Proactive Jamming Towards Interference Alignment Networks: Beneficial and Adversarial Aspects

Jing Guo, *Student Member, IEEE,* Nan Zhao, *Senior Member, IEEE,* Zhutian Yang, *Member, IEEE,* F. Richard Yu, *Senior Member, IEEE,* Yunfei Chen, *Senior Member, IEEE* and Victor C.M. Leung, *Fellow, IEEE*

***Abstract*—Interference alignment (IA) is a prospective method to achieve interference management in wireless networks. On the other hand, jamming can be deemed either as a potential threat to degrade the performance of wireless networks, or as a helper to combat the eavesdropping for the legitimate networks. In this paper, we consider these two opposite scenarios, beneficial and adversarial jamming, towards IA networks, and based on which two proactive jamming schemes are proposed. In the first scheme, the jammer utilizes its precoding vector to constrain the jamming signal into the same subspace as the interference at each IA receiver, which will disrupt the potential eavesdropping significantly without affecting the transmission of IA users. Specifically, secure transmission can be guaranteed through the jamming without any additional cooperation with the IA users. In the second scheme, the jammer utilizes its precoding vector to project the jamming signal into the same subspace as that of the desired signal at each IA receiver secretly. Thus, the IA users cannot detect the concealed jamming signal, which will result in the performance degradation of the IA network. Extensive simulation results are presented to show the effectiveness of the two proposed jamming schemes towards IA networks.**

***Index Terms*—Eavesdropping, interference alignment, physical layer security, proactive jamming.**

I. Introduction

Due to the broadcast nature, interference is always an important factor that impacts the performances of wireless networks. Thus, interference management becomes increasingly important in wireless communications [2]–[6]. Interference alignment (IA) is a prospective method to achieve interference management in multi-user networks, through which the interference among users can be projected into the lower-dimensional subspaces by precoding matrices, and then the desired signal can be retrieved by decoding matrices with no residual interference [7]–[9]. In the past decade, IA has attracted significant attention from academia, industry and government, and several challenging problems have been presented and solved accordingly [7], [10]–[17]. In [7], Cadambe and Jafar analyzed the degrees of freedom (DoFs) and the sum rate of a K-user IA network, and showed that it is difficult to obtain the closed-form solutions of IA when the number of users becomes larger. Whereafter, two iterative algorithms were proposed by Gomadam *et al*. to solve this intractable problem of IA, i.e., MinIL and Max-SINR algorithms [10]. The feasibility conditions of IA have been studied in [11], which determine the relationship between the number of users, antennas and DoFs. The signal-to-interference-plus-noise ratio (SINR) of the received signal may decrease severely in some cases, which will affect the quality of service (QoS) of IA networks [10]. In our previous works, we have also focused on this aspect [12]–[14]. In addition, global channel state information (CSI) of the entire IA network should be available at each transceiver, which is also a critical requirement to achieve [15]–[19].

On the other hand, the security of information transmission is a challenging issue in wireless applications [20], when wireless networks are often used for transmission of private information, such as credit card transaction or banking related data communication. Different from the traditional network security aspect, physical layer security has attracted great attention in recent research, through which the security of wireless transmission can be guaranteed through physical-layer techniques. Eavesdropping and jamming are two main attacks at the physical layer, which aim at intercepting confidential information and disrupting the information transmission of legitimate networks, respectively [21]–[31]. In [32], [33], excellent works has been done by Darsena *et al.* on resisting narrowband interference for multicarrier systems. Some fundamental research work on the physical layer security of IA networks has been done in [34]. When jamming is considered, the jamming signal can be utilized not only to degrade the transmission performance of wireless networks, but also to help the legitimate networks to disrupt the potential eavesdropping. Thus, in this paper, we consider these two opposite scenarios, i.e., the beneficial and adversarial jamming

Manuscript received May 10, 2017; revised September 10, 2017; accepted October 31, 2017. This research was supported in part by the open research fund of National Mobile Communications Research Laboratory, Southeast University (No. 2018D03), the Xinghai Scholars Program, the National Natural Science Foundation of China (NSFC) under Grant 61771089 and 61671101, and the Fundamental Research Funds for the Central Universities under DUT17JC43. Part of this work has been published in preliminary form in the Proceedings of 2017 9th International Conference on Wireless Communications & Signal Processing (WCSP) [1]. *(Corresponding author: Nan Zhao.)*

J. Guo and N. Zhao are with the School of Info. and Commun. Eng., Dalian University of Technology, Dalian 116024 China, and also with National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China (email: guojing94@mail.dlut.edu.cn, zhaonan@dlut.edu.cn).

Z. Yang is with the School of Electronics and Information Engineering, Harbin Institute of Technology, Harbin 150001 China (e-mail: yangzhutian@hit.edu.cn).

F.R. Yu are with the Department of Systems and Computer Engineering, Carleton University, Ottawa, ON K1S 5B6, Canada (email: richard.yu@carleton.ca).

Y. Chen is with the School of Engineering, University of Warwick, Coventry CV4 7AL, U.K. (e-mail: Yunfei.Chen@warwick.ac.uk).

V.C.M. Leung is with the Depart. of Electrical and Computer Eng., the University of British Columbia, Vancouver BC V6T 1Z4, Canada (email: vleung@ece.ubc.ca).

signals, towards IA networks as follows.

First, jamming can be beneficial for IA networks. When some potential eavesdropper exists, it is important to ensure that the confidential information will not be intercepted by the eavesdropper. There are several methods to prevent the eavesdropping, and a reliable one is to generate artificial noise (AN), also called friendly jamming, to combat the eavesdropping [21]–[24]. However, the major challenge of utilizing jamming to guarantee the security is that while destroying the eavesdropping, the transmission of legitimate users will also be affected. To solve this problem, IA can be leveraged due to its capability in interference management, and some initial research works have been done to utilize jamming to guarantee the security of IA networks [35]–[37]. In [35], [36], a generalized interference alignment (GIA) technique was proposed by Ruan *et al*. to generate strong jamming signal at the eavesdropper with the help of IA users to enhance the secrecy rate. In [37], AN was generated along with the transmitted signal of IA users to prevent eavesdropping. Nevertheless, additional overload will be imposed on the legitimate IA network by these methods, in addition to the high requirement of CSI and solutions of IA. Thus, in this paper, from the perspective of jammer, we design the precoding jamming vector to proactively align the jamming into the same subspace as that of the interference at each legitimate receiver without additional cooperation of the IA users, so that the IA users can eliminate the interference and jamming at the same time only by using the original decoding matrices.

Moreover, the jamming signal can also be adversarial for IA networks. Recently, criminals and terrorists can easily establish infrastructure-free wireless communications to commit crimes or terror attacks, and IA is an effective way to construct such an illegal multi-user network. In [38], [39], the information surveillance was performed to control the suspicious transmission by proactive eavesdropping methods, in which legitimate monitor overhears the suspicious transmitter and concurrently forwards a spoofing signal to the suspicious receiver to degrade its transmission. However, when the anti-jamming IA scheme is leveraged [28], [29], the illegal IA network can eliminate the jamming signal and guarantee its transmission. Thus, how to design the proactive jamming signal to disrupt the IA network without its noticing is the key issue for the surveillance of illegal IA networks. In this paper, an appropriate method is proposed to proactively align the jamming signal into the same subspace as that of the desired signal at each IA receiver, so that the IA users cannot perceive the existence of jamming signal.

Considering the beneficial and adversarial aspects of proactive jamming for IA networks, the main contributions of this paper are summarized as follows.

- With regard to the physical layer security, the jamming signal can be either beneficial or adversarial towards IA networks. Thus, in this paper, two proactive jamming schemes are proposed towards IA networks from a novel point of view, to guarantee the secure transmission or to disrupt the transmission, respectively.
- When a potential eavesdropper may exist, we fully utilize the beneficial aspect of the jamming signal as spurious data to disrupt the eavesdropping. To further ensure that the IA transmission is not affected by the jamming signal, the precoding vector of the jammer is designed to proactively constrain the jamming into the same subspace as that of the interference at each IA receiver, without cooperation of the IA network.
- On the other hand, when the adversarial aspect of jamming is considered towards IA networks, the IA transmission can be degraded by the jamming signal without being noticed. To achieve this goal, the precoding vector of the jammer is designed to proactively align the jamming signal into the same subspace as the desired signal at each IA receiver, and thus the IA network cannot perceive the jamming.

The rest of this paper is organized as follows. In Section II, the system model is presented. The beneficial jamming scheme towards IA networks is proposed in Section III, and the eavesdropping performance is analyzed. In Section IV, the adversarial jamming scheme towards IA networks is proposed. In Section V, simulation results are presented and discussed, followed by the conclusions and future work in Section VI.

Notation: $\mathbf{I}_d$ represents the $d \times d$ identity matrix. $\mathbf{A}^\dagger$ is the Hermitian transpose of matrix $\mathbf{A}$. $\|\cdot\|$ is the Euclidean norm of a complex vector. $\mathcal{CN}(\mathbf{a}, \mathbf{A})$ denotes a circularly symmetric complex Gaussian distribution with mean $\mathbf{a}$ and covariance matrix $\mathbf{A}$. $\mathbf{a} \wedge \mathbf{b}$ denotes the cross product of $\mathbf{a}$ and $\mathbf{b}$. $\mathbb{E}(\cdot)$ stands for expectation.

II. System Model

We consider a K-user IA network, where a potential eavesdropper with N_e antennas is intended to wiretap the confidential information from IA links. A jammer with N_j independent antennas also exists to transmit spurious data to degrade the transmission of IA network or to disrupt the eavesdropping. $M^{[k]}$ and $N^{[k]}$ antennas are equipped at the kth transmitter and the kth receiver of the IA network, respectively. Based on these assumptions, the recovered signal at the kth IA receiver can be expressed as

$$\mathbf{y}^{[k]} = \mathbf{U}^{[k]\dagger}\mathbf{H}^{[kk]}\mathbf{V}^{[k]}\mathbf{x}^{[k]} + \sum_{i=1, i\neq k}^{K} \mathbf{U}^{[k]\dagger}\mathbf{H}^{[ki]}\mathbf{V}^{[i]}\mathbf{x}^{[i]} + \mathbf{U}^{[k]\dagger}\mathbf{H}_j^{[k]}\mathbf{w}x_j + \mathbf{U}^{[k]\dagger}\mathbf{n}^{[k]}, \quad (1)$$

where $\mathbf{H}^{[ki]} \in \mathbb{C}^{N^{[k]} \times M^{[i]}}$ is the channel coefficient matrix from the ith IA transmitter to the kth IA receiver[1], whose elements are independent and identically distributed (i.i.d.) and follow $\mathcal{CN}(0, 1)$. $\mathbf{H}_j^{[k]} \in \mathbb{C}^{N^{[k]} \times N_j}$ is the channel coefficient matrix between the jammer and the kth IA receiver. $\mathbf{w} \in \mathbb{C}^{N_j \times 1}$ is the precoding vector of the jammer. x_j denotes the jamming signal generated by the jammer, with its transmit power set to P_j. $d^{[k]}$ is the number of data streams transmitted by the kth IA user. $\mathbf{x}^{[k]} \in \mathbb{C}^{d^{[k]} \times 1}$ is the signal emitted by the kth IA user, whose transmit power equals to $\mathbb{E}\left[\left\|\mathbf{x}^{[k]}\right\|^2\right] = P^{[k]}$. $\mathbf{V}^{[k]} \in \mathbb{C}^{M^{[k]} \times d^{[k]}}$ and $\mathbf{U}^{[k]} \in \mathbb{C}^{N^{[k]} \times d^{[k]}}$

[1]In this paper, perfect CSI is assumed at each legitimate node. Methods in [15]–[17] can be used to evaluate imperfect CSI in our proposed schemes.

TABLE I
EXISTING ANTI-EAVESDROPPING SCHEMES FOR IA NETWORKS

Reference	Method	Superiority	Drawback
[35], [36]	LJs are cooperated with the IA network.	Transmit power of the jammer is not limited.	(1) Jamming and AN are designed with the help of IA. (2) More antennas are needed than the original IA network.
[37]	AN is generated along with the transmitted signal.	No additional transmitters are needed to perform jamming; fewer antennas are needed than [35], [36].	

are the precoding and decoding matrices of the kth IA transmitter and receiver, respectively, satisfying $\mathbf{V}^{[k]\dagger}\mathbf{V}^{[k]} = \mathbf{I}_{d^{[k]}}$ and $\mathbf{U}^{[k]\dagger}\mathbf{U}^{[k]} = \mathbf{I}_{d^{[k]}}$. $\mathbf{n}^{[k]} \in \mathbb{C}^{N^{[k]}\times 1}$ is the additive white Gaussian noise (AWGN) at the kth IA receiver, which follows the distribution $\mathcal{CN}(0, \sigma_n^2\mathbf{I}_{N^{[k]}})$.

When the interference among IA transceivers can be effectively eliminated, the precoding matrices and the decoding matrices should satisfy the following conditions.

$$\text{rank}\left(\mathbf{U}^{[k]\dagger}\mathbf{H}^{[kk]}\mathbf{V}^{[k]}\right) = d^{[k]}, \tag{2}$$

$$\mathbf{U}^{[k]\dagger}\mathbf{H}^{[ki]}\mathbf{V}^{[i]} = 0,\ \forall i \neq k. \tag{3}$$

Consequently, the expression of the recovered signal at the kth IA receiver in (1) can be rewritten as

$$\mathbf{y}^{[k]} = \mathbf{U}^{[k]\dagger}\mathbf{H}^{[kk]}\mathbf{V}^{[k]}\mathbf{x}^{[k]} + \mathbf{U}^{[k]\dagger}\mathbf{H}_j^{[k]}\mathbf{w}x_j + \mathbf{U}^{[k]\dagger}\mathbf{n}^{[k]}. \tag{4}$$

Due to the existence of the jamming signal, the transmission rate of the kth IA user can be denoted as

$$R^{[k]} = \log_2\left|\mathbf{I}_{d^{[k]}} + \frac{\frac{P^{[k]}}{d^{[k]}}\mathbf{U}^{[k]\dagger}\mathbf{H}^{[kk]}\mathbf{V}^{[k]}\mathbf{V}^{[k]\dagger}\mathbf{H}^{[kk]\dagger}\mathbf{U}^{[k]}}{\mathbf{U}^{[k]\dagger}\left(P_j\mathbf{H}_j^{[k]}\mathbf{w}\mathbf{w}^\dagger\mathbf{H}_j^{[k]\dagger} + \sigma_n^2\mathbf{I}_{N^{[k]}}\right)\mathbf{U}^{[k]}}\right|. \tag{5}$$

From (5), we can observe that the transmission rate of IA users will be degraded severely if the jamming signal is not properly removed. The transmission rate will decrease when the transmit power of the jammer increases. For simplicity, all the IA users are assumed to have the same parameters in the rest of this paper, i.e., $M^{[k]} = M$, $N^{[k]} = N$, $d^{[k]} = 1$.

Remark 1: In this paper, we consider two opposite aspects, i.e., beneficial and adversarial jamming towards IA networks, and two proactive jamming schemes are proposed correspondingly. First, to guarantee the security of IA network, jamming can be utilized to disrupt the eavesdropping by generating spurious data in Section III, without affecting the legitimate transmission. Then, the jamming signal can also be designed to degrade the performance of the IA network without noticing in Section IV.

III. BENEFICIAL JAMMING TOWARDS IA NETWORKS

To guarantee the secure transmission of IA networks, several anti-eavesdropping schemes have been proposed in [35]–[37]. In [35], [36], the GIA technique was proposed to enhance the secrecy rate of IA networks, which jointly coordinates the transmission policy of the legitimate jammer (LJ) and IA users to generate stronger interference at the eavesdropper. In [37], the AN was designed to be generated along with the information data streams at each IA transmitter to disrupt the eavesdropping. The contributions of these schemes are outlined in Table I.

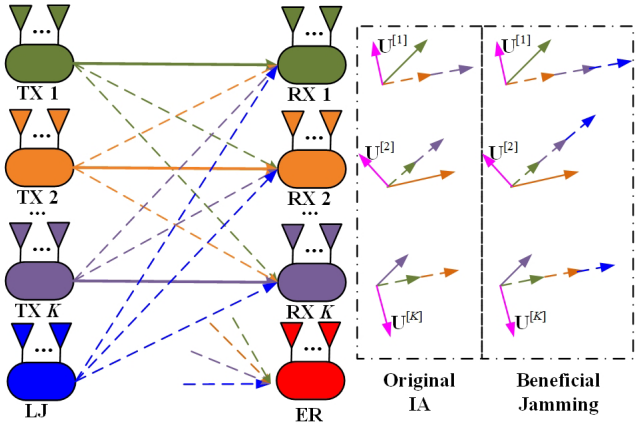


Fig. 1. Configuration of beneficial jamming towards the IA network to combat the eavesdropping.

From Table I, we can conclude that, although the potential eavesdropping of the IA network can be effectively disrupted by these two methods, there still exist some drawbacks. First, additional overload will be imposed on the legitimate IA network by these methods, in addition to the high requirement of CSI and solutions of IA. Thus, the IA network should make more effort to combat the eavesdropping through cooperating with the jammers. In addition, the number of antennas equipped at the transceivers of these two schemes increase compared to the original IA network. Thus, the jamming signal should be further designed to guarantee the secure transmission of the IA network without its additional help.

Thus, in this section, the proactive jamming scheme to combat potential eavesdropping for IA networks is presented first, and then, the performance of the eavesdropping will be analyzed for the proposed scheme.

A. Proactive Jamming Design

As shown in Fig. 1, we consider a legitimate IA network with an adversarial eavesdropper and a friendly jammer. The existence of the eavesdropper will threaten the secure transmission between the legitimate IA transmitters and receivers. The friendly jammer is intended to emit spurious data to disrupt the eavesdropping for the IA network. Nevertheless, from the expression of transmission rate for the kth IA user in (5), we can conclude that the jamming signal will also deteriorate the information transmission of the IA users, which should be properly designed to be compatible with the legitimate IA network. Specifically, the precoding vector of the jammer

should be designed to constrain the jamming signal into the same subspace as that of the interference among IA users at each receiver, as shown in Fig. 1, without any additional overload of the IA network. As a result, the jamming signal and interference can be eliminated together by the original decoding matrix at each IA receiver.

In order to constrain the jamming signal into the same subspace as the interference, the following conditions for the ith IA user should be satisfied as

$$\mathbf{H}_j^{[i]}\mathbf{w} = \alpha^{[i]}\mathbf{H}^{[iq]}\mathbf{v}^{[q]},\ \forall i = 1, 2, ..., K,\ q \neq i, \tag{6}$$

where $\alpha^{[i]}$ is a scaling factor to make the equation balanced.

As $i = 1, 2, ..., K$ in (6), we can rewrite the equation (6) as

$$\mathbf{A}\mathbf{w} = \mathbf{b}, \tag{7}$$

where

$$\mathbf{A} = \begin{pmatrix} \mathbf{H}_j^{[1]} \\ \mathbf{H}_j^{[2]} \\ \vdots \\ \mathbf{H}_j^{[K]} \end{pmatrix}, \tag{8}$$

and

$$\mathbf{b} = \begin{pmatrix} \alpha^{[1]}\mathbf{H}^{[1q]}\mathbf{v}^{[q_1]} \\ \alpha^{[2]}\mathbf{H}^{[2q]}\mathbf{v}^{[q_2]} \\ \vdots \\ \alpha^{[K]}\mathbf{H}^{[Kq]}\mathbf{v}^{[q_K]} \end{pmatrix},\ q_i \neq i,\ i = 1, 2, \ldots, K. \tag{9}$$

In (9), the jamming signal can be aligned at each IA receiver to the interference from any IA user, but not the interference from all the other users, because the interference from the other users has been aligned into the same subspace according to (3).

The design of the jamming precoding vector $\mathbf{w}$ to achieve (7) can be summarized in Theorem 1.

Theorem 1: To align the jamming signal into the same subspace as that of the interference at each IA user according to (7), the jamming precoding vector $\mathbf{w}$ should be designed as

$$\mathbf{w} = \mathbf{A}^{-1}\mathbf{b} + (\mathbf{I}_{N_j} - \mathbf{A}^{-1}\mathbf{A})\boldsymbol{\zeta}, \tag{10}$$

where $\boldsymbol{\zeta} \in \mathbb{C}^{N_j \times 1}$ is an arbitrary vector.

Proof: Based on the matrix theory, for the linear equation (7), when $\mathbf{A}$ is a non-singular matrix, the solution will be $\mathbf{A}^{-1}\mathbf{b}$, where $\mathbf{A}^{-1}$ satisfying $\mathbf{A}^{-1}\mathbf{A} = \mathbf{I}_{N_j}$ is the generalized inverse matrix of $\mathbf{A}$.

When $\mathbf{A}$ is a singular matrix, the equation (7) has either no solution, or infinitely many solutions. If the solution exists, it will be $\mathbf{A}^{-1}\mathbf{b} + (\mathbf{I}_{N_j} - \mathbf{A}^{-1}\mathbf{A})\boldsymbol{\zeta}$, where $\mathbf{A}^{-1}$ satisfying $\mathbf{A}\mathbf{A}^{-1}\mathbf{A} = \mathbf{A}$ is the generalized inverse matrix of $\mathbf{A}$.

Specifically, when $\mathbf{A}$ is non-singular, $\mathbf{A}^{-1}\mathbf{A} = \mathbf{I}_{N_j}$ also satisfies $\mathbf{A}\mathbf{A}^{-1}\mathbf{A} = \mathbf{A}$, and $\mathbf{A}^{-1}\mathbf{b} + (\mathbf{I}_{N_j} - \mathbf{A}^{-1}\mathbf{A})\boldsymbol{\zeta} = \mathbf{A}^{-1}\mathbf{b}$. Thus, the jamming precoding vector $\mathbf{w}$ has a unified expression as (10). ■

According to (3) and (6), after generating the jamming signal with the vector $\mathbf{w}$ according to Theorem 1, the jamming signal can be eliminated together with the interference by the original decoding vector at each legitimate IA receiver.

In (10), the main purpose of $\mathbf{w}$ is to align the jamming signal into the same subspace as that of the interference at each IA user, so that the jamming signal can be eliminated perfectly together with the interference between users. Thus, the arbitrary vector $\boldsymbol{\zeta}$ will not affect the performance of the proposed beneficial jamming scheme, due to the fact that the jamming signal will be eliminated perfectly at each IA receiver, no matter what value $\boldsymbol{\zeta}$ is. In addition, since we do not have the knowledge of the eavesdropping CSI, we cannot design $\boldsymbol{\zeta}$ to disrupt the eavesdropping more effectively.

Based on Theorem 1, the beneficial jamming scheme towards the IA network to disrupt the potential eavesdropping can be summarized as in Algorithm 1.

Algorithm 1 Beneficial jamming scheme

1: The nth time slot begins.
2: The legitimate IA network calculate its precoding and decoding vectors for all the users.
3: The instantaneous CSI of the IA network is obtained by the jammer.
4: The jammer sets the value of the scaling factor $\alpha^{[i]}$, $i = 1, 2, \ldots, K$.
5: According to (10), the jammer calculates its precoding vector $\mathbf{w}$.
6: Perform secure transmission of the IA network with the help of the jammer.
7: Current time slot ends, $n = n + 1$, back to Step 1.

Through Algorithm 1, the recovered signal at the kth IA receiver can be expressed as

$$\begin{aligned}\mathbf{y}^{[k]} &= \sum_{i=1}^{K} \mathbf{u}^{[k]\dagger}\mathbf{H}^{[ki]}\mathbf{v}^{[i]}x^{[i]} + \mathbf{u}^{[k]\dagger}\mathbf{H}_j^{[k]}\mathbf{w}x_j + \mathbf{u}^{[k]\dagger}\mathbf{n}^{[k]} \\ &= \mathbf{u}^{[k]\dagger}\mathbf{H}^{[kk]}\mathbf{v}^{[k]}x^{[k]} + \mathbf{u}^{[k]\dagger}\mathbf{n}^{[k]},\end{aligned} \tag{11}$$

in which the jamming signal and interference from other users can be perfectly eliminated by the original decoding vector of IA. Accordingly, the transmission rate of the kth user expressed in (5) can be rewritten as

$$\begin{aligned}R^{[k]} &= \log_2\left(1 + \frac{P^{[k]}\mathbf{u}^{[k]\dagger}\mathbf{H}^{[kk]}\mathbf{v}^{[k]}\mathbf{v}^{[k]\dagger}\mathbf{H}^{[kk]\dagger}\mathbf{u}^{[k]}}{\mathbf{u}^{[k]\dagger}\left(P_j\mathbf{H}_j^{[k]}\mathbf{w}\mathbf{w}^{\dagger}\mathbf{H}_j^{[k]\dagger} + \sigma_n^2\right)\mathbf{u}^{[k]}}\right) \\ &= \log_2\left(1 + \frac{P^{[k]}\mathbf{u}^{[k]\dagger}\mathbf{H}^{[kk]}\mathbf{v}^{[k]}\mathbf{v}^{[k]\dagger}\mathbf{H}^{[kk]\dagger}\mathbf{u}^{[k]}}{\sigma_n^2}\right).\end{aligned} \tag{12}$$

From (12), we can also conclude that the legitimate transmission of the IA network will not be affected by the jamming signal, and secure transmission of the IA network can be guaranteed by the beneficial jamming according to Algorithm 1 without performance degradation.

To perfectly achieve (11) and (12) through Algorithm 1, the feasibility condition of the beneficial jamming scheme should be developed, through which we can determine the minimal number of antennas that should be equipped at the jammer. According to Bezout's Theorem, we can know that a generic polynomial system is solvable if and only if the number of variables is no less than the number of equations [11]. Thus,

the feasibility condition of the beneficial jamming scheme can be derived as Theorem 2.

Theorem 2: The feasibility condition of the beneficial jamming scheme can be expressed as

$$KN \leq N_j. \tag{13}$$

Proof: The total number of equations in conditions (7) can be denoted as

$$\mathscr{N}_e = KN. \tag{14}$$

The precoding vector $\mathbf{w}$ of the jammer has N_j variables, i.e., the total number of variables in conditions (7) can be calculated as

$$\mathscr{N}_v = N_j. \tag{15}$$

Based on Bezout's Theorem, when the polynomial (7) is solvable, we have

$$\mathscr{N}_e \leq \mathscr{N}_v \Rightarrow KN \leq N_j. \tag{16}$$

Thus, Theorem 2 is proved. ∎

From Theorem 2, we can know that when the number of antennas at the jammer is no less than the total number of antennas at the K IA receivers, the proposed beneficial jamming scheme is feasible, i.e., the secure transmission of the IA network can be guaranteed by the jamming signal without affecting the transmission rate of the IA users. Thus, we can conclude that in the beneficial jamming scheme, the jamming signal will not affect the DoFs of the original IA network, when the feasibility conditions can be satisfied.

B. Eavesdropping Performance Analysis

To further demonstrate the effectiveness of the jamming signal, we analyze the performance of the eavesdropping when the jamming signal is present or not. In the design of the proposed beneficial jamming scheme in Section III-A, the CSI from eavesdropper is not needed; while to analyze the eavesdropping performance towards our proposed scheme, the eavesdropping CSI is needed, which does not mean that the CSI from eavesdropper is needed in our proposed scheme.

First, consider the situation that the jamming signal is not generated towards the legitimate IA network. To eavesdrop the information of the kth IA user, the received signal at the eavesdropper through its decoding vector $\mathbf{u}_e^{[k]}$ can be expressed as

$$y_e^{[k]} = \mathbf{u}_e^{[k]\dagger}\mathbf{G}_e^{[k]}\mathbf{v}^{[k]}x^{[k]} + \sum_{i=1,i\neq k}^{K} \mathbf{u}_e^{[k]\dagger}\mathbf{G}_e^{[i]}\mathbf{v}^{[i]}x^{[i]} + \mathbf{u}_e^{[k]\dagger}\mathbf{n}_e, \tag{17}$$

where $\mathbf{G}_e^{[i]} \in \mathbb{C}^{N_e \times M^{[i]}}$ is the channel coefficient matrix from the ith transmitter to the eavesdropper, each entity of which is i.i.d. and follows $\mathcal{CN}(0,1)$. $\mathbf{u}_e^{[k]} \in \mathbb{C}^{N_e \times 1}$ is the decoding vector at the eavesdropper targeting the kth user. $\mathbf{n}_e^{[k]} \in \mathbb{C}^{N_e \times 1}$ is the AWGN vector at the eavesdropper.

The eavesdropping rate of the kth IA user can be expressed as

$$R_e^{[k]} = \log_2\left(1 + \frac{P^{[k]}\mathbf{u}_e^{[k]\dagger}\mathbf{G}_e^{[k]}\mathbf{v}^{[k]}\mathbf{v}^{[k]\dagger}\mathbf{G}_e^{[k]\dagger}\mathbf{u}_e^{[k]}}{\sigma_n^2 + P^{[i]}\sum\limits_{i=1,i\neq k}^{K}\mathbf{u}_e^{[k]\dagger}\mathbf{G}_e^{[i]}\mathbf{v}^{[i]}\mathbf{v}^{[i]\dagger}\mathbf{G}_e^{[i]\dagger}\mathbf{u}_e^{[k]}}\right). \tag{18}$$

Accordingly, the secrecy rate of the kth legitimate IA user can be expressed as (19) (on the next page), where $x^+ = \max(x, 0)$.

To eavesdrop the information transmitted by the kth legitimate IA user without any residual interference, the following condition should be satisfied.

$$\mathbf{u}_e^{[k]\dagger}\mathbf{G}_e^{[i]}\mathbf{v}^{[i]} = 0, \ \forall i \neq k. \tag{20}$$

Thus, the zero-forcing method should be utilized by the eavesdropper with enough antennas to eliminate the interference, and the feasibility condition of the eavesdropper can be derived in Proposition 1.

Proposition 1: In the case that no jamming signal exists, to eavesdrop a certain IA user free of interference, the number of antennas equipped at the eavesdropper should satisfy

$$N_e \geq K. \tag{21}$$

Proof: To eavesdrop the transmitted information of the kth IA user free of interference, the interference from other users should be zero-forced perfectly with (20) satisfied.

According to the conclusion in [11], the number of variables and equations in (20) can be expressed as in (22) and (23), respectively.

$$\mathscr{N}_v = N_e - 1. \tag{22}$$

$$\mathscr{N}_e = K - 1. \tag{23}$$

Based on Bezout's Theorem, when the polynomial (20) is solvable, we have

$$\mathscr{N}_v \geq \mathscr{N}_e \Rightarrow N_e - 1 \geq K - 1 \Rightarrow N_e \geq K. \tag{24}$$

∎

When the condition (21) can be satisfied, the interference from other IA users will be eliminated perfectly at the eavesdropper, and the eavesdropping rate will be enhanced greatly. In consequence, the secrecy rate will also be reduced close to zero.

Then, we consider the situation that the beneficial jamming is generated towards the IA network to prevent eavesdropping. To eavesdrop the information of the kth IA user, the received signal at the eavesdropper through its decoding vector $\hat{\mathbf{u}}_e^{[k]}$ can be expressed as

$$\begin{aligned}\hat{y}_e^{[k]} \ &= \ \hat{\mathbf{u}}_e^{[k]\dagger}\mathbf{G}_e^{[k]}\mathbf{v}^{[k]}x^{[k]} + \sum_{i=1,i\neq k}^{K}\hat{\mathbf{u}}_e^{[k]\dagger}\mathbf{G}_e^{[i]}\mathbf{v}^{[i]}x^{[i]} \\ &+ \ \hat{\mathbf{u}}_e^{[k]\dagger}\mathbf{G}_j\mathbf{w}x_j + \hat{\mathbf{u}}_e^{[k]\dagger}\mathbf{n}_e.\end{aligned} \tag{25}$$

where $\mathbf{G}_j \in \mathbb{C}^{N_e \times N_j}$ is the channel coefficient matrix between the jammer and the eavesdropper, each entity of which is i.i.d. and follows $\mathcal{CN}(0,1)$.

The eavesdropping rate of the kth IA user when considering the jamming signal can be expressed as

$$\hat{R}_e^{[k]} = \log_2\left(1 + \frac{P^{[k]}\hat{\mathbf{u}}_e^{[k]\dagger}\mathbf{G}_e^{[k]}\mathbf{v}^{[k]}\mathbf{v}^{[k]\dagger}\mathbf{G}_e^{[k]\dagger}\hat{\mathbf{u}}_e^{[k]}}{\sigma_n^2 + \hat{Q}_e^{[k]}}\right), \tag{26}$$

$$R_s^{[k]} = \left(R^{[k]} - R_e^{[k]}\right)^+ = \left(\log_2 \left(\frac{1 + \frac{P^{[k]}}{\sigma_n^2} \mathbf{u}^{[k]\dagger} \mathbf{H}^{[kk]} \mathbf{v}^{[k]} \mathbf{v}^{[k]\dagger} \mathbf{H}^{[kk]\dagger} \mathbf{u}^{[k]}}{1 + \frac{P^{[k]} \mathbf{u}_e^{[k]\dagger} \mathbf{G}_e^{[k]} \mathbf{v}^{[k]} \mathbf{v}^{[k]\dagger} \mathbf{G}_e^{[k]\dagger} \mathbf{u}_e^{[k]}}{\sigma_n^2 + P^{[i]} \sum\limits_{i=1, i\neq k}^{K} \mathbf{u}_e^{[k]\dagger} \mathbf{G}_e^{[i]} \mathbf{v}^{[i]} \mathbf{v}^{[i]\dagger} \mathbf{G}_e^{[i]\dagger} \mathbf{u}_e^{[k]}}} \right) \right)^+ . \tag{19}$$

$$\hat{R}_s^{[k]} = (R^{[k]} - \hat{R}_e^{[k]})^+ = \left(\log_2 \left(\frac{1 + \frac{P^{[k]}}{\sigma_n^2} \mathbf{u}^{[k]\dagger} \mathbf{H}^{[kk]} \mathbf{v}^{[k]} \mathbf{v}^{[k]\dagger} \mathbf{H}^{[kk]\dagger} \mathbf{u}^{[k]}}{1 + \frac{P^{[k]} \hat{\mathbf{u}}_e^{[k]\dagger} \mathbf{G}_e^{[k]} \mathbf{v}^{[k]} \mathbf{v}^{[k]\dagger} \mathbf{G}_e^{[k]\dagger} \hat{\mathbf{u}}_e^{[k]}}{\sigma_n^2 + P^{[i]} \sum\limits_{i=1, i\neq k}^{K} \hat{\mathbf{u}}_e^{[k]\dagger} \mathbf{G}_e^{[i]} \mathbf{v}^{[i]} \mathbf{v}^{[i]\dagger} \mathbf{G}_e^{[i]\dagger} \hat{\mathbf{u}}_e^{[k]} + P_j \hat{\mathbf{u}}_e^{[k]\dagger} \mathbf{G}_j \mathbf{w}\mathbf{w}^\dagger \mathbf{G}_j^\dagger \hat{\mathbf{u}}_e^{[k]}}} \right) \right)^+ . \tag{28}$$

where

$$\hat{Q}_e^{[k]} = P^{[i]} \sum_{i=1, i\neq k}^{K} \hat{\mathbf{u}}_e^{[k]\dagger} \mathbf{G}_e^{[i]} \mathbf{v}^{[i]} \mathbf{v}^{[i]\dagger} \mathbf{G}_e^{[i]\dagger} \hat{\mathbf{u}}_e^{[k]} + P_j \hat{\mathbf{u}}_e^{[k]\dagger} \mathbf{G}_j \mathbf{w}\mathbf{w}^\dagger \mathbf{G}_j^\dagger \hat{\mathbf{u}}_e^{[k]}. \tag{27}$$

Therefore, the secrecy rate of the kth legitimate IA user can be expressed as (28).

To eavesdrop the information transmitted by the kth legitimate user without any residual interference and jamming signal, the interference and jamming signal must be eliminated completely. According to (9) and (10), we can know that the precoding vector $\mathbf{w}$ of the jammer can be changed according to the parameters $\alpha^{[1]}, \alpha^{[2]}, \ldots, \alpha^{[K]}$. To combat the eavesdropping, we can make the vector $\mathbf{w}$ varying all the time when the parameters $\alpha^{[1]}, \alpha^{[2]}, \ldots, \alpha^{[K]}$ are set to be varying, and the eavesdropper cannot estimate $\mathbf{w}$ at each time slot like $\mathbf{v}^{[i]}$, $i = 1, 2, \ldots, K$. Therefore, in addition to (20), the following condition must be satisfied.

$$\hat{\mathbf{u}}_e^{[k]\dagger} \mathbf{G}_j = \mathbf{0}_{1\times N_j}. \tag{29}$$

Thus, the zero-forcing method should be leveraged by the eavesdropper with enough antennas to eliminate the interference and the jamming signal, and the feasibility condition of the eavesdropper with the existence of jamming signal can be derived in Proposition 2.

Proposition 2: In the case that the beneficial jamming exists, to eavesdrop a certain IA user free of interference and jamming signal, the number of antennas equipped at the eavesdropper should satisfy

$$N_e \geq K + N_j. \tag{30}$$

Proof: To eavesdrop the transmitted information of the the k IA user, the interference and jamming signal should be zero-forced together with equations (20) and (29) satisfied.

According to the conclusion in [11], the number of variables and equations in (29) are $N_e - 1$ and N_j, respectively. Thus, together with the conclusion in Proposition 1, we can know that the total number of variables and equations in (20) and (29) can be expressed as

$$\mathscr{N}_v = N_e - 1 \tag{31}$$

$$\mathscr{N}_e = K - 1 + N_j. \tag{32}$$

Based on Bezout's Theorem, when the polynomials (20) and (29) are solvable, we have

$$\mathscr{N}_v \geq \mathscr{N}_e \Rightarrow N_e - 1 \geq K - 1 + N_j \Rightarrow N_e \geq K + N_j. \tag{33}$$

■

Remark 2: Observing Proposition 1 and Proposition 2, we can conclude that when the beneficial jamming signal is generated towards the IA network, the eavesdropper has to add additional N_j number of antennas to achieve perfect eavesdropping compared to that without jamming. Especially, when the proposed beneficial jamming scheme is feasible, $N_j = KN$, which means that at least KN additional eavesdropping antennas should be equipped, which is a challenging requirement for the eavesdropper. Besides, from (19) and (28), we can also know that the performance of the secure transmission will be improved by the jamming signal with the same number of eavesdropping antennas.

IV. Adversarial Jamming Towards IA Networks

The openness of wireless channel makes it more vulnerable to be abused by some vicious organizations to commit crimes. Recently, criminals and terrorists can easily establish infrastructure-free wireless communications to commit crimes or terror attack, and IA is an effective way to construct such an illegal multi-user network. Therefore, it becomes increasingly important for governmental agencies to monitor the suspicious links and take some valid measures to disrupt the illegal transmission.

In [38], [39], the information surveillance was performed to combat the suspicious transmission, in which the governmental monitor overhears the suspicious transmitter and concurrently forwards a spoofing signal to the suspicious receiver to disrupt its transmission. However, when the anti-jamming IA scheme

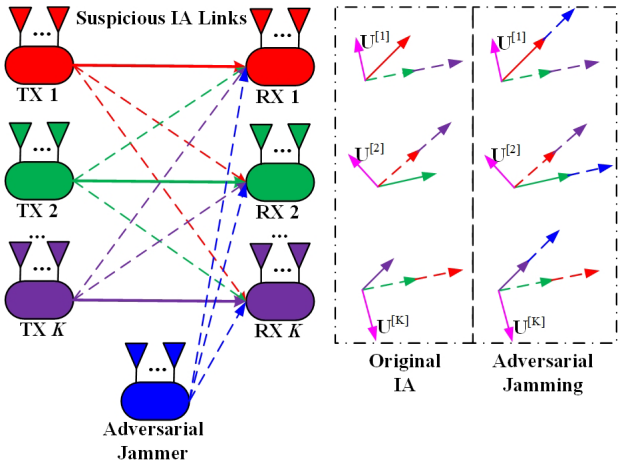


Fig. 2. Configuration of adversarial jamming to disrupt the IA network without noticing.

is exploited [28], the illegal IA network can eliminate the jamming signal and guarantee its transmission. Thus, how to design the proactive jamming signal to disrupt the IA network without its noticing is the key issue for the surveillance of illegal IA networks. Thus, in this section, we consider an information surveillance scenario, where an adversarial jammer is intended to send spurious data to degrade the performance of IA network secretly, as shown in Fig. 2. From the figure, we can see that the adversarial jamming signal is aligned into the same subspace as that of the desired signal at each IA receiver. Thus, the transmission of IA network will be severely disrupted, while the IA users cannot easily perceive.

When IA is performed, the transmission rate of the kth IA user has the same expression as (12). To deteriorate the IA transmission, we propose an adversarial jamming scheme, through which the jamming signal is constrained into the same subspace as that of the desired signal at each IA receiver, and thus, it is difficult for the IA users to perceive the adversarial jamming signal.

In order to project the jamming signal into the same subspace as that of the desired signal at each IA receiver, the following conditions should be satisfied.

$$\mathbf{H}_j^{[i]}\mathbf{w} = \beta^{[i]}\mathbf{H}^{[ii]}\mathbf{v}^{[i]},\ \forall i = 1, 2, ..., K, \tag{34}$$

where $\beta^{[i]}$ is a scaling factor to make the equation balanced.

As $i = 1, 2, ..., K$ in (34), we can rewrite the equation (34) as

$$\mathbf{C}\mathbf{w} = \mathbf{d}, \tag{35}$$

where

$$\mathbf{C} = \mathbf{A} = \begin{pmatrix} \mathbf{H}_j^{[1]} \\ \mathbf{H}_j^{[2]} \\ \vdots \\ \mathbf{H}_j^{[K]} \end{pmatrix}, \tag{36}$$

and

$$\mathbf{d} = \begin{pmatrix} \beta^{[1]}\mathbf{H}^{[11]}\mathbf{v}^{[1]} \\ \beta^{[2]}\mathbf{H}^{[22]}\mathbf{v}^{[2]} \\ \vdots \\ \beta^{[K]}\mathbf{H}^{[KK]}\mathbf{v}^{[K]} \end{pmatrix}. \tag{37}$$

The design of the jamming precoding vector $\mathbf{w}$ to achieve (35) can be summarized in Theorem 3.

Theorem 3: To constrain the jamming signal into the same subspace as that of the desired signal at each IA receiver according to (35), the jamming precoding vector $\mathbf{w}$ should be designed as

$$\mathbf{w} = \mathbf{C}^{-1}\mathbf{d} + (\mathbf{I}_{N_j} - \mathbf{C}^{-1}\mathbf{C})\boldsymbol{\xi}, \tag{38}$$

where $\boldsymbol{\xi} \in \mathbb{C}^{N_j \times 1}$ is an arbitrary vector.

Proof: The proof is the same as that of Theorem 1, which will not be repeated here. ■

According to (3) and (34), after generating the adversarial jamming signal with the vector $\mathbf{w}$ according to Theorem 3, the jamming signal can be aligned into the same subspace as that of the desired signal at each IA receiver. Thus, with the jamming signal not noticing, the transmission performance of the IA network will be severely degraded, due to the fact that the jamming signal is treated as background noise by IA users.

In (38), the main purpose of $\mathbf{w}$ is to constrain the jamming signal into the same subspace as that of the desired signal at each IA receiver, and the transmission of IA network will be disrupted without noticing. For the arbitrary vector $\boldsymbol{\xi}$, it will not affect the alignment of the jamming signal, and the effective jamming power at the kth IA receiver is only determined by $\beta^{[k]}$, instead of $\boldsymbol{\xi}$. Thus, the value of $\boldsymbol{\xi}$ will not affect the performance of the proposed adversarial jamming scheme.

Based on Theorem 3, the adversarial jamming scheme towards the IA network can be summarized as in Algorithm 2.

Algorithm 2 Adversarial jamming scheme

1: The nth time slot begins.
2: The IA network calculate its precoding and decoding vectors for all the users.
3: The jammer monitors the information transmission of the IA network, and obtain its instantaneous CSI.
4: The jammer sets the value of the scaling factor $\beta^{[i]}$, $i = 1, 2, \ldots, K$.
5: According to (38), the jammer calculate its precoding vector $\mathbf{w}$.
6: The jammer sends spurious data to disrupt the transmission of the IA network throughout the time slot.
7: Current time slot ends, $n = n + 1$, back to Step 1.

Similar to the beneficial jamming scheme in Section III, the feasibility condition of the adversarial jamming scheme can be derived as Theorem 4.

Theorem 4: The feasibility condition of the adversarial jamming scheme can be expressed as

$$KN \leq N_j. \tag{39}$$

Proof: The proof is the same as that of Theorem 2, which will not be repeated here. ■

Disrupted by the adversarial jammer, the transmission rate of the kth IA user can be rewritten as

$$R^{[k]} = \log_2 \left(1 + \frac{P^{[k]} \mathbf{u}^{[k]\dagger} \mathbf{H}^{[kk]} \mathbf{v}^{[k]} \mathbf{v}^{[k]\dagger} \mathbf{H}^{[kk]\dagger} \mathbf{u}^{[k]}}{\mathbf{u}^{[k]\dagger} \left(P_j \mathbf{H}_j^{[k]} \mathbf{w} \mathbf{w}^\dagger \mathbf{H}_j^{[k]\dagger} + \sigma_n^2 \right) \mathbf{u}^{[k]}} \right), \quad (40)$$

where the received jamming signal is treated in the same way as the background noise, due to the fact that the IA receivers cannot notice it.

Comparing (12) and (40), we can know that, through generating the adversarial jamming signal towards the IA network, the transmission rate of each IA users will be reduced significantly. In addition, when the feasibility condition of the proposed adversarial jamming scheme can be satisfied, the jamming signal will be perfectly aligned into the same subspace as that of the desired signal at each IA receiver, which ensures that the jamming signal cannot be easily perceived by the IA users.

Remark 3: (1) We can observe that the proposed beneficial and adversarial jamming schemes towards IA networks are quite similar, due to the fact that in the beneficial jamming scheme, the jamming signal is aligned with the interference at each receiver, while in the adversarial jamming scheme, the jamming signal is aligned with the desired signal at each receiver. Therefore, we can exploit similar mechanisms to achieve totally different goals.

(2) In the adversarial jamming scheme, the performance of the legitimate IA network will be degraded severely, and the jamming signal will reduce its DoFs to zero.

(3) The value of β in (34) also reflects the transmit power of the jamming signal, which will be shown in the simulation results of Section V. Thus, we can also manage the value of β to control the transmit power of the jammer.

(4) In practical systems, we may want to measure the alignment of the jamming signal and the desired signal at each IA receiver, which reflects the quality in performing the proposed adversarial jamming scheme. Thus, we define an indicator as

$$\Gamma = \sum_{i=1}^{K} \left\| \left(\mathbf{H}_j^{[i]} \mathbf{w} \right) \wedge \left(\mathbf{H}^{[ii]} \mathbf{v}^{[i]} \right) \right\|^2, \quad (41)$$

which shows the quantity of residual jamming signal that is not aligned at the direction of the desired signal. We will use this parament Γ to measure the performance of the proposed adversarial jamming scheme in Section V.

V. Simulation Results and Discussions

In this section, simulation results are presented to evaluate the performances of the proposed two jamming schemes towards IA networks. Assume that the MinIL algorithm is adopted to calculate the solutions of IA [10].

A. Beneficial Jamming Scheme

In this subsection, the performance of the beneficial jamming scheme towards IA networks is simulated. $K = 3$ IA users are considered, with $M = 2$ antennas at each transmitter and $N = 2$ antennas at each receiver. We also assume that $\alpha^{[1]} = \alpha^{[2]} = \ldots = \alpha^{[K]} = \alpha$. The transmit power of each IA user and the transmit power at the jammer is set to $P^{[k]} = P_j = 1$, $k = 1, 2, \ldots, K$.

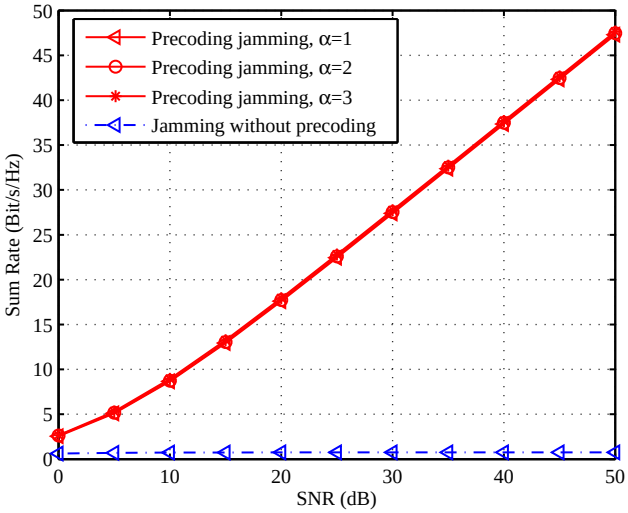


Fig. 3. Comparison of the sum rate of the IA network when the beneficial jamming scheme is adopted with different values of α and when no precoding is performed at the jammer. ($M = 2$, $N = 2$, $K = 3$, $N_j = 6$.)

First, the sum rate of the IA network is compared in Fig. 3, when the beneficial jamming scheme is adopted with different values of α and the conventional scheme when no precoding is performed at the jammer. $N_j = KN = 6$, and according to Theorem 2, the beneficial jamming scheme is feasible in this scenario. From the results, we can see that the sum rate of the IA network when the beneficial jamming scheme is adopted is much higher than the conventional case when no precoding is performed at the jammer. In addition, we can also find that the performance of the IA network is the same, for different values of α, due to the fact that the jamming signal can be perfectly eliminated at the IA receivers by the beneficial jamming scheme no matter how large α is. Nevertheless, larger value of α means higher transmit power of the jamming signal, which will disrupt the eavesdropping more effectively.

Then, the sum rate of the IA network is compared in Fig. 4, when the beneficial jamming scheme is adopted with different values of N_j. α is set to 1. From the results, we can see that, when $N_j \geq KN = 6$, the beneficial jamming scheme is feasible, which is consistent with Theorem 2, and the sum rate of the IA network will not be affected. However, when $N_j \leq 5$, the proposed scheme is not feasible according to Theorem 2, and the sum rate of the IA network will decrease greatly, although the potential eavesdropping can be disrupted.

In addition, the eavesdropping rate with different number of N_e is compared in Fig. 5, when the jamming signal exists with different values of N_j or no jamming signal is generated. SNR=40dB and $\alpha = 1$. From the results, we can see that, when no jamming exists, perfect eavesdropping will be achieved when $N_e \geq K = 3$, which is consistent with Proposition 1. When the beneficial jamming scheme is adopted, perfect will be achieved when $N_e \geq K + N_j$ according to Proposition 2,

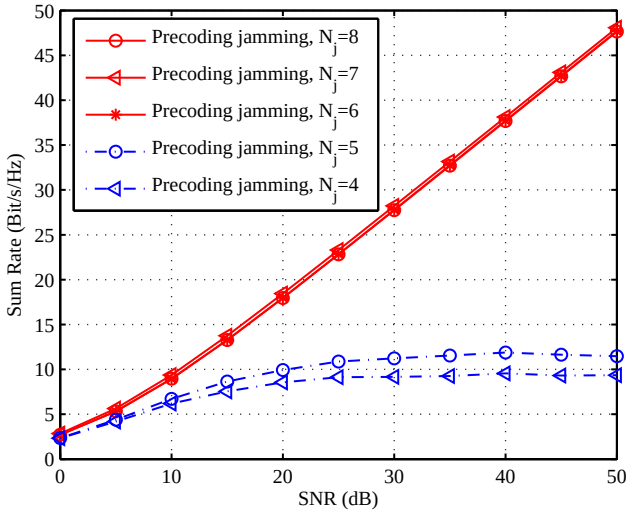


Fig. 4. Comparison of the sum rate of the IA network when the beneficial jamming scheme is adopted with different values of N_j. ($M = 2$, $N = 2$, $K = 3$, $\alpha = 1$.)

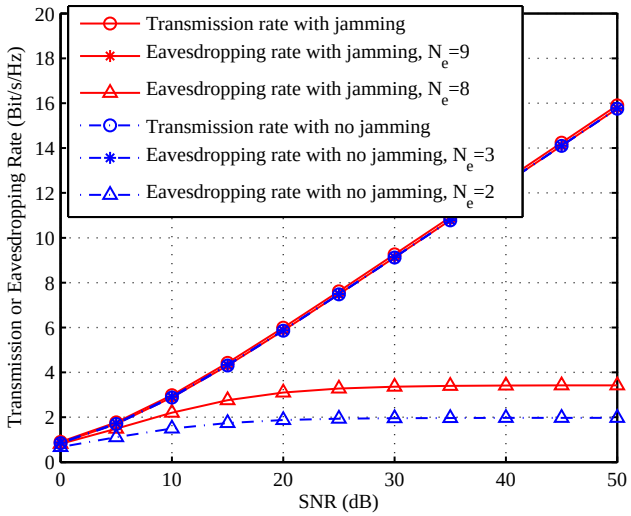


Fig. 6. Comparison of the transmission rate of the certain IA user and the eavesdropper rate with different values of N_e, when the jamming signal exists or not. ($M = 2$, $N = 2$, $K = 3$, $N_j = 6$, $\alpha = 1$.)

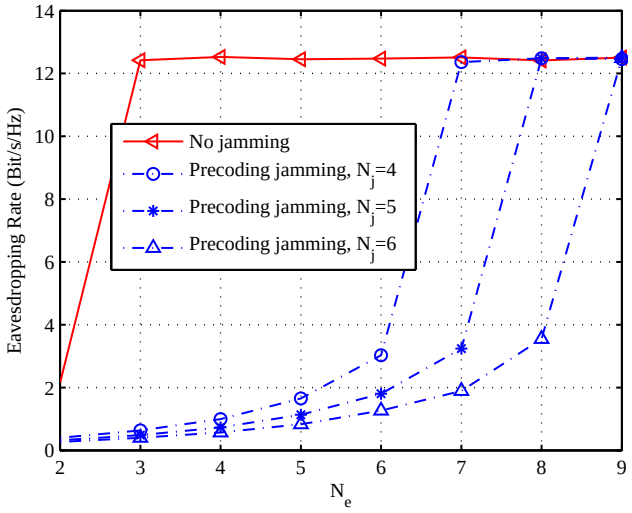


Fig. 5. Comparison of the eavesdropping rate with different number of N_e, when the jamming signal exists with different values of N_j or no jamming signal is generated. ($M = 2$, $N = 2$, $K = 3$, SNR= 40dB, $\alpha = 1$.)

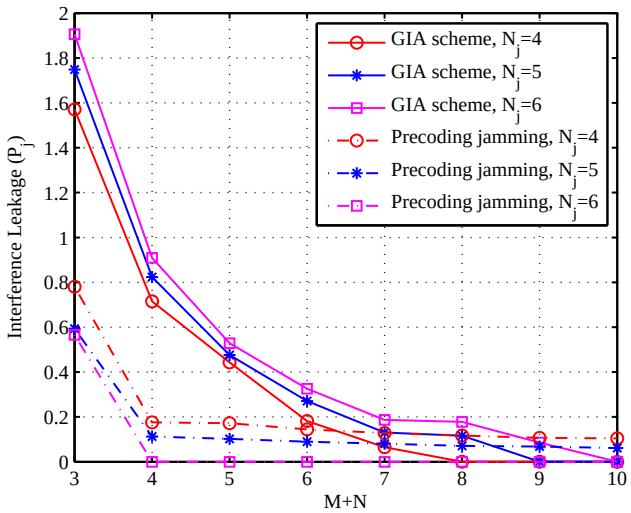


Fig. 7. Comparison of interference leakage at each IA receiver of the proposed beneficial jamming scheme and the GIA scheme with different number of antennas $M + N$. ($K = 3$, SNR= 30dB, $\alpha = 1$.)

no matter whether the scheme is feasible. Thus, increasing the number of antennas at the jammer will make the IA network much securer.

In Fig. 6, the transmission rate of the certain IA user and the eavesdropper rate with different values of N_e are compared, when the jamming signal exists or not. $N_j = 6$ and $\alpha = 1$. From the results, we can see that, when the beneficial jamming signal exists, the perfect eavesdropping towards a certain IA user can be achieved only when $N_e \geq K + N_j = 9$, which is consistent with Proposition 2. Besides, when no jamming signal exists, the perfect eavesdropping can be achieved when $N_e \geq K = 3$. Thus, we can conclude that the proposed beneficial jamming scheme can enhance the performance of secure transmission for the IA network significantly, and N_j additional antennas should be equipped at the eavesdropper to perform perfect eavesdropping compared to the traditional IA scheme without any jamming signal.

In Fig. 7, the interference leakage at each IA receiver using the proposed beneficial jamming scheme and the GIA scheme is compared with different numbers of antennas $M+N$. In the simulation, three IA users are considered, $\alpha^{[1]} = \alpha^{[2]} = ... = \alpha^{[K]} = \alpha = 1$, and SNR= 30dB. From the results, we can see that less antennas are required for each IA user to eliminate the jamming signal perfectly by the proposed jamming scheme, i.e., $M + N \geq 4$, due to the fact that the jamming signal is aligned into the interference subspace at each IA receiver only by the jammer, instead of the IA network. Nevertheless, enough antennas should be equipped at the jammer to achieve this, i.e., $N_j \geq 6$. On the other hand, for the GIA scheme, the interference can be perfectly eliminated at each IA receiver for all the values of N_j, as long as $M + N$ is large enough, i.e., $M+N$ should be become larger with more jamming antennas. This is due to the fact that the jamming signal is handled only by the IA network, and more antennas are needed by each IA

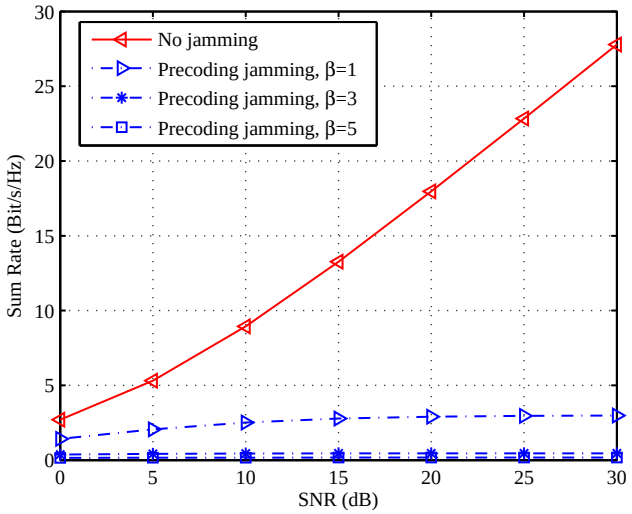


Fig. 8. Comparison of the sum rate of the IA network when the adversarial jamming scheme is adopted with different values of β and when no jamming signal is generated. ($M = 2$, $N = 2$, $K = 3$, $N_j = 6$.)

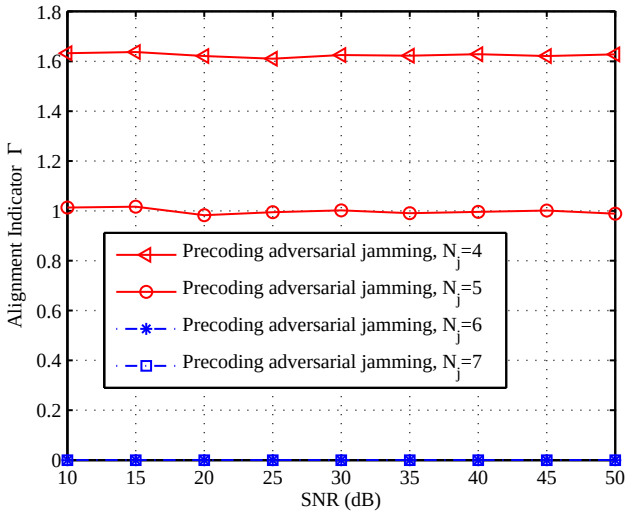


Fig. 9. Comparison of the alignment indicator Γ in the adversarial jamming with different number of antennas equipped at the jammer, when the jamming Algorithm 2 is adopted. ($M = 2$, $N = 2$, $K = 3$, $\beta = 1$.)

user to achieve this. Thus, these two schemes are suitable to be utilized in different cases with different computing capabilities of the IA users and jammer.

B. Adversarial Jamming Scheme

In this subsection, the performance of the adversarial jamming scheme towards IA networks is analyzed through simulation. $K = 3$ IA users are considered, with $M = 2$ antennas at each transmitter and $N = 2$ antennas at each receiver. We also assume that $\beta^{[1]} = \beta^{[2]} = ... = \beta^{[K]} = \beta$. The transmit power of each IA user and the transmit power at of the jammer is set to $P^{[k]} = P_j = 1$, $k = 1, 2, \ldots, K$.

First, the sum rate of the IA network is compared in Fig. 8, when the adversarial jamming scheme is adopted with different values of β and when no jamming signal is generated. $N_j = KN = 6$, and according to Theorem 4, the adversarial jamming scheme is feasible in this scenario. From the results, we can see that, when the adversarial jamming scheme is adopted, the sum rate of the IA network will be decreased severely. Besides, we can also see that the sum rate of the IA network will become lower with larger value of β, this is due to the fact that the parameter β also reflects the transmit power of the adversarial jammer, according to (34).

Although the proposed adversarial jamming scheme can achieve excellent performance according to the results in Fig. 9, we cannot know whether the adversarial jamming signal can be perceived by the IA network. To further verify the capability of the adversarial jamming scheme in concealing the jamming signal, the alignment indicator Γ defined in (41) is compared with different values of N_j in Fig. 9. $\beta = 1$. From the results, we can see that, when the adversarial jamming scheme is feasible according to Theorem 4, i.e., $N_j \geq KN = 6$, the indicator Γ becomes equal to 0, which means that the jamming signal has been constrained into the same subspace as that of the desired signal at each IA receiver. Thus, the IA users cannot perceive the eavesdropping when the proposed adversarial jamming scheme is feasible.

VI. Conclusions

In this paper, we have proposed two proactive jamming schemes, which are beneficial and adversarial towards IA networks, respectively. First, in the beneficial jamming scheme, the precoding vector of the jammer is designed to constrain the jamming signal into the same subspace as that of the interference among users at each IA receiver, and thus the potential eavesdropping will be disrupted effectively without affecting the transmission of the IA network. Then, in the adversarial jamming scheme, the precoding vector of the jammer is designed to project the jamming signal into the same subspace as that of the desired signal at each IA receiver, which will result in the performance degradation of the IA network without its noticing. Plenty of simulation results have been presented to verify the effectiveness of the two proposed jamming schemes.

References

[1] J. Guo, Y. Cao, Z. Yang, N. Zhao, F. R. Yu, Y. Chen, and V. C. M. Leung, "Beneficial jamming design for interference alignment networks," in *Proc. WCSP'17*, pp. 1–6, Nanjing, China, Oct. 2017.

[2] Y. Wu, C. Xiao, X. Gao, J. D. Matyjas, and Z. Ding, "Linear precoder design for MIMO interference channels with finite-alphabet signaling," *IEEE Trans. Commun.*, vol. 61, no. 9, pp. 3766–3780, Sept. 2013.

[3] A. Nabil, Y. T. Hou, R. Zhu, and W. Lou , "Recent advances in interference management for wireless networks," *IEEE Network*, vol. 29, no. 5, pp. 83–89, Sept. 2015.

[4] W. Feng, Y. Wang, D. Lin, N. Ge, J. Lu, and S. Li, "When mmWave communications meet network densification: A scalable interference coordination perspective," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 7, pp. 1459–1471, Jul. 2017.

[5] J. Tian, H. Zhang, D. Wu, and D. Yuan, "Interference-aware cross-layer design for distributed video transmission in wireless networks," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 26, no. 5, pp. 978–991, May 2016.

[6] W. Feng, Y. Wang, N. Ge, J. Lu, and J. Zhang, "Virtual MIMO in multi-cell distributed antenna systems: Coordinated transmissions with large-scale CSIT," *IEEE J. Select. Areas Commun.*, vol. 31, no. 10, pp. 2067–2081, Oct. 2013.

[7] V. R. Cadambe and S. A. Jafar, "Interference alignment and degrees of freedom of the *K*-user interference channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3425–3441, Aug. 2008.

[8] N. Zhao, F. R. Yu, M. Jin, Q. Yan, and V. C. M. Leung, "Interference alignment and its applications: A survey, research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1779–1803, 3rd Quart. 2016.

[9] A. Dong, H. Zhang, D. Yuan, and X. Zhou, "Interference alignment transceiver design by minimizing the maximum mean square error for MIMO interfering broadcast channel," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6024–6037, Aug. 2016.

[10] K. Gomadam, V. R. Cadambe, and S. A. Jafar, "A distributed numerical approach to interference alignment and applications to wireless interference networks," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3309–3322, Jun. 2011.

[11] C. M. Yetis, T. Gou, S. A. Jafar, and A. H. Kayran, "On feasibility of interference alignment in MIMO interference networks," *IEEE Trans. Signal Process.*, vol. 58, no. 9, pp. 4771–4782, Sept. 2010.

[12] N. Zhao, F. R. Yu, H. Sun, A. Nallanathan, and H. Yin, "A novel interference alignment scheme based on sequential antenna switching in wireless networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 10, pp. 5008–5021, Oct. 2013.

[13] N. Zhao, F. R. Yu, and V. C. M. Leung, "Opportunistic communications in interference alignment networks with wireless power transfer," *IEEE Wireless Commun.*, vol. 22, no. 1, pp. 88–95, Feb. 2015.

[14] N. Zhao, F. R. Yu, H. Sun, and M. Li, "Adaptive power allocation schemes for spectrum sharing in interference-alignment-based cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 5, pp. 3700–3714, May 2016.

[15] O. E. Ayach, A. Lozano, and R. W. Heath, "On the overhead of interference alignment: Training, feedback, and cooperation," *IEEE Trans. Wireless Commun.*, vol. 11, no. 11, pp. 4192–4203, Nov. 2012.

[16] S. Jafar, "Blind interference alignment," *IEEE J. Sel. Topics Signal Proc.*, vol. 6, no. 3, pp. 216–227, Jun. 2012.

[17] N. Zhao, F. R. Yu, H. Sun, H. Yin, A. Nallanathan, and G. Wang, "Interference alignment with delayed channel state information and dynamic AR-model channel prediction in wireless networks," *Wireless Netw.*, vol. 21, no. 4, pp. 1227–1242, May 2015.

[18] F. Gao, T. Cui, and A. Nallanathan, "On channel estimation and optimal training design for amplify and forward relay networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 5, pp. 1907–1916, May 2008.

[19] F. Gao, R. Zhang, and Y. C. Liang, "Optimal channel estimation and training design for two-way relay networks," *IEEE Trans. Commun.*, vol. 57, no. 10, pp. 3024–3033, Oct. 2009.

[20] Y. Zou, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sept. 2016.

[21] F. Zhu, F. Gao, M. Yao, and H. Zou, "Joint information- and jamming-beamforming for physical layer security with full duplex base station," *IEEE Trans. Signal Process.*, vol. 62, no. 24, pp. 6391–6401, Dec. 2014.

[22] L. Fan, R. Zhao, F. K. Gong, N. Yang, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying over correlated fading channels," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 2811–2820, Jul. 2017.

[23] H.-M. Wang, C. Chao, D. W. K. Ng, M. H. Lee, and J. Xiao, "Artificial noise assisted secure transmission for distributed antenna systems," *IEEE Trans. Signal Process.*, vol. 64, no. 15, pp. 4050–4064, Aug. 2016.

[24] 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, Oct. 2016.

[25] T. Basar, "The Gaussian test channel with an intelligent jammer," *IEEE Trans. Inform. Theory*, vol. 29, no. 1, pp. 152–157, Jan. 1983.

[26] A. Kashyap, T. Basar, and R. Srikant, "Correlated jamming on MIMO gaussian fading channels," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 2119–2123, Sept. 2004.

[27] X. Zhou, D. Niyato, and A. Hjϕrungnes, "Optimizing training-based transmission against smart jamming," *IEEE Trans. Veh. Technol.*, vol. 60, no. 6, pp. 2644–2655, Jul. 2011.

[28] N. Zhao, J. Guo, F. R. Yu, M. Li, and V. C. M. Leung, "Antijamming schemes for interference-alignment-based wireless networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 1271–1283, Feb. 2017.

[29] J. Guo, N. Zhao, F. R. Yu, X. Liu, and V. C. M. Leung, "Exploiting adversarial jamming signals for energy harvesting in interference networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 2, pp. 1267–1280, Feb. 2017.

[30] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure massive MIMO transmission with an active eavesdropper," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3880–3900, Jul. 2016.

[31] 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.

[32] D. Darsena, G. Gelli, L. Paura, and F. Verde, "Widely linear equalization and blind channel identification for interference-contaminated multicarrier systems," *IEEE Trans. Signal Process.*, vol. 53, no. 3, pp. 1163–1177, Feb. 2005.

[33] D. Darsena, G. Gelli, L. Paura, and F. Verde, "A constrained maximum-SINR NBI-resistant receiver for OFDM systems," *IEEE Trans. Signal Process.*, vol. 55, no. 6, pp. 3032–3047, Jun. 2007.

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

[35] L. Ruan, V. K. N. Lau, and M. Z. Win, "Generalized interference alignment-part I: theoretical framework," *IEEE Trans. Signal Process.*, vol. 64, no. 10, pp. 2675–2687, Aug. 2015.

[36] L. Ruan, V. K. N. Lau, and M. Z. Win, "Generalized interference alignment-part II: application to wireless secrecy," *IEEE Trans. Signal Process.*, vol. 64, no. 10, pp. 2688–2701, Aug. 2015.

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

[38] Y. Zeng and R. Zhang, "Wireless information surveillance via proactive eavesdropping with spoofing relay," *IEEE Journal of Selected Topics in Signal Process.*, vol. 10, no. 8, pp. 1449–1461, Aug. 2016.

[39] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via cognitive jamming in fading channels," *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 2790–2806, May 2017.

Jing Guo (S'15) is currently a graduate student in the School of Information and Communication Engineering at Dalian University of Technology, China. She received the B.S. degree from China University of Geosciences, Beijing, China.

Her current research interests include interference alignment, physical layer security, energy harvesting, and resource allocation.

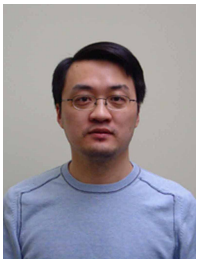
Nan Zhao (S'08-M'11-SM'16) is currently an Associate Professor in the School of Information and Communication Engineering at Dalian University of Technology, China. He received the B.S. degree in electronics and information engineering in 2005, the M.E. degree in signal and information processing in 2007, and the Ph.D. degree in information and communication engineering in 2011, from Harbin Institute of Technology, Harbin, China. His recent research interests include Interference Alignment, Cognitive Radio, Wireless Power Transfer, and Physical Layer Security. He has published more than 120 papers in refereed journals and international conferences.

Dr. Zhao is a senior member of the IEEE and a senior member of the Chinese Institute of Electronics. He is serving or served on the editorial boards of several journals, including Journal of Network and Computer Applications, IEEE ACCESS, Wireless Networks, Physical Communication, AEU-International Journal of Electronics and Communications, Ad Hoc & Sensor Wireless Networks, and KSII Transactions on Internet and Information Systems. He received Top Reviewer Award from IEEE Transactions on Vehicular Technology in 2016, and was nominated as an Exemplary Reviewer by IEEE Communications Letters in 2016. He won the best paper awards in IEEE VTC'2017-Spring and MLICOM 2017. Additionally, he served as a TPC member for many interferences, e.g., Globecom, ICC, VTC, ICCC, WCSP.

Zhutian Yang (M'13) received the M.E. degree in 2008 and Ph.D. degree in 2013 from Harbin Institute of Technology, China. He is currently working as an associate professor in Harbin Institute of Technology, and worked as a visiting research associate in King's College London, UK, in 2015. His current research interests include machine learning, signal processing, UWB communications, and smart city communications.

F. Richard Yu (S'00-M'04-SM'08) received the PhD degree in electrical engineering from the University of British Columbia (UBC) in 2003. From 2002 to 2006, he was with Ericsson (in Lund, Sweden) and a start-up in California, USA. He joined Carleton University in 2007, where he is currently a Professor. He received the IEEE Outstanding Service Award in 2016, IEEE Outstanding Leadership Award in 2013, Carleton Research Achievement Award in 2012, the Ontario Early Researcher Award (formerly Premiers Research Excellence Award) in 2011, the Excellent Contribution Award at IEEE/IFIP TrustCom 2010, the Leadership Opportunity Fund Award from Canada Foundation of Innovation in 2009 and the Best Paper Awards at IEEE ICC 2014, Globecom 2012, IEEE/IFIP TrustCom 2009 and Int'l Conference on Networking 2005. His research interests include cross-layer/cross-system design, security, green ICT and QoS provisioning in wireless-based systems.

He serves on the editorial boards of several journals, including Co-Editor-in-Chief for Ad Hoc & Sensor Wireless Networks, Lead Series Editor for IEEE Transactions on Vehicular Technology, and IEEE Transactions on Green Communications and Networking, IEEE Communications Surveys & Tutorials. He has served as the Technical Program Committee (TPC) Co-Chair of numerous conferences. Dr. Yu is a registered Professional Engineer in the province of Ontario, Canada, a Fellow of the Institution of Engineering and Technology (IET), and a senior member of the IEEE. He serves as a member of Board of Governors of the IEEE Vehicular Technology Society.



Yunfei Chen (S'02-M'06-SM'10) received his B.E. and M.E. degrees in electronics engineering from Shanghai Jiaotong University, Shanghai, P.R.China, in 1998 and 2001, respectively. He received his Ph.D. degree from the University of Alberta in 2006. He is currently working as an Associate Professor at the University of Warwick, U.K. His research interests include wireless communications, cognitive radios, wireless relaying and energy harvesting.

Victor C. M. Leung (S'75-M'89-SM'97-F'03) received the B.A.Sc. (Hons.) degree in electrical engineering from the University of British Columbia (UBC) in 1977, and was awarded the APEBC Gold Medal as the head of the graduating class in the Faculty of Applied Science. He attended graduate school at UBC on a Canadian Natural Sciences and Engineering Research Council Postgraduate Scholarship and received the Ph.D. degree in electrical engineering in 1982.

From 1981 to 1987, Dr. Leung was a Senior Member of Technical Staff and satellite system specialist at MPR Teltech Ltd., Canada. In 1988, he was a Lecturer in the Department of Electronics at the Chinese University of Hong Kong. He returned to UBC as a faculty member in 1989, and currently holds the positions of Professor and TELUS Mobility Research Chair in Advanced Telecommunications Engineering in the Department of Electrical and Computer Engineering. Dr. Leung has co-authored more than 1000 journal/conference papers, 37 book chapters, and co-edited 12 book titles. Several of his papers had been selected for best paper awards. His research interests are in the broad areas of wireless networks and mobile systems.

Dr. Leung is a registered Professional Engineer in the Province of British Columbia, Canada. He is a Fellow of IEEE, the Royal Society of Canada, the Engineering Institute of Canada, and the Canadian Academy of Engineering. He was a Distinguished Lecturer of the IEEE Communications Society. He is serving on the editorial boards of the IEEE Wireless Communications Letters, IEEE Transactions on Green Communications and Networking, IEEE Transactions on Cloud Computing, IEEE Access, Computer Communications, and several other journals, and has previously served on the editorial boards of the IEEE Journal on Selected Areas in Communications - Wireless Communications Series and Series on Green Communications and Networking, IEEE Transactions on Wireless Communications, IEEE Transactions on Vehicular Technology, IEEE Transactions on Computers, and Journal of Communications and Networks. He has guest-edited many journal special issues, and provided leadership to the organizing committees and technical program committees of numerous conferences and workshops. He received the IEEE Vancouver Section Centennial Award and 2011 UBC Killam Research Prize. He is the recipient of the 2017 Canadian Award for Telecommunications Research. He co-authored papers that won the 2017 IEEE ComSoc Fred W. Ellersick Prize and the 2017 IEEE Systems Journal Best Paper Award.