IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 23, 2020, accepted December 29, 2020, date of publication January 5, 2021, date of current version January 19, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3049258

Security Improvement With QoS Provisioning Using Service Priority and Power Allocation for NOMA-IoT Networks

WAQAS KHALID [1] AND HEEJUNG YU [2,3], (Senior Member, IEEE)

[1]Institute of Industrial Technology, Korea University, Sejong 30019, South Korea
[2]Department of Electronics and Information Engineering, Korea University, Sejong 30019, South Korea
[3]Interdisciplinary Graduate Program for Artificial Intelligence Smart Convergence Technology, Korea University, Sejong 30019, South Korea

Corresponding author: Heejung Yu (heejungyu@korea.ac.kr)

This work was supported in part by the National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIT) under Grant 2019R1A2C1083988, and in part by the MSIT, South Korea, through the Information Technology Research Center (ITRC) Support Program, supervised by the Institute for Information & Communications Technology Promotion (IITP), under Grant IITP-2020-2016-0-00313.

ABSTRACT Non-orthogonal multiple access (NOMA) has gained attention as a promising multiple access scheme for the Internet of Things (IoT). A typical setting of user ordering in NOMA networks with user priority difference allows a service priority for solely low-rate high-priority users. In contrast, the diverse quality of service (QoS) requirements and service priorities are prerequisite features of users in the IoT. In this paper, we consider a downlink transmission scenario for NOMA-IoT networks in which the base station (BS) simultaneously serves the two users with a priority difference. To tackle the requirements of the IoT, we consider two schemes: a service priority scheme for high-priority user (SP-HP), and a service priority scheme for low-priority user (SP-LP). Meanwhile, the BS adopts a power allocation strategy to realize the desirable QoS provision for high-priority user and optimize the outage experience of low-priority user in an opportunistic manner. It is novel and interesting to extend the NOMA-IoT framework for a malicious attempt of a passive eavesdropper. To investigate the efficiency and security performances of both schemes, the connection and secrecy outage probabilities of both users are characterized, and their closed-form expressions are derived over Rayleigh fading channels. An effective secrecy throughput (EST) is presented to holistically characterize the performance of the system. Numerical results validate the accuracy of the theoretical results. The results suggest that the transmit power of both users in each scheme can be optimized for the maximum EST, and a selection of an optimal scheme for the reliable and secure transmissions of both users is possible under certain channel conditions.

INDEX TERMS Physical layer security, non-orthogonal multiple access (NOMA), IoT networks, service priority, power allocation, Rayleigh fading.

I. INTRODUCTION

A. Background

Recent developments in wireless communication have presented a new networking paradigm, the Internet of Things (IoT) [1]. The IoT connects devices to the Internet, that is, makes the devices uniquely addressable. Further, the IoT provides machine-to-machine or human-to-machine communications anytime, anyplace, with anyone, using any network (or service). Internet-based smart terminals, services, and applications (e.g., smart gadgets, home appliances, remote management systems, autonomous cars, health-care devices, online courses, cyber gaming, artificial intelligence, and virtual reality) have led to a massive volume of data traffic. By 2030, the Internet-connected mobile terminals are expected to be over 30 billion, and the global mobile traffic volume is predicted to be 5016 Ebytes/month [2]. This statistic imposes the challenging requirements of ubiquitous connectivity and bandwidth demands and leads to spectrum scarcity because of the limited spectrum resources. Furthermore, it depicts the importance of promising techniques and improved communication systems that ameliorate spectrum

The associate editor coordinating the review of this manuscript and approving it for publication was Qing Yang.

efficiency. Compared with 4G, 5G provides improvements in orders of magnitude, including 1000 times higher mobile data volume per geographical area, 10-1000 times more connected devices, 10-1000 times higher user data rate (with a peak terminal data rate up to 10 GB/s), one-tenth the energy consumption, and sub-millisecond end-to-end latency [3]. Owing to their technological advantages and highly demanding disruptive capabilities, including low-latency, high-throughput, spectrum allocation flexibility, and utilization efficiency, 5G cellular networks provide solutions to the ubiquitous connectivity and spectral demands of IoT networks [4]. Apart from the crux technologies of 5G networks, such as long-term evolution (LTE) - wireless local area network (WLAN) aggregation (LWA) [5], operations in the millimeter wave band (i.e., mmWave communications) [6], advanced spectrum approaches such as licensed-assisted access and 5G New Radio in the unlicensed spectrum [7], multicasting [8], layer division multiplexing (LDM) [9], ultra-dense small cells [10], software-defined cognitive radio [11], [12], the novel multiple access (MA) techniques exhibit the potential to increase spectrum utilization [13]–[17].

B. Related Works

Owing to the superior spectrum utilization efficiency and system throughput, non-orthogonal multiple access (NOMA) has the inherent features to support large-scale heterogeneous data traffic and has been envisioned as a key enabling technique for 5G-connected IoT systems [17]–[26]. The characteristic of heterogeneous data traffic in IoT provides a natural fit for the adoption of NOMA, and the combination of two technologies results in the unrivaled effectiveness. In contrast to the conventional orthogonal multiple access (OMA) schemes, NOMA suggests a paradigm shift in accessing networks. The primary approach of NOMA is to remove the orthogonality between the allocated resource blocks and serve multiple users simultaneously. The power-domain NOMA, multi-user shared access, lattice partition MA, sparse code MA, and pattern division MA are the recent NOMA approaches proposed for 5G wireless networks. Furthermore, the NOMA principles have been considered in the development of standards, including LDM in the next-generation broadcasting systems and multi-user superposition transmission in the 3GPP LTE Advanced. Without any doubt, NOMA techniques have attracted significant research interest from both the academia and industry. In particular, the power-domain NOMA allows multiple users to share the same non-orthogonal radio resources (i.e., time/frequency/code) via superposition coding, power allocation (PA), and successive interference cancellation (SIC) and results in significant channel capacity and spectrum efficiency gains [26]–[30]. The signals of multiple users are superimposed with distinct PA factors at the transmitter side in order to transmit over the same channel, while the SIC is carried out at the receiver side exploiting the difference in channel gain. Nonetheless, the design of optimal PA and decoding order strategies is required to obtain the performance benefits of the power-domain NOMA networks.

Apart from the random and diverse high-volume user data, IoT networks deal with the heterogeneity in terms of the services, classification of devices, deployment scenarios, environments, and mobility. The large number of users (i.e., active connections), with diversified quality of service (QoS) requirements and service priorities, cause serious challenges for researchers in the design of efficient transmission schemes for NOMA-IoT networks [15], [16]. In addition, any form of data leakage is unacceptable for the users. However, it is a remarkable fact that the private data is susceptible to the malicious overhearing attacks because of the inherent broadcasting nature of wireless transmission. Therefore, information security is an imminent concern particularly in IoT networks, and is a prerequisite for most IoT applications [17]–[19]. Guaranteeing the transmission security from application layer to physical layer is crucial. Traditionally, secure communication at higher layers has been realized with encryption and cryptographic techniques. For example, encryption techniques, such as a shared-key method and a private-key method, are considered in the network layer. However, the high layer security approaches are becoming inadequate and impractical owing to the complicated 5G-IoT architecture and advancements in the computational capabilities of eavesdroppers.

Triggered by this, the physical layer security (PLS), which is unaffected by the network scale, was proposed as an alternative [30]–[33]. The key idea in PLS is to utilize the physical characteristics of the wireless channels to secure the confidentiality of the data transmission. The PLS controls the physical signal, that is, makes it decodable for legitimate users only. In PLS, the difference between the channel capacities of the main data link, that is, between the source and destination, and the wiretap link, that is, between the source and eavesdropper, is termed as the secrecy capacity, which is a performance measure for the PLS. In addition, the probability of a secrecy outage for a given secrecy rate is used to evaluate the secrecy performance of systems.

The remainder of this paper is organized as follows. Section II details the motivation and contributions. In Section III, we present the novel NOMA-IoT framework, including the system description and design of both schemes. To analyze the reliability and security of users, the closed-form expressions of connection outage probability (COP), secrecy outage probability (SOP) and effective secrecy throughput (EST) are characterized for both schemes in Section IV. The numerical results are presented in Section V to validate the analytical results and demonstrate the performance comparison. Finally, the conclusions of the paper are presented in Section VI.

Notations: Pr[.] denotes the probability of an event. $\mathcal{E}(.)$ is the expectation operation. $F_X(.)$ and $f_X(.)$ represent the cumulative density function (CDF) and probability density function (PDF) of a random variable X, respectively. $W_{k,m}(.)$,

and $K_v(.)$ are the Whittaker and modified Bessel functions of the second kind, respectively.

It is noted that the abbreviations and symbols used in this paper are listed in Tables 1 and 2, respectively.

TABLE 1. A list of abbreviations.

Abbreviation	Description
MA	Multiple access
NOMA	Non-orthogonal multiple access
IoT	Internet of Things
4G	The fourth generation
5G	The fifth generation
LDM	Layer division multiplexing
BS	Base station
SINR	Signal-to-interference-plus-noise ratio
PA	Power allocation
SIC	Successive interference cancellation
CSI	Channel state information
QoS	Quality of service
PDF	Probability density function
CDF	Cumulative density function
PLS	Physical layer security
SP-HP	Service priority for high-priority user
SP-LP	Service priority for low-priority user
COP	Connection outage probability
SOP	Secrecy outage probability
EST	Effective secrecy throughput

TABLE 2. Notations in the system model.

Notations	Definition
Γ_i^1	Decoding SINR at user i in SP-HP scheme
Γ_i^2	Decoding SINR at user i in SP-LP scheme
$\|h_p\|^2$	Channel power gain
g_p	Mean of $\|h_p\|^2$
ω_p	Rate parameter of $\|h_p\|^2$
y_i	Received signal at user i
r_i	Target transmission rate of user i
r_{si}	Target secrecy rate of user i
$r_i - r_{si}$	Redundancy rate (against eavesdropping) of user i
χ_i	Detection SNR threshold of user i
ρ_B	Average SNR at BS (transmit SNR)
b^*	Optimal PA coefficient in SP-HP scheme
$b^\dagger$	Optimal PA coefficient in SP-LP scheme
$P_{CO.i}^1$	COP of user i in SP-HP scheme
$P_{CO.i}^2$	COP of user i in SP-LP scheme
$P_{SO.i}^1$	SOP of user i in SP-HP scheme
$P_{SO.i}^2$	SOP of user i in SP-LP scheme
η_i^1	EST of user i in SP-HP scheme
η_i^2	EST of user i in SP-LP scheme

II. Motivation AND Contributions

The users in conventional NOMA networks are distinguished by their QoS requirements or the channel conditions. In particular, the users in the NOMA networks with user priority difference are ordered according to the different QoS requirements, as such an approach offers the advantage of designing the user scheduling, PA, and SIC ordering more appropriately to meet the QoS demands [21]. The QoS requirements of NOMA users can be supported effectively for different IoT scenarios, i.e., small packet business, telemedicine services, or performing some background tasks. For such networks, an appropriate target problem is to obtain the best performance of low-priority users while satisfying the QoS requirements of high-priority users. The low-priority users are served in an opportunistic manner when the QoS requirements of high-priority users are guaranteed [22]. Alternatively, we can view the addressed NOMA scenario, i.e., NOMA networks with different priority levels, as a special case of cognitive ratio inspired NOMA networks. Here, high-priority users are regarded as primary users whose QoS requirements are needed to be satisfied strictly, and low-priority users are the secondary users who are served opportunistically. In particular, the two commonly used PA policies, that is, the fixed and dynamic PA, are considered for NOMA networks with user priority difference. In the fixed PA approach [23], [24], a set of PA coefficients is predefined, and a typical setting is to allocate more power to high-priority user. However, the fixed PA strategy does not guarantee the QoS requirement of high-priority user because a wrong choice of PA coefficients always leads to an outage probability, and it also fails to provide the best performance to low-priority user. In the latter approach [22], a set of PA coefficients is not predetermined and is dynamically adjusted to satisfy the target problem.

Most existing works [27], [28] considered a typical setting of user ordering and adopted a fixed decoding order policy. Under such a setting, high-priority user is always assumed to be a delay-sensitive user, that is, it gets the service priority with less demanding QoS requirement. Consequently, low-priority user is always served in a delay-tolerant manner, that is, it is served after the high-priority user and is considered to have a high target data rate. The authors in [29] considered the diverse service priorities of both users in the conventional NOMA networks, that is, without user priority difference. Moreover, service priority is provided based on the channel condition, irrespective of the QoS requirement. In particular, the weaker user is decoded first. Note that such a typical setting of user ordering is unable to tackle the diverse QoS requirements and service priorities of the users in IoT. In addition, while improving the reliability, it is also necessary to improve the security of the system. The security aspect of NOMA networks with priority difference has not been extensively studied. Related work is still missing in the existing literature and to bridge these gaps is the motivation behind our work.

In a nutshell, the massive connectivity in IoT networks causes problems associated with spectral congestion. The NOMA technology accommodates multiple devices in same radio resource block and promotes next-generation IoT networks on the spectral efficiency and massive connectivity. Nonetheless, the handling of a large number of IoT users with diversified QoS requirements and service priorities is a crucial task. The typical setting of user ordering, that is, a fixed service priority policy, in NOMA networks with user priority difference is unfit to tackle the prerequisite requirements of the IoT. In addition, the security issues have become a major restriction on the further development of the IoT. Motivated

by this, in this paper, we employ the diverse service priorities for NOMA networks, and extend the novel NOMA-IoT framework for a malicious attempt of a passive eavesdropper. Our key contributions in this work can be summarized as follows:

- Novel system setting: We consider a downlink transmission scenario in the NOMA-IoT networks where the base station BS) simultaneously serve two users with a priority difference. By employing the service priority for both users, we consider two schemes: a service priority for high-priority user (SP-HP) and a service priority for low-priority user (SP-LP). The PA strategy is developed for both the QoS provisioning for high-priority user and to obtain the optimal outage performance for low-priority user simultaneously. Furthermore, a malicious attempt of a single-antenna passive eavesdropper is introduced to consider the security aspect.
- Optimal solution and performance analysis: The optimal PA for both schemes is derived in the closed form. The closed-form expressions for COP and SOP are derived under the Rayleigh fading channels and are considered as the metrics of the reliability and security performances of users in each scheme, respectively. Furthermore, the EST is presented to effectively characterize the performance of the system.
- Insightful observations: Numerical results confirm that the theoretical results are in agreement with the simulation results and demonstrate the reliable and secure performances of users under each scheme. The results suggest that the COP and SOP of both users under each scheme are decreasing and increasing functions of the transmit power, respectively, and thus, the optimal transmit power can be identified to maximize the EST. Furthermore, the proposed framework provides valuable insights into the selection of an optimal scheme for the reliable and secure communications of users. For example, under the condition that low-priority user is a strong user (i.e., the channel condition of low-priority user is better than that of high-priority user), the SP-HP scheme provides better COP and SOP performances, and consequently, the maximum EST for low-priority user. From the perspective of high-priority user, the SP-LP scheme provides the minimum leakage information, and consequently, the better SOP performance.

III. System MODEL OF THE PROPOSED Schemes

We consider a downlink transmission scenario for the NOMA-IoT networks where a BS serves multiple users, for example, an access point is serving multiple IoT devices, under the malicious attempt of a passive eavesdropper (E). Owing to the strong downlink co-channel interference, it is not feasible to employ the power-domain NOMA for a large number of users in hardware- and interference-limited NOMA-IoT networks. The pairing of large number of users for the NOMA-implementation also causes high computation-overhead at BSs. A feasible approach to reduce the complexity can be realized by constructing a hybrid MA system in which the orthogonal bandwidth resources are allocated between the groups, and NOMA is only implemented within the group [29]. In this paper, we consider a two-user power-domain NOMA setting in the framework because it provides the best intuitive view of the reliability and security performances of the users with priority difference.[1] Without loss of generality, the high-priority user (U_1) and low-priority user (U_2) are scheduled and paired in a group for the NOMA transmission.

Meanwhile, we assume that the channel amplitudes are independent and follow distinct Rayleigh distributions.[2] Therefore, for all $p \in \{1, 2, E\}$, the channel gain, $|h_p|^2$, is an exponentially distributed random variable, that is, $Exp(\omega_p)$, where ω_p is a rate parameter. In addition, we assume that the average channel gain of each link can be determined by the path-loss, that is, $g_p = 1/\omega_p \triangleq d_p^{-\kappa}$, where d_p denotes the distance between the BS and involved node and κ denotes a path loss exponent [11], [30]. In this paper, the channel state information of the legitimate users can be obtained by the channel estimate, and only the channel distribution information of E is assumed to be available [31]. In addition, all nodes are equipped with a single antenna and work in half-duplex mode.

According to the principle of NOMA, superposition coding and PA are implemented at the BS. The BS transmits the superimposed signal $\sqrt{(1-b)}x_1 + \sqrt{b}x_2$, where x_1 and x_2 are the private signals intended to U_1 and U_2, respectively, with $\mathcal{E}\left(|x_1|^2\right) = \mathcal{E}\left(|x_2|^2\right) = 1$. Conceiving the power of the BS is P_B, the BS assigns the section bP_B to the signal of U_2, and $(1-b)P_B$ to the signal of U_1, where $b \in (0, 1]$ is the PA coefficient for x_2. Correspondingly, the received signals at U_1, U_2, and E are given by

$$y_{U1} = \sqrt{P_B}h_1\left(\sqrt{(1-b)}x_1 + \sqrt{b}x_2\right) + n_{U1}, \quad (1)$$

$$y_{U2} = \sqrt{P_B}h_2\left(\sqrt{(1-b)}x_1 + \sqrt{b}x_2\right) + n_{U2}, \quad (2)$$

$$y_E = \sqrt{P_B}h_E\left(\sqrt{(1-b)}x_1 + \sqrt{b}x_2\right) + n_E, \quad (3)$$

where h_1 represents the channel coefficient for the $BS \rightarrow U_1$ link, h_2 represents the channel coefficient for the $BS \rightarrow U_2$ link, and h_E represents the channel coefficient for the $BS \rightarrow E$ link. n_{U1}, n_{U2}, and n_E are the additive white Gaussian noise at U_1, U_2, and E, respectively, with the variance σ_{U1}^2, σ_{U2}^2, and σ_E^2, respectively.

A. SP-HP SCHEME

In this subsection, we present the SP-HP scheme in which the high-priority user (U_1) is served first. In this respect, x_2

[1]The rate performance of NOMA users can be further improved by applying the optimal selection scheme for a pair. However, this is beyond the scope of this paper.

[2]Relaxing a setting of Rayleigh fading channels to Nakagami-m fading channels will provide a more general system setup, and thus has been left as a future work.

is regarded as the interference signal when U_1 decodes x_1, and x_1 is removed by employing SIC when U_2 decodes x_2. For mathematical tractability, hereafter, we assume that each receiver is corrupted by the independent and identically distributed (i.i.d.) Gaussian noise, i.e., $\sigma_{U1}^2 = \sigma_{U2}^2 = \sigma_E^2 = \sigma^2$ and refer to $\rho_B \triangleq P_B/\sigma^2$ as the signal-to-noise ratio (SNR). With regard to x_2 as the interference, the instantaneous signal-to-interference-plus-noise ratio (SINR) decoding x_1 at U_1 can be denoted as

$$\Gamma_{U1}^1(b) = \frac{(1-b)\rho_B|h_1|^2}{b\rho_B|h_1|^2+1}. \tag{4}$$

The SINR decoding x_1 at U_2 can be denoted as

$$\Gamma_{U1\to U2}^1(b) = \frac{(1-b)\rho_B|h_2|^2}{b\rho_B|h_2|^2+1}. \tag{5}$$

Conditioned on x_1 being perfectly decoded, the SNR decoding x_2 at U_2 can be denoted as

$$\Gamma_{U2}^1(b) = b\rho_B|h_2|^2. \tag{6}$$

Similar to [30], we assume that E has the same detection capability as the legitimate users, that is, it detects the desired signal by considering the signal from the other user as the interference.[3] The SINRs decoding x_1 and x_2 at E can be represented as

$$y_{U1\to E}(b) = \frac{(1-b)\rho_B|h_E|^2}{b\rho_B|h_E|^2+1}, \tag{7}$$

$$y_{U2\to E}(b) = \frac{b\rho_B|h_E|^2}{(1-b)\rho_B|h_E|^2+1}. \tag{8}$$

Let χ_1 and χ_2 denote the predetermined detection thresholds of x_1 and x_2, respectively. As U_2 is served on the condition that χ_1 is met, mathematically, $\Gamma_{U1}^1(b)$, and $\Gamma_{U1\to U2}^1(b)$ must satisfy the following constraint simultaneously:

$$\chi_1 \le \min\left(\Gamma_{U1}^1(b), \Gamma_{U1\to U2}^1(b)\right). \tag{9}$$

In terms of the PA coefficient b, the constraint (9) can be reformulated as

$$b \le \frac{\rho_B\beta - \chi_1}{\rho_B\beta(1+\chi_1)}. \tag{10}$$

where $\beta \triangleq \min\left(|h_1|^2, |h_2|^2\right)$. Eq. (10) implies the constraint for b, which simultaneously guarantees the QoS requirements of U_1 and ensures successful SIC at U_2. Note that the adopted PA policy is valid for any channel order. Given by Eq. (4), U_1 can decode x_1 when the constraint $|h_1|^2 \ge \frac{\chi_1}{\rho_B}$ is satisfied.[4] Furthermore, when the constraint $\beta \le \frac{\chi_1}{\rho_B}$ is satisfied, the total power is allocated to the signal of U_1 only, that is, $b = 0$. When $b = 0$, the BS allocates all power to U_1. This occurs when the target data rate of U_1 is too high to meet or U_2 fails to perform successful SIC. Meanwhile, $\Gamma_{U2}^1(b)$ in Eq. (6) is an increasing function. To maximize $\Gamma_{U2}^1(b)$, the maximum value of b in its range is required. By noting that $0 \le b < 1$, we express the optimal b as

$$b^* = \frac{\rho_B\beta - \chi_1}{\rho_B\beta(1+\chi_1)}. \tag{11}$$

By employing b^*, the maximum SNR decoding x_2 at U_2 is given by

$$\Gamma_{U2}^1(b^*) = \frac{|h_2|^2(\rho_B\beta - \chi_1)}{\beta(1+\chi_1)}. \tag{12}$$

In the SP-HP scheme, the maximum SINRs decoding x_1 and x_2 at E can be respectively obtained as

$$\Gamma_{U1\to E}^1(b^*) = \frac{\chi_1|h_E|^2(\rho_B\beta+1)}{|h_E|^2(\rho_B\beta-\chi_1)+\beta(1+\chi_1)}, \tag{13}$$

$$\Gamma_{U2\to E}^1(b^*) = \frac{|h_E|^2(\rho_B\beta-\chi_1)}{\chi_1|h_E|^2(\rho_B\beta+1)+\beta(1+\chi_1)}. \tag{14}$$

B. SP-LP SCHEME

In this subsection, we present the SP-LP scheme in which the low-priority user (U_2) is served first. In this respect, x_1 is regarded as an interference signal when U_2 decodes x_2, and x_2 is removed by employing SIC when U_1 decodes x_1. With regard to x_1 as the interference, the instantaneous SINR decoding x_2 at U_2 can be denoted as

$$\Gamma_{U2}^2(b) = \frac{b\rho_B|h_2|^2}{(1-b)\rho_B|h_2|^2+1}. \tag{15}$$

The SINR decoding x_2 at U_1 can be denoted as

$$\Gamma_{U2\to U1}^2(b) = \frac{b\rho_B|h_1|^2}{(1-b)\rho_B|h_1|^2+1}. \tag{16}$$

Conditioned on x_2 being perfectly decoded, the SNR decoding x_1 at U_1 can be denoted as

$$\Gamma_{U1}^2(b) = (1-b)\rho_B|h_1|^2. \tag{17}$$

Given by Eqs. (16) and (17), the conditions to achieve the target transmission rate of U_1 are given by

$$\chi_2 \le \Gamma_{U2\to U1}^2(b),\ \chi_1 \le \Gamma_{U1}^2(b). \tag{18}$$

where the first constraint ensures that x_2 is removed by employing the SIC at U_1 and the second constraint ensures that U_1 decodes x_1 after the interference of x_2 is removed. Substituting Eqs. (16) and (17) into Eq. (18), we obtain the constraint for b as

$$\frac{\chi_2\left(\rho_B|h_1|^2+1\right)}{\rho_B|h_1|^2(1+\chi_2)} \le b \le \frac{\rho_B|h_1|^2-\chi_1}{\rho_B|h_1|^2}. \tag{19}$$

Given by Eq. (19), a valid b can be found when $\frac{\chi_2(\rho_B|h_1|^2+1)}{\rho_B|h_1|^2(1+\chi_2)} \le \frac{\rho_B|h_1|^2-\chi_1}{\rho_B|h_1|^2}$, which can be simplified as $|h_1|^2 \ge \frac{\chi_T}{\rho_B}$, where $\chi_T \triangleq \chi_1+\chi_2+\chi_1\chi_2$. Meanwhile, $\Gamma_{U2}^2(b)$ in Eq. (15) is an increasing function. To maximize $\Gamma_{U2}^2(b)$, b

[3] The worst-case eavesdropping scenario from the perspective of U_1, U_2 (i.e., E detects the multiuser data) will be studied in our future work. With multi-user detection capabilities, the received data stream can be distinguished at E, that is, the signal of $U_2(U_1)$ can be detected without being interfered by the signal of $U_1(U_2)$.

[4] The probability for the event that the constraint cannot be satisfied will be taken into consideration for the connection outage probability calculation for U_1.

takes the maximum value in its range. Thus, we express the optimal b as

$$b^{\dagger} = \frac{\rho_B |h_1|^2 - \chi_1}{\rho_B |h_1|^2}. \tag{20}$$

By employing $b^{\dagger}$, the maximum SNR decoding x_2 at U_2 is given by

$$\Gamma^2_{U2}(b^{\dagger}) = \frac{|h_2|^2 \left(\rho_B |h_1|^2 - \chi_1\right)}{\chi_1 |h_2|^2 + |h_1|^2}. \tag{21}$$

In the SP-LP scheme, the maximum SINRs decoding x_1 and x_2 at E can be respectively represented as

$$\Gamma^2_{U1\to E}(b^{\dagger}) = \frac{\chi_1 |h_E|^2}{|h_E|^2 \left(\rho_B |h_1|^2 - \chi_1\right) + |h_1|^2}, \tag{22}$$

$$\Gamma^2_{U2\to E}(b^{\dagger}) = \frac{|h_E|^2 \left(\rho_B |h_1|^2 - \chi_1\right)}{\chi_1 |h_E|^2 + |h_1|^2}. \tag{23}$$

IV. PERFORMANCE ANALYSIS

In this section, we derive the closed-form expressions for key performance metrics, i.e., COP, SOP, and EST, to analyze the performances of the users under each scheme. According to transmission protocol, the connection outage occurs when a user is failed to decode the intended message. For a predefined detection threshold, the COP is defined as the probability that the SNR decoding x_1 (x_2) is less than the detection (SNR) threshold χ_1 (χ_2). According to Wyner's wiretap code [32], [33], the SOP is defined as the probability that the wiretap channel capacity is higher than the redundancy rate of wiretap code.

To proceed, we first derive the close-form expression based on the statistical characteristics of the received SINRs, which is shown in the following theorem.

Theorem 1: The expression $Pr\,(I) = Pr\,(Y_0 Y_1 \le Y_3 + Y_4)$ *in closed form can be derived as*

$$Pr\,(I) = \frac{\lambda_{Y3}}{\lambda_{Y3} - \lambda_{Y4}} \left\{ 1 - \exp\left(\frac{\lambda_{Y0}\lambda_{Y1}}{2\lambda_{Y4}}\right) W_{-1,\frac{1}{2}}\left(\frac{\lambda_{Y0}\lambda_{Y1}}{\lambda_{Y4}}\right) \right\}, \tag{24}$$

where Y_a, *for* $a = 0, 1, 3, 4$, *is an exponentially distributed random variable with the rate parameter* λ_{Ya}. $W_{k,m}(.)$ *is a Whittaker function defined in Eq. (9.22) in [34].*

Proof: See Appendix A. □

A. ANALYSIS OF THE SP-HP SCHEME

The COP is an important indicator to evaluate the reliability of the networks. In particular, the connection outage for U_1 occurs when U_1 fails to decode x_1, that is, the achievable rate of x_1 at U_1 is less than the predefined target transmission rate of U_1 (r_{U1}). In the light of Shannon channel capacity formula [17], the COP of U_1 can be defined as

$$P^1_{CO.U1} = Pr\left(|h_1|^2 < \frac{\chi_1}{\rho_B}\right). \tag{25}$$

Lemma 1: The COP of U_1 *in closed form is given as*

$$P^1_{CO.U1} = 1 - \exp\left(-\frac{\chi_1}{\rho_B g_1}\right). \tag{26}$$

Proof: A proof of this lemma is provided in Appendix B. □

The connection outage for U_2 occurs when U_2 fails to decode x_2, that is, the achievable rate of x_2 at U_2 given in Eq. (12) is less than the predefined target transmission rate of U_2 (r_{U2}). In this respect, the COP of U_2 is written as

$$\begin{aligned} P^1_{CO.U2} &= Pr\left(\Gamma^1_{U2}(b^*) < \chi_2\right) \\ &= Pr\left(\frac{|h_2|^2 \left(\rho_B \beta - \chi_1\right)}{\beta\left(1 + \chi_1\right)} < \chi_2\right). \end{aligned} \tag{27}$$

Lemma 2: The COP of U_2 *in closed form is given as*

$$\begin{aligned} P^1_{CO.U2} &= \left(\frac{(\chi_1 g_2)^{-1}}{(\chi_1 g_2)^{-1} - \left(\chi_2 g_\beta\left(1 + \chi_1\right)\right)^{-1}}\right) \\ &\times \left\{ 1 - \exp\left(\frac{\chi_2\left(1 + \chi_1\right)}{2\rho_B g_2}\right) W_{-1,\frac{1}{2}}\left(\frac{\chi_2\left(1 + \chi_1\right)}{\rho_B g_2}\right) \right\}. \end{aligned} \tag{28}$$

Proof: Using the results in Appendix A, and substituting $\lambda_{Y0} \triangleq \left(g_\beta\right)^{-1}$, $\lambda_{Y1} \triangleq (\rho_B g_2)^{-1}$, $\lambda_{Y3} \triangleq (\chi_1 g_2)^{-1}$, $\lambda_{Y4} \triangleq \left(\chi_2 g_\beta\left(1 + \chi_1\right)\right)^{-1}$, we obtain the closed-form COP of U_2 in Eq. (28). The proof is completed. □

The SOP is an important indicator to evaluate the security performance of the networks. In the light of Eq. (13), the SOP of U_1 is written as

$$\begin{aligned} P^1_{SO.U1} &= Pr\left(\Gamma^1_{U1\to E}(b^*) \ge \chi_{1s}\right) \\ &= 1 - Pr\left(\frac{\chi_1 |h_E|^2 \left(\rho_B \beta + 1\right)}{|h_E|^2 \left(\rho_B \beta - \chi_1\right) + \beta\left(1 + \chi_1\right)} < \chi_{1s}\right), \end{aligned} \tag{29}$$

where $\chi_{1s} = 2^{(r_{U1} - r_{sU1})} - 1$. r_{sU1} is the target secrecy rate of U_1, and $r_{U1} - r_{sU1}$ is the redundancy rate against eavesdropping.

Lemma 3: The SOP of U_1 *in closed form is given as*

$$P^1_{SO.U1} = 1 - Q_1 \tag{30}$$

where Q_1 *is represented as*

$$\begin{aligned} Q_1 &= \left(\frac{\left(-\chi_1 g_E\left(\chi_{1s} + 1\right)\right)^{-1}}{\left(-\chi_1 g_E\left(\chi_{1s} + 1\right)\right)^{-1} - \left(\chi_{1s} g_\beta\left(\chi_1 + 1\right)\right)^{-1}}\right) \\ &\times \left\{ 1 - \exp\left(\frac{\chi_{1s}\left(1 + \chi_1\right)}{2\rho_B g_E\left(\chi_1 - \chi_{1s}\right)}\right) \right. \\ &\left. \times W_{-1,\frac{1}{2}}\left(\frac{\chi_{1s}\left(1 + \chi_1\right)}{\rho_B g_E\left(\chi_1 - \chi_{1s}\right)}\right) \right\}. \end{aligned} \tag{31}$$

Proof: Using the results in Appendix A, and substituting $\lambda_{Y0} \triangleq \left(g_\beta\right)^{-1}$, $\lambda_{Y1} \triangleq \left(\rho_B g_E\left(\chi_1 - \chi_{1s}\right)\right)^{-1}$, $\lambda_{Y3} \triangleq \left(-\chi_1\, g_E\left(\chi_{1s} + 1\right)\right)^{-1}$, $\lambda_{Y4} \triangleq \left(\chi_{1s} g_\beta\left(\chi_1 + 1\right)\right)^{-1}$, we obtain the closed-form SOP of U_1 in Eq. (30). The proof is completed. □

With predefined χ_{2s}, the SOP of U_2 can be acquired by Eq. i(14) as

$$P^1_{SO.U2} = Pr\left(\Gamma^1_{U2\to E}(b^*) \geq \chi_{2s}\right) = 1 - Pr\left(\frac{|h_E|^2\left(\rho_B\beta - \chi_1\right)}{\chi_1|h_E|^2\left(\rho_B\beta + 1\right) + \beta\left(1+\chi_1\right)} < \chi_{2s}\right). \quad (32)$$

where $\chi_{2s} = 2^{(r_{U2}-r_{sU2})} - 1$. r_{sU2} is the target secrecy rate of U_2, and $r_{U2} - r_{sU2}$ is the redundancy rate against eavesdropping.

Lemma 4: The SOP of U_2 in closed form is given as

$$P^1_{SO.U2} = 1 - Q_2 \quad (33)$$

where Q_2 is represented as

$$Q_2 = \left(\frac{\left(\chi_1 g_E\left(\chi_{2s}+1\right)\right)^{-1}}{\left(\chi_1 g_E\left(\chi_{2s}+1\right)\right)^{-1} - \left(\chi_{2s} g_\beta\left(\chi_1+1\right)\right)^{-1}}\right) \times \left\{1 - \exp\left(\frac{\chi_{2s}\left(1+\chi_1\right)}{2\rho_B g_E\left(1-\chi_{2s}\chi_1\right)}\right) \times W_{-1,\frac{1}{2}}\left(\frac{\chi_{2s}\left(1+\chi_1\right)}{\rho_B g_E\left(1-\chi_{2s}\chi_1\right)}\right)\right\}. \quad (34)$$

Proof: Using the results in Appendix A, and substituting $\lambda_{Y0} \triangleq \left(g_\beta\right)^{-1}$, $\lambda_{Y1} \triangleq \left(\rho_B g_E\left(1-\chi_{2s}\chi_1\right)\right)^{-1}$, $\lambda_{Y3} \triangleq \left(\chi_1\, g_E\left(\chi_{2s}+1\right)\right)^{-1}$, $\lambda_{Y4} \triangleq \left(\chi_{2s} g_\beta\left(\chi_1+1\right)\right)^{-1}$, we obtain the closed-form SOP of U_2 in Eq. (33). The proof is completed. □

While the COP is a metric for reliability performance and the SOP is a metric for security performance, either the COP or SOP is inadequate to evaluate both the reliability and security performances. In this regard, EST is analyzed to holistically characterize the performance of the system. According to the definition of EST, the EST of U_1 and U_2 can be written as

$$\eta^1_{U1} = r_{sU1}\left(1 - P^1_{CO.U1}\right)\left(1 - P^1_{SO.U1}\right) \quad (35)$$

$$\eta^1_{U2} = r_{sU2}\left(1 - P^1_{CO.U2}\right)\left(1 - P^1_{SO.U2}\right). \quad (36)$$

By substituting Eqs. (26) and (30) into (35), and Eqs. (28) and (33) into (36), we obtain the closed-form expressions of EST for U_1 and U_2, respectively, achieved by the SP-HP scheme.

B. ANALYSIS OF THE SP-LP SCHEME

The COP of U_1 achieved by the SP-LP scheme is written as

$$P^2_{CO.U1} = Pr\left(|h_1|^2 < \frac{\chi_T}{\rho_B}\right). \quad (37)$$

Similar to Eq. (26), the COP of U_1 in closed form is given as

$$P^2_{CO.U1} = 1 - \exp\left(-\frac{\chi_T}{\rho_B g_1}\right). \quad (38)$$

Similar to Eq. (27), the COP of U_2 achieved by the SP-LP scheme is written as

$$P^2_{CO.U2} = Pr\left(\Gamma^2_{U2}(b^\dagger) < \chi_2\right) = Pr\left(\frac{|h_2|^2\left(\rho_B|h_1|^2 - \chi_1\right)}{\chi_1|h_2|^2 + |h_1|^2} < \chi_2\right). \quad (39)$$

Lemma 5: The COP of U_2 in closed form is given as

$$P^2_{CO.U2} = \left(\frac{\left(\chi_2 g_1\right)^{-1}}{\left(\chi_2 g_1\right)^{-1} - \left(\chi_2\, g_2\left(1+\chi_1\right)\right)^{-1}}\right) \times \left\{1 - \exp\left(\frac{\chi_2\left(1+\chi_1\right)}{2\rho_B g_1}\right) W_{-1,\frac{1}{2}}\left(\frac{\chi_2\left(1+\chi_1\right)}{\rho_B g_1}\right)\right\}. \quad (40)$$

Proof: Using the results in Appendix A, and substituting $\lambda_{Y0} \triangleq \left(g_2\right)^{-1}$, $\lambda_{Y1} \triangleq \left(\rho_B g_1\right)^{-1}$, $\lambda_{Y3} \triangleq \left(\chi_2 g_1\right)^{-1}$, $\lambda_{Y4} \triangleq \left(\chi_2 g_2\left(1+\chi_1\right)\right)^{-1}$, we obtain the closed-form COP of U_2 in (40). The proof is completed. □

With predefined χ_{1s} and Eq. (22), the SOP of U_1 achieved by the SP-LP scheme can be acquired as

$$P^2_{SO.U1} = Pr\left(\Gamma^2_{U1\to E}(b^\dagger) \geq \chi_{1s}\right) = 1 - Pr\left(\frac{\chi_1|h_E|^2}{|h_E|^2\left(\rho_B|h_1|^2 - \chi_1\right) + |h_1|^2} < \chi_{1s}\right). \quad (41)$$

Lemma 6: The SOP of U_1 in closed form is given as

$$P^2_{SO.U1} = 1 - Q_3 \quad (42)$$

where Q_3 is represented as

$$Q_3 = \left(\frac{\left(-\chi_1 g_E\left(\chi_{1s}+1\right)\right)^{-1}}{\left(-\chi_1 g_E\left(\chi_{1s}+1\right)\right)^{-1} - \left(\chi_{1s} g_1\right)^{-1}}\right) \times \left\{1 - \exp\left(\frac{1}{2\rho_B g_E}\right) W_{-1,\frac{1}{2}}\left(\frac{1}{\rho_B g_E}\right)\right\}. \quad (43)$$

Proof: Using the results in Appendix A, and substituting $\lambda_{Y0} \triangleq \left(g_1\right)^{-1}$, $\lambda_{Y1} \triangleq \left(-\rho_B g_E \chi_{1s}\right)^{-1}$, $\lambda_{Y3} \triangleq \left(-\chi_1\, g_E\left(\chi_{1s}+1\right)\right)^{-1}$, $\lambda_{Y4} \triangleq \left(g_1\chi_{1s}\right)^{-1}$, we obtain the closed-form SOP of U_1 in (42). The proof is completed. □

With predefined χ_{2s} and Eq. (23), the SOP of U_2 achieved by the SP-LP scheme can be calculated as

$$P^2_{SO.U2} = Pr\left(\Gamma^2_{U2\to E}(b^\dagger) \geq \chi_{2s}\right) = 1 - Pr\left(\frac{|h_E|^2\left(\rho_B|h_1|^2 - \chi_1\right)}{|h_E|^2\chi_1 + |h_1|^2} < \chi_{2s}\right), \quad (44)$$

Lemma 7: The SOP of U_2 in closed form is given as

$$P^2_{SO.U2} = 1 - Q_4 \quad (45)$$

where Q_4 is represented as

$$Q_4 = \left(\frac{\left(\chi_1 g_E\left(\chi_{2s}+1\right)\right)^{-1}}{\left(\chi_1 g_E\left(\chi_{2s}+1\right)\right)^{-1} - \left(\chi_{2s} g_1\right)^{-1}}\right) \times \left\{1 - \exp\left(\frac{\chi_{2s}}{2\rho_B g_E}\right) W_{-1,\frac{1}{2}}\left(\frac{\chi_{2s}}{\rho_B g_E}\right)\right\}. \quad (46)$$

Proof: Using the results in Appendix A, and substituting $\lambda_{Y0} \triangleq \left(g_1\right)^{-1}$, $\lambda_{Y1} \triangleq \left(\rho_B g_E\right)^{-1}$, $\lambda_{Y3} \triangleq \left(\chi_1\, g_E\left(\chi_{2s}+1\right)\right)^{-1}$, $\lambda_{Y4} \triangleq \left(\chi_{2s} g_1\right)^{-1}$, we obtain the closed-form SOP of U_2 in (45). The proof is completed. □

By substituting Eqs. (38) and (42) into (35), and Eqs. (40) and (45) into (36), we obtain the closed-form expressions of EST for U_1 and U_2, respectively, achieved by the SP-LP scheme.

V. NUMERICAL RESULTS

This section provides numerical results to verify the analytical results presented in previous sections along with valuable insights. Unless otherwise specified, the transmit SNR means the SNR at BS: $\rho_B = \frac{P_B}{\sigma^2}$. The target rates of U_1 and U_2 were set to 0.8 bps/Hz. The target secrecy rates of U_1 and U_2 are preset as 0.4 bps/Hz. These parameters were selected to validate the behavior of the system. The simulation performance is obtained by performing the Monte Carlo simulations over 10^6 different channel realizations. To better demonstrate the reliability performances of users achieved by the SP-HP and SP-LP schemes, the scheme proposed in [28] is considered as a benchmark strategy. Although the COP performances of U_1 and U_2 in the proposed SP-HP scheme and benchmark strategy match, the benchmark strategy does not consider a setting in the user ordering where U_1 is served after U_2. Such a setting is a prerequisite for the users in IoT networks. In addition, the security aspect is not considered in the benchmark strategy.

Notably, the analytical results precisely match the simulation results and validate the accuracy of the theoretical analysis.

Fig. 1 shows the relationship between connection outage probability of U_1 with the transmit SNR (ρ_B). The analysis points are calculated from Eqs. (26) and (38). The figure shows that the COP of U_1 under both schemes decreases because of the increment in ρ_B. Further, a high transmit SNR improves the system reliability, which is similar to that in the OMA systems. In particular, we can determine that the COP of U_1 under the SP-HP scheme is lower than that under the SP-LP scheme. The SP-HP scheme guarantees better reliability performance of U_1. We can also observe that the SP-HP scheme and benchmark strategy achieve the same COP. The reason is that the SP-HP scheme follows the benchmark strategy, that is, both schemes serve U_1 first and ensure the QoS requirements. In addition, we can observe that the better channel for U_1 has a positive effect on the COP performance of U_1 under both schemes.

Fig. 2 depicts the relationship between connection outage probability of U_2 with ρ_B. The analysis points are calculated from Eqs. (28) and (40). When the channel condition of U_1 is comparatively better than that of U_2, the COP of U_2 under the SP-LP scheme is lower than the SP-HP scheme. The reason is that under the suggested channel condition, the decoding SNR provided by the SP-LP scheme, given by Eq. (21), is higher than the decoding SNR provided by the SP-HP scheme, given by Eq. (12). Therefore, compared with the SP-HP scheme, the SP-LP scheme provides better reliability performance of U_2. In contrast, when the channel of U_1 is comparatively worse than that of U_2, the SP-HP scheme provides the better COP performance of U_2. Fig. 2 also shows that the COP of U_2 is same for both the benchmark strategy and the SP-HP scheme. The reason is that the SP-HP scheme follows the benchmark strategy for U_2 as well, that is, serve U_2 after U_1 and maximize the SNR decoding x_2 at U_2. Importantly, Figs. 1 and 2 suggest that the proposed

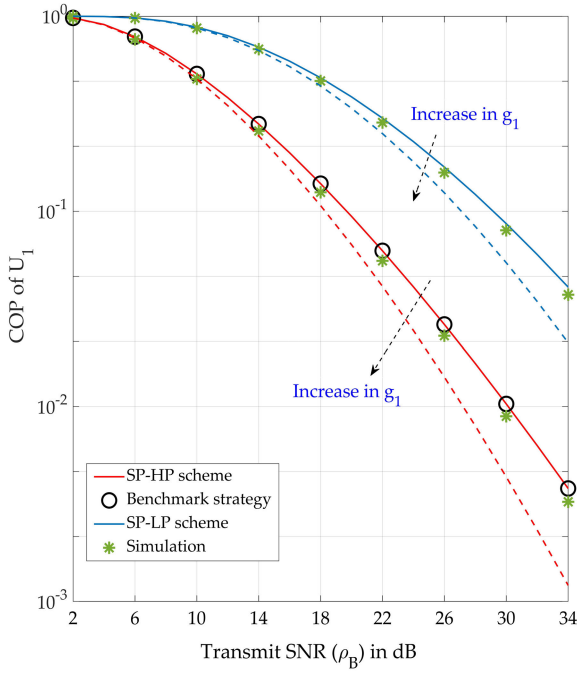

FIGURE 1. Connection outage probability of U_1 vs. transmit SNR (ρ_B).

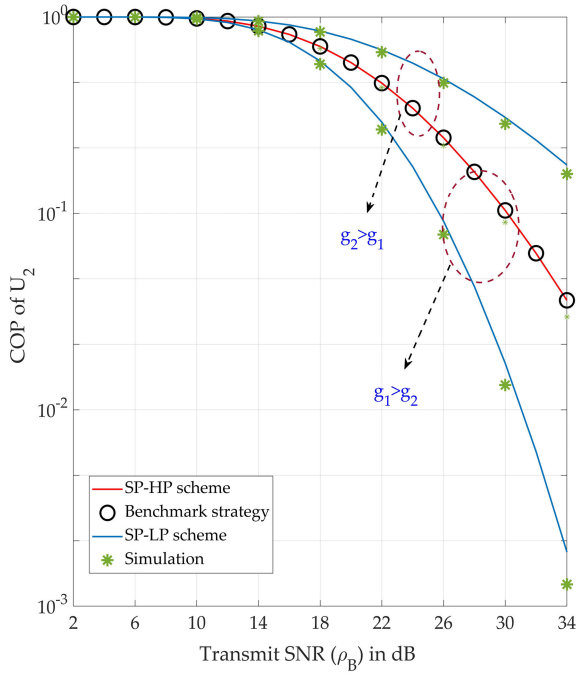

FIGURE 2. Connection outage probability of U_2 vs. transmit SNR (ρ_B).

framework provides easy selection of an optimal scheme for the reliable communications for both U_1 and U_2.

Fig. 3 shows the impact of the channel condition of U_1, g_1, and target rate of U_1, r_{U1}, on the connection outage probability of U_2. The increase in g_1 indicates a better channel condition for $BS \rightarrow U_1$ link. The COP of U_2 is an increasing and a decreasing function with respect to r_{U1} and g_1, respectively. Fig. 3 demonstrates that increasing r_{U1} or decreasing g_1 significantly undermines (deteriorates) the connection outage performance of U_2, that is, higher g_1 or lower r_{U1} make the QoS (target rate) of U_1 easier to be satisfied. Therefore, U_2 allocates more power to its intended message, which consequently improves the connection outage performance of U_2.

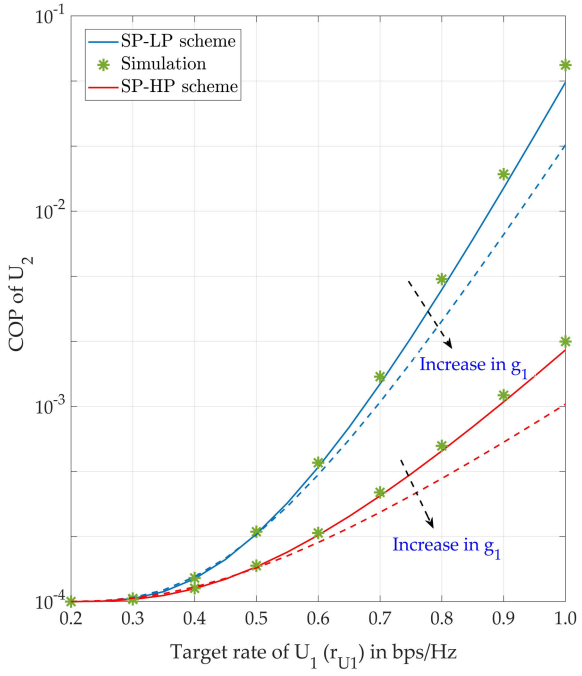

FIGURE 3. Connection outage probability of U_2 vs. target rate of U_1 (r_{U1}) and average channel gain of $BS \rightarrow U_1$ link (g_1).

Fig. 4 reveals the relationship between secrecy outage probability of U_1 with the ρ_B. The analysis points are calculated from Eqs. (30) and (42). In contrast with the reliability performances, the security performance of the users is weakened because of the increment in ρ_B. The reason for U_1 is that the maximum SINRs decoding x_1 at E under the SP-HP and SP-LP schemes, given by Eqs. (13) and (22), respectively, increases with ρ_B. Fig. 4 also shows that the SOP of U_1 under the SP-HP scheme is higher than that under the SP-LP scheme (i.e., the SP-LP scheme provides better security performance of U_1) when the channel condition of U_1 is comparatively worse than that of U_2. The reason is that the leakage information for U_1 under the SP-HP scheme is higher than under the SP-LP scheme under the suggested channel condition. In contrast, the secrecy performance comparison between two

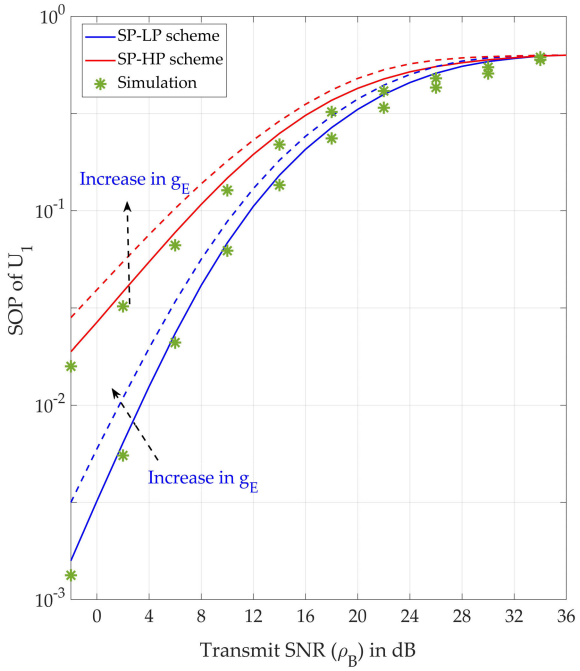

FIGURE 4. Secrecy outage probability of U_1 vs. transmit SNR (ρ_B).

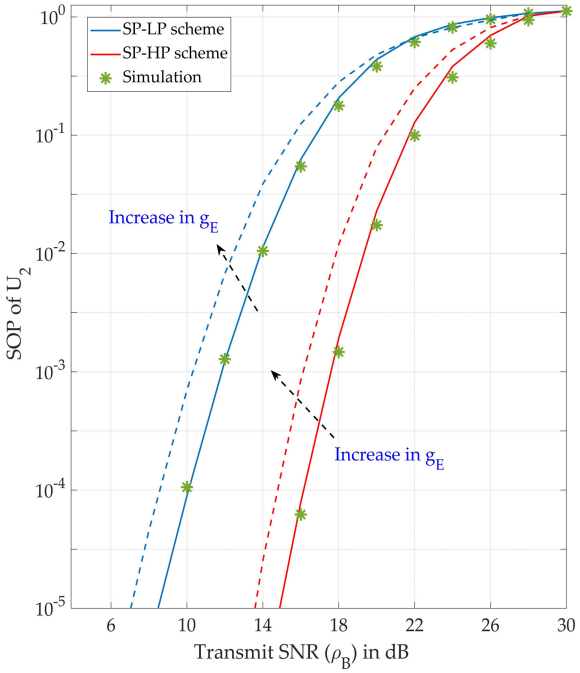

FIGURE 5. Secrecy outage probability of U_2 vs. transmit SNR (ρ_B).

schemes depends on the system parameters for a condition $g_1 > g_2$.

Fig. 5 depicts the relationship between SOP of U_2 with the ρ_B and compares the security performance of U_2 under the SP-HP and SP-LP schemes. The analysis points are calculated from Eqs. (33) and (45). The security performance

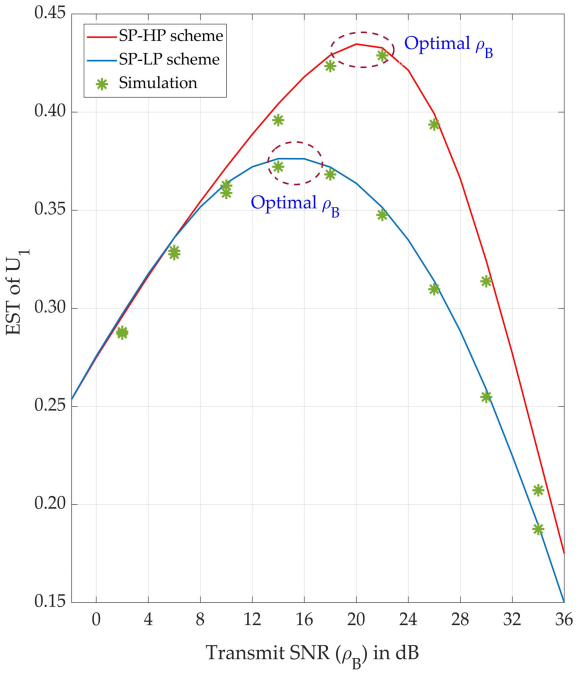

FIGURE 6. Effective secrecy throughput of U_1 vs. transmit SNR (ρ_B).

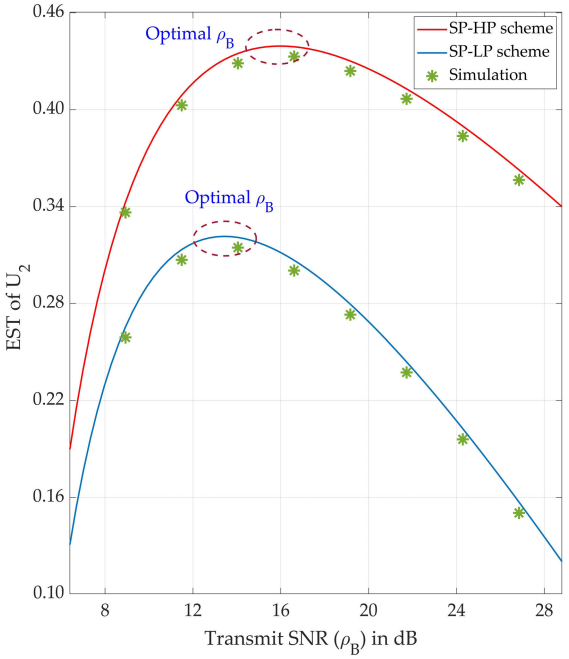

FIGURE 7. Effective secrecy throughput of U_2 vs. transmit SNR (ρ_B).

of U_2, under both schemes, is also weakened with increasing ρ_B due to the increment in maximum decoding SINRs x_2 at E. In contrast to U_1, the leakage information for U_2 under the SP-LP scheme is higher than that under the SP-HP scheme when the channel condition of U_1 is comparatively worse than that of U_2. As a result, the SP-LP scheme has the higher SOP and provides the comparatively worst security performance of U_2 than the SP-HP scheme. Similar to U_1, the security performance comparison for two schemes depends on the system parameters for a condition $g_1 > g_2$.

Fig. 6 plots effective secrecy throughput of U_1 with ρ_B and compares the EST performances of the SP-HP and SP-LP schemes under the condition $g_2 > g_1$. The curves of EST under both schemes increase first, then decrease, as the ρ_B increases. The results validate the security-reliability tradeoff and demonstrate that ρ_B can be optimized to maximize EST under both schemes. Importantly, Fig. 6, while validating the previous results of U_1, shows that the SP-HP scheme provides the better COP performance, and the SP-LP scheme provides the better SOP performance. Therefore, the selection of an optimal scheme for U_1 in term of EST depends on the system parameters.

Fig. 7 plots effective secrecy throughput of U_2 with ρ_B, and compares the EST performances of the SP-HP and SP-LP schemes under the condition $g_2 > g_1$. For U_2, ρ_B can be optimized under both schemes. Importantly, Fig. 7, while validating the previous results of U_2, shows that the SP-HP scheme guarantees the better EST performance as it provides better COP and SOP performances than the SP-LP scheme.

VI. CONCLUSION

To leverage power-domain NOMA in the context of IoT, this article presented a novel downlink transmission framework for the NOMA-IoT networks. The two schemes, i.e., SP-HP and SP-LP, were proposed by employing the service priority for each user. The PA strategy was adopted to bring the desirable QoS provision for high-priority user and to maximize the achievable rate for low-priority user; further, a malicious attempt of an eavesdropper was considered for the security aspect. The connection and secrecy outage probabilities and the effective secrecy throughput were derived to estimate the performance of the system. Finally, the numerical results validated the accuracy of the analytical results and demonstrated that if low-priority user is a strong user, the SP-HP scheme is an optimal scheme for low-priority user in terms of both the reliable and secure performances. From the perspective of high-priority user, the SP-LP is an optimal scheme with respect to the secure performance. The analytical results developed in this paper could provide design insights for the downlink architecture in NOMA-IoT networks.

APPENDIX A
PROOF OF THEOREM 1

We evaluate the expression $Pr\,(I) = Pr\,(Y_0Y_1 \leq Y_3 + Y_4)$. By setting $v = 0$, $\beta = \lambda_{Y1}y$, and $\gamma = \lambda_{Y0}$ in Eqs. (3.471.9) and (3.324.1) [34], the PDF and CDF of Y_0Y_1 are respectively derived as

$$\begin{aligned} f_{Y_0Y_1}(y) &= \int_0^\infty \frac{1}{x} f_{Y1}\left(\frac{y}{x}\right) f_{Y0}(x)\, dx \\ &= \lambda_{Y0}\lambda_{Y1} \int_0^\infty \frac{1}{x} \exp\left(-\frac{\lambda_{Y_1} y}{x} - \lambda_{Y_0} x\right) dx \\ &= 2\lambda_{Y_0}\lambda_{Y_1} K_0\left(2\sqrt{\lambda_{Y_0}\lambda_{Y_1} y}\right). \end{aligned} \tag{47}$$

$$
\begin{aligned}
F_{Y_0Y_1}(y) &= \int_0^{\infty}\int_0^{\frac{y}{x}} f_{Y1}(z) f_{Y0}(x)\, dxdz \\
&= \int_0^{\infty} F_{Y1}\left(\frac{y}{x}\right) f_{Y0}(x)\, dx \\
&= \int_0^{\infty}\left(1-\exp\left(-\frac{\lambda_{Y_1} y}{x}\right)\right)\lambda_{Y_0}\exp\left(-\lambda_{Y_0}x\right) dx \\
&= \lambda_{Y_0}\int_0^{\infty}\exp\left(-\lambda_{Y_0}x\right) dx \\
&\quad -\lambda_{Y_0}\int_0^{\infty}\exp\left(-\lambda_{Y_0}x\right)\exp\left(-\frac{\lambda_{Y_1} y}{x}\right) dx \\
&= 1-\lambda_{Y_0}\int_0^{\infty}\exp\left(-\frac{\lambda_{Y_1} y}{x}-\lambda_{Y_0}x\right) dx \\
&= 1-2\sqrt{\lambda_{Y_0}\lambda_{Y_1} y}K_1\left(2\sqrt{\lambda_{Y_0}\lambda_{Y_1} y}\right). \qquad (48)
\end{aligned}
$$

where $K_v(.)$ is the modified Bessel function of the second kind defined in Eq. (8.432) [34].

By applying $p = \lambda_{Y_3} - \lambda_{Y_4}$ in Eq. (3.310) [34], the PDF of $Y_3 + Y_4$ is derived as

$$
\begin{aligned}
f_{Y_3+Y_4}(y) &= \int_0^{\infty} f_{Y3}(x) f_{Y4}(y-x)\, dx \\
&= \lambda_{Y_3}\lambda_{Y_4}\exp\left(-\lambda_{Y_4} y\right)\int_0^{\infty}\exp\left(-x\left(\lambda_{Y_3}-\lambda_{Y_4}\right)\right) dx \\
&= \frac{\lambda_{Y_3}\lambda_{Y_4}}{\lambda_{Y_3}-\lambda_{Y_4}}\exp\left(-\lambda_{Y_4} y\right). \qquad (49)
\end{aligned}
$$

Given Eqs. (47)-(49), we can determine $Pr(I) = Pr(Y_0Y_1 \le Y_3 + Y_4)$ by setting $\beta = \sqrt{\lambda_{Y_0}\lambda_{Y_1}}$, $\mu = 1$, $v = \frac{1}{2}$, $\alpha = \lambda_{Y_4}$ in Eq. (6.643.3) [34] and $p = \lambda_{Y_4}$ in Eq. (3.310) [34] as

$$
\begin{aligned}
Pr(I) &= \int_0^{\infty}\int_0^{y} f_{Y_0Y_1}(y) f_{Y_3+Y_4}(y) dxdy \\
&= \int_0^{\infty} F_{Y_0Y_1}(y) f_{Y_3+Y_4}(y) dy \\
&= \frac{\lambda_{Y_3}\lambda_{Y_4}}{\lambda_{Y_3}-\lambda_{Y_4}}\int_0^{\infty}\left(1-2\sqrt{\lambda_{Y_0}\lambda_{Y_1} y}K_1\left(2\sqrt{\lambda_{Y_0}\lambda_{Y_1} y}\right)\right) \\
&\quad \times\exp\left(-\lambda_{Y_4} y\right) dy \\
&= \frac{\lambda_{Y_3}\lambda_{Y_4}}{\lambda_{Y_3}-\lambda_{Y_4}}\int_0^{\infty}\exp\left(-\lambda_{Y_4} y\right) dy - \frac{2\lambda_{Y_3}\lambda_{Y_4}\sqrt{\lambda_{Y_0}\lambda_{Y_1}}}{\lambda_{Y_3}-\lambda_{Y_4}} \\
&\quad \times\int_0^{\infty}\exp\left(-\lambda_{Y_4} y\right)\sqrt{y}K_1\left(2\sqrt{\lambda_{Y_0}\lambda_{Y_1} y}\right) dy \\
&= \frac{\lambda_{Y3}}{\lambda_{Y3}-\lambda_{Y4}} \\
&\quad \times\left\{1-\exp\left(\frac{\lambda_{Y0}\lambda_{Y1}}{2\lambda_{Y4}}\right) W_{-1,\frac{1}{2}}\left(\frac{\lambda_{Y0}\lambda_{Y1}}{\lambda_{Y4}}\right)\right\}. \qquad (50)
\end{aligned}
$$

Theorem 1 is proved.

APPENDIX B
PROOF OF LEMMA 1

Here, $|h_{\hat{p}}|^2$, $\hat{p} \in \{1, 2, E, \beta\}$, is an exponentially distributed random variable with the rate parameter $\omega_{\hat{p}} = \frac{1}{g_{\hat{p}}}$. When $z \ge 0$, the PDF and CDF of $|h_{\hat{p}}|^2$ are respectively given by

$$
f_{|h_{\hat{p}}|^2}(z) = \omega_{\hat{p}}\exp\left(-\omega_{\hat{p}} z\right), \qquad (51)
$$

$$
F_{|h_{\hat{p}}|^2}(z) = 1-\exp\left(-\omega_{\hat{p}} z\right), \qquad (52)
$$

where $\omega_1 = \frac{1}{g_1}$, $\omega_2 = \frac{1}{g_2}$, $\omega_E = \frac{1}{g_E}$, $\omega_\beta = \frac{1}{g_\beta}$, and $g_\beta = \frac{g_1 g_2}{g_1+g_2}$. The proof is completed.

REFERENCES

[1] S. Sinche, D. Raposo, N. Armando, A. Rodrigues, F. Boavida, V. Pereira, and J. S. Silva, "A survey of IoT management protocols and frameworks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1168–1190, 2nd Quart., 2020.

[2] M. Z. Chowdhury, M. Shahjalal, S. Ahmed, and Y. M. Jang, "6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 957–975, Jul. 2020.

[3] L. Chettri and R. Bera, "A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 16–32, Jan. 2020.

[4] A. Ghosh, A. Maeder, M. Baker, and D. Chandramouli, "5G evolution: A view on 5G cellular technology beyond 3GPP release 15," *IEEE Access*, vol. 7, pp. 127639–127651, 2019.

[5] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A survey on 5G networks for the Internet of Things: Communication technologies and challenges," *IEEE Access*, vol. 6, pp. 3619–3647, 2018.

[6] A. S. Mubarak, H. Esmaiel, and E. M. Mohamed, "LTE/Wi-Fi/mmWave RAN-level interworking using 2C/U plane splitting for future 5G networks," *IEEE Access*, vol. 6, pp. 53473–53488, 2018.

[7] S. Lagen, L. Giupponi, S. Goyal, N. Patriciello, B. Bojovic, A. Demir, and M. Beluri, "New radio beam-based access to unlicensed spectrum: Design challenges and solutions," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 8–37, 1st Quart., 2020.

[8] E. Garro, M. Fuentes, J. L. Carcel, H. Chen, D. Mi, F. Tesema, J. J. Gimenez, and D. Gomez-Barquero, "5G mixed mode: NR multicast-broadcast services," *IEEE Trans. Broadcast.*, vol. 66, no. 2, pp. 390–403, Jun. 2020.

[9] L. Zhang, W. Li, Y. Wu, X. Wang, S.-I. Park, H. M. Kim, J.-Y. Lee, P. Angueira, and J. Montalban, "Layered-division-multiplexing: Theory and practice," *IEEE Trans. Broadcast.*, vol. 62, no. 1, pp. 216–232, Mar. 2016.

[10] A. Behnad and X. Wang, "Virtual small cells formation in 5G networks," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 616–619, Mar. 2017.

[11] W. Khalid, H. Yu, and S. Noh, "Residual energy analysis in cognitive radios with energy harvesting UAV under reliability and secrecy constraints," *Sensors*, vol. 20, no. 10, pp. 2998–3017, May 2020.

[12] W. Khalid and H. Yu, "Sum Utilization of spectrum with spectrum handoff and imperfect sensing in interweave multi-channel cognitive radio networks," *Sustainability*, vol. 10, no. 6, pp. 1764–1782, May 2018.

[13] G. Liu, Z. Wang, J. Hu, Z. Ding, and P. Fan, "Cooperative NOMA broadcasting/multicasting for low-latency and high-reliability 5G cellular V2X communications," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7828–7838, Oct. 2019.

[14] B. Zheng, M. Wen, C.-X. Wang, X. Wang, F. Chen, J. Tang, and F. Ji, "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.

[15] A. Montazerolghaem and M. H. Yaghmaee, "Load-balanced and QoS-aware software-defined Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3323–3337, Apr. 2020.

[16] X. Chen, Z. Li, Y. Chen, and X. Wang, "Performance analysis and uplink scheduling for QoS-aware NB-IoT networks in mobile computing," *IEEE Access*, vol. 7, pp. 44404–44415, 2019.

[17] H. Yu and I.-G. Lee, "Physical layer security based on NOMA and AJ for MISOSE channels with an untrusted relay," *Future Gener. Comput. Syst.*, vol. 102, pp. 611–618, Jan. 2020.

[18] M. S. Abdalzaher, L. Samy, and O. Muta, "Non-zero-sum game-based trust model to enhance wireless sensor networks security for IoT applications," *IET Wireless Sensor Syst.*, vol. 9, no. 4, pp. 218–226, Aug. 2019.

[19] M. S. Abdalzaher and O. Muta, "A game-theoretic approach for enhancing security and data trustworthiness in IoT applications," *IEEE Internet Things J.*, vol. 7, no. 11, pp. 11250–11261, Nov. 2020.

[20] Z. Xiang, W. Yang, Y. Cai, Z. Ding, and Y. Song, "Secure transmission design in HARQ assisted cognitive NOMA networks," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2528–2541, Jan. 2020.
[21] Z. Ding, R. Schober, and H. V. Poor, "Unveiling the importance of SIC in NOMA systems—Part 1: State of the art and recent findings," *IEEE Commun. Lett.*, vol. 24, no. 11, pp. 2373–2377, Nov. 2020.
[22] Z. Ding, H. Dai, and H. Vincent Poor, "Relay selection for cooperative NOMA," *IEEE Wireless Commun. Lett.*, vol. 5, no. 4, pp. 416–419, Aug. 2016.
[23] X. Yue, Y. Liu, S. Kang, A. Nallanathan, and Z. Ding, "Spatially random relay selection for full/half-duplex cooperative NOMA networks," *IEEE Trans. Commun.*, vol. 66, no. 8, pp. 3294–3308, Aug. 2018.
[24] Q. Li, P. Ren, and D. Xu, "Security enhancement and QoS provisioning for NOMA-based cooperative D2D networks," *IEEE Access*, vol. 7, pp. 129387–129401, 2019.
[25] Z. Ding, L. Dai, and H. V. Poor, "MIMO-NOMA design for small packet transmission in the Internet of Things," *IEEE Access*, vol. 4, pp. 1393–1405, 2016.
[26] X. Shao, C. Yang, D. Chen, N. Zhao, and F. R. Yu, "Dynamic IoT device clustering and energy management with hybrid NOMA systems," *IEEE Trans. Ind. Informat.*, vol. 14, no. 10, pp. 4622–4630, Oct. 2018.
[27] Z. Yang, Z. Ding, Y. Wu, and P. Fan, "Novel relay selection strategies for cooperative NOMA," *IEEE Trans. Veh. Technol.*, vol. 66, no. 11, pp. 10114–10123, Nov. 2017.
[28] Y. Yu, H. Chen, Y. Li, Z. Ding, and L. Zhuo, "Antenna selection in MIMO cognitive radio-inspired NOMA systems," *IEEE Commun. Lett.*, vol. 21, no. 12, pp. 2658–2661, Dec. 2017.
[29] Y. Yu, H. Chen, Y. Li, Z. Ding, L. Song, and B. Vucetic, "Antenna selection for MIMO nonorthogonal multiple access systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 4, pp. 3158–3171, Apr. 2018.
[30] M. K. Shukla, H. H. Nguyen, and O. J. Pandey, "Secrecy performance analysis of two-way relay non-orthogonal multiple access systems," *IEEE Access*, vol. 8, pp. 39502–39512, 2020.
[31] L. Wang, K. J. Kim, T. Q. Duong, M. Elkashlan, and H. V. Poor, "Security enhancement of cooperative single carrier systems," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 1, pp. 90–103, Jan. 2015.
[32] K. Cao, B. Wang, H. Ding, L. Lv, R. Dong, T. Cheng, and F. Gong, "Improving physical layer security of uplink NOMA via energy harvesting jammers," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 786–799, Sep. 2021.
[33] W. Khalid, H. Yu, and J. Joung, "Physical layer security for hybrid-ARQ protocols with massive antennas," in *Proc. Korea Inst. Commun. Sci. Winter Conf.*, Feb. 2020, pp. 183–184.
[34] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. Amsterdam, The Netherlands: Elsevier, 2007.

WAQAS KHALID received the B.S. degree in electronics engineering from the GIK Institute of Engineering Sciences and Technology, Pakistan, in 2011, the M.S. degree in information and communication engineering from Inha University, Incheon, South Korea, in 2016, and the Ph.D. degree in information and communication engineering from Yeungnam University, Gyeongsan, South Korea, in 2019. He is currently working as a Research Professor with the Institute of Industrial Technology, Korea University, Sejong, South Korea. His research interests include physical layer modeling, signal processing for wireless communications, and emerging solutions and technologies for 5G/B5G networks, such as energy harvesting, physical-layer security, NOMA, cognitive radio, UAVs, and the IoTs.

HEEJUNG YU (Senior Member, IEEE) received the B.S. degree in radio science and engineering from Korea University, Seoul, South Korea, in 1999, and the M.S. and Ph.D. degrees in electrical engineering from the Korea Advanced Institute of Science and Technology, Daejeon, South Korea, in 2001 and 2011, respectively. From 2001 to 2012, he was with the Electronics and Telecommunications Research Institute, Daejeon. From 2012 to 2019, he was with Yeungman University, Gyeongsan, South Korea. He is currently an Associate Professor with the Department of Electronics and Information Engineering, Korea University, Sejong, South Korea. His research interests include statistical signal processing and communication theory.