Hindawi Publishing Corporation
International Journal of Antennas and Propagation
Volume 2015, Article ID 594791, 12 pages
http://dx.doi.org/10.1155/2015/594791

Research Article

Aligned Space Time Block Codes for the 2-User X Channel with Secrecy Constraints

Manar Mohaisen

Department of EEC Engineering, Korea Tech, Cheonan 330-708, Republic of Korea

Correspondence should be addressed to Manar Mohaisen; manar.subhi@koreatech.ac.kr

Received 18 March 2015; Revised 29 June 2015; Accepted 1 July 2015

Academic Editor: Junping Geng

Interference alignment (IA) is a technique used to reduce the dimension of the interference, where consequently the multiplexing rate is increased. In the 2-user X channel, combining IA with space-time block codes increases the diversity gain. These gains are achieved with the cost of leaked information at unintended receivers, where this leaked information can be used to decode other receiver's signals. In this paper, we consider each of the two two-antenna receivers as an eavesdropper with 1 or 2 additional eavesdropping antennas. As such, we suggest receiver structures to answer the question: "Is the leaked information sufficient to properly decode the unintended signals?" besides quantifying the leaked information in terms of secrecy sum rates (SSR). Interestingly, we show that the SSR is negative, indicating that the quality of the eavesdropped signals is superior to that of the intended signals. To assure confidentiality, we propose an interleaved multiple rotation-based transformation scheme that neutralizes any a priori knowledge about the structure of the eavesdropped information and rotates the transmitted symbols using orthogonal matrices, preserving both the power and the distance between symbols.

1. Introduction

In wireless communications systems, interference plays a major role in defining the achievable performance and capacity [1]. In conventional receivers, in multiuser scenarios, the interference is either ignored, hence considered as an additional noise, or jointly decoded via employing successive interference cancellation (SIC) detectors [2–4]. In both cases, the dimensions of the interference remain the same, leading to degraded performance and diversity gain in the first case, while powerful algorithms should be employed in the case of SIC algorithms so as to avoid degradation in the performance due to interference.

Interference alignment is a transmission technique used to reduce the dimensions of the interference while maintaining the useful signals discernible at the intended receivers. This is achievable by precoding the transmitter signals such that the interference is aligned at unintended receivers [5]. As such, interference is removed at the intended receivers using simple mathematical operations leading to an interference-free system, where appropriate decoding algorithms can then be used to decode the useful signals. In [5], Jafar and Shamai proposed a linear alignment algorithm for the two-user X channel, which achieves the maximum data rate of $(n_T \times (4/3))$ symbols/channel use and a diversity gain of 1, with n_T as the number of transmit antennas.

In addition to the multiplexing gain, quantified by the unit symbols/channel use, the diversity gain is an important measure of the system performance. When the channel is in deep fading, systems with unity diversity gain suffer from low signal-to-noise ratio (SNR) at the receiver side, leading to degradation in the bit-error rate (BER). Several diversity techniques have been proposed in the literature to explore further diversity gain [6–8]. In [9], a technique that combines interference alignment in X channel and Alamouti diversity scheme with two transmit antennas has been proposed to achieve the maximum multiplexing gain of $(n_T \times (4/3) = 8/3)$ and the full diversity gain of 2, which is equal to the number of antennas at each of the four nodes. Furthermore, the proposed scheme inherits the space-time orthogonality of the Alamouti algorithm, and hence a simple linear receiver, that avoids computationally complex matrix inversion is required to achieve the aforementioned gains.

In analogy to other multiuser communication systems with interuser interference [10–12], keeping confidentiality

arises as one of the main challenges in the two-user X channel system with interference alignment. In such a system, each receiver can be seen as an internal eavesdropper that, besides decoding its intended symbols, it uses the leaked information to decode other receiver's intended symbols. The accuracy of decoding the unintended symbols depends on the number of additional spatial resources available at the eavesdropper.

In [13], the eavesdropper is an external agent and the system is modeled as a wiretap channel. However, in the X-channel with interference alignment system considered in this paper, the eavesdropper is the other intended receiver in the X-channel system. While in [13] it is possible to design the precoding matrices in order to deprive the eavesdropper of the capability of decoding the unintended symbols, and it is impossible to do so in the case of the X-channel system since both transmitters are employing joint precoding as will be explained later. We conclude therefore that the work introduced in [13], though very solid, cannot be applied to the case of the X-channel with interference alignment.

Another related work was introduced in [14], where authors proposed a secrecy algorithm which can be only applied in time-division duplex (TDD) systems because authors make use of the channel reciprocity principle. Another shortcoming of the proposed algorithm in [14] is that it is mainly based on the received signal strength indication (RSSI) which is inaccurate and insecure. The RSSI of users that have totally independent channels might be the same especially in indoor pico- or microcells scenarios, where they are so common in the long-term evolution (LTE) system. The drawbacks of using the RSSI in communication systems are outlined in [15] based on experimental study.

The merits of this paper are summarized as follows:

(1) Unlike in conventional works [11, 12] where only the amount of leaked information is examined and therefore is given in terms of secrecy sum rate (SSR) values, we go beyond this first stage by answering the question: "Is the leaked information sufficient to decode the unintended signals?" To this end, we investigate the receiver structures in the case of a single and two additional eavesdropping antennas. The BER performance is then evaluated for both the intended and unintended signals.

(2) Based on the obtained receiver structures, the mutual information and the SSRs are derived taking into consideration the information used in the decoding stage.

(3) To render useless the leaked information about other receiver's signals, we propose an interleaved multiple rotation-based transformation (IMRBT) algorithm that consists of two stages, namely, interleaving stage and rotation stage. In the interleaving stage, symbols are interleaved so that any a priori information about the structure of the eavesdropped signals becomes useless. Then, interleaved symbols are rotated using orthonormal matrices such that both the power and the distance between symbols in the Euclidean space are kept intact.

The rest of the paper is organized as follows. In Section 2, we introduce the system model and review related works. In Section 3, we investigate the decoding capabilities of the unintended signals at the eavesdropper, in the cases of no additional, single additional, and two additional eavesdropping antennas. In Section 4, we derive the SSRs of the intended symbols and the unintended symbols. We introduce the proposed IMRBT scheme in Section 5 and present simulation results in Section 6. Finally, we draw conclusions in Section 7.

We briefly introduce the notations used in this paper. We employ boldface uppercase letters for matrices and boldface lowercase letters for vectors. The superscripts $(\cdot)^t$, $(\cdot)^H$, and $(\cdot)^*$ denote transpose, conjugate transpose, and conjugate, respectively. $\mathcal{CN}(\mu, \sigma^2)$ is a circular symmetric complex Gaussian random variable with mean μ and variance σ^2. Finally, prob(x) is the probability of x.

2. System Model and Previous Work

2.1. System Model. Consider a two-user X channel with eavesdropping as depicted in Figure 1. Each transmitter has independent and *confidential* symbols for each of the receivers. These symbols are drawn independently from a finite modulation set Ω. Transmitter 1 has $\mathbf{s}_{11} = [s_{11}^1 \;\; s_{11}^2]^t$ and $\mathbf{s}_{12} = [s_{12}^1 \;\; s_{12}^2]^t$ intended for receiver 1 and receiver 2, respectively. In s_{ij}^k, the superscript k denotes the index of the symbol, the first subscript i denotes the index of the transmitter, and the second subscript j denotes the index of the intended receiver. Likewise, transmitter 2 has $\mathbf{s}_{21} = [s_{21}^1 \;\; s_{21}^2]^t$ and $\mathbf{s}_{22} = [s_{22}^1 \;\; s_{22}^2]^t$ intended for receiver 1 and receiver 2, respectively. Vectors $\mathbf{s}_{ij}$, for $i, j = 1, 2$, are encoded using the space-time block coder (STBC) block to generate the matrices $\mathbf{S}_{ij}$, for $i, j = 1, 2$. Finally, encoded symbols are beamformed and linearly combined to generate $T \times 2$ block codes $\mathbf{X}_i$, for $i = 1, 2$, with $T = 3$ denoting the number of channel uses. In the deployed scenario, each receiver is equipped with $n_R = 2$ *legal* receive antennas and n_E *eavesdropping* receive antennas. To denote the channels between the transmitters and the legal receive antennas, we use $\mathbf{H}$, $\mathbf{G}$, $\mathbf{A}$, and $\mathbf{B}$ to denote the 2×2 matrices coupling transmitter 1 and receiver 1, transmitter 2 and receiver 1, transmitter 1 and receiver 2, and transmitter 2 and receiver 2, respectively. While employing n_R receive antennas at each receiver is sufficient to recover its intended symbols, extra eavesdropping antennas are required to leak more information about other receiver's symbols, so that efficient decoding is achieved. To denote the channels between the transmitters and the eavesdropping receive antennas, we use $\mathbf{K}$, $\mathbf{M}$, $\mathbf{L}$, and $\mathbf{Q}$ to denote the channels between transmitter 1 and receiver 1, transmitter 2 and receiver 1, transmitter 1 and receiver 2, and transmitter 2 and receiver 2, respectively. The elements in the channel matrices in Figure 1 are independently and identically distributed (i.i.d.) circular Gaussian random variables, $\mathcal{CN}(0, 1)$. These matrices were pseudorandomly generated following the aforementioned characteristics. $T \times 2$

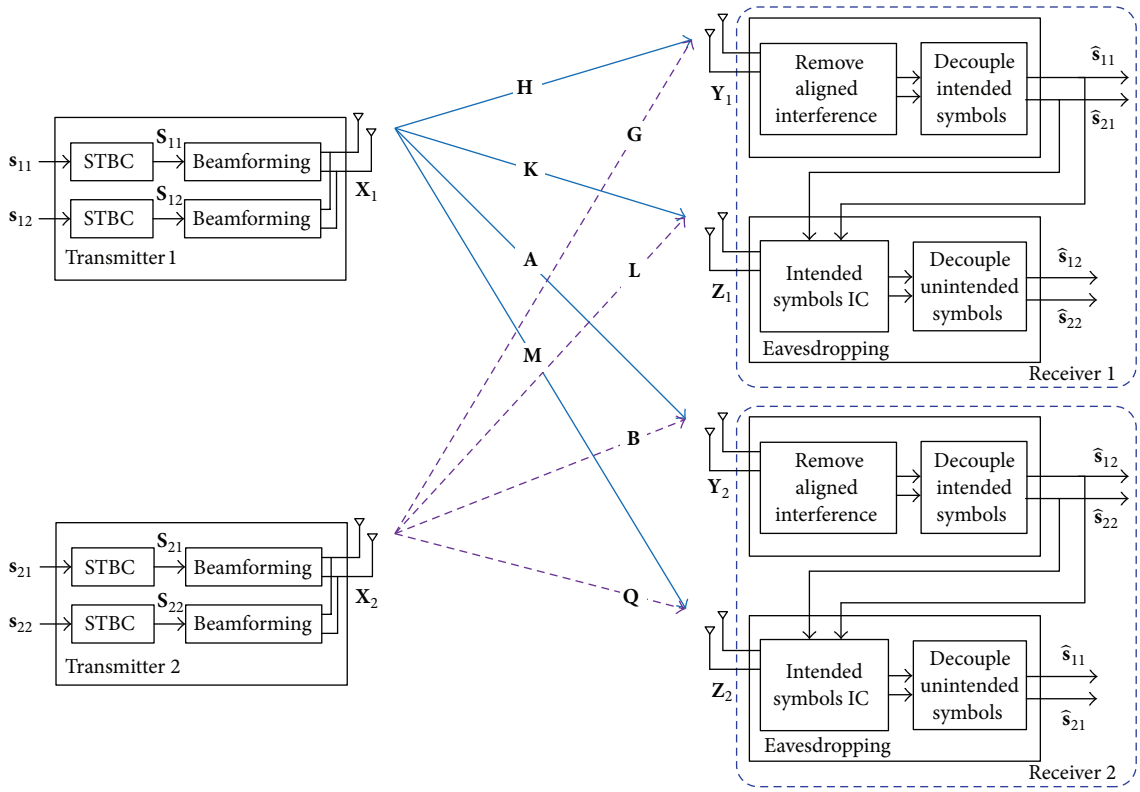

FIGURE 1: System model of a 2-user X channel with eavesdropping.

signal matrices received at the legal antennas of receiver 1 and receiver 2, respectively, are given by

$$\begin{aligned} \mathbf{Y}_1 &= \mathbf{X}_1\mathbf{H} + \mathbf{X}_2\mathbf{G} + \mathbf{W}_1, \\ \mathbf{Y}_2 &= \mathbf{X}_1\mathbf{A} + \mathbf{X}_2\mathbf{B} + \mathbf{W}_2. \end{aligned} \tag{1}$$

Similarly, the received signal matrices at the eavesdropping antennas of receiver 1 and receiver 2 are given by

$$\begin{aligned} \mathbf{Z}_1 &= \mathbf{X}_1\mathbf{K} + \mathbf{X}_2\mathbf{L} + \mathbf{N}_1, \\ \mathbf{Z}_2 &= \mathbf{X}_1\mathbf{M} + \mathbf{X}_2\mathbf{Q} + \mathbf{N}_2. \end{aligned} \tag{2}$$

Entries in the additive white Gaussian noise (AWGN) matrices, $\mathbf{W}_1$, $\mathbf{W}_2$, $\mathbf{N}_1$, and $\mathbf{N}_2$, are i.i.d. $\mathcal{CN}(0, \sigma_n^2)$, where $\sigma_n^2 = 2/(3\rho)$ and ρ denotes the SNR.

2.2. Review of Li-Jafarkhani-Jafar (LJJ) Algorithm. To achieve a diversity order of 2, while still achieving the maximum multiplexing rate of $n_T \times (4/3) = 8/3$ symbols per channel use, LJJ algorithm has been proposed in [9]. In this scheme, Alamouti coding was independently performed on each couple of symbols intended for each of two receivers. That is, at each coding instant, four symbols, two intended for receiver 1 and two intended for receiver 2, are independently encoded and then linearly combined at each transmitter. These symbols are transmitted over $T = 3$ channel uses, leading to a sum rate of 8/3 symbols per channel use.

2.2.1. Transmitter Structure. The transmitted 3×2 block codes from transmitter 1 and transmitter 2 are designed, respectively, as

$$\begin{aligned} \mathbf{X}_1 &= \mathbf{S}_{11}\mathbf{V}_{11} + \mathbf{S}_{12}\mathbf{V}_{12}, \\ \mathbf{X}_2 &= \mathbf{S}_{21}\mathbf{V}_{21} + \mathbf{S}_{22}\mathbf{V}_{22}, \end{aligned} \tag{3}$$

where

$$\begin{aligned} \mathbf{S}_{i1} &= \begin{bmatrix} s_{i1}^1 & s_{i1}^2 \\ -s_{i1}^{2*} & s_{i1}^{1*} \\ 0 & 0 \end{bmatrix}, \\ \mathbf{S}_{i2} &= \begin{bmatrix} 0 & 0 \\ -s_{i2}^{2*} & s_{i2}^{1*} \\ s_{i2}^1 & s_{i2}^2 \end{bmatrix}, \end{aligned} \tag{4}$$

$$\text{for } i = 1, 2,$$

where s_{ij}^k is the kth symbol transmitted from the ith transmitter to the jth receiver, with $\mathbb{E}[s_{ij}s_{ij}^*] = 1$, for $i, j = 1, 2$. The symbols s_{11}^k and s_{21}^k are intended for receiver 1, and hence they become interference at receiver 2. The 2×2 beamforming matrices $\mathbf{V}_{i1}$, for $i = 1, 2$, assure that the interference symbols s_{11}^k and s_{21}^k are aligned at receiver 2. Likewise, the symbols s_{12}^k and s_{22}^k, which are intended for receiver 2, are precoded using

$\mathbf{V}_{i2}$, for $i = 1, 2$, so that they are aligned at receiver 1. To fulfill these conditions, the beamforming matrices are given by

$$\begin{aligned} \mathbf{V}_{11} &= \alpha_{\mathbf{A}}\mathbf{A}^{-1}, \\ \mathbf{V}_{12} &= \alpha_{\mathbf{H}}\mathbf{H}^{-1}, \\ \mathbf{V}_{21} &= \alpha_{\mathbf{B}}\mathbf{B}^{-1}, \\ \mathbf{V}_{22} &= \alpha_{\mathbf{G}}\mathbf{G}^{-1}, \end{aligned} \tag{5}$$

where the real scalars $\alpha_{\mathbf{A}}, \alpha_{\mathbf{H}}, \alpha_{\mathbf{B}}$, and $\alpha_{\mathbf{G}}$ satisfy the power constraint $\mathrm{tr}(\mathbf{V}_{ij}\mathbf{V}_{ij}^{H}) = 1$, and hence we have $\alpha_{\mathbf{R}} = \sqrt{1/\mathrm{tr}(\mathbf{R}^{-1}\mathbf{R}^{-1H})}$.

2.2.2. Receiver Structure. Based on Figure 1, the received 3×2 signal matrices at receiver 1 and receiver 2, respectively, are written as

$$\mathbf{Y}_1 = \mathbf{S}_{11}\underbrace{\mathbf{V}_{11}\mathbf{H}}_{\widetilde{\mathbf{H}}} + \mathbf{S}_{21}\underbrace{\mathbf{V}_{21}\mathbf{G}}_{\widetilde{\mathbf{G}}} + \underbrace{\left(\alpha_{\mathbf{H}}\mathbf{S}_{12} + \alpha_{\mathbf{G}}\mathbf{S}_{22}\right)}_{\mathrm{AI}} + \mathbf{W}_1, \tag{6}$$

$$\mathbf{Y}_2 = \mathbf{S}_{12}\underbrace{\mathbf{V}_{12}\mathbf{A}}_{\widetilde{\mathbf{A}}} + \mathbf{S}_{22}\underbrace{\mathbf{V}_{22}\mathbf{B}}_{\widetilde{\mathbf{B}}} + \underbrace{\left(\alpha_{\mathbf{A}}\mathbf{S}_{11} + \alpha_{\mathbf{B}}\mathbf{S}_{21}\right)}_{\mathrm{AI}} + \mathbf{W}_2. \tag{7}$$

In (6) and (7), AI stands for aligned interference. Also, $\mathbf{Y}_1, \mathbf{Y}_2, \mathbf{W}_1$, and $\mathbf{W}_2 \in \mathbb{C}^{3\times 2}$. The matrices $\widetilde{\mathbf{H}}, \widetilde{\mathbf{G}}, \widetilde{\mathbf{A}}$, and $\widetilde{\mathbf{B}} \in \mathbb{C}^{2\times 2}$ are the effective channels of the intended symbols. Let $y_{k,ij}$ and $w_{k,ij}$ be the (i, j)th elements of $\mathbf{Y}_k$ and $\mathbf{W}_k$, respectively, and let $\widetilde{h}_{ij}, \widetilde{g}_{ij}, \widetilde{a}_{ij}$, and $\widetilde{b}_{ij}$ be the (i, j)th elements of the matrices $\widetilde{\mathbf{H}}$, $\widetilde{\mathbf{G}}, \widetilde{\mathbf{A}}$, and $\widetilde{\mathbf{B}}$, respectively, and then (6) and (7) can be rewritten as

$$\widetilde{\mathbf{y}}_1 = \begin{bmatrix} \widetilde{h}_{11} & \widetilde{h}_{21} & \widetilde{g}_{11} & \widetilde{g}_{21} & 0 & 0 \\ \widetilde{h}_{21}^* & -\widetilde{h}_{11}^* & \widetilde{g}_{21}^* & -\widetilde{g}_{11}^* & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ \widetilde{h}_{12} & \widetilde{h}_{22} & \widetilde{g}_{12} & \widetilde{g}_{22} & 0 & 0 \\ \widetilde{h}_{22}^* & -\widetilde{h}_{12}^* & \widetilde{g}_{22}^* & -\widetilde{g}_{12}^* & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} s_{11}^1 \\ s_{11}^2 \\ s_{21}^1 \\ s_{21}^2 \\ I_1 \\ I_2 \end{bmatrix} + \widetilde{\mathbf{w}}_1, \tag{8}$$

$$\widetilde{\mathbf{y}}_2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ \widetilde{a}_{21}^* & -\widetilde{a}_{11}^* & \widetilde{b}_{21}^* & -\widetilde{b}_{11}^* & 0 & -1 \\ \widetilde{a}_{11} & \widetilde{a}_{21} & \widetilde{b}_{11} & \widetilde{b}_{21} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ \widetilde{a}_{22}^* & -\widetilde{a}_{12}^* & \widetilde{b}_{22}^* & -\widetilde{b}_{12}^* & 1 & 0 \\ \widetilde{h}_{12} & \widetilde{a}_{22} & \widetilde{b}_{12} & \widetilde{b}_{22} & 0 & 0 \end{bmatrix} \begin{bmatrix} s_{12}^1 \\ s_{12}^2 \\ s_{22}^1 \\ s_{22}^2 \\ I_3 \\ I_4 \end{bmatrix} + \widetilde{\mathbf{w}}_2, \tag{9}$$

where

$$\widetilde{\mathbf{y}}_i = \begin{bmatrix} y_{i,11} \\ y_{i,21}^* \\ y_{i,31} \\ y_{i,12} \\ y_{i,22}^* \\ y_{i,32} \end{bmatrix}, \qquad \widetilde{\mathbf{w}}_i = \begin{bmatrix} w_{i,11} \\ w_{i,21}^* \\ w_{i,31} \\ w_{i,12} \\ w_{i,22}^* \\ w_{i,32} \end{bmatrix}. \tag{10}$$

In (8), $I_1 = (\alpha_{\mathbf{H}}s_{12}^1 + \alpha_{\mathbf{G}}s_{22}^1)$ and $I_2 = (\alpha_{\mathbf{H}}s_{12}^2 + \alpha_{\mathbf{G}}s_{22}^2)$, while in (9), $I_3 = (\alpha_{\mathbf{A}}s_{11}^1 + \alpha_{\mathbf{B}}s_{21}^1)$ and $I_4 = (\alpha_{\mathbf{A}}s_{11}^2 + \alpha_{\mathbf{B}}s_{21}^2)$.

Each receiver recovers its intended symbols using interference cancellation (IC) that comprises two stages, which are explained in the following two subsections. Without loss of generality and due to space limits, we consider the decoding at receiver 1, where the performance at receiver 2 is identical since the system is symmetric.

Stage 1 (removal of the aligned interference). From (8), the channel associated with the intended data symbols has an Alamouti structure. As such, symbols can be recovered using Alamouti decoder. At first, the aligned interference, I_1 and I_2, is simply removed by adding $\widetilde{y}_{12}$ to $\widetilde{y}_{16}$ and subtracting $\widetilde{y}_{13}$ from $\widetilde{y}_{15}$, where $\widetilde{y}_{1j}$ is the jth element of $\widetilde{\mathbf{y}}_1$. The resulting system is rewritten as

$$\begin{bmatrix} \widehat{\mathbf{y}}_1 \\ \widehat{\mathbf{y}}_2 \end{bmatrix} = \begin{bmatrix} \widehat{\mathbf{H}}_1 \\ \widehat{\mathbf{H}}_2 \end{bmatrix} \mathbf{s}_{11} + \begin{bmatrix} \widehat{\mathbf{G}}_1 \\ \widehat{\mathbf{G}}_2 \end{bmatrix} \mathbf{s}_{21} + \begin{bmatrix} \widehat{\mathbf{w}}_1 \\ \widehat{\mathbf{w}}_2 \end{bmatrix}, \tag{11}$$

where

$$\begin{aligned} \widehat{\mathbf{H}}_i &= \begin{bmatrix} \widetilde{h}_{1i} & \widetilde{h}_{2i} \\ \widetilde{h}_{2i}^* & -\widetilde{h}_{1i}^* \end{bmatrix}, \\ \widehat{\mathbf{G}}_i &= \begin{bmatrix} \widetilde{g}_{1i} & \widetilde{g}_{2i} \\ \widetilde{g}_{2i}^* & -\widetilde{g}_{1i}^* \end{bmatrix} \qquad \text{for } i = 1, 2, \\ \widehat{\mathbf{y}}_1 &= \left[\widetilde{y}_{11} \quad \widetilde{y}_{12} + \widetilde{y}_{16}\right]^t, \\ \widehat{\mathbf{y}}_2 &= \left[\widetilde{y}_{14} \quad \widetilde{y}_{15} - \widetilde{y}_{13}\right]^t, \\ \widehat{\mathbf{w}}_1 &= \left[\widetilde{w}_{11} \quad \widetilde{w}_{12} + \widetilde{w}_{16}\right]^t, \\ \widehat{\mathbf{w}}_2 &= \left[\widetilde{w}_{14} \quad \widetilde{w}_{15} - \widetilde{w}_{13}\right]^t, \end{aligned} \tag{12}$$

with $\widehat{\mathbf{H}}_i$ and $\widehat{\mathbf{G}}_i$ having Alamouti structure.

Stage 2 (decoupling symbols from different transmitters). All the matrices in (11) have the Alamouti structure and operations on them are complete; that is, the result of multiplying two matrices having the Alamouti structure is also an Alamouti matrix. Also, since matrices having Alamouti structure are orthogonal, their Gramian matrices are weighted identity matrices, with the weight being the matrix Frobenius norm. Therefore, when $\widehat{\mathbf{y}}_1$ is multiplied by $\widehat{\mathbf{G}}_1^H/\|\widehat{\mathbf{G}}_1\|^2$, the resulting channel matrix of $\mathbf{s}_{21}$ becomes the identity matrix. Also, when $\widehat{\mathbf{y}}_2$ is multiplied by $\widehat{\mathbf{G}}_2^H/\|\widehat{\mathbf{G}}_2\|^2$, the resulting channel matrix of $\mathbf{s}_{21}$ becomes the identity matrix as well. When the second equation is subtracted from the first, the resulting equation becomes a function of only $\mathbf{s}_{11}$ which can be decoded using a linear receiver. Mathematically, symbols s_{11}^1 and s_{11}^2 are decoupled from s_{21}^1 and s_{21}^2 as follows:

$$\underbrace{\frac{\widehat{\mathbf{G}}_1^H}{\|\widehat{\mathbf{G}}_1\|^2}\widehat{\mathbf{y}}_1 - \frac{\widehat{\mathbf{G}}_2^H}{\|\widehat{\mathbf{G}}_2\|^2}\widehat{\mathbf{y}}_2}_{\breve{\mathbf{y}}_1} = \underbrace{\left(\frac{\widehat{\mathbf{G}}_1^H}{\|\widehat{\mathbf{G}}_1\|^2}\widehat{\mathbf{H}}_1 - \frac{\widehat{\mathbf{G}}_2^H}{\|\widehat{\mathbf{G}}_2\|^2}\widehat{\mathbf{H}}_2\right)}_{\breve{\mathbf{H}}_1}\mathbf{s}_{11} + \underbrace{\frac{\widehat{\mathbf{G}}_1^H}{\|\widehat{\mathbf{G}}_1\|^2}\widehat{\mathbf{w}}_1 - \frac{\widehat{\mathbf{G}}_2^H}{\|\widehat{\mathbf{G}}_2\|^2}\widehat{\mathbf{w}}_2}_{\breve{\mathbf{w}}_1}. \tag{13}$$

The matrix $\breve{\mathbf{H}}_1$ still has the Alamouti structure. Therefore, the following linear decoding is still applicable:

$$\widetilde{\mathbf{s}}_{11} = \frac{2\cdot\breve{\mathbf{H}}_1^H}{\|\breve{\mathbf{H}}_1\|^2}\breve{\mathbf{y}}_1 = \mathbf{s}_{11} + \frac{2\cdot\breve{\mathbf{H}}_1^H}{\|\breve{\mathbf{H}}_1\|^2}\breve{\mathbf{w}}_1, \tag{14}$$

where the demodulated symbols $\widehat{\mathbf{s}}_{11} = \mathcal{Q}(\widetilde{\mathbf{s}}_{11})$, with $\mathcal{Q}(\cdot)$ as the demodulation function. The symbols s_{21}^1 and s_{21}^2 can be decoupled by employing the same method due to the system symmetry.

3. Eavesdropping and Decoding Capabilities

3.1. Case 1: No Eavesdropping Antennas. Let receivers 1 and 2 act as eavesdroppers, where, in addition to decoding their intended data symbols, they try to decode the aligned interference, that is, other receiver's symbols. Again, without loss of generality, we focus on receiver 1 due to system symmetry. From (8), the leaked information about unintended symbols, that is, s_{12}^i, s_{22}^i for $i = 1, 2$, can be rewritten as

$$\begin{bmatrix}\widetilde{y}_{13}\\ \widetilde{y}_{16}\end{bmatrix} = \alpha_{\mathbf{H}}\mathbf{s}_{12} + \alpha_{\mathbf{G}}\mathbf{s}_{22} + \begin{bmatrix}\widetilde{w}_{13}\\ \widetilde{w}_{16}\end{bmatrix}. \tag{15}$$

In light of (15), we emphasize on the following two remarks.

Remark 1. Although receiver 1 has the leaked information represented in (15), it cannot decode the symbols designated for receiver 2 due to the lack of sufficient information, four unknowns with only two equations.

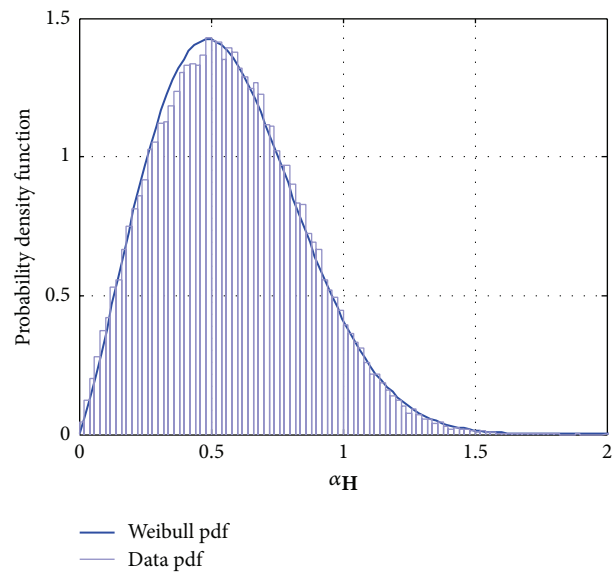

Figure 2: The probability density function of $\alpha_{\mathbf{H}}$. The pdf is modeled as a Weibull random variable with a scale parameter $\lambda = 0.644$ and a shape parameter $k = 2.20$. The results are averaged over 100,000 independent trials, where the mean and variance of $\alpha_{\mathbf{H}}$ are approximately given by 0.57 and 0.075.

Remark 2. The signal-to-noise ratio (SNR) in (15) is a function of $\alpha_{\mathbf{H}}$ and $\alpha_{\mathbf{G}}$. The value of $\alpha_{\mathbf{H}}$ is given by

$$\alpha_{\mathbf{H}} = \sqrt{\frac{1}{\operatorname{tr}(\mathbf{H}^{-1}\mathbf{H}^{-1H})}} = \sqrt{\frac{1}{\sigma_1^2(\mathbf{H}^{-1}) + \sigma_2^2(\mathbf{H}^{-1})}} = \frac{\sigma_1(\mathbf{H})}{\sqrt{\operatorname{cond}^2(\mathbf{H}) + 1}}, \tag{16}$$

where $\sigma_1(\mathbf{H})$ and $\sigma_2(\mathbf{H})$ are the maximal and minimal singular values of $\mathbf{H}$, respectively, and $\operatorname{cond}(\mathbf{H})$ is the condition number of $\mathbf{H}$. For orthonormal $\mathbf{H}$, that is, $\mathbf{H}^H\mathbf{H} = \mathbf{I}$, $\alpha_{\mathbf{H}}^2 = 0.5$. Figure 2 depicts the probability density function (pdf) of $\alpha_{\mathbf{H}}$, where $\operatorname{prob}(\alpha_{\mathbf{H}} \le 1) \approx 0.93$. This means that, in 93% of the cases, the power of the eavesdropped symbols is lower than 1 which indicates that the average receiver SNR of the interference terms is much lower than that of the intended symbols, which makes it hard, if not impossible, to eavesdrop on and decode other receiver's intended symbols.

3.2. Case 2: Number of Eavesdropping Antennas = 1. Adding an extra eavesdropping antenna at receiver 1, that is, $n_E = 1$, increases the leakage of information about the symbols intended for receiver 2. Hence, receiver 1 can use this leaked information to decode $\mathbf{s}_{12}$ and $\mathbf{s}_{22}$, after decoding its intended symbols $\mathbf{s}_{11}$ and $\mathbf{s}_{21}$, via SIC.

Based on Figure 1, the received signal matrix at the eavesdropping antenna of receiver 1 is given by

$$\mathbf{Z}_1 = \mathbf{S}_{11}\underbrace{\mathbf{V}_{11}\mathbf{K}}_{\mathbf{C}} + \mathbf{S}_{12}\underbrace{\mathbf{V}_{12}\mathbf{K}}_{\mathbf{D}} + \mathbf{S}_{21}\underbrace{\mathbf{V}_{21}\mathbf{L}}_{\mathbf{E}} + \mathbf{S}_{22}\underbrace{\mathbf{V}_{22}\mathbf{L}}_{\mathbf{F}} + \mathbf{N}_1. \tag{17}$$

Let $z_{k,ij}$ and $n_{k,ij}$ be the (i, j)th elements of the $\mathbf{Z}_k$ and $\mathbf{N}_k \in \mathbb{C}^{3\times 1}$, respectively, and let c_{ij}, d_{ij}, e_{ij}, and f_{ij} be the (i, j)th elements of the matrices $\mathbf{C}$, $\mathbf{D}$, $\mathbf{E}$, and $\mathbf{F} \in \mathbb{C}^{2\times 1}$, respectively, and then the system can be rewritten as

$$\begin{aligned}\tilde{\mathbf{z}}_1 = &\begin{bmatrix} c_{11} & c_{21} & e_{11} & e_{21} \\ c_{21}^* & -c_{11}^* & e_{21}^* & -e_{11}^* \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \hat{\mathbf{s}}_{11} \\ \hat{\mathbf{s}}_{21} \end{bmatrix} \\ &+ \begin{bmatrix} 0 & 0 & 0 & 0 \\ d_{21}^* & -d_{11}^* & f_{21}^* & -f_{11}^* \\ d_{11} & d_{21} & f_{11} & f_{21} \end{bmatrix} \begin{bmatrix} \mathbf{s}_{12} \\ \mathbf{s}_{22} \end{bmatrix} + \tilde{\mathbf{n}}_1,\end{aligned} \tag{18}$$

where

$$\begin{aligned}\tilde{\mathbf{z}}_1 &= \begin{bmatrix} z_{1,11} \\ z_{1,21}^* \\ z_{1,31} \end{bmatrix}, \\ \tilde{\mathbf{n}}_1 &= \begin{bmatrix} n_{1,11} \\ n_{1,21}^* \\ n_{1,31} \end{bmatrix}.\end{aligned} \tag{19}$$

Combining (15) and (18) yields the following:

$$\begin{bmatrix} \hat{\mathbf{z}}_1 \\ \hat{\mathbf{z}}_2 \end{bmatrix} = \begin{bmatrix} \hat{\mathbf{D}}_1 \\ \hat{\mathbf{D}}_2 \end{bmatrix} \mathbf{s}_{12} + \begin{bmatrix} \hat{\mathbf{F}}_1 \\ \hat{\mathbf{F}}_2 \end{bmatrix} \mathbf{s}_{22} + \begin{bmatrix} \hat{\mathbf{n}}_1 \\ \hat{\mathbf{n}}_2 \end{bmatrix}. \tag{20}$$

Let $\tilde{z}_{1i}$ and $\tilde{n}_{1i}$ be the ith elements of $\tilde{\mathbf{z}}_1$ and $\tilde{\mathbf{n}}_1$, respectively, and then

$$\begin{aligned}\hat{\mathbf{z}}_1 &= \begin{bmatrix} \tilde{z}_{13} \\ \theta_1 \end{bmatrix}, \\ \hat{\mathbf{z}}_2 &= \begin{bmatrix} \tilde{y}_{13} \\ \tilde{y}_{16} \end{bmatrix}, \\ \hat{\mathbf{n}}_1 &= \begin{bmatrix} \tilde{n}_{13} \\ \tilde{n}_{12} \end{bmatrix}, \\ \hat{\mathbf{n}}_2 &= \begin{bmatrix} \tilde{w}_{13} \\ \tilde{w}_{16} \end{bmatrix}, \\ \hat{\mathbf{D}}_1 &= \begin{bmatrix} d_{11} & d_{21} \\ d_{21}^* & -d_{11}^* \end{bmatrix}, \\ \hat{\mathbf{F}}_1 &= \begin{bmatrix} f_{11} & f_{21} \\ f_{21}^* & -f_{11}^* \end{bmatrix}, \\ \hat{\mathbf{D}}_2 &= \alpha_{\mathbf{H}}\mathbf{I}, \\ \hat{\mathbf{F}}_2 &= \alpha_{\mathbf{G}}\mathbf{I},\end{aligned} \tag{21}$$

where $\theta_1 = (\tilde{z}_{12} - c_{21}^* \hat{s}_{11}^1 + c_{11}^* \hat{s}_{11}^2 - e_{21}^* \hat{s}_{21}^1 + e_{11}^* \hat{s}_{21}^2)$. The elements of $\mathbf{s}_{12}$ are decoupled as follows:

$$\begin{aligned}\underbrace{\frac{\hat{\mathbf{F}}_1^H}{\|\hat{\mathbf{F}}_1\|^2}\hat{\mathbf{z}}_1 - \frac{\hat{\mathbf{F}}_2^H}{\|\hat{\mathbf{F}}_2\|^2}\hat{\mathbf{z}}_2}_{\check{\mathbf{z}}_1} = &\underbrace{\left(\frac{\hat{\mathbf{F}}_1^H}{\|\hat{\mathbf{F}}_1\|^2}\hat{\mathbf{D}}_1 - \frac{\hat{\mathbf{F}}_2^H}{\|\hat{\mathbf{F}}_2\|^2}\hat{\mathbf{D}}_2\right)}_{\check{\mathbf{G}}_1}\mathbf{s}_{12} \\ &+ \underbrace{\frac{\hat{\mathbf{F}}_1^H}{\|\hat{\mathbf{F}}_1\|^2}\hat{\mathbf{n}}_1 - \frac{\hat{\mathbf{F}}_2^H}{\|\hat{\mathbf{F}}_2\|^2}\hat{\mathbf{n}}_2}_{\check{\mathbf{n}}_1}.\end{aligned} \tag{22}$$

The matrices $\hat{\mathbf{D}}_1$, $\hat{\mathbf{D}}_2$, $\hat{\mathbf{F}}_1$, and $\hat{\mathbf{F}}_2$ still have the Alamouti structure, and hence $\check{\mathbf{G}}_1$ also has the Alamouti structure. The simple conventional Alamouti decoding is still applicable. Also, $\mathbf{s}_{22}$ can be decoded in a similar way due to the system symmetry.

Note that the SNR of $\mathbf{s}_{12}$ and $\mathbf{s}_{22}$ in $\hat{\mathbf{z}}_2$ is much lower than that in $\hat{\mathbf{z}}_1$ due to the low average power of $\alpha_{\mathbf{H}}$ and $\alpha_{\mathbf{G}}$. This leads to degradation in the performance of $\mathbf{s}_{12}$ and $\mathbf{s}_{22}$. In the following section, we investigate the receiver structure for decoding $\mathbf{s}_{12}$ and $\mathbf{s}_{22}$ with better error performance and a diversity order of 2; the same diversity of the intended symbols.

3.3. Case 3: Number of Eavesdropping Antennas = 2. Equation (17) can be still used to model the system for $n_E = 2$, with the exception that $\mathbf{Z}_k$ and $\mathbf{N}_k \in \mathbb{C}^{3\times 2}$ and the matrices $\mathbf{C}$, $\mathbf{D}$, $\mathbf{E}$, and $\mathbf{F} \in \mathbb{C}^{2\times 2}$. Since the leaked information about the unintended symbols in the first $n_R = 2$ receive antennas experiences low SNR, we will discard this leaked information and consider only the leaked information from $n_E = 2$ eavesdropping antennas. In contrast to the case of $n_E = 1$, the leaked information via the $n_E = 2$ eavesdropping antennas is sufficient to accurately recover the unintended symbols. As such, the system can be written as

$$\begin{aligned}\tilde{\mathbf{z}}_1 = &\begin{bmatrix} c_{11} & c_{21} & e_{11} & e_{21} \\ c_{21}^* & -c_{11}^* & e_{21}^* & -e_{11}^* \\ 0 & 0 & 0 & 0 \\ c_{12} & c_{22} & e_{12} & e_{22} \\ c_{22}^* & -c_{12}^* & e_{22}^* & -e_{12}^* \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \hat{\mathbf{s}}_{11} \\ \hat{\mathbf{s}}_{21} \end{bmatrix} \\ &+ \begin{bmatrix} 0 & 0 & 0 & 0 \\ d_{21}^* & -d_{11}^* & f_{21}^* & -f_{11}^* \\ d_{11} & d_{21} & f_{11} & f_{21} \\ 0 & 0 & 0 & 0 \\ d_{22}^* & -c_{12}^* & f_{22}^* & -f_{12}^* \\ d_{12} & d_{22} & f_{12} & f_{22} \end{bmatrix} \begin{bmatrix} \mathbf{s}_{12} \\ \mathbf{s}_{22} \end{bmatrix} + \tilde{\mathbf{n}}_1,\end{aligned} \tag{23}$$

where

$$\tilde{\mathbf{z}}_1 = \begin{bmatrix} z_{1,11} \\ z_{1,21}^* \\ z_{1,31} \\ z_{1,12} \\ z_{1,22}^* \\ z_{1,23} \end{bmatrix}, \quad \tilde{\mathbf{n}}_1 = \begin{bmatrix} n_{1,11} \\ n_{1,21}^* \\ n_{1,31} \\ n_{1,12} \\ n_{1,22}^* \\ n_{1,23} \end{bmatrix}. \tag{24}$$

The system can be rewritten in the form of (20) with

$$\begin{aligned} \hat{\mathbf{z}}_1 &= \begin{bmatrix} \tilde{z}_{13} \\ \theta_2 \end{bmatrix}, \\ \hat{\mathbf{z}}_2 &= \begin{bmatrix} \tilde{z}_{16} \\ \theta_3 \end{bmatrix}, \\ \hat{\mathbf{n}}_1 &= \begin{bmatrix} \tilde{n}_{13} \\ \tilde{n}_{12} \end{bmatrix}, \\ \hat{\mathbf{n}}_1 &= \begin{bmatrix} \tilde{n}_{16} \\ \tilde{n}_{15} \end{bmatrix}, \\ \widehat{\mathbf{D}}_i &= \begin{bmatrix} d_{1i} & d_{2i} \\ d_{2i}^* & -d_{1i}^* \end{bmatrix}, \\ \widehat{\mathbf{F}}_i &= \begin{bmatrix} f_{1i} & f_{2i} \\ f_{2i}^* & -f_{1i}^* \end{bmatrix}, \end{aligned} \tag{25}$$

where $\theta_2 = (\tilde{z}_{12} - c_{21}^* \hat{s}_{11}^1 + c_{11}^* \hat{s}_{11}^2 - e_{21}^* \hat{s}_{21}^1 + e_{11}^* \hat{s}_{21}^2)$ and $\theta_3 = (\tilde{z}_{15} - c_{22}^* \hat{s}_{11}^1 + c_{12}^* \hat{s}_{11}^2 - e_{22}^* \hat{s}_{21}^1 + e_{12}^* \hat{s}_{21}^2)$. The vectors $\mathbf{s}_{12}$ and $\mathbf{s}_{22}$ are then decoded the same as in the case of $n_E = 1$. From (25), which is similar to the model representing the intended symbols, we can conclude that the diversity order for the unintended symbols is equal to 2 [9].

4. Mutual Information and Secrecy Sum Rate

4.1. Mutual Information at the Intended Receivers. Again, we focus on receiver 1, where due to system symmetry the same analysis applies to receiver 2. Let $\mathbf{s}_{11} \in \Omega^{2\times 1}$ be the transmitted vector such that $\mathbb{E}[\mathbf{s}_{11}\mathbf{s}_{11}^H] = \mathbf{I}_2$, and let $\check{\mathbf{y}}_1 \in \mathbb{C}^{2\times 1}$ be the equivalent received vector defined in (13). Then, the mutual information between $\mathbf{s}_{11}$ and $\check{\mathbf{y}}$ at receiver 1 is given by

$$I\left(\mathbf{s}_{11}, \check{\mathbf{y}}_1 \mid \check{\mathbf{H}}_1\right) = \log\left\{\det\left(\mathbf{I}_2 + \check{\mathbf{H}}_1 \mathbf{R}_{\check{\mathbf{w}}}^{-1} \check{\mathbf{H}}_1^H\right)\right\}, \tag{26}$$

where $\check{\mathbf{H}}_1$ is the effective channel matrix and $\mathbf{R}_{\check{\mathbf{w}}}$ is the covariance matrix of the equivalent noise. Let

$$\begin{aligned} \widehat{\Theta}_1 &\in \mathbb{C}^{2\times 4} = \left[\frac{\widehat{\mathbf{G}}_1^H}{\left\|\widehat{\mathbf{G}}_1\right\|^2} - \frac{\widehat{\mathbf{G}}_2^H}{\left\|\widehat{\mathbf{G}}_2\right\|^2}\right], \\ \widehat{\Psi}_1 &\in \mathbb{C}^{4\times 2} = \left[\widehat{\mathbf{H}}_1^t \;\; \widehat{\mathbf{H}}_2^t\right]^t, \\ \widehat{\Xi}_1 &\in \mathbb{C}^{4\times 1} = \left[\widehat{\mathbf{w}}_1^t \;\; \widehat{\mathbf{w}}_2^t\right]^t, \end{aligned} \tag{27}$$

and then (13) can be rewritten as

$$\check{\mathbf{y}}_1 = \widehat{\Theta}_1 \widehat{\Psi}_1 \mathbf{s}_{11} + \widehat{\Theta}_1 \widehat{\Xi}_1. \tag{28}$$

As such, $\mathbf{R}_{\check{\mathbf{w}}} = \widehat{\Theta}_1 \mathbf{R}_{\widehat{\Xi}_1} \widehat{\Theta}_1^H$, where $\mathbf{R}_{\widehat{\Xi}_1} = \sigma_n^2 \cdot \mathrm{diag}(1, 2, 1, 2)$. Due to the system symmetry, the overall mutual information of the intended symbols at receiver 1 and receiver 2 can be given by

$$I_i = 4 \cdot \log\left\{\det\left(\mathbf{I}_2 + \check{\mathbf{H}}_1 \mathbf{R}_{\check{\mathbf{w}}}^{-1} \check{\mathbf{H}}_1^H\right)\right\}, \tag{29}$$

with $\check{\mathbf{H}}_1 = \widehat{\Theta}_1 \widehat{\Psi}_1$.

4.2. Mutual Information at the Unintended Receivers. At receiver 1, leaked information can be used to decode $\mathbf{s}_{12}$ and $\mathbf{s}_{22}$. Evidently, the amount of leaked information decides the accuracy of the decoding process. In the following, we investigate the mutual information in the case of 1 and 2 eavesdropping antennas.

4.2.1. Case 1: Number of Eavesdropping Antennas = 1. Based on (21), the mutual information is given by

$$\begin{aligned} I\left(\mathbf{s}_{12}, \check{\mathbf{z}}_1 \mid \check{\mathbf{G}}_1\right) &= \log\left\{\det\left(\mathbf{I}_2 + \check{\mathbf{G}}_1 \mathbf{R}_{\check{\mathbf{n}}}^{-1} \check{\mathbf{G}}_1^H\right)\right\} \\ \widehat{\Theta}_2 &\in \mathbb{C}^{2\times 4} = \left[\frac{\widehat{\mathbf{F}}_1^H}{\left\|\widehat{\mathbf{F}}_1\right\|^2} - \frac{\widehat{\mathbf{F}}_2^H}{\left\|\widehat{\mathbf{F}}_2\right\|^2}\right], \\ \widehat{\Psi}_2 &\in \mathbb{C}^{4\times 2} = \left[\widehat{\mathbf{D}}_1^t \;\; \widehat{\mathbf{D}}_2^t\right]^t, \\ \widehat{\Xi}_2 &\in \mathbb{C}^{4\times 1} = \left[\hat{\mathbf{n}}_1^t \;\; \hat{\mathbf{n}}_2^t\right]^t. \end{aligned} \tag{30}$$

Note that the elements of $\hat{\mathbf{n}}_1$ and $\hat{\mathbf{n}}_2$ are i.i.d. with equal variance of σ_n^2; therefore $\mathbf{R}_{\check{\mathbf{n}}} = \sigma_n^2 \cdot \widehat{\Theta}_2 \widehat{\Theta}_2^H$. Finally, the overall mutual information of the unintended symbols at receiver 1 and receiver 2 can be given by

$$\begin{aligned} I_u &= 4 \cdot \log\left\{\det\left(\mathbf{I}_2 + \check{\mathbf{G}}_1 \mathbf{R}_{\check{\mathbf{n}}}^{-1} \check{\mathbf{G}}_1^H\right)\right\} \\ &= 4 \cdot \log\left\{\det\left(\mathbf{I}_2 + \frac{1}{\sigma_n^2} \check{\mathbf{G}}_1 \left(\widehat{\Theta}_2 \widehat{\Theta}_2^H\right)^{-1} \check{\mathbf{G}}_1^H\right)\right\}, \end{aligned} \tag{31}$$

with $\check{\mathbf{G}}_1 = \widehat{\Theta}_2 \widehat{\Psi}_2$.

4.2.2. Case 2: Number of Eavesdropping Antennas = 2. Equation (31) still applies for the case of $n_E = 2$, with the exception that $\check{\mathbf{z}}_1$, $\hat{\mathbf{n}}_1$, $\hat{\mathbf{n}}_2$, $\widehat{\mathbf{D}}_1$, $\widehat{\mathbf{D}}_2$, $\widehat{\mathbf{F}}_1$, and $\widehat{\mathbf{F}}_2$ are given in (23)–(25).

4.3. Secrecy Sum Rate. Finally, the secrecy sum rate is given by [11]

$$R_s = \underset{\check{\mathbf{H}}_1,\widehat{\Theta}_1}{\mathbb{E}}\left[I_i\right] - \underset{\check{\mathbf{G}}_1,\widehat{\Theta}_2}{\mathbb{E}}\left[I_u\right]. \tag{32}$$

Although a negative value of the mathematical expression for R_s is unrealistic, we will keep it for the sake of comparison. Note that a negative sign of R_s means that the eavesdropper has information about the unintended data symbols, which is used in the decoding process, more than that available at the intended receiver, for the same data symbols.

5. Achieving Confidentiality Using Interleaved Pseudorandom Rotation-Based Transformation

In this section, we propose to geometrically transform the data symbols sent from each of the transmitters such that each receiver cannot decode unintended symbols using the leaked information. To this end, we propose to use the rotation-based transformation (RBT), which has been extensively used for privacy preserving data mining, among other fields [16]. The main idea of RBT is to precode the data using orthogonal matrix, referred to as rotation matrix, such that both the power of each data symbol and the distance between symbols are preserved. A two-dimensional rotation matrix is given by

$$\mathbf{R}_{\theta_{ij}^k} = \begin{bmatrix} \cos\left(\theta_{ij}^k\right) & \sin\left(\theta_{ij}^k\right) \\ -\sin\left(\theta_{ij}^k\right) & \cos\left(\theta_{ij}^k\right) \end{bmatrix}, \tag{33}$$

where $\mathbf{R}_{\theta_{ij}^k}^t \mathbf{R}_{\theta_{ij}^k} = \mathbf{R}_{\theta_{ij}^k} \mathbf{R}_{\theta_{ij}^k}^t = \mathbf{I}$ and θ_{ij}^k is the counterclockwise rotation angle for the kth data symbol, for $k = 1, 2$, transmitted from transmitter i to receiver j, with $\theta_{11}^1 \neq \theta_{11}^2 \neq \theta_{12}^1 \neq \theta_{12}^2 \neq \theta_{21}^1 \neq \theta_{21}^2 \neq \theta_{22}^1 \neq \theta_{22}^2$. Each receiver knows a priori the angles used at the transmitters to rotate its intended data symbols; that is, receiver j knows only θ_{ij}^k for $i, k = 1, 2$. Based on that, the symbol s_{ij}^k is rotated at transmitter i to produce u_{ij}^k as follows:

$$\begin{bmatrix} \text{real}\left(u_{ij}^k\right) \\ \text{imag}\left(u_{ij}^k\right) \end{bmatrix} = \mathbf{R}_{\theta_{ij}^k} \begin{bmatrix} \text{real}\left(s_{ij}^k\right) \\ \text{imag}\left(s_{ij}^k\right) \end{bmatrix}. \tag{34}$$

The symbols $\mathbf{u}_{ij}$ are then encoded using the STBC block as shown in Figure 3 before being beamformed, linearly combined, and transmitted as in (3). Since each receiver knows the rotation matrices applied to its intended symbols, it can *only* decode its intended symbols. That is, without knowing other receiver's rotation matrices, receiver cannot use the leaked information to recover the unintended symbols.

At the receiver side, rotated intended symbols, $\tilde{\mathbf{u}}_{ij}$, are recovered as in (14). The intended symbols are therefore given by

$$\begin{bmatrix} \text{real}\left(\tilde{s}_{ij}^k\right) \\ \text{imag}\left(\tilde{s}_{ij}^k\right) \end{bmatrix} = \mathbf{R}_{\theta_{ij}^k}^t \begin{bmatrix} \text{real}\left(\tilde{u}_{ij}^k\right) \\ \text{imag}\left(\tilde{u}_{ij}^k\right) \end{bmatrix}. \tag{35}$$

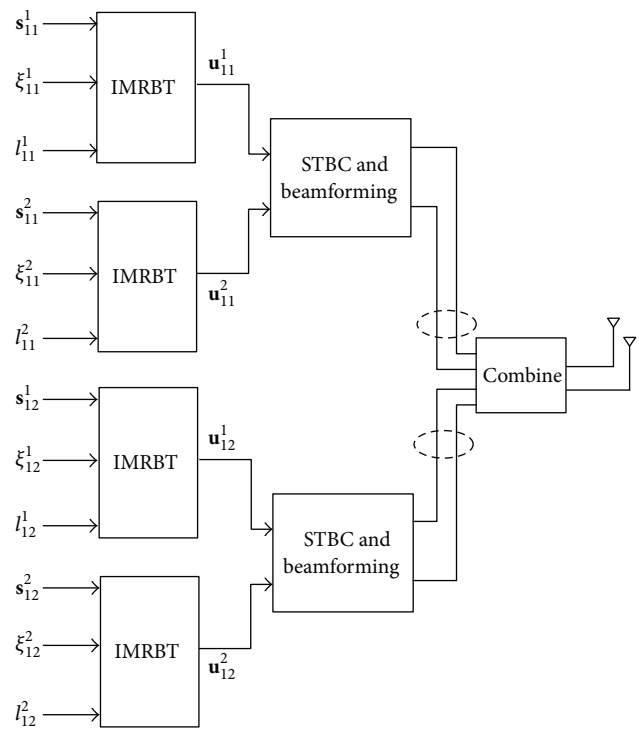

Figure 3: System model of transmitter 1 in a 2-user X channel configuration with IMRBT.

Although RBT scheme is simple and cost-efficient, it is effective to avoid eavesdropping. However, a drawback of this scheme might arise when the eavesdropper tries to recover unintended symbols by applying brute-force scheme to estimate the rotation angles. Even though employing the brute-force scheme is costly in terms of power consumption and hence impractical for power- and memory-limited wireless devices, we will discuss a method to overcome this drawback. Mohaisen and Hong proposed a multiple RBT (MRBT) in which each packet of length m is divided into v subpackets and each is rotated using a different rotation matrix [17]. Using the MRBT algorithm in our system has two advantages: eavesdropper requires to (i) estimate $2 \times v$ angles instead of only two angles and (ii) avoid statistical attacks such as the a priori knowledge-independent component analysis (AK-ICA) [18], which requires longer observations of data symbols rotated using the same rotation matrix. This MRBT algorithm might become vulnerable if the eavesdropper has a partial preknowledge on the structure of eavesdropped data symbols, helping him to recover the message. To randomize the data before rotation, we propose to interleave the data symbols before being rotated, leading to an interleaved MRBT (IMRBT) algorithm, that makes it practically impossible to recover the original data even with the preknowledge on the structure of the unintended data.

To integrate the IMRBT scheme in our system, we first introduce the following settings:

(1) We consider that transmitter i, for $i = 1, 2$, has two packets, $\mathbf{s}_{i1}$ and $\mathbf{s}_{i2}$, each of length m, intended for receiver 1 and 2, respectively.

(2) Each of these packets of length m is split into two equal-size subpackets $\mathbf{s}_{ij}^1 = [s_{ij,1}^1, s_{ij,2}^1, \ldots, s_{ij,n}^1]$ and $\mathbf{s}_{ij}^2 = [s_{ij,1}^2, s_{ij,2}^2, \ldots, s_{ij,n}^2]$, for $i, j = 1, 2$ and $n = m/2$.

(3) Transmitter i, for $i = 1, 2$, has *four* pseudorandom interleaving sequences $\boldsymbol{\pi}_{ij}^k = [\pi_{ij,1}^k, \pi_{ij,2}^k, \ldots, \pi_{ij,n}^k]$ for $j, k = 1, 2$, which are used to interleave symbols $\mathbf{s}_{ij}^k$; that is, $\boldsymbol{\pi}_{i1}^1$ is used to interleave $\mathbf{s}_{i1}^1$, resulting in the interleaved subpacket $\bar{\mathbf{s}}_{i1}^1$ and so forth.

(4) Transmitter i, for $i = 1, 2$, has *four* pseudorandom rotation sequences $\boldsymbol{\theta}_{ij}^k = [\theta_{ij,1}^k, \theta_{ij,2}^k, \ldots, \theta_{ij,n}^k]$ for $j, k = 1, 2$, which are used to rotate symbols $\bar{\mathbf{s}}_{ij}^k$ resulting in the rotated subpackets $\mathbf{u}_{i1}^k$; that is, $\boldsymbol{\theta}_{i1}^1$ is used to rotate $\bar{\mathbf{s}}_{i1}^1$, and hence $\theta_{i1,l}^1$ rotates $\bar{s}_{i1,l}^1$ and so forth.

Accordingly, the IMRBT is applied as follows:

(1) Receiver j, for $j = 1, 2$, picks four random offsets l_{ij}^k that are associated with $\boldsymbol{\theta}_{ij}^k$, for $i, k = 1, 2$. These offsets are sent to the corresponding ith transmitter, for $i = 1, 2$, at the initiation stage preceding the transmission of the data packet.

(2) Receiver j, for $j = 1, 2$, picks four random offsets ξ_{ij}^k that are associated with $\boldsymbol{\pi}_{ij}^k$, for $i, k = 1, 2$. These offsets are sent to the corresponding ith transmitter, for $i = 1, 2$, at the initiation stage.

(3) At transmitter i, for $i = 1, 2$, the four streams $\mathbf{s}_{ij}^k$, for $j, k = 1, 2$, are interleaved using the interleaving sequences that are rearranged as $[\pi_{ij,\xi_{ij}^k}^k, \pi_{ij,\xi_{ij}^k+1}^k, \ldots, \pi_{ij,n}^k, \ldots, \pi_{ij,\xi_{ij}^k-1}^k]$, for $j, k = 1, 2$, to obtain the interleaved streams $\bar{\mathbf{s}}_{ij}^k$, for $j, k = 1, 2$, respectively.

(4) At transmitter i, for $i = 1, 2$, the four streams $\bar{\mathbf{s}}_{ij}^k$, for $j, k = 1, 2$, are rotated using the rotation matrices, whose associated rotation angles are rearranged as $[\theta_{ij,l_{ij}^k}^k, \theta_{ij,l_{ij}^k+1}^k, \ldots, \theta_{ij,n}^k, \ldots, \theta_{ij,l_{ij}^k-1}^k]$, for $j, k = 1, 2$, to obtain the rotated streams $\mathbf{u}_{ij}^k$, for $j, k = 1, 2$.

From the IMRBT scheme description, it is evident that the interleavers $\boldsymbol{\pi}_{ij}^k$ and the rotation angles $\boldsymbol{\theta}_{ij}^k$, for $i, j, k = 1, 2$, are static, that is, having fixed sequences. Hence, they might be estimated using statistical analysis, which requires long observations of the unintended data symbols. That is why the random offsets ξ_{ij}^k and l_{ij}^k, for $i, j, k = 1, 2$, are used to reset the statistical analysis, hence adding further immunity to eavesdropping in the proposed system under the aforementioned type of attacks.

After applying the proposed IMRBT scheme on the data subpackets, the rotated subpackets are encoded using the STBC block, beamformed, linearly combined, and transmitted via the 2 transmit antennas. The block diagram of transmitter 1 deploying the proposed IMRBT is depicted in Figure 3. At the intended receiver, after the decoding process, the received symbols are derotated and deinterleaved to recover the intended data symbols. Since the eavesdropper does not have any of the parameters necessary to recover the unintended data symbols, our proposed system assures full confidentiality of the transmission over the X channel with interference alignment depicted in Figure 1.

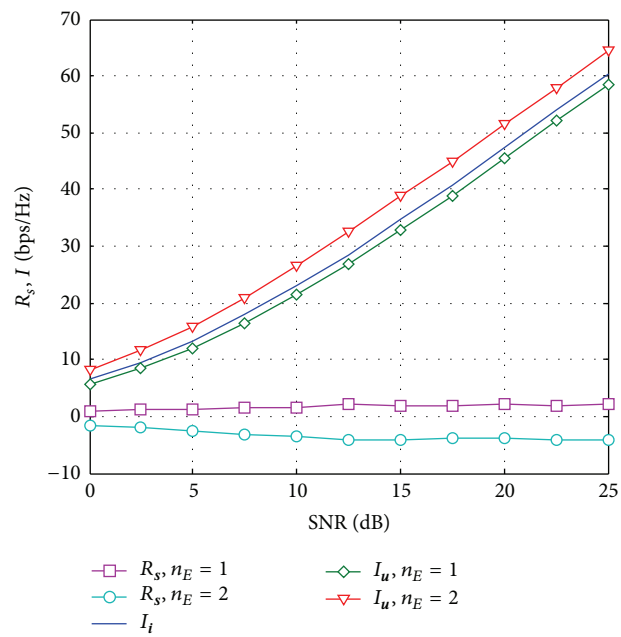

Figure 4: Mutual information and secrecy sum rate versus SNR for $n_E = 1$ and $n_E = 2$. The depicted values are the average over 5,000 independent trials.

Finally, it is worth mentioning that the IMRBT scheme is only applied to complex-valued modulation sets such as quadrature-amplitude modulation (QAM) or phase-shift keying (PSK) modulation. This is not a limitation to our proposed scheme since future generation communication systems, such as long-term evolution (LTE) and LTE-advanced, use only QPSK, 16-QAM, or 64-QAM, which are complex-valued modulation scheme, for data modulation [19].

6. Simulation Results and Discussion

We consider that each transmitter has perfect knowledge of the channels coupling its transmit antennas and n_R receive antennas of the two receivers. The elements of the channel matrices are i.i.d. complex Gaussian with zero mean and unit variance. For the transmitted symbols s_{ij}^k, for $i, j, k = 1, 2$, each has an average power of unity. The noise variance at each receive antenna is set, in accordance with [9], to $2/3\rho$ with ρ as the SNR.

Figure 4 shows the mutual information and the SSR for the system depicted in Figure 1 for $n_E = 1$ and $n_E = 2$. Since $n_R = 2$ antennas are used to receive the intended symbols, the mutual information of the intended symbols I_i is independent of the value of n_E. However, when the number of eavesdropping antennas increases, the amount of leaked

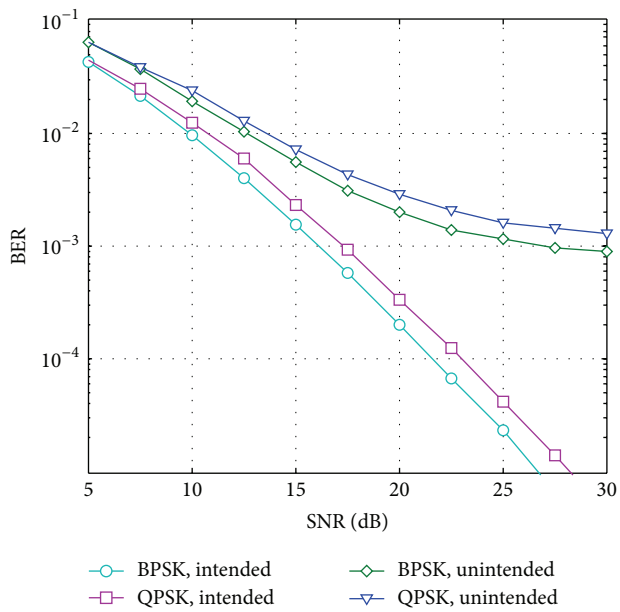

Figure 5: BER of the intended and unintended symbols for $n_E = 1$ and both BPSK and QPSK modulation schemes.

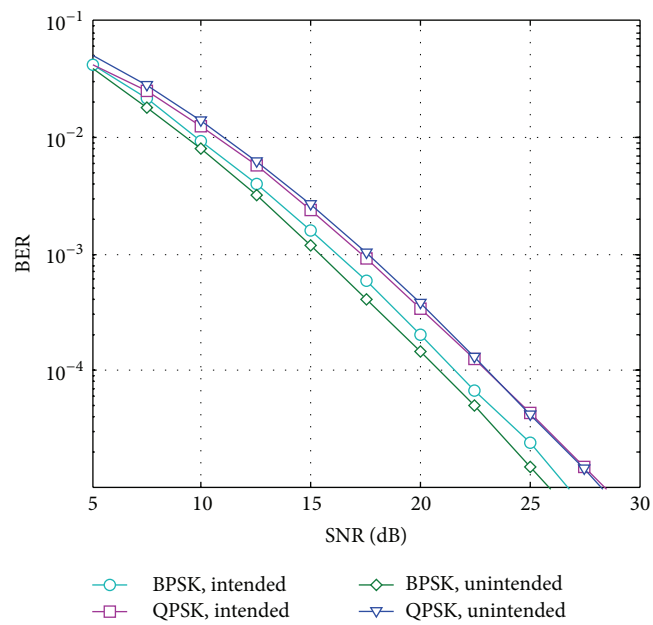

Figure 6: BER of the intended and unintended symbols for $n_E = 2$ and both BPSK and QPSK modulation schemes.

information about the the unintended symbols (I_u) also increases. In the case of $n_E = 1$, I_u is less than I_i because the leaked information about the unintended symbols at the first $n_R = 2$ antennas has low SNR as explained earlier. To collect information sufficient to recover the unintended symbols, the leaked information at $n_R = 2$ antennas is combined with that received at the $n_E = 1$ eavesdropping antenna. Note that, in this case, the noise affecting the unintended symbols is still i.i.d. with equal variances. In the case $n_E = 2$, the leaked information about the unintended symbols at the two eavesdropping antennas is sufficient to recover those symbols without requiring the leaked information at the first $n_R = 2$ antennas, where symbols suffer high noise power. It is worth mentioning that the removal of alignment interference increases the noise variance affecting the intended symbols, leading to degradation in the mutual information and hence in the BER performance. On the other hand, the unintended symbols are recovered by first removing the intended symbols via SIC, leaving the noise variance intact. Hence, if intended symbols are error-free, the error performance of the unintended symbols is superior to that of the intended symbols, as will be explained later.

Figure 5 depicts the bit error rate (BER) of the intended and unintended data symbols using both binary and quadrature phase shift keying (BPSK and QPSK, resp.) with $n_E = 1$. The diversity order, as proved in [9], equals 2 for the intended symbols with a superior BER performance when BPSK modulation is used as compared to using QPSK modulation. However at high SNR values, an error floor appears in the BER curves associated with the unintended symbols. This is due to the low SNR value of the leaked information of the unintended symbols in the first $n_R = 2$ antennas, leading to an overall degradation in the BER.

Figure 6 shows the BER of intended and unintended symbols for $n_E = 2$ with BPSK and QPSK modulations. In the case of BPSK, the BER performance of the unintended symbols is superior to that of the intended symbols. This is due to the noise amplification imposed due to the decoding structure of the intended symbols, which does not exist in the decoding process of the unintended symbols. However, the performance of the unintended symbols, in terms of BER, is affected by error propagation due to the SIC stage, where the intended symbols are removed. The effect of the SIC is not apparent when the BPSK in employed, where the unintended symbols have better BER performance in all the simulated range of values of SNR. In the case of QPSK, the error propagation due to the SIC stage comes into play, where at low to medium SNR values (<23 dB) the performance of the intended symbols is slightly superior to that of the unintended symbols. At higher SNR values, the performance of the unintended symbols starts to slightly become superior to that of the intended symbols due to the decreased effect of the error propagation.

Figure 7 depicts the BER of the intended and unintended symbols with IMRBT using QPSK modulation. To obtain these results, a different angle is used for each symbol at each channel use. For instance, angle $\theta_{ij,l}^{k}$ is used to rotate symbol s_{ij}^{k} at the lth channel use. This implies that the interleaved symbols $\bar{\mathbf{s}}_{11}, \bar{\mathbf{s}}_{12}, \bar{\mathbf{s}}_{21}$, and $\bar{\mathbf{s}}_{22}$ are rotated using independent angles at each channel use l. Since the intended receiver has prior knowledge of the rotation angles of its designated symbols, it can recover those symbols after employing the decoding procedure explained earlier, while the unintended receiver cannot recover the unintended symbols due to unknowing the interleaving and rotation parameters used at the transmitters to treat those symbols. As shown in Figure 7,

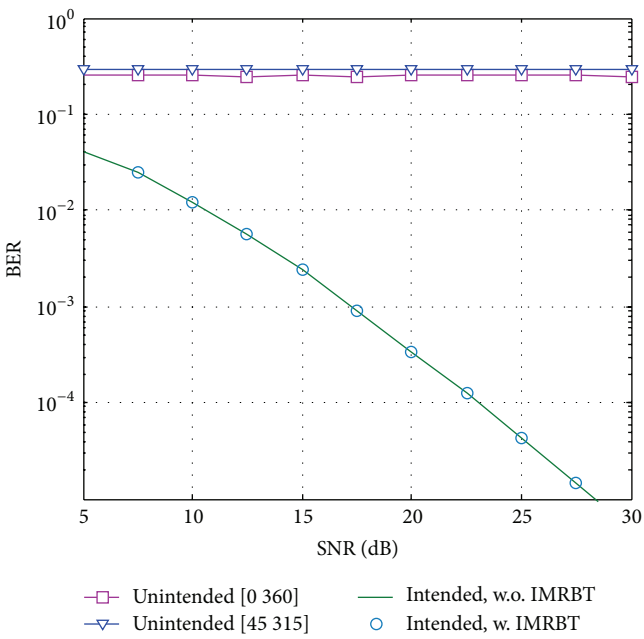

Figure 7: BER of the intended and unintended symbols with transmitters employing the proposed IMRBT scheme for $n_E = 2$ and QPSK modulation.

applying the IMRBT does not affect the BER performance of the intended symbols. However, the unintended receiver ignores the fact that symbols were rotated and decodes them without derotation, leading to degraded performance manifested by a fixed BER at about 0.3. Restricting the rotation angles to $[45, 315]$ leads to further improvement in the proposed algorithm since this assures that, after employing the proposed IMRBT scheme, each symbol will lie in the Voronoi region of other symbols from the constellation set Ω.

7. Conclusion

In this paper, we assumed that each receiver in the explained 2-user X channel system with interference alignment and STBC plays the role of an eavesdropper that, in addition to decoding its intended symbols, it decodes the symbols intended for the other receiver. We analyze the mutual information and SSRs in cases of a single and two eavesdropping antennas, where we propose decoding algorithms for the unintended symbols in both cases. Interestingly enough, we show that, in the case of two eavesdropping antennas, the performance of the eavesdropped symbols is superior to that of the intended symbols. As such, to guarantee confidentiality, hence rendering useless the leaked information about unintended symbols, we proposed an IMRBT scheme, which consists of two stages, namely, interleaving and orthogonal rotation. Interleaving neutralizes any a priori knowledge at the eavesdropper side about the structure of the transmitted packet, whereas the orthogonal transformation, which preserves both the power of and distance among the data symbols, rotates the data symbols in such a way the angular information of data symbols is perturbed. Knowing the interleaving and rotation parameters, intended receiver recovers the transmitted data, while unintended receiver cannot. Simulation results and discussions demonstrate the effectiveness of the proposed scheme.

Conflict of Interests

The author declares that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This work was supported by research subsidy by Korea University of Technology and Education (Korea Tech), for the period from 2014 to 2015.

References

[1] A. Iyer, C. Rosenberg, and A. Karnik, "What is the right model for wireless channel interference?" *IEEE Transactions on Wireless Communications*, vol. 8, no. 5, pp. 2662–2671, 2009.

[2] J. H. Lee, D. Toumpakaris, and W. Yu, "Interference mitigation via joint detection," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 6, pp. 1172–1184, 2011.

[3] W. Chen, K. B. Letaief, and Z. Cao, "Network interference cancellation," *IEEE Transactions on Wireless Communications*, vol. 8, no. 12, pp. 5982–5995, 2009.

[4] M. Mohaisen and K. H. Chang, "Maximum-likelihood co-channel interference cancellation with power control for cellular OFDM networks," in *Proceedings of the IEEE International Symposium on Communications and Information Technologies (ISCIT '07)*, pp. 198–202, October 2007.

[5] S. A. Jafar and S. Shamai, "Degrees of freedom region of the MIMO X channel," *IEEE Transactions on Information Theory*, vol. 54, no. 1, pp. 151–170, 2008.

[6] S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 8, pp. 1451–1458, 1998.

[7] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Transactions on Information Theory*, vol. 45, no. 5, pp. 1456–1467, 1999.

[8] H. El Gamal and R. Hammons Jr., "On the design of algebraic space-time codes for MIMO block-fading channels," *IEEE Transactions on Information Theory*, vol. 49, no. 1, pp. 151–163, 2003.

[9] L. Li, H. Jafarkhani, and S. Jafar, "When Alamouti codes meet interference alignment: transmission schemes for two-user X channel," in *Proceedings of the IEEE International Symposium on Information Theory Proceedings (ISIT '11)*, pp. 2717–2721, July 2011.

[10] M. Mohaisen and K. H. Chang, "Fixed-complexity sphere encoder for multi-user MIMO systems," *Journal of Communications and Networks*, vol. 13, no. 1, pp. 63–69, 2011.

[11] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, no. 4, pp. 2083–2114, 2011.

[12] G. Geraci, J. Yuan, A. Razi, and I. B. Collings, "Secrecy sum-rates for multi-user MIMO linear precoding," in *Proceedings*

of the 8th International Symposium on Wireless Communication Systems (ISWCS '11), pp. 286–290, November 2011.

[13] S. A. Fakoorian, H. Jafarkhani, and A. L. Swindlehurst, "Secure space-time block coding via artificial noise alignment," in *Proceedings of the Conference Record of the 45th Asilomar Conference on Signals, Systems and Computers (ASILOMAR '11)*, pp. 651–655, November 2011.

[14] T. Allen, J. Cheng, and N. Al-Dhahir, "Secure space-time block coding without transmitter CSI," *IEEE Wireless Communications Letters*, vol. 3, no. 6, pp. 573–576, 2014.

[15] A. T. Parameswaran, M. I. Husain, and S. Upadhyaya, "Is RSSI a reliable in sensor localization algorithms an experimental study," in *Proceedings of the International Symposium on Reliable Distributed Systems*, pp. 1–5, Niagara Falls, NY, USA, September 2009.

[16] S. Oliveira and O. Zaïane, "Privacy preserving clustering by data transformation," in *Proceedings of the Brazilian Symposium on Databases (SBBD '03)*, pp. 304–318, 2003.

[17] A. Mohaisen and D. Hong, "Mitigating the ICA attack against rotation-based transformation for privacy preserving clustering," *ETRI Journal*, vol. 30, no. 6, pp. 868–870, 2008.

[18] S. Guo and X. Wu, "Deriving private information from arbitrarily projected data," in *Proceedings of the 11th Pacific-Asia Conference on Advances in Knowledge Discovery and Data Mining (PAKDD '07)*, pp. 84–95, 2007.

[19] F. Khan, *LTE for 4G Mobile Broadband: Air Interface and Performance*, Cambridge University Press, Cambridge, UK, 2009.