On the Secrecy Sum-Rate of Uplink Multiuser Networks with Potential Eavesdroppers

Inkyu Bang
Dept. of Intelligence Media Engineering
Hanbat National University
Daejeon 34158, Republic of Korea
ikbang@hanbat.ac.kr

Seong Ho Chae
Dept. of Electronics Engineering
Tech University of Korea
Siheung 15073, Republic of Korea
shchae@tukorea.ac.kr

Bang Chul Jung*
Dept. of Electronics Engineering
Chungnam National University
Daejeon 34134, Republic of Korea
bcjung@cnu.ac.kr (C.A)

2024 Fifteenth International Conference on Ubiquitous and Future Networks (ICUFN) | 979-8-3503-8529-8/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICUFN61752.2024.10625531

***Abstract*—In this paper, we investigate achievable secrecy sum-rate in uplink multiuser networks where some base stations are compromised to operate as potential eavesdroppers. Due to the difficulty of analyzing the exact secrecy capacity region in multiuser networks, we focus on analyzing the secrecy sum-rate scaling in terms of the number of transmitters based on multiuser diversity (MUD). We propose an opportunistic user scheduling scheme able to achieve optimal MUD gain in uplink multiuser networks where N transmitters (users), a single desired receiver (i.e., base station), and K potential eavesdroppers (i.e., compromised base stations) are assumed. The proposed scheme enables multiuser transmissions in one scheduling time slot by employing orthogonal random beamforming at the receiver. In addition, the proposed scheme can fully exploit the degrees-of-freedom (DoF) gain when each transmitter is equipped with a single antenna, and base station and potential eavesdroppers are equipped with M antennas. The main results show that the proposed scheduling scheme achieves the optimal secrecy sum-rate scaling indicating that the achievable secrecy sum-rate scales as $M \log(\mathbf{SNR} \log N)$ in a high signal-to-noise ratio (SNR) regime when a certain user scaling condition.**

***Index Terms*—Physical-layer security, multiuser diversity, opportunistic scheduling, random beamforming, multiple access channel.**

I. Introduction

In the 6G era, information security has become more important than ever [1]. However, unfortunately, the wireless communication systems can be easily exposed to eavesdropping attacks due to the broadcasting nature of radio signals. Traditionally, for information protection, an encryption/decryption such as AES (Advanced Encryption Standard) has been generally used in upper layers (e.g., transport layer) in wireless communication systems. In recent, a notion of achieving information theoretic secrecy in wireless networks, so-called a *physical-layer security*, has attracted much attention. The physical-layer security exploits the randomness of the wireless channel, instead of using computational hardness commonly used in conventional cryptographic approaches, to guarantee confidentiality [2].

The fundamental notions of physical-layer security have been established by Shannon [3]. Since then, there have been lots of efforts to investigate information-theoretic secrecy at the physical-layer in wireless communication systems [4]. Especially, we seek to investigate the achievable secrecy sum-rate in uplink multiuser networks where multiple users transmit data to the desired receiver (e.g., a base station) at the same time under eavesdropping attacks.

There have been several studies which investigate various aspects of the secrecy rate in multiuser wiretap networks, such as *secure degrees-of-freedom* [5], *secrecy diversity* [6], [7], and *secrecy rate scaling* [8]–[10]. Xie and Ulukus studied secure degrees-of-freedom (DoF) regions of the multiple access channel and the multiuser interference channel under several secrecy constraints [5]. Like the notion of DoF is readily modified to the secure DoF, secrecy diversity order, similar to the definition of traditional diversity order, is a notion to indicate diversity gain when we consider the secrecy outage probability. Chae *et al.* investigated secrecy outage probability in multiple-input and multiple-ouput (MIMO) wiretap channels [6]. Zou *et al.* investigated the effects of various user scheduling schemes on secrecy diversity order in terms of secrecy outage probability, considering multiple users in cognitive radio networks [7]. In other words, multiuser diversity (MUD), i.e., the number of users, can contribute to enhancing secrecy in wireless networks. The authors of [8]–[10] investigated ways to opportunistically exploit multiple users during the scheduling process in order to achieve optimal MUD gain in terms of secrecy rate scaling. Particularly, previous studies only investigated single-user transmission during one scheduling time slot even for multiple antenna settings. It has not been explored yet to analyze the secrecy sum-rate scaling of a user scheduling scheme that supports multiuser transmissions at the same time in multiple antenna settings.

In this paper, we propose an opportunistic user scheduling scheme, which achieves optimal MUD gain in uplilnk multiuser networks, which consists of N transmitters (users), a single desired receiver (base station), and K potential eavesdroppers (i.e., compromised base stations). Our proposed scheme enables multiuser transmissions in one scheduling time slot by employing orthogonal random beamforming at the receiver. The proposed scheme can fully exploit the degrees-of-freedom gain when each transmitter is equipped with a single antenna, and base station and potential eavesdroppers are equipped with M antennas. The main contributions of our work are summarized as follows;

* Corresponding Author: Bang Chul Jung

- To the best of our knowledge, it is the first study to investigate secrecy sum-rate scaling in uplink multiuser networks where independent multiple potential eavesdroppers exist;
- We have proved that the achievable secrecy sum-rate of the proposed scheme scales as $M \log(\mathrm{SNR} \log N)$ when a user scaling condition is satisfied;
- Numerical results show that the proposed scheme outperforms conventional scheduling schemes in terms of secrecy sum-rate.

Notations: Throughout the paper, we use the following notations. $\triangleq$ stands for "is defined as". $|\cdot|$ represents a cardinality when it applies to the set or an absolute value when it applies to the scalar value. $\mathbf{I}_n$ represents an n by n identity matrix. $[x]^+$ denotes $\max(x, 0)$. $(\cdot)^T$ is transpose operator. Similarly, $(\cdot)^H$ denotes conjugate transpose. $\det(\cdot)$ and $\|\cdot\|$ denote determinant of a matrix and Euclidean norm, respectively.

II. System Model

We consider a time-division duplexing (TDD) uplink multiuser network which consists of N transmitters (users), a single desired receiver (base station), and K potential eavesdroppers (i.e., uplink wiretap channel). We assume that some base stations located close to the desired base station can be compromised by the adversary for the purpose of eavesdropping and thus we regard them as potential eavesdroppers.[1] We assume that each transmitter is equipped with a single antenna, and base station (BS) and each eavesdropper (Eve) have the same M antennas. We consider a block-fading channel model, where the channel is constant within a single block and independently varying in the next block. During one symbol time, S users are scheduled for data transmission. Thus, it can be modeled by a single-input and multiple-output (SIMO) multiple access channel (MAC). Fig. 1 describes an example of the system model.

The term $\alpha_n \mathbf{h}_n \in \mathbb{C}^{M\times 1}$ denotes the channel vector from the n-th transmitter to the base station, where α_n and $\mathbf{h}_n$ for $n \in \{1, \cdots, N\}$ represent the large-scale and small-scale fading components, respectively. Similarly, the term $\beta_{nk}\mathbf{g}_{nk} \in \mathbb{C}^{M\times 1}$ denotes the channel vector from the n-th transmitter to the k-th eavesdropper, where β_{nk} and $\mathbf{g}_{nk}$ for $k \in \{1, \cdots, K\}$ represent the large-scale and small-scale fading components, respectively. Each element of $\mathbf{h}_n$ and $\mathbf{g}_{nk}$ is assumed to be an independent and identically distributed (i.i.d.) complex Gaussian random variable with zero mean and unit variance. Further, $\mathbf{h}_n$ and $\mathbf{g}_{nk}$ are available during the scheduling process since we assume the potential eavesdropping scenario as in [11]. The term $\mathcal{N}_S$ denotes a selected transmitter index set with $|\mathcal{N}_S| = S$.

A. Random Beamforming at Receiver

To support simultaneous data transmission from multiple transmitters, we employ random beamforming at the desired receiver, which can decode maximum M signals at the same time [12]. For each time slot, the base station constructs beamforming vectors represented for selected S transmitters by an $M \times S$ matrix ($S \leq M$),

$$\mathbf{U} = \left[\mathbf{u}^{[1]}, \cdots, \mathbf{u}^{[S]}\right], \tag{1}$$

where $\mathbf{u}^{[l]} \in \mathbb{C}^{M\times 1}$ is the l-th orthonormal random vector and generated according to the isotropic distribution for $l \in \{1, \cdots, S\}$. The information of generated beamforming vectors is broadcasted to all transmitters for scheduling process. The detailed scheduling procedure will be explained in the Section III.

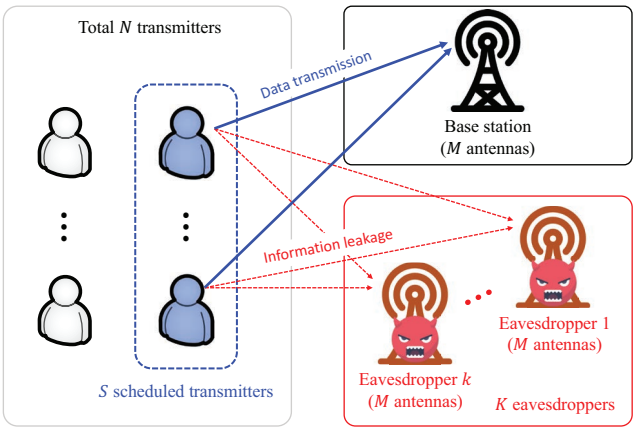

Fig. 1: An uplink multiuser network consisting of N users (S scheduled transmitters for data), a single base station and K potential eavesdroppers: the SIMO MAC model

B. Achievable Secrecy Sum-Rate

It is difficult to obtain an individual secrecy capacity region in wireless multiuser networks. Instead, we consider secrecy sum-rate as in [13] and use a lower bound of the achievable secrecy sum-rate. For analytical tractability, we assume that $\alpha_n = 1$ and $\beta_{nk} = 1$ for all n and k. Then, the received signals at the base station, $\mathbf{y} \in \mathbb{C}^{M\times 1}$, and at the k-th eavesdropper, $\mathbf{y}_k \in \mathbb{C}^{M\times 1}$, are expressed, respectively, as

$$\mathbf{y} = \sum_{s\in\mathcal{N}_S} \mathbf{h}_s x_s + \mathbf{z}, \text{ and } \mathbf{y}_k = \sum_{s\in\mathcal{N}_S} \mathbf{g}_{sk} x_s + \mathbf{z}_k, \tag{2}$$

where x_s denotes the desired data symbol for the s-th transmitter among selected S users (i.e., $s \in \mathcal{N}_S$), each of which meets the average power constraint P_0, and $\mathbf{z}$ and $\mathbf{z}_k$ denote the i.i.d. and circularly symmetric complex additive white Gaussian noise vectors with zero mean and covariance of $\sigma^2\mathbf{I}_M$.

Note that the achievable secrecy sum-rate is obtained based on the sum of secrecy rates between *main channel* (between transmitters and base station) and *wiretap channel* (between transmitters and eavesdroppers). Thus, the achievable secrecy sum-rate can be different depending on the post-processing at base station and eavesdroppers.

For the main channel, the desired base station decodes received signal in (2) by using receive random beamforming

[1]Throughout the paper, we use both terms 'potential eavesdropper' and 'eavesdropper' interchangeably for concise expressions.

based on (1) and, the achievable rate of each transmitter and base station pair in the main channel is given by

$$r_{\text{BS}}^{[s]} = \log\left(1 + \frac{|\mathbf{u}_0^{[s]T}\mathbf{h}_{\pi_s}|^2\rho}{1+\sum_{l=1,l\neq s}^{S}|\mathbf{u}_0^{[l]T}\mathbf{h}_{\pi_l}|^2\rho}\right), \quad (3)$$

where $\mathbf{u}_0^{[s]}$ represents s-th receive random beamforming vector defined in (1), π_s denotes scheduled transmitter index for the beam $\mathbf{u}_0^{[s]}$, and ρ is the transmit SNR defined as $\rho \triangleq \frac{P_0}{\sigma^2}$.[2]

Eavesdroppers are assumed to be internal nodes such as compromised base stations. Thus, we assume that eavesdroppers operate the same as the base station and use the receive random beamforming technique. Similar to the desired base station, each eavesdropper independently decodes its received signal in (2) by using receive random beamforming based on (1).

From the perspective of s-th receive random beamforming, information leakage by all eavesdroppers (i.e., the achievable rate by eavesdroppers) is given by

$$r_{\text{Eve}}^{[s]} = \max_{k\in\mathcal{K}}\left\{\log\left(1 + \frac{|\mathbf{u}_k^{[s]T}\mathbf{g}_{\pi_s k}|^2\rho}{1+\sum_{l=1,l\neq s}^{S}|\mathbf{u}_k^{[l]T}\mathbf{g}_{\pi_l k}|^2\rho}\right)\right\}, \quad (4)$$

where $\mathcal{K}$ denotes eavesdropper index set, i.e., $\mathcal{K} \triangleq \{1,\cdots,K\}$, $\mathbf{u}_k^{[s]}$ represents s-th receive random beamforming vector defined in (1), and subscript k in $\mathbf{u}_k^{[s]}$ indicates receive random beamforming vectors at k-th eavesdropper. (4) is represented as maximum of each eavesdropper's achievable sum-rate among K eavesdroppers since we assume each eavesdropper operates independently.

Therefore, the achievable secrecy sum-rate is given by

$$R_{\text{sec}} = \sum_{s}^{S}\left[r_{\text{BS}}^{[s]} - r_{\text{Eve}}^{[s]}\right]^+, \quad (5)$$

where $r_{\text{BS}}^{[s]}$ and $r_{\text{Eve}}^{[s]}$ are defined in (3) and (4), respectively.

III. Opportunistic User Scheduling Scheme for Optimal Multiuser Diversity Gain

In this section, we define the scheduling parameters, introduce our proposed user scheduling scheme, and analyze its secrecy sum-rate scaling.

A. Scheduling Parameters

For n-th transmitter and its expected scheduling beam index $l^* \in \{1,\cdots,S\}$, we define the following scheduling metrics.

$$\eta_{\text{Q}}^{[n,l^*]} \triangleq |\mathbf{u}_0^{[l^*]T}\mathbf{h}_n|^2, \quad (6a)$$

$$\eta_{\text{I}}^{[n,l^*]} \triangleq \sum_{l=1,l\neq l^*}^{S}|\mathbf{u}_0^{[l]T}\mathbf{h}_n|^2, \quad (6b)$$

$$\eta_{\text{L}}^{[n]} \triangleq \max_{k\in\mathcal{K}}\|\mathbf{g}_{nk}\|^2, \quad (6c)$$

where we define a normalized signal quality in main channel, a normalized generating interference of n-th transmitter at the desired base station, and a maximum of normalized information leakage in wiretap channel as $\eta_{\text{Q}}^{[n,l^*]}$, $\eta_{\text{I}}^{[n,l^*]}$, and $\eta_{\text{L}}^{[n]}$, respectively.

Additionally, we devise pre-determined positive threshold values, $\eta_{\text{I}}^{\star}$ and $\eta_{\text{L}}^{\star}$, which represent for the maximum of allowable generating interference and information leakage, respectively. The optimal values of $\eta_{\text{I}}^{\star}$ and $\eta_{\text{L}}^{\star}$ can be obtained through simulation for given system parameters such as N, K, M, and S.

B. Opportunistic User Scheduling Scheme

The proposed user scheduling scheme opportunistically selects S transmitters based on signal quality on the main channel and wiretap channel indicated by scheduling parameters defined in (6). The entire procedure of the proposed user scheduling scheme consists of the following four steps during one scheduling time slot.

*1) **Step 1. Broadcast receive random vectors & pre-determined threshold values**:* The base station first constructs S orthogonal random vectors (i.e., $\mathbf{U}_0 = \left[\mathbf{u}_0^{[1]},\cdots,\mathbf{u}_0^{[S]}\right]$) and broadcast the information of $\mathbf{U}_0$, $\eta_{\text{I}}^{\star}$ and $\eta_{\text{L}}^{\star}$ to all transmitters.

*2) **Step 2. Scheduling metric feedback information**:* For given an expected scheduling beam index l^* ($\forall l^* \in \{1,\cdots,S\}$), each transmitter estimates its scheduling parameters in (6) and compares them with $\eta_{\text{I}}^{\star}$ and $\eta_{\text{L}}^{\star}$. If estimated generating interference or information leakage exceeds the maximum allowable level of the system (i.e., $\eta_{\text{I}}^{[n,l^*]} \geq \eta_{\text{I}}^{\star}$ or $\eta_{\text{L}}^{[n]} \geq \eta_{\text{L}}^{\star}$), the transmitter does not transmit feedback information for the corresponding beam index. Further, the transmitter might not transmit any feedback information if none of the beams satisfies the system constraints. In other words, the transmitter opportunistically transmits feedback information for a certain beam when it satisfies (6).

*3) **Step 3. User selection**:* After receiving N transmitters' feedback information, the base station selects the best S transmitters corresponding to S receive vectors and broadcast scheduling transmitter index set to all transmitters.

*4) **Step 4. Uplink communication & receive processing**:* S selected transmitters simultaneously transmit their data to the base station. The base station receives the signals and decodes the desired data using the receive beamforming vectors.

C. Analysis of Secrecy Sum-Rate Scaling

Now, we analyze the secrecy performance of proposed scheduling algorithm in terms of secrecy sum-rate scaling. We show that the proposed scheme asymptotically achieves the optimal secrecy sum-rate scaling, where the secrecy sum-rate scales as $M\log(\rho\log N)$ when the number of users (N) increases with SNR (ρ). In other words, we analyze how N scales with ρ to achieve the optimal secrecy rate scaling.

We investigate a lower bound of the achievable secrecy sum-rate and prove the optimal secrecy sum-rate scaling using the

[2]Here, subscript zero in $\mathbf{u}_0^{[s]}$ indicates receive random beamforming vectors at the desired BS.

lower bound. The lower bound of R_{sec} is given by

$$\begin{aligned} R_{\text{sec}} &= \sum_{s}^{S} \left[r_{\text{BS}}^{[s]} - r_{\text{Eve}}^{[s]} \right]^{+} \\ &\geq \left[\sum_{s}^{S} r_{\text{BS}}^{[s]} - \sum_{s}^{S} r_{\text{Eve}}^{[s]} \right]^{+} = [R_{\text{BS}}^{\text{sum}} - R_{\text{Eve}}^{\text{sum}}]^{+} \\ &\geq \left[R_{\text{BS}}^{\text{sum}} - \max_{k \in \mathcal{K}} \left\{ \log\det \left(\mathbf{I}_M + \rho \sum_{s \in \mathcal{N}_S} \mathbf{g}_{sk} \mathbf{g}_{sk}^H \right) \right\} \right]^{+} \\ &= [R_{\text{BS}}^{\text{sum}} - C_{\text{Eve}}^{\text{sum}}]^{+} \geq R_{\text{BS}}^{\text{sum}} - C_{\text{Eve}}^{\text{sum}}, \end{aligned} \tag{7}$$

where $\max_{k \in \mathcal{K}} \left\{ \log\det \left(\mathbf{I}_M + \rho \sum_{s \in \mathcal{N}_S} \mathbf{g}_{sk} \mathbf{g}_{sk}^H \right) \right\}$ is denoted by $C_{\text{Eve}}^{\text{sum}}$ and $R_{\text{BS}}^{\text{sum}}$ and $R_{\text{Eve}}^{\text{sum}}$ denote $\sum_s^S r_{\text{BS}}^{[s]}$ and $\sum_s^S r_{\text{Eve}}^{[s]}$, respectively. In (7), the first and the third inequalities hold due to characteristics of $[\cdot]^+$ function and the second inequality holds since $C_{\text{Eve}}^{\text{sum}}$ indicates capacity of the wiretap channel. Thus, we consider $R_{\text{BS}}^{\text{sum}} - C_{\text{Eve}}^{\text{sum}}$ instead of R_{sec} during the main proof.

We consider a slightly modified version of the proposed scheduling algorithm to prove the achievability of the optimal secrecy sum-rate scaling. The modified scheduling scheme additionally considers a threshold value for the minimum signal quality for the main channel (i.e., $\eta_{\text{Q}}^{\star}$) for given transmitter index n and beam index l^*. Thus, the modified scheduling scheme only utilizes the information of transmitter index n and beam index l^* satisfying the following scheduling criteria:

$$\begin{aligned} &(\mathbf{C1}) \quad \eta_{\text{Q}}^{[n,l^*]} \geq \eta_{\text{Q}}^{\star}, \\ &(\mathbf{C2}) \quad \eta_{\text{I}}^{[n,l^*]} \leq \eta_{\text{I}}^{\star}, \\ &(\mathbf{C3}) \quad \eta_{\text{L}}^{[n]} \leq \eta_{\text{L}}^{\star}, \end{aligned} \tag{8}$$

where $\eta_{\text{Q}}^{[n,l^*]}$, $\eta_{\text{I}}^{[n,l^*]}$, and $\eta_{\text{L}}^{[n]}$ are defined in (6).

Definitely, the modified scheduling scheme shows the degraded performance compared with the original proposed scheduling scheme since modified version additionally consider (**C1**) constraint. Therefore, the proof for the achievability of the modified scheduling scheme is enough to show the achievability of the proposed scheme.

To prove the achievability, we first show that there exists at least one transmitter satisfying all criteria in (8) with high probability and next verify the optimal secrecy sum-rate scaling. We introduce the following two lemmas in order to prove our main theorem.

Lemma 1. *Let $f(x)$ denote a continuous function of $x \in [0, \infty)$, where $0 < f(x) \leq 1$. Then, $\lim_{x\to\infty} (1 - f(x))^x = 0$ if and only if $\lim_{x\to\infty} x f(x) \to \infty$.*

Proof: If $\lim_{x\to\infty} x f(x) \to \infty$, then it follows that $f(x) = \omega(\frac{1}{x})$, thus resulting in

$$\lim_{x\to\infty} (1 - f(x))^x = o\left(\lim_{x\to\infty} \left(1 - \frac{1}{x} \right)^x \right) = o(1)$$

for $0 < f(x) \leq 1$. It is hence seen that $\lim_{x\to\infty} (1 - f(x))^x$ converges to zero. If $\lim_{x\to\infty} x f(x)$ is finite, then there exists a constant $c_3 > 0$ such that $x f(x) < c_3$ for any $x \geq 0$. We then have

$$\lim_{x\to\infty} (1 - f(x))^x = \lim_{x\to\infty} \left(1 - \frac{c_3}{x} \right)^x = e^{-c_3} > 0,$$

which completes the proof. ∎

Lemma 2. *For any $0 \leq x < 1$ and $z > 0$, the lower incomplete Gamma function $\gamma(z, x)$ is lower-bounded by*

$$\gamma(z, x) \geq \frac{1}{z} x^z e^{-1}. \tag{9}$$

Proof: The inequality in (9) holds since

$$\begin{aligned} \gamma(z, x) &= \frac{1}{z} x^z e^{-x} + \gamma(z + 1, x) \\ &= \frac{1}{z} x^z e^{-x} + \frac{1}{z(z)} x^{z+1} e^{-x} + \cdots \\ &\geq \frac{1}{z} x^z e^{-1}, \end{aligned}$$

which completes the proof. ∎

Let $p^{[l^*]}$ denote a probability that at least one transmitter satisfying all criteria in (8) for l^*-th beam. To analyze $p^{[l^*]}$, we characterize the probability such that each criterion is satisfied for a certain transmitter, i.e., $\Pr(\mathbf{C1})$, $\Pr(\mathbf{C2})$, and $\Pr(\mathbf{C3})$. Hereafter, we omit the transmitter index n and the beam index l^* for representing each probability due to the fact that we assume the i.i.d. channel vectors. In other word, $\Pr(\mathbf{C1})$, $\Pr(\mathbf{C2})$, or $\Pr(\mathbf{C3})$ is same regardless of a certain transmitter index $n \in \{1, \cdots, N\}$ and beam index $l^* \in \{1, \cdots, M\}$.

First, $\Pr(\mathbf{C1})$ is given by

$$\Pr(\mathbf{C1}) \triangleq \Pr\left\{ |\mathbf{u}_0^{[l^*]T} \mathbf{h}_n|^2 \geq \eta_{\text{Q}}^{\star} \right\} = e^{-\eta_{\text{Q}}^{\star}}, \tag{10}$$

since the receive beam $\mathbf{u}_0^{[l^*]T}$ is assumed to be isotropically distributed and thus $|\mathbf{u}_0^{[l^*]T} \mathbf{h}_n|^2$ is exponentially distributed [12].

Second, $\Pr(\mathbf{C2})$ is given by

$$\Pr(\mathbf{C2}) \triangleq \Pr\left\{ \sum_{l=1, l\neq l^*}^{S} |\mathbf{u}_0^{[l]T} \mathbf{h}_n|^2 \leq \eta_{\text{I}}^{\star} \right\} = \frac{\gamma(S - 1, \eta_{\text{I}}^{\star}/2)}{\Gamma(S - 1)}, \tag{11}$$

where $\Gamma(z) = \int_0^\infty t^{z-1} e^{-t} dt$ is the Gamma function and $\gamma(z, x) = \int_0^x t^{z-1} e^{-t} dt$ is the lower incomplete Gamma function.

In (11), the last equality holds due to the fact that $|\mathbf{u}_0^{[l]T} \mathbf{h}_n|^2$ is exponentially distributed and the sum of $S - 1$ independent exponential random variables is distributed according to the chi-square distribution with $2(S - 1)$ degrees-of-freedom [14].

Third, $\Pr(\mathbf{C3})$ is given by

$$\Pr(\mathbf{C3}) \triangleq \Pr\left\{ \max_{k \in \mathcal{K}} \|\mathbf{g}_{nk}\|^2 \leq \eta_{\text{L}}^{\star} \right\} = \left(\frac{\gamma(M, \eta_{\text{L}}^{\star}/2)}{\Gamma(M)} \right)^K,$$

since the term $\|\mathbf{g}_{nk}\|^2$ is the sum of M independent exponential random variables and thus it is distributed according to the chi-square distribution with $2M$ degrees-of-freedom, i.e., $\frac{\gamma(M,\eta_{\mathrm{L}}^\star/2)}{\Gamma(M)}$. Therefore, according to [14], the term $\max_{k\in\mathcal{K}}\|\mathbf{g}_{nk}\|^2$ is distributed as $\left(\frac{\gamma(M,\eta_{\mathrm{L}}^\star/2)}{\Gamma(M)}\right)^K$.

Finally, we introduce our main theorem to show the achievable secrecy sum-rate scaling of the proposed scheduling scheme.

Theorem 1. *For an $\epsilon \in (0,1)$, $\eta_{\mathrm{Q}}^\star = \epsilon \log N$, and $\eta_{\mathrm{I}}^\star = \eta_{\mathrm{L}}^\star = \rho^{-1}$, the proposed scheduling scheme achieves secrecy sum-rate scaling as $\Theta\left(M\log\left(\rho\log N\right)\right)$ with high probability when*

$$N = \Theta\left(\rho^{\frac{M(K-1)+1}{1-\epsilon_0}}\right), \tag{12}$$

where $\epsilon_0 \in (\epsilon, 1)$ is a constant.[3]

Proof: We consider the modified scheduling scheme instead of the proposed scheduling scheme for the proof. First, we focus on the probability that at least one transmitter satisfying all criteria in (8) for l^*-th beam, i.e., $p^{[l^*]}$. Using the probability $\Pr(\mathbf{C1})$, $\Pr(\mathbf{C2})$, and $\Pr(\mathbf{C3})$, $p^{[l^*]}$ is lower-bounded by

$$\begin{aligned} p^{[l^*]} &\geq 1 - \left(1 - \Pr(\mathbf{C1})\Pr(\mathbf{C2})\Pr(\mathbf{C3})\right)^N \\ &= 1 - \left(1 - e^{-\eta_{\mathrm{Q}}^\star} F_{\mathrm{C2}}\left(\eta_{\mathrm{I}}^\star\right) F_{\mathrm{C3}}\left(\eta_{\mathrm{L}}^\star\right)\right)^N, \end{aligned}$$

where we define $F_{\mathrm{C2}}\left(\eta_{\mathrm{I}}^\star\right) \triangleq \Pr(\mathbf{C2})$ and $F_{\mathrm{C3}}\left(\eta_{\mathrm{L}}^\star\right) \triangleq \Pr(\mathbf{C3})$.

From Lemma 1 with $0 < e^{-\eta_{\mathrm{Q}}^\star} F_{\mathrm{C2}}\left(\eta_{\mathrm{I}}^\star\right) F_{\mathrm{C3}}\left(\eta_{\mathrm{L}}^\star\right) \leq 1$, it follows that $p^{[l^*]}$ converges to one as N tends to infinity if

$$\lim_{N\to\infty} N e^{-\eta_{\mathrm{Q}}^\star} F_{\mathrm{C2}}\left(\eta_{\mathrm{I}}^\star\right) F_{\mathrm{C3}}\left(\eta_{\mathrm{L}}^\star\right) \to \infty. \tag{13}$$

Using Lemma 2, $F_{\mathrm{C2}}\left(\eta_{\mathrm{I}}^\star\right)$ and $F_{\mathrm{C3}}\left(\eta_{\mathrm{L}}^\star\right)$ are lower bounded as follows, respectively:

$$\begin{aligned} F_{\mathrm{C2}}\left(\eta_{\mathrm{I}}^\star\right) &\geq c_1 \left(\eta_{\mathrm{I}}^\star\right)^{S-1}, \\ F_{\mathrm{C3}}\left(\eta_{\mathrm{L}}^\star\right) &\geq c_2 \left(\eta_{\mathrm{L}}^\star\right)^{MK}, \end{aligned} \tag{14}$$

where $c_1 = \frac{e^{-1}2^{-(S-1)}}{(S-1)\Gamma(S-1)}$ and $c_2 = \left(\frac{e^{-1}2^{-M}}{M\Gamma(M)}\right)^K$. Thus, by using (14), the term in (13) can be lower-bounded by

$$\lim_{N\to\infty} c_1 c_2 N \left(\eta_{\mathrm{I}}^\star\right)^{S-1} \left(\eta_{\mathrm{L}}^\star\right)^{MK} e^{-\eta_{\mathrm{Q}}^\star}.$$

Substituting $S = M$, $\eta_{\mathrm{Q}}^\star = \epsilon \log N$, and $\eta_{\mathrm{I}}^\star = \eta_{\mathrm{L}}^\star = \rho^{-1}$, it is further reduced to

$$\lim_{N\to\infty} c_1 c_2 \frac{N}{\rho^{M(K+1)-1}} e^{-\epsilon \log N} = \lim_{N\to\infty} \frac{N^{1-\epsilon}}{\rho^{M(K+1)-1}},$$

which tends to infinity when N scales as $\rho^{\frac{M(K-1)+1}{1-\epsilon_0}}$. Therefore, the probability $p^{[l^*]}$ converges to one when $N = \Theta\left(\rho^{\frac{M(K-1)+1}{1-\epsilon_0}}\right)$.

[3]We use the following notations: i) $f(x) = \mathcal{O}\left(g(x)\right)$ means that there exist constants C and c such that $f(x) \leq C g(x)$ for all $x > c$. ii) $f(x) = \Theta\left(g(x)\right)$ if $f(x) = \mathcal{O}\left(g(x)\right)$ and $g(x) = \mathcal{O}\left(f(x)\right)$.

It remains to show the achievable secrecy sum-rate scales $\Theta\left(M\log\left(\rho\log N\right)\right)$. From (7), a lower bound of the sum-rate of the main channel is given by

$$\begin{aligned} R_{\mathrm{BS}}^{\mathrm{sum}} &= \sum_{l^*=1}^{M} \log\left(1 + \frac{|\mathbf{u}_0^{[l^*]T}\mathbf{h}_{\pi_{l^*}}|^2\rho}{1+\sum_{l=1,l\neq l^*}^{M}|\mathbf{u}_0^{[l]T}\mathbf{h}_{\pi_l}|^2\rho}\right) \\ &\geq \sum_{l^*=1}^{M} p^{[l^*]} \log\left(1 + \frac{\eta_{\mathrm{Q}}^\star\rho}{1+(M-1)\eta_{\mathrm{I}}^\star\rho}\right) \\ &= M\log\left(1 + \frac{\epsilon}{M}\rho\log N\right). \end{aligned}$$

Similarly, an upper bound of the sum-rate of wiretap channel is given by

$$\begin{aligned} R_{\mathrm{Eve}}^{\mathrm{sum}} &= \max_{k\in\mathcal{K}}\left\{\sum_{s=1}^{S}\log\left(1 + \frac{|\mathbf{u}_k^{[s]T}\mathbf{g}_{\pi_s k}|^2\rho}{1+\sum_{l=1,l\neq s}^{S}|\mathbf{u}_k^{[l]T}\mathbf{g}_{\pi_l k}|^2\rho}\right)\right\} \\ &\leq \max_{k\in\mathcal{K}}\left\{\log\det\left(\mathbf{I}_M + \rho\sum_{s\in\mathcal{N}_S}\mathbf{g}_{sk}\mathbf{g}_{sk}^H\right)\right\} \\ &\leq M\log\left(1+\eta_{\mathrm{L}}^\star\rho\right) = M\log(2). \end{aligned}$$

where the first inequality holds from the fact that $R_{\mathrm{Eve}}^{\mathrm{sum}}$ is always smaller than or equal to the channel capacity of the wiretap channel.

Therefore, secrecy sum-rate is lower-bounded by

$$\begin{aligned} R_{\mathrm{sec}} &\geq R_{\mathrm{BS}}^{\mathrm{sum}} - C_{\mathrm{Eve}}^{\mathrm{sum}} \\ &\geq M\log\left(1 + \frac{\epsilon}{M}\rho\log N\right) - M\log(2) \\ &= M\log\left(\frac{1}{2} + \frac{\epsilon}{2M}\rho\log N\right), \end{aligned}$$

which achieves full degree-of-freedom gain M and optimal MUD gain $\log\log N$ as N tends to infinity. This completes the proof of the theorem. ■

IV. Numerical Results

In this section, we evaluate the performance of our proposed schemes in term of the achievable secrecy sum-rate through simulations. We consider three conventional user scheduling schemes as references: *MaxSNR*, *MinGI*, and *OS-MRC*. *MaxSNR* indicates a user scheduling scheme that selects the users having the maximum desired signal strength to each beam. Contrary to *MaxSNR*, *MinGI* is a user scheduling scheme that selects the users generating minimum amount of interference to other beams. *OS-MRC* represents a threshold-based opportunistic scheduling scheme with maximum ratio combining instead of random beamforming at receiver and eavesdroppers [9].

Fig. 2 shows the average achievable secrecy sum-rate for varying the number of users. In details, *MaxSNR* and *MinGI* shows the degraded secrecy performance compared to the proposed scheme since they do not fully utilize channel information for user scheduling. Even though *OS-MRC* adopts threshold-based opportunistic scheduling, there is a significant performance gap between the proposed scheme and *OSMRC*

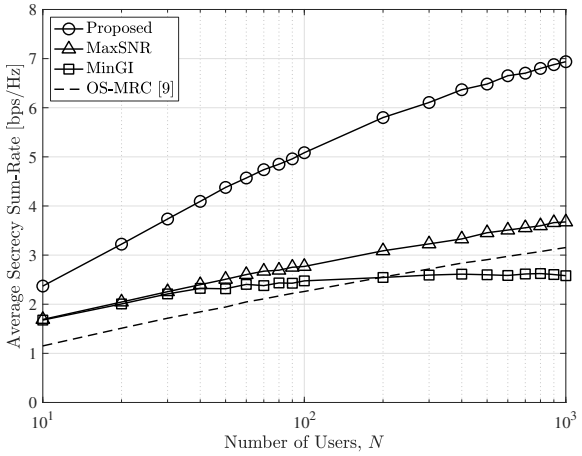

Fig. 2: Average achievable secrecy sum-rate for varying the number of users when $M = 2$, $K = 2$, and $\rho = 10$ dB.

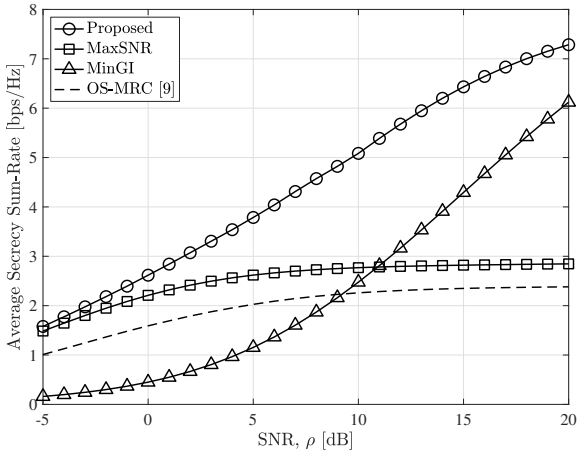

Fig. 3: Average achievable secrecy rate for varying SNR when $M = 2$, $N = 100$, and $K = 2$.

since *OS-MRC* does not fully utilize spatial diversity (i.e., $S = 1$) whereas the proposed scheme does.

Fig. 3 shows the average achievable secrecy sum-rate for varying SNR, where system parameters are set as $M = 2$, $N = 100$, and $K = 2$. Similar to the result of Fig. 2, the proposed scheme outperforms conventional schemes. Interestingly, *MinGI* shows good secrecy performance in high SNR regime whereas secrecy sum-rate of *MaxSNR* is saturated as SNR increases. It indicates that inter-beam interference at the desired receiver is the dominant factor to determine secrecy sum-rate since eavesdroppers use the same random beamforming techniques at receiving process.

Remark 1. *Note that we considered terrestrial communication environment. However, our proposed scheme can be applied to satellite communication networks. Specifically, our proposed scheduling scheme can enhance the secrecy performance of satellite communications by minimizing information leakage to unauthorized nodes. As we discussed, our proposed scheme is particularly effective as the number of nodes increases.*

V. Conclusions

In this paper, we proposed the threshold-based opportunistic user scheduling, which achieves secrecy sum-rate scaling as $M \log(\rho \log N)$ when the number of transmitters goes to infinity in high SNR regime. Further, the secrecy performance of the proposed scheme was evaluated through simulations and the results show the superiority of our proposed user scheduling scheme compared with conventional schemes, in terms of secrecy sum-rate, especially, when the number of transmitters is sufficiently large. The analysis for secrecy sum-rate scaling in various environment (e.g., satellite communication networks) would be one of the future issues of this work.

Acknowledgment

This work was partially supported by Korea Research Institute for defense Technology planning and advancement(KRIT) grant funded by the Korea government(DAPA(Defense Acquisition Program Administration)) (21-106-A00-007, Space-Layer Intelligent Communication Network Laboratory, 2022) and was also partially supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. 2022R1F1A1076126).

References

[1] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The roadmap to 6G security and privacy," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1094–1122, 2021.

[2] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[3] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[4] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, 2018.

[5] J. Xie and S. Ulukus, "Secure degrees of freedom regions of multiple access and interference channels: The polytope structure," *IEEE Transactions on Information Theory*, vol. 62, no. 4, pp. 2044–2069, 2016.

[6] S. H. Chae, I. Bang, and H. Lee, "Physical layer security of QSTBC with power scaling in MIMO wiretap channels," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 5647–5651, 2020.

[7] Y. Zou, X. Li, and Y.-C. Liang, "Secrecy outage and diversity analysis of cognitive radio systems," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 11, pp. 2222–2236, 2014.

[8] H. Jin, W.-Y. Shin, and B. C. Jung, "On the multi-user diversity with secrecy in uplink wiretap networks," *IEEE Communications Letters*, vol. 17, no. 9, pp. 1778–1781, 2013.

[9] I. Bang, S. M. Kim, and D. K. Sung, "Effects of multiple antennas and imperfect channel knowledge on secrecy multiuser diversity," *IEEE Communications Letters*, vol. 19, no. 9, pp. 1564–1567, 2015.

[10] I. Bang, S. M. Kim, and D. K. Sung, "Artificial noise-aided user scheduling for optimal secrecy multiuser diversity," *IEEE Communications Letters*, vol. 21, no. 3, pp. 528–531, 2017.

[11] I. Bang and B. C. Jung, "Secrecy rate analysis of opportunistic user scheduling in uplink networks with potential eavesdroppers," *IEEE Access*, vol. 7, pp. 127078–127089, 2019.

[12] M. Sharif and B. Hassibi, "On the capacity of MIMO broadcast channels with partial side information," *IEEE Transactions on Information Theory*, vol. 51, pp. 506 – 522, Feb. 2005.

[13] I. Krikidis and B. Ottersten, "Secrecy sum-rate for orthogonal random beamforming with opportunistic scheduling," *IEEE Signal Processing Letters*, vol. 20, pp. 141 – 144, Feb. 2013.

[14] Athanasios Papoulis and S. Unnikrishna Pillai, *Probability, Random Variables and Stocahstic Processes*. New York, McGraw-Hill, 1984.