Wiretapping Strategies for Artificial Noise Assisted Communication in MU-MIMO wiretap channel

Shu **Wang, Xinyu Da and Zhenyong Chu**
Information and Navigation College, Air Force Engineering University
Xi'an, 710077 - People's Republic of China
[e-mail: xss_wang@163.com]
*Corresponding author: Shu Wang

Received October 30, 2015; revised February 3, 2016; revised February 25, 2016; accepted March 6, 2016; published May 31, 2016

Abstract

We investigate the opposite of artificial noise (AN)-assisted communication in multiple-input–multiple-output (MIMO) wiretap channels for the multiuser case by taking the side of the eavesdropper. We first define a framework for an AN-assisted multiuser multiple-input–multiple-output (MU-MIMO) system, for which eavesdropping methods are proposed with and without knowledge of legitimate users' channel state information (CSI). The proposed method without CSI is based on a modified joint approximate diagonalization of eigen-matrices algorithm, which eliminates permutation indetermination and phase ambiguity, as well as the minimum description length algorithm, which blindly estimates the number of secret data sources. Simulation results show that both proposed methods can intercept information effectively. In addition, the proposed method without legitimate users' CSI performs well in terms of robustness and computational complexity.

Keywords: Physical layer security, artificial noise(AN), joint approximate diagonalization of eigen-matrices (JADE) algorithm, wiretapping

This work was supported by the National Natural Science Foundation of China (NSFC) (No.61271250& 61571460).

http://dx.doi.org/10.3837/tiis.2016.05.012 **ISSN : 1976-7277**

1. Introduction

The issues of privacy and security in wireless communication are gaining increasing attention. Many physical layer security techniques have been proposed to guarantee security by exploiting inherent randomness of the wireless channel [1]-[3]. Wyner first introduced the "wiretap channel" model and proposed the use of the secrecy rate to measure physical layer security performance [4]. Securing data is possible only when the secrecy rate is positive, i.e., the legitimate channel has better quality than the eavesdropper channel. However, maintaining the advantage of the legitimate channel is difficult because the eavesdropper is always passive and its location is unknown to the transmitter. To deal with this situation, Goel [5] proposed an artificial noise (AN)-assisted strategy, which masks the beamformed information to degrade the eavesdropper channel. The AN-assisted strategy is widely used in multiple-input–multiple-output (MIMO) and multiuser MIMO (MU-MIMO) wiretap channels in [6]–[8] to meet the target quality of service through optimal power allocation (PA) between the information signal and AN. In [9], noisy and outdated channel state information (CSI) is assumed at the transmitter. The authors propose a robust beamforming algorithm to achieve the minimum mean square error, while transmitting maximum power for the AN. Work in [10] extends the scheme from the analysis to the imperfect CSI at the eavesdropper. The closed-form expression for the ergodic secrecy sum-rate is derived in the large system limit, where the objective is to optimize the PA between information signals and the AN to maximize secrecy sum-rates.

However, all the above studies only explain the condition that the number of antennas at the eavesdropper is less than that at the transmitter. Private message in physical essence is transmitted in the desired direction, whereas that in deliberate interference is transmitted in other orthogonal directions. Unfortunately, the interference is not white in spatial domain because of the limitation of transmitted antenna number. An eavesdropper can eliminate directional interferences by the aid of multiple antennas. Thus, numerous wiretapping strategies are proposed when equal or more antennas exist at the eavesdropper than that at the transmitter [11]–[13]. For single-user system in AN-assisted multi-input single-output (MISO) channels, the MUSIC-like algorithm [11] using the orthogonality between signal and noise subspace was proposed to recover secret messages successfully by ergodic searching all possible signal sequences in finite alphabet. The hyperplane clustering algorithm (HC) algorithm [12] that uses the distribution of received scrambled signals on parallel hyperplanes was proposed to estimate blindly the hyperplane parameters which reveal the secret information. For single-user system in AN-assisted MIMO channels, the attack on AN-assisted scheme was proposed in [13] to overhear secret messages with the perfect CSI of legitimate users. However, all aforementioned studies aim at single user cases. In multiuser cases, the spatial signature of received scrambled signals changes. Thus, the methods [11], [12] and [13] are not applicable.

In this paper, we investigate the AN-assisted communication in MIMO wiretap channels for the multiuser case from the point of the eavesdropper. We initially define a framework for the AN-assisted system in MU-MIMO wiretap channels. A wiretapping strategy with CSI of legitimate users is then proposed. Another wiretapping strategy without CSI of legitimate users is also proposed based on modified joint approximate diagonalization of eigen-matrices (JADE) and minimum description length (MDL) algorithm. The numerical results verify the effectiveness of our schemes.

The following contributions can be identified. (1) We first investigate the opposite of AN-assisted communication systems for multiuser scenarios, while [11], [12] and [13] are only suitable for single-user scenarios. (2) We consider a general eavesdropping case where no CSI of legitimate users is available in MIMO wiretap channels whereas the algorithm [13] requires that the eavesdropper knows the perfect CSI of the legitimate users; and (3) our proposed method is also applicable when the CSI of perfect legitimate users is unavailable at the transmitter, which relaxes the wiretapping condition.

Our notations are as follows. $(\cdot)^T$, $(\cdot)^H$, $tr(\cdot)$, and $(\cdot)^+$ are matrix conjugate, transpose, trace, and pseudoinverse, respectively. $\mathbb{C}^{m\times n}$ represents the set $m\times n$ matrices in complex fields. $\mathbb{E}\{\cdot\}$ denotes the expected value of a random variable. $\mathcal{CN}(\mu,\delta^2)$ indicates the normal distribution with a mean value μ and a variance δ^2.

2. System Model

We consider a MU-MIMO system, where a transmitter with *Nt* antenna simultaneously sends independent data streams to *K* legitimate receivers with *Nr* antennas each. A *Ne*-antenna eavesdropper attempts to recover all *K* data streams without CSI of the legitimate users. All legitimate users and eavesdroppers have full CSI of their own. The transmitter knows the perfect CSI on the legitimate users but knows nothing about the eavesdropper's CSI. To confuse the eavesdropper, the transmitter sends intended signals together with AN. The overall transmitted signal is given as:

$$\mathbf{x}=\mathbf{W}\mathbf{s}+\mathbf{s}'=\sum_{k=1}^{K}\mathbf{w}_k s_k+\mathbf{s}', \tag{1}$$

where s_k is the information symbol for legitimate user *k* with $\mathbb{E}\{\mathbf{s}\mathbf{s}^H\}=\mathbf{I}$. The vector $\mathbf{s}'$ is the AN signal and $\mathbf{w}_k\in\mathbb{C}^{Nt\times 1}$ is the beamforming vector.

Denoting the $Nt\times Nr$ channel vectors between the transmitter and user *k* by $\mathbf{h}_k$ and the $Nt\times Ne$ channel vectors between the transmitter and the eavesdropper by $\mathbf{G}$. In a broadcast scenario, the signals received by the *k*th legitimate user can be:

$$\mathbf{y}_k=\mathbf{h}_k^H\mathbf{w}_k s_k+\sum_{j=1,j\neq k}^{K}\mathbf{h}_j^H\mathbf{w}_j s_j+\mathbf{h}_k^H\mathbf{s}'+\mathbf{n}_k \tag{2}$$

and by the eavesdropper:

$$\mathbf{y}_e=\mathbf{G}^H\sum_{k=1}^{K}\mathbf{w}_k s_k+\mathbf{G}^H\mathbf{s}'+\mathbf{n}_e \tag{3}$$

where $\mathbf{n}_k$ and $\mathbf{n}_e$ are naturally-occurring independent and identically-distributed (i.i.d.) zero-mean additive white Gaussian noise vector with variances σ_k^2 and σ_e^2, respectively.

Note that legitimate user *k* receives interference signals of other legitimate users $\sum_{j=1,j\neq k}^{K}\mathbf{h}_j^H\mathbf{w}_j s_j$ and the AN $\mathbf{h}_k^H\mathbf{s}'$ in addition to the desired signal $\mathbf{h}_k^H\mathbf{w}_k s_k$. To eliminate interference signals generated by other legitimate users, we design the beamforming matrix by a widely used scheme, block diagonalization (BD) [14] precoding technique. The

beamforming matrix $\mathbf{W}=[\mathbf{w}_1,\mathbf{w}_2,\cdots,\mathbf{w}_K]$ at the legitimate user k should satisfy the following condition:

$$\mathbf{h}_k\mathbf{w}_j=0,\ j=1,2,\cdots,K,\ j\neq k \tag{4}$$

That is, the beamforming vector $\mathbf{w}_k$ is generated in null space of the complement matrix $\tilde{\mathbf{H}}_k$. Define the complement matrix as $\tilde{\mathbf{H}}_k=[\tilde{\mathbf{h}}_1\cdots,\tilde{\mathbf{h}}_{k-1},\tilde{\mathbf{h}}_{k+1},\cdots,\tilde{\mathbf{h}}_K]^T$ where $\tilde{\mathbf{h}}_l=(\mathbf{w}_l^H\mathbf{h}_l)^T$. The singular value decomposition (SVD) of $\tilde{\mathbf{H}}_l$ is:

$$\tilde{\mathbf{H}}_k=\tilde{\mathbf{U}}_k\tilde{\mathbf{\Sigma}}_k[\tilde{\mathbf{V}}_k^{(1)}\tilde{\mathbf{V}}_k^{(0)}]^H \tag{5}$$

where $\tilde{\mathbf{V}}_k^{(0)}$ is the collection of the last $(Nt-\tilde{\mathrm{R}}_k)$ right singular vectors of the complement matrix $\tilde{\mathbf{H}}_l$ whose rank is $\tilde{\mathrm{R}}_k$. $\tilde{\mathbf{V}}_k^{(0)}$ is an orthogonal basis of the null space of $\tilde{\mathbf{H}}_l$. We assume the initial beamforming vector $\mathbf{w}_k=\tilde{\mathbf{V}}_k^{(0)}$, then the equivalent channel for user k is $\mathbf{h}_k\tilde{\mathbf{V}}_k^{(0)}$. The SVD of $\mathbf{h}_k\tilde{\mathbf{V}}_k^{(0)}$ is:

$$\mathbf{h}_k\tilde{\mathbf{V}}_k^{(0)}=\mathbf{U}_k\mathbf{\Sigma}_k[\mathbf{V}_k^{(1)}\mathbf{V}_k^{(0)}]^H \tag{6}$$

where $\mathbf{V}_k^{(1)}$ is the collection of the first R_k' right singular vectors of $\mathbf{h}_k\tilde{\mathbf{V}}_k^{(0)}$ whose rank is R_k' . The final beamforming matrix $\mathbf{W}=[\mathbf{w}_1,\mathbf{w}_2,\cdots,\mathbf{w}_K]$ for user k is given by:

$$\mathbf{W}=[\tilde{\mathbf{V}}_1^{(0)}\mathbf{V}_1^{(1)},\tilde{\mathbf{V}}_2^{(0)}\mathbf{V}_2^{(1)},\cdots,\tilde{\mathbf{V}}_K^{(0)}\mathbf{V}_K^{(1)}]\mathbf{\Lambda}^{1/2}, \tag{7}$$

where $\mathbf{\Lambda}$ is a diagonal matrix whose elements are supposed to be one in this paper. Then, (7) reduces to

$$\mathbf{W}=[\tilde{\mathbf{V}}_1^{(0)}\mathbf{V}_1^{(1)},\tilde{\mathbf{V}}_2^{(0)}\mathbf{V}_2^{(1)},\cdots,\tilde{\mathbf{V}}_K^{(0)}\mathbf{V}_K^{(1)}]. \tag{8}$$

To guarantee that AN will not affect all legitimate receivers, AN is designed to be generated in the null space of $\mathbf{H}=[\mathbf{h}_1,\mathbf{h}_2,\cdots,\mathbf{h}_K]$, i.e., $\mathbf{s}'=\mathbf{Z}\mathbf{t}$, where $\mathbf{Z}\in\mathbb{C}^{Nt\times(Nt-K)}$ is an orthogonal basis of the null space of $\mathbf{H}$ and $\mathbf{t}$ are i.i.d. $\mathcal{CN}(0,1)$ variables. Here, we assume $K<Nt$ to ensure the existence of $\mathbf{Z}$.

Thus, (1) can be represented as:

$$\begin{aligned}\mathbf{x}&=\mathbf{W}\mathbf{s}+\mathbf{s}'=[\mathbf{W}\ \mathbf{Z}][\mathbf{s}\ \mathbf{t}]^{\mathrm{T}}\\&=[\tilde{\mathbf{V}}_1^{(0)}\mathbf{V}_1^{(1)}\ \tilde{\mathbf{V}}_2^{(0)}\mathbf{V}_2^{(1)}\cdots\tilde{\mathbf{V}}_K^{(0)}\mathbf{V}_K^{(1)}\ \mathbf{z}_1\cdots\mathbf{z}_{\mathrm{Nt-K}}][\mathrm{s}_1\cdots\mathrm{s}_{\mathrm{K}}\ \mathrm{t}_1\cdots\mathrm{t}_{\mathrm{Nt-K}}]^{\mathrm{T}},\end{aligned} \tag{9}$$

By substituting (9) into (2) and (3), the signals received by the kth legitimate user and by the eavesdropper can be derived as follows:

$$\mathbf{y}_k=\mathbf{h}_k^H\tilde{\mathbf{V}}_k^{(0)}\mathbf{V}_k^{(1)}s_k+\mathbf{n}_k \tag{10}$$

and

$$\mathbf{y}_e=\mathbf{G}^H\mathbf{W}\mathbf{s}+\mathbf{G}^H\mathbf{Z}\mathbf{t}+\mathbf{n}_e. \tag{11}$$

Note that legitimate user k can easily demodulate s_k using the maximum likelihood (ML) rule.

$$\overline{s_k}=\arg\min_{s_k\in U}\{\|\,s_k-(\mathbf{h}_k^H\tilde{\mathbf{V}}_k^{(0)}\mathbf{V}_k^{(1)})^+\mathbf{y}_k\,\|^2\} \tag{12}$$

where $U=\{U_1,U_2,\cdots,U_m\}$ is the symbol set with a total of m symbols. While for the eavesdropper, recovering the desired signals contaminated by AN is difficult.

3. Existing Wiretapping Methods for Single-user System

In this section, we consider a single-user multi-input single-output (SU-MISO) system, where a transmitter with *Nt* antenna sends a data stream to the only legitimate receiver with single antenna. An *Ne*-antenna eavesdropper attempts to recover the data stream without CSI of the legitimate user.

By denoting the $Nt\times 1$ channel vectors between the transmitter and the only legitimate user by $\mathbf{h}_{AB}$ and the $Nt\times Ne$ channel vectors between the transmitter and the eavesdropper by $\mathbf{G}$, the overall transmitted signal $\mathbf{x}'$ changes in form with (9):

$$\begin{aligned}\mathbf{x}' &= \mathbf{w}s+\mathbf{s}'' = \mathbf{W}\mathbf{S}^{\mathrm{T}}\\ &= [\frac{\mathbf{h}_{AB}}{\|\mathbf{h}_{AB}\|}\ \mathbf{z}_1\cdots\mathbf{z}_{\mathrm{Nt}-1}][s\ \mathrm{t}_1\cdots\mathrm{t}_{\mathrm{Nt}-1}]^{\mathrm{T}},\end{aligned} \tag{13}$$

where s is the information symbol for the legitimate user. Vector $\mathbf{s}''=\mathbf{Z}\mathbf{t}$ is AN signal, $\mathbf{Z}=[\mathbf{z}_1\cdots\mathbf{z}_{\mathrm{Nt}-1}]\in\mathbb{C}^{Nt\times(Nt-1)}$ is an orthogonal basis of the null space of $\mathbf{h}_{AB}$, and $\mathbf{t}=[t_1\cdots t_{\mathrm{Nt}-1}]$ are i.i.d. $\mathcal{CN}(0,1)$ variables.

Thus, the signals received by the legitimate user can be:

$$y_{AB}=\mathbf{h}_{AB}^{H}\mathbf{x}'+\mathbf{n}_{AB}=\mathbf{h}_{AB}^{H}\frac{\mathbf{h}_{AB}}{\|\mathbf{h}_{AB}\|}s+\mathbf{n}_{AB} \tag{14}$$

and by the eavesdropper:

$$\mathbf{y}_e'=\mathbf{G}^{H}\mathbf{x}'+\mathbf{n}_e=\mathbf{G}^{H}\frac{\mathbf{h}_{AB}}{\|\mathbf{h}_{AB}\|}s+\mathbf{G}^{H}\mathbf{s}''+\mathbf{n}_e \tag{15}$$

where $\mathbf{n}_{AB}$ and $\mathbf{n}_e$ are naturally occurring independent and i.i.d. zero-mean additive white Gaussian noise vector with variances σ_k^2 and σ_e^2, respectively.

3.1 MUSIC-like algorithm

Next, we present a brief introduction of the MUSIC-like algorithm and the HC algorithm. Then, we verify that both are invalid for the multiuser system.

For the MUSIC-like algorithm, suppose the block length is L, then the received signal by eavesdropper in one block is:

$$\mathbf{y}_e'=[\mathbf{y}(1),\mathbf{y}(2),\cdots,\mathbf{y}(L)] \tag{16}$$

The eavesdropper aims to estimate the *L* information symbols in the first row of matrix $\mathbf{S}$ as accurate as possible, and not the equivalent channel $\mathbf{G}^{H}\mathbf{W}$. To transpose both sides of (15), we obtain:

$$\mathbf{y}_e'^{H}=\mathbf{x}'^{H}\mathbf{G}+\mathbf{n}_e^{H}=\mathbf{S}\mathbf{W}^{H}\mathbf{G}+\mathbf{n}_e^{H} \tag{17}$$

where $\mathbf{n}_e=[\mathbf{n}_e(1),\mathbf{n}_e(2),\cdots,\mathbf{n}_e(L)]$,

$$\mathbf{S}=\begin{pmatrix}S(1)\\S(2)\\\vdots\\S(L)\end{pmatrix}=\begin{pmatrix}s(1)&t_1(1)&\cdots&t_{\mathrm{Nt}-1}(1)\\s(2)&t_1(2)&\cdots&t_{\mathrm{Nt}-1}(2)\\\vdots&\vdots&\ddots&\vdots\\s(L)&t_1(L)&\cdots&t_{\mathrm{Nt}-1}(L)\end{pmatrix}, \tag{18}$$

Next, the estimation of the first rank of matrix $\mathbf{S}$ is evaluated. Let $\mathbf{b}=[s(1)\ \ s(2)\cdots s(L)]^T$ be the secret message to be estimated by the SVD, $\mathbf{y}_e^H$ is then decomposed as:

$$\mathbf{y}_e'^H=[\mathbf{U}_s\ \ \mathbf{U}_n]\begin{bmatrix}\mathbf{\Sigma}_s & 0\\ 0 & \mathbf{\Sigma}_n\end{bmatrix}[\mathbf{U}_s\ \ \mathbf{U}_n]^H \tag{19}$$

When $Ne\geq Nt$ and $L>Nt$, $\mathbf{U}_s$ is the *Nt* dimensional signal subspace expanded by $\mathbf{S}$ and $\mathbf{U}_n$ is the (*L-Nt*) dimensional noise subspace and orthogonal to the vector $\mathbf{b}$ i.e.,

$$\mathbf{U}_n^H\mathbf{b}=0 \tag{20}$$

Based on (20), the MUSIC-like constructs an objective function $J(\hat{\mathbf{b}})$ to search the maximum

$$J(\hat{\mathbf{b}})=\frac{\hat{\mathbf{b}}^H\hat{\mathbf{b}}}{\hat{\mathbf{b}}^H\mathbf{U}_n\mathbf{U}_n^H\hat{\mathbf{b}}} \tag{21}$$

The optimization procedure is performed by enumerating all the possible combination of the symbol set; when traversing into $\hat{\mathbf{b}}=\mathbf{b}$, the objective function result $J(\hat{\mathbf{b}})$ is the maximum given that its denominator becomes zero. However, for MU-MIMO systems, the signal subspace $\mathbf{U}_s$ is the $Nt\times K$ dimensional, that is, *K* vectors $\mathbf{b}$ satisfy the term (20); when traversing the symbol set, the information symbol for all legitimate users could result in the maximum $J(\hat{\mathbf{b}})$. Moreover, the MUSIC-like algorithm cannot ensure the corresponding legitimate users for the *K* vectors. Thus, it cannot be directly applied to MU-MIMO systems.

3.2 HC algorithm

We present a brief introduction of the HC algorithm. The transmitted vector signals $\mathbf{x}'$ in (13), which is contaminated with AN, are distributed within parallel hyperplanes in unitary signal space, with each hyperplane corresponding to one certain transmitted symbol $U_i, i=1,2,\cdots,m$. The normal vector of these hyperplanes is $\frac{\mathbf{h}_{AB}}{\|\mathbf{h}_{AB}\|}$ and the offset of each hyperplane is the corresponding $U_i, i=1,2,\cdots,m$.

In [11], Liu has proven that this hyperplane signature still holds in $\mathbf{y}_e$ when the eavesdropper has equal or more antennas than the transmitter, which can be used for eavesdropping. Let $\mathbf{w}=\mathbf{G}^+\mathbf{h}_{AB}$ and ignore $\mathbf{n}_e$; by projecting $\mathbf{y}_e'$ into the direction of $\mathbf{w}$, the following can be obtained:

$$\begin{aligned}<\mathbf{y}_e',\mathbf{w}>&\approx\mathbf{w}^H\mathbf{G}^H\mathbf{x}'=\mathbf{h}_{AB}^H(\mathbf{G}\mathbf{G}^H)^{-1}\mathbf{G}\mathbf{G}^H\mathbf{x}'\\&=<\mathbf{x}',\mathbf{h}_{AB}>=U_i\end{aligned} \tag{22}$$

For MU-MIMO systems, let $\mathbf{w}'=\mathbf{G}^+\mathbf{H}$ and ignore $\mathbf{n}_e$; by projecting $\mathbf{y}_e$ into the direction of $\mathbf{w}'$, the following can be obtained:

$$\begin{aligned}<\mathbf{y}_e,\mathbf{w}'>&=\mathbf{w}'^H\mathbf{G}^H\mathbf{x}=\mathbf{H}^H(\mathbf{G}\mathbf{G}^H)^{-1}\mathbf{G}\mathbf{G}^H\mathbf{x}\\&=<\mathbf{x},\mathbf{H}>=\mathbf{u}\end{aligned} \tag{23}$$

where $\mathbf{u}=[u_1,u_2,\cdots,u_K]$ and $u_k \in U$. The received signals $\mathbf{y}_e$ in MU-MIMO systems are clearly at the point of intersection of the *K* hyperplanes, which is different from the received signals $\mathbf{y}'_e$ in SU-MISO systems. The signal space of $\mathbf{y}_e$ has a discrete symmetric pattern. Without the knowledge of $\mathbf{H}$, the eavesdropper cannot distinguish the main direction in the *K* normal vectors. Thus, the HC algorithm is also not available in MU-MIMO systems.

4. Proposed Wiretapping Methods for Multiuser System

Two types of eavesdropper approaches exist: (1) the eavesdropper attempts to decode one of the *K* data information-bearing waveforms he is interested in and (2) the eavesdropper attempts to decode all the *K* information-bearing waveforms. Here, we choose the latter approach. The eavesdropping condition that the antennas at the eavesdropper should be equal or more than the transmitter is necessary. The analyses meet $Ne \geq Nt$ hereinafter.

4.1 With perfect CSI of legitimate users

In this section, we assume that perfect CSI about the legitimate users is available to the eavesdropper. To extract all *K* private symbols $\mathbf{s}$ from the AN-embedded signals, we need to design the received beamformers $\bar{\mathbf{W}}$, which can eliminate the interference term $\mathbf{G}^H\mathbf{Zt}$ in (7). $\mathbf{G}^H$ has a left inverse, denoted by $\mathbf{G}^{\dagger}$, then multiply $\mathbf{y}_e$ by $\bar{\mathbf{W}}=\mathbf{H}^H\mathbf{G}^{+}$, i.e.,

$$\bar{\mathbf{W}}\mathbf{y}_e=\mathbf{H}^H\tilde{\mathbf{V}}_k^{(0)}\mathbf{V}_k^{(1)}\mathbf{s}+\bar{\mathbf{W}}\mathbf{n}_e\approx\mathbf{y}_B \tag{24}$$

where $\mathbf{y}_B=[\mathbf{y}_1,\mathbf{y}_2,\cdots,\mathbf{y}_K]$. The private symbol $\mathbf{s}$ can be decoded by the eavesdropper using the ML detector, as given in (12).

4.2 Without the CSI of legitimate users

The CSI of legitimate users is difficult to obtain by an eavesdropper; hence, we next consider how an eavesdropper implements eavesdropping when CSI of legitimate users is not available. From the aspect of signal processing, wiretapping can be categorized as blind source separation (BSS). The JADE algorithm [15] is an effective method to solve BSS problems. In applying JADE algorithm, the typical requirements are as follows: (1) the source signals should ensure statistical independence; (2) the channel transfer matrix should be full column rank; (3) the number of receiving antennas should be greater than or equal to the number of transmitted antennas; and (4) at most one Gaussian source signal is allowed. For eavesdropping, all prerequisites are satisfied except the fourth one. Several Gaussian signals and a complex-valued communication signal in (11) exist. Because eavesdropping only aims to obtain accurate estimation of that complex-valued $\mathbf{s}$, whose nongaussianity are the most obvious, the idea of JADE can be applied to extract these nongaussianity sources. However, the complex signals are recovered with permutation indetermination and phase ambiguity of JADE because of the independent in-phase and quadrature (I/Q) components. We modify JADE using the constrained scheme in [16] to eliminate permutation indetermination and phase ambiguity.

The signal model can be reformulated from (7) as:

$$\begin{aligned}\mathbf{y}_e &= \mathbf{G}^H\mathbf{W}\mathbf{s} + \mathbf{G}^H\mathbf{Z}\mathbf{t} + \mathbf{n}_e \\ &= \mathbf{A}\mathbf{S} + \mathbf{n}_e\end{aligned} \tag{25}$$

where $\mathbf{A} = \mathbf{G}^H[\mathbf{W}\ \mathbf{Z}]$ is a steering matrix and $\mathbf{S} = [\mathbf{s}\ \mathbf{t}]$ is the overall symbol matrix. The covariance matrix of received signal $\mathbf{y}_e$ can be expressed as:

$$\mathbf{R} = E[\mathbf{y}_e\mathbf{y}_e^{\mathbf{H}}] = \mathbf{A}\mathbf{A}^{\mathbf{H}} + \sigma_e^2\mathbf{I} \tag{26}$$

The eigenvalue decomposition of $\mathbf{R}$ yields:

$$\begin{aligned}\mathbf{R} &= V_y\Lambda_y V_y^H = [V_s, V_n]\begin{bmatrix}\Lambda_s & 0\\ 0 & \Lambda_n\end{bmatrix}[V_s, V_n]^H \\ &= V_s\Lambda_s V_s^H + V_n\Lambda_n V_n^H\end{aligned} \tag{27}$$

where $V_s \in \mathbb{C}^{Ne\times K}$ and $V_n \in \mathbb{C}^{Ne\times(Ne-K)}$ are the eigenvectors of $\Lambda_s = diag\{\lambda_1 \ge \lambda_2 \cdots \ge \lambda_K\}$ and $\Lambda_n = diag\{\lambda_{K+1} \ge \lambda_{K+2} \cdots \ge \lambda_{Ne}\}$, which are diagonal matrices with K and Ne-K eigenvalues in descending order, respectively.

Note that the number of signal sources K is unknown for the eavesdropper; hence, we propose to estimate K by MDL algorithm [17]. The objective function is:

$$MDL(k) = -\ln[(\prod_{i=k+1}^{Ne}\lambda_i^{\frac{1}{Ne-k}})\Big/(\frac{1}{Ne-k}\sum_{i=k+1}^{Ne}\lambda_i)]^{(Ne-k)N} + \frac{k}{2}(2Ne-k)\ln N \tag{28}$$

where N is the sample number. When k increases from 0 to $Ne-1$, the estimated number of signal sources $\hat{K}$ is the integer that minimizes $MDL(k)$, i.e.,

$$\hat{K} = \min\{MDL(k), k = 0,1,2,\cdots,Ne-1\} \tag{29}$$

The estimated variance of noise $\hat{\sigma}_e^2$ can be calculated from the mean value of the Ne-K eigenvalues. The whitening matrix $\mathbf{V}$ is given by:

$$\begin{aligned}\mathbf{V} &= \hat{\Lambda}_s^{-1/2}V_s^H = (\Lambda_s - \hat{\sigma}_e^2 I)^{-1/2}V_s^H \\ &= diag\{\frac{1}{\sqrt{(\lambda_1 - \hat{\sigma}_e^2)}},\cdots,\frac{1}{\sqrt{(\lambda_K - \hat{\sigma}_e^2)}}\}V_s^H\end{aligned} \tag{30}$$

Then, the whitening signal is written as:

$$\hat{\mathbf{y}}_e = \mathbf{V}\mathbf{y}_e \tag{31}$$

To avoid I/Q-associated problems, we turn the Ne complex whitening signals $\hat{\mathbf{y}}_e$ into the mixtures of $2Ne$ real signals $\overline{\mathbf{y}}_e$, which are I/Q components of the signals i.e.,

$$\overline{\mathbf{y}}_e = \begin{bmatrix}\hat{y}_{1i}\\ \hat{y}_{1q}\\ \vdots\\ \hat{y}_{Nei}\\ \hat{y}_{Neq}\end{bmatrix} = \begin{bmatrix}g_{11i} & -g_{11q} & \cdots & g_{1Nei} & -g_{1Neq}\\ g_{11q} & -g_{11i} & \cdots & g_{1Neq} & -g_{1Nei}\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ g_{Ne1i} & -g_{Ne1q} & \cdots & g_{NeNei} & -g_{NeNeq}\\ g_{Ne1q} & -g_{Ne1i} & \cdots & g_{NeNeq} & -g_{NeNei}\end{bmatrix}\begin{bmatrix}y_{1i}\\ y_{1q}\\ \vdots\\ y_{Nei}\\ y_{Neq}\end{bmatrix} \tag{32}$$

The fourth-order cumulant matrix of the modified whitening signals are used in the eigenvalue decomposition in the following form:

$$\begin{aligned}\mathbf{C}_{\bar{y}} &= \frac{1}{Ne}\sum_{n=1}^{Ne}[\bar{\mathbf{y}}_e{}^T\bar{\mathbf{y}}_e\bar{\mathbf{y}}_e\bar{\mathbf{y}}_e{}^T] - 2\hat{R}_{\bar{y}}(0)\hat{R}_{\bar{y}}(0) - tr(\hat{R}_{\bar{y}}(0))\hat{R}_{\bar{y}}(0) \\ &= \hat{\mathbf{U}}\Lambda_C\hat{\mathbf{U}}^H\end{aligned} \tag{33}$$

where $\hat{R}_{\bar{y}}(0)=\frac{1}{Ne}\sum_{n=1}^{Ne}[\bar{\mathbf{y}}_e\bar{\mathbf{y}}_e^T]$ and the unitary matrix $\hat{\mathbf{U}}^H$ is the separation matrix. In this paper, only K complex signals must be recovered; thus, the separation matrix $\hat{\mathbf{U}}_S^H$ is the first $2K$ rows of $\hat{\mathbf{U}}^H$, i.e.,

$$\hat{\mathbf{U}}_S^H = \begin{bmatrix} u_{11} & u_{12} & \cdots & u_{1,2Ne-1} & u_{1,2Ne} \\ u_{11} & u_{12} & \cdots & u_{1,2Ne-1} & u_{1,2Ne} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ u_{2K-1,1} & u_{2K-1,2} & \cdots & u_{2K-1,2Ne-1} & u_{2K-1,2Ne} \\ u_{2K,1} & u_{2K,2} & \cdots & u_{2K,2Ne-1} & u_{2K,2Ne} \end{bmatrix} \tag{34}$$

To keep the structure of (15), we impose a constraint on $\hat{\mathbf{U}}_S^H$. The separation matrix $\hat{\mathbf{U}}_S^H$ is modified as:

Table 1. OUR PROPOSED MODIFIED JADE ALGORITHM FOR EAVESDROPPING

Step 1: Estimate the number of legitimate users (1) Calculate the covariance matrix $\mathbf{R}$ of received signal $\mathbf{y}_e$ using (26). (2) Get the eigenvalue of $\mathbf{R}$ using (27). (3) Use the eigenvalue to estimate the number of legitimate users K using (28).
Step 2: Get the whitening signal Perform whitening over the received signal by using (31) and obtain a whitening signal $\hat{\mathbf{y}}_e$.
Step 3: Estimate the separation matrix (1) Form a new vector $\bar{\mathbf{y}}_e$ containing $2Ne$ real components from the real and imaginary parts of all $\hat{\mathbf{y}}_e$ using (32). (2) The fourth-order cumulant matrix in eigenvalue decomposition yields the unitary matrix $\hat{\mathbf{U}}^H$ using (33). (3) Take the first $2K$ rows of $\hat{\mathbf{U}}^H$ and impose a constraint on them using (35). (4) Get the final separation matrix $\hat{\mathbf{U}}_S^H$ and estimate desired signal $\hat{\mathbf{s}}_{real}$ containing $2K$ real components using (36).
Step 4: Estimate the secret data (1) Reform the real form signals $\hat{\mathbf{s}}_{real}$ into complex form as $\hat{\mathbf{s}}=[\hat{s}(1,:)+\mathrm{j}\hat{s}(2,:),\cdots,\hat{s}(2K-1,:)+\mathrm{j}\hat{s}(2K,:)]$, where $\hat{s}(k,:)$ is the kth row of $\hat{\mathbf{s}}$. (2) Decode the secret symbols by maximum likelihood detector using (37).

$$\hat{\mathbf{U}}_S^H = \begin{bmatrix} \frac{u_{11}+u_{22}}{2} & -\frac{u_{21}-u_{12}}{2} & \cdots & \frac{u_{1,2Ne-1}+u_{2,2Ne}}{2} & -\frac{u_{2,2Ne-1}-u_{1,2Ne}}{2} \\ \frac{u_{21}-u_{12}}{2} & \frac{u_{11}+u_{22}}{2} & \cdots & \frac{u_{2,2Ne-1}-u_{1,2Ne}}{2} & \frac{u_{1,2Ne-1}+u_{2,2Ne}}{2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \frac{u_{2K-1,1}+u_{2Ne,2}}{2} & -\frac{u_{2K,1}-u_{2Ne-1,2}}{2} & \cdots & \frac{u_{2K-1,2Ne-1}+u_{2K,2Ne}}{2} & -\frac{u_{2K,2Ne-1}-u_{2K-1,2Ne}}{2} \\ \frac{u_{2K,1}-u_{2Ne-1,2}}{2} & \frac{u_{2K-1,1}+u_{2Ne,2}}{2} & \cdots & \frac{u_{2K,2Ne-1}-u_{2K-1,2Ne}}{2} & \frac{u_{2K-1,2Ne-1}+u_{2K,2Ne}}{2} \end{bmatrix} \tag{35}$$

The 2 K real signals can be estimated in the following form:

$$\hat{\mathbf{s}}_{real} = \hat{\mathbf{U}}_S^H \overline{\mathbf{y}}_e \tag{36}$$

Then, the complex form of the desired signals are $[\hat{s}(1,:) + \mathrm{j}\hat{s}(2,:), \cdots, \hat{s}(2K-1,:) + \mathrm{j}\hat{s}(2K,:)]$, where $\hat{s}(k,:)$, $k = 1, 2, \cdots, 2K-1, 2K$ is the kth row of $\hat{\mathbf{s}}_{real}$. Finally, the secret message could be decoded using the ML detector as:

$$s_k' = \arg\min_{s_k \in U} \{\| s_k - \hat{s} \|^2\} \tag{37}$$

The eavesdropping procedure can be implemented with the steps in Table 1. Note that when the CSI of the transmitter is imperfect, the beamforming matrix and the AN designed based on the imperfect CSI may change. However, their changes also meet the prerequisites of JADE. While the expected signal sources will remain the same, the modified JADE can still work for eavesdropping.

5. Simulation Results and Analysis

In the following, we assess the proposed wiretapping method from computer simulations. $\mathbf{H}$ and $\mathbf{G}$ are modeled as Rayleigh block fading channels. We consider four cases: (1) $Nt = 5$ and 2 legitimate users equipped with $Nr = 2$ antennas each; (2) $Nt = 7$ and 3 legitimate users equipped with $Nr = 2$ antennas each. Both of them transmit BPSK signals; (3) the transmitter knows perfect CSI of the legitimate users; and (4) the transmitter knows imperfect CSI of the legitimate users. The received noise of each antenna is i.i.d. zero-mean additive white Gaussian noise with unit variances. The signal-to-noise ratio (SNR) and signal-to-interference ratio (SIR) are defined as the ratio between the power of information signal and the power of noise and the ratio between the power of information signal and the power of AN, respectively. We call the proposed method with perfect CSI of the legitimate user Method 1 and the proposed method without CSI of the legitimate user Method 2 for convenience.

First, **Fig. 1** shows the influence of data block length N to the bit error rate (BER) performance using Method 2 in case 2. Method 2 uses JADE algorithm, in which the sample number should be large; however, a larger N will allow more computational capability to run. In **Fig. 1**, when N increases to 300, BER no longer reduces. Hence, we take $N = 300$ in the following simulations.

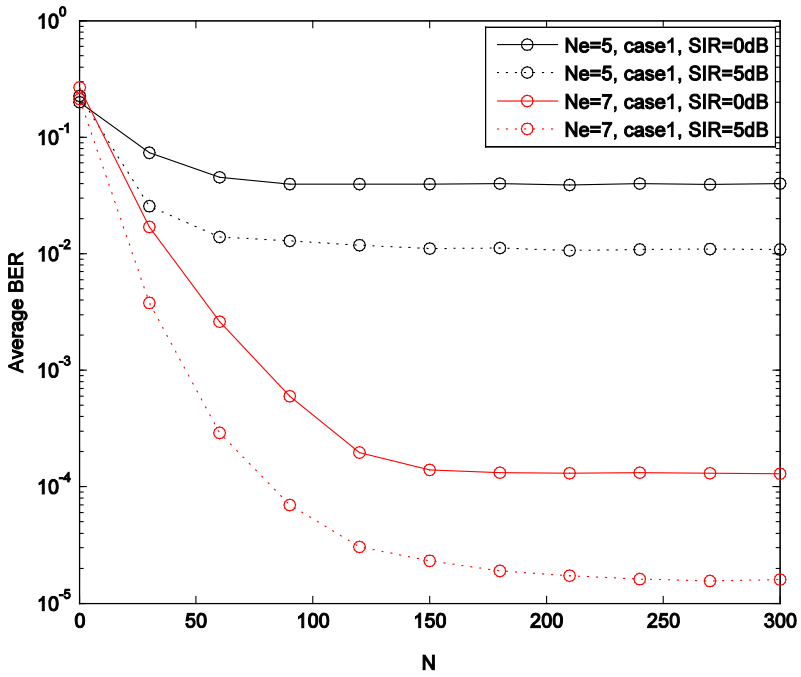

Fig. 1. BER performance as signal samples increases (SNR=10dB)

Next, we evaluate the average BER performance of the eavesdropper as the SNR increases from 0 dB to 20 dB with a fixed SIR = 0 dB using Methods 1 and 2 in **Fig. 2**. Following are the observations. (1) The larger the number of eavesdropper antennas, the smaller the differences of BER performance between Methods 1 and 2. (2) The number of legitimate users has little effect on the average BER because the separation results of the JADE algorithm are not sensitive to the number of source signals. (3) Both proposed methods with $Ne > Nt$ can obtain BER improvements with $Ne = Nt$. Moreover, the more antennas the eavesdropper is equipped with, the better the average BER. (4) Method 2 in cases 3 and 4 almost obtains the same BER, which verifies whether the CSI at the transmitter is perfect and will not affect eavesdropping.

In **Fig. 3**, we evaluate the performance of the proposed methods as the SIR increases from –10 dB to 10 dB with a fixed SNR = 2 dB. We can observe that the BERs of Method 1 are always constant because Method 1 completely eliminates AN and its BER is no longer under SIR influence. The BERs of Method 2 reduce with increasing SIR, which indicates that Method 2 has robustness to AN. When SIR increases to a critical value, the BERs of Method 2 are even lower than the BERs of the proposed method with CSI because Method 1 eliminates AN while increasing channel noise. The BER performance of Method 2 in cases 3 and case 4 are almost the same, which suggests that the different signal forms of AN in cases 3 and case 4 would not affect the BER of Method 2; however, the power of AN would affect the BER.

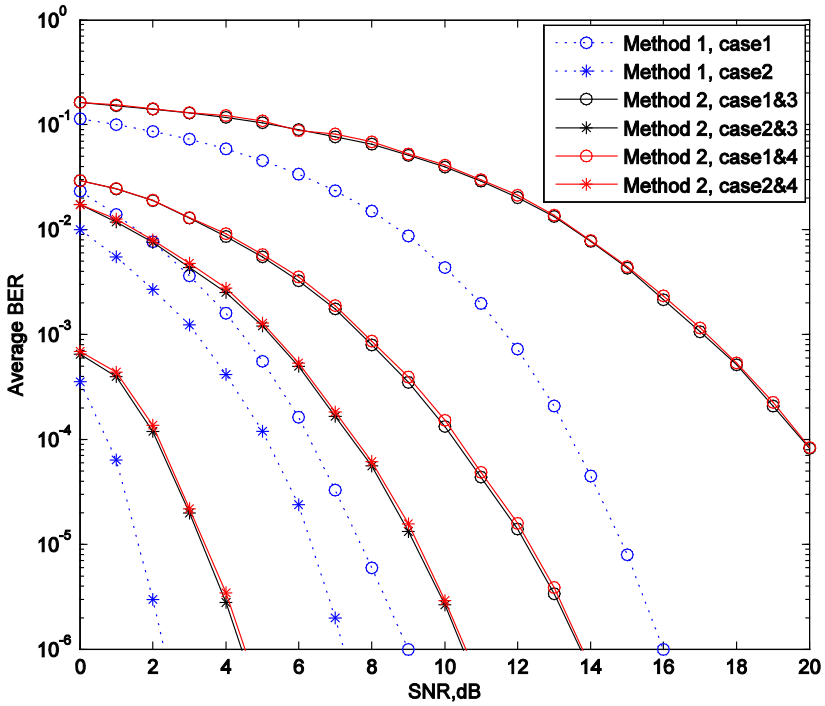

Fig. 2. BER performance as SNR increases (SIR=0dB).

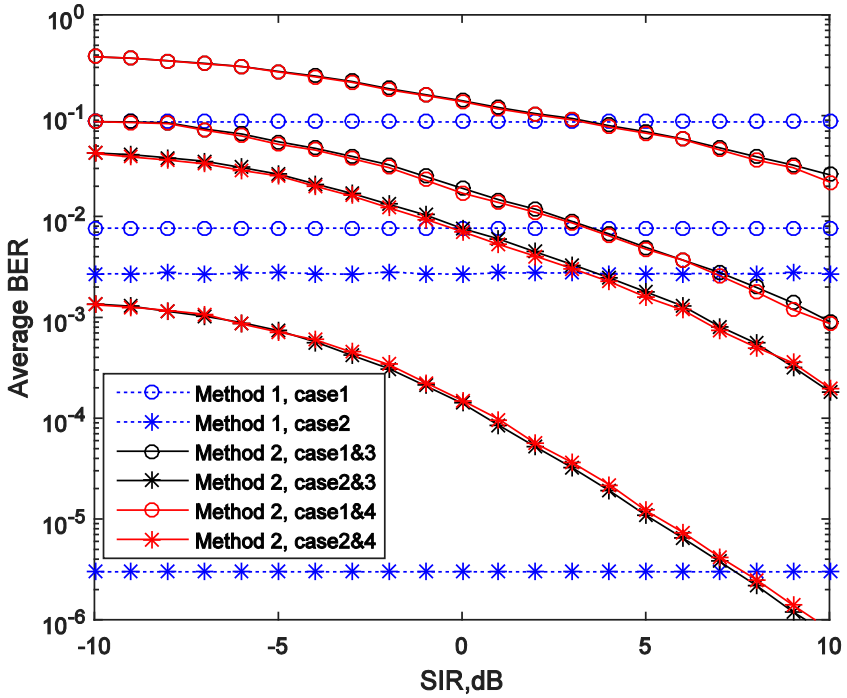

Fig. 3. BER performance as SIR increases (SNR=2dB).

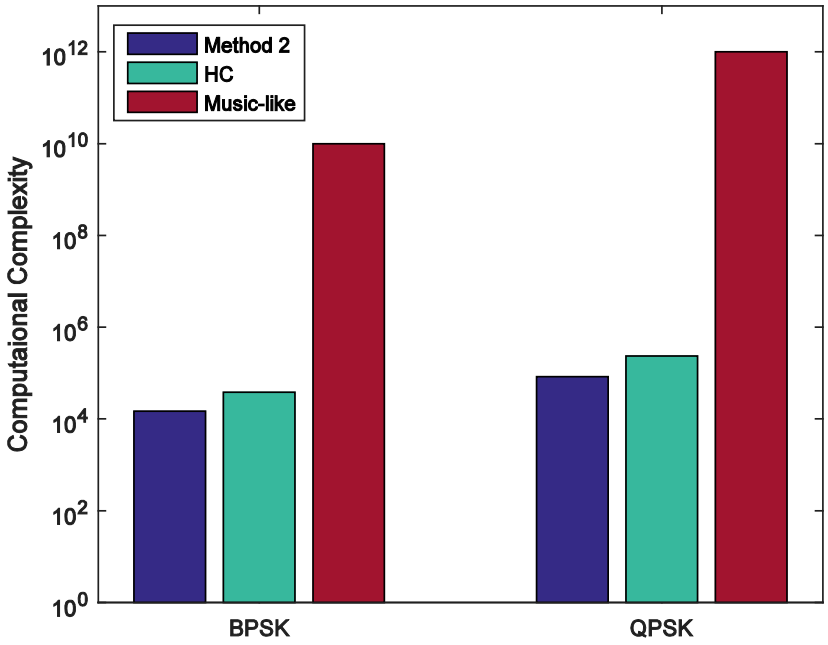

Fig. 4. Computational complexity

Finally, we compare the computational complexity of MUSIC-like, HC, and Method 2 considering that all of them are blind identification. For Method 2, the numbers of computational complexity for covariance matrix $\mathbf{R}$ are proportional to $2Ne^2N$. The eigen decomposition for an $Ne \times Ne$ matrix is proportional to $O(Ne^3)$. The approximate joint diagonalization for fourth-order cumulant matrix (two $Nt \times Nt$ matrices) is proportional to $2O(Nt^3)$. The total computational complexities of our proposed method is $2Ne^2N + O(Ne^3) + 2O(Nt^3)$. While MUSIC-like [10] requires the size of symbol set m; thus, the permutation and combination for a symbol with data block length $\hat{N}$ is $m^{\hat{N}}$. The total computational complexities for MUSIC-like is $O(\hat{N}^3 m^{\hat{N}})$. For HC, the computational complexity is proportional to $O(mNNe)$ [11]. The comparison results are plotted in **Fig. 4** with $Ne = Nt = 5$, $N = 250$, $\hat{N} = 9$, and $m = 2$ *or* 4. The computational complexity of our proposed method is shown to be 6–7 orders of magnitude less than that of MUSIC-like algorithm and slightly less than that of HC.

5. Conclusion

We focused on the conflicting AN strategy and proposed wiretapping methods for AN-assisted MU-MIMO system with and without CSI of legitimate users. The eavesdropper can successfully recover secret messages from signals contaminated with AN using both proposed methods. Simulations show that if the eavesdropper has more antennas than that of the transmitter, both proposed algorithms can intercept information effectively. Moreover, our wiretapping method without CSI of legitimate users performs well in terms of both robustness and computational complexity.

References

[1] X. Chen and R. Yin, "Performance analysis for physical layer security in multi-antenna downlink networks with limited CSI feedback," *IEEE Wireless Commun. Lett.*, vol. 2, no. 5, pp. 503–506, October. 2013. Article (CrossRef Link).

[2] N. Li, X. Tao, and J. Xu, "Artificial Noise Assisted Communication in the Multiuser Downlink: Optimal Power Allocation," *IEEE Commun. Lett.*, vol. 19, no. 2, pp. 295–298, February. 2015. Article (CrossRef Link).

[3] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, and T. Q. Duong, "Relay selection for security enhancement in cognitive relay networks," *IEEE Commun. Lett.*, vol. 4, no. 1, pp. 46–49, February. 2015. Article (CrossRef Link).

[4] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journ*al, vol. 54, no.8, pp. 1355-1387, August. 1975. Article (CrossRef Link).

[5] S. Goel, R. Negi, "Guaranteeing Secrecy Using Artificial Noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, June. 2008. Article (CrossRef Link).

[6] T. Shang-Ho, H. Vincent, "Power Allocation for Artificial-Noise Secure MIMO Precoding Systems," *IEEE Transactions on. Signal Processing*, vol. 62, no.13, pp. 3479-3492, July. 2014. Article (CrossRef Link).

[7] Q. Li, W. Ma, and S. Anthony, "A Safe Approximation Approach to Secrecy Outage Design for MIMO Wiretap Channels," *IEEE Signal Processing Letters*, vol. 21, no.1, pp. 118–121, January. 2014. Article (CrossRef Link).

[8] A. Mukherjee and A. L. Swindlehurst, "Utility of beamforming strategies for secrecy in multiuser MIMO wiretap channels," in *Proc. of 2009 Allerton Conf. Commun., Control, Comput.*, pp. 1134–1141. September. 30-October. 2, 2009. Article (CrossRef Link).

[9] M. Pei, J. Wei, K. Wong, and X. Wang, "Masked Beamforming for Multiuser MIMO Wiretap Channels with Imperfect CSI," *IEEE Trans. Wireless Commun.*, vol. 11, no.2, pp. 544-549, February. 2012. Article (CrossRef Link).

[10] N. Li, X. Tao, H. Wu, J. Xu and Q. Cui "Large System Analysis of Artificial Noise Assisted Communication in the Multiuser Downlink: Ergodic Secrecy Sum-rate and Optimal Power Allocation," *IEEE Vehicular Technology Society*, to appear. Article (CrossRef Link).

[11] F. Wu, W. Wang, B. Yao and Q.Y. Yin, "Effective eavesdropping in the Artificial noise aided security scheme," in *Proc. of 2013 IEEE/CIC International Conference on Communications in China (ICCC)*, pp. 214 - 218, August.12-14, 2013. Article (CrossRef Link).

[12] L. Lu, L. Jin, and K. Huang, "Eavesdropping Against Artificial Noise: Hyperplane Clustering," in *Proc. of IEEE International Conference on Information Science and Technology*, pp. 1571–1575, March. 23-25, 2013. Article (CrossRef Link).

[13] S. Liu, Y. Hong, and E. Viterbo, "Artificial Noise Revisited: When Eve Has more Antennas than Alice," in *Proc. of IEEE Int. Conf. Signal Process. Commun. (SPCOM)*, pp. 1-5, July.22-25, 2014. Article (CrossRef Link).

[14] Q. H. Spencer, A. L. Swindlehurst, and M. Haardt., "Zero forcing methods for downlink spatial multiplexing in multiuser MIMO channels," *IEEE Trans. Signal Process.*, vol. 52, no.2,.pp.461-471, February. 2004. Article (CrossRef Link).

[15] D. T. Pham and J. Cardoso., "Blind separation of instantaneous mixtures of nonstationary sources," *IEEE Trans. Signal Process.*, vol. 49, no.9, pp.1837-1848, September. 2001. Article (CrossRef Link).

[16] F. Gu, Z. Hang, and Y. Xiao, "Multichannel blind deconvolution of complex I/Q independent sources with phase recovery," in *Proc. of International Conference on Wireless Communications and Signal Processing (WCSP)*, pp.1-6, October 24-26,2013. Article (CrossRef Link).

[17] J. Rissanen, F. R. Hill; R. L. Pickholtz "Estimating the number of signals using the eigenvalues of the correlation matrix," in *Proc. of Military Communications Conference 1989 (MILCOM '89). Conference Record. Bridging the Gap. Interoperability, Survivability, Security*, pp. 353-358, October 15-18, 1989. Article (CrossRef Link).

Shu Wang was born in 1987. She received her M.S. degrees in circuits and system from Air Force Engineering University in 2010. She is now studying in Air Force Engineering University to reach his Ph. D degree of electronic science and technology. Her research interests are physical layer security and communication signal processing. E-mail: xss_wang@163.com

Xinyu Da was born in 1961. He received his Ph.D. degree in communication and information system from Northwestern polytechnical university, in 2008. He is currently a professor in Institute of Information and Navigation, AFEU. He has been engaged in teaching and researching on wireless communication and communication signal processing. E-mail: daxinyu_dy@163.com

Zhenyong Chu was born in 1972. He received his Ph.D. degrees in communication and information system from Xidian University in 2005. He is currently an associate professor and working in Institute of of Information and Navigation, AFEU. His research interests are wireless communication and communication signal processing. E-mail:zane_chu@163.com