Pseudo-Random Beamforming with Beam Selection for Improving Physical-Layer Security

Woong Son, Bang Chul Jung, Choul-Young Kim
Dept. of Electronics Engineering
Chungnam National University
Daejeon 34134, Republic of Korea
{woongson,bcjung,cykim}@cnu.ac.kr

Jong Min Kim
Dept. of Math. and Info. Science
Korea Science Academy of KAIST
Busan 47162, Republic of Korea
franzkim@gmail.com

***Abstract*—In this paper, we propose a novel pseudo-random beamforming technique with beam selection for improving physical-layer security (PLS) in a downlink cellular network where consists of a base station (BS) with N_t antennas, N_{MS} legitimate mobile stations (MSs), and N_{E} eavesdroppers. In the proposed technique, the BS generates multiple candidates of beamforming matrix each of which consists of orthogonal beamforming vectors in a pseudo-random manner. Each legitimate MS *opportunistically* feeds back the received signal-to-interference-and-noise ratio (SINR) value for all beamforming vectors to the BS. The BS transmits data to the legitimate MSs with the optimal beamforming matrix among multiple beam forming matrices that maximizes the secrecy sum-rate. Simulation results show that the proposed technique outperforms the conventional random beamforming technique in terms of the achievable secrecy sum-rate.**

***Index Terms*—Random beamforming, physical-layer security, opportunistic scheduling, secrecy rate, opportunistic feedback.**

I. Introduction

Secure information transfer via wireless networks is one of the most challenging issues. Physical-layer security, also known as secrecy capacity, denotes a information theoretical performance measure that quantifies security level of a communication link [1], [2], and it has been received much attention from many researchers and many techniques have been proposed to improve the security at the physical-layer in wireless networks [3].

The secret information broadcast was investigated in a downlink cellular network, where it was shown that the average secrecy rate is rather reduced as the number of receivers/users increases, thus resulting in no multi-user diversity gain [4]. In a single-cell *uplink* wire-tap network with multiple eavesdroppers, however, it was shown that the optimal multi-user diversity gain can be obtained using a simple user scheduling method based on a pre-determined threshold [5]. Recently, a threshold-based user scheduling algorithm was also proposed to improve the secrecy capacity for multi-cell uplink networks with multiple eavesdroppers, which achieves the optimal multi-user diversity gain even in the inter-cell interference [6]. In [4]–[6], all communication nodes including base station (BS), mobile station (MS), and eavesdroppers are equipped with a single antenna.

On the other hand, a user scheduling algorithm with random beamforming technique was proposed to improve secrecy capacity in a single cell downlink, where the BS is equipped with multiple antennas but the MSs and the eavesdroppers are equipped with a single antenna [7]. In [7], the number of legitimate MSs and eavesdroppers are assumed to be the same each other and each MS is assumed to be wire-tapped by a corresponding eavesdropper, which can be considered as a worst-case scenario. In addition, another opportunistic beamforming technique was proposed in a cellular downlink network which consists of a BS with multiple antennas, multiple MSs, and a single eavesdropper with multiple antennas [8]. In [8], two different user scheduling algorithms were proposed and their performance was mathematically analyzed in terms of ergodic secrecy rate.

In this paper, we propose a novel pseudo-random beamforming technique with beam selection for improving physical-layer security in a single cell downlink network, which was originally proposed in [9]. We also consider an opportunistic feedback strategy at MSs. Thus, the proposed technique not only improves the secrecy sum-rate but also reduces the signaling overhead. It is shown that the proposed technique significantly outperforms the conventional random beamforming technique [7] at the cost of slightly increased feedback overhead from MSs.

II. System Model

We consider a single downlink cellular network that consists of a BS with N_t antennas, N_{MS} legitimate MSs, and N_{E} unauthorized eavesdroppers as shown in Fig. 1. We assume a single antenna at both the legitimate MSs and the eavesdroppers. The wireless channel vector from the BS to the i-th legitimate MS is denoted as $\mathbf{h}_{\mathsf{MS},i} \in \mathbb{C}^{N_t \times 1}$ and the wireless channel vector from the BS to the j-th eavesdropper is denoted as $\mathbf{h}_{\mathsf{E},j} \in \mathbb{C}^{N_t \times 1}$, where $i \in \{1, ..., N_{\mathsf{MS}}\}$ and $j \in \{1, ..., N_{\mathsf{E}}\}$. Each element of $\mathbf{h}_{\mathsf{MS},i}$ and $\mathbf{h}_{\mathsf{E},j}$ is assumed to be independent and identically distributed (i.i.d.) and drawn from a complex Gaussian distribution with zero mean and unit variance, i.e., $\mathbf{h}_{\mathsf{MS},i}, \mathbf{h}_{\mathsf{E},j} \sim \mathcal{CN}\left(\mathbf{0}, \mathbf{I}_{N_t}\right)$. We assume that the BS knows $\mathbf{h}_{\mathsf{E},j}$ for all j. The BS generates M candidates of beamforming matrix in a *pseudo-random manner*. Let $\mathbf{V}^{[m]} = \left[\mathbf{v}^{[m,1]}, ..., \mathbf{v}^{[m,b]}, ..., \mathbf{v}^{[m,B]}\right] \in \mathbb{C}^{N_t \times B}$ denote the m-th beamforming matrix, where $m \in \{1, ..., M\}$, $b \in \{1, ..., B\}$, and $B \leq N_t$. Note that B denotes the number of

978-1-5386-4646-5/18/$31.00 ©2018 IEEE

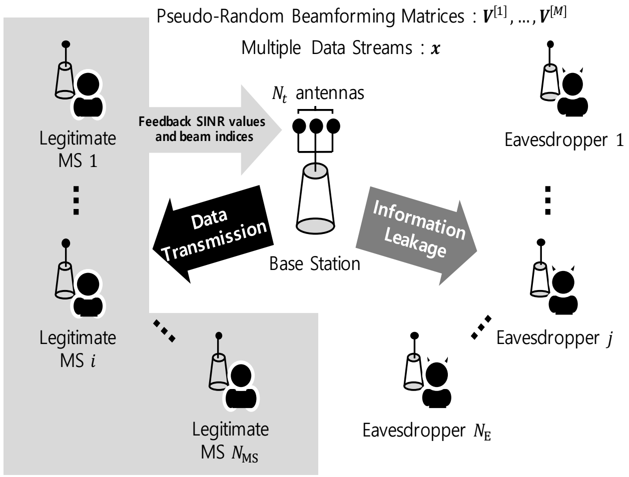
Pseudo-Random Beamforming Matrices : $\boldsymbol{V}^{[1]}, \ldots, \boldsymbol{V}^{[M]}$
Multiple Data Streams : $\boldsymbol{x}$
N_t antennas
Feedback SINR values and beam indices
Legitimate MS 1
Eavesdropper 1
Data Transmission
Information Leakage
Base Station
Legitimate MS i
Eavesdropper j
Legitimate MS N_{MS}
Eavesdropper N_{E}

Fig. 1. A single-cell downlink network consisting of a BS, N_{MS} legitimate MSs, and N_{E} eavesdroppers.

signals to be sent to multiple users simultaneously. Assuming that the BS sends signal vector via the b-th beamforming vector of the m-th beamforming matrix, the received signal at both the i-th legitimate MS and the j-th eavesdropper are given as:

$$y_{\mathsf{MS},i}^{[m,b]} = \left(\mathbf{h}_{\mathsf{MS},i}\right)^T \mathbf{v}^{[m,b]} x_b + \sum_{l=1,l\neq b}^{B} \left(\mathbf{h}_{\mathsf{MS},i}\right)^T \mathbf{v}^{[m,l]} x_l + n_{\mathsf{MS},i}, \quad (1)$$

$$y_{\mathsf{E},j}^{[m,b]} = \left(\mathbf{h}_{\mathsf{E},j}\right)^T \mathbf{v}^{[m,b]} x_b + \sum_{l=1,l\neq b}^{B} \left(\mathbf{h}_{\mathsf{E},j}\right)^T \mathbf{v}^{[m,l]} x_l + n_{\mathsf{E},j}, \quad (2)$$

where $\mathbf{x} = \left[x_1, ..., x_B\right]^T \in \mathbb{C}^{B\times 1}$ denotes the transmit signal vector of the BS and $\mathbb{E}\left[\|\mathbf{x}\|_2^2\right] = P$. In addition, $n_{\mathsf{MS},i} \in \mathbb{C}$ and $n_{\mathsf{E},j} \in \mathbb{C}$ denote the thermal noise at the i-th legitimate MS and the j-th eavesdropper, respectively, which are assumed to be drawn from a complex Gaussian distribution with zero mean and variance of N_0.

III. Pseudo-Random Beamforming Technique with Beam Section

In this section, we explain the overall procedure of the proposed technique.

A. Reference Signal Broadcast from the BS

The BS broadcasts the reference signal. After receiving the reference signal, all legitimate MSs and eavesdroppers attain the wireless channel vector from the BS.

B. SINR Computation and Feedback from Legitimate MSs

Each legitimate MS calculates the effective SINR values for all m and b:

$$\mathsf{SINR}_{\mathsf{MS},i}^{[m,b]} = \frac{|\left(\mathbf{h}_{\mathsf{MS},i}\right)^T \mathbf{v}^{[m,b]}|^2}{\sum_{l=1,l\neq b}^{B} |\left(\mathbf{h}_{\mathsf{MS},i}\right)^T \mathbf{v}^{[m,l]}|^2 + 1/\rho}, \forall m, \forall b, \quad (3)$$

where $\rho = P/N_0$.

In this paper, we consider two different feedback strategies: the conventional feedback (C-FB) and the opportunistic feedback (O-FB).

- In the C-FB, each legitimate MS feeds back the optimal beamforming vector index that maximizes effective SINR values for all m. Thus, the number of feedback bits for each legitimate MS is given by
$$\mathsf{N}_{\mathsf{C\text{-}FB}} = M\left(\log_2 B + Q\right), \quad (4)$$
where Q denotes the required bits for the SINR quantization.
- In the O-FB, each legitimate MS feeds back the best $n\,(\leq M)$ beamforming vector indices that maximizes effective SINR values among M candidates. Then, the number of feedback bits for each legitimate MS is given by
$$\mathsf{N}_{\mathsf{O\text{-}FB}} = n(\log_2 MB + Q). \quad (5)$$

For example, when $M = 32$, $B = 4$, and $Q = 6$, $\mathsf{N}_{\mathsf{C\text{-}FB}} = 32 \times (\log_2 4 + 6) = 256$ bits. On the other hand, for the *opportunistic feedback* with $n = 4$, $\mathsf{N}_{\mathsf{O\text{-}FB}} = 4 \times (\log_2(32 \times 4) + 6) = 52$.

C. Effective SINR at the Eavesdroppers

As noted before, the BS is assumed to know the wireless channel vector from itself to all eavesdroppers, and thus the BS calculates the effective SINR values at eavesdroppers for all candidates of beamforming matrix. The effective SINR values for the b-th beamforming vector of the m-th beamforming matrix is given by

$$\mathsf{SINR}_{\mathsf{E},j}^{[m,b]} = \frac{|\left(\mathbf{h}_{\mathsf{E},j}\right)^T \mathbf{v}^{[m,b]}|^2}{\sum_{l=1,l\neq b}^{B} |\left(\mathbf{h}_{\mathsf{E},j}\right)^T \mathbf{v}^{[m,l]}|^2 + 1/\rho}, \forall m, \forall b. \quad (6)$$

D. User Scheduling at the BS

Basic idea of the user scheduling at the BS is select a set of legitimate MSs that have the maximum effective SINR values for given beamforming matrix. Then, the achievable sum-rate for the m-th beamforming matrix is given by

$$\mathsf{R}_{\mathsf{sum}}^{[m]} = \sum_{b=1}^{B} \left[\log_2\left(1 + \max_{1\leq i\leq N_{\mathsf{MS}}} \mathsf{SINR}_{\mathsf{MS},i}^{[m,b]}\right)\right], \forall m. \quad (7)$$

Similarly, the BS calculates the information leakage rate due to eavesdroppers for the m-th beamforming matrix as follows:

$$\mathsf{R}_{\mathsf{e}}^{[m]} = \sum_{b=1}^{B} \left[\log_2\left(1 + \max_{1\leq j\leq N_{\mathsf{E}}} \mathsf{SINR}_{\mathsf{E},j}^{[m,b]}\right)\right], \forall m. \quad (8)$$

Then, the achievable secrecy sum-rate for the m-th beamforming matrix is given by

$$\mathsf{R}_{\mathsf{sec}}^{[m]} = \max\left\{\mathsf{R}_{\mathsf{sum}}^{[m]} - \mathsf{R}_{\mathsf{e}}^{[m]}, 0\right\}, \forall m. \quad (9)$$

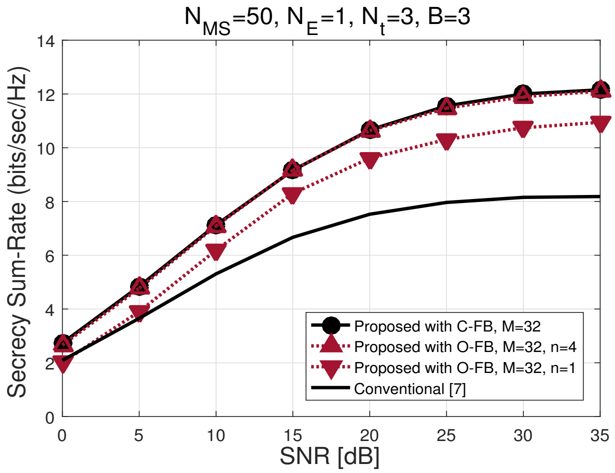

Fig. 2. Secrecy sum-rate of the proposed technique for varying SNR values.

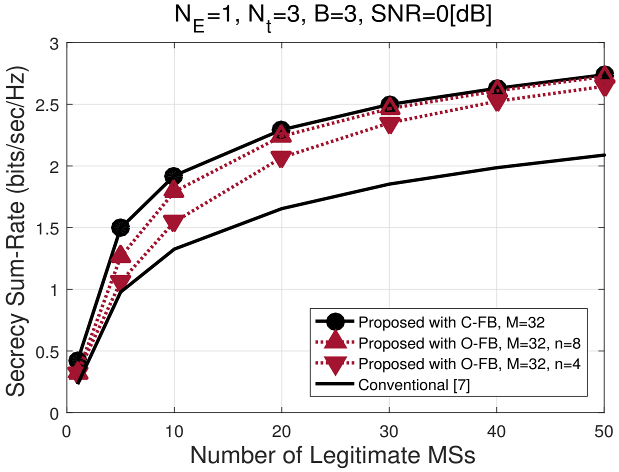

Fig. 3. Secrecy sum-rate of the proposed technique for varying number of legitimate MSs.

E. Optimal Beamforming Matrix Selection at the BS

Based on the (9), the BS selects the optimal beamforming matrix that maximizes the secrecy sum-rate among M candidates, which can be expressed as:

$$\widehat{m} = \arg\max_{1\leq m\leq M} \mathsf{R}_{\mathsf{sec}}^{[m]}. \tag{10}$$

F. Downlink Data Transmission

With the optimal beamforming matrix, the BS sends data with the selected beamforming matrix, $\mathbf{V}^{[\widehat{m}]}$. Finally, the achievable secrecy sum-rate of the proposed pseudo-random beamforming with beam selection is given by $\mathsf{R}_{\mathsf{sec}}^{[\widehat{m}]}$.

IV. Simulation Results

In this section, we evaluate the secrecy sum-rate of the proposed pseudo-random beamforming technique with beam selection under various system parameters. Fig. 2 shows the secrecy sum-rate performance of the proposed technique for varying SNR values. Both the conventional feedback and the opportunistic feedback are considered and compared. In Fig. 2, we assume that $N_{\mathsf{MS}} = 50$, $N_{\mathsf{E}} = 1$, $N_t = 3$, and $B = 3$. The secrecy sum-rate increases of the proposed technique as M increases, and the proposed technique significantly outperforms the conventional random beamforming technique [7]. The secrecy sum-rate of the proposed technique with O-FB with $n = 4$ for $M = 32$ is almost the same as that with C-FB over all SNR values, while significantly reducing the feedback overhead. Fig. 3 shows the secrecy sum-rate performance of the proposed technique according to the number of legitimate MSs when $\rho = 0$dB. We also assume that $N_{\mathsf{E}} = 1$, $B = 3$, and $N_t = 3$. As the number of legitimate MSs increases, the secrecy sum-rate becomes increased accordingly due to multi-user diversity gain. Note that the secrecy sum-rate of the proposed technique with O-FB approaches to that with C-FB as N_{MS} increases.

V. Conclusion

In this paper, we proposed a novel pseudo-random beamforming technique with beam selection to enhance physical-layer security in the downlink cellular network with multiple eavesdroppers. In order to reduce the feedback overhead of the proposed technique, we also consider the opportunistic feedback strategy. Through extensive computer simulations, we show that the proposed technique significantly outperforms the conventional random beamforming technique in terms of secrecy sum-rate especially when the SNR is high or the number of legitimate MSs is large.

Acknowledgement

This work was supported in part by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science and ICT (NRF-2016R1A2B4014834) and in part by the Korea Science Academy of KAIST with funds from the Ministry of Science and ICT.

References

[1] A. D. Wyner, “The wire-tap channel,” *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[2] M. Bloch *et al.*, “Wireless information-theoretic security,” *IEEE Trans. Info. Theory*, vol. 54, no. 6, pp. 2515–2534, May 2008.

[3] Y.-S. Shiu *et al.*, “Physical layer security in wireless networks: A tutorial,” *Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[4] H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, “On multiuser secrecy rate in flat fading channel,” *in Proc. IEEE MILCOM*, Oct. 2009

[5] H. Jin, W. -Y. Shin, and B. C. Jung, “On the multi-User diversity with secrecy in uplink wiretap networks,” *IEEE Commun. Lett.*, vol. 17, no. 9, pp.1778–1781, Sep. 2013.

[6] H. Jin, B. C. Jung, and W.-Y. Shin, “On the secrecy capacity of multi-cell uplink networks with opportunistic scheduling,” *in Proc. IEEE ICC*, May 2016.

[7] I. Krikidis and B. Ottersten, “Secrecy sum-rate for orthogonal random beamforming with opportunistic scheduling,” *IEEE Signal Process. Lett.*, vol. 20, no. 2, pp. 141–144, Feb. 2013.

[8] M. Pei, A. L. Swindlehurst, D. Ma, and J. Wei, “On ergodic secrecy rate for MISO wiretap braodcast channels with opportunistic scheduling,” *IEEE Commun. Lett.*, vol. 18, no. 1, pp. 50–53, Jan. 2014.

[9] W. Son, B. C. Jung, W.-Y. Shin, and Y. Shin, “Multi-cell pseudo-random beamforming: Opportunistic feedback and beam selection,” *in Proc. ICTC*, pp. 447–449, Oct. 2017.