entropy

MDPI

Article

A Pseudo-Random Beamforming Technique for Improving Physical-Layer Security of MIMO Cellular Networks

Woong Son [1], Han Seung Jang [2,*] and Bang Chul Jung [1,*]

[1] Department of Electronics Engineering, Chungnam National University, Daejeon 34134, Korea; woongson@cnu.ac.kr

[2] School of Electrical, Electronic Communication and Computer Engineering, Chonnam National University, Yeosu 59626, Korea

* Correspondence: hsjang@jnu.ac.kr (H.S.J.); bcjung@cnu.ac.kr (B.C.J.); Tel.: +82-61-659-7234 (H.S.J.); +82-42-821-6580 (B.C.J.)

Received: 30 August 2019 ; Accepted: 24 October 2019; Published: 25 October 2019

Abstract: In this paper, we propose a pseudo-random beamforming (PRBF) technique for improving physical-layer security (PLS) in multiple input multiple output (MIMO) downlink cellular networks consisting of a legitimate base station (BS), multiple legitimate mobile stations (MSs) and potential eavesdroppers. The legitimate BS can obtain available potential eavesdroppers' channel state information (CSI), which is registered in an adjacent cell. In the proposed PRBF technique, the legitimate BS *pseudo-randomly* generates multiple candidates of the transmit beamforming (BF) matrix, in which each transmit BF matrix consists of multiple orthonormal BF vectors and shares BF information with legitimate MSs before data transmission. Each legitimate MS generates receive BF vectors to maximize the receive signal-to-interference-plus-noise (SINR) for all pseudo-randomly generated transmit beams and calculates the corresponding SINR. Then, each legitimate MS sends a single beam index and the corresponding SINR value of the BF vector that maximizes the received SINR for each BF matrix since a single spatial stream is sent to each legitimate MS. Based on the feedback information from legitimate MSs and the CSI from the legitimate BS to eavesdroppers, the legitimate BS selects the optimal transmit BF matrix and the legitimate MSs that maximizes secrecy sum-rate. We also propose a codebook-based opportunistic feedback (CO-FB) strategy to reduce feedback overhead at legitimate MSs. Based on extensive computer simulations, the proposed PRBF with the proposed CO-FB significantly outperforms the conventional random beamforming (RBF) with the conventional opportunistic feedback (O-FB) strategies in terms of secrecy sum-rate and required feedback bits.

Keywords: pseudo-random beamforming; beam selection; physical-layer security; secrecy capacity; user scheduling; opportunistic feedback

1. Introduction

Security of wireless communication has received much attention from both academia and industry. Secure transmission is significantly important especially for military communications. To define the degree of security of communications, the concept of physical-layer security (PLS) was first defined in [1], and *secrecy capacity* has been used as a metric for PLS performance evaluations, which is defined as the difference between the channel capacity of authorized and unauthorized communication links [2–5].

Recent studies for improving PLS were reviewed and summarized in various multi-user wireless networks environments such as single-user single-antenna wire-tap channel, single-user multi-antenna

wire-tap channel, wire-tap broadcast channel, wire-tap multiple-access channel, wire-tap interference channel, wire-tap relay and cooperative channels, etc. [6]. Several user scheduling algorithms combined with a beamforming (BF) technique were proposed for multi-user wireless networks for enhancing secrecy capacity. Jin et al. [7] showed that the optimal multi-user diversity can be obtained with a threshold-based user scheduling algorithm in a single-cell single-input single output (SISO) uplink wiretap network. In his another study [8], the threshold-based user scheduling algorithm for multi-cell SISO uplink wiretap networks was proposed. An artificial noise (AN)-aided opportunistic user scheduling algorithm was recently proposed for a single multi-user SISO uplink wiretap network with multiple eavesdroppers, where non-scheduled users generate AN in order to improve the PLS [9]. Even though there exist many recent BF techniques with an opportunistic user scheduling algorithm for a single-cell downlink wire-tap network in the literature, most recent studies assumed a single antenna at legitimate MSs and eavesdroppers.

Below are some of recent studies on multi-antenna based BF techniques for improving PLS. In [10], when an imperfect channel state information (CSI) between the legitimate base station (BS) and the eavesdropper is assumed, on–off opportunistic BF technique based on *statistical* CSI was proposed in a single-cell multi-user multiple-input single-output (MISO) downlink wire-tap network. In addition, a random beamforming (RBF) technique was proposed to maximize secrecy sum-rate in a single-cell multi-user MISO downlink network, where the legitimate BS selects a subset of active beams according to system parameters such as the number of users in a cell, the number of transmit antennas at the legitimate BS, and wireless channel conditions [11]. A RBF technique with variable number of active beams, which is similar to the one in [11], was also proposed to minimize secrecy *outage* capacity in a single-cell multi-user MISO downlink network [12]. A maximum signal-to-leakage-and-noise ratio (SLNR)-based BF technique was proposed in multiple input multiple output (MIMO) downlink wiretap networks [13], and, based on SLNR and zero-forcing technique, the BF matrix can be designed to increase the secrecy capacity.

Eavesdroppers are generally defined as passive or active eavesdroppers with respect to their eavesdropping strategies. A passive eavesdropper attempts to eavesdrop the data transmission without another operation [14–16]. However, an active eavesdropper attempts to eavesdrop the data transmission using fake information feedback [15,16]. Some eavesdroppers can also generate jamming signals, interfering with the data transmission of legitimate links [17–21]. They are called potential eavesdroppers, are registered in another cell but unauthorized in the legitimate cell, and can be classified as active eavesdroppers [22–25]. There are some related studies with respect to potential eavesdroppers. In [22], an orthogonal RBF technique with a opportunistic user scheduling algorithm was proposed to improve PLS in a single-cell MISO downlink cellular network where it is assumed that each legitimate MS is wire-tapped by an eavesdropper as a worst-case secrecy scenario. In particular, the authors called the eavesdroppers registered (but unintended) on the legitimate network. In addition, the eavesdroppers are obligated to feed their signal-to-interference-plus-noise ratio (SINR) values to the legitimate BS. Therefore, the authors considered a system model in which potential eavesdroppers exist. In [23], the authors considered potential eavesdropper that have a shorter access distance than legitimate receivers due to wireless channel attenuation. In secrecy wireless information and power transfer (SWIPT) systems, the legitimate transmitter can exploit near potential eavesdroppers' CSI since they are legitimate devices for harvesting power. Then, based on potential eavesdroppers' CSI, the legitimate transmitter can properly transmit to maximize PLS performance requirement of energy harvesting. In [24], the public access point (AP) for downlink transmission does not know which users are eavesdroppers. However, the AP considers only one legitimate user, which is selected for downlink transmission, and the other unscheduled users as potential eavesdroppers. In addition, the authors assumed the non-colluding eavesdroppers model (i.e., the non-cooperative potential eavesdroppers assumption). They also assumed that the secrecy rate only depends on the best CSI among potential eavesdropper. All users' CSIs are estimated at AP by received packet from users. Then, the AP generates the BF vector based on all estimated CSIs

for secure transmission. In [25], the authors considered a multi-user SISO uplink wire-tap network consisting of multiple users with a single antenna and multiple potential eavesdropper with a single antenna. Similar to [24], the authors considered a non-colluding eavesdroppers model. Thus, they considered only one potential eavesdropper, which has best CSI from the scheduled legitimate user. They proposed the optimal user scheduling and threshold-based user scheduling for PLS enhancement and analyzed the secrecy rate according to the proposed scheduling scheme.

There are some related studies with respect to beamforming algorithms for PLS enhancement.

- In [13], the authors considered two wire-tap channel models in different users condition. In multiple-input single-output multi-eavesdropping antennas (MISOME) wiretap network, the authors assumed that all of the wireless channel matrices are known to the legitimate sender with multiple antennas and legitimate receiver with a single antenna. Otherwise, in multi-user multiple-input single-output multi-eavesdropping antennas (MU-MISOME) wire-tap network, the authors also assumed that all of wireless channel matrices are known to the legitimate sender with multiple antennas and multiple legitimate receivers with a single antenna. However, an eavesdropper with multiple antennas only knows the wireless channel matrices from legitimate sender in the above system models. The authors proposed some beamforming algorithms for improving PLS such as a maximum-SLNR-based beamforming algorithm and a zero-forcing beamforming algorithm based on the eavesdropper's CSI in MISOME and MU-MISOME wire-tap networks.
- In [26], the authors originally proposed a novel pseudo-random beamforming (PRBF) technique to maximize the achievable sum-rate in multi-cell downlink cellular networks. Each cell has a BS with multiple antennas and multiple MSs with a single antenna. By announcing an optimal BF candidate among multiple candidates of pseudo-randomly generated BF matrices at the BS coordinator, the multi-cell downlink sum-rate is maximized.
- In [27], the authors proposed a PRBF technique to improve PLS in single-cell downlink cellular networks. In addition, the authors assumed a system model consisting a legitimate BS with multiple antennas, multiple legitimate MSs with a single antenna and a potential eavesdropper with a single antenna. To maximize the achievable secrecy sum-rate in downlink cellular networks consisting of legitimate MSs with a single antenna and a potential eavesdropper, the PRBF technique based on legitimate MSs' feedback information and a potential eavesdropper's CSI is proposed.

The main contributions of this paper are summarized as follows:

- We investigate the secrecy sum-rate in single-cell MIMO downlink cellular networks consisting of a legitimate BS with multiple antennas, legitimate MSs with multiple antennas and eavesdroppers with multiple antennas.
- We also consider the conventional F-FB, opportunistic feedback (O-FB) and newly proposed the codebook-based opportunistic feedback (CO-FB) strategy.
- In addition, we compare the conventional F-FB, O-FB [26,27] and the proposed CO-FB in terms of secrecy sum-rate and required feedback bits (feedback overhead).

The remainder of this paper is organized as follows. In Section 2, we describe the system model of MIMO downlink celluar networks with eavesdroppers In Section 3, we explain the overall procedure of the proposed PRBF technique and also compare the conventional F-FB and O-FB with the proposed CO-FB. Computer simulation results are presented in Section 4. Finally, the conclusions are briefly drawn in Section 5.

2. System Model

Let us consider a TDD MIMO downlink network consisting of a legitimate BS with N_{T} antennas, N_{MS} legitimate MSs with N_{R} antennas, and N_{E} eavesdroppers with N_{R} antennas, as shown in Figure 1.

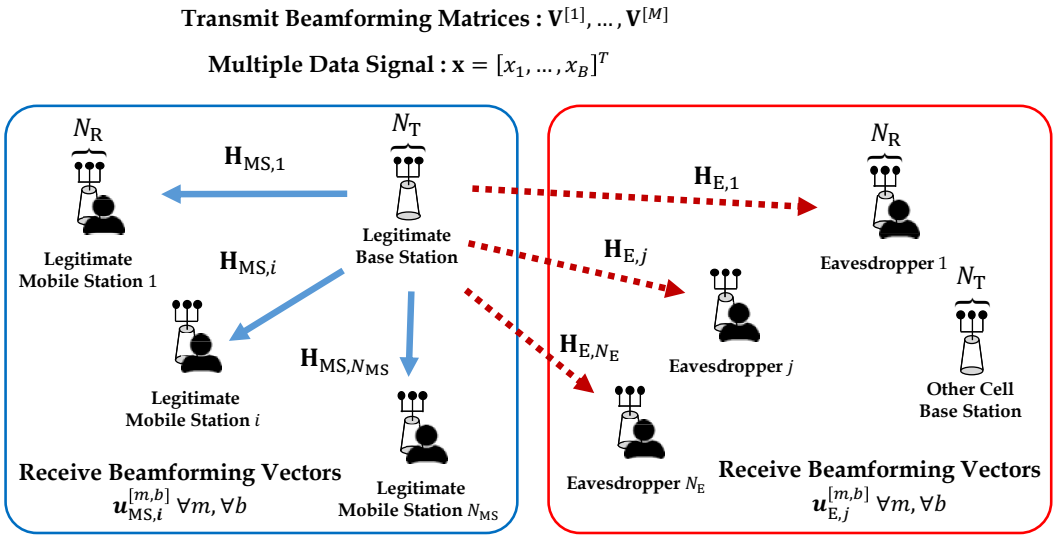

Figure 1. System model of MIMO downlink cellular network.

We assume that the legitimate BS is in the blue box and other cell BSs are in the red box. In particular, legitimate MSs existing in other cells (marked with a red box) can become *potential eavesdroppers* who are unauthorized MSs for the legitimate network in the blue box. We assume the CSI of potential eavesdroppers is available at the legitimate BS, which implies that the legitimate BS is assumed to know the wireless channel from itself to the potential eavesdroppers. This is possible by *overhearing* the pilot signals from the potential eavesdroppers when the eavesdroppers send packets to their own BSs in TDD systems. Thus, each BS can estimate all the channel coefficients from not only the MSs belonging to itself but also the MSs in other cells, which is also known as *local CSI* assumption. Many studies on multi-cell MIMO networks assume the local CSI as well [28–30]. In addition, many previous studies on physical-layer security assume that the legitimate communication nodes know the wireless channel to the eavesdroppers based on local CSI assumption [7,8,25,27]. In addition, we assume that the same frequency band is used for data transmission. All devices are affected by the interference caused by the desired signal from other cells. M candidates of transmit BF matrix are *pseudo-randomly* generated at the legitimate BS. Then, M candidates of transmit BF matrix are represent as $\mathbf{V}^{[1]}, ..., \mathbf{V}^{[M]}$. The mth transmit BF matrix is denoted by $\mathbf{V}^{[m]} = \left[\mathbf{v}^{[m,1]}, ..., \mathbf{v}^{[m,b]}, ..., \mathbf{v}^{[m,B]}\right] \in \mathbb{C}^{N_T \times B}$, where $m \in \mathcal{M} \triangleq \{1, ..., M\}$ and $b \in \mathcal{B} \triangleq \{1, ..., B(= N_T)\}$. $\mathbf{v}^{[m,b]} \in \mathbb{C}^{N_T \times 1}$ represents the bth transmit BF vector in the mth transmit BF matrix. Corresponding to MB transmit BF vectors, each legitimate MS generates MB receive BF vectors based on MMSE. Then, M candidates of receive BF matrix at the ith legitimate MS are represented as $\mathbf{U}_{MS,i}^{[1]}, ..., \mathbf{U}_{MS,i}^{[M]}$, where $i \in \mathcal{N}_{MS} \triangleq \{1, ..., N_{MS}\}$. The mth receive BF matrix at the ith legitimate MS is represented as $\mathbf{U}_{MS,i}^{[m]} = \left[\mathbf{u}_{MS,i}^{[m,1]}, ..., \mathbf{u}_{MS,i}^{[m,b]}, ..., \mathbf{u}_{MS,i}^{[m,B]}\right] \in \mathbb{C}^{N_R \times B}$. In addition, $\mathbf{u}_{MS,i}^{[m,b]} \in \mathbb{C}^{N_R \times 1}$ represents the bth receive BF vector in the mth receive BF matrix at the ith legitimate MS. Similarly, each eavesdropper also generates MB receive BF vectors corresponding MB transmit BF vectors based on MMSE. This assumption is reasonable to consider the worst-case in terms of PLS of legitimate devices. Then, M candidates receive BF matrix at the jth eavesdropper are represented by $\mathbf{U}_{E,j}^{[1]}, ..., \mathbf{U}_{E,j}^{[M]}$, where $j \in \mathcal{N}_E \triangleq \{1, ..., N_E\}$. The mth receive BF matrix at the jth eavesdropper is denoted as $\mathbf{U}_{E,j}^{[m]} = \left[\mathbf{u}_{E,j}^{[m,1]}, ..., \mathbf{u}_{E,j}^{[m,b]}, ..., \mathbf{u}_{E,j}^{[m,B]}\right] \in \mathbb{C}^{N_R \times B}$. $\mathbf{u}_{E,j}^{[m,b]} \in \mathbb{C}^{N_R \times 1}$ denotes the bth receive BF vector in the mth receive BF matrix at the jth eavesdropper. $\mathbf{H}_{MS,i} \in \mathbb{C}^{N_R \times N_T}$ and $\mathbf{H}_{E,j} \in \mathbb{C}^{N_R \times N_T}$ denote the wireless channel matrix from the legitimate BS to ith legitimate MS and the wireless channel matrix from the legitimate BS to jth eavesdropper, respectively.

We assume that wireless channel components are independent and identically distributed (i.i.d.). In addition, we assume that wireless channel components are constant during one block (e.g., one

frame), and large-scale fading components are equal to 1 from the legitimate BS to legitimate MSs and eavesdroppers. The legitimate BS transmits a data signal vector $\mathbf{x} \triangleq [x_1, ..., x_B]^T \in \mathbb{C}^{B\times 1}$, which is satisfied by the power constraint $\mathbb{E}\left[|\mathbf{x}|^2\right] = P$. Without any loss of generality, the received signal vector $\mathbf{y}_{\mathsf{MS},i}^{[m,b]} \in \mathbb{C}^{N_\mathsf{R}\times 1}$ at the ith legitimate MS with the bth transmit BF vector when the legitimate BS transmits a data signal vector $\mathbf{x}$ with the mth transmit BF matrix is given by

$$\mathbf{y}_{\mathsf{MS},i}^{[m,b]} = \mathbf{H}_{\mathsf{MS},i}\mathbf{V}^{[m]}\mathbf{x} + \mathbf{n}_{\mathsf{MS},i} = \mathbf{H}_{\mathsf{MS},i}\mathbf{v}^{[m,b]}x_b + \sum_{l\neq b}^{B}\mathbf{H}_{\mathsf{MS},i}\mathbf{v}^{[m,l]}x_l + \mathbf{n}_{\mathsf{MS},i}, \tag{1}$$

where the additive thermal Gaussian noise vector at the ith legitimate MS is denoted by $\mathbf{n}_{\mathsf{MS},i} \in \mathbb{C}^{N_\mathsf{R}\times 1}$ according to $\mathcal{CN}\left(0, N_0\mathbf{I}_{N_\mathsf{R}}\right)$.

The post-processed received signal $\widetilde{y}_{\mathsf{MS},i}^{[m,b]} \in \mathbb{C}$ with the bth receive BF vector in the mth receive BF matrix is given as

$$\begin{aligned}\widetilde{y}_{\mathsf{MS},i}^{[m,b]} &= \left(\mathbf{u}_{\mathsf{MS},i}^{[m,b]}\right)^H \mathbf{y}_{\mathsf{MS},i}^{[m,b]} \\ &= \left(\mathbf{u}_{\mathsf{MS},i}^{[m,b]}\right)^H \mathbf{H}_{\mathsf{MS},i}\mathbf{v}^{[m,b]}x_b + \left(\mathbf{u}_{\mathsf{MS},i}^{[m,b]}\right)^H \sum_{l\neq b}^{B}\mathbf{H}_{\mathsf{MS},i}\mathbf{v}^{[m,l]}x_l + \left(\mathbf{u}_{\mathsf{MS},i}^{[m,b]}\right)^H \mathbf{n}_{\mathsf{MS},i} \\ &= \widetilde{h}_{\mathsf{MS},i}^{[m,b]}x_b + \left(\mathbf{u}_{\mathsf{MS},i}^{[m,b]}\right)^H \sum_{l\neq b}^{B}\mathbf{h}_{\mathsf{MS},i}^{[m,l]}x_l + \widetilde{n}_{\mathsf{MS},i},\end{aligned} \tag{2}$$

where the desired and interference signals at the ith legitimate MS are represented as the first and second terms on the right side of Equation (2), respectively. The post-processed additive thermal Gaussian noise at the ith legitimate MS follows $\widetilde{n}_{\mathsf{MS},i} \triangleq \left(\mathbf{u}_{\mathsf{MS},i}^{[m,b]}\right)^H \mathbf{n}_{\mathsf{MS},i} \sim \mathcal{CN}(0,1)$. In this case, the post-processed effective channel $\widetilde{h}_{\mathsf{MS},i}^{[m,b]} \in \mathbb{C}$ at the ith legitimate MS is defined as

$$\widetilde{h}_{\mathsf{MS},i}^{[m,b]} \triangleq \left(\mathbf{u}_{\mathsf{MS},i}^{[m,b]}\right)^H \mathbf{h}_{\mathsf{MS},i}^{[m,b]}, \tag{3}$$

where the effective channel vector is given by $\mathbf{h}_{\mathsf{MS},i}^{[m,b]} \triangleq \mathbf{H}_{\mathsf{MS},i}\mathbf{v}^{[m,b]} \in \mathbb{C}^{N_R\times 1}$.

Similarly, the received signal vector $\mathbf{y}_{\mathsf{E},j}^{[m,b]} \in \mathbb{C}^{N_R\times 1}$ at the jth eavesdropper with the bth transmit BF vector when the legitimate BS transmits a data signal vector $\mathbf{x}$ with the mth transmit BF matrix is given by

$$\mathbf{y}_{\mathsf{E},j}^{[m,b]} = \mathbf{H}_{\mathsf{E},j}\mathbf{V}^{[m]}\mathbf{x} + \mathbf{n}_{\mathsf{E},j} = \mathbf{H}_{\mathsf{E},j}\mathbf{v}^{[m,b]}x_b + \sum_{l=1,l\neq b}^{B}\mathbf{H}_{\mathsf{E},j}\mathbf{v}^{[m,l]}x_l + \mathbf{n}_{\mathsf{E},j}, \tag{4}$$

where the additive thermal Gaussian noise vector at the jth eavesdropper is denoted by $\mathbf{n}_{\mathsf{E},j} \in \mathbb{C}^{N_R\times 1}$ following $\mathcal{CN}\left(0, N_0\mathbf{I}_{N_R}\right)$. The post-processed received signal $\widetilde{y}_{\mathsf{E},j}^{[m,b]} \in \mathbb{C}$ with the bth receive BF vector in the mth receive BF matrix is given as

$$\begin{aligned}\widetilde{y}_{\mathsf{E},j}^{[m,b]} &= \left(\mathbf{u}_{\mathsf{E},j}^{[m,b]}\right)^H \mathbf{y}_{\mathsf{E},j}^{[m,b]} \\ &= \left(\mathbf{u}_{\mathsf{E},j}^{[m,b]}\right)^H \mathbf{H}_{\mathsf{E},j}\mathbf{v}^{[m,b]}x_b + \left(\mathbf{u}_{\mathsf{E},j}^{[m,b]}\right)^H \sum_{l\neq b}^{B}\mathbf{H}_{\mathsf{E},j}\mathbf{v}^{[m,l]}x_l + \left(\mathbf{u}_{\mathsf{E},j}^{[m,b]}\right)^H \mathbf{n}_{\mathsf{E},j} \\ &= \widetilde{h}_{\mathsf{E},j}^{[m,b]}x_b + \left(\mathbf{u}_{\mathsf{E},j}^{[m,b]}\right)^H \sum_{l\neq b}^{B}\mathbf{h}_{\mathsf{E},j}^{[m,l]}x_l + \widetilde{n}_{\mathsf{E},j},\end{aligned} \tag{5}$$

where the desired and interference signals at the jth eavesdropper are represented as the first and second terms on the right side of Equation (5), respectively. The post-processed additive thermal

Gaussian noise at the jth eavesdropper follows $\widetilde{n}_{\mathsf{E},j} \triangleq \left(\mathbf{u}_{\mathsf{E},j}^{[m,b]}\right)^H \mathbf{n}_{\mathsf{E},j} \sim \mathcal{CN}(0,1)$. In this case, the post-processed effective channel $\widetilde{h}_{\mathsf{E},j}^{[m,b]} \in \mathbb{C}$ at the jth eavesdropper is defined as

$$\widetilde{h}_{\mathsf{E},j}^{[m,b]} \triangleq \left(\mathbf{u}_{\mathsf{E},j}^{[m,b]}\right)^H \mathbf{h}_{\mathsf{E},j}^{[m,b]}, \tag{6}$$

where the effective channel vector is given by $\mathbf{h}_{\mathsf{E},j}^{[m,b]} \triangleq \mathbf{H}_{\mathsf{E},j}\mathbf{v}^{[m,b]} \in \mathbb{C}^{N_R \times 1}$.

3. Pseudo-Random Beamforming for Improving Physical-Layer Security

In this section, we explain the proposed technique for PLS enhancement in downlink cellular networks in detail. Pseudo-random beamforming algorithm for PLS enhancement, as shown in Algorithm 1.

Algorithm 1: Pseudo-random beamforming algorithm for PLS enhancement.

Initialization
Generate $\mathbf{V}^{[1]}, ..., \mathbf{V}^{[M]}$ at legitimate BS and share transmit BF information with legitimate MSs
Broadcast a pilot signal at legitimate BS
Obtain $\mathbf{h}_{\mathsf{MS},i}$, $\mathbf{h}_{\mathsf{E},j}$ at legitimate MSs and eavesdroppers

Generate of receive BF vectors
Generate $\mathbf{u}_{\mathsf{MS},i}^{[m,b]}$ for all m and b at legitimate MSs
Generate $\mathbf{u}_{\mathsf{E},j}^{[m,b]}$ for all m and b at eavesdroppers

Feedback of SINR values
Feedback the SINRs $\Gamma_{\mathsf{MS},i}^{[m,b]}$ and corresponding b and m at legitimate MSs
Calculate the SINRs $\Gamma_{\mathsf{E},j}^{[m,b]}$ and corresponding b and m of eavesdroppers at legitimate BS

User scheduling
Calculate $\mathsf{R}_{\mathsf{MS}}^{[m]}$ and $\mathsf{R}_{\mathsf{E}}^{[m]}$ for all m at legitimate BS

Data transmission
Transmit data signals $\mathbf{x}$ via $\mathbf{V}^{[\widehat{m}]}$ to maximize the secrecy sum-rate at legitimate BS
Achieve the secrecy sum-rate $\mathsf{R}_{\mathsf{S}}^{[\widehat{m}]}$ for downlink data transmission at legitimate BS

3.1. Initialization

M candidates of transmit BF matrix are generated by the legitimate BS in a *pseudo-random manner*. These candidates are shared with legitimate MSs. After that, to announce a wireless channel vector from the legitimate BS to legitimate MS, the legitimate BS broadcasts a pilot signal.

3.2. Generate of Receive Beamforming Vectors

Legitimate MSs who received a pilot signal generate MB receive BF vectors based on effective channel vector $\mathbf{h}_{\mathsf{MS},i}$. Based on MMSE, the receive BF vector $\mathbf{u}_{\mathsf{MS},i}^{[m,b]}$ corresponding to the bth transmit BF vector in the mth transmit BF matrix for all m and b is given by

$$\mathbf{u}_{\mathsf{MS},i}^{[m,b]} = \frac{\left(N_0\mathbf{I}_{N_R} + \mathbf{R}_{\mathsf{MS},i}^{[m,b]}\right)^{-1}\mathbf{h}_{\mathsf{MS},i}^{[m,b]}}{\left\|\left(N_0\mathbf{I}_{N_R} + \mathbf{R}_{\mathsf{MS},i}^{[m,b]}\right)^{-1}\mathbf{h}_{\mathsf{MS},i}^{[m,b]}\right\|}, \quad \forall m, \forall b, \tag{7}$$

where the interference covariance matrices $\mathbf{R}_{\mathsf{MS},i} \in \mathbb{C}^{N_R \times N_R}$ for all m and b are given by

$$\mathbf{R}_{\mathsf{MS},i}^{[m,b]} = \mathbb{E}\left[\mathbf{y}_{\mathsf{MS},i}\left(\mathbf{y}_{\mathsf{MS},i}\right)^H\right] - \mathbf{h}_{\mathsf{MS},i}^{[m,b]}\left(\mathbf{h}_{\mathsf{MS},i}^{[m,b]}\right)^H - N_0\mathbf{I}_{N_R}, \quad \forall m, \forall b. \tag{8}$$

Similar to the above procedure, by considering worst-case at legitimate devices, eavesdroppers also generate MB received BF vectors based on MMSE, which are given by

$$\mathbf{u}_{\mathsf{E},j}^{[m,b]} = \frac{\left(N_0\mathbf{I}_{N_R} + \mathbf{R}_{\mathsf{E},j}^{[m,b]}\right)^{-1}\mathbf{h}_{\mathsf{E},j}^{[m,b]}}{\left\|\left(N_0\mathbf{I}_{N_R} + \mathbf{R}_{\mathsf{E},j}^{[m,b]}\right)^{-1}\mathbf{h}_{\mathsf{E},j}^{[m,b]}\right\|}, \quad \forall m, \forall b, \tag{9}$$

where the interference covariance matrices $\mathbf{R}_{\mathsf{E},j} \in \mathbb{C}^{N_R \times N_R}$ for all m and b are given by

$$\mathbf{R}_{\mathsf{E},j}^{[m,b]} = \mathbb{E}\left[\mathbf{y}_{\mathsf{E},j}\left(\mathbf{y}_{\mathsf{E},j}\right)^H\right] - \mathbf{h}_{\mathsf{E},j}^{[m,b]}\left(\mathbf{h}_{\mathsf{E},j}^{[m,b]}\right)^H - N_0\mathbf{I}_{N_R}, \quad \forall m, \forall b. \tag{10}$$

3.3. Feedback of SINR Values

The SINR values at the ith legitimate MS for all m and b can be calculated by

$$\Gamma_{\mathsf{MS},i}^{[m,b]} = \frac{\left|\left(\mathbf{u}_{\mathsf{MS},i}^{[m,b]}\right)^H\mathbf{h}_{\mathsf{MS},i}^{[m,b]}\right|^2}{\left(\mathbf{u}_{\mathsf{MS},i}^{[m,b]}\right)^H\left(N_0\mathbf{I}_{N_R} + \mathbf{R}_{\mathsf{MS},i}^{[m,b]}\right)\mathbf{u}_{\mathsf{MS},i}^{[m,b]}}, \quad \forall m, \forall b. \tag{11}$$

Similarly, the SINR values at the jth eavesdropper for all m and b can be calculated at the legitimate BS.

$$\Gamma_{\mathsf{E},j}^{[m,b]} = \frac{\left|\left(\mathbf{u}_{\mathsf{E},j}^{[m,b]}\right)^H\mathbf{h}_{\mathsf{E},j}^{[m,b]}\right|^2}{\left(\mathbf{u}_{\mathsf{E},j}^{[m,b]}\right)^H\left(N_0\mathbf{I}_{N_R} + \mathbf{R}_{\mathsf{E},j}^{[m,b]}\right)\mathbf{u}_{\mathsf{E},j}^{[m,b]}}, \quad \forall m, \forall b. \tag{12}$$

We consider three types of feedback strategies: the conventional *full feedback* (F-FB), the conventional *opportunistic feedback* (O-FB) [26,27], and the proposed *codebook-based opportunistic feedback* (CO-FB) strategy. For the detailed explanations, we assume that the number of required bits to deliver the quantized SINR value is Q bits.

- In the conventional F-FB strategy [26,27], each legitimate MS provides a feedback of the maximal SINR value for all m. Hence, M SINR values are received back at the legitimate BS from each legitimate MS. Then, the number of required feedback bits per legitimate MS is represented as

$$\mathsf{N}_{\mathsf{F\text{-}FB}} = M\left(\lceil \log_2 B \rceil + Q\right). \tag{13}$$

  However, many feedback bits are required. Thus, we consider opportunistic feedback strategies for the reduction of feedback bits.
- In the conventional opportunistic feedback (O-FB) strategy [26,27], each legitimate MS selects $n\ (\leq M)$ maximal SINR values among M transmit BF vectors, where n is a *predetermined* value based on policy before data transmission. n SINR values and beam indices are received back from each legitimate MS. Then, the number of required feedback bits per legitimate MS is represented as

$$\mathsf{N}_{\mathsf{O\text{-}FB}} = n(\lceil \log_2 MB \rceil + Q). \tag{14}$$

- To further reduce the required feedback bits per legitimate MS, the proposed codebook-based opportunistic feedback (CO-FB) strategy can be applied instead of the conventional O-FB with

one-time codebook sharing before data transmission. Each legitimate MS selects the maximal SINR in n transmit BF matrices out of M transmit BF matrix candidates. n SINR values and n codebook indices are received back from each legitimate MS. Then, the number of required feedback bits per legitimate MS is represented as

$$\mathsf{N}_{\mathsf{CO\text{-}FB}} = \lceil \log_2 \binom{M}{n} \rceil + n \left(\lceil \log_2 B \rceil + Q \right). \tag{15}$$

To compare the feedback amount for each feedback strategy, we consider the number of required feedback bits per legitimate MS when the number of candidates of transmit BF matrix M is equal to 16, the number of transmit BF vectors in each transmit BF matrix B is equal to 3, and the number of required bits for the quantized SINR Q is equal to 6 bits. In the conventional F-FB strategy, the number of required feedback bits per legitimate MS can be calculated by $\mathsf{N}_{\mathsf{F\text{-}FB}} = 16 \left(\lceil \log_2 3 \rceil + 6 \right) = 128$ bits. On the other hand, the number of required feedback bits per legitimate MS in the conventional O-FB strategy can be calculated as $\mathsf{N}_{\mathsf{O\text{-}FB}} = 4(\lceil \log_2 16 \times 3 \rceil + 6) = 48$ bits when the predetermined valued is equal to $n = 4$. Furthermore, in the proposed CO-FB strategy, the number of required feedback bits per legitimate MS can be calculated as $\mathsf{N}_{\mathsf{CO\text{-}FB}} = \lceil \log_2 \binom{16}{4} \rceil + 4 \left(\lceil \log_2 3 \rceil + 6 \right) = 43$ bits.

3.4. User Scheduling

Since eavesdroppers' CSI is available at the legitimate BS, the legitimate BS selects the optimal transmit BF matrix based on legitimate MSs' feedback information and eavesdroppers' CSI. In the first step, the legitimate BS selects a legitimate MSs with the maximal SINR value for all b. Then, the achievable sum-rate for all m is given by

$$\mathsf{R}_{\mathsf{MS}}^{[m]} = \sum_{b=1}^{B} \left[\log_2 \left(1 + \max_{1 \le i \le N_{\mathsf{MS}}} \Gamma_{\mathsf{MS},i}^{[m,b]} \right) \right], \forall m. \tag{16}$$

Similarly, the eavesdropping rate due to eavesdropper for all m is given by

$$\mathsf{R}_{\mathsf{E}}^{[m]} = \sum_{b=1}^{B} \left[\log_2 \left(1 + \max_{1 \le j \le N_{\mathsf{E}}} \Gamma_{\mathsf{E},j}^{[m,b]} \right) \right], \forall m. \tag{17}$$

3.5. Data Transmission

In the last step, the legitimate BS transmits a data signal vector $\mathbf{x}$ with the $\widehat{m}$th optimal transmit BF matrix. Thus, the achievable secrecy sum-rate is obtained as

$$\mathsf{R}_{\mathsf{S}}^{[\widehat{m}]} = \left(\mathsf{R}_{\mathsf{MS}}^{[\widehat{m}]} - \mathsf{R}_{\mathsf{E}}^{[\widehat{m}]} \right)^{+}. \tag{18}$$

The achievable secrecy sum-rate can be obtained from both the achievable sum-rate in Equation (16) and the data-loss in Equation (17).

4. Simulation Results

We evaluated the conventional RBF and the proposed PRBF in MIMO downlink cellular network consisting of legitimate MSs and eavesdroppers according to various system parameters such as the number of transmit BF matrix candidates, the number of legitimate MSs, and the predetermined value in the conventional O-FB and the proposed CO-FB. The system parameter definitions are shown in Table 1. We also analyzed the number of required feedback bits at each legitimate MSs with all of considered feedback strategies.

Table 1. System parameters.

Definition	Parameter
Number of antennas at the legitimate BS	N_{T}
Number of antennas at the legitimate MSs and eavesdroppers	N_{R}
Number of legitimate MSs	N_{MS}
Number of eavesdroppers	N_{E}
Number of transmit BF matrix candidates	M
Number of transmit BF vectors in each BF matrix candidate	$B(=N_{\mathsf{T}})$
Number of bits for SINR quantization	Q
Predetermined value in O-FB and CO-FB	n

Figure 2 shows that the secrecy sum-rate according to the number of transmit BF matrix candidates M when the number of eavesdroppers N_{E} is equal to 2, and the number of antennas at legitimate BS N_{T}, the number of antennas of both the legitimate MSs and eavesdroppers N_{R} and the number of transmit BF vectors in each transmit BF matrix candidate B are all equal to 3. In addition, the received SNR at each communication device (legitimate MS or eavesdropper) is equal to 0 dB. When the number of transmit BF matrix candidates is equal to 1, the curves show the secrecy sum-rate of the conventional PRBF. When the number of transmit BF matrix candidates is 2 or more, the curves show the secrecy sum-rate of the proposed PRBF. In addition, we consider the number of legitimate MSs $N_{\mathsf{MS}} = 10$ and 40 cases in all of considered feedback strategies. The conventional O-FB and the proposed CO-FB show the same performance in terms of secrecy sum-rate with the same system parameters. Hence, we only consider the secrecy sum-rate of the proposed CO-FB in the following figures. The secrecy sum-rate increases as the number of transmit BF matrix candidates M increases in the conventional F-FB. In both the conventional O-FB and the proposed CO-FB, as the number of transmit BF matrix candidates M increases, the secrecy sum-rate does not always monotonically increase since the number of legitimate MSs N_{MS} and the predetermined value n are not large enough. However, when the predetermined value n or the number of legitimate MSs N_{MS} are large enough, the proposed CO-FB and the conventional F-FB show almost the same performance in terms of secrecy sum-rate.

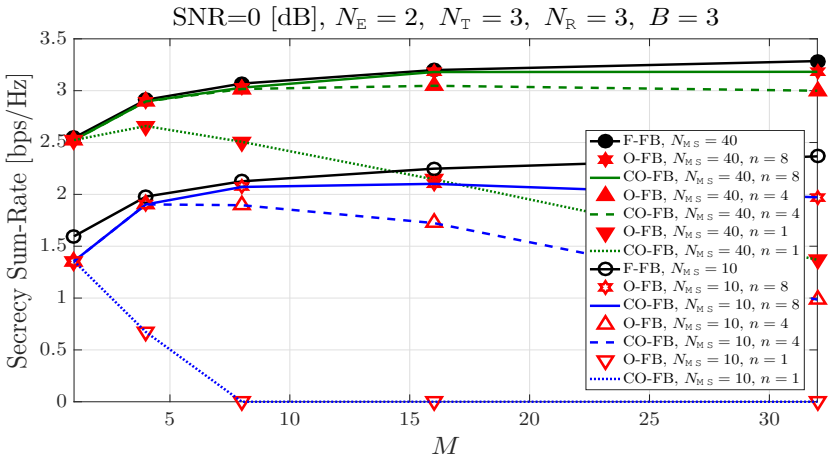

Figure 2. Secrecy sum-rate according to the number of BF candidates.

Figure 3 shows that the secrecy sum-rate according to the number of legitimate MSs N_{MS} when the number of eavesdroppers N_{E} is equal to 2, and the number of antennas at legitimate BS N_{T}, the number of antennas at both of legitimate MSs and eavesdroppers N_{R}, the number of transmit BF vectors in each transmit BF matrix candidate B are all equal to 3. In addition, the received SNR at each communication device is equal to 0 dB.In general, as the number of legitimate MSs N_{MS} increases, the secrecy sum-rate increases in the all of feedback strategies. The proposed CO-FB does not reach the

performance of the conventional F-FB in terms of secrecy sum-rate when the predetermined value n or the number of legitimate MSs N_{MS} are not large enough. When the predetermined value n or the number of legitimate MSs N_{MS} are large enough, the proposed CO-FB and the conventional F-FB show almost the same performance in terms of secrecy sum-rate.

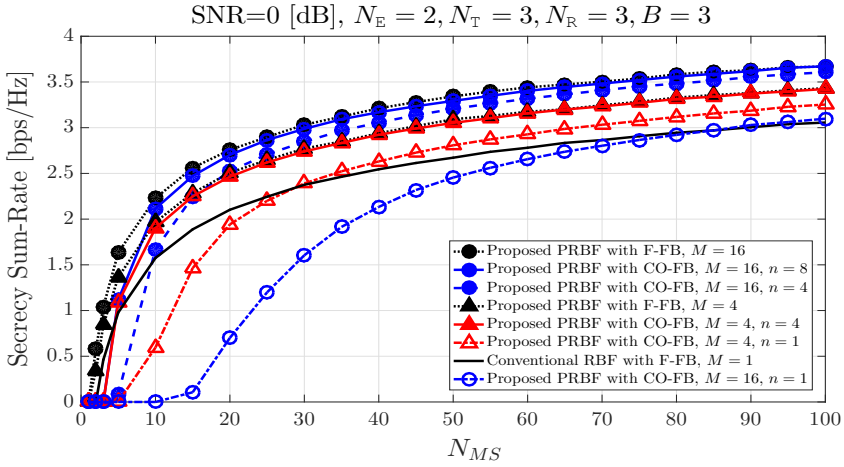

Figure 3. Secrecy sum-rate according to the number of legitimate MSs.

Figure 4 shows that the secrecy sum-rate according to the received SNR at each communication device when the number of legitimate MSs N_{MS} is equal to 100, snf the number of eavesdroppers N_{E} is equal to 2, the number of antennas of both legitimate MSs and eavesdroppers N_{R}, and the number of transmit BF vectors in each transmit BF matrix candidate B are all equal to 3. The secrecy sum-rate increases as the received SNR and the number of transmit BF candidates M increases. In particular, when the number of transmit BF candidates M is equal to 4, the proposed PRBF with the conventional F-FB outperforms the proposed PRBF with the proposed CO-FB and the predetermined value $n = 1$ in terms of secrecy sum-rate. However, the proposed PRBF with the conventional F-FB and the proposed PRBF with the proposed CO-FB and the predetermined value $n = 4$ are almost the same in terms of secrecy sum-rate. When the predetermined value n is large enough, the proposed CO-FB and the conventional F-FB show almost the same performance in terms of secrecy sum-rate. However, when the predetermined value n increases, the number of required feedback bits per legitimate MS also increases.

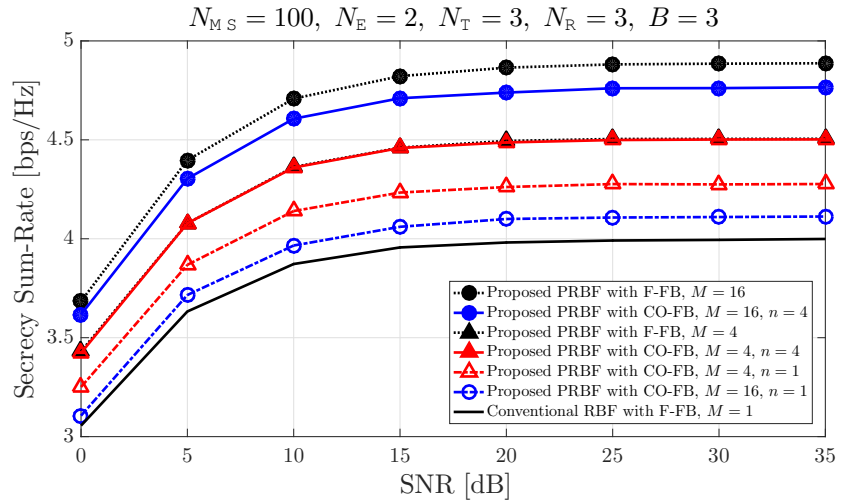

Figure 4. Secrecy sum-rate according to the received SNR.

Figure 5 shows that the number of required feedback bits per legitimate MS according to the number of transmit BF matrix candidates M and the predetermined value n when the number of transmit BF vectors in each transmit BF matrix candidate B is equal to 3, and the number of required bits for SINR quantization Q is equal to 6 bits. As explained in Section 3.2, each legitimate MS provides back totally M SINR values and beam indices in the conventional F-FB. In the conventional F-FB, the number of required feedback bits do not depend on the predetermined value n. Thus, the number of required feedback bits is fixed regardless of the predetermined value n. When the number of transmit BF matrix candidates M is equal to 16 and the number of transmit BF vectors in each transmit BF matrix candidate B is equal to 3 in the conventional F-FB strategy, each legitimate MS provides back totally 16 SINR values for 16 BF matrix candidates regardless of n. On the other hand, each legitimate MS provides back totally n SINR values and beam indices in both of the conventional O-FB and the proposed CO-FB. The predetermined value n indicates the number of feedback SINR values, and the number of required feedback bits depends on the predetermined value n in both of the conventional O-FB and the proposed CO-FB. When the predetermined value n and the number of transmit BF vectors in each transmit BF matrix candidate M are equal to 4 and 16, respectively, each legitimate MS provides back only four maximal SINR values for 16 BF matrix candidates in the conventional O-FB. Furthermore, in the proposed CO-FB, the number of required feedback bits per legitimate MS can be reduced compared to the conventional O-FB. The conventional F-FB shows the best performance than the proposed CO-FB in terms of secrecy sum-rate. However, it is difficult to apply the conventional F-FB in practice due to the large number of required feedback bits. Hence, the proposed CO-FB maintains a similar performance as the conventional F-FB in terms of secrecy sum-rate when the number of legitimate MSs, the number of transmit BF matrix candidates M and the predetermined value n are large enough. As a result, the feedback overhead can be significantly reduced.

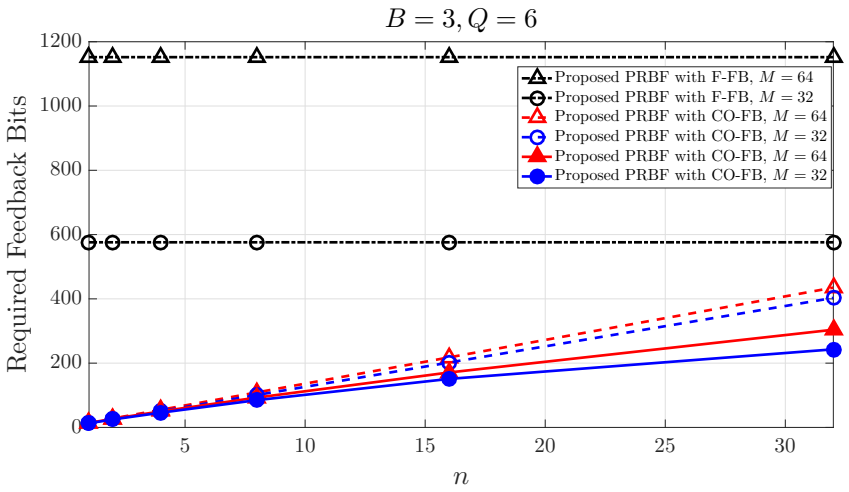

Figure 5. Required feedback bits per legitimate MS according to the predetermined value.

In summary, the conventional PRBF uses only one pseudo-random BF matrix ($M = 1$) for downlink data transmission. Accordingly, each legitimate MS feedbacks SINR values with transmit BF vector index to the legitimate BS according to the number of transmit BF vectors B. However, the proposed PRBF uses one more pseudo-random BF matrix candidates ($M \geq 2$). Thus, each legitimate MS feedbacks SINR values with transmit BF vector and matrix index to the legitimate BS according to the number of transmit BF matrix candidates M and the number of transmit BF vectors B. The proposed PRBF technique has the effect of increasing the number of legitimate MSs who feedback CSI by the number of transmit BF matrix candidates M. In other words, the proposed PRBF technique exploits *multi-user diversity gain*. As the number of transmit BF matrix candidates M increases, the sum-rate increases, however, the feedback overhead also significantly increases in the proposed PRBF

with the conventional F-FB. Thus, the proposed PRBF technique should be used with the conventional O-FB or the proposed CO-FB, which can significantly reduce the feedback overhead. However, in the proposed PRBF with the conventional O-FB or the proposed CO-FB, if the number of transmit BF matrix candidates M is large and the number of legitimate MSs N_{MS} is small, the sum-rate is reduced because some transmit BF vectors may not be selected and used during user scheduling. To solve this problem, the predetermined value n should be designed considering the number legitimate MSs N_{MS} in a downlink cell to obtain a sufficient sum-rate improvement.

5. Conclusions

In this paper, we propose a PRBF technique for MIMO downlink cellular networks. Legitimate MSs can receive the data signal from the legitimate BS via MMSE-based receive BF vector. By considering worst-case at legitimate devices, we assume that potential eavesdroppers can also receive the data signal via MMSE-based receive BF vector. Based on the feedback information from legitimate MSs and potential eavesdroppers' CSI, the legitimate BS selects the optimal transmit BF matrix among multiple BF candidates in order to maximize the secrecy sum-rate performance. Extensive computer simulations show that the proposed PRBF outperforms the conventional RBF in terms of secrecy sum-rate. In addition, the proposed CO-FB and the conventional O-FB have the same performance in terms of secrecy sum-rate; however, the proposed CO-FB outperforms the conventional O-FB in terms of required feedback bits. Furthermore, when the number of legitimate MSs and the predetermined value are large enough, the proposed PRBF with the proposed CO-FB outperforms the conventional RBF with the conventional O-FB in terms of sum-rate and required feedback bits for user scheduling at the legitimate BS.

Author Contributions: Formal analysis, W.S.; Investigation, W.S., H.S.J., and B.C.J.; Methodology, B.C.J.; Project administration, B.C.J.; Resources, B.C.J.; Software, W.S.; Supervision, H.S.J. and B.C.J.; Validation, H.S.J.; Writing—original draft, W.S.; and Writing—review and editing, H.S.J. and B.C.J.

Funding: This research received no external funding.

Acknowledgments: This work was supported in part by the NRF through the Basic Science Research Program funded by the Ministry of Science and ICT under Grant NRF2019R1A2B5B01070697 and in part by the NRF grant funded by the Korea government Ministry of Science and ICT (No. 2019R1F1A1061023).

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

References

1. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *10*, 656–715. [CrossRef]
2. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
3. Leung-Yan-Cheong, S.K.; Hellman, M.E. The Gaussian wire-tap channel. *IEEE Trans. Inf. Theory* **1978**, *24*, 451–456. [CrossRef]
4. Bloch, M.; Barros, J.; Rodrigues, M.R.D.; McLaughlin, S.W. Wireless information-theoretic security. *IEEE Trans. Inf. Theory* **2008**, *24*, 451–456. [CrossRef]
5. Shiu, Y.-S.; Chang, S.Y.; Wu, H.-C.; Huang, S.C.-H.; Chen, H.-H. Physical layer security in wireless networks: A tutorial. *IEEE Wirel. Commun.* **2011**, *18*, 66–74. [CrossRef]
6. 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. Tuts.* **2014**, *16*, 1550–1573. [CrossRef]
7. 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]
8. 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, 22–27 May 2016.
9. 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]

10. Pei, M.; Swindlehurst, A.L.; Ma, D.; Wei, J. On ergodic secrecy rate for MISO wiretap broadcast channels with opportunistic scheduling. *IEEE Commum. Lett.* **2014**, *18*, 50–53. [CrossRef]
11. Wang, L.; Wang, Z.; Pei, M. Orthogonal random beamforming with beam selection for MISO wiretap broadcast channels. In Proceedings of the 2016 2nd IEEE International Conference on Computer and Communications (ICCC), Chengdu, China, 14–17 October 2016.
12. Chen, X.; Zhang, Y. Mode selection in MU-MIMO downlink networks: A physical-layer security perspective. *IEEE Syst. J.* **2015**, *11*, 1128–1136. [CrossRef]
13. Gao, C.; Han, S.; Wang, X.; Meng, W.; Gao, F. Performance Analysis of Beamforming Algorithms In Physical Layer Security. In Proceedings of the 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), Limassol, Cyprus, 25–29 June 2018.
14. Mukherjee, A.; Swindlehurst, A.L. Detecting passive eavesdroppers in the MIMO wiretap channel. In Proceedings of the 2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Kyoto, Japan, 25–30 March 2012.
15. Chorti, A.; Perlaza, S.M.; Han, Z.; Poor, H.V. Physical layer security in wireless networks with passive and active eavesdroppers. In Proceedings of the 2012 IEEE Global Communications Conference (GLOBECOM), Anaheim, CA, USA, 3–7 December 2012.
16. Kapetanovic, D.; Zheng, G.; Rusek, F. Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks. *IEEE Commun. Mag.* **2015**, *53*, 21–27. [CrossRef]
17. Do, T.T.; Ngo, H.Q.; Duong, T.Q.; Oechtering, T.J.; Skoglund, M. Massive MIMO pilot retransmission strategies for robustification against jamming. *IEEE Wirel. Commun. Lett.* **2017**, *6*, 58–61. [CrossRef]
18. Tseng, S.-M.; Chen, Y.-F.; Chiu, P.-H.; Chi, H.-C. Jamming resilient cross-layer resource allocation in uplink HARQ-based SIMO OFDMA video transmission systems. *IEEE Access* **2017**, *5*, 24908–24919. [CrossRef]
19. Guo, J.; Zhao, N.; Yu, F.R.; Zhang, S.; Yang, Z.; Leung, V.C. Disrupting Anti-Jamming Interference Alignment Sensor Networks with Optimal Signal Design. *IEEE Sens. Lett.* **2017**, *1*, 7500204. [CrossRef]
20. Liang, L.; Cheng, W.; Zhang, W.; Zhang, H. Mode hopping for anti-jamming in radio vortex wireless communications. *IEEE Trans. Veh. Technol.* **2018**, *67*, 7018–7032. [CrossRef]
21. Wang, H.; Fu, Y.; Song, R.; Shi, Z.; Sun, X. Power Minimization Precoding in Uplink Multi-Antenna NOMA Systems With Jamming. *IEEE Trans. Green Commun. Netw.* **2019**, *3*, 591–602. [CrossRef]
22. Krikidis, I.; Ottersten, B. Secrecy sum-rate for orthogonal random beamforming with opportunistic scheduling. *IEEE Signal Process Lett.* **2012**, *20*, 141–144. [CrossRef]
23. Chen, X.; Ng, D.W.K.; Chen, H.-H. Secrecy wireless information and power transfer: Challenges and opportunities. *IEEE Wirel. Commun.* **2016**, *23*, 54–61. [CrossRef]
24. Abbas, M.A.; Song, H.; Hong, J.-P. Opportunistic scheduling for average secrecy rate enhancement in fading downlink channel with potential eavesdroppers. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 969-980. [CrossRef]
25. Bang, I.; Jung, B.C. Secrecy Rate Analysis of Opportunistic User Scheduling in Uplink Networks With Potential Eavesdroppers. *IEEE Access* **2019**, *7*, 127078–127089. [CrossRef]
26. Son, W.; Jung, B.C.; Shin, W.-Y.; Shin, Y. Multi-cell pseudo-random beamforming: Opportunistic feedback and beam selection. In Proceedings of the 2017 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, South Korea, 18–20 October 2017.
27. Son, W.; Jung, B.C.; Kim, C.-Y.; Kim, J.M. Pseudo-Random Beamforming with Beam Selection for Improving Physical-Layer Security. In Proceedings of the 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN), Prague, Czech Republic, 3–6 July 2018.
28. Yang, H.J.; Shin, W.-Y.; Jung, B.C.; Paulraj, A. Opportunistic interference alignment for MIMO interfering multiple-access channels. *IEEE Trans. Wirel. Commun.* **2013**, *12*, 2180–2192. [CrossRef]
29. Yang, H.J.; Shin, W.-Y.; Jung, B.C.; Suh, C.; Paulraj, A. Opportunistic downlink interference alignment for multi-cell MIMO networks. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 1533–1548. [CrossRef]
30. Ko, K.S.; Jung, B.C.; Hoh, M. Distributed interference alignment for multi-antenna cellular networks with dynamic time division duplex. *IEEE Commun. Lett.* **2018**, *22*, 792–795. [CrossRef]