# Joint Beamforming and Jamming for Physical Layer Security

Jungho Myung, Hwanjo Heo, and Jongdae Park

**In this paper, we consider a joint beamforming and jamming design to enhance physical layer security against potential multiple eavesdroppers in a multiple-input and single-output cellular broadcast channel. With perfect channel state information at the base station, we propose various design approaches to improve the secrecy of the target user. Among the proposed approaches, the combined beamforming of maximum ratio transmission and zero-forcing transmission with a combination of maximum ratio jamming and zero-forcing jamming (MRT + ZFT with MRJ + ZFJ) shows the best security performance because it utilizes the full transmit antenna dimensions for beamforming and jamming with an efficient power allocation. The simulation results show that the secrecy rate of this particular proposed approach is better than the rates of the considered conventional approaches with quality-of-service and outage probability constraints.**

**Keywords: Beamforming, jamming, physical layer security.**

## I. Introduction

Wireless communication with multiple antennas has attracted considerable attention due to the potential performance improvements in spatial multiplexing or diversity gain [1]–[10]. Among the proposed methods of [1]–[10], it has been well known that maximum ratio transmission (MRT) beamforming is an efficient technique for providing improved performance in fading channels [3]. Since each transmit antenna in an MRT is weighted by a properly designed gain and phase shift using the channel state information (CSI) of the desired user, the user can receive a transmit signal with the maximum signal-to-noise ratio (SNR) condition, and therefore can overcome any wireless propagation impairments, such as fading and shadowing.

Due to the broadcast nature of a wireless medium, wireless confidential communication is intrinsically vulnerable to eavesdropping attacks [11]–[24]. Although a great number of security measures have already been developed and deployed throughout network layers (that is, from wired equivalent privacy in the wireless link layer to transport layer security in the application layer), the fact remains that it is these very measures that must now confront substantial challenges by attackers with immense computing resources acquirable from a cloud or bounded error quantum polynomial time algorithms leveraging quantum computers, to list just a few.

Physical layer security (PLS) has been studied to provide fundamental secrecy in the sense that it does not rely on any intractability assumptions unlike cryptographic algorithms implemented in higher network layers. In [11], Wyner first introduced a wiretap channel and the associated secrecy capacity to evaluate secure communication at the physical layer, the results of which show the feasibility of secure message

Manuscript received Feb. 5, 2015; revised May 6, 2015; accepted June 8, 2015.

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No. B0126-15-1026, Development of Core Technologies for SDN-based Moving Target Defense).

Jungho Myung (corresponding author, jhmyung@etri.re.kr), Hwanjo Heo (hwanjo@etri.re.kr), and Jongdae Park (parkjd@etri.re.kr) are with the Communications & Internet Research Laboratory, ETRI, Daejeon, Rep. of Korea.

http://dx.doi.org/10.4218/etrij.15.2415.0002

exchanges under the condition of a single antenna. However, secrecy is not provided if the gain of the eavesdropping channels is higher than the gain of the main channel; that is, the channel of the target user. To resolve this problem, PLS based on a multiple antenna system has been studied [15]–[19]. Equipped with multiple transmit antennas at the base station, the secrecy of the target user can be provided by beamforming even though the main channel gain is lower than that of the eavesdropper. Also, with imperfect CSI and channel correlation, PLS has been studied [20]–[22]. In [23], by degrading the channel of the eavesdropper using artificially generated jamming from the base station, secret communication can be guaranteed. Although beamforming and jamming can be simultaneously operated under the condition of multiple transmit antennas previous works have only focused on designing a beamforming to increase the user throughput without jamming.

In this paper, we propose joint beamforming and jamming designs to enhance the secrecy of a target user under a multiple-input and single-output (MISO) cellular broadcast channel. Among the proposed approaches, the combined beamforming of MRT and zero-forcing transmission (ZFT) with the combination of maximum ratio jamming (MRJ) and zero-forcing jamming (ZFJ) shows the best security performance because it utilizes the full transmit antenna dimensions for beamforming and jamming with an efficient power allocation. For the CSI of the target user available only at the base station (without the channel of the eavesdropper), MRT with jamming is also proposed. We verify that our analysis is in good agreement with Monte-Carlo simulation results.

The remainder of this paper is organized as follows. We present preliminaries including a MISO cellular broadcast channel with multiple eavesdroppers in Section II. The proposed joint beamforming and jamming approaches and simulation results are presented in Sections III and IV, respectively. Finally, we provide some concluding remarks in Section V.

Throughout the paper, we use the notations $\mathbf{x}^*$, inv($\mathbf{x}$), and $\|\mathbf{x}\|$, which denote the conjugate transpose, inverse, and Euclidean norm of vector $\mathbf{x}$, respectively.

## II. System Model

In this paper, we consider a wireless communication in which a single base station, equipped with $N_\mathrm{t}$ transmit antennas, serves multiple mobile users, $K$. As the base station communicates with a single target user at a time, the other users are assumed to be potential eavesdroppers from which the system provides mutual confidentiality. Figure 1 shows a MISO broadcast channel with a base station, target user, and remaining users (potential eavesdroppers). When the base station transmits a signal (depicted by a solid line) to the target user, the radio signal is exposed to the untargeted users over the cross channels (dotted lines) due to the broadcast nature of wireless communication. In our model, the channel coefficients are assumed to be flat Rayleigh fading with additive white Gaussian noise (AWGN) terms that are mutually independent of each other and have zero mean and unit variance, $CN(0,\sigma^2)$. To design joint beamforming and jamming efficiently, it is also assumed that perfect CSI is available at the base station.

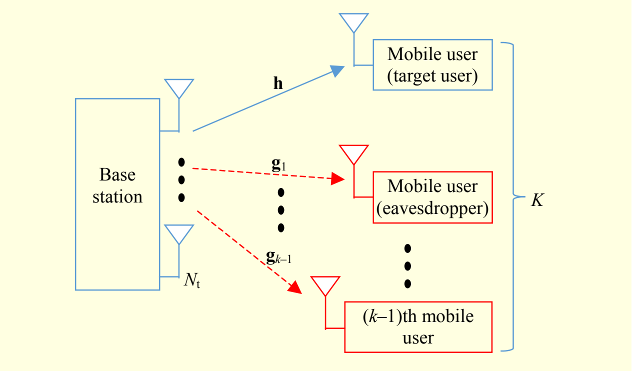

Fig. 1. MISO cellular broadcast channel model with single base station, target user, and multiple potential eavesdroppers.

### 1. Secrecy Rate

According to [11], *secrecy rate* (of a target user) can be defined as the gap between the achievable rate of the target user and the maximum achievable rate of the eavesdropping users. Given that $\mathbf{f}$ and $\mathbf{w}$ are, respectively, defined as beamforming and jamming vectors with the power constraint $\|\mathbf{f}\|^2 = \|\mathbf{w}\|^2 = 1$, the secrecy rate ($R_\mathrm{s}$) of a target user is expressed by

$$R_\mathrm{s} = \left[\log_2\left(1+\frac{\|\mathbf{h}\cdot\mathbf{f}\|^2 p_\mathrm{b}}{\sigma^2+\|\mathbf{h}\cdot\mathbf{w}\|^2 p_\mathrm{j}}\right) - \max_{i\in[1,k-1]}\log_2\left(1+\frac{\|\mathbf{g}_i\cdot\mathbf{f}\|^2 p_\mathrm{b}}{\sigma^2+\|\mathbf{g}_i\cdot\mathbf{w}\|^2 p_\mathrm{j}}\right)\right]^+, \quad (1)$$
$$\text{s.t. } p_\mathrm{b}+p_\mathrm{j}\le p_\mathrm{t},$$

where $\mathbf{h}$, $\mathbf{g}_i$, $p_\mathrm{b}$, $p_\mathrm{j}$, and $p_\mathrm{t}$ denote the channel vector of the desired target user, the channel vector of potential eavesdropper $i$, the transmit power of the beamforming signal, the transmit power of the jamming signal, and the total transmit power, respectively.

### 2. Secrecy Rate with Beamforming Approaches

#### *A. MRT*

Since the MRT is a scheme used to maximize only the throughput of the target user, beamforming $\mathbf{f}_{\mathrm{MRT}}$ can be designed as [3]

$$\mathbf{f}_{\mathrm{MRT}} = \frac{\mathbf{h}^*}{\|\mathbf{h}\|}. \tag{2}$$

Thus, the secrecy rate of an MRT can be rewritten as

$$R_{\mathrm{s}}(\mathbf{f}_{\mathrm{MRT}}) = \left[ \log_2 \left( 1 + \frac{\|\mathbf{h}\|^2 p_{\mathrm{t}}}{\sigma^2} \right) - \max_{i\in[1,k-1]} \log_2 \left( 1 + \frac{\|\mathbf{g}_i \cdot \mathbf{f}_{\mathrm{MRT}}\|^2 p_{\mathrm{t}}}{\sigma^2} \right) \right]^+ . \tag{3}$$

Due to the property of MRT beamforming, the throughput of the target user can be maximized. However, since the beamforming is designed without consideration of the eavesdropping channels, it is easy to eavesdrop on the communications. In particular, with a high correlation between $\mathbf{h}$ and $\mathbf{g}_i$, or with high SNR, the security performance of the MRT is degraded.

### *B. ZFT*

ZFT is a scheme of spatial signal processing by which a base station with multiple antennas can nullify eavesdropped signals. To nullify an eavesdropped signal, beamforming $\mathbf{f}_{\mathrm{ZFT}}$ is obtained as [4]

$$\mathbf{f}_{\mathrm{ZFT}} = \frac{\mathbf{G}(:,1)}{\|\mathbf{G}(:,1)\|}, \tag{4}$$

where

$$\mathbf{H} = [\mathbf{h}; \mathbf{g}_1; \ldots; \mathbf{g}_{k-1}], \qquad \mathbf{G} = \mathbf{H}^* \cdot \mathrm{inv}(\mathbf{H}\cdot\mathbf{H}^*). \tag{5}$$

With orthogonality to an eavesdropped channel ($\mathbf{f}_{\mathrm{ZFT}}^{\perp}$ $\forall_{i\in[1,k-1]}$ $\mathbf{g}_i$), the secrecy rate can be rewritten as

$$R_{\mathrm{s}}(\mathbf{f}_{\mathrm{ZFT}}) = \log_2 \left( 1 + \frac{\|\mathbf{h}\cdot\mathbf{f}_{\mathrm{ZFT}}\|^2 p_{\mathrm{t}}}{\sigma^2} \right). \tag{6}$$

Using ZFT, perfect security can be guaranteed, because the throughput of an eavesdropper becomes zero. However, due to the nulling of an eavesdropped channel, the target user's throughput is quite degraded. Therefore, with multiple eavesdroppers, it is difficult to guarantee the desired throughput of the target user.

## III. Joint Beamforming and Jamming Approaches

In this section, we evaluate the secrecy rates corresponding to various joint beamforming and jamming combinations.

### 1. MRT with ZFT

To make up for the weaknesses of MRT and ZFT described in Section II, the beamforming can be designed as a combination of MRT and ZFT. After finding an orthogonal basis from ZFT using a channel nulling technique as

$$\begin{aligned} \hat{\mathbf{f}}_{\mathrm{MRT}}^{\perp} &= \mathbf{f}_{\mathrm{MRT}} - (\mathbf{f}_{\mathrm{ZFT}}^{*} \cdot \mathbf{f}_{\mathrm{MRT}}) \cdot \mathbf{f}_{\mathrm{ZFT}}, \\ \mathbf{f}_{\mathrm{MRT}}^{\perp} &= \frac{\hat{\mathbf{f}}_{\mathrm{MRT}}^{\perp}}{\|\hat{\mathbf{f}}_{\mathrm{MRT}}^{\perp}\|}, \end{aligned} \tag{7}$$

the combination beamforming can be obtained as

$$\mathbf{f}_{\mathrm{COM}} = \alpha \cdot \mathbf{f}_{\mathrm{MRT}}^{\perp} + \beta \cdot \mathbf{f}_{\mathrm{ZFT}}, \tag{8}$$

where $\alpha$ and $\beta$ are complex weights. The optimal complex weights are obtained by

$$\begin{aligned} &\max_{\alpha,\,\beta} \;\; R_{\mathrm{s}}(\mathbf{f}_{\mathrm{COM}}), \\ &\text{s.t.} \;\; \|\alpha\|^2 + \|\beta\|^2 \le 1. \end{aligned} \tag{9}$$

The secrecy rate of MRT with ZFT is then expressed as

$$R_{\mathrm{s}}(\mathbf{f}_{\mathrm{MRT}}) = \left[ \log_2 \left( 1 + \frac{\|\mathbf{h}\cdot\mathbf{f}_{\mathrm{COM}}\|^2 p_{\mathrm{t}}}{\sigma^2} \right) - \max_{i\in[1,k-1]} \log_2 \left( 1 + \frac{\|\mathbf{g}_i \cdot \alpha \cdot \mathbf{f}_{\mathrm{MRT}}^{\perp}\|^2 p_{\mathrm{t}}}{\sigma^2} \right) \right]^+ . \tag{10}$$

Although combination beamforming is more complicated, the security performance is better than those of conventional MRT and ZFT due to proper power allocation between MRT and ZFT.

### 2. With Jamming

Jamming is a transmit signal that disrupts communications by decreasing the SNR. Through beamforming and jamming, the base station can increase the secrecy rate offensively due to the jamming for eavesdroppers. In this subsection, we propose a joint beamforming and jamming design for PLS.

### *A. MRT with Jamming*

In this scheme, MRT beamforming is utilized for user throughput with jamming. After nulling and normalizing, jamming with MRT beamforming can be designed as

$$\mathbf{w}_{\mathrm{J}} = \sum_{i=1}^{k-1} \hat{\mathbf{w}}_{\mathrm{J}}^{i}, \tag{11}$$

where

$$\hat{\mathbf{w}}_{\mathrm{J}}^{i} = \frac{\overline{\mathbf{w}}_{\mathrm{J}}^{i}}{\left\| \sum_{i=1}^{k-1} \overline{\mathbf{w}}_{\mathrm{J}}^{i} \right\|}, \qquad \overline{\mathbf{w}}_{\mathrm{J}}^{i} = \mathbf{G}(:, i+1). \tag{12}$$

The secrecy rate is then given by

$$\begin{aligned} R_{\mathrm{s}}(\mathbf{f}_{\mathrm{MRT}}, \mathbf{w}_{\mathrm{J}}, p_{\mathrm{b}}, p_{\mathrm{j}}) \\ = \Bigg[ \log_2 \left( 1 + \frac{\|\mathbf{h} \cdot \mathbf{f}_{\mathrm{MRT}}\|^2 p_{\mathrm{b}}}{\sigma^2} \right) \\ - \max_{i \in [1, k-1]} \log_2 \left( 1 + \frac{\|\mathbf{g}_i \cdot \mathbf{f}_{\mathrm{MRT}}\|^2 p_{\mathrm{b}}}{\sigma^2 + \|\mathbf{g}_i \cdot \mathbf{w}_{\mathrm{J}}\|^2 p_{\mathrm{j}}} \right) \Bigg]^+ . \end{aligned} \tag{13}$$

With the total transmit power constraint at the base station, the power allocation between MRT beamforming and jamming can be obtained by

$$\begin{aligned} &\max_{p_{\mathrm{b}}, p_{\mathrm{j}}} \ R_{\mathrm{s}}(p_{\mathrm{b}}, p_{\mathrm{j}}), \\ &\text{s.t.} \ p_{\mathrm{b}} + p_{\mathrm{j}} \le p_{\mathrm{t}}. \end{aligned} \tag{14}$$

Due to a balance between jamming for eavesdroppers and MRT for the target user, the performance of the secrecy rate is considerably improved compared with that of MRT without jamming. In addition, the performance can be improved with the power allocation among jamming signals as

$$\begin{aligned} &\max_{p_{\mathrm{b}}, \mathbf{p}_{\mathrm{j}}} \ R_{\mathrm{s}}(p_{\mathrm{b}}, \mathbf{p}_{\mathrm{j}}), \\ \text{s.t.} \ & \forall_{i, p \in [1, k-1]} \ \mathrm{SINR}_i = \mathrm{SINR}_p, \\ & p_{\mathrm{b}} + \|\mathbf{p}_{\mathrm{j}}\| \le p_{\mathrm{t}}, \ \mathbf{p}_{\mathrm{j}} = \{p_{\mathrm{j}}^1, p_{\mathrm{j}}^2, \ldots, p_{\mathrm{j}}^{k-1}\}, \\ & \sum_{i=1}^{k-1} p_{\mathrm{j}}^i = p_{\mathrm{j}} = \|\mathbf{p}_{\mathrm{j}}\|, \end{aligned} \tag{15}$$

where $\mathbf{p}_{\mathrm{j}}$ and $p$ denote the power allocation vector for efficient jamming and the eavesdropper's index parameter, respectively. The signal-to-interference-plus-noise ratio of the $i$th eavesdropper is denoted by $\mathrm{SINR}_i$ and is given by

$$\mathrm{SINR}_i = \frac{\|\mathbf{g}_i \cdot \mathbf{f}_{\mathrm{MRT}}\|^2 p_{\mathrm{b}}}{\sigma^2 + \|\mathbf{g}_i \cdot \hat{\mathbf{w}}_{\mathrm{J}}^i\|^2 p_{\mathrm{j}}^i}. \tag{16}$$

### *B. MRT+ZFT with MRJ+ZFJ*

Due to a security improvement, the beamforming can be designed as a combination of MRT and ZFT, as in (8). With combined beamforming, the base station can transmit data to the target user with a perfectly secure dimension from $\mathbf{f}_{\mathrm{ZFT}}$ and throughput enhancement dimension from $\mathbf{f}_{\mathrm{MRT}}^{\perp}$. Similarly, using (2) and (3), the jamming can also be divided into the MRJ and ZFJ as

$$\mathbf{w}_{\mathrm{MRJ}}^i = \frac{\mathbf{g}_i^*}{\|\mathbf{g}_i\|}, \qquad \mathbf{w}_{\mathrm{ZFJ}}^i = \frac{\mathbf{G}(:, i+1)}{\|\mathbf{G}(:, i+1)\|}. \tag{17}$$

For a harmonious jamming combination, after finding an orthogonal basis from ZFJ as

$$\begin{aligned} \hat{\mathbf{w}}_{\mathrm{MRJ}}^{i,\perp} &= \mathbf{w}_{\mathrm{MRJ}}^i - \left( (\mathbf{w}_{\mathrm{ZFJ}}^i)^* \cdot \mathbf{w}_{\mathrm{MRJ}}^i \right) \cdot \mathbf{w}_{\mathrm{ZFJ}}^i, \\ \mathbf{w}_{\mathrm{MRJ}}^{i,\perp} &= \frac{\hat{\mathbf{w}}_{\mathrm{MRJ}}^{i,\perp}}{\|\hat{\mathbf{w}}_{\mathrm{MRJ}}^{i,\perp}\|}, \end{aligned} \tag{18}$$

the $i$th jamming can be expressed as

$$\begin{aligned} \mathbf{w}_{\mathrm{COM}}^i = \gamma_i \cdot \mathbf{w}_{\mathrm{MRJ}}^{i,\perp} + \omega_i \cdot \mathbf{w}_{\mathrm{ZFJ}}^i, \\ \text{s.t.} \ \|\gamma_i\|^2 + \|\omega_i\|^2 \le 1, \end{aligned} \tag{19}$$

where $\gamma_i$ and $\omega_i$ are complex weights for the $i$th jamming. Then, the total jamming signal can be obtained by

$$\mathbf{w}_{\mathrm{COM}} = \frac{\sum_{i=1}^{k-1} \mathbf{w}_{\mathrm{COM}}^i}{\left\| \sum_{i=1}^{k-1} \mathbf{w}_{\mathrm{COM}}^i \right\|}. \tag{20}$$

Using the proposed jamming, the base station can transmit jamming to the $i$th eavesdropper with perfect uninfluential dimension ($\mathbf{w}^i_{\mathrm{ZFJ}}$) and jamming enhancement dimension ($\mathbf{w}_{\mathrm{MRJ}}^{i,\perp}$). The optimal weights and power allocation can be obtained by

$$\begin{aligned} &\max_{\alpha, \beta, \boldsymbol{\gamma}, \boldsymbol{\omega}, p_{\mathrm{b}}, \mathbf{p}_{\mathrm{j}}} \ R_{\mathrm{s}}(\mathbf{f}_{\mathrm{COM}}, \mathbf{w}_{\mathrm{COM}}) \\ \text{s.t.} \ & \|\alpha\|^2 + \|\beta\|^2 \le 1, \ \|\gamma_i\|^2 + \|\omega_i\|^2 \le 1, \\ & p_{\mathrm{b}} + \|\mathbf{p}_{\mathrm{j}}\| \le p_{\mathrm{t}}, \ \sum_{i=1}^{k-1} p_{\mathrm{j}}^i = \|\mathbf{p}_{\mathrm{j}}\|, \\ & \boldsymbol{\gamma} = \{\gamma_1, \gamma_2, \ldots, \gamma_{k-1}\}, \boldsymbol{\omega} = \{\omega_1, \omega_2, \ldots, \omega_{k-1}\}, \end{aligned} \tag{21}$$

where $\boldsymbol{\gamma}$ and $\boldsymbol{\omega}$ are vectors of complex weights.

## 3. Performance Analysis

In Table 1, we compare the proposed beamforming and jamming (MRT + ZFT, MRT with jamming, and MRT + ZFT with MRJ + ZFJ) with conventional beamforming (MRT and ZFT) in terms of the availability of CSI, complexity, achievable secrecy rate, and defense type (which will be explained later in this section). Throughout the table, we use the following notation. Let ***C***, ***I***, ***N***, and ***P*** denote the mathematical operators for conjugate transpose, inverse matrix, channel nulling, and power allocation, respectively. Also, ***K*** and SNR denote the exponent number for operation (= the number of users) and SNR, respectively.

The conventional MRT for maximizing the throughput of the target user has the lowest computational complexity. However, since it does not consider the eavesdropping channels, the achievable secrecy rate is poor; with jamming, the rate of MRT can be improved. Also, due to the decrease in channel gain as a result of nullifying the eavesdropping channels, the security performance of ZFT is the worst in low

Table 1. Performance comparison.

| | MRT | ZFT | MRT+ZFT | MRT with jamming | MRT+ZFT with MRJ+ZFJ |
|---|---|---|---|---|---|
| Availability of CSI | (Only) target user | All user | All user | All user | All user |
| Complexity (necessary operator) | Lowest ($\underline{\boldsymbol{C}}$) | Low ($\underline{\boldsymbol{I}}$) | Medium ($\underline{\boldsymbol{C}}+\underline{\boldsymbol{I}}+\underline{\boldsymbol{N}}+\underline{\boldsymbol{P}}$) | Medium ($\underline{\boldsymbol{C}}+\underline{\boldsymbol{I}}+\underline{\boldsymbol{P}}$) | High ($\underline{\boldsymbol{I}}+(\underline{\boldsymbol{C}}+\underline{\boldsymbol{N}})^{\boldsymbol{K}}+\underline{\boldsymbol{P}}$) |
| Achievable secrecy rate | (Low SNR) worse (high SNR) worst | (Low SNR) worst (high SNR) good | (Low SNR) good (high SNR) good | (Low SNR) good (high SNR) worse | (Low SNR) best (high SNR) best |
| Defense type | N.A. | Passive | Passive | Active | Active |

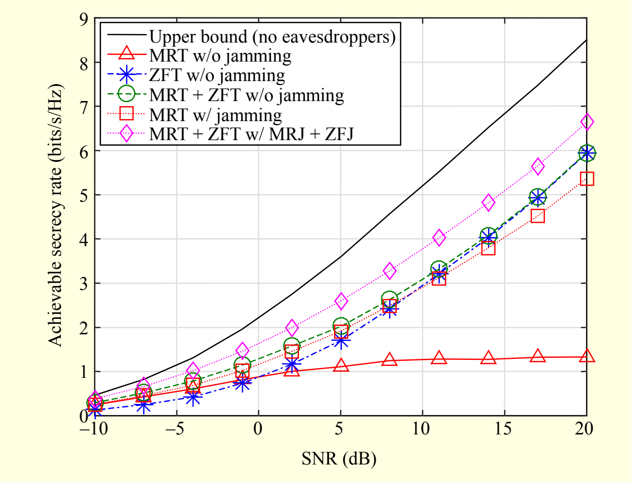

Fig. 2. Achievable secrecy rate vs. SNR, where $N_t = 4$ and $K = 4$.

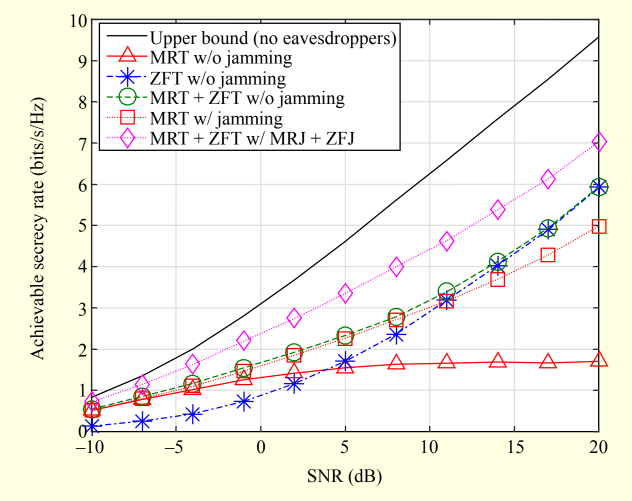

Fig. 3. Secrecy rate vs. SNR, where $N_t = 8$ and $K = 8$.

SNR regions. MRT + ZFT combines the benefits of both MRT and ZFT; it results in an improved security performance but at the cost of increased computational complexity. Although MRT + ZFT with MRJ + ZFJ is the most complicated, the secrecy rate is better than those of the aforementioned approaches due to the full transmit dimensions for beamforming and jamming and an efficient power allocation.

The proposed approaches can be divided into two groups in accordance with the type of defense offered against eavesdropping. First, ZFT and MRT + ZFT are *passive* in the sense that the design of beamforming seeks to avoid the use of the eavesdropping channels. On the other hand, MRT with jamming and MRT + ZFT with MRJ + ZFJ are *active*, since they deliberately interfere with any potential eavesdroppers.

## IV. Numerical Results

In this section, we provide the simulation results using various joint beamforming and jamming approaches for PLS. For simulation, a MISO broadcast channel is considered, as shown in Fig. 1. The channel coefficients are assumed to be flat Rayleigh fading with AWGN terms that are mutually independent of each other and have zero mean and unit variance. In all figures, “Upper bound” means a theoretical or ideal performance result — one that can be obtained by MRT without eavesdroppers. The specific parameters are given below each figure.

In Figs. 2 and 3, the achievable secrecy rates versus SNR are evaluated for different approaches. By utilizing a full transmit dimension with efficient power allocation, MRT + ZFT with MRJ + ZFJ achieves a much better performance compared with other approaches. In a low SNR region, conventional ZFT (without jamming) shows the worst performance due to a transmit dimension reduction for the nullified eavesdropping channels. However, in a high SNR region, the performance of ZFT grows better with the eavesdropping-free transmit dimension and high transmit power. Also, since it is hard to eavesdrop on the transmit signal in a low SNR region, conventional MRT (without jamming) shows a moderate performance. However, conventional MRT (without jamming) shows the worst performance and is saturated in a high SNR region because it does not consider the eavesdropped channels. The saturation problem of conventional MRT can be resolved through active jamming of eavesdroppers. Without jamming, the performance of MRT + ZFT is better than that of conventional MRT and ZFT due to the combination effect with a power allocation. In Fig. 3, as the numbers of antennas and eavesdroppers increase, the performance of MRT + ZFT with MRJ + ZFJ increases due to the increase of transmit antenna dimensions. On the other hand, the performance of MRT with jamming in a high SNR region is degraded because the average jamming power decreases. The performance of

http://dx.doi.org/10.4218/etrij.15.2415.0002

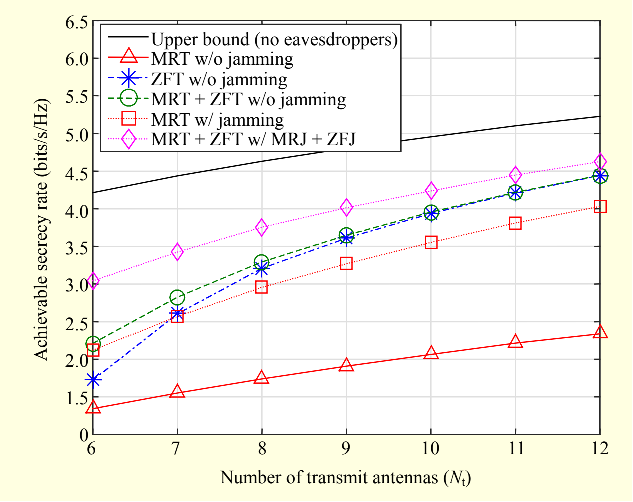

Fig. 4. Secrecy rate vs. number of antennas, where $K$ = 6, and SNR = 5 dB.

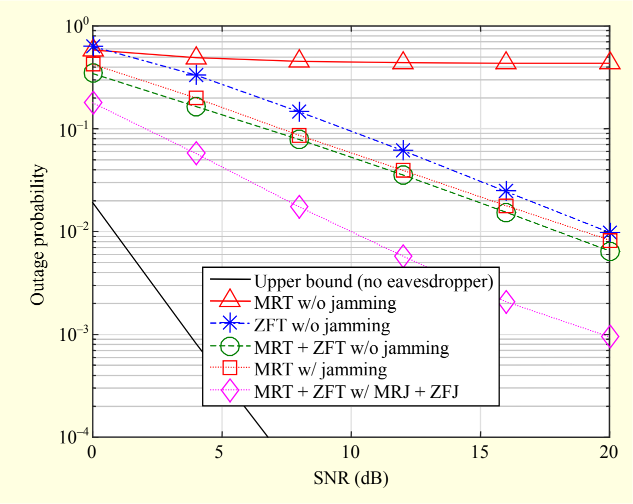

Fig. 5. Outage probability vs. SNR, where $N_t$ = 4, $K$ = 4, and target QoS = 1 bits/s/Hz.

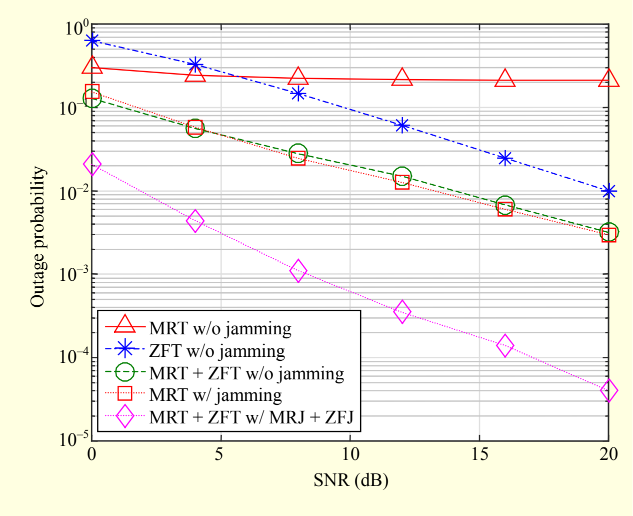

Fig. 6. Outage probability vs. SNR, where $N_t$ = 8, $K$ = 8, and target QoS = 1 bits/s/Hz.

conventional ZFT in a low SNR region is also degraded due to a decrease in channel gain from nulling more eavesdropping channels.

Figure 4 shows the secrecy rate versus the number of transmit antennas by fixing the number of eavesdroppers ($K$ = 6) at an SNR of 5 dB. All secrecy rates are absolutely improved due to a dimension increase for the beamforming and jamming as the number of antennas increases. Among the approaches, MRT + ZFT with MRJ + ZFJ still shows the best performance. When the number of antennas increases, however, the performance gap between MRT + ZFT with MRJ + ZFJ and conventional ZFT is reduced. The reason for this phenomenon is that the channel gain of the eavesdropping-free transmit dimension in ZFT is sufficient even after nulling the eavesdropping channels. Under large transmit antenna conditions, the performance of ZFT is eventually equivalent to that of MRT + ZFT with MRJ + ZFJ due to an increase in the transmit dimensions.

Figures 5 and 6 show the outage probability versus SNR by fixing the target QoS to 1 bits/s/Hz. In Fig. 5, to satisfy the $10^{-2}$ outage probability constraint, the required SNRs of ZFT, MRT + ZFT, MRT with jamming, and MRT + ZFT with MRJ + ZFJ are 20 dB, 19 dB, 18 dB, and 10 dB, respectively. Therefore, a base station using MRT + ZFT with MRJ + ZFJ can save more total transmit power than with any of the other approaches under a fixed QoS and outage probability. From the simulation results, since it is hard to guarantee the system constraint (target QoS), we consider that a conventional MRT must be inadequate for a secure wireless communication.

In Fig. 6, as the numbers of antennas and eavesdroppers increase, the outage probabilities of the proposed approaches are significantly increased due to the increase in transmit dimension. However, since the channel gain of the eavesdropping-free dimension after application of the nulling technique is almost the same as that in Fig. 5, the performance of ZFT remains unaffected. In spite of an increase in the number of antennas, for conventional MRT, it is still difficult to guarantee the outage probability constraint due to a saturation of the performance. To satisfy the probability constraint, the required SNRs of ZFT, MRT + ZFT, MRT with jamming, and MRT + ZFT with MRJ + ZFJ are 20 dB, 14 dB, 13 dB, and 2 dB, respectively. Under this condition, base station using MRT + ZFT with MRJ + ZFJ can save a transmit power of almost 18 dB in comparison to using ZFT.

## V. Conclusion

In this paper, we proposed various joint beamforming and jamming combinations for physical layer security. Among the proposed approaches, MRT + ZFT with MRJ + ZFJ shows the best security performance due to the full transmit dimension usage for beamforming and jamming with efficient power allocation. We also demonstrated that our approaches are in good agreement with the simulation results and provide a good basis for an extension to more general eavesdropping topologies. Our proposed approaches can be extended to more general eavesdropping systems employing multiple received antennas, along with partial CSI or without CSI of the eavesdroppers at the base station.

## References

[1] M. Costa, "Writing on Dirty Paper," *IEEE Trans. Info. Theory*, vol. 29, no. 3, May 1983, pp. 439–441.

[2] G.J. Foschini and M.J. Gans, "On Limits of Wireless Communications in a Fading Environment When Using Multiple Antennas," *Wireless Pers. Commun.*, vol. 6, no. 3, Mar. 1998, pp. 311–335.

[3] T.K.Y. Lo, "Maximum Ratio Transmission," *IEEE Int. Conf. Commun.*, Vancouver, Canada, June 6–10, 1999, pp. 1310–1314.

[4] C.B. Peel, B.M. Hochwald, and A.L. Swindlehurst, "A Vector-Perturbation Technique for Near-Capacity Multiantenna Multiuser Communication - Part I: Channel Inversion and Regularization," *IEEE Trans. Commun.*, vol. 53, no. 1, Jan. 2005, pp. 195–202.

[5] G. Caire and S. Shamai, "On the Achievable Throughput of a Multi-antenna Gaussian Broadcast Channel," *IEEE Trans. Info. Theory*, vol. 49, no. 7, July 2003, pp. 1691–1706.

[6] P. Viswanath and D.N.C. Tse, "Sum Capacity of the Vector Gaussian Broadcast Channel and Uplink-Downlink Duality," *IEEE Trans. Info. Theory*, vol. 49, no. 8, Aug. 2003, pp. 1912–1921.

[7] S. Vishwanath, N. Jindal, and A. Goldsmith, "Duality, Achievable Rates, and Sum Capacity of Gaussian MIMO Broadcast Channels," *IEEE Trans. Info. Theory*, vol. 49, no. 10, Oct. 2003, pp. 2658–2668.

[8] C. Windpassisnger et al., "Precoding in Multi-antenna and Multiuser Communications," *IEEE Trans. Wireless Commun.*, vol. 3, no. 4, July 2004, pp. 1305–1315.

[9] Z. Shen et al., "Low Complexity User Selection Algorithms for Multiuser MIMO Systems with Block Diagonalization," *IEEE Trans. Signal Process.*, vol. 54, no. 9, Sept. 2006, pp. 3658–3663.

[10] R. Chen, R.W. Heath Jr., and J.G. Andrews, "Transmit Selection Diversity for Unitary Precoded Multiuser Spatial Multiplexing Systems with Linear Receivers," *IEEE Trans. Signal Process.*, vol. 55, no. 3, Mar. 2007, pp. 1159–1171.

[11] A.D. Wyner, "The Wire-Tap Channel," *The Bell Sys. Tech. J.*, vol. 54, no. 8, Oct. 1975, pp. 1355–1387.

[12] M. Bloch et al., "Wireless Information-Theoretic Security," *IEEE Trans. Info. Thory*, vol. 54, no. 6, June 2008, pp. 2515–2534.

[13] A. Khisti, A. Tchamkerten, and G.W. Wornell, "Secure Broadcasting over Fading Channels," *IEEE Trans. Info. Theory*, vol. 54, no. 6, June 2008, pp. 2453–2469.

[14] E.G. Larsson and E.A. Jorswieck, "Competition versus Cooperation on the MISO Interference Channel," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 7, Sept. 2008, pp. 1059–1069.

[15] A. Khisti and G.W. Wornell, "Secure Transmission with Multiple Antennas I: The MISOME Wiretap Channel," *IEEE Trans. Info. Theory*, vol. 56, no. 7, July 2010, pp. 3088–3104.

[16] R. Liu and H.V. Poor, "Secrecy Capacity Region of a Multiple-Antenna Gaussian Broadcast Channel with Confidential Messages," *IEEE Trans. Info. Theory*, vol. 55, no. 3, Mar. 2009, pp. 1235–1249.

[17] T. Liu and S. Shamai, "A Note on the Secrecy Capacity of the Multiple Antenna Wiretap Channel," *IEEE Trans. Info. Theory*, vol. 55, no. 6, June 2009, pp. 2547–2553.

[18] F. Oggier and B. Hassibi, "The Secrecy Capacity of the MIMO Wiretap Channel," *IEEE Trans. Info. Theory*, vol. 57, no. 8, Aug. 2011, pp. 4961–4972.

[19] J. Zhang et al., "Ergodic Secrecy Sum-Rate for Multiuser Downlink Transmission via Regularized Channel Inversion: Large System Analysis," *IEEE Commun. Lett.*, July 2014, pp. 1627–1630.

[20] N. Yang et al., "Physical Layer Security of TAS/MRC with Antenna Correlation," *IEEE Trans. Info. Forensics Security*, Jan. 2013, pp. 254–259.

[21] X. Chen, C. Yuen, and Z. Zhang, "Exploiting Large-Scale MIMO Techniques for Physical Layer Security with Imperfect Channel State Information," *IEEE GLOBECOM*, Austin, TX, USA, Dec. 8–12, 2014, pp. 1648–1653.

[22] X. Chen et al., "On the Secrecy Outage Capacity of Physical Layer Security in Large-Scale MIMO Relaying Systems with Imperfect CSI," *IEEE Int. Conf.*, Sydney, Australia, June 10–14, 2014, pp. 2052–2057.

[23] S. Goel and R. Negi, "Guaranteeing Secrecy Using Artificial Noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, June 2008, pp. 2180–2189.

[24] N. Sklavos and X. Zhang, *Wireless Security and Cryptography: Specifications and Implementations*, Boca Raton, FL, USA: CRC Press, 2007.

http://dx.doi.org/10.4218/etrij.15.2415.0002

**Jungho Myung** received his BS degree in electrical engineering from Chungnam National University, Daejeon, Rep. of Korea, in 2008 and his MS and PhD degrees in engineering from the Korea Advanced Institute of Science and Technology, Daejeon, Rep. of Korea, in 2010 and 2014, respectively. Since 2014, he has been with ETRI, where he is currently a senior engineer. He has been primarily involved in smart and trusted networks.

**Hwanjo Heo** received his BS degree in electrical engineering from Korea University, Seoul, Rep. of Korea, in 2004 and his MS degree in computer science from Purdue University, West Lafayette, IN, USA, in 2009. He is currently a senior researcher at ETRI. His research interests include network measurement, network protocols, and software-defined networking.

**Jongdae Park** received his BS, MS, and PhD degrees in electronic engineering from Yeungnam University, Gyeongsan, Rep. of Korea, in 1985, 1987, and 1994, respectively. He was a research fellow with the Department of Electrical and Electronics, Toyohashi University of Technology, Japan, from 1995 to 1996. In 1997, he joined ETRI, where he is currently with the Fixed-Mobile Trustworthy Networking Research Section as a section leader.

http://dx.doi.org/10.4218/etrij.15.2415.0002