Robust Secure Transmission of Using Main-Lobe-Integration-Based Leakage Beamforming in Directional Modulation MU-MIMO Systems

Feng Shu, *Member, IEEE*, Wei Zhu, Xiangwei Zhou, Jun Li, *Senior Member, IEEE*, and Jinhui Lu

***Abstract*—In this paper, we make an investigation of robust beamforming for secure directional modulation in the multiuser multiple-input and multiple-output systems in the presence of direction angle measurement errors. When statistical knowledge of direction angle measurement errors is unavailable, a novel robust beamforming scheme of combining main-lobe-integration and leakage is proposed to simultaneously transmit multiple different independent parallel confidential message streams to the associated multiple distinct desired users. The proposed scheme includes two steps: designing the beamforming vectors of the useful confidential messages and constructing artificial noise (AN) projection matrix. Here, in its first step, the beamforming vectors for the useful confidential messages of desired user k are given by minimizing the useful signal power leakage from the main-lobe of desired user k to the sum of main-lobes of the remaining desired directions plus main-lobes of all eavesdropper directions. In its second step, the AN projection matrix is constructed by simultaneously maximizing the AN power leakage to all eavesdropper directions such that all eavesdroppers are disrupted seriously, where AN is viewed by the transmitter as a useful signal for eavesdroppers. Due to independent beamforming vectors for different desired users, a more secure transmission is achieved. Compared with conventional nonrobust methods, the proposed method can provide a significant improvement in bit error rate along the desired directions and secrecy-sum-rate toward multiple desired users without needing the statistical property or distribution of angle measurement errors.**

***Index Terms*—Artificial noise (AN), directional modulation (DM), leakage, main-lobe-integration (MLI), multiuser multiple input and multiple output (MU-MIMO), robust, secrecy-sum-rate (SSR).**

I. Introduction

THE privacy and security of information transmission are extremely important for wireless communications and networking [1]–[6]. Due to the broadcasting nature and lack of physical boundaries of wireless transmission, the information is readily intercepted by unauthorized users, and the growing cyber criminal events in mobile terminals have exposed the enormous hidden risks in wireless communications and networking. Traditional encryption techniques can only provide computational security and rely heavily on the complexity of their keys, which are very easy to be cracked if an efficient method to solve the corresponding mathematical problem is found [1]–[4]. In the emerging social aware network, in order to take full advantage of wireless network resources, several incentive mechanisms based on credit or friendship had been presented to stimulate selfish users to forward data for other terminals, which will result in more serious security problems if the useful messages are intercepted by malicious users [5], [6]. In 1975, Wyner first proposes the remarkable wiretap channel model and lays the foundations of information theory of physical-layer security communications [7]–[9]. In recent years, the physical-layer security has ever been becoming a promising research field in wireless communications and networking by exploiting the physical-layer characteristics of wireless channels [10]–[15].

As a novel physical-layer security technology in wireless communications and networking, directional modulation (DM) has been attracting widespread attention and research activities from both academia and industry. In [16], Babakhani *et al.* introduce a technique of near-field direct antenna modulation, changing the antenna boundary conditions at the symbol rate thereby modulating the phase and amplitude of the antenna pattern. A simplified structure of DM synthesis relying on actively excited elements in phased arrays is described in [17] and [18]. Subsequently, the artificial noise (AN) aided security emerges

Manuscript received March 10, 2017; revised June 23, 2017 and August 26, 2017; accepted October 5, 2017. Date of publication November 3, 2017; date of current version November 22, 2018. This work was supported in part by the National Natural Science Foundation of China under Grant 61771244, Grant 61501238, Grant 61702258, Grant 61472190, and Grant 61271230, in part by the Open Research Fund of the National Key Laboratory of Electromagnetic Environment, China Research Institute of Radiowave Propagation under Grant 201500013, in part by the Jiangsu Provincial Science Foundation under Project BK20150786, in part by the Specially Appointed Professor Program in Jiangsu Province, 2015, in part by the Fundamental Research Funds for the Central Universities under Grant 30916011205, and in part by the Open Research Fund of the National Mobile Communications Research Laboratory, Southeast University, China under Grant 2017D04 and Grant 2013D02. *(Corresponding author: Feng Shu.)*

F. Shu is with the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing 210094, China, with the College of Computer and Information Sciences, Fujian Agriculture and Forestry University, Fuzhou 350002, China, and also with the National Key Laboratory of Electromagnetic Environment, China Research Institute of Radiowave Propagation, Qingdao 266107, China (e-mail: shufeng@njust.edu.cn).

W. Zhu and J. Lu are with the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing 210094, China (e-mail: wei.zhu@njust.edu.cn; jinhui.lu@njust.edu.cn).

X. Zhou is with the Division of Electrical and Computer Engineering, Louisiana State University, Baton Rouge, LA 70803 USA (e-mail: xwzhou@lsu.edu).

J. Li is with the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing 210094, China, with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210018, China, and also with the Department of Software Engineering, Institute of Cybernetics, National Research Tomsk Polytechnic University, Tomsk 634050, Russia (e-mail: jun.li@njust.edu.cn).

Digital Object Identifier 10.1109/JSYST.2017.2764142

and is applied to confidential transmission [19]–[21], which enables the transmitter to transmit AN, as an interference signal, and confidential messages together, such that the AN is only used to interfere with the eavesdroppers without affecting the legitimate receivers. The algorithm proposed in [11] enables all the remaining available transmit power to transmit AN in the case that the desired receivers are guaranteed to achieve a target signal-to-interference-plus-noise ratio. Based on the previous work, Ding and Fusco [22], [23] initiate the DM research on the baseband signal processing and propose to add the orthogonal vector, which can be chosen and updated in the null space of channel vector at the desired direction, to the transmitted baseband signal as AN [22], [23]. An orthogonal-vector-approach-based synthesis of multibeam DM follows immediately from [24]. The methods presented in [22] and [23] are shown to perform very well for the perfect direction angles but are quite sensitive to the measurement errors of direction angles. To reduce the impact of the measurement errors, Hu *et al.* [25] propose a robust DM synthesis method that is capable of achieving an excellent performance of bit error rate (BER) under imperfect direction angle in a single-desired-user scenario. In [25], a closed-form projection matrix is derived to force the AN to the null space of steering vector of the desired direction by utilizing the uniform distribution of measurement angle errors. In [26], Shu *et al.* propose a robust beamforming scheme for multibeam DM broadcasting systems and derive the expressions of different beamformers for various scenarios, in which case only one confidential message stream is broadcasted to multiple desired users.

However, most existing work focuses on robust and nonrobust synthesis schemes of DM. Such schemes require perfect knowledge of direction angles or imperfect one with distribution of angle measurement errors at the transmitters. In a practical DM system, it is impossible to obtain perfect knowledge of direction angles or precisely model the distribution of angle measurement errors. This motivates us to develop a low-complexity, robust synthesis scheme needing only the estimated direction angles, without requiring perfect direction angles or the distribution of angle measurement errors under the imperfect case.

In this paper, we consider multiple confidential message stream transmission of using DM in the multiuser multiple-input and multiple-output (MU-MIMO) scenario. We propose a main-lobe-integration (MLI) based leakage synthesis scheme. This method is based on leakage idea presented in [27]–[30] and MLI, and shown robust to angle measurement errors in our simulation. Our main contributions are as follows.

1) We propose a totally distinct robust beamfroming method of using the concept of leakage in an MU-MIMO situation, which does not require the statistical knowledge of direction angle measurement error, i.e., to estimate the variances of direction error. However, in [25] and [26], the proposed robust methods need to predict the variances of direction estimation errors or even know the distributions of measurement errors in advance. Also, the proposed method may simultaneously send multiple distinct independent parallel confidential message streams to the associated multiple desired receivers. However, those methods in [25] and [26] transmit only single confidential message stream toward one or more desired users.
2) The beamforming vectors for different desired users are individually designed and distinct in this paper. This guarantees that any desired receiver cannot intercept confidential messages of others desired user, which further improves the transmit security. However, in [26], all desired-user channels are combined into one total large virtual channel and only single identical desired beamforming vector is required and devised for all desired users due to broadcasting scenario.
3) In the following, AN is viewed as a virtual useful signal for eavesdroppers, and we construct the AN projecting matrix by minimizing the leakage of AN power to the main-lobes of the desired directions. This will reduce the effect of AN on desired receivers and maximize the effect of AN on eavesdroppers. In [26], the AN projection matrix is designed by using the criterion of maximizing receiving-AN-to-signal-noise ratio at undesired receivers.

The proposed scheme can be typically applied to the future line-of-propagation environments. Its major application scenarios include satellite communications, unmanned aerial vehicles (UAV) networks, secure military communications, millimeter wave communications, device-to-device (D2D), vehicle-to-vehicle (V2V), and Internet of Things (IOT).

The rest of this paper is organized as follows. System model is described in Section II. Section III presents the proposed robust synthesis method with desired angle uncertainty under two cases: imperfect and unknown eavesdropper directions. The numerical results are shown and discussed in Section IV, and Section V concludes this paper.

Notations: Throughout this paper, matrices, vectors, and scalars are denoted by letters of bold upper case, bold lower case, and lower case, respectively. Signs $(\cdot)^T$, $(\cdot)^H$, $(\cdot)^{-1}$, and $\mathrm{tr}(\cdot)$ denote matrix transpose, conjugate transpose, Moore–Penrose inverse, and trace, respectively. Operation $(x)^+$ returns zero if x is negative, otherwise x is returned. The notation $\mathbb{E}\{\cdot\}$ refers to the expectation operation. The symbol $\mathbf{I}_N$ denotes the $N \times N$ identity matrix. Since there are a lot of variables in this paper, we have summarized main variables in Table I.

II. System Model

A schematic diagram of DM MU-MIMO system is shown in Fig. 1, where N is the number of elements at the base station (BS). In such a system, we assume that K independent confidential messages $\{d_k\}_{k=1}^K$ are transmitted toward K distinct desired users with direction angles $\{\theta_{d_1}, \theta_{d_2}, \ldots, \theta_{d_K}\}$. Additionally, there are M eavesdroppers with direction angles $\{\theta_{e_1}, \theta_{e_2}, \ldots, \theta_{e_M}\}$. Due to the irregular reflection and refraction in the multipath fading channel, the propagation direction of the signal is unpredictable, while the DM is very sensitive to the arrival direction at desired receiver in the wireless channel. Until now, the extension of DM to multipath fading channel is a challenging problem. For example, if the blocking object locates at the eavesdropper direction, then it can reflect the AN to the desired receiver. We call the result as the effect of gathering

TABLE I
SUMMARY OF MAIN VARIABLES

N	Number of antennas at the BS
K	Number of desired users
M	Number of eavesdroppers
θ_{d_k}	The kth desired direction angle
θ_{e_m}	The mth eavesdropping direction angle
$\mathbf{s}$	Transmit signal vector at the BS
d_k	The kth confidential message
$\mathbf{v}_k$	Beamforming vector of the kth confidential message
$\mathbf{T}_{\text{AN}}$	Projection matrix of AN
$\mathbf{z}$	Random AN vector
P_s	Total transmit power constraint at the BS
α_1	Normalized power factors for confidential messages
α_2	Normalized power factors for AN
β_1	Power allocation of confidential messages
β_2	Power allocation of AN
$\mathbf{h}(\theta)$	Normalized steering vector along the direction θ
$\varphi_\theta(n)$	Phase difference between the nth element in $\mathbf{h}(\theta)$ and the array phase center
$y(\theta)$	Received signal along the direction θ
ω	AWGN with distribution $\mathcal{CN}(0,\ \sigma_\omega^2)$
$C_k(\theta)$	Achievable rate of receiving the kth useful data along the direction θ
C_{sec}	SSR
$\hat{\theta}_{d_k}$	The kth estimated desired direction angle
$\hat{\theta}_{e_m}$	The mth estimated eavesdropping direction angle
θ_{BW}	BWFN for a long broadside array
S	Integral interval with single continuous interval or the union of several subintervals
$\mathbf{R}_S$	Integral result of the matrix $h(\theta)h(\theta)^H$ within the interval S, i.e., $\mathbf{R}_S = \int_S \mathbf{h}(\theta)\mathbf{h}^H(\theta)\,\mathrm{d}\theta$

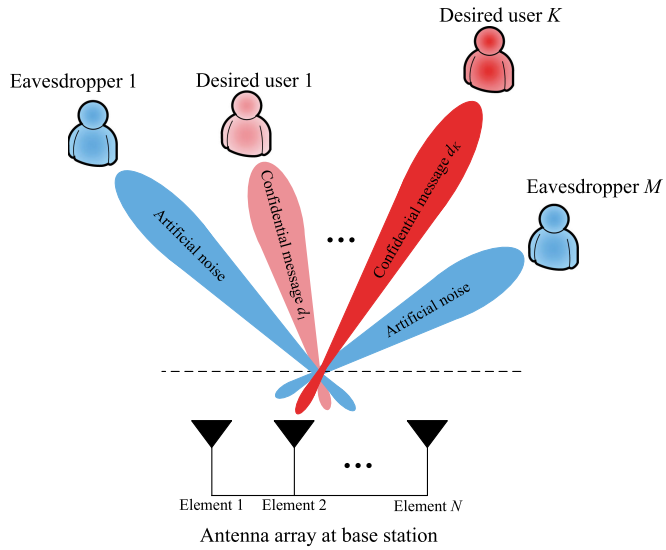


Fig. 1. DM MU-MIMO system, where different gray-scale reds denote different confidential message streams for different desired users.

AN. This effect will dramatically degrade the performance of the desired receiver by collecting a large amount of AN from reflecting objects at the undesired directions. Therefore, in this paper, we only consider the line-of-propagation channels.

The confidential message d_k with $\mathbb{E}\left\{d_k^H d_k\right\} = 1$ is sent to the desired receiver k, and multiplied by an $N \times 1$ beamforming vector $\mathbf{v}_k$ before being transmitted through the channel, where $\mathbf{v}_k$ is called the confidential useful vector for desired user k below. Thus, the transmit signal vector is written as

$$\mathbf{s} = \underbrace{\alpha_1\beta_1\sqrt{P_s}\sum_{k=1}^{K}\mathbf{v}_k d_k}_{\text{Confidential messages}} + \underbrace{\alpha_2\beta_2\sqrt{P_s}\mathbf{T}_{\text{AN}}\mathbf{z}}_{\text{AN}} \tag{1}$$

where P_s is the total transmit power constraint at BS, β_1 and β_2 are the power allocation between confidential messages and AN such that

$$\beta_1^2 + \beta_2^2 = 1 \tag{2}$$

α_1 and α_2 are the normalized power factors for confidential messages and AN such that

$$\alpha_2^2\mathbb{E}\left\{\text{tr}\left[\mathbf{T}_{\text{AN}}\mathbf{z}\mathbf{z}^H\mathbf{T}_{\text{AN}}^H\right]\right\} = 1 \tag{3}$$

and $\mathbf{T}_{AN}$ is the projection matrix of forcing AN to the eavesdropping directions. The transmit signal vector in (1) satisfies the following power constraint:

$$\alpha_1^2\mathbb{E}\left\{\sum_{k=1}^{K}\sum_{k'=1}^{K}\mathbf{v}_{k'}^H\mathbf{v}_k d_k d_{k'}^H\right\} = 1. \tag{4}$$

If $\mathbb{E}\left\{d_k d_k^H\right\} = 1, \mathbf{v}_k^H\mathbf{v}_k = 1$, and $\mathbb{E}\left\{\mathbf{z}\mathbf{z}^H\right\} = \frac{1}{N-K}\mathbf{I}_{N-K}$, (3) and (4) can be further simplified as

$$\alpha_2^2\text{tr}\left[\mathbf{T}_{\text{AN}}\mathbf{T}_{\text{AN}}^H\right] = N - K \tag{5}$$

and

$$\alpha_1^2 = \frac{1}{K}. \tag{6}$$

The $N \times 1$ vector $\mathbf{s}$ passes through the LoS channel, the received signal along direction θ is given by

$$y(\theta) = \mathbf{h}^H(\theta)\mathbf{s} + \omega \tag{7}$$

where ω is the additive white Gaussian noise (AWGN) with distribution $\mathcal{CN}(0, \sigma_\omega^2)$, and

$$\mathbf{h}(\theta) = \frac{1}{\sqrt{N}}\left[\underbrace{e^{j2\pi\varphi_\theta(1)}}_{h_1(\theta)}, \ldots, \underbrace{e^{j2\pi\varphi_\theta(n)}}_{h_n(\theta)}, \ldots, \underbrace{e^{j2\pi\varphi_\theta(N)}}_{h_N(\theta)}\right]^T \tag{8}$$

is the normalized steering vector along the direction θ with function $\varphi_\theta(n)$ defined by

$$\varphi_\theta(n) \triangleq \frac{(n-(N+1)/2)d\cos\theta}{\lambda}, \quad n = 1, 2, \ldots, N \tag{9}$$

where d denotes the spacing between two adjacent elements of transmit antenna array and λ is the wavelength of transmit carrier. According to (7), the received signal at the kth desired user is given by

$$\begin{aligned} y(\theta_{d_k}) &= \mathbf{h}^H(\theta_{d_k})\mathbf{s} + \omega_{d_k} \\ &= \underbrace{\alpha_1\beta_1\sqrt{P_s}\mathbf{h}^H(\theta_{d_k})\mathbf{v}_k d_k}_{\text{Useful data}} + \underbrace{\alpha_1\beta_1\sqrt{P_s}\mathbf{h}^H(\theta_{d_k})\sum_{i=1,i\neq k}^{K}\mathbf{v}_i d_i}_{\text{Interference from other users}} \\ &\quad + \underbrace{\alpha_2\beta_2\sqrt{P_s}\mathbf{h}^H(\theta_{d_k})\mathbf{T}_{\text{AN}}\mathbf{z}}_{\text{AN}} + \underbrace{\omega_{d_k}}_{\text{AWGN}} \end{aligned} \tag{10}$$

where the first term of the above expression is the useful received signal for user k, the second one is the multiuser interference from other users, the third one is the AN, and the last one is the AWGN with distribution $\mathcal{CN}(0,\sigma_{d_k}^2)$ at receiver. Similarly, the received signal at eavesdropper m is

$$\begin{aligned} y(\theta_{e_m}) &= \mathbf{h}^H(\theta_{e_m})\mathbf{s}+\omega_{e_m} \\ &= \underbrace{\alpha_1\beta_1\sqrt{P_s}\mathbf{h}^H(\theta_{e_m})\sum_{k=1}^{K}\mathbf{v}_k d_k}_{\text{Confidential messages}} \\ &\quad + \underbrace{\alpha_2\beta_2\sqrt{P_s}\mathbf{h}^H(\theta_{e_m})\mathbf{T}_{\text{AN}}\mathbf{z}}_{\text{AN}} + \underbrace{\omega_{e_m}}_{\text{AWGN}} \end{aligned} \tag{11}$$

where the first term of the above expression is composed of the confidential messages intercepted by eavesdropper m, the second one is the AN to disturb eavesdropper m, and the last one is the AWGN with distribution $\mathcal{CN}(0,\sigma_{e_m}^2)$.

To evaluate the security performance for multiuser scenario in this paper, the secrecy-sum-rate (SSR) is adopted and can be defined as the sum of difference in available rate receiving useful data between secure transmission channel and eavesdropper channel [31], [32]

$$C_{\text{sec}} = \sum_{k=1}^{K}\left[C_k(\theta_{d_k}) - \max_m C_k(\theta_{e_m})\right]^+ \tag{12}$$

where $C_k(\theta_{d_k})$ and $C_k(\theta_{e_m})$ shown in (13) and (14), at the bottom of the page, are the achievable rates of receiving useful data d_k along the kth desired direction θ_{d_k} and the mth eavesdropper direction θ_{e_m}, respectively. Function $I(y;[d,\theta])$ denotes the mutual information along the direction θ between the input d and the output y.

The SSR in (12) is one of the most important metrics for assessing the performance of the DM system. Under the multiuser scenario, the expression of the SSR in (12) contains multiple variables, i.e., $R_k(\theta_{d_k})$ and $R_k(\theta_{e_m})$. In addition, $R_k(\theta_{d_k})$ and $R_k(\theta_{e_m})$ are both $K+1$ coupled variables with $\{\mathbf{v}_{d_k}\}_{k=1}^K$ and $\mathbf{T}_{AN}$ as shown in (13) and (14), respectively. Apparently, it is challenging to solve the $K+1$ coupled optimization problems. Maximizing the SSR in (12) directly is an NP-hard problem with exponential complexity. Maybe, with a high-computational amount, only suboptimal solution is achieved. On the other hand, minimizing the BER, which is another important metric for evaluating the DM system, of a selected user will depend heavily on other users' beamforming vectors and direction angles. The coupled property requires the iteration operation. Additionally, it is not easy to guarantee its convergence. To address the above, we propose an MLI-based leakage beamforming method, which can provide an approximate closed-form solution with low complexity and high performance. More importantly, due to MLI, it is also robust to direction angle measurement errors.

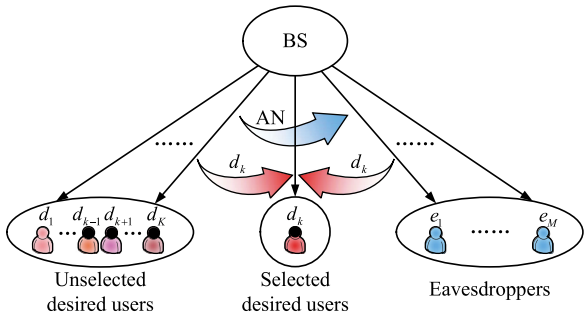


Fig. 2. Schematic diagram of the proposed scheme.

III. Proposed Robust Synthesis Method With Desired Angle Uncertainty

In Fig. 2, we sketch the basic idea of the proposed robust precoding method based on MLI and leakage. As shown in Fig. 2, if desired user k is chosen as the current desired user, the corresponding confidential useful beamforming vector is given by minimizing its useful signal power leakage to the remaining desired users and all eavesdroppers. Confidential beamforming vector corresponding to each desired user is designed individually in order to safeguard each desired user privacy. The AN projection matrix $\mathbf{T}_{\text{AN}}$ is optimized by maximizing the AN power leakage to all eavesdroppers. In other words, the influence of AN on all desired users is minimized. Here, $\mathbf{T}_{\text{AN}}$ is constructed in the all-in-one way not individually. In the following, we mainly consider the imperfect desired direction, where imperfect means that there exists measurement errors on the measured desired direction angles. Eavesdropper direction angles fall into two categories: imperfect (see Section III-A) and unknown (see Section III-B). In the first scenario, both desired and eavesdropper directions are imperfect. In other words, there usually exists errors in the measured desired and eavesdropper directions. In the second scenario, eavesdropper directions are

$$\begin{aligned} C_k(\theta_{d_k}) &\triangleq I(y(\theta_{d_k});[d_k,\theta_{d_k}]) \\ &= \log_2\left(1+\frac{\alpha_1^2\beta_1^2 P_s\mathbf{h}^H(\theta_{d_k})\mathbf{v}_k\mathbf{v}_k^H\mathbf{h}(\theta_{d_k})}{\sigma_{d_k}^2+\sum_{i=1,i\neq k}^{K}\alpha_1^2\beta_1^2 P_s\mathbf{h}^H(\theta_{d_k})\mathbf{v}_i\mathbf{v}_i^H\mathbf{h}(\theta_{d_k})+\alpha_2^2\beta_2^2 P_s\mathbf{h}^H(\theta_{d_k})\mathbf{T}_{\text{AN}}\mathbf{T}_{\text{AN}}^H\mathbf{h}(\theta_{d_k})}\right) \end{aligned} \tag{13}$$

$$\begin{aligned} C_k(\theta_{e_m}) &\triangleq I(y(\theta_{e_m});[d_k,\theta_{e_m}]) \\ &= \log_2\left(1+\frac{\alpha_1^2\beta_1^2 P_s\mathbf{h}^H(\theta_{e_m})\mathbf{v}_k\mathbf{v}_k^H\mathbf{h}(\theta_{e_m})}{\sigma_{e_m}^2+\sum_{i=1,i\neq k}^{K}\alpha_1^2\beta_1^2 P_s\mathbf{h}^H(\theta_{e_m})\mathbf{v}_i\mathbf{v}_i^H\mathbf{h}(\theta_{e_m})+\alpha_2^2\beta_2^2 P_s\mathbf{h}^H(\theta_{e_m})\mathbf{T}_{\text{AN}}\mathbf{T}_{\text{AN}}^H\mathbf{h}(\theta_{e_m})}\right) \end{aligned} \tag{14}$$

unknown while the measured desired directions are imperfect. In the two situations, we accordingly show how to design the AN projection matrix $\mathbf{T}_{\text{AN}}$ and confidential useful beamforming vectors $\mathbf{v}_{d_k}$.

A. Imperfect Desired and Eavesdropper Directions

In practice, the desired and eavesdropper directions are unknown. In this case, the BS can estimate both the values of desired and eavesdropper direction angles with the traditional spatial spectrum estimation, such as MUSIC, Capon, and ESPRIT [33]. Due to the effect of channel noise, there always exist errors in the estimated direction angles. Given the estimated direction angles $\hat{\theta}_{d_k}$ and $\hat{\theta}_{e_m}$ associated with desired user k and eavesdropper m, we define their main-lobe intervals as

$$S_{d_k} = \left[\hat{\theta}_{d_k} - \frac{\theta_{\text{BW}}}{2},\ \hat{\theta}_{d_k} + \frac{\theta_{\text{BW}}}{2}\right] \tag{15}$$

and

$$S_{e_m} = \left[\hat{\theta}_{e_m} - \frac{\theta_{\text{BW}}}{2},\ \hat{\theta}_{e_m} + \frac{\theta_{\text{BW}}}{2}\right] \tag{16}$$

where

$$\theta_{\text{BW}} = \frac{2\lambda}{Nd} \tag{17}$$

is the beam width between first nulls (BWFN) for a long broadside array [34]. Therefore, the overall direction angle intervals of all main-lobes of desired users and eavesdroppers are

$$S_d = \bigcup_{k=1}^{K}\left[\hat{\theta}_{d_k} - \frac{\theta_{\text{BW}}}{2}, \hat{\theta}_{d_k} + \frac{\theta_{\text{BW}}}{2}\right] \quad \bar{S}_d = [0,\ \pi]\setminus S_d \tag{18}$$

and

$$S_e = \bigcup_{m=1}^{M}\left[\hat{\theta}_{e_m} - \frac{\theta_{\text{BW}}}{2},\ \hat{\theta}_{e_m} + \frac{\theta_{\text{BW}}}{2}\right] \tag{19}$$

respectively. Based on the above discussion, the average power of confidential message stream d_k sent to desired user k is

$$\begin{aligned} P_{d_k,U} &= \mathbb{E}\left\{\int_{S_{d_k}} \alpha_1^2\beta_1^2 P_s d_k^H \mathbf{v}_{d_k}^H \mathbf{h}(\theta)\mathbf{h}^H(\theta)\mathbf{v}_{d_k} d_k\, d\theta\right\} \\ &= \int_{S_{d_k}} \alpha_1^2\beta_1^2 P_s \mathbf{v}_{d_k}^H \mathbf{h}(\theta)\mathbf{h}^H(\theta)\mathbf{v}_{d_k}\, d\theta. \end{aligned} \tag{20}$$

The remaining power leakage of confidential message stream d_k to other desired users and all eavesdroppers is represented as

$$\begin{aligned} P_{d_k,L} &= \sum_{i=1,i\neq k}^{K} \mathbb{E}\left\{\int_{S_{d_i}} \alpha_1^2\beta_1^2 P_s d_k^H \mathbf{v}_{d_k}^H \mathbf{h}(\theta)\mathbf{h}^H(\theta)\mathbf{v}_{d_k} d_k\, d\theta\right\} \\ &\quad + \sum_{m=1}^{M} \mathbb{E}\left\{\int_{S_{e_m}} \alpha_1^2\beta_1^2 P_s d_k^H \mathbf{v}_{d_k}^H \mathbf{h}(\theta)\mathbf{h}^H(\theta)\mathbf{v}_{d_k} d_k\, d\theta\right\} \end{aligned} \tag{21}$$

which can be simplified as

$$\begin{aligned} P_{d_k,L} &= \sum_{i=1,i\neq k}^{K} \int_{S_{d_i}} \alpha_1^2\beta_1^2 P_s \mathbf{v}_{d_k}^H \mathbf{h}(\theta)\mathbf{h}^H(\theta)\mathbf{v}_{d_k}\, d\theta \\ &\quad + \sum_{m=1}^{M} \int_{S_{e_m}} \alpha_1^2\beta_1^2 P_s \mathbf{v}_{d_k}^H \mathbf{h}(\theta)\mathbf{h}^H(\theta)\mathbf{v}_{d_k}\, d\theta \end{aligned} \tag{22}$$

where the first and second terms are the leakage powers to other desired users and all eavesdroppers, respectively. We define the corresponding MLI-SLNR as follows:

$$\text{MLI-SLNR}(\mathbf{v}_{d_k}) = \frac{P_{d_k,U}}{\int_{S_{d_k}} \sigma_{d_k}^2\, d\theta + P_{d_k,L}} \tag{23}$$

which, according to Appendix A, can be simplified as

$$\begin{aligned} &\text{MLI-SLNR}(\mathbf{v}_{d_k}) \\ &= \frac{\mathbf{v}_{d_k}^H \mathbf{R}_{S_{d_k}} \mathbf{v}_{d_k}}{\mathbf{v}_{d_k}^H \left(\frac{\sigma_{d_k}^2 \theta_{\text{BW}}}{\alpha_1^2\beta_1^2 P_s}\mathbf{I}_N + \mathbf{R}_{S_d\setminus S_{d_k}} + \mathbf{R}_{S_e}\right)\mathbf{v}_{d_k}} \end{aligned} \tag{24}$$

where matrix $\mathbf{R}_S$ is defined as

$$\mathbf{R}_S = \int_S \mathbf{h}(\theta)\mathbf{h}^H(\theta)\, d\theta \tag{25}$$

where S is the integral interval with single continuous interval or the union of several subintervals and each element of $\mathbf{R}_S$ is the definite integration of the corresponding element in the $N \times N$ matrix $\mathbf{h}(\theta)\mathbf{h}^H(\theta)$, which is a function of θ, over the interval S. The detailed derivation of matrix $\mathbf{R}_S$ is given in Appendix B. Maximizing the MLI-SLNR in (24) by using the generalized Rayleigh–Ritz theorem presented in [35] yields that the optimal $\mathbf{v}_{d_k}$ is the normalized eigenvector corresponding to the largest eigenvalue of

$$\left[\frac{\sigma_{d_k}^2 \theta_{\text{BW}}}{\alpha_1^2\beta_1^2 P_s}\mathbf{I}_N + \mathbf{R}_{S_d\setminus S_{d_k}} + \mathbf{R}_{S_e}\right]^{-1} \mathbf{R}_{S_{d_k}}. \tag{26}$$

Until now we complete the design of $\mathbf{v}_{d_k}$. Below, we similarly construct the projection matrix $\mathbf{T}_{\text{AN}}$ of AN. The basic idea is to project less power of AN onto the subspace spanned by all desired steering vectors and more onto its null space. Here, we view the AN as a useful signal. The average AN power sent to all main-lobes of all eavesdropper directions is as follows:

$$\begin{aligned} &P_{\text{AN},U} \\ &= \mathbb{E}\left\{\int_{S_e} \alpha_2^2\beta_2^2 P_s \text{tr}\left[\mathbf{h}^H(\theta)\mathbf{T}_{\text{AN}}\mathbf{z}\mathbf{z}^H\mathbf{T}_{\text{AN}}^H\mathbf{h}(\theta)\right]\, d\theta\right\} \\ &= \int_{S_e} \alpha_2^2\beta_2^2 P_s \text{tr}\left[\mathbf{h}^H(\theta)\mathbf{T}_{\text{AN}}\mathbb{E}\left\{\mathbf{z}\mathbf{z}^H\right\}\mathbf{T}_{\text{AN}}^H\mathbf{h}(\theta)\right]\, d\theta. \end{aligned} \tag{27}$$

Given $\mathbb{E}\left\{\mathbf{z}\mathbf{z}^H\right\} = \frac{1}{N-K}\mathbf{I}_{N-K}$ and $\text{tr}(\mathbf{AB}) = \text{tr}(\mathbf{BA})$, the above equation is reduced to

$$P_{\text{AN},U} = \frac{\alpha_2^2\beta_2^2 P_s}{N-K}\text{tr}\left[\mathbf{T}_{\text{AN}}^H\mathbf{R}_{S_e}\mathbf{T}_{\text{AN}}\right]. \tag{28}$$

The average leakage power of AN to main-lobes of all desired directions is given by

$$P_{\text{AN},L} = \mathbb{E}\left\{\int_{S_d} \alpha_2^2\beta_2^2 P_s \text{tr}\left[\mathbf{z}^H \mathbf{T}_{\text{AN}}^H \mathbf{h}(\theta)\mathbf{h}^H(\theta)\mathbf{T}_{\text{AN}}\mathbf{z}\right]\, d\theta\right\}. \quad (29)$$

Similar to (28), we have

$$P_{\text{AN},L} = \frac{\alpha_2^2\beta_2^2 P_s}{N-K}\text{tr}\left[\mathbf{T}_{\text{AN}}^H \mathbf{R}_{S_d}\mathbf{T}_{\text{AN}}\right]. \quad (30)$$

Combining the above two expressions and using the definition of SLNR, we have the MLI-SLNR of AN as

$$\text{MLI-SLNR}(\mathbf{T}_{\text{AN}}) = \frac{P_{\text{AN},U}}{\int_{S_e}\sigma_e^2\, d\theta + P_{\text{AN},L}} = \frac{\text{tr}\left[\mathbf{T}_{\text{AN}}^H \mathbf{R}_{S_e}\mathbf{T}_{\text{AN}}\right]}{\frac{(N-K)M\theta_{\text{BW}}\sigma_e^2}{\alpha_2^2\beta_2^2 P_s} + \text{tr}\left[\mathbf{T}_{\text{AN}}^H \mathbf{R}_{S_d}\mathbf{T}_{\text{AN}}\right]} \quad (31)$$

where

$$\sigma_e^2 = \frac{1}{M}\sum_{m=1}^{M}\sigma_{e_m}^2. \quad (32)$$

As a result, the optimal $\mathbf{T}_{\text{AN}}$ when maximizing the MLI-SLNR in (31) is composed of the $N-K$ normalized eigenvectors corresponding to the $N-K$ largest eigenvalues of matrix

$$\left[\frac{(N-K)M\theta_{\text{BW}}\sigma_e^2}{\alpha_2^2\beta_2^2 P_s}\mathbf{I}_N + \mathbf{R}_{S_d}\right]^{-1}\mathbf{R}_{S_e}. \quad (33)$$

B. Unknown Eavesdropper Directions

In the following, we consider a more practical scenario, where the BS does not know the exact or estimated direction values of eavesdroppers. In such a situation, all the remaining angle region excluding the union of main-lobes of all desired directions, which is actually the complementary set $\bar{S}_d$ of S_d, will be viewed as the potential eavesdropper directions. For desired user k, the main-lobe profile of all eavesdropper and the remaining desired directions are virtually viewed as a potential set of intercepting directions, defined as the complementary set $\bar{S}_{d_k}$ of its main-lobe region S_{d_k}, i.e.,

$$\bar{S}_{d_k} = [0,\ \pi]\setminus S_{d_k} = \left[0,\ \hat{\theta}_{d_k} - \frac{\theta_{\text{BW}}}{2}\right]\bigcup\left[\hat{\theta}_{d_k} + \frac{\theta_{\text{BW}}}{2},\ \pi\right]. \quad (34)$$

Note that the useful part $P'_{d_k,U}$ of transmit signal power of desired user k has the same expression as $P_{d_k,U}$ in (20). The power leakage of confidential message stream d_k transmitted by BS to the set $\bar{S}_{d_k}$ of all potential eavesdropper directions is represented as

$$P'_{d_k,L} = \mathbb{E}\left\{\int_{\bar{S}_{d_k}} \alpha_1^2\beta_1^2 P_s d_k^H \mathbf{v}_{d_k}^H \mathbf{h}(\theta)\mathbf{h}^H(\theta)\mathbf{v}_{d_k} d_k\, d\theta\right\} = \int_{\bar{S}_{d_k}} \alpha_1^2\beta_1^2 P_s \mathbf{v}_{d_k}^H \mathbf{h}(\theta)\mathbf{h}^H(\theta)\mathbf{v}_{d_k}\, d\theta. \quad (35)$$

Similar to (23), we can readily obtain the MLI-SLNR expression corresponding to the kth desired user as follows:

$$\text{MLI-SLNR}'(\mathbf{v}_{d_k}) = \frac{P'_{d_k,U}}{\int_{S_{d_k}}\sigma_{d_k}^2\, d\theta + P'_{d_k,L}} = \frac{\mathbf{v}_{d_k}^H \mathbf{R}_{S_{d_k}}\mathbf{v}_{d_k}}{\mathbf{v}_{d_k}^H\left(\frac{\sigma_{d_k}^2\theta_{\text{BW}}}{\alpha_1^2\beta_1^2 P_s}\mathbf{I}_N + \mathbf{R}_{\bar{S}_{d_k}}\right)\mathbf{v}_{d_k}}. \quad (36)$$

The optimal $\mathbf{v}_{d_k}$ to maximize the MLI-SLNR in (36) is the generalized eigenvector corresponding to the largest normalized eigenvalue of

$$\left[\frac{\sigma_{d_k}^2\theta_{\text{BW}}}{\alpha_1^2\beta_1^2 P_s}\mathbf{I}_N + \mathbf{R}_{\bar{S}_{d_k}}\right]^{-1}\mathbf{R}_{S_{d_k}}. \quad (37)$$

For the design of $\mathbf{T}_{\text{AN}}$ with unknown directions of eavesdroppers, the angle range of all potential eavesdropping directions is $\bar{S}_d$, the average transmit AN power in $\bar{S}_d$ is

$$P'_{\text{AN},U} = \mathbb{E}\left\{\int_{\bar{S}_d} \alpha_2^2\beta_2^2 P_s \text{tr}\left[\mathbf{h}^H(\theta)\mathbf{T}_{\text{AN}}\mathbf{z}\mathbf{z}^H\mathbf{T}_{\text{AN}}^H\mathbf{h}(\theta)\right]\, d\theta\right\} = \frac{\alpha_2^2\beta_2^2 P_s}{N-K}\text{tr}\left[\mathbf{T}_{\text{AN}}^H\mathbf{R}_{\bar{S}_d}\mathbf{T}_{\text{AN}}\right] \quad (38)$$

and the average leakage AN power $P'_{\text{AN},L}$ to main-lobes of all desired directions is the same as (30). Based on the definition of SLNR, we have the MLI-SLNR expression of AN as

$$\text{MLI-SLNR}'(\mathbf{T}_{\text{AN}}) = \frac{P'_{\text{AN},U}}{\int_{\bar{S}_d}\sigma_e^2\, d\theta + P'_{\text{AN},L}} = \frac{\text{tr}\left[\mathbf{T}_{\text{AN}}^H\mathbf{R}_{\bar{S}_d}\mathbf{T}_{\text{AN}}\right]}{\frac{(N-K)(\pi-K\theta_{\text{BW}})\sigma_e^2}{\alpha_2^2\beta_2^2 P_s} + \text{tr}\left[\mathbf{T}_{\text{AN}}^H\mathbf{R}_{S_d}\mathbf{T}_{\text{AN}}\right]}. \quad (39)$$

Similar to (33), via maximizing the MLI-SLNR in (39), the optimal $\mathbf{T}_{\text{AN}}$ is composed of the $N-K$ normalized eigenvectors corresponding to the $N-K$ largest eigenvalues of matrix

$$\left[\frac{(N-K)(\pi-K\theta_{\text{BW}})\sigma_e^2}{\alpha_2^2\beta_2^2 P_s}\mathbf{I}_N + \mathbf{R}_{S_d}\right]^{-1}\mathbf{R}_{\bar{S}_d}. \quad (40)$$

IV. Simulation and Discussion

To evaluate the BER and SSR performance of the proposed robust method, quadrature phase-shift keying is chosen, and main simulation parameters are listed in Table II.

Here, signal-to-noise ratio is defined as $\text{SNR} = 10\log_{10}(\alpha_1^2\beta_1^2 P_s/\sigma_\omega^2)$, where $\sigma_{d_k}^2 = \sigma_{e_m}^2 = \sigma_\omega^2, \forall k \in \{1,2\}, \forall m \in \{1,2,3\}$. All measurement errors of desired and eavesdropper direction angles are assumed to be independently uniform distributed over the interval $[-\Delta\theta_{\max}, \Delta\theta_{\max}]$. The orthogonal projection (OP) method presented in [24] and the conventional leakage-based method presented in [28] are adopted as performance references, respectively. All the remaining angle region excluding the union of main-lobes of all desired directions will

TABLE II
MAIN SIMULATION PARAMETERS AND THEIR VALUES

Parameter	Value
d	$\lambda/2$
N	16
K	2
$\{\theta_{d_k}\}_{k=1}^{K}$	$\{60^\circ, 120^\circ\}$
M	3
$\{\theta_{e_m}\}_{m=1}^{M}$	$\{30^\circ, 90^\circ, 150^\circ\}$
P_s	1
β_1	$\sqrt{0.9}$
β_2	$\sqrt{0.1}$
$\Delta\theta_{\max}$	5°

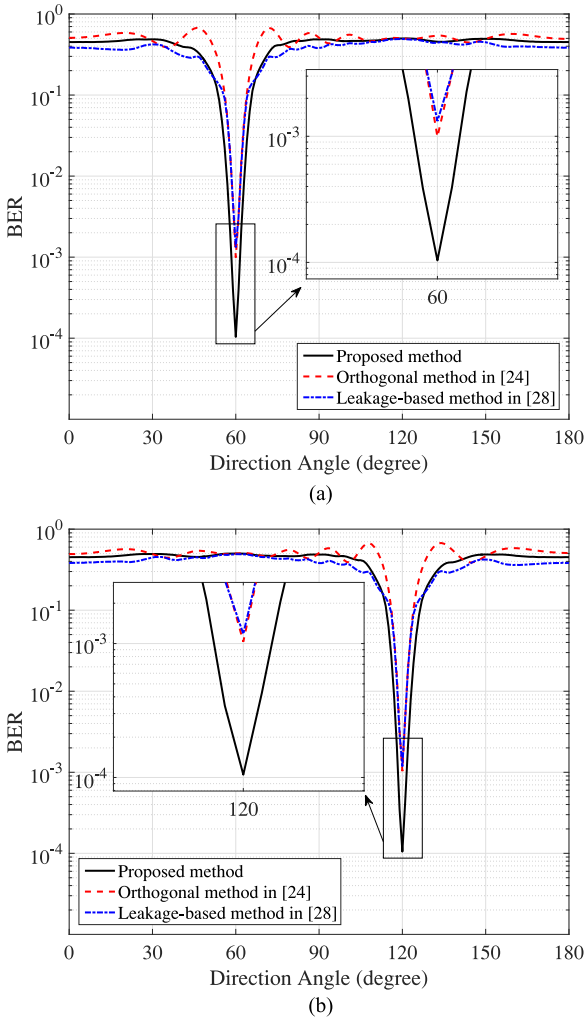


Fig. 3. BER versus direction angle with imperfect desired and eavesdropper directions (SNR = 14 dB). (a) $\theta_{d_1} = 60^\circ$. (b) $\theta_{d_2} = 120^\circ$

be viewed as the potential eavesdropper directions when eavesdroppers' information are unable to be available.

Given the estimated desired and eavesdropper directions, Fig. 3(a) and (b) illustrates the curves of BER versus direction angle of the proposed robust method in Section III-A, the OP method presented in [24] and the conventional leakage-based method presented in [28] for the first and second desired receivers, respectively. In the Fig. 3(a), it can be observed that our

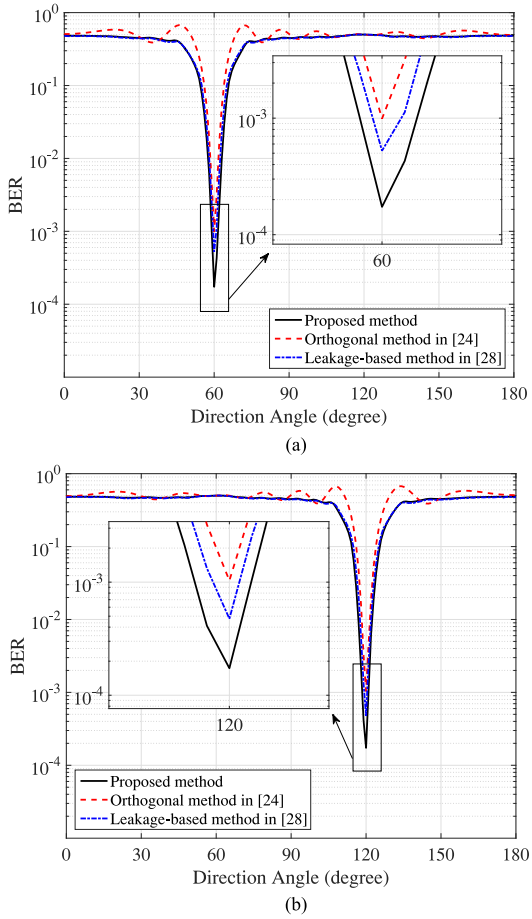


Fig. 4. BER versus direction angle with unknown eavesdropper directions (SNR = 14 dB). (a) $\theta_{d_1} = 60^\circ$. (b) $\theta_{d_2} = 120^\circ$

proposed method at the desired direction 60° shows about an order-of-magnitude improvement over that of the OP method and the conventional leakage-based method. The lowest BER values of the OP method and the conventional leakage-based method are approximately at the same level. As the receiver direction angle steers away from the desired direction, the BER performance of both methods degrade rapidly. Compared to the remaining two methods, the BER curve of our proposed method fluctuates less outside the main-lobe of the desired direction. For the second desired user with direction $\theta_{d_2} = 120^\circ$ in Fig. 3(b), the performance trend is similar to the first desired user.

Given the estimated desired directions and under unknown eavesdropper directions, Fig. 4(a) and (b) plots the curves of BER versus direction angle of the proposed robust method in Section III-B, the OP method presented in [24], and the conventional leakage-based method presented in [28], respectively, for the first and second desired receivers. From Fig. 4(a), similar to Fig. 3(a), we can see that the proposed method still outperforms the OP by approximately an order-of-magnitude in the desired direction 60°, where the BER value of the proposed method is about one-third of the conventional leakage-based method. More importantly, the BER of the proposed method is about 40 percent in the remaining region outside the main-lobe of the desired direction, and the curve fluctuates less than that

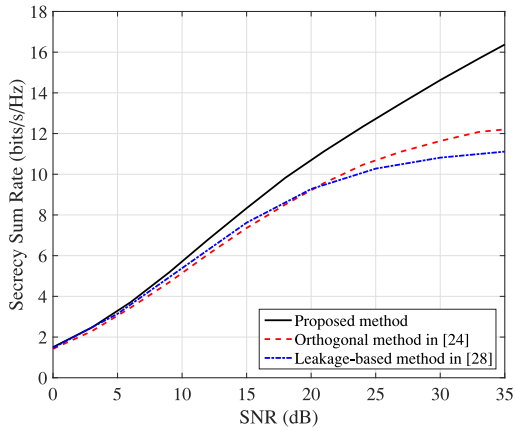


Fig. 5. SSR versus SNR with imperfect desired and eavesdropper directions.

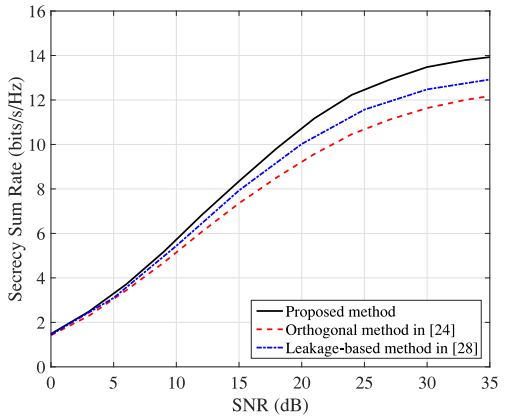


Fig. 6. SSR versus SNR with unknown eavesdropper directions.

of the other two methods. This provides an effective barrier to prevent potential eavesdroppers recovering confidential information. Fig. 4(b) presents a similar BER performance trend for the second desired direction 120° to Fig. 4(a).

In the following, we will evaluate the performance of the proposed method from the SSR aspect. Fig. 5 demonstrates the curves of SSR versus SNR for the proposed method with imperfect desired and eavesdropper directions in Section III-A, the OP method presented in [24], and the conventional leakage-based method presented in [28]. As can be seen from Fig. 5, with the increase in SNR, the SSRs of all three methods increase continuously and monotonously. The SSR of the proposed method is always larger than that of the remaining two methods. Their SSR values are up to 16.4 b/s/Hz, 12.2 b/s/Hz, and 11.1 b/s/Hz at SNR $=$ 35 dB, respectively. Hence, the SSR improvement of the proposed method over the OP method and the conventional leakage-based method is significant. Additionally, the SSRs of the three methods approach the same value as SNR goes to 0 dB. The rate gap between the proposed method and the other two methods grows gradually with the increase in SNR.

In the scenario of unknown eavesdropper directions, Fig. 6 demonstrates the curves of SSR versus SNR for the proposed method in Section III-B, the OP method presented in [24], and the conventional leakage-based method presented in [28]. As indicated in Fig. 6, the proposed method performs better than the OP method and the conventional leakage-based method in terms of SSR, in particular, in the medium and high SNR regions. Their SSR values are up to 14.0 b/s/Hz, 12.2 b/s/Hz, and 12.8 b/s/Hz at SNR $=$ 35 dB, respectively, in which case the proposed method shows an approximate 15% and 9% SSR improvement over the OP and the conventional leakage-based method, respectively. Additionally, the SSRs of all three methods tend to be the same in the low SNR region. The rate gap between the proposed method and the other two methods, similar to Fig. 5, grows gradually with the increase in SNR.

Note that the SSRs of the proposed method in Fig. 6 are less than the corresponding SSRs of the proposed method in Fig. 5 in the middle and high regions. This implies that the measured values of eavesdropper direction angles play an important role in improving the SSR performance.

In this paper, the numerical simulation results is presented to verify the effectiveness of the proposed method. Due to MLI, the channel noise and the measurement errors are smoothed and filtered along the main-lobe interval of the desired directions. This enhances the robustness of the presented method, and results in a better performance compared with the conventional nonrobust methods.

V. Conclusion

In this paper, we study robust precoding in MU-MIMO DM systems under imperfect desired directions and eavesdropper directions or unknown eavesdropper directions. To realize the high-performance robust secure multi-message-stream simultaneous transmission in MU-MIMO systems, we propose an MLI-based precoding method. In the first stage, the precoding vector per desired user is optimized to maximize the transmit power of useful confidential messages along the main-lobe of the corresponding desired direction and correspondingly minimize the transmit power of AN along all eavesdropper directions. In the second stage, the AN projection matrix is designed to force AN to all eavesdropper directions with only a small amount of residual AN along the main-lobes of the desired directions. Due to the use of MLI, the proposed method requires no perfect direction knowledge or the distribution of measurement errors of direction angle, and at the same time provides a robust performance. Simulation results verify the performance benefits of our method. Compared with OP, the proposed method can achieve an one-order-magnitude improvement on BER and at the same time its SSR along the desired directions is shown to have a substantial enhancement over that of OP in the high SNR region. The proposed scheme can be applied to the future satellite communications, mobile communications, D2D, V2V, UAV networks, and IoT.

Appendix A
Simplification of MLI-SLNR$(\mathbf{v}_{d_k})$

Proof: The simplification of MLI-SLNR$(\mathbf{v}_{d_k})$ is shown in (41) at the bottom of the next page, where $\stackrel{a}{=}$ is achieved by extracting integral term $\mathbf{h}(\theta)\mathbf{h}^H(\theta)$, $\stackrel{b}{=}$ is

achieved by replacing $\int_{S_{d_k}} \mathbf{h}(\theta)\mathbf{h}^H(\theta)\,d\theta$, $\int_{S_{d_i}} \mathbf{h}(\theta)\mathbf{h}^H(\theta)\,d\theta$, and $\int_{S_{e_m}} \mathbf{h}(\theta)\mathbf{h}^H(\theta)\,d\theta$ by $\mathbf{R}_{S_{d_k}}$, $\mathbf{R}_{S_{d_i}}$, and $\mathbf{R}_{S_{e_m}}$, respectively. ■

APPENDIX B
DERIVATION OF $\mathbf{R}_S$

Proof: The integral matrix $\mathbf{R}_S$ in (25) is an $N \times N$ matrix. Here, we assume that set S is a union of I separate subintervals as follows:

$$S = \bigcup_{i=1}^{I} S_i \tag{42}$$

where

$$S_i = [\theta^i_{\min},\ \theta^i_{\max}]. \tag{43}$$

Then the (p,q) entry of $\mathbf{R}_{S_i}$ has the following form:

$$\begin{aligned}\mathbf{R}_{S_i}(p,q) &= \int_{\theta^i_{\min}}^{\theta^i_{\max}} \mathbf{h}_p(\theta)\mathbf{h}_q^H(\theta)\,d\theta \\ &= \int_{\theta^i_{\min}}^{\theta^i_{\max}} \frac{1}{\sqrt{N}} e^{\frac{j2\pi(p-(N+1)/2)d\cos\theta}{\lambda}} \\ &\quad \cdot \frac{1}{\sqrt{N}} e^{-\frac{j2\pi(q-(N+1)/2)d\cos\theta}{\lambda}}\,d\theta \\ &= \frac{1}{N}\int_{\theta^i_{\min}}^{\theta^i_{\max}} e^{\frac{j2\pi(p-q)d\cos\theta}{\lambda}}\,d\theta. \end{aligned} \tag{44}$$

Let us define the center point and length of integral interval as

$$\theta^i_0 = \frac{\theta^i_{\min} + \theta^i_{\max}}{2} \tag{45}$$

and

$$\Delta\theta_i = \theta^i_{\max} - \theta^i_{\min} \tag{46}$$

respectively, and the new integral variable is

$$x = \frac{2\pi}{\Delta\theta_i}(\theta - \theta^i_0) \tag{47}$$

i.e.,

$$\theta = \frac{\Delta\theta_i}{2\pi}x + \theta^i_0. \tag{48}$$

Using the above definition or transformation, (44) is re-written as

$$\begin{aligned}&\mathbf{R}_{S_i}(p,q) \\ &= \frac{1}{N}\int_{-\pi}^{\pi} e^{\frac{j2\pi(p-q)d\cos(\frac{\Delta\theta_i}{2\pi}x+\theta^i_0)}{\lambda}} \cdot \frac{\Delta\theta_i}{2\pi}\,dx \\ &= \frac{\Delta\theta_i}{2\pi N}\int_{-\pi}^{\pi} e^{\frac{j2\pi(p-q)d\cos(\frac{\Delta\theta_i}{2\pi}x+\theta^i_0)}{\lambda}}\,dx \\ &= \frac{\Delta\theta_i}{2\pi N}\int_{-\pi}^{\pi} e^{\frac{j2\pi(p-q)d\left[\cos(\theta^i_0)\cos(\frac{\Delta\theta_i}{2\pi}x)-\sin(\theta^i_0)\sin(\frac{\Delta\theta_i}{2\pi}x)\right]}{\lambda}}\,dx \\ &= \frac{\Delta\theta_i}{2\pi N}\int_{-\pi}^{\pi} e^{\left[a^i_{pq}\cos(c_i x)+b^i_{pq}\sin(c_i x)\right]}\,dx \\ &= \frac{\Delta\theta_i}{N}\mathrm{g}_B(a^i_{pq}, b^i_{pq}, c_i) \end{aligned} \tag{49}$$

where $\mathrm{g}_B(\cdot)$ is the extension of the modified Bessel function of the first kind with the integer order 0 [36], i.e.

$$\mathrm{g}_B(a^i_{pq}, b^i_{pq}, c_i) = \frac{1}{2\pi}\int_{-\pi}^{\pi} e^{\left[a^i_{pq}\cos(c_i x)+b^i_{pq}\sin(c_i x)\right]}\,dx \tag{50}$$

$$a^i_{pq} \triangleq \frac{j2\pi(p-q)d\cos(\theta^i_0)}{\lambda} \tag{51}$$

$$b^i_{pq} \triangleq -\frac{j2\pi(p-q)d\sin(\theta^i_0)}{\lambda} \tag{52}$$

$$\begin{aligned}\text{MLI-SLNR}(\mathbf{v}_{d_k}) &= \frac{\int_{S_{d_k}} \alpha_1^2\beta_1^2 P_s \mathbf{v}_{d_k}^H \mathbf{h}(\theta)\mathbf{h}^H(\theta)\mathbf{v}_{d_k}\,d\theta}{\int_{S_{d_k}} \sigma_{d_k}^2\,d\theta + \sum_{i=1,i\neq k}^{K}\int_{S_{d_i}} \alpha_1^2\beta_1^2 P_s \mathbf{v}_{d_k}^H \mathbf{h}(\theta)\mathbf{h}^H(\theta)\mathbf{v}_{d_k}\,d\theta + \sum_{m=1}^{M}\int_{S_{e_m}} \alpha_1^2\beta_1^2 P_s \mathbf{v}_{d_k}^H \mathbf{h}(\theta)\mathbf{h}^H(\theta)\mathbf{v}_{d_k}\,d\theta} \\ &\overset{a}{=} \frac{\alpha_1^2\beta_1^2 P_s \mathbf{v}_{d_k}^H \int_{S_{d_k}} \mathbf{h}(\theta)\mathbf{h}^H(\theta)\,d\theta\mathbf{v}_{d_k}}{\int_{S_{d_k}} \sigma_{d_k}^2\,d\theta + \alpha_1^2\beta_1^2 P_s \mathbf{v}_{d_k}^H \sum_{i=1,i\neq k}^{K}\int_{S_{d_i}} \mathbf{h}(\theta)\mathbf{h}^H(\theta)\,d\theta\mathbf{v}_{d_k} + \alpha_1^2\beta_1^2 P_s \mathbf{v}_{d_k}^H \sum_{m=1}^{M}\int_{S_{e_m}} \mathbf{h}(\theta)\mathbf{h}^H(\theta)\,d\theta\mathbf{v}_{d_k}} \\ &\overset{b}{=} \frac{\alpha_1^2\beta_1^2 P_s \mathbf{v}_{d_k}^H \mathbf{R}_{S_{d_k}}\mathbf{v}_{d_k}}{\sigma_{d_k}^2\theta_{\text{BW}} + \alpha_1^2\beta_1^2 P_s \mathbf{v}_{d_k}^H \sum_{i=1,i\neq k}^{K}\mathbf{R}_{S_{d_i}}\mathbf{v}_{d_k} + \alpha_1^2\beta_1^2 P_s \mathbf{v}_{d_k}^H \sum_{m=1}^{M}\mathbf{R}_{S_{e_m}}\mathbf{v}_{d_k}} \\ &= \frac{\alpha_1^2\beta_1^2 P_s \mathbf{v}_{d_k}^H \mathbf{R}_{S_{d_k}}\mathbf{v}_{d_k}}{\sigma_{d_k}^2\theta_{\text{BW}} + \alpha_1^2\beta_1^2 P_s \mathbf{v}_{d_k}^H \mathbf{R}_{S_d\setminus S_{d_k}}\mathbf{v}_{d_k} + \alpha_1^2\beta_1^2 P_s \mathbf{v}_{d_k}^H \mathbf{R}_{S_e}\mathbf{v}_{d_k}} \\ &= \frac{\mathbf{v}_{d_k}^H \mathbf{R}_{S_{d_k}}\mathbf{v}_{d_k}}{\frac{\sigma_{d_k}^2\theta_{\text{BW}}}{\alpha_1^2\beta_1^2 P_s} + \mathbf{v}_{d_k}^H \mathbf{R}_{S_d\setminus S_{d_k}}\mathbf{v}_{d_k} + \mathbf{v}_{d_k}^H \mathbf{R}_{S_e}\mathbf{v}_{d_k}} \\ &= \frac{\mathbf{v}_{d_k}^H \mathbf{R}_{S_{d_k}}\mathbf{v}_{d_k}}{\mathbf{v}_{d_k}^H\left(\frac{\sigma_{d_k}^2\theta_{\text{BW}}}{\alpha_1^2\beta_1^2 P_s}\mathbf{I}_N + \mathbf{R}_{S_d\setminus S_{d_k}} + \mathbf{R}_{S_e}\right)\mathbf{v}_{d_k}} \end{aligned} \tag{41}$$

and

$$c_i \triangleq \frac{\Delta\theta_i}{2\pi}. \quad (53)$$

This completes the derivation of the (p, q) entry $\mathbf{R}_{S_i}(p, q)$ of matrix $\mathbf{R}_{S_i}$. Note that set S is a union of I separated subintervals, as shown in (41). Then, the (p, q) element of matrix $\mathbf{R}_S$ is expanded as the summation of integrations over all subintervals

$$\mathbf{R}_S(p, q) = \sum_{i=1}^{I} \mathbf{R}_{S_i}(p, q) = \sum_{i=1}^{I} \frac{\Delta\theta^i}{N} \mathrm{g}_B(a_{pq}^i, b_{pq}^i, c_i). \quad (54)$$

This completes the derivation of matrix $\mathbf{R}_S$. ■

REFERENCES

[1] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, *Signal Processing Approaches to Secure Physical Layer Communications in Multi-Antenna Wireless Systems (Springer Briefs in Electrical and Computer Engineering)*. New York, NY, USA: Springer, 2013.

[2] Y. Zou and J. Zhu, *Physical-Layer Security for Cooperative Relay Networks*. New Year, NY, USA: Springer, 2016.

[3] C. Huang, M. Ma, X. Liu, A. Liu, and Z. Zuo, "Unequal probability marking approach to enhance security of traceback scheme in tree-based WSNS," *Sensors*, vol. 17, no. 6, pp. 1418–1442, Jun. 2017.

[4] Y. Liu, M. Dong, K. Ota, and A. Liu, "Activetrust: Secure and trustable routing in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 9, pp. 2013–2027, Sep. 2016.

[5] Z. Ning, F. Xia, X. Hu, Z. Chen, and M. S. Obaidat, "Social-oriented adaptive transmission in opportunistic internet of smartphones," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 810–820, Apr. 2017.

[6] Z. Ning, L. Liu, F. Xia, B. Jedari, I. Lee, and W. Zhang, "CAIS: A copy adjustable incentive scheme in community-based socially aware networking," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3406–3419, Apr. 2017.

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

[8] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

[9] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[10] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin , "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[11] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[12] Y. L. Zou, J. Zhu, X. Wang, and V. Leung, "Improving physical-layer security in wireless communications through diversity techniques," *IEEE Netw.*, vol. 29, no. 1, pp. 42–48, Jan. 2015.

[13] Y. L. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, "Relay-selection improves the security-reliability trade-off in cognitive radio systems," *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 215–228, Jan. 2015.

[14] X. Chen, D. W. K. Ng, and H. H. Chen, "Secrecy wireless information and power transfer: Challenges and opportunities," *IEEE Wireless Commun.*, vol. 23, no. 2, pp. 54–61, Apr. 2016.

[15] N. Zhao, F. R. Yu, M. Li, Q. Yan, and V. C. Leung, "Physical layer security issues in interference-alignment-based wireless networks," *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 162–168, Aug. 2016.

[16] A. Babakhani, D. B. Rutledge, and A. Hajimiri, "Transmitter architectures based on near-field direct antenna modulation," *IEEE J. Solid-State Circuits*, vol. 43, no. 12, pp. 2674–2692, Dec. 2008.

[17] M. P. Daly, E. L. Daly, and J. T. Bernhard, "Directional modulation technique for phased arrays," *IEEE Trans. Antennas Propag.*, vol. 57, no. 9, pp. 2633–2640, Sep. 2009.

[18] M. P. Daly, E. L. Daly, and J. T. Bernhard, "Demonstration of directional modulation using a phased array," *IEEE Trans. Antennas Propag.*, vol. 58, no. 5, pp. 1545–1550, May 2010.

[19] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[20] X. Zhou and M. R. McKay, "Physical layer security with artificial noise: Secrecy capacity and optimal power allocation," in *Proc. Int. Conf. Signal Process. Commun. Syst.*, Sep. 2009, pp. 1–5.

[21] N. Zhao, F. R. Yu, M. Li, and V. C. Leung, "Anti-eavesdropping schemes for interference alignment (IA)-based wireless networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5719–5732, Aug. 2016.

[22] Y. Ding and V. Fusco, "A vector approach for the analysis and synthesis of directional modulation transmitters," *IEEE Trans. Antennas Propag.*, vol. 62, no. 1, pp. 361–370, Jan. 2014.

[23] Y. Ding and V. Fusco, "Directional modulation far-field pattern separation synthesis approach," *IET Microw. Antennas Propag.*, vol. 9, no. 1, pp. 41–48, Jan. 2015.

[24] Y. Ding and V. Fusco, "Orthogonal vector approach for synthesis of multi-beam directional modulation transmitters," *IEEE Antennas Wireless Propag. Lett.*, vol. 14, pp. 1330–1333, Feb. 2015.

[25] J. Hu, F. Shu, and J. Li, "Robust synthesis method for secure directional modulation with imperfect direction angle," *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1084–1087, Jun. 2016.

[26] F. Shu, X. Wu, J. Li, R. Chen, and B. Vucetic, "Robust synthesis scheme for secure multi-beam directional modulation in broadcasting systems," *IEEE Access*, vol. 4, pp. 6614–6623, 2016.

[27] A. Tarighat, M. Sadek, and A. H. Sayed, "A multi-user beamforming scheme for downlink MIMO channels based on maximizing signal-to-leakage ratios," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, Philadelphia, PA, USA, Mar. 2005, vol. 3, pp. 1129–1132.

[28] M. Sadek, A. Tarighat, and A. H. Sayed, "A leakage-based procoding scheme for downlink multi-user MIMO channels," *IEEE Trans. Wireless Commun.*, vol. 6, no. 5, pp. 1711–1721, Jun. 2007.

[29] F. Shu, M. M. Wang, Y. X. Wang, H. Q. Fan, and J. H. Lu, "An efficient power allocation scheme for leakage-based precoding in multi-cell multiuser MIMO downlink," *IEEE Commun. Lett.*, vol. 6, no. 5, pp. 1053–1055, Oct. 2011.

[30] F. Shu, J. J. Tong, X. H. You, C. Gu, and J. J. Wu, "Adaptive robust Max-SLNR precoder for MU-MIMO-OFDM systems with imperfect CSI," *Sci. China Inf. Sci.*, vol. 59, no. 6, pp. 1–14, Jun. 2016.

[31] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[32] N. Li, X. Tao, and J. Xu, "Ergodic secrecy sum-rate for downlink multiuser MIMO systems with limited CSI feedback," *IEEE Commun. Lett.*, vol. 18, no. 6, pp. 969–972, Jun. 2014.

[33] F. Gross, *Smart Antennas for Wireless Communications: With MATLAB*. New York, NY, USA: McGraw-Hill, 2005.

[34] J. D. Kraus and R. J. Marhefka, *Antennas for All Applications*, 3rd ed. New York, NY, USA: McGraw-Hill, 2006.

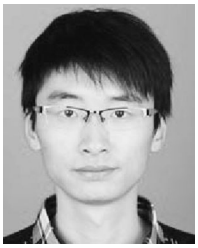
[35] R. A. Horn and C. R. Johnson, *Matrix Analysis*. Cambridge, U.K.: Cambridge Univ. Press, 1987.

[36] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. San Diego, CA, USA: Academic, 2007.

Feng Shu (M'16) was born in 1973. He received the B.S. degree from the Fuyang Teaching College, Fuyang, China, in 1994, the M.S. degree from Xidian University, Xi'an, China, in 1997, and the Ph.D. degree from the Southeast University, Nanjing, China, in 2002.

From October 2003 to October 2005, he was a Postdoctoral Researcher with the National Key Mobile Communication Lab, Southeast University. From September 2009 to September 2010, he held a visiting postdoctoral position with the University of Texas at Dallas. In October 2005, he joined the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing, China, where he is currently a Professor and supervisor of Ph.D. and graduate students. He is also with Fujian Agriculture and Forestry University. He has authored or co-authored about 200 scientific and conference papers of which more than 100 are in archival journals, including more than 20 papers on IEEE journals and 43 SCI-indexed papers. He holds four Chinese patents. His research interests include wireless networks, wireless location, and array signal processing.

Dr. Feng was bestowed the Mingjian Scholar Chair Professor in Fujian Province. He serves as an Editor for IEEE ACCESS. He has served as the Session Chair or Technical Program Committee member for various international conferences such as IEEE WCSP 2016, IEEE VTC 2016, etc.



Wei Zhu received the B.S. degree in electronic information engineering from the Suzhou University of Science and Technology, Suzhou, China, in 2015. He is currently working toward the Ph.D. degree at the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing, China.

His research interests include wireless communication, physical-layer security, and mobile networks.

Xiangwei Zhou received the B.S. degree in communication engineering from the Nanjing University of Science and Technology, Nanjing, China, in 2005, the M.S. degree in information and communication engineering from Zhejiang University, Hangzhou, China, in 2007, and the Ph.D. degree in electrical and computer engineering from the Georgia Institute of Technology, Atlanta, GA, USA, in 2011, under the guidance of Prof. Geoffrey Ye Li.

From 2011 to 2013, he was a Senior Systems Engineer with Marvell Semiconductor, Santa Clara, CA, USA. From 2013 to 2015, he was an Assistant Professor with the Department of Electrical and Computer Engineering, Southern Illinois University Carbondale. Since August 2015, he has been with the Division of Electrical and Computer Engineering, School of Electrical Engineering and Computer Science, Louisiana State University, Baton Rouge, LA, USA. His general research interests include wireless communications, statistical signal processing, and cross-layer optimization, with current emphasis on cognitive radio and spectrum coexistence.

Dr. Zhou was the recipient of the ECE Outstanding Teacher of Year 2014 of Southern Illinois University Carbondale and the Best Paper Award of the 2014 International Conference on Wireless Communications and Signal Processing. He is currently serving on the Editorial Board of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS.

Jun Li (M'09–SM'16) received the Ph.D. degree in electronic engineering from Shanghai Jiao Tong University, Shanghai, China, in 2009.

From January 2009 to June 2009, he was with the Department of Research and Innovation, Alcatel Lucent Shanghai Bell, as a Research Scientist. Since 2015, he has been with the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing, China. His research interests include network information theory, channel coding theory, wireless network coding, and cooperative communications.

Jinhui Lu received the M.S. degree in communication and information system from the Nanjing University of Science and Technology, Nanjing, China, in 1985.

He is currently a Professor with the School of Electronic and Optical Engineering, Nanjing University of Science and Technology. He is a Senior Member with the Chinese Institute of Electronics and the Director of the China Education Society of Electronics. His research interests include millimeter-wave monitoring systems and echo simulation of radar and passive location technology.