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

INKYU BANG¹, (Member, IEEE), and BANG CHUL JUNG², (Senior Member, IEEE),
¹Department of Information & Communication Engineering, Hanbat National University, Daejeon 34158, South Korea (e-mail: ikbang@hanbat.ac.kr)
²Department of Electronics Engineering, Chungnam National University, Daejeon 34134, South Korea (e-mail: bcjung@cnu.ac.kr)
Corresponding author: Bang Chul Jung (e-mail: bcjung@cnu.ac.kr).

This research was partially supported by the research fund of Hanbat National University in 2019 and was partially supported by the NRF through the Basic Science Research Program funded in part by 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].

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 [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 overlay 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 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 $n \in \mathcal{N} \triangleq \{1, \ldots, N\}$ and is assumed to be a complex Gaussian random variables with zero mean and variance $\sigma^2_{h_n}$, i.e., $h_n \sim \mathcal{C}N(0, \sigma^2_{h_n})$. 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 $\sigma^2_{g_{nk}}$, i.e., $g_{nk} \sim \mathcal{C}N(0, \sigma^2_{g_{nk}})$. For analytical tractability, we assume that $h_n$ and $g_{nk}$ are independent and identically distributed (i.i.d.), i.e., $\sigma^2_{h_n} = \sigma^2_h$ and $\sigma^2_{g_{nk}} = \sigma^2_{g_{nk}} \forall n, k$.

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-slot 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.

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 $\mathbb{E}[|x_n|^2] \leq P$, and $z$ and $z_k$ denote the circularly symmetric complex additive white Gaussian noises (AWGNs) with zero mean and variance $\sigma^2$. We define the transmit SNR as $\rho \triangleq \frac{P}{\sigma^2}$.

The achievable secrecy rate of user $n$ is obtained as

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

(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

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

(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.
the scheduled user $n^*$, the ergodic secrecy rate of the OUS scheme is obtained as
\[
C_{n^*} = E \left[ \log \left( \frac{1 + |h_{n^*}|^2 \rho}{1 + \max_{k \in K} |g_{nk}|^2 \rho} \right) | C_{n^*} \geq 0 \right] \Pr \{ C_{n^*} \geq 0 \}
\approx E \left[ \log \left( \frac{1 + |h_{n^*}|^2 \rho}{1 + \max_{k \in K} |g_{nk}|^2 \rho} \right) \right] = \int_0^\infty \log(z) \, dF_{Z_{n^*}}(z),
\] (3)

where the approximation holds from the fact that $\Pr \{ C_{n^*} \geq 0 \} \approx 1$ for sufficiently large $N$. $F_{Z_{n^*}}(z)$ is the cumulative density function (CDF) of a random variable $Z_{n^*}$ which is defined as
\[
Z_{n^*} = \frac{1 + |h_{n^*}|^2 \rho}{1 + \max_{k \in K} |g_{nk}|^2 \rho} = \max_{n \in N} \left\{ \frac{|h_{n}|^2 + 1/\rho}{\max_{k \in K} |g_{nk}|^2 + 1/\rho} \right\}.
\]

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

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]
\[
F_Z(z) = \int_0^{\infty} \int_0^{\infty} f_X(x) f_Y(y) \left( x - \frac{1}{\rho} \right) dx dy = 1 + \sum_{i=1}^{K} \binom{K}{i} (-1)^i \frac{\sigma_{h_i}^2}{\sigma_{z}^2 + \sigma_{h_i}^2} e^{-\frac{z-1}{\sigma_{h_i}^2}},
\]
where $f_X(x)$ and $f_Y(y)$ are probability density functions (PDFs) of $X$ and $Y$, respectively.

Since $Z_{n^*}$ is a maximum of $N$ i.i.d. random variable $Z$, the CDF of $Z_{n^*}$ is obtained as follows:
\[
F_{Z_{n^*}}(z) = \left( 1 + \sum_{i=1}^{K} \binom{K}{i} (-1)^i \frac{\sigma_{h_i}^2}{\sigma_{z}^2 + \sigma_{h_i}^2} e^{-\frac{z-1}{\sigma_{h_i}^2}} \right)^N.
\] (4)

Using (3) and (4), the ergodic secrecy rate of the OUS scheme can be calculated as follows:
\[
C_{n^*} = N \int_0^\infty \log(z) \left( 1 + \sum_{i=1}^{K} \binom{K}{i} (-1)^i \frac{\sigma_{h_i}^2}{\sigma_{z}^2 + \sigma_{h_i}^2} e^{-\frac{z-1}{\sigma_{h_i}^2}} \right)^{N-1} \left[ \sum_{i=1}^{K} \binom{K}{i} (-1)^{i+1} \frac{\sigma_{h_i}^2 \sigma_{h_i}^2 \rho + \sigma_{z}^2 \rho + \sigma_{h_i}^2 \rho}{\rho (\sigma_{z}^2 + \sigma_{h_i}^2)^2} e^{-\frac{z-1}{\sigma_{h_i}^2}} \right] dz.
\] (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:
\[
C_{n^*} = \sum_{i=1}^{N} \binom{N}{i} (-1)^i \left( \gamma + \psi(i) + \log \left( \frac{\sigma_{h_i}^2}{\sigma_{h_i}^2} \right) \right),
\]
where $\gamma \approx 0.577216$ is Euler’s constant, and $\psi(x)$ is the digamma function defined as $\psi(x) = \frac{d}{dx} \log \Gamma(x)$ where $\Gamma(x)$ is the gamma function defined as $\Gamma(x) = \int_0^\infty e^{-t} t^{x-1} dt$.

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., $\max_{k \in K} |g_{nk}|^2$.
- **Step 2**: Only users who satisfy the following threshold criterion $(C1)$ transmit a feedback message, i.e., $|h_n|^2$, to the receiver.

\[
(C1) \max_{k \in K} |g_{nk}|^2 \leq \eta_h,
\]
where $\eta_h$ 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. EROGIC SECREEY 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 $\eta_h$, the ergodic secrecy rate of the TUS scheme is given by (7) shown at the top of next page, where $p_n$ is a probability that a certain user satisfies the threshold criterion $(C1)$, given by $p_n \equiv \left( 1 - \exp \left( -\frac{\eta_h}{\sigma_{h_i}^2} \right) \right)^K$ and $E_1(x) \equiv \int_x^\infty \frac{e^{-t}}{t} dt$. 
\[
\tilde{C}_{n^*}(\eta_n) = \sum_{n=1}^{N} \binom{N}{n} p_0^n (1 - p_0)^{N-n} \sum_{i=1}^{n} \binom{n}{i} (-1)^{i+1} e^{-\eta_n \sigma_g^2} E_1 \left( \frac{i}{\sigma_g^2 \rho} \right) - \frac{1}{p_\eta} \sum_{i=1}^{K} \binom{K}{i} (-1)^{i+1} e^{-\eta_n \sigma_g^2} E_1 \left( \frac{i}{\sigma_g^2 \rho} \right) E \left( \frac{i}{\sigma_g^2 \rho} + \frac{i \eta_n}{\sigma_g^2} \right) - e^{-\eta_n \sigma_g^2} \log(1 + \eta_n \rho),
\]

(7)

Proof: Similar to the OUS scheme, for the scheduled user \(n^*\) and a given threshold value \(\eta_n\), the ergodic secrecy rate of the TUS scheme is derived as

\[
\tilde{C}_{n^*}(\eta_n) \approx E \left[ \log(1 + |h_{n^*}|^2 \rho) - \log \left(1 + \max_{k \in K} |g_{n^*,k}|^2 \rho\right) \right] = \tilde{C}_d(\eta_n) - \tilde{C}_w(\eta_n),
\]

where the approximation holds with the same assumption in (3). Here, we define \(\tilde{C}_d(\eta_n) \triangleq E \left[ \log(1 + |h_{n^*}|^2 \rho) \right]\) and \(\tilde{C}_w(\eta_n) \triangleq E \left[ \log \left(1 + \max_{k \in K} |g_{n^*,k}|^2 \rho\right) \right]\), respectively, for notation simplicity during the proof.

Next, we need to obtain \(\tilde{C}_d(\eta_n)\) and \(\tilde{C}_w(\eta_n)\) in (8) for a given threshold value \(\eta_n\). In the TUS scheme, the number of users who transmit their feedback message varies depending on a value of \(\eta_n\). 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 \(\tilde{C}_d(\eta_n; N_c)\) given by

\[
\tilde{C}_d(\eta_n; N_c) = E \left[ \log(1 + |h_{n^*}|^2 \rho) \mid N_c \right] = \int_0^\infty \log(1 + \rho x) dF_{|h_{n^*}|^2}(x) = \sum_{i=1}^{N_c} \binom{N_c}{i} (-1)^{i+1} e^{\eta_n \sigma_g^2} E_1 \left( \frac{i}{\sigma_g^2 \rho} \right),
\]

(9)

where the last equality holds from [29, (4.373.2)] and \(E_1(\cdot)\) is the exponential integral function [29].

Accordingly, \(\tilde{C}_d(\eta_n)\) in (8) is obtained through the expected value of all possible conditional expectation in (9) when \(N_c = n\) for \(n \in \{1, \cdots, N\}\) and it is given by

\[
\tilde{C}_d(\eta_n) = E \left[ \log(1 + |h_{n^*}|^2 \rho) \right] = \sum_{n=1}^{N} \binom{N}{n} p_0^n (1 - p_0)^{N-n} E \left[ \log(1 + |h_{n^*}|^2 \rho) \right] = \sum_{n=1}^{N} \binom{N}{n} p_0^n (1 - p_0)^{N-n} \tilde{C}_d(\eta_n; n),
\]

(10)

where \(p_0\) is a probability that a certain user satisfies the threshold criterion (C1), given by \(p_0 \triangleq \left(1 - \exp \left( -\frac{\eta_n}{\sigma_g^2} \right) \right)^K\).

To obtain \(\tilde{C}_w(\eta_n)\) in (8), we first need to derive the CDF of \(Y^* = \max_{k \in K} |g_{n^*,k}|^2\). 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, \(\tilde{C}_w(\eta_n)\) is given by (11) shown at the top of next page. Finally, substituting (10) and (11) into (8) yields the ergodic secrecy rate of the TUS scheme (i.e., \(\tilde{C}_d(\eta_n) - \tilde{C}_w(\eta_n)\)) and it is given by (7).

Note that we derive the ergodic secrecy rate of the TUS scheme for general parameters such as \(N, K, \rho, \sigma_h^2, \sigma_g^2\), and \(\eta_n\).

**Corollary 1** (Secrecy performance of TUS in high SNR). For \(\rho \to \infty\), the ergodic secrecy rate of the TUS scheme \(\tilde{C}_{n^*}(\eta_n)\) is reduced to (12) shown at the top of next page, where \(\gamma \approx 0.577216\) is Euler’s constant.

Proof: See Appendix B.

**B. DETERMINATION OF THRESHOLD VALUE**

For given system parameters \((N, K, \rho, \sigma_h^2, \sigma_g^2)\), the ergodic secrecy rate of the TUS scheme is a function of \(\eta_n\). 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 \(\eta_n\). Thus, the threshold value set by the optimal-determination method is given by

\[
\eta_n^{opt} = \arg \max_{\eta_n} \tilde{C}_{n^*}(\eta_n).
\]

(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 \(\eta_n\).

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:

\[
p_0 = 1 - \left(1 - \left(1 - \exp \left( -\frac{\eta_n}{\sigma_g^2} \right) \right)^K \right)^N.
\]

(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.,
Similarly, a circle marker in each line indicates comparison in high SNR regime. 

\[ C_w(\eta_N) = \frac{1}{p_N} \sum_{i=1}^{K} \binom{K}{i} (-1)^{i+1} \left( e^{-\frac{\rho}{\sigma^2}} E_1 \left( \frac{i}{\sigma^2} \rho \right) - E_1 \left( \frac{i}{\sigma^2} \rho + \frac{i \eta_N}{\sigma^2} \right) - e^{-\frac{\eta_N}{\sigma^2}} \log \left( 1 + \eta_N \rho \right) \right), \]  

(11)

\[ C_{w}^\infty(\eta_N) = \sum_{n=1}^{N} \binom{N}{n} p_n (1 - p_n)^{N-n} \sum_{i=1}^{n} \binom{n}{i} (-1)^{i} \left( \gamma + \log \left( \frac{i}{\sigma^2} \right) \right) - \sum_{i=1}^{K} \binom{K}{i} (-1)^{i} \left( \gamma + \log \left( \frac{i}{\sigma^2} \right) \right), \]  

(12)

\[ \eta_{NL}^{\text{pre}} = -\sigma^2 \eta \log \left( 1 - \left( 1 - \epsilon_0 \right)^{\frac{1}{T}} \right). \]  

(15)

Note that \( \epsilon_0 \) is the control parameter which we can determine. We empirically choose \( \epsilon_0 \) between \( 10^{-5} \) and \( 10^{-3} \). The predictable-determination method does not provide an optimal threshold value for \( C_{w}^\infty(\eta_N) \). 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., \( |h_{iG}|^2 \)). In addition, for \( \rho \to \infty \), the ergodic secrecy rate of the MaxSNR scheme can be calculated as

\[ C_{\text{MaxSNR}}^\infty \sum_{i=1}^{N} \binom{N}{i} (-1)^{i} \left( \gamma + \log \left( \frac{i}{\sigma^2} \right) \right), \]  

(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.

**A. NUMERICAL RESULTS**

Fig. 3 shows the average achievable secrecy rate for varying threshold values \( \eta_N \). For comparison, we consider four different \((N, K)\) pairs. For each line, a star-shaped marker indicates \( \eta_N^{\text{opt}} \), and its corresponding average secrecy rate. Similarly, a circle marker in each line indicates \( \eta_N^{\text{pre}} \) and its corresponding average secrecy rate. As \( N \) increases for fixed \( K \), values of both \( \eta_N^{\text{opt}} \) and \( \eta_N^{\text{pre}} \) 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 \( \eta_N^{\text{pre}} \) and that of \( \eta_N^{\text{opt}} \) is negligible. Thus, using \( \eta_N^{\text{pre}} \) instead of \( \eta_N^{\text{opt}} \) is one of reasonable alternatives.

Fig. 4 shows the average achievable secrecy rate for varying SNRs. System parameters are set to \( N = 30, K = 1, \sigma^2_g = 1, \text{ and } \sigma^2_h = 1 \). For determining \( \eta_N^{\text{pre}}, \epsilon_0 = 10^{-3} \) is used. As the SNR \( (\rho) \) 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 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 \( K = 3, \rho = 10 \text{ dB}, \sigma^2_g = 1, \text{ and } \sigma^2_h = 1 \). We use \( \epsilon_0 = 10^{-4} \) to determine \( \eta_N^{\text{pre}} \). 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 $\eta_{\text{pre}}$ and that with $\eta_{\text{opt}}$ are almost similar. However, the secrecy performance gap between the TUS scheme with $\eta_{\text{pre}}$ and that with $\eta_{\text{opt}}$ increases when $K$ increases due to the fact that $e_0 = 10^{-4}$ 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 $\lambda \triangleq \frac{\sigma_h^2}{\sigma_g^2}$. 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 $\lambda$ equivalently implies the relative distance ratio since values of $\sigma_h^2$ and $\sigma_g^2$ are inversely proportional to distances of main and wiretap links, respectively. As $\lambda$ increases, the secrecy rates of all schemes decrease and finally converge to zero since a large value of $\lambda$ 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 $\lambda$ decreases.

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

\[
g_{nk} = g_{nk} + g_{e}, \tag{17}
\]

where \( g_{nk} \sim CN(0, \sigma_n^2) \) and \( g_{e} \sim CN(0, \sigma_e^2) \) 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 \( \sigma_n^2 \) 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 \( \sigma_g^2 = 1 \).

Interestingly, as 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 constant. To confirm this, we newly define optimality of TUS shows approximately equal to that of OUS.

Fig. 10 shows the optimality which we defined as the ratio of secrecy rate of TUS (or MaxSNR) and that of OUS as

\[
\eta_L \rightarrow \infty, \quad \eta_L \rightarrow \infty.
\]

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

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

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 \( N = 30, \rho = 30 \) dB, \( K = 1, \sigma_h^2 = 1, \) and \( \sigma_g^2 = 1 \), and varying \( M \) (1 ~ 16), which corresponds to Fig. 9. For all \( M \), optimality of TUS shows approximately equal to that of OUS.

\(^3\)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.
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 \( O(N + KN) = O(N^2) \) 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. CONCLUSIONS

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

<table>
<thead>
<tr>
<th></th>
<th>The required number of mini-slots for CSI feedback</th>
<th>CSI feedback time complexity</th>
<th>Scheduling policy</th>
<th>Robustness of channel estimation errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>OUS</td>
<td>$N + KN$</td>
<td>$\mathcal{O}(N^2)$</td>
<td>centralized</td>
<td>$\times$</td>
</tr>
<tr>
<td>TUS</td>
<td>$N + 1 \sim 2N$</td>
<td>$\mathcal{O}(N)$</td>
<td>centralized</td>
<td>$\checkmark$</td>
</tr>
</tbody>
</table>

APPENDIX A PROOF FOR PROPOSITION 1

From (4), we have the PDF of $Z_n$ given by

$$f_{Z_n}(z) = \frac{d}{dz} F_{Z_n}(z) = N \left( 1 + \sum_{i=1}^{K} \binom{K}{i} (-1)^i \frac{\sigma^2_y}{\sigma^2_y + \sigma^2_h} e^{-\frac{z_i}{\sigma^2_y}} \right)^{N-1} \times \left\{ \sum_{i=1}^{K} \binom{K}{i} (-1)^{i+1} \frac{\sigma^2_y}{\sigma^2_y + \sigma^2_h} \right\}.$$

Using L'Hopital's Rule, in the case of $K = 1$ and $\rho \to \infty$, we can get the PDF of $Z_n$ as follows:

$$f_{Z_n}(z) = \sum_{i=1}^{N} \binom{N}{i} (-1)^i \left( \frac{\sigma^2_y}{\sigma^2_y + \sigma^2_h} \right)^i \left( \frac{1}{\sigma^2_y + \sigma^2_h} \right)^{i+1}.$$

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

$$C^\infty_{n^*} = \int_0^\infty \log(z) f_{Z_n^*}(z) \, dz$$
$$= \int_0^\infty \log(z) \sum_{i=1}^{N} \binom{N}{i} (-1)^i \left( \frac{\sigma^2_y}{\sigma^2_y + \sigma^2_h} \right)^i \left( \frac{1}{\sigma^2_y + \sigma^2_h} \right)^{i+1} \, dz$$
$$= \sum_{i=1}^{N} \binom{N}{i} (-1)^i \left( \frac{\sigma^2_y}{\sigma^2_y + \sigma^2_h} \right)^i \log(z) \left( \gamma + \psi(i) + \log \left( \frac{\sigma^2_y}{\sigma^2_h} \right) \right),$$

where the last equality holds from [29, (4.253.6)], and $\gamma$ 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 $Y^* = \max_{k \in K} |g_{n^*k}|^2$. Thus, $Y^*$ is the maximum of $K$ i.i.d. truncated exponential random variables. From [27], the CDF of $Y^*$ is given by

$$F_{Y^*}(y) = \left( \frac{1 - \exp \left( \frac{-y}{\sigma^2_g} \right)}{1 - \exp \left( \frac{-y}{\rho \sigma^2_g} \right)} \right)^K,$$

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

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

$$f_{Y^*}(y) = \frac{K}{\sigma^2_g \rho} \sum_{i=0}^{K-1} \binom{K-1}{i} (-1)^i e^{-\frac{(i+1)\eta_n}{\sigma^2_g}}.$$

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

$$C^\infty_{n^*} \approx \lim_{\rho \to \infty} \mathbb{E} \left[ \log \left( \frac{1 + |h_{n^*}|^2 \rho}{1 + \max_{k \in K} |g_{n^*k}|^2 \rho} \right) \right]$$
$$= \mathbb{E} \left[ \log \left( \frac{|h_{n^*}|^2}{\max_{k \in K} |g_{n^*k}|^2} \right) \right]$$
$$= \mathbb{E} \left[ \log \left( \max_{k \in K} |g_{n^*k}|^2 \right) \right],$$

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

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

$$\mathbb{E} \left[ \log \left( |h_{n^*}|^2 \right) \right]$$
$$= \sum_{n=1}^{N} \binom{N}{n} p_n^n (1 - p_n)^{N-n} \mathbb{E} \left[ \log \left( |h_{n^*}|^2 \right) | N_c = n \right]$$
$$= \sum_{n=1}^{N} \binom{N}{n} p_n^n (1 - p_n)^{N-n} \times \sum_{i=1}^{n} \binom{n}{i} (-1)^{i+1} \left( \frac{\sigma^2_y}{\sigma^2_h} \right)^i \int_0^\infty \log(x) e^{-\frac{ix}{\sigma^2_h}} \, dx$$
$$= \sum_{n=1}^{N} \binom{N}{n} p_n^n (1 - p_n)^{N-n} \times \sum_{i=1}^{n} \binom{n}{i} (-1)^i \left( \gamma + \log \left( \frac{i}{\sigma^2_h} \right) \right),$$

where the last equality holds from [29, (4.331.1)] and $\gamma$ denotes Euler’s constant.
For the wiretap link in (24), \( E \left[ \log \left( \max_{k \in K} |g_{nk}|^2 \right) \right] \) is obtained as

\[
E \left[ \log \left( \max_{k \in K} |g_{nk}|^2 \right) \right] = \int_0^{\infty} \log(y) f_{Y^*}(y) \, dy
\]

(26)

\[
= \frac{K}{\sigma_g^2 p_\eta} \sum_{i=0}^{K-1} \binom{K-1}{i} (-1)^i \int_0^{\infty} \log(y) e^{-\frac{(i+1)\eta}{\sigma_g^2}} \, dy
\]

(27)

\[
= \sum_{i=1}^{K} \binom{K}{i} (-1)^i \left( \gamma + \log \left( \frac{i}{\sigma_g^2} \right) \right) + E_1 \left( \frac{im_1}{\sigma_g^2} \right) + e^{-\frac{m_1}{\sigma_g^2}} \log \eta_1,
\]

(28)

where the last equality holds 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 \( \tilde{C}_{\text{MaxSNR}}^\infty \)**

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

\[
\hat{n} = \arg \max_{n \in N} \{ |h_n|^2 \}.
\]

(29)

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

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

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

(30)

where the approximation holds from the fact that

\[
\Pr \left\{ |h_{\hat{n}}|^2 \geq \max_{k \in K} |g_{nk}|^2 \right\} \approx 1 \text{ for sufficiently large } N.
\]

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

\[
E \left[ \log \left( |h_{\hat{n}}|^2 \right) \right] = \sum_{i=0}^{N} \binom{N}{i} \frac{i}{\sigma_h^2} (-1)^{i+1}
\]

\[
\times \int_0^{\infty} \log \left( x \right) \exp \left( -\frac{ix}{\sigma_h} \right) \, dx
\]

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

(31)

where the last equality holds from [29, (4.331.1)] and \( \gamma \) denotes Euler’s constant.

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

\[
E \left[ \log \left( \max_{k \in K} |g_{nk}|^2 \right) \right] = \sum_{i=1}^{K} \binom{K}{i} (-1)^i \left( \gamma + \log \left( \frac{i}{\sigma_g^2} \right) \right).
\]

(32)

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

**REFERENCES**


---

INKYU BANG (S’11-M’17) received the B.S degree in Electrical and Electronic Engineering from Yonsei University, Seoul, Korea, in 2010, and the M.S. and Ph.D. degrees in Electrical Engineering from Korea Advanced Institute for Science and Technology (KAIST), Daejeon, Korea, in 2012 and 2017, respectively.

He was a Research Fellow in the department of computer science from National University of Singapore (NUS) from 2017 to 2019. Between March 2019 and July 2019, he was a Senior Research with the Agency for Defense Development (ADD). He has been an Assistant Professor with the Department of Information & Communication Engineering, Hanbat National University, since August 2019. His research interests include information-theoretic security (physical-layer security), wireless system security, 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 BS degree in electronics engineering from Ajou University, Suwon, Korea, in 2002, and the MS and PhD degrees in electrical & computer engineering from KAIST, Daejeon, Korea, in 2004 and 2008, respectively.

He was a senior researcher/research professor with the KAIST Institute for Information Technology Convergence, Daejeon, Korea, from January 2009 to February 2010. From March 2010 to August 2015, he was a faculty of Gyeongsang National University, Tongyeong, Korea. He is currently a Professor in the Department of Electronics Engineering, Chungnam National University, Daejeon, Korea. He has served as Associate Editor of IEICE Transactions on Fundamentals of Electronics, Communications, and Computer Sciences since 2018.

Dr. Jung was the recipient of the 5th IEEE Communication Society Asia–Pacific Outstanding Young Researcher Award in 2011, KICS Haedong Young Scholar Award in 2015, and the 29th KOFST Science and Technology Best Paper Award in 2019. His 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.

---

---

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/.