IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 5, 2019, accepted August 28, 2019, date of publication September 2, 2019, date of current version September 18, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2939048

Secrecy Rate Analysis of Opportunistic User Scheduling in Uplink Networks With Potential Eavesdroppers

INKYU BANG[1], (Member, IEEE), AND BANG CHUL JUNG[2], (Senior Member, IEEE)
[1]Department of Information and Communication Engineering, Hanbat National University, Daejeon 34158, South Korea
[2]Department of Electronics Engineering, Chungnam National University, Daejeon 34134, South Korea

Corresponding author: Bang Chul Jung (bcjung@cnu.ac.kr)

This work was supported in part by the research fund of Hanbat National University in 2019 and in part by the Basic Science Research Program of NRF through the Ministry of Science and ICT under Grant NRF2019R1A2B5B01070697.

ABSTRACT In this paper, we investigate two user scheduling algorithms (optimal user and threshold-based user scheduling algorithms) when we consider potential eavesdroppers in an uplink wiretap network. The optimal user scheduling (OUS) algorithm selects the user who has the maximum secrecy rate, based on channel feedback from all users. On the other hand, the threshold-based user scheduling (TUS) algorithm first considers the information leakage from the users to potential eavesdroppers and then selects the user among candidates who satisfy a threshold criterion on the information leakage. The OUS algorithm shows an optimal performance in terms of secrecy rate, but the TUS algorithm can achieve secrecy rate comparable with the OUS algorithm with reduced feedback overhead. For main contributions, we mathematically analyze the asymptotic behavior of the achievable secrecy rate of two scheduling algorithms when the signal-to-noise ratio (SNR) approaches to infinity. Further, we derive the approximated secrecy rate of the TUS algorithm and propose criteria to determine threshold values which maximize the achievable secrecy rate of the TUS algorithm. We verify our analytical results through simulations. We perform an extra simulation to investigate the effect of channel estimation error in the wiretap links on the average secrecy rate. Due to different scheduling principles in OUS and TUS schemes, the TUS scheme yields robustness against the channel estimation error in the wiretap links, compared with the OUS schemes.

INDEX TERMS Physical-layer security, potential eavesdropper, achievable secrecy rate, multiuser diversity, opportunistic scheduling.

I. INTRODUCTION

The broadcasting nature of radio signals over the wireless channel arises anxiety about data confidentiality from eavesdropping. To address this problem, cryptographic methods have been commonly used in upper layers of protocol stacks (e.g., transport layer) in wireless communication systems. In recent years, achieving security at the physical-layer (so-called, physical-layer security) has been considered as one of the alternatives to improve the conventional crypto-based security. Physical-layer security is based on a notion of information-theoretic secrecy which exploits the randomness of wireless channels rather than using computational hardness [1].

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

Since Shannon [2] established the fundamental principles of information-theoretic security at physical-layer, many researchers have studied physical-layer security to guarantee the confidentiality of information over wireless channels in the presence of eavesdropping attacks. Wyner [3] and Cheong and Hellman [4] established the notions of wiretap channel and secrecy capacity. Subsequent to early studies of the basic principles of the secrecy capacity [3]–[5], the secrecy capacity was investigated in wireless fading channel of single-input and single-output (SISO) environments [6]–[8]. Barros and Rodrigues [6], and Bloch *et al.* [7] characterized the secrecy rate and the secrecy outage probability for the transmission of confidential data over a quasi-static fading channel. Gopala *et al.* [8] investigated the secrecy capacity along with the optimal power and rate allocation strategies. In addition to the analysis of the

secrecy capacity in wireless fading channel of SISO environments, the analysis in multiple antennas environments was investigated [9]–[11]. Further, physical-layer security has been studied in various network settings such as energy harvesting relaying networks, cognitive relaying networks, and multi-hop relaying networks [12]–[14]. Nguyen *et al.* analyzed and derived the secrecy outage probability when channel-aware relay selection schemes are considered in the underlay cognitive relaying networks with energy harvesting constraints [12]. Liu *et al.* proposed several relay selection schemes to guarantee secure communication in cognitive decode-and-forward relay networks against eavesdropping (e.g., one of the relays performs as a jammer.) [13]. Hung *et al.* considered low-energy adaptive clustering hierarchy (LEACH) networks where a cluster-based multi-hop transmission employing artificial noises and investigated the security-reliability tradeoff [14].

Particularly, in this paper, we focus on multiuser network settings. Compared to the achievable secrecy rate analysis in single-user networks [6]–[11], the secrecy rate analysis in multiuser networks has been less highlighted. In the multiuser downlink wiretap networks (or wiretap broadcast channel), Pei *et al.* [15] and Ge *et al.* [16] derived the secrecy rate in closed-forms when opportunistic scheduling algorithms were employed. Yang *et al.* investigated a joint secure transmission scheme employing a combination of the transmit antenna selection and threshold-based user (i.e., a receiver) selection schemes in multiuser downlink wiretap networks [17]. Especially, they set a threshold value to guarantee the main channel quality between the transmitter and the receiver, and further analyzed the ergodic secrecy rate under the assumption that eavesdroppers' channel information is available during the scheduling.

In the multiuser uplink wiretap networks (or wiretap multiple access channel), the asymptotic behavior of the secrecy rate has been studied when the number of legitimate users tends to infinity [18]–[21]. In [18] and [19], Jin *et al.* investigated secrecy rate scaling in terms of the number of users in a cell to achieve the optimal multi-user diversity when a single-cell and multi-cell uplink wiretap networks are considered, respectively. In [20] and [21], Bang *et al.* analyzed the effect of multiple antennas and artificial noise, respectively, on the secrecy rate to achieve the optimal multiuser diversity in a single-cell uplink wiretap network. Further, Ge *et al.* proposed cumulative distribution function (CDF)-based scheduling and derived the closed-form expressions of the secrecy rate in [22].

In short, in multiuser uplink wiretap networks, the analysis of the secrecy rate was already investigated in terms of secrecy rate scaling or the closed-form expression. However, we further notice two things in previous work related to secrecy rate analysis in multiuser uplink wiretap networks; **(1)** The exact closed-form expression was derived in [22] but the proposed scheduling scheme might be vulnerable to channel estimation errors on wiretap links (i.e., the wireless link between transmitter and eavesdropper); **(2)** A threshold-based user scheduling scheme which was commonly considered in [18]–[21] is robust to channel estimation errors on wiretap links. However, when the number of users is finite, the achievable secrecy rate of this scheduling scheme has not been investigated yet. Accordingly, still, it is important to derive the achievable secrecy rate even in a single cell uplink wiretap network when we consider various scheduling schemes such as the threshold-based user scheduling scheme in [18]–[21]. This will be helpful to fill the gap between secrecy rate analysis of different scheduling schemes and to fully understand the characteristics of the secrecy rate in uplink multiuser networks.

In this paper, we investigate two user scheduling algorithms in a single cell uplink wiretap network: optimal user scheduling (OUS) and threshold-based user scheduling (TUS) algorithms. The uplink wiretap network consists of a single desired receiver and a finite number of users (i.e., transmitters) including potential eavesdroppers and we analyze various aspects of two user scheduling algorithms. The main contributions of this paper are summarized as follows:

- We provide the approximated ergodic secrecy rate of the threshold-based user scheduling algorithm, propose criteria of threshold values to maximize the secrecy rate, and validate the analytical results through simulations (see Sections IV and V).
- We mathematically analyze asymptotic behavior of the achievable secrecy rate of two scheduling algorithms as the signal-to-noise ratio (SNR) approaches to infinity (see Sections III and IV).
- We investigate the impact of wiretap links' channel estimation errors and the effect of multiple antennas at the receiver, on the secrecy rate of two user scheduling algorithms, respectively, through simulations (see Section VI).

The rest of this paper is organized as follows. In Section II, the overall system model is presented. In Section III, OUS algorithm is introduced and its analytical results are provided. Similarly, TUS algorithm is introduced, its analytical results are provided, and, additionally, criteria of threshold values to maximize the secrecy rate is proposed in Section IV. The performance of OUS and TUS in terms of the secrecy rate is evaluated in Section V. In Section VI, we additionally discuss featured issues in applying our proposed scheduling schemes. Finally, conclusive remarks and future work are provided in Section VII.

II. SYSTEM MODEL

As described in Fig. 1, we consider a multiuser SISO uplink wiretap network which consists of a single desired receiver and N legitimate users (transmitters) including K *potential eavesdroppers* (i.e., $K < N$) [23], [24]. From the perspective of the system, a total of N users are considered during each scheduling time slot, regardless of the number of potential eavesdroppers. However, the system properly sets the number of potential eavesdroppers before a specific scheduling algorithm is running. For example, all unscheduled

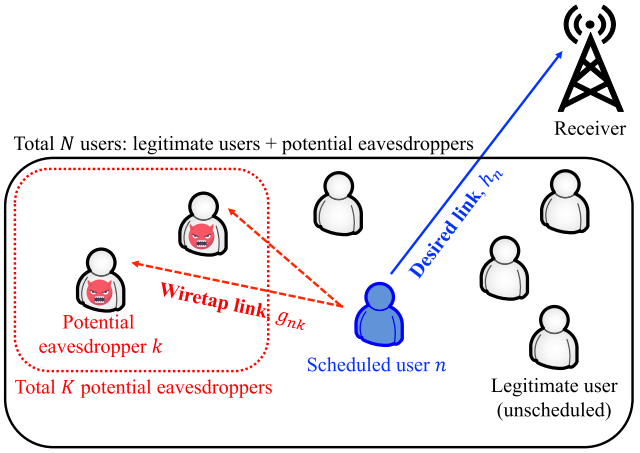

FIGURE 1. An example of multiuser SISO uplink network: a single receiver and N users (index n) including K potential eavesdroppers (index k).

users are considered as potential eavesdroppers if we set $K = N - 1$ [24]. On the other hands, only one user can be considered as a potential eavesdropper (e.g., a user near the scheduled user) if we set $K = 1$ [25]. We assume that the potential eavesdroppers operate without any cooperation among them (i.e., the non-colluding eavesdroppers model). Throughout the paper, we use terms 'desired' and 'wiretap' links to indicate transmission links from a scheduled user to the desired receiver and a potential eavesdropper, respectively.

Let $h_n \in \mathbb{C}$ denotes a channel fading coefficient from user n to the desired receiver for $n \in \mathcal{N} \triangleq \{1, \cdots, N\}$ and is assumed to be a complex Gaussian random variables with zero mean and variance $\sigma_{h_n}^2$, i.e., $h_n \sim \mathcal{CN}(0, \sigma_{h_n}^2)$. Similarly, let $g_{nk} \in \mathbb{C}$ denotes a channel fading coefficient from user n to potential eavesdropper k and is assumed to be a complex Gaussian random variables with zero mean and variance $\sigma_{g_{nk}}^2$, i.e., $g_{nk} \sim \mathcal{CN}(0, \sigma_{g_{nk}}^2)$. For analytical tractability, we assume that h_n and g_{nk} are independent and identically distributed (i.i.d.), i.e., $\sigma_{h_n}^2 = \sigma_h^2$ and $\sigma_{g_{nk}}^2 = \sigma_g^2$ $\forall n, k$.[1]

We consider a time slot based system where a single user is scheduled in one time slot (or one scheduling slot) to securely send data to the desired receiver against potential eavesdroppers. As shown in Fig. 2, one time slot is split into multiple mini-slots and each user transmits a pilot during one mini-slots for channel estimation purpose (total N mini-slots). Accordingly, the *local channel state information (CSI)* including both desired and wiretap links is available at each user (i.e., h_n and g_{nk} $\forall k$ for only user n). Note that a specific channel feedback method after local CSI estimation at each user mainly relies on a user scheduling algorithm. We assume that the signaling overhead for the channel estimation and feedback is negligible.

[1]For example, we can set $\sigma_{h_n}^2 = \sigma_h^2$ to consider equal-distance users (or equivalently using proper power control at each user) and set $\sigma_g^2 = \max_{\forall k} \left\{\sigma_{g_{nk}}^2\right\}$ to consider the worst case of secrecy performance.

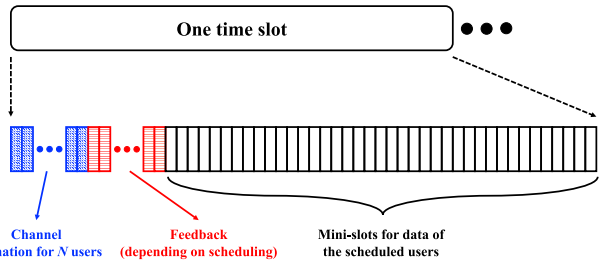

FIGURE 2. An example of a time slot which consists of multiple mini-slots for channel estimations, channel feedbacks, and data transmission.

When user n is scheduled, the received signals at the desired receiver and at potential eavesdropper k are expressed, respectively, as

$$y = h_n x_n + z,$$
$$y_k = g_{nk} x_n + z_k,$$

where x_n denotes the desired data symbol for user n with an average power constraint $\mathbb{E}[x_n] \leq P$, and z and z_k denote the circularly symmetric complex additive white Gaussian noises (AWGNs) with zero mean and variance σ^2. We define the transmit SNR as $\rho \triangleq \frac{P}{\sigma^2}$.

The achievable secrecy rate of user n is obtained as

$$C_n = \left[\log\left(1 + |h_n|^2\rho\right) - \log\left(1 + \max_{k\in\mathcal{K}} |g_{nk}|^2\rho\right)\right]^+, \quad (1)$$

where the first and second terms in right-hand side represent the achievable rate of the desired and wiretap links, respectively, and $[x]^+ = \max\{x, 0\}$.

The achievable rate of the wiretap link (i.e., information leakage from the scheduled user to potential eavesdroppers) in (1) is formulated into a maximum of each eavesdropper's achievable rate due to a noncooperation assumption. Further, the achievable secrecy rate of the scheduled user in (1) highly depends on user scheduling schemes. Throughout the paper, we focus on the centralized scheduling in which the receiver explicitly determines the scheduled user even though the user scheduling algorithms can be implemented in a distributed manner by exploiting backoff timer as in [26].

III. OPTIMAL USER SCHEDULING SCHEME

In this section, we introduce an optimal user scheduling (OUS) scheme in terms of the achievable secrecy rate. In order to maximize the achievable secrecy rate, a served user has to be selected by taking (1) into consideration. Accordingly, the selected user index of the OUS scheme is given by

$$n^\star = \arg\max_{n\in\mathcal{N}} \left\{\log\left(\frac{1 + |h_n|^2\rho}{1 + \max_{k\in\mathcal{K}} |g_{nk}|^2\rho}\right)\right\}. \quad (2)$$

The OUS requires $N + KN$ mini-slots for channel estimation (N mini-slots) and feedback (KN mini-slots) since each user has to report CSI of K wiretap links to the receiver.

For the scheduled user $n^\star$, the ergodic secrecy rate of the OUS scheme is obtained as

$$\begin{aligned}\bar{C}_{n^\star} &= \mathbb{E}\left[\log\left(\frac{1+|h_{n^\star}|^2\rho}{1+\max\limits_{k\in\mathcal{K}}|g_{n^\star k}|^2\rho}\right)\middle| C_{n^\star}\geq 0\right]\Pr\{C_{n^\star}\geq 0\}\\ &\approx \mathbb{E}\left[\log\left(\frac{1+|h_{n^\star}|^2\rho}{1+\max\limits_{k\in\mathcal{K}}|g_{n^\star k}|^2\rho}\right)\right]\\ &= \int_0^\infty \log(z)\, dF_{Z_{n^\star}}(z), \end{aligned} \tag{3}$$

where the approximation holds from the fact that $\Pr\{C_{n^\star}\geq 0\} \approx 1$ for sufficiently large N. $F_{Z_{n^\star}}(z)$ is the cumulative density function (CDF) of a random variable $Z_{n^\star}$ which is defined as

$$Z_{n^\star} \triangleq \frac{1+|h_{n^\star}|^2\rho}{1+\max\limits_{k\in\mathcal{K}}|g_{n^\star k}|^2\rho} = \max_{n\in\mathcal{N}}\left\{\frac{|h_n|^2+1/\rho}{\max\limits_{k\in\mathcal{K}}|g_{nk}|^2+1/\rho}\right\}.$$

In order to calculate the ergodic secrecy rate of the OUS scheme, we first need to derive the CDF of $Z_{n^\star}$. For notational simplicity, we use the following notations given by $X=|h_n|^2$, $Y=\max\limits_{k\in\mathcal{K}}|g_{nk}|^2$, and, $Z=\frac{|h_n|^2+1/\rho}{\max\limits_{k\in\mathcal{K}}|g_{nk}|^2+1/\rho}=\frac{X+1/\rho}{Y+1/\rho}$.

Both $|h_n|^2$ and $|g_{nk}|^2$ follow an exponential distribution. Further, Y is the maximum of K i.i.d. exponential random variables. Thus, the CDF of Z is obtained using the relationship among X, Y, and Z, and it is given by [27]

$$\begin{aligned}F_Z(z) &= \int_{1/\rho}^{\infty}\int_{1/\rho}^{zy} f_X\left(x-\frac{1}{\rho}\right) f_Y\left(y-\frac{1}{\rho}\right) dxdy\\ &= 1+\sum_{i=1}^{K}\binom{K}{i}(-1)^i\frac{\sigma_h^2\, i}{\sigma_g^2\, z+\sigma_h^2\, i}e^{-\frac{z-1}{\sigma_h^2\rho}},\end{aligned}$$

where $f_X(x)$ and $f_Y(y)$ are probability density functions (PDFs) of X and Y, respectively.

Since $Z_{n^\star}$ is a maximum of N i.i.d. random variable Z, the CDF of $Z_{n^\star}$ is obtained as follows:

$$F_{Z^\star}(z) = \left(1+\sum_{i=1}^{K}\binom{K}{i}(-1)^i\frac{\sigma_h^2\, i}{\sigma_g^2\, z+\sigma_h^2\, i}e^{-\frac{z-1}{\sigma_h^2\rho}}\right)^N. \tag{4}$$

Using (3) and (4), the ergodic secrecy rate of the OUS scheme can be calculated as follows:

$$\begin{aligned}\bar{C}_{n^\star} = N\int_0^\infty \log(z)\left(1+\sum_{i=1}^{K}\binom{K}{i}\frac{(-1)^i\sigma_h^2 i}{\sigma_g^2 z+\sigma_h^2 i}e^{-\frac{z-1}{\sigma_h^2\rho}}\right)^{N-1}\\ \times\left\{\sum_{i=1}^{K}\binom{K}{i}\frac{(-1)^{i+1}\sigma_h^2\sigma_g^2\rho i+\sigma_g^2 iz+\sigma_h^2 i^2}{\rho\left(\sigma_g^2 z+\sigma_h^2 i\right)^2}e^{-\frac{z-1}{\sigma_h^2\rho}}\right\}dz.\end{aligned} \tag{5}$$

Note that (5) generally cannot be expressed as a closed form but it can be evaluated through numerical calculations [28]. Additionally, for the special case of $K=1$ and $\rho\to\infty$, we derive the closed-form expression of (5).

Proposition 1 (Secrecy performance of the OUS scheme for $K=1$ and high SNR): In the case of $K=1$ and $\rho\to\infty$, the closed form of (5) is obtained as follows:

$$\bar{C}_{n^\star}^{\infty} = \sum_{i=1}^{N}\binom{N}{i}(-1)^i\left(\boldsymbol{\gamma}+\psi(i)+\log\left(\frac{\sigma_g^2}{\sigma_h^2}\right)\right), \tag{6}$$

where $\boldsymbol{\gamma}\approx 0.577216$ is Euler's constant, and $\psi(x)$ is the digamma function defined as $\psi(x)\triangleq\frac{d}{dx}\ln\Gamma(x)$ where $\Gamma(x)$ is the gamma function defined as $\Gamma(x)\triangleq\int_0^\infty t^{x-1}e^{-t}dt$.

Proof: See Appendix A. ∎

IV. THRESHOLD-BASED USER SCHEDULING SCHEME

In this section, we introduce a threshold-based user scheduling (TUS) scheme discussed in [18]–[21]. The basic idea of the TUS scheme is to select a user in order to prevent information leakage from a user against eavesdroppers by using an appropriate threshold value (i.e., applying at the wiretap links). It is worth noting that the threshold-based selection scheme in [17] mainly considers the desired link (i.e., CSI between the transmitter and the receiver) instead of the wiretap link. This difference results in a new analysis in this paper, compared with the results in [17]. The overall scheduling process of the TUS scheme in a certain time slot is described as follows:

- **Step 1**: Each user estimates its expected information leakage based on CSI from K eavesdroppers, i.e., $\max\limits_{k\in\mathcal{K}}|g_{nk}|^2$.
- **Step 2**: Only users who satisfy the following threshold criterion **(C1)** transmit a feedback message, i.e., $|h_n|^2$, to the receiver.

  $$(C1)\quad \max_{k\in\mathcal{K}}|g_{nk}|^2\leq\eta_{\mathrm{L}},$$

  where η_{L} is the predetermined positive threshold value, which can be determined through simulation or our proposed methods.
- **Step 3**: After collecting feedback from only selected users, the receiver schedules the user (n^*) who has the largest $|h_n|^2$. Then, the scheduled user transmit its data.

The TUS requires $N+1$ to $2N$ mini-slots for channel estimation (N mini-slots) and feedback ($1\sim N$ mini-slots) since selected users only send an indication instead of K wiretap links' CSI.

A. ERGODIC SECRECY RATE OF THE TUS SCHEME

Now we focus on deriving the ergodic secrecy rate of the TUS scheme summarized in the following theorem.

*Theorem 1: For the scheduled user n^* and a given threshold value η_L, the ergodic secrecy rate of the TUS scheme is given by (7), as shown at the top of next page, where p_η is a probability that a certain user satisfies the threshold criterion **(C1)**, given by $p_\eta \triangleq \left(1-\exp\left(-\frac{\eta_L}{\sigma_g^2}\right)\right)^K$ and $E_1(x)\triangleq\int_x^\infty\frac{\exp(-t)}{t}dt$.*

$$\bar{C}_{n^*}(\eta_{\mathrm{L}}) = \sum_{n=1}^{N} \binom{N}{n} p_\eta^n (1-p_\eta)^{N-n} \sum_{i=1}^{n} \binom{n}{i} (-1)^{i+1} e^{\frac{i}{\sigma_h^2 \rho}} \mathrm{E}_1\left(\frac{i}{\sigma_h^2 \rho}\right) - \frac{1}{p_\eta} \sum_{i=1}^{K} \binom{K}{i} (-1)^{i+1} \left(e^{\frac{i}{\sigma_g^2 \rho}} \left(\mathrm{E}_1\left(\frac{i}{\sigma_g^2 \rho}\right) - \mathrm{E}_1\left(\frac{i}{\sigma_g^2 \rho} + \frac{i\eta_{\mathrm{L}}}{\sigma_g^2}\right)\right) - e^{-\frac{i\eta_{\mathrm{L}}}{\sigma_g^2}} \log(1+\eta_{\mathrm{L}}\rho) \right), \quad (7)$$

Proof: Similar to the OUS scheme, for the scheduled user n^* and a given threshold value η_{L}, the ergodic secrecy rate of the TUS scheme is derived as

$$\begin{aligned}\bar{C}_{n^*}(\eta_{\mathrm{L}}) &\approx \mathbb{E}\left[\log\left(1+|h_{n^*}|^2\rho\right) - \log\left(1+\max_{k\in\mathcal{K}}|g_{n^*k}|^2\rho\right)\right] \\ &= \bar{C}_{\mathrm{d}}(\eta_{\mathrm{L}}) - \bar{C}_{\mathrm{w}}(\eta_{\mathrm{L}}), \end{aligned} \quad (8)$$

where the approximation holds with the same assumption in (3). Here, we define $\bar{C}_{\mathrm{d}}(\eta_{\mathrm{L}}) \triangleq \mathbb{E}\left[\log\left(1+|h_{n^*}|^2\rho\right)\right]$ and $\bar{C}_{\mathrm{w}}(\eta_{\mathrm{L}}) \triangleq \mathbb{E}\left[\log\left(1+\max_{k\in\mathcal{K}}|g_{n^*k}|^2\rho\right)\right]$, respectively, for notation simplicity during the proof.

Next, we need to obtain $\bar{C}_{\mathrm{d}}(\eta_{\mathrm{L}})$ and $\bar{C}_{\mathrm{w}}(\eta_{\mathrm{L}})$ in (8) for a given threshold value η_{L}. In the TUS scheme, the number of users who transmit their feedback message varies depending on a value of η_{L}. Let N_{c} denote the number of users who satisfy the threshold criterion **(C1)** in a certain time slot. On condition of a given N_{c}, $|h_{n^*}|^2$ is the maximum of N_{c} i.i.d. exponential random variables since each $|h_n|^2$ follows an exponential distribution independent of $|g_{nk}|^2$. Thus, we can obtain $\bar{C}_{\mathrm{d}}(\eta_{\mathrm{L}}; N_{\mathrm{c}})$ given by

$$\begin{aligned}\bar{C}_{\mathrm{d}}(\eta_{\mathrm{L}}; N_{\mathrm{c}}) &= \mathbb{E}\left[\log\left(1+|h_{n^*}|^2\rho\right)|N_{\mathrm{c}}\right] \\ &= \int_0^\infty \log(1+\rho x)\, dF_{|h_{n^*}|^2}(x) \\ &= \sum_{i=1}^{N_{\mathrm{c}}} \binom{N_{\mathrm{c}}}{i} (-1)^{i+1} e^{\frac{i}{\sigma_h^2\rho}} \mathrm{E}_1\left(\frac{i}{\sigma_h^2\rho}\right), \end{aligned} \quad (9)$$

where the last equality holds from [29, (4.337.2)] and $\mathrm{E}_1(x)$ is the exponential integral function [29].

Accordingly, $\bar{C}_{\mathrm{d}}(\eta_{\mathrm{L}})$ in (8) is obtained through the expected value of all possible conditional expectation in (9) when $N_{\mathrm{c}} = n$ for $n \in \{1, \cdots, N\}$ and it it given by

$$\begin{aligned}\bar{C}_{\mathrm{d}}(\eta_{\mathrm{L}}) &= \mathbb{E}\left[\log\left(1+|h_{n^*}|^2\rho\right)\right] \\ &= \sum_{n=1}^{N} \binom{N}{n} p_\eta^n (1-p_\eta)^{N-n}\, \mathbb{E}\left[\log\left(1+|h_{n^*}|^2\rho\right)|N_{\mathrm{c}}\right] \\ &= \sum_{n=1}^{N} \binom{N}{n} p_\eta^n (1-p_\eta)^{N-n}\, \bar{C}_{\mathrm{d}}(\eta_{\mathrm{L}}; n), \end{aligned} \quad (10)$$

where p_η is a probability that a certain user satisfies the threshold criterion **(C1)**, given by $p_\eta \triangleq \left(1-\exp\left(-\frac{\eta_{\mathrm{L}}}{\sigma_g^2}\right)\right)^K$.

To obtain $\bar{C}_{\mathrm{w}}(\eta_{\mathrm{L}})$ in (8), we first need to derive the CDF of $Y^* = \max_{k\in\mathcal{K}}|g_{n^*k}|^2$. Since the scheduled user (n^*) always satisfies the threshold criterion **(C1)**, the CDF of Y^* is the maximum of K i.i.d. truncated exponential random variables [27]. Thus, $\bar{C}_{\mathrm{w}}(\eta_{\mathrm{L}})$ is given by (11), as shown at the bottom of the next page. Finally, substituting (10) and (11) into (8) yields the ergodic secrecy rate of the TUS scheme (i.e., $\bar{C}_{\mathrm{d}}(\eta_{\mathrm{L}}) - \bar{C}_{\mathrm{w}}(\eta_{\mathrm{L}})$) and it is given by (7). ■

Note that we derive the ergodic secrecy rate of the TUS scheme for general parameters such as N, K, ρ, σ_h^2, σ_g^2, and η_{L}.

Corollary 1: [Secrecy performance of TUS in high SNR] For $\rho \to \infty$, the ergodic secrecy rate of the TUS scheme $\bar{C}_{n^*}(\eta_L)$ is reduced to (12)*, as shown at the bottom of the next page, where $\boldsymbol{\gamma} \approx 0.577216$ is Euler's constant.*

Proof: See Appendix B. ■

B. DETERMINATION OF THRESHOLD VALUE

For given system parameters (N, K, ρ, σ_h^2, and σ_g^2), the ergodic secrecy rate of the TUS scheme is a function of η_{L}. Therefore, we propose two methods to determine the threshold value: an optimal-determination method and a predictable-determination method.

1) OPTIMAL-DETERMINATION METHOD

The optimal-determination method is to set the threshold value by using a linear search algorithm on (7) for all η_{L}. Thus, the threshold value set by the optimal-determination method is given by

$$\eta_{\mathrm{L}}^{\mathrm{opt}} = \arg\max_{\forall \eta_{\mathrm{L}}} \bar{C}_{n^*}(\eta_{\mathrm{L}}). \quad (13)$$

Definitely, the optimal-determination method guarantees the optimal secrecy performance of the TUS scheme. However, it inherently incurs a computational cost since it requires an exhaustive search for all η_{L}.

2) PREDICTABLE-DETERMINATION METHOD

The predictable-determination method is to set the threshold value by exploiting the basic principles of the TUS scheme. In the TUS protocol, if there is no user satisfying the threshold criterion **(C1)**, the corresponding time slot would be wasted. Let p_0 denote the probability that there exists at least one user satisfying the threshold criterion **(C1)** and it is expressed

as follows:

$$p_0 = 1 - \left(1 - \left(1 - \exp\left(-\frac{\eta_{\mathrm{L}}}{\sigma_g^2}\right)\right)^K\right)^N. \tag{14}$$

In order to regulate the number of wasted time slots under a certain level, p_0 should be greater than some constant, i.e., $p_0 \geq 1-\epsilon_0$ where ϵ_0 represents the wasted time slot ratio. Using $p_0 = 1-\epsilon_0$, the threshold value set by the predictable-determination method is obtained as follows:

$$\eta_{\mathrm{L}}^{\mathrm{pre}} = -\sigma_g^2 \log\left(1 - \left(1 - \epsilon_0^{\frac{1}{N}}\right)^{\frac{1}{K}}\right). \tag{15}$$

Note that ϵ_0 is the control parameter which we can determine. We empirically choose ϵ_0 between 10^{-5} and 10^{-3}. The predictable-determination method does not provide an optimal threshold value for $\bar{C}_{n^*}(\eta_{\mathrm{L}})$. However, it is directly calculated from (15) and provides quite good secrecy performance.

V. PERFORMANCE EVALUATION

In this section, we evaluate the performance of OUS and TUS schemes in terms of the average secrecy rate through our analysis and simulations, compared with a conventional *MaxSNR* user scheduling scheme. The MaxSNR scheme selects a user having the largest value of SNR on the desired link (i.e., $|h_n|^2$). In addition, for $\rho \to \infty$, the ergodic secrecy rate of the MaxSNR scheme can be calculated as

$$\bar{C}_{\mathrm{MaxSNR}}^{\infty} = \sum_{i=1}^{N} \binom{N}{i} (-1)^i \left(\gamma + \log\left(\frac{i}{\sigma_h^2}\right)\right) - \sum_{i=1}^{K} \binom{K}{i} (-1)^i \left(\gamma + \log\left(\frac{i}{\sigma_g^2}\right)\right), \tag{16}$$

where $\gamma \approx 0.577216$ is Euler's constant and the detailed derivation is provided in Appendix C.

Note that the MaxSNR scheme does not utilize CSI of wiretap links, (i.e., g_{nk}) and thus it shows a baseline secrecy performance when g_{nk} is unavailable. We use (16) for comparison in high SNR regime.

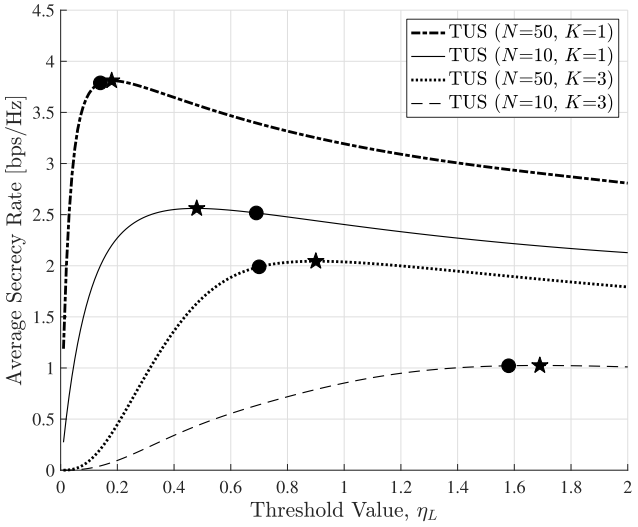

FIGURE 3. Average achievable secrecy rate for varying threshold value η_{L} when $\epsilon_0 = 10^{-3}$, $\rho = 10$ dB, $\sigma_h^2 = 1$, $\sigma_g^2 = 1$, and various sets of N and K.

A. NUMERICAL RESULTS

Fig. 3 shows the average achievable secrecy rate for varying threshold values η_{L}. For comparison, we consider four different (N, K) pairs. For each line, a star-shaped marker indicates $\eta_{\mathrm{L}}^{\mathrm{opt}}$, and its corresponding average secrecy rate. Similarly, a circle marker in each line indicates $\eta_{\mathrm{L}}^{\mathrm{pre}}$ and its corresponding average secrecy rate. As N increases for fixed K, values of both $\eta_{\mathrm{L}}^{\mathrm{opt}}$ and $\eta_{\mathrm{L}}^{\mathrm{pre}}$ decrease since the criterion **(C1)** can be satisfied with high probability even for a small threshold value when the number of users in the system increases. On the contrary, threshold values of both methods increase when K increases for fixed N. The gap between the secrecy rate of $\eta_{\mathrm{L}}^{\mathrm{pre}}$ and that of $\eta_{\mathrm{L}}^{\mathrm{opt}}$ is negligible. Thus, using $\eta_{\mathrm{L}}^{\mathrm{pre}}$ instead of $\eta_{\mathrm{L}}^{\mathrm{opt}}$ is one of reasonable alternatives.

Fig. 4 shows the average achievable secrecy rate for varying SNRs. System parameters are set to $N = 30$, $K = 1$, $\sigma_h^2 = 1$, and $\sigma_g^2 = 1$. For determining $\eta_{\mathrm{L}}^{\mathrm{pre}}$, $\epsilon_0 = 10^{-3}$ is used. As the SNR (ρ) increases, the secrecy rates of all schemes increase but finally converge to certain values since an increase in the transmit power increases the achievable rate of desired channel and that of wiretap channel at the same time. The analytical results for the average secrecy rate of the

$$\bar{C}_{\mathrm{w}}(\eta_{\mathrm{L}}) = \frac{1}{p_\eta} \sum_{i=1}^{K} \binom{K}{i} (-1)^{i+1} \left(e^{\frac{i}{\sigma_g^2 \rho}} \left(\mathrm{E}_1\left(\frac{i}{\sigma_g^2 \rho}\right) - \mathrm{E}_1\left(\frac{i}{\sigma_g^2 \rho} + \frac{i\eta_{\mathrm{L}}}{\sigma_g^2}\right)\right) - e^{-\frac{i\eta_{\mathrm{L}}}{\sigma_g^2}} \log(1 + \eta_{\mathrm{L}}\rho)\right), \tag{11}$$

$$\bar{C}_{n^*}^{\infty}(\eta_{\mathrm{L}}) = \sum_{n=1}^{N} \binom{N}{n} p_\eta^n (1-p_\eta)^{N-n} \sum_{i=1}^{n} \binom{n}{i} (-1)^i \left(\gamma + \log\frac{i}{\sigma_h^2}\right) - \sum_{i=1}^{K} \binom{K}{i} \frac{(-1)^i}{p_\eta} \left(\gamma + \log\left(\frac{i}{\sigma_g^2}\right) + \mathrm{E}_1\left(\frac{i\eta_{\mathrm{L}}}{\sigma_g^2}\right) + e^{-\frac{i\eta_{\mathrm{L}}}{\sigma_g^2}} \log\eta_{\mathrm{L}}\right), \tag{12}$$

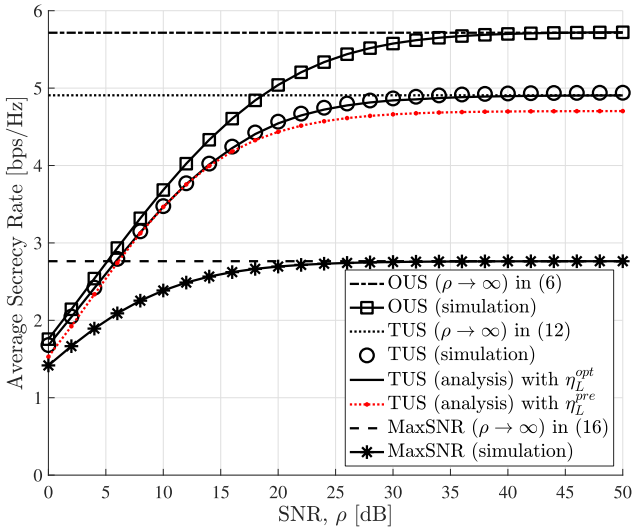

FIGURE 4. Average achievable secrecy rate for varying SNR when $\epsilon_0 = 10^{-3}$, $N = 30$, $K = 1$, $\sigma_h^2 = 1$, and $\sigma_g^2 = 1$.

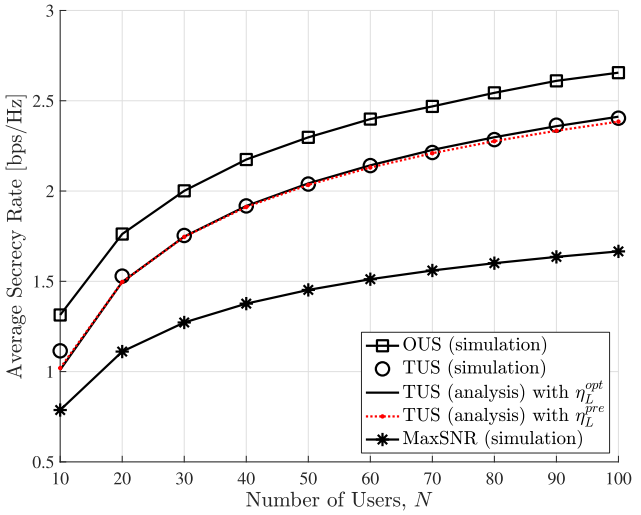

FIGURE 5. Average achievable secrecy rate for varying the number of users when $\epsilon_0 = 10^{-4}$, $K = 3$, $\rho = 10$ dB, $\sigma_h^2 = 1$, and $\sigma_g^2 = 1$.

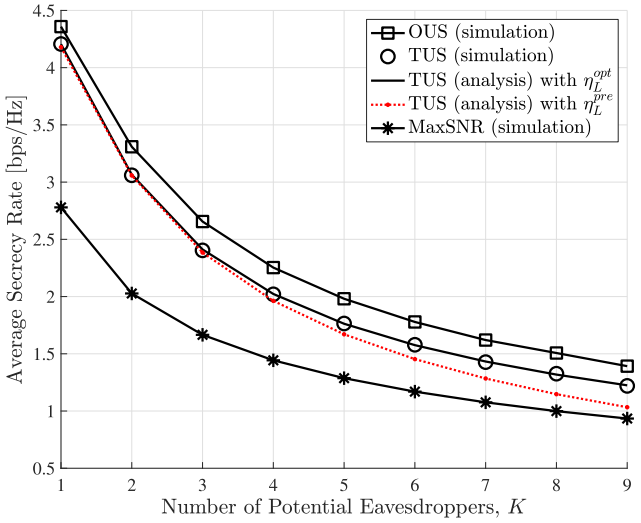

FIGURE 6. Average achievable secrecy rate for varying the number of eavesdroppers when $\epsilon_0 = 10^{-4}$, $N = 100$, $\rho = 10$ dB, $\sigma_h^2 = 1$, and $\sigma_g^2 = 1$.

TUS scheme, including analytical convergence points in (12) when $\rho \to \infty$, matches well with simulation results.

Fig. 5 shows the average achievable secrecy rate for varying the number of users. The system parameters are set as $K = 3$, $\rho = 10$ dB, $\sigma_h^2 = 1$, and $\sigma_g^2 = 1$. We use $\epsilon_0 = 10^{-4}$ to determine $\eta_{\mathrm{L}}^{\mathrm{pre}}$. For all three schemes, the average secrecy rates increase as N increases since an increase in the number of users in the system provides additional multiuser diversity which contributes to enhancing secrecy performance. OUS and TUS schemes outperform the conventional scheduling scheme because those schemes effectively take the wiretap channel state of the desired users, i.e., $|g_{nk}|^2$, into consideration. The OUS scheme yields the best performance among three schemes since it always guarantees the optimal user selection in terms of the secrecy rate. However, the OUS scheme requires feedback messages from all users, whereas the TUS scheme only requires feedback messages from users satisfying the threshold criterion **(C1)**. In addition, the average secrecy rate of the TUS scheme with $\eta_{\mathrm{L}}^{\mathrm{pre}}$ and that with $\eta_{\mathrm{L}}^{\mathrm{opt}}$ are almost similar for all ranges of N.

Fig. 6 shows the average achievable secrecy rate for varying the number of potential eavesdroppers. System parameters are set as $N = 100$, $\rho = 10$ dB, $\sigma_h^2 = 1$, and $\sigma_g^2 = 1$. We use $\epsilon_0 = 10^{-4}$ to determine $\eta_{\mathrm{L}}^{\mathrm{pre}}$. For a small number of potential eavesdroppers ($K \leq 5$), the average secrecy rate of the TUS scheme with $\eta_{\mathrm{L}}^{\mathrm{pre}}$ and that with $\eta_{\mathrm{L}}^{\mathrm{opt}}$ are almost similar. However, the secrecy performance gap between the TUS scheme with $\eta_{\mathrm{L}}^{\mathrm{pre}}$ and that with $\eta_{\mathrm{L}}^{\mathrm{opt}}$ increases when K increases due to the fact that $\epsilon_0 = 10^{-4}$ is not appropriate to reflect the effect of potential eavesdroppers in the system. For all three schemes, the average secrecy rates decrease as K increases since the information leakage of the desired users increases.

Fig. 7 shows the average achievable secrecy rate when we consider a relative channel-quality ratio between a mean channel-quality of the desired link and that of the wiretap link, which is defined as $\lambda \triangleq \frac{\sigma_g^2}{\sigma_h^2}$. System parameters are set as $N = 30$, $\sigma_h^2 = 1$, and $\sigma_g^2 = 1$. We utilize (6), (12), and (16) to obtain results. Note that λ equivalently implies the relative distance ratio since values of σ_h^2 and σ_g^2 are inversely proportional to distances of main and wiretap links, respectively. As λ increases, the secrecy rates of all schemes decrease and finally converge to zero since a large value of λ implies that scheduled user is located closer to potential eavesdroppers rather than the desired receiver, i.e., $\sigma_g^2 \gg \sigma_h^2$. On contrary to this, the secrecy rates of all schemes increase as λ decreases.

VI. DISCUSSION

In this section, we discuss some issues in applying our proposed scheduling schemes (OUS and TUS) such as the impact

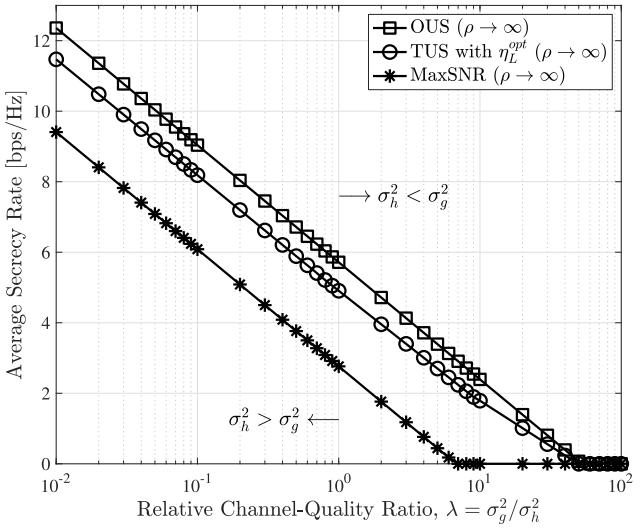

FIGURE 7. Average achievable secrecy rate for varying the relative channel-quality ratio λ when $N = 30$, $K = 1$, and $\rho \to \infty$.

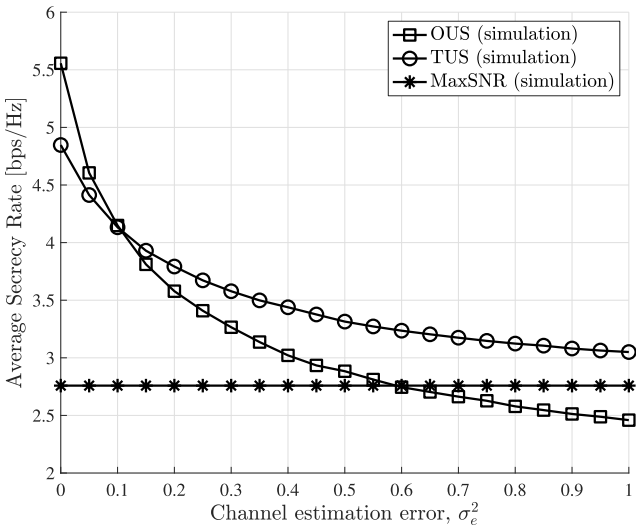

FIGURE 8. Average secrecy rate when σ_e^2 of g_e in (17) varies from 0 (i.e., no channel estimation error) to 1, we set $N = 30$, $K = 1$, $\sigma_h^2 = 1$, and $\sigma_g^2 = 1$.

of channel estimation errors, multiple antennas, and lots of eavesdroppers. Here, we also provide a summary of CSI related properties of OUS and TUS.

A. IMPACT OF CHANNEL ESTIMATION ERRORS ON AVERAGE SECRECY RATE

We investigate the effect of imperfect CSI between the user and the potential eavesdroppers on the secrecy rate. We consider estimated CSI of the wiretap link between user n and potential eavesdropper k as follows:

$$\hat{g}_{nk} = g_{nk} + g_e, \tag{17}$$

where $g_{nk} \sim \mathcal{CN}(0, \sigma_g^2)$ and $g_e \sim \mathcal{CN}(0, \sigma_e^2)$ denote the original CSI and the channel estimation error of the wiretap link, respectively. The Gaussian error is commonly used in modeling the channel estimation error [20].

Fig. 8 shows average secrecy rate when σ_e^2 of g_e in (17) varies from 0 (i.e., no channel estimation error) to 1. Also, we have set other system parameters as $N = 30$, $K = 1$, $\sigma_h^2 = 1$, and $\sigma_g^2 = 1$. Interestingly, the TUS scheme shows a better performance in terms of secrecy rate than the OUS scheme when channel estimation error increases. Also, the secrecy performance degradation in the OUS scheme is even worse than our expectation. For example, the MaxSNR scheme outperforms the OUS scheme when channel estimation error is quite large (e.g., $\sigma_e^2 = 0.6$).[2] Please note that severe secrecy performance degradation in the OUS scheme comes from the high dependency of CSI of the wiretap links in its scheduling policy. Suppose $\hat{g}_{nk}$ is completely different from the original g_{nk}, the OUS scheme does not guarantee the optimal secrecy performance anymore since it may select the scheduled user which might have the poor channel condition. However, in the TUS scheme, at least the secrecy performance of the MaxSNR scheme can be guaranteed even in this situation. If we set a threshold value of the TUS as large as possible (i.e., $\eta_L \to \infty$), then the TUS operates the same as the MaxSNR scheme since all users report indications of the threshold condition and the receiver selects the scheduled user using only the CSI of the desired link, which is exactly the same as the MaxSNR scheme.

B. APPLYING MULTIPLE ANTENNA ON OUS AND TUS

We investigate the effect of multiple antennas at the receiver which employs a maximum ratio combining (MRC) technique.[3] We still consider that transmitters including potential eavesdroppers equip with a single antenna.

If we consider MRC at the receiver, only a distribution of the desired channel (i.e., $|h_n|^2$ in (1)) changes from the exponential distribution to Chi-squared distribution. Thus, the analysis in this paper can be extended. However, the extended analysis would not be straightforward and not be easily tractable. We leave this issue for future work. Instead, we provide simulation results.

Fig. 9 shows average secrecy rate when the number of antennas (M) at the receiver varies from 1 (a single antenna) to 16. Additionally, we have set other system parameters as $N = 30$, $\rho = 30$ dB, $K = 1$, $\sigma_h^2 = 1$, and $\sigma_g^2 = 1$. As we expect, the secrecy rate of all scheduling schemes is improved when the number of antennas at the receiver increases. Interestingly, as the number of antennas at the receiver increases, the performance gap between different scheduling schemes (e.g., OUS and TUS) also increases. However, it seems that the ratio of secrecy rate of TUS and that of OUS keeps

[2]The MaxSNR scheme shows the same secrecy performance regardless of channel estimation error since it only requires CSI of the desired link.

[3]Including the MRC technique, several multiple antennas techniques (e.g., zero-forcing technique) can be applied. However, we limit our focus to the MRC technique.

TABLE 1. The summary of CSI related information on OUS and TUS.

	The required number of mini-slots for CSI feedback	CSI feedback time complexity	Scheduling policy	Robustness of channel estimation errors
OUS	$N + KN$	$\mathcal{O}\left(N^2\right)$	centralized	✗
TUS	$N + 1 \sim 2N$	$\mathcal{O}\left(N\right)$	centralized	✓

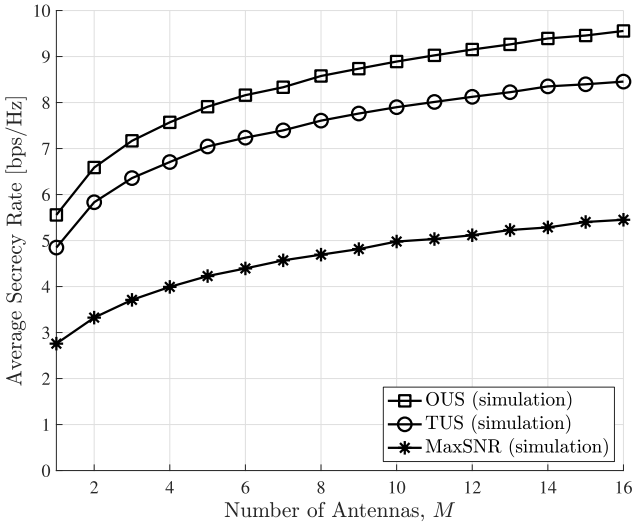

FIGURE 9. Average achievable secrecy rate for varying the number of antennas (M) at the receiver when $N = 30$, $\rho = 30$ dB, $K = 1$, $\sigma_h^2 = 1$, and $\sigma_g^2 = 1$.

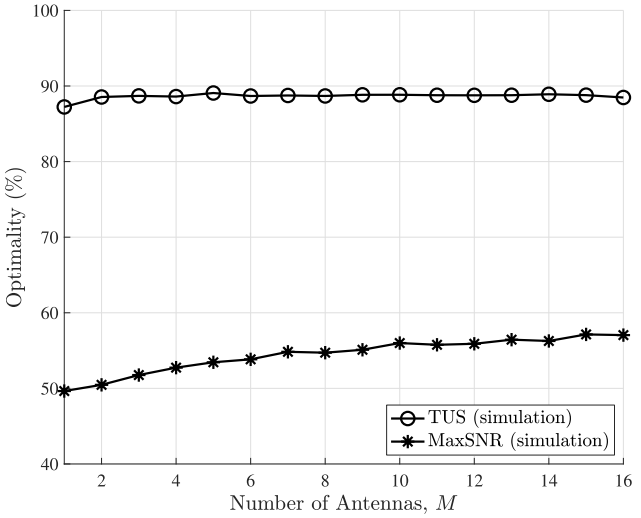

FIGURE 10. Optimality for varying the number of antennas (M) at the receiver when $N = 30$, $\rho = 30$ dB, $K = 1$, $\sigma_h^2 = 1$, and $\sigma_g^2 = 1$.

constant. To confirm this, we newly define the ratio of secrecy rate of TUS (or MaxSNR) and that of OUS as *optimality*.

Fig. 10 shows the optimality which we defined as the ratio of secrecy rate of TUS (or MaxSNR) and that of OUS when we have set $N = 30$, $\rho = 30\,\text{dB}$, $K = 1, \sigma_h^2 = 1, \sigma_g^2 = 1$, and varying M ($1 \sim 16$), which corresponds to Fig. 9. For all M, optimality of TUS shows approximately 89% but optimality of MaxSNR increases when the number of antennas at the receiver increases.

C. A CASE OF TOO MANY EAVESDROPPERS

From our analysis such as (6), (7), and (12), we can obtain the secrecy rate of an extreme case where there exist too many potential eavesdroppers (e.g., $K = N - 1$). In the case of too many eavesdroppers existing, multiuser diversity from user scheduling might not be enough to guarantee a certain level of the secrecy rate. In this situation, we might combine OUS and TUS with other techniques such as multiple antennas [30], artificial noise [31], and full duplexing [32] to additionally improve secrecy performance. As discussed in Section VI-B and shown in Fig. 9, using the simple MRC-based multiple antennas technique can effectively increase the secrecy rate.

D. SUMMARY

In this subsection, we summarize some featured information of our proposed scheduling schemes, especially related to CSI (e.g., feedback and estimation errors).

Table 1 shows the summary of CSI related information on OUS and TUS. For the required number of mini-slots for CSI feedback, as we discussed in Sections III and IV, the OUS requires $N + KN$ mini-slots whereas the TUS only requires $N + 1$ to $2N$ mini-slots. For CSI feedback time complexity, we consider processing time complexity in terms of the required number of mini-slots for CSI feedback when $K = N - 1$. It can be expressed in a big-O notation which describes the limiting behavior of a function when the argument tends towards a particular value or infinity [33]. The OUS shows a quadratic characteristic since $\mathcal{O}(N + KN) = \mathcal{O}(N^2)$ when $K = N - 1$, but TUS only shows a linear characteristic since the required number of mini-slots for CSI feedback does not depend on the number of potential eavesdroppers. Both OUS and TUS are centralized scheduling schemes but they can be implemented in the distributed manner, as we discussed in Section II. Interestingly, the TUS is robust to channel estimation errors on wiretap links whereas the OUS is not, as we discussed in Section VI-A.

VII. CONCLUSION

In this paper, we investigated two user scheduling algorithms (OUS and TUS schemes) in uplink wiretap networks when we consider the potential eavesdropping scenario. The OUS scheme achieves the optimal secrecy rate but it requires feedback from all legitimate users. The TUS scheme shows a suboptimal secrecy performance comparable to OUS scheme

while reducing the feedback overhead using the threshold value. We analyzed the approximated secrecy rate of two scheduling algorithms, including asymptotic behavior of the achievable secrecy rate when SNR tends to infinity. Further, we performed additional simulations to investigate the impact of channel estimation error in the wiretap links, and the effect of multiple antennas at the receiver employing MRC, on the average secrecy rate, respectively. Due to different scheduling principles in OUS and TUS schemes, the TUS scheme yields robustness against the channel estimation error in the wiretap links, compared with the OUS scheme. For both OUS and TUS schemes, the secrecy performance is improved when we consider multiple antennas at the receiver. Instead of the secrecy rate analysis, analyzing the secrecy outage probability of various user scheduling algorithms in uplink wiretap networks remains for future work. We leave the diversity order analysis of the secrecy outage probability with both OUS and TUS schemes as a further study.

APPENDIX A
PROOF FOR PROPOSITION 1

From (4), we have the PDF of $Z_{n^\star}$ given by

$$\begin{aligned} f_{Z^\star}(z) &= \frac{d}{dz}F_{Z^\star}(z) \\ &= N\left(1+\sum_{i=1}^{K}\binom{K}{i}\frac{(-1)^i\sigma_h^2 i}{\sigma_g^2 z+\sigma_h^2 i}e^{-\frac{z-1}{\sigma_h^2\rho}}\right)^{N-1} \\ &\quad\times\left\{\sum_{i=1}^{K}\binom{K}{i}(-1)^{i+1}\frac{\sigma_h^2\sigma_g^2\rho i+\sigma_g^2 iz+\sigma_h^2 i^2}{\rho\left(\sigma_g^2 z+\sigma_h^2 i\right)^2}e^{-\frac{z-1}{\sigma_h^2\rho}}\right\}. \end{aligned} \tag{18}$$

Using L'Hopital's Rule, in the case of $K=1$ and $\rho\to\infty$, we can get the PDF of $Z_{n^\star}$ as follows:

$$f_{Z^\star}(z)=\sum_{i=1}^{N}\binom{N}{i}(-1)^{i+1}\,i\left(\frac{\sigma_h^2}{\sigma_g^2}\right)^i\left(\frac{1}{\sigma_g^2 z+\sigma_h^2}\right)^{i+1}. \tag{19}$$

Therefore, by using (19), we can get the result in Proposition 1 as follows:

$$\begin{aligned} \bar{C}_{n^\star}^{\infty} &= \int_0^\infty \log(z) f_{Z_{n^\star}}(z)\,dz \qquad (20)\\ &= \int_0^\infty \log(z)\sum_{i=1}^{N}\binom{N}{i}(-1)^{i+1}\,i \\ &\quad\times\left(\frac{\sigma_h^2}{\sigma_g^2}\right)^i\left(\frac{\sigma_h^2}{\sigma_g^2 z+\sigma_h^2}\right)^{i+1}dz \\ &= \sum_{i=1}^{N}\binom{N}{i}(-1)^{i+1}\,i\left(\frac{\sigma_h^2}{\sigma_g^2}\right)^i \\ &\quad\times\int_0^\infty\frac{\log(z)}{\left(z+\sigma_h^2/\sigma_g^2\right)^{i+1}}dz \\ &= \sum_{i=1}^{N}\binom{N}{i}(-1)^i\left(\gamma+\psi(i)+\log\left(\frac{\sigma_g^2}{\sigma_h^2}\right)\right), \qquad (21) \end{aligned}$$

where the last equality holds from [29, (4.253.6)], and γ and $\psi(x)$ are Euler's constant and the digamma function, respectively, defined in (6).

APPENDIX B
PROOF FOR COROLLARY 1

For the scheduled user (n^*), Let us denote $Y^*=\max_{k\in\mathcal{K}}|g_{n^*k}|^2$. Thus, Y^* is the maximum of K i.i.d. truncated exponential random variables. From [27], the CDF of Y^* is given by

$$F_{Y^*}(y)=\left(\frac{1-\exp\left(-\frac{y}{\sigma_g^2}\right)}{1-\exp\left(-\frac{\eta_L}{\sigma_g^2}\right)}\right)^K, \tag{22}$$

where $y\in[0,\eta_L]$.

Using a differentiation of $F_{Y^*}(y)$ in (22) and the binomial theorem, the PDF of Y^* is given by

$$f_{Y^*}(y)=\frac{K}{\sigma_g^2 p_\eta}\sum_{i=0}^{K-1}\binom{K-1}{i}(-1)^i e^{-\frac{(i+1)y}{\sigma_g^2}}. \tag{23}$$

When $\rho\to\infty$, (8) is reduced to

$$\begin{aligned} \bar{C}_{n^*}^{\infty}(\eta_L) &\approx \lim_{\rho\to\infty}\mathbb{E}\left[\log\left(\frac{1+|h_{n^*}|^2\rho}{1+\max_{k\in\mathcal{K}}|g_{n^*k}|^2\rho}\right)\right] \\ &= \mathbb{E}\left[\log\left(\frac{|h_{n^*}|^2}{\max_{k\in\mathcal{K}}|g_{n^*k}|^2}\right)\right] \\ &= \underbrace{\mathbb{E}\left[\log\left(|h_{n^*}|^2\right)\right]}_{\text{desired link}}-\underbrace{\mathbb{E}\left[\log\left(\max_{k\in\mathcal{K}}|g_{n^*k}|^2\right)\right]}_{\text{wiretap link}}, \end{aligned} \tag{24}$$

where the approximation holds from the fact that $Prob\left\{|h_{n^*}|^2\ge\max_{k\in\mathcal{K}}|g_{n^*k}|^2\right\}\approx 1$ for sufficiently large N.

For the desired link in (24), $\mathbb{E}\left[\log\left(|h_{n^*}|^2\right)\right]$ is derived as

$$\begin{aligned} &\mathbb{E}\left[\log\left(|h_{n^*}|^2\right)\right] \\ &= \sum_{n=1}^{N}\binom{N}{n}p_\eta^n\left(1-p_\eta\right)^{N-n}\mathbb{E}\left[\log\left(|h_{n^*}|^2\right)|N_c=n\right] \\ &= \sum_{n=1}^{N}\binom{N}{n}p_\eta^n\left(1-p_\eta\right)^{N-n} \\ &\quad\times\sum_{i=1}^{n}\binom{n}{i}(-1)^{i+1}\frac{i}{\sigma_h^2}\int_0^\infty\log(x)\,e^{-\frac{ix}{\sigma_h^2}}dx \\ &= \sum_{n=1}^{N}\binom{N}{n}p_\eta^n\left(1-p_\eta\right)^{N-n} \\ &\quad\times\sum_{i=1}^{n}\binom{n}{i}(-1)^i\left(\gamma+\log\left(\frac{i}{\sigma_h^2}\right)\right), \end{aligned} \tag{25}$$

where the last equality holds from [29, (4.331.1)] and γ denotes Euler's constant.

For the wiretap link in (24), $\mathbb{E}\left[\log\left(\max_{k\in\mathcal{K}}|g_{n^*k}|^2\right)\right]$ is obtained as

$$\mathbb{E}\left[\log\left(\max_{k\in\mathcal{K}}|g_{n^*k}|^2\right)\right] = \int_0^{\eta_{\mathrm{L}}} \log(y) f_{Y^*}(y)\, dy \tag{26}$$

$$= \frac{K}{\sigma_g^2 p_\eta}\sum_{i=0}^{K-1}\binom{K-1}{i}(-1)^i \int_0^{\eta_{\mathrm{L}}} \log(y)\, e^{-\frac{(i+1)y}{\sigma_g^2}}\, dy \tag{27}$$

$$= \sum_{i=1}^{K}\binom{K}{i}\frac{(-1)^i}{p_\eta}\left(\gamma + \log\left(\frac{i}{\sigma_g^2}\right) + \mathrm{E}_1\left(\frac{i\eta_{\mathrm{L}}}{\sigma_g^2}\right) + e^{-\frac{i\eta_{\mathrm{L}}}{\sigma_g^2}}\log\eta_{\mathrm{L}}\right), \tag{28}$$

where the last equality holds from from [29, (4.331.1)] and the definition of the exponential integral function.

Finally, by substituting (25) and (28) into (24), the result in Corollary 1 is obtained.

APPENDIX C
DERIVATION OF $\bar{C}^{\infty}_{MaxSNR}$

For the MaxSNR scheme, the scheduled user index is determined as

$$\hat{n} = \arg\max_{n\in\mathcal{N}}\left\{|h_n|^2\right\}. \tag{29}$$

Thus, for $\rho\to\infty$, the ergodic secrecy rate of the *MaxSNR* scheme is given by

$$\bar{C}^{\infty}_{\mathrm{MaxSNR}} \approx \lim_{\rho\to\infty}\mathbb{E}\left[\log\left(\frac{1+|h_{\hat{n}}|^2\rho}{1+\max_{k\in\mathcal{K}}|g_{\hat{n}k}|^2\rho}\right)\right]$$

$$= \mathbb{E}\left[\log\left(\frac{|h_{\hat{n}}|^2}{\max_{k\in\mathcal{K}}|g_{\hat{n}k}|^2}\right)\right]$$

$$= \underbrace{\mathbb{E}\left[\log\left(|h_{\hat{n}}|^2\right)\right]}_{\text{desired link}} - \underbrace{\mathbb{E}\left[\log\left(\max_{k\in\mathcal{K}}|g_{\hat{n}k}|^2\right)\right]}_{\text{wiretap link}}, \tag{30}$$

where the approximation holds from the fact that $Prob\left\{|h_{\hat{n}}|^2 \geq \max_{k\in\mathcal{K}}|g_{\hat{n}k}|^2\right\} \approx 1$ for sufficiently large N.

For the desired link in (30), $\mathbb{E}\left[\log\left(|h_{\hat{n}}|^2\right)\right]$ is obtained as

$$\mathbb{E}\left[\log\left(|h_{\hat{n}}|^2\right)\right] = \sum_{i=1}^{N}\binom{N}{i}\frac{i}{\sigma_h^2}(-1)^{i+1} \times \int_0^{\infty}\log(x)\exp\left(-\frac{ix}{\sigma_h^2}\right)dx$$

$$= \sum_{i=1}^{N}\binom{N}{i}(-1)^i\left(\gamma + \log\left(\frac{i}{\sigma_h^2}\right)\right), \tag{31}$$

where the last equality holds from [29, (4.331.1)] and γ denotes Euler's constant.

Similar to $\mathbb{E}\left[\log\left(|h_{\hat{n}}|^2\right)\right]$, $\mathbb{E}\left[\log\left(\max_{k\in\mathcal{K}}|g_{\hat{n}k}|^2\right)\right]$ is given by

$$\mathbb{E}\left[\log\left(\max_{k\in\mathcal{K}}|g_{\hat{n}k}|^2\right)\right] = \sum_{i=1}^{K}\binom{K}{i}(-1)^i\left(\gamma + \log\left(\frac{i}{\sigma_g^2}\right)\right). \tag{32}$$

Finally, by plugging (31) and (32) into (30), $\bar{C}^{\infty}_{\mathrm{MaxSNR}}$ in (16) is obtained.

REFERENCES

[1] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.
[2] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[3] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
[4] S. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.
[5] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.
[6] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE ISIT*, Jul. 2006, pp. 356–360.
[7] 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.
[8] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.
[9] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE ISIT*, Sep. 2005, pp. 2152–2155.
[10] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4033–4039, Sep. 2009.
[11] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.
[12] S. Q. Nguyen, H. T. Nguyen, D. D. Van, and W.-J. Hwang, "Exact outage analysis of cognitive energy harvesting relaying networks under physical layer security," *EAI Endorsed Trans. Ind. Netw. Intell. Syst.*, vol. 6, no. 18, pp. 1–15, Mar. 2019.
[13] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, and T. Q. Duong, "Relay selection for security enhancement in cognitive relay networks," *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 46–49, Feb. 2015.
[14] D. T. Hung, T. T. Duy, and D. Q. Trinh, "Security-reliability analysis of multi-hop LEACH protocol with fountain codes and cooperative jamming," *EAI Endorsed Trans. Ind. Netw. Intell. Syst.*, vol. 6, no. 18, pp. 1–7, Mar. 2019.
[15] M. Pei, A. L. Swindlehurst, D. Ma, and J. Wei, "On ergodic secrecy rate for MISO wiretap broadcast channels with opportunistic scheduling," *IEEE Commun. Lett.*, vol. 18, no. 1, pp. 50–53, Jan. 2014.
[16] X. Ge, P. Wu, H. Jin, and V. C. M. Leung, "Secrecy analysis of multiuser downlink wiretap networks with opportunistic scheduling," in *Proc. IEEE ICC*, Jun. 2015, pp. 7370–7375.
[17] M. Yang, D. Guo, Y. Huang, T. Q. Duong, and B. Zhang, "Physical layer security with threshold-based multiuser scheduling in multi-antenna wireless networks," *IEEE Trans. Commun.*, vol. 64, no. 12, pp. 5189–5202, Dec. 2016.
[18] H. Jin, W.-Y. Shin, and B. C. Jung, "On the multi-user diversity with secrecy in uplink wiretap networks," *IEEE Commun. Lett.*, vol. 17, no. 9, pp. 1778–1781, Sep. 2013.
[19] H. Jin, B. C. Jung, and W.-Y. Shin, "On the secrecy capacity of multi-cell uplink networks with opportunistic scheduling," in *Proc. IEEE ICC*, May 2016, pp. 1–5.
[20] I. Bang, S. M. Kim, and D. K. Sung, "Effects of multiple antennas and imperfect channel knowledge on secrecy multiuser diversity," *IEEE Commun. Lett.*, vol. 19, no. 9, pp. 1564–1567, Sep. 2015.

[21] I. Bang, S. M. Kim, and D. K. Sung, "Artificial noise-aided user scheduling for optimal secrecy multiuser diversity," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 528–531, Mar. 2017.
[22] X. Ge, H. Jin, J. Zhu, J. Cheng, and V. C. M. Leung, "Exploiting opportunistic scheduling in uplink wiretap networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 4886–4897, Jun. 2017.
[23] X. Chen, D. W. K. Ng, and H.-H. Chen, "Secrecy wireless information and power transfer: Challenges and opportunities," *IEEE Wireless Commun.*, vol. 23, no. 2, pp. 54–61, Apr. 2016.
[24] M. A. Abbas, H. Song, and J.-P. Hong, "Opportunistic scheduling for average secrecy rate enhancement in fading downlink channel with potential eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 4, pp. 969–980, Apr. 2019.
[25] I. Bang, S. M. Kim, and D. K. Sung, "Artificial noise-aided user scheduling from the perspective of secrecy outage probability," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 7816–7820, Aug. 2018.
[26] S. H. Chae, B. C. Jung, and W. Choi, "On the achievable degrees-of-freedom by distributed scheduling in (N,K)-user interference channels," *IEEE Trans. Commun.*, vol. 61, no. 6, pp. 2568–2579, Jun. 2013.
[27] A. Papoulis and S. U. Pillai, *Probability—Random Variables and Stochastic Processes*. New York, NY, USA: McGraw-Hill, 2002.
[28] P. J. Davis and P. Rabinowitz, *Methods of Numerical Integration*. North Chelmsford, MA, USA: Courier Corp., 2007.
[29] I. Gradshteyn and I. Ryzhik, *Table of Integrals, Series, and Products*. London, U.K.: Academic, 2003.
[30] X. Chen, D. W. K. Ng, W. Gerstacker, and H. H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1027–1053, 2nd Quart., 2016.
[31] W. Wang, K. C. Teh, and K. Li, "Artificial noise aided physical layer security in multi-antenna small-cell networks," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1470–1482, Jun. 2017.
[32] F. Zhu, F. Gao, M. Yao, and H. Zou, "Joint information- and jamming-beamforming for physical layer security with full duplex base station," *IEEE Trans. Signal Process.*, vol. 62, no. 24, pp. 6391–6401, Dec. 2014.
[33] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to Algorithms*. Cambridge, MA, USA: MIT Press, 2009.

INKYU BANG (S'11–M'17) received the B.S. degree in electrical and electronic engineering from Yonsei University, Seoul, South Korea, in 2010, and the M.S. and Ph.D. degrees in electrical engineering from the Korea Advanced Institute for Science and Technology (KAIST), Daejeon, South Korea, in 2012 and 2017, respectively.

He was a Research Fellow with the Department of Computer Science from the National University of Singapore (NUS), from 2017 to 2019. In 2019, he was a Senior Researcher with the Agency for Defense Development (ADD). He has been an Assistant Professor with the Department of Information and Communication Engineering, Hanbat National University, since 2019. His current research interests include information-theoretic security (physical-layer security), wireless system security, the Internet of Things, simultaneous wireless information and power transfer (SWIPT), and machine learning application in wireless communications.

BANG CHUL JUNG (S'02–M'08–SM'14) received the B.S. degree in electronics engineering from Ajou University, Suwon, South Korea, in 2002, and the M.S. and Ph.D. degrees in electrical and computer engineering from the Korea Advanced Institute for Science and Technology (KAIST), Daejeon, South Korea, in 2004 and 2008, respectively.

He was a Senior Researcher/Research Professor with the KAIST Institute for Information Technology Convergence, Daejeon, from 2009 to 2010. From 2010 to 2015, he was a Faculty Member with Gyeongsang National University, Tongyeong, South Korea. He is currently a Professor with the Department of Electronics Engineering, Chungnam National University, Daejeon. His current research interests include wireless communications, statistical signal processing, information theory, interference management, radar signal processing, spectrum sharing, multiple antennas, multiple access techniques, radio resource management, machine learning, and deep learning.

Dr. Jung was a recipient of the 5th IEEE Communication Society Asia–Pacific Outstanding Young Researcher Award, in 2011, the KICS Haedong Young Scholar Award, in 2015, and the 29th KOFST Science and Technology Best Paper Award, in 2019. He has been an Associate Editor of the *IEICE Transactions on Fundamentals of Electronics, Communications, and Computer Sciences*, since 2018.