve an optimal secrecy performance for the uplink NOMA. Mathematically, the IIbOUS scheme can be given by

$$U_{\text{OUS}}^{II} = \underset{u_i \in U}{\text{argmax}} \left\{ \log_2 \left(\frac{1+\frac{\rho_s |h_{u_i b}|^2}{\rho_0 |h_{u_0 b}|^2+1}}{1+\rho_s |h_{u_i e}|^2} \right) \right\}. \tag{12}$$

It is worth pointing out that from the perspective of an eavesdropper's CSI, the implementations of the proposed IbMUS and IIbMUS schemes do not need the CSI of the eavesdropper, while the proposed IbOUS and IIbOUS schemes exploit the CSI of the eavesdropper to achieve an optimal secrecy performance.

III. Performance Analysis for Scenario-I

In this section, we analyze the performance achieved by the IbMUS and IbOUS schemes for the scenario-I, and derive the exact closed-form expressions of SOP to quantify the impact of the proposed schemes. It is observed from the above section that the proposed schemes can guarantee that the grant-free user U_n is completely transparent to the grant-based user U_0, and the experience of U_0 is the same as with OMA. In this sense, the SOP of U_0 can be obtained from existing OMA works. Therefore, this work mainly focuses on the SOP analysis of U_n.

A. SOP of IbMUS Scheme

The SOP is the probability of event that secrecy capacity is smaller than target secrecy rate. In particular, for the semi-grant-free NOMA transmission, the SOP also includes the probability of the event that any grant-free user can not guarantee the QoS of a grant-based user. Accordingly, the following lemma can be obtained.

Lemma 1: The SOP of U_n in the scenario-I can be written as follows:

$$P_{\text{SOP}} = \Pr(|S_u| = 0) + \Pr(C_s < R_s, |S_u| > 0) \tag{13}$$

where $|S_u|$ denotes the cardinality of the set S_u, $\Pr(|S_u| = 0)$ denotes the probability of the event that any of the grant-free users U_n can not guarantee the QoS of U_0, and R_s denotes the target secrecy rate of U_n. Moreover, C_s denotes the secrecy capacity given by $C_s = \log_2(1+\rho_s \max_{u_i \in S_u}\{|h_{u_i b}|^2\}) - \log_2(1+\rho_s|h_{u_v e}|^2)$ in the IbMUS scheme or $C_s = \max_{u_i \in S_u}\{\log_2(1+\rho_s|h_{u_i b}|^2) - \log_2(1+\rho_s|h_{u_i e}|^2)\}$ in the IbOUS scheme, where U_v denotes the scheduled user from the set S_u.

To proceed forward, we first derive $\Pr(|S_u| = 0)$ in Lemma 1. As the channels in the system are subject to the Rayleigh fading (i.e., the statistic of channel gain is subject to an exponential distribution), the probability of the event that no grant-free users can guarantee the QoS of a grant-based user U_0 is given by

$$\begin{aligned}
\Pr(|S_u|=0) &= \Pr\left(\log_2 \left(1+\frac{\rho_0 |h_{u_0 b}|^2}{\rho_s \min\limits_{u_i \in U}\left\{|h_{u_i b}|^2\right\}+1} \right) < R_0 \right) \\
&= \Pr\left(\frac{\rho_0 |h_{u_0 b}|^2}{\rho_s \min\limits_{u_i \in U}\left\{|h_{u_i b}|^2\right\}+1} < \varepsilon_0 \right) \\
&= \Pr\left(\frac{\rho_0 |h_{u_0 b}|^2 - \varepsilon_0}{\varepsilon_0 \rho_s} < \min_{u_i \in U}\left\{|h_{u_i b}|^2\right\} \right) \\
&= \int_{\frac{\varepsilon_0}{\rho_0}}^{\infty} \frac{1}{\lambda_{u_0 b}} e^{-\frac{x}{\lambda_{u_0 b}}} \left[\Pr\left(\frac{\rho_0 x - \varepsilon_0}{\varepsilon_0 \rho_s} < |h_{u_i b}|^2 \right) \right]^N dx \\
&\quad + \int_0^{\frac{\varepsilon_0}{\rho_0}} \frac{1}{\lambda_{u_0 b}} e^{-\frac{x}{\lambda_{u_0 b}}} dx \\
&= \int_{\frac{\varepsilon_0}{\rho_0}}^{\infty} \frac{1}{\lambda_{u_0 b}} e^{-\frac{N(\rho_0 x - \varepsilon_0)}{\lambda_{u_n b} \rho_s \varepsilon_0} - \frac{x}{\lambda_{u_0 b}}} dx
\end{aligned}$$

$$+\int_0^{\frac{\varepsilon_0}{\rho_0}} \frac{1}{\lambda_{u_0b}} e^{-\frac{x}{\lambda_{u_0b}}} dx = 1 - \frac{\lambda_{u_0b} N \rho_0 e^{-\frac{\varepsilon_0}{\rho_0 \lambda_{u_0b}}}}{\lambda_{u_0b} N \rho_0 + \lambda_{u_n s} \rho_s \varepsilon_0} \tag{14}$$

where $\varepsilon_0 = 2^{R_0} - 1$.

Then, we derive the probability $\Pr(C_s < R_s, |S_u| > 0)$ in Lemma 1. The key idea of the derivation is the transition of $|S_u| > 0$. Recall the definition of the set S_u, any user in the set S_u can ensure the QoS of U_0 (i.e., the channel capacity of U_0 is above the target rate R_0 under the interference of the strongest user in S_u), while any user in the set $U \setminus S_u$ can not meet the QoS of U_0 (i.e., the channel capacity of U_0 drops below the target rate R_0 under the interference of the weakest user in $U \setminus S_u$). Furthermore, the permutation and combination of selecting l from N can be given by $\binom{N}{l}$. Based on the above analysis, we have

$$\begin{aligned}
&\Pr(C_s < R_s, |S_u| > 0) \\
&= \sum_{l=1}^{N} \Pr(C_s < R_s, |S_u| = l) \\
&= \sum_{l=1}^{N} \sum_{v=1}^{l} \binom{N}{l} \Pr(\text{ScheduledUser} = U_v) \\
&\times \Pr\left(\frac{1 + \rho_s \max\limits_{u_i \in S_u} \{|h_{u_i b}|^2\}}{1 + \rho_s |h_{u_v e}|^2} < \varepsilon_s, \frac{\rho_0 |h_{u_0 b}|^2}{1 + \rho_s \min\limits_{u_i \in U \setminus S_u} \{|h_{u_i b}|^2\}} \right. \\
&\quad \left. < \varepsilon_0, \frac{\rho_0 |h_{u_0 b}|^2}{1 + \rho_s \max\limits_{u_i \in S_u} \{|h_{u_i b}|^2\}} > \varepsilon_0 \right)
\end{aligned} \tag{15}$$

where $\varepsilon_s = 2^{R_s}$, $\Pr(\text{ScheduledUser} = U_v)$ denotes the probability of the event that U_v is scheduled from S_u, and $U \setminus S_u$ denotes the set difference between U and S_u. By substituting (14) and (15) into Lemma 1, the SOP of the IbMUS scheme can be derived as follows.

Theorem 1: The SOP of U_n in the IbMUS scheme is given by (16), shown at the bottom of the page, where $\theta_1 = ((k\varepsilon_s \lambda_{u_n e} + \lambda_{u_n b})/(\lambda_{u_n b} \lambda_{u_n e}))$, $\theta_2 = ((\lambda_{u_0 b} \rho_0 (N - l) + \lambda_{u_n b} \varepsilon_0 \rho_s)/(\lambda_{u_n b} \lambda_{u_0 b} \varepsilon_0 \rho_s))$, and $\theta_3 = ((\lambda_{u_0 b} \rho_0 (N + k - l) + \lambda_{u_n b} \varepsilon_0 \rho_s)/(\lambda_{u_n b} \lambda_{u_0 b} \varepsilon_0 \rho_s))$.

Proof: See Appendix A. ∎

The new closed-form expression in (16) gives an efficient way for system designers to compute the performance achieved by the proposed scheme, without implementing extensive computer simulations.

B. SOP of IbOUS Scheme

For the IbOUS scheme, $\Pr(|S_u| = 0)$ is equal to the result in (14). Similar to the analysis of the IbMUS scheme in (15), $\Pr(C_s < R_s, |S_u| > 0)$ of the IbOUS scheme can be expressed as follows:

$$\begin{aligned}
&\Pr(C_s < R_s, |S_u| > 0) \\
&= \sum_{l=1}^{N} \Pr(C_s < R_s, |S_u| = l) \\
&= \sum_{l=1}^{N} \binom{N}{l} \Pr\left(\max_{u_i \in S_u} \left\{ \frac{1 + \rho_s |h_{u_i b}|^2}{1 + \rho_s |h_{u_i e}|^2} \right\} < \varepsilon_s, \right. \\
&\quad \left. \frac{\rho_0 |h_{u_0 b}|^2}{1 + \rho_s \min\limits_{u_i \in U \setminus S_u} \{|h_{u_i b}|^2\}} < \varepsilon_0, \frac{\rho_0 |h_{u_0 b}|^2}{1 + \rho_s \max\limits_{u_i \in S_u} \{|h_{u_i b}|^2\}} > \varepsilon_0 \right).
\end{aligned} \tag{17}$$

By substituting (14) and (17) into Lemma 1, the SOP achieved by the IbOUS scheme can be derived as follows.

Theorem 2: The SOP of U_n achieved by the IbOUS scheme is given by (18), shown at the bottom of the page, where $\eta_1 = ([k\rho_0(\lambda_{u_n b} + \lambda_{u_n e}\varepsilon_s)]/[\lambda_{u_n e}\lambda_{u_n b}\varepsilon_0\varepsilon_s\rho_s]) + ([\rho_0(N-l)]/\lambda_{u_n b}\varepsilon_0\rho_s) + (1/\lambda_{u_0 b})$ and $\eta_2 = (k\rho_0/\lambda_{u_n b}\varepsilon_0\rho_s) + (\rho_0(N-l)/\lambda_{u_n b}\varepsilon_0\rho_s) + (1/\lambda_{u_0 b})$.

Proof: See Appendix B. ∎

Remark 1: It is observed from Theorems 1 and 2 that the SOPs are related to the target rate of a grant-based user R_0. This means that the SOPs achieved by the proposed schemes characterize both the security and reliability of the system, and the security of grant-free users can be enhanced with

$$\begin{aligned}
P_{\text{IbMUS}} = 1 - \frac{\lambda_{u_0 b} N \rho_0 e^{-\frac{\varepsilon_0}{\rho_0 \lambda_{u_0 b}}}}{\lambda_{u_0 b} N \rho_0 + \lambda_{u_n s} \rho_s \varepsilon_0} + \sum_{l=1}^{N} \sum_{k=0}^{l} \binom{N}{l} \binom{l}{k} (-1)^k \\
\times \left[\frac{e^{\frac{\varepsilon_0 (N-l)}{\varepsilon_0 \rho_s \lambda_{u_n b}} - \frac{k(\varepsilon_s - 1)}{\rho_s \lambda_{u_n b}} - \frac{\varepsilon_0 \varepsilon_s \theta_2}{\rho_0}}}{\lambda_{u_n e} \lambda_{u_0 b} \theta_1} \left(\frac{1}{\theta_2} - \frac{\varepsilon_0 \varepsilon_s \rho_s}{\rho_0 \theta_1 + \varepsilon_0 \varepsilon_s \rho_s \theta_2} \right) + \frac{e^{\frac{N+k-l}{\rho_s \lambda_{u_n b}}}}{\lambda_{u_0 b} \theta_3} \left(e^{-\frac{\varepsilon_0 \theta_3}{\rho_0}} - \frac{\rho_0 e^{-\frac{\varepsilon_0 \varepsilon_s \theta_3}{\rho_0}}}{\rho_0 + \varepsilon_0 \varepsilon_s \lambda_{u_n e} \rho_s \theta_3} \right) \right]
\end{aligned} \tag{16}$$

$$\begin{aligned}
P_{\text{IbOUS}} = 1 - \frac{\lambda_{u_0 b} N \rho_0 e^{-\frac{\varepsilon_0}{\rho_0 \lambda_{u_0 b}}}}{\lambda_{u_0 b} N \rho_0 + \lambda_{u_n s} \rho_s \varepsilon_0} + \sum_{l=1}^{N} \sum_{k=0}^{l} \binom{N}{l} \binom{l}{k} (-1)^k \\
\times \left[\frac{1}{\lambda_{u_0 b} \eta_1} \left(\frac{\varepsilon_s \lambda_{u_n e}}{\varepsilon_s \lambda_{u_n e} + \lambda_{u_n b}} \right)^k \left(1 - \frac{\lambda_{u_n b} e^{-\frac{\varepsilon_s - 1}{\rho_s \lambda_{u_n b}}}}{\varepsilon_s \lambda_{u_n e} + \lambda_{u_n b}} \right)^{l-k} e^{\frac{k(\lambda_{u_n e} + \lambda_{u_n b}) + \lambda_{u_n e}(N-l)}{\rho_s \lambda_{u_n b} \lambda_{u_n e}} - \frac{\varepsilon_0 \varepsilon_s \eta_1}{\rho_0}} + \frac{e^{\frac{N+k-l}{\rho_s \lambda_{u_n b}}}}{\lambda_{u_0 b} \eta_2} \left(e^{-\frac{\varepsilon_0 \eta_2}{\rho_0}} - e^{-\frac{\varepsilon_0 \varepsilon_s \eta_2}{\rho_0}} \right) \right]
\end{aligned} \tag{18}$$

the decrease of the target rate R_0 or increase of the channel condition $\lambda_{u_0 b}$.

Remark 2: The IbMUS and IbOUS schemes can not only improve the security of grant-free user U_n but also guarantee the QoS of a grant-based user U_0, which are preferable for semi-grant-free NOMA where the grant-free user access the resource block of the grant-based user and hence interfere with the grant-based user.

IV. Performance Analysis for Scenario-II

In this section, we analyze the secrecy performance achieved by the IIbMUS and IIbOUS schemes for the scenario-II, and derive the exact closed-form expressions of SOP to quantify the impact of the proposed schemes.

A. SOP of IIbMUS Scheme

The SOP of U_n achieved by the IIbMUS scheme can be expressed as follows:

$$P_{\text{IIbMUS}} = \sum_{v=1}^{N} \Pr(\text{ScheduledUser} = U_v) \times \Pr\left(\log_2\left(1 + \frac{\rho_s \max\limits_{u_i \in U}\{|h_{u_i b}|^2\}}{1 + \rho_0 |h_{u_0 b}|^2}\right) - \log_2\left(1 + \rho_s |h_{u_v e}|^2\right) < R_s \right). \tag{19}$$

To proceed forward, we first derive the cumulative distribution function (CDF) of $X = ((\rho_s \max_{u_i \in U}\{|h_{u_i b}|^2\})/(1 + \rho_0 |h_{u_0 b}|^2))$ in (19). As the channels are subject to the Rayleigh fading, the CDF of X is given by

$$\begin{aligned} F_X(x) &= \Pr\left(\frac{\rho_s \max\limits_{u_i \in U}\{|h_{u_i b}|^2\}}{1 + \rho_0 |h_{u_0 b}|^2} < x \right) \\ &= \Pr\left(\rho_s \max_{u_i \in U}\{|h_{u_i b}|^2\} < \rho_0 x |h_{u_0 b}|^2 + x \right) \\ &= \int_0^\infty \frac{e^{-\frac{y}{\lambda_{u_0 b}}}}{\lambda_{u_0 b}} \left(\Pr\left(\rho_s |h_{u_i b}|^2 < \rho_0 x y + x \right) \right)^N dy \\ &= \int_0^\infty \frac{e^{-\frac{y}{\lambda_{u_0 b}}}}{\lambda_{u_0 b}} \left(1 - e^{-\frac{\rho_0 x y + x}{\lambda_{u_n b} \rho_s}} \right)^N dy \\ &= \sum_{k=0}^{N} \binom{N}{k} (-1)^k \frac{\rho_s \lambda_{u_n b} e^{-\frac{kx}{\rho_s \lambda_{u_n b}}}}{k \rho_0 \lambda_{u_0 b} x + \rho_s \lambda_{u_n b}} \end{aligned} \tag{20}$$

where the last step of derivation is with the aid of the binomial theorem $(a+b)^N = \sum_{k=0}^{N} \binom{N}{k} a^{N-k} b^k$.

On the basis of (20), the SOP achieved by the IIbMUS scheme is shown as follows.

Theorem 3: The SOP of U_n in the IIbMUS scheme can be given by

$$P_{\text{IIbMUS}} = 1 + \sum_{k=1}^{N} (-1)^{k+1} \binom{N}{k} \frac{\lambda_{u_n b}}{k \varepsilon_s \rho_0 \lambda_{u_n e} \lambda_{u_0 b}} \times e^{\mu\beta - \frac{k(\varepsilon_s - 1)}{\rho_s \lambda_{u_n b}}} \text{Ei}(-\mu\beta) \tag{21}$$

where $\mu = ((k\varepsilon_s \lambda_{u_n e} + \lambda_{u_n b})/(\lambda_{u_n b} \lambda_{u_n e}))$, $\beta = ([k\rho_0 \lambda_{u_0 b}(\varepsilon_s - 1) + \rho_s \lambda_{u_n b}]/k\varepsilon_s \rho_0 \rho_s \lambda_{u_0 b})$, and $\text{Ei}(\cdot)$ is the exponential integral function [45, eq. (8.21)].

Proof: See Appendix C. ∎

B. SOP of IIbOUS Scheme

The SOP of U_n with the IIbOUS scheme can be written as follows:

$$P_{\text{IIbOUS}} = \Pr\left(\max_{u_i \in U} \left\{ \log_2 \left(\frac{1 + \frac{\rho_s |h_{u_i b}|^2}{1 + \rho_0 |h_{u_0 b}|^2}}{1 + \rho_s |h_{u_i e}|^2} \right) \right\} < R_s \right). \tag{22}$$

Then, the following theorem can be given.

Theorem 4: The SOP of U_n achieved by the IIbOUS scheme can be expressed as follows:

$$P_{\text{IIbOUS}} = 1 + \frac{\lambda_{u_n b} N}{\lambda_{u_0 b} \lambda_{u_n e} \varepsilon_s \rho_0} e^{\alpha\beta_1 - \frac{\varepsilon_s - 1}{\lambda_{u_n b} \rho_s}} \text{Ei}(-\alpha\beta_1) + \sum_{k=2}^{N} (-1)^k \binom{N}{k} \frac{\lambda_{u_n b}^k e^{\frac{-k(\varepsilon_s - 1)}{\lambda_{u_n b} \rho_s}}}{\lambda_{u_0 b} \lambda_{u_n e}^k \varepsilon_s^k \rho_0^k} \Theta \tag{23}$$

where $\Theta = (1/(k-1)!) \sum_{j=1}^{k-1} (j-1)! (-\mu_1)^{k-j-1} \beta_1^{-j} - ([(-\mu_1)^{k-1}]/[(k-1)! e^{\mu_1 \beta_1}]) \text{Ei}(-\mu_1 \beta_1)$, $\alpha = ([\rho_0 \lambda_{u_0 b}(\varepsilon_s - 1) + \rho_s \lambda_{u_n b}]/\rho_s \lambda_{u_0 b} \lambda_{u_n b})$, $\beta_1 = ((\varepsilon_s \lambda_{u_n e} + \lambda_{u_n b})/\lambda_{u_n e} \varepsilon_s \rho_0)$, and $\mu_1 = ([k\rho_0 \lambda_{u_0 b}(\varepsilon_s - 1) + \rho_s \lambda_{u_n b}]/\rho_s \lambda_{u_0 b} \lambda_{u_n b})$.

Proof: See Appendix D. ∎

Remark 3: Different from the SOPs of scenario-I that are dependent on the target rate R_0 and reduced with the increase of the channel condition $\lambda_{u_0 b}$, the SOPs of scenario-II are independent from R_0 and reduced with the decrease of $\lambda_{u_0 b}$.

Remark 4: It is concluded from (15), (17), (19), and (22) that the IbOUS and IIbOUS schemes can achieve better performance than the IbMUS and IIbMUS schemes due to the use of active eavesdropper's CSI.

V. Simulation Results and Discussion

This section shows numerical results about the IbMUS, IbOUS, IIbMUS, and IIbOUS schemes to validate the theoretical analysis. In order to better demonstrate the performance enhancement of the proposed schemes, the traditional random user scheduling (TRUS) scheme [34] is used into the semi-grant-free NOMA transmission as a benchmark. For the scenario-I, the traditional maximal user scheduling (TMUS) and traditional optimal user scheduling (TOUS) schemes used in grant-based NOMA [32], [34] are also considered for the semi-grant-free NOMA transmission, where a grant-free user with maximal main channel capacity or maximal secrecy capacity is directly scheduled from all the grant-free users to access the NOMA channel without considering the QoS of the grant-based user. It is noteworthy that due to different configuration of key parameters, e.g., different locations of the grant-based user and grant-free users, the considered two scenarios are verified separately. Moreover, as one of grant-free users U_n is granted to access the resource block of U_0 by NOMA, the spectral efficiency of the system is enhanced twofold compared to the traditional grant-based NOMA using joint resource blocks consisting of U_0 and U_n. This is not

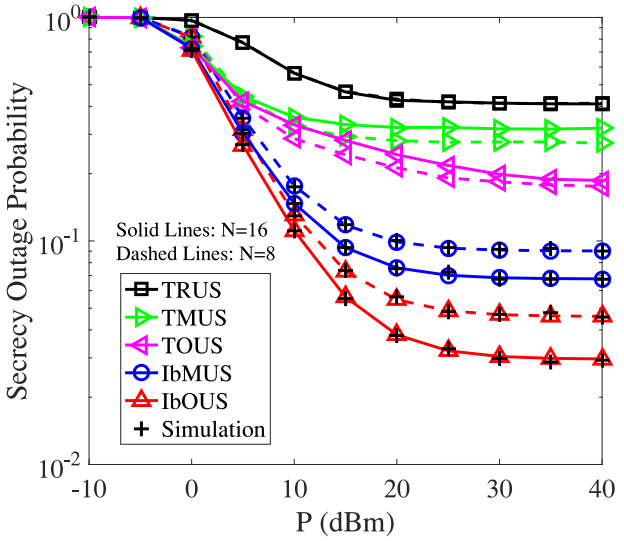


Fig. 3. SOP versus transmission power P in the scenario-I with different transmission schemes, where $d_{u_0b} = 10$ m, $d_{u_nb} = d_{u_ne} = 20$ m, $R_0 = 0.8$ BPCU, and $R_s = 0.5$ BPCU.

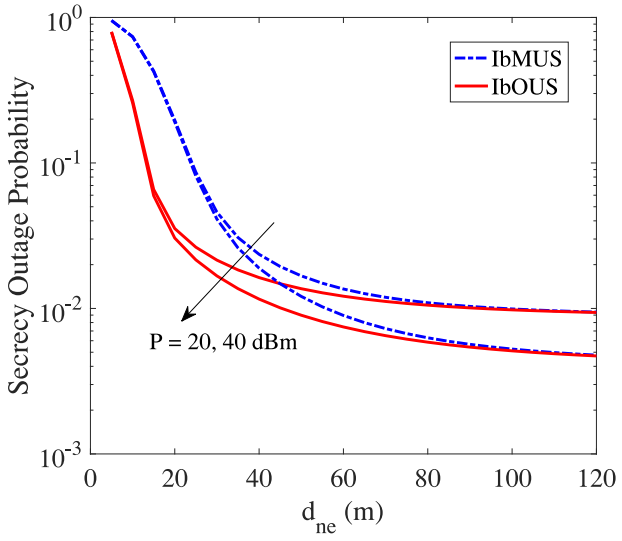


Fig. 4. Impact of distance from U_n to the eavesdropper d_{u_ne} on the SOP in the scenario-I, where $N = 16$, $d_{u_0b} = 10$ m, $d_{u_nb} = 20$ m, and $R_0 = R_s = 0.5$ BPCU.

shown in the simulation results due to its obviousness. Without loss of generality, the average channel conditions are expressed as $\lambda_{xy} = d_{xy}^{-\delta}$, where d_{xy} denotes the distance between node x and node y, and δ denotes path loss exponent. We set that $\delta = 2.7$, $N_0 = -28$ dBm, $P_0 = P_s = P$, and $\rho = P/N_0$. Moreover, some related parameters would be stated in (below) the figures. The simulated performance is obtained by performing Monte Carlo simulations over 10^5 different channel realizations.

Fig. 3 shows the SOP versus transmission power P in the scenario-I based on different transmission schemes. It is observed from the figure that the theoretical analysis for SOP of the IbMUS and IbOUS schemes accurately matches the simulation results throughout the whole power region, which verifies the correctness of the derived exact expressions. In particular, both the IbMUS and IbOUS schemes can significantly decrease the SOP compared with the TRUS, TMUS, and TOUS schemes, indicating the superiority of the proposed schemes. The mechanism behind the superiority is that the TRUS, TMUS, and TOUS schemes can not guarantee a successful SIC, but the proposed schemes can achieve a perfect SIC. Moreover, although the successful SIC can be guarantee with the proposed schemes, the performance still converges to the floors. This is because that the channel of eavesdropper is also enhanced with the increase of transmission power at users. Furthermore, owing to the use of eavesdropper's CSI, the IbOUS scheme outperforms the IbMUS scheme. The increasing number of users N is beneficial to the improvement in performance of the proposed schemes, but has no effect on the TRUS scheme.

Fig. 4 shows the impact of distance from U_n to the eavesdropper d_{u_ne} on SOP in the scenario-I. It is observed from the figure that when the eavesdropper is close to U_n, the increase of transmission power P can not improve the performance. When the eavesdropper is far away from U_n, the performance is improved with the increase of P. This is because that the

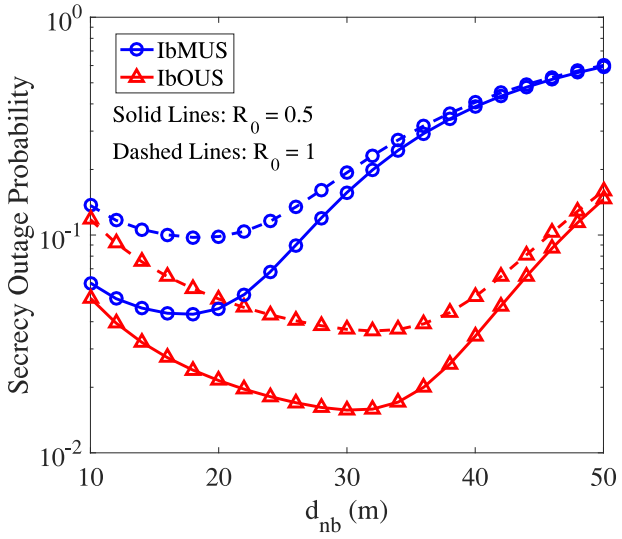


Fig. 5. Impact of distance from U_n to BS d_{u_nb} on the SOP in the scenario-I, where $N = 16$, $d_{u_0b} = 10$ m, $d_{u_ne} = 30$ m, $R_s = 0.5$ BPCU, and $P = 20$ dBm.

increase of P is beneficial to the eavesdropper with a small d_{u_ne}, while the increasing P can enhance the QoS of U_0 that has a dominant impact on the performance compared to eavesdropping in the case of a large d_{u_ne}. In particular, when the eavesdropper is far away from U_n, the IbMUS and IbOUS schemes achieve the same performance.

Fig. 5 shows the impact of distance from U_n to BS d_{u_nb} on SOP in the scenario-I. It is obtained from the figure that as d_{u_nb} increases, the SOP is first decreased and then increased. This is because that a strong channel condition of U_n is not beneficial to the implementation of successful SIC, but a weak channel condition of U_n deteriorates the secrecy performance. Moreover, the reduction of R_0 will improve the performance.

Fig. 6 shows the impact of distance from U_0 to BS d_{u_0b} on SOP in the scenario-I. It is concluded from the figure that

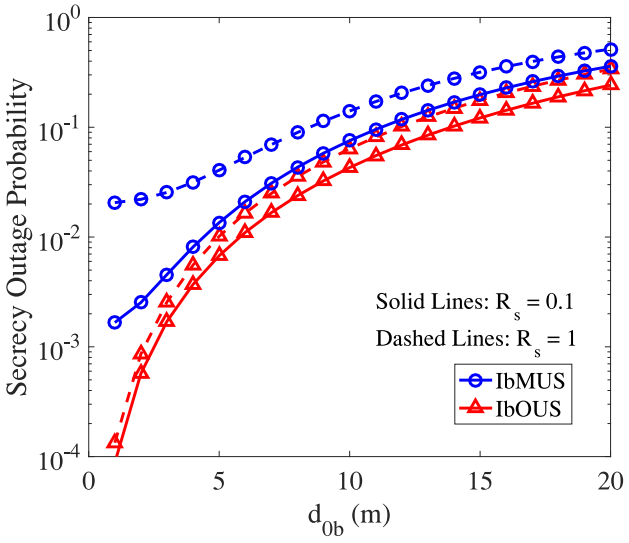


Fig. 6. Impact of distance from U_0 to BS d_{u_0b} on the SOP in the scenario-I, where $N = 16$, $d_{u_nb} = 20$ m, $d_{u_ne} = 30$ m, $R_0 = 1$ BPCU, and $P = 20$ dBm.

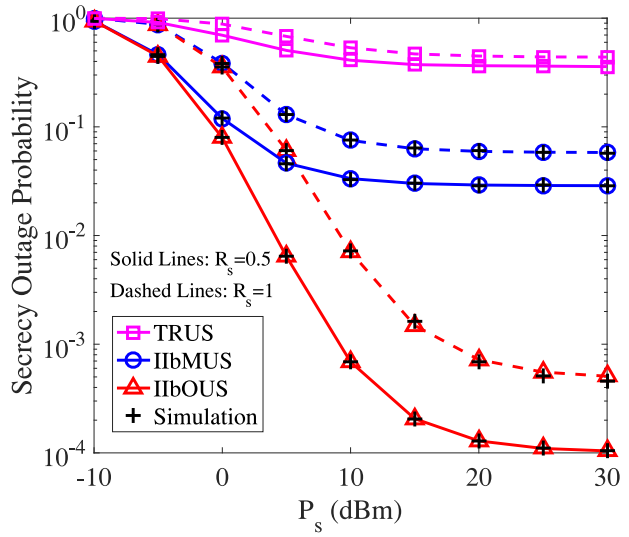


Fig. 7. SOP versus transmission power P_s in the scenario-II with different transmission schemes, where $N = 16$, $d_{u_0b} = d_{u_ne} = 20$ m, $d_{u_nb} = 10$ m, $R_s = 0.5$ BPCU, and $P_0 = 10$ dBm.

the SOP is a monotonically increasing function of d_{u_0b} and reduced with the decrease of R_s.

Fig. 7 shows the SOP versus transmission power P_s in the scenario-II based on different transmission schemes. The correctness of our theoretic analysis is validated in the figure. In particular, both the proposed IIbMUS and IIbOUS schemes observably outperform the TRUS scheme, while the IIbOUS scheme can achieve better performance than the IIbMUS scheme. Moreover, the SOP is reduced with the decrease of the target secrecy rate R_s. This indicates that the eavesdropper would be more difficult to wiretap the confidential information as the secrecy rate increases.

Fig. 8 shows the SOP versus transmission power P_0 in the scenario-II based on different transmission schemes. It is observed from the figure that the secrecy performance can be

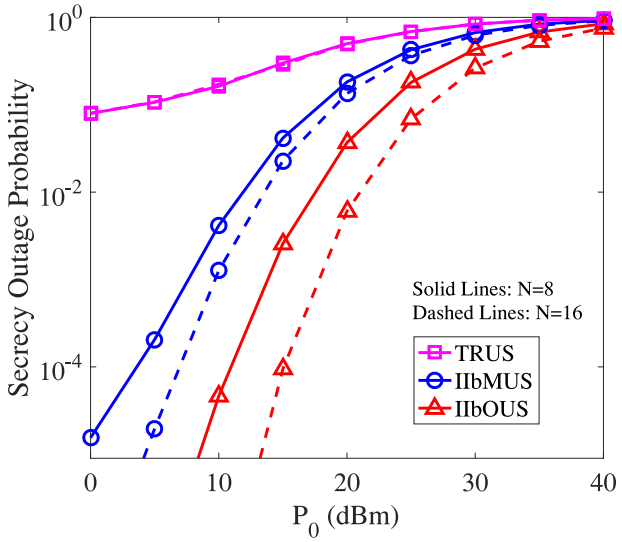


Fig. 8. SOP versus transmission power P_0 in the scenario-II with different transmission schemes, where $d_{u_nb} = 10$ m, $d_{u_0b} = d_{u_ne} = 20$ m, $R_s = 0.5$ BPCU, and $P_s = 40$ dBm.

significantly improved with the decrease of P_0, which is different from the scenario-I. In addition, similar to the scenario-I, the increasing N can enhance the performance of the proposed schemes, but has no impact on the TRUS scheme.

VI. Conclusion

In this article, we studied the security of semi-grant-free NOMA transmission for IoT. Particularly, the IbMUS and IbOUS schemes were proposed to combat the passive and active eavesdropping attacks for the scenario-I with a strong grant-based user and weak grant-free users, while the IIbMUS and IIbOUS schemes were proposed to enhance the secrecy under the passive and active eavesdropping attacks for the scenario-II with weak grant-based user and strong grant-free users. Then, the exact closed-form expressions of SOP were obtained to evaluate the performance for the system with the proposed schemes. Theoretical and simulation results indicate that the proposed schemes outperform the traditional user scheduling schemes used in grant-based NOMA in terms of the performance enhancement of semi-grant-free NOMA transmission, while the IbOUS and IIbOUS schemes can achieve better performance than the IbMUS and IIbMUS schemes owing to the use of active eavesdropper's CSI. The SOP achieved by the proposed schemes can be further improved with the increased number of grant-free users and decreasing target rate (or target secrecy rate).

Appendix A
Proof of Theorem 1

Since the fading coefficients h_{u_nb} are identically and independently distributed, we have $\Pr(\text{ScheduledUser} = U_v) = 1/l$. With the identically and independently distributed fading coefficients h_{u_ne}, $\Pr(C_s < R_s, |S_u| > 0)$ in (15) can be further expressed as (24), shown at the bottom of the next page.

In (24), the first probability term P_1 can be derived as follows:

$$\begin{aligned}P_1 &= \int_{\frac{\varepsilon_0\varepsilon_s}{\rho_0}}^{\infty}\int_0^{\frac{\rho_0 x-\varepsilon_0\varepsilon_s}{\varepsilon_0\varepsilon_s\rho_s}} \Pr\left(\max_{u_i\in S_u}\left\{|h_{u_ib}|^2\right\} < \frac{\varepsilon_s\rho_s y+\varepsilon_s-1}{\rho_s}\right)\\ &\quad\times\Pr\left(\frac{\rho_0 x-\varepsilon_0}{\varepsilon_0\rho_s} < \min_{u_i\in U\setminus S_u}\left\{|h_{u_ib}|^2\right\}\right)\frac{1}{\lambda_{u_ne}\lambda_{u_0b}}\\ &\quad\times e^{-\frac{y}{\lambda_{u_ne}}}e^{-\frac{x}{\lambda_{u_0b}}}dydx\\ &= \int_{\frac{\varepsilon_0\varepsilon_s}{\rho_0}}^{\infty}\int_0^{\frac{\rho_0 x-\varepsilon_0\varepsilon_s}{\varepsilon_0\varepsilon_s\rho_s}}\left(1-e^{-\frac{\varepsilon_s\rho_s y+\varepsilon_s-1}{\lambda_{u_nb}\rho_s}}\right)^l e^{-\frac{(\rho_0 x-\varepsilon_0)(N-l)}{\lambda_{u_nb}\varepsilon_0\rho_s}}\\ &\quad\times\frac{e^{-\frac{y}{\lambda_{u_ne}}}e^{-\frac{x}{\lambda_{u_0b}}}}{\lambda_{u_ne}\lambda_{u_0b}}dydx. \end{aligned}\tag{25}$$

By using binomial theorem and after some mathematical manipulations, P_1 in (25) can be further calculated as follows:

$$\begin{aligned}P_1 &= \sum_{k=0}^{l}\binom{l}{k}(-1)^k\frac{e^{\frac{\varepsilon_0(N-l)}{\lambda_{u_nb}\varepsilon_0\rho_s}-\frac{k(\varepsilon_s-1)}{\lambda_{u_nb}\rho_s}-\frac{\varepsilon_0\varepsilon_s\theta_2}{\rho_0}}}{\lambda_{u_ne}\lambda_{u_0b}\theta_1}\\ &\quad\times\left(\frac{1}{\theta_2}-\frac{\varepsilon_0\varepsilon_s\rho_s}{\rho_0\theta_1+\varepsilon_0\varepsilon_s\rho_s\theta_2}\right)\end{aligned}\tag{26}$$

where $\theta_1 = ((k\varepsilon_s\lambda_{u_ne}+\lambda_{u_nb})/\lambda_{u_nb}\lambda_{u_ne})$ and $\theta_2 = ([\lambda_{u_0b}\rho_0(N-l)+\lambda_{u_nb}\varepsilon_0\rho_s]/\lambda_{u_nb}\lambda_{u_0b}\varepsilon_0\rho_s)$.

In (24), the second probability term P_2 can be given by

$$\begin{aligned}P_2 &= \int_0^{\infty}\int_{\frac{\varepsilon_0}{\rho_0}}^{\frac{\varepsilon_0\varepsilon_s\rho_s x+\varepsilon_0\varepsilon_s}{\rho_0}}\left(1-e^{-\frac{\rho_0 y-\varepsilon_0}{\lambda_{u_nb}\varepsilon_0\rho_s}}\right)^l e^{-\frac{(\rho_0 y-\varepsilon_0)(N-l)}{\lambda_{u_nb}\varepsilon_0\rho_s}}\\ &\quad\times\frac{e^{-\frac{y}{\lambda_{u_0b}}}e^{-\frac{x}{\lambda_{u_ne}}}}{\lambda_{u_0b}\lambda_{u_ne}}dydx\\ &= \sum_{k=0}^{l}\binom{l}{k}(-1)^k\frac{e^{\frac{N+k-l}{\lambda_{u_nb}\rho_s}}}{\lambda_{u_0b}\theta_3}\left(e^{-\frac{\varepsilon_0\theta_3}{\rho_0}}-\frac{\rho_0 e^{-\frac{\varepsilon_0\varepsilon_s\theta_3}{\rho_0}}}{\rho_0+\varepsilon_0\varepsilon_s\lambda_{u_ne}\rho_s\theta_3}\right)\end{aligned}\tag{27}$$

where $\theta_3 = ([\lambda_{u_0b}\rho_0(N+k-l)+\lambda_{u_nb}\varepsilon_0\rho_s]/\lambda_{u_nb}\lambda_{u_0b}\varepsilon_0\rho_s)$.

By substituting (26) and (27) into (24), the solution of $\Pr(C_s < R_s, |S_u| > 0)$ can be obtained. Combining with the result in (14), the theorem is proved.

Appendix B
Proof of Theorem 2

The probability $\Pr(C_s < R_s, |S_u| > 0)$ in (17) can be calculated as (28), shown at the bottom of the next page.

In (28), the first integral term I_1 can be derived as follows:

$$\begin{aligned}I_1 &= \sum_{k=0}^{l}\binom{l}{k}(-1)^k\frac{1}{\lambda_{u_0b}\eta_1}\left(\frac{\varepsilon_s\lambda_{u_ne}}{\varepsilon_s\lambda_{u_ne}+\lambda_{u_nb}}\right)^k\\ &\quad\times\left(1-\frac{\lambda_{u_nb}e^{-\frac{\varepsilon_s-1}{\lambda_{u_nb}\rho_s}}}{\varepsilon_s\lambda_{u_ne}+\lambda_{u_nb}}\right)^{l-k}e^{\frac{k\left(\lambda_{u_ne}+\lambda_{u_nb}\right)+\lambda_{u_ne}(N-l)}{\lambda_{u_nb}\lambda_{u_ne}\rho_s}-\frac{\varepsilon_0\varepsilon_s\eta_1}{\rho_0}}\end{aligned}\tag{29}$$

where $\eta_1 = ([k\rho_0(\lambda_{u_nb}+\lambda_{u_ne}\varepsilon_s)]/\lambda_{u_ne}\lambda_{u_nb}\varepsilon_0\varepsilon_s\rho_s) + ([\rho_0(N-l)]/[\lambda_{u_nb}\varepsilon_0\rho_s]) + (1/\lambda_{u_0b})$. In (28), the second integral term I_2 can be given by

$$\begin{aligned}&\Pr(C_s < R_s, |S_u| > 0)\\ &= \sum_{l=1}^{N}\binom{N}{l}\Pr\left(\frac{1+\rho_s\max_{u_i\in S_u}\left\{|h_{u_ib}|^2\right\}}{1+\rho_s|h_{u_ne}|^2} < \varepsilon_s, \frac{\rho_0|h_{u_0b}|^2}{1+\rho_s\min_{u_i\in U\setminus S_u}\left\{|h_{u_ib}|^2\right\}} < \varepsilon_0, \frac{\rho_0|h_{u_0b}|^2}{1+\rho_s\max_{u_i\in S_u}\left\{|h_{u_ib}|^2\right\}} > \varepsilon_0\right)\\ &= \sum_{l=1}^{N}\binom{N}{l}\Pr\left(\max_{u_i\in S_u}\left\{|h_{u_ib}|^2\right\} < \frac{\varepsilon_s\rho_s|h_{u_ne}|^2+\varepsilon_s-1}{\rho_s}, \frac{\rho_0|h_{u_0b}|^2-\varepsilon_0}{\varepsilon_0\rho_s} < \min_{u_i\in U\setminus S_u}\left\{|h_{u_ib}|^2\right\},\right.\\ &\qquad\left.\frac{\rho_0|h_{u_0b}|^2-\varepsilon_0}{\varepsilon_0\rho_s} > \max_{u_i\in S_u}\left\{|h_{u_ib}|^2\right\}\right)\\ &= \sum_{l=1}^{N}\binom{N}{l}\left[\underbrace{\Pr\left(\frac{\rho_0|h_{u_0b}|^2-\varepsilon_0}{\varepsilon_0} > \varepsilon_s\rho_s|h_{u_ne}|^2+\varepsilon_s-1, |h_{u_0b}|^2 > \frac{\varepsilon_0}{\rho_0},\right.}_{P_1}\right.\\ &\qquad\underbrace{\left.\max_{u_i\in S_u}\left\{|h_{u_ib}|^2\right\} < \frac{\varepsilon_s\rho_s|h_{u_ne}|^2+\varepsilon_s-1}{\rho_s}, \frac{\rho_0|h_{u_0b}|^2-\varepsilon_0}{\varepsilon_0\rho_s} < \min_{u_i\in U\setminus S_u}\left\{|h_{u_ib}|^2\right\}\right)}_{P_1}\\ &\qquad+\underbrace{\Pr\left(\frac{\rho_0|h_{u_0b}|^2-\varepsilon_0}{\varepsilon_0} < \varepsilon_s\rho_s|h_{u_ne}|^2+\varepsilon_s-1, |h_{u_0b}|^2 > \frac{\varepsilon_0}{\rho_0}, \max_{u_i\in S_u}\left\{|h_{u_ib}|^2\right\} < \frac{\rho_0|h_{u_0b}|^2-\varepsilon_0}{\varepsilon_0\rho_s},\right.}_{P_2}\\ &\qquad\left.\left.\underbrace{\frac{\rho_0|h_{u_0b}|^2-\varepsilon_0}{\varepsilon_0\rho_s} < \min_{u_i\in U\setminus S_u}\left\{|h_{u_ib}|^2\right\}\right)}_{P_2}\right]\end{aligned}\tag{24}$$

$$I_2=\sum_{k=0}^{l}\binom{l}{k}(-1)^k\frac{e^{\frac{N+k-l}{\lambda_{u_nb}\rho_s}}}{\lambda_{u_0b}\eta_2}\left(e^{-\frac{\varepsilon_0\eta_2}{\rho_0}}-e^{-\frac{\varepsilon_0\varepsilon_s\eta_2}{\rho_0}}\right) \quad (30)$$

where $\eta_2 = (k\rho_0/\lambda_{u_nb}\varepsilon_0\rho_s) + ([\rho_0(N-l)]/\lambda_{u_nb}\varepsilon_0\rho_s) + (1/\lambda_{u_0b})$.

By substituting (29) and (30) into (28), the solution of $\Pr(C_s < R_s, |S_u| > 0)$ can be obtained. Combining with the result in (14), the theorem is proved.

Appendix C
Proof of Theorem 3

Similar to the proof of Theorem 1, P_{IIbMUS} in (19) can be rewritten as follows:

$$P_{\text{IIbMUS}}=\Pr\left(1+\frac{\rho_s\max\limits_{u_i\in U}\{|h_{u_ib}|^2\}}{1+\rho_0|h_{u_0b}|^2}<\varepsilon_s\rho_s|h_{u_ne}|^2+\varepsilon_s\right). \quad (31)$$

With the helps of (20) and [45, eq. (3.352.4)], P_{IIbMUS} is further derived as follows:

$$\begin{aligned}P_{\text{IIbMUS}}&=\int_0^\infty F_X(\varepsilon_s\rho_s y+\varepsilon_s-1)\frac{e^{-\frac{y}{\lambda_{u_ne}}}}{\lambda_{u_ne}}dy\\&=1+\sum_{k=1}^{N}\binom{N}{k}(-1)^k\frac{\lambda_{u_nb}e^{-\frac{k(\varepsilon_s-1)}{\lambda_{u_nb}\rho_s}}}{k\lambda_{u_0b}\lambda_{u_ne}\varepsilon_s\rho_0}\\&\quad\times\int_0^\infty e^{-\frac{(k\varepsilon_s\lambda_{u_ne}+\lambda_{u_nb})y}{\lambda_{u_nb}\lambda_{u_ne}}}\frac{1}{y+\beta}dy\\&=1+\sum_{k=1}^{N}(-1)^{k+1}\binom{N}{k}\frac{\lambda_{u_nb}}{k\varepsilon_s\lambda_{u_ne}\lambda_{u_0b}\rho_0}\\&\quad\times e^{\mu\beta-\frac{k(\varepsilon_s-1)}{\lambda_{u_nb}\rho_s}}\text{Ei}(-\mu\beta)\end{aligned} \quad (32)$$

where $\mu = ((k\varepsilon_s\lambda_{u_ne}+\lambda_{u_nb})/\lambda_{u_nb}\lambda_{u_ne})$, $\beta = ([k\lambda_{u_0b}\rho_0(\varepsilon_s-1)+\lambda_{u_nb}\rho_s]/k\varepsilon_s\lambda_{u_0b}\rho_0\rho_s)$, and $\text{Ei}(\cdot)$ is the exponential integral function [45, eq. (8.21)].

Hence, the proof is completed.

Appendix D
Proof of Theorem 4

The SOP P_{IIbOUS} in (22) can be derived as follows:

$$\begin{aligned}P_{\text{IIbOUS}}&=\int_0^\infty\Pr\left(\max_{u_i\in U}\left\{\frac{1+\frac{\rho_s|h_{u_ib}|^2}{1+\rho_0x}}{1+\rho_s|h_{u_ie}|^2}\right\}<\varepsilon_s\right)\frac{e^{-\frac{x}{\lambda_{u_0b}}}}{\lambda_{u_0b}}dx\\&=\int_0^\infty\left(\int_0^\infty\left(1-e^{-\frac{(\varepsilon_s-1)(\rho_0x+1)+\varepsilon_s\rho_s(\rho_0x+1)y}{\lambda_{u_nb}\rho_s}}\right)\right.\\&\quad\left.\times\frac{e^{-\frac{y}{\lambda_{u_ne}}}}{\lambda_{u_ne}}dy\right)^N\frac{e^{-\frac{x}{\lambda_{u_0b}}}}{\lambda_{u_0b}}dx\\&=\sum_{k=0}^{N}\binom{N}{k}(-1)^k\frac{\lambda_{u_nb}^k}{\lambda_{u_0b}\lambda_{u_ne}^k\varepsilon_s^k\rho_0^k}e^{-\frac{k(\varepsilon_s-1)}{\lambda_{u_nb}\rho_s}}\\&\quad\times\int_0^\infty\frac{e^{-\left(\frac{k\rho_0(\varepsilon_s-1)}{\lambda_{u_nb}\rho_s}+\frac{1}{\lambda_{u_0b}}\right)x}}{\left(x+\frac{\varepsilon_s\lambda_{u_ne}+\lambda_{u_nb}}{\varepsilon_s\lambda_{u_ne}\rho_0}\right)^k}dx.\end{aligned} \quad (33)$$

With the aid of [45, eq. (3.353.2)], P_{IIbOUS} in (33) can be further calculated as follows:

$$\begin{aligned}P_{\text{IIbOUS}}&=1+\frac{\lambda_{u_nb}N}{\lambda_{u_0b}\lambda_{u_ne}\varepsilon_s\rho_0}e^{\alpha\beta_1-\frac{\varepsilon_s-1}{\lambda_{u_nb}\rho_s}}\text{Ei}(-\alpha\beta_1)\\&\quad+\sum_{k=2}^{N}(-1)^k\binom{N}{k}\frac{\lambda_{u_nb}^k e^{\frac{-k(\varepsilon_s-1)}{\lambda_{u_nb}\rho_s}}}{\lambda_{u_0b}\lambda_{u_ne}^k\varepsilon_s^k\rho_0^k}\Theta\end{aligned} \quad (34)$$

where $\Theta = (1/(k-1)!)\sum_{j=1}^{k-1}(j-1)!(-\mu_1)^{k-j-1}\beta_1^{-j} - ((-\mu_1)^{k-1}/(k-1)!)e^{\mu_1\beta_1}\text{Ei}(-\mu_1\beta_1)$, $\alpha = ([\lambda_{u_0b}\rho_0(\varepsilon_s-1)+\lambda_{u_nb}\rho_s]/\lambda_{u_0b}\lambda_{u_nb}\rho_s)$, $\beta_1 = ((\varepsilon_s\lambda_{u_ne}+\lambda_{u_nb})/\lambda_{u_ne}\varepsilon_s\rho_0)$, and $\mu_1 = ([k\lambda_{u_0b}\rho_0(\varepsilon_s-1)+\lambda_{u_nb}\rho_s]/\lambda_{u_0b}\lambda_{u_nb}\rho_s)$.

Therefore, the proof is completed.

$$\begin{aligned}&\Pr(C_s<R_s,|S_u|>0)\\&=\sum_{l=1}^{N}\binom{N}{l}\int_{\frac{\varepsilon_0}{\rho_0}}^{\infty}\Pr\left(\max_{u_i\in S_u}\left\{\frac{1+\rho_s|h_{u_ib}|^2}{1+\rho_s|h_{u_ie}|^2}\right\}<\varepsilon_s,\frac{\rho_0x}{1+\rho_s\max\limits_{u_i\in S_u}\{|h_{u_ib}|^2\}}>\varepsilon_0\right)\\&\quad\times\Pr\left(\frac{\rho_0x-\varepsilon_0}{\varepsilon_0\rho_s}<\min_{u_i\in U\setminus S_u}\{|h_{u_ib}|^2\}\right)\frac{1}{\lambda_{u_0b}}e^{-\frac{x}{\lambda_{u_0b}}}dx\\&=\sum_{l=1}^{N}\binom{N}{l}\left[\underbrace{\int_{\frac{\varepsilon_0\varepsilon_s}{\rho_0}}^{\infty}\prod_{i=1}^{l}\left\{\Pr\left(|h_{u_ie}|^2>\frac{\rho_0x-\varepsilon_0\varepsilon_s}{\varepsilon_0\varepsilon_s\rho_s},|h_{u_ib}|^2<\frac{\rho_0x-\varepsilon_0}{\varepsilon_0\rho_s}\right)+\Pr\left(|h_{u_ie}|^2<\frac{\rho_0x-\varepsilon_0\varepsilon_s}{\varepsilon_0\varepsilon_s\rho_s},\right.\right.\right.}_{I_1}\\&\quad\underbrace{\left.\left.\left.|h_{u_ib}|^2<\frac{\varepsilon_s\rho_s|h_{u_ie}|^2+\varepsilon_s-1}{\rho_s}\right)\right\}e^{-\frac{(\rho_0x-\varepsilon_0)(N-l)}{\lambda_{u_nb}\varepsilon_0\rho_s}}\frac{1}{\lambda_{u_0b}}e^{-\frac{x}{\lambda_{u_0b}}}dx}_{I_1}\\&\quad+\underbrace{\int_{\frac{\varepsilon_0}{\rho_0}}^{\frac{\varepsilon_0\varepsilon_s}{\rho_0}}\prod_{i=1}^{l}\left\{\Pr\left(|h_{u_ib}|^2<\frac{\rho_0x-\varepsilon_0}{\varepsilon_0\rho_s}\right)\right\}e^{-\frac{(\rho_0x-\varepsilon_0)(N-l)}{\lambda_{u_nb}\varepsilon_0\rho_s}}\frac{1}{\lambda_{u_0b}}e^{-\frac{x}{\lambda_{u_0b}}}dx}_{I_2}\Bigg]\end{aligned} \quad (28)$$

REFERENCES

[1] Z. Ding, "Harvesting devices' heterogeneous energy profiles and QoS requirements in IoT: WPT-NOMA vs BAC-NOMA," *IEEE Trans. Commun.*, vol. 69, no. 5, pp. 2837–2850, May 2021.

[2] Z. Ding *et al.*, "Application of non-orthogonal multiple access in LTE and 5G networks," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 185–191, Feb. 2017.

[3] D. Wan, M. Wen, F. Ji, H. Yu, and F. Chen, "Non-orthogonal multiple access for cooperative communications: Challenges, opportunities, and trends," *IEEE Wireless Commun.*, vol. 25, no. 2, pp. 109–117, Apr. 2018.

[4] L. Dai, B. Wang, Z. Ding, Z. Wang, S. Chen, and L. Hanzo, "A survey of non-orthogonal multiple access for 5G," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2294–2323, 3rd Quart., 2018.

[5] Y. Saito, Y. Kishiyama, A. Benjebbour, T. Nakamura, A. Li, and K. Higuchi, "Non-orthogonal multiple access (NOMA) for cellular future radio access," in *Proc. IEEE VTC-Spring*, Dresden, Germany, Jun. 2013, pp. 1–5.

[6] L. Dai, B. Wang, Y. Yuan, S. Han, I. Chin-Lin, and Z. Wang, "Non-orthogonal multiple access for 5G: Solutions, challenges, opportunities, and future research trends," *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 74–81, Sep. 2015.

[7] Z. Ding, M. Peng, and H. V. Poor, "Cooperative non-orthogonal multiple access in 5G systems," *IEEE Commun. Lett.*, vol. 19, no. 8, pp. 1462–1465, Aug. 2015.

[8] N. Zhang, J. Wang, G. Kang, and Y. Liu, "Uplink nonorthogonal multiple access in 5G systems," *IEEE Commun. Lett.*, vol. 20, no. 3, pp. 458–461, Mar. 2016.

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

[10] 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.

[11] S. M. R. Islam, N. Avazov, O. A. Dobre, and K.-S. Kwak, "Power-domain non-orthogonal multiple access (NOMA) in 5G systems: Potentials and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 721–742, 2nd Quart., 2017.

[12] Y. Liu, Z. Qin, M. Elkashlan, Z. Ding, A. Nallanathan, and L. Hanzo, "Nonorthogonal multiple access for 5G and beyond," *Proc. IEEE*, vol. 105, no. 12, pp. 2347–2381, Dec. 2017.

[13] N. Jayanth, P. Chakraborty, M. Gupta, and S. Prakriya, "Performance of semi-grant free uplink with non-orthogonal multiple access," in *Proc. IEEE Annu. Int. Symp. Pers. Indoor Mobile Radio Commun.*, London, U.K., 2020, pp. 1–6.

[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, Z. Qin, Y. Liu, and K. K. Chai, "Semi-grant-free uplink NOMA with contention control: A stochastic geometry model," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Dublin, Ireland, 2020, pp. 1–6.

[16] 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.

[17] 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.

[18] 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.

[19] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[20] 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.

[21] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quat., 2014.

[22] L. Sun and Q. Du, "Physical layer security with its applications in 5G networks: A review," *China Commun.*, vol. 14, no. 12, pp. 1–14, Dec. 2017.

[23] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, 1st Quart., 2016.

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

[25] Y. Zhang, H.-M. Wang, Q. Yang, and Z. Ding, "Secrecy sum rate maximization in non-orthogonal multiple access," *IEEE Commun. Lett.*, vol. 20, no. 5, pp. 930–933, May 2016.

[26] 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.

[27] X. Chen, Z. Zhang, C. Zhong, D. W. K. Ng, and R. Jia, "Exploiting inter-user interference for secure massive non-orthogonal multiple access," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 788–801, Apr. 2018.

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

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

[30] Y. Feng, S. Yan, Z. Yang, N. Yang, and J. Yuan, "Beamforming design and power allocation for secure transmission with NOMA," *IEEE Trans. Wireless Commun.*, vol. 18, no. 5, pp. 2639–2651, May 2019.

[31] B. M. ElHalawany, R. Ruby, T. Riihonen, and K. Wu, "Performance of cooperative NOMA systems under passive eavesdropping," in *Proc. IEEE Global Commun. Conf.*, Abu Dhabi, UAE, 2018, pp. 1–6.

[32] H. 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.

[33] 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, pp. 3191–3205, 2019.

[34] K. Cao, B. Wang, H. Ding, L. Lv, J. Tian, and F. Gong, "On the security enhancement of uplink NOMA systems with jammer selection," *IEEE Trans. Commun.*, vol. 68, no. 9, pp. 5747–5763, Sep. 2020.

[35] K. Cao *et al.*, "Improving physical layer security of uplink NOMA via energy harvesting jammers," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 786–799, 2021.

[36] W. Wang *et al.*, "Joint precoding optimization for secure SWIPT in UAV-aided NOMA networks," *IEEE Trans. Commun.*, vol. 68, no. 8, pp. 5028–5040, Aug. 2020.

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

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

[39] Y. Feng, S. Yan, C. Liu, Z. Yang, and N. Yang, "Two-stage relay selection for enhancing physical layer security in non-orthogonal multiple access," *IEEE Trans. Inf. Forensics Security*, vol. 14, pp. 1670–1683, 2019.

[40] F. Zhou, Z. Chu, H. Sun, R. Q. Hu, and L. Hanzo, "Artificial noise aided secure cognitive beamforming for cooperative MISO-NOMA using SWIPT," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 930–931, Apr. 2018.

[41] K. Cao, B. Wang, H. Ding, T. Li, and F. Gong, "Optimal relay selection for secure NOMA systems under untrusted users," *IEEE Trans. Veh. Technol.*, vol. 69, no. 2, pp. 1942–1955, Feb. 2020.

[42] C. Zhang, F. Jia, Z. Zhang, J. Ge, and F. Gong, "Physical layer security designs for 5G NOMA systems with a stronger near-end internal eavesdropper," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13005–13017, Nov. 2020.

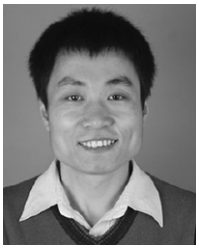
[43] B. M. ElHalawany and K. Wu, "Physical-layer security of NOMA systems under untrusted users," in *Proc. IEEE Global Commun. Conf.*, Abu Dhabi, UAE, 2018, pp. 1–6.

[44] S. Thapar, D. Mishra, and R. Saini, "Novel outage-aware NOMA protocol for secrecy fairness maximization among untrusted users," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13259–13272, Nov. 2020.

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

Kunrui Cao received the Ph.D. degree from Air Force Engineering University, Xi'an, China, in 2020.

He is currently an Assistant Professor with the School of Information and Communications, National University of Defense Technology, Wuhan, China, and an Academic Visitor with the State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an. His research interests include physical-layer security, nonorthogonal multiple access, and intelligent reflecting surface.



Haiyang Ding (Member, IEEE) received the B.Sc. degree in communications engineering from Xi'an Communications Institute, Xi'an, China, in 2003, the M.Sc. degree (Hons.) in electrical engineering from Beijing University of Technology, Beijing, China, in 2006, and the Ph.D. degree (Hons.) in telecommunications engineering from Xidian University, Xi'an, in 2013.

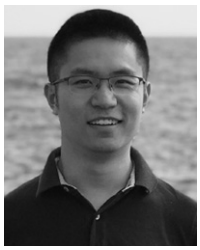
From 2016 to 2017, he was a Visiting Scholar with the Department of Electrical Engineering, Columbia University, New York, NY, USA. Since 2017, he has been with the faculty of the School of Information and Communications, National University of Defense Technology, Wuhan, China. His research interests include backscatter communications, energy harvesting, cooperative communications, and cognitive radio systems.

Dr. Ding was a recipient of the Research in Motion Wireless Research Scholarship from Xidian University in 2012, the IEEE COMMUNICATIONS LETTERS Exemplary Reviewer Certificate in 2013, the IEEE TRANSACTIONS ON COMMUNICATIONS Exemplary Reviewer Certificate in 2014, and the Excellent Ph.D. Dissertation Certificate of Shaanxi Province in 2015. He has served as an Editor for the IEEE OPEN JOURNAL OF THE COMMUNICATIONS SOCIETY and a Guest Editor for the IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING.

Buhong Wang (Member, IEEE) received the M.S. and Ph.D. degrees in signal and information processing from Xidian University, Xi'an, China, in 2000 and 2003, respectively.

From 2003 to 2005, with the support of the National Post-Doctoral Science Foundation, he was a Postdoctoral Fellow with the Post-Doctoral Technical Innovation Center, Nanjing Research Institute of Electronics Technology, Nanjing, China. From 2006 to 2008, he was an Associate Professor with the School of Electronic Engineering, Xidian University. From 2009 to 2010, he was a Research Fellow with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore. Since 2012, he has been a Professor with the Information and Navigation College, Air Force Engineering University, Xi'an. His research interests include MIMO communication, array signal processing, and physical-layer security.

Prof. Wang was honored as the Excellent Doctoral Dissertation of Shaanxi Province for his Ph.D. degree thesis "On Some Crucial Aspects of High-Resolution Direction of Arrival Estimation" from Xidian University.



Lu Lv (Member, IEEE) received the Ph.D. degree from Xidian University, Xi'an, China, in 2018.

From 2016 to 2018, he was an Academic Visitor with Lancaster University, Lancaster, U.K., and the University of Alberta, Edmonton, AB, Canada. In 2019, he was a Postdoctoral Fellow with Dalhousie University, Halifax, NS, Canada. He is currently an Associate Professor with the State Key Laboratory of Integrated Services Networks, Xidian University. His research interests include nonorthogonal multiple access, physical-layer security, intelligent reflecting surface, and covert communication.

Dr. Lv was a recipient of the Outstanding Ph.D. Thesis Award of Shannxi Province in 2020, the IEEE ICCC Best Paper Award in 2021, and the Exemplary Reviewer Certificate for the IEEE TRANSACTIONS ON COMMUNICATIONS from 2018 to 2020. He serves as an Associate Editor for the IEEE Internet of Things, Ad Hoc and Sensor Networks Technical Committee Newsletter and *Frontiers of Computer Science*. He is the Lead Guest Editor for the IEEE INTERNET OF THINGS JOURNAL on "Symbiotic Active/Passive Communications for the Internet of Things."

Jiwei Tian received the Ph.D. degree from Air Force Engineering University, Xi'an, China, in 2021.

He is currently a Lecturer with the Air Traffic Control and Navigation College, Air Force Engineering University. His research interests include cyber–physical system security and AI security.

Qingmei Wei received the B.S. and M.S. degrees from Xidian University, Xi'an, China, in 2006 and 2015, respectively. She is currently pursuing the Ph.D. degree with the School of Information and Navigation, Air Force Engineering University, Xi'an.

She is currently an Associate Professor with Air Force Engineering University. Her research interests include physical-layer security and nonorthogonal multiple access.

Fengkui Gong (Member, IEEE) was born in Shandong Province, China, in 1979. He received the M.Sc. and Ph.D. degrees from Xidian University, Xi'an, China, in 2004 and 2007, respectively.

From October 2011 to October 2012, he worked as a Visiting Scholar with the Department of Electrical and Computer Engineering, McMaster University, Hamilton, ON, Canada. He is currently a Professor with the State Key Laboratory of Integrated Services Networks, Department of Communication Engineering, Xidian University. His research interests include cooperative communication, distributed space-time coding, digital video broadcasting systems, satellite communication, and 4G/5G techniques.