electronics

Article

On the Secrecy Sum-Rate of Internet of Things Networks: Scheduling and Power Control †

Inkyu Bang [1], Seong Ho Chae [2] and Bang Chul Jung [3,*]

[1] Department of Intelligence Media Engineering, Hanbat National University, Daejeon 34158, Republic of Korea; ikbang@hanbat.ac.kr
[2] Department of Electronics Engineering, Tech University of Korea, Siheung 15073, Republic of Korea; shchae@tukorea.ac.kr
[3] Department of Electronics Engineering, Chungnam National University, Daejeon 34134, Republic of Korea
* Correspondence: bcjung@cnu.ac.kr; Tel.: +82-42-821-7704

† This paper is an extended version of our paper presented in Bang, I.; Chae, S. H.; Jung, B. C. On the Secrecy Sum-Rate of Uplink Multiuser Networks with Potential Eavesdroppers. In Proceedings of the IEEE 2024 15th International Conference on Ubiquitous and Future Networks (ICUFN), Budapest, Hungary, July 2024.

Abstract: Physical-layer security (PLS) has attracted much attention in wireless communications and has been considered one of the main candidates for enhancing wireless security in future 6G networks. Recent studies in the PLS area have focused on investigating and analyzing the characteristics of secure transmissions in multiuser networks (e.g., the massive number of Internet of Things (IoT) devices in 6G networks). Due to the difficulty of obtaining the exact secrecy capacity region in wireless multiuser networks, several alternative methods are used to characterize the secrecy performance of multiuser networks. For example, we can analyze the secrecy sum-rate scaling in terms of the number of users based on multiuser diversity (MUD). In this paper, we propose an opportunistic user scheduling scheme that achieves optimal MUD gain, combined with a power control mechanism for reducing information leakage to multiple eavesdroppers in wireless networks. The proposed scheme considers multiuser transmissions in one scheduling time slot by adopting orthogonal random beamforming at the receiver to exploit the full degrees-of-freedom gain with an assumption that each user (or IoT device) is equipped with a single antenna, and base station and eavesdroppers have multiple antennas. The main contribution of this paper is to derive the analytic result of the achievable secrecy sum-rate scaling in a high signal-to-noise ratio (SNR) regime. We evaluate the performance of the proposed scheduling scheme with a power control mechanism through simulations with both internal and external eavesdropping scenarios. We further discuss the extensibility of our analysis to various applications such as satellite communications and IoT networks.

Keywords: physical-layer security; Internet of Things; multiuser diversity; scheduling; power control

check for updates

Citation: Bang, I.; Chae, S. H.; Jung, B. C. On the Secrecy Sum-Rate of Internet of Things Networks: Scheduling and Power Control. *Electronics* **2024**, *13*, 2074. https://doi.org/10.3390/electronics13112074

Academic Editors: Ali Khoshkholghi, Javid Taheri and Andreas Johnsson

Received: 22 March 2024
Revised: 12 May 2024
Accepted: 16 May 2024
Published: 27 May 2024

1. Introduction

The 6G networks have been expected to lead a significant leap forward in massive Internet-of-Things (IoT) connectivity [1]. With enhanced requirements such as extremely high data rates, extremely low latency, and always-on broadband global network coverage, 6G is poised to revolutionize the current mobile networks including IoT applications [2]. In the 6G era, information security has become more important than ever [3]. However, unfortunately, wireless communication systems are prone 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. Recently, the notion of achieving information theoretic secrecy in wireless networks, so-called *physical-layer security* (PLS), 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 [4]. Further, the PLS technologies have been considered as one of the possible candidates for the next-generation 6G communication systems [3].

The fundamental notions of physical-layer security have been established by Shannon [5] and Wyner [6]. Since then, there have been many efforts to investigate information-theoretic secrecy at the physical-layer in wireless communication systems [7–12]. Among many topics related to physical-layer security, we seek to investigate characteristics of secure transmissions in *wireless multiuser networks* (e.g., the massive number of IoT devices in the networks). Specifically, we focus on analyzing the characteristics of the secrecy rate, which is one of the challenging problems when we consider wireless multiuser wiretap networks. There have been several studies which investigate various aspects of the secrecy rate in multiuser wiretap networks, such as *secure degrees-of-freedom* [13,14], *secrecy diversity* [15–18], and *secrecy rate scaling* [19–23].

Koyluoglu et al. investigated secure degrees-of-freedom (DoF) under two distinct models, namely the interference channel with confidential messages and the interference channel with an external eavesdropper [13]. Xie and Ulukus further studied secure DoF regions of the multiple access channel and the multiuser interference channel under several secrecy constraints [14]. 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, and it has been investigated from various perspectives [15–18].

Chae et al. investigated secrecy outage probability in multiple-input and multiple-ouput (MIMO) wiretap channels [15]. Particularly, Zou et al. investigated the effects of various user scheduling schemes on secrecy diversity order, in terms of intercept probability and secrecy outage probability, considering multiple users in cognitive radio networks, respectively, [16,17]. In other words, multiuser diversity (MUD), i.e., the number of users, can contribute to enhancing secrecy in wireless networks. Differently from [16,17], authors of [19–23] investigated opportunistically exploiting multiple users in networks to achieve optimal MUD gain in terms of secrecy rate scaling. Jin et al. first introduced the notion of secrecy rate scaling in terms of the number of users to characterize the secrecy rate in a single-cell environment, instead of the exact secrecy rate analysis impossible at most of the multiuser network settings [19]. Subsequently, the secrecy rate scaling has been analyzed in various network environments such as multi-cell [20], multiple receive antenna [21,22], and artificial noise [23] settings. Further, secrecy rate scaling has been investigated combined with recent advanced techniques such as reconfigurable intelligent surface and massive MIMO with one-bit feedback [24,25]. The authors of [24] derived the ergodic secrecy rate of a RIS-assisted communication system against multiple eavesdroppers. Both non-colluding and colluding scenarios were investigated and finally scaling law in terms of the number of RIS elements was analyzed. Teeti investigated the impact of the power-scaling law on the secrecy rate when the massive MIMO with one-bit feedback is considered [25].

Interestingly, in multiuser networks, instead of single user transmission in one time slot, multiuser transmissions in one time slot can be exploited to achieve full degrees-of-freedom gain from the perspective of the system. It still remains one of the open issues to study multiuser transmissions in terms of secrecy sum-rate scaling with respect to the number of users in the system whereas there have been several studies on multiuser transmissions in conventional network settings without eavesdroppers. Adopting multiple antennas at the receiver requires a proper post-processing technique such as zero-forcing or minimum-mean-square-estimation (MMSE) receivers [26,27]. In multiuser networks, orthogonal random beamforming [28] is also widely used for multiuser transmissions since it achieves the optimal rate scaling by fully exploiting MUD gain. In wireless secure communications, orthogonal random beamforming was utilized with opportunistic scheduling to improve the secrecy performance [29]. The authors of [29] considered downlink multiuser networks (i.e., broadcast channel) since orthogonal random beamforming was originally proposed for a transmitter. According to the uplink (i.e., multiple access channel) and downlink duality, orthogonal random beamforming can also be applied at the receiver. Analyzing the sum-rate scaling in uplink networks was previously investigated in [30] by adopting orthogonal random beamforming at receivers in conventional wireless multiuser networks. However, to the best of our knowledge, it is the first trial to study the secrecy sum-rate scaling in wireless multiuser uplink networks where independent multiple eavesdroppers exist. Thus, studying wireless secure communications by adopting orthogonal random beamforming at receiver represents an interesting problem.

The development of 6G networks promises many opportunities and advancements. One of the main features of 6G networks is the massive number of devices and enhanced security and privacy protection. Accordingly, in this paper, we tackle a PLS problem considering wireless multiuser networks which consist of N transmitters (users or IoT devices), a single desired receiver (base station), and M eavesdroppers. To be specific, we characterizes the asymptotic behavior of secrecy sum-rate scaling in multiuser networks, applicable to future 6G applications such as massive IoT scenarios and military satellite communications. Our main contributions are summarized as follows:

- We propose an opportunistic user scheduling scheme, which achieves optimal MUD gain, combined with a power control mechanism for reducing information leakage to eavesdroppers in wireless multiuser networks;
- We prove that the achievable secrecy sum-rate scales as $M \log(\text{SNR} \log N)$ when the number of users scales as $\text{SNR}^{\frac{M(K-1)+1}{1-\epsilon_0}}$ for a constant $\epsilon_0 > 0$ in high signal-to-noise ratio (SNR) regime when we consider M antennas at the receiver and each eavesdropper, respectively;
- We evaluate our analytic result of the proposed scheduling scheme with a power control mechanism through simulations in two eavesdropping scenarios: internal and external eavesdropping environments;
- We further discuss the extensibility of our analysis to various applications such as massive IoT scenarios and military satellite communications in future 6G networks.

The rest of this paper is organized as follows. In Section 2, the overall system model is presented. Our proposed scheduling procedure and power control mechanism are described in Section 3. Secrecy sum-rate scaling of the proposed scheduling scheme is analyzed in Section 4. The performance of the proposed scheduling scheme is verified through simulations in Section 5. Finally, conclusive remarks and future work are provided in Section 7.

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. $\mathbf{I}_M$ represents an M by M 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. We also consider complexity analysis notations. $f(x) = \mathcal{O}(g(x))$ indicate that there exist constants C and c such that $f(x) \leq Cg(x)$ for all $x > c$. $f(x) = \Theta(g(x))$ indicate $f(x) = \mathcal{O}(g(x))$ and $g(x) = \mathcal{O}(f(x))$ [31].

2. System Model

In this section, we introduce system parameters, basics of random beamforming, and two eavesdropping scenarios.

2.1. System Parameters

As illustrated in Figure 1, we consider a time-division duplexing (TDD) uplink multiuser network which consists of N transmitters (users or IoT devices), a single desired receiver (base station: BS), and K independent eavesdroppers. We assume that each transmitter is equipped with a single antenna, and base station and each eavesdropper have M antennas, respectively. 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 transmitters are scheduled for data transmission. Thus, it can be modeled by a single-input and multiple-output (SIMO) multiple access channel (MAC).

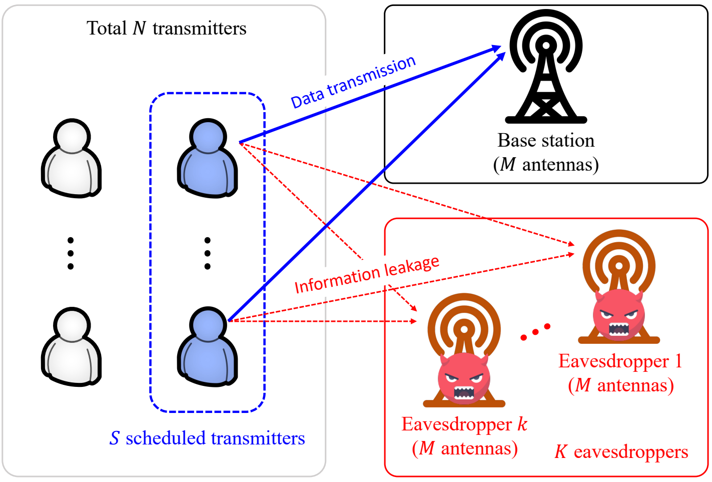

Figure 1. An uplink multiuser network consisting of N users (S scheduled transmitters for data), a single base station and K eavesdroppers: the SIMO MAC model.

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. The term $\mathcal{N}_S$ denotes a selected user index set with $|\mathcal{N}_S| = S$.

2.2. Random Beamforming at Receiver

We adopt random beamforming at a desired receiver for decoding the signal from the selected S users [28]. For each time slot, the base station constructs beamforming vectors represented by an $M \times S$ matrix,

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

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 Section 3.

2.3. Achievable Secrecy Sum-Rate

It is difficult to accurately analyze an individual secrecy capacity region in wireless multiuser networks. Instead, we consider secrecy sum-rate as in [29]. Specially, we use a lower bound of the achievable secrecy sum-rate. For analytical simplicity, 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

$$\mathbf{y} = \sum_{s\in\mathcal{N}_S} \mathbf{h}_s x_s + \mathbf{z}, \tag{2}$$

$$\mathbf{y}_k = \sum_{s\in\mathcal{N}_S} \mathbf{g}_{sk} x_s + \mathbf{z}_k, \tag{3}$$

where x_s denotes the desired data symbol for the s-th transmitter among selected S transmitters (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 independent and identically distributed and circularly symmetric complex additive white Gaussian noise vectors with zero mean and covariance of $\sigma_0^2\mathbf{I}_M$ and $\sigma_e^2\mathbf{I}_M$, respectively. For analytical tractability, we assume $\sigma_0^2 = \sigma_e^2$.

Note that the achievable secrecy sum-rate is obtained based on the sum of secrecy rates between main channel (transmitters and base station) and wiretap channel (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 Equation (2) by using receive random beamforming based on Equation (1) and, the achievable rate of each transmitter and base station pair in the main channel is given by

$$r_{\mathrm{BS}}^{[s]} = \log\left(1 + \frac{|\mathbf{u}_0^{[s]T}\mathbf{h}_{\pi_s}|^2\rho}{1+\sum_{l=1,l\neq s}^{S}|\mathbf{u}_0^{[l]T}\mathbf{h}_{\pi_l}|^2\rho}\right), \tag{4}$$

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

Note that all signals except the desired signal of the scheduled transmitter for a beam index s in Equation (2) are considered interference and, thus, it is represented as denominators in the logarithm function in Equation (4).

For the wiretap channel, we consider two eavesdropping scenarios: internal and external eavesdropping scenarios [32]. Depending on eavesdropping scenarios, the achievable secrecy sum-rate is differently defined, discussed in the next subsection.

2.3.1. Internal Eavesdropping Scenario

Eavesdroppers are assumed to be internal nodes such as compromised base stations. Thus, we assume that eavesdroppers operate same as the base station and thus use the receive random beamforming technique. Similar to the desired base station, each eavesdropper independently decodes its received signal in (3) 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

$$\begin{aligned} r_{\mathrm{Int}}^{[s]} &= \max_{k\in\mathcal{K}}\left\{\log\left(1+\frac{|\mathbf{u}_k^{[s]T}\mathbf{g}_{\pi_s k}|^2\rho}{1+\sum_{l=1,l\neq s}^{S}|\mathbf{u}_k^{[l]T}\mathbf{g}_{\pi_l k}|^2\rho}\right)\right\} \\ &= \log\left(1+\max_{k\in\mathcal{K}}\left\{\frac{|\mathbf{u}_k^{[s]T}\mathbf{g}_{\pi_s k}|^2\rho}{1+\sum_{l=1,l\neq s}^{S}|\mathbf{u}_k^{[l]T}\mathbf{g}_{\pi_l k}|^2\rho}\right\}\right), \end{aligned} \tag{5}$$

where subscript 'Int' indicates an internal eavesdropping scenario, $\mathcal{K}$ 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. (5) is represented as maximum of each eavesdropper's achievable rate among K eavesdroppers since we assume each eavesdropper operates independently.

Therefore, for internal eavesdropping, the achievable secrecy sum-rate is given by

$$R_{\mathrm{Int}}^{\mathrm{sec}} = \sum_{s}^{S}\left[r_{\mathrm{BS}}^{[s]} - r_{\mathrm{Int}}^{[s]}\right]^{+}, \tag{6}$$

where $r_{\mathrm{BS}}^{[s]}$ and $r_{\mathrm{Int}}^{[s]}$ are defined in (4) and (5), respectively.

2.3.2. External Eavesdropping Scenario

Eavesdroppers are assumed to be external nodes and their receiving operations are not restricted to the receive random beamforming technique. Generally, we consider the worst case (i.e., the best performance at the eavesdroppers) when the eavesdroppers' capabilities are not specifically revealed. Thus, we assume that the eavesdroppers exploit an ideal receiving signal processing (i.e., a theoretically optimal receiver) and achieve their channel capacity to intercept the information from desired transmitters. In this case, information leakage by all eavesdroppers (i.e., the achievable rate by eavesdroppers) is given by

$$r_{\text{Ext}}^{[s]} = \max_{k \in \mathcal{K}} \left\{ \log\left(1 + \|\mathbf{g}_{sk}\|^2 \rho\right) \right\} = \log\left(1 + \max_{k \in \mathcal{K}} \left\{ \|\mathbf{g}_{sk}\|^2 \right\} \rho\right), \tag{7}$$

where subscript 'Ext' indicates an external eavesdropping scenario.

Similar to internal eavesdropping, the achievable secrecy sum-rate in the case of external eavesdropping is given by

$$R_{\text{Ext}}^{\text{sec}} = \sum_{s}^{S} \left[r_{\text{BS}}^{[s]} - r_{\text{Ext}}^{[s]} \right]^+, \tag{8}$$

where $r_{\text{BS}}^{[s]}$ and $r_{\text{Ext}}^{[s]}$ are defined in (4) and (7), respectively.

3. Opportunistic User Scheduling with Information-Hiding Power Control

In this section, we define the scheduling parameters and describe the overall procedure of the proposed opportunistic scheduling scheme with information-hiding power control.

3.1. Scheduling Parameters

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

$$\eta_{\text{Q}}^{[n,l^*]} \triangleq |\mathbf{u}_0^{[l^*]T} \mathbf{h}_n|^2, \tag{9a}$$

$$\eta_{\text{I}}^{[n,l^*]} \triangleq \sum_{l=1, l \neq l^*}^{S} |\mathbf{u}_0^{[l]T} \mathbf{h}_n|^2, \tag{9b}$$

$$\eta_{\text{L}}^{[n]} \triangleq \max_{k \in \mathcal{K}} \|\mathbf{g}_{nk}\|^2, \tag{9c}$$

where $\eta_{\text{Q}}^{[n,l^*]}$, $\eta_{\text{I}}^{[n,l^*]}$, and $\eta_{\text{L}}^{[n]}$ indicate 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 the wiretap channel, 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.

If we assume the internal eavesdroppers are compromised base stations in the network, it is feasible to acquire channel state information (CSI) of the eavesdroppers. However, it is hard for each user to acquire CSI of the eavesdroppers if eavesdroppers are external nodes. Even in this case, assuming CSI of the eavesdroppers at each user is still meaningful since it provides the theoretical intuitions on the achievable secrecy sum-rate. Including [19,22,29], lots of previous studies assumed the perfect CSI of eavesdroppers.

Note that $\eta_{\text{L}}^{[n]}$ in (9c) only depends on transmitter index n since the expected scheduling beam index l^* in main channel does not affect information leakage in wiretap channel. In addition, regardless of eavesdropping scenarios, we consider the same scheduling metric for information leakage in wiretap channel. Further, the optimal values of $\eta_{\text{I}}^{\star}$ and $\eta_{\text{L}}^{\star}$ can be obtained through simulation based on system parameters such as N, K, M, and S.

3.2. Overall Scheduling Procedure

The entire procedure of proposed scheduling and power control mechanism is described in Figure 2.

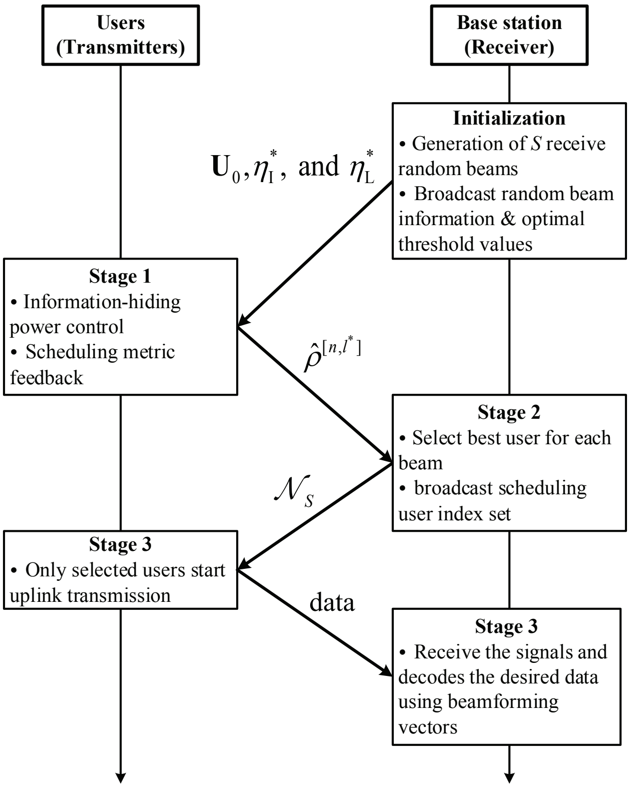
Users (Transmitters)
Base station (Receiver)
Initialization
• Generation of S receive random beams
• Broadcast random beam information & optimal threshold values
$\mathbf{U}_0, \eta_\mathrm{I}^*$, and η_L^*
Stage 1
• Information-hiding power control
• Scheduling metric feedback
$\hat{\rho}^{[n,l^*]}$
Stage 2
• Select best user for each beam
• broadcast scheduling user index set
$\mathcal{N}_S$
Stage 3
• Only selected users start uplink transmission
data
Stage 3
• Receive the signals and decodes the desired data using beamforming vectors

Figure 2. The overview of the proposed scheduling process and power control mechanism.

3.2.1. **Initialization** (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 broadcasts the information of $\mathbf{U}_0$, $\eta_\mathrm{I}^\star$ and $\eta_\mathrm{L}^\star$ to all transmitters (users or IoT devices).

3.2.2. **Stage 1** (Information-Hiding Power Control Based on Scheduling Parameters & Feedback Information)

For given an expected scheduling beam index l^*, each transmitter estimates its scheduling parameters in (9) and compares them with $\eta_\mathrm{I}^\star$ and $\eta_\mathrm{L}^\star$. If estimated generating interference or information leakage exceeds the maximum allowable level of the system, i.e., $\eta_\mathrm{I}^{[n,l^*]} \geq \eta_\mathrm{I}^\star$ or $\eta_\mathrm{L}^{[n]} \geq \eta_\mathrm{L}^\star$, transmitter adjusts its transmit power for satisfying the threshold values ($\eta_\mathrm{I}^\star$ and $\eta_\mathrm{L}^\star$). Therefore, for n-th transmitter with an expected scheduling beam index l^*, its transmit power is determined as

$$P^{[n,l^*]} = \min\left\{1, \frac{\eta_\mathrm{I}^{[n,l^*]}}{\eta_\mathrm{I}^\star}, \frac{\eta_\mathrm{L}^{[n]}}{\eta_\mathrm{L}^\star}\right\} \times P_0. \tag{10}$$

Note that the main objective of power control in (10) is to hide transmitter's information to other receive beams and eavesdroppers by decreasing transmit power which is upper bounded by the maximum transmit power P_0. The concept of using power control in the opportunistic user scheduling was introduced in [33] without considering eavesdroppers (i.e., conventional wireless multiuser networks).

The effective SNR of l^*-th receive beam for n-th user is defined as

$$\hat{\rho}^{[n,l^*]} \triangleq \frac{\eta_{\mathrm{Q}}^{[n,l^*]} \times P^{[n,l^*]}}{\sigma_0^2}, \tag{11}$$

which is fed back from each transmitter to the base station as a scheduling metric. For each user, feedback information in (11) can be calculated for all beam indices to provide accurate scheduling metrics or for some selected beam indices to reduce feedback overhead. Proper beam indices can be selected by using pre-determined positive threshold value (e.g., $\eta_{\mathrm{Q}}^{\star}$) which is determined at the base station for guaranteeing the minimum signal quality. Each transmitter finds the index $l^* \in \{1, \cdots, S\}$ satisfying $\eta_{\mathrm{Q}}^{[n,l^*]} \geq \eta_{\mathrm{Q}}^{\star}$.

3.2.3. **Stage 2** (User Selection)

After receiving N transmitter's feedback information, the base station selects the best S transmitters corresponding to S receive vectors and broadcast scheduling transmitter index set to all transmitters. The Hungarian method [34] is one of the possible candidate algorithms for assigning the best transmitters to the receive beams.

3.2.4. **Stage 3** (Uplink Communication and Post-Processing at Receiver)

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.

4. Secrecy Sum-Rate Scaling Analysis

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 (It means optimal degree-of-freedom gain M and multiuser diversity gain $\log\log N$ can be achieved.), 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 sum-rate scaling.

We investigate a lower bound of the achievable secrecy sum-rate and prove the optimal secrecy sum-rate scaling using the lower bound. Note that we have $R_{\mathrm{Int}}^{\mathrm{sec}} \geq R_{\mathrm{Ext}}^{\mathrm{sec}}$ since we do not limit eavesdroppers' capability in the case of the external eavesdropping scenario. Further, the lower bound of $R_{\mathrm{Ext}}^{\mathrm{sec}}$ is given by

$$\begin{aligned} R_{\mathrm{Ext}}^{\mathrm{sec}} = \sum_{s}^{S}\left[r_{\mathrm{BS}}^{[s]} - r_{\mathrm{Ext}}^{[s]}\right]^{+} &\geq \left[\sum_{s}^{S} r_{\mathrm{BS}}^{[s]} - \sum_{s}^{S} r_{\mathrm{Ext}}^{[s]}\right]^{+} \\ &= \left[R_{\mathrm{BS}}^{\mathrm{sum}} - R_{\mathrm{Ext}}^{\mathrm{sum}}\right]^{+} \\ &\geq \left[R_{\mathrm{BS}}^{\mathrm{sum}} - \max_{k\in\mathcal{K}}\left\{\log\det\left(\mathbf{I}_M + \rho\sum_{s\in\mathcal{N}_S}\mathbf{g}_{sk}\mathbf{g}_{sk}^{H}\right)\right\}\right]^{+} \\ &= \left[R_{\mathrm{BS}}^{\mathrm{sum}} - C_{\mathrm{Ext}}^{\mathrm{sum}}\right]^{+} \\ &\geq R_{\mathrm{BS}}^{\mathrm{sum}} - C_{\mathrm{Ext}}^{\mathrm{sum}}, \end{aligned} \tag{12}$$

where $C_{\mathrm{Ext}}^{\mathrm{sum}}$ denotes $\max_{k\in\mathcal{K}}\left\{\log\det\left(\mathbf{I}_M + \rho\sum_{s\in\mathcal{N}_S}\mathbf{g}_{sk}\mathbf{g}_{sk}^{H}\right)\right\}$ and $R_{\mathrm{BS}}^{\mathrm{sum}}$ and $R_{\mathrm{Ext}}^{\mathrm{sum}}$ denote $\sum_{s}^{S} r_{\mathrm{BS}}^{[s]}$ and $\sum_{s}^{S} r_{\mathrm{Ext}}^{[s]}$, respectively. In (12), the first and the third inequalities hold due to characteristics of $[\cdot]^{+}$ function and the second inequality holds since we have $C_{\mathrm{Ext}}^{\mathrm{sum}} \geq R_{\mathrm{Ext}}^{\mathrm{sum}}$. Thus, we consider $R_{\mathrm{BS}}^{\mathrm{sum}} - C_{\mathrm{Ext}}^{\mathrm{sum}}$ instead of $R_{\mathrm{Ext}}^{\mathrm{sec}}$ during the main proof.

Next, we consider a slightly modified version of the proposed scheduling algorithm to prove the achievability of the optimal secrecy sum-rate scaling. We do not consider power control mechanism in the modified version. Instead, the modified scheduling scheme only utilizes the information of transmitter index n and beam index l^* satisfying the following scheduling criteria:

$$\begin{aligned} &(\mathbf{C1}) \quad \eta_{\mathrm{Q}}^{[n,l^*]} \geq \eta_{\mathrm{Q}}^{\star}, \\ &(\mathbf{C2}) \quad \eta_{\mathrm{I}}^{[n,l^*]} \leq \eta_{\mathrm{I}}^{\star}, \\ &(\mathbf{C3}) \quad \eta_{\mathrm{L}}^{[n]} \leq \eta_{\mathrm{L}}^{\star}, \end{aligned} \tag{13}$$

where $\eta_{\mathrm{Q}}^{[n,l^*]}$, $\eta_{\mathrm{I}}^{[n,l^*]}$, and $\eta_{\mathrm{L}}^{[n]}$ are defined in (9).

Definitely, the modified scheduling scheme shows degraded performance compared with the original proposed scheduling scheme since the modified version does not utilize all transmitters in the system. 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 (13) with high probability and next verify the optimal secrecy sum-rate scaling. We introduce the following lemma 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 $\lim_{x\to\infty} xf(x) \to \infty$.*

Proof. If $\lim_{x\to\infty} xf(x) \to \infty$, then it follows that $f(x) = \omega(\frac{1}{x})$ [31], 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 $\lim_{x\to\infty} xf(x)$ is finite, then there exists a constant $c_3 > 0$ such that $xf(x) < c_3$ 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. □

Let $p^{[l^*]}$ denote a probability that at least one transmitter satisfying all criteria in (13) for l^*-th beam. To analyze $p^{[l^*]}$, we characterize the probability 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 since we assume i.i.d. channel vectors. In other words, $\Pr(\mathbf{C1})$, $\Pr(\mathbf{C2})$, or $\Pr(\mathbf{C3})$ are the same regardless of the transmitter index $n \in \{1, \cdots, N\}$ and beam index $l^* \in \{1, \cdots, M\}$. First, $\Pr(\mathbf{C1})$ is given by

$$\Pr(\mathbf{C1}) \triangleq \Pr\left\{|\mathbf{u}_0^{[l^*]T}\mathbf{h}_n|^2 \geq \eta_{\mathrm{Q}}^{\star}\right\} = e^{-\eta_{\mathrm{Q}}^{\star}}, \tag{14}$$

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 [28].

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

$$\begin{aligned} \Pr(\mathbf{C2}) &\triangleq \Pr\left\{\sum_{l=1,l\neq l^*}^{S} |\mathbf{u}_0^{[l]T}\mathbf{h}_n|^2 \leq \eta_{\mathrm{I}}^{\star}\right\} \\ &= \frac{\gamma(S-1, \eta_{\mathrm{I}}^{\star}/2)}{\Gamma(S-1)}, \end{aligned} \tag{15}$$

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 (15), 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 [35].

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

$$\begin{aligned}\Pr(\mathbf{C3}) &\triangleq \Pr\left\{\max_{k\in\mathcal{K}}\|\mathbf{g}_{nk}\|^2 \le \eta_{\mathrm{L}}^{\star}\right\}\\ &= \left(\frac{\gamma(M,\eta_{\mathrm{L}}^{\star}/2)}{\Gamma(M)}\right)^K,\end{aligned} \tag{16}$$

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 [35], the term $\max_{k\in\mathcal{K}}\|\mathbf{g}_{nk}\|^2$ is distributed as $\left(\frac{\gamma(M,\eta_{\mathrm{L}}^{\star}/2)}{\Gamma(M)}\right)^K$.

Additionally, $\Pr(\mathbf{C2})$ and $\Pr(\mathbf{C3})$ can be lower-bounded by using the following lemma.

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

$$\gamma(z,x) \ge \frac{1}{z}x^z e^{-1}. \tag{17}$$

Proof. The inequality in (17) holds since

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

which completes the proof. □

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 a secrecy sum-rate scaling of $\Theta(M\log(\rho\log N))$ with high probability when*

$$N = \Theta\left(\rho^{\frac{M(K-1)+1}{1-\epsilon_0}}\right), \tag{18}$$

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

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 (13) 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

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

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

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

$$\lim_{N\to\infty} N e^{-\eta_{\mathrm{Q}}^{\star}} F_{\mathrm{C2}}(\eta_{\mathrm{I}}^{\star}) F_{\mathrm{C3}}(\eta_{\mathrm{L}}^{\star}) \to \infty. \tag{19}$$

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

$$\begin{aligned} F_{\mathrm{C2}}(\eta_{\mathrm{I}}^{\star}) &\geq c_1 (\eta_{\mathrm{I}}^{\star})^{S-1}, \\ F_{\mathrm{C3}}(\eta_{\mathrm{L}}^{\star}) &\geq c_2 (\eta_{\mathrm{L}}^{\star})^{MK}, \end{aligned} \tag{20}$$

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 (20), the term in (19) can be lower-bounded by

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

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

It remains to be shown that the achievable secrecy sum-rate scales $\Theta(M\log(\rho\log N))$. From (12), 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, from (12), an upper bound of the sum-rate of wiretap channel with external eavesdropping is given by

$$\begin{aligned} C_{\mathrm{Ext}}^{\mathrm{sum}} &= \max_{k\in\mathcal{K}}\left\{\log\det\left(\mathbf{I}_M + \rho\sum_{s\in\mathcal{N}_S}\mathbf{g}_{sk}\mathbf{g}_{sk}^H\right)\right\} \\ &\leq M\log(1+\eta_{\mathrm{L}}^{\star}\rho) = M\log(2). \end{aligned}$$

Therefore, secrecy sum-rate is lower-bounded by

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

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. □

Remark 1. *Regardless of eavesdropping scenario, our proposed scheme achieves secrecy sum-rate scaling as* $\Theta(M\log(\rho\log N))$ *since we consider* $\max_{k\in\mathcal{K}}\|\mathbf{g}_{nk}\|^2$ *as a scheduling metric for restricting the maximum information leakage level. However, the actual performance will be different* *depending on eavesdropping scenarios because secrecy sum-rate scaling is an asymptotical analysis metric as N tends to infinity. It will be verified through simulation results in Section 5.*

Remark 2. *When $M = 1$, our system model is reduced to single-input and single-output (SISO) system with multiple single antenna equipped eavesdroppers. Thus, our scaling law is reduced by $N = \Theta\left(\rho^{\frac{M(K-1)+1}{1-\epsilon_0}}\right) = \Theta\left(\rho^{\frac{K}{1-\epsilon_0}}\right)$. This result exactly agrees with the previous result in [19] (i.e., $\rho^{\frac{K}{1-\epsilon_0}}$). Therefore, our result generalizes the conventional scaling law in [19].*

5. Numerical Results

In this section, we evaluate the performance of our proposed schemes in terms of the achievable secrecy sum-rate through simulations for two different eavesdropping scenarios: internal eavesdropping and external eavesdropping scenarios. To observe the effect of the power control mechanism on the secrecy sum-rate, we also consider the proposed scheme without adopting the power control mechanism. Our proposed schemes refer to *IHPC* for the proposed scheme with the power control mechanism (IHPC: Information Hiding Power Control) and *TOS* for the proposed scheme without the power control mechanism (TOS: Threshold-based Opportunistic Scheduling), respectively. Additionally, we consider three conventional user scheduling schemes as references: *MaxSNR*, *MinGI*, and *OS-MRC*. *MaxSNR* indicates a user scheduling scheme that selects the transmitters having the maximum desired signal strength to each beam. Contrary to *MaxSNR*, *MinGI* is a user scheduling scheme that selects the transmitters generating a minimum amount of interference to other beams. *OS-MRC* represents a threshold-based opportunistic scheduling with a maximum ratio combining scheme instead of random beamforming at the receiver, as proposed in [21]. Note that although some recent studies in PLS [24] show a higher achievable secrecy rate than our proposed scheme, direct comparison with our scheme is difficult since those studies consider additional system elements such as RIS elements.

Remark 3. *Similarly to the proposed schemes, MaxSNR and MinGI select multiple transmitters by adopting random beamforming at receiver (i.e., $S = M$). However, OS-MRC selects only one user in one time slot (i.e., $S = 1$). Additionally, metrics for scheduling and power control criteria (i.e., $\eta_I^\star$ and $\eta_L^\star$) is optimized for the given system parameters M, N and K.*

5.1. Results in Internal Eavesdropping Scenario

In an internal eavesdropping scenario, eavesdroppers are assumed to be internal nodes such as compromised base stations. Thus, we assume that the eavesdroppers operate in the same way as the base station does. Except for the case of *OS-MRC*, eavesdroppers are assumed to use receive random beamforming at receivers. In case of *OS-MRC*, we assume eavesdroppers adopt MRC at the receivers.

Figure 3 shows the average achievable secrecy sum-rate for varying the number of users, where system parameters are set as $M = 2$, $K = 2$, and $\rho = 10$ dB. Both *IHP* and *TOS* outperform conventional schemes. Comparing *IHP* with *TOS*, the performance gain for using power control is very marginal. This indicates that there are enough users satisfing (13) without using power control. In addition, *MaxSNR* and *MinGI* show degraded secrecy performance compared to the proposed schemes 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 schemes and *OS-MRC* since it is hard for eavesdroppers to obtain desired users' information when the eavesdroppers use the receive random beamforming technique.

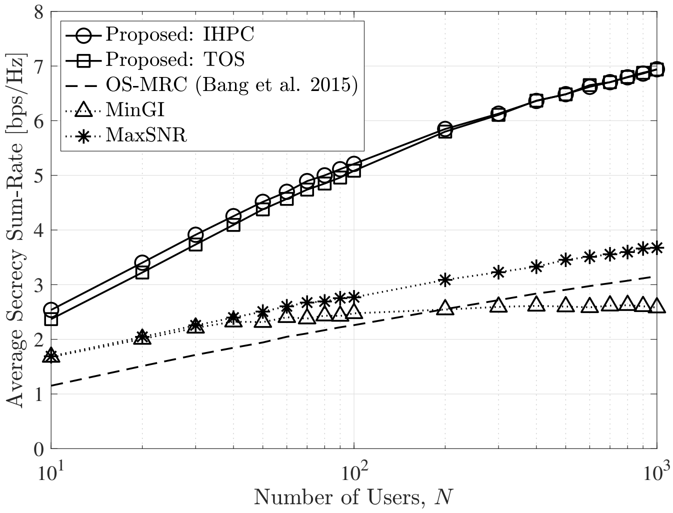

Figure 3. Average achievable secrecy sum-rate for varying the number of users when $M = 2$, $K = 2$, and $\rho = 10$ dB [21].

Figure 4 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 Figure 3, the proposed schemes outperform conventional schemes. Interestingly, *MinGI* shows good secrecy performance in a high SNR regime whereas the secrecy sum-rate of *MaxSNR* is saturated as SNR increases. It indicates that inter-beam interference at desired receiver is dominant factor to determine secrecy sum-rate when the eavesdroppers use random beamforming at the receiver. In addition, when eavesdroppers are assumed to adopt MRC at receivers (*OS-MRC*), information leakage to the eavesdroppers is also a main factor in restricting secrecy rate of the *OS-MRC*.

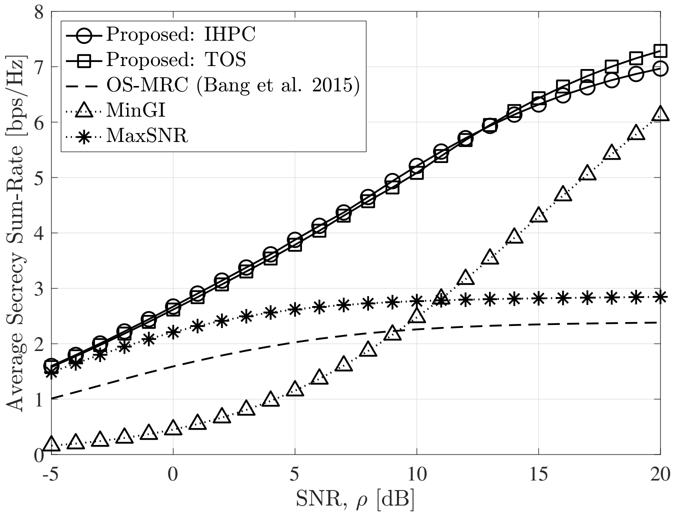

Figure 4. Average achievable secrecy sum-rate for varying SNR when $M = 2$, $N = 100$, and $K = 2$ [21].

Remark 4. *In an internal eavesdropping scenario, the secrecy sum-rate depends on the operations of eavesdroppers. When eavesdroppers use random beamforming at receivers, the amount of information leakage is small since it is hard for eavesdroppers to obtain desired users' information. Thus, a main factor that affects the secrecy sum-rate is inter-beam interference at desired receiver. However, when eavesdroppers are assumed to adopt MRC at receivers (results of OS-MRC), there is no inter-beam interference ($S = 1$) and information leakage is a key factor to restrict secrecy rate.*

5.2. Results in External Eavesdropping Scenario

In an external eavesdropping scenario, eavesdroppers are assumed to be external nodes and their receiving operations are not restricted to the receive random beamforming technique. Thus, we assume that eavesdroppers could achieve their channel capacity for intercepting the information from desired users.

Figure 5 shows the average achievable secrecy sum-rate for varying the number of users, where system parameters are set as $M = 2$, $K = 2$, and $\rho = 10$ dB. Differently from the results of internal eavesdropping scenario, compared to *OS-MRC*, the secrecy performance of the proposed schemes is not good when the number of users is small. In addition, a significant performance gap is shown between *IHP* and *TOS*. These results come from the fact that information leakage is significant in case of external eavesdropping scenario since we assume that eavesdroppers achieve the channel capacity. However, by comparing the slopes of proposed schemes and *OS-MRC*, we observe that proposed schemes still achieve full degrees-of-freedom gain.

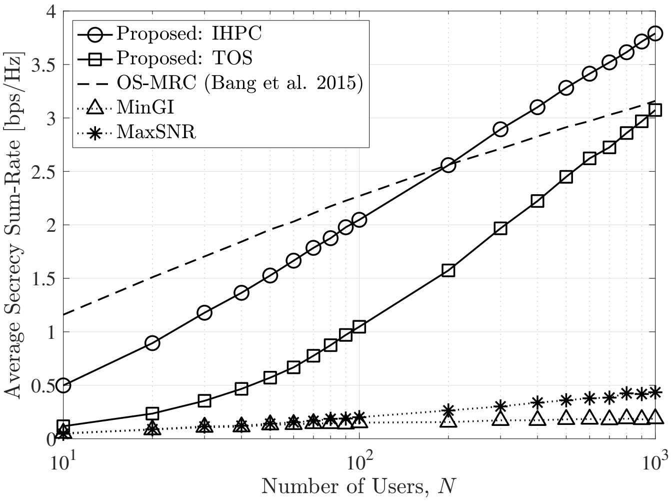

Figure 5. Average achievable secrecy sum-rate for varying the number of users when $M = 2$, $K = 2$, and $\rho = 10$ dB [21].

Figure 6 shows the average achievable secrecy sum-rate for varying SNR, where system parameters are set as $M = 2$, $N = 200$, and $K = 2$. Interestingly, all schemes except for *OS-MRC*, which selects single users ($S = 1$), show performance degradation as SNR increases and secrecy sum-rate finally converges to zero whereas the performance of *OS-MRC* is saturated. Since we assume that eavesdroppers achieve the channel capacity, the capacity between eavesdroppers and users scales as $\log(\rho)$ whereas the sum-rate between users and desired receiver is limited by inter-beam interference. Although both proposed schemes and *OS-MRC* are effectively utilizing multiuser diversity to improve secrecy performance, the proposed schemes require a large number of users than *OS-MRC* since they have to select users having a small amount of information leakage and inter-beam interference at the same time. Specifically, for the proposed schemes, the required number of users to fully exploit the multiuser diversity scales as $\Theta\left(\rho^{\frac{M(K-1)+1}{1-\epsilon_0}}\right) \approx \rho^3$ whereas it scales as ρ^2 in the case of *OS-MRC*. Thus, the proposed schemes show better secrecy performance than *OS-MRC* only in a low SNR regime since we consider a finite number of users (i.e., $N = 100$).

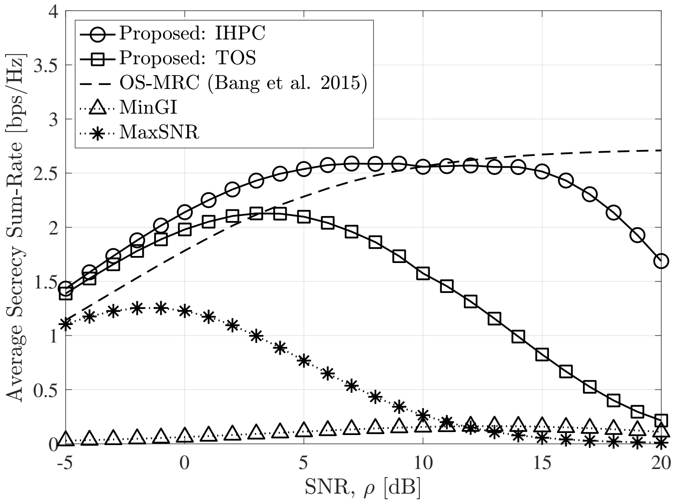

Figure 6. Average achievable secrecy sum-rate for varying SNR when $M = 2$, $N = 200$, and $K = 2$ [21].

Remark 5. *In an external eavesdropping scenario, differently from an internal eavesdropping scenario, the information leakage from the desired user to the eavesdroppers is significant since we assume that eavesdroppers achieve the channel capacity. It results in the severe performance degradation of the proposed schemes compared to OS-MRC. However, the proposed schemes still can achieve the secrecy sum-rate scaling as* $\Theta(M \log(\rho \log N))$ *as the number of users increases.*

6. Discussion

In this section, we discuss the possible extensibility of our analysis and proposed scheme to various applications such as satellite communications and IoT networks.

6.1. IoT Networks

The development of 6G networks promises many opportunities and advancements, particularly in the IoT networks. A massive number of IoT devices and enhanced security and privacy protection are the main features of 6G IoT networks [1,2]. Fortunately, our analysis and proposed opportunistic scheduling schemes can provide wireless network security against eavesdropping attacks by exploiting physical-layer security techniques. Further, the proposed scheme that opportunistically selects multiple transmitters can achieve improved secrecy performance with a high probability when the number of IoT devices increases.

6.2. Satellite Communications

The evolution of wireless communication systems, exemplified by the current 5G technology and the forthcoming 6G advancements, should fulfill significant milestones in terms of enhanced performance, including data rate, latency, reliability, and connectivity. In recent years, satellite communications have been expected to play a crucial role in 5G and 6G networks by offering expansive coverage in several applications such as broadcasting, navigation, and military operations [36]. However, wireless communications, including satellite communication, remain vulnerable to eavesdropping by malicious attackers. Consequently, security and privacy are among the most important design factors in 6G satellite communication systems [37].

Traditionally, advanced encryption algorithms, secure key management protocols, and authentication mechanisms have been studied to safeguard satellite transmissions. Furthermore, in addition to cryptology-based security measures, physical-layer security can significantly bolster the security of satellite communications. Accordingly, our proposed scheduling scheme aims to enhance the secrecy performance of satellite communications by minimizing information leakage to unauthorized nodes. It is worth noting that our proposed scheme is particularly effective as the number of nodes increases.

7. Conclusions

In this paper, we proposed threshold-based opportunistic user scheduling with an information hiding power control mechanism, which achieves secrecy sum-rate scaling as $M\log(\rho\log N)$ when the number of users scales as $\rho^{\frac{M(K-1)+1}{1-\epsilon_0}}$ for a constant $\epsilon_0 > 0$ in a high SNR regime. The secrecy performance of the proposed schemes has been evaluated through simulations in two eavesdropping scenarios: internal and external eavesdropping environments. Although the average achievable secrecy sum-rates of the proposed schemes are different depending on the eavesdropping scenario, simulation results show that the proposed schemes achieve the secrecy sum-rate scaling as $\Theta(M\log(\rho\log N))$ regardless of the eavesdropping scenario when the number of users is sufficiently large. Further, we discussed the possible extensibility of our analysis and proposed scheme to various applications such as satellite communications and IoT networks. In this work, we focused on multiuser SIMO channels in a single-cell environment. The analysis for secrecy sum-rate scaling in various system models (multiuser SIMO channel in a multi-cell environment or multiple-input and multiple-output (MIMO) channel in a single-cell environment) remains for future work.

Author Contributions: Conceptualization, I.B.; formal analysis, I.B.; investigation, S.H.C.; supervision, B.C.J.; project administration, B.C.J.; writing—original draft preparation, I.B.; writing—review and editing, S.H.C. and B.C.J. All authors have read and agreed to the published version of the manuscript.

Funding: This work was 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).

Data Availability Statement: Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

PLS	Physical-Layer Security
6G	Sixth Generation
IoT	Internet of Things
MUD	Multiuser Diversity
SNR	Signal-to-Noise Ratio
AES	Advanced Encryption Standard
DoF	Degrees-of-Freedom
TDD	Time-Division Duplexing
BS	Base Station
SIMO	Single-Input and Multiple-Output
MAC	Multiple Access Channel
CSI	Channel State Information
SISO	Single-Input and Single-Output
IHPC	Information Hiding Power Control
TOS	Threshold-based Opportunistic Scheduling
MIMO	Multiple-Input and Multiple-Output

References

1. Nguyen, D.C.; Ding, M.; Pathirana, P.N.; Seneviratne, A.; Li, J.; Niyato, D.; Dobre, O.; Poor, H.V. 6G Internet of Things: A comprehensive survey. *IEEE Internet Things J.* **2021**, *9*, 359–383. [CrossRef]
2. Giordani, M.; Polese, M.; Mezzavilla, M.; Rangan, S.; Zorzi, M. Toward 6G networks: Use cases and technologies. *IEEE Commun. Mag.* **2020**, *58*, 55–61. [CrossRef]
3. Porambage, P.; Gür, G.; Osorio, D.P.M.; Liyanage, M.; Gurtov, A.; Ylianttila, M. The roadmap to 6G security and privacy. *IEEE Open J. Commun. Soc.* **2021**, *2*, 1094–1122. [CrossRef]

4. Bloch, M.; Barros, J. *Physical-Layer Security: From Information Theory to Security Engineering*; Cambridge University Press: New York, NY, USA, 2011.
5. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
6. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
7. Mitev, M.; Chorti, A.; Poor, H.V.; Fettweis, G.P. What physical layer security can do for 6G security. *IEEE Open J. Veh. Technol.* **2023**, *4*, 375–388. [CrossRef]
8. Khalid, W.; Rehman, M.A.U.; Van Chien, T.; Kaleem, Z.; Lee, H.; Yu, H. Reconfigurable intelligent surface for physical layer security in 6G-IoT: Designs, issues, and advances. *IEEE Internet Things J.* **2023**, *11*, 3599–3613. [CrossRef]
9. Mukherjee, A.; Fakoorian, S.A.A.; Huang, J.; Swindlehurst, A.L. Principles of physical layer security in multiuser wireless networks: A survey. *IEEE Commun. Surv. Tutor* **2014**, *16*, 1550–1573. [CrossRef]
10. Chen, X.; Ng, D.W.K.; Gerstacker, W.H.; Chen, H.H. A survey on multiple-antenna techniques for physical layer security. *IEEE Commun. Surv. Tutor* **2016**, *19*, 1027–1053. [CrossRef]
11. Wu, Y.; Khisti, A.; Xiao, C.; Caire, G.; Wong, K.K.; Gao, X. A survey of physical layer security techniques for 5G wireless networks and challenges ahead. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 679–695. [CrossRef]
12. Jameel, F.; Wyne, S.; Kaddoum, G.; Duong, T.Q. A comprehensive survey on cooperative relaying and jamming strategies for physical layer security. *IEEE Commun. Surv. Tutor.* **2018**. [CrossRef]
13. Koyluoglu, O.O.; El Gamal, H.; Lai, L.; Poor, H.V. Interference alignment for secrecy. *IEEE Trans. Inf. Theory* **2011**, *57*, 3323–3332. [CrossRef]
14. Xie, J.; Ulukus, S. Secure degrees of freedom regions of multiple access and interference channels: The polytope structure. *IEEE Trans. Inf. Theory* **2016**, *62*, 2044–2069. [CrossRef]
15. Chae, S.H.; Bang, I.; Lee, H. Physical layer security of QSTBC with power scaling in MIMO wiretap channels. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5647–5651. [CrossRef]
16. Zou, Y.; Wang, X.; Shen, W. Physical-layer security with multiuser scheduling in cognitive radio networks. *IEEE Trans. Commun.* **2013**, *61*, 5103–5113. [CrossRef]
17. Zou, Y.; Li, X.; Liang, Y.C. Secrecy outage and diversity analysis of cognitive radio systems. *IEEE J. Sel. Areas Commun.* **2014**, *32*, 2222–2236. [CrossRef]
18. An, K.; Liang, T.; Yan, X.; Zheng, G. On the secrecy performance of land mobile satellite communication systems. *IEEE Access* **2018**, *6*, 39606–39620. [CrossRef]
19. Jin, H.; Shin, W.Y.; Jung, B.C. On the multi-user diversity with secrecy in uplink wiretap networks. *IEEE Commun. Lett.* **2013**, *17*, 1778–1781. [CrossRef]
20. Jin, H.; Jung, B.C.; Shin, W.Y. On the secrecy capacity of multi-cell uplink networks with opportunistic scheduling. In Proceedings of the 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, 23–27 May 2016, pp. 1–5.
21. Bang, I.; Kim, S.M.; Sung, D.K. Effects of multiple antennas and imperfect channel knowledge on secrecy multiuser diversity. *IEEE Commun. Lett.* **2015**, *19*, 1564–1567. [CrossRef]
22. Bang, I.; Kim, S.M.; Sung, D.K. Secrecy multiuser diversity for distributed antenna systems from the perspective of user-scaling law. In Proceedings of the 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, 23–27 May 2016, pp. 1–6.
23. Bang, I.; Kim, S.M.; Sung, D.K. Artificial noise-aided user scheduling for optimal secrecy multiuser diversity. *IEEE Commun. Lett.* **2017**, *21*, 528–531. [CrossRef]
24. Xu, P.; Chen, G.; Pan, G.; Di Renzo, M. Ergodic secrecy rate of RIS-assisted communication systems in the presence of discrete phase shifts and multiple eavesdroppers. *IEEE Wirel. Commun. Lett.* **2020**, *10*, 629–633. [CrossRef]
25. Teeti, M.A. Downlink secrecy rate of one-bit massive MIMO system with active eavesdropping. *IEEE Access* **2020**, *8*, 37821–37842. [CrossRef]
26. Veetil, S.T.; Kuchi, K.; Ganti, R.K. Performance of PZF and MMSE receivers in cellular networks with multi-user spatial multiplexing. *IEEE Trans. Wirel. Commun.* **2015**, *14*, 4867–4878. [CrossRef]
27. Chae, S.H.; Jung, B.C.; Choi, W. On the achievable degrees-of-freedom by distributed scheduling in (n,K)-user interference channels. *IEEE Trans. Commun.* **2013**, *61*, 2568–2579. [CrossRef]
28. Sharif, M.; Hassibi, B. On the capacity of MIMO broadcast channels with partial side information. *IEEE Trans. Inf. Theory* **2005**, *51*, 506–522. [CrossRef]
29. Krikidis, I.; Ottersten, B. Secrecy sum-rate for orthogonal random beamforming with opportunistic scheduling. *IEEE Signal Process Lett.* **2012**, *20*, 141–144. [CrossRef]
30. Shin, W.Y.; Park, D.; Jung, B.C. On the multiuser diversity in SIMO interfering multiple access channels: Distributed user scheduling framework. *J. Commun. Netw.* **2015**, *17*, 267–274. [CrossRef]
31. Knuth, D.E. Big Omicron and Big Omega and Big Theta. *ACM SIGACT News* **1976**, *8*, 18–24. [CrossRef]
32. Tekin, E.; Yener, A. The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming. *IEEE Trans. Inf. Theory* **2008**, *54*, 2735–2751. [CrossRef]
33. Cho, M.J.; Ban, T.W.; Jung, B.C.; Yang, H.J. A distributed scheduling with interference-aware power control for ultra-dense networks. In Proceedings of the 2015 IEEE International Conference on Communications (ICC), London, UK, 8–12 June 2015, pp. 1661–1666.

34. Kuhn, H.W. The Hungarian Method for the Assignment Problem. *Nav. Res. Logist. Q.* **1955**, *2*, 83–97. [CrossRef]
35. Papoulis, A.; Hoffman, J.G. *Probability, Random Variables and Stocahstic Processes*; McGraw-Hill: New York, NY, USA, 2002.
36. Giordani, M.; Zorzi, M. Non-terrestrial networks in the 6G era: Challenges and opportunities. *IEEE Netw.* **2020**, *35*, 244–251. [CrossRef]
37. Ahmad, I.; Suomalainen, J.; Porambage, P.; Gurtov, A.; Huusko, J.; Höyhtyä, M. Security of satellite-terrestrial communications: Challenges and potential solutions. *IEEE Access* **2022**, *10*, 96038–96052. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.