Index Modulation Based Coordinate Interleaved Orthogonal Design for Secure Communications

Burak Ozpoyraz, *Student Member, IEEE*,
Ibrahim Yildirim, *Student Member, IEEE*,
and Ertugrul Basar, *Senior Member, IEEE*

***Abstract*—In this paper, we propose a physical layer security scheme that exploits a novel index modulation (IM) technique for coordinate interleaved orthogonal designs (CIOD). Utilizing the diversity gain of CIOD transmission, the proposed scheme, named CIOD-IM, provides an improved spectral efficiency by means of IM. In order to provide a satisfactory secrecy rate, we design a particular artificial noise matrix, which does not affect the performance of the legitimate receiver, while deteriorating the performance of the eavesdropper. We derive expressions of the ergodic secrecy rate and the theoretical bit error rate upper bound. In addition, we analyze the case of imperfect channel estimation by taking practical concerns into consideration. It is shown via computer simulations that the proposed scheme outperforms the existing IM-based schemes and might be a candidate for future secure communication systems.**

***Index Terms*—Index modulation, coordinate interleaved orthogonal designs, artificial noise, physical layer security.**

I. Introduction

Index modulation (IM) schemes have been gaining a tremendous interest over the years considering innovative ways to convey additional information [1]. Spatial modulation (SM), which employs IM by utilizing the indices of transmit antennas as an additional information source, has been a promising advancement on conventional multiple-input multiple-output (MIMO) transmission [1], [2]. In SM systems, inter-channel interference (ICI) and inter-antenna synchronization (IAS) can be prevented due to the activation of a single antenna during transmission. Besides, SM can reduce the hardware cost by using only a single RF chain. However, the broadcast nature of wireless communication channels introduces SM the risk of information leakage to eavesdroppers. Therefore, physical layer (PHY) security has attracted the attention of researchers in recent years. PHY security exploits the channel between the transmitter and the intended receiver in order to prevent information leakage. SM and PHY security exploit the same principle as they both utilize the randomness and uniqueness of wireless channels. SM based solutions originate new degrees of freedom for PHY security. There are numerous systems in the literature utilizing SM for PHY security. In [3], the authors proposed a precoding-aided SM (PSM) scheme, where the transmitter (Alice) is aware of the channel state information (CSI) of both intended receiver (Bob) and eavesdropper (Eve). Considering the passive eavesdropper case, where Alice is not aware of Eve, a secret PSM (SPSM) scheme is introduced in [4]. Here, along with a precoding matrix, which is constructed by zero-forcing method, a fast time-varying precoder is proposed to provide a further enhancement in the secrecy rate. The SPSM principle is integrated to multi-user (MU) systems in [5], where MU interference cancellation is implemented to improve the signal-to-interference plus noise ratio (SINR) at Bob. PHY security is explored using an artificial noise (AN) signal in [6]. In this study, a jamming signal, which lies in the null space of the channel between Alice and Bob, is transmitted along with an amplitude-phase modulation (APM) symbol. Moreover, the security performance of AN-aided SM is analyzed under the case of imperfect channel estimation in [7]. As a further improvement on earlier AN schemes, an AN cancellation scheme is introduced where transmit antenna selection (TAS) is applied to select a number of transmit antennas in [8]. Here, two AN signals cancel out each other at Bob using the knowledge of Bob's CSI. However, the BER performance of this system model is open to improvement through diversity techniques. Thus, in [9], Alamouti's space time block code (STBC) is utilized to provide diversity gain. Two AN signals are transmitted from the active antennas of Alamouti's scheme and they are cancelled out at Bob. Nonetheless, [9] has a strict limitation that Alice is always equipped with three antennas, which is not suitable for flexible large-scale MIMO systems.

Against this background, we propose a novel PHY security scheme for single-user (SU) multiple-input single-output (MISO) systems, which is called as CIOD-IM. The main motivation of our system is to ensure PHY security along with high spectral efficiency and diversity by means of a novel IM method and coordinate interleaved orthogonal designs (CIOD). In this system, we introduce a special AN matrix design that enables the cancellation of AN signals at Bob for each time slot. We analyzed the bit error rate (BER) as well as ergodic secrecy rate (ESR) performance over Rayleigh fading channels. In addition, we analyze the BER and ESR performance in the presence of imperfect channel estimation since it might be challenging to obtain perfect CSI in practice. Furthermore, the BER results are verified by the theoretical upper bounds. Our extensive computer simulations reveal that the proposed scheme outperforms the conventional [8] and the efficient Alamouti [9] schemes in terms of the secrecy and the BER performance. Finally, we note that the CIOD-IM scheme is suitable for future low-complexity and massive MIMO systems by providing satisfactory BER results.

II. System Model

In this section, we introduce the essentials of CIODs and the working principle of the CIOD-IM scheme.

A. Coordinate Interleaved Orthogonal Designs

We utilize CIOD in our system, which is a promising concept for MIMO systems. The main idea is the transmission of the in-phase and the quadrature components of APM symbols via different transmit antennas during different time slots to provide a diversity gain. Considering the specific CIOD for four transmit antennas, we note that two RF chains are required at each time slot which reduces the complexity.

Manuscript received September 21, 2020; revised January 9, 2021, March 5, 2021, and April 25, 2021; accepted April 27, 2021. Date of publication April 29, 2021; date of current version June 9, 2021. This work was supported by TUBITAK under Grant 218E035. The review of this article was coordinated by Dr. Jingon Joung. *(Corresponding author: Ertugrul Basar.)*

Burak Ozpoyraz and Ertugrul Basar are with the Communications Research and Innovation Laboratory (CoreLab), Department of Electrical and Electronics Engineering, Koç University, Sariyer Istanbul 34450, Turkey (e-mail: bozpoyraz20@ku.edu.tr; ebasar@ku.edu.tr).

Ibrahim Yildirim is with the Faculty of Electrical and Electronics Engineering, Istanbul Technical University, Istanbul 34469, Turkey (e-mail: yildirimib@itu.edu.tr).

Digital Object Identifier 10.1109/TVT.2021.3076688

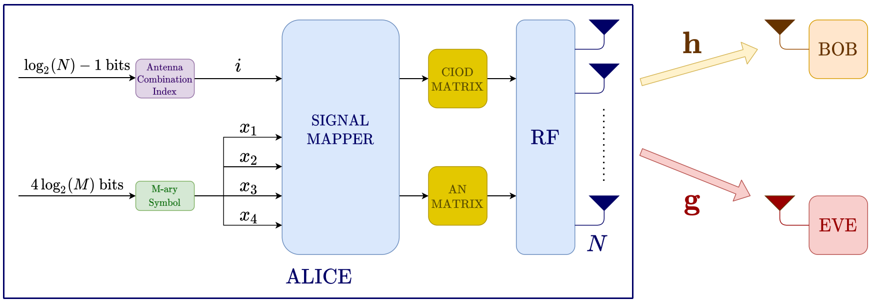

Fig. 1. The system model of the CIOD-IM scheme.

Conventional size 4 and rate 1 CIOD matrix is given by

$$\mathbf{S}(x_1,\ldots,x_4)=\begin{bmatrix}\boldsymbol{\theta}(\tilde{x}_1,\tilde{x}_2) & \mathbf{0}\\ \mathbf{0} & \boldsymbol{\theta}(\tilde{x}_3,\tilde{x}_4)\end{bmatrix}=\begin{bmatrix}\tilde{x}_1 & -\tilde{x}_2^* & 0 & 0\\ \tilde{x}_2 & \tilde{x}_1^* & 0 & 0\\ 0 & 0 & \tilde{x}_3 & -\tilde{x}_4^*\\ 0 & 0 & \tilde{x}_4 & \tilde{x}_3^*\end{bmatrix} \tag{1}$$

where $\tilde{x}_i=\Re\{x_i\}+\mathrm{j}\Im\{x_a\}, i\in\{1,\ldots,4\}$ with x_i representing the i^{th} symbol transmitted by the CIOD matrix, a equals to $3,4,1,2$ for increasing values of i, respectively, and $(.)^*$ denotes the complex conjugate. It should be noted that full diversity is achieved if and only if the coordinate product distance (CPD) of the constellation set Ω is different than zero. The CPD is given by $\Lambda=\min_{x_k\neq x'_k\in\Omega}|x_{kI}-x'_{kI}|.|x_{kQ}-x'_{kQ}|$ where x_{kI} and x_{kQ} represent the in-phase and the quadrature components of the k^{th} symbol, respectively. In order to satisfy this condition, constellations with $\Lambda=0$ such as QAM are rotated with a certain angle. The CPD is maximized for square lattice constellations and QPSK when the rotation angle is $\theta=31.7175^\circ$ and $\theta=13.2885^\circ$, respectively [10]. Another important feature of the CIOD transmission is its symbol-by-symbol detection capability which reduces the decoding complexity [11].

B. Proposed CIOD-IM Method

We consider a large-scale MISO secure communication system with a transmitter called Alice equipped with N transmit antennas, a legitimate receiver called Bob, and an eavesdropper called Eve, both equipped with a single receive antenna, as shown in Fig. 1. Here, $4\log_2(M)$ bits determine four M-ary APM symbols transmitted during four different time slots while $\log_2(N)-1$ bits determine an antenna combination from $N/2$ possible combinations. Therefore, the spectral efficiency is $l=(4\log_2(M)+\log_2(N)-1)/4$ bits per channel use (bpcu).

In practice, imperfect CSI can be faced due to the channel estimation errors. Therefore, we assume that the imperfect CSI of the main channel (Alice-to-Bob) is available at Alice and Bob, whereas the imperfect CSI of the eavesdropping channel (Alice-to-Eve) is only available at Eve. The main and the eavesdropping channels are given by [7]

$$\begin{aligned}\mathbf{h}&=\sqrt{1-\sigma^2}\mathbf{h}_{est}+\sqrt{\sigma^2}\mathbf{h}_{err},\\ \mathbf{g}&=\sqrt{1-\sigma^2}\mathbf{g}_{est}+\sqrt{\sigma^2}\mathbf{g}_{err}\end{aligned} \tag{2}$$

where $\mathbf{h}_{est}, \mathbf{h}_{err}, \mathbf{g}_{est}$, and $\mathbf{g}_{err}$ are $1\times N$ vectors indicating estimates and estimation errors of the main and the eavesdropping channels, respectively, and σ^2 is the power of estimation error. The entries of both main and eavesdropping channels are independent and identically distributed (i.i.d) complex Gaussian variables with zero-mean and unit-variance.

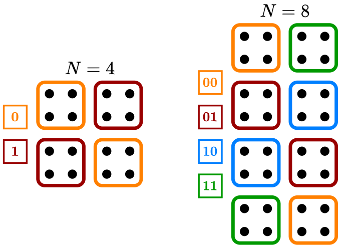

Fig. 2. The antenna combinations of the CIOD-IM scheme for $N=4$ and 8.

1) Novel Index Modulation: As shown in Fig. 2, antenna combination index bits select one of $N/2$ antenna combinations, where the IM is employed. Regardless of the selected antenna combination, the box on the left is filled with $\boldsymbol{\theta}(\tilde{x}_1,\tilde{x}_2)$ and on the right with $\boldsymbol{\theta}(\tilde{x}_3,\tilde{x}_4)$. When i^{th} antenna combination is selected where $i\in\{0,\ldots,N/2-1\}$, $(2i+1)^{\text{th}}$ and $(2i+2)^{\text{th}}$ antennas are active during the first two time slots while $(N-2i-1)^{\text{th}}$ and $(N-2i)^{\text{th}}$ antennas are active during the last two time slots, and the CIOD matrix is constructed by $\mathbf{S}_i=\sum_{k=1}^{4}\mathbf{A}_{2k-1,i}x_{kI}+\mathbf{A}_{2k,i}x_{kQ}$ where $\mathbf{A}_{u,i}, u\in\{1,\ldots,8\}$ are the complex weight matrices of the CIOD matrix when i^{th} antenna combination is selected, and $\mathbb{E}[|x_k|^2]=\alpha P_{tot}/8$, where α represents the power ratio allocated to the CIOD matrix, and P_{tot} represents the total transmit power. For example, assuming $N=8$ and antenna combination index bits of [0, 1] the transmitted CIOD matrix is obtained as

$$\mathbf{S}_1=\begin{bmatrix}\mathbf{0} & \mathbf{0}\\ \boldsymbol{\theta}(\tilde{x}_1,\tilde{x}_2) & \mathbf{0}\\ \mathbf{0} & \boldsymbol{\theta}(\tilde{x}_3,\tilde{x}_4)\\ \mathbf{0} & \mathbf{0}\end{bmatrix} \tag{3}$$

where $\mathbf{0}$ is a 2×2 all zeros matrix.

2) Artificial Noise Cancellation: In order to implement AN cancellation, the AN matrix of the i^{th} combination, $\mathbf{Z}_i$, should be carefully designed with respect to IM so that it is cancelled out while passing through the main channel. $\mathbf{Z}_i$ is constructed by replacing $\boldsymbol{\theta}(\tilde{x}_1,\tilde{x}_2)$ and $\boldsymbol{\theta}(\tilde{x}_3,\tilde{x}_4)$ in $\mathbf{S}_i$ with $\mathbf{Q}(z_{11},z_{21})$ and $\mathbf{Q}(z_{12},z_{22})$, respectively. Here, $\mathbf{Q}$ matrices are given as

$$\mathbf{Q}(z_{11},z_{21})=\begin{bmatrix}z_{11} & z_{11}\\ z_{21} & z_{21}\end{bmatrix}\ \mathbf{Q}(z_{12},z_{22})=\begin{bmatrix}z_{12} & z_{12}\\ z_{22} & z_{22}\end{bmatrix} \tag{4}$$

where $z_{lt}=\beta_{lt}v, l,t\in\{1,2\}$ is the AN signal transmitted from l^{th} active transmit antenna during t^{th} half of the time slots, β_{lt} is the coefficient of the corresponding AN signal, and v is a complex Gaussian random variable with zero-mean and unit-variance. When the i^{th} antenna combination is selected, the interference caused by $\mathbf{Z}_i$ at Bob, $\mathbf{h}\mathbf{Z}_i$, is obtained as

$$[[h_{2i+1}h_{2i+2}]\mathbf{Q}(z_{11},z_{21})\,[h_{N-2i-1}h_{N-2i}]\mathbf{Q}(z_{12},z_{22})] \tag{5}$$

where $h_j, j \in 1,\ldots,N$ is the channel coefficient from j^{th} transmit antenna to Bob. When this interference equals to zero, AN signals are cancelled out at Bob. Thus, Bob is not affected by the AN matrix. However, since Alice has the imperfect CSI of the main channel, the AN coefficients are also obtained erroneously as $\beta_{11} = -h_{est}^{2i+2}, \beta_{21} = h_{est}^{2i+1}$ or $\beta_{11} = h_{est}^{2i+2}, \beta_{21} = -h_{est}^{2i+1}$, while $\beta_{12} = -h_{est}^{N-2i}, \beta_{22} = h_{est}^{N-2i-1}$ or $\beta_{12} = h_{est}^{N-2i}, \beta_{22} = -h_{est}^{N-2i-1}$, where h_{est}^{j} is the estimate of the channel coefficient from j^{th} transmit antenna to Bob. It should be noted that the AN effect cannot be eliminated by Eve even with the knowledge of Alice-Bob channel because of the random effect of v.

3) Received Signals: The vector of received signals at Bob is given as

$$\begin{aligned}\mathbf{y}_B &= \mathbf{h}(\mathbf{S}_i + \mathbf{Z}_i^N) + \mathbf{n}_B,\\ &= \sqrt{1-\sigma^2}\mathbf{h}_{est}\mathbf{S}_i\\ &\quad \underbrace{+ \sqrt{\sigma^2}\mathbf{h}_{err}\mathbf{S}_i + \sqrt{\frac{\sigma^2(1-\alpha)P_{tot}}{P_Z}}\mathbf{h}_{err}\mathbf{Z}_i + \mathbf{n}_B}_{\hat{\mathbf{n}}_B}\end{aligned} \tag{6}$$

where $\mathbf{Z}_i^N$ represents the normalized AN matrix, and P_Z represents the power of the AN matrix, where $P_Z = 8$, $\mathbf{n}_B$ is the complex additive white Gaussian noise (AWGN) vector with zero-mean and N_0 variance entries, and $\hat{\mathbf{n}}_B$ is the colored Gaussian noise vector of which the entries are uncorrelated with the variance of $\hat{N}_B = \mathbb{E}[\hat{\mathbf{n}}_B\hat{\mathbf{n}}_B^H]/4$. Thus, the received signal at Bob can be rewritten by

$$\mathbf{y}_B = \sqrt{1-\sigma^2}\mathbf{h}_{est}\mathbf{S}_i + \hat{\mathbf{n}}_B. \tag{7}$$

Since the entries of $\hat{\mathbf{n}}_B$ are colored, the linear whitening transformation function ($\Psi_{\mathrm{B}} = \sqrt{\mathrm{N}_0}(\hat{\mathrm{N}}_{\mathrm{B}})^{-1/2}$) is applied on each entry to make them white Gaussian noise entries with zero-mean and N_0 variance [8]. Thus, the processed received signal at Bob becomes $\tilde{\mathbf{y}}_B = \tilde{\mathbf{h}}_{est}\mathbf{S}_i + \tilde{\mathbf{n}}_B$, where $\tilde{\mathbf{y}}_B = \Psi_B\mathbf{y}_B$, $\tilde{\mathbf{h}}_{est} = \Psi_{\mathrm{B}}\sqrt{1-\sigma^2}\mathbf{h}_{\mathrm{est}}$, and $\tilde{\mathbf{n}}_B = \Psi_{\mathrm{B}}\hat{\mathbf{n}}_B$.

The received signal model of Eve is almost the same with Bob, where the only difference is the AN, which is given as

$$\mathbf{y}_E = \mathbf{g}(\mathbf{S}_i + \mathbf{Z}_i^N) + \mathbf{n}_E = \sqrt{1-\sigma^2}\mathbf{g}_{est}\mathbf{S}_i + \hat{\mathbf{n}}_E \tag{8}$$

where $\mathbf{n}_E$ is the AWGN vector with zero-mean and N_0 variance elements, and $\hat{\mathbf{n}}_E$ is the colored Gaussian noise vector of which the entries are uncorrelated with the variance of $\hat{N}_E = \mathbb{E}[\hat{\mathbf{n}}_E\hat{\mathbf{n}}_E^H]/4$, which is given in (9). Applying the linear whitening transformation function ($\Psi_E = \sqrt{N_0}(\hat{N}_E)^{-1/2}$), the received signal at Eve can be obtained as $\tilde{\mathbf{y}}_E = \tilde{\mathbf{g}}_{est}\mathbf{S}_i + \tilde{\mathbf{n}}_E$, where $\tilde{\mathbf{y}}_E = \Psi_E\boldsymbol{y}_E$, $\tilde{\mathbf{g}}_{est} = \Psi_E\sqrt{1-\sigma^2}\mathbf{g}_{est}$, and $\tilde{\mathbf{n}}_E = \Psi_E\hat{\mathbf{n}}_E$.

$$\begin{aligned}\hat{\mathbf{n}}_E = &\sqrt{\frac{(1-\sigma^2)(1-\alpha)P_{tot}}{P_Z}}\mathbf{g}_{est}\mathbf{Z}_i + \sqrt{\sigma^2}\mathbf{g}_{err}\mathbf{S}_i\\ &+ \sqrt{\frac{\sigma^2(1-\alpha)P_{tot}}{P_Z}}\mathbf{g}_{err}\mathbf{Z}_i + \mathbf{n}_E.\end{aligned} \tag{9}$$

4) Detection: Both Bob and Eve use the two-stage detection method, which is a symbol-by-symbol and low complexity detection scheme. At the first stage, antenna combination is detected via summing minimum decision metrics of each symbol, which is given by

$$\hat{i} = \underset{i\in\{0,\ldots,\frac{N}{2}-1\}}{\operatorname{argmin}} \sum_{k=1}^{4}\epsilon_r^{i,k}, \quad r \in \{B,E\} \tag{10}$$

where $\epsilon_B^{i,k} = \|\tilde{\mathbf{y}}_B - \tilde{\mathbf{h}}_{est}(\mathbf{A}_{2k-1,i}x_{\zeta_B^{i,k}I} + \mathbf{A}_{2k,i}x_{\zeta_B^{i,k}Q})\|^2$ and $\epsilon_E^{i,k} = \|\tilde{\mathbf{y}}_E - \tilde{\mathbf{g}}_{est}(\mathbf{A}_{2k-1,i}x_{\zeta_E^{i,k}I} + \mathbf{A}_{2k,i}x_{\zeta_E^{i,k}Q})\|^2$ represent the metric of the k^{th} symbol when i^{th} antenna combination is selected for Bob and Eve, respectively, while $\zeta_B^{i,k} = \operatorname{argmin}_{\zeta\in\{1,\ldots,M\}}\|\tilde{\mathbf{y}}_B - \tilde{\mathbf{h}}_{est}(\mathbf{A}_{2k-1,i}x_{\zeta I} + \mathbf{A}_{2k,i}x_{\zeta Q})\|^2$ and $\zeta_E^{i,k} = \operatorname{argmin}_{\zeta\in\{1,\ldots,M\}}\|\tilde{\mathbf{y}}_E - \tilde{\mathbf{g}}_{est}(\mathbf{A}_{2k-1,i}x_{\zeta I} + \mathbf{A}_{2k,i}x_{\zeta Q})\|^2$ represent the symbol index that provides minimum metric of the k^{th} symbol when i^{th} antenna combination is selected for Bob and Eve, respectively. At the second stage, each symbol is separately detected as $\hat{x}_1 = \Omega(\zeta_r^{\hat{i},1})$, $\hat{x}_2 = \Omega(\zeta_r^{\hat{i},2})$, $\hat{x}_3 = \Omega(\zeta_r^{\hat{i},3})$, and $\hat{x}_4 = \Omega(\zeta_r^{\hat{i},4})$.

III. Performance Analysis

In this section, we derive the ESR and theoretical BER expressions in order to evaluate the secrecy and error performance and verify our computer simulations.

A. Ergodic Secrecy Rate

There are a total of $N/2$ antenna combinations and each APM symbol is chosen from the normalized M-ary constellation. Assuming that χ is the set of all possible CIOD matrices, the elements of χ are discrete variables with the same probability of $2/NM^4$, and $\mathbf{X}_n$ denotes the n^{th} CIOD matrix in the set. The ESR of the CIOD-IM scheme is expressed as $R_S = [R_B - R_E]^+$ where $[a]^+$ indicates $\max\{0,a\}$, R_B and R_E indicate the ergodic rate of Bob and Eve, respectively. Since the received signal at Bob can be given as $\tilde{\mathbf{y}}_B = \tilde{\mathbf{h}}_{est}\mathbf{X}_n + \tilde{\mathbf{n}}_B$, its complex received vector has the conditional probability density function (PDF) that is given by [12]

$$p(\tilde{\mathbf{y}}_B|\mathbf{X} = \mathbf{X}_n) = \left[\frac{1}{\pi N_0}\right]^4 \exp\left(\frac{-\|\tilde{\mathbf{y}}_B - \tilde{\mathbf{h}}_{est}\mathbf{X}_n\|^2}{N_0}\right). \tag{11}$$

The marginal PDF of the complex received vector is expressed as

$$p(\tilde{\mathbf{y}}_B) = \frac{2}{NM^4}\sum_{n=1}^{\frac{N}{2}M^4}\left[\frac{1}{\pi N_0}\right]^4 \exp\left(\frac{-\|\tilde{\mathbf{y}}_B - \tilde{\mathbf{h}}_{est}\mathbf{X}_n\|^2}{N_0}\right). \tag{12}$$

The mutual information of Bob can be obtained as follows

$$\begin{aligned}I(\tilde{\mathbf{y}}_B;\mathbf{X}) &= \sum_n\int_{\tilde{\mathbf{y}}_B} p(\mathbf{X},\tilde{\mathbf{y}}_B)\log_2\frac{p(\mathbf{X},\tilde{\mathbf{y}}_B)}{p(\mathbf{X})p(\tilde{\mathbf{y}}_B)}d\tilde{\mathbf{y}}_B,\\ &= \log_2\frac{N}{2}M^4 - \frac{2}{NM^4}\sum_{n=1}^{\frac{N}{2}M^4}\mathbb{E}_{\tilde{\mathbf{n}}_B}\Bigg[\log_2\sum_{n_2=1}^{\frac{N}{2}M^4}\\ &\quad\times\exp\left(-\frac{\|\tilde{\mathbf{h}}_{est}(\mathbf{X}_n - \mathbf{X}_{n_2}) + \tilde{\mathbf{n}}_B\|^2 - \|\tilde{\mathbf{n}}_B\|^2}{N_0}\right)\Bigg].\end{aligned} \tag{13}$$

Since the transmission is conducted in four time slots, the ergodic rate of Bob can be obtained as $R_B = I(\tilde{\mathbf{y}}_B;\mathbf{X})/4$.

Using a similar approach, the mutual information and the ergodic rate of Eve can be obtained as given

$$I(\tilde{\mathbf{y}}_E;\mathbf{X}) = \log_2 \frac{N}{2}M^4 - \frac{2}{NM^4}\sum_{n=1}^{\frac{N}{2}M^4} \mathbb{E}_{\tilde{\mathbf{n}}_E}$$

$$\times \left[\log_2 \sum_{n_2=1}^{\frac{N}{2}M^4} \exp\left(-\frac{\|\tilde{\mathbf{g}}_{est}(\mathbf{X}_n - \mathbf{X}_{n_2}) + \tilde{\mathbf{n}}_E\|^2 - \|\tilde{\mathbf{n}}_E\|^2}{N_0}\right)\right],$$

$$R_E = \frac{I(\tilde{\mathbf{y}}_E;\mathbf{X})}{4}. \tag{14}$$

B. Theoretical Bit Error Rate

Utilizing the union bound technique with associated pairwise error probabilities (PEPs), the theoretical BER upper bound is derived for the case of perfect channel estimation. Assuming that $\mathbf{X}_u$ is erroneously detected when $\mathbf{X}_n$ is transmitted, the theoretical BER upper bound can be given as [13]

$$P_b \leq \frac{2}{NM^4}\sum_{n=1}^{\frac{NM^4}{2}}\sum_{u=1}^{\frac{NM^4}{2}} \frac{e_{n,u}}{\log_2\left(\frac{NM^4}{2}\right)}\bar{P}_e(\mathbf{X}_n \rightarrow \mathbf{X}_u) \tag{15}$$

where $\bar{P}_e(\mathbf{X}_n \rightarrow \mathbf{X}_u)$ represents the PEP of deciding $\mathbf{X}_u$ when $\mathbf{X}_n$ is transmitted, and $e_{n,u}$ is the number of bit errors for the corresponding pairwise error event. The conditional PEP (CPEP) depending on $\mathbf{h}$ can be given by $\bar{P}_e(\mathbf{X}_n \rightarrow \mathbf{X}_u|\mathbf{h}) = Q(\sqrt{\gamma_S\gamma})$ where $\gamma_S = \alpha P_{tot}/2N_0$, and $\gamma = \|\mathbf{h}\mathbf{\Phi}_{nu}\|^2$ in which $\mathbf{\Phi}_{nu} = \mathbf{X}_n - \mathbf{X}_u$ with $\mathbf{X}_n, \mathbf{X}_u \in \chi$. The unconditional PEP can be obtained by taking the expectation of CPEP, which can be represented as $\int_0^\infty Q(\sqrt{\gamma_S\gamma})p_\gamma(\gamma)d\gamma$. Using the moment generating function of γ, $M_\gamma(s) = [\det(\mathbf{I}_4 - s\Delta)]^{-1} = \prod_{d=1}^{D}(1 - s\lambda_d)^{-1}$ where $\Delta = (\mathbf{\Phi}_{nu}^H\mathbf{\Phi}_{nu})$, $D = \mathrm{rank}(\Delta)$, and $\lambda_d, d \in \{1,\ldots,4\}$ representing the eigenvalues of Δ, and the alternative expression of Q-function, the PEP can be obtained as [14]

$$\bar{P}_e(\mathbf{X}_n \rightarrow \mathbf{X}_u) = \frac{1}{\pi}\int_0^{\frac{\pi}{2}}\prod_{d=1}^{D}\left(1 + \frac{\alpha P_{tot}\lambda_d}{2N_0\sin^2\theta}\right)^{-1} d\theta. \tag{16}$$

IV. Simulation Results

In this section, BER and ESR performances of the CIOD-IM scheme are investigated with respect to the efficient Alamouti [9] and the conventional [8] schemes, and the BER performances are verified by the theoretical BER upper bound given in (15). The impact of imperfect channel estimation and power allocation are analyzed in terms of BER and ESR performances, respectively. For the sake of fairness of the comparisons, it is assumed that $P_{tot} = 1$ for all schemes. In all simulations, signal-to-noise ratio (SNR) is defined as E_s/N_0, where $E_s = \alpha P_{tot}/8$ for the CIOD-IM scheme, $E_s = \alpha P_{tot}/4$ for the efficient Alamouti scheme, and $E_s = \alpha P_{tot}$ for the conventional scheme, and perfect channel estimation is assumed unless otherwise stated. In addition, the results of the conventional scheme is obtained assuming SLNR based TAS [8]. In Fig. 4 and Fig. 6, N_a and N_t represents the number of total and selected transmit antennas at Alice, respectively.

Fig. 3 illustrates the BER performance of the CIOD-IM scheme for a large-scale MISO system with $N = 4$ and 32 by employing different modulation levels as QPSK and 16-QAM. It can be seen that as N increases, the BER performance gets worse in the most of the SNR regions while the spectral efficiency rises. Also, we verify our simulation results with theoretical upper bounds for the reference two systems, which shows that our simulation results match with the upper bounds at high SNR values. It can also be observed that Eve's BER is almost 0.5 for all N and M values, which indicates that Eve cannot obtain any information.

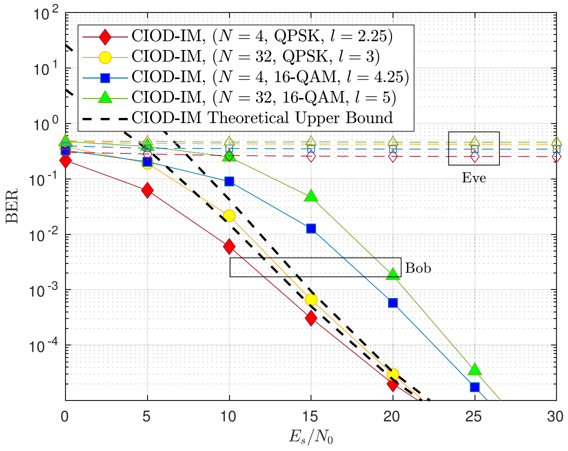

Fig. 3. BER performance of the CIOD-IM scheme for $N = 4$ and 32 with QPSK and 16-QAM.

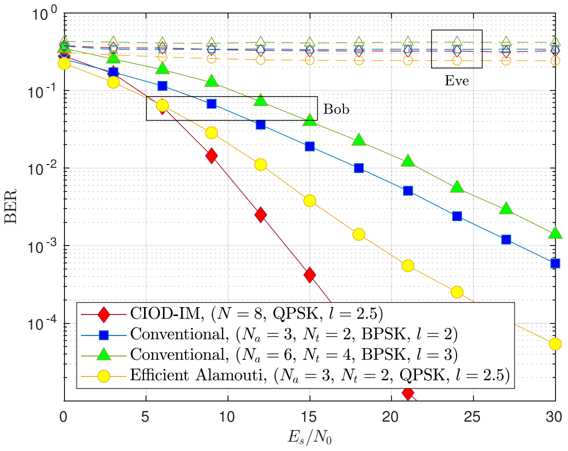

Fig. 4. Comparison of the BER performances of the CIOD-IM and benchmark schemes for $2 \leq l \leq 3$.

In Fig. 4, we compare the BER performance of the CIOD-IM scheme with the efficient Alamouti and the conventional schemes for $2 \leq l \leq 3$. It is clear that the proposed scheme outperforms benchmark schemes. It should be noted that regardless of the number of transmit antennas at Alice, there are only two active RF chains in the CIOD-IM scheme, which ensures improved performance without additional complexity. Diversity orders will be more evident in the higher SNR regimes.

In Figs. 5(a) and (b), we investigate the effect of imperfect channel estimation and power allocation on the BER and ESR performances of the CIOD-IM scheme, respectively, for $N = 4$ and QPSK. In Fig. 5(a), we considered the cases of $\sigma^2 = 0$ which corresponds to perfect channel estimation, $\sigma^2 = 0.03$, and $\sigma^2 = 0.1$. It is clear that any error in channel estimation significantly deteriorates the BER performance.

Fig. 5(b) illustrates that the security performance degrades as α increases. Also, it can be observed that secrecy behavior is different when most of the power is allocated to APM symbols. As the SNR increases, the more power allocated to APM symbols becomes more significant as channel quality increases. Therefore, secrecy diminishes in the high SNR region.

Finally, the ESR performances of the CIOD-IM and benchmark schemes are compared in Fig. 6. The CIOD-IM scheme achieves a better ESR performance than the efficient Alamouti scheme for the

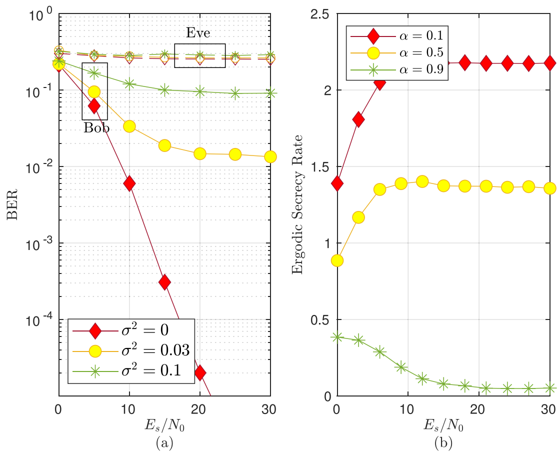

Fig. 5. The effect of (a) imperfect CSI on the BER. (b) power allocation on the ESR performance of the CIOD-IM scheme for $N = 4$ and QPSK.

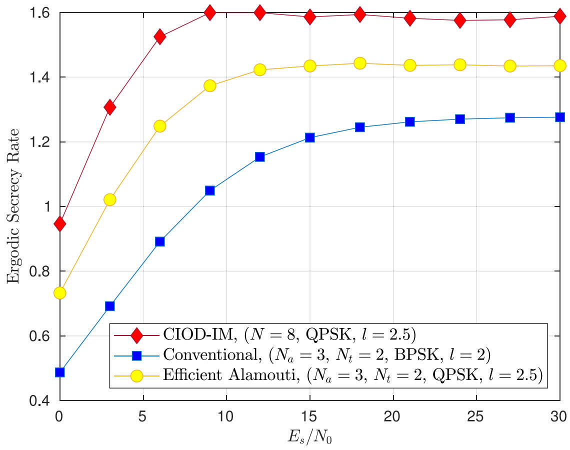

Fig. 6. Comparison of the ESR performances of the CIOD-IM and benchmark schemes for $2 \leq l \leq 3$.

same spectral efficiency in all SNR regions. These results ensure that the CIOD-IM scheme achieves a competitive secrecy rate.

V. Conclusion

In this paper, a new secrecy scheme, which is called as CIOD-IM, has been introduced. The proposed system model increases the spectral efficiency of CIOD transmission by means of a novel IM technique. Moreover, the special design of the AN matrix provides a satisfactory secrecy performance. The security and the BER performances have been investigated under Rayleigh fading environment and compared with benchmark schemes. The ergodic rates of Bob and Eve have been derived and the ergodic secrecy rate has been obtained. In order to verify the correctness of our simulation results, the theoretical upper bound of the BER has been derived. Our simulations show that the CIOD-IM scheme achieves better results than the benchmark schemes both in terms of the secrecy and the BER performances. Finally, it has been observed by its improved BER results in large-scale MISO setups that the CIOD-IM scheme can be a promising candidate for future massive MIMO systems requiring both high reliability and secrecy.

References

[1] E. Basar, M. Wen, R. Mesleh, M. Di Renzo, Y. Xiao, and H. Haas, “Index modulation techniques for next-generation wireless networks,” *IEEE Access*, vol. 5, pp. 16693–16746, 2017.

[2] R. Y. Mesleh, H. Haas, S. Sinanovic, C. W. Ahn, and S. Yun, “Spatial modulation,” *IEEE Trans. Veh. Technol.*, vol. 57, no. 4, pp. 2228–2241, Jul. 2008.

[3] F. Wu, R. Zhang, L. Yang, and W. Wang, “Transmitter precoding-aided spatial modulation for secrecy communications,” *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 467–471, Jan. 2016.

[4] F. Wu, L. Yang, W. Wang, and Z. Kong, “Secret precoding-aided spatial modulation,” *IEEE Commun. Lett.*, vol. 19, no. 9, pp. 1544–1547, Sep. 2015.

[5] Y. Chen, L. Wang, Z. Zhao, M. Ma, and B. Jiao, “Secure multiuser mimo downlink transmission via precoding-aided spatial modulation,” *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1116–1119, Jun. 2016.

[6] L. Wang, S. Bashar, Y. Wei, and R. Li, “Secrecy enhancement analysis against unknown eavesdropping in spatial modulation,” *IEEE Commun. Lett.*, vol. 19, no. 8, pp. 1351–1354, Aug. 2015.

[7] X. Yu, Y. Hu, Q. Pan, X. Dang, N. Li, and M. H. Shan, “Secrecy performance analysis of artificial-noise-aided spatial modulation in the presence of imperfect CSI,” *IEEE Access*, vol. 6, pp. 41060–41067, 2018.

[8] W. Yu *et al.*, “Security enhancing spatial modulation using antenna selection and artificial noise cancellation,” in *Proc. Int. Conf. Comput., Netw. Commun.*, 2019, pp. 105–109.

[9] P. Shang, S. Kim, and X. Jiang, “Efficient alamouti-coded spatial modulation for secrecy enhancing,” in *Proc. Int. Conf. Inf. Commun. Technol. Convergence*, 2019, pp. 860–864.

[10] M. Z. A. K. Khan, B. S. Rajan, and M. H. Lee, “Rectangular co-ordinate interleaved orthogonal designs,” in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, San Francisco, CA, USA, Dec. 2003, pp. 2004–2009.

[11] D. N. Dao and C. Tellambura, “On space-time block codes from coordinate interleaved orthogonal designs,” in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, 2006, pp. 1–5.

[12] X. Guan, Y. Cai, and W. Yang, “On the secrecy mutual information of spatial modulation with finite alphabet,” in *Proc. 2nd Int. Conf. Wireless Commun. Signal Process.*, 2012, pp. 1–4.

[13] A. Younis, R. Mesleh, and H. Haas, “Quadrature spatial modulation performance over nakagami- m fading channels,” *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10227–10231, Dec. 2016.

[14] E. Basar and I. Altunbas, “Space-time channel modulation,” *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7609–7614, Aug. 2017.