IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 15, 2017 accepted March 5, 2017, date of publication March 15, 2017, date of current version April 24, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2682838

Destination Assisted Jamming and Beamforming for Improving the Security of AF Relay Systems

NIAN OUYANG[1], XUE-QIN JIANG[1], (Member, IEEE), ENJIAN BAI[1], AND HUI-MING WANG[2], (Senior Member, IEEE)

[1]Donghua University, Shanghai 201620, China
[2]Xi'an Jiaotong University, Xi'an 710049, China

Corresponding author: E. Bai (baiej@dhu.edu.cn)

This work was supported in part by National Natural Science Foundation of China under Grant 61671143, in part by Shanghai Rising-Star Program under Grant 15QA1400100, and in part by Innovation Program of Shanghai Municipal Education Commission under Grant 15ZZ03.

ABSTRACT In this paper, we propose a destination-assisted jamming and beamforming (DAJB) scheme for physical layer security in a one-way cooperative amplify-and-forward (AF) relay communication system. The system model consists of one source, one destination, one eavesdropper, and N relay nodes, with the individual power constraint of each relay node and the destination-assisted jamming node as well as unknown instantaneous channel state information (CSI) of the eavesdropper. Due to the half-duplex constraint of the relay nodes, there are two phases in our proposed DAJB scheme. In the first phase, the source node broadcasts information signal and all N relay nodes listen simultaneously. In the meantime, the destination node transmits the jamming signal to confuse the potential eavesdropper. In the second phase, all N relay nodes amplify and forward the received signals, covered by the artificial noise (AN), to the destination using the distributed beamforming technology. The optimal beamformer weights and power allocation are obtained by solving the second-order convex cone programming (SOCP) together with a linear programming (LP) problem. Furthermore, the performance of the DAJB scheme is analyzed in terms of the achievable secrecy rate. Compared with the scheme that selects a relay node as the jammer, we obtain larger power gain to achieve higher secrecy rates. Finally, the simulation results verify that the DAJB scheme greatly improves the secrecy rate of a one-way cooperative AF relay communication system.

INDEX TERMS Jamming, beamforming, artificial noise (AN), amplify-and-forward (AF), secrecy rate.

I. INTRODUCTION

Because of the broadcast nature of the wireless communication system, the confidential messages can be received by the legitimate users or wiretapped by the unfriendly eavesdroppers as long as they are located in the coverage area of a transmission. Thus, it can be seen that information security is crucial to protect our privacy. In [1], Wyner showed that in the discrete memoryless channel, if each eavesdropper's channel is a degraded version of the main channel, we can always use channel coding to prevent eavesdroppers from getting any information from the transmitted signals while the legitimate users are able to decode signals correctly. The upper limit of the code rate of this channel coding is defined as the secrecy capacity which can be increased by decreasing the capacity of eavesdropper channel.

Commonly, for a wireless communication system with all users provided with only a single antenna, we can apply cooperative jamming [2]–[6] and cooperative beamforming [7]–[11] methods to multiple nodes. The former assists to degrade the condition of eavesdropper's channel, while the latter helps to enhance the channel quality towards the legitimate users. Moreover, in [12] these two methods are combined to secure the one-way cooperative amplify-and-forward (AF) relay communication system. In this scheme, one jamming node is selected from N relay nodes to send the jamming signal in the whole process of transmission when the remaining $N-1$ relay nodes amplify and forward the source signal. Although, this joint cooperative jamming and beamforming (JCJB) scheme can provide a good secrecy rate, it sacrifices one relay node and the corresponding power gain. On the other hand, utilizing one or more relays for jamming would require inter-relay channel state information (CSI) at the relays.

In order to make use of all the relay nodes to amplify and forward the source signal, in this paper we propose a destination assisted jamming and beamforming (DAJB) scheme for

the security of an AF based relay communication system. Due to the half-duplex constraint of the relay nodes, our proposed scheme includes two phases, i.e., broadcasting phase and amplify-and-forwarding phase. It is very probably for the eavesdroppers to wiretap the information during these two phases. Therefore, in the first phase, the destination transmits jamming signal to confuse the eavesdroppers as a jammer, while all the relay nodes will listen to the source node. In the second phase, due to unknown CSI of the eavesdropper, artificial noise (AN) is used to cover amplify-and-forwarded signals to avoid information leakage. The contributions of our work are as follows:

- Our proposed DAJB scheme takes full advantage of all the relay nodes to increase the secrecy rate without inter-relay CSI.
- The effects of total power, power constraint of destination assisted jammer and threshold of the received SNR on secrecy rate are analyzed.

We note that in [13]–[15] the destination is also used as a jammer to confuse the eavesdropper. However, it worth noting that there are some differences between our scheme and the schemes proposed in [13]–[15] as follows:

- In [13], the best of all the relay nodes is selected to decode-and-forward the source signals and cooperate with the source to jam the eavesdropper without influencing the destination. Furthermore, it assumes in [13] that the main and wiretap channels are noiseless. However, in our proposed scheme, the amplify-and-forward protocol is considered and the main and wiretap channels in our system are not noiseless.
- The relays use the zero-forcing beamforming to avoid leaking the information to the eavesdropper in [14], while we use the jamming and beamforming technologies.
- In [15], the destination and the helpers send jamming signals to the source simultaneously in the broadcasting phase. Moreover, there is a line-of-sight channel between the source and the destination without considering any relay nodes. However, our proposed scheme just utilizes the destination to transmit the jamming signal and there is no direct link between the source and the destination.

The remainder of this paper is organized as follows. In Section II, we provide the system model of our DAJB scheme. In Section III, we study the achievable maximum secrecy rate of our proposed scheme. In Section IV, we provide the simulation results to demonstrate the good security performance of the proposed scheme. Finally, Section V concludes the paper.

Notation: The following notations are utilized throughout the paper. Bold upper case letters represent matrices, while bold lower case letters denote vectors. $\max[a]^+$ is equal to the value of $\max(a, 0)$. $(\cdot)^*$, $(\cdot)^T$ and $(\cdot)^\dagger$ indicate the conjugate, the transpose and the conjugate transpose operation, respectively. $diag(\cdot)$ denotes a diagonal matrix. $[\cdot]^{(i)}$ denotes the i-th row of a matrix, while $[\cdot]_{(i)}$ means the i-th element of a vector. Besides, $[\cdot]_{(m,i)}$ indicates the (m,i)-th component of a matrix. Furthermore, $\boldsymbol{I}_i$ denotes a $(i \times i)$ identity matrix and $\boldsymbol{a}_{opt}$ denotes the optimal value of $\boldsymbol{a}$.

II. SYSTEM MODEL

We consider an AF wireless cooperative relay communication system as depicted in Fig.1, which includes a source node $\mathbb{S}$, a destination node $\mathbb{D}$, an eavesdropper node $\mathbb{E}$ and N friendly relay nodes $\mathbb{R}_i$, $i = 1, 2, \cdots, N$. The source node, the destination node and all the relay nodes are only equipped with a single antenna. Assume that there is no direct link between the source and the destination due to the shadowing and the fading effects, and we do not know the CSI of the eavesdropper. The channels between these nodes are the quasi-stationary flat-fading channel. The characters $\boldsymbol{f}_R, \boldsymbol{f}_E, \boldsymbol{c}_E, \boldsymbol{g}_E, \boldsymbol{h}_R$ and $\boldsymbol{g}_R$ represent the channel coefficients between the source $\mathbb{S}$ and the relay $\mathbb{R}$, the source $\mathbb{S}$ and the eavesdropper $\mathbb{E}$, the relay $\mathbb{R}$ and the eavesdropper $\mathbb{E}$, the destination $\mathbb{D}$ and the eavesdropper $\mathbb{E}$, the relay $\mathbb{R}$ and the destination $\mathbb{D}$, respectively.

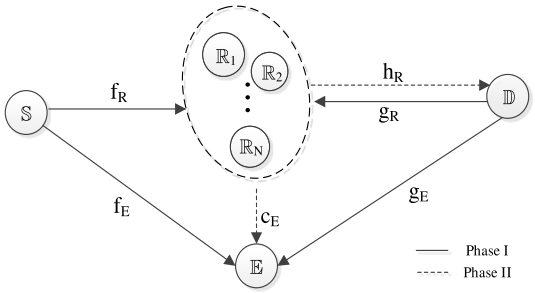

FIGURE 1. DAJB scheme, where the solid and the dash lines denote the transmissions in the first and the second phase, respectively.

The relay nodes are half duplex, i.e., each relay just need to receive the source signal in the first phase before amplify-and-forwarding it in the second phase. In[16] and [17], the authors extend the Wyner's discrete memoryless wiretap channel model to the Gaussian wiretap channel, which is proved that the secrecy rate C_s is the difference between the capacity of the source-destination channel and that of the source-eavesdropper channel. Therefore, the achievable maximum secrecy rate is

$$C_s = \max[I(y_D; s) - I(\boldsymbol{y}_E; s)]^+, \tag{1}$$

where $I(y_D; s)$ and $I(\boldsymbol{y}_E; s)$ denote the mutual information of the source-destination channel and the source-eavesdropper channel. Let γ_D and γ_E denote the corresponding signal-to-noise ratio (SNR). $I(y_D; s)$ and $I(\boldsymbol{y}_E; s)$ can be calculated, respectively, by

$$I(y_D; s) = \frac{1}{2}\log_2(1 + \gamma_D), \tag{2}$$

$$I(\boldsymbol{y}_E; s) = \frac{1}{2}\log_2(1 + \gamma_E). \tag{3}$$

In this paper, we will utilize the destination node to send the jamming signal to cover the information transmission in

the first phase. On one hand, the destination assisted jamming scheme can make the best of all the relay nodes to amplify and forward the signals to the destination and further increase the secrecy rate. On the other hand, utilizing one or more relays for jamming would require inter-relay CSI at the relays. However, the destination assisted jamming scheme do not require inter-relay CSI.

III. SECRECY RATES WITHOUT EAVESDROPPER's CSI

In this section, the DAJB scheme is introduced. Then the system secrecy rate is analyzed. Finally, the optimization methods for obtaining the optimal beamformer weights and the power allocation are also presented and discussed.

A. THE PROPOSED DAJB SCHEME

There are two phases in our scheme. During the first phase, the source $\mathbb{S}$ broadcasts the source signal s and all N relay nodes listen to the signal. In the meantime, the destination $\mathbb{D}$ transmits the jamming signal z_J to cover the information transmission, simultaneously. The received signals at $\mathbb{R}_i$, $\boldsymbol{y}_R \triangleq [y_{(R,1)}, y_{(R,2)}, \cdots, y_{(R,N)}]^T$ and signals at the eavesdropper $\mathbb{E}$, $y_E^{(1)}$, are respectively

$$\boldsymbol{y}_R = \sqrt{P_S}\boldsymbol{f}_R s + \sqrt{P_Z}\boldsymbol{g}_R z_J + \boldsymbol{n}_R, \tag{4}$$

$$y_E^{(1)} = \sqrt{P_S} f_E s + \sqrt{P_Z} g_E z_J + n_E^{(1)}, \tag{5}$$

where P_S and P_Z are the transmit powers of the source $\mathbb{S}$ and the destination $\mathbb{D}$, respectively. The jamming signal z_J is complex Gaussian random variables. $\boldsymbol{n}_R$ and $n_E^{(1)}$ are both time-spatially white independent complex Gaussian random variables with zero mean and variance σ^2 at the relay $\mathbb{R}$ and the eavesdropper $\mathbb{E}$, respectively. Besides, the powers of s and z_J are normalized as $E\{|s|^2\} = E\{|z_J|^2\} = 1$.

During the second phase, the relay $\mathbb{R}$ amplify and forward the received signals $\boldsymbol{y}_R$ using the distributed beamforming technology to the destination $\mathbb{D}$. Obviously, the eavesdropper $\mathbb{E}$ has the opportunity to eavesdrop the source information signal in this phase. Furthermore, it is difficult to do any optimization to avoid leaking the information to the passive eavesdropper $\mathbb{E}$ while the CSI of source-eavesdropper channel is unknown. In order to degrade the eavesdropper's channel condition, all N relay nodes send ANs to cover the concurrent information bearing signals $\boldsymbol{y}_R$ to the destination $\mathbb{D}$ in this phase. Therefore, the signals transmitted at the relay $\mathbb{R}$ are given by

$$\boldsymbol{x}_R = \boldsymbol{W}\boldsymbol{y}_R + \boldsymbol{n}_a, \tag{6}$$

where $\boldsymbol{x}_R \triangleq [x_{(R,1)}, x_{(R,2)}, \cdots, x_{(R,N)}]^T$, $\boldsymbol{W} \triangleq diag\left([w_1^*, w_2^*, \cdots, w_N^*]\right)$, which is the beamforming matrix as well and $\boldsymbol{n}_a$ are the ANs. Besides, the total power P_{sum} consumed by all the relay nodes and the destination node is formulated as

$$P_{sum} = N \times \bar{P}_{Ri} + \bar{P}_N, \tag{7}$$

which needs to satisfy the following power constraints: $E\{|x_{(R,i)}|^2\} \le \bar{P}_{Ri},\ i = 1, 2, \cdots, N$ and $P_Z \le \bar{P}_N$.

Let us define

$$\begin{aligned}
\tilde{\boldsymbol{n}}_D &= \boldsymbol{h}_R^T \boldsymbol{W}\boldsymbol{n}_R + n_D, \\
\tilde{\boldsymbol{n}}_E &= \boldsymbol{c}_E^T \boldsymbol{W}\boldsymbol{n}_R + n_E^{(2)}, \\
\boldsymbol{c}_E &= [c_{(E,1)}, c_{(E,2)}, \ldots, c_{(E,N)}]^T,
\end{aligned}$$

where n_D and $n_E^{(2)}$ are the time-spatially white independent complex Gaussian random variables at the destination $\mathbb{D}$ and the eavesdropper $\mathbb{E}$, respectively, with zero mean and variance σ^2. Then, the signals received at the destination $\mathbb{D}$ and the eavesdropper $\mathbb{E}$, respectively, are

$$y_D = \sqrt{P_S}\boldsymbol{h}_R^T \boldsymbol{W}\boldsymbol{f}_R s + \sqrt{P_Z}\boldsymbol{h}_R^T \boldsymbol{W}\boldsymbol{g}_R z_J + \boldsymbol{h}_R^T \boldsymbol{n}_a + \tilde{\boldsymbol{n}}_D, \tag{8}$$

$$y_E^{(2)} = \sqrt{P_S}\boldsymbol{c}_E^T \boldsymbol{W}\boldsymbol{f}_R s + \sqrt{P_Z}\boldsymbol{c}_E^T \boldsymbol{W}\boldsymbol{g}_R z_J + \boldsymbol{c}_E^T \boldsymbol{n}_a + \tilde{\boldsymbol{n}}_E. \tag{9}$$

The ANs $\boldsymbol{n}_a$ should be spatially isotropic as the CSI of the source-eavesdropper channel is unknown. Furthermore, ANs should not impact the destination node $\mathbb{D}$. Let $\boldsymbol{T}$ denotes the projection matrix such that $\boldsymbol{n}_a = \boldsymbol{T}\boldsymbol{z}_a$, which means each column of $\boldsymbol{T}$ is orthogonal to $\boldsymbol{h}_R^T$, i.e. $\boldsymbol{h}_R^T \boldsymbol{n}_a = 0$. It is assumed that the elements of $\boldsymbol{z}_a$ is i.i.d. Gaussian variables with zero-mean and variance $\sigma_{(z_a,j)}^2$, $j = 1, 2, \cdots, N-1$. Then, (8) can be rewritten as

$$y_D = \sqrt{P_S}\boldsymbol{w}^\dagger \boldsymbol{\phi}_{fh} s + \sqrt{P_Z}\boldsymbol{w}^\dagger \boldsymbol{\phi}_{gh} z_J + \tilde{\boldsymbol{n}}_D, \tag{10}$$

where $\boldsymbol{\phi}_{fh} \triangleq [f_{(R,1)}h_{(R,1)}, f_{(R,2)}h_{(R,2)}, \cdots, f_{(R,N)}h_{(R,N)}]^T$, $\boldsymbol{\phi}_{gh} \triangleq [g_{(R,1)}h_{(R,1)}, g_{(R,2)}h_{(R,2)}, \cdots, g_{(R,N)}h_{(R,N)}]^T$ and $\boldsymbol{w} \triangleq [w_1, w_2, ..., w_N]^T$. Combining the eavesdropped information in (5) and (9), the eavesdropped information can be represented as

$$\boldsymbol{y}_E = \begin{pmatrix} \sqrt{P_S} f_E \\ \sqrt{P_S}\boldsymbol{w}^\dagger \boldsymbol{\phi}_{fc} \end{pmatrix} s + \begin{pmatrix} \sqrt{P_Z}\boldsymbol{g}_E z_J + n_E^{(1)} \\ \sqrt{P_Z}\boldsymbol{w}^\dagger \boldsymbol{\phi}_{gc} z_J + \boldsymbol{c}_E^T \boldsymbol{n}_a + \tilde{\boldsymbol{n}}_E \end{pmatrix}, \tag{11}$$

with $\boldsymbol{\phi}_{fc} \triangleq [f_{(R,1)}c_{(E,1)}, f_{(R,2)}c_{(E,2)}, \cdots, f_{(R,N)}c_{(E,N)}]^T$ and $\boldsymbol{\phi}_{gc} \triangleq [g_{(R,1)}c_{(E,1)}, g_{(R,2)}c_{(E,2)}, \cdots, g_{(R,N)}c_{(E,N)}]^T$.

B. SECRECY RATES

Next, we will analyze the secrecy rate of the DAJB scheme and then compare it with that of the JCJB scheme. Before analyzing the secrecy rate, let us define

$$\begin{aligned}
\boldsymbol{R}_{fh} &= \boldsymbol{\phi}_{fh}\boldsymbol{\phi}_{fh}^\dagger, \\
\boldsymbol{R}_{hh} &= diag\left(|h_{(R,1)}|^2, |h_{(R,2)}|^2, \cdots, |h_{(R,N)}|^2\right), \\
\boldsymbol{R}_{gh} &= \boldsymbol{\phi}_{gh}\boldsymbol{\phi}_{gh}^\dagger, \\
\boldsymbol{R}_{fc} &= \boldsymbol{\phi}_{fc}\boldsymbol{\phi}_{fc}^\dagger, \\
\boldsymbol{R}_{gc} &= \boldsymbol{\phi}_{gc}\boldsymbol{\phi}_{gc}^\dagger, \\
\boldsymbol{R}_{cc} &= diag\left(|c_{(E,1)}|^2, |c_{(E,2)}|^2, \cdots, |c_{(E,N)}|^2\right), \\
\Lambda &= diag\left(\sigma_{(z_a,1)}^2, \sigma_{(z_a,2)}^2, \cdots, \sigma_{(z_a,N-1)}^2\right).
\end{aligned}$$

Grouping the information signal s and noise terms z_J, $\boldsymbol{n}_a$ and $\tilde{\boldsymbol{n}}_D$, we obtain the SNR at the destination as

$$\gamma_D = \frac{P_S \boldsymbol{w}^\dagger \boldsymbol{R}_{fh} \boldsymbol{w}}{\sigma^2\left(1 + \boldsymbol{w}^\dagger \boldsymbol{R}_{hh} \boldsymbol{w}\right) + P_Z \boldsymbol{w}^\dagger \boldsymbol{R}_{gh} \boldsymbol{w}}, \tag{12}$$

and the SNR in the first and the second phase at the eavesdropper as

$$\gamma_E^{(1)} = \frac{P_S|f_E|^2}{P_Z|g_E|^2+\sigma^2},$$
$$\gamma_E^{(2)} = \frac{P_S \boldsymbol{w}^\dagger \boldsymbol{R}_{fc} \boldsymbol{w}}{\sigma^2 + \boldsymbol{w}^\dagger \left(P_Z \boldsymbol{R}_{gc} + \sigma^2 \boldsymbol{R}_{cc}\right) \boldsymbol{w} + \boldsymbol{c}_E^\dagger \boldsymbol{U} \Lambda \boldsymbol{U}^\dagger \boldsymbol{c}_E},$$

respectively. Consequently, the total SNR at the eavesdropper is

$$\gamma_E = \gamma_E^{(1)} + \gamma_E^{(2)}. \tag{13}$$

Then, substituting (12) and (13) into (2) and (3) yields $I\left(y_D; s\right)$ and $I\left(\boldsymbol{y}_E; s\right)$, respectively, at the top of the next page.

C. SECRECY RATES OPTIMIZATION

In the DAJB scheme, we want to achieve the maximum secrecy rate C_s by means of searching for the optimal $\boldsymbol{w}$ and P_Z while P_S is fixed. However, we may not do any optimization to obtain the maximum C_s without eavesdropper's CSI. Hence, a suboptimal scheme will be introduced. It worth noting that this suboptimal scheme is similar to the optimization scheme in [12]. However, since our jamming signal is sent from the destination node, and the jamming signal is sent from a relay node in [12], the details of our optimization scheme is different from the optimization scheme in [12].

From (1), it is easy to see that in order to get higher C_s, we can increase $I\left(y_D; s\right)$ in (14) as shown at the bottom of this page as large as possible while reducing $I\left(\boldsymbol{y}_E; s\right)$ in (15) as shown at the bottom of this page as small as possible. Then, we should consider the following factors:

- In the first phase, the security only depends on power of the jamming signal transmitted from the destination. Therefore, we expect that P_Z is as large as possible. Hence, we let $P_Z = \bar{P}_N$.
- In the second phase, the relay nodes $\mathbb{R}$ will feedback the jamming signal to the destination, if they receive the jamming signal from the destination $\mathbb{D}$ in the first phase. Therefore, we should let $\boldsymbol{w}^\dagger \boldsymbol{\phi}_{gh} = 0$ in (14) to increase the mutual information $I\left(y_D; s\right)$ between the source and the destination.
- Let $\boldsymbol{R}_{ff} = diag\left(|f_{(R,1)}|^2, |f_{(R,2)}|^2, \cdots, |f_{(R,N)}|^2\right)$ and $\boldsymbol{R}_{gg} = diag\left(|g_{(R,1)}|^2, |g_{(R,2)}|^2, \cdots, |g_{(R,N)}|^2\right)$. In the whole two phases, the power P_R consumed by all N relay nodes can be expressed as $P_R = P_{IN} + P_{AN}$, where $P_{IN} \triangleq \boldsymbol{w}^\dagger \boldsymbol{Q} \boldsymbol{w}$ with $\boldsymbol{Q} \triangleq P_S \boldsymbol{R}_{ff} + P_Z \boldsymbol{R}_{gg} + \sigma^2 \boldsymbol{I}_N$ is employed by information transmission and $P_{AN} \triangleq E\left\{\boldsymbol{n}_a^\dagger \boldsymbol{n}_a\right\}$ is used for ANs. With limited power P_R and unknown CSI of the eavesdropper, the power P_{IN} is minimized so that more power P_{AN} can be utilized to send ANs to interfere the potential eavesdropper $\mathbb{E}$.

Consequently, (12) can be simplified to

$$\gamma_D = \frac{P_S \boldsymbol{w}^\dagger \boldsymbol{R}_{fh} \boldsymbol{w}}{\sigma^2 \left(1 + \boldsymbol{w}^\dagger \boldsymbol{R}_{hh} \boldsymbol{w}\right)}. \tag{16}$$

Then, we can get

$$I\left(y_D; s\right) = \frac{1}{2} \log\left(1 + \frac{P_S \boldsymbol{w}^\dagger \boldsymbol{R}_{fh} \boldsymbol{w}}{\sigma^2 \left(1 + \boldsymbol{w}^\dagger \boldsymbol{R}_{hh} \boldsymbol{w}\right)}\right), \tag{17}$$

which can be optimized by searching for the optimal beamformer weights $\boldsymbol{w}_{opt}$ under the constraints that $\boldsymbol{w}^\dagger \boldsymbol{\phi}_{gh} = 0$ and $P_Z = \bar{P}_N$. Mathematically, we have the following optimization problem

$$\begin{aligned} &\min\ P_{IN} \\ &s.t.\ \gamma_D \geq \zeta, \\ &\quad E\{|x_{(R,i)}|^2\} \leq \bar{P}_{Ri}, \quad i = 1, 2, \cdots, N, \end{aligned} \tag{18}$$

where ζ is the threshold of the received SNR γ_D at the destination $\mathbb{D}$ which has to meet the requirements of quality of service (QoS). Therefore, we can obtain

$$\begin{aligned} &\min_{\boldsymbol{w}}\ \boldsymbol{w}^\dagger \boldsymbol{Q} \boldsymbol{w} \\ &s.t.\ \frac{P_S \boldsymbol{w}^\dagger \boldsymbol{R}_{fh} \boldsymbol{w}}{\sigma^2 \left(1 + \boldsymbol{w}^\dagger \boldsymbol{R}_{hh} \boldsymbol{w}\right)} \geq \zeta, \quad \boldsymbol{w} = \boldsymbol{G} \boldsymbol{v}, \\ &\quad [\boldsymbol{w}\boldsymbol{w}^\dagger]_{(i,i)} [\boldsymbol{Q}]_{(i,i)} \leq \bar{P}_{Ri}, \quad i = 1, 2, \cdots, N, \end{aligned} \tag{19}$$

where the projection matrix $\boldsymbol{G}$ is onto the null space of $\boldsymbol{\phi}_{gh}$, i.e. $\boldsymbol{\phi}_{gh}^\dagger \boldsymbol{G} = 0$. The last constraint is the individual power constraint and $\bar{P}_{Ri}$ is the power constraint of i-th relay node. By substituting $\boldsymbol{w} = \boldsymbol{G}\boldsymbol{v}$ into the objective function and the other constraints of (19), we have

$$\begin{aligned} &\min_{\boldsymbol{v}}\ \boldsymbol{v}^\dagger \tilde{\boldsymbol{Q}} \boldsymbol{v} \\ &s.t.\ \boldsymbol{v}^\dagger \tilde{\boldsymbol{R}}_{fh} \boldsymbol{v} \geq \frac{\sigma^2 \zeta}{P_S} \left(1 + \boldsymbol{v}^\dagger \tilde{\boldsymbol{R}}_{hh} \boldsymbol{v}\right), \\ &\quad [\boldsymbol{G}\boldsymbol{v}\boldsymbol{v}^\dagger \boldsymbol{G}^\dagger]_{(i,i)} \leq \frac{\bar{P}_{Ri}}{[\boldsymbol{Q}]_{(i,i)}}, \quad i = 1, 2, \cdots, N, \end{aligned} \tag{20}$$

where $\tilde{\boldsymbol{Q}} \triangleq \boldsymbol{G}^\dagger \boldsymbol{Q} \boldsymbol{G}$, $\tilde{\boldsymbol{R}}_{fh} \triangleq \boldsymbol{G}^\dagger \boldsymbol{R}_{fh} \boldsymbol{G}$ and $\tilde{\boldsymbol{R}}_{hh} \triangleq \boldsymbol{G}^\dagger \boldsymbol{R}_{hh} \boldsymbol{G}$. As $\boldsymbol{Q}$ is a diagonal matrix with positive elements, $\sqrt{\boldsymbol{Q}}$ is

$$I\left(y_D; s\right) = \frac{1}{2} \log_2\left(1 + \frac{P_S \boldsymbol{w}^\dagger \boldsymbol{R}_{fh} \boldsymbol{w}}{\sigma^2 \left(1 + \boldsymbol{w}^\dagger \boldsymbol{R}_{hh} \boldsymbol{w}\right) + P_Z \boldsymbol{w}^\dagger \boldsymbol{R}_{gh} \boldsymbol{w}}\right), \tag{14}$$

$$I\left(\boldsymbol{y}_E; s\right) = \frac{1}{2} \log_2\left(1 + \frac{P_S|f_E|^2}{P_Z|g_E|^2+\sigma^2} + \frac{P_S \boldsymbol{w}^\dagger \boldsymbol{R}_{fc} \boldsymbol{w}}{\sigma^2 + \boldsymbol{w}^\dagger \left(P_Z \boldsymbol{R}_{gc} + \sigma^2 \boldsymbol{R}_{cc}\right) \boldsymbol{w} + \boldsymbol{c}_E^\dagger \boldsymbol{U} \Lambda \boldsymbol{U}^\dagger \boldsymbol{c}_E}\right), \tag{15}$$

used to denote the element-wise square root of $\boldsymbol{Q}$. Then (20) becomes

$$\begin{aligned}
&\min_{\boldsymbol{v}} \ \|\sqrt{\boldsymbol{Q}}\boldsymbol{G}\boldsymbol{v}\|^2 \\
&s.t. \ \left\| \begin{matrix} \sqrt{\boldsymbol{R}_{hh}}\boldsymbol{G}\boldsymbol{v} \\ 1 \end{matrix} \right\|^2 \leq \frac{P_S}{\sigma^2\zeta}|\boldsymbol{v}^\dagger\boldsymbol{G}^\dagger\boldsymbol{\phi}_{fh}|^2, \\
&\quad |\boldsymbol{G}^{(i)}\boldsymbol{v}| \leq \sqrt{\frac{\bar{P}_{Ri}}{[\boldsymbol{Q}]_{(i,i)}}}, \quad i = 1, 2, \cdots, N. \qquad (21)
\end{aligned}$$

Note that the constraint functions of (21) are based on Euclidean vector norm. It is similar to [12], we assume that $\boldsymbol{v}^\dagger\boldsymbol{G}^\dagger\boldsymbol{\phi}_{fh}$ is a positive real value without loss of generality. Let us define

$$\begin{aligned}
\hat{\boldsymbol{Q}} &= diag(\sqrt{\boldsymbol{Q}}\boldsymbol{G}, 0, 0), \\
\hat{\boldsymbol{R}}_{hh} &= diag(\sqrt{\boldsymbol{R}_{hh}}\boldsymbol{G}, 0, 1), \\
\tilde{\boldsymbol{v}} &\triangleq [\boldsymbol{v}^T, q, 1]^T, \\
\tilde{\boldsymbol{\phi}}_{fh}^\dagger &\triangleq [\boldsymbol{G}^\dagger\boldsymbol{\phi}_{fh}, 0, 0], \\
\tilde{\boldsymbol{G}}^{(i)} &\triangleq [\boldsymbol{G}^{(i)}, 0, 0].
\end{aligned}$$

We reformulate (21) as

$$\begin{aligned}
&\min_{\tilde{\boldsymbol{v}}} \ q \\
&s.t. \ \left\|\hat{\boldsymbol{Q}}\tilde{\boldsymbol{v}}\right\| \leq q, \\
&\quad \left\|\hat{\boldsymbol{R}}_{hh}\tilde{\boldsymbol{v}}\right\| \leq \sqrt{\frac{P_S}{\sigma^2\zeta}}\tilde{\boldsymbol{\phi}}_{fh}^\dagger\tilde{\boldsymbol{v}}, \\
&\quad |\tilde{\boldsymbol{G}}^{(i)}\tilde{\boldsymbol{v}}| \leq \sqrt{\frac{\bar{P}_{Ri}}{[\boldsymbol{Q}]_{(i,i)}}}, \quad i = 1, 2, \cdots, N, \\
&\quad [\tilde{\boldsymbol{v}}]_{(N+2)} = 1. \qquad (22)
\end{aligned}$$

It is easy to see that (22) is an seconde-order convex cone programming (SOCP) problem with linear equation constraints [18]. Because of the convexity, the optimal $\boldsymbol{v}_{opt}$ is unique and global, which may be solved by interior point methods [19].

When we obtain the optimal $\boldsymbol{v}_{opt}$, we can get $\boldsymbol{w}_{opt}$ through $\boldsymbol{w}_{opt} = \boldsymbol{G}\boldsymbol{v}_{opt}$. Then, we can calculate the power consumption of the i-th relay node $\mathbb{R}_i$ for data transmission as $P_{Ii} \triangleq [\boldsymbol{w}_{opt}\boldsymbol{w}_{opt}^\dagger]_{(i,i)}[\boldsymbol{Q}]_{(i,i)}$, $i = 1, 2, \cdots, N$ and the remaining power used for ANs as $P_{Ai} \triangleq \bar{P}_{Ri} - P_{Ii}$, $i = 1, 2, \cdots, N$. Subject to this updated power constraint, we have to maximize the ANs power P_{AN} to reduce the information leakage as much as possible. As the ANs power $P_{AN} = E\left\{\boldsymbol{n}_a^\dagger\boldsymbol{n}_a\right\} = \sum_{j=1}^{N-1}\sigma_{(z_a,j)}^2$, we have the following optimization problem

$$\begin{aligned}
&\max_{\sigma_{(z_a,j)}^2} \ \sum_{j=1}^{N-1}\sigma_{(z_a,j)}^2 \\
&s.t. \ E\left\{|[\boldsymbol{n}_a]_{(i,1)}|^2\right\} \leq P_{Ai}, \quad i = 1, 2, \cdots, N, \qquad (23)
\end{aligned}$$

where $[\boldsymbol{n}_a]_{(i,1)} = \boldsymbol{T}^{(i)}\boldsymbol{z}_a = \sum_{j=1}^{N-1} t_{(i,j)}z_{a_j}$. As z_{a_j} is i.i.d., we get $E\{|[\boldsymbol{n}_a]_{(i,1)}|^2\} = \sum_{j=1}^{N-1}|t_{(i,j)}|^2\sigma_{(z_a,j)}^2$.

Let us define

$$\begin{aligned}
\boldsymbol{\sigma} &\triangleq [\sigma_{(z_a,1)}^2, \sigma_{(z_a,2)}^2, \cdots, \sigma_{(z_a,N-1)}^2]^T, \\
\boldsymbol{p}_{AN} &= \bar{\boldsymbol{p}}_{RN} - \boldsymbol{p}_{IN}, \\
[\tilde{\boldsymbol{T}}]_{(i,j)} &\triangleq |t_{(i,j)}|^2.
\end{aligned}$$

Then, (23) is reformulated as

$$\begin{aligned}
&\max_{\sigma_{(z_a,j)}^2} \ \boldsymbol{1}^T\boldsymbol{\sigma} \\
&s.t. \ \tilde{\boldsymbol{T}}\boldsymbol{\sigma} \preceq \boldsymbol{p}_{AN}, \quad [\boldsymbol{\sigma}]_{(i,1)} \geq 0, \qquad (24)
\end{aligned}$$

where $\tilde{\boldsymbol{T}}$ is a $N \times (N-1)$ matrix and $\boldsymbol{1} = [1, 1, \cdots, 1]^T$. Furthermore, $\boldsymbol{p}_{AN}$, $\bar{\boldsymbol{p}}_{RN}$ and $\boldsymbol{p}_{IN}$ are N vector with the i-th element P_{Ai}, $\bar{P}_{Ri}$ and P_{Ii}, respectively. (24) is obviously a linear programming (LP) problem, and thus we can obtain the optimal $\boldsymbol{\sigma}_{opt}$. Consequently, we can substitute the optimal $\boldsymbol{w}_{opt}$ and $\boldsymbol{\sigma}_{opt}$ into (14) and (15) to calculate the secrecy rate (1) of the proposed scheme.

IV. SIMULATION AND DISCUSSION

In our simulations, the transmit power P_S of the source $\mathbb{S}$ is fixed to be 14 dB and the noise power σ^2 is normalized to be 0 dB. Besides, in each simulation, all channel coefficients are generated at random, which are complex Gaussian random vector with zero mean and unit covariance. Furthermore, we utilize the CVX toolbox [19] to solve the second-order convex cone programming (SOCP) problem together with linear programming (LP).

A. EFFECT OF THE TOTAL POWER P_{sum} ON SECRECY RATE

In this subsection, we explore the impact of the total power, P_{sum} in (7), on the secrecy rate. As shown in Fig. 2, the x-axis is the total power P_{sum}. It is assumed that $\bar{P}_{Ri} = P_{sum}/(N+1)$, $i = 1, 2, \cdots, N$ and $\bar{P}_N = P_{sum}/(N+1)$, which satisfies the constraints in (7), in these two schemes. We illustrate the comparison between the secrecy rates of the DAJB scheme and the JCJB scheme with varying P_{sum} in Fig. 2. It can be seen that as the total power P_{sum} increases, the secrecy rate of these two schemes increase accordingly. Furthermore, we can also see that when P_{sum} is fixed, increasing N may increase the secrecy rate. This is mainly because of the higher power gain provided by more relay nodes. Moreover, the secrecy rate of the DAJB scheme is higher than that of the JCJB scheme under the same configuration, as there is one more relay node in the DAJB scheme can be used to amplify and forward the received signals.

B. EFFECT OF THE POWER CONSTRAINT $\bar{P}_N$ ON SECRECY RATE

Here, we analyze the effect of the power constraint of the destination assisted jammer, $\bar{P}_N$, on secrecy rate. In Fig. 3, the total power P_{sum} consumed by all the relay nodes $\mathbb{R}_i$ and the destination assisted jammer $\mathbb{D}$ is fixed to be 25 dB. The x-axis is the ratio $\eta = \bar{P}_N/\bar{P}_{Ri}$ in the DAJB scheme, where $\bar{P}_{Ri}^{(DAJB)} = P_{sum}/(N+\eta)$, $i = 1, 2, \cdots, N$ and $\bar{P}_N^{(DAJB)} = \eta \times P_{sum}/(N+\eta)$ are selected while satisfying the constraints

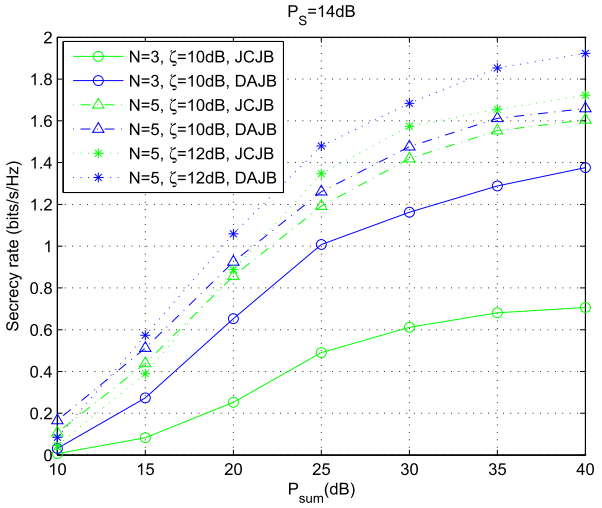

FIGURE 2. Comparison of the secrecy rate of the DAJB scheme and that of the JCJB scheme with various values of P_{sum}.

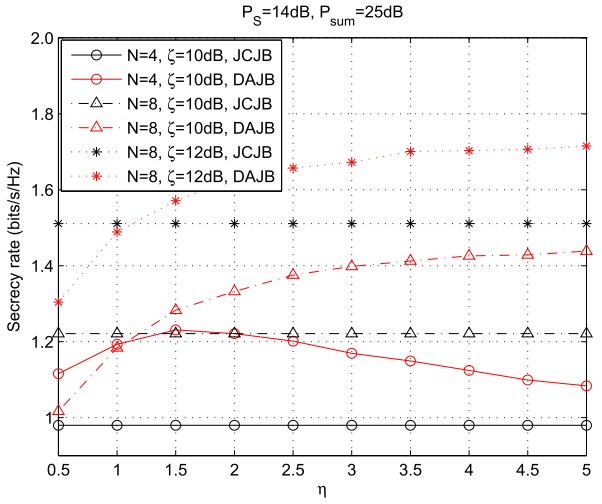

FIGURE 3. Comparison of the secrecy rate of the DAJB scheme and that of the JCJB scheme with various values of η.

in (7). In the JCJB scheme, the ratio η is fixed to 1 in the JCJB scheme, i.e. $\bar{P}_{Ri}^{(JCJB)} = P_{sum}/(N+1),\ i = 1, 2, \cdots, N$ and $\bar{P}_{N}^{(JCJB)} = P_{sum}/(N+1)$. From Fig. 3, we can see that the DAJB scheme always outperforms the JCJB scheme when $N = 4$. In addition, it is also easy to see that increasing ratio η makes the secrecy rate of the DAJB scheme increases when $N = 8$. Moreover, the secrecy rate of the DAJB scheme is higher than the JCJB scheme when the ratio η is larger than 1. Therefore, we conclude that we can choose a proper $\bar{P}_N$ to obtain the higher secrecy rate in our DAJB scheme.

C. EFFECT OF THE THRESHOLD ζ ON SECRECY RATE

Now, we analyze the effect of the threshold of received SNR at the destination, ζ, on secrecy rate. It is assumed that $\bar{P}_{Ri} = P_{sum}/(N+1),\ i = 1, 2, \cdots, N$ and $\bar{P}_N = P_{sum}/(N+1)$, in these two schemes. From Fig. 4, we can see that there is a proper value of ζ to obtain the higher secrecy rate of the DAJB

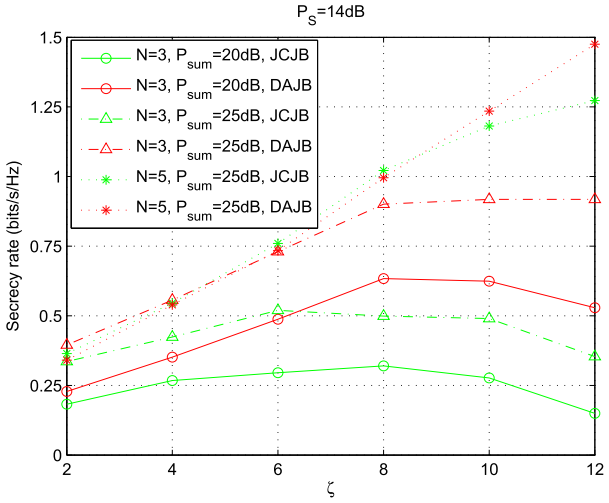

FIGURE 4. Comparison of the secrecy rate of the DAJB scheme and that of the JCJB scheme with various values of ζ.

scheme and the JCJB scheme when $N = 3$. It can also be seen that when $N = 5$ and $\zeta = 12$, the JCJB scheme has somewhat worse performance than the DAJB scheme. The higher total power P_{sum} can obviously yield the higher secrecy rate with the same configuration.

V. CONCLUSIONS

In this paper, a DAJB scheme is proposed to improve the security of an AF cooperative relay system, subject to the more practical individual power constraint of the relay and the jammer and with no eavesdropper's CSI. The source node, the destination node and all the relay nodes are only equipped with a single antenna. By solving a SOCP along with a LP problem, the optimal beamformer weights and power allocation can be attained. Finally, the comparisons of the DAJB scheme and the JCJB scheme are illustrated with various values of the total power P_{sum}, the power constraint $\bar{P}_N$ and the threshold ζ, respectively. The simulation results confirmed that the DAJB scheme greatly improves the secrecy rate of the JCJB scheme. The DAJB scheme with all the nodes equipped with multiple antennas is an open issue for future research.

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
[2] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Friendly jamming for wireless secrecy," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2010, pp. 1–6.
[3] N. Kolokotronis, K. Fytrakis, A. Katsiotis, and N. Kalouptsidis, "A cooperative jamming protocol for physical layer security in wireless networks," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, Apr. 2015, pp. 5803–5807.
[4] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.
[5] P. H. Kuo and S. L. Shieh, "Achieving physical-layer secrecy via friendly jamming with dynamic role assignment for coordinating transmitters," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2014, pp. 434–439.
[6] J. Yang, I.-M. Kim, and D. I. Kim, "Optimal cooperative jamming for

multiuser broadcast channel with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2840–2852, Jun. 2013.

[7] 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.

[8] L.-X. Li, C. Huang, and Z. Chen, "Cooperative secrecy beamforming in wiretap interference channels," *IEEE Signal Process. Lett.*, vol. 22, no. 12, pp. 2435–2439, Dec. 2015.

[9] T. M. Hoang, T. Q. Duong, H. A. Suraweera, C. Tellambura, and H. V. Poor, "Cooperative beamforming and user selection for physical layer security in relay systems," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2015, pp. 1–6.

[10] Y. Zhang, G.-B. Li, Q.-H. Du, G. Lyu, and G. Zhang, "High-rate cooperative beamforming for physical-layer security in wireless cyber-physical systems," in *Proc. IEEE Int. Conf. Commun. Workshop (ICCW)*, Jun. 2015, pp. 2622–2626.

[11] Y. Yang, Q. Li, W.-K. Ma, J. Ge, and P. C. Ching, "Cooperative secure beamforming for AF relay networks with multiple eavesdroppers," *IEEE Signal Process. Lett.*, vol. 20, no. 1, pp. 35–38, Jan. 2013.

[12] H.-M. Wang, M. Luo, X.-G. Xia, and Q. Yin, "Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's CSI," *IEEE Signal Process. Lett.*, vol. 20, no. 1, pp. 39–42, Jan. 2013.

[13] Y. Liu, J. Li, and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 4, pp. 682–694, Apr. 2013.

[14] T. Chen, "Improving physical layer security of cooperative relay networks via destination jamming," *J. Comput. Inf. Syst.*, vol. 9, no. 11, pp. 4231–4238, Jun. 2013.

[15] B. Yang, W. Wang, B. Yao, and Q. Yin, "Destination assisted secret wireless communication with cooperative helpers," *IEEE Signal Process. Lett.*, vol. 20, no. 11, pp. 1030–1033, Nov. 2013.

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

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

[18] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[19] G. Michael and B. Stephen. (Apr. 2011). *CVX Users' Guide for CVX Ver. 1.21*. [Online]. Available: http://cvxr.com/

NIAN OUYANG received the B.S. degree in telecommunication engineering from Donghua University, Shanghai, China, where she is currently pursuing the master's degree with the School of Information Science and Technology. Her main research interests include wireless communication and physical layer security.

XUE-QIN JIANG received the B.S. degree in computer science from the Nanjing Institute of Technology, Nanjing, China, and the M.S. and Ph.D. degrees in electronics engineering from Chonbuk National University, Jeonju, South Korea. He is currently an Associate Professor with the School of Information Science and Technology, Donghua University, Shanghai, China. His main research interests include wireless communication and coding theory.

ENJIAN BAI received the B.S. degree in mathematics from Qufu Normal University, and the M.S. and Ph.D. degrees in cryptography from Xidian University. He is currently an Associate Professor with the College of Information Science and Technology, Donghua University, Shanghai, China. His mainly research interests are in applied mathematics, cryptography, and fuzzy system.

HUI-MING WANG (S'07–M'10–SM'16) received the B.S. and Ph.D. degrees (Hons.) in electrical engineering from Xi'an Jiaotong University, Xi'an, China, in 2004 and 2010, respectively. He is currently a Full Professor with the Department of Information and Communications Engineering, Xi'an Jiaotong University, and the Ministry of Education Key Laboratory for Intelligent Networks and Network Security, China. From 2007 to 2008 and from 2009 to 2010, he was a Visiting Scholar with the Department of Electrical and Computer Engineering, University of Delaware, USA. He has co-authored the book *Physical Layer Security in Random Cellular Networks* (Springer, 2016). His current research interests include cooperative communication systems, physical-layer security of wireless communications, MIMO, and space-timing coding. He received the National Excellent Doctoral Dissertation Award in China in 2012, the Best Paper Award of International Conference on Wireless Communications and Signal Processing, 2011, and the Best Paper Award of the IEEE/CIC International Conference on Communications in China, 2014. He also served as the Symposium Chair of Wireless Communications and Networking in ChinaCom in 2015, the Technical Program Committee Chair of the Workshop on physical layer security in the IEEE Globecom in 2016, and the TPC members of various IEEE sponsored conferences, including the IEEE Globecom, the ICC, the WCNC, the VTC, and the PIMRC. He is currently an Associate Editor of the IEEE Access.