Secured Green Communication Scheme for Interference Alignment Based Networks

Zhibin Xie, Member, IEEE, Xinquan Geng, Yunfei Chen, Senior Member, IEEE, Kening Song, Benjamin Panful, Yajun Wang, Yinjie Su, Zhenkai Zhang, and Ying Hu

Abstract: **In this paper, a new security and green communication scheme is proposed to the interference-alignment (IA) based networks. To achieve a secured communication, full-duplex receivers are utilized to transmit artificial noise (AN). Both the signals and the ANs are used to harvest energy to realize green communication. For these reasons, the feasible conditions of this scheme are analyzed first. Secondly, the average transmission rate, the secrecy performance and the harvested energy are investigated. Thirdly, an optimization scheme of simultaneous wireless information and power transfer (SWIPT) is given to optimize the information transmission and the energy harvesting efficiency. Meanwhile, an improved IA iteration algorithm is designed to eliminate both the AN and the interference. Furthermore, relay cooperation is considered and its system performance is analyzed. The simulations show that the target average transmission rate is not affected by AN, while the secrecy performance can be greatly improved. The energy harvesting efficiency is also better than the traditional schemes. As expected, the average transmission rate further is improved with the relay cooperation.**

Index Terms: **Artificial noise (AN), eavesdropping, interference alignment (IA), relay, secrecy, simultaneous wireless information and power transfer (SWIPT)**

I. INTRODUCTION

THE broadcast characteristics of the wireless communication networks (WCNs) determine that it is an open communication environment. The sharing of its information medium leads to intricate electromagnetic radiation problems. Of these, multi-user interference, wireless transmission secrecy and radio signal enabled wireless power transfer are intensively discussed in these WCNs [1]–[3].

Interference exists widely in multi-user WCNs, and this affects multiplexing rate of time slots, frequencies, and code space, which severely limits the reusability of channel resources and reduces the spectrum of networks. It has become the bottleneck of system capacity enhancement. With the increase of users and data services in WCNs, conventional interference management methodologies either have difficulty in achieving good interference cancellation and suppression effects or have achieved the purpose of interference at the expense of network capacity. In recent years, the emergence of interference alignment (IA) technology has subverted the traditional understanding of the upper limit of communication network capacity in the academic community [4]–[6], and many researches have shown that IA can significantly improve the system's degree of freedom and can be applied to many kinds of multiuser WCNs with excellent performance [7], [8].

Also, personal privacy and security have become important requirement in the design of communication networks as a result of the growth of mobile data services. However, convenient wireless communications face more serious security problems than wired communications because, the open channel and the eavesdropping characteristics of the former are major security threats to wireless communication. Traditional cryptography-based privacy algorithms have been challenged with the development of high-performance processors. Hence, many efforts have been made to secure the communications.

The physical layer security is intended to limit the achievable information at the physical layer. In particular, the pioneering work at physical layer was firstly demonstrated by Wyner [8]. Subsequently, for realizing information security transfer, the physical layer security technology, notably artificial noise (AN), beamforming, and phase rotation were received much concern in different communication scenarios [10]–[28]. By utilizing the property of wireless channel and the idea of random coding, the information flow is hidden in the external noise in the eavesdropping channel, and as a result, the information cannot be obtained by the eavesdropper [10], [11]. In all kinds of methods, AN is an intuitive and effective method to realize communication security [12]–[14]. Beamforming can maximize the power of jamming signal to hide the desired signal from a potential eavesdropper, while maintaining a prespecified SINR at the desired receiver [15], [16], [19]. For eavesdropper with massive antenna, transmitters randomly rotate the phase of original symbols to interrupt eavesdropper, and the legitimate users are able to take proper inverse operations to recover the received signals [17]. As helper, relay can improve communication security in the presence of eavesdropper, especially when the source-destination channel is worse than the source-eavesdropper channel [18], [19], [23], [27], [52]. Besides that, some typical secure communication approaches are proposed for special network scenario, such as wireless ad-hoc network, ultra-dense network, social network and cognitive radio system [20]–[23]. In addi-

Z. Xie, X. Geng, B. Panful, Y. Wang, Y. Su, Z. Zhang, and Y. Hu are with the School of Electronic and Information, Jiangsu University of Science and Technology, Zhenjiang, China, email: xiezhibin@just.edu.cn, 1242633008@qq.com, juniorben77@gmail.com, wangyj1859@just.edu.cn, yinjiesu@just.edu.cn, zhangzhenkai@just.edu.cn, 75298303@qq.com.

Y. Chen is with the School of Engineering, University of Warwick, Coventry, UK, email: Yunfei.Chen@warwick.ac.uk.

K. Song is with the PLA AF 95829, Xiaogan, China, email: sking@163.com.

Digital Object Identifier: 10.1109/JCN.2019.000057

tion, full duplex receiver is a forthcoming technique which acts as a jammer and a receiver, and eliminates the need for external helpers and provides system robustness [24]–[28].

However, self-interference is one of the key challenges faced in designing practical full-duplex transceivers. Fortunately, we can use aforementioned IA-based network intrinsic property adequately, and combine many techniques have been developed to suppress the self-interference [25]. For secure communications, we adequately exploit IA network in this paper, and make use of AN to realize physical layer security. Our object is to investigate the achievable performance of the IA-based network. Whereas it is such a full of electromagnetic interference environment, we should consider the dual character of electromagnetic radiation further.

Since communications have been integrated into all aspects of our daily lives, the energy efficiency problem has become increasingly prominent in green WCNs [29], [30]. Especially, for wireless communications, effective energy supply is needed for all kinds of mobile terminals in mobile communication. Therefore, the concept of wireless powered communication (WPC) was raised [31], [32]. In fact, with the advent of collecting energy methods using radio frequency (RF) signals, WPC have caused extensive research and attention [33]–[42]. In these studies, the authors studied the sustainability analysis of WPC and the relation between interference and energy harvesting in [35]–[37]. Moreover, researchers found that the wireless power transfer process can be used in some wireless service such as secure wireless communications [16], [19], [38]–[42]. Motivated by these literature analyses, we believe that it is necessary to analyze the coexisting performance, which is the secure transmission for wireless information and power transfer in IA-based MIMO network using full-duplex jamming receivers.

In summary, the interference in a WCN is a mixed blessing [37], [43]–[46], [53]. In particular, for an IA-based network, the interferences can not only be used as energy source in [44], but also can be used to distract the eavesdropper in [45]. However, if antennas are equipped at the eavesdropper adequately, the inherent interference will still be eliminated. In order to ensure the security of information transmission, Ruan *et al.* proposed a scheme for IA-based network by utilizing jammers to transmit AN [47], [48]. On this basis, in [49], transmitters were used to transmit AN to achieve security, where the AN and signal from a certain user-pair are in the same channel. This scheme uses zero-forcing (ZF) of ANs and thus, it affects the designs of precoding and decoding, and reduces the transmission rate. Moreover, the improvement of the secrecy performance is not prominent, this is because that the ANs can also be eliminated by the eavesdropper except for target users. Thus far, although interference management, secure and green communication have had many excellent researches, the combination of the three areas is often ignored. Especially, with the rapid development of wireless communication technology in recent years, these three thorny problems are aggravated in the design of wireless communication systems. Thus, a thorough and comprehensive analysis of interference, security, and energy harvesting problems is of great significance.

In order to improve the anti-eavesdropping performance and energy harvesting efficiency in an IA-based network simultane-ously, in this paper, we propose a new scheme to achieve secure communication by using full-duplex receivers to transmit AN in an IA-based network, and to harvest the energies of signal and AN. The feasible conditions are analyzed. In the proposed scheme, since the AN and the signal from a certain user-pair are in the different channels and are independent of each other, the designs of precoding and decoding will not be affected by the ZF of ANs compared with previous work, and thus the average transmission rate are guaranteed. While the ANs from receivers cannot be eliminated by the eavesdropper and the anti-eavesdropping performance is improved. Also, the energy harvesting efficiency is improved by the introduced AN. Then, the relay technology is also considered for the proposed IA-based scheme based on AN transmitted by the receiver. After the relay node joins in the scheme, average transmission rate is further improved.

The main contributions of this paper are summarized as follows.

1) A new scheme is proposed to realize secure communication in an IA-based network. In this scheme, full-duplex receivers are used to transmit AN, the residual self-interference problem of full-duplex device is solved effectively by IA. Nevertheless, the AN cannot be eliminated at the eavesdropper.

2) The feasible conditions of IA and the anti-eavesdropping performance are analyzed. If IA is feasible, all the ANs transmitted by receivers can be used to disturb the eavesdropper, which can largely improve the secrecy performance.

3) An improved IA iteration algorithm is proposed in this paper, and the zero-forcing operation of the AN and the interference are simultaneously considered in the proposed algorithm.

4) An optimization scheme is proposed to optimize energy harvesting and information transmission.

5) System performance is analyzed after the relay node joins. The average transmission rate is obviously improved with the cooperation of relay.

Compared with previous work, the proposed scheme presents better secrecy transmission performance in the simulations. It is expected that overall performance will be significantly enhanced if the proposed scheme is widely adopted, because the performance of the IA-based network with limited nodes has been improved obviously. The rest of this paper is arranged as follows. In Section II, the system model is given, the feasible conditions of IA and the performance of the external eavesdropper in an IA-based network are analyzed later on, and the simultaneous wireless information and power transfer (SWIPT) analysis is also studied. In Section III, a new scheme is proposed to realize secure communication, similarly, the feasible conditions of IA and the performance of the external eavesdropper in this kind of IA-based network are analyzed, and an improved IA iteration algorithm is introduced. In Section IV, the SWIPT optimization method based on the proposed scheme is given. In Section V, we studied the relay technology and joined the relay in the proposed scheme, then introduced the IA iteration algorithm in the case of joining the relay node. In Section VI, we presented the simulation results and analyzed the performance of our proposed scheme. Finally, conclusions and further work are given in Section VII.

Notation:
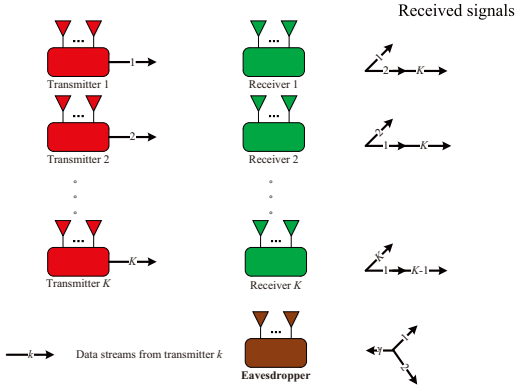
Fig. 1. K-user IA-based network with an external eavesdropper.

$(\cdot)^{\mathrm{H}}$ denotes conjugate transpose,

$V_i[\cdot]$ is the eigenvector which corresponds to the ith smallest eigenvalue of a matrix,

$(\cdot)_i$, $(\cdot)_{*i}$ are the ith column and the ith row of a matrix, respectively,

$\mathbb{C}^{N \times M}$ is a space of $N \times M$ matrices,

$\boldsymbol{I}_N$ is $N \times N$ identity matrix,

$\boldsymbol{0}_{M \times N}$ is $M \times N$ zero matrix.

II. SYSTEM MODEL

Consider a typical K-user IA-based network with an external eavesdropper as shown in Fig. 1. The eavesdropper only receives data, and thus legitimate users can not know the existence of eavesdropper.

A. Typical IA-Based Network

Assume that transmitter k has $M_{[k]}$ antennas and transmits $d_{[k]}$ data streams, receiver k has $N_{[k]}$ antennas, $k = 1, 2, 3, \cdots, K$. The signal at receiver k can be expressed as

$$
\begin{aligned}
\boldsymbol{y}_{[k]} =& \boldsymbol{U}_{[k]}^{\mathrm{H}} \boldsymbol{H}_{[kk]} \boldsymbol{V}_{[k]} \boldsymbol{x}_{[k]} \\
& + \sum_{j=1, j \neq k}^{K} \boldsymbol{U}_{[k]}^{\mathrm{H}} \boldsymbol{H}_{[kj]} \boldsymbol{V}_{[j]} \boldsymbol{x}_{[j]} + \boldsymbol{U}_{[k]}^{\mathrm{H}} \boldsymbol{n}_{[k]}, \quad (1)
\end{aligned}
$$

where $x_{[k]}$ is the signal vector containing $d_{[k]}$ data streams transmitted by transmitter k with power $P_{[k]}$, $\boldsymbol{V}_{[k]} \in \mathbb{C}^{M_{[k]} \times d_{[k]}}$ and $\boldsymbol{U}_{[k]} \in \mathbb{C}^{N_{[k]} \times d_{[k]}}$ are the unitary precoding matrix and unitary interference suppression matrix, respectively, so that $\boldsymbol{V}_{[k]}^{\mathrm{H}} \boldsymbol{V}_{[k]} = \boldsymbol{I}_{d_{[k]}}$, $\boldsymbol{U}_{[k]}^{\mathrm{H}} \boldsymbol{U}_{[k]} = \boldsymbol{I}_{d_{[k]}}$. Assume that the channel estimations are perfect for legitimate transceivers. $\boldsymbol{H}_{[kj]} \in \mathbb{C}^{N_{[j]} \times M_{[k]}}$ is the channel matrix from transmitter j to receiver k, and its elements follow independent and identically distributions, $\boldsymbol{n}_{[k]} \in {}^{N_{[k]} \times 1} \sim \mathcal{CN}\left(0, \sigma^2 \boldsymbol{I}_N\right)$ is the additive white Gaussian noise (AWGN) vector at receiver k.

In order to obtain the desired signal, it is necessary to eliminate all the interferences from other users, thus the following conditions must be satisfied.

$$
\boldsymbol{U}_{[k]}^{\mathrm{H}} \boldsymbol{H}_{[ki]} \boldsymbol{V}_{[i]} = \boldsymbol{0}_{d_{[k]} \times d_{[k]}}, \forall i \neq k, \quad (2)
$$

$$
\mathrm{rank}(\boldsymbol{U}_{[k]}^{\mathrm{H}} \boldsymbol{H}_{[kk]} \boldsymbol{V}_{[k]}) = d_{[k]}, \forall k = 1, 2, \cdots, K. \quad (3)
$$

When (2) and (3) are satisfied, we call the IA-based network feasible. The transmission rate of receiver k can be expressed as [44]

$$
R_{t[k]} = \log_2 \left| \boldsymbol{I}_d + \frac{1}{\sigma^2} \boldsymbol{U}_{[k]}^{\mathrm{H}} \boldsymbol{H}_{[kk]} \boldsymbol{V}_{[k]} \boldsymbol{S}_{[k]} \boldsymbol{V}_{[k]}^{\mathrm{H}} \boldsymbol{H}_{[kk]}^{\mathrm{H}} \boldsymbol{U}_{[k]} \right|, \quad (4)
$$

where $\boldsymbol{S}_{[k]}$ indicates the covariance matrix of the signal transmitted by transmitter k.

B. Feasible Conditions of IA

The feasible conditions of IA are analyzed in [50]. The IA-based network itself is equivalent to a polynomial system. For a polynomial system, it can be solved only when the number of variables is larger than or equal to the number of equations. Thus, the feasibility of an IA-based network usually depends on the number of antennas from each user and the number of data streams transmitted by transmitter. Here, we can directly utilize the conclusions about the number of equations and variables in [50].

That is, for an IA-based network shown in Fig. 1, the number of equations in (2) and (3) can be expressed as

$$
N_{\mathrm{E}} = \sum_{\substack{k, i \in \{1, 2, \cdots, K\} \\ k \neq i}} d_{[k]} d_{[i]}, \quad (5)
$$

The number of variables can be expressed as

$$
N_{\mathrm{V}} = \sum_{k=1}^{K} d_{[k]}(M_{[k]} + N_{[k]} - 2d_{[k]}). \quad (6)
$$

In order to simplify in this paper, all the parameters of the user are set to the same, that is, $M_{[k]} = M$, $N_{[k]} = N$, $d_{[k]} = d$, and $P_{[k]} = P$. If and only if $N_{\mathrm{V}} \geq N_{\mathrm{E}}$, IA is feasible, which is

$$
dK(M + N - 2d) \geq d^2 K(K - 1). \quad (7)
$$

After simplification, we can get

$$
d \leq \frac{M + N}{K + 1}. \quad (8)
$$

C. Eavesdropper

When an external eavesdropper with N_e antennas exists in the IA-based network as shown in Fig. 1, it is assumed that the channel state information (CSI) between transmitter and eavesdropper is known by the eavesdropper, but the CSI between transmitter and receiver is unknown. The received signals of target user k at the eavesdropper can be expressed as

$$
\begin{aligned}
\boldsymbol{y}_{e[k]} =& \boldsymbol{U}_{e[k]}^{\mathrm{H}} \boldsymbol{H}_{te[k]} \boldsymbol{V}_{[k]} \boldsymbol{x}_{[k]} \\
& + \sum_{j=1, j \neq k}^{K} \boldsymbol{U}_{e[k]}^{\mathrm{H}} \boldsymbol{H}_{te[j]} \boldsymbol{V}_{[j]} \boldsymbol{x}_{[j]} + \boldsymbol{U}_{e[k]}^{\mathrm{H}} \boldsymbol{n}_e, \quad (9)
\end{aligned}
$$

where $\boldsymbol{U}_{e[k]}$ is the decoding matrix at the eavesdropper, $\boldsymbol{H}_{te[k]}$ is the channel matrix from transmitter k to the eavesdropper, and

n_e is the AGWN vector at the eavesdropper. In order to obtain the information from the target user, the interferences from other users should be eliminated. That is, the following condition must be satisfied.

$$U_{\mathrm{e}[k]}^{\mathrm{H}} H_{\mathrm{te}[j]} V_{[j]} = \mathbf{0}_{1 \times d}, \forall j \neq k. \tag{10}$$

Therefore, the number of antennas at the eavesdropper must meet Proposition 1 proposed in [49]. Assume that enough antennas are equipped at the eavesdropper, although the eavesdropper can eliminate the interferences from other users, the interference between data streams from the target user still exists. Thus, (9) can be re-expressed as

$$\begin{aligned} y_{\mathrm{e}[k]} &= U_{\mathrm{e}[k]}^{\mathrm{H}} H_{\mathrm{te}[k]} V_{[k]} x_{[k]} + U_{\mathrm{e}[k]}^{\mathrm{H}} n_{\mathrm{e}} \\ &= \sum_{i=1}^{d} U_{\mathrm{e}[k]}^{\mathrm{H}} H_{\mathrm{te}[k]} (V_{[k]})_i (x_{[k]})_i + U_{\mathrm{e}[k]}^{\mathrm{H}} n_{\mathrm{e}}. \end{aligned} \tag{11}$$

Then, the eavesdropping rate of user k at the eavesdropper can be expressed as

$$\begin{aligned} &R_{\mathrm{e}[k]} \\ &= \sum_{i=1}^{d} \log_2 (1 \\ &+ \frac{U_{\mathrm{e}[k]}^{\mathrm{H}} H_{\mathrm{te}[k]} (V_{[k]})_i S_{[k]} (V_{[k]})_i^{\mathrm{H}} H_{\mathrm{te}[k]}^{\mathrm{H}} U_{\mathrm{e}[k]}}{\sigma^2 + \sum_{j=1, j \neq i}^{d} U_{\mathrm{e}[k]}^{\mathrm{H}} H_{\mathrm{te}[k]} (V_{[k]})_j S_{[k]} (V_{[k]})_j^{\mathrm{H}} H_{\mathrm{te}[k]}^{\mathrm{H}} U_{\mathrm{e}[k]}}). \end{aligned} \tag{12}$$

D. SWIPT Analysis

For the IA-based network as shown in Fig. 1, power splitting (PS) scheme and antenna selection (AS) scheme can be applied to harvest energy.

1) *PS scheme*: The idea of power splitting refers to that the received signal at the receiver is divided into two parts after passing through the power splitting device: One part is used for information transmission, and the other part is used for energy harvesting. In this mode, the transmitter's information and energy are transmitted at the same time, frequency, and space resources.

2) *AS scheme*: In energy harvesting networks, AS scheme can be considered as a special case of PS schemes. At the receivers with multiple antennas, the energy harvesting and information transmission are implemented on different antennas, and a part of the antenna is selected for energy harvesting. The remaining antennas are used for information transmission.

III. PROPOSED SECURE COMMUNICATION SCHEME

A. IA-Based Network with AN Transmitted by Receiver

Using transmitters to transmit AN decreases transmission rate, because the AN and signal from a certain user-pair are in the same channel. In order to ensure the performance of rate and secrecy simultaneously, we propose a new scheme which uses full-duplex receivers to transmit AN in IA-based network,
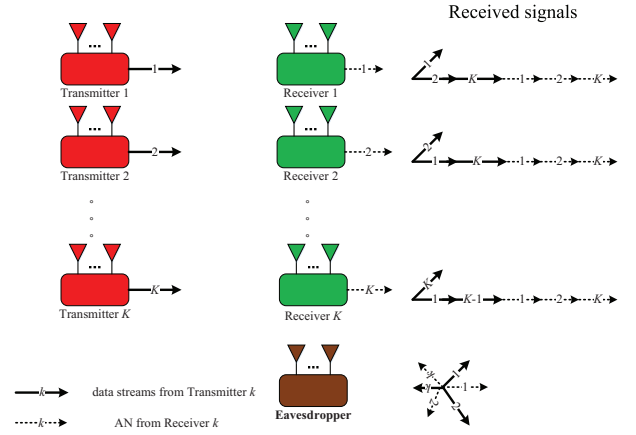

Fig. 2. K-user IA-based network of AN transmitted by receiver with an external eavesdropper.

as shown in Fig. 2. Assume that $z_{[k]}$ is the AN vector containing $d_{\mathrm{an}[k]}$ data streams transmitted by receiver k with transmission power $P_{\mathrm{an}[k]}$, $H_{\mathrm{r}[kj]} \in \mathbb{C}^{N_{[k]} \times N_{[j]}}$ is the channel matrix from receiver j to receiver k, and follows independent and identically Rayleigh distribution, and the channel estimations between receiver and receiver are also perfect. Thus, the received signals at receiver k is

$$\begin{aligned} y_{[k]} &= U_{[k]}^{\mathrm{H}} H_{[kk]} V_{[k]} x_{[k]} + \sum_{j=1, j \neq k}^{K} U_{[k]}^{\mathrm{H}} H_{[kj]} V_{[j]} x_{[j]} \\ &+ \sum_{j=1, j \neq k}^{K} U_{[k]}^{\mathrm{H}} H_{\mathrm{r}[kj]} V_{\mathrm{an}[j]} z_{[j]} \\ &+ U_{[k]}^{\mathrm{H}} H_{\mathrm{r}[kk]} V_{\mathrm{an}[k]} z_{[k]} + U_{[k]}^{\mathrm{H}} n_{[k]}, \end{aligned} \tag{13}$$

where $V_{\mathrm{an}[k]} \in \mathbb{C}^{N_{[k]} \times d_{\mathrm{an}[k]}}$ is the unitary precoding matrix of AN at receiver k, and $V_{\mathrm{an}[k]}^{\mathrm{H}} V_{\mathrm{an}[k]} = I_{d_{\mathrm{an}[k]}}$.

To obtain the desired signal at receiver k, the following conditions should be satisfied simultaneously

$$\begin{aligned} &U_{[k]}^{\mathrm{H}} H_{[kj]} V_{[j]} = \mathbf{0}_{d_{[k]} \times d_{[k]}}, \forall j \neq k, \\ &\mathrm{rank}(U_{[k]}^{\mathrm{H}} H_{[kk]} V_{[k]}) = d_{[k]}, \forall k = 1, 2, \cdots, K, \\ &U_{[k]}^{\mathrm{H}} H_{\mathrm{r}[kj]} V_{\mathrm{an}[j]} = \mathbf{0}_{d_{[k]} \times d_{\mathrm{an}[k]}}, \forall j, k = 1, 2, \cdots, K. \end{aligned} \tag{14}$$

In order to simplify, several parameters of the users are set to the same from now on, that is, $d_{\mathrm{an}[k]} = d_{\mathrm{an}}$ and $P_{\mathrm{an}[k]} = P_{\mathrm{an}}$. Since the IA-based network is equivalent to a polynomial system [50], if an IA-based network shown in Fig. 2 is feasible, it should meet Lemma 1.

Lemma 1: For the proposed scheme, in order to make IA feasible, the numbers of antenna and data stream must satisfy

$$\begin{aligned} &dM + (d + d_{\mathrm{an}})N \geq d^2 + d_{\mathrm{an}}^2 + d^2 K + dd_{\mathrm{an}}K, \\ &d \leq M \cap d \leq N. \end{aligned} \tag{15}$$

Proof: The number of variables in (14) can be expressed as

$$C_{\mathrm{V}} = dK(M + N - 2d) + d_{\mathrm{an}}K(N - d_{\mathrm{an}}), \tag{16}$$

and the number of equations can be expressed as

$$C_{\mathrm{E}} = d^2 K(K - 1) + dd_{\mathrm{an}} K^2. \tag{17}$$

Thus, from $C_{\mathrm{V}} \geq C_{\mathrm{E}}$, one has

$$dM + (d + d_{\mathrm{an}})N \geq d^2 + d_{\mathrm{an}}^2 + d^2 K + dd_{\mathrm{an}} K. \tag{18}$$

Also, the number of information data streams cannot be greater than the number of antennas at the receiver and the transmitter. That is,

$$d \leq M \bigcap d \leq N. \tag{19}$$

Therefore, if the IA-based network is feasible, it must satisfy (18) and (19). ∎

Since the radio link resources are usually more valuable than energy resources, it is reasonable to set the number of AN data streams as 1, Thus, (18) can be rewritten as

$$dM + (d + 1)N \geq d^2 K + dK + d^2 + 1. \tag{20}$$

Also, considering that the AN transmitted by receiver and the signal transmitted by transmitter are through independent channels, the ZF operations of AN won't affect the precoding matrix $\boldsymbol{V}$ and decoding matrix $\boldsymbol{U}$. Thus, after IA is performed, the transmission rate of receiver k can be expressed as

$$R_{\mathrm{t}[k]} = \log_2 \left| \boldsymbol{I}_d + \frac{1}{\sigma^2} \boldsymbol{U}_{[k]}^{\mathrm{H}} \boldsymbol{H}_{[kk]} \boldsymbol{V}_{[k]} \boldsymbol{S}_{[k]} \boldsymbol{V}_{[k]}^{\mathrm{H}} \boldsymbol{H}_{[kk]}^{\mathrm{H}} \boldsymbol{U}_{[k]} \right|. \tag{21}$$

When the CSI between receiver and eavesdropper is unknown at the eavesdropper, the most appropriate way of the receiver is to send Gaussian white noise with the same band of transmitting signal. Thus, the received signals at the eavesdropper can be rewritten as

$$\boldsymbol{y}_{\mathrm{e}[k]} = \boldsymbol{U}_{\mathrm{e}[k]}^{\mathrm{H}} \boldsymbol{H}_{\mathrm{te}[k]} \boldsymbol{V}_{[k]} \boldsymbol{x}_{[k]} + \sum_{j=1, j \neq k}^{K} \boldsymbol{U}_{\mathrm{e}[k]}^{\mathrm{H}} \boldsymbol{H}_{\mathrm{te}[j]} \boldsymbol{V}_{[j]} \boldsymbol{x}_{[j]} \tag{22}$$

$$+ \sum_{j=1}^{K} \boldsymbol{U}_{\mathrm{e}[k]}^{\mathrm{H}} \boldsymbol{H}_{\mathrm{re}[j]} \boldsymbol{V}_{\mathrm{an}[j]} \boldsymbol{z}_{[j]} + \boldsymbol{U}_{\mathrm{e}[k]}^{\mathrm{H}} \boldsymbol{n}_{\mathrm{e}},$$

where $\mathbf{H}_{\mathrm{re}[k]} \in \mathbb{C}^{N_{\mathrm{e}} \times N}$ is the channel matrix from receiver k to the eavesdropper. Although the feasible condition of eavesdropper in Fig. 2 which looks like the appearance of Proposition 1 in [49], we have to state Lemma 2 for the proposed scheme, because the new model induces an extra AN term in (22), which makes eavesdropper unable to eradicate the AN from other users and thus improves secrecy performance.

Proposition 1: Consider an IA-based network which satisfies (18) and (19) as shown in Fig. 2, the interferences from other users can be eliminated at the eavesdropper, if at least $(dK - d + 1)$ antennas are used at the eavesdropper.

$Proof$: In order to cancel the second term of (22), the total number of equations can be expressed as

$$C_{\mathrm{E}}^{\mathrm{e}} = d(K - 1). \tag{23}$$

As the precoding matrices are determined by the legitimate transmitters in the network, the number of variables can be expressed as

$$C_{\mathrm{V}}^{\mathrm{e}} = N_{\mathrm{e}} - 1. \tag{24}$$

According to Lemma 1, the eavesdropper considers its IA feasible only when

$$N_{\mathrm{e}} \geq dK - d + 1. \tag{25}$$

Here, since the AN transmitted by receiver is just white noise, the CSI between receiver and eavesdropper will not be estimated at the eavesdropper and the ANs cannot be eliminated. Thus, the interference covariance matrix estimated by the eavesdropper can be expressed as

$$\boldsymbol{Q}_{\mathrm{e}[k]} \approx \sum_{j=1, j \neq k}^{K} \frac{P}{d} \boldsymbol{H}_{\mathrm{te}[j]} \boldsymbol{V}_{[j]} \boldsymbol{V}_{[j]}^{\mathrm{H}} \boldsymbol{H}_{\mathrm{te}[j]}^{\mathrm{H}}, \tag{26}$$

and the decoding matrix at the eavesdropper can be expressed as

$$\boldsymbol{U}_{\mathrm{e}[k]} = V_1[\boldsymbol{Q}_{\mathrm{e}[k]}], \tag{27}$$

where $V_1[\cdot]$ is the eigenvector which corresponds to the first smallest eigenvalue of matrix $Q_{e[k]}$.

After the interferences from other users are eliminated, the remaining signal at the eavesdropper is

$$\boldsymbol{y}_{\mathrm{e}[k]} = \sum_{i=1}^{d} \boldsymbol{U}_{\mathrm{e}[k]}^{\mathrm{H}} \boldsymbol{H}_{\mathrm{te}[k]} (\boldsymbol{V}_{[k]})_i (\boldsymbol{x}_{[k]})_{*i} \tag{28}$$

$$+ \sum_{j=1}^{K} \boldsymbol{U}_{\mathrm{e}[k]}^{\mathrm{H}} \boldsymbol{H}_{\mathrm{re}[j]} \boldsymbol{V}_{\mathrm{an}[j]} \boldsymbol{z}_{[j]} + \boldsymbol{U}_{\mathrm{e}[k]}^{\mathrm{H}} \boldsymbol{n}_{\mathrm{e}}.$$

Then, the eavesdropping rate of user k can be expressed as (29). From (29) we can see that all the ANs from receivers can be used to distract the eavesdropper and the eavesdropping rate can be decreased by increasing the transmission power of AN to make secure communications possible.

$$R_{\mathrm{e}[k]} = \sum_{i=1}^{d} \log_2 \left(1 + \frac{\boldsymbol{U}_{\mathrm{e}[k]}^{\mathrm{H}} \boldsymbol{H}_{\mathrm{te}[k]} (\boldsymbol{V}_{[k]})_i \boldsymbol{S}_{[k]} (\boldsymbol{V}_{[k]})_i^{\mathrm{H}} \boldsymbol{H}_{\mathrm{te}[k]}^{\mathrm{H}} \boldsymbol{U}_{\mathrm{e}[k]}}{\sigma^2 + \sum\limits_{j=1, j \neq i}^{d} \boldsymbol{U}_{\mathrm{e}[k]}^{\mathrm{H}} \boldsymbol{H}_{\mathrm{te}[k]} (\boldsymbol{V}_{[k]})_j \boldsymbol{S}_{[k]} (\boldsymbol{V}_{[k]})_j^{\mathrm{H}} \boldsymbol{H}_{\mathrm{te}[k]}^{\mathrm{H}} \boldsymbol{U}_{\mathrm{e}[k]} + P_{an} \sum\limits_{s=1}^{K} \boldsymbol{U}_{\mathrm{e}[k]}^{\mathrm{H}} \boldsymbol{H}_{\mathrm{re}[k]} (\boldsymbol{V}_{\mathrm{an}[k]})_i (\boldsymbol{V}_{\mathrm{an}[k]})_i^{\mathrm{H}} \boldsymbol{H}_{\mathrm{re}[k]}^{\mathrm{H}} \boldsymbol{U}_{\mathrm{e}[k]}} \right) \tag{29}$$

B. Iterative Algorithm

For full-duplex devices, the self-interference is an annoying thing. In order to solve self-interference problem, antenna can-

cellation, radio frequency offset, and digital signal processing can be used to reduce the self-interference to an acceptable level, then we propose an improved iterative IA algorithm to

---

Algorithm 1: IA iteration algorithm with AN transmitted by receiver.

1. Initialize the precoding matrix $\boldsymbol{V}_{[j]}$ and $\boldsymbol{V}_{\mathrm{an}[j]}$,
   $j = 1, 2, \cdots, K$.
2. Begin iteration.
3. Calculate the interference covariance matrix $\boldsymbol{Q}_{[k]}$, which contains both interference of other users and ANs
$$\boldsymbol{Q}_{[k]} = \sum_{i=1,i\neq k}^{K} \boldsymbol{H}_{[ki]}\boldsymbol{V}_{[i]}\boldsymbol{S}_{[i]}\boldsymbol{V}_{[i]}^{\mathrm{H}}\boldsymbol{H}_{[ki]}^{\mathrm{H}} + \sum_{j=1}^{K} P_{\mathrm{an}}\boldsymbol{H}_{\mathrm{r}[kj]}\boldsymbol{V}_{\mathrm{an}[j]}\boldsymbol{V}_{\mathrm{an}[j]}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{r}[kj]}^{\mathrm{H}}.$$
4. Calculate the decoding vector $\boldsymbol{U}_{[k]}$,
   $\boldsymbol{U}_{[k]} = [(\boldsymbol{U}_{[k]})_1, (\boldsymbol{U}_{[k]})_2, \cdots, (\boldsymbol{U}_{[k]})_d], k = 1, 2, \cdots, K,$
   $(\boldsymbol{U}_{[k]})_i = V_i[\boldsymbol{Q}_{[k]}], i = 1, 2, \cdots, d; k = 1, 2, \cdots, K.$
5. Set $\overleftarrow{\boldsymbol{V}}_{[k]}$ as the precoding matrix in the reciprocity network,
   $\overleftarrow{\boldsymbol{V}}_{[k]} = \boldsymbol{U}_{[k]}, k = 1, 2, \cdots, K.$
6. Calculate the interference covariance matrix in the reciprocity network $\overleftarrow{\boldsymbol{Q}}_{[k]}$ and $\overleftarrow{\boldsymbol{Q}}_{\mathrm{w}[k]}$,
$$\overleftarrow{\boldsymbol{Q}}_{[k]} = \sum_{i=1,i\neq k}^{K} \overleftarrow{\boldsymbol{H}}_{[ki]}\overleftarrow{\boldsymbol{V}}_{[i]}\boldsymbol{S}_{[i]}\overleftarrow{\boldsymbol{V}}_{[i]}^{\mathrm{H}}\overleftarrow{\boldsymbol{H}}_{[ki]}^{\mathrm{H}},$$
$$\overleftarrow{\boldsymbol{Q}}_{\mathrm{w}[k]} = \sum_{j=1}^{K} \overleftarrow{\boldsymbol{H}}_{\mathrm{r}[kj]}\overleftarrow{\boldsymbol{V}}_{[j]}\boldsymbol{S}_{[j]}\overleftarrow{\boldsymbol{V}}_{[j]}^{\mathrm{H}}\overleftarrow{\boldsymbol{H}}_{\mathrm{r}[kj]}^{\mathrm{H}}.$$
7. Calculate the decoding matrix $\overleftarrow{\boldsymbol{U}}_{[k]}$ in the reciprocity network,
   $\overleftarrow{\boldsymbol{U}}_{[k]} = [(\overleftarrow{\boldsymbol{U}}_{[k]})_1, (\overleftarrow{\boldsymbol{U}}_{[k]})_2, \cdots, (\overleftarrow{\boldsymbol{U}}_{[k]})_d], k = 1, 2, \cdots, K,$
   $(\overleftarrow{\boldsymbol{U}}_{[k]})_i = V_i[\overleftarrow{\boldsymbol{Q}}_{[k]}], i = 1, 2, \cdots, d; k = 1, 2, \cdots, K.$
8. Calculate the precoding matrix of AN $\boldsymbol{V}_{\mathrm{an}[k]}$,
   $\boldsymbol{V}_{\mathrm{an}[k]} = V_1[\overleftarrow{\boldsymbol{Q}}_{\mathrm{w}[k]}], k = 1, 2, \cdots, K.$
9. Reverse the direction, and set $\overleftarrow{\boldsymbol{U}}_{[k]}$ as the precoding matrix $\boldsymbol{V}_{[k]}$.
10. Calculate the interference leakage, if the difference between this iteration and the last iteration is less than the threshold, the interference leakage convergence and end the iteration. Otherwise, return to step 3.

---

align the interference of the other users, the remaining self-interference and the AN into the interference space. As in [51], we consider a reciprocal network in this section to implement the IA-based communication in Fig. 2. Each user aims at minimizing their own interference leakage. For user k, its interference leakage is $I_{\mathrm{e}[k]} = \mathrm{trace}\left(\boldsymbol{U}_{[k]}^{\mathrm{H}}\boldsymbol{Q}_{[k]}\boldsymbol{U}_{[k]}\right)$ where $\boldsymbol{Q}_{[k]}$ is the interference covariance matrix of user k. The pseudocode of the proposed iterative algorithm is as Algorithm 1 where $\overleftarrow{\boldsymbol{H}}_{[ij]} = \boldsymbol{H}_{[ji]}^{\mathrm{H}}, \overleftarrow{\boldsymbol{H}}_{\mathrm{r}[ij]} = \boldsymbol{H}_{\mathrm{r}[ji]}^{\mathrm{H}}$, and $\overleftarrow{\boldsymbol{V}}_{[k]} = \boldsymbol{U}_{[k]}$. Similarly to [51], the proposed iterative algorithm also is convergent. However, if residual self-interference exists, the proposed algorithm needs more iterations compared with [49].

IV. SWIPT OPTIMIZATION SCHEME WITH AN

Energy efficiency is a key factor to be considered in green communication network. Especially, in the proposed scheme, the AN can be used not only for physical layer security but also for energy harvesting. Consequently, in order to improve the energy efficiency and transmission rate for proposed scheme, SWIPT optimization is presented in this section.

A. Conventional SWIPT Scheme

For the multi-user MIMO system shown in Fig. 1, we firstly discuss the conventional SWIPT scheme based on [3], [49].

1) *AS scheme*: Assuming that each receiver is equipped with N antennas, and L antennas are selected for information decoding, the remaining antennas are used to harvest energy, and L must satisfy $(L + M) \geq (K + 1)d$.
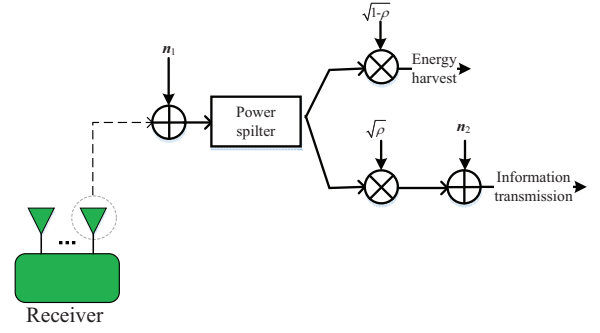

Fig. 3. Power splitting device model.

For information transmission, we assume that the interference can be completely eliminated by IA, the transmission rate of receiver k can be expressed as
$$R_{\mathrm{AS}[k]} = \log_2\left|\boldsymbol{I}_d + \frac{1}{\sigma^2}\boldsymbol{U}_{[k]}^{\mathrm{H}}\boldsymbol{D}_{[kk]}\boldsymbol{V}_{[k]}\boldsymbol{S}_{[k]}\boldsymbol{V}_{[k]}^{\mathrm{H}}\boldsymbol{D}_{[kk]}^{\mathrm{H}}\boldsymbol{U}_{[k]}\right|, \tag{30}$$
where $\boldsymbol{D}_{[ki]} \in \mathbb{C}^{L \times M}$ is the channel matrix for information transmission from transmitter i to receiver k, which is composed of L rows of $\boldsymbol{H}_{ki}$.

In terms of energy harvesting, since the remaining antennas are used to harvest energy, assuming that $\boldsymbol{F}_{[ki]} \in \mathbb{C}^{(N-L) \times M}$ is the channel matrix for energy harvesting from transmitter i to receiver k, which is composed of the remaining $N - L$ rows of $\boldsymbol{H}_{ki}$. The energy harvested by receiver k can be expressed as
$$E_{\mathrm{AS}[k]} = \mu\mathrm{Tr}\left[\sum_{i=1}^{K} \left(\boldsymbol{F}_{[ki]}\boldsymbol{V}_{[i]}\boldsymbol{S}_{[i]}\boldsymbol{V}_{[i]}^{\mathrm{H}}\boldsymbol{F}_{[ki]}^{\mathrm{H}}\right)\right], \tag{31}$$
where μ is the loss of energy converted to electrical energy during energy harvesting and is a constant.

Since each receiver selects L antennas for information transmission, there exists $\left(C_N^L\right)^K$ antenna combining modes. For a certain scenario, there has to be a unique combination to make the AS scheme optimal. Assume that all CSI is known at the receiver, the optimization problem can be expressed as
$$\max_{\boldsymbol{S}_1,\cdots,\boldsymbol{S}_K} \sum_{k=1}^{K} \left[\alpha_k R_{\mathrm{AS}[k]} + (1 - \alpha_k)\beta E_{\mathrm{AS}[k]}\right]$$
$$\text{s.t. } \mathrm{Tr}\left(\boldsymbol{S}_k\right) = \mathrm{P}, k = 1, \cdots, K, \tag{32}$$
$$\boldsymbol{S}_k \geq 0, k = 1, \cdots, K,$$
where $0 \leq \alpha_k \leq 1$ is the power configuration weights for information transmission at receiver k. β is a constant in a unit of bit/Joule. For a given α_k, the above optimization problem can be divided into K independent subspace problems,
$$\max_{\boldsymbol{S}_k} \alpha_k R_{\mathrm{AS}[k]} + (1 - \alpha_k)\beta E_{\mathrm{AS}[k]}, k = 1, \cdots, K$$
$$\text{s.t. } \mathrm{Tr}\left(\boldsymbol{S}_k\right) = P, \boldsymbol{S}_k \geq 0. \tag{33}$$

It can be found that for receiver k, the above optimization problem is a convex problem that can be solved by convex optimization.

2) *PS scheme*: We assume that each antenna of each receiver can simultaneously harvest energy and transmit information through a power splitting device, and the power splitting device is as shown in Fig. 3, where $\boldsymbol{n}_1 \in \mathbb{C}^{N \times 1} \sim \mathcal{CN}(0, \sigma_1{}^2\boldsymbol{I}_N)$

and $\boldsymbol{n}_2 \in \mathbb{C}^{N \times 1} \sim \mathcal{CN}(0, \sigma_2{}^2 \boldsymbol{I}_N)$ denote the path noise and antenna noise of the receiver respectively, and ρ is the splitting ratio. Specifically, let $\rho_{[kj]}$ denote the power distribution ratio for information transmission at the jth antenna of receiver $k, 0 \le \rho_{kj} \le 1, k = 1, 2, \cdots, K; j = 1, 2, \cdots, N$.

In terms of information transmission, the transmission rate of receiver k can be expressed as

$$
\begin{aligned}
R_{\mathrm{PS}[k]} = \log_2 \Big| \boldsymbol{I}_d &+ \boldsymbol{U}_{[k]}^{\mathrm{H}} \boldsymbol{C}_{[k]}^{1/2} \boldsymbol{Q}_{1[k]} \boldsymbol{C}_{[k]}^{1/2} \boldsymbol{U}_{[k]} \left(\boldsymbol{U}_{[k]}^{\mathrm{H}} \right. \\
&\times \left. \left(\boldsymbol{C}_{[k]}^{1/2} \left(\sigma_1^2 \boldsymbol{I}_N + \boldsymbol{Q}_{2[k]} \right) \boldsymbol{C}_{[k]}^{1/2} + \sigma_2^2 \boldsymbol{I}_N \right) \boldsymbol{U}_{[k]} \right)^{-1} \Big|,
\end{aligned}
\tag{34}
$$

where $\boldsymbol{C}_{[k]} = \mathrm{diag}\left(\rho_{[k1]}, \rho_{[k2]}, \cdots, \rho_{[kN]}\right)$ is the power distribution diagonal for information transmission of all the antennas at receiver k. When it is equal power distribution among different antennas at receiver k, the $\boldsymbol{C}_{[k]}$ can be rewritten as

$$
\boldsymbol{C}_{[k]} = \mathrm{diag}\left(\rho_{[k]}, \rho_{[k]}, \cdots, \rho_{[k]}\right),
$$

$$
\boldsymbol{Q}_{1[k]} = \boldsymbol{H}_{[kk]} \boldsymbol{V}_{[k]} \boldsymbol{S}_{[k]} \boldsymbol{V}_{[k]}^{\mathrm{H}} \boldsymbol{H}_{[k]}^{\mathrm{H}},
$$

$$
\boldsymbol{Q}_{2[k]} = \sum_{l=1, l \ne K}^{\bar{K}} \boldsymbol{H}_{[kl]} \boldsymbol{V}_{[l]} \boldsymbol{S}_{[l]} \boldsymbol{V}_{[l]}^{\mathrm{H}} \boldsymbol{H}_{[kl]}^{\mathrm{H}}.
$$

If the interference is complete alignment, (34) can be rewritten as

$$
\begin{aligned}
&R_{\mathrm{PS}[k]} \\
&= \log_2 \left| \boldsymbol{I}_d + \frac{\rho}{\rho \sigma_1^2 + \sigma_2^2} \boldsymbol{U}_{[k]}^{\mathrm{H}} \boldsymbol{H}_{[kk]} \boldsymbol{V}_{[k]} \boldsymbol{S}_{[k]} \boldsymbol{V}_{[k]}^{\mathrm{H}} \boldsymbol{H}_{[kk]}^{\mathrm{H}} \boldsymbol{U}_{[k]} \right|.
\end{aligned}
\tag{35}
$$

In terms of energy harvesting, the harvested energy at receiver k can be expressed as

$$
E_{\mathrm{PS}[k]} = \mu \mathrm{Tr} \left(\sum_{i=1}^{K} \bar{\boldsymbol{C}}_{[k]} (\boldsymbol{H}_{[ki]} \boldsymbol{V}_{[i]} \boldsymbol{S}_{[i]} \boldsymbol{V}_{[i]}^{\mathrm{H}} \boldsymbol{H}_{[ki]}^{\mathrm{H}}) \right),
\tag{36}
$$

where $\bar{\boldsymbol{C}}_{[k]} = \boldsymbol{I}_N - \boldsymbol{C}_{[k]}$. There is also a unique power allocation ratio for a scenario to make the PS scheme optimal. Therefore, its optimization problem can be expressed as

$$
\begin{aligned}
\max_{\boldsymbol{C}_1, \cdots, \boldsymbol{C}_{[K]}} &\sum_{k=1}^{K} \left(\alpha_k R_{\mathrm{PS}[k]} + (1 - \alpha_k) \beta E_{\mathrm{PS}[k]} \right) \\
\text{s.t.} \quad &0 \le \rho_{[k]} \le 1, k = 1, \cdots, K.
\end{aligned}
\tag{37}
$$

Similarly, the above problem can be decomposed into K independent subspace problems, and then the convex optimization methods can be used to find the optimal solution.

B. New SWIPT Optimization Scheme with AN

For the proposed scheme model as shown in Fig. 2, we consider SWIPT optimization algorithm to harvest the energy both from signals and ANs simultaneously. Because radio link resource is more expensive, we only adopt the PS scheme to optimal energy harvesting and information transmission in this section.

Algorithm 2: Interior point optimization method.

1. Construct a penalty function $\varphi\left(\rho, r\right) = f\left(\rho\right) - r \ln \left(\frac{1-\rho}{\rho}\right)$.
2. Initialize the penalty factor $r_{[0]} > 0$ and $\rho_{[0]}$, set $m = 1$.
3. Start with $\rho_{[m-1]}$ and calculate the extreme point of the penalty function $\varphi\left(\rho, r\right)$ with the unconstrained optimization method.
4. Determine if $\left\| \rho^*\left(r_{[m]}\right) - \rho^*\left(r_{[m-1]}\right) \right\| \le \varepsilon = 10^{-5} \sim 10^{-7}$ is satisfied. If it is satisfied, then obtain the optimal solution and end the iteration. Otherwise, go to step 5.
5. Set $r_{[m+1]} = c r_{[m]}, \rho_{[m]} = \rho^*\left(r_{[m]}\right), m = m + 1$, and take the decrement factor $c = 0.1$, repeat step 3.

Under this condition, the interference-free transmission rate at receiver k is

$$
\begin{aligned}
&R_{\mathrm{PS}[k]} \\
&= \log_2 \left| \boldsymbol{I}_d + \frac{\rho}{\rho \sigma_1^2 + \sigma_2^2} \boldsymbol{U}_{[k]}^{\mathrm{H}} \boldsymbol{H}_{[kk]} \boldsymbol{V}_{[k]} \boldsymbol{S}_{[k]} \boldsymbol{V}_{[k]}^{\mathrm{H}} \boldsymbol{H}_{[kk]}^{\mathrm{H}} \boldsymbol{U}_{[k]} \right|.
\end{aligned}
\tag{38}
$$

Because there are ANs, the harvested energy at receiver k is

$$
\begin{aligned}
E_{\mathrm{PS}[k]} = \mu \mathrm{Tr} \Bigg[\sum_{i=1}^{K} \bar{\boldsymbol{C}}_{[k]} \boldsymbol{H}_{[ki]} \boldsymbol{V}_{[i]} &\left(\boldsymbol{S}_{[i]} \boldsymbol{V}_{[i]}^{\mathrm{H}} \boldsymbol{H}_{[ki]}^{\mathrm{H}} \right. \\
&\left. + \boldsymbol{H}_{\mathrm{an}[ki]} \boldsymbol{V}_{\mathrm{an}[i]} \boldsymbol{S}_{\mathrm{an}[i]} \boldsymbol{V}_{\mathrm{an}[i]}^{\mathrm{H}} \boldsymbol{H}_{\mathrm{an}[ki]}^{\mathrm{H}} \right) \Bigg].
\end{aligned}
\tag{39}
$$

Thus, the optimization problem can be described as

$$
\begin{aligned}
\max_{\boldsymbol{C}_1, \cdots, \boldsymbol{C}_{[K]}} &\sum_{k=1}^{K} \left[\alpha_k R_{\mathrm{PS}[k]} + (1 - \alpha_k) \beta E_{\mathrm{PS}[k]} \right] \\
\text{s.t.} \quad &0 \le \rho_{[k]} \le 1, k = 1, \cdots, K.
\end{aligned}
\tag{40}
$$

The objective function (40) can be decomposed into subobjective functions of K independent subspaces. The power distribution index is henceforth suppressed to avoid cumbersome notation, therefore, the kth sub-objective function can be expressed as

$$
\begin{aligned}
f\left(\rho\right) &= \alpha_k R_{\mathrm{PS}[k]} + (1 - \alpha_k) \beta E_{\mathrm{PS}[k]} \\
\text{s.t.} \quad &0 \le \rho \le 1.
\end{aligned}
\tag{41}
$$

The optimal power distribution ratio ρ can be solved according to the interior point method. The optimization algorithm is as Algorithm 2.

V. PERFORMANCE IMPROVEMENT SCHEME

A. Relay Cooperation for IA-Based Network with AN Transmitted by Receiver

For an IA-based network, in order to realize IA, each user of the network must know all the CSI, greatly increasing the complexity of the network. However, when relay cooperation joins in IA-based network, the network only needs the relay node to get the global CSI. Moreover, the system performance can also be improved with the cooperation of relay. Considering the excellent characteristics of relay cooperation in IA-based networks, we proposed an IA-based network model with relay cooperation based on AN transmitted by receiver, as shown in Fig. 4. The K-user relay-cooperative MIMO system consists
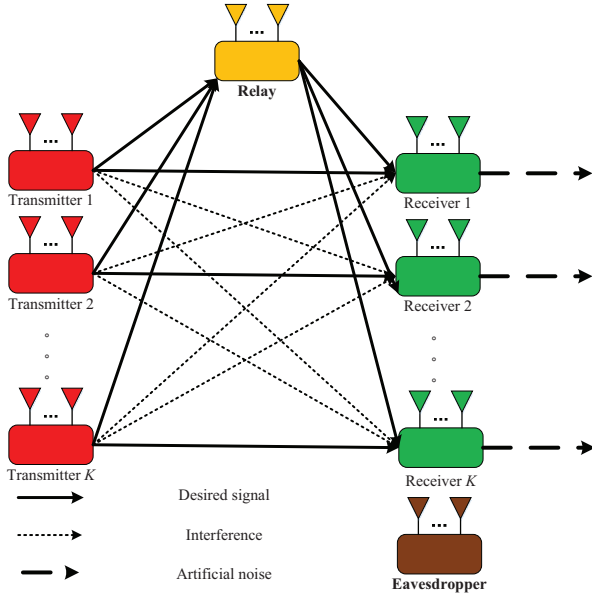
Fig. 4. Relay cooperation for IA-based network with AN transmitted by receiver.

of K user-pair and a half-duplex relay node, where the number of antennas at transmitters and receivers are M and N, respectively. The number of data streams is d, and the number of AN is 1. The number of antennas of the relay node is R, the working mode of the relay node is forward amplification, and the $d \leq R$. Here, we take the two-slot transmission method by time-division duplex. In Fig. 4, the solid lines indicate useful signals, the thicker dashed lines indicate artificial noises, and the dashed lines indicate interference signals. Assume $\boldsymbol{H}_{[ri]}(t) \in \mathbb{C}^{R \times M}$ is the channel matrix from transmitter i to the relay node, $\boldsymbol{H}_{[ir]}(t) \in \mathbb{C}^{N \times R}$ is the channel matrix form the relay node to receiver i, $\boldsymbol{H}_{[ji]}(t) \in \mathbb{C}^{N \times M}$ is the channel matrix from transmitter i to receiver j, and $t = 1, 2$ represents the time slot. Assume that the channel coefficients are independent and identically distributed.

In the first time slot, the transmitter sends signal, and the full-duplex receiver sends AN. Then, the received signals at receiver k and relay node can be expressed as

$$\boldsymbol{y}_{[k]}(1) = \sum_{i=1}^{K} \boldsymbol{H}_{[ki]}(1)\boldsymbol{x}_{[i]}(1) + \sum_{j=1}^{K} \boldsymbol{H}_{r[kj]}(1)\boldsymbol{z}_{[j]}(1) + \boldsymbol{n}_{[k]}(1),$$
(42)

$$\boldsymbol{y}_r(1) = \sum_{i=1}^{K} \boldsymbol{H}_{[ri]}(1)\boldsymbol{x}_{[i]}(1) + \sum_{j=1}^{K} \boldsymbol{H}_{r[rj]}(1)\boldsymbol{z}_{[j]}(1) + \boldsymbol{n}_{[r]}(1),$$
(43)

where $\boldsymbol{H}_{r[ki]}(t) \in \mathbb{C}^{N \times N}$ is the channel matrix from receiver i to receiver k, $\boldsymbol{H}_{r[ri]}(t) \in \mathbb{C}^{R \times N}$ is the channel matrix from receiver i to the relay node, $\boldsymbol{z}_{[i]}(t)$ is the AN transmitted by receiver i. In the second time slot, the relay node forwards the

received signal, the transmitter still sends the signal in the second time slot, and the receiver still sends AN. At this time, the received signal at receiver k in the second time slot can be expressed as

$$\boldsymbol{y}_{[k]}(2) = \sum_{i=1}^{K} \boldsymbol{H}_{[ki]}(2)\boldsymbol{x}_{[i]}(2) + \sum_{i=1}^{K} \boldsymbol{H}_{r[ki]}(2)\boldsymbol{z}_{[i]}(2)$$
$$+ \boldsymbol{H}_{[kr]}\boldsymbol{y}_r(1) + \boldsymbol{n}_{[k]}(2).$$
(44)

Superimposing the signals of the first and the second time slot at receiver k, and the matrix form of the superimposed signals can be expressed as

$$\boldsymbol{Y}_{[k]} = \bar{\boldsymbol{H}}_{[kk]}\boldsymbol{X}_{[k]}$$
$$+ \sum_{i=1,i\neq k}^{K} \bar{\boldsymbol{H}}_{[ki]}\boldsymbol{X}_{[i]} + \sum_{j=1}^{K} \bar{\boldsymbol{H}}_{r[kj]}\boldsymbol{Z}_{[k]} + \boldsymbol{N}_{[k]},$$
$$k = 1, 2, \cdots, K,$$
(45)

where $\boldsymbol{Z}_{[k]} = [\boldsymbol{z}_{[k]}(1), \boldsymbol{z}_{[k]}(2)]^{\mathrm{T}}$,
$\bar{\boldsymbol{H}}_{r[ki]} = \begin{bmatrix} \boldsymbol{H}_{r[ki]}(1) & \boldsymbol{0} \\ \boldsymbol{H}_{[kr]}(2)\boldsymbol{H}_{r[ri]}(1) & \boldsymbol{H}_{r[ki]}(2) \end{bmatrix}$,
and $\boldsymbol{N}_{[k]} = \begin{bmatrix} \boldsymbol{n}_{[k]}(1) \\ \boldsymbol{H}_{[kr]}(2)\boldsymbol{n}_{[r]}(1) + \boldsymbol{n}_{[k]}(2) \end{bmatrix}$.

If $\boldsymbol{U}_{[k]}$ is the interference suppression matrix of receiver k, the final achieved transmission rate of receiver k is

$$R_{\mathrm{t}[k]} = \log_2 \left| \boldsymbol{I}_d + \frac{P}{d\sigma^2} \left(\boldsymbol{U}_{[k]}^{\mathrm{H}} \bar{\boldsymbol{H}}_{[kk]} \boldsymbol{V}_{[k]} \boldsymbol{V}_{[k]}^{\mathrm{H}} \bar{\boldsymbol{H}}_{[kk]}^{\mathrm{H}} \boldsymbol{U}_{[k]} \right) \right|.$$
(46)

Similarly, when there is an external eavesdropper in the proposed relay assisted scheme, the received 1st time slot signal of target user k at eavesdropper is

$$\boldsymbol{y}_{e[k]}(1) = \sum_{i=1}^{K} \boldsymbol{G}_{e[i]}(1)\boldsymbol{x}_{[i]}(1) + \sum_{j=1}^{K} \boldsymbol{G}_{r[j]}\boldsymbol{z}_{[j]}(1) + \boldsymbol{n}_{e[k]}(1).$$
(47)

The received 2nd time slot signal of target user k at eavesdropper is

$$\boldsymbol{y}_{e[k]}(2) = \sum_{i=1}^{K} \boldsymbol{G}_{e[i]}(2)\boldsymbol{x}_{[i]}(2) + \sum_{j=1}^{K} \boldsymbol{G}_{r[j]}(2)\boldsymbol{z}_{[j]}(2)$$
$$+ \boldsymbol{G}_{re}\boldsymbol{y}_r(1) + \boldsymbol{n}_e(2),$$
(48)

where $\boldsymbol{G}_{e[k]} \in \mathbb{C}^{N_e \times M}$ is the channel matrix from the kth transmitter to eavesdropper, $\boldsymbol{G}_{r[k]} \in \mathbb{C}^{N_e \times N}$ is the channel matrix from the kth receiver to eavesdropper, $\boldsymbol{G}_{re} \in \mathbb{C}^{N_e \times R}$ is channel coefficient matrix between relay node and eavesdropper. The reachable eavesdropping transmission rate is (49).

$$R_{e[k]} = \sum_{i=1}^{d} \log_2(1 + \frac{\sum\limits_{t=1}^{2} \boldsymbol{U}_{e[k]}^{\mathrm{H}}(t)\boldsymbol{G}_{e[k]}(t)(\boldsymbol{V}_{[k]}(t))_i \boldsymbol{S}_{[k]}(t)(\boldsymbol{V}_{[k]}(t))_i^{\mathrm{H}}\boldsymbol{G}_{e[k]}^{\mathrm{H}}(t)\boldsymbol{U}_{e[k]}(t)}{\sigma^2 + \sum\limits_{t=1}^{2}\sum\limits_{j=1,j\neq i}^{d} \boldsymbol{U}_{e[k]}^{\mathrm{H}}(t)\boldsymbol{G}_{e[k]}(t)(\boldsymbol{V}_{[k]}(t))_j \boldsymbol{S}_{[k]}(t)(\boldsymbol{V}_{[k]}(t))_j^{\mathrm{H}}\boldsymbol{G}_{e[k]}^{\mathrm{H}}(t)\boldsymbol{U}_{e[k]}(t) + P_{an}\sum\limits_{t=1}^{2}\sum\limits_{k=1}^{K} \boldsymbol{U}_{e[k]}^{\mathrm{H}}(t)\boldsymbol{G}_{r[k]}(t)(\boldsymbol{W}_{[k]}(t))_i (\boldsymbol{W}_{[k]}(t))_i^{\mathrm{H}}\boldsymbol{G}_{r[k]}^{\mathrm{H}}(t)\boldsymbol{U}_{e[k]}(t)}).$$
(49)

Algorithm 3: IA iteration algorithm with AN transmitted by receiver and relay cooperation.

---

1. Initialize the precoding matrix of two time slots
   $\boldsymbol{V}_{[k]} = [\boldsymbol{v}_{[k]}(1), \boldsymbol{v}_{[k]}(2)]^{\mathrm{T}}$ and $\boldsymbol{W}_{[k]} = [\boldsymbol{w}_{[k]}(1), \boldsymbol{w}_{[k]}(2)]^{\mathrm{T}}$
   $k = 1, 2, \cdots, K$.
2. Begin iteration.
3. Calculate the interference covariance matrix of each
   receiver on the downlink$\boldsymbol{Q}_{[k]} = [\boldsymbol{Q}_{[k]}(1), \boldsymbol{Q}_{[k]}(2)]^{\mathrm{T}}$.
4. Calculate the interference suppression matrix of the two
   time slots
   $\boldsymbol{u}_{[k]}(t) = [(\boldsymbol{u}_{[k]}(t))_1, (\boldsymbol{u}_{[k]}(t))_2, \cdots, (\boldsymbol{u}_{[k]}(t))_d],$
   $\quad k = 1, 2, \cdots, K; t = 1, 2$
   $(\boldsymbol{u}_{[k]}(t))_i = V_i[\boldsymbol{Q}_{[k]}(t)],$
   $\quad i = 1, 2, \cdots, d; k = 1, 2, \cdots, K; t = 1, 2$
5. According to the reciprocity of the channel, set
   $\boldsymbol{u}_{[k]}(1), \boldsymbol{u}_{[k]}(2)$ of $\boldsymbol{U}_{[k]}$ as the precoding matrix of two time
   slots on the uplink $\overleftarrow{\boldsymbol{V}}_{[k]} = [\boldsymbol{u}_{[k]}(1), \boldsymbol{u}_{[k]}(2)]^{\mathrm{T}}$.
6. Calculate the interference covariance matrix sum for each
   receiver on the uplink $\overleftarrow{\boldsymbol{Q}}_{[k]} = [\overleftarrow{\boldsymbol{Q}}_{[k]}(1), \overleftarrow{\boldsymbol{Q}}_{[k]}(2)]^{\mathrm{T}}$ and
   $\overleftarrow{\boldsymbol{Q}}_{\mathrm{w}[k]} = [\overleftarrow{\boldsymbol{Q}}_{\mathrm{w}[k]}(1), \overleftarrow{\boldsymbol{Q}}_{\mathrm{w}[k]}(2)]^{\mathrm{T}}$.
7. Calculate the interference suppression matrix of the two
   time slots on the uplink
   $\overleftarrow{\boldsymbol{u}}_{[k]}(t) = [(\overleftarrow{\boldsymbol{u}}_{[k]}(t))_1, (\overleftarrow{\boldsymbol{u}}_{[k]}(t))_2, \cdots, (\overleftarrow{\boldsymbol{u}}_{[k]}(t))_d],$
   $\quad k = 1, 2, \cdots, K; t = 1, 2$
   $(\overleftarrow{\boldsymbol{u}}_{[k]}(t))_i = V_i[\overleftarrow{\boldsymbol{Q}}_{[k]}], i = 1, 2, \cdots, d;$
   $\quad k = 1, 2, \cdots, K; t = 1, 2$
8. Calculate the precoding matrix for AN of two time slots,
   $\boldsymbol{w}_{[k]}(t) = V_1[\overleftarrow{\boldsymbol{Q}}_{\mathrm{w}[k]}(t)], k = 1, 2, \cdots, K; t = 1, 2.$
9. Reverse the direction, and set $\overleftarrow{\boldsymbol{U}}_{[k]}$ as the precoding matrix.
10. Calculate the interference leakage, if the difference
    between this iteration and the last iteration is less than the
    threshold, the interference leakage convergence and end the
    iteration. Otherwise, return to step 3.

B. Iterative Algorithm

Firstly, the self-interference problem of the full duplex receiver can be reduced to an acceptable degree by means of antenna cancellation, radio frequency cancellation or digital signal processing cancellation. Then, the precoding matrix and the interference cancellation matrix in both two time slots are designed simultaneously by the improved distributed IA algorithm. Assuming $\boldsymbol{V}_{[k]}$, $\boldsymbol{W}_{[k]}$, and $\boldsymbol{U}_{[k]}$ are the precoding matrix at transmitter k, the AN precoding matrix and interference suppression matrix at receiver k, respectively.

Since the space formed by the eigenvectors corresponding to the dth smallest eigenvalues of the interference covariance matrix of user k is a subspace containing the least leakage, the eigenvector corresponding to the dth smallest eigenvalues of the interference covariance matrix can be used as the interference cancellation matrix. The pseudo-code of the improved iterative algorithm is as Algorithm 3.

C. Optimization

Similarly to the proposed scheme without relay cooperation, the power split is adopted in this section. The transmission rate at receiver k is

$$
\begin{aligned}
&R_{\mathrm{PS}[k]} \\
&= \log_2 \left| \boldsymbol{I}_d + \frac{\rho}{\rho\sigma_1^2 + \sigma_2^2} \left(\boldsymbol{U}_{[k]}^{\mathrm{H}} \bar{\boldsymbol{H}}_{[kk]} \boldsymbol{V}_{[k]} \boldsymbol{S}_{[k]} \boldsymbol{V}_{[k]}^{\mathrm{H}} \bar{\boldsymbol{H}}_{[kk]}^{\mathrm{H}} \boldsymbol{U}_{[k]} \right) \right|.
\end{aligned}
\tag{50}
$$

The transmission rate and harvested energy at receiver k is

$$
E_{\mathrm{PS}[k]} = \mu \mathrm{Tr} \left(\sum_{i=1}^{K} \bar{\boldsymbol{C}}_{[k]} \left(\bar{\boldsymbol{H}}_{[ki]} \boldsymbol{X}_{[i]} + \bar{\boldsymbol{H}}_{r[kj]} \boldsymbol{Z}_{[k]} \right) \right). \tag{51}
$$

Therefore, the optimization problem can be modeled as

$$
\begin{aligned}
\max_{\boldsymbol{C}_1, \cdots, \bar{\boldsymbol{C}}_{[K]}} & \sum_{k=1}^{K} \left(\alpha_k R_{\mathrm{PS}[k]} + (1 - \alpha_k)\beta E_{\mathrm{PS}[k]} \right) \\
\text{s.t. } & 0 \leq \rho_{[k]} \leq 1, k = 1, \cdots, K.
\end{aligned}
\tag{52}
$$

Because the objective function is sub-objective of K independent subspaces, the solving process of the optimal solution is similar to the Algorithm 2, and thus it is not repeated here.

VI. SIMULATIONS AND ANALYSIS

For the simulation, we set $K = 5$, $d = 2$, $M = 9$, $N = 4$, and assume that the eavesdropper is equipped with enough antennas and $N_e = 13$. All the channels suffer from slow Rayleigh block fading. For the PS scheme, let the transmitting power of the transmitter $P = 30$ dBm, constants $\mu = 0.5$, $\beta = 10^{-3}$, and the antenna noise and processing noise have the same distributions and are respectively set as [3]. Assuming that all users have the same power distribution ratio, $\alpha_{[k]} = \alpha, k = 1, 2, \cdots, K$. For the IA-based network with relay cooperation, assume that the number of antennas at the relay node is $R = 10$. For the comparison of the proposed two schemes with and without relay cooperation, we set the transmitting power as P and $2P$ at the transmitters for them, respectively. In the following simulations, the average of the system sum rate is written as average transmission rate for short.

Fig. 5(a) shows the average transmission rate of the proposed scheme with different transmission powers of AN. From Fig. 5(a), one can see that the average transmission rates of legitimate user are almost same when P_{an} equals P or P_{an} equals $5P$. Because the AN and the signal from the certain user-pair are independent, it makes the ZF of the AN separable. Thus, the ANs transmitted by receivers don't affect the transmission rate. Also, from Fig. 5(b), one can see that the eavesdropping rate at the eavesdropper decreases when the transmission power of AN increases. It means that the secrecy performance can be actually improved by increasing the power of AN, while the average transmission rate of legitimate user can be maintained.

Fig. 6(a) shows the average transmission rate of three different schemes, where $P_{an} = P$. From Fig. 6(a), one sees that the average transmission rate in the proposed scheme is the same as in the IA-based network without ANs. Both average transmission rates of the two schemes are larger than the IA-based network with ANs transmitted by transmitters. The growth of the average transmission rate using the proposed scheme has not been influenced, because the AN and the signal are independent. In other words, the average transmission rate of the scheme using transmitter to transmit AN is affected by ZF, and thus is lower than the other two schemes.

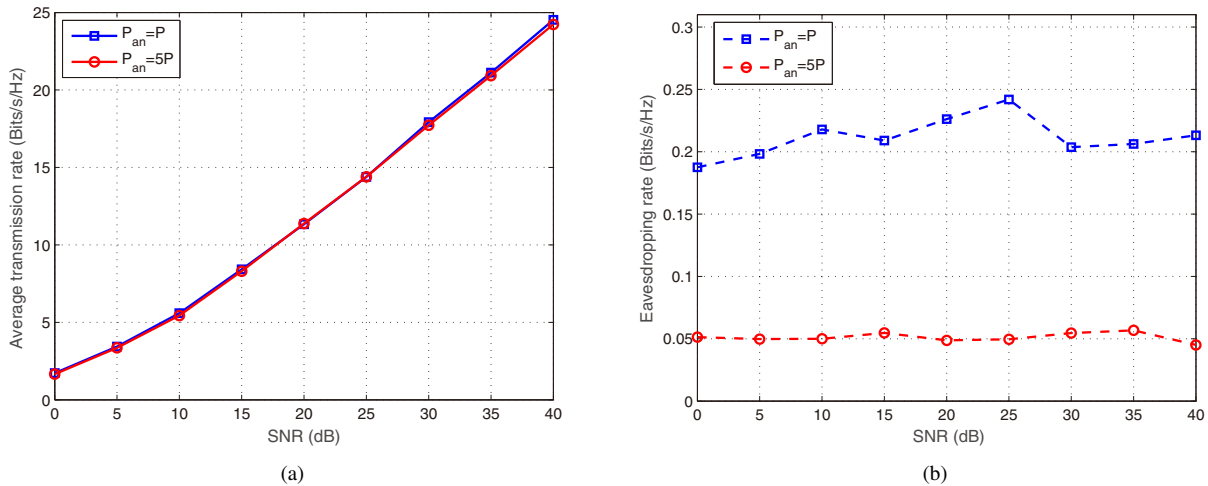The eavesdropping rate at the eavesdropper is presented in

Fig. 5. (a) Average transmission rate for different SNRs, when $P_{\text{an}} = P$ or $P_{\text{an}} = 5P$ and (b) eavesdropping rate for different SNRs, when $P_{\text{an}} = P$ or $P_{\text{an}} = 5P$.
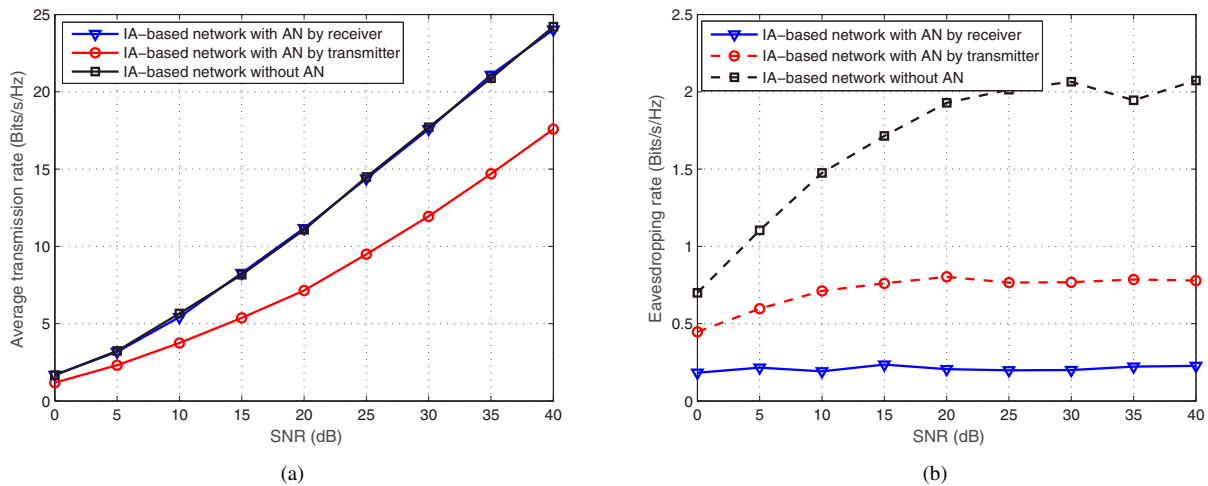

Fig. 6. (a) Average transmission rate in the three different schemes and (b) eavesdropping rate in the three different schemes.

Fig. 6(b). For high SNR, one sees that the eavesdropping rate of the IA-based network without AN is close to 2 bits/s/Hz, although it does not have the CSI between the eavesdropper and the receiver. In the IA-based network with AN transmitted by transmitter, its eavesdropping rate is about 0.8 bits/s/Hz and higher than that of the proposed scheme. For the proposed scheme, because the eavesdropper does not know the CSI between the eavesdropper and the receiver, all the ANs can be used to disturb the eavesdropper. Therefore, its eavesdropping rate is less than 0.25 bits/s/Hz.

It must be pointed out that the average transmission rate is the average value of all the user's transmission rate, while the secrecy rate is defined as the difference between the transmission rate and the eavesdropping rate. If we are concerned about the secrecy rate, combining Figs. 6(a) and 6(b), we can see that the secrecy rate in our proposed scheme is the highest. Thus, the proposed scheme is much securer than the other two.

Fig. 7 shows the average harvested energy and transmission rate in the three different schemes. The x-axis is the bm for in-

formation transmission. In Fig. 7(a), the bigger harvested energy means the higher harvesting efficiency. For energy harvesting efficiency, due to the addition of AN, the harvested energy is significantly higher than the IA-based network without AN. It can be predicted that the harvested energy performance can be already improved well in the proposed scheme with limited nodes, then the overall performance could be significantly improved if the proposed scheme is used in a large scale network. Regarding to the average transmission rate, one can see that the result in Fig. 7(b) is similar to the result in Fig. 6(a). The reason is the AN and the signal are independent in the proposed scheme, and hence the growth of the average transmission rate is similar to the scheme without AN and better than the scheme with AN transmitted by the transmitter.

Fig. 8 represents the change of the average transmission rate and the eavesdropping rate in our proposed scheme, before and after the relay node joins. From Fig. 8(a), one can see that the average transmission rate is greatly improved after the relay node joins in the network. The higher the transmission power (i.e.,
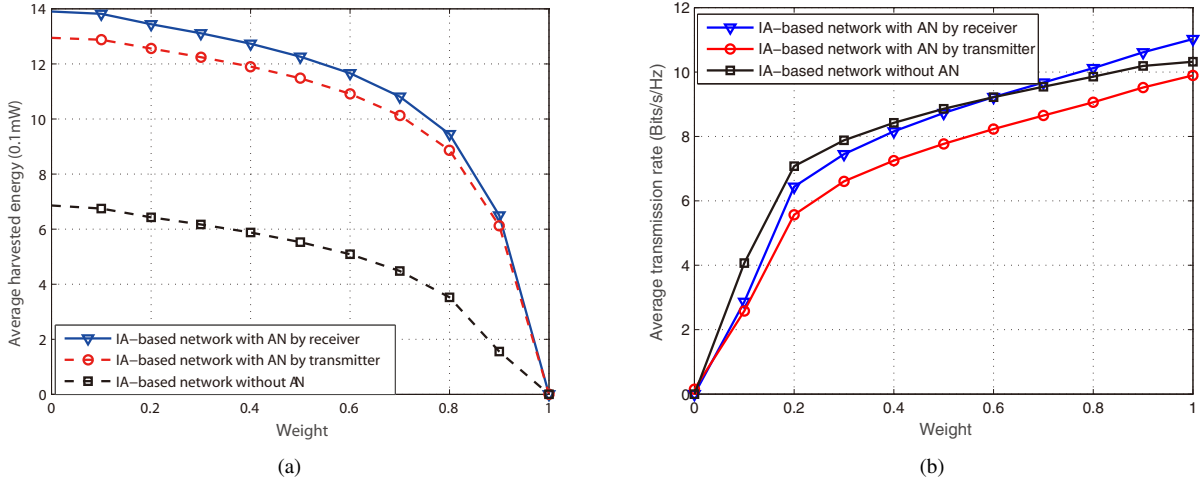
(a)

(b)

Fig. 7. (a) Average harvested energy in the three different schemes and (b) average transmission rate in the three different schemes.
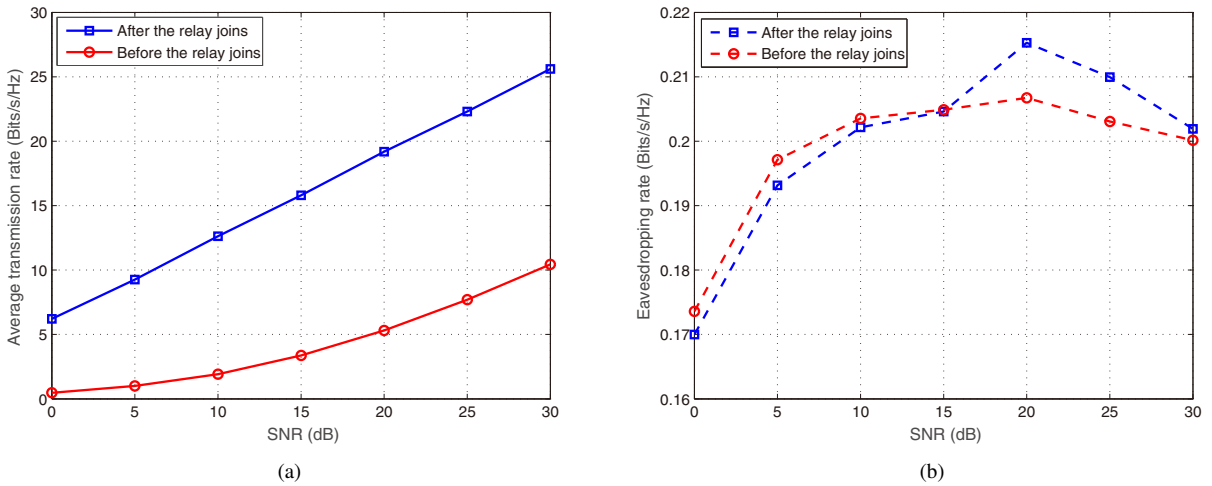

(a)

(b)

Fig. 8. (a) Average transmission rate with and without relay cooperation and (b) eavesdropping rate with and without relay cooperation.

the signal to noise ratio), the more obvious the superiority of the relay, and the more obvious the growth of the average transmission rate. In Fig. 8(b), whether or not the relay node joins in, the eavesdropping rate is similar in the two schemes. That is to say, the eavesdropper is unable to improve its performance using relay node, and is still jammed by the AN.

Fig. 9 shows the average transmission rate and harvested energy of the proposed schemes with relay and without relay co-operation. Along with the increase of the bm for information transmission, both the two average transmission rates rise in Fig. 9(a). Especially, the proposed relay cooperation scheme has better rate performance. For the average harvested energy in Fig. 9(b), the harvested energy of the relay cooperation scheme is higher than the scheme without relay. It is because the re-ceived signal contains the signal sent by the transmitter, the ar-tificial noise and the signal sent by relay node. Therefore, the relay cooperation scheme has better harvesting efficiency.

VII. CONCLUSION

The security and the green communications are two important aspects in designing WCNs. In this paper, we investigated the potential performance of IA-based network. Based on the pro-posed scheme, we drew several conclusions that IA-based net-work can get satisfied rate by using full-duplex receiver. That is, the anti-eavesdropping performance are obviously improved while the transmission rate isn't affected. Compared with trans-mitting AN by transmitter, it avoids the co-channel of AN and desired signal for certain user-pair. The purpose-designed IA scheme can mitigate remaining self-interference of full-duplex receiver effectively. In addition, we proposed a new PS scheme to improve the energy harvesting efficiency of the IA-based net-work, which is fraught with electromagnetic wave. Finally, we also studied a more realistic relay scheme to get an improved transmission rate and harvesting energy in the IA-based net-work. It shows an encouraging result that the performance of IA-based network can be fully exploited in future communica-tion network with elaborate design, and also the tradeoff be-
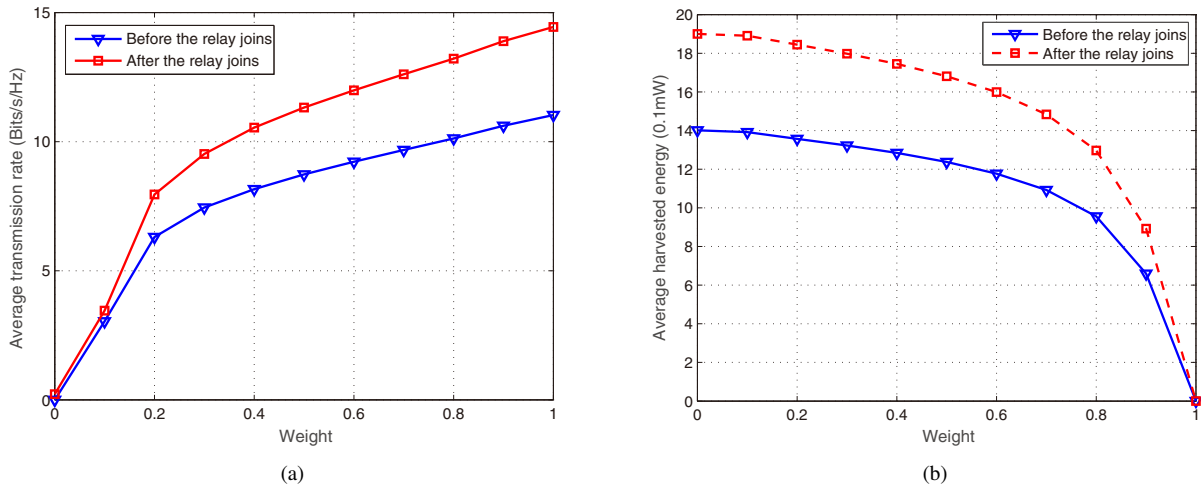
(a)

(b)

Fig. 9. (a) Average transmission rate of the proposed schemes in the different weights and (b) average harvested energy of the proposed schemes in the different weights.

tween security and reliability deserves attention and investigation in following works.

REFERENCES

[1] D. Gesbert *et al.*, "Multi-cell MIMO cooperative networks: A new look at interference," *IEEE J. Sel. Areas Commun.*, vol. 28, no. 9, pp. 1380–1408, 2010.

[2] M. Bloch and J. Barros, "Physical-layer security: From information theory to security engineering," *Cambridge University Press*, 2011.

[3] R. Zhang and C. K. Ho, "MIMO broadcasting for simultaneous wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 1989–2001, May 2013.

[4] S. A. Jafar and S. Shamai, "Degrees of freedom region for the MIMO x channel. mathematics," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 151–170, 2006.

[5] 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, 2008.

[6] T. Gou and S. A. Jafar, "Degrees of freedom of the K user M N MIMO interference channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 6040–6057, 2008.

[7] C. Huang and S. A. Jafar, "Degrees of freedom of the MIMO interference channel with cooperation and cognition," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4211–4220, 2009.

[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, third-quarter, 2016.

[9] A. D. Wyner, "The wire-tap channel," Bell System Technical J., vol. 54, no. 8, pp. 1355–1387, 1975.

[10] M. R. Bloch and J. N. Laneman, "Strong secrecy from channel resolvability," *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 8077–8098, 2013.

[11] H. D. Ly, T. Liu, and Y. Liang, "Multiple-input multiple-output gaussian broadcast channels with common and confidential messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4215–4227, 2010.

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

[13] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis," *IEEE Commun. Letters*, pp. 1628–1631, Oct. 2012.

[14] H. Wang, T. Zheng, and X. Xia, "Secure MISO wiretap channels with multiantenna passive eavesdropper: Artificial noise vs. artificial fast fading," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 94–106, Jan. 2015.

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

[16] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4599–4615, Aug. 2014.

[17] B. Chen *et al.*, "Original symbol phase rotated secure transmission against powerful massive MIMO eavesdropper," *IEEE Access*, vol. 4, pp. 3016–3025, July 2016.

[18] Y. L. Dong, Z. Han, A. P. Petropulu, and H. V.Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[19] Y. Feng, Z. Yang, W. Zhu, Q.Li, and B. Lv, "Robust cooperative secure beamforming for simultaneous wireless information and power transfer in amplify-and-forward relay networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2354–2366, Mar. 2017.

[20] M. Kamel, W. Hamouda, and A. Youssef, "Physical layer security in ultra-dense networks," *IEEE Wireless Communications Letters*, vol.6, no. 5, pp. 690–693, Oct. 2017.

[21] Y. Gao *et al.*, "Physical layer security in 5G based large scale social networks: Opportunities and challenges," *IEEE Access*, vol. 6, pp. 26350–26357, May 2018.

[22] M. K. Kiskani and H. Sadjadpour, "A secure approach for caching contents in wireless ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 11, pp. 10249–10258, Sept. 2017.

[23] H. A. Shah and I. Koo, "A novel physical layer security scheme in OFDM-based cognitive radio networks," *IEEE Access*, vol. 6, pp. 29486–29498, June 2018.

[24] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.

[25] A. Sabharwal, P. Schniter, D. Guo, D. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless: Challenges and opportunities," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 9, pp. 1637–1652, Sept. 2014.

[26] Y. Zhou, Z. Z. Xiang, Y. Zhu, and Z. Xue, "Application of full-duplex wireless technique into secure MIMO communication achievable secrecy rate based optimization," *IEEE Signal Letter*, vol. 21, no. 7, pp.804–808, July 2014.

[27] J. H. Lee, "Full-duplex relay for enhancing physical layer security in multi-hop relaying system," *IEEE Commun. Letters*, vol. 19, no. 4, pp.525–528, Apr. 2015.

[28] S. Yan, X. Zhou, N. Yang, T. D. Abhayapala, and A. L. Swindlehurst, "Channel training design in full-duplex wiretap channels to enhance physical layer security," in *Proc. IEEE ICC*, May 2017, pp. 1–6.

[29] Z. Hasan, H. Boostanimehr, and V. K. Bhargava, "Green cellular networks: A survey, some research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 524–540, 2011, Nov. 03.

[30] Y. Chen, S. Zhang, S. Xu, and G. Y. Li, "Fundamental trade-offs on green wireless networks," *IEEE Commun. Magazine*, vol. 49, no. 6, pp. 30–37, 2011, June 2007.

[31] L. R. Varshney, "Transporting information and energy simultaneously", in *Proc. IEEE ISIT*, July 2008, pp. 1612–1616.

[32] P. Grover and A. Sahai, "Shannon meets Tesla: Wireless information and power transfer," in *Proc. 2010 IEEE ISIT*, June 2010, pp. 2363–2367.

[33] M. Sinaie, P. H. Lin, A. Zappone, P. Azmi, and E. A. Jorswieck, "Resource

allocation in OFDM-based SWIPT with statistical delay constraints," in *Proc. IEEE Globecom Workshops*, Dec. 2017, pp. 1-6.

[34] S. Wang, M. Xia, and Y. C. Wu, "Space-time signal optimization for SWIPT: Linear versus nonlinear energy harvesting model," *IEEE Commun. Letters*, vol. 22, no. 2, pp. 408–411, Feb. 2018.

[35] Y. Chen, Z. Xie, and N. Zhao, "Energy analysis of co-channel harvesting in wireless networks," *IEEE Commun. Letters*, vol. 22, no. 3, pp. 530–533, Mar. 2018.

[36] Z. Xie, Y. Chen, Y. Gao, Y. Wang, and Y. Su, "Wireless powered communication networks using peer harvesting," *IEEE Access*, vol. 5, pp. 3454–3464, Feb. 2017.

[37] Z. Xie, Y. Chen, and Y. Gao, "Joint iterative interference alignment and energy harvesting for multi-user networks," *IEEE Wireless Commun. Letters*, vol. 4, no. 6, pp. 597–600, Dec. 2015.

[38] L. Liu, R. Zhang, and K. C. Chua, "Secrecy wireless information and power transfer with MISO beamforming," *IEEE Trans. Signal Process.*, vol. 62, no. 7, pp. 1850–1863, Oct. 2014.

[39] Q. Zhang, X. Huang, Q. Li, and J. Qin, "Cooperative jamming aided robust secure transmission for wireless information and power transfer in MISO channels," *IEEE Trans. Commun.*, vol. 63, no. 3, pp. 906–915, Mar. 2015.

[40] W. Liu, X. Zhou, S. Durrani, and P. Popovski, "Secure communication with a wireless-powered friendly jammer," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 401–415, Jan. 2016.

[41] Z. Chu, Z. Zhu, M. Johnston, and S. Y. L. Goff, "Simultaneous wireless information power transfer for MISO secrecy channel," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 6913–6925, Sept. 2016.

[42] N. Zhao *et al.*, "Artificial noise assisted secure interference networks with wireless power transfer," *IEEE Trans. Veh. Technol.*, vol. 67, no. 2, pp. 1087–1098, Feb. 2018.

[43] Y. Chen, D. B. D. Costa, and H. Ding, "Interference analysis in wireless power transfer," *IEEE Commun. Letters*, vol. 21, no. 10, pp. 2318–2321, Mar. 2017.

[44] X. Li, Y. Sun, F. Yu, and N. Zhao, "Antenna selection and power splitting for simultaneous wireless information and power transfer in interference alignment networks," in *Proc. IEEE Globecom*, Dec. 2014, pp. 2667–2672.

[45] M. Z. Win, L. Ruan, A. Rabbachin, Y. Shen, and A. Conti, "Multi-tier network secrecy in the ether," *IEEE Commun. Magazine*, vol. 53, no. 6, pp. 28–32, June 2015.

[46] N. Zhao *et al.*, "Exploiting interference for energy harvesting: A survey, research issues and challenges," *IEEE Access*, vol. 5, pp. 10403–10421, June 2017.

[47] 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, May 2016.

[48] 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, May 2016.

[49] 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, Aug. 2016.

[50] 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, Oct. 2010.

[51] 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, June 2011.

[52] L. Zheng, L. Sang, J. Liu, B. Lu, and Z. Dong, "Maximising the degrees of freedom of the physical-layer secured relay networks with artificial jamming," *IET Commun.*, vol. 12, no. 6, pp. 665–671, Apr. 2018.

[53] I. Nikoloska, N. Zlatanov, Z. Hadzi-Velkov, and R. Zhang, "On the secrecy capacity of a full-duplex wirelessly powered communication system," *IEEE Trans. Wireless Commun.*, vol. 18, no. 11, pp. 5424–5439, 2019.

Zhibin Xie received the M.E. degree in Pattern Recognition and Intelligent Systems in 2007, and the Ph.D. degree in Communication and Information Systems in 2009, from Northeastern University, Shenyang, China. He is working as a Professor currently in the School of Electronic and Information, Jiangsu University of Science and Technology, Zhenjiang, China. His current research interests include green communication, cognitive radio, and heterogeneous networks.
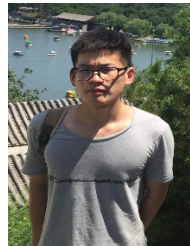
Xinquan Geng received the M.E. degree in Signal and Information Processing from Jiangsu University of Science and Technology, Zhenjiang, China, in 2018. His current research interests include interference alignment and energy harvesting.

Yunfei Chen is working as an Associate Professor in the School of Engineering at the University of Warwick, Coventry, UK. He received his B.E. and M.E. degrees from Shanghai Jiaotong University, Shanghai, China, in 1998 and 2001, respectively. He received his Ph.D. degree from University of Alberta, Canada, in 2006. His current research interests include cognitive radios, energy harvesting, wireless relaying, and performance analysis.

Kening Song received the M.E. degree in Computer Science and Technology from Shenyang Institute of Aeronautical Engineering, Sehnyang, China, in 2008. His current research interests include pattern recognition and the signal processing in communication network.

Benjamin Panful received the M.E. degree in Information and Communication Engineering from Jiangsu University of Science and Technology, Zhenjiang, China, in 2019. His current research interest is wireless sensor network.
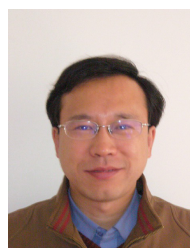
Yajun Wang received Ph.D. degree in Electronic Engineering from Shanghai Jiao Tong University, Shanghai, P. R. China in 2011. He is currently an Associate Professor in the Department of Information and Computing Sciences, Jiangsu University of Science and Technology, Zhenjiang, China. His research interests include OFDM, MIMO-OFDM systems, signal processing, communications theory, relaying networks, network coding, MIMO transceiver design, cooperative communications, 5G cellular systems and application of optimization theory and algorithms to wireless communications.
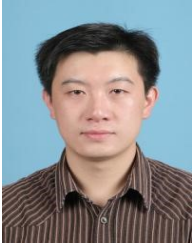
Yinjie Su is working as an Associate Professor in the School of Electronic and Information, Jiangsu University of Science and Technology. His research interests include next generation wireless communication systems, cognitive radio networks, cooperative communication, and MIMO techniques.

Zhenkai Zhang is working as an Associate Professor in the in the School of Electronic and Information, Jiangsu University of Science and Technology, Zhenjiang, China. His research interests include optimization, target detection, and radar and communication integration.
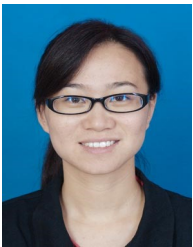
Ying Hu is working as an Associate Professor in the School of Electronic and Information, Jiangsu University of Science and Technology. Her research interests include next generation wireless communication systems, relay communication, and MIMO-OFDM techniques.